opentext™

ArcSight Platform

Software Version: 24.2

Administrator's Guide for the ArcSight Platform (AWS)

Document Release Date: June 2024
Software Release Date: June 2024

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2013-2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Contents

Administrator's Guide for the 24.2 ArcSight Platform - AWS Deployment 16
- Additional Documentation 16
- Contact Information 17

Where Do You Want to Start? 17
- Learn More about ArcSight Platform 17
- Install ArcSight Platform for the First Time 18
- Upgrade Your Environment 18
- Add Products or Licenses 18
- Perform Maintenance 19
- Troubleshoot Issues 19

Chapter 1: Introducing ArcSight Platform 20
- Understanding the Platform Architecture 21
- Understanding the OMT Infrastructure 22
  - OMT Installer 23
  - OMT Management Portal 23
  - Kubernetes 24
  - Master Nodes 24
  - Network File System 25
  - Worker Nodes 25
  - Virtual IP Address 25
- Understanding the Core Components 26
  - Core components 26
  - Licensing 26
  - Multi-Tenancy 27
- Understanding the Capabilities that You Can Deploy 27
  - ArcSight ESM Web App (ESM Command Center) 28
  - Intelligence 28
  - Recon 29
  - Transformation Hub 30
  - SOAR 31
- Understanding Related Components 31
  - ArcSight Database 32
  - Data Sources 33
  - Enterprise Security Manager 34
  - SMTP Server 34

Understanding Multi-tenancy 34
Providers 35
Tenants 35
Chapter 2: Planning to Install and Deploy 36
Checklist: Planning to Deploy the Platform 36
Identifying Your Installation Team 37
Reviewing the Considerations and Best Practices 37
Understanding Object Storage Options for the ArcSight Database 41
Understanding Firewall Ports for the ArcSight Platform 41
Firewall Ports for OMT Infrastructure Components 41
Firewall Ports for Deployed Capabilities 48
Firewall Ports for Supporting Components 57
Understanding Security Modes 58
Understanding the Components of Secure Communication 59
Understanding Public Key Infrastructure and TLS Components 59
Using ArcSight Platform and Products in FIPS Mode 64
Determining a Security Mode Between Components 66
Understanding Kubernetes Network Subnets 69
Chapter 2: Planning for Multi-tenancy 70
Capabilities that Support Multi-tenancy 70
Reviewing the Security Considerations of Multi-tenancy 71
Planning to Create Multiple Tenants 73
Planning to Optimize Resources in Transformation Hub 73
Planning to Update Kafka Scheduler 73
Tuning the Ingest Pool Concurrency Parameter 73
Planning to Integrate Tenants from ArcSight ESM 74
Scenario 1: New Integration of ArcSight Platform Tenants with ArcSight ESM Tenants 74
Scenario 2: ArcSight ESM Is Already Integrated With Single Tenant ArcSight Platform 74
Example: Mapping ArSight ESM Tenant Details with ArcSight Platform Tenant Details 75
Installation Method 76
Chapter 3: Creating an Amazon Web Services Deployment 77
Checklist: Creating an AWS Deployment 77
Understanding the Prerequisites for an AWS Deployment 78
Reviewing the Minimal Permissions for IAM User 79
Reviewing Storage Considerations 83

Using the AWS Deployment Worksheet 83
Using AWS Configuration Worksheets 84
Preparing the AWS Deployment Environment 87
Setting Up an AWS Virtual Network 87
Creating Security Groups 98
Creating and Configuring the Bastion 101
Downloading Installation Tools and Packages 117
Creating the Elastic File System 118
Creating Mount Targets 123
Configuring EFS for the ArcSight Suite 125
Configuring the Elastic Kubernetes Service 128
Configuring the Kubernetes Client (kubectl) 140
Applying the AWS ConfigMap to Enable Worker Nodes to Join the Cluster 141
Creating and Configuring Worker Nodes 141
Configuring Route 53 161
Uploading Product Images to the ECR 167
Uploading Image Requirements 167
Installing the Database in AWS 169
Understanding Methods for Connecting to AWS S3 Buckets 170
Launching Database Instances in AWS 171
Creating the Swap File 172
Formatting Devices for the Installation 173
Persisting Operating System Settings 175
Enabling Root Login for AWS Passwordless Communication 178
Setting Up and Installing the Database for AWS 180
(Conditional – Intelligence) Configuring Settings for Elasticsearch in AWS 188
Bootstrapping OMT 189
Preparing the OMT Deployer 189
Retrieving the ECR Credentials 190
Securing External Communication with the RE Certificate 191
191
Understanding the ArcSight Platform Certificate Authorities 192
Using an RE External Communication Certificate Signed by Your Trusted Certificate Authority 193
Creating and Validating the Route 53 Certificate 196
Configuring the Application Load Balancer (ALB) 199
Creating the Application Load Balancer 200
Retrieving the OMT Ingress Service Node Port 206
Creating the Target Group for Port 3000 207

Adding the Listener for Port 3000 ... 212
Creating a Target Group for Ports 32081 and 32080 ... 213
Adding Targets to the Target Group for Ports 32081 or 32080 ... 218
Adding a Listener for Ports 32081 and 32080 to the ALB ... 219
Directing the Route 53 Record Set to the ALB ... 221
Labeling Cloud (AWS) Worker Nodes ... 223
Installing ArcSight in AWS ... 224
Connecting to the OMT ... 225
Deploying the ArcSight Capabilities ... 226
Configuring the Deployed Capabilities ... 230
Checking Deployment Status ... 235
Checking Cluster Status ... 235
Tuning Your Deployment for Recon or Intelligence ... 237
Performing Post Installation Network Configuration ... 240
Get OMT Ingress Service Node Port for Port 5443 ... 240
Get Product Ingress Service Node Port for Port 443 ... 240
Creating a Target Group for Port 5443 and 443 ... 241
Adding Targets to the Target Group for Port 5443 and 443 ... 245
Adding a Listener for Port 5443 and 443 to the ALB ... 246
Completing the Database Kafka Scheduler Setup - AWS ... 248
Gathering Certificates for the Kafka Scheduler Setup ... 248
Enabling the Database to Ingest Events from Transformation Hub ... 250
Enabling Pod Logs in AWS ... 252

Chapter 4: Adding Additional Capabilities to an Existing Cluster ... 253
Prerequisites and Considerations for Adding Capabilities ... 253
Deploying Additional Capabilities to an Existing Cluster ... 253

Chapter 5: Post-deployment Configuration ... 256
Installing Your License Key ... 256
Report and SOAR capabilities with an ESM License ... 257
Configuring the Database with HDFS for Intelligence ... 258
Creating the First System Admin User ... 264
Enabling Integration with AWS Transformation Hub ... 264
Completing Additional Procedures for SmartConnectors, Logger, or ESM ... 265
Configuring ArcMC Parser Upgrades ... 265
Change the Number of Parser Upgrade Versions Displayed ... 266
Disable the Marketplace Connection ... 266
Checklist: Performing Regular Maintenance ... 267
Configuring Intelligence Analytics Targeted Events ... 267

Chapter 6: Integrating the Platform Into Your Environment 270
Connecting to Your SMTP Server 270
Core ArcMC SMTP 271
Configuring an External Identity Provider 271
Configuring LDAP Authentication 272
Configuring SAML Authentication 276
Integrating ESM Data and Users 279
Understanding How ESM Users Access Core 279
Enabling SSO with ESM 288
Integrating Data from ESM 291
Configuring ESM as a Transformation Hub Producer in Distributed Correlation Mode 292
Obtaining and Importing the Transformation Hub CA Certificate 293
Configuring the Filter and Destination 294
Modifying the Filter and Configuration 296
Troubleshooting Event Forwarding Throughput 296
Configuring ESM as a Transformation Hub Consumer 297
Configuring ESM as a Transformation Hub Consumer – Non-FIPS Mode 298
Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - Non-FIPS Mode 301
Configuring ESM as a Transformation Hub Consumer - FIPS Mode (Server Authentication Only) 306
Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - FIPS Mode 309
Enabling Client-side Authentication Between Transformation Hub and ESM: 309
Configuring Logger as a Transformation Hub Consumer 312
Configuring Logger as a Transformation Hub Consumer – Client Authentication in FIPS Mode 313
Configuring Logger as a Transformation Hub Consumer – Client Authentication in non-FIPS Mode 315
Configuring Logger as a Transformation Hub Consumer – No Client Authentication in FIPS Mode 318
Configuring Logger as a Transformation Hub Consumer – No Client Authentication in non-FIPS Mode with TLS 319
Configuring Logger as a Transformation Hub Consumer – No Client Authentication in non-FIPS Mode without TLS 320
Configuring Logger as a Transformation Hub Producer 320
Configuring Logger with a Transformation Hub Destination – Client Authentication in FIPS Mode 320

Configuring Logger with a Transformation Hub Destination – Client Authentication in non-FIPS Mode ... 325
Configuring Logger with a Transformation Hub Destination – No Client Authentication in FIPS Mode ... 329
Configuring Logger with a Transformation Hub Destination – No Client Authentication in non-FIPS Mode ... 332
Configuring SmartConnector as a Transformation Hub Producer ... 334
Configuring a SmartConnector with a Transformation Hub Destination without Client Authentication in non-FIPS Mode ... 334
Configuring a SmartConnector with a Transformation Hub Destination with Client Authentication in FIPS Mode ... 338
Configuring a SmartConnector with Transformation Hub Destination with Client Authentication in Non-FIPS Mode ... 345
Configuring a SmartConnector with a Transformation Hub Destination without Client Authentication in FIPS Mode ... 351
Configuring ArcMC to Manage a Transformation Hub ... 355
Standalone ArcMC Instructions ... 356
Understanding How Data is Produced and Consumed ... 357
Producing Events with SmartConnectors ... 357
Consuming Events with ESM ... 358
Consuming Events with Logger ... 359
Consuming Events with Third-Party Applications ... 361
Consuming Transformation Hub Events with Apache Hadoop ... 362
Configuring Consumers and Producers for High Availability ... 366
Understanding Data Compression ... 366
Pushing JKS files from ArcMC ... 368
Integrating Intelligence with ESM ... 369
Using the JSON Parser Files ... 369
Installing and Configuring the FlexConnectors ... 374
Performing FlexConnector Post-Installation Tasks ... 377
Installing ESM and Configuring Transformation Hub with ESM ... 378
Sending Data to Transformation Hub From Intelligence ... 378
Viewing the Intelligence Entities and Alerts Information in the ArcSight (ESM) Console ... 379
Integrating SOAR with ESM ... 379
Understanding the Prerequisites for ESM and SOAR Integration ... 380
Importing the ESM-SOAR Integration Content ... 383
Completing the Integration in SOAR ... 384
Tuning ESM and SOAR Integration ... 387

Integrating SOAR with Intelligence 388
Use Cases 389
Capabilities 393
Chapter 7: Upgrading Your Environment 395
Upgrading an AWS Installation 395
Checklist: Upgrading Your AWS Cluster 396
Upgrade Prerequisites 397
Downloading the Upgrade Packages for an AWS Deployment 398
Upgrading the Database in AWS 399
Running the ArcSight Platform OMT Upgrade (AWS) 403
Configuring Controller Services 408
Modifying Listeners on Ports 3000 and 5443 413
Upgrading Deployed Capabilities in AWS 413
Configure the Load Balancer for capabilities 418
Upgrading EKS 419
Enable the search-manager 423
Scale down logstash 423
Elasticsearch data backup 423
Verify the job status 424
Completing Post-Upgrade Tasks 438
Upgrading ESM 440
Chapter 8: Maintaining the Platform and Deployed Capabilities 441
Changing ArcSight Platform Configuration Properties 441
Managing a Multi-tenant Environment 441
Enabling Multi-tenancy 442
Create a Database User for the Provider 442
Create a Database Schema and Users for a Tenant 443
Tune Tenant Topic Settings 444
Configure Tenant Topics in Kafka Scheduler 450
Configure Customer URI in SmartConnectors 452
Tune the Ingest Pool Concurrency Parameter in ArcSight Database 453
Understanding Labels and Pods 453
Adding Labels to Worker Nodes 454
fusion:yes 455
intelligence:yes 457
intelligence-datanode:yes 459
intelligence-namenode:yes 459

intelligence-spark:yes 459
kafka:yes 460
th-platform:yes 460
th-processing:yes 461
zk:yes 461
Understanding the Pods that Do Not Have Labels 462
Understanding Pods that Run Master Nodes 462
Managing OMT Logs 462
About OMT Logs 463
Log Retention 463
Log Rotation and Deletion 464
Changing the Log Rotation or Deletion 464
Additional ConfigMap Parameters 465
Configuring the Automatic Log Cleanup Settings 467
Configuring the System Log Settings 468
Installation Log Locations 468
Log and Trace Model 469
Accessing Pod Logs 469
Configuring Log Levels 470
Uninstalling and Reinstalling the Platform 470
Undeploying a Capability 470
Uninstalling Installed Products and OMT from AWS 471
Reinstalling the Platform 474
Using REST APIs 475
Setting up Access to REST APIs 476
Setting up Access for SOAR Endpoints 476
Authenticating to and Calling REST APIs 477
For Endpoints Other than SOAR 477
For SOAR Endpoints: 480
Links to REST API Documentation 481
Retrieving the OMT Root CA 481
Retrieving the OMT Root CA from a Browser 481
Retrieving the OMT Root CA Using Command Line 482
Understanding License Keys 482
Considerations for Product Licensing 482
Understanding the Types of Licenses 483
How Your License Affects Available Features 485
How Your License Affects Data Storage Policies 487
How Data Ingestion Affects Your License 488

Creating Widgets for the Dashboard 488
Using the Widget SDK 489
Considerations for Updating the Widget Store 489
Updating resources in the worker nodes (AWS only) 489
Checklist: Updating AWS Node Resources 490
Create Launch Templates 490
Prepare the Environment 491
Backing Up the Elasticsearch Data 491
Performing the Nodes Update/Replacement 493
Managing the OMT Infrastructure 507
Accessing the OMT Management Portal 507
Managing OMT Management Portal Access 507
Changing the IP Address of a Master or Worker Node 509
Checking Kubernetes Dashboard for Status and Errors 510
Maintaining the RE Certificate 511
Method 1 - Signing the RE External Communication Certificate with Your Trusted Certificate Authority 512
515
Method 2 - Importing an Externally Created Intermediate CA 515
Maintaining Certificates 524
Diagnose and Repair the OMT Infrastructure (CDF Doctor Utility) 527
Managing the ArcSight Database 530
Monitoring the ArcSight Database 531
Understanding the ArcSight Database Installer Options 533
Configuring the Policy for Retaining Data 533
Setting the Maximum Number of Storage Groups for Tenants 535
Rebooting the ArcSight Database Cluster 536
Configuring the ArcSight Database for MinIO Storage (Examples Only) 537
Specifying Kafka Scheduler Options 547
Managing Search 548
Making Searches Case-insensitive 548
Performing a Keyword Search on Raw Event Data 548
Understanding the Schema for Events 550
Managing ArcMC 567
Managing Repositories 567
Audit Logs 583
Managing Intelligence 600
Enabling Windowed Analytics 600
Running Analytics on Demand 601

Changing Passwords for a Secure Environment 602
Changing the Elasticsearch Node Data Path 602
Enabling Elasticsearch to Start on Limited Hardware Sizing 604
Updating the Logstash Config Map for Custom Data Identifiers 605
Enabling Custom Model Support 606
Adding Support for New Devices 618
Securing HDFS for Intelligence 620
Setting an Encoding Option for the URL 630
Intelligence Data Types and Schemas 631
Managing Recon 646
Configuring Event Integrity Checks 646
Migrating Reports and Data From ArcSight Logger 648
Migrating Logger Reports to the ArcSight Platform 648
Migrating Logger Data to the ArcSight Database 652
Managing Transformation Hub 660
Maintaining a Deployment on AWS 660
Understanding the Transformation Hub Kafka Manager 673
Stream Processor Groups 691
Overriding Application Properties 698
Transformation Hub Liveness Probes 701
Migrating the NFS Server to a New Location 704
Usage: 704
Preparation 706
Migrate itom-logging PV 707
Migrate itom-monitor PV 710
Migrate itom-vol PV 712
Migrate db-single PV 714
Migrate arcsight-installer-xxxxx-arcsight-volume PV 716
Backing Up and Restoring 718
FBacking Up and Restoring Core Secrets 718
Backing Up and Restoring Configuration Data for Deployed Capabilities 720
Backing Up and Restoring the ArcSight Database 726
Backup Overview 726
Backup Terminology 727
(Conditional) Prerequisites to Configuring Database Backup 727
Backing Up and Restoring the Postgres Database 734
Chapter 9: Managing Your ArcSight Infrastructure with ArcMC 746
The User Interface 746
The Menu Bar 746

User Management Workflow 749
ArcMC Name 750
Stats (EPS In/Out) 750
Job Manager 751
Site Map 751
History Management 751
Dashboard 752
Monitoring Managed Nodes 752
Host Status Exceptions 759
Monitoring Rules 760
Topology View 780
Deployment View 781
Managing Nodes 793
Node Management 793
The Navigation Tree 794
The Management Panel 794

Updating (or Installing) the ArcMC Agent 799

Modifying logger.properties 800
Uploading Files Larger Than 100 MB under Repository 800

Installing the ArcMC Agent 802
Locations 811
Hosts 813

Permission Groups 817

Preparing to Add Transformation Hub 2.01 or Earlier as a Host 819

Preparing to Add Transformation Hub as a Host (Standalone ArcMC) 820
Generator ID Manager 829
Generator ID Management 830
Setting Up Generator ID Management 830
Getting Generator ID for Non-managed Nodes 830
Setting Generator IDs on Managed Nodes 830
The Topology View and Unmanaged Devices 831
Logger Consumption Report 833

Exporting PDF Reports 834
Managing ArcSight Products 835
Managing Connector Appliances (ConApps) 835
Managing Other ArcSight Management Centers 837
Managing Loggers 841
Managing Containers 846
Managing Connectors 860
Managing Configurations 882
Configuration Management 884
Managing Subscribers 889
Pushing a Subscriber Configuration 891
Checking Subscriber Compliance 893
Comparing Configurations 894
Configuration Management Best Practices 895
Subscriber Configuration Types 896
Logger Initial Configuration Management 918
Managing Logger Event Archives 922
Managing Logger Peers 924
Managing Transformation Hub 927
ColleDeployment Templates 931
Bulk Operations 933
Destination Runtime Parameters 945
Special Connector Configurations 952
System Administration 953
SMTP 957
Troubleshooting Your Cluster 958
Troubleshooting Issues with Your Product License 961
System Fails to Recognize a License Change 961
Conflicting Indicators about Your License 961
Erroneous Warning about Recon License 962
Send Documentation Feedback 963

Administrator's Guide for the 24.2 ArcSight Platform - AWS Deployment

The *Administrator's Guide for the ArcSight Platform* provides installation, operations, and deployment guidance for IT administrators responsible for managing ArcSight software products and components deployed on the ArcSight containerized platform version.

Additional Documentation

ArcSight Platform documentation library also includes the following resources:

- This document, *Administrator's Guide to ArcSight Platform*, which provides concepts, use cases, and contextual help for the Dashboard and user management of the Core components in ArcSight Platform.
- *Technical Requirements for ArcSight Platform 24.2*, which provides information about the hardware and software requirements for installing ArcSight Platform and the deployed capabilities.
- *Release Notes for ArcSight Platform 24.2*, which provides information about the latest release, including known issues.

For the most recent version of this guide and other ArcSight documentation resources, visit the ArcSight documentation site.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact OpenText Customer Care.

Open topic with navigation

Where Do You Want to Start?

If you are already familiar with ArcSight Platform components and functionality, you might go straight to the part of this Administrator's Guide that you need. However, if you are new to ArcSight Platform, or are unsure where to find specific information, you could use the following options as your starting point:

- Learn More about ArcSight Platform
- Install ArcSight Platform for the First Time
- Upgrade Your Environment
- Add Products or Licenses
- Perform Maintenance
- Troubleshoot Issues

Learn More about ArcSight Platform

The following topics provide descriptions of the components for ArcSight Platform and guidance regarding pertinent functionality.

- Introducing ArcSight Platform
- Choosing Your Installation Method
- Integrating the Platform Into Your Environment
- Planning to Install and Deploy
- Understanding License Keys
- Understanding Labels and Pods

- Managing OMT Logs
- Managing Your ArcSight Infrastructure with ArcMC

Install ArcSight Platform for the First Time

If you're installing the ArcSight Platform for the first time, this guide includes a lot of information. To start, we provide a planning chapter that covers many of the considerations related to your environment's setup as well as information about functionality that might affect how you manage the process. You should start with the first topic below—and keep the Planning Checklist on hand to guide you. Then, depending on the type of deployment that you want to create, select the appropriate deployment topic to read.

Before you begin the installation process, we recommend that you first thoroughly review the checklists for your chosen deployment. Note that any licensed product that you deploy will require you to also deploy the Core components and Transformation Hub capability. Also, if you purchase more licensed capabilities, you can deploy them at a later time to your ArcSight Platform environment.

- Choosing Your Installation Method
- Planning to Install and Deploy
- Checklist: Planning to Deploy the Platform
- **AWS** – Checklist: Creating an AWS Deployment
- Accessing the OMT Management Portal

Upgrade Your Environment

To upgrade your existing ArcSight Platform environment, select the topic that matches your deployment. We recommend that you review the checklist in that chapter before starting the upgrade process. Note that the ArcSight Platform includes several components that should be backed up before you upgrade your environment.

- **AWS** – Checklist: Upgrading Your AWS Cluster

Add Products or Licenses

If you have recently purchased a license for a new capability that you want to add to your deployment, see the following topics.

- Adding Additional Capabilities to an Existing Cluster
- Understanding the Capabilities that You Can Deploy
- Learn about the ArcSight Database

Note that if you're adding ArcSight Intelligence or ArcSight Recon to an environment that has neither capability, you will also need to install the ArcSight Database.

Perform Maintenance

If you want to understand how to maintain your deployment, see the following topics. Note that the ArcSight Platform includes several components that should be backed up on a regular schedule.

- Checklist: Performing Regular Maintenance
- Accessing the OMT Management Portal
- Maintaining the Platform and Deployed Capabilities
- Back up or restore a database or configuration data
- Incorporate data from SmartConnectors, Logger, and ESM

Troubleshoot Issues

If you want to troubleshoot an issue, see the following common topics. You can also review the chapter about maintaining the deployment:

- Troubleshooting Your Cluster
- Troubleshooting Issues with Your Product License
- Maintaining the Platform and Deployed Capabilities
- Understanding Labels and Pods
- Managing OMT Logs

Chapter 1: Introducing ArcSight Platform

ArcSight Platform (the Platform) enables you to deploy a combination of security, user, and entity solutions into a single cluster within the OPTIC Management Toolkit (OMT) environment. With OMT, you can add and remove product capabilities, as well as manage the workload across the installed nodes.

The Platform enables you to visualize, identify, and analyze potential threats by incorporating intelligence from the multiple layers of security sources that might be installed in your security environment.

These product capabilities might include the following:

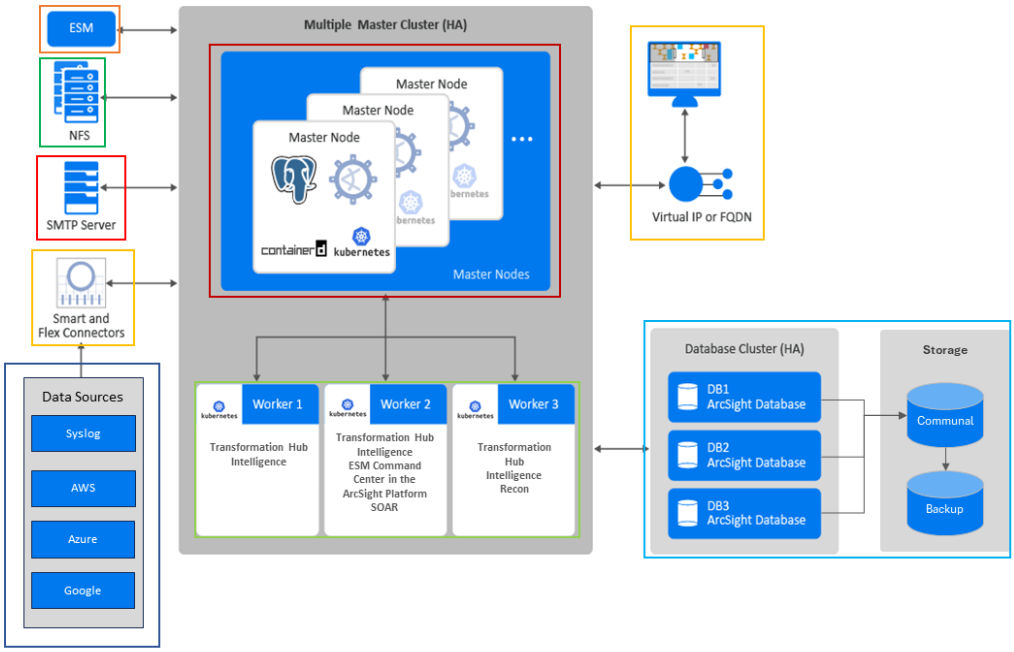
- Real-time event monitoring and correlation with data from ArcSight Enterprise Security Manager (ESM)
- Analyzing end-user behavior with ArcSight Intelligence
- Performing deep-dive investigations with ArcSight Recon
- Responding to and mitigating cyber attacks with ArcSight SOAR
- Coordinating and managing data streams with Transformation Hub

The Platform's Single Sign-On (SSO) function ensures that users can navigate among the features in the Platform or launch applications from the Platform without having to log in for each product solution.

Understanding the Platform Architecture

The Platform includes three primary elements:

- The underlying OMT infrastructure
- The capabilities you deploy into the infrastructure
- The functions and applications that support the deployed capabilities



Click components with colored outlines to learn more about each.

The following sections describe these three elements of the Platform architecture.

Although you can also deploy NetIQ Identity Intelligence in this OMT-based environment, this *Administrator's Guide* does not provide instructions for deploying or managing that capability. For more information, see the Administrator's Guide to NetIQ Identity Intelligence.

Understanding the OMT Infrastructure

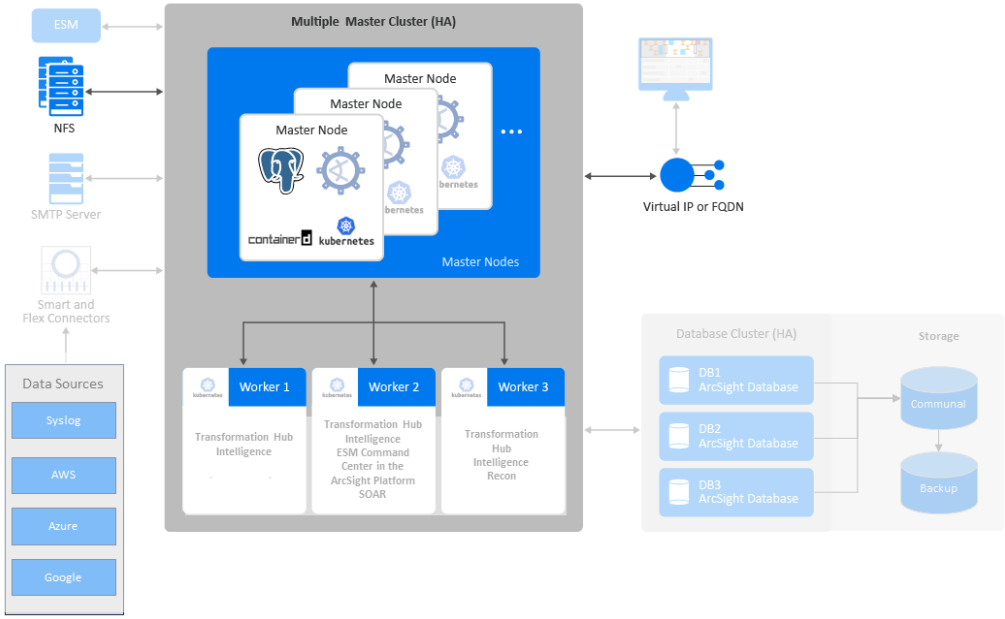
The Platform runs in the OPTIC Management Toolkit (OMT) infrastructure, which incorporates container management functions from Kubernetes. This containerized environment enables you to swiftly install and manage an integrated solution of ArcSight products in a single interface. The OMT has both an "OMT Installer" on the next page and a browser-based "OMT Management Portal" on the next page.

> You cannot use the automated installation tool for a cloud deployment.

You will also need to install additional software and components to support your security solution. Your ArcSight environment might include the containerized capabilities, which are distributed across multiple host systems, plus servers for databases and the supporting products. The number of hosts you need depends on several factors, such as the need for high availability and the size of workloads based on events per second.

The OMT architecture requires several components:

- "OMT Installer" on the next page
- "OMT Management Portal" on the next page
- "Kubernetes" on page 24
- "Master Nodes" on page 24
- "Network File System" on page 25
- "Worker Nodes" on page 25
- "Virtual IP Address" on page 25



OMT Installer

Used for installing, configuring, and upgrading the OMT infrastructure. For more information about using the OMT Installer, see the following topics:

- "Planning to Install and Deploy" on page 36
- "Installation Method" on page 76
- "Bootstrapping OMT" on page 189
- "Reinstalling the Platform" on page 474

OMT Management Portal

The Management Portal enables you to manage and reconfigure your deployed environment after the installation process is complete. You can add or remove deployed capabilities and worker nodes, as well as manage license keys.

During installation, you specify the credentials for the administrator of the Management Portal. This administrator is not the same as the admin user that you are prompted to create the first time that you log in to the Platform after installation. You'll use the Management Portal to upgrade the deployed capabilities with every Platform upgrade.

For more information about the OMT Management Portal, see the following topics:

- "Accessing the OMT Management Portal" on page 507
- "Managing OMT Management Portal Access" on page 507
- "Maintaining Certificates" on page 524

Kubernetes

Kubernetes automates deployment, scaling, maintenance, and management of the containerized capabilities across the cluster of host systems. Applications running in Kubernetes are defined as pods, which group containerized components. Kubernetes clusters use Docker containers as the pod components. A **pod** consists of one or more containers that are guaranteed to be co-located on the host server and can share resources. Each pod in Kubernetes is assigned a unique IP address within the cluster, allowing applications to use ports without the risk of conflict.

Persistent services for a pod can be defined as a volume, such as a local disk directory or a network disk, and exposed by Kubernetes to the containers in the pod to use. A cluster relies on a Network File System (NFS) as its shared persistent storage. The clusters require master and worker nodes. For more information about the Platform pods, see Understanding Labels and Pods.

For more information about Kubernetes, see the following topics:

- "Understanding Kubernetes Network Subnets" on page 69
- "Connect to Bastion and Install Software Packages" on page 112
- "Configuring the Elastic Kubernetes Service" on page 128
- "Configuring the Kubernetes Client (kubectl)" on page 140
- "Refreshing the ECR Credentials in Kubernetes" on page 661
- "Installing the Kubernetes Metrics Server" on page 662

Master Nodes

The master nodes control the Kubernetes cluster, manage the workload on the worker nodes, and direct communication across the system. You should deploy three master nodes to ensure high availability. However, you can use the Platform with a single master node.

For more information about master nodes, see the following topics:

- "Understanding Pods that Run Master Nodes" on page 462

Network File System

The Network File System (NFS) is a protocol for distributed file sharing. Some of the persistent data generated by Transformation Hub, Intelligence, and other capabilities is stored in the NFS. This data includes component configuration data for ArcSight Platform-based capabilities unrelated to event data.

For more information about the Network File System, see the following topics:

- "Migrating the NFS Server to a New Location" on page 704
- "Configuring EFS for the ArcSight Suite" on page 125
- "Cleaning or deleting NFS/EFS" on page 665

Worker Nodes

Worker nodes run the application components and perform the work in the Kubernetes cluster. For all highly available configurations, we recommend deploying a minimum of three dedicated worker nodes.

You can add and remove worker nodes from the cluster as needed. Scaling the cluster to perform more work requires additional worker nodes, all of which are managed by the master nodes. The workload assigned to each node depends on the labels assigned to them during deployment or reconfiguration after deployment.

For more information about worker nodes, see the following topics:

- "Creating and Configuring Worker Nodes" on page 141

Virtual IP Address

OMT supports high availability (HA) through load balancers and the Keepalived service. You can configure either external load balancers or Keepalived for high availability. If you have configured a virtual IP for a multi-master installation, the HA virtual IP address you defined bonds to one of the three master nodes. If a master node fails, the virtual IP address is assigned to an active master node. This setup helps to provide high availability for the cluster.

When you configure a connection to the cluster, configure the connection to use the virtual IP so that it benefits from the HA capability. One exception to this recommendation is when you are configuring a connection to Transformation Hub's Kafka, in which case you can achieve better performance by configuring the Kafka connection to connect directly to the list of worker nodes where Kafka is deployed.

Understanding the Core Components

- "Core components" below
- "Licensing" below
- "Multi-Tenancy" on the next page
- " Understanding the Core Components " above

Core components

All capabilities require that the Core components be deployed in the same cluster.

To ensure a unified solution experience, the Core components provide the elements needed for the products that you deploy in the Platform environment: user management, the Dashboard, SOAR, ArcMC, and other core services. The Core components services also support single sign-on (SSO) configuration across the capabilities, high-capacity data management, and a search engine.

The Core components enable you to add users and groups, as well as manage their roles and permissions. The *My Profile* section of user management enables users to set their preferences for features like Search. The **Dashboard** enables you to visualize, identify, and analyze potential threats by incorporating intelligence from the multiple layers of security sources that might be installed in your security environment.

Core ArcMC, the containerized version of ArcSight Management Center (ArcMC), serves as a centralized management interface to help you effectively administer and monitor Transformation Hub and the SmartConnectors. Core ArcMC communicates with the Platform by connecting to the virtual IP address or fully qualified domain name (FQDN) assigned to the primary master node in the cluster. You can configure Fusion ArcMC to manage another instance of Fusion ArcMC or to manage the standalone ArcMC product. Note that, although a standalone instance of ArcMC can manage other standalone instances of ArcMC, it cannot manage Fusion ArcMC.

For more information about the Core components, see the following topics:

- "Connecting to Your SMTP Server" on page 270
- "Integrating ESM Data and Users " on page 279

Licensing

"How Your License Affects Available Features" on page 485

Multi-Tenancy

"Managing a Multi-tenant Environment" on page 441

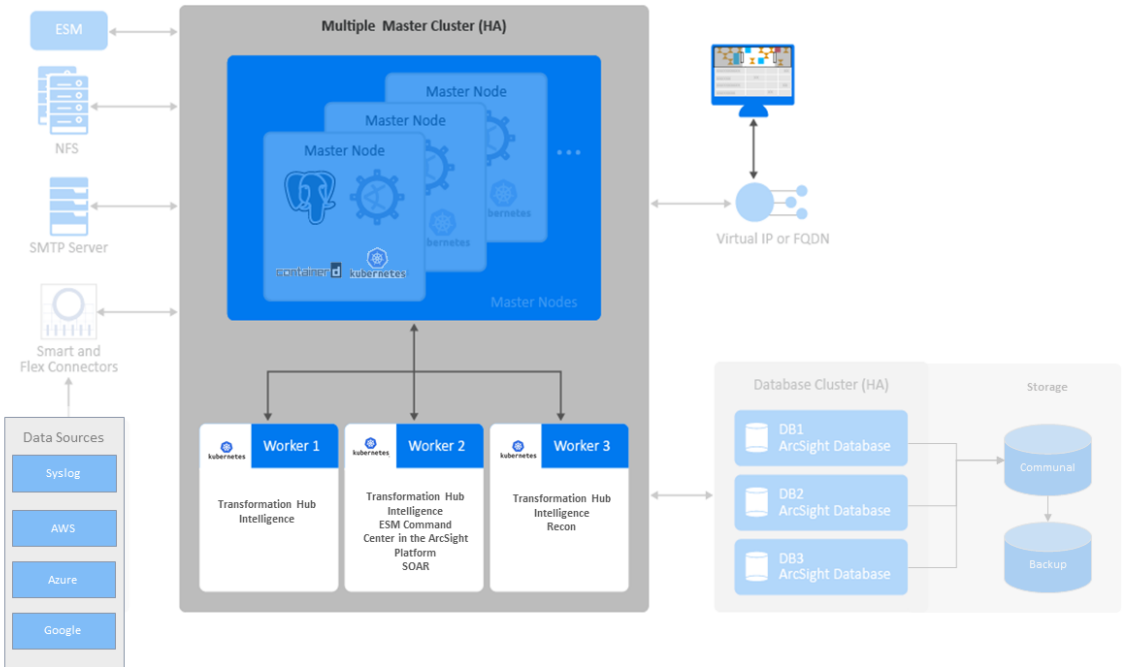
Understanding the Capabilities that You Can Deploy

The Platform infrastructure enables you to deploy a combination of container-based **capabilities**, which represent licensed products and functions that shape your ArcSight environment. Each release of the Platform supports a specific set of capabilities that you can deploy.

To perform appropriately, some capabilities that you deploy depend on the presence of additional capabilities. For example, most capabilities need the Core components because it provides the user management functions in the Platform.

> The capabilities that can be deployed in the Core components are designed to automatically integrate with each other when deployed to the same cluster. You must deploy capabilities to the same cluster for them to operate in an integrated manner.

For a complete security, user, and entity solution, you might also need to integrate software and components that are not deployed within the Core components. For example, your solution might need a database for data storage and OpenText ArcSight SmartConnectors for data collection from various data sources.



You can deploy the following capabilities in the Platform:

- "ArcSight ESM Web App (ESM Command Center)" below
- "Recon" on the next page
- "Transformation Hub " on page 30
- SOAR

Core components (formerly called Fusion) now include Layered Analytics and is a mandatory deployment. For more information on shared capabilities, see "Understanding Labels and Pods" on page 453

ArcSight ESM Web App (ESM Command Center)

The ArcSight ESM Web App (ESM Command Center in the ArcSight Platform) is a licensed product that provides widgets and dashboards that you can customize in the Dashboard feature for detecting threats to your enterprise. If you deploy "Intelligence" below in the same cluster as ESM Command Center, certain widgets will combine data from ESM and Intelligence to provide you greater insight into events and entity behavior.

With Transformation Hub deployed in the same cluster, ESM can receive event data for dashboarding and further correlation. The Core components must be deployed in the same cluster for this to work.

For more information about ESM Command Center, see the following topics:

- "Integrating ESM Data and Users " on page 279
- "Integrating Data from ESM" on page 291
- "Understanding How Data is Produced and Consumed " on page 357
- "Consuming Events with ESM " on page 358
- "Upgrading ESM" on page 440

Intelligence

ArcSight Intelligence provides a market-leading analytics platform, using unsupervised online machine learning to identify unknown threats like insider threats or targeted outside attacks such as APTs. These types of threats simply cannot be identified by searching for a known “bad signature.” Unsupervised machine learning gives threat hunters a high-quality set of leads to help them identify these elusive threats. The analytics platform in ArcSight Intelligence uses:

- ArcSight SmartConnectors
- Supporting Active Directory/Authentication data

- Web proxy data
- Additional data sources

In addition, you can use FlexConnectors to pull ArcSight Intelligence analytical results and push them into ESM for higher accuracy correlation rules that leverage unsupervised learning anomalies, as well as correlation rule filtering using top risky entity lists.

If you deploy "ArcSight ESM Web App (ESM Command Center)" on the previous page in the same cluster as the ArcSight Intelligence capability, certain widgets will combine data from ESM and ArcSight Intelligence to provide you greater insight into events and entity behavior. This capability requires the Core components and Transformation Hub to be deployed in the same cluster, and the ArcSight Database.

For more information about Intelligence, see the following topics:

- "Prerequisites and Considerations for Adding Capabilities" on page 253
- "Deploying Additional Capabilities to an Existing Cluster" on page 253
- "Configuring Intelligence Analytics Targeted Events" on page 267
- "Integrating Intelligence with ESM" on page 369
- "Integrating SOAR with Intelligence" on page 388
- "Changing ArcSight Platform Configuration Properties " on page 441
- "Undeploying a Capability" on page 470
- "Reinstalling the Platform" on page 474
- "How Your License Affects Data Storage Policies" on page 487
- "Managing Intelligence " on page 600

Recon

ArcSight Recon, also known as *Log Management and Compliance*, is a licensed product that enables you to search, analyze, and visualize machine-generated data gathered from web sites, applications, sensors, and devices that make up your monitored network. Recon indexes the events from your data source so that you can view and search them. The intuitive search language makes it easy to formulate queries. You can use the large set of dashboards and reports available in the Reports Portal to monitor and identify vulnerabilities and threats in your enterprise.

Recon integrates with "Transformation Hub " on the next page for event transport. Recon also can integrate with ESM to receive alerts and start the investigation process. This capability requires the Core components and Transformation Hub to be deployed in the same cluster, and the ArcSight Database.

For more information about Recon, see the following topics:

- "Configuring the Deployed Capabilities" on page 230
- "Prerequisites and Considerations for Adding Capabilities" on page 253
- "Changing ArcSight Platform Configuration Properties " on page 441
- "How Your License Affects Available Features" on page 485
- "Managing Recon " on page 646

Transformation Hub

Transformation Hub is a licensed product that lets you take advantage of scalable, high-throughput, multi-broker clusters for publishing and subscribing to event data. It coordinates and manages data streams, which enables your environment to scale, and opens events to third-party data solutions.

Transformation Hub ingests, enriches, normalizes, then routes event data from data producers to connections between existing data lakes, analytics platforms, and other security technologies and the multiple systems within the Security Operations Center (SOC).

Transformation Hub can seamlessly broker data from any source and to any destination. Its architecture is based on Apache Kafka and it supports native Hadoop Distributed File System (HDFS) capabilities, enabling both the ArcSight Logger and ArcSight Recon technologies to push to HDFS for long-term, low-cost storage. This architecture reduces the overall ArcSight infrastructure footprint, scales event ingestion using built-in capabilities, and greatly simplifies upgrades to newer Transformation Hub releases. It also positions the Platform to support an analytics streaming plug-in framework, supporting automated machine learning and artificial intelligence engines for data source onboarding, event enrichment, and detection and attribution of entities and actors.

This capability requires the Core components to be deployed in the same cluster.

For more information about Transformation Hub, see the following topics:

- "Configuring the Deployed Capabilities" on page 230
- "Integrating the Platform Into Your Environment" on page 270
- "Understanding How Data is Produced and Consumed " on page 357
- "How Your License Affects Available Features" on page 485
- "Managing Transformation Hub" on page 927
- "Backing Up and Restoring Configuration Data for Deployed Capabilities" on page 720

SOAR

ArcSight SOAR delivers an automated case response solution for repetitive security events and imparts a seamless security management experience by performing faster threat detection and remediation.

Existing cybersecurity landscape presents lots of challenges to the organizations including:

Attack Speed: Modern attacks are becoming faster and are often automated.

Attack Volume: Organizations receive over 300 cyber alerts daily, and investigating and responding to each alert can take up to 8 hours.

Disparate Tools: SOC analysts juggle 15-20 different tools daily, making it challenging for Tier-1 analysts to effectively investigate and respond.

Lack of Single Pane of Glass: There's no centralized view of investigation and response activities, leading to confusion about who is handling which case.

KPIs and Metrics Gap: Many SOCs struggle to define relevant KPIs and metrics due to a lack of investigative practices.

Cybersecurity Skill Shortage: The industry faces a severe shortage of experts, with 350,000 vacant positions in the U.S. alone and an expected shortfall of 3.5 million cyber experts.

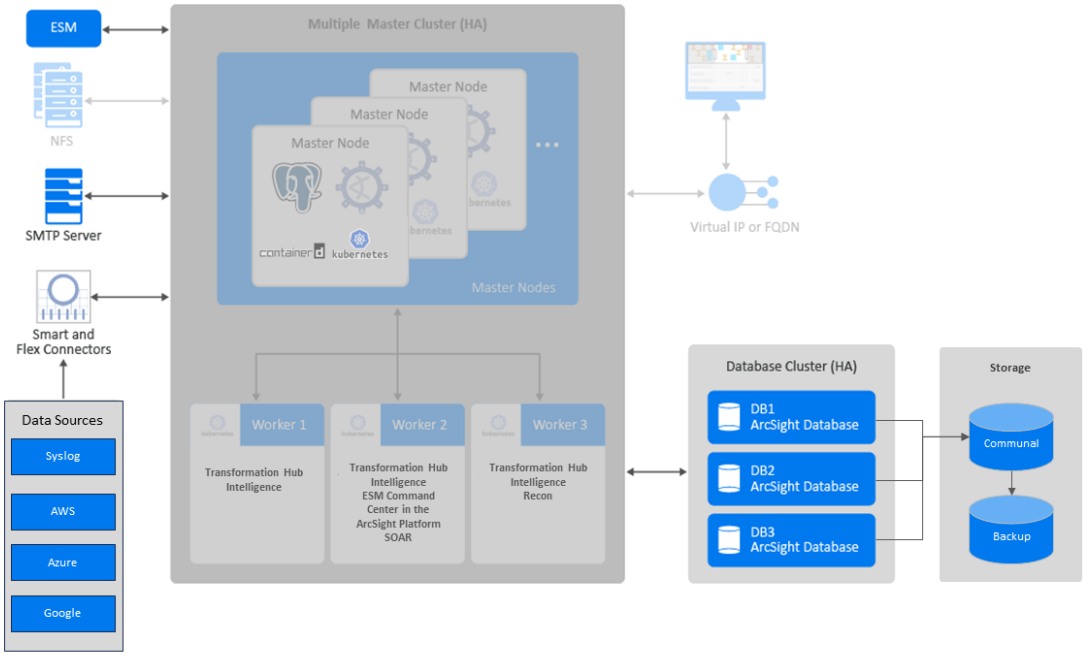
The main value proposition of SOAR lies in assisting your organization for human and machine-led analysis of the alerts, and leveraging an automated solution for threat response and remediation.

SOAR is fully programmable and can easily integrate with the existing technology stack of your organization. This application is capable to meet security teams' unique needs, and enables multiple forms of automation, analyst augmentation, collaborative investigation and response through an intuitive interface.

For more information on SOAR and its features, see Responding to Threats.

Understanding Related Components

The capabilities you deploy in the Platform depend on functions and applications installed in your environment. For example, Transformation Hub consumes data from a wide variety of collectors and connectors before passing that content to ESM and other products. Recon and Intelligence need the ArcSight Database to store their data.

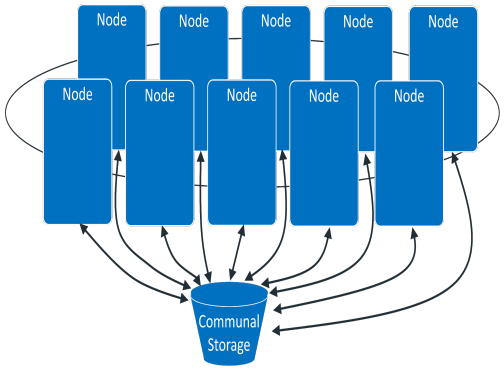


- "ArcSight Database" below
- "Data Sources" on the next page
- "Enterprise Security Manager" on page 34
- "SMTP Server" on page 34

ArcSight Database

The ArcSight Database stores all collected events and provides event searches and analysis capabilities. The Database keeps the primary copy of your data in **Communal Storage**, and the local cache serves as the secondary copy. Communal storage is the database's centralized storage location, shared among the database nodes. This means that adding and removing nodes does not redistribute the primary copy. Communal storage is based on an object store, such as Amazon's S3 service in the cloud or an S3-compatible object store in an Off-cloud deployment. The database relies on the object store to maintain the durable copy of the data.

Within communal storage, data is divided into portions called **shards**. The Database uses the shards to divide the data among the nodes. Nodes subscribe to particular shards, with subscriptions balanced among the nodes. When loading or querying data, each node is responsible for the data in the shards that it subscribes to.



This shared storage model enables elasticity, meaning it is both time and cost-effective to adapt the cluster resources to fit the usage pattern of the cluster. If a node goes down, other nodes are not impacted because of shared storage. Node restarts are fast and no recovery is needed. Thus, you do not need to explicitly keep track of, or load/unload long-term event data. The Database can bring the data to the cache on demand automatically and then move the data out when not in use. To expand communal storage, you can purchase additional storage devices rather than purchasing additional CPU and memory.

For more information about the Database, see the following topics:

- "Understanding Object Storage Options for the ArcSight Database" on page 41
- "Installing the Database in AWS " on page 169
- "Configuring the Deployed Capabilities" on page 230
- "Changing ArcSight Platform Configuration Properties " on page 441
- "Backing Up and Restoring the ArcSight Database" on page 726

Data Sources

The deployed capabilities incorporate data from a variety of sources.

- **SmartConnectors** collect events from supported data sources, normalize those events, then send them to the Transformation Hub's Kafka cluster.
  - When collecting data and sending it to Transformation Hub, the SmartConnector normalizes the values (such as severity, priority, and time zone) into the common format and normalizes the data structure into the common schema.
  - Next, the connectors filter and aggregate events to reduce the event volume sent to the system.
  - You need to install and maintain connectors separately.
  - You can subscribe to the data Transformation Hub manages.
- Third-party collectors and connectors also provide data to the deployed capabilities.

For more information about data sources, see the following topics:

- "Understanding How Data is Produced and Consumed " on page 357
- "Enabling Integration with AWS Transformation Hub " on page 264
- "Intelligence Data Types and Schemas " on page 631
- "Configuring Event Integrity Checks" on page 646
- "Managing Connectors" on page 860

Enterprise Security Manager

ArcSight Enterprise Security Manager (ESM) operates outside of the Platform OMT environment, but integrates with capabilities that operate within the Platform environment. For example, ESM shares SSO, event processing, and event search behavior with the Platform.

You can deploy the ESM Command Center capability to the Platform OMT environment to provide a more seamless user experience with other capabilities that integrate with the Core components, such as Intelligence and SOAR. When deployed in this manner, ESM Command Center integrates with ESM operating outside of the Platform OMT environment.

For more information about ESM Command Center, see the following topics:

- "Integrating ESM Data and Users " on page 279
- "Integrating Data from ESM" on page 291
- "Understanding How Data is Produced and Consumed " on page 357
- "Consuming Events with ESM " on page 358
- "Upgrading ESM" on page 440

SMTP Server

The SMTP server enables the Platform to send notification messages to users. For example, when you create new users, you need the SMTP server to notify the users about their account and how to change their passwords.

For more information about SMTP server, see the following topics:

- "Connecting to Your SMTP Server" on page 270
- "System Admin Configuration Types" on page 913

Understanding Multi-tenancy

The Multi-tenancy mode in ArcSight Platform allows you to create and manage multiple tenants in your environment. A multi-tenant environment consists of the provider and tenants.

> You can install ArcSight Platform in the Multi-tenant mode either with an Enterprise license or with an MSSP license.

When integrated with ESM, you have access to Optics, that provide near real-time alert information for various Security Operations Center (SOC) personas, such as the Chief Information Security Officer (CISO) and security analysts.

Providers

In a multi-tenant environment, a provider provides platform services to its tenants. A provider can be an Enterprise, which wants to create different tenants for different groups or regions within the organization or an MSSP organization, who can have tenant organizations that have subscribed to the MSSP's services.

Only the system administrator can create the provider.

Users from the provider organization include, but are not limited to the following:

- Administrators: Users in this role have the highest level of access within ArcSight Platform. They are responsible for managing the overall functionality and onboarding tenants.
- Analysts: Users in this role are responsible for monitoring and investigating alerts for all tenants in the dashboard.

Tenants

A tenant is a customer of the service provider. Each tenant has their own set of users, roles, and settings. The provider administrator onboards a tenant and creates an administrative user to manage the tenant. The tenant administrator can add other tenant users and assign roles to them for specific tasks. Tenant users can only access their tenant; they cannot access other tenants managed by the provider.

Users from the tenant organization include, but are not limited to the following:

- Administrator: Tenant administrators manage roles and permissions, users, and groups within their respective tenants.
- CISO: Users in this role monitor various security metrics for their tenant to gain a comprehensive view of the tenant's security posture and identify areas that need attention.
- Analyst: Users in this role are responsible for monitoring and investigating alerts for their tenants.

To understand the requirements to enable ArcSight Platform in the Multi-tenant mode, see "Planning for Multi-tenancy" on page 70.

Chapter 2: Planning to Install and Deploy

This section describes the installation and deployment options, considerations, and caveats that you need to know for a successful deployment.

Checklist: Planning to Deploy the Platform

Use the following checklist to install and configure the Platform infrastructure. Perform the tasks in the listed order.

	Task	See
❑	1. Learn about the software and components that you need to install, deploy, and configure	"Understanding the Capabilities that You Can Deploy" on page 27 "Understanding Related Components " on page 31
❑	2. Decide how you want to configure your Platform environment, and ensure that the computers on which you are installing the Platform components meet the specified requirements.	*Technical Requirements for ArcSight Platform 24.2*
❑	3. Review the knowledge and individuals needed to perform the installation processes	"Identifying Your Installation Team" on the next page
❑	4. Review the considerations for creating the Platform infrastructure	"Reviewing the Considerations and Best Practices" on the next page
❑	5. Understand the security modes and their prerequisites needed for establishing communication between the infrastructure components	"Understanding Object Storage Options for the ArcSight Database" on page 41
❑	6. Understanding Firewall Ports for the ArcSight Platform	"Understanding Firewall Ports for the ArcSight Platform " on page 41
❑	7. Understanding Security Modes	"Understanding Security Modes" on page 58
❑	8. Learn how the OMT sets up the Kubernetes network subnet	"Understanding Kubernetes Network Subnets" on page 69
❑	9. Planning for Multi-tenancy	"Planning for Multi-tenancy" on page 70

Identifying Your Installation Team

Your installation will require specific administration skills, and coordination with corporate IT departments, including the following:

- Linux operating system administration (including applying operating system updates; configuring networks, firewalls, ports, and user access; and performing additional tasks)
- Familiarity with editing configuration files
- Running operating system commands and scripts
- Familiarity with OpenText components
- Familiarity with Kafka processing and configuration

Your installation team will need team members in the following roles and responsibilities to properly configure the infrastructure environment.

Role	Responsibility
ArcSight admin, also called Application admin	The person in this role must ensure successful execution of the entire installation including verification and post-installation tasks. This person must have a good understanding of the entire installation process, request support from other appropriate roles as needed, and complete the installation once the environment is ready for installation. This person is also in charge of ArcSight Database administration.
IT admin	The person in this role prepares physical or virtual machines as requested by the application administrator.
Network admin	he person in this role manages network-related configuration for your organization. This person needs to perform network configuration tasks as requested by the application administrator.
Storage admin	The person in this role plans and deploys all types of storage for your organization. This person needs to set up one or more NFS servers required by the OMT installation.
Cloud Technology admin	he person in this role demonstrates an understanding of the cloud key concepts and their relevant terminology. As such, they manage cloud-related configurations for your organization.

Reviewing the Considerations and Best Practices

Before starting the installation process, there are several decisions to be made to plan and prepare your infrastructure. The list below contains considerations to be made, and an outline of steps to guide you during this planning and preparation process. We will explain details in later sections of this guide.

Consideration	Best Practices

Host Systems	• Your host systems must meet or exceed the technical requirements for CPU cores, memory, and disk storage capacity, and anticipated requirements for end-to-end events processing throughput. With insufficient resources available on a host, the installation process may fail. Consult the *Technical Requirements for ArcSight Platform 24.2* for guidance.
	• Provision cluster (master and worker node) host systems and operating environments, including OS, storage, network, and Virtual IP (VIP) if needed for high availability (HA). Note the IP addresses and FQDNs of these systems for use during product deployment.
	• You can install the cluster using a `sudo` USER with sufficient privileges, or, alternatively, you can install it using the `root` USERID.
	• Master and worker nodes can be deployed on virtual machines. However, since most of the processing occurs on worker nodes, if possible, you should deploy worker nodes on physical servers.
	• When using virtual environments, please ensure:
	  ◦ Resources are reserved and not shared.
	  ◦ The IP and MAC addresses are static and do not change after a reboot or a VM move. Dynamic IP addresses will cause the Kubernetes cluster to fail.
	• All master and worker nodes must be installed in the same subnet.
	• If a master and worker are sharing a node, follow the higher-capacity worker node sizing guidelines. OpenText does not recommend this configuration for production Transformation Hub environments.

Consideration	Best Practices
High Availability	• For high availability (HA) of master nodes on a multi-master installation, you must create a Virtual IP (VIP) which will be shared by all master nodes. Prior to installation, a VIP must not respond when pinged. • All master nodes should use the same hardware configuration, and all worker nodes should use the same hardware configuration (which is likely to be different from that of the master nodes). • For HA, exactly three master nodes, at least three worker nodes, and at least three database nodes should be used so that if one of each node type fails, the remaining nodes can continue to operate the system without downtime. This is the configuration illustrated in the diagram. You can use fewer nodes of each node type. However, this configuration will result in that node type not being HA. • For HA, use an NFS server that is separate from the Kubenetes cluster nodes, and has HA capabilities, so there is not a single point of failure. For example, this could be 2 NFS servers (active/passive) configured with replication with a Virtual IP managed between them which OMT is configured to use to connect to the NFS server. An example of configuring the 2 NFS servers in replication mode is described here. ***Note:*** *Link opens an external site.* • For master nodes, only 1 or 3 master nodes are allowed. • If you deploy a single master node, failure of the single master node could cause you to lose the ability to manage the entire cluster until you recover the single master node. In some extreme scenarios, failure of the single master node could cause the entire cluster to become unrecoverable, requiring a complete reinstall and reconfiguration. When using only a single master node, the system will be more reliable if you also host the NFS server on the same master node. • When the installer is configured to create more than one database node, the database fault tolerance will be set to one. This means the data in the database will be replicated so that one database node can fail and the system will continue to operate properly. Database storage utilization will double as a result of the data replication. In a failure scenario, the failed node should urgently be restored before there is a chance of another node failure, which will shut down the database to avoid additional problems. • If you configure the installer to create only a single database node, the database fault tolerance is set to zero because there is only a single node. Therefore, no other node will continue during a failure, and no data replication will occur in this scenario.
Storage	• Create or use an existing NFS storage environment with sufficient capacity for the throughput needed. Guidelines are provided below. Determine the size and total throughput requirements of your environment using total EPS. For example, if there are 50K EPS inbound, and 100K EPS consumed, then the size would be 150K EPS. • Data compression is performed on the producer side (for example, in a Smart Connector).

Consideration	Best Practices
Scaling	• Adding more worker nodes is typically more effective than installing bigger and faster hardware because individual workloads on worker nodes are usually relatively small and some of them work better when there are fewer different workloads on the same node. Using more worker nodes also enables you to perform maintenance on your cluster nodes with minimal impact to your production environment. Adding more nodes also helps with predicting costs due to new hardware. • Unlike worker nodes, for the database it is typically more effective to use bigger and faster hardware than to increase the number of database nodes because the database technology can fully utilize larger hardware and this decreases the need for coordination between database nodes. With that said, for HA it is important to deploy enough database nodes to be resilient in case of a database node failure or individual node downtime for maintenance.
Network	• Although event data containing IPv6 content is supported, the cluster infrastructure is not supported on IPv6-only systems.
Cloud	• All SmartConnector remote connections depend on the Operating System random number pool (entropy pool) to generate private keys for secure communication. For a cloud environment, you might need to increase the entropy pool beyond the lower limit of 3290 to ensure uninterrupted communication. For more information see, **"SmartConnector Remote Connections Failing Due to Low Entropy"** in the Installation Guide for ArcSight SmartConnectors (ArcSight SmartConnectors 24.2 documentation).
Security	• Determine a security mode (FIPS, TLS, Client Authentication) for communication between components. See "Determining a Security Mode Between Components" on page 66
Performance	• If SmartConnector is configured to send events to Transformation Hub in CEF format and the events are being stored in ArcSight Database, consider the potential performance effects of the CEF-to-Avro data transformation, and allow a 20% increase in CPU utilization. This will generally have a large impact only with very high EPS (250K+) rates. Consider configuring the SmartConnector to use the Avro event format instead, which avoids the need for this transformation.
Downloads and Licensing	• Ensure that you have access to the OpenText software download location. You will download installation packages to the Initial Master Node in the cluster. • Ensure that you have a valid OpenText license key for the software being installed.
Installing with Enterprise Security Manager	• If you want to install the Platform and the ESM server in the same environment, specify during the Platform installation a OMT API Server Port that does not use the same port as the ESM server (default 8443). For example, when using the Platform Install tool, the `example-install-config-esm_cmd_center-single-node.yaml` sets the master-api-ssl-port to port 7443.

Understanding Object Storage Options for the ArcSight Database

Object Storage is the industry standard technical term for the type of storage component used for ArcSight Database's communal storage. The information on this page relates to "bring-your-own" ArcSight Database S3-compatible storage only.

When deploying to the cloud, it is recommended to use the cloud-provided Object Storage technology as it would almost always be more reliable, easier to manage and less expensive. For more information on what Object Storage technology to use, when a cloud-provided one is not readily available, see **Hybrid Cloud Support** in the *Technical Requirements for ArcSight Platform 24.2*.

When installing the database Off-cloud, you can choose one of the S3-compatible object store technologies that works with the ArcSight Database. You can see the supported object store technologies in the ArcSight Database 24.1 Guide.

> Not all S3-compatible object store technologies provide the same performance or capabilities. Research is important to determine the ideal solution for your needs. We've found that MinIO works well in the testing we've performed in our labs, but other solutions might work better for your environment. To help you get an idea of how to configure MinIO for use with ArcSight Database, see the example in ""Configuring the ArcSight Database for MinIO Storage (Examples Only)" on page 537."

Understanding Firewall Ports for the ArcSight Platform

This section lists the ports that must be open for the elements that make up the ArcSight Platform:

- "Firewall Ports for OMT Infrastructure Components" below
- "Firewall Ports for Deployed Capabilities" on page 48
- "Firewall Ports for Supporting Components" on page 57

Firewall Ports for OMT Infrastructure Components

The following tables list the ports that must be open for the OMT infrastructure components:

- OMT Vault
- OMT Management Portal

- Kubernetes
- Network File System (NFS)

In most cases, the firewalls for these components are host-based. These components are not likely to have network-based firewalls between them.

In most cases, you do not need to take action to configure the firewalls for these ports.

OMT Vault

Ports	Protocol	Source Server	Target Server	Description
8200	TCP	Control plane and worker	Control plane	Used by the `itom-vault` service, which provides a secured configuration store All cluster nodes should be able to access this port for the client connection.
8201	TCP	Control plane and worker	Control plane	Used by the `itom-vault` service, which provides a secured configuration store Web clients must be able to access this port for peer member connections.

OMT Management Portal

Ports	Protocol	Source Server	Target Server	Description
3000	TCP	All clients	Control plane	The port is exposed on the ingress node. All clients should be able to access this port. Used only for accessing the OMT Management Portal during OMT installation from a web browser Web clients must be able to access this port during the OMT installation. Post-installation, this port can be blocked, and re-opened only if re- installation is required. After installation, web clients use port 5443 to access the OMT Management Portal.

5443	TCP	All clients	Control plane	The port is exposed on the ingress node. All clients should be able to access this port. Used for accessing the OMT Management Portal post OMT deployment from a web browser Web clients must be able to access this port for OMT administration and management.

5444	TCP	All clients	Control plane	The port is exposed on the ingress node. All nodes should be able to access this port when using 2-way certificate authentication. Used for accessing the OMT Management Portal post OMT deployment from a web browser, when using two-way (mutual) TLS authentication Web clients must be able to access this port for OMT administration and management, when using two-way (mutual) TLS authentication.

Kubernetes

Ports	Protocol	Source Server	Target Server	Description
2380	TCP	Control plane	Control plane	Used by the `etcd` component, which provides a distributed configuration database All the master nodes should be able to access this port for the `etcd` cluster communication. This port will need to be opened only in multi-master deployments

4001	TCP	Control plane and Worker	Control plane	Used by the `etcd` component, which provides a distributed configuration database All cluster nodes should be able to access this port for the client connection. This port will need to be opened only in multi-master deployments, or if worker nodes require access to this port
7443	TCP	Control plane and Worker	Control plane	*(Conditional)* Used by the Kubernetes API server when performing one of the following methods of installation: • Using the provided scripts • Installing manually and on the same node as ESM All cluster nodes should be able to access this port for internal communication.
8443	TCP	Control plane and Worker	Control plane	*(Conditional)* Used by the Kubernetes API server when manually installing on a different node from ESM. All cluster nodes should be able to access this port for internal communication. For more information about `HTTPServerPort` Offset, see General parameters in the ArcSight Database documentation. For information about how `UDP` ports are used for broadcast and point-to-point modes, see Spread Configuration Best Practices in the ArcSight Database documentation.
8472	UDP	Control plane and Worker	Control plane and Worker	*Uses UDP protocol* Used by the Flannel service component, which manages the internal cluster networking All cluster nodes should be able to access this port for internal communication.

10250	TCP	Control plane and Worker	Control plane and Worker	Used by the Kubelet service, which functions as a local node agent that watches pod specifications through the Kubernetes API server All cluster nodes should be able to access this port for internal communications, and the Kubelet API worker node for exec and logs.
10259	TCP	Access by localhost only	Control plane	Used by the `kube-scheduler` component that watches for any new pod with no assigned node and assigns a node to the pod All cluster nodes should be able to access this port for internal communication. This port will need to be opened only in multi-master deployments
10257	TCP	Control plane and Worker nodes	Control plane	Used by the `kube-controller-manager` component that runs controller processes which regulate the state of the cluster. All cluster nodes should be able to access this port for internal communication This port will need to be opened only in multi-master deployments
10256	TCP	Control plane and worker	Control plane and Worker	Used by the `Kube-proxy` component, which is a network proxy that runs on each node, for exposing the services on each node All cluster nodes should be able to access this port for internal communication.

Network File System (NFS)

Ports	Protocol	Source Server	Target Server	Description
111	TCP/NFS UDP/NFS	Control plane and worker	NFS	NFS server port. Used by the `portmapper` service All cluster nodes should be able to access this port. This port must be opened if NFS is running on a cluster node
2049	TCP/NFS	Control plane and worker	NFS	Used by the `nfsd` daemon All cluster nodes should be able to access this port. This port must be opened if NFS is running on a cluster node **Note:** This port must be open even during a single-node deployment.
20048	TCP/NFS	Control plane and worker	NFS	Used by the `mountd` daemon All cluster nodes should be able to access this port. This port must be opened if NFS is running on a cluster node

Firewall Ports for Deployed Capabilities

The following tables list the ports that must be available when you deploy the associated capability into the OMT infrastructure:

- ArcMC
- Intelligence

- SOAR
- Transformation Hub

In most cases, you do not need to take action to configure the firewalls for these ports.

ArcMC

Ports	Protocol	Description
32080, 9000	TCP	Used for Transformation Hub and ArcMC communication

Intelligence

Ports	Node	Direction	Description
30820/TCP	Worker (HDFS Namenode)	Inbound	Used for the database to connect to HDFS during Analytics processing
30070/TCP	Worker (HDFS Namenode)	Inbound	Used for the Hadoop Monitoring Dashboard (optional)
30010/TCP	Worker (HDFS Datanodes)	Inbound	Used for communication between the HDFS Namenode and the HDFS Datanodes
30210/TCP	Worker (HDFS Datanodes)	Inbound	Used by the database to establish secure communication with HDFS during Analytics processing
30110/TCP	Worker (HDFS Datanodes and Namenode)	Inbound	Used for communication between the ArcSight Database and HDFS worker nodes
30071/TCP	Worker (HDFS Namenode)	Inbound	Used for Secure Data Transfer with the HDFS cluster

SOAR

The SOAR cluster listens on the following ports on all Kubernetes master and worker nodes, but OpenText recommends that you only use the ports on the master virtual IP.

Port	Description
32200	Data from ESM

Transformation Hub

Ports	Protocol	Source Server	Target Server	Description
2181, 2182	TCP	Worker Node	Worker Node	Used by ZooKeeper as internal communication ports to client requests (i.e from Kafka). All cluster nodes should be able to access this port for internal communication.
9092	TCP	Client machine, Worker node	Worker Node	Only needs to be opened if Transformation Hub is configured to accept connections over a clear text channel. While this type of setup is not recommended by OpenText, it represents an option in case the goal is to prioritize performance over security. If the Kafka consumer or producer connecting to this port (such as a SmartConnector) is logically deployed in a network with a firewall in between them, please consider that the firewall then will also need to permit traffic through this port accordingly.

9093	TCP	Client machine, Worker node	Worker Node	Required for secure communications with clients. If the Kafka consumer or producer connecting to this port (such as a SmartConnector) is logically deployed in a network with a firewall in between them, please consider that the firewall then will also need to permit traffic through this port accordingly.

32092	TCP	Client machine, Worker node	Worker Node	Only needs to be opened if Transformation Hub is configured to accept connections over a clear text channel. While this type of setup is not recommended by OpenText, it represents an option in case the goal is to prioritize performance over security. If the Kafka consumer or producer connecting to this port (such as a SmartConnector) is logically deployed in a network with a firewall in between them, please consider that the firewall then will also need to permit traffic through this port accordingly.

32093	TCP	Client machine, Worker node	Worker Node	Required for secure communications with clients. If the Kafka consumer or producer connecting to this port (such as a SmartConnector) is logically deployed in a network with a firewall in between them, please consider that the firewall then will also need to permit traffic through this port accordingly.
32080	HTTPS	Client machine, Worker node	Worker Node	Used by Transformation Hub (TH) WebServices as external communication port to serve HTTP requests from ArcMC (externally)

32081	HTTPS	Client machine, Worker node	Worker Node	Used by Schema Registry as external communication port to serve HTTP requests for providing Schemas information for external Avro consumers. If the Kafka Avro consumer or producer connecting to this port (such as a SmartConnector) is logically deployed in a network with a firewall in between them, please consider that the firewall then will also need to permit traffic through this port accordingly.
443	HTTPS	Client machine		Used by Transformation Hub, ArcMC, Core components, etc., for UI access
9000	HTTPS	Worker Node	Worker Node	Used by Kafka Manager as internal communication port to provision the Kafka Manager UI access in Transformation Hub. All cluster nodes should be able to access this port for internal communication.

9999	JMX	Worker Node	Worker Node	Used by Kafka as internal communication port to provide monitoring information to Kafka Manager and WebServices (for monitoring purposes). All cluster nodes should be able to access this port for internal communication.
10000	JMXRMI	Worker Node	Worker Node	Used by Kafka as internal communication port to provide extra monitoring information (for monitoring purposes). All cluster nodes should be able to access this port for internal communication.
32101 - 32150	TCP	Client machine, Worker node	Worker Node	Used by Transformation Hub (TH) as external communication ports to allow ArcMC to communicate with and manage Connectors in Transformation Hub (CTH) These ports are needed only if the plan is to deploy Connectors in Transformation Hub

2888	TCP	Worker Node	Worker Node	Used by Zookeeper for peer-to-peer traffic and communication.
3888	TCP	Worker Node	Worker Node	Used by Zookeeper for Zookeeper Leader election.
8081	TCP	Worker Node	Worker Node	Used by Schema Registry to serve HTTP requests for providing Schemas information for internal Avro consumers (internally).
2101, 2150	TCP	Worker Node	Worker Node	Used by Transformation Hub (TH) to allow Core ArcMC to communicate with and manage Connectors in Transformation Hub (CTH). These ports are needed only if the plan is to deploy Connectors in Transformation Hub.
8080	TCP	Worker Node	Worker Node	Used by Transformation Hub (TH) WebServices to serve HTTP requests from Core ArcMC and other components (internally).
9094	TCP	Worker Node	Worker Node	Required by Kafka for secure communications with clients within the cluster.

Firewall Ports for Supporting Components

The following tables list the ports that must be available for supporting components:

- Database
- SmartConnectors

Database

The database requires several ports to be open on the local network. OpenText does not recommend placing a firewall between nodes (all nodes should be behind a firewall), but if you must use a firewall between nodes, ensure that the following ports are available:

Ports	Description
TCP 22	Required for the Administration Tools and Management Console Cluster installation wizard
TCP 5433	Used by database clients, such as vsql, ODBC, JDBC, and so on
TCP 5434	Used for Intra-cluster and inter-cluster communication
UDP 5433	Used for database spread monitoring
TCP 5438	Used as Management Console-to-node and node-to-node (agent) communication port
TCP 5450	Used to connect to Management Console from a web browser and allows communication from nodes to the Management Console application/web server
TCP 4803	Used for client connections
UDP 4803	Used for daemon to daemon connections
UDP 4804	Used for daemon to daemon connections
UDP 6543	Used to monitor daemon connections

SmartConnectors

If you have SmartConnectors that are deployed logically far away in the network with firewalls in between, those intermediate firewalls will need to permit traffic on port 9092 (for non-TLS traffic) and 9093 (for TLS traffic).

Port	Direction	Description
• 1515 (Raw TCP) • 1999 (TLS)	Inbound	Used by SmartConnector to receive events

• 9092 (Non-TLS) • 9093 (TLS)	Outbound	Used by SmartConnector to send data to Transformation Hub Port 9092 needs to be opened only if your configuration is set to communicate with Transformation Hub over a non- encrypted communication channel. While this type of setup is not recommended by OpenText, it represents an option in case the goal is to prioritize performance over security.

Understanding Security Modes

The ArcSight Platform comprises multiple products, services, and infrastructure components. The products and services communicate with each other and with administrative applications. You must secure the communication channels using your selected security mode between the components to prevent security breaches and to protect your data.

IMPORTANT: You must deploy all components using the same security mode. If not, communication between the components will not function. If you want to change a security mode for a component, you must uninstall it and reinstall it with the correct security mode for communication to function correctly.

ArcSight Platform supports several secure modes of communication between infrastructure components and ArcSight products or services. Understanding these security modes will assist you to securely install and administer the Platform. The supported security modes are:

- **Allow Plain Text:** All communication between components occurs as plain text. ArcSight recommends that you never use this mode in a production environment, as using plain text causes security issues and data breaches.
- **FIPS-compliant TLS Settings:** All communication between the components meets the Federal Information Processing Standard (FIPS) established by the United States. For more information, see Using ArcSight Platform and Products in FIPS Mode
- **TLS Client Authentication:** Permits secure communication between components that do not use client user name and password authentication, such as producers and consumers connecting to Transformation Hub. With TLS Client Authentication enabled, the client and the server authenticate each other to ensure that both parties involved in the communication are trusted.
- **TLS:** Permits secure communication between the components that have been configured with public key infrastructure certificates to be able to communicate over the transport layer security (TLS). For more information, see "Understanding the Components of Secure Communication" on the next page.

Understanding the Components of Secure Communication

ArcSight uses common industry standards to secure communication such as X.509 certificate, public key infrastructure (PKI), and transport layer security (TLS). You must decide which security mode you will use during the deployment of the ArcSight products and the infrastructure products.

This section contains the following topics:

- "Understanding Public Key Infrastructure and TLS Components" below
- "Using ArcSight Platform and Products in FIPS Mode" on page 64
- "Determining a Security Mode Between Components" on page 66

Understanding Public Key Infrastructure and TLS Components

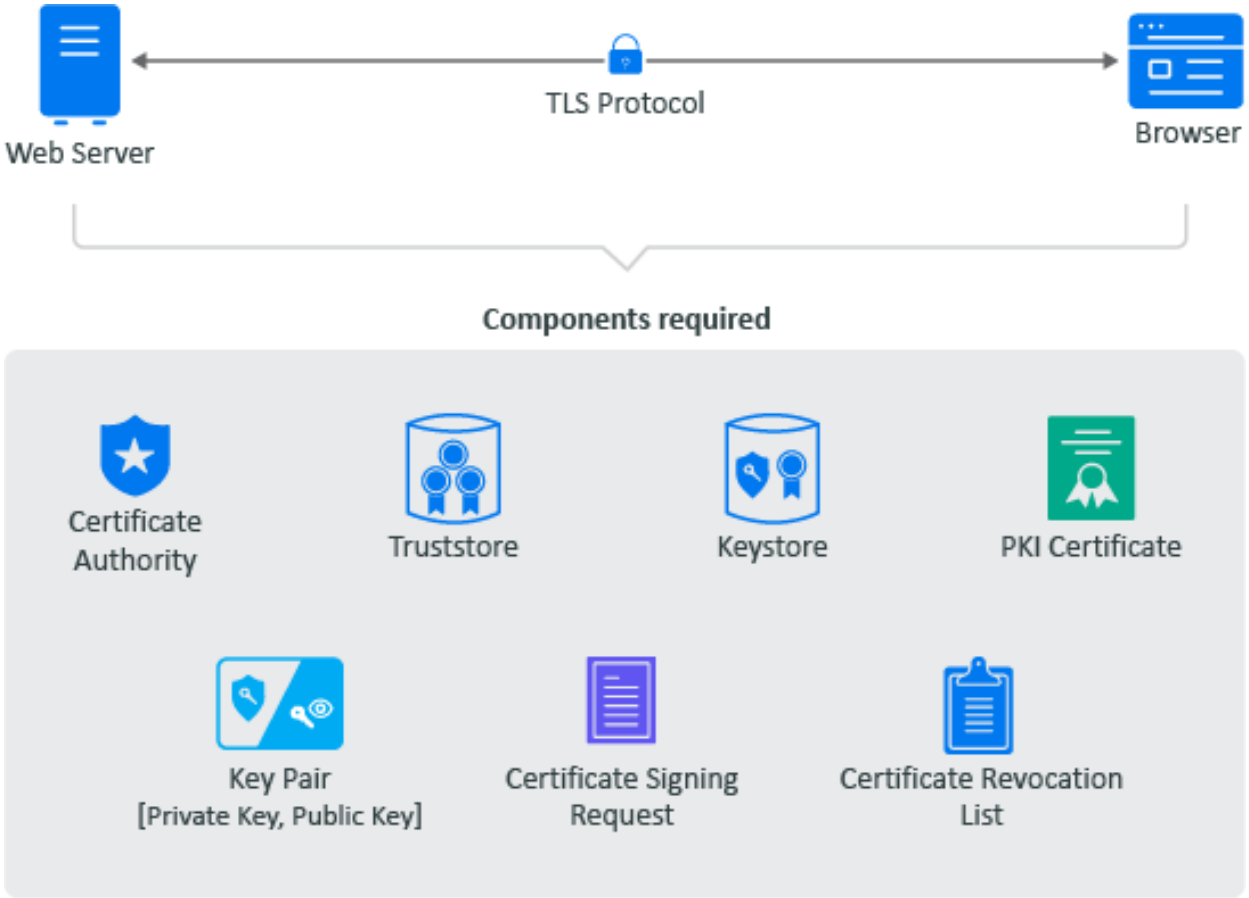
In order to configure secure communication between the ArcSight products, infrastructure products, and any administrative tools, you must have a good understanding of the components that enable the secure communication to occur. ArcSight uses the industry standards of X.509 certificates, public key infrastructure (PKI), and transport layer security (TLS). This section provides a basic introductions to these components. For more detailed information, see (links open an external site):

- Internet X.509 Public Key Infrastructure Certificates and Certificate Revocation List (CRL) Profile
- The Transport Layer Security (TLS) Protocol Version 1.2
- The Transport Layer Security (TLS) Protocol Version 1.3

You must secure the communication channels between servers and clients to protect your data and stop security breaches from happening in your environment. The following graphic depicts the different components required for secure communication using certificates, PKI, TLS, and tools to manage the keys.

The secure communication occurs between a server and a client. An example server is a web server and a client could be a browser. The following items are the terms that you need to

understand to create a secure connection between a server and a client.

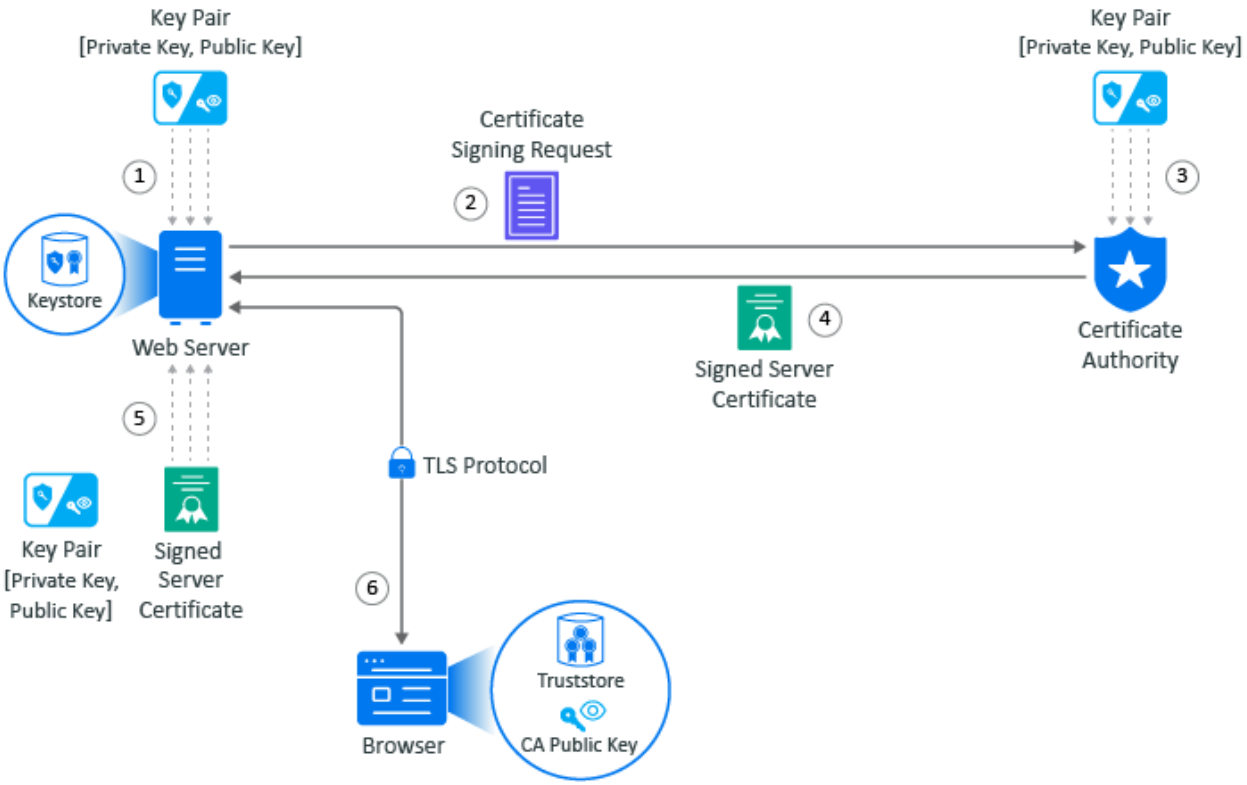


- **Certificate Authority (CA)**: It is an entity that issues digital certificates. A certificate authority (CA) acts as a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. There are two different types of CAs:
  - **Well-known:** A certificate authority that provides server certificates signed by well-known CAs such as IdenTrust or DigiCert.
  - **Self-signed:** A certificate authority used by other products such as openSSL, eDirectory, and Active Directory that contain a certificate authority. You can create self-signed certificates through the certificate authorities in these other products to use in test environments. A security recommendation is to use a well-known CA to issue certificates in productions environments.
- **Public Key Infrastructure (PKI) Certificates:** CA-issued digital certificates that prove ownership of the certificate. The CA can issue certificates for users, applications, or devices. The PKI certificates contain the following information:
  - Version number
  - Unique serial number
  - CA digital signature and algorithm used

  - Validity period
  - Certificate Usage
  - Subject name, URL, email address
  - Public and private keys (sometimes it is only the public key)
- **Key Pair:** Consists of a private key and public key that work together to encrypt and decrypt messages. PKI is based on the fact that everyone will trust any communication encrypted with a public key or trust any certificate signed by a private key.
  - Private Key: A cryptographic key that you use to decrypt any communication encrypted by the public key. Only the private key of the key pair can decrypt the communication encrypted with the corresponding public key. You keep the private key private and do not share it.
  - Public Key: A cryptographic key that you use to encrypt communications to keep the communication secure. Only someone with the private key can decrypt the communications. You share the public key so that anyone with access to the public key can verify that any communication signed with this public key is really from the sending source.
- **Certificate Revocation List:** A list that the CA creates and manages that contains a list of unique serial numbers that it has revoked. The CA uses the certificate revocation list (CLR) to deny requests from any user, application, or device that contain a serial number on the CLR.
- **Certificate Signing Request:** A message sent from an applicant to the CA to apply for a PKI certificate. Usually the certificate signing request (CSR) contains a copy of the public key of the applicant making the request, identifying information such as a domain name, and a digital signature.
- **KeyStore:** A secure Java repository that stores the private key and identity certificate for the server in the trust relationship. The information is stored encrypted on the server with a KeyStore password that you set and manage. Use either the keytool or keytoolgui tools to set and manage the KeyStore passwords.
- **TrustStore:** A secure Java repository that stores the certificates signed by a CA in a secure repository on the client. The information is stored and encrypted on the client with a TrustStore password that you set and manage. Use either the keytool or keytoolgui tools to set and manage the TrustStore passwords.
- **TransportLayerSecurityProtocol:** A secure protocol created by all of the components defined in this section. It allows the server and client to communicate securely by using certificates and key pairs to prove identity on the server and client.

Example: Establishing Secure Communication for a Web Server

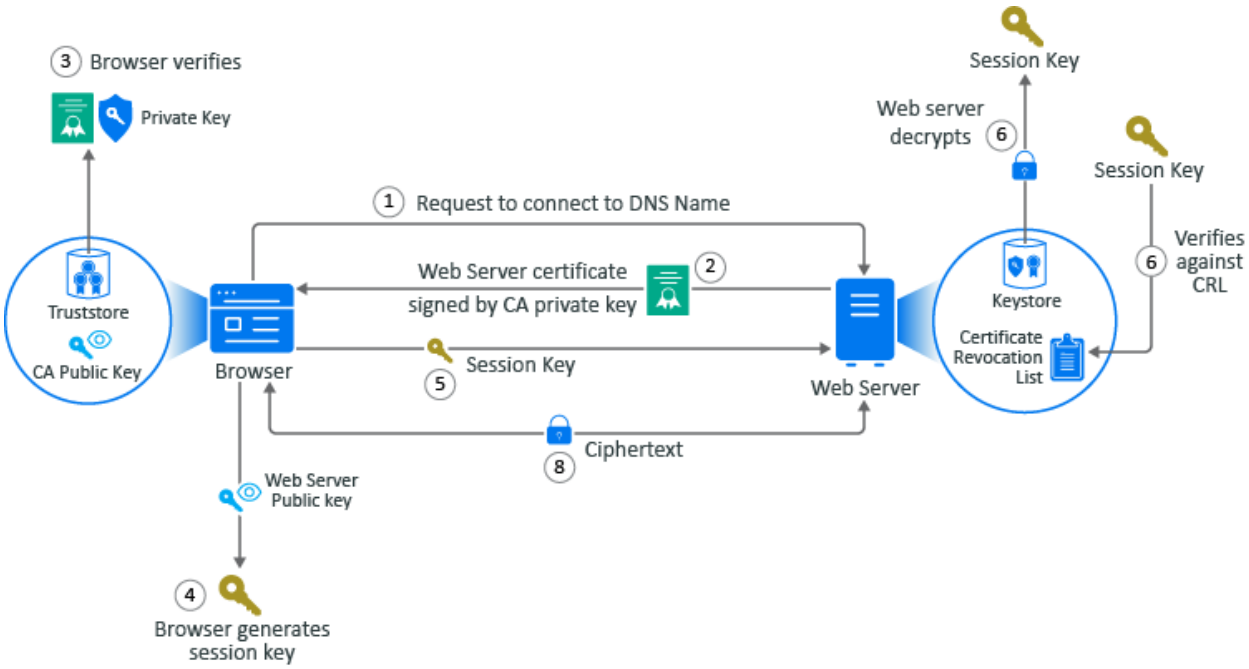
When you install a web server, communication is not secure by default. If the communication is secure, it is usually using a self-signed certificate. The following example shows how the web server obtains a server certificate signed by a well-known certificate authority (CA) to use in establishing secure communications with any client. In the example, Adam the administrator requests a signed server certificate from the well-known CA and uses the certificate to establish secure communications with a client that is a web application.



1. Adam generates a key pair on the web server using keytool. Adam uses the key pair to create a certificate signing request (CSR) using keytool. The CSR contains the fully qualified DNS name of the server, the key pair, and other such information to help identity the web server.
2. Adam sends the CSR that contains the web server's information to a well-known CA such as DigCert.
3. The CA uses the CSR to generate a server certificate for the web server. The CA uses its private key to sign the certificate. The server certificate contains the key pair and the web server's information included in the CSR. The CA signs the certificate with its private key.
4. The CA sends the signed web server certificate back to Adam.

5. Adam imports the signed web server certificate into the web server and the web server's certificate and private key are stored in the KeyStore on the web server.
6. When a browser accesses the web server, the web server sends a certificate signed by the private key of the CA to the browser. The browser has a copy of the CA's public key in its TrustStore and uses the public key to decrypt the signature of the CA. Now, the browser will trust any communication coming from this web server.

Example: Secure Handshake for the Client



This example show how the secure handshake occurs between a client and a server so that they can create their own secure communication channel that no other entities can use or access. In this example, Adam the administrator logs into the administration console that is a web application. Every action (except for Adam entering the URL in the web browser) happens automatically between the browser and the web server. No user interaction is required.

1. Adam adds a the URL into the browser. The browser sends a request to connect to the fully qualified DNS names of the web server.
2. The web server sends a copy of its server certificate that has been signed by the private key of a well-known CA.
3. The browser accesses the public key of the well-known CA that is stored in the browser's TrustStore. The browser uses the public key of the well-known CA to decrypt the signature on the web server's certificate to verify that the certificate is valid.
4. The browser generates a session key using the public key in the web server's certificate.
5. The browser sends the newly generated session key back to the web server.

6. The web server uses its private key stored in the KeyStore to decrypt the session key.
7. The web server verifies that the session key is not on the certificate revocation list (CLR). At this point the secure handshake between the browser and web server is established.
8. The web server encrypts the data using the session key and sends the data back in ciphertext to the browser. The browser uses the session key to decrypt the data and then uses the session key to encrypt data and then it sends the data back in ciphertext. This secure communication continues until the session ends.

.

Using ArcSight Platform and Products in FIPS Mode

The **Federal Information Processing Standard (FIPS)** comprises a set of rules and regulations defined by the United States government that specify the security requirements for data processing and communication between the components.

- Understanding FIPS 140 Security Requirements
- Enabling FIPS Mode for ArcSight Platform Components

For a more thorough understanding of FIPS, official FIPS documentation (FIPS PUBS) is available online.

Understanding FIPS 140 Security Requirements

FIPS 140 is one of the standards of FIPS that governs the use of encryption and cryptographic services. FIPS 140 defines security rules and regulations for cryptographic modules to keep sensitive information secure.

According to the **Federal Information Security Management Act (FISMA)**, all the United States government agencies, United States government contractors, and third parties working for the federal agencies must adhere to the FIPS 140 standard.

For testing cryptographic modules, the two revised editions of FIPS 140 are given below:

FIPS Publication	Standard
FIPS 140-2	Includes changes in technology and standards defined by other standards bodies. Includes modifications based on comments from vendors, laboratories, and user communities.
FIPS 140-3	Aligns with standards defined by the **International Organization for Standardization (ISO)** and the **International Electrotechnical Commission (IEC)**

Enabling FIPS Mode for ArcSight Platform Components

Most components in the ArcSight Platform architecture can operate in the FIPS 140 mode: this includes all of the components that directly handle event data from edge ingestion, to storage in the database, to retrieval from the database supports FIPS 140 Mode. FIPS 140 mode is active by default for some components and cannot be disabled. ArcSight Platform establishes a secure communication between its components using FIPS-validated cryptographic modules.

The table below describes the component level FIPS 140 support:

Component	Sub-components that support FIPS mode	Enabling FIPS mode
ArcSight Management Center (ArcMC)	fusion-arcmc-web-app	• Always enabled
Database	All	• See the Setting FIPS Mode on the Database Server section.
Enterprise Security Manager (ESM)	All	• Enabled by default on fresh installations. • See the Configuring the Deployed Capabilities section. • See the ESM Administrator's Guide. • Complete the process described in the ESM Administrator's Guide..
Core components	All	• Always enabled
Intelligence	All	• Always enabled
Layered Analytics	All	• Always enabled
Recon	All	• Always enabled

Component	Sub-components that support FIPS mode	Enabling FIPS mode
SmartConnectors	All	• See the SmartConnectors section

SOAR	`soar-web-app`
	`soar-message-broker`
	`soar-jms-migration`
		For the sub-components listed that support FIPS mode, FIPS mode is always enabled.

Transformation Hub	`th-kafka`
	`th-kafka-manager`
	`th-schemaregistry`
	`th-routing-processor`
	`th-c2av-processor`
	`th-web-service`
	`th-cth`
	`th-c2av-processor-esm`
	`th-enrichment-processor`
	`th-zookeeper`
		• For the sub-components listed that support FIPS mode, FIPS mode can be enabled during deployment.
		• When using the ArcSight Platform Installer tool, add the property `th-init-fips: true` to the `suite > config-params` section of your installation configuration `yaml` file. For example:
		`suite:`
		`  products: [esm, soar, transformationhub]`
		`  config-params:`
		`  th-init-fips: true`
		• When performing the installation manually, configure the `Transformation Hub > Connections use FIPS encryption` option as described in the Configuring the Deployed Capabilities section.

Components that can not operate in the FIPS 140 mode use strong industry standard encryption to establish secure communication. However, our objective is to increase the coverage of components that can operate in the FIPS 140 mode.

For more information about each of the pods listed above, see Understanding Labels and Pods.

For information on creating a RedHat operating system with FIPS enabled, see "10.2 Federal Information Processing Standard (FIPS)" on the RedHat Customer Portal. **Note:** This link opens an external site.

Determining a Security Mode Between Components

You must determine a security mode for communication between your infrastructure components. The security mode of connected producers and consumers must be the same across all components.

The secure communication described applies only in the context of the components that relate to the OpenText container-based application you are using, which is specified in that application's documentation.

When possible, configure the OpenText components with the security mode you intend to use *before* connecting them to additional ArcSight Platform products.

To enhance security, you can configure TLS Client Authentication between components that do not utilize client username and password authentication, such as producers and consumers connecting to Transformation Hub. With TLS Client Authentication enabled, the client and the server authenticate each other to ensure that both parties involved in the communication are trusted.

> Changing the Allow Plain Text, TLS Client Authentication, or FIPS-compliant TLS settings after the deployment will necessitate system downtime.

OpenText product documentation for ArcSight products in the table is available from the OpenText support community.

Unless otherwise indicated in the table below, the ArcSight Platform and the capabilities that deploy to it, communicate with each other using TLS with authentication performed in a manner appropriate for the component.

Product	Preparations Needed	TCP Ports	Supported Security Modes
Standalone ArcMC	• Be sure to use v2.9.5 or later. • Install ArcMC before the Platform installation.	• 443 • 32080	• TLS • FIPS-Compliant TLS • TLS Client Authentication
SmartConnectors	• You can install and run SmartConnectors and ArcMC onboard connectors before you install the Platform. Or, you can install them after you deploy the Platform. • FIPS mode setup is not supported between SmartConnector v7.5 and the Platform. • Only TLS and TLS Client Authentication are supported. • FIPS mode *is* supported between Connectors v7.6 and later and the Platform.	• 9092 (Plain Text) • 9093 (TLS)	• TLS • FIPS-Compliant TLS (SC 7.6+ only) • TLS Client Authentication • Plain text

ArcSight ESM	• You can install and run ESM before you install the Platform. • You can change compact mode ESM from TLS to FIPS-compliant TLS after you install ESM. • Changing compact mode ESM from FIPS-compliant TLS to TLS requires reinstalling ESM. • In distributed mode, the ESM security mode is set at installation time. Any change between TLS and FIPS-compliant TLS requires reinstalling ESM.	• 9092 (Plain Text) • 8443	• TLS in ESM Administrator's Guide. • FIPS-Compliant TLS • TLS Client Authentication
ArcSight Logger	• You can install and run Logger before you install the Platform.	• 9092 (Plain Text) • 9093 (TLS)	• TLS • FIPS-Compliant TLS • TLS Client Authentication • Plain text
ArcSight Database	• You install the ArcSight Database before the Platform.	• 9092 (Plain Text) • 9093 (TLS)	• Plain text • TLS • TLS Client Authentication • FIPS-Compliant TLS
NFS Server	• For optimal security, secure all NFS settings to allow only required hosts to connect to the NFS server.	• 2049	• Plain text
Web Browser	• By default, TLS is enabled.	• 443 • 5443 • 3000	• TLS
ArcSight Intelligence (HDFS)	Secure HDFS for Intelligence.	• 30070 (HDFS master) • 30820 (HDFS master) • 30010 (HDFS datanode) • 30210 (HDFS datanode)	• TLS • FIPS-Compliant TLS • TLS Client Authentication • Plain Text

Understanding Kubernetes Network Subnets

Kubernetes automates the deployment of its management services and the pods associated with deployed capabilities to master and worker nodes. As part of this process, it allocates a unique IP address to each service and pod.

In order to do so, Kubernetes must be provided with a reserved range of private network IP addresses for its services (service-CIDR parameter, default is 172.17.17.0/24) and a separate reserved range of private network IP addresses for pods (pod-CIDR parameter, default is 172.16.0.0/16).

The two IP ranges must not overlap, must not be allocated to other systems in the network, and are provided to Kubernetes at install time by specifying a network subnet in Classless Inter-Domain Routing (CIDR) format. CIDR notation includes an IP address, a slash ('/') character, and a network prefix (a decimal number).

The minimum useful network prefix is `/22` and the maximum useful network prefix is `/8`. The default value is `172.16.0.0/16`. For example:

```
POD_CIDR=172.16.0.0/16
```

The pod-CIDR IP range must contain an adequate number of IP addresses to accommodate the functions of all of the pods deployed to the cluster. Each node in the cluster is allocated a segment of the pod-CIDR IP range for use by the pods that are deployed to that node as determined by the pod-CIDR-subnetlen parameter.

The default value for pod-cidr-subnetlen is automatically computed depending on the value of pod-CIDR, as described below. The default value of pod-CIDR-subnetlen is expected to be adequate. However, if for some unexpected reason you find that pods on nodes run out of available IP addresses, you can set the pod-CIDR-subnetlen parameter to a value that makes more IP addresses available to each node.

POD_CIDR Prefix	POD_CIDR_SUBNETLEN defaults	POD_CIDR_SUBNETLEN allowed values
/8 to /21	/24	/(POD_CIDR prefix + 3) to /27
/22 to /24	/(POD_CIDR prefix + 3)	/(POD_CIDR prefix + 3) to /27

Smaller prefix values indicate a larger number of available addresses. The minimum useful network prefix is /27 and the maximum useful network prefix is /12. The default value is 172.17.17.0/24.

Chapter 2: Planning for Multi-tenancy

You cannot disable Multi-tenancy after it has been enabled. If you attempt to disable and save, the ArcSight Platform returns an error message to indicate that you cannot disable the function. Multi-tenancy cannot be enabled if ArcSight Intelligence is installed on the ArcSight Platform.

Before you proceed to deploy the ArcSight Platform, you must determine whether your environment requires multiple tenants to be created. To enable multi-tenancy in ArcSight Platform, you must either upgrade to ArcSight Platform version 24.2 or install ArcSight Platform 24.2.

If you are enabling Multi-tenancy in an already running environment a default topic will be created for existing events. As part of the new routing rules, all events from the avro enriched topic will be transferred to the default topic. This results in duplication of events, as Recon would have already ingested those events into the table. In case you want to avoid such event duplication on the default tenant, you must drain the events from the avro enriched event topic. New events will continue to arrive normally and they will be delivered to the proper tenant.

After you have reviewed information in the following topics, to enable multi-tenancy, see Enabling Multi-tenancy.

Capabilities that Support Multi-tenancy

Consider the following:

- If Intelligence is deployed on the ArcSight Platform, you do not have the provision to enable multi-tenancy on the platform. If you need to enable multi-tenancy, you must first uninstall Intelligence.
- Once you uninstall Intelligence and enable multi-tenancy in the platform, you cannot reinstall Intelligence.

To enable Multi-tenancy, you must have one or both of the following capabilities with ArcSight Core in your environment:

- SOAR
- Recon

To understand the combination of ArcSight capabilities that support Multi-tenancy, refer to the following table:

ArcSight Capabilities	Supports Multi-tenancy?
ArcSight Core + ArcSight SOAR + ArcSight ESM Command Center (optional) If you enable Multi-tenancy with this combination and you want to enable Recon by using OMT configuration page at a later stage, you must reconfigure the tenants in the environment, for Recon to work seamlessly.	Yes
ArcSight Core + ArcSight Transformation Hub + ArcSight Recon + ArcSight ESM Command Center (optional)	Yes
ArcSight Core + ArcSight Transformation Hub + ArcSight Recon + ArcSight SOAR+ ArcSight ESM Command Center (optional)	Yes
ArcSight Core + ArcSight ESM Command Center	No
ArcSight Core + ArcSight Transformation Hub + ArcSight ESM Command Center	No
ArcSight Core + ArcSight Transformation Hub + ArcSight Intelligence	No
ArcSight Core + ArcSight Transformation Hub + ArcSight Recon + ArcSight Intelligence	No

If you enable Multi-tenancy, ensure that the Transformation Hub compression algorithm is set to *gzip*.

Reviewing the Security Considerations of Multi-tenancy

Review the security considerations provided in the following table before proceeding to enable Multi-tenancy in your environment:

Focus Areas	Security Considerations
Customer URI Integrity	ArcSight SmartConnectors collect and process all events coming from tenant devices such as firewalls and IDS and send them to ArcSight Platform based on the Customer URI configured for a tenant. Multi-tenancy in the ArcSight Platform relies on the integrity of the Customer URI to uniquely identify events data for one customer from the other. Ensure that the Customer URI is updated with the tenant key for each of the Smart Connectors deployed for a tenant. To ensure the integrity of the Customer URI, consider the following: 1. Ensure that your tenant onboarding process incorporates the appropriate checks and balances to catch common mistakes. 2. Automate onboarding activity where possible. 3. Deploy and manage Smart Connectors at each tenant site to ensure integrity of their configuration.
Tenant Key Confidentiality	1. A tenant key is a critical element of the Customer URI and must be treated as a secret. Ensure that the tenant key provided for each tenant is not easily guessable and is not shared with any other tenant. Disclosing the tenant key might result in spoofing of tenant event data. In this version, the tenant key cannot be rotated. In case a tenant key is compromised, it is recommended to do the following: • Disable the original tenant to prevent ingestion of new events. • Create a new tenant associated with a new tenant key. • Update the Customer URI in each of the tenant's deployed Smart Connectors to reflect the new tenant key. • Verify that events sent by the tenant's Smart Connectors are successfully ingested in the newly created tenant. • Migrate the data from the old tenant's schema in the ArcSight Database to the new tenant's schema. 2.
Tenant Events Data Ingestion	You are responsible to ensure that only events from legitimate tenants are ingested, and at the appropriate throttling of events or requests. For example, to avoid noisy neighbor issues.
Tenant Events Data Isolation	Tenant events data is stored and isolated in the ArcSight Database, based on the tenant's Customer URI.
Tenant Data Retention	If a tenant is deactivated, none of the tenant data (events, users) is deleted by the ArcSight Platform. If the tenant data needs to be deleted, contact OpenText Support.
Tenant Users	Tenant user's email addresses must be unique across all tenants. If a tenant is deactivated, all users for that tenant are deactivated.
Integration with ArcSight ESM	You must deploy the ArcSight Platform and ArcSight ESM in secure subnets.
Monitoring Logs	You must monitor the ArcSight Platform logs for suspicious tenant activity such as authentication or authorization failures, use of invalid customer URIs or tenant keys.

Planning to Create Multiple Tenants

If you are planning to deploy ArcSight Platform in the Multi-tenancy mode, make sure that you gather the following details:

- The number of tenants that you want to create.
- The data ingestion rate for each of the tenants that you want to create.
- The aggregated rate of ingestion for all the tenants for the provider.

Planning to Optimize Resources in Transformation Hub

To optimize resources in Transformation Hub, plan the following:

- Number of Routing Stream Processor Instances required to facilitate event routing. For more information, see "Stream Processor Groups" on page 691.
- Determine the event ingestion rate and event retention period for each tenant.

By default, new tenants are created with the topic partitions count and retention size specified in the OMT configuration. However, you must manually tune the values for each tenant in the OMT portal based on the event ingestion rate, number of topic partitions needed and the topic retention size for your environment. For more information, see "Tune Tenant Topic Settings" on page 444

Planning to Update Kafka Scheduler

Identify tenants that have high ingestion rate so that you can determine the number of Kafka schedulers for your environment. The ArcSight Database uses Kafka Scheduler to ingest events from a tenant specific Kafka topic in Transformation Hub. For more information, see "Configure Tenant Topics in Kafka Scheduler" on page 450.

Tuning the Ingest Pool Concurrency Parameter

The default value for the planned concurrency of ingested resource pool is 6. This enables one microbatch or one tenant to load events at a time. When you are enabling Multi-tenancy, this value must be increased to at least 12. You can either modify the value for `ingest_pool_planned_concurrency parameter` in the *`config.yaml`* file if you are opting for the automated installation of ArcSight Platform or tune the ingest pool concurrency value after installing or upgrading ArcSight Platform, by using the `tuning_util.sh utility`. For more information, see Tuning the Ingest Pool Concurrency Parameter in ArcSight Database.

Planning to Integrate Tenants from ArcSight ESM

You can integrate a multi-tenant enabled ArcSight plantform with ArcSight ESM that is already configured for Multi-tenancy or MSSP. However, you must ensure that the tenant details and user details used in the ArcSight Platform are mapped to the details in ArcSight ESM.

Before integrating, make sure that you have the following details related to ArcSight ESM tenants:

- Number of Tenants in ArSight ESM and their details
- Number of users for each of these tenants and details of user groups
- Customer tag specified for each tenant in ArSight ESM
- External ID for each of the tenant users
- Roles assigned to each of the users

For more information, see "Integrating ESM Data and Users " on page 279

Depending on whether you are upgrading from a previous version of ArcSight Platform, where you have already imported ESM data or it is a new integration, refer to one of the following scenarios:

Scenario 1: New Integration of ArcSight Platform Tenants with ArcSight ESM Tenants

You have a newly installed ArcSight Platform or have upgraded an existing installation and now want to integrate with an ArcSight ESM environment that is Multi-tenant enabled.

In this scenario, gather all the details for ESM tenants and users during planning and while provisioning the provider and onboarding tenants in ArcSight Platform, make sure that you do a one-to-one mapping of the ESM teants and users with the ArcSight tenants and users.

Scenario 2: ArcSight ESM Is Already Integrated With Single Tenant ArcSight Platform

You are upgrading an ArcSight Platform environment that is already integrated with ArSight ESM in Multi-tenant mode.

In this scenario, ArSight ESM data and users are already imported into ArcSight Platform. When you enabe Multi-tenancy in ArcSight Platform, all the imported ESM data and users will be migrated to the default tenant. You must manually move these users from the default tenant to their respective tenants, as they are structured in ArSight ESM.

For example, if there are any customer user groups in ArSight ESM, then they must be part of the Provider in ArcSight Platform. For more information, see Move Users from a Provider to a Tenant.

Example: Mapping ArSight ESM Tenant Details with ArcSight Platform Tenant Details

For example, the following table provides a mapping of an ArcSight Platform tenant when ArSight ESM has a provider named Provider X with 2 admin users and 3 tenants with 3 users each. Note that the tenant name and user details are mapped in ArcSight Platform exactly as it is in ArSight ESM.

ArcSight ESM Tenant Details	ArcSight Platform Tenant Details
Customer name: Customer X	**Provider name:** Customer X
Customer User Groups: • user1@customerx.com • user2@customerx.com	**Provider Users:** • user1@customerx.com • user2@customerx.com
Tenant Name: Tenant 1 **Tenant Users:** • t1u1@tenant1.com • t1u2@tenant1.com • t1u3@tenant1.com	**Tenant Name:** Tenant 1 **Tenant Users:** • t1u1@tenant1.com • t1u2@tenant1.com • t1u3@tenant1.com
Tenant Name: Tenant 2 **Tenant Users:** • t2u1@tenant2.com • t2u2@tenant2.com • t2u3@tenant2.com	**Tenant Name:** Tenant 2 **Tenant Users:** • t2u1@tenant2.com • t2u2@tenant2.com • t2u3@tenant2.com
Tenant Name: Tenant 3 **Tenant Users:** • t3u1@tenant3.com • t3u2@tenant3.com • t3u3@tenant3.com	**Tenant Name:** Tenant 3 **Tenant Users:** • t3u1@tenant3.com • t3u2@tenant3.com • t3u3@tenant3.com

Installation Method

Cloud deployments must be installed using the manual installation method. The ArcSight Platform Installer is not supported for cloud deployments.

- AWS deployment

Chapter 3: Creating an Amazon Web Services Deployment

This section explains how to set up your deployment architecture for ArcSight capabilities that runs on the Amazon Web Services (AWS) cloud platform.

Checklist: Creating an AWS Deployment

The complete process of deploying on AWS includes the following steps, which should be performed in the listed order. Each of these steps is explained in the following sections.

	Task	See...
❑	1. Ensure that your AWS environment is ready for deployment	"Understanding the Prerequisites for an AWS Deployment" on the next page
❑	2. Prepare your AWS Deployment environment	
	Create and configure the AWS Virtual Private Cloud, including security groups and IAM roles	
	Create two security groups, one for the bastion host and one for intra-VPC connectivity	
	Create the IAM role for Elastic Kubernetes Service (EKS)	
	Ensure that you have the latest installation files	"Downloading Installation Tools and Packages" on page 117
	Prepare the Elastic File System (EFS) instance used for the AWS deployment environment	"Creating the Elastic File System" on page 118
	Set up your EKS cluster	"Configuring the Elastic Kubernetes Service" on page 128
	Create and label the worker nodes, where application processing takes place	"Creating and Configuring Worker Nodes" on page 141
	Configure a public hosted zone for the OMT structure	"Configuring Route 53" on page 161
	3. Transfer the product images to the Elastic Container Registry (ECR)	"Uploading Product Images to the ECR" on page 167
	4. (Conditional) If you plan to deploy Intelligence or Recon, install the ArcSight Database in AWS	"Installing the Database in AWS " on page 169
❑	5. (Conditional) If you plan to deploy Intelligence, configure settings for Elasticsearch in AWS	"(Conditional – Intelligence) Configuring Settings for Elasticsearch in AWS" on page 188

	6. Install ArcSight capabilities	
	Install basic pods onto the Kubernetes cluster to bootstrap the OMT infrastructure	"Bootstrapping OMT" on page 189
	Ensure that you have secure, trusted communication between pods within the Kubernetes cluster and components outside of the cluster	"Method 1 - Signing the RE External Communication Certificate with Your Trusted Certificate Authority" on page 512
	To create the Application Load Balancer (ALB), import your certificate or a CA-signed certificate into Amazon Certificate Manager	"Creating and Validating the Route 53 Certificate" on page 196
	Configure an ALB to serve as the single point of contact for clients	"Configuring the Application Load Balancer (ALB)" on page 199
	Create and label the worker nodes, where application processing takes place	"Labeling Cloud (AWS) Worker Nodes " on page 223
	Deploy capabilities	"Installing ArcSight in AWS" on page 224
	7. Configure the Load Balancer to serve as the single point of contact for clients	
	Configure access to the OMT management portal and to reconfiguration	"Performing Post Installation Network Configuration" on page 240
❑	8. Post deployment configurations	
	Configure the database and Kafka Scheduler	"Completing the Database Kafka Scheduler Setup - AWS" on page 248
	9. Enable the ArcSight products application (pod) logs in AWS, including FluentD for logging the cluster functionality (Cloudwatch)	"Enabling Pod Logs in AWS" on page 252
	10. Performing Post-deployment Configuration	"Post-deployment Configuration" on page 256
	11. Integrating the Platform Into Your Environment	"Integrating the Platform Into Your Environment" on page 270

Understanding the Prerequisites for an AWS Deployment

To deploy ArcSight capabilities on AWS, the user must have an active AWS subscription, as well a properly configured IAM user account. You perform the installation under the local IAM user. If you do not have a local IAM user, ask your AWS administrator to create a user for you and assign the required IAM policies as described below.

- "Reviewing the Minimal Permissions for IAM User" on the next page
- "Configuring the Local Host" on page 82
- Reviewing Storage Considerations
- "Using the AWS Deployment Worksheet" on page 83

Reviewing the Minimal Permissions for IAM User

Access to various AWS resources is controlled by permissions assigned to the IAM user. For easier management, you can create a policy holding the minimal set of permissions required to complete tasks in this guide. The policy must contain the following permissions.

JSON file for required permissions

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "route53:*",
            "iam:AddRoleToInstanceProfile",
            "iam:AttachRolePolicy",
            "iam:CreateAccessKey",
            "iam:CreateInstanceProfile",
            "iam:CreatePolicy",
            "iam:CreateRole",
            "iam:DeleteAccessKey",
            "iam:DeleteInstanceProfile",
            "iam:DeletePolicy",
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:GenerateServiceLastAccessedDetails",
            "iam:GetAccessKeyLastUsed",
            "iam:GetAccountSummary",
            "iam:GetLoginProfile",
            "iam:GetPolicyVersion",
            "iam:GetRole",
            "iam:GetRolePolicy",
            "iam:GetServiceLastAccessedDetails",
            "iam:GetServiceLastAccessedDetailsWithEntities",
            "iam:GetUser",
            "iam:ListAccessKeys",
            "iam:ListAccountAliases",
            "iam:ListAttachedGroupPolicies",
            "iam:ListAttachedRolePolicies",
            "iam:ListAttachedUserPolicies",
            "iam:ListEntitiesForPolicy",
            "iam:ListGroupPolicies",
            "iam:ListGroups",
```

```
            "iam:ListGroupsForUser",
            "iam:ListInstanceProfiles",
            "iam:ListInstanceProfilesForRole",
            "iam:ListMFADevices",
            "iam:ListOpenIDConnectProviders",
            "iam:ListPolicies",
            "iam:ListPoliciesGrantingServiceAccess",
            "iam:ListPolicyVersions",
            "iam:ListRolePolicies",
            "iam:ListRoleTags",
            "iam:ListRoles",
            "iam:ListSAMLProviders",
            "iam:ListSSHPublicKeys",
            "iam:ListServerCertificates",
            "iam:ListServiceSpecificCredentials",
            "iam:ListSigningCertificates",
            "iam:ListUserPolicies",
            "iam:ListUserTags",
            "iam:ListUsers",
            "iam:ListVirtualMFADevices",
            "iam:PassRole",
            "iam:PutRolePolicy",
            "iam:RemoveRoleFromInstanceProfile",
            "iam:TagRole",
            "iam:TagUser",
            "iam:UntagRole",
            "iam:UntagUser",
            "iam:UpdateAccessKey",
            "iam:UpdateLoginProfile"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "acm:*",
            "autoscaling:*",
            "cloudformation:*",
            "ec2:*",
            "ecr:*",
            "eks:*",
            "elasticfilesystem:*",
            "elasticloadbalancing:*",
            "s3:CreateBucket",
            "s3:DeleteObject",
            "s3:GetObject",
```

```
            "s3:PutObject",
            "sns:ListSubscriptions",
            "sns:ListTopics",
            "ssm:DescribeActivations",
            "ssm:DescribeAssociation",
            "ssm:DescribeAssociationExecutionTargets",
            "ssm:DescribeAssociationExecutions",
            "ssm:DescribeAutomationExecutions",
            "ssm:DescribeAutomationStepExecutions",
            "ssm:DescribeAvailablePatches",
            "ssm:DescribeDocument",
            "ssm:DescribeDocumentParameters",
            "ssm:DescribeDocumentPermission",
            "ssm:DescribeEffectiveInstanceAssociations",
            "ssm:DescribeEffectivePatchesForPatchBaseline",
            "ssm:DescribeInstanceAssociationsStatus",
            "ssm:DescribeInstanceInformation",
            "ssm:DescribeInstancePatchStates",
            "ssm:DescribeInstancePatchStatesForPatchGroup",
            "ssm:DescribeInstancePatches",
            "ssm:DescribeInstanceProperties",
            "ssm:DescribeInventoryDeletions",
            "ssm:DescribeMaintenanceWindowExecutionTaskInvocations",
            "ssm:DescribeMaintenanceWindowExecutionTasks",
            "ssm:DescribeMaintenanceWindowExecutions",
            "ssm:DescribeMaintenanceWindowSchedule",
            "ssm:DescribeMaintenanceWindowTargets",
            "ssm:DescribeMaintenanceWindowTasks",
            "ssm:DescribeMaintenanceWindows",
            "ssm:DescribeMaintenanceWindowsForTarget",
            "ssm:DescribeOpsItems",
            "ssm:DescribeParameters",
            "ssm:DescribePatchBaselines",
            "ssm:DescribePatchGroupState",
            "ssm:DescribePatchGroups",
            "ssm:DescribePatchProperties",
            "ssm:DescribeSessions",
            "ssm:GetAutomationExecution",
            "ssm:GetCommandInvocation",
            "ssm:GetConnectionStatus",
            "ssm:GetDefaultPatchBaseline",
            "ssm:GetDeployablePatchSnapshotForInstance",
            "ssm:GetDocument",
            "ssm:GetInventory",
            "ssm:GetInventorySchema",
            "ssm:GetMaintenanceWindow",
```

```
            "ssm:GetMaintenanceWindowExecution",
            "ssm:GetMaintenanceWindowExecutionTask",
            "ssm:GetMaintenanceWindowExecutionTaskInvocation",
            "ssm:GetMaintenanceWindowTask",
            "ssm:GetManifest",
            "ssm:GetOpsItem",
            "ssm:GetOpsSummary",
            "ssm:GetParameter",
            "ssm:GetParameterHistory",
            "ssm:GetParameters",
            "ssm:GetParametersByPath",
            "ssm:GetPatchBaseline",
            "ssm:GetPatchBaselineForPatchGroup",
            "ssm:GetServiceSetting",
            "ssm:ListAssociationVersions",
            "ssm:ListAssociations",
            "ssm:ListCommandInvocations",
            "ssm:ListCommands",
            "ssm:ListComplianceItems",
            "ssm:ListComplianceSummaries",
            "ssm:ListDocumentVersions",
            "ssm:ListDocuments",
            "ssm:ListInstanceAssociations",
            "ssm:ListInventoryEntries",
            "ssm:ListResourceComplianceSummaries",
            "ssm:ListResourceDataSync",
            "ssm:ListTagsForResource",
            "ssm:PutConfigurePackageResult"
         ],
         "Resource":"*"
      }
   ]
}
```

Configuring the Local Host

To configure a local host:

You can configure and use any local host which has Internet access for the initial steps in setting up your deployment environment. Later, you will create a bastion instance, and use the bastion to perform the installation, as well as to access the cluster after installation.

Requirements: The `AWS CLI` (v2) and `jq` tools must be installed on the local host. `AWS CLI` is a unified tool to manage AWS services. If it is not already installed, then install and configure the `AWS CLI` (version 2) tool for your platform. All references to CLI in this guide refer to the `AWS CLI` version 2 interface.

- Amazon provides the instructions for installing AWS CLI.
- After installation, configure the `AWS CLI` to properly authenticate and connect to AWS as described in Configuring AWS CLI.

> Most procedures for configuring AWS are supplied in both the AWS CLI and web UI versions.

`jq` is a lightweight and flexible open-source command-line JSON processor.

- You can download the `jq` binaries from the `jq` homepage.

Reviewing Storage Considerations

Your cloud administrator needs to setup AWS S3 storage before you install the database. When setting up the AWS instance, do not create a folder for the database in the S3 bucket. You can create a folder on the database node during database installation, but you cannot configure a folder pre-created in AWS during installation.

Your cloud administrator will also need to set up default encryption for the S3 bucket before installing the database. For information about enabling S3 bucket encryption, see AWS documentation, *Enabling Amazon S3 default bucket encryption*.

In the ArcSight Platform, you can organize data into **storage groups**, which allows you to partition the incoming events data and provide different retention periods, based on the query filter. To preserve space in the database and improve data retrieval from storage groups, you can configure the database to remove events older than a certain number of months. Your product license affects the maximum value that you set for the data retention policy.

Using the AWS Deployment Worksheet

To use the worksheet:

The process of setting up an AWS deployment environment will require configuration of many AWS resources. As a result, you will need convenient access to important details of these resources, such as resource names, IP addresses, settings for AWS entities, and so on, which you will determine during the setup process.

For ease of reference, it's strongly recommended that you print out and use the AWS worksheet to record the details of your configuration. The procedures given here assume you are using the worksheet for reference and will note when particular details should be recorded.

Using AWS Configuration Worksheets

During the setup and configuration of your AWS deployment environment, use the following worksheets.

- "AWS Infrastructure Settings" below
- "Subnets" below
- "Security Groups" on the next page
- System and Environment Settings

AWS Infrastructure Settings

Region	
Vpc ID	
Vpc CIDR	
Vpc Name	
Cluster Name	
Public IP ID	
Public IP	
Internet GW ID	
NAT GW ID	
DNS Enabled (Y/N)	
Hostname Resolution Enabled (Y/N)	

Subnets

Availability Zone	*CIDR*	*Name*	*ID*	*Tagged Load Balancing *Y/N/NA*

Subnets

Availability Zone	*CIDR*	*Name*	*ID*	*Tagged Load Balancing *Y/N/NA*

Security Groups

Bastion Security Group Name	
Bastion Security Group ID	
Intra VPC Security Group Name	
Intra VPC Security Group ID	
IAM Roles	
EKS Role Name	
EKS Role ARN	
EKS Instance Profile Name	
EKS Instance Profile ARN	
Workernodes Role Name	
Workernodes Role ARN	
Workernodes Instance Profile Name	
Workernodes Instance Profile ARN	

System and Environment Settings

Bastion	Kubernetes Version	
	Key Pair Name	
	Key Pair Fingerprint	
	Image ID	

	Instance Type	
	Instance ID	
	Public IP Address	
EFS	EFS Name	
	FileSystemID	
	Filesystem FQDN	
	Mount Target 1 ID	
	Mount Target 2 ID	
	Mount Target 3 ID	
	Parent Folder Name	
EKS	Cluster ARN	
Worker Nodes	Launch Template Name	
	Launch Template AMI ID	
	Instance Type	
	Autoscaling Group Name	
	Instance IDs	
ECR Registry Upload	Organization Name	
Route 53 Records	Name In Hosted Zone	
	Hosted Zone Name	
	Hosted Zone ID	
	RecordSet Name	
	Certificate ARN	
Networking	ALB Name	
	ALB ARN	
	ALB DNS Name	
	ALB Canonical Hosted Zone ID	
	Node Port for 3000	
	Target Group 3000 Name	

	Target Group 3000 ARN	
	Target Group 5443 Name	
	Target Group 5443 ARN	
	Target Group 443 Name	
	Target Group 443 ARN	

Preparing the AWS Deployment Environment

The tasks involved to prepare your AWS environment are included in this section.

Setting Up an AWS Virtual Network

The section prepares your AWS virtual network.

Create the Virtual Private Cloud

An VPC is a virtual network. For more information, see Amazon VPC.

- "Creating the VPC" below
- "Enabling DNS and Hostname Resolution" on the next page

Creating the VPC

To create the VPC, in the AWS CLI, run the following command:

```
# aws ec2 create-vpc \
--cidr-block <CIDR allocated for new VPC> \
| jq -r '.Vpc.VpcId'
```

The command will return the new VPC's VPC ID. Record the VPC ID and VPC CIDR to the AWS worksheet.

For example below is an input and output:

```
# aws ec2 create-vpc \
--cidr-block 10.0.0.0/16 \
| jq -r '.Vpc.VpcId'
```

```
vpc-0143197ca9bd9c117
```

To (optionally) verify assigned tags:

Run the command:

```
# aws ec2 describe-tags \
--filters "Name=resource-id,Values=<VPC ID>"
```

For example:

```
# aws ec2 describe-tags \
--filters "Name=resource-id,Values=vpc-0143197ca9bd9c117"
```

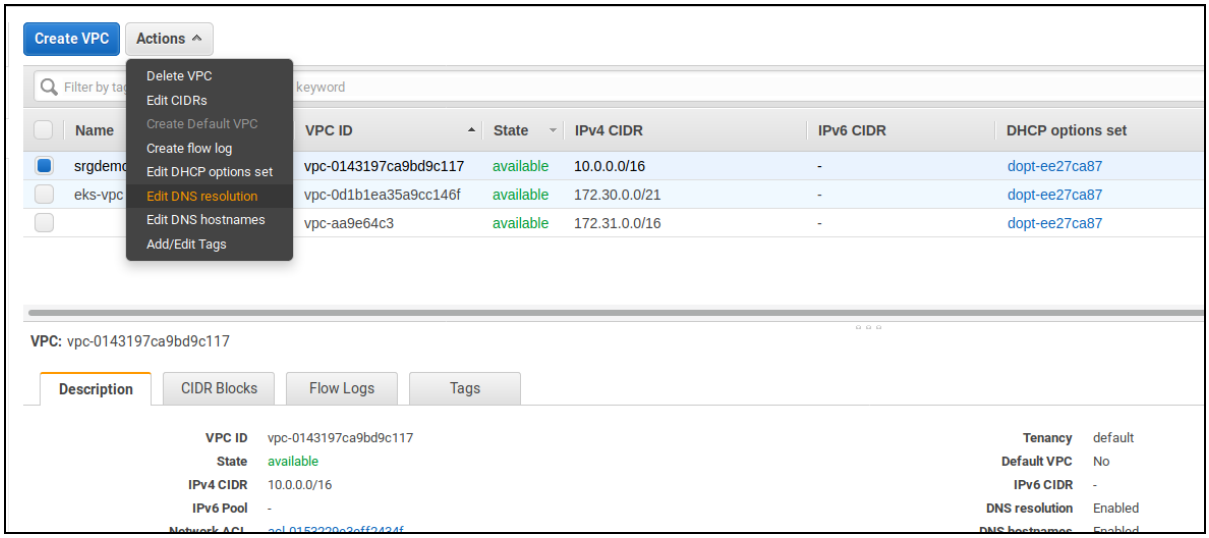

```
{
                        "Tags":[
                        {
                        "Key":"Name",
                        "ResourceId":"vpc-0143197ca9bd9c117",
                        "ResourceType":"vpc",
                        "Value":"srgdemo-vpc"
                        },
                        {
                        "Key":"kubernetes.io/cluster/srgdemo-cluster",
                        "ResourceId":"vpc-0143197ca9bd9c117",
                        "ResourceType":"vpc",
                        "Value":"shared"
                        }
                        ]
                }
```


Enabling DNS and Hostname Resolution

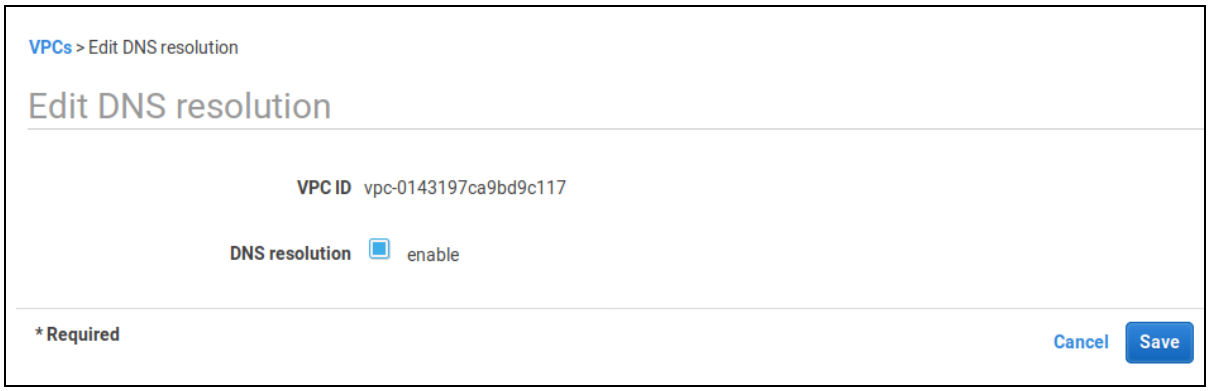
DNS support and hostname resolution should be enabled to make IP addresses more easily human-readable.

To enable DNS using the web UI:

1. Using the Find Services search tool, locate and browse to the VPC dashboard.
2. On the left navigation panel, under **Virtual Private Cloud,** click **Your VPCs.**
3. Select the check box corresponding to your VPC. Then, under **Actions**, select **Edit VPC settings**.



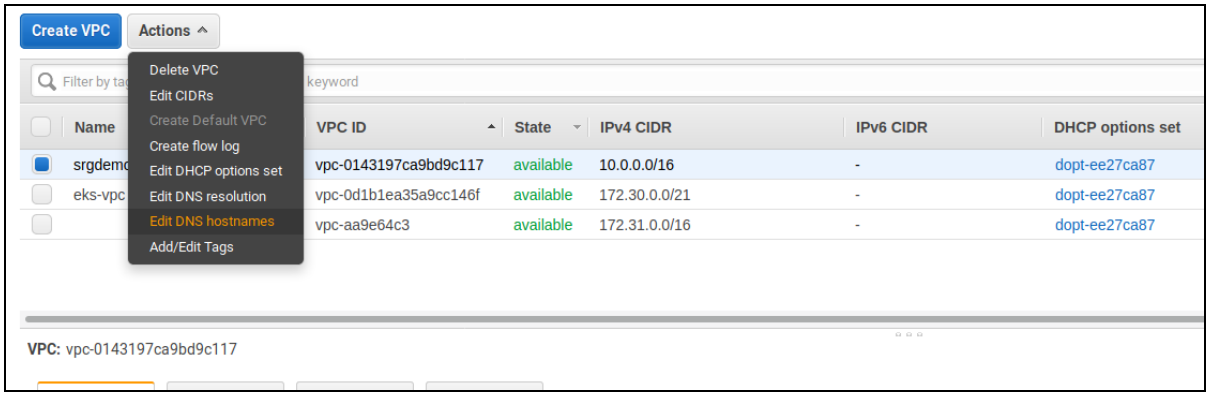
4. On the **Edit DNS Resolution** page, for **DNS resolution**, select the **enable** check box.



5. Click **Save**, then click **Close**.

To enable hostname resolution using the web UI:

1. Using the **Find Services** search tool, locate and browse to the VPC dashboard.
2. On the left navigation panel, under **Virtual Private Cloud**, click **Your VPCs.**
3. Select the check box corresponding to your VPC. Then, under **Actions**, select **Edit VPC settings**.



4. On the **Edit VPC Settings** page, for **DNS hostnames**, select the **enable** check box.
5. Click Save, then click **Close**.

To enable DNS using the AWS CLI:

Execute the following commands *in order*, using the VPC ID of your created VPC:

```
# aws ec2 modify-vpc-attribute \
--vpc-id <VPC Id> \
--enable-dns-support

# aws ec2 modify-vpc-attribute\
 --vpc-id <VPC Id> \
--enable-dns-hostnames
```

These commands have no output.

For example:

```
# aws ec2 modify-vpc-attribute \
--vpc-id vpc-0143197ca9bd9c117 \
--enable-dns-support
# aws ec2 modify-vpc-attribute \
--vpc-id vpc-0143197ca9bd9c117 \
--enable-dns-hostnames
```

Create the External IP Address

The external IP address (EIP) is required for the NAT Gateway, used by the worker nodes, to access the Elastic Container Registry (ECR). In this step, you will create the EIP and then tag it.

- "Creating the EIP" on the next page
- "Tagging the EIP" on the next page

Creating the EIP

1. Run the following command:

```
aws ec2 allocate-address --domain vpc
```

2. Record the `AllocationId` value in the AWS worksheet.

   For example:

```
{
"PublicIp": "18.194.179.100",
"AllocationId": "eipalloc-004be822658206abe",
"PublicIpv4Pool": "amazon",
"NetworkBorderGroup": "eu-central-1",
"Domain": "vpc"
}
```

Tagging the EIP

Run the following command:

```
aws ec2 create-tags \
--resources <Allocation Id> \
--tags Key=Name,Value=<eip-name>
```

Where:

- `<Allocation Id>`: Use the Allocation ID of the EIP.
- `<eip-name>`: Assign an EIP name for easier identification.

For example:

```
aws ec2 create-tags \
--resources eipalloc-004be822658206abe \
--tags Key=Name,Value=srgdemo-eip
```

Creating and Tagging the Subnets

In this section, you will create one private and one public subnet for each of the three availability zones, for a total of six subnets. Each availability zone requires one private and one public subnet to support high availability.

- "Creating a Subnet" on the next page
- "Tagging the Subnets" on page 93

Each subnet must meet the following criteria:

- Each subnet comes from the VPC IP range.
- Subnets must not overlap one another.

All six subnets will be created in the same way. They will be distinguished based on the:

- Route table
- Internet gateway
- NAT gateway attachments

Before proceeding, make sure you have completed your AWS worksheet with your subnet names, CIDRs, and availability zones.

Creating a Subnet

1. Retrieve the availability zone names by running the following command:

```
# aws ec2 describe-availability-zones \
| jq -r '.AvailabilityZones[ ].ZoneName'
```

   Example output:

```
eu-central-1a
```

```
eu-central-1a
```

```
eu-central-1b
```

```
eu-central-1c
```

2. Create the first subnet by running the following command, which will output the subnet ID:

```
# aws ec2 create-subnet \
--availability-zone <availability zone> \
--cidr-block <CIDR> --vpc-id <VpcId> | jq -r '.Subnet.SubnetId'
```

   For example:

```
# aws ec2 create-subnet \
--availability-zone eu-central-1a \
--cidr-block 10.0.1.0/24 \
```

```
--vpc-id vpc-0143197ca9bd9c117 | jq -r '.Subnet.SubnetId'
```

```
subnet-06a8caab19022c544
```

3. Repeat Step 2 for all rows from the subnet planning table in the AWS worksheet.

You should now tag the new subnets to differentiate between public and private subnets, as well as tag the private subnets for load balancing.

Tagging the Subnets

1. Tag each **public** subnet by running the following command for each public subnet:

```
# aws ec2 create-tags \
--resources <public subnet id> \
--tags Key=Name,Value=<subnet name>
```

1. Tag each **private** subnet by running this command for each private subnet:

```
# aws ec2 create-tags \
--resources <private subnet id> \
--tags Key=Name,Value=<subnet name> Key=kubernetes.io/role/internal-
elb,Value=1
```

Where:

- `<public/private subnet id>`: The value from column **Subnet ID** in your planning table on the AWS worksheet.
- `<public/private subnet name>`: The value from column **Subnet name** in your planning table on the AWS worksheet.

For example:

```
# aws ec2 create-tags \
--resources subnet-06a8caab19022c544 \
--tags Key=Name,Value=srgdemo-public-subnet-1
```

```
# aws ec2 create-tags \
--resources subnet-0fb2ebb5882c061f0 \
--tags Key=Name,Value=srgdemo-private-subnet-1
Key=kubernetes.io/role/internal-elb,Value=1
```

Creating the Internet Gateway

The Internet gateway is the prerequisite for the NAT gateway, which will be created later.

To create the internet gateway and attach it to the VPC:

1. Run the following command:
   `aws ec2 create-internet-gateway`

Example output:

```
{
   "InternetGateway":{
      "Tags":[

      ],
      "InternetGatewayId":"igw-0ddcfa7511fe10b43",
      "Attachments":[

      ]
   }
}
```

2. Record the value of `InternetGatewayId` in your AWS worksheet.
3. Optionally, you might tag the internet gateway by running the following command:
   `aws ec2 create-tags --resources <InternetGatewayId> --tags Key=Name,Value=<internet gateway name>`
4. Attach the internet gateway to your previously-created VPC by running the following command (command has no output):
   `aws ec2 attach-internet-gateway --internet-gateway-id <InternetGatewayId> --vpc-id <VPC Id>`

For example:

```
aws ec2 attach-internet-gateway \
--internet-gateway-id igw-0ddcfa7511fe10b43 \
--vpc-id vpc-0143197ca9bd9c117
```

Creating the NAT Gateway

The NAT gateway is required for worker nodes to connect to the Elastic Container Registry (ECR), which is used for downloading OMT and product images.

To create the NAT gateway:

1. Run the following command:
   `aws ec2 create-nat-gateway \`
   `--allocation-id <EIP allocation Id> \`
   `--subnet-id <public subnet id>`

Example input and output:

```
aws ec2 create-nat-gateway \
--allocation-id eipalloc-004be822658206abe \
--subnet-id subnet-0c0ca63f2f793907d
```

```
{
   "NatGateway":{
      "CreateTime":"2021.05-20T20:53:01.000Z",
      "NatGatewayAddresses":[
         {
            "AllocationId":"eipalloc-004be822658206abe"
         }
      ],
      "NatGatewayId":"nat-013416dad7b7656ea",
      "State":"pending",
      "SubnetId":"subnet-0c0ca63f2f793907d",
      "VpcId":"vpc-0143197ca9bd9c117"
   }
}
```

2. Record the `NatGatewayId` value in your AWS worksheet.

Creating the Route Tables

Route tables define the routing paths between resources in private and public subnets and the Internet.

To create the private and public route tables:

1. Run the following command to create a route table and retrieve its ID:

   ```
   aws ec2 create-route-table \
   --vpc-id <VpcId> \
   | jq -r '.RouteTable.RouteTableId'
   ```

2. Run the command in Step 1 a second time, to create another route table and retrieve its ID.

Example input and output:

```
aws ec2 create-route-table \
--vpc-id vpc-0143197ca9bd9c117 \
| jq -r '.RouteTable.RouteTableId'
```

```
rtb-0deda70daa09ca3bfw
```

3. Tag the first route table as private. Run the command:

```
aws ec2 create-tags --resources <route table ID> \
--tags Key=Name,Value=<route table name indicating private>
```

Example:

```
aws ec2 create-tags \
--resources rtb-0deda70daa09ca3bf \
--tags Key=Name,Value=srgdemo-private-route-table
```

4. Repeat Step 3 for the second route table, with the `--tags` value indicating `public` instead of `private`.

Associating the Route Tables to Subnets

The route tables will now need to be associated to the subnets you have created.

To associate the route tables to your public subnets:

1. Select one of your **public** subnets.
2. Associate the **public** route table to the selected **public** subnet by running the command:

```
aws ec2 associate-route-table \
--route-table-id <public route table ID> \
--subnet-id <public subnet ID>
```

3. Repeat the command in Step 2 for each of the other two **public** subnets.

To associate the route tables to your private subnets:

1. Select one of your **private** subnets.
2. Associate the **private** route table to the selected **private** subnet by running the command:

```
aws ec2 associate-route-table \
--route-table-id <private route table ID> \
--subnet-id <private subnet ID>
```

3. Repeat the command in Step 2 for each of the other two **private** subnets.

Example input and output:

```
aws ec2 associate-route-table \
--route-table-id rtb-0deda70daa09ca3bf \
--subnet-id subnet-0fb2ebb5882c061f0
```

```
{
   "AssociationId":"rtbassoc-781d0d1a",
   "AssociationState":{
      "State":"associated"
   }
}
```

Adding the NAT Gateway Route Path to the Private Route Table

To add the NAT gateway route path to the private route table:

1. Run the following command:

   ```
   aws ec2 create-route \
   --route-table-id <private route table Id> \
   --destination-cidr-block "0.0.0.0/0" \
   --nat-gateway-id <NAT GW Id>
   ```

2. The command will return the creation status. A status of `true` indicates that the request succeeded.

Example input and output:

```
aws ec2 create-route \
--route-table-id rtb-0deda70daa09ca3bf \
--destination-cidr-block "0.0.0.0/0" \
--nat-gateway-id nat-013416dad7b7656ea
```

```
{
   "Return":true
}
```

Adding the Internet Gateway Route Path to the Public Routing Table

To add the Internet Gateway route path to the public routing table:

1. Run the following command:

```
aws ec2 create-route \
--route-table-id <public route table Id> \
--destination-cidr-block "0.0.0.0/0" \
--gateway-id <Internet Gateway Id>
```

Example:

```
>aws ec2 create-route \
--route-table-id rtb-0fa9f294a3743c9aa \
--destination-cidr-block "0.0.0.0/0" \
--gateway-id igw-0ddcfa7511fe10b43
```

Creating Security Groups

A *security group* is an AWS resource that acts as a firewall for the subnets. Every AWS resource must be assigned a security group so they will be network accessible. If a resource is assigned to multiple security groups, then all rules from all groups will be applied to the resource.

You will need to create two security groups, one for the bastion host and one for intra-VPC connectivity. The procedures are explained in the following sections.

Creating the Security Group for the Bastion Host

In order to connect to the bastion from the Internet and perform the configuration and installation tasks, you must open the connection on the default SSH port (port 22) from any address.

> Optionally, you can limit the access to the bastion by specifying your own public, static IP address while adding your own inbound rule as described below. Replace `0.0.0.0/0` with your own public IP address. If you choose to specify your own IP address, talk to your AWS infrastructure administrator before proceeding.

To create the security group for the bastion host:

1. Run the following command:

```
# aws ec2 create-security-group \
--description "Enables SSH Access to Bastion Hosts" \
--group-name <group name> --vpc-id <VpcId>
```

Where:

`<group name>`: A descriptive security group name of your choice; in our examples we will use `srgdemo-bastion-sg`.

`<VpcID>`:The VPC ID of the VPC you created earlier.

Example:

```
aws ec2 create-security-group \
--description "Enables SSH Access to Bastion Hosts" \
--group-name srgdemo-bastion-sg \
--vpc-id vpc-0143197ca9bd9c117
```

```
{
   "GroupId":"sg-00b5fcc4294d234f6"
}
```

2. Record the bastion security group ID in your AWS worksheet.

Adding the Inbound Rule

You will connect to the bastion using SSH on default port 22, so the newly-created security group needs to be opened to inbound connection on port 22 and the TCP protocol.

To add the inbound rule:

1. Open the security group to inbound connections on the default SSH port 22 (TCP) by running the following command:

```
aws ec2 authorize-security-group-ingress \
--group-id <bastion security group ID> \
--ip-permissions IpProtocol=tcp,FromPort=22,ToPort=22,IpRanges='
[{CidrIp=0.0.0.0/0,Description="SSH access; unlimited."}]'
```

Example:

```
# aws ec2 authorize-security-group-ingress \
--group-id sg-00b5fcc4294d234f6 \
--ip-permissions
```

2. Remove the default wide-open outbound rule by running the following command:

```
aws ec2 revoke-security-group-egress \
--group-id <security group ID> \
--protocol all \
--port -1 \
--cidr 0.0.0.0/0
```

While working from the bastion you will need to connect to various resources on the internet. Protocols and description for ports are shown in the following table

Port	Protocol	Allowed CIDR	Description
80	TCP	`0.0.0.0/0`	HTTP
443	TCP	`0.0.0.0/0`	HTTPS

3. Add HTTP and HTTPS outbound rules by running the following command:

```
aws ec2 authorize-security-group-egress \
--group-id sg-00b5fcc4294d234f6 \
--ip-permissions IpProtocol=tcp,FromPort=80,ToPort=80,IpRanges='
[{CidrIp=10.0.0.0/0,Description="HTTP"}]'
```

In the command above, the values for `<FromPort>` and `<ToPort>` correspond to the `Port` value in the table, and `<IpProtocol>` and `<Description>` to the `Protocol` and `Description` values in the table, respectively.

Example:

```
aws ec2 authorize-security-group-egress \
--group-id sg-00b5fcc4294d234f6 \
--ip-permissions IpProtocol=tcp,FromPort=22,ToPort=22,IpRanges='
[{CidrIp=0.0.0.0/0,Description="SSH access; unlimited."}]'
```

Creating the Security Group for Intra-VPC Communication

The intra-VPC security group (SG) is dedicated to resources inside the VPC, and will allow unlimited communication between them. It will also allow outbound connection to the HTTP and HTTPS worldwide.

To create the security group for intra-VPC communication, use the same steps for creating the bastion's security group. However, for the new group, change the description of the security group to an appropriate value, such as `<cluster name> intra VPC SG`.

- Note the group's name and ID to the AWS worksheet.
- Remove the default wide-open outbound rule. Repeat the process you performed for the bastion security group, of course using the newly-created intra-VPC security group ID.

Add inbound rule from itself

For communication between intra-VPC resources, we will add a rule enabling all communication coming from this security group. For example:

```
aws ec2 authorize-security-group-ingress \
--group-id <Intra-vpc security group ID> \
--protocol all \
--port -1 \
--source-group <Bastion security group ID>
```

Where `<security group ID>` is the ID of the newly-created intra-VPC security group.

Add HTTP and HTTPS outbound rules

For retrieving external resources (such as for OMT) and product images from the ECR, OS updates, and similar files, resources inside the VPC need to be able to connect using HTTP/HTTPS on the internet. Repeat the process you performed for the bastion security group.

To add outbound rule to itself, run the following command:

```
aws ec2 authorize-security-group-egress \
--group-id <security group Id> \
--protocol all \
--port -1 \
--cidr <VPC CIDR>
```

- `<security group ID>`: Use the ID of the newly-created intra-VPC security group.
- `<VPC CIDR>`: Use the same CIDR you used for creating the VPC.

Creating and Configuring the Bastion

The bastion is the dedicated host which provides secure access to Linux instances located in the private and public subnets of your virtual private cloud (VPC). The bastion host must be located in the management subnet you created earlier. In this section, you will configure the bastion for your deployment environment.

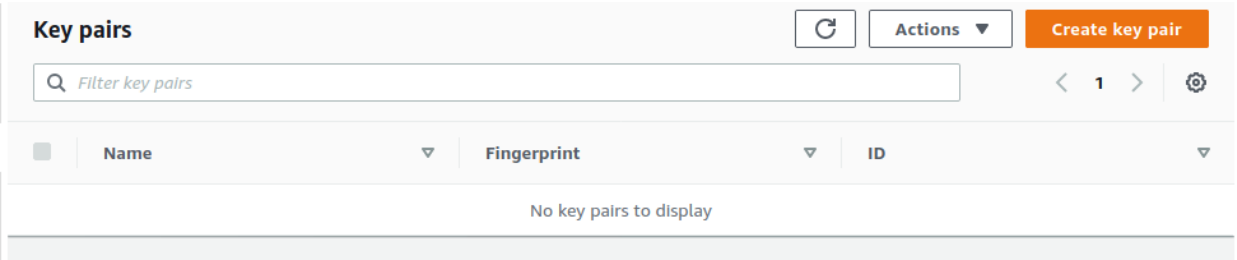
Creating the SSH Keypair

In order to connect to and perform tasks on the bastion, you will use SSH with keypair authentication. In this section, you will create a key pair and store its private value and fingerprint to local files.

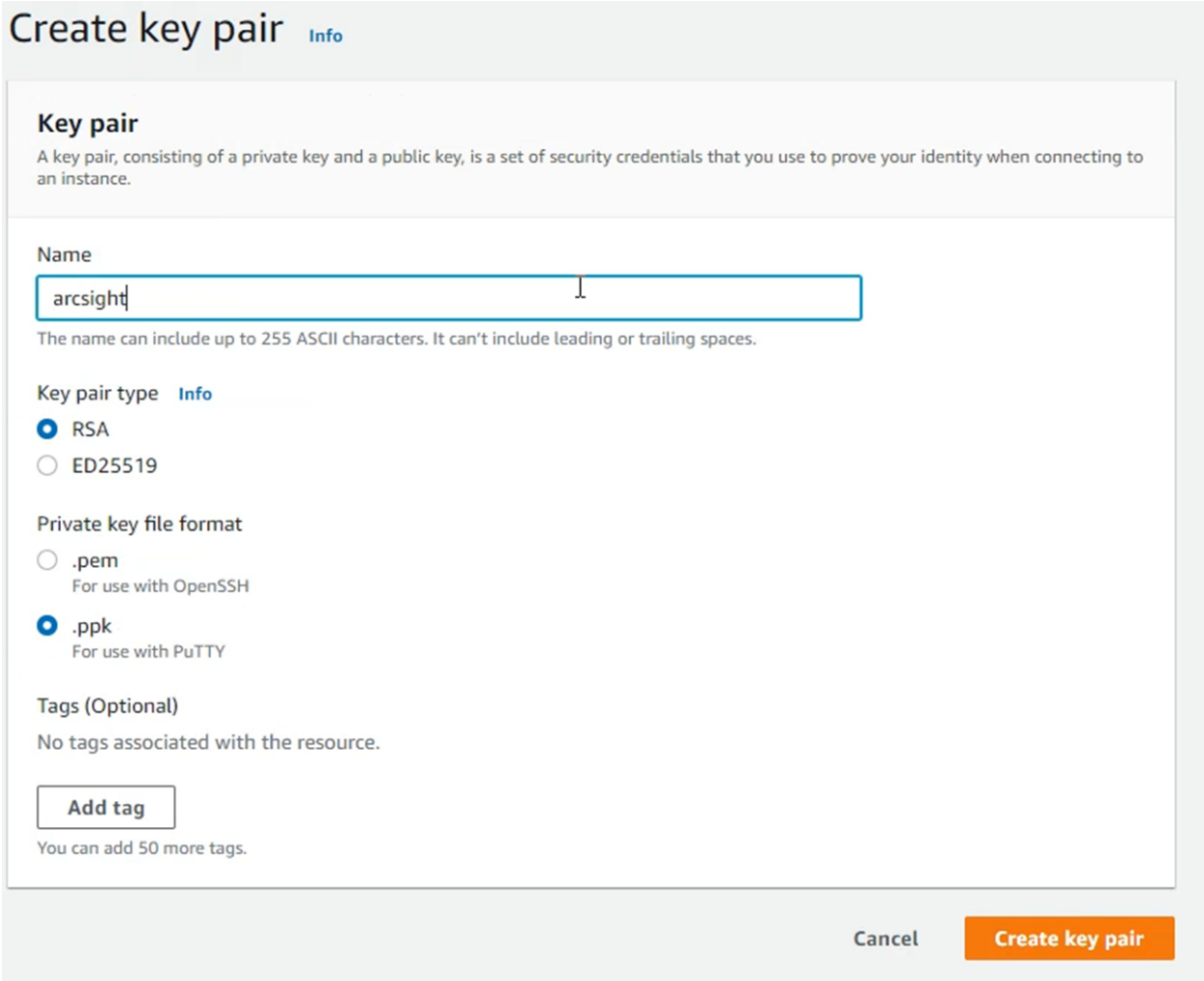
> The SSH keypair will be used later for instantiating worker nodes. Optionally, you can create a separate keypair for the bastion and for worker nodes. In that case, follow the steps described here, and give each keypair a distinct name.

To create the keypair using the web UI:

1. Using the Find Services search tool, locate and browse to the EC2 dashboard.
2. In the left navigation pane, under **Network and Security**, select **Key Pairs**
3. On the **Key Pairs** management dialog, click **Create key pair.**



4. On the **Create Key Pair** page, specify values for the following:
   - **Name:** The key pair name will be later used for instantiating bastion as well as worker nodes. You will also use it as a CLI parameter when using an SSH client.
   - **File format:** Choose the format suitable for your client; check the description as shown.



5. Click **Create Key Pair.**
6. On the **Key pair** management dialog, save the private part to a secure location when prompted.

> **You *must* save the value now, and will not be able to save it later.**

5. Optionally, save the key pair fingerprint to the same secure location. The optimal way to store this value is in the file named the same as the private part, exchanging the suffix. For example:
   `srgdemo.fingerprint.`
   You can later compare your locally-stored fingerprint value with the one presented on the table on the web UI.
6. To store the fingerprint value, copy the value in the **Fingerprint** column to a text document on your local host.

7. Record the keypair name and keypair fingerprint to the AWS worksheet.

To create the SSH key pair using the CLI:

1. Specify the following commands:

```
export KEYPAIR_NAME=<Key pair name>
```

```
export KEYPAIR_CREATION=$(aws ec2 create-key-pair \
--key-name ${KEYPAIR_NAME})
```

```
echo $KEYPAIR_CREATION | jq -r '.KeyMaterial' \
| sed "s/\\\\n/\n/g" > ~/.ssh/${KEYPAIR_NAME}.pem
```

```
echo $KEYPAIR_CREATION \
| jq -r '.KeyFingerprint' > ~/.ssh/${KEYPAIR_NAME}.fingerprint
```

```
chmod 400 ~/.ssh/${KEYPAIR_NAME}.pem
```

Replace the `<KEYPAIR_NAME>` value with your real key pair name. In our examples, we use `srgdemo`.

Example commands:

```
export KEYPAIR_NAME=srgdemo
```

```
export KEYPAIR_CREATION=$(aws ec2 create-key-pair \
--key-name ${KEYPAIR_NAME})
```

```
echo $KEYPAIR_CREATION | jq -r '.KeyMaterial' \
| sed "s/\\\\n/\n/g" > ~/.ssh/${KEYPAIR_NAME}.pem
```

```
echo $KEYPAIR_CREATION \
| jq -r '.KeyFingerprint' > ~/.ssh/${KEYPAIR_NAME}.fingerprint
```

```
chmod 400 ~/.ssh/${KEYPAIR_NAME}.pem
```

Determining the AMI ID

Determine the AMI (Amazon Machine Image) ID used for your bastion instance. You can select an OS image and its corresponding AMI from the AWS Marketplace.

Alternatively, you can find AMIs using the Amazon EC2 console. You can select from the list of AMIs when you use the launch wizard to launch an instance, or you can search through all available AMIs using the Images page. AMI IDs are unique to each AWS Region. Open the

Amazon EC2 console at https://console.aws.amazon.com/ec2/. (**Note**: This link opens an external web site.)

You can also get new image IDs by running OS-based commands:

> A subscription may be required for some AMIs in the AWS Marketplace.

For Amazon Linux, run the following command:

```
aws ec2 describe-images --owner amazon --filters
"Name=description,Values=Amazon Linux AMI *" "Name=architecture,Values=x86_
64" "Name=virtualization-type,Values=hvm" "Name=root-device-type,Values=ebs"|
jq '.Images | sort_by(.CreationDate) | [last]'
```

Record the `ImageId` value in the AWS worksheet.

Selecting a Bastion Hardware Instance Type

The type of host to use for your bastion depends on your deployment plans. Amazon offers a detailed list of EC2 Instance Types with hardware specifications for each. Select and prepare a host that balances and optimizes CPU, memory, storage, and pricing.

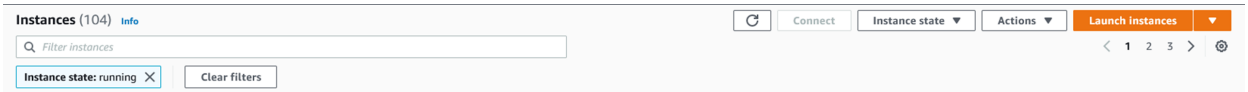
For purposes of examples here, we will assume `t2.medium` as your bastion instance type, which will be used only to perform a few configuration tasks and OMT bootstrap install. Your own environment needs might differ.

Once you've selected a bastion host, record its type in your AWS worksheet.

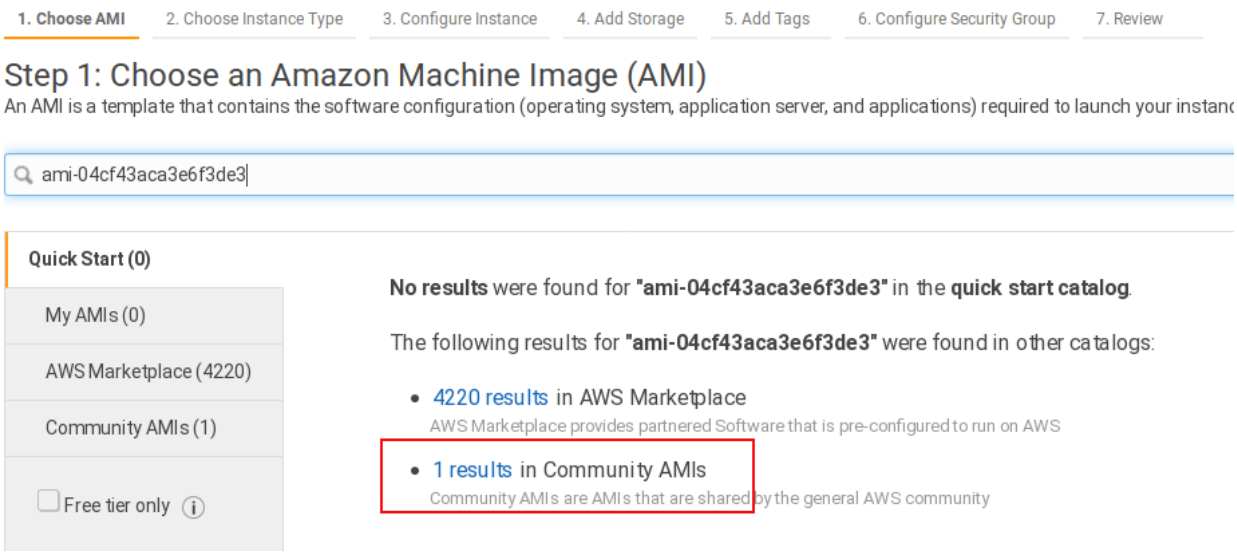
Starting the Bastion Instance

To start the bastion instance through the Web UI:

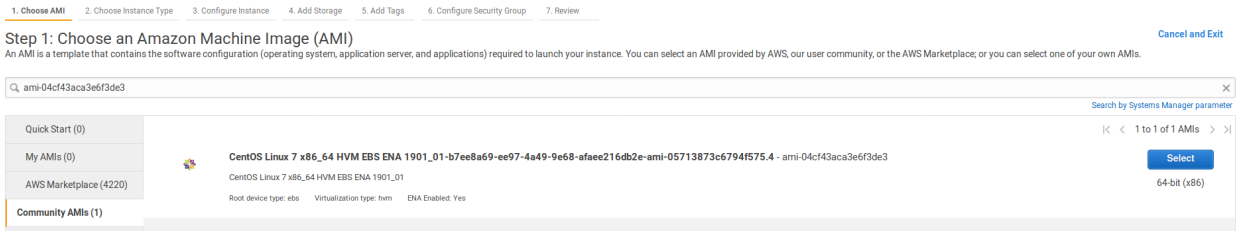
1. Using the Find Services search tool, locate and browse to the EC2 Dashboard.
2. In the left navigation pane, under **INSTANCES**, click **Instances**.
3. On the Instances management dialog, click **Launch Instance** to start the wizard.



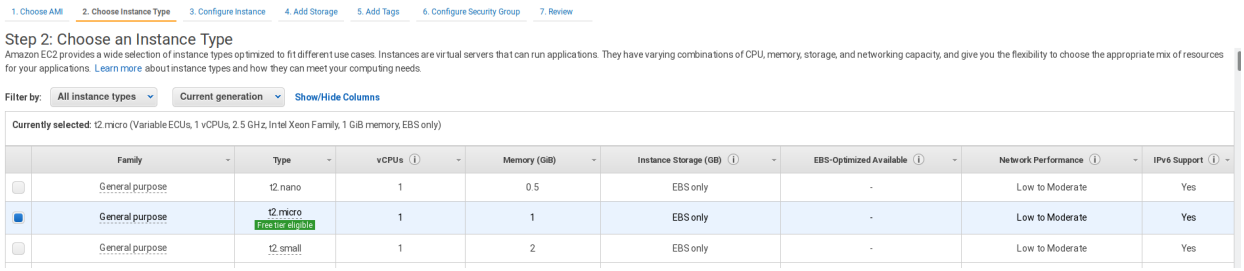
4. On the **Step 1: Choose an AMI** page, in the search box, specify your AMI ID (from your AWS worksheet) and press Enter. The page displays a single result in **Community AMIs.**



5. Click the link for **1 results in Community AMIs.** The selected OS is displayed.
6. Click **Select**.



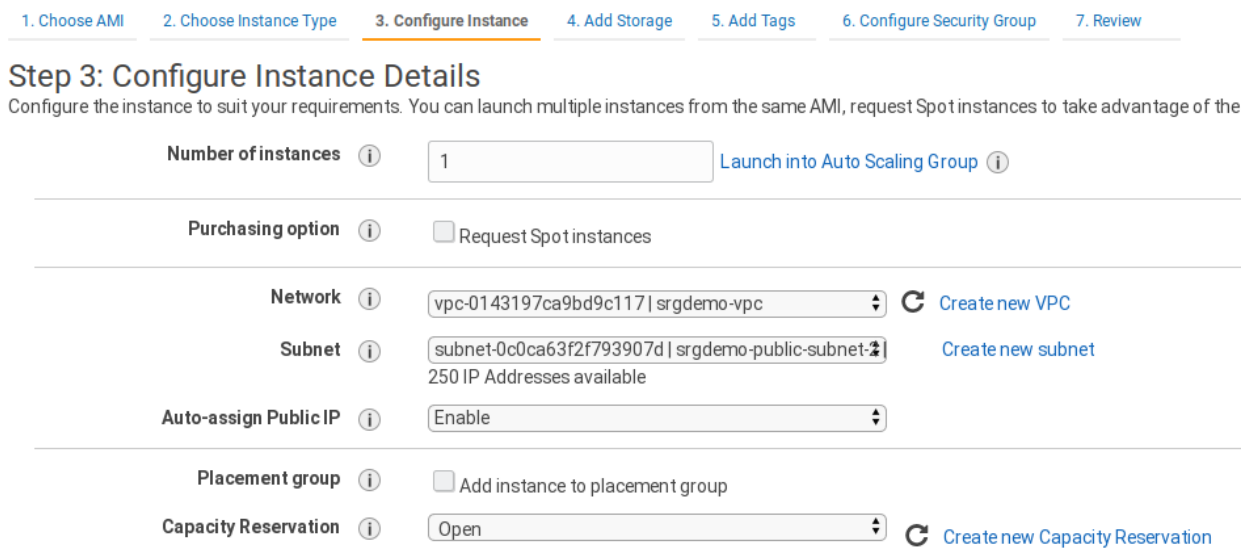
7. On the **Step 2: Choose an Instance Type** page, on the Instance Type list, search for and select your own instance type (use the browser search function if needed). Then, click **Next: Configure Instance Details.**



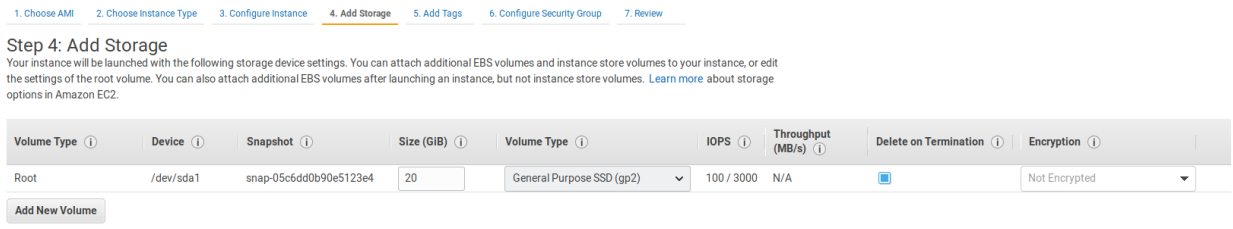
8. On the **Step 3: Configure Instance Details** page, specify these values for the following settings:

- **Network:** Choose your VPC.
- **Subnet:** Choose one of your three public subnets.
- **Auto-assign Public IP:** Enable this value.

9. Click **Next: Add Storage** .

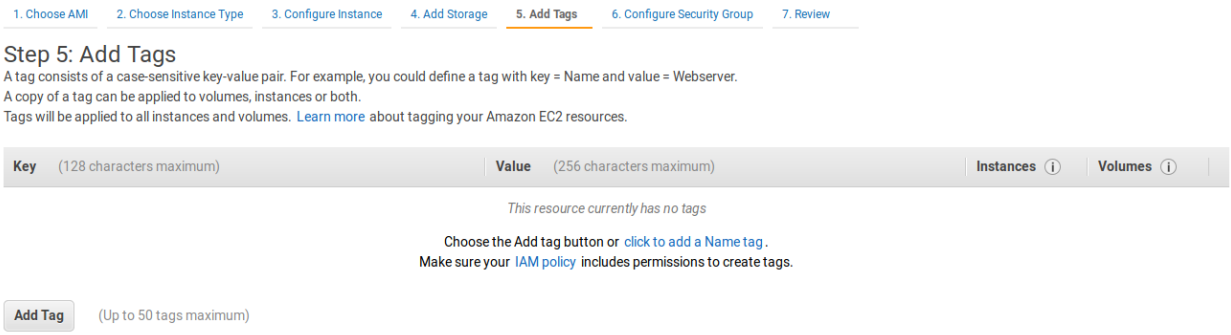


10. On the **Step 4: Add Storage** page, set the root volume size according to your previously-decided needs. In this example, we assume that we will be using it only to upload product images, so we will set it to 20 GB.

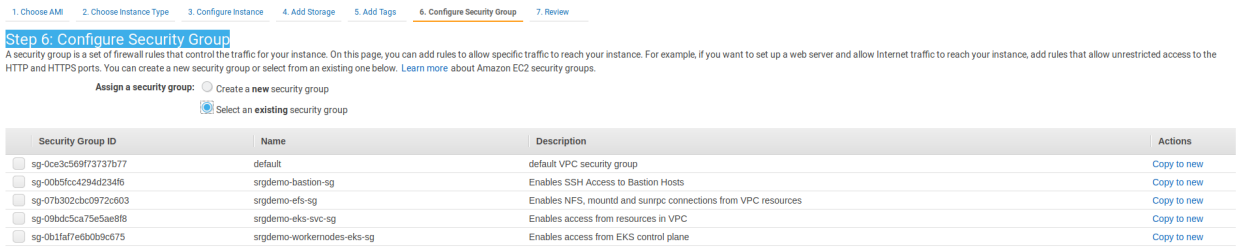


11. Enable **Delete on Termination.**
12. Click **Next: Add Tags**.
13. On the **Step 5: Add Tags** page, click **Add Tag.**
14. Specify and save a tag called *Name* with the value of your bastion name (for example, *srgdemo-bastion.*)

15. Optionally, you can add other tags as needed.
16. Click **Next: Configure Security Group.**

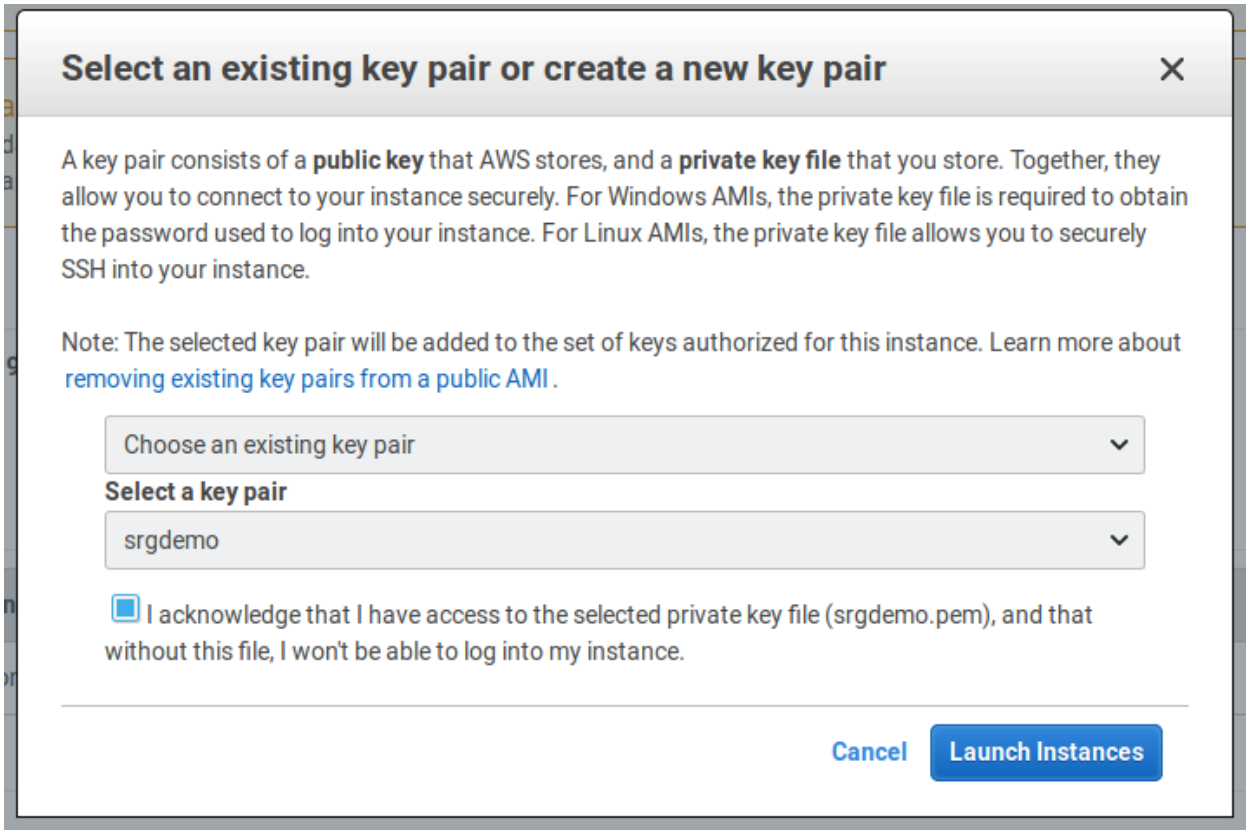


17. On the **Step 6: Configure Security Group** page, under **Assign a security group**, choose **Select an existing security group**.
18. The list shows all security groups associated with your VPC. Select **both** the Bastion security group and Intra VPC security group. (Choose by name or ID from your AWS worksheet.)
19. Click **Review and Launch.**

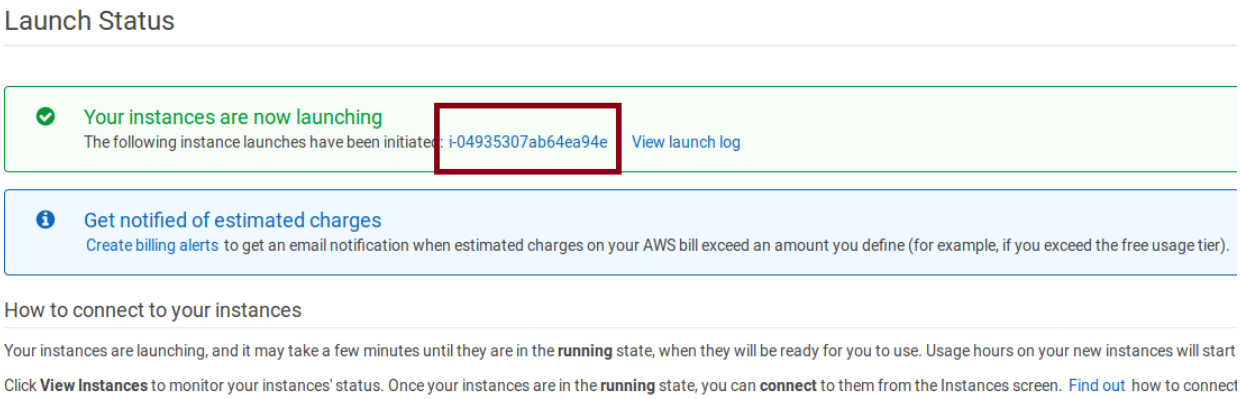


20. On the **Step 7: Review Instance and Launch** page, review all parameters for correctness and fix if necessary. Then click **Launch**.
21. On the **Select an existing key pair...** dialog, pick **Choose an existing key pair** from the drop-down, then select your previously-created key pair.

> **Important!** Confirm that you have the private part of your key pair accessible on your local host. Without the private part, your bastion will not be accessible through SSH.



22. Click **Launch Instances**. The instance is launched and displayed.



23. From on the **Launch Status** page, from the green box, copy your instance ID to your AWS worksheet under Notes.
24. Click **View Instances** to return to the **Instances management** page.

To start the bastion instance using the AWS CLI:

1. Run the following command:

```
aws ec2 run-instances \
--image-id <Image Id> --count 1 \
--instance-type <Instance type> \
--key-name <Key pair name> \
--security-group-ids <security group Ids> \
--subnet-id <public subnet Id> \
--block-device-mappings <device mapping parameters> \
--tag-specifications 'ResourceType=instance,Tags=
[{Key=Name,Value=<bastion instance name>}]' 'ResourceType=volume,Tags=
[{Key=Name,Value=<bastion instance volume name>}]' \
--associate-public-ip-address | jq '.Instances[].InstanceId'
```

Where:

`<Image Id>`: Your AMI ID.

`<Instance type>`: Your bastion type.

`<Key pair name>`: Name of the key pair previously created in SSH Keypair.

`<Security group IDs>`: IDs of the two security groups created by your AWS infrastructure administrators. Add **both** the Bastion Security group Id and Intra VPC Security group ID; separate entries with a single space character.

`<public subnet Id>`: ID of one of the three public subnets created by your AWS infrastructure administrators.

`<Device mapping parameters>`: See the example; used for changing root volume size. For more information about parameters and values, please run:
`aws ec2 run-instances help`.

`<bastion instance name>`: Name assigned to the bastion instance for easier identification.

`<bastion instance volume name>`: Name for the storage volume attached to the current bastion instance.

Example:

```
aws ec2 run-instances --image-id ami-04cf43aca3e6f3de3 \
--count 1 --instance-type t2.medium \
--key-name srgdemo --security-group-ids sg-00b5fcc4294d234f6 sg-
0ce3c569f73737b77 \
--subnet-id subnet-0c0ca63f2f793907d \
--block-device-mappings "DeviceName=/dev/xvda,Ebs=
{VolumeSize=70,VolumeType=gp3}" \
```

```
--tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=srgdemo-
bastion}]' 'ResourceType=volume,Tags=[{Key=Name,Value=srgdemo-bastion-
volume}]' \
--associate-public-ip-address | jq '.Instances[].InstanceId'
```

2. The command returns an instance ID (for example, `i-06773a3ef6acd24f0`). Record your instance ID to the AWS worksheet.
3. Check the instance status by running the following command:

```
aws ec2 describe-instances \
--instance-ids <Instance Id> | jq '.Reservations[].Instances[].State'
```

Example output (JSON):

```
{
   "Code":16,
   "Name":"running"
}
```

4. Repeat the check until the result shows *Name: running*. For example:

```
aws ec2 describe-instances \
--instance-ids i-06773a3ef6acd24f0 | jq '.Reservations[].Instances
[].State'
```

5. For easier identification of your bastion instance, tag it with a name by running the following command:

```
aws ec2 create-tags --resources <Instance Id> \
--tags Key=Name,Value=<tag value>
```

For example:

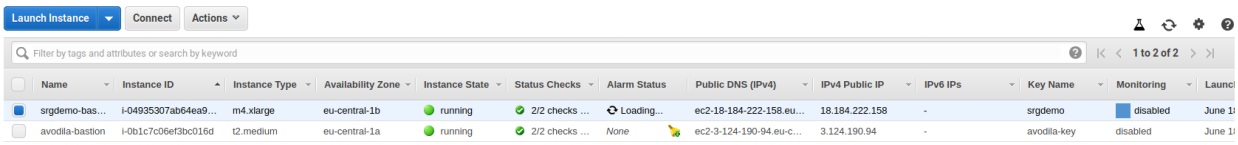
```
aws ec2 create-tags \
--resources i-06773a3ef6acd24f0 \
--tag Key=Name,Value=srgdemo-bastion
```

Retrieving the Bastion Public IP

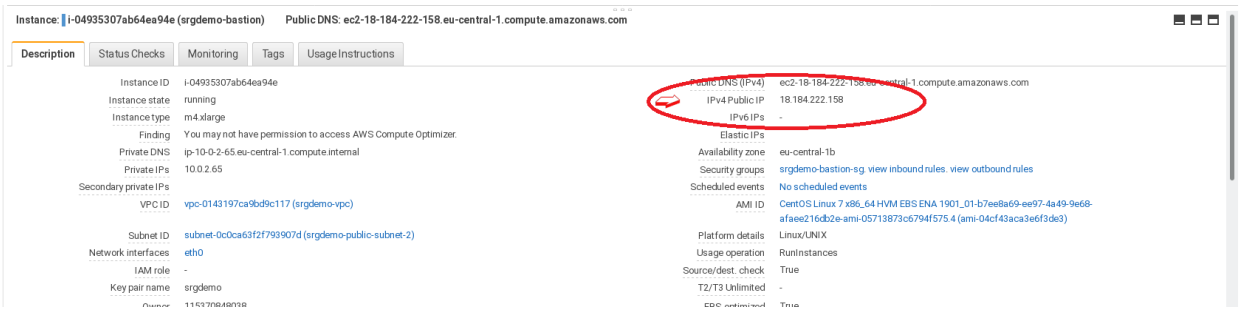
The bastion host provides the only access to the VPC and its resources. Therefore, you will need to know how to connect to it through its public IP address.

To retrieve the bastion public IP address using the Web UI:

1. On the **View Instances** page, select the bastion instance.



2. On the **Description** tab, locate the public IP address.



3. Record the bastion public IP address in the AWS worksheet.

To retrieve the bastion public IP address using the CLI:

1. Run the following command:
```
aws ec2 describe-instances \
--instance-ids <Instance Id> | jq -r '.Reservations[].Instances
[].PublicIpAddress'
```
2. Record the bastion public IP in the AWS worksheet.

Example input and output:

```
aws ec2 describe-instances \
--instance-ids i-06773a3ef6acd24f0 | jq -r '.Reservations[].Instances
[].PublicIpAddress'
```

```
18.184.151.208
```

Connect to Bastion and Install Software Packages

Using the bastion's public IP address and the private part of your key pair, you will connect to the Bastion, install required tools, and perform several configuration tasks.

> In examples, we assume the keypair is stored in `~/.ssh`

To connect to the bastion and install required software packages:

Run the following command:

```
ssh -i ~/.ssh/<key pair name>.pem <OS username>@<Bastion Public IP address>
```

For example, on Amazon Linux:
`ssh -i ~/.ssh/srgdemo.pem ec2-user@18.184.151.208`

Installing `kubectl`

Next, you will need to install the `kubectl` tool for Kubernetes. AWS continually updates the `kubectl` version. You must use the version corresponding to the Kubernetes version used for the cluster (with a tolerance of one minor version).

> To determine the Kubernetes version to use when deploying the ArcSight Platform to AWS, check the Hybrid Cloud Support page of the *Technical Requirements for ArcSight Platform 24.2*.

> You will be managing your EKS cluster with this version of `kubectl`, so its version must match the version required by OMT.

To install `kubectl`:

1. Record the required Kubernetes version in the AWS worksheet.

> In the following list of commands, find the URL for the `kubectl` version on the page Installing kubectl. Then replace the `curl -o kubectl...` command below with the correct command from that page.

2. Run the following commands to configure the bastion:

```
sudo yum install -y vim docker mc nfs-utils unzip jq htop ncdu nload nano
xauth firefox
```

- **Amazon Linux 2 bastion.** Install the required tools packages:

```
sudo yum -y update
```

```
sudo yum install -y make gcc perl-core pcre-devel wget zlib-devel
```

```
sudo groupadd docker
sudo usermod -a -G docker root
sudo usermod -a -G docker ec2-user
```

```
sudo systemctl start docker
sudo systemctl enable docker
```

```
curl -LO "https://dl.k8s.io/release/$(curl -L -s
https://dl.k8s.io/release/stable.txt)/bin/linux/amd64/kubectl"
```

```
chmod +x ./kubectl
sudo mv kubectl /usr/bin
```

3. Update the AWS CLI version by running these commands:

```
aws --version
which aws
sudo rm /usr/bin/aws
sudo rm /usr/bin/aws_completer
aws --version
```

```
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o
"awscliv2.zip"
```

```
unzip awscliv2.zip
sudo ./aws/install -i /usr/local/aws -b /usr/local/bin
hash aws
aws --version
```

Configuring AWS CLI

To configure AWS CLI:

Connect to the bastion, and run the following command:

```
aws configure
```

You will be prompted for the same security data, region, and output format when you previously configured `AWS CLI` for the local host. Repeat the process outlined for AWS CLI configuration.

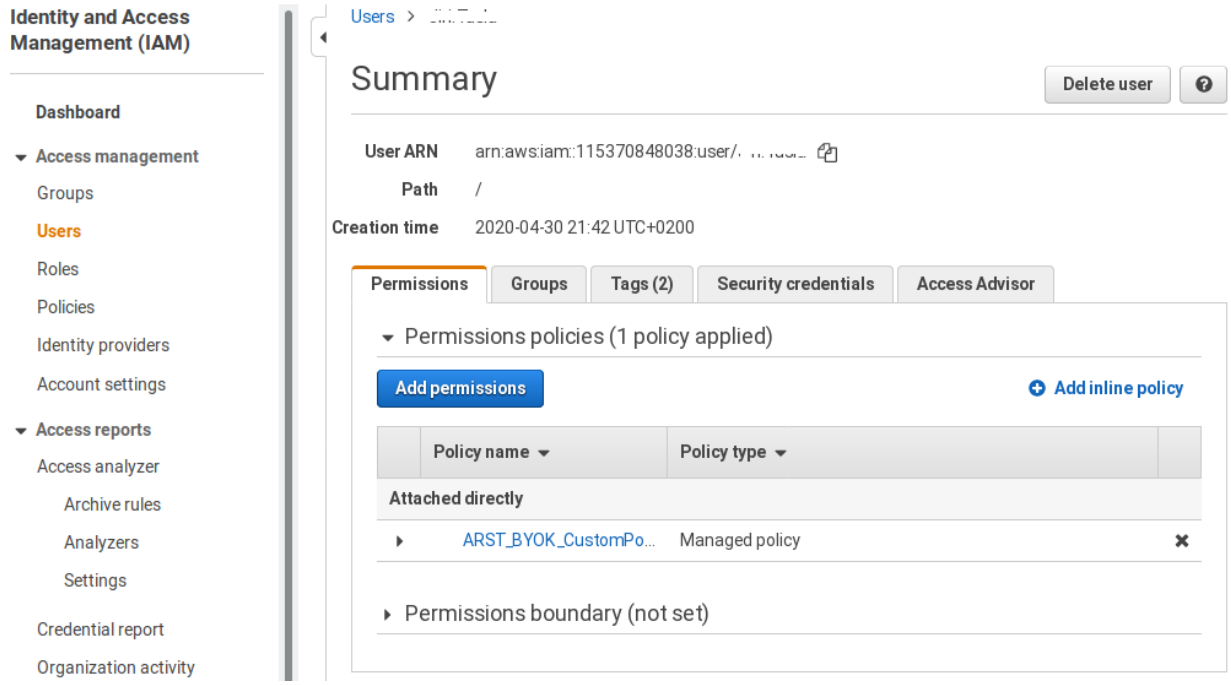
Configuring AWS CLI

Follow these steps to configure AWS CLI.

First, create and retrieve the AWS access keys.

1. Log in to the AWS Management Console using your IAM account.

2. Using the Find Services search box, browse to and open the IAM dashboard.
3. In the left navigation panel, choose **Users**.
4. Locate and open the user with which you are performing the installation.



5. Select the user in IAM and display the user summary.
6. On the **Security Credentials** tab, click **Create Access Key.**
7. Record both the Access key ID and secret access key, and download the `.csv` file for later use.

To configure the AWS CLI:

1. Launch the AWS CLI tool.
2. Run the following command:

```
# aws configure
```

3. Enter the following information:
   - **AWS Access Key ID:** Enter the access key ID that you previously recorded.
   - **AWS Secret Access Key:** Enter the secret access key that you previously recorded, or copy and paste the contents from the CSV file that you downloaded earlier.
   - **Default region name:** Enter the region in which you are installing the ArcSight Suite. If you are unsure, verify your current region from the information in the top right corner of AWS console. Click on the city name and find the region name in the list. For example, *eu-central-1*.]

     Not all AWS regions support all required services. Your selected region must support the Elastic Container Service (ECS) and Elastic Kubernetes Service (EKS).

   - **Default output format:** Enter *json*.

Example input:

```
# aws configure
```

```
AWS Access Key ID [****************VPMC]: AKIA*************VPMC↲
```

```
AWS Secret Access Key [****************wFap]: eZO**********************wFap↲
```

```
Default region name [eu-central-1]: eu-central-1↲
```

```
Default output format [json]: json↲
```

4. To verify configuration, in the AWS Cloud API, enter the command to view the default VPC description:

   ```
   # aws ec2 describe-vpcs
   ```

Example output:

```
{
    "Vpcs": [
        {
            "CidrBlock": "172.31.0.0/16",
            "DhcpOptionsId": "dopt-3a1efe53",
            "State": "available",
            "VpcId": "vpc-a71cfcce",
            "OwnerId": "115370848038",
            "InstanceTenancy": "default",
            "CidrBlockAssociationSet": [
                {
                    "AssociationId": "vpc-cidr-assoc-13d7337a",
```

```
                    "CidrBlock": "172.31.0.0/16",
                    "CidrBlockState": {
                        "State": "associated"
                    }
                }
            ],
            "IsDefault": true
        }
    ]
}
```

Downloading Installation Tools and Packages

Download the installation packages for the OMT Installer and the product of your choice from the OpenText Entitlement Portal to a secure network location. After download, validate the digital signature of each file. You can store all the packages on you local computer, as most of the tasks could be performed on it. To identify the files to download to your secure network location, see "Downloading and Installing the ArcSight Platform Installation Files" in the *Release Notes for ArcSight Platform 24.2*.

For installation, you must have the following files (each package requires its corresponding `md5` file for authentication):

```
arcsight-platform-cloud-installer-XX.X.X.XXX.zip/.md5
```

```
arcsight-suite-metadata-<version>.tar/.md5
```

```
<product package file>.tar/md5 [1 set for each product package you intend to install]
```

Installation tools

The `arcsight-platform-cloud-installer-XX.X.X.XXX.zip` archive contains utility scripts and some templates used during the deployment process.

The `aws_scripts/scripts` directory includes these scripts:

- `generate_aws_secrets`: Used to generate new Kubernetes Secrets for connecting from the cluster to the Elastic Container Registry (ECR). Generated credentials/secrets are valid only 12 hours after generation. For accessing the ECR after this timeframe, use this script according to Refresh the ECR credentials in the K8s.
- `init_efs`: Used to create the required folder structure on the Elastic File Storage (EFS) and assign correct ownership and permissions. You will use it when configuring EFS for the

ArcSight Suite. Parameters for this script are discussed in the following sections. Execute this script without parameters to display the help.

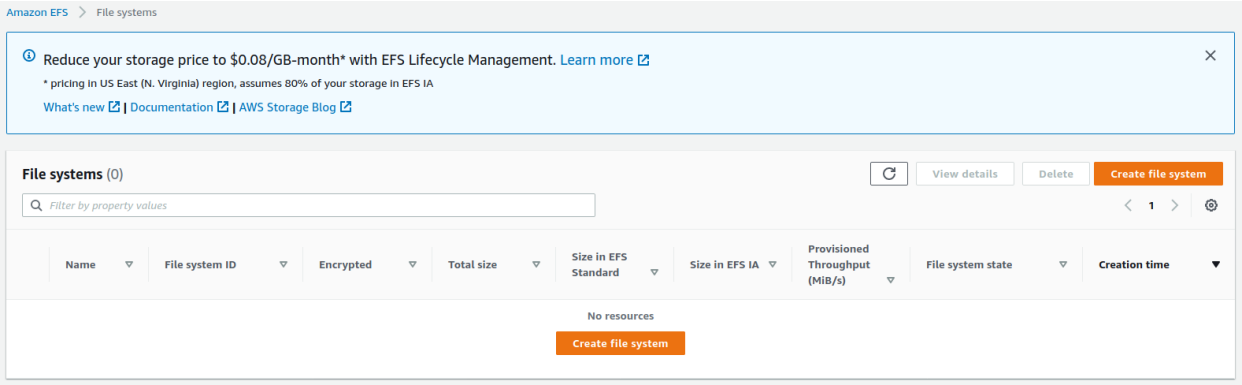
- `upload_images_to_ECR`: Used for uploading the OMT and product images to the ECR to make them accessible to K8s. The script performs tasks in the background required specifically by the AWS ECR. Parameters for this script are detailed below. Execute this script without parameters to display the help.
- `workernodes-userdata`: Used indirectly for enabling worker nodes to join the Kubernetes cluster.

Creating the Elastic File System

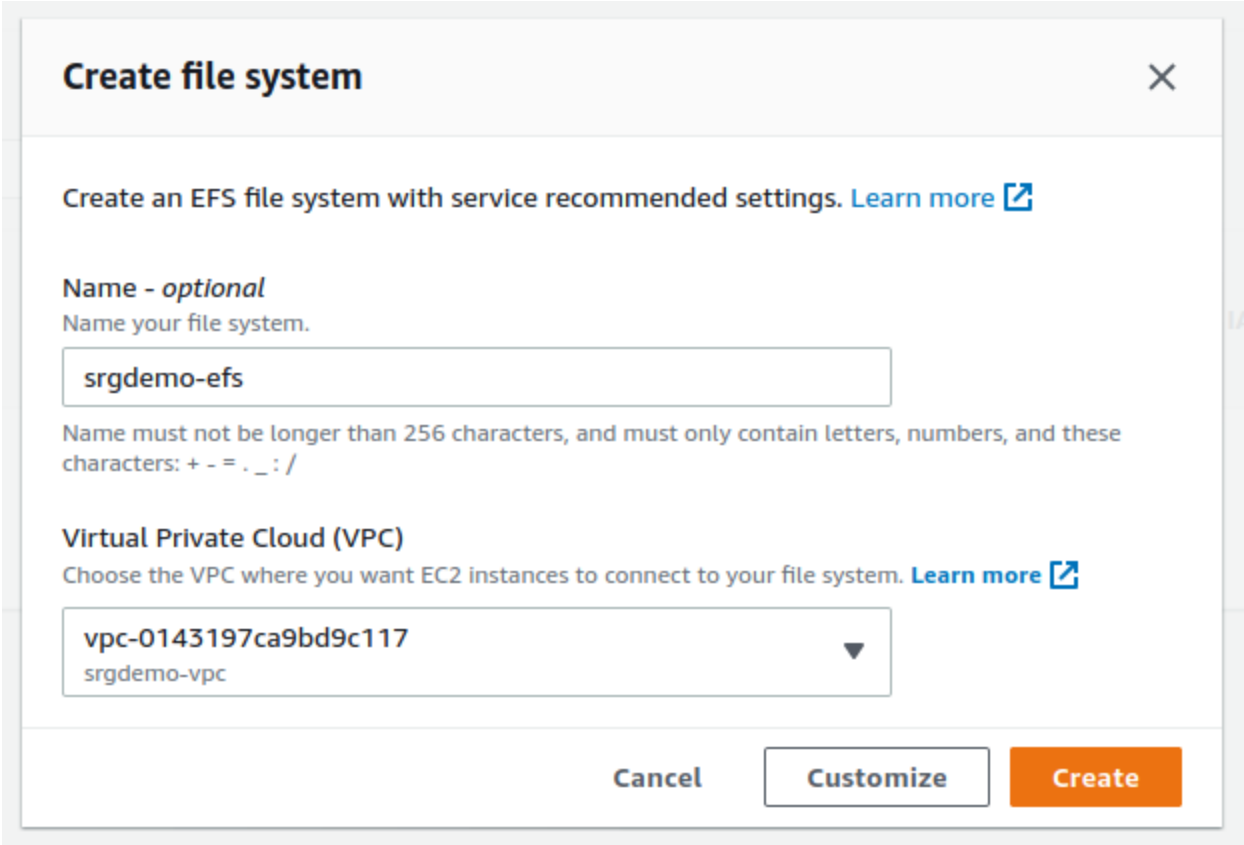
Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system. You can create an EFS through the web UI or the CLI.

To create an EFS using the web UI:

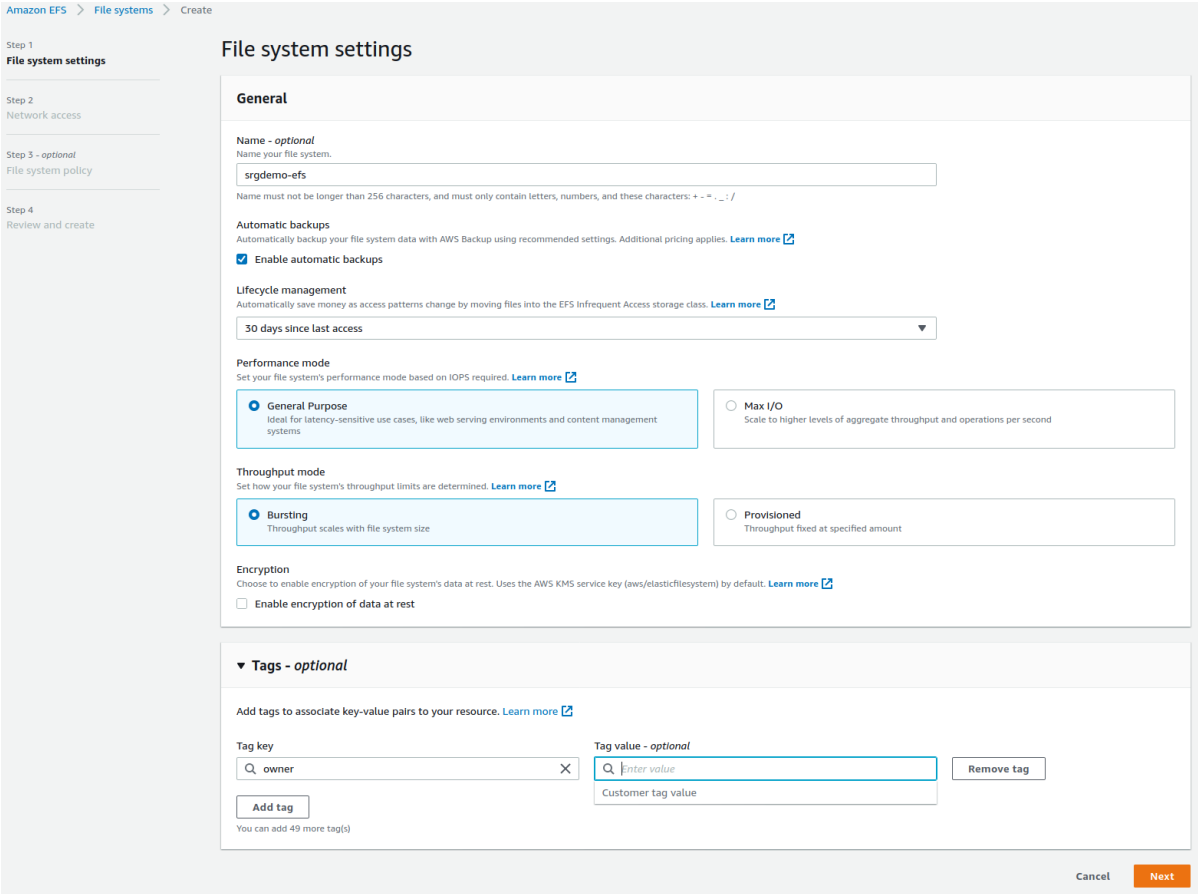
1. Using the Find Services search tool, locate and browse to the EFS dashboard.



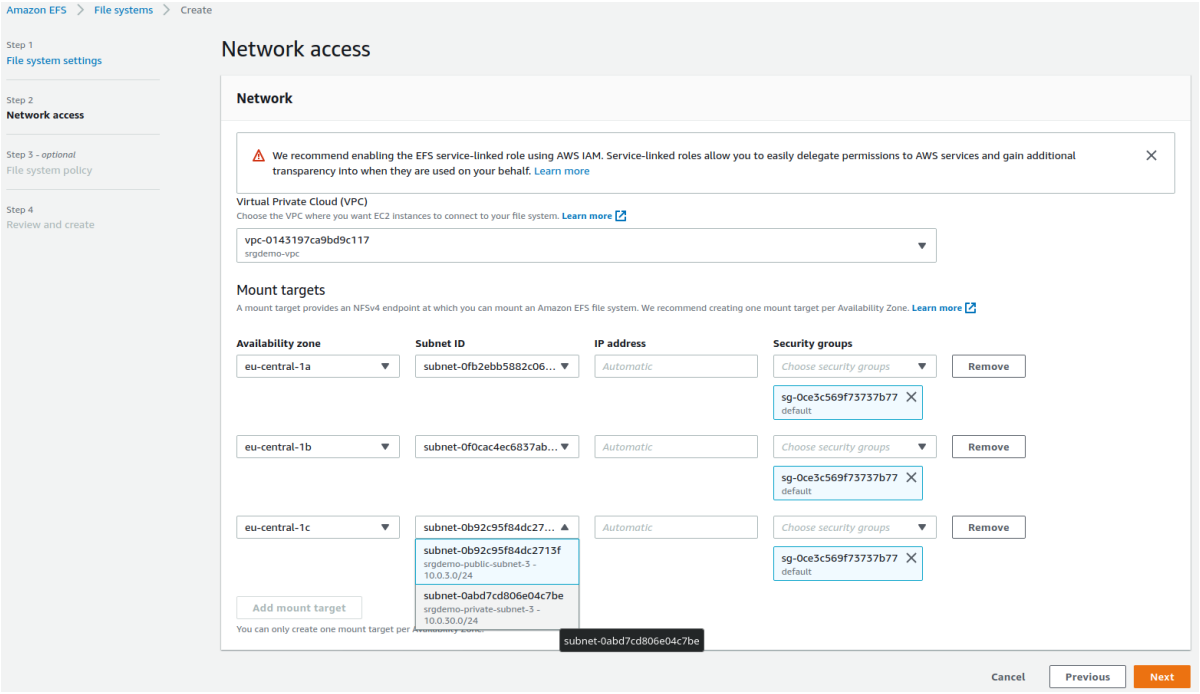
2. Click **Create file system.**



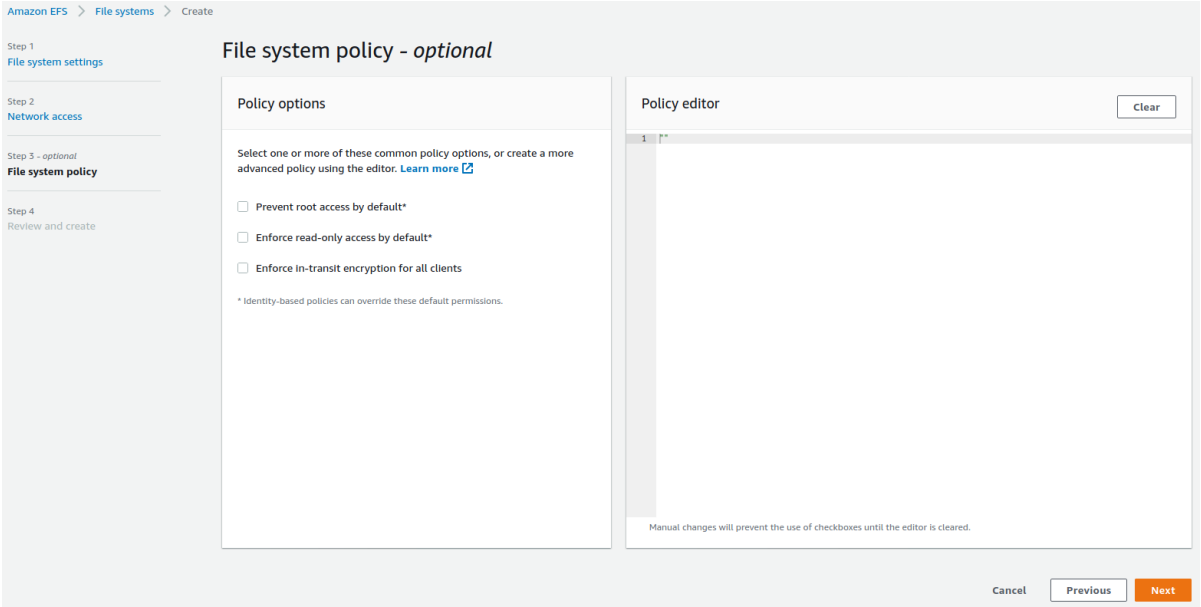
3. On the **Create file system** dialog:
   a. In **Name**, specify a name for the EFS.
   b. Under **Virtual Private Cloud (VPC)**, select the VPC you recorded in your AWS worksheet.
   c. Click **Customize** to start the custom EFS wizard.
4. On the **File system settings** page:
   a. In **General**, deselect **Enable encryption of data at rest.**
   b. In **Tags**, add one or more identification tags as desired.
   c. Click **Next**.



5. On the **Network Access** page:
   a. Under **Mount Targets**, for each target:
   b. Under **Subnet ID,** select the subnet ID of the private subnet.
   c. Change the **Security groups** by adding the Intra VPC security group to the dropdown, and remove any other security groups from the list.
   d. Click **Next**.



6. On the **File system policy - optional** page, leave all settings as is and click **Next**.



7. On the **Review and create** page, review all settings for accuracy, then click **Create**. You are redirected to the EFS dashboard.

> The creation process may take a few moments; please give the process time to complete.

8. Record the File system ID in the AWS worksheet.

To create the EFS using the CLI:

1. Run the following command to create an encrypted EFS file system:

```
aws efs create-file-system \
--encrypted \
--tags Key=Name,Value=<EFS name chosen for easy identification>
```

Example input and output:

```
aws efs create-file-system \
--encrypted \
--tags Key=Name,Value=srgdemo-efs
```

```
{
   "OwnerId":"115370811111",
   "CreationToken":"a53deaf5-ecd6-4dfa-9206-0e1a3db3e1d9",
   "FileSystemId":"fs-ebe456b3",
   "CreationTime":1589557528.0,
   "LifeCycleState":"creating",
   "Name":"srgdemo-efs",
   "NumberOfMountTargets":0,
   "SizeInBytes":{
      "Value":0,
      "ValueInIA":0,
      "ValueInStandard":0
   },
   "PerformanceMode":"generalPurpose",
   "Encrypted":true,
   "ThroughputMode":"bursting",
   "Tags":[
      {
         "Key":"Name",
         "Value":"srgdemo-efs"
      }
   ]
```

2. From the description, record the `FileSystemId` in the AWS worksheet.
3. Examine the value of `LifeCycleState`. Provisioning is complete when the value changes to `available`. (In the example, it has the value `creating`.)
4. To check the provisioning status while the process is running, run the following command:

```
aws efs describe-file-systems \
--file-system-id <FileSystemId>
```

Provisioning usually takes approximately 5 minutes.

Example input and output:

```
aws efs describe-file-systems --file-system-id fs-ebe456b3
```


```
{
   "FileSystems":[
      {
         "OwnerId":"115370811111",
         "CreationToken":"a53deaf5-ecd6-4dfa-9206-0e1a3db3e1d9",
         "FileSystemId":"fs-ebe456b3",
         "CreationTime":1589557528.0,
         "LifeCycleState":"available",
         "Name":"srgdemo-efs",
         "NumberOfMountTargets":0,
         "SizeInBytes":{
            "Value":6144,
            "ValueInIA":0,
            "ValueInStandard":6144
         },
         "PerformanceMode":"generalPurpose",
         "Encrypted":true,
         "ThroughputMode":"bursting",
         "Tags":[
            {
               "Key":"Name",
               "Value":"srgdemo-efs"
            }
         ]
      }
   ]
}
```


Creating Mount Targets

A *mount target* connects the EFS to a specific subnet in the VPC. The instances contained in the VPC can mount the target using the NFS protocol and utilize NFS.

In this section, you will create mount targets between the newly-created EFS and all three private subnets.

To create a mount target in a private subnet:

1. Select one of your **private** subnets and run the following command:
```
aws efs create-mount-target \
--file-system-id <FileSystemId> \
--security-groups <Intra VPC Security group Id> \
--subnet-id <private subnet Id>
```

Where:

`<FileSystemId>`: The file system ID of the EFS you just created

`<Intra VPC Security group Id>`: The ID of the Intra VPC security group you previously created.

> The command only accepts one subnet ID at a time. You must run this command separately for each private subnet which you are using for the cluster.

2. The command will respond with a mount target description. From the output, record the `MountTargetId` in your AWS worksheet.
3. Repeat Steps 1 and 2 for each of the other 2 private subnets (use the subnet IDs on your worksheet) and then record the values of `MountTargetId` for each in your AWS worksheet.

Example input and output:

```
aws efs create-mount-target \
--file-system-id fs-ebe456b3 \
--security-groups sg-07b302cbc0972c603 \
--subnet-id subnet-0fb2ebb5882c061f0
```

```
{
   "OwnerId":"115370811111",
   "MountTargetId":"fsmt-63eaae3a",
   "FileSystemId":"fs-ebe456b3",
   "SubnetId":"subnet-0fb2ebb5882c061f0",
   "LifeCycleState":"creating",
   "IpAddress":"10.0.10.131",
   "NetworkInterfaceId":"eni-03ecba7e5eb46dc9f",
   "AvailabilityZoneId":"euc1-az2",
   "AvailabilityZoneName":"eu-central-1a"
}
```

To check the creation status of a mount target:

1. Run the following command:
```
aws efs describe-mount-targets --mount-target-id <Mount target X Id>
```

2. Record the value of `MountTargetId` in the AWS worksheet.

Immediately after creation, a mount target has a value for `LifeCycleState` value of `creating`. The transition to available usually takes approximately 3 minutes. To check the status, run the following command:

```
aws efs describe-mount-targets --mount-target-id <Mount target X Id>
```

Example input and output:

```
aws efs describe-mount-targets --mount-target-id fsmt-63eaae3a
```

```
{
   "OwnerId":"115370811111",
   "MountTargetId":"fsmt-63eaae3a",
   "FileSystemId":"fs-ebe456b3",
   "SubnetId":"subnet-0fb2ebb5882c061f0",
   "LifeCycleState":"creating",
   "IpAddress":"10.0.10.131",
   "NetworkInterfaceId":"eni-03ecba7e5eb46dc9f",
   "AvailabilityZoneId":"euc1-az2",
   "AvailabilityZoneName":"eu-central-1a"
}
```

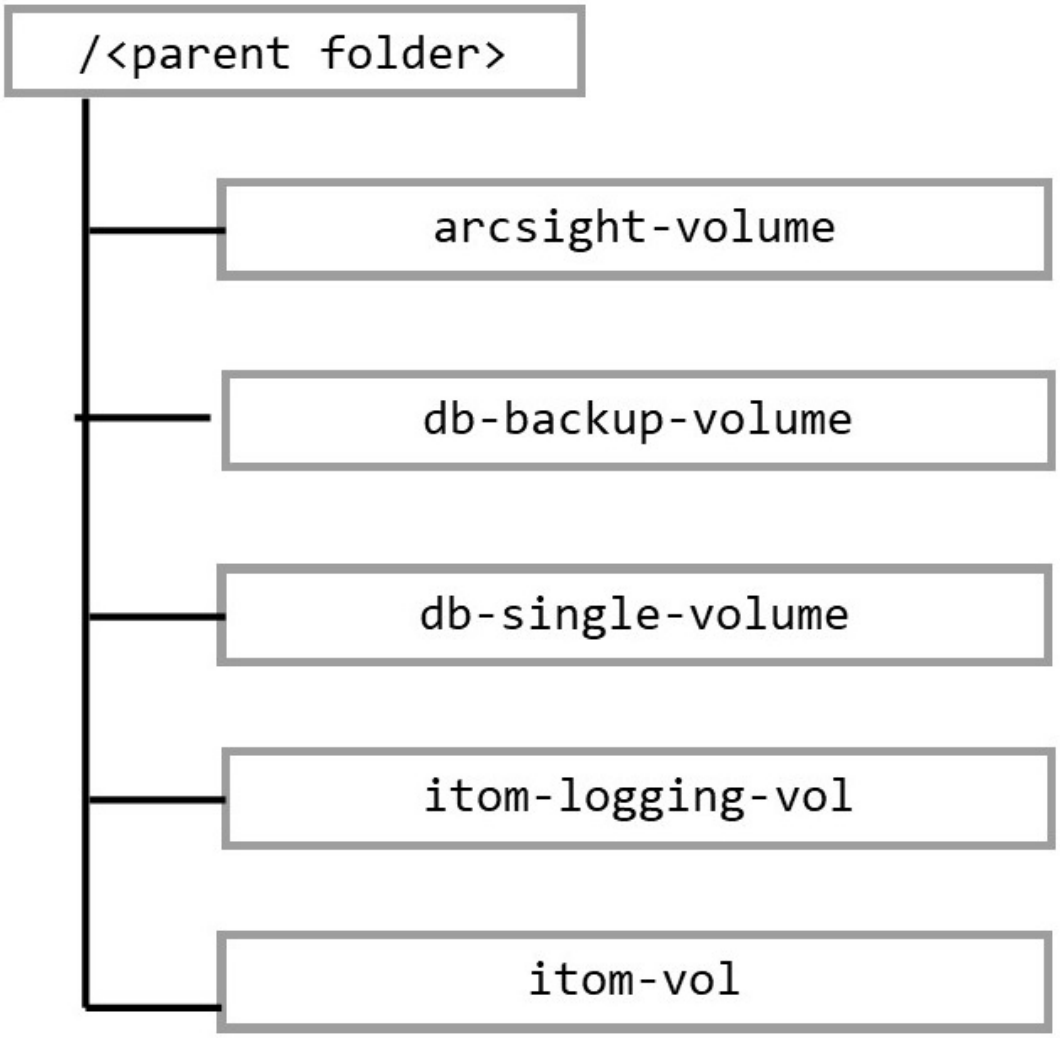
Once all three mount targets are in the `available` state, you can proceed to the next step.

Configuring EFS for the ArcSight Suite

OMT and the ArcSight suite require several separated folders for storing various types of information, such database files, log files, and runtime data. In this step, you will create the following folders:

- `arcsight-volume`
- `db-backup-vol`
- `db-single-vol`
- `itom-logging-vol`
- `itom-vol`

All of these folders are created in a parent folder from the filesystem, as follows:



Using different parent folders, you can use a single EFS for several different file systems (assuming they are in the same region and same VPC, and have the correct mount targets).

To configure EFS for ArcSight Suite:

1. Using an `scp` client, copy the `arcsight-platform-cloud-installer-XX.X.X.XXX.zip` package to the bastion and unpack it.
2. For creating the folders and setting respective permissions, unzip the `aws-scripts` script archive and then run the script `init_efs` from the `aws-scripts/scripts` directory.
3. Construct the filesystem FQDN. The filesystem FQDN should have the following format: `<FileSystemId>.efs.<Region>.amazonaws.com`

Where:

`<FileSystemId>`: Previously created and recorded in the AWS worksheet.

`<Region>`:The ID of the region in which you have originally asked to create restricted resources.

4. Record the filesystem FQDN in the AWS worksheet.

> The FQDN will be used for initializing the folder structures; and will later be used during the Bootstrap OMT step and during OMT Web UI installation processes.

5. Execute the script:

```
./arcsight-platform-cloud-installer/aws-scripts/scripts/init_efs \
-p <Parent folder name> \
-s <Filesystem FQDN>
```

Where:

`<Parent folder name>`: An optional parameter. If not specified, this value will be replaced with ArcSight. Record the chosen parent folder name to the AWS worksheet.

`<Filesystem FQDN>`: The filesystem FQDN you have just created.

Example:

```
./arcsight-platform-cloud-installer/aws-scripts/scripts/init_efs \
-p srgdemo \
-s fs-ebe456b3.efs.eu-central-1.amazonaws.com
```

6. The mount point is created as commented in the `etc/fstab` file. Open the `etc/fstab` file and uncomment the mount point. Then run the command:

```
sudo vim /etc/fstab
```

7. Run the following command:

```
sudo mount -a
```

8. (Conditional) If Intelligence is part of the deployment, run the following command only for `arcsight-volume` so that the Logstash and Elasticsearch pods do not fail because of permission issues:

```
cd /mnt/efs/<parent_folder_name>
sudo chown -R 1999:1999 arcsight-volume
```

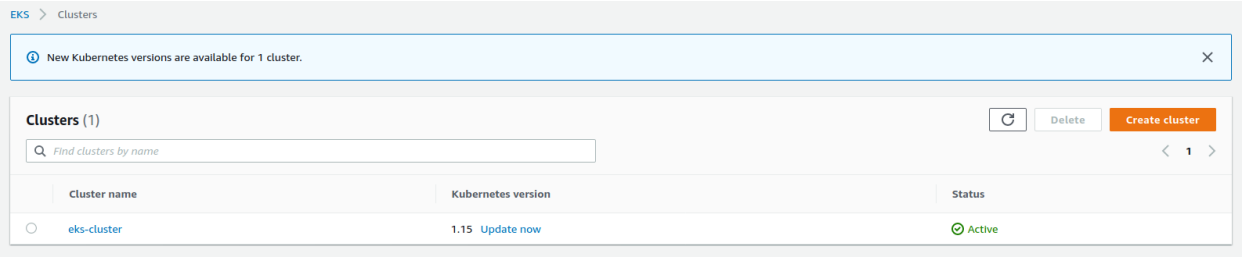
9. Verify whether the created folders correspond to the structure described above, with respect to your chosen parent folder.

Configuring the Elastic Kubernetes Service

Amazon Elastic Kubernetes Service (Amazon EKS) is a fully-managed Kubernetes service control plane. In this section you will set up your EKS cluster.

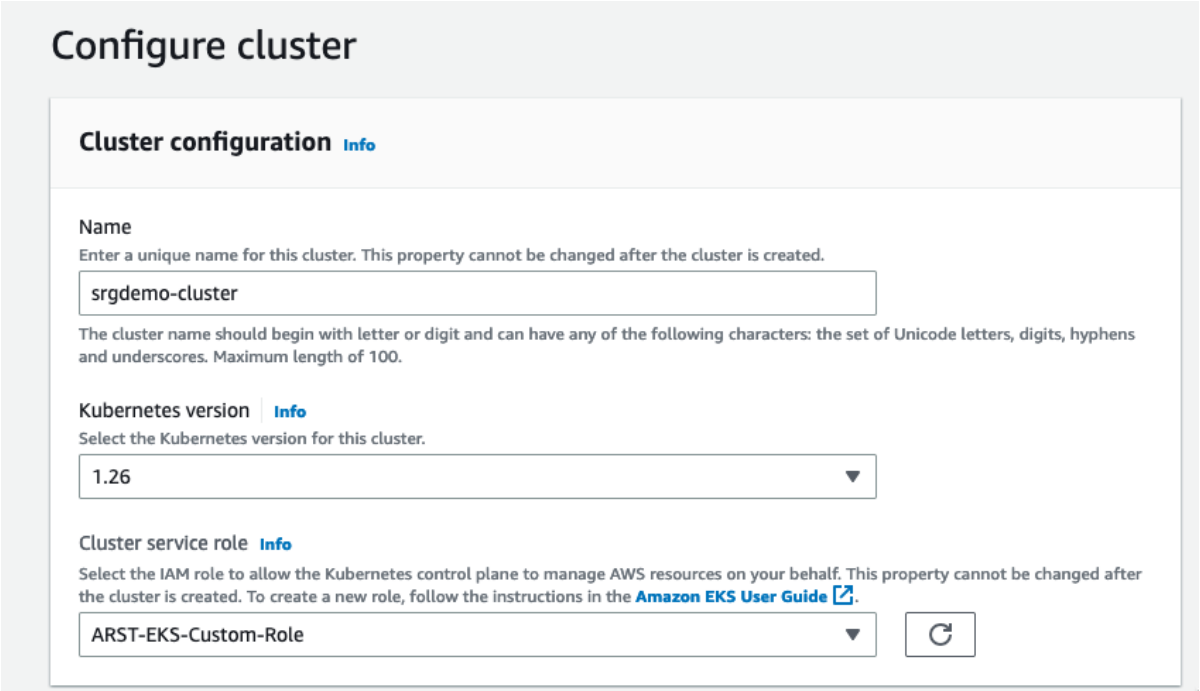
To configure EKS using the web UI:

1. Using the Find Services search tool, locate and browse to the EKS Dashboard.
2. Click **Create Cluster.**

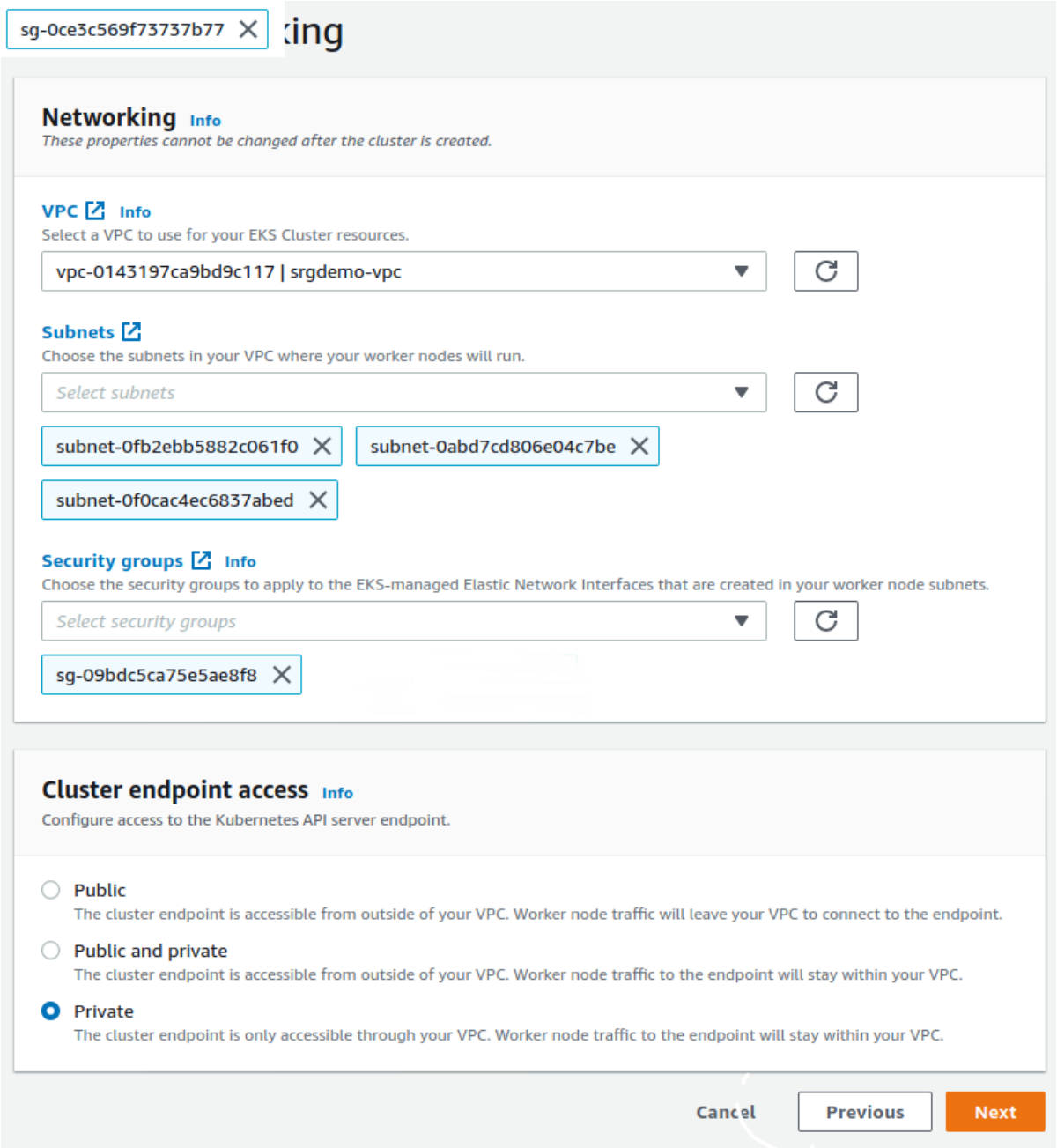


3. On the **Configure Cluster** page, specify values for the following:
   a. **Name**: Cluster name. Use the same value you passed in your resources creation request to your AWS infrastructure administrators, and recorded in the AWS worksheet. For example, `srgdemo-cluster`.
   b. **Kubernetes version**:
   c.
   > To determine the Kubernetes version to use when deploying the ArcSight Platform to AWS, check the Hybrid Cloud Support page of the *Technical Requirements for ArcSight Platform 24.2*.

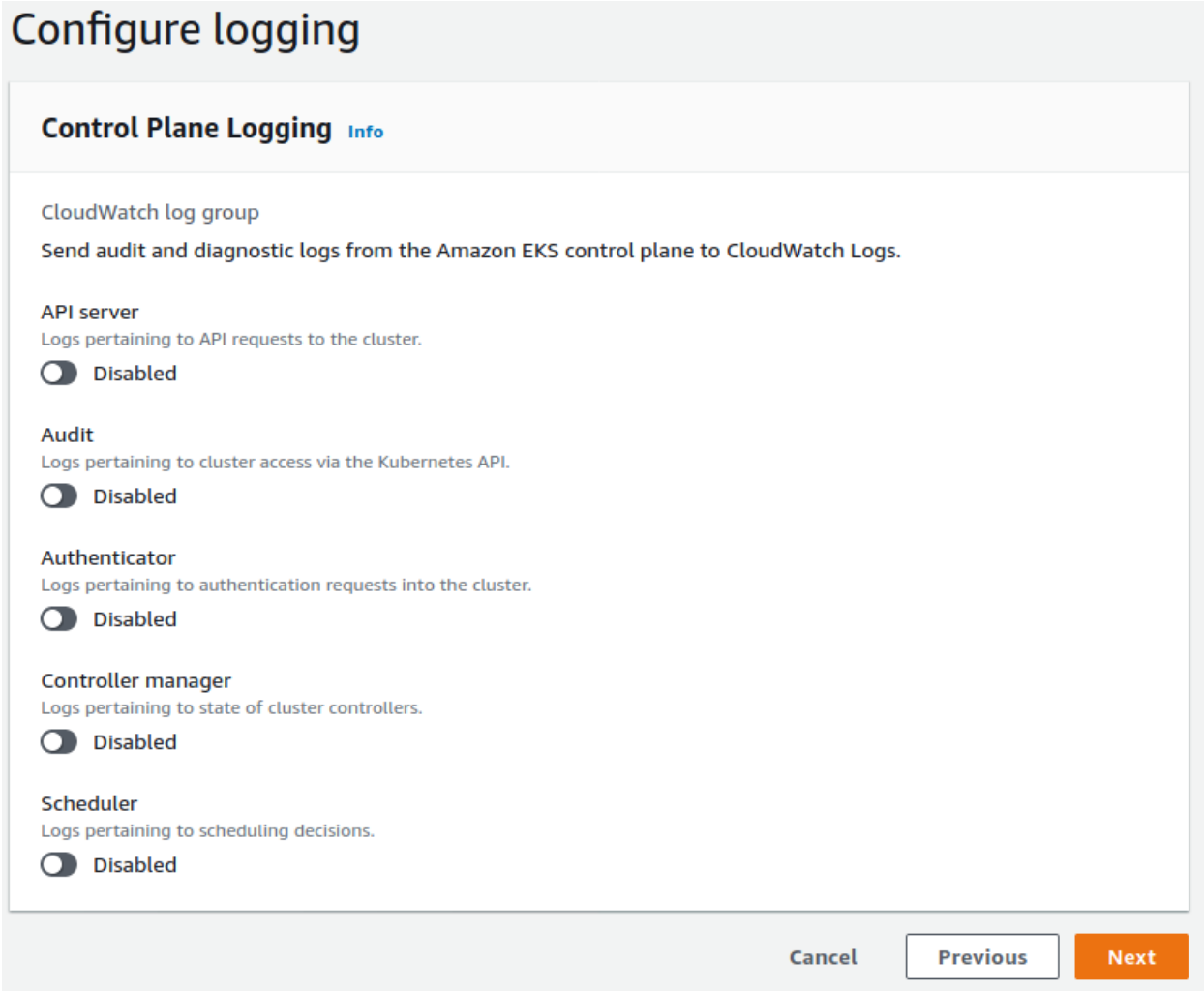
   a. **Cluster Service Role:** Select the role specified for cluster management.
   b. **Tags:** Tags are optional, but you might add tags to identify the cluster.



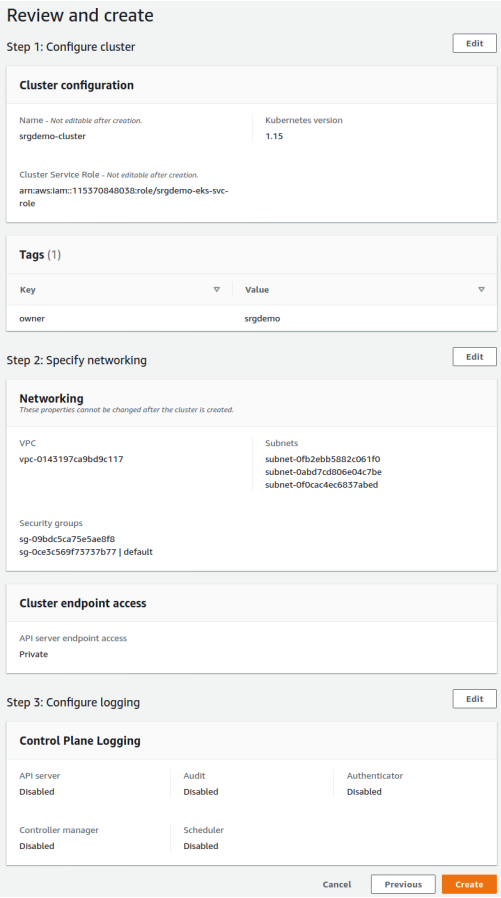
4. Click **Next.**
5. On the **Specify Networking** page, specify values for the following:
   a. **VPC:** Select your VPC from the dropdown.
   b. **Subnets:** Ensure **only** your private subnets are selected from the dropdown (subnet names are recorded in the AWS worksheet).
   c. **Security groups:** Add the Intra VPC security group named in the AWS worksheet.
   d. **Cluster endpoint access:** Select **Private** to keep the cluster isolated.



6. On the **Configure Logging** page, leave all values at default settings, then click **Next**.



7. On the **Review and Create** page, check all settings for accuracy and then click **Create**. The cluster details are displayed.



The creation process usually takes approximately 20 minutes and the status will change to *Active* when complete. Click **Refresh** to refresh the creation status display.

To configure EKS using the CLI:

1. Run the following command:

```
aws eks create-cluster \
--name <Cluster Name> \
--role-arn <EKS role ARN> \
--resources-vpc-config subnetIds=<private subnet
Ids>,endpointPublicAccess=false,endpointPrivateAccess=true,securityGroupI
ds=<Intra VPC Security group Id> \
--kubernetes-version <Kubernetes version>
```

Where:

`<Cluster Name>`: Use the same value you passed in your resources creation request to your AWS infrastructure administrators; check the AWS worksheet for the value.

`<EKS role>`: The IAM role ARN created by your AWS infrastructure administrators; check the AWS worksheet for the value.

`<private subnet Ids>`: Comma-separated IDs of private subnets created together with the VPC; these values are recored in the AWS worksheet.

`<Intra VPC Security group Id>`: The ID of the previously created security group.

The value for `resources-vpc-config` cannot contain spaces; it must be one string.

NOTE: Ensure that the Kubernetes version is the same as the version used when creating the worker nodes

`<Kubernetes version>`: Use the value from the AWS worksheet.

2. Record the ARN value in your AWS worksheet.

Example input and output:

```
aws eks create-cluster \
--name srgdemo-cluster \
--role-arn arn:aws:iam::115370811111:role/srgdemo-eks-svc-role \
--resources-vpc-config subnetIds=subnet-0fb2ebb5882c061f0,subnet-
0f0cac4ec6837abed,subnet-0abd7cd806e04c7be,\
endpointPublicAccess=false,endpointPrivateAccess=true,securityGroupIds=sg-
09bdc5ca75e5ae8f8 \
--kubernetes-version 1.26
```

```
{
   "cluster":{
      "name":"srgdemo-cluster",
      "arn":"arn:aws:eks:eu-central-1:115370811111:cluster/srgdemo-cluster",
      "createdAt":1589877429.005,
      "version":"1.15",
      "roleArn":"arn:aws:iam::115370811111:role/srgdemo-eks-svc-role",
      "resourcesVpcConfig":{
         "subnetIds":[
            "subnet-0fb2ebb5882c061f0",
            "subnet-0f0cac4ec6837abed",
            "subnet-0abd7cd806e04c7be"
         ],
         "securityGroupIds":[
            "sg-09bdc5ca75e5ae8f8"
         ],
         "vpcId":"vpc-0143197ca9bd9c117",
         "endpointPublicAccess":false,
         "endpointPrivateAccess":true,
```

```
         "publicAccessCidrs":[

         ]
      },
      "logging":{
         "clusterLogging":[
            {
               "types":[
                  "api",
                  "audit",
                  "authenticator",
                  "controllerManager",
                  "scheduler"
               ],
               "enabled":false
            }
         ]
      },
      "status":"CREATING",
      "certificateAuthority":{

      },
      "platformVersion":"eks.2",
      "tags":{

      }
   }
}
```

Cluster creation usually takes approximately 20 minutes. Check the cluster status by running the command:

```
aws eks describe-cluster \
--name <Cluster Name> \
| jq '.cluster.status'
```

The output immediately after creation should state `CREATING`. Repeat the command until the output changes to `ACTIVE`.

A newly created EKS might take up to 20 minutes to become `ACTIVE`.

Example:

```
aws eks describe-cluster \
--name srgdemo-cluster \
| jq '.cluster.status'
```

Creating the IAM Roles in AWS

An *IAM role* is an IAM (AWS Identity and Access Management) entity that defines a set of permissions for making AWS service requests and manipulating various resources. They are needed for those capabilities that require the ArcSight Database when deploying via AWS in the cloud. An IAM role is required for all database nodes participating in the cluster to allow connectivity to S3 bucket communal storage. For more information, see Installing the Database in AWS .

> Roles are shareable. Instead of creating new roles, you might use existing roles your organization has previously created. IAM is not region dependent, roles can be reused in all regions your organization uses.

You will create two roles: one for EKS (Elastic Kubernetes Service) and one for worker nodes, and assign them specific policies to define permissions.

Roles, policy names, and corresponding policy ARNs are shown in the following table:

Role	Policy Name	Policy ARN
EKS	AmazonEKSClusterPolicy	arn:aws:iam::aws:policy/AmazonEKSClusterPolicy
EKS	AmazonEKSServicePolicy	arn:aws:iam::aws:policy/AmazonEKSServicePolicy
Worker Nodes	AmazonEKSWorkerNodePolicy	arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy
Worker Nodes	AmazonEC2ContainerRegistryReadOnly	arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly
Worker Nodes	AmazonEKS_CNI_Policy	arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy

EKS Policies

EKS requires the following policies to be granted:

- **AmazonEKSClusterPolicy**

  This policy provides Kubernetes the permissions required to manage resources on your behalf. Kubernetes requires EC2: CreateTags permissions to place identifying information on EC2 resources including but not limited to Instances, Security Groups, and Elastic Network Interfaces.

  `ARN: arn:aws:iam::aws:policy/AmazonEKSClusterPolicy`

- **AmazonEKSServicePolicy**

  This policy allows Amazon Elastic Container Service for Kubernetes to create and manage the necessary resources to operate EKS Clusters.

  `ARN: arn:aws:iam::aws:policy/AmazonEKSServicePolicy`

For more information, see AWS documentation by signing into your AWS account: https://aws.amazon.com/

Worker Node Policies

For worker nodes in EKS, the following policies must be granted:

- **AmazonEKSWorkerNodePolicy**

  This policy allows Amazon EKS worker nodes to connect to Amazon EKS Clusters.

  `ARN: arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy`
- **AmazonEC2ContainerRegistryReadOnly**

  This policy provides read-only access to Amazon EC2 Container Registry repositories.

  `ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`
- **AmazonEKS_CNI_Policy**

  This policy provides the Amazon VPC CNI Plugin (amazon-vpc-cni-k8s) the permissions it requires to modify the IP address configuration on your EKS worker nodes. This permission set enables the CNI to list, describe, and modify Elastic Network Interfaces on your behalf. For more information about the AWS VPC CNI Plugin, see the link here: https://github.com/aws/amazon-vpc-cni-k8s

  `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

For more information, see AWS documentation by signing into your AWS account: https://aws.amazon.com/

Creating the IAM Role for EKS

To create the EKS role and assign policies to it:

1. Run the following command:

```
aws iam create-role \
--role-name <role name> \
--assume-role-policy-document <role policy document>
```

Where:

`<role name>`: A name chosen for ease of reference; in our examples, we will use `srgdemo-eks-svc-role`.

`<role policy document>`: The location of a JSON document granting temporary security credentials to perform actions on resources and defining which resources are accessible. The downloadable package `arcsight-platform-cloud-installer-XX.X.X.XXX.zip` contains a ready-to-use document named `EksRolePolicyDocument.json` in the `arcsight-platform-cloud-installer-XX.X.X.XXX/aws-scripts/objectdefs` folder (after unzipping it). This

document defines that the cluster can request temporary security credentials to `eks.amazonaws.com` only.

Example output:

```
{
  "Role": {
    "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
    "RoleId": "AKIAIOSFODNN7EXAMPLE",
    "CreateDate": "2013-06-07T20:43:32.821Z",
    "RoleName": "Test-Role",
    "Path": "/",
    "Arn": "arn:aws:iam::123456789012:role/Test-Role"
    }
}
```

2. Record the ARN (Amazon Resource Name) value in your AWS worksheet.

Example input and output:

```
aws iam create-role \
--role-name srgdemo-eks-svc-role \
--assume-role-policy-document file://./jsons/EksRolePolicyDocument.json
```

```
{
    "Role": {
        "Path": "/",
        "RoleName": "srgdemo-eks-svc-role",
        "RoleId": "AROARVXFDN4TOT5P3E3AQ",
        "Arn": "arn:aws:iam::115370811111:role/srgdemo-eks-svc-role",
        "CreateDate": "2020-05-18T12:10:48Z",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "eks.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

Note the `Arn` value `*arn:aws:iam::115370811111:role/srgdemo-eks-svc-role*`.

3. Attach a policy to the EKS role by running the command:
   `aws iam attach-role-policy \`

```
--role-name <role name> \
--policy-arn <policy arn>
```

Where:

`<role name>` is the role name you have chosen when creating a new role

`<policy arn>` is the policy ARN from the description above.

4. Repeat Step 3 for the next policy, changing the policy ARN to match.

Example command with example policy name:

```
aws iam attach-role-policy \
--role-name srgdemo-eks-svc-role \
--policy-arn arn:aws:iam::aws:policy/AmazonEKSClusterPolicy
```

Creating the Worker Node Role

To create the worker node role and assign policies to it:

1. Run the following command:

```
# aws iam create-role \
--role-name <role name> \
--assume-role-policy-document <role policy document>
```

Where:

`<role name>`: A name chosen for ease of reference; in our examples, we will use srgdemo-eks-svc-role.

`<role policy document>`:The location of a JSON document granting temporary security credentials to perform actions on resources and defining which resources are accessible. The downloadable package `arcsight-platform-cloud-installer-XX.X.X.XXX.zip` contains a ready-to-use document named `WorkerNodesRolePolicyDocument.json` in the `rcsight-platform-cloud-installer-XX.X.X.XXX/aws-scripts/objectdefs` folder (after unzipping it). This document defines that the cluster can request temporary security credentials to `eks.amazonaws.com` only.

Example output:

```
{
  "Role": {
    "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
    "RoleId": "AKIAIOSFODNN7EXAMPLE",
    "CreateDate": "2013-06-07T20:43:32.821Z",
    "RoleName": "Test-Role",
    "Path": "/",
    "Arn": "arn:aws:iam::123456789012:role/Test-Role"
```

```
    }
}
```

2. Record the ARN (Amazon Resource Name) value in your AWS worksheet.

Example input and output:

```
# aws iam create-role \
--role-name srgdemo-workernodes-svc-role \
--assume-role-policy-document
file://./jsons/WorkerNodesRolePolicyDocument.json
```

```
{
    "Role": {
        "Path": "/",
        "RoleName": "srgdemo-workernodes-svc-role",
        "RoleId": "AROARVXFDN4TICMZYPKJ2",
        "Arn": "arn:aws:iam::115370811111:role/srgdemo-workernodes-svc-role",
        "CreateDate": "2020-05-19T16:20:11Z",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "ec2.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

3. Attach a policy to the **worker node** role by running the following command:

```
# aws iam attach-role-policy \
--role-name <role name> \
--policy-arn <policy arn>
```

Where:

`<role name>`: The role name you have chosen when creating a new role.

`<policy arn>`: The policy ARN from the description above.

4. Repeat Step 3 each policy, changing the policy ARN to match.

Example commands:

```
# aws iam attach-role-policy \
--role-name srgdemo-workernodes-svc-role \
--policy-arn arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy
```

```
# aws iam attach-role-policy \
--role-name srgdemo-workernodes-svc-role \
--policy-arn arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly
```

```
# aws iam attach-role-policy \
--role-name srgdemo-workernodes-svc-role \
--policy-arn arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy
```

Configuring the Kubernetes Client (`kubectl`)

Several Kubernetes configuration and diagnostic tasks using `kubectl` will be performed on the bastion. In order to do that, the `kubectl` utility needs be configured with bastion credentials.

To configure `kubectl`:

1. Connect to the bastion instance and run the following command:

   ```
   aws eks update-kubeconfig --name <Cluster Name>
   ```

   The command will return an updated context <eks cluster arn> in `/home/<user>/.kube/config`

   ```
   Example:
   aws eks update-kubeconfig --name srgdemo-cluster
   ```

   Updated context:`arn:aws:eks:eu-central-1:115370811111:cluster/srgdemo-cluster` in `/home/<user>/.kube/config`

2. On the bastion, check the Kubernetes service status by running:

   ```
   kubectl get svc
   ```

   ```
   Output example:

   NAME         TYPE        CLUSTER-IP   EXTERNAL-IP   PORT(S)   AGE
   kubernetes   ClusterIP   172.20.0.1   <none>        443/TCP   54m
   ```

   The EKS control plane is now ready and accessible from the bastion.

Applying the AWS ConfigMap to Enable Worker Nodes to Join the Cluster

The AWS ConfigMap needs to be applied so that the worker nodes can join your EKS cluster.

1. Connect to the bastion host.
2. Open the file the `cm-aws-auth.yaml` in any text editor. (The file is from the unpacked `arcsight-platform-cloud-installer-XX.X.X.XXX.zip` located in the directory `/aws-scripts/objectdefs`).
3. Replace the placeholder `${WORKERS_ROLE_ARN}` with the `Role ARN` value from your AWS worksheet, and then save your changes. The ConfigMap will then resemble the following example:

```
apiVersion: v1
kind: ConfigMap
metadata:
name: aws-auth
namespace: kube-system
data:
mapRoles: |
- rolearn: arn:aws:iam::115370848038:role/srgdemo-workernodes-svc-role
username: system:node:{{EC2PrivateDNSName}}
groups:
- system:bootstrappers
- system:nodes
```

4. On the bastion, run the following command:

```
# kubectl apply -f cm-aws-auth.yaml
```

5. This command will output:

```
configmap/aws-auth created.
```

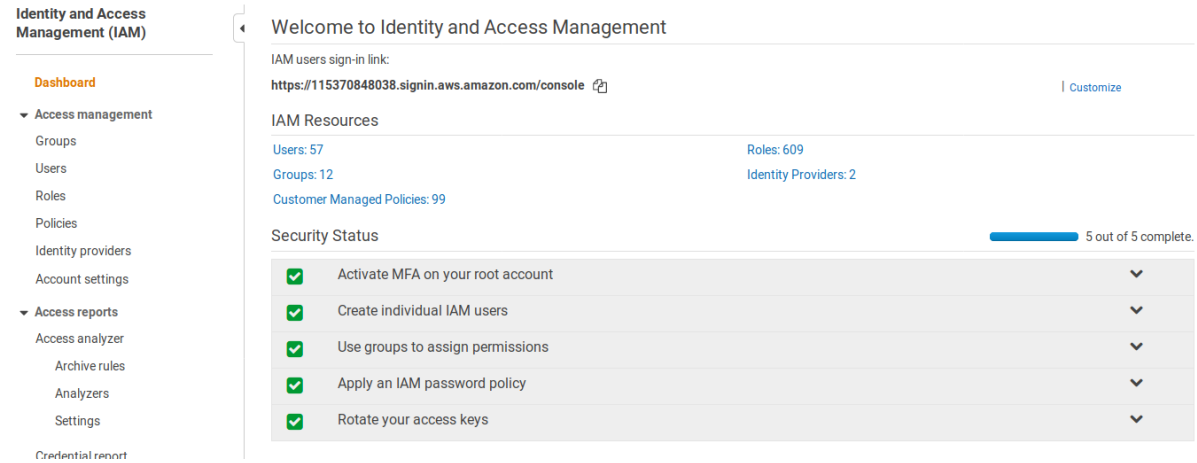
Creating and Configuring Worker Nodes

The *worker nodes* (EC2 nodes) are the Kubernetes nodes that will perform application processing. A cluster contains one or more Amazon EC2 nodes on which pods are scheduled. Amazon EKS nodes run in your AWS account and connect to your cluster's control plane through the cluster API server endpoint.

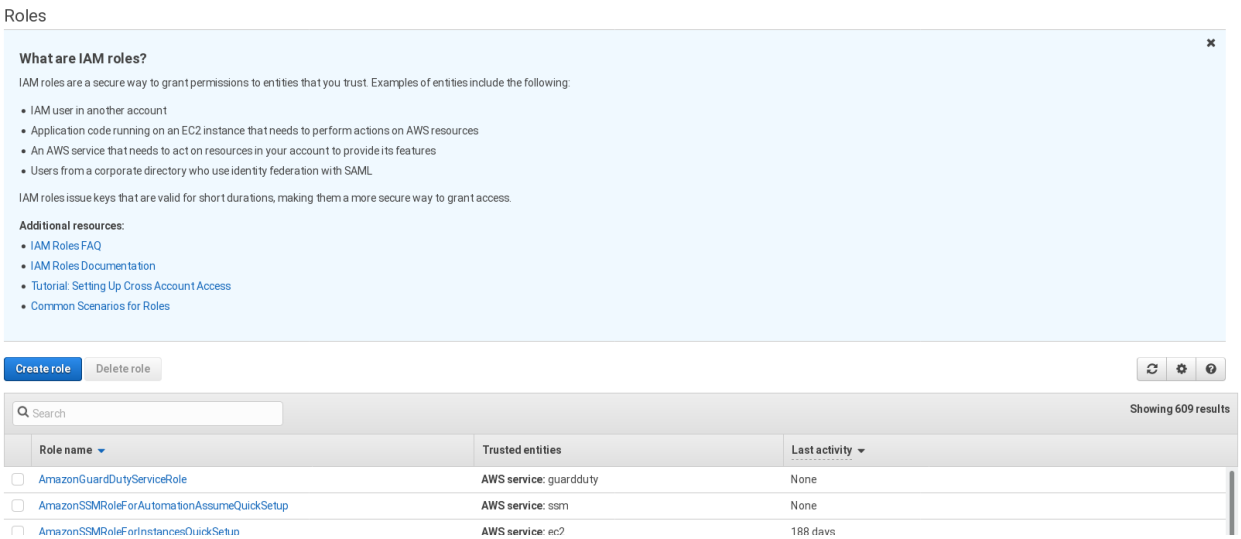
Checking for a Worker Node Instance Profile

To check for a worker node instance profile using the web UI:

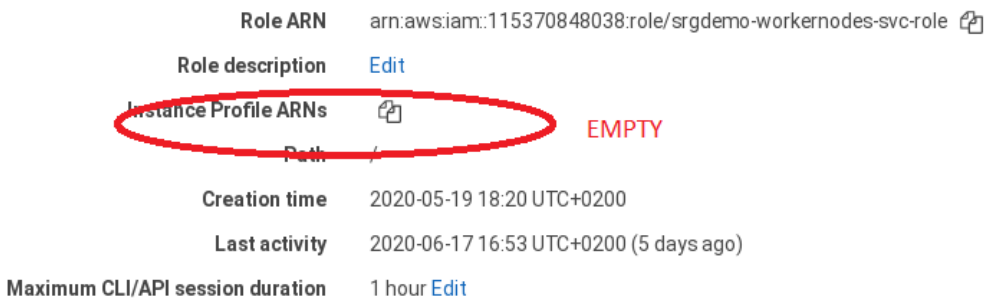
1. Using the **Find Services** search tool, browse to the IAM dashboard.
2. In the left navigation panel, under **Access management,** click **Roles** to get a list of existing roles.



3. In the search box, specify the Worker Nodes role name (from the AWS worksheet) to filter it from the other roles.



4. Click the role name to get its details, then check the row **Instance Profile ARNs.**



a. (Conditional) If no instance profile has been assigned to the role (that is, the row Instance Profile is empty, as illustrated here), then continue with creating an instance profile.

b. (Conditional) If the row **Instance Profile ARNs** is filled, then record the value in the AWS worksheet.

> The Instance Profile creation guide works only on the command-line interface. It is not possible to create a separate instance profile without an assigned role.

To check for a worker node instance profile using the CLI:

1. Run the following command:

```
# aws iam list-instance-profiles-for-role \
--role-name <Workernodes role name from AWS worksheet>
```

```
Example:
# aws iam list-instance-profiles-for-role \
--role-name ARST-EKS-Workers-Custom-Role
```

The command will return only of the following outputs:

No instance profile for the role exists. Example output for this case:

```
{
   "InstanceProfiles":[

   ]
}
```

An instance profile exists for the role. Example output for this case:

```
{
   "InstanceProfiles":[
      {
         "Path":"/",
```

```
         "InstanceProfileName":"ARST-EKS-Workers-Custom-Role",
         "InstanceProfileId":"AIPARVXFDN4TBQBCRKX45",
         "Arn":"arn:aws:iam::115370811111:instance-profile/ARST-EKS-Workers-
Custom-Role",
         "CreateDate":"2020-06-16T05:57:59+00:00",
         "Roles":[
            {
               "Path":"/",
               "RoleName":"ARST-EKS-Workers-Custom-Role",
               "RoleId":"AROARVXFDN4TNRSAMVCVX",
               "Arn":"arn:aws:iam::115370811111:role/ARST-EKS-Workers-Custom-
Role",
               "CreateDate":"2020-06-16T05:57:58+00:00",
               "AssumeRolePolicyDocument":{
                  "Version":"2012-10-17",
                  "Statement":[
                     {
                        "Effect":"Allow",
                        "Principal":{
                           "Service":"ec2.amazonaws.com"
                        },
                        "Action":"sts:AssumeRole"
                     }
                  ]
               }
            }
         ]
      }
   ]
}
```

2. Do one of the following:
   - (Conditional) If no instance profile exists for the role, proceed with creating an instance profile, OR,
   - (Conditional) If the instance profile already exists for the role, record its name (`InstanceProfiles -> InstanceProfileName`) and ARN (`InstanceProfile -> Arn`) in the AWS worksheet, then continue with the procedure to create a launch template.

Creating an Instance Profile

To create an instance profile:

1. Run the following command:
   ```
   aws iam create-instance-profile \
   --instance-profile-name <Workernodes Instance profile name>
   ```
2. Record your assigned worker node's instance profile name in the AWS worksheet. In our example we will use `srgdemo-workernodes-instance-profile`. The command will return a description of the newly-created instance profile. For example:

```
{
   "InstanceProfile":{
      "InstanceProfileId":"AIPAJMBYC7DLSPEXAMPLE",
      "Roles":[

      ],
      "CreateDate":"2015-03-09T20:33:19.626Z",
      "InstanceProfileName":"Webserver",
      "Path":"/",
      "Arn":"arn:aws:iam::123456789012:instance-profile/Webserver"
   }
}
```

3. Record the Arn value in the AWS Worksheet as `Workernodes Instance profile ARN.`
4. Run the following command to add the role to the instance profile:
   ```
   aws iam add-role-to-instance-profile \
   --instance-profile-name <Workernodes Instance profile name> \
   --role-name <Workernodes role name>
   ```

Where:

`<Workernodes Instance profile name>`: Use the instance profile name created above or by your AWS infrastructure administrators and recorded in the AWS worksheet. For example, `srgdemo-workernodes-instance-profile.`

`<Workernodes role name>`: Use the role name created by your AWS infrastructure administrators and recorded in the AWS worksheet. For example, `srgdemo-workernodes-svc-role.`

Example:
`aws iam add-role-to-instance-profile --instance-profile-name srgdemo-workernodes-instance-profile --role-name srgdemo-workernodes-svc-role`

The command has no output.

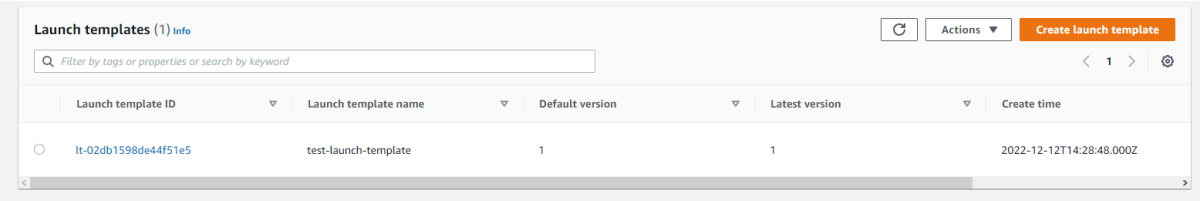
Creating and Configuring a Launch Template

A *launch template* is an configuration template that an Auto Scaling group uses to launch EC2 instances. Creating a launch template requires collecting some infrastructure data, specifically the Amazon Machine Image ID (AMI ID) and instance type. You can have more than one launch template created with different parameters, such as instance type or root volume size, and instantiate the auto-scaling groups from them.

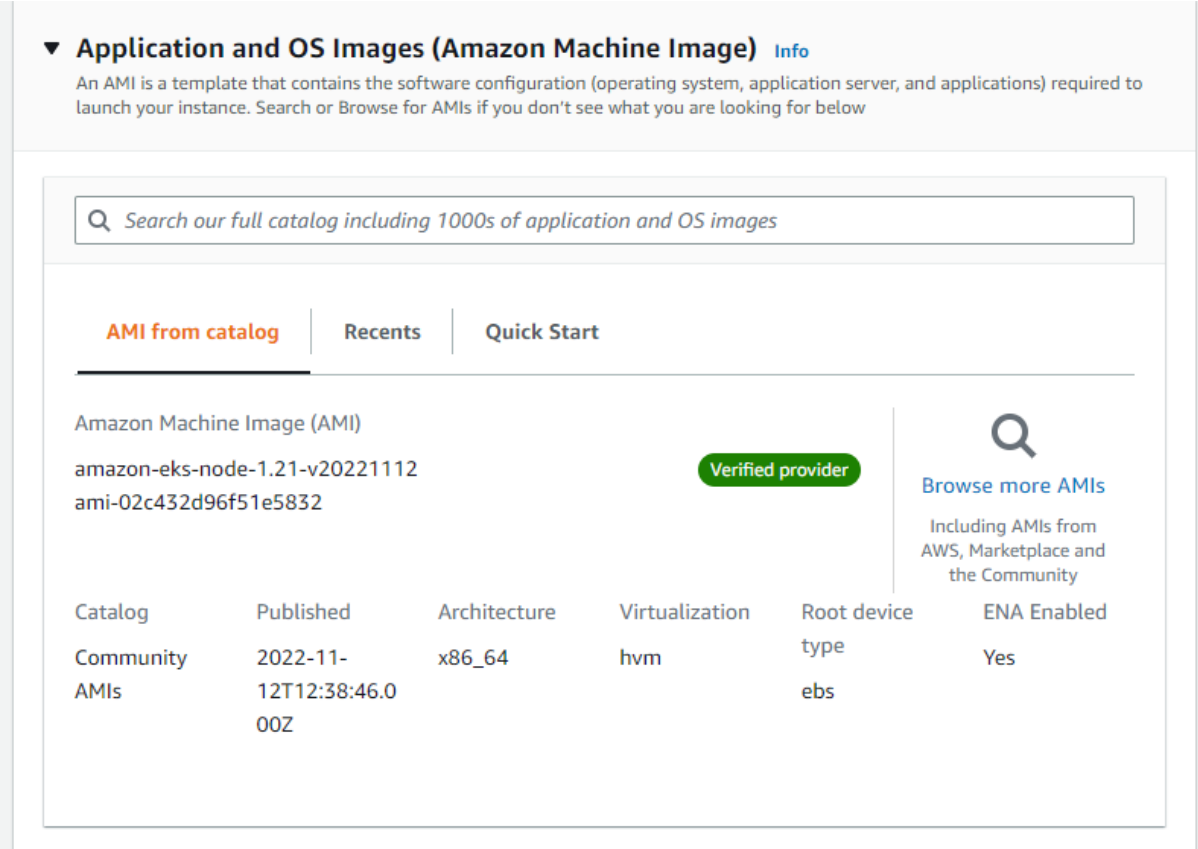
> Launch templates replace the deprecated launch configurations feature found in earlier versions of AWS. See Migrating a Launch Configuration to a Launch Template for instructions on migrating an existing launch configuration to a launch template. ArcSight recommends you migrate to launch templates as soon as possible.

To create a launch template using the web UI:

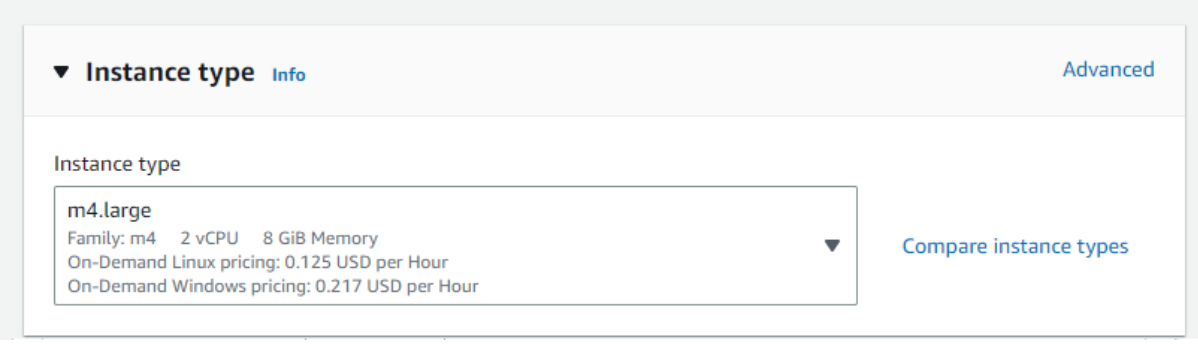
1. Using the **Find Services** search tool, locate and browse to the EC2 Dashboard.
2. In the left navigation panel, under **Instances**, select **Launch templates.**
3. On the **Launch templates** page, click **Create Launch templates.**



4. On the **Create Launch template** page, in **Launch template name,** specify a name for the launch template.
5. Under **Application and OS Images (Amazon Machine Image)**, provide the AMI for the worker node.



6. Under **Instance type**, specify the virtual machine hardware, such as *m4.large.*



If you are deploying the Intelligence capability, you must use a minimum of m5.4xlarge with 16 core CPUs and 64 GB RAM.

7. Under **Key pair (login)**, select the existing key pair or create a new one.
8. Each resource must be accessible through the network and all worker nodes must have the correct security groups assigned to them. Under Network settings, choose **Select an existing security group,** and then select the security group you created for intra-VPC communications, recorded in the AWS worksheet.

9. Under **Storage (volumes),** specify the value of **Size** with a minimum value of 50 GB. You may specify more depending on your plans for product installation and workload.
10. Under **Advanced details,** specify values for the following settings:

- **IAM instance profile:** Choose the instance profile name for the worker nodes from the AWS worksheet.
- **User data**: Copy the contents of the script workernodes-userdata located in the aws-scripts folder. In the text area, replace <cluster name> with your own cluster name from the AWS worksheet.

11. Click **Create launch template**.

To create a launch template using the CLI:

1. Run the following command:

```
aws ec2 create-launch-template \
--launch-template-name <Launch Template name> \
--launch-template-data '{"NetworkInterfaces":[{"DeviceIndex":0,"Groups":
["<Intra VPC Security group Id>"]}],"ImageId":"<Launch template AMI
Id>","InstanceType":"<Instance type>","KeyName":"<Key pair name>
","IamInstanceProfile":{"Arn":"<Workernodes Instance profile
ARN>"},"BlockDeviceMappings":[{"DeviceName":"<root device name>","Ebs":
{"VolumeSize":<root volume
size>,"VolumeType":"gp3","DeleteOnTermination":true}}],"UserData":"'$USER
DATA'"}'
```

Where:

`<Launch Template name>`: Choose a name that helps with easier identification. In our examples we will use `srgdemo-workers-launch-template`. Record the chosen value in your AWS worksheet.

`<Launch Template AMI ID>`: Run the following command to get the actual AMI ID.

```
aws ec2 describe-images \--filters "Name=architecture,Values=x86_64"
"Name=name,Values=amazon-eks-node-<Kubernetes version>*" | jq '.Images | map
(select((.Description!=null) and (.Description | contains("GPU") | not) and
(.ImageLocation | contains("gpu") | not))) | sort_by(.CreationDate) | [last]'
```

> **Important!** Replace the value `<Kubernetes version>` with the Kubernetes version number you used to create the EKS, and recorded as the `Kubernetes version` in your AWS worksheet. **Retain the asterisk** at the end of the value for the name filter.

`<Key pair name>`: Use the key pair name from the AWS worksheet.

`<Intra VPC Security group Id>`: ID of Intra VPC security group recorded in the AWS worksheet.

`<Instance type>`: From Amazon EC2 Instance Types, choose your host hardware configuration. Consider CPU, RAM, storage type, network performance, and price.

> Instance type resources must be selected based on the *Technical Requirements for ArcSight Platform 24.2*.

`<root device name>`: In the description obtained for AMI ID above, locate the value for key `RootDeviceName`.

`<root volume size>`: Size depends on planned installation size: 50GB for SMALL, 100GB for MEDIUM, and 256GB for LARGE. Sizes refer to the sizes from ArcSight Suite metadata definition, in gigabytes.

`<Workernodes instance profile ARN>`: Use the instance profile ARN you created above or created by your AWS infrastructure administrators and recorded in your AWS worksheet.

`$USERDATA`: To specify a value for this environment variable, copy the file `workernodes-userdata` located in `aws-byok-installer-<version>/scripts/` to the current working directory on the local host or the bastion, then open in a text editor. Replace the parameter cluster name with the value from the AWS worksheet and save the file.

Example of workernodes-userdata:

```
#!/bin/bash
set -o xtrace
/etc/eks/bootstrap.sh srgdemo-cluster --kubelet-extra-args \
--node-labels='Worker=label,role=loadbalancer,node.type=worker'
```

Extending labels, as shown here, during the launch configuration creation will be important for scaling up the cluster later. However, if you do not assign labels automatically, you must manually add new labels every time you add a new node.

To prepare the environment variable execute the following command:

```
USERDATA=$(base64 workernodes-userdata | tr -d "[:space:]")
```

> Validate the content of USERDATA by executing echo `$USERDATA | base64 -d`

Full example of the command to create a launch template:

```
aws ec2 create-launch-template \
--launch-template-name srgdemo-workers-launch-template \
--launch-template-data '{"NetworkInterfaces":[{"DeviceIndex":0,"Groups":["sg-
022a13e4e54ddfbb6"]}],"ImageId":"ami-
02c432d96f51e5832","InstanceType":"m4.large","KeyName":"my_ssh_key_
pair","IamInstanceProfile":{"Arn":"arn:aws:iam::115370848038:instance-
profile/srgdemo-workernodes-instance-profile"},"BlockDeviceMappings":
```

```
[{"DeviceName":"/dev/xvda","Ebs":
{"VolumeSize":100,"DeleteOnTermination":true}}],"UserData":"'$USERDATA'"}'
```

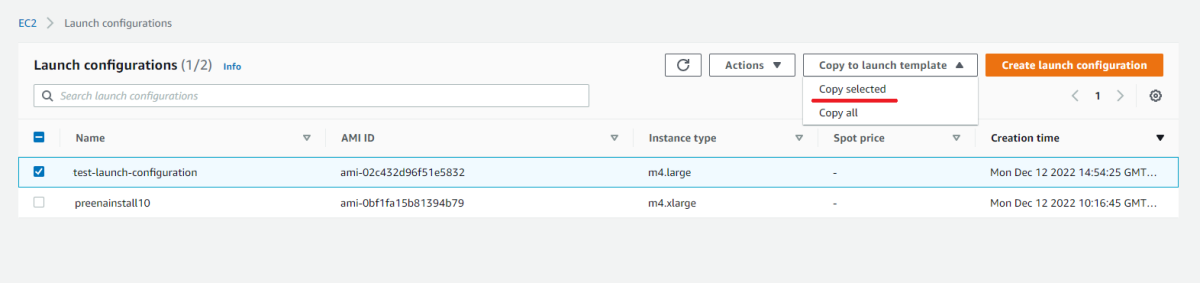
Note the `LaunchTemplateId`, which will be used in the next step.

Migrating a Launch Configuration to a Launch Template

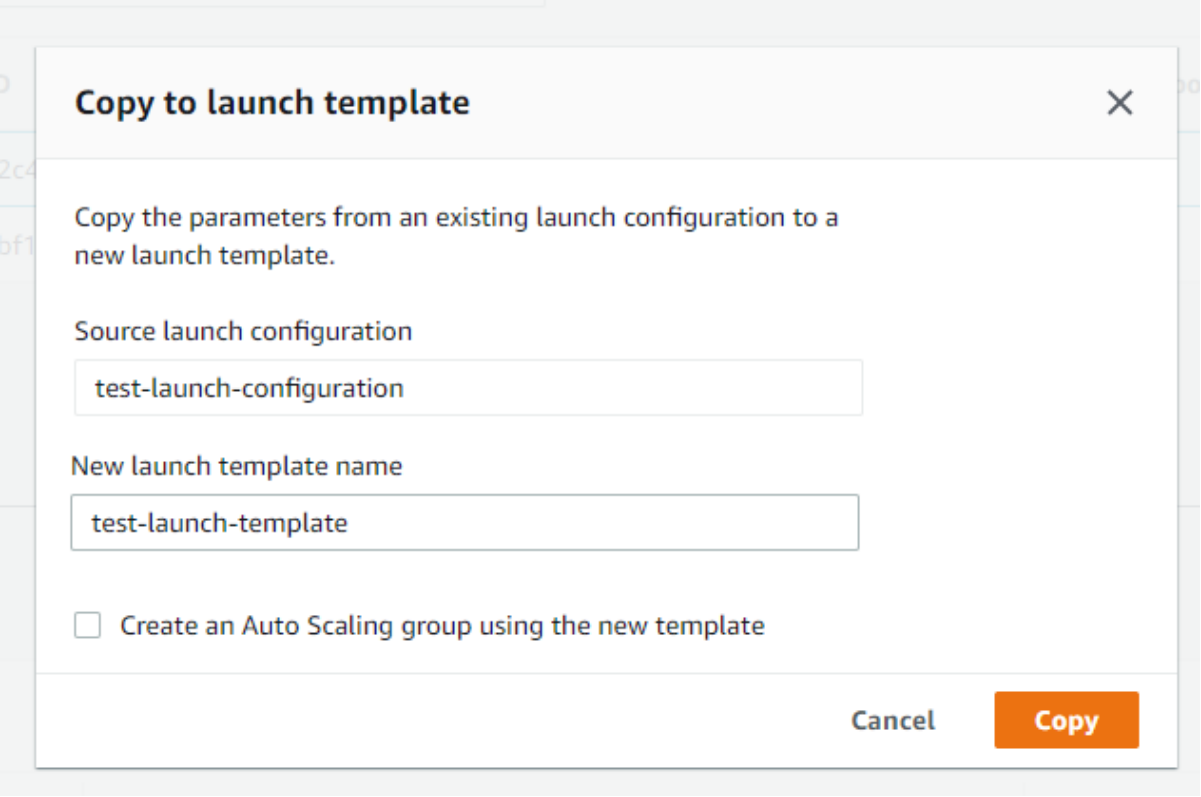
AWS has deprecated the launch configuration feature, which has been replaced by launch templates. You can migrate an existing launch configuration to a launch template by following the procedures given here. This procedure will use the AWS web UI (management console).

> ArcSight recommends that you migrate any existing launch configurations to launch templates as soon as possible.

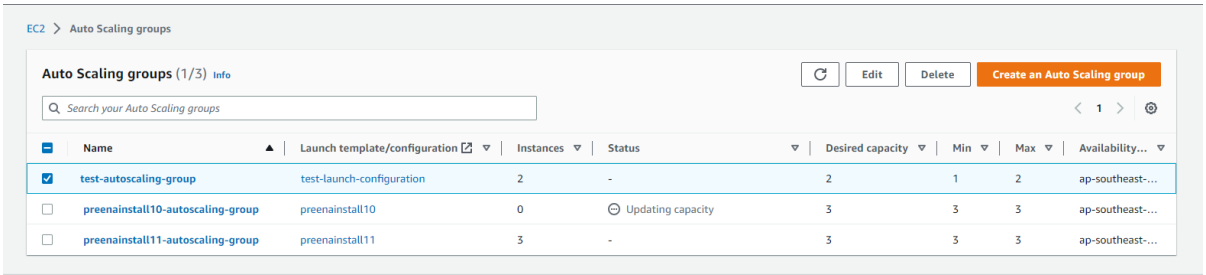
1. In AWS, locate and browse to the EC2 Configuration dashboard.
2. From the list of launch configurations, select the configuration you want to migrate.
3. Click **Copy to launch template**, and from the drop-down, select **Copy Selected.**



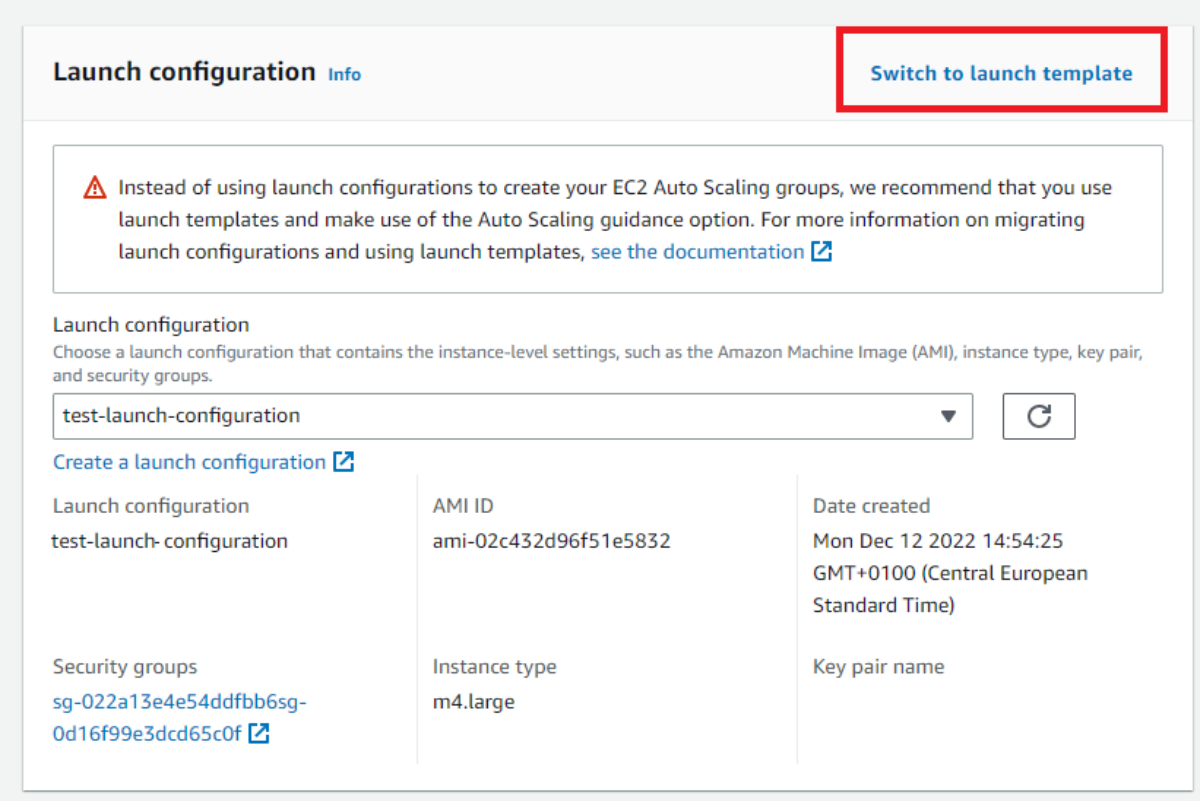
4. On the **Copy to launch template** dialog, validate the new launch template name and then click **Copy**.



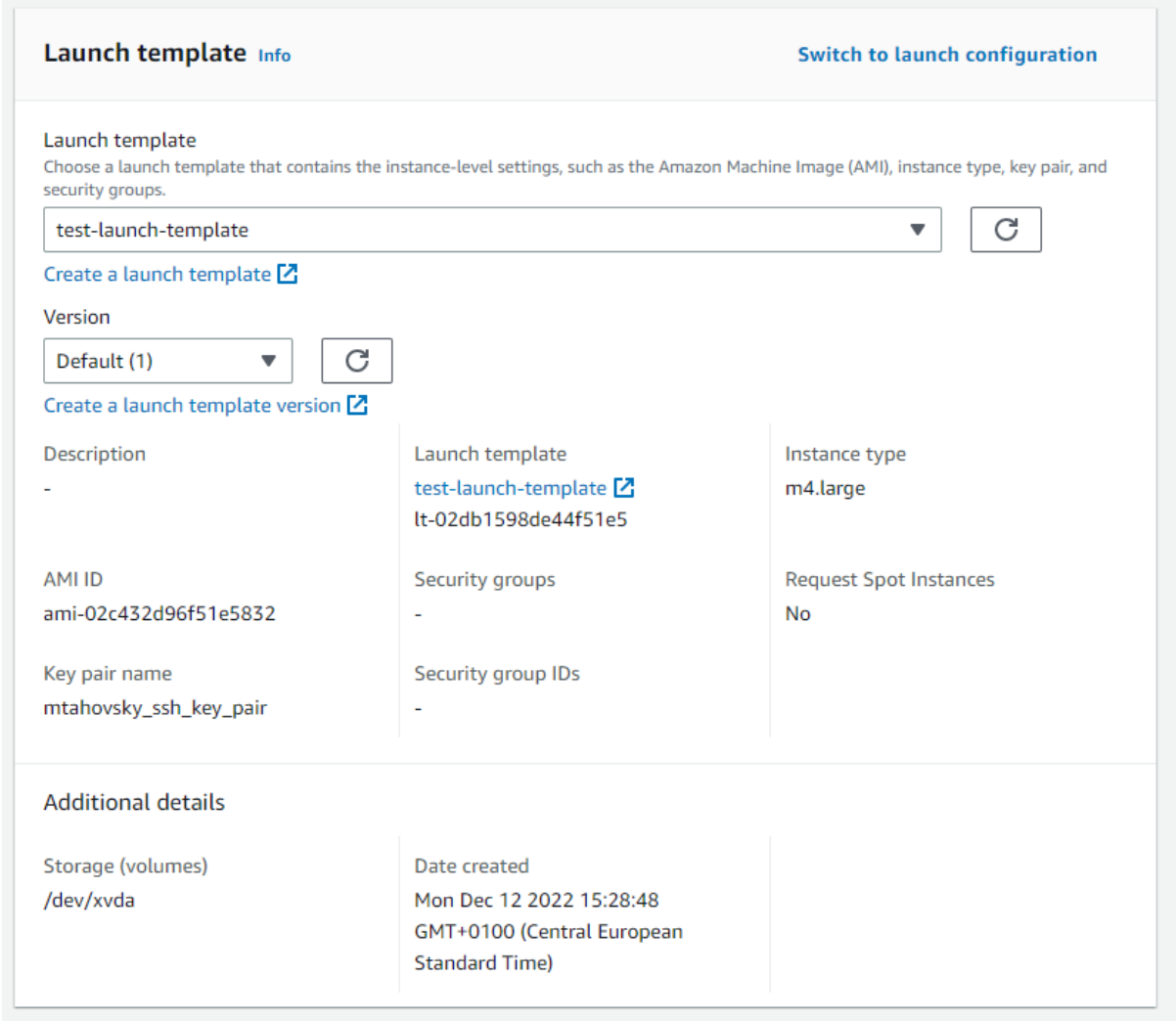
5. The new template is displayed in the list of launch templates. You are now ready to replace your existing launch configuration (already in use) with the new launch template.
6. Navigate to the **Auto Scaling groups** console.
7. Select your **Auto Scaling group** and click **Edit**.



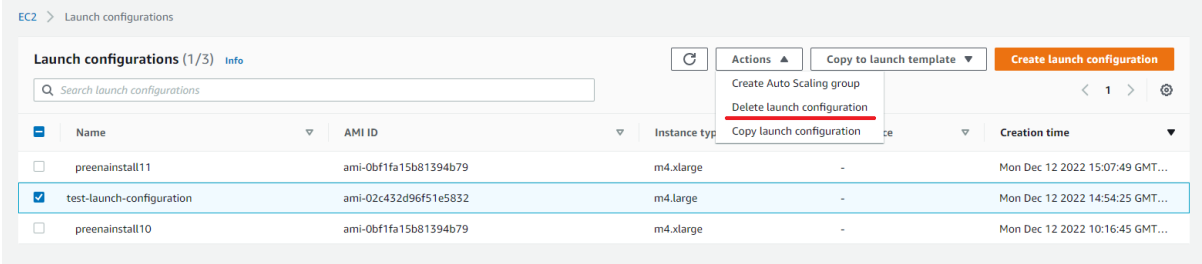
8. Scroll down to the **Launch configuration** section and then click **Switch to launch template.**



9. Select your newly-created launch template. On the Launch template dialog, review and verify your configuration, and when ready, scroll down and click **Update.**



10. You can now delete the old launch configuration. In the list of launch configurations, select the old configuration.
11. Click **Actions**, and from the drop-down select **Delete launch configuration.**



Creating the AWS Auto Scaling Group

AWS Auto Scaling enables you to build scaling plans that automate how groups of different resources respond to changes in demand. You can optimize availability, costs, or a balance of both.

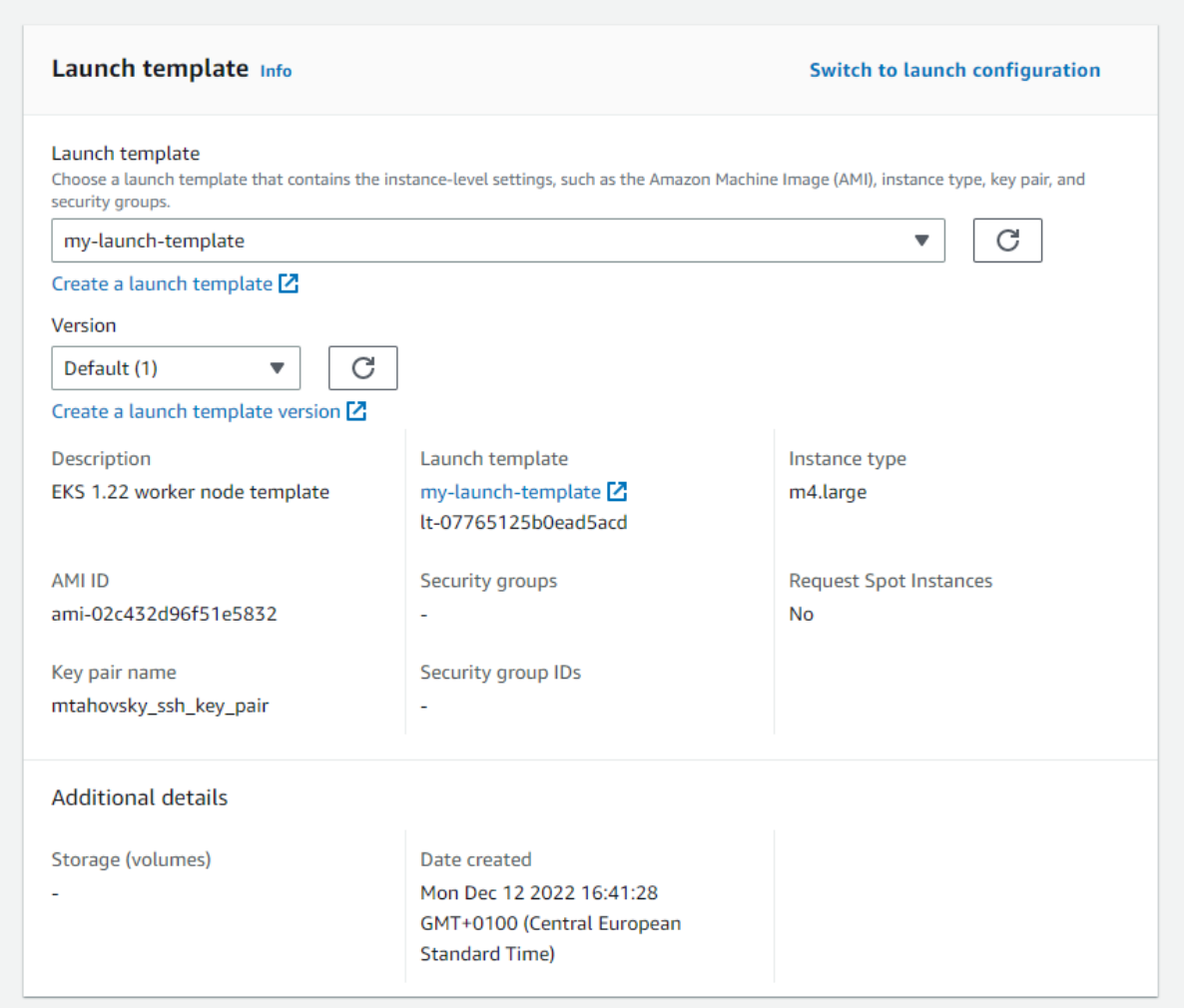
Before proceeding, verify that the correct tag has been assigned to the VPC.

To create the Auto Scaling group using the web UI:

1. Using the Find Services search tool, locate and browse to the EC2 dashboard.
2. In the left navigation panel, under **Auto Scaling**, select **Auto Scaling Groups.**
3. On the landing page, click **Create Auto Scaling Group** to launch the creation wizard.

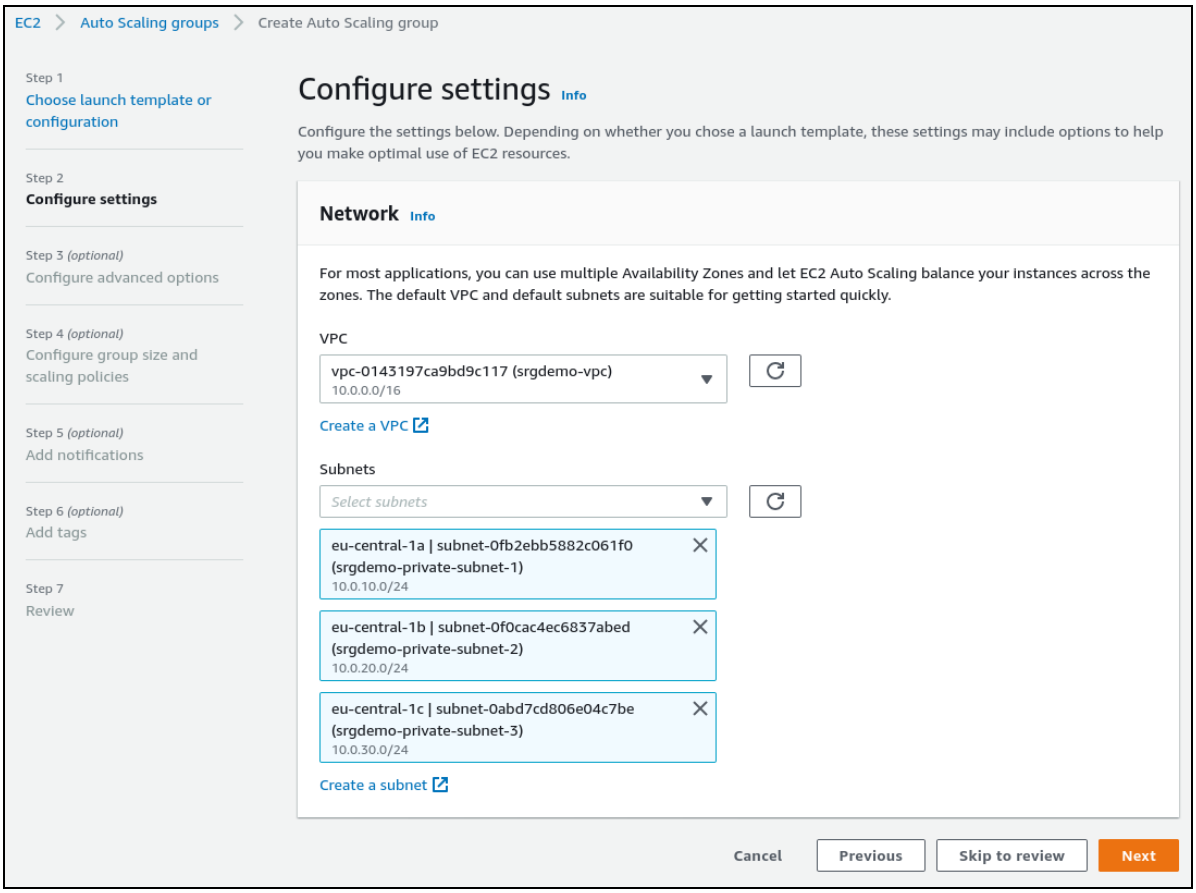
If no Auto Scaling groups have been created yet, the introduction to Auto Scaling implementation in AWS is displayed.

4. On the **Choose Launch template or configuration** page, enter values for the following:
   a. **Name:** Enter a descriptive name for the Auto Scaling group.
   b. Under **Launch template**, select the launch template you created previously.

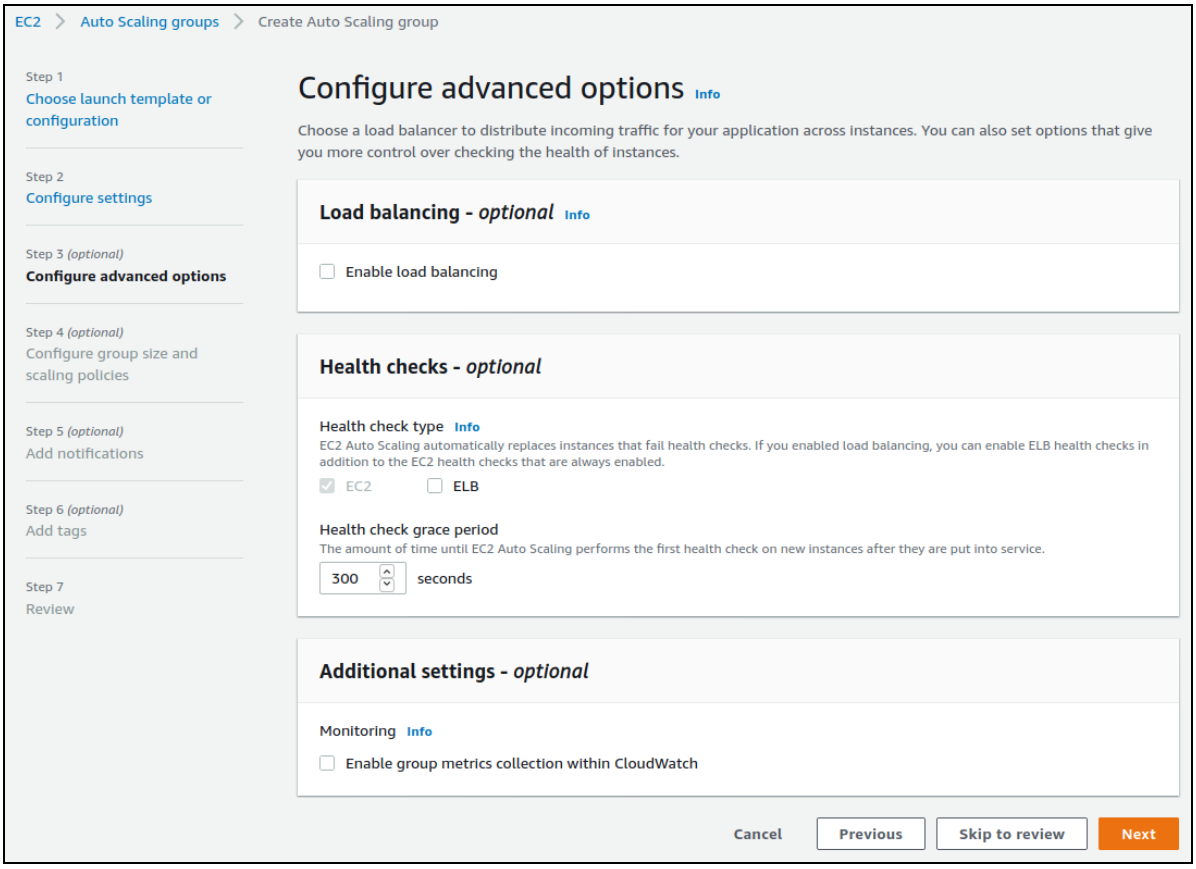


5. Click **Next**.

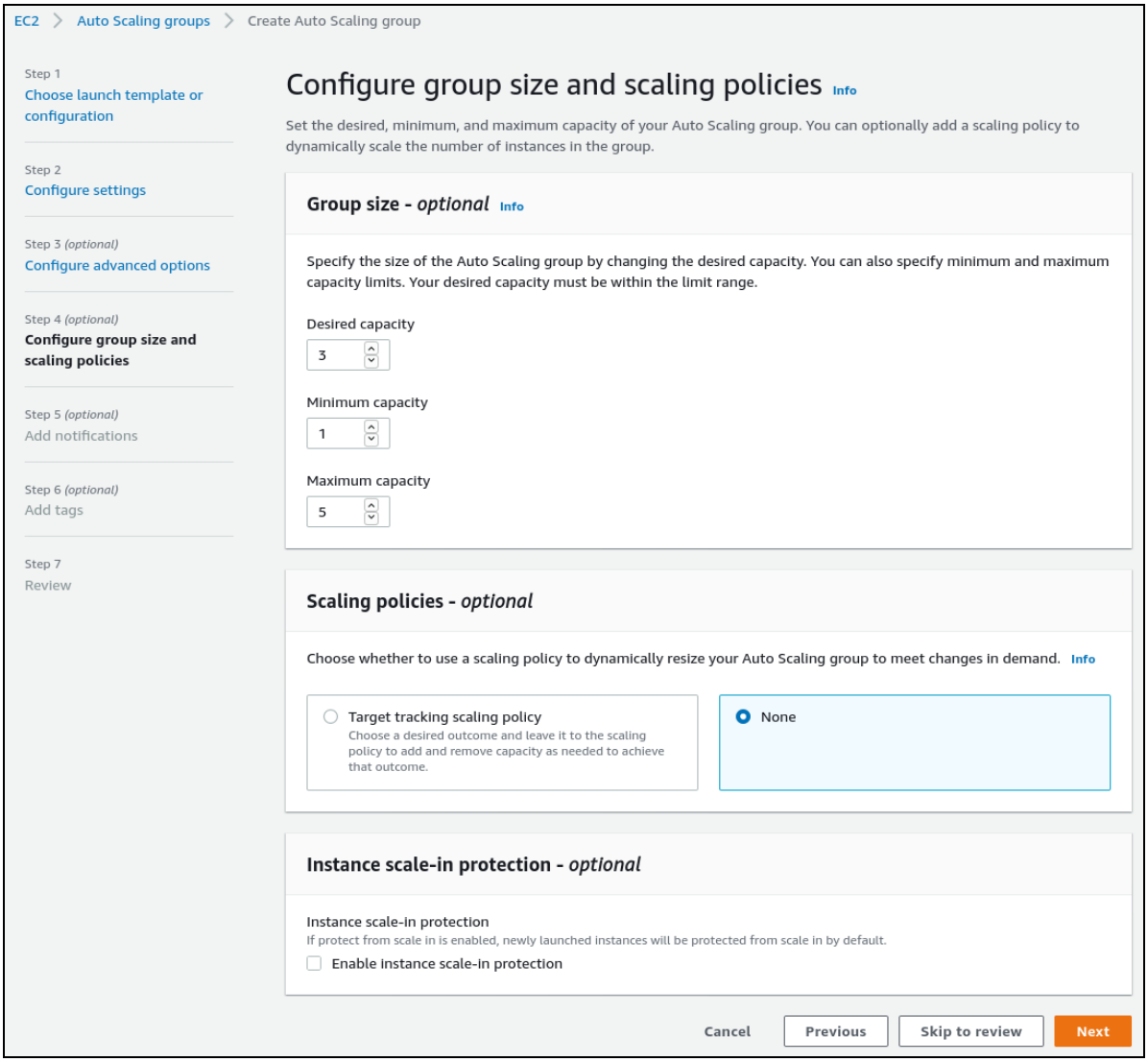
6. On the **Configure settings** page, enter values for the following:
   a. **VPC:** Choose the previously-created VPC recorded in the AWS worksheet.
   b. **Subnets:** Select all 3 **private** subnets (recorded on the AWS worksheet).



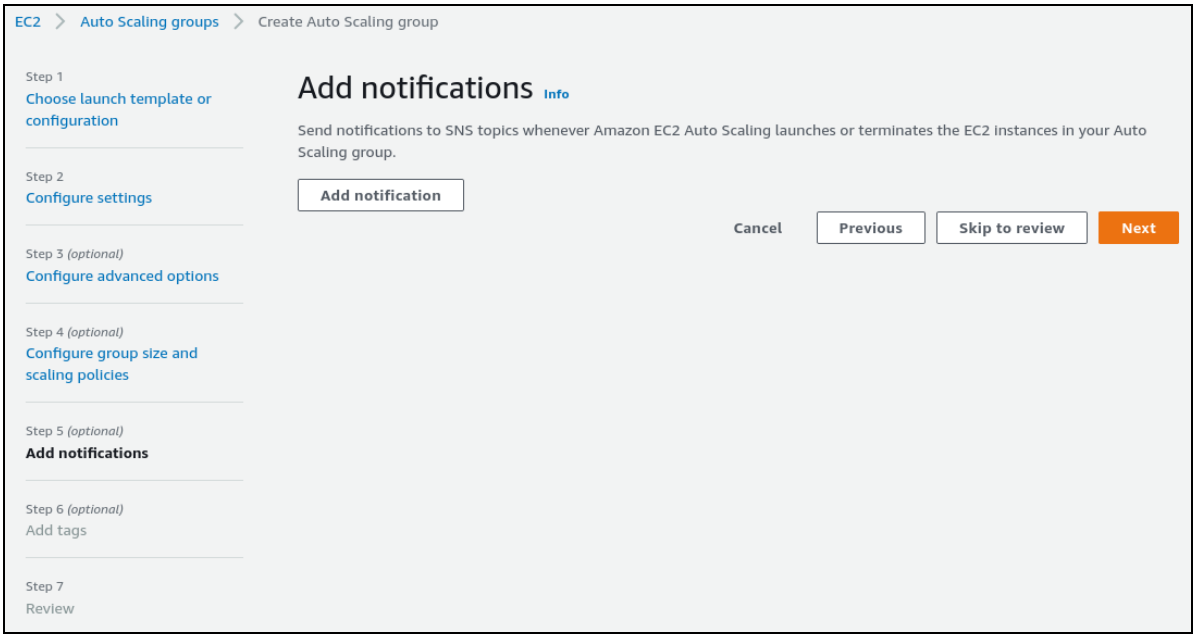
7. Click **Next**.
8. On the **Configure advanced options** page, leave all values at default and click **Next**.



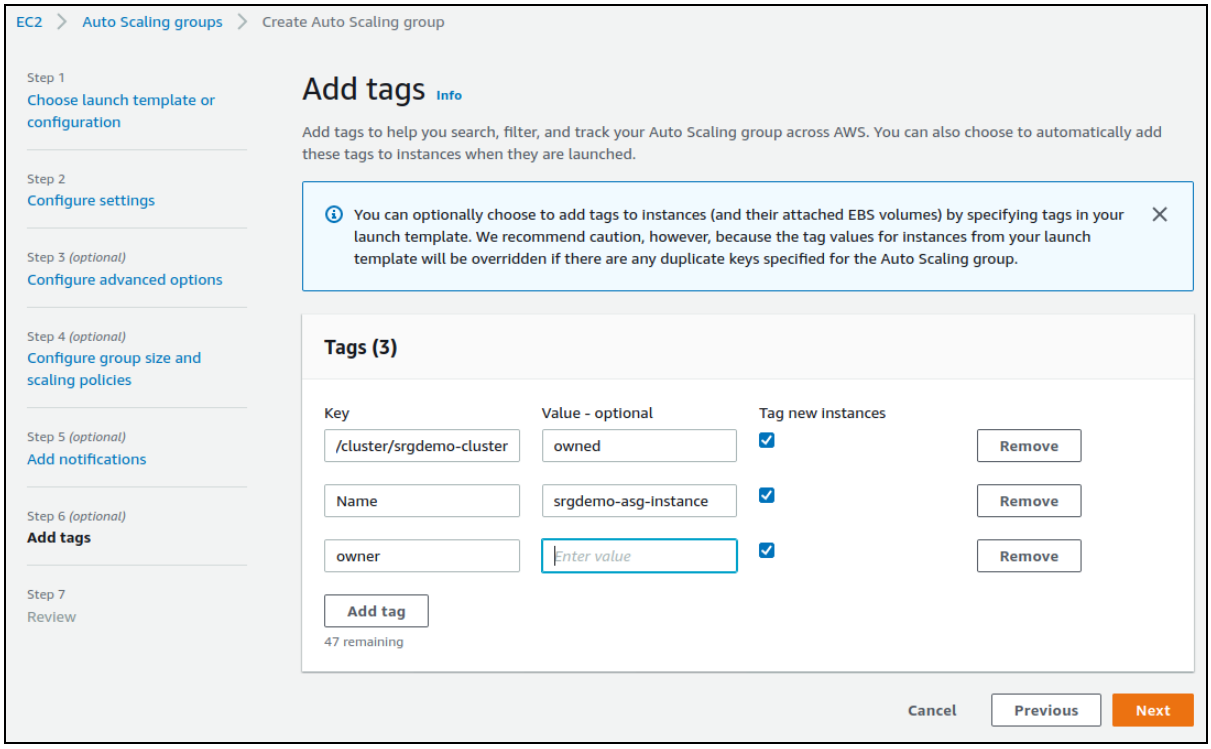
9. On the **Configure group size and scaling policies** page, set values for **Desired capacity** and **Maximum capacity**. In the example shown here, there will initially be 3 nodes and enough space to instantiate 2 more by simply increasing the desired capacity. (For a production cluster, the minimum capacity setting should not be less than 2.)



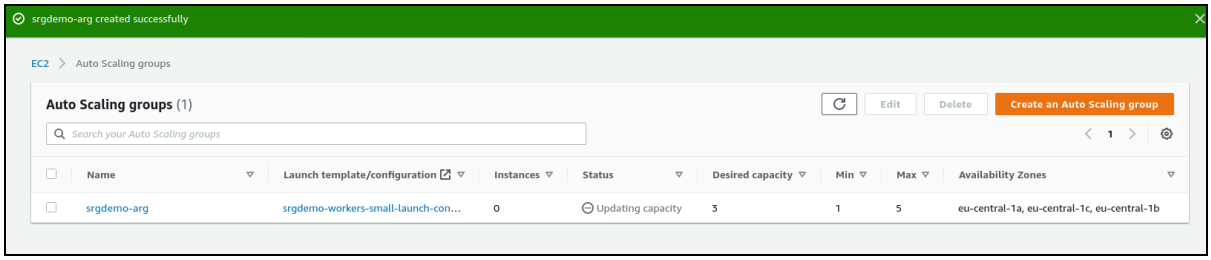
10. Click **Next**.
11. On the **Add Notifications** page, ignore all settings and click **Next**.



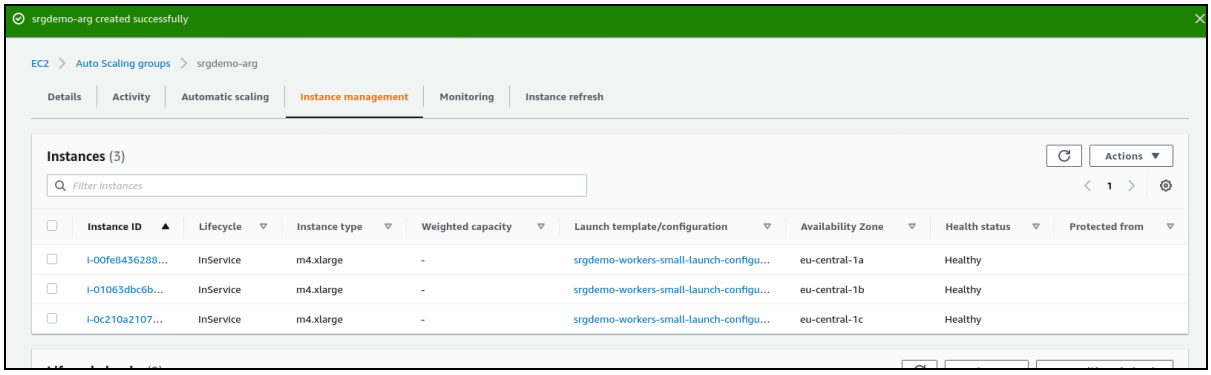
12. On the **Add Tags** page, add tags as follows:
    a. Add the mandatory tag key: `kubernetes.io/cluster/<your cluster name>` with value: `owned` (replace `<your cluster name>` with your actual cluster name).
    b. Optionally, add these tags as desired:
        i. Key: `Name` with value: derived from the auto-scaling group name.
        ii. Key: `owner` with value: corresponding to you.
    c. For all new tags you add, select the **Tag new instances** checkbox so new instances are automatically tagged.
13. Click **Next**.



14. On the **Review** page, verify your settings, and then click **Create Auto Scaling Group.**



15. For networking configurations, we will need to know the machine instance IDs in the new Auto Scaling group. On the **Auto Scaling Groups** management page, select your new group.



16. From the **Instances** tab, record all instance IDs in the AWS worksheet.

To create the Auto Scaling group using the CLI:

1. Run the following command:

```
# aws autoscaling create-auto-scaling-group \
--auto-scaling-group-name <Autoscaling group name> \
--launch-configuration-name <Launch template name> \
--min-size <min size> \
--desired-capacity <desired size> \
--max-size <max size> \
--tags "Key=kubernetes.io/cluster/<cluster name>,Value=owned"
"Key=Name,Value=<auto scaling group name>" \
--vpc-zone-identifier "<subnet Ids>"
```

Parameters:

`<Autoscaling group name>`: Choose a name which helps with easier identification; in this guide we will use srgdemo-autoscaling-group. Record the value in the AWS worksheet.

`<Launch template name>`: Name of the launch template created earlier.

`<min size>`: The minimum size of the group. For a production cluster, this should not be less than 2. If installing Transformation Hub, no less than 3.

`<desired size>`: The number of Amazon EC2 instances that the Auto Scaling group attempts to maintain. This number must be greater than or equal to the minimum size of the group and less than or equal to the maximum size of the group. If you do not specify a desired capacity, the default is the minimum size of the group.

`<max size>`: The maximum size of the group.

`<Cluster Name>`: Use the cluster name from the AWS worksheet.

`<subnet Ids>`: A comma-separated list of private subnet IDs for your virtual private cloud (VPC); use values from from the AWS worksheet.

Example:

```
aws autoscaling create-auto-scaling-group \
--auto-scaling-group-name srgdemo-autoscaling-group \
--launch-template LaunchTemplateId=lt-0d2a237fcf4f5193e \
--min-size 1 \
--desired-capacity 3 \
--max-size 3 \
--tags "Key=kubernetes.io/cluster/srgdemo-cluster,Value=owned"
"Key=Name,Value=srgdemo-autoscaling-group"
--vpc-zone-identifier "subnet-0fb2ebb5882c061f0,subnet-
0f0cac4ec6837abed,subnet-0abd7cd806e04c7be"
```

It can take approximately 5 minutes for nodes to be created and join the cluster.

Retrieve the instance IDs from auto-scaling group

For networking configurations, we will need to know the machine instances in the new Auto Scaling group.

To retrieve the instance IDs:

1. Run the command:

```
# aws autoscaling describe-auto-scaling-instances \
| jq -r '.AutoScalingInstances[] | select
(.AutoScalingGroupName=="srgdemo-autoscaling-group").InstanceId'
```

2. Record the returned IDs in the AWS worksheet.

Example command and output:

```
# aws autoscaling describe-auto-scaling-instances \
| jq -r '.AutoScalingInstances[] | select(.AutoScalingGroupName=="srgdemo-
autoscaling-group").InstanceId'
i-05662f9ef84c182ca
i-07cfcd6716e9890b5
i-08d819b5ccabe83cb
```

After approximately 5 minutes, the nodes will be created and be joined to the cluster. You can then list all the worker nodes.

To list the worker nodes:

1. On the bastion host, run the following command:

```
# kubectl get nodes
```

At this point, you should see all nodes listed in the Ready state with the expected Kubernetes version.

Configuring Route 53

Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. This section describes how to create a publicly available OMT installation, and the OMT management portal, as well as how to reconfigure a suite. Your own business requirements might dictate a different secure configuration.

Selecting a Public Hosted Zone and Creating a Record Set

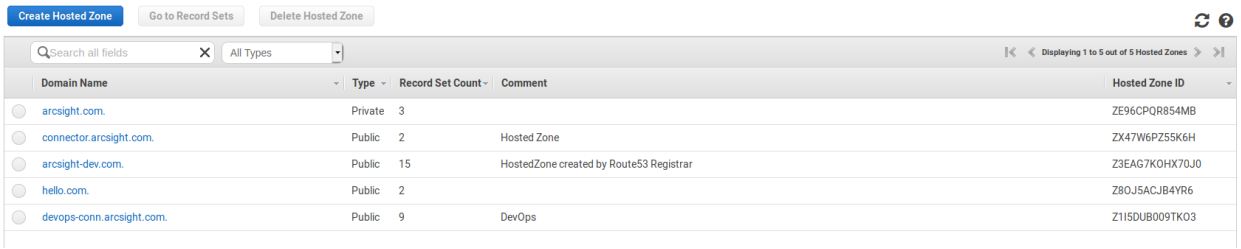
In the Route 53 service, DNS records are organized in *hosted zones.* A hosted zone is analogous to a traditional DNS zone file; it represents a collection of records that can be managed together, belonging to a single parent domain name. All resource record sets within a hosted zone must have the hosted zone's domain name as a suffix.

In this section you will select a **public** hosted zone, which must be previously created by an AWS administrator, and create the record set.

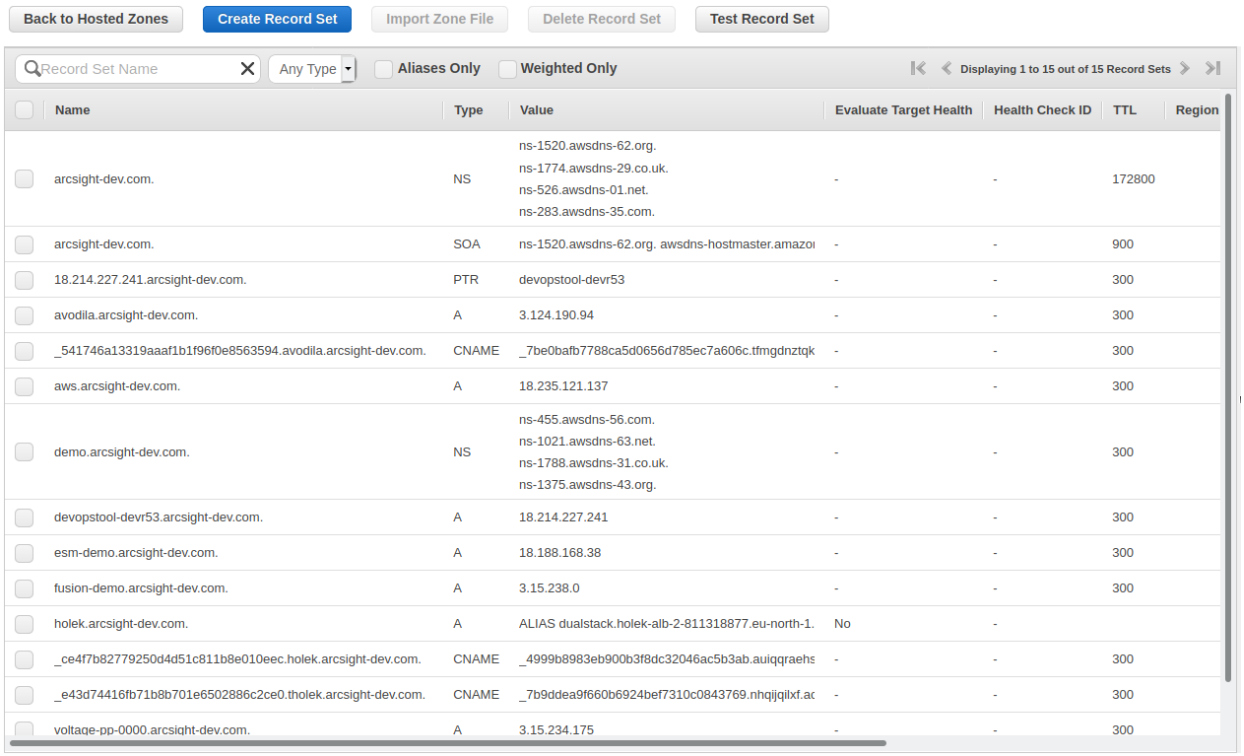
> Do not use a private hosted zone.

To select an existing public (not private) hosted zone and create the record set using the web UI:

1. Using the Find Services search tool, locate and browse to the Route 53 dashboard.
2. In the left navigation panel, select **Hosted Zones**. Ignore any error message about insufficient permission.
3. From the list of hosted zones, select a **public** zone. For our example, we use `arcsight-dev.com`.

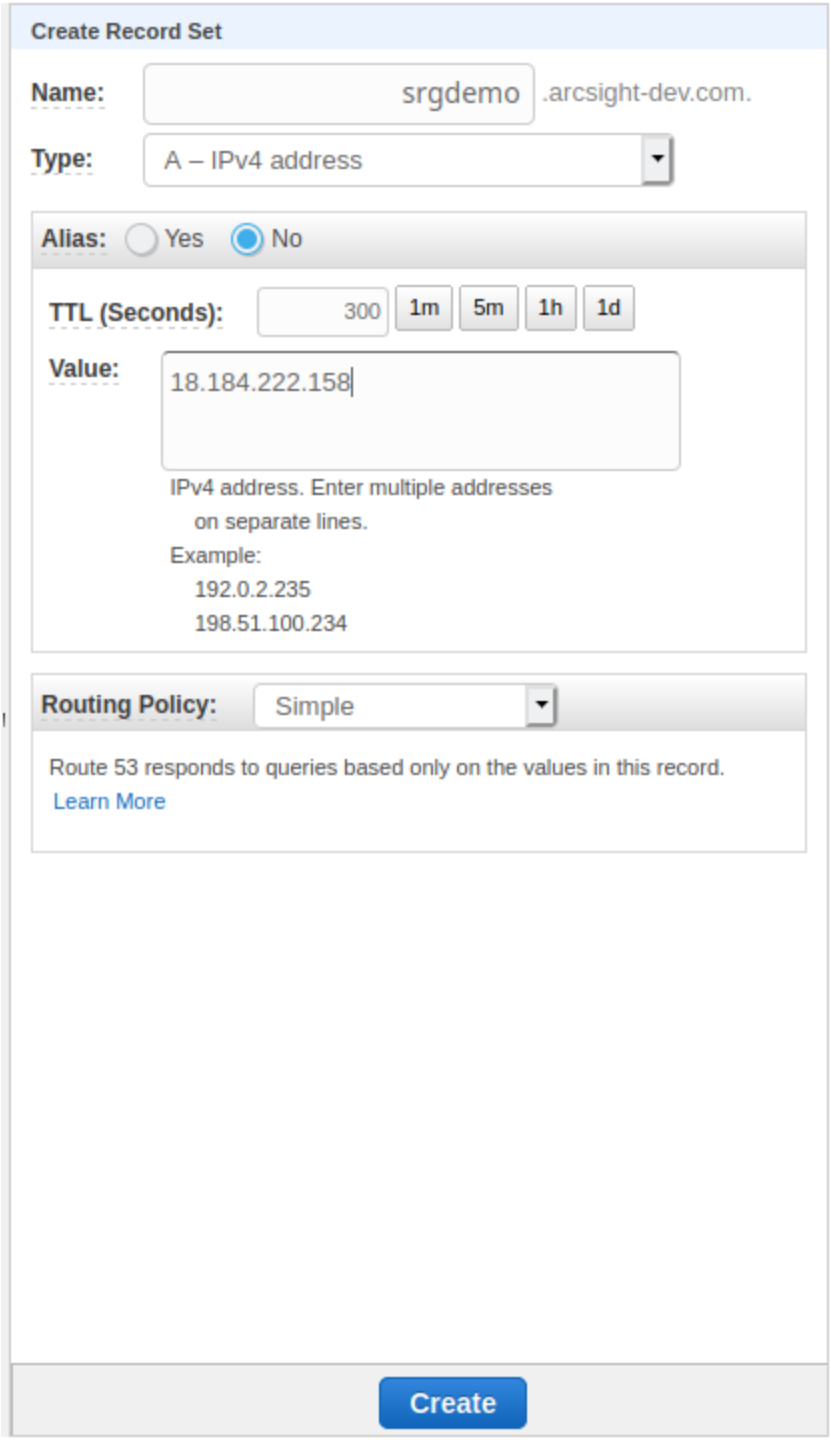


4. Click the public hosted zone domain name to list the record sets in the public zone.



Name	Type	Value	Evaluate Target Health	Health Check ID	TTL	Region
arcsight-dev.com.	NS	ns-1520.awsdns-62.org. ns-1774.awsdns-29.co.uk. ns-526.awsdns-01.net. ns-283.awsdns-35.com.	-	-	172800	
arcsight-dev.com.	SOA	ns-1520.awsdns-62.org. awsdns-hostmaster.amazo	-	-	900	
18.214.227.241.arcsight-dev.com.	PTR	devopstool-devr53	-	-	300	
avodila.arcsight-dev.com.	A	3.124.190.94	-	-	300	
_541746a13319aaaf1b1f96f0e8563594.avodila.arcsight-dev.com.	CNAME	_7be0bafb7788ca5d0656d785ec7a606c.tfmgdnztqk	-	-	300	
aws.arcsight-dev.com.	A	18.235.121.137	-	-	300	
demo.arcsight-dev.com.	NS	ns-455.awsdns-56.com. ns-1021.awsdns-63.net. ns-1788.awsdns-31.co.uk. ns-1375.awsdns-43.org.	-	-	300	
devopstool-devr53.arcsight-dev.com.	A	18.214.227.241	-	-	300	
esm-demo.arcsight-dev.com.	A	18.188.168.38	-	-	300	
fusion-demo.arcsight-dev.com.	A	3.15.238.0	-	-	300	
holek.arcsight-dev.com.	A	ALIAS dualstack.holek-alb-2-811318877.eu-north-1.	No	-		
_ce4f7b82779250d4d51c811b8e010eec.holek.arcsight-dev.com.	CNAME	_4999b8983eb900b3f8dc32046ac5b3ab.auiqqraehs	-	-	300	
_e43d74416fb71b8b701e6502886c2ce0.tholek.arcsight-dev.com.	CNAME	_7b9ddea9f660b6924bef7310c0843769.nhqjjqilxf.ac	-	-	300	
voltage-pp-0000.arcsight-dev.com.	A	3.15.234.175	-	-	300	

5. Click **Create Record Set** and specify or verify values for the following parameters:
   - **Name:** Choose a name for the A-record. The record set FQDN will then be composed from this name and the public hosted zone domain name. In our example we will use `srgdemo`. Our example installation will then be available at the URL: `srgdemo.arcsight-dev.com`.
     Record the record set FQDN in the AWS worksheet.
   - **Type:** *A - IPv4 address.*
   - **Alias:** *No*
   - **TTL:** Leave default.
   - **Value:** Specify your bastion's public IP address.
   - **Routing Policy:** *Simple*



6. Click **Create.** The new record set is displayed in the list.

To select an existing public (not private) hosted zone and create a record set using the CLI:

1. Run the following command to select **public** hosted zones:

```
aws route53 list-hosted-zones \
| jq -r '.HostedZones[] | select(.Config.PrivateZone==false) | "Id:   " +
.Id,"Name: " + .Name," " '
```

A list of hosted **public** zones is returned. For example:

```
Id:   /hostedzone/ZX47W6PZ55K6H
Name: connector.arcsight.com.
```

```
Id:   /hostedzone/Z3EAG7KOHX70J0
Name: arcsight-dev.com.
```

```
Id:   /hostedzone/Z8OJ5ACJB4YR6
Name: hello.com.
```

```
Id:   /hostedzone/Z1I5DUB009TKO3
Name: devops-conn.arcsight.com.
```

> The dots and period characters (.) at the end of each value are present intentionally. **Please do not remove them.**

2. Choose one of the **public** hosted zones. For example, we will use the **public** hosted zone (name shown includes a period):
   `arcsight-dev.com.`
   Record the chosen **public** hosted zone name and ID in the AWS worksheet under `Hosted zone name` and `Hosted zone Id` respectively.
3. Choose a subdomain in the selected public hosted zone. For example, we will use `srgdemo`. Combining the subdomain and hosted zone name with a final period will give us the complete DNS name where our new cluster will be accessible.
   Example:
   `srgdemo.arcsight-dev.com.`
4. From the directory `arcsight-platform-cloud-installer-<version>/aws-scripts/objectdefs/`, copy the supplied template `CreateRecordSetInHostedZone.json` to the working folder.
5. Open the template in a text editor and set values for the following placeholders:
   a. `<Record name>`: Combine the name of the hosted zone (for example, `srgdemo`) and Hosted zone name (for example, `arcsight-dev.com`) to create the DNS name and then append the dot character (.) `Example: srgdemo.arcsight-dev.com.`

b. `<Record type>`: Replace with a value of `A`.

c. `<Record value>`: Use your bastion IP address.

> The placeholders in the template use syntax `<placeholder name>`, for example, `<Record name>`.

The following example shows a modified JSON template. Notice that the trailing period in the record name is mandatory.

```
{
   "Changes":[
      {
         "Action":"UPSERT",
         "ResourceRecordSet":{
            "Name":"srgdemo.arcsight-dev.com.",
            "Type":"A",
            "TTL":300,
            "ResourceRecords":[
               {
                  "Value":"3.120.237.11"
               }
            ]
         }
      }
   ]
}
```

6. Run the following command:

```
aws route53 change-resource-record-sets \
--hosted-zone-id <Hosted zone Id> \
--change-batch file://CreateRecordSetInHostedZone.json
```

Where:

`<Hosted zone Id>`: Use the hosted zone ID retrieved above. For example: `/hostedzone/Z3EAG7KOHX70J0`

`--change-batch`: Replace the parameter here with your own modified instance of the JSON file `CreateRecordSetInHostedZone.json`.

The command returns a change request. For example:

```
{
   "ChangeInfo":{
      "Id":"/change/C04669622EJ7JNXG69KJO",
      "Status":"PENDING",
```

```
      "SubmittedAt":"2020-06-09T09:35:06.376000+00:00"
   }
}
```

Later, the status will change to `INSYNC. To validate the status, run this command:`

```
aws route53 get-change --id <change id>
```

Output example:

```
{
   "ChangeInfo":{
      "Id":"/change/C04669622EJ7JNXG69KJO",
      "Status":"INSYNC",
      "SubmittedAt":"2020-06-09T09:35:06.376000+00:00"
   }
}
```

Uploading Product Images to the ECR

The Amazon Elastic Container Registry (ECR) is an AWS managed Container Registry. OMT and Kubernetes will search for product images to download from the ECR and instantiate them.

The ECR is accessible from the internet and protected by username and password credentials. You can perform tasks in this section from a local host or from the bastion, as long as the AWS CLI has been configured.

Uploading images requires the `upload_images_to_ECR` script to be installed and located in the `aws-scripts/scripts/` directory.

This script parses the `manifest.json` description file and creates the ECR and its repositories. Then the OMT script `uploadimages.sh` is called, which passes the correct parameters and uploads the product images.

Uploading Image Requirements

In order to be able to upload images to the ECR, the following requirements must be met:

- You must be able to execute a bash script.
- The system used must have the following basic Linux/Unix utilities installed:
  - `cat`
  - `find`
  - `awk`
  - `jq`

  - `pwd`
  - `unzip`
  - `tar`
- You must have `aws cli` configured on your system.
- You must have fulfilled all requirements for the OMT `uploadimages.sh` script.

To create the ECR and then upload the product images to it:

1. Verify that you have downloaded the product image files for the capabilities you wish to install.
2. Run the following command:

```
<path to upload script>/upload_images_to_ECR \
-d <images' folder> \
-F <product package> \
-o <organization> \
-y \
[-c <parallel uploads count>]\
[-uip <uploadimages.sh path>]
```

Where:

`<path to upload script>`

It is possible to execute the upload script from any folder. The recommendation is to have the current folder set to the one with downloaded images; then the path would resemble `aws-scripts/`.

`<images' folder>`

Folder where all images in their subfolders are located; usually it is the folder where you have unpacked downloaded packages. Can be specified multiple times for situations where images are located in various folders.

> You must specify at least one image location, either in form of a folder (`-d` option) or as a file path (`-F` option, recommended). If you use the `-d` option, you must unpack the image package before running the script.

`<product package>`

Path to the package file. For example: `./transformationhub-<version>.tar`. It can be specified multiple times.

`<organization>`

Specifies the organization name (namespace) where the suite images are placed in the ECR. Record the chosen organization name in the AWS worksheet. There might be

multiple repositories in the ECR which might be shared or overlap. Pay special attention to specify the correct organization name. The organization name must be valid ASCII, and can be from 2 to 255 characters. It can only contain lowercase letters, numbers, dashes (-), and underscores (_).

`<parallel upload counts>`

Maximum allowed parallel uploads; this is limited based on the CPU cores. The parameter is optional. If not specified, defaults to 8.

`<uploadimages.sh path>`

Path to the original OMT `uploadimages.sh` script. Parameter is optional. When not specified, the `upload_images_to_ECR` script will try to locate it in the images' folder or in the unpacked `cdf-deployer` package, which is contained in the `arcsight-platform-cloud-installer` package. Note that normally you should not unpack this package.

Example:

```
./arcsight-platform-cloud-installer-23.2.00153-23.2.599/aws-
scripts/upload_images_to_ECR \
-F ./transformationhub-3.6.0.1284-master.tar -o srgdemo \
-y \
-c 8
```

3. Run the following command:

```
<path to upload script>/upload_images_to_ECR \
-F cdf-byok-images.tar \
-o <organization>\
-y \
-c <parallel uploads count>
```

Ensure that you give the upload process sufficient time to complete. You can check the returned messages or check the log file in the directory where you are executing the upload script to determine successful upload. While the upload progresses, the repositories are created in the ECR, followed by image uploads to the repositories.

> Multiple suite images can be uploaded as a single command as long as each image package is prefaced with `-F`.

Installing the Database in AWS

This section provides information about installing the ArcSight Database in Amazon Web Services Deployment (AWS).

Understanding Methods for Connecting to AWS S3 Buckets

The database uses a single communal storage location for all data and for the catalog (metadata). Communal storage is the database's centralized storage location, shared among the database nodes. This mode supports communal storage in Amazon S3, which must be set up by your cloud administrator before you can install the database.

Other prerequisites or considerations for the S3 bucket:

- Set up default encryption for the S3 bucket in advance. For information about enabling S3 bucket encryption, see AWS documentation, *Enabling Amazon S3 default bucket encryption*.
- If you require a folder under your S3 bucket, it must be created in the communal storage procedure. Folders pre-created under the bucket via the AWS console are not supported for a new installation of the database.

  For more information, see Installing and Configuring the Database Server
- The database supports connecting to AWS S3 buckets using IAM roles. IAM roles are the default access control method for AWS resources. The database uses this method if you do not configure the legacy access control session parameters.

  To use an IAM role, the bucket must be in the same region as the database cluster and the role needs to be set with the proper permissions for reading and writing to the S3 bucket.

  For more information about IAM roles, see AWS documentation, *IAM Roles for Amazon EC2* and *Creating a role to delegate permissions to an AWS service*.

  The example policy below shows the permissions needed for the IAM policy role:

```
 {
"Sid": "s3CommunalLocationAccess",
"Action": [
"s3:ListBucket",
"s3:GetObject",
"s3:DeleteObject",
"s3:PutObject",
"s3:*MultipartUpload*"
],
"Resource": [
"arn:aws:s3:::<db-communal-storage-bucket-name>/*",
"arn:aws:s3:::<db-communal-storage-bucket-name>"
]
}
```

> In the example above you would replace the <db-communal-storage-bucket-name> with the name of the S3 bucket you created for the database communal storage. For example, `222222222-ap-southeast-1-arcsight-db`

Launching Database Instances in AWS

The ArcSight Database compute operations are performed on a cluster of AWS EC2 (Elastic Compute Cloud) nodes. These nodes must be deployed in AWS before the database can be installed on them.

1. Sign in to the Amazon EC2 console and select a region.
2. Select **Launch Instances**.
3. Enter a name for your instance and add required tags.
4. Search for **AMIs**. The database supports `Red Hat 9.2` AMIs. For information about finding an up-to-date AMI, see the AWS documentation, *Find a Linux AMI*.
5. After selecting the AMI, and reviewing the details, select an **Instance Type**. Choose the AWS EC2 instance type that best matches your requirements.

   > We recommend using an m5d instance type, because it has the best balance of cost, performance, and ease of setup for ArcSight workloads. Take into account that m5d is an instance store that provides temporary storage. For example, data files stored on the instance are lost when the instance is stopped. The durable EBS instance is also supported with Elastic Block Store (EBS). This instance type provides durable storage. For example, data files stored on the instance persist after the instance is stopped.

   > For more information on which size of m5d (instance store) and /m4 (EBS) to use for your workload, see the *Technical Requirements for ArcSight Platform 24.2*.

6. For **Key pair**, select an existing one or create new.
7. Configure your instance with the **VPC**, private **subnets** and **security groups**.
8. In the **Configure storage** section, change the size for the **Root volume** type to 30 GiB, the minimum size for root, or higher.

   > If you use the EBS Instance type, m4, add an EBS volume that follows the System Performance Benchmarks for Sizing and Tuning in the *Technical Requirements for ArcSight Platform 24.2*.

9. In the **Advanced details** section, go to the **IAM instance profile** (IAM role) and select the **IAM profile** you configured to access the S3 bucket for database communal storage. For more information, see Understanding Methods for Connecting to AWS S3 Buckets.

10. In the **Summary** section, configure the number of AWS EC2 instances to deploy. A minimum of three is required for a highly available database cluster, but more might be necessary to handle your workload. For more information on how many instances you need, see the *Technical Requirements for ArcSight Platform 24.2*.
11. Configure the number of AWS EC2 instances to deploy. A minimum of three is needed for a highly available database cluster. For more information, on how many instances you need, see the *Technical Requirements for ArcSight Platform 24.2*.
12. Click **Launch Instances**.
13. Navigate to EC2, and verify your instances are available.

Creating the Swap File

A partition with swap space configured is required to enable virtual memory access. The database requires a minimum of 2 GB of swap space on all database nodes. Perform the following procedure on all database nodes to setup the swap space.

1. From the bastion, login to the database node using SSH and the key pair selected during instance launching. For example:

```
ssh -i <FilePath to the ec2 keypair/IdentityFile> root@<node1..n>
```

2. Create the file that will be used for swap:

```
sudo dd if=/dev/zero of=/swapfile bs=1024 count=2621440
```

> The count 261440 is the minimum value required for installation, but it is also an example. You can set the value higher.

3. Enable read and write to the swap file for the root user (only):

```
sudo chmod 600 /swapfile
```

4. Set up the file as a Linux swap area:

```
sudo mkswap /swapfile
```

5. Enable the swap with the following command:

```
sudo swapon /swapfile
```

6. Enable the swap permanently as root user by editing the `/etc/fstab` file and appending the following line:

```
echo "/swapfile swap swap defaults 0 0" | sudo tee -a /etc/fstab
```

7. Verify that swap is enabled:

```
sudo swapon --show
```

```
Output example:

NAME      TYPE SIZE USED PRIO
/swapfile file 2.5G   0B   -2
```

Formatting Devices for the Installation

The database requires a storage device formatted in ext4 for all nodes. Perform the following procedure on all database nodes to setup ext4 in devices.

> The steps below are required to be performed on all AWS EC2 instances that are created. For more information about creating instances, see Formatting Devices for the Installation

Format the device type applicable to the AWS EC2 type you are using in the instance, either an instance Store type or EBS type:

- Formatting Instance Store Type Devices
- Formatting EBS Type Devices

Formatting Instance Store Type Devices

The steps below are required to be performed on all AWS EC2 instances that are created.

> ONLY perform this procedure if you are using **Instance Store** type devices.

1. From the bastion, login to the database node using SSH and the key pair selected during launching.
   For example:

```
ssh -i <FilePath to the ec2 keypair/IdentityFile> root@<node1..n>
```

2. Install the `nvme` tool:

```
sudo dnf install -y nvme-cli
```

3. Create an `/opt mount` point. If `/opt` already exists, skip this step.

```
sudo mkdir /opt/vertica
```

4. Use the `nvme` tool to locate the `nvme` device and format it:

```
EPHEMERAL_DISK=$(sudo nvme list | grep 'Amazon EC2 NVMe Instance Storage'
| awk 'NR==1{ print $1 }')
```

```
echo $EPHEMERAL_DISK
```

```
sudo mkfs.ext4 $EPHEMERAL_DISK
```

```
sudo mount -t ext4 $EPHEMERAL_DISK /opt
```

5. Add the ephemeral disk mount to `/etc/fstab`:

```
echo "$EPHEMERAL_DISK /opt ext4 defaults,nofail 0 0" | sudo tee -a
/etc/fstab
```

6. To list the mount points for verification, run the `lsblk` command:

```
lsblk
```

Formatting EBS Type Devices

The steps below are required to be performed on all AWS EC2 instances that are created. These steps for EBS also assume you are formatting a single device. For more information about creating instances, see Formatting Devices for the Installation.

ONLY perform this procedure if you are using **EBS** type devices.

1. Run the following command to locate the EBS device attached to the instance, and to select the device that is not mounted:

```
lsblk -f
```

```
#Output from lsblk -f
NAME FSTYPE LABEL UUID MOUNTPOINT
xvda
└─xvda1 xfs 35761952-413c-42e8-b047-a5deb7510f29 /
xvdb
```

2. Run the following command to format the device to ext4:

```
sudo mkfs.ext4 /dev/xvdb
```

NOTE: `xvdb` is an example and will be <yourDeviceName> from the output in the previous step.

3. Format the device:

```
sudo mount -t ext4 /dev/xvdb /opt
```

4. Create the mount point. If `/opt` already exists, skip this step.

```
sudo mkdir /opt/vertica
```

5. Modify the `/etc/fstab` file, and add an entry to mount the device on OS boot:

```
echo "/dev/xvdb /opt ext4 defaults 0 0" | sudo tee -a /etc/fstab
```

Persisting Operating System Settings

The database requires that you manually configure several general operating system settings. Perform the following procedures on all database nodes to setup ext4 in devices.

1. Run this command to set the limit for open files so that it meets database requirements. This will add the parameters to the `/etc/sysctl.conf` file.

```
cat << EOF | sudo tee -a /etc/sysctl.conf
net.core.somaxconn = 1024
net.core.wmem_max = 16777216
net.core.rmem_max = 16777216
net.core.wmem_default = 262144
net.core.rmem_default = 262144
net.core.netdev_max_backlog = 100000
net.ipv4.tcp_mem = 16777216 16777216 16777216
net.ipv4.tcp_wmem = 8192 262144 8388608
net.ipv4.tcp_rmem = 8192 262144 8388608
net.ipv4.udp_mem = 16777216 16777216 16777216
net.ipv4.udp_rmem_min = 16384
net.ipv4.udp_wmem_min = 16384
vm.swappiness = 0
EOF
```

Where:

Parameter	Description
`net.core.somaxconn = 1024`	Increases the number of incoming connections
`net.core.wmem_max = 16777216`	Sets the send socket buffer maximum size in bytes
`net.core.rmem_max = 16777216`	Sets the receive socket buffer maximum size in bytes
`net.core.wmem_default = 262144`	Sets the receive socket buffer default size in bytes
`net.core.rmem_default = 262144`	Controls the default size of receive buffers used by sockets

`net.core.netdev_max_backlog = 100000`	Increase the length of the network interface input queue
`net.ipv4.tcp_mem = 16777216 16777216 16777216`	
`net.ipv4.tcp_wmem = 8192 262144 8388608`	
`net.ipv4.tcp_rmem = 8192 262144 8388608`	
`net.ipv4.udp_mem = 16777216 16777216 16777216`	
`net.ipv4.udp_rmem_min = 16384`	
`net.ipv4.udp_wmem_min = 16384`	
`vm.swappiness = 0`	Defines the amount and frequency at which the kernel copies RAM contents to a swap space For more information, see Check for Swappiness in the ArcSight Database 24.1 Guide.

2. Update the `/etc/rc.local` file by running the commands below. This file contains scripts and commands that run each time the system is booted, and the database requires that I/O Scheduling be set to *deadline* or *noop*. The command will add the applicable lines to the file, based on the devices type in your AWS instance, either **instance Store** type or **EBS** type:

   Instance Store type rc.local settings (only)

```
cat << EOF | sudo tee -a /etc/rc.local
echo deadline > /sys/block/nvme0n1/queue/scheduler
echo deadline > /sys/block/nvme1n1/queue/scheduler
echo deadline > /sys/block/nvme2n1/queue/scheduler
echo deadline > /sys/block/md0p1/queue/scheduler

/sbin/blockdev --setra 2048 /dev/nvme0n1
/sbin/blockdev --setra 2048 /dev/nvme1n1
/sbin/blockdev --setra 2048 /dev/nvme2n1
/sbin/blockdev --setra 2048 /dev/md0p1

if test -f /sys/kernel/mm/transparent_hugepage/enabled; then
echo never > /sys/kernel/mm/transparent_hugepage/enabled
fi

if test -f /sys/kernel/mm/transparent_hugepage/defrag; then
echo never > /sys/kernel/mm/transparent_hugepage/defrag
fi
EOF
```

> **Note:** Replace the device in the example command above with your own instance device on which the `/opt` is mounted. For example, the following device must be replaced with your own device: `sys/block/nvmen0n1`

EBS type rc.local settings (only)

```
cat << EOF | sudo tee -a /etc/rc.local
echo deadline > /sys/block/xvda/queue/scheduler
echo deadline > /sys/block/xvdb/queue/scheduler
echo deadline > /sys/block/xvdc/queue/scheduler

/sbin/blockdev --setra 2048 /dev/xvda
/sbin/blockdev --setra 2048 /dev/xvdb
/sbin/blockdev --setra 2048 /dev/xvdc

if test -f /sys/kernel/mm/transparent_hugepage/enabled; then
echo never > /sys/kernel/mm/transparent_hugepage/enabled
fi

if test -f /sys/kernel/mm/transparent_hugepage/defrag; then
echo never > /sys/kernel/mm/transparent_hugepage/defrag
fi
EOF
```

> **Note:** Replace the device in the example command above with your own instance device on which the `/opt` is mounted. For example, the following device must be replaced with your own instance device:
>
> `sys/block/dev/xvdb`

3. Modify the file permissions:

```
sudo chmod +x /etc/rc.d/rc.local
```

4. If a firewall is enabled, open the ports for all the database nodes using the following commands:

```
sudo firewall-cmd --permanent --zone=public --add-port=<port_number>/<tcp
or ucp>
```

```
sudo firewall-cmd --reload
```

> During installation, the Database requires that host-based firewalls are disabled on database nodes. After installation, the host-based firewalls can be enabled and the database requires several ports to be open on the local network. We recommend for optimal performance using host-based firewalls between database nodes and a network-based firewall to protect the segment that database cluster is within. However, there is no restriction against using a network-based firewall between database nodes. When using any kind of firewall, ensure that all the database ports are available (see Technical Requirements for ArcSight Platform 24.2). For more information, see Firewall Considerations in the *ArcSight Database Guide*

5. Set SELinux to permissive mode in `/etc/selinux/config`.

   ```
   SELINUX=permissive
   ```

   For more information, see ArcSight Database 24.1 Guide.

6. Run this command to ensure that `rng-tools` packages are installed in all cluster nodes:

   ```
   sudo dnf install rng-tools -y
   ```

7. Set the UTC time for all cluster nodes:

   ```
   sudo timedatectl set-timezone UTC
   ```

8. Reboot the system for your changes to take effect.

   > This step is required to update the device mounts and other settings.

Enabling Root Login for AWS Passwordless Communication

This section describes how to configure passwordless communication from the node1 server to all of the node servers in the cluster. You can perform this procedure as a root or the sudo (non-root) user.

> You must repeat the authentication process for all nodes in the cluster.

> All commands require root privileges which can be obtained through the sudo command.

1. Connect to one of your nodes and edit the `/etc/ssh/sshd_config` configuration file:

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   Change the following parameters to **yes** if the values are not already set to that:

   ```
   PermitRootLogin yes
   ```

```
PasswordAuthentication yes
```

If you had to update any of the parameters above, run this command:

```
sudo service sshd reload
```

Otherwise, you may proceed to the next step.

2. On the node1 server, login as root (or sudo user), run the `ssh-keygen` command:

```
ssh-keygen -q -t rsa
```

3. Copy the key from node1 to all of the nodes, including node1, using the node IP address: For a root installation of the database:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub root@<node_IP_address>
```

For a non-root installation of the database:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub <non_root_user>@<node_IP_address>
```

Examples:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub root@11.111.111.111
```

```
ssh-copy-id -i ~/.ssh/id_rsa.pub <non_root_user>@11.111.111.111
```

> Execute the command above once for **each database node** (including node1), replacing *<node_IP_address>* with each corresponding database node IP

The system displays the key fingerprint and requests to authenticate with the node server.

4. Specify the required credentials for the node.
5. The operation is successful when the system displays the following message:

```
Number of key(s) added: 1
```

6. To verify successful key installation, run the following command from node1 to the target node to verify that node1 can successfully log in:

```
ssh <node_IP_address>
```

> Replace the *<node_IP_address>* variable with IP value before you run the command.

Setting Up and Installing the Database for AWS

The procedures in this section will finish the setup and installation process.

Modifying the System Clock

A network time server must be available. `chrony` implements this protocol and is installed by default on some versions of RHEL. `chrony` must be installed on every node.

Verify the `chrony` configuration by using the command:

```
chronyc tracking
```

To install `chrony`, start the `chrony` daemon, then verify operation with these commands:

```
yum install chrony -y
systemctl start chronyd
systemctl enable chronyd
chronyc tracking
```

After modifying the system clock, you must reboot each node.

Installing and Configuring the Database Server

This section describes how to configure and install the AWS database.

Before installing the database, ensure that you estimate the storage needed for the incoming EPS (event per second) and event size, and also evaluate the retention policy accordingly. You also must create an IAM role prior to installing the database. For information about creating an IAM Role, see Installing the Database in AWS .

- "Installing Database" below
- "Creating the Database Server Key and Certificate" on page 184
- "Setting up the Database SSL Configuration" on page 185

Installing Database

Perform the following steps as root user:

1. On all Database nodes, create a folder for the database installer.
   For example:

```
sudo mkdir -p /opt/arcsight-db-tools
```

```
<If non-root user is executing commands only>: chown <non-root user>
/opt/arcsight-db-tools
```

```
sudo cd /opt/arcsight-db-tools
```

   `/opt/arcsight-db-tools` should not be under `/root` or `/opt/vertica`.

2. Download `arcsight-platform-cloud-installer-xx.x.x.zip` and unzip. The directory to where you unzip it will be referred to as {`Unzipped-arcsight-platform-cloud-installer-folder`}.
3. Copy the Database binaries from {`Unzipped-arcsight-platform-cloud-installer-folder/database`} to your Database cluster node1 server, at the `/opt/arcsight-db-tools` directory.
4. Extract the database binaries with the following command:

```
tar xvfz db-installer_x.x.x.x.tar.gz
```

5. Edit the `config/db_user.properties` file and add all database node IPs to the hosts property.

Property	Description
`hosts`	A comma separated list of the database servers in IPv4 format (for example, 1.1.1.1,1.1.1.2,1.1.1.3). If it is necessary to construct the cluster, avoid using local loopback (localhost, 127.0.0.1, etc.).

6. If this is an all-in-one deployment (all nodes deployed to a single host), run the following commands:

```
export DATABASE_NODES=$(hostname)
export KAFKA_NODE=${DATABASE_NODES}
```

7. Install the database using the following command:

When installing as a sudo user, do not prefix sudo to any of the `db_installer` commands.

Please make sure you have performed the steps detailed in "Installing the Database in AWS " on page 169 before attempting the installation command.

```
./db_installer install
```

```
*****************************************************
License file not found. Community license will be used.
Would you like to continue? (y/n)?
---------------------------------------
```

Entering Y will take you straight to the next screen, no need to hit `Enter`.

8. When prompted, create the **database administrator** user.

   The database administrator user account is used during database deployment, configuration, upgrade, and debugging. For security reasons, the platform deployed capabilities will not ask you for the credentials for this user.

   ```
   ---------------------------------------
   Please specify a username for [ DB Admin ] user:
   dbadmin

   ---------------------------------------
   Please specify a password for [ DB Admin ] user:
   ********
   Re-enter password:
   ********
   ```

   For a list of options that you can specify when installing the database, see Understanding the Database Installer Options.

9. Specify the shard count. The default shard count is:

   - One for single node environments
   - Twice the number of database nodes for multi-node environments (to allow for scalability)

   The prompt options are based on your environment, single-node or multi-node:

   - Single-node:

     ```
     # ========================================
     # STEP 1: Specify Database Shard Count for Eon Mode
     Data in communal storage is broken into segments called shards. Number
     of shards in the system should always be an even divisor of the number
     of nodes in your database.
     For the best performance, the number of shards you choose should be no
     greater than 2× the number of nodes. At most, you should limit the
     shard-to-node ratio to no greater than 3:1.
     For smaller databases 1:1 ratio can be used. You can re-shard the
     ```

```
database in future if you add or remove nodes to accommodate new
workload.

Use Shard Count [1]:
Confirm shard count [1]?(y/n):y
Check memory size, 48GB required for single node installation with
shard count > 1.
PASS: Single node installation for shard count: 1
```

- Multi-node (with a 3 database node environment):

```
# ========================================
# STEP 1: Specify Database Shard Count for Eon Mode
Data in communal storage is broken into segments called shards. Number
of shards in the system should always be an even divisor of the number
of nodes in your database.
For the best performance, the number of shards you choose should be no
greater than 2× the number of nodes. At most, you should limit the
shard-to-node ratio to no greater than 3:1.
For smaller databases 1:1 ratio can be used. You can re-shard the
database in future if you add or remove nodes to accommodate new
workload.

Use shard Count [1]:6
Confirm shard count [6]?(y/n):y
```

10. Set up the communal storage type for S3 when prompted. For example:

```
# ========================================
# STEP 2: Specify communal storage details
Supported communal storage types -
1) S3
2) Azure Blob Storage
3) Google Cloud Storage

Choose a communal storage type from the above (1-3):1
Are you using IAM role authentication for AWS S3 Storage?(y/n):y
Specify S3 bucket for communal storage:<yourS3BucketName>
Specify the folder under bucket for communal storage if
applicable:<newFolderNametoCreate>
Communal storage url is: <s3://<yourS3BucketName> /newFolderNametoCreate>


Check S3 storage write access
```

```
Test writing to S3 storage succeeded.

Starting Database installation...
# ========================================
```

11. Create the schema.

```
./db_installer create-schema
```

12. When prompted, create the following users:
    - **App admin user:** A regular database user granted elevated permissions for performing operations on the database to manage the database, schema, and resource pools. The credentials for this user will need to be provided later in the OMT Management Portal when you are deploying capabilities.
    - **Search user:** A regular database user with permissions restricted to event search operations. The credentials for this user will need to be provided later in the OMT Management Portal when you are deploying capabilities.

Creating the Database Server Key and Certificate

Follow these steps to generate database CAs and certificates:

1. Log in to database node1.
2. Change to your own certificates directory path:

```
cd <yourOwnCertPath>
```

> For deployment with `arcsight-platform-instsaller`, the default location is `/opt/arcsight-db-tools/cert/`. For a manual deployment the <yourOwnCertPath> directory must be created manually. Example : `mkdir -p /opt/arcsight-db-tools/cert`

(not specified)

3. Run this command to create a certificate authority (CA) for the database:

```
openssl req -newkey rsa:4096 -sha256 -keyform PEM -keyout generated-db-
ca.key -x509 -days 3650 -outform PEM -out generated-db-ca.crt -subj
"/C=US/ST=State/L=City/O=Company
Inc./OU=IT/CN=Database/emailAddress=admin@opentext.com" -nodes
```

4. Run this command to create the database server key:

```
openssl genrsa -out generated-db-server.key 4096
```

5. Create the database server certificate signing request by running the following command:

```
openssl req -new -key generated-db-server.key -out generated-db-
server.csr -subj "/C=US/ST=State/L=City/O=Company
Inc./OU=IT/CN=DatabaseServer/emailAddress=admin@opentext.com" -nodes -
sha256
```

6. Sign the Certificate Signing Request with self-signed CA by running the following command:

```
openssl x509 -req -in generated-db-server.csr -CA generated-db-ca.crt -
CAkey generated-db-ca.key -CAcreateserial -extensions server -days 3650 -
outform PEM -out generated-db-server.crt -sha256
```

Setting up the Database SSL Configuration

These steps will update the SSL configuration in the database.

1. Move the following files to database node1 <*yourOwnCertPath*> as root by running these commands:

   > This step is only required for a new database installation. You can skip this step if this is an upgrade and the files are already there.

   ```
   cd <yourOwnCertPath>/
   ls <yourOwnCertPath>/
   ```

   - The output should have the following files:
     - `generated-db-ca.crt`
     - `generated-db-server.crt`
     - `generated-db-server.key`
     - `generated-db-ca.key`
     - `generated-db-ca.srl`
     - `generated-db-server.csr`

2. Run the following commands on database node1 to update the database SSL configuration:

   ```
   cd /opt/arcsight-db-tools
   ```

   ```
   ./db_ssl_setup --disable-ssl
   ```

If the attempt fails, drop the certificate manually by running the three commands below:

```
sudo su - dbadmin
```

```
vsql -U <dbadminuser> -w <dbadminpassword> -c "ALTER TLS CONFIGURATION
server CERTIFICATE NULL;"
```

```
vsql -U <dbadminuser> -w <dbadminpassword> -c "DROP CERTIFICATE IF EXISTS
server CASCADE;"
```

3. Enable Database SSL by running the command:

```
./db_ssl_setup --enable-ssl --vertica-cert-path
<yourOwnCertPath>/generated-db-server.crt --vertica-key-path
<yourOwnCertPath>/generated-db-server.key --vertica-ca-path
<yourOwnCertPath>/generated-db-ca.crt
```

Next Step - Monitor your database cluster constantly.
For more information, see Monitoring the Database and **Database Cluster Node Status** in the *User guide for ArcSight Platform 24.2*.

- **Database nodes status:** Ensures all nodes are up
- **Database nodes storage status:** Ensures storage is sufficient

Note: If you have a Recon license, the default retention period for Default Storage Group events is 12 months. You can modify this value based on your data storage policy. If you do not have a Recon license, the retention period for the Default Storage Group is one month.

Next Step - If your deployment includes Intelligence: "(Conditional – Intelligence) Configuring Settings for Elasticsearch in AWS" on page 188

Next Step - If your deployment does not include Intelligence: "Bootstrapping OMT" on page 189

- **Database nodes status:** Ensures all nodes are up
- **Database nodes storage status:** Ensures storage is sufficient

Enabling FIPS Mode on the Database Server

This step is needed only if your environment requires FIPS.

To enable the FIPS mode for the ArcSight database, you must configure the operating system to FIPS mode.

Note: Some of the following steps are performed in a single node (ArcSight**Database** node1), while some are performed in all nodes. For clarity, when not specified, the step must be executed only on ArcSight**Database** node1.

If you're performing an upgrade, you can perform the procedure below starting from step 1. If you're performing a fresh install, please proceed to step 5 of the procedure.

1. Log in to ArcSight Database node1.
2. Navigate to the `/opt/arcsight-db-tools` directory.
3. Stop data ingestion:

   ```
   ./kafka_scheduler stop
   ```

4. Stop the database:

   ```
   ./db_installer stop-db
   ```

5. Run the following commands (**to be performed in all nodes**):

   ```
   fips-mode-setup --enable
   ```

   ```
   reboot
   ```

6. To verify whether FIPS mode is enabled on the server, run the following command (**to be performed in all nodes**):

   ```
   /usr/bin/fips-mode-setup --check
   ```

   In case the above command fails, you can verify with these alternative commands:

   ```
   sysctl crypto.fips_enabled
   ```

   ```
   cat /proc/sys/crypto/fips_enabled
   ```

7. Run the following command (**to be performed in all nodes**):

   ```
   rm /opt/vertica/lib/libcrypto.* /opt/vertica/lib/libssl.*
   ```

   This command in the database nodes will generate a verification prompt for the deletion of each folder. Enter a "y" to agree, and then hit enter.

8. Verify that the Zulu8 RPM package is installed using the following command.

```
rpm -qa | grep zulu
```

The command will return an empty message if Zulu8 is not installed, but will return the filename of the Zulu8 package if installed. If Zulu8 is already installed, skip to Step 11.

9. (Conditional) If Step 8 returns an empty message, then determine the latest Zulu8 package on the Azul web site (www.azul.com) for Java8 and your OS. Download the file using this command:

```
wget <Zulu8 download URL>
```

10. (Conditional) Install the Zulu8 file that you downloaded by running the following command on each node:

```
rpm --nodigest --nofiledigest -i <Zulu8 filename>
```

11. Restart the ArcSight database:

```
./db_installer start-db
```

12. Restart data ingestion:

```
./kafka_scheduler start
```

Disabling FIPS Mode

To disable FIPS mode, run the following commands on each ArcSight database node.

```
fips-mode-setup --disable
reboot
```

(Conditional – Intelligence) Configuring Settings for Elasticsearch in AWS

Once the new nodes are available their values must be updated following these steps, which must be performed in each of the EKS nodes:

1. Run the following command to check the `vm.max_map_count` in your `/etc/sysctl.conf`:

```
sudo sysctl -a | grep vm.max_map_count
```

2. If your `vm.max_map_count` is less than 262144, run the following commands to set the new value. (If the value equals or exceeds 262144 already, then skip this step.)

```
cat << EOF | sudo tee -a /etc/sysctl.conf
vm.max_map_count = 262144
EOF
```

```
sudo sysctl -p
```

Make sure these steps have been performed in all EKS nodes before proceeding further.

Bootstrapping OMT

Bootstrapping OMT is a method of installing a few basic pods onto the Kubernetes cluster created previously (when you configured EKS and worker nodes).

During this process, the OMT bootstrap script does the following:

- Downloads Docker images from the ECR (Elastic Container Registry).
- Instantiates pods for various checks like the EFS space and the structure created on it.
- Creates `nginx` pods for use as a load balancer, and for allowing connections to the web installation process.

After the OMT bootstrap process completes, you will need to import the intermediate certificate to the OMT, configure some required networking settings, then continue installation using the OMT web installation interface.

Note: If you used a non-root user to install Kubernetes, you must use the same non-root user to install OMT as well. In addition, the non-root user installation process will prompt for additional steps.

- Preparing the OMT Deployer
- "Retrieving the ECR Credentials" on the next page

Preparing the OMT Deployer

The EKS and worker nodes you have configured are completely isolated from access from the internet, each of the nodes can access it if needed. As a result, the process of bootstrapping OMT must be performed from the bastion.

You have already copied the package `arcsight-platform-cloud-installer-<version>.zip` to the bastion and unpacked it during configuration of EFS. As a part of this package, the `cdf-deployer.zip` is included.

To prepare the OMT deployer:

Unpack the `cdf-deployer.zip` archive by running the following command:

```
unzip ./arcsight-platform-cloud-installer-<version>/cdf-deployer.zip
```

This will create the directory `arcsight-platform-cloud-installer-<version>/cdf-deployer`.

Retrieving the ECR Credentials

OMT needs the credentials to access the ECR in order to be able to download images.

To retrieve the ECR credentials:

1. On the bastion, run the command:

   ```
   ./arcsight-platform-cloud-installer-<version>/aws-scripts/scripts/upload_images_to_ECR --get-ecr-credentials
   ```

2. The file `ecr_credentials` is created in the directory where the script was run, containing username, password, and ECR URL.
3. Run the following command:

   ```
   source ecr_credentials
   ```

> The password retrieved here is valid for only 12 hours after creation.

To bootstrap OMT:

Change the working folder to `cdf-deployer` and run the following command:

```
./install \
--k8s-provider aws \
--external-access-host <RecordSet name> \
--nfs-server <Filesystem FQDN> \
--nfs-folder <OMT ITOM volume> \
--registry-url $ECR_URL \
--registry-username $ECR_USER_NAME \
--registry-password $ECR_USER_PASSWORD \
--registry-orgname <orgname> \
-P <suite admin password>
```

Where:

Variables **$ECR_URL, $ECR_USER_NAME,** and **$ECR_USER_PASSWORD** come from the `ecr_credentials` file which you sourced previously.

`<suite admin password>`: Choose a password between 8 to 20 characters in length. A password must include numbers, lowercase chars, uppercase chars and special characters. Exclude whitespace characters, such as space, newline, and so on.

`<orgname>` : Use the same value as for upload images; check the AWS worksheet for this value.

`<Filesystem FQDN>`: Use the value from the AWS worksheet.

`<OMT ITOM volume>`: The directory on NFS/EFS into which OMT starts the installation. The path is a combination of the parent directory as specified in your AWS worksheet as **Parent Folder Name**, plus the predefined subfolder name. For example, `/srgdemo/itom-vol`.

`<RecordSet name>` : The A-record (FQDN) used for connecting to the OMT installation and management portal. Use the value from the AWS worksheet.

Note: Ensure that you remove the trailing period from the FQDN.

Example:

```
./install --registry-url $ECR_URL \
--registry-username $ECR_USER_NAME \
--registry-password $ECR_USER_PASSWORD \
-P "Password@123" \
--registry-orgname srgdemo \
--nfs-server fs-ebe456b3.efs.eu-central-1.amazonaws.com \
--nfs-folder /srgdemo/itom-vol \
--k8s-provider aws \
--external-access-host srgdemo.arcsight-dev.com
```

After the OMT bootstrap completes, you are prompted to log in at the following URL: `https://<external access host>:3000`

However, you will not be able to log in successfully yet, as there are some network infrastructure resources still to prepare, as explained in the succeeding steps.

Securing External Communication with the RE Certificate

At the center of the Platform is a Kubernetes cluster where communication occurs between pods within the cluster and with non-containerized ArcSight components outside of the cluster. In order to ensure secure trusted communication between pods within the cluster and

components outside of the cluster, encrypted communication with client certificate authentication is configured by default.

- Understanding the ArcSight Platform Certificate Authorities
- Using an RE External Communication Certificate Signed by Your Trusted Certificate Authority

Understanding the ArcSight Platform Certificate Authorities

During installation, three self-signed Certificate Authorities (CA) are created automatically, two for signing certificates used exclusively for pod to pod communication within the cluster (RIC and RID CA), and the other for signing certificates for each pod that performs communication external to the cluster (RE CA). Only pods that perform external communication have a certificate that is signed by the external CA.

External cluster communication occurs not only with ArcSight components, but also with user web browsers and, in some cases, user clients of ArcSight APIs (such as the REST API). By default, when the user connects to the cluster, they will be presented with a certificate that has been signed by the self-signed external CA. Since the external CA is self-signed, the user's connection will not automatically trust the certificate because it will not be verifiable using a certificate chain that is already in the user's trust store.

To give users confidence they are connecting to the trusted cluster, we recommend signing the certificates that are presented to the user with a CA that is trusted by the user's trust store. There are two approaches to doing this that are described in the documentation below. These approaches are:

Method 1 - Signing the RE External Communication Certificate with Your Trusted Certificate Authority

This is the recommended approach, because it is theoretically more secure than the other approach, in that it only involves transferring a CSR and public certificate between systems, which does not put any private secrets at risk.

Method 2 - Importing an Externally Created Intermediate CA

This approach involves creating an Intermediate CA (key and certificate pair) in a system outside of the ArcSight Platform, and then importing it into the ArcSight Platform. While this approach does work, it is theoretically less secure than the other approach, because it involves transferring a CA private key between systems, which potentially exposes it to unintended parties.

Use only one of the two approaches above.

Using an RE External Communication Certificate Signed by Your Trusted Certificate Authority

Use only one of the two approaches below. The first one, "Signing the RE External Communication Certificate with Your Trusted Certificate Authority" approach is recommended for the reasons described in Understanding the ArcSight Platform Certificate Authorities.

Method 1 - Signing the RE External Communication Certificate with Your Trusted Certificate Authority

Signing the RE External Communication Certificate with Your Trusted Certificate Authority approach is recommended for the reasons described in Understanding the ArcSight Platform Certificate Authorities.

In order to sign the RE external communication certificate with your trusted CA, you need to (1) create a certificate signing request (CSR) from vault, (2) take it to your organization, (3) sign it, and (4) return the signed CSR and all the public chain-of-certificates used to sign it.

1. Export the following access token dependencies (you can remove these later if not needed):

```
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o json
2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n core
-o json 2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-cbc -
md sha256 -a -d -pass pass:"${PASSPHRASE}")
```

2. Delete the existing vault secrets by running the following command:

```
kubectl exec -it -n core ${VAULT_POD} -- bash -c "VAULT_TOKEN=$VAULT_
TOKEN vault secrets disable -tls-skip-verify RE" && kubectl exec -it -n
core ${VAULT_POD} -- bash -c "VAULT_TOKEN=$VAULT_TOKEN vault secrets
enable -tls-skip-verify -max-lease-ttl=87600h -path=RE pki"
```

3. Ask vault to generate the CSR by running the following command:

> **Important:** When you execute this command, proceed expeditiously through steps 3 and 4, as your cluster will not be able to issue external certificates while it waits for the CSR to be signed.

```
kubectl exec -it -n core ${VAULT_POD} -c vault -- bash -c "VAULT_
TOKEN=$VAULT_TOKEN vault write -tls-skip-verify -format=json
RE/intermediate/generate/internal common_name=\"none-MF CDF RE CA on
<FQDN of ArcSight Platform Virtual IP for HA or single master node>\"
country=<Country> locality=<Locality> province=<Province>
organization=<Organization> ou=<Organizational Unit>" | jq -r '.data.csr'
> /tmp/pki_intermediate.csr
```

Note: The `common_name` in the command above is an example common name. Substitute your own values for the common name to fit your environment. Additionally, your trusted certificate authority might require additional parameters in the CSR besides `common_name`. Ask your PKI team for what the required CSR parameters are and add the appropriate parameters to the command (similar to how the parameter common_name is specified). The parameter names for the vault command used above are documented at https://www.vaultproject.io/api-docs/secret/pki#generate-intermediate

4. Sign the CSR file with your trusted certificate authority, and save the result into the `intermediate.cert.pem` file.

   Example only. A basic example is provided below. Your environment will likely be different.

```
openssl ca -keyfile your-rootca-sha256.key -cert your-rootca-sha256.crt -
config your-openssl-configuration-file -extensions v3_ca -notext -md
sha256 -in /tmp/pki_intermediate.csr -out intermediate.cert.pem
```

   Make sure the `v3_ca` and `authorityKeyIdentifier` extensions are enabled and a new certificate is useable as a certificate authority on its own. Otherwise, you will receive a warning in the next step that given certificates are not marked for CA use.

5. Create an `intermediate.chain.pem` file that includes the combination of the `intermediate.cert.pem`, the public certificate of your trusted certificate authority, and all intermediate public certificates in the chain between them so that `intermediate.chain.pem` includes the full trust chain.

```
cp intermediate.cert.pem intermediate.chain.pem
cat [parent-intermediate1.crt] [parent-intermediate2.crt] [...] your-
rootca-sha256.crt >> intermediate.chain.pem
```

   If you have intermediate certificates between your `intermediate.cert.pem` and your trusted certificate authority, you must add the certificates in the specific order of the sequence of the chain, with the last certificate being the certificate of the root trusted CA.

6. Import the `intermediate.chain.pem` file into the cluster vault:

```
chaincerts=$(cat intermediate.chain.pem) && kubectl exec -it -n core
${VAULT_POD} -c vault -- bash -c "VAULT_TOKEN=$VAULT_TOKEN vault write -
tls-skip-verify -format=json RE/intermediate/set-signed
certificate=\"${chaincerts}\""
```

Re-create the vault coretech role by running the following command:

```
kubectl exec -it -n core ${VAULT_POD} -- bash -c "VAULT_TOKEN=${VAULT_
TOKEN} vault write -format=json -tls-skip-verify RE/roles/coretech allow_
any_name=true allow_ip_sans=true max_ttl=87600h ttl=8760h"
```

7. Update `ConfigMap RE_ca.crt` by running these commands:

```
reCrtForJson=$(sed -E ':a;N;$!ba;s/\r{0,1}\n/\\n/g'
intermediate.chain.pem) && kubectl patch configmap -n core public-ca-
certificates -p "{\"op\": \"replace\", \"data\":{\"RE_
ca.crt\":\"${reCrtForJson}\"}}"
```

```
ARCSIGHT_NS=$(kubectl get namespaces --no-headers -o custom-
columns=":metadata.name" | grep arcsight-installer)
```

```
if [ -n "$ARCSIGHT_NS" ];then reCrtForJson=$(sed -E ':a;N;$!ba;s/\r
{0,1}\n/\\n/g' intermediate.chain.pem); kubectl patch configmap -n
$ARCSIGHT_NS public-ca-certificates -p "{\"op\": \"replace\", \"data\":
{\"RE_ca.crt\":\"${reCrtForJson}\"}}";fi
```

8. (Conditional) If you already deployed ArcSight Capabilities onto the OMT, update the ArcSight Capabilities to use the updated RE external communication certificate, by following the instructions in Configuring ArcSight Kubernetes Pods to Use the Updated RE External Communication Certificate.

   If you deployed OMT but have not yet deployed any ArcSight Capabilities, you can skip those instructions.

Method 2 - Importing an Externally Created Intermediate CA

This is an alternate approach for signing certificates to connect to the trusted cluster. Before choosing this approach, ensure that you understand the other approach recommended in Understanding the ArcSight Platform Certificate Authorities.

1. Obtain an intermediate CA (key and certificate pair) from your trusted certificate authority.
   a. Name the certificate files as follows:
      - key file: `intermediate.key.pem`
      - certificate file: `intermediate.cert.pem`
   b. Obtain the root CA certificate (including chain), and put it in a file named ca.cert.pem.
   c. Create an `intermediate.cert.chain.pem` file that includes the combination of the `intermediate.cert.pem`, and the root CA certificate (including chain) `ca.cert.pem`. This way, `intermediate.chain.pem` includes the full trust chain.

      ```
      cat intermediate.cert.pem ca.cert.pem >> intermediate.cert.chain.pem
      ```

2. Replace the existing RE CA in the ArcSight Platform with the intermediate CA you obtained in the step above.
   a. Change the directory:
      - For a cloud deployment, run these commands:

        ```
        cd <path to OMT installer>/cdf-deployer/scripts/
        ```

   b. Run the following command to replace the existing RE CA:

      ```
      ./cdf-updateRE.sh write --re-crt=/pathto/intermediate.cert.chain.pem -
      -re-key=/pathto/intermediate.key.pem
      ```

3. (Conditional) If you already deployed ArcSight Capabilities onto OMT, proceed to the next section to update the ArcSight Capabilities to use the updated RE external communication certificate, Configuring ArcSight Kubernetes Pods to Use the Updated RE External Communication Certificate.

   However, if you have only deployed OMT, but have not deployed ArcSight Capabilities yet, you can skip that section.

Creating and Validating the Route 53 Certificate

A user-provided self-signed or CA-signed certificate is required for creating the Application Load Balancer (ALB). In this section, you will:

- Create a configuration file for the certificate signing request (CSR)
- Sign the CSR
- Create a chained file for import
- Import the self-signed certificate into Amazon Certificate Manager (ACM)

1. Create or update Route 53 certificates:
   a. Run the applicable command on a secure machine to generate the Route 53 certificate:
      - For a current version of SSL, run this command:

```
openssl req -nodes -newkey rsa:2048 -keyout
<your.route53dnsRecordsetName>.key.pem -out
<your.route53dnsRecordsetName>.csr.pem -subj
"/C=US/ST=State/L=City/O=Company
Inc./OU=IT/CN=<your.route53dnsRecordsetName>" -addext
"subjectAltName = DNS:<your.route53dnsRecordsetName>"
```

      - If your operating system does not support `-addext` for SSL, run this command:

```
openssl req -newkey rsa:2048 -sha256 -nodes -keyout
your.route53dnsRecodsetName.key.pem -out
your.route53dnsRecodsetName.csr.pem -subj
"/C=US/ST=CA/L=SU/O=MF/OU=IT/CN=<your.route53dnsRecordsetName>" -
extensions san -config <(echo '[req]'; echo 'distinguished_
name=req';echo 'req_extensions=san';echo '[san]'; echo
'subjectAltName=DNS:your.route53dnsRecodsetName')
```

> `your.route53dnsRecordsetName` is your route53 record set name tracked in your AWS configuration worksheet. This command will create the private key file `<your.route53dnsRecordsetName>.key.pem` and the certificate signing request file `<your.route53dnsRecordsetName>.csr.pem`.

   b. Copy the certificate signing request `<your.route53dnsRecordsetName>.csr.pem` to your bastion or jump host machine.
   c. Run the following commands to sign the certificate signing request using your cluster RE certificate:

```
export COMMON_NAME=<your.route53dnsRecordsetName>
```

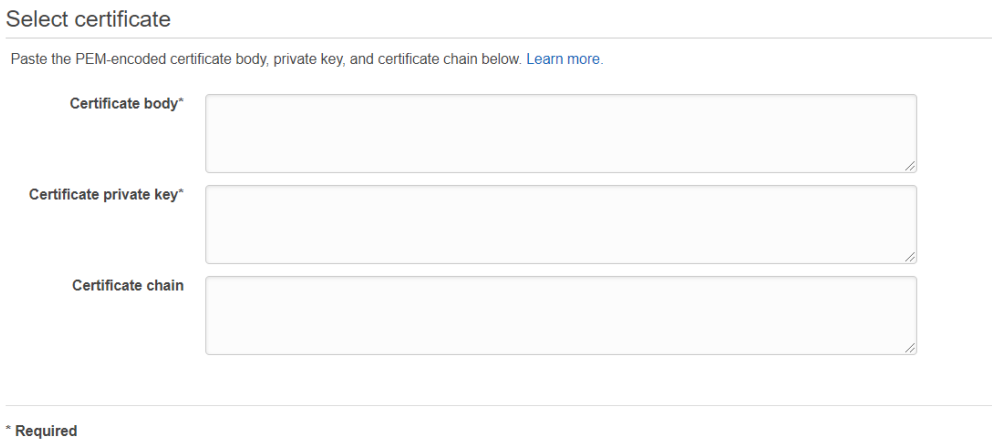
```
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o
json 2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n
core -o json 2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-
cbc -md sha256 -a -d -pass pass:"${PASSPHRASE}")
```

```
export CSR=$(cat ${COMMON_NAME}.csr.pem)
```

```
export WRITE_RESPONSE=$(kubectl exec -it -n core ${VAULT_POD} -c vault
-- bash -c "VAULT_TOKEN=$VAULT_TOKEN vault write -tls-skip-verify -
format=json RE/sign/coretech csr=\"${CSR}\"") && \
echo ${WRITE_RESPONSE} | jq -r ".data | .certificate" > ${COMMON_
NAME}.signed.crt.pem && \
echo ${WRITE_RESPONSE} | jq -r ".data | if .ca_chain then .ca_chain[]
else .issuing_ca end" > ${COMMON_NAME}.ca_chain.pem
```

The RE signed certificate is in file `${COMMON_NAME}.signed.crt.pem`. The certificate chain is in file `${COMMON_NAME}.ca_chain.pem`.

2. Import or update the certificate in Amazon Certificate Manager (ACM).
   a. Import the self-signed certificate into ACM (for a fresh installation):
      i. Log in to the AWS Console.
      ii. Browse to the Amazon Certificate Manager (ACM).
      iii. Click **Import a certificate**, and then complete the fields as follows:
         - **Certificate body:** Specify the contents of the signed certificate you created earlier. For example, `<your.route53dnsRecordsetName>.crt.pem`
         - **Certificate private key:** Specify the contents of the private key created by the CSR request creation. For example, `<your.route53dnsRecordsetName>.key.pem`
         - **Certificate chain:** Specify the contents of the chain file. For example, `<your.route53dnsRecordsetName>.ca.pem`



   b. To update the certificate in ACM (for a current running installation):
      i. Log in to the AWS Console.
      ii. Browse to the Amazon Certificate Manager (ACM).

iii. Search for your certificate Domain name or ID.

iv. Select your Certificate ID, and click **Reimport**.

v. Complete the fields as follows:

- **Certificate body:** Specify the contents of the new signed certificate you created earlier. For example, `<your.route53dnsRecordsetName>.crt.pem`
- **Certificate private key:** Specify the new contents of the private key created by the CSR request creation. For example, `<your.route53dnsRecordsetName>.key.pem`
- **Certificate chain:** Specify the new contents of the chain file. For example, `<your.route53dnsRecordsetName>.ca.pem`

For more details, see https://docs.aws.amazon.com/acm/latest/userguide/import-reimport.html

3. Click **Next**. Optionally, add any tags you wish to the import.
4. Click **Next**, and then, click **Import**.

   After the import, click the arrow next to the certificate ARN value. Note the value to your AWS worksheet for later use. For example:

Imported at	2021-04-01T00:11:48UTC
Not after	2022-04-11T00:06:47UTC
Expires in	374 Days
Public key info	RSA 2048-bit
Signature algorithm	SHA256WITHRSA
ARN	arn:aws:acm:us-west-2:115370848038:certificate/9a03c730-0923-4b2d-8a0d-ea7868917377
Validation state	None

Configuring the Application Load Balancer (ALB)

A load balancer serves as the single point of contact for clients. The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple availability zones. Balancing the load increases the availability of your application. AWS supports several types of load balancers: application, network, and (obsoleted) classic. In this section, you will configure an application load balancer (ALB).

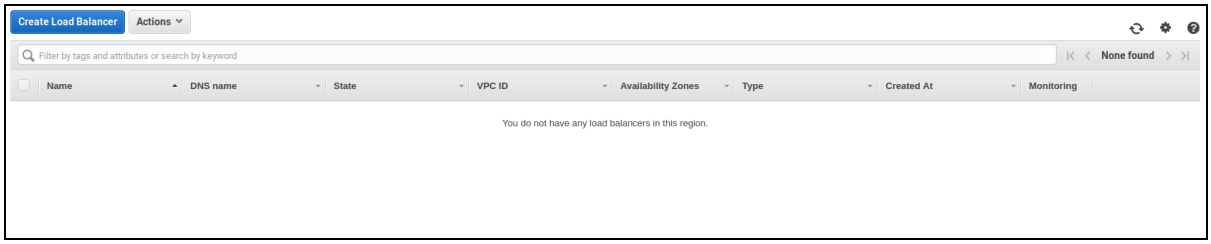
The ALB needs to be configured with locations to balance requests; this is realized by target groups. During the installation process you will create target groups for various ports: 3000 (OMT installation), 5443 (OMT management portal), and 443 (ArcSight Suite configuration).

> Immediately after the core OMT bootstrap, only the installation portal is available on port 3000. The remaining two ports will be configured after the OMT UI installation process is completed.

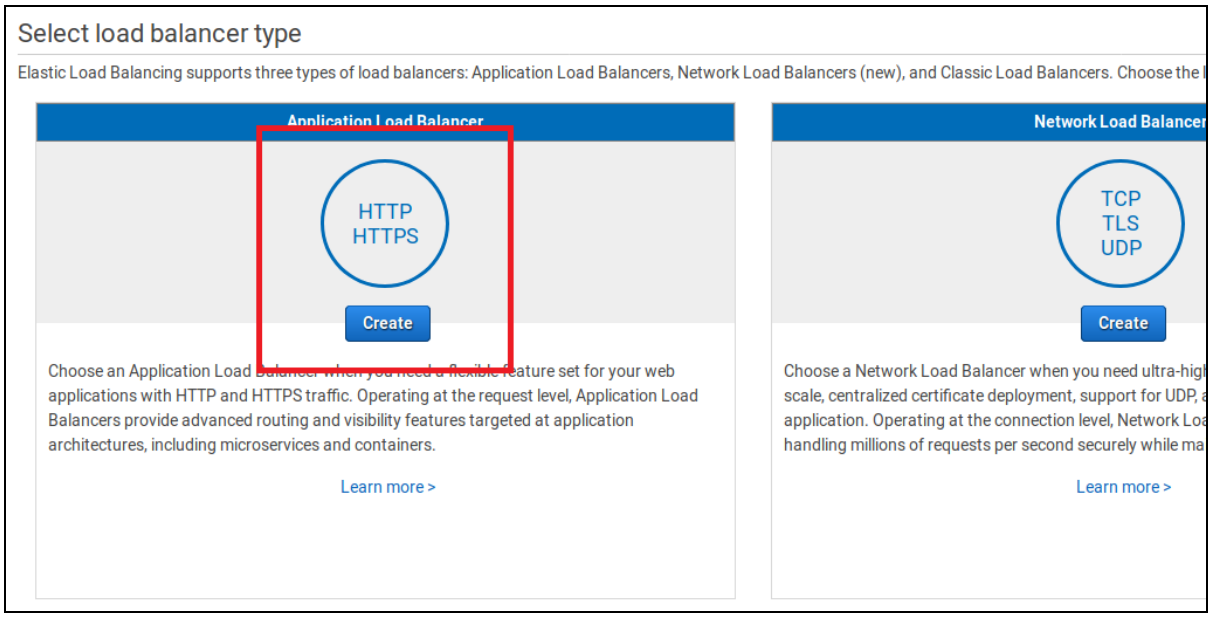
Creating the Application Load Balancer

To create the ALB using the Web UI:

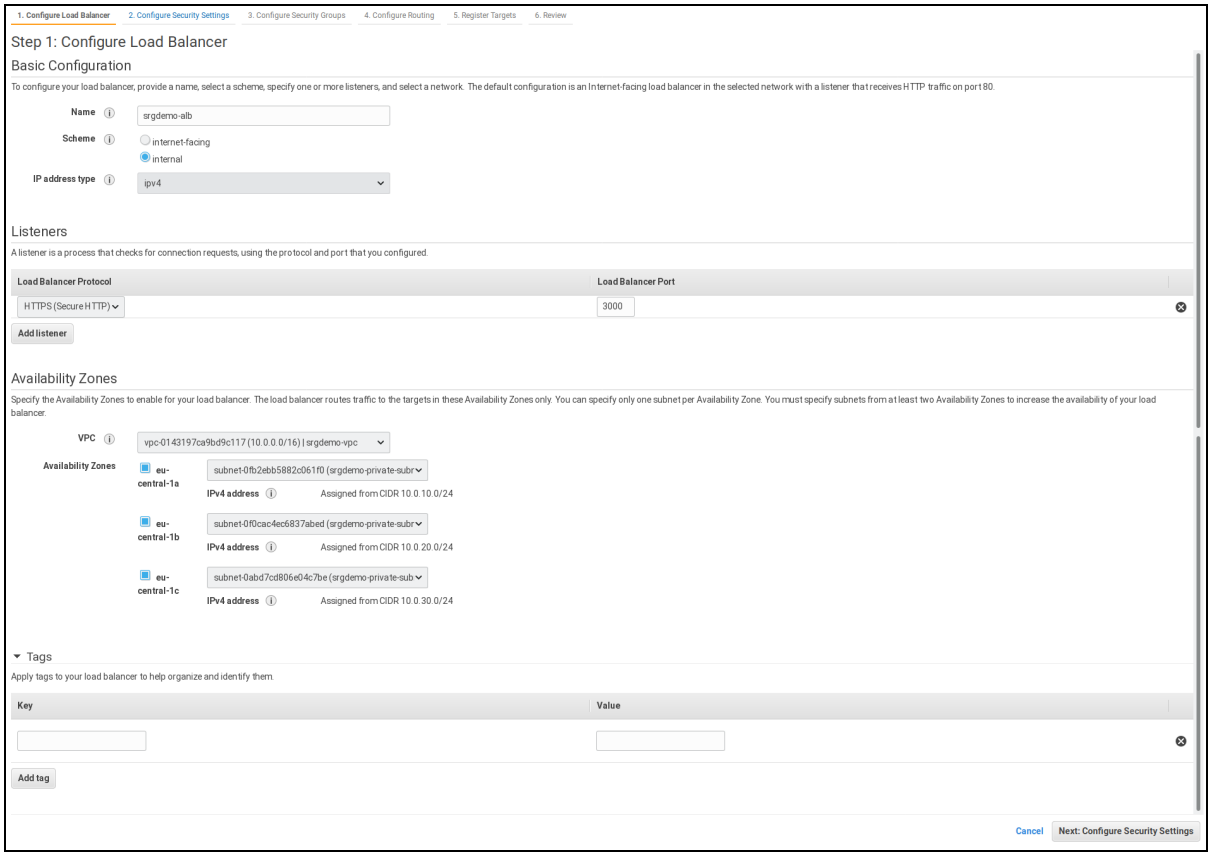
1. Using the Find Services search tool, locate and browse to the EC2 dashboard.
2. In the left navigation panel, under **Load Balancing**, select **Load Balancers.**



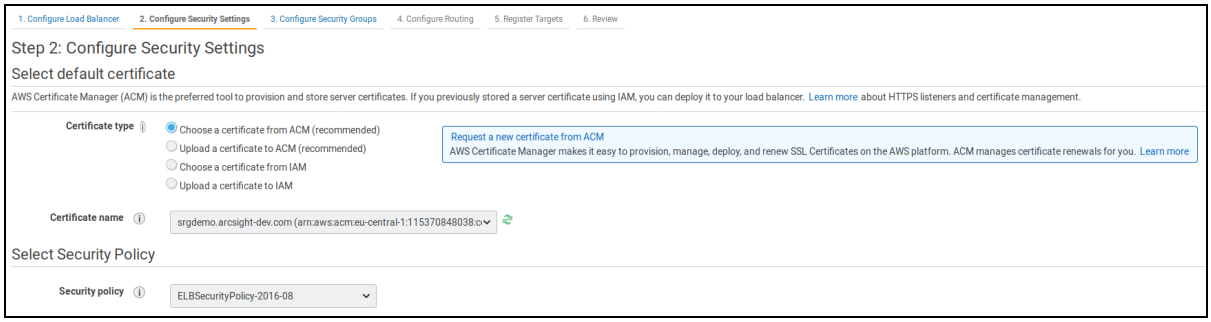
3. On the **Load Balancing** management page, click **Create Load Balancer.**



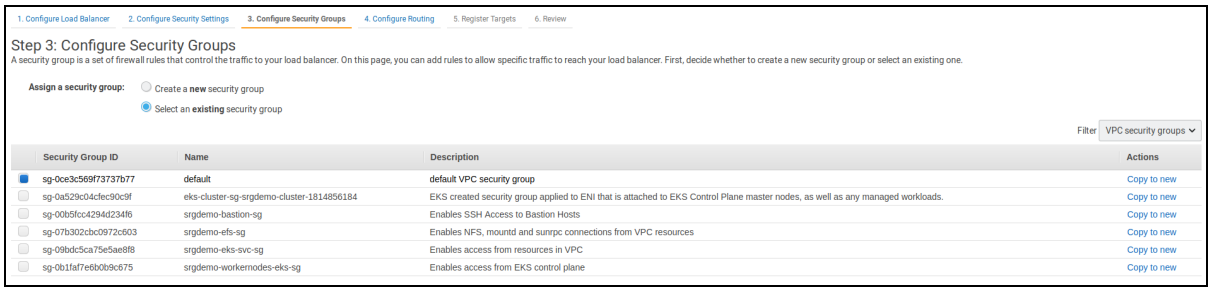
4. In the **Application Load Balancer** panel to the left, click **Create**.



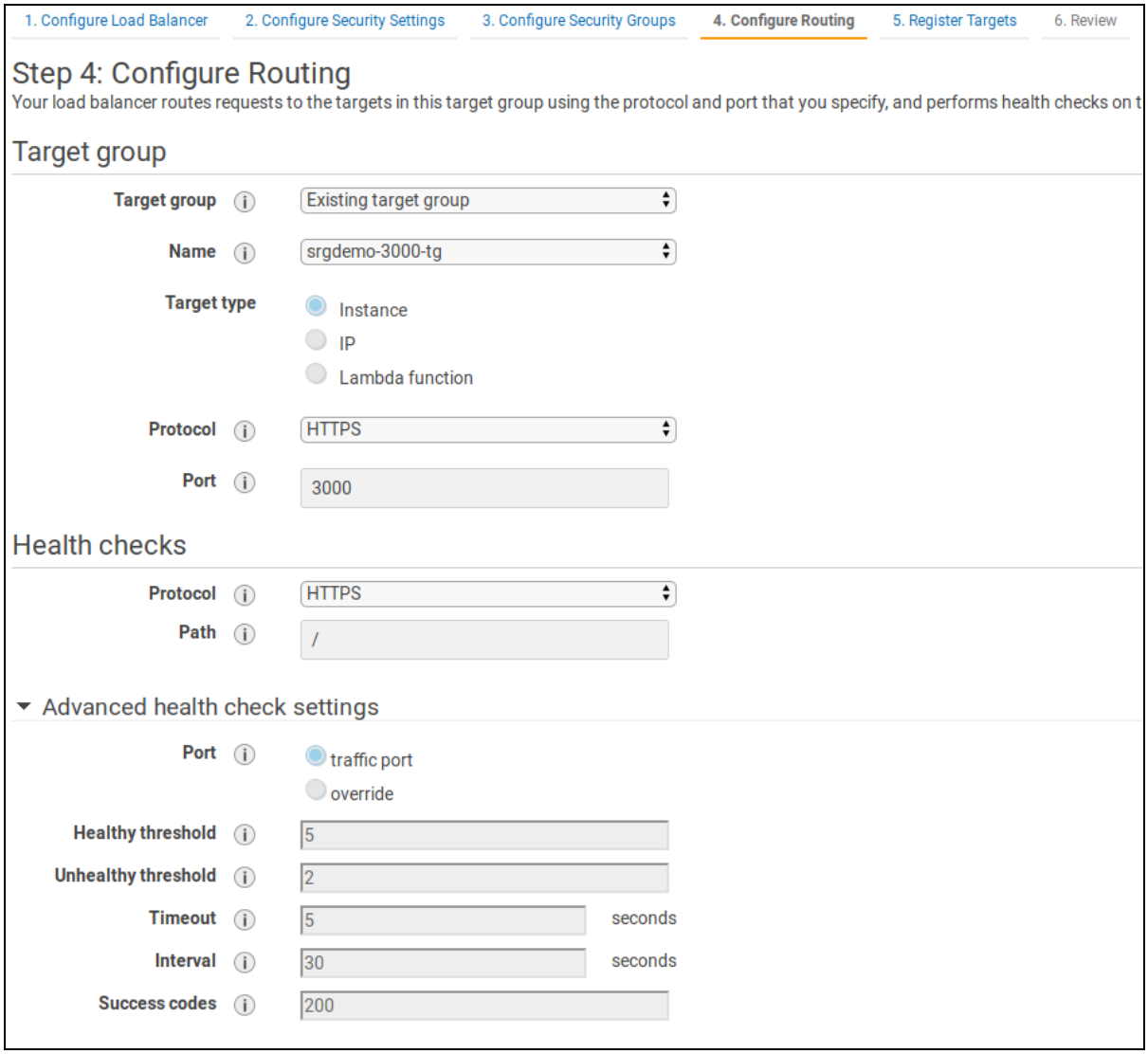
5. On the **Configure Load Balancer** page, enter values for the following:
   a. **Name:** Choose an ALB name
   b. **Scheme:** Internal
   c. **Protocol:** HTTPS
   d. **Port:**3000
   e. **VPC:** Choose your VPC
   f. **Availability Zones:** Check all three zones, then in each, select corresponding private subnet.
   g. **Tags:** Optionally, enter any tags desired.
6. Click **Next: Configure Security Settings**.



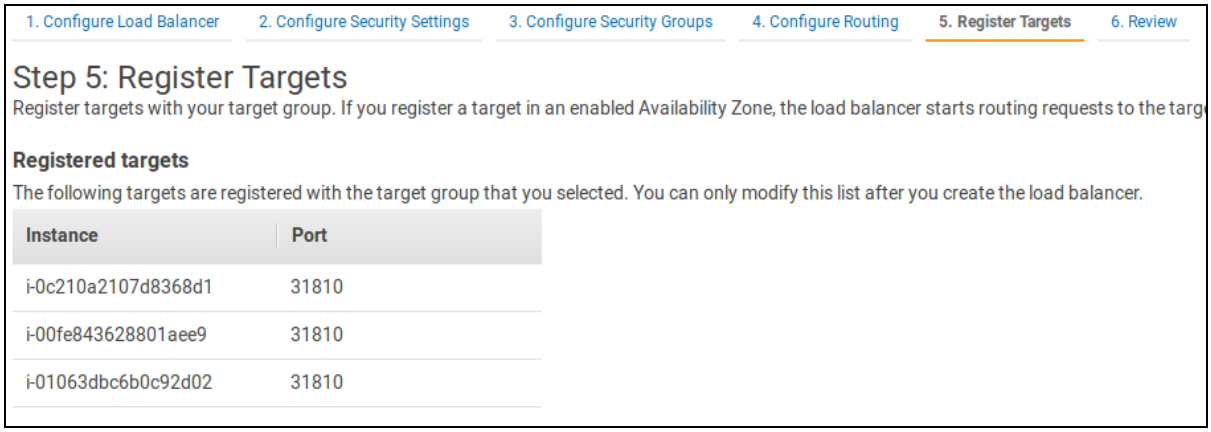
7. On the **Configure security settings** page, enter values for the following:
   a. **Certificate type:** Choose a certificate from ACM (recommended)
   b. **Certificate name:** Choose the certificate you have previously created
   c. **Security policy:** Leave unchanged.
8. Click **Next: Configure Security Groups.**



9. On the **Configure security groups** page, enter values for the following:
   a. **Assign a security group:** Leave on Select an existing security group
   b. In the list below, make sure only the Intra VPC security group created by your AWS infrastructure administrators (and recorded on the AWS worksheet) is selected.
10. Click **Next: Configure Routing**.



11. On the **Configure routing** page, enter values for the following:
    a. **Target group:** Change to **Existing target group.**
    b. **Name:** Choose the target group you have previously created.
12. Click **Next: Register** targets.



13. On the **Register targets** page, select (check) your instance IDs and node ports.
14. Click **Next: Review.**
15. On the **Review** page, verify all settings and then click **Create.** An ALB creation status will be displayed but will not be updated. (The page is not dynamic.) However, you might close the wizard.
16. From the Description tab, select **Edit attributes**.
17. For **Idle timeout**, specify a value of **300** in seconds, and click **Save**.

To create the ALB using the CLI:

1. Run the following command:
```
# aws elbv2 create-load-balancer \
--name <ALB Name> \
--subnets <subnetIds> \
--security-groups <Intra VPC Security group Id> \
--scheme internal \
--type application \
--ip-address-type ipv4
```

Parameters:

`<ALB Name>`: Choose a name for easy application load balancer identification, and record it to the AWS worksheet.

`<subnet Ids>`: Use the space-separated IDs of all three private subnets in the VPC.

`<Intra VPC Security group Id>`: ID of the Intra VPC security group created previously and recorded in the AWS worksheet.

Example input and output:

```
#aws elbv2 create-load-balancer \
--name srgdemo-alb \
--subnets subnet-0fb2ebb5882c061f0 subnet-0f0cac4ec6837abed subnet-
```

```
0abd7cd806e04c7be \
--security-groups sg-0ce3c569f73737b77 \
--scheme internal \
--type application \
--ip-address-type ipv4
```


```
{
   "LoadBalancers":[
      {
         "LoadBalancerArn":"arn:aws:elasticloadbalancing:eu-central-
1:115370848038:loadbalancer/app/srgdemo-alb/8718b24107ef591b",
         "DNSName":"internal-srgdemo-alb-505957021.eu-central-
1.elb.amazonaws.com",
         "CanonicalHostedZoneId":"Z215JYRZR1TBD5",
         "CreatedTime":"2020-06-15T09:16:12.480000+00:00",
         "LoadBalancerName":"srgdemo-alb",
         "Scheme":"internal",
         "VpcId":"vpc-0143197ca9bd9c117",
         "State":{
            "Code":"provisioning"
         },
         "Type":"application",
         "AvailabilityZones":[
            {
               "ZoneName":"eu-central-1c",
               "SubnetId":"subnet-0abd7cd806e04c7be",
               "LoadBalancerAddresses":[

               ]
            },
            {
               "ZoneName":"eu-central-1b",
               "SubnetId":"subnet-0f0cac4ec6837abed",
               "LoadBalancerAddresses":[

               ]
            },
            {
               "ZoneName":"eu-central-1a",
               "SubnetId":"subnet-0fb2ebb5882c061f0",
               "LoadBalancerAddresses":[

               ]
            }
         ],
         "SecurityGroups":[
            "sg-0ce3c569f73737b77"
```

```
        ],
        "IpAddressType":"ipv4"
      }
   ]
}
```

2. Record the `LoadBalancerArn`, `DNSName` and `CanonicalHostedZoneId` values in the AWS worksheet as **`ALB ARN, ALB DNS name`** and **`ALB Canonical hosted zone ID.`**
3. Creation of the ALB takes approximately 5 minutes. To check the ALB creation status, run the following command using the `ALB ARN` value:
```
#aws elbv2 describe-load-balancers \
--load-balancer-arns <LoadBalancerArn> \
| jq -r '.LoadBalancers[0].State.Code'
```
4. Repeat Step 3 until the returned status changes to *Active*.

   Do not proceed until the status has changed to Active.

   For Example

```
# aws elbv2 describe-load-balancers \
--load-balancer-arns arn:aws:elasticloadbalancing:eu-central-
1:115370848038:loadbalancer/app/srgdemo-alb/8718b24107ef591b \
| jq -r '.LoadBalancers[0].State.Code'
```

5. After the status is Active, run the following command to increase connection idle timeout for Load Balancer:

```
# aws elbv2 modify-load-balancer-attributes \
--load-balancer-arn <LoadBalancerArn> \
--attributes Key=idle_timeout.timeout_seconds,Value=300
```

Retrieving the OMT Ingress Service Node Port

To retrieve the OMT ingress service node port for 3000:

1. Run the following command on the bastion:

```
kubectl get svc -n core | grep frontend-ingress-controller-svc
```

   Example output:

```
frontend-ingress-controller-svc LoadBalancer 172.20.150.202 <none>
3000:30058/TCP 18h
```

2. Record the highlighted port number in your AWS worksheet as `Node port for 3000.` In the example shown, the port number is 30058.

Creating the Target Group for Port 3000

To create, tag, and add targets to the target group for port 3000 using the web UI:

1. Using the Find Services search tool, locate and browse to the EC2 Dashboard.
2. In the left navigation panel, under **Load Balancing**, click **Target Groups**.
3. On the **Target Groups** management page, click **Create target group.**
4. On the **Specify group details** page, specify values for the following:
   - Under **Choose a target type,** select **Instances**.
   - **Target group name:** Choose a descriptive name for easier identification. For example *srgdemo-3000-tg.*
   - **Protocol:** Change to *HTTPS*.
   - **Port:** Specify *3000*.
   - **VPC:** Select your VPC.
   - **Tags:** (Optional) Add descriptive tags as desired.

EC2 > Target groups > Create target group

Step 1
Specify group details

Step 2
Register targets

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Choose a target type

- (●) **Instances**
  A target group consisting of instances:
  - Supports load balancing to instances within a specific VPC.
- ( ) **IP addresses**
  A target group consisting of IP addresses:
  - Supports load balancing to VPC and on-premises resources.
  - Facilitates routing to multiple IP addresses and network interfaces on the same instance.
  - Offers flexibility with microservice based architectures, simplifying inter-application communication.
- ( ) **Lambda function**
  A target group consisting of a Lambda function:
  - Facilitates routing to a single Lambda function.
  - Accessible to Application Load Balancers only.

Target group name

srgdemo-3000-tg

Up to 32 alphanumeric characters, including hyphens. Must not begin or end with a hyphen.

Protocol : Port

HTTPS : 3000

VPC

Select the VPC containing the instances you want to choose from for inclusion in this target group.

srgdemo-vpc
vpc-0143197ca9bd9c117
IPv4: 10.0.0.0/16

Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol

HTTPS

Health check path

Use the default path of "/" to ping the root, or specify a custom path if preferred.

/

Up to 1024 characters allowed.

▶ **Advanced health check settings**

▼ Tags - *optional*

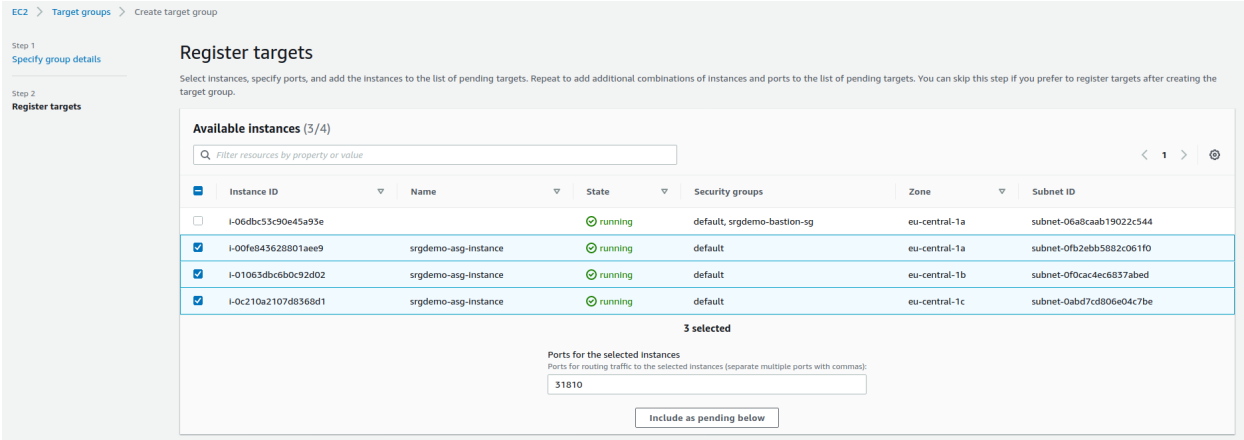
Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

Add tag

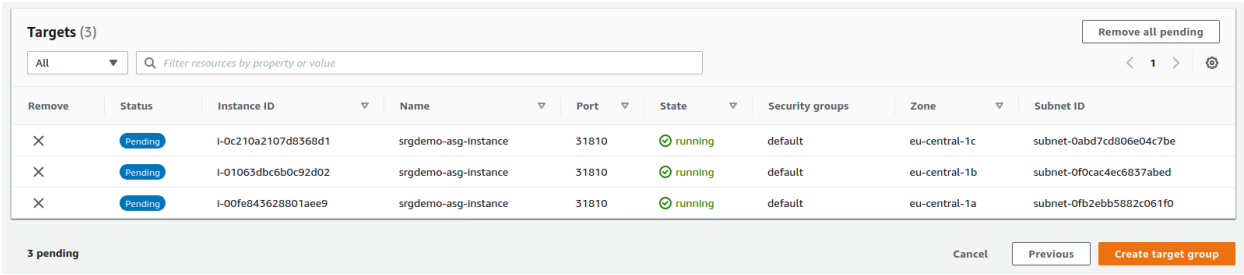
You can add up to 10 more tags.

Cancel Next

5. Under **Health Checks**, leave the **Health Check Protocol** set to *HTTPS*.
6. Click **Next**.
7. On the **Register targets** page, set values for the following:
   a. **Available instances:** Select your worker node instances, but **do not** select the bastion.
   b. **Ports:** For the selected instances, use the value you retrieved previously for the bastion as the corresponding node port for port 3000 and recorded in the AWS worksheet.



8. Click **Include as pending below.** All selected instances will be added to the list of pending instances.



9. Click **Create target group.** You will be redirected back to the target group management page.
10. From the list, select the newly created target group.
11. From the bottom of the page, record its ARN in the AWS worksheet.

To create, tag, and assign targets to the target group for port 3000 using the CLI:

1. Run the following command:

```
# aws elbv2 create-target-group \
--name <Target group 3000 Name> \
--protocol HTTPS \
--port 3000 \
--vpc-id <VPC ID> \
--health-check-protocol HTTPS \
--target-type instance
```

Where:

`<Target group 3000 Name>`: Choose some descriptive name such as `srgdemo-3000-tg`. Record the value in the AWS worksheet.

`<VPC ID>`: The ID of your VPC, as recorded in your AWS worksheet.

Example input and output:

```
# aws elbv2 create-target-group --name srgdemo-3000-tg --protocol HTTPS --
port 3000 --vpc-id vpc-0143197ca9bd9c117 --health-check-protocol HTTPS --
target-type instance
Target group for port 3000 description
{
"TargetGroupArn": "arn:aws:elasticloadbalancing:eu-central-
1:115370811111:targetgroup/srgdemo-3000-tg/c0684be94405b6b7",
"TargetGroupName": "srgdemo-3000-tg",
"Protocol": "HTTPS",
"Port": 3000,
"VpcId": "vpc-0143197ca9bd9c117",
"HealthCheckProtocol": "HTTPS",
"HealthCheckPort": "traffic-port",
"HealthCheckEnabled": true,
"HealthCheckIntervalSeconds": 30,
"HealthCheckTimeoutSeconds": 5,
"HealthyThresholdCount": 5,
"UnhealthyThresholdCount": 2,
"HealthCheckPath": "/",
"Matcher": {
"HttpCode": "200"
},
"TargetType": "instance"
}
]
}
```

From the output, record the value of `TargetGroupArn` in your AWS worksheet.

Tagging the Target Group (CLI)

Optionally, you can tag the target group for easier identification.

To tag the target group using the CLI:

1. Run the following command:

```
# aws elbv2 add-tags \
--resource-arns <Target group 3000 ARN> \
--tags Key=owner,Value=<owner>
```

Example:

```
# aws elbv2 add-tags \
--resource-arns arn:aws:elasticloadbalancing:eu-central-
1:115370811111:targetgroup/srgdemo-3000-tg/c0684be94405b6b7 \
--tags Key=owner,Value=srgdemo
```

Adding Targets to the Target Group Using the CLI

To add targets to the target group:

1. Run the following command:

```
# aws elbv2 register-targets \
--target-group-arn <Target group 3000 ARN> \
--targets Id="Instance 1 ID,Port=<Node port for 3000>" Id="Instance 2
ID,Port=<Node port for 3000>" Id="Instance 3 ID,Port=<Node port for
3000>"
```

Where:

`<Instance x ID>`: Use the instance IDs you gathered for instances of the Auto Scaling group. Refer to the AWS worksheet for these values.

`<Node port for 3000>`: Use the port number for 3000 from your AWS worksheet.

Example:

```
# aws elbv2 register-targets \
--target-group-arn arn:aws:elasticloadbalancing:eu-central-
1:115370811111:targetgroup/srgdemo-3000-tg/c0684be94405b6b7 \
```

```
--targets Id="i-05662f9ef84c182ca,Port=30058" Id="i-
07cfcd6716e9890b5,Port=30058" Id="i-08d819b5ccabe83cb,Port=30058"
```

Adding the Listener for Port 3000

This action will connect the ALB to NLB 3000 through the target group. Incoming requests to the ALB on port 3000 will be directed to the Kubernetes `itom-cdf-ingress-frontend-svc` service.

To add the listener:

Run the following command:

```
# aws elbv2 create-listener \
--load-balancer-arn <ALB ARN> \
--protocol HTTPS \
--port 3000 \
--certificates CertificateArn=<Certificate ARN> \
--default-actions Type=forward,TargetGroupArn=<Target group 3000 ARN>
```

Parameters:

`<ALB ARN>`: Use ALB ARN recorded in the AWS worksheet.

`<Certificate ARN>`: Use certificate ARN recorded in the AWS worksheet.

`<Target group 3000 ARN>`: Use the target group for port 3000 ARN recorded in the AWS worksheet.

Example input and output:

```
# aws elbv2 create-listener \
--load-balancer-arn arn:aws:elasticloadbalancing:eu-central-
1:115370848038:loadbalancer/app/srgdemo-alb/8718b24107ef591b \
--protocol HTTPS --port 3000 --certificates CertificateArn=arn:aws:acm:eu-
central-1:115370848038:certificate/691ec232-98ff-45ed-8e69-1d15c0447538 \
--default-actions \
Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:eu-central-
1:115370848038:targetgroup/srgdemo-3000-tg/c0684be94405b6b7
```

```
"Listeners":[
   {
      "ListenerArn":"arn:aws:elasticloadbalancing:eu-central-
1:115370848038:listener/app/srgdemo-alb/8718b24107ef591b/32a42e4edb52466b",
      "LoadBalancerArn":"arn:aws:elasticloadbalancing:eu-central-
1:115370848038:loadbalancer/app/srgdemo-alb/8718b24107ef591b",
```

```
      "Port":3000,
      "Protocol":"HTTPS",
      "Certificates":[
         {
            "CertificateArn":"arn:aws:acm:eu-central-
1:115370848038:certificate/691ec232-98ff-45ed-8e69-1d15c0447538"
         }
      ],
      "SslPolicy":"ELBSecurityPolicy-2016-08",
      "DefaultActions":[
         {
            "Type":"forward",
            "TargetGroupArn":"arn:aws:elasticloadbalancing:eu-central-
1:115370848038:targetgroup/srgdemo-3000-tg/c0684be94405b6b7",
            "ForwardConfig":{
               "TargetGroups":[
                  {
                     "TargetGroupArn":"arn:aws:elasticloadbalancing:eu-
central-1:115370848038:targetgroup/srgdemo-3000-tg/c0684be94405b6b7",
                     "Weight":1
                  }
               ],
               "TargetGroupStickinessConfig":{
                  "Enabled":false
               }
            }
         }
      ]
   }
]
}
```


Creating a Target Group for Ports 32081 and 32080

In order for deployed products to correctly operate, you must set up target groups, and then a listener, for ports 32081 and 32080.

To create a target group for port 32081 using the web UI:

1. Using the Find Services search tool, locate and browse to the EC2 dashboard.
2. In the left navigation panel, under **Load Balancing**, click **Target Groups**.
3. On the **Target Groups** management page, click **Create target group.**

4. On the **Specify group details** page, specify values for the following:
   a. Under **Choose a target type,** select **Instances**.
   b. **Target group name:** Choose a descriptive name for easier identification; for example *srgdemo-32081-tg*.
   c. **Protocol:** Change to *HTTPS*.
   d. **Port:** Select *32081*.
   e. **VPC:** Select your VPC.
   f. **Tags:** (Optional) Add descriptive tags as desired.
   g. **Health Checks:** Under **Health check protocol,** select HTTPS. For path, specify */th/cmak.*

EC2 > Target groups > Create target group

Step 1
Specify group details

Step 2
Register targets

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Choose a target type

- (●) **Instances**
  A target group consisting of instances:
  - Supports load balancing to instances within a specific VPC.
- ( ) **IP addresses**
  A target group consisting of IP addresses:
  - Supports load balancing to VPC and on-premises resources.
  - Facilitates routing to multiple IP addresses and network interfaces on the same instance.
  - Offers flexibility with microservice based architectures, simplifying inter-application communication.
- ( ) **Lambda function**
  A target group consisting of a Lambda function:
  - Facilitates routing to a single Lambda function.
  - Accessible to Application Load Balancers only.

Target group name

srgdemo-32081-tg

Up to 32 alphanumeric characters, including hyphens. Must not begin or end with a hyphen.

Protocol : Port

HTTPS : 32081

VPC

Select the VPC containing the instances you want to choose from for inclusion in this target group.

srgdemo-vpc
vpc-0143197ca9bd9c117
IPv4: 10.0.0.0/16

Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol

HTTPS

Health check path

Use the default path of "/" to ping the root, or specify a custom path if preferred.

/

Up to 1024 characters allowed.

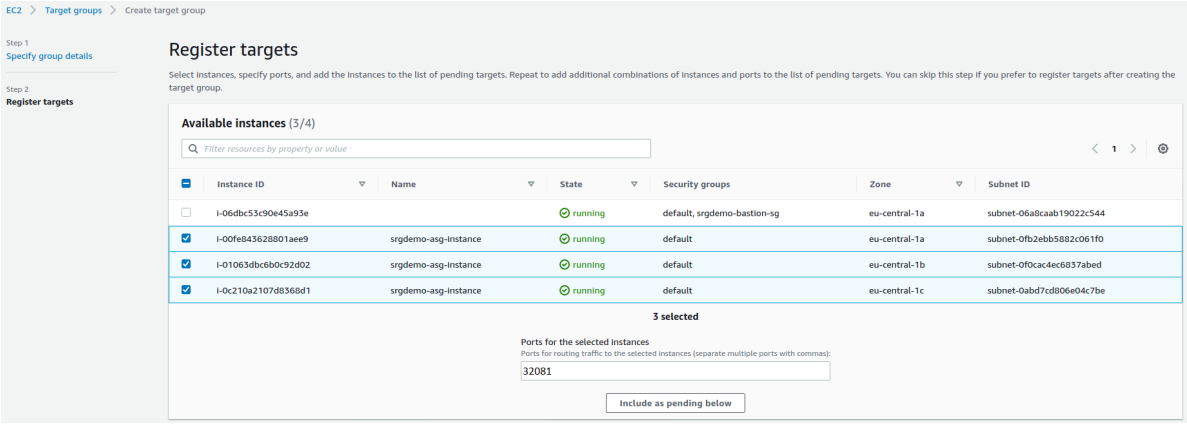
▶ **Advanced health check settings**

▶ **Tags - *optional***

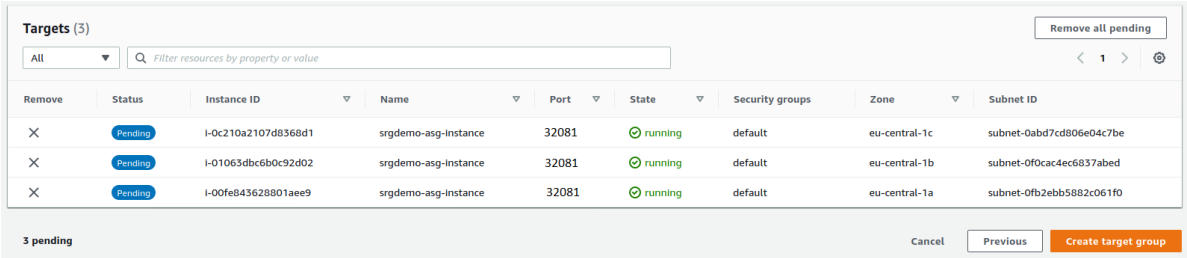
Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

Cancel Next

5. Click **Next**.
6. On the **Register Targets** page, set values for the following:
   a. **Available instances:** Select your instances; do not select the bastion.
   b. **Ports:** For the selected instances, use the value you retrieved previously and recorded in the AWS worksheet as the `Node Port for Port 32081`.



7. Click **Include as pending below.** All marked instances will be added to the list of pending instances.



8. Click **Create target group.**
9. You will be redirected back to the target group management page. From the list, select the newly created target group. From the bottom of the page, note its ARN in the AWS worksheet.
10. Repeat the steps above for ports 32080.

To create a target group for port 32081 using the CLI:

1. Run the following command:

```
# aws elbv2 create-target-group \
--name <Target group 32081 Name> \
--protocol HTTPS \
--port 32081 --vpc-id <VPC ID> \
--health-check-protocol HTTPS \
--target-type instance
```

Where:

`<Target group 32081 Name>`: Choose a descriptive name, such as `srgdemo-32081-tg`, and record the value in the AWS worksheet.

`<VPC ID>`: The ID of your VPC as recorded in your AWS worksheet.

Example input and output:

```
# aws elbv2 create-target-group \
--name srgdemo-32081-tg --protocol HTTPS \
--port 32081 --vpc-id vpc-0143197ca9bd9c117 \
--health-check-protocol HTTPS \
--target-type instance
```

```
{
   "TargetGroups":[
      {
         "TargetGroupArn":"arn:aws:elasticloadbalancing:eu-central-
1:115370811111:targetgroup/srgdemo-32081-tg/6d30f1c7be588bb6",
         "TargetGroupName":"srgdemo-32081-tg",
         "Protocol":"HTTPS",
         "Port":32081,
         "VpcId":"vpc-0143197ca9bd9c117",
         "HealthCheckProtocol":"HTTPS",
         "HealthCheckPort":"traffic-port",
         "HealthCheckEnabled":true,
         "HealthCheckIntervalSeconds":30,
         "HealthCheckTimeoutSeconds":5,
         "HealthyThresholdCount":5,
         "UnhealthyThresholdCount":2,
         "HealthCheckPath":"/",
         "Matcher":{
            "HttpCode":"200"
         },
         "TargetType":"instance"
      }
```

```
    ]
}
```

2. From the output, record the value of `TargetGroupArn` in your AWS worksheet.
3. Repeat Steps 1-2 for port 32080.

Tagging the Target Group (CLI)

Optionally, you can tag any newly-created target group for easier identification.

To tag the target group for port 32081 using the CLI:

1. Run the following command:

```
# aws elbv2 add-tags \
--resource-arns <Target group 32081 ARN> \
--tags Key=owner,Value=<owner>
```

2. Repeat the step above for port 32080.

Example:

```
# aws elbv2 add-tags \
--resource-arns arn:aws:elasticloadbalancing:eu-central-
1:115370811111:targetgroup/srgdemo-32081-tg/c0684be94405b6b7 \
--tags Key=owner,Value=srgdemo
```

Adding Targets to the Target Group for Ports 32081 or 32080

To add targets to a target group:

1. Run the following command:

```
aws elbv2 register-targets \
--target-group-arn <Target group 32081 ARN> \
--targets Id="Instance 1 ID" \
Id="Instance 2 ID" \
Id="Instance 3 ID"
```

Where:
`<Instance x ID>`: Use the instance IDs you gathered for instances of the Auto Scaling group. Refer to AWS worksheet for values.
`<Target group 32081 ARN>`: Use the ARN of the target group you just created.

`<Node port for 32081>`: Use the node port number for 32081 from the AWS worksheet.

Example:

```
aws elbv2 register-targets \
--target-group-arn arn:aws:elasticloadbalancing:us-west-
2:062373060138:targetgroup/rcchaincta-32081-tg/4fcb60e16be46ada \
--targets Id="i-01eb0557e54d10e7b,Port=32081" Id="i-
062e428614279bdee,Port=32081" Id="i-0d0223498bfff57d0,Port=32081"
```

2. Repeat the step above for port 32080.

Adding a Listener for Ports 32081 and 32080 to the ALB

This action will connect the ALB to the specified port through the target group. Then, incoming requests to the ALB on the port will be directed to the node instances.

To add a listener for port 32081 using the web UI:

1. Using the Find Services search tool, locate and browse to the EC2 Dashboard.
2. In the left navigation panel, under **Load Balancing**, click **Load Balancers.**
3. From the list of load balancers, select your previously-created Application Load Balancer (ALB).
4. On the **Listeners** tab, click **Add Listener** and set values for the following:
   a. **Protocol: port:** Change to *HTTPS* and 32081.
   b. **Default action(s):** Select the action **Forward to...** then choose your target group for port 32081.
   c. **Default SSL certificate:** Select the SSL certificate you have created previously.
5. Click **Save.**
6. Repeat Steps 1-5 for port 32080.

To add a listener for port 32080 and 32081 using the CLI:

1. Run the following command:

```
# aws elbv2 create-listener \
--load-balancer-arn <ALB ARN> \
--protocol HTTPS --port 32081 \
--certificates CertificateArn=<Certificate ARN> \
--default-actionsType=forward,TargetGroupArn=<Target group 32081 ARN>
```

Where:

`<ALB ARN>`: Use the ALB ARN recorded in the AWS worksheet.

`<Certificate ARN>`: Use the certifcate ARN recorded in the AWS worksheet.

`<Target group 32081 ARN>`: is the target group for port 32081 ARN recorded in the AWS worksheet.

Example input and output:

```
# aws elbv2 create-listener \
--load-balancer-arn arn:aws:elasticloadbalancing:eu-central-
1:115370811111:loadbalancer/app/srgdemo-alb/8718b24107ef591b \
--protocol HTTPS --port 32081 --certificates CertificateArn=arn:aws:acm:eu-
central-1:115370811111:certificate/691ec232-98ff-45ed-8e69-1d15c0447538 \
--default-actions
Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:eu-central-
1:115370811111:targetgroup/srgdemo-32081-tg/a096cb67c2f9144dv
```

```
{
   "Listeners":[
      {
         "ListenerArn":"arn:aws:elasticloadbalancing:eu-central-
1:115370811111:listener/app/srgdemo-alb/8718b24107ef591b/66915d0da2adb8a9",
         "LoadBalancerArn":"arn:aws:elasticloadbalancing:eu-central-
1:115370811111:loadbalancer/app/srgdemo-alb/8718b24107ef591b",
         "Port":32081,
         "Protocol":"HTTPS",
         "Certificates":[
            {
               "CertificateArn":"arn:aws:acm:eu-central-
1:115370811111:certificate/691ec232-98ff-45ed-8e69-1d15c0447538"
            }
         ],
         "SslPolicy":"ELBSecurityPolicy-2016-08",
         "DefaultActions":[
            {
               "Type":"forward",
               "TargetGroupArn":"arn:aws:elasticloadbalancing:eu-central-
1:115370811111:targetgroup/srgdemo-32081-tg/6d30f1c7be588bb6",
               "ForwardConfig":{
                  "TargetGroups":[
                     {
                        "TargetGroupArn":"arn:aws:elasticloadbalancing:eu-
central-1:115370811111:targetgroup/srgdemo-32081-tg/6d30f1c7be588bb6",
                        "Weight":1
                     }
                  ],
                  "TargetGroupStickinessConfig":{
                     "Enabled":false
                  }
               }
```

```
            }
        ]
    }
  ]
}
```

2. Repeat the command for port 32080 for the ArcSight Platform platform.

Directing the Route 53 Record Set to the ALB

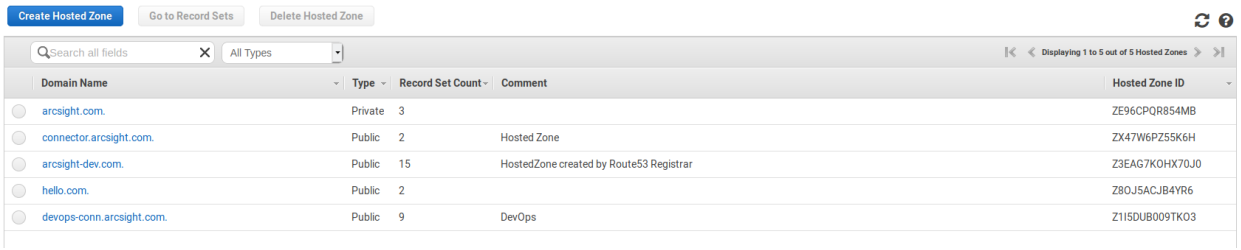
Although it is technically possible to connect to the ALB using its DNS name (such as `internal-srgdemo-alb-505957021.eu-central-1.elb.amazonaws.com`), this is not recommended for the following reasons:

- The URL is hard to remember and a user is forced to bookmark it in order to use it.
- You are unable to create the certificate for this domain, so browsers will always warn users about the insecure connection.

Previously, we created a record set in the Route 53 hosted zone and requested a certificate for the chosen domain name. You can now direct the record set to the application load balancer.

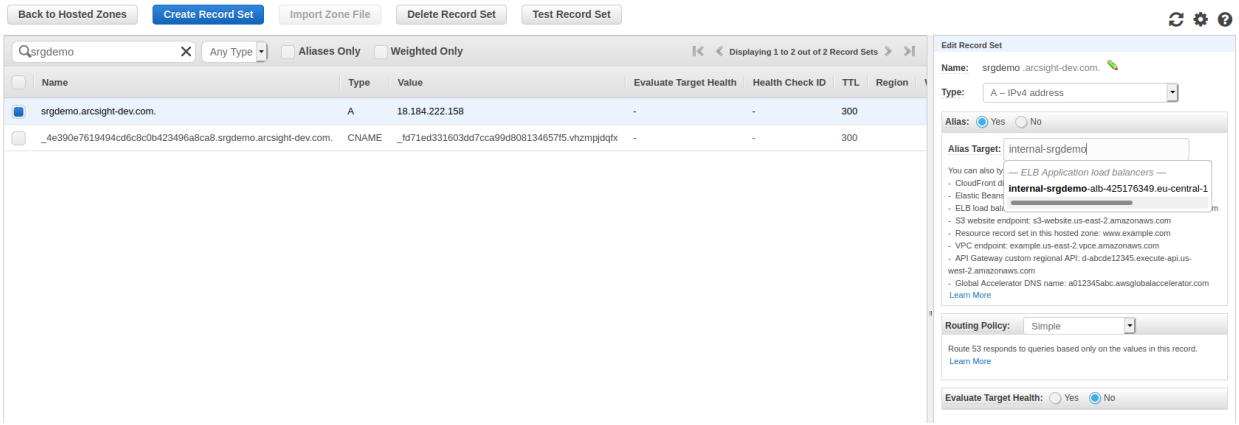
To direct the Route 53 record set to the ALB using the web UI:

1. Using the Find Services search tool, locate and browse to the Route 53 Dashboard.
2. In the left navigation panel, select **Hosted zones**. Ignore any errors generated during this process.
3. From the hosted zones list, select the same hosted zone as you chose for creating the new Route 53 record set. (Use the search box to search for the zone if necessary.)



4. Create the record set as outlined here, using the following values in the details pane.
   a. **Alias:** Change to *Yes.*
   b. **Alias Target:** Start typing `internal-<domain name>`; for example, `internal-srgdemo`. The long list will be filtered and only your ALB will be displayed. Select it.

> Upon selection the word *dialstack* will be prefixed to the name you entered. This prefix can be ignored.



5. Click **Save Record Set.**

To direct the Route 53 record set to the ALB Using the CLI:

1. Copy the template `UpdateRecordSetToALB.json` and open the copy in a text editor. This template is available in the `arcsight-platform-cloud-installer-<version>/aws-scripts/objectdefs/` subfolder.
2. Edit the following:
   a. **Record name:** Combine the subdomain (such as `srgdemo`) and hosted zone name. For example, `arcsight-dev.com`). You can also refer to the AWS worksheet for the RecordSet name.
   b. **ALB Canonical hosted zone ID:** Get the value from the AWS Worksheet.
   c. **ALB DNS name:** Get the value from the AWS Worksheet.
3. Run the following command:
```
aws route53 change-resource-record-sets \
--hosted-zone-id <Hosted zone Id> \
--change-batch file://UpdateRecordSetToALB.json
```

Where:

`<Hosted zone Id>`:Use the Hosted Zone ID from the AWS Worksheet. For example, `/hostedzone/Z3EAG7KOHX70J0`.

`<change-batch file>`: Replace the parameter with the name of your own modified instance of the linked JSON template.

Configure Browser

Finally, configure the browser on your bastion to trust the certificate.

For example, in Mozilla Firefox,

1. Select **Preferences > Privacy & Security > Certificates.**
2. Click **View Certificates.**
3. Cick **Authorities**.
4. Click **Import** and then browse to the ca.cert.pem to import the file.

Consult your browser documentation for the exact procedure on your browser.

Labeling Cloud (AWS) Worker Nodes

Labeling is a means for identifying application processing and qualifying the application as a candidate to run on a specific node. For example, labeling a node with the label `kafka=yes` specifies that a Kafka instance runs on that node. The labels tell Kubernetes the types of workloads that can run on a specific host system.

Immediately following deployment of your chosen capabilities, many of their associated pods will remain in a *Pending* state until you complete the labeling process. For example, the following Transformation Hub pods will be pending: `th-kafka`, `th-zookeeper`, `th-kafka-manager`, `th-web-service`, and `th-schemaregistry`.

When you finish labeling the nodes, Kubernetes immediately schedules and starts the label-dependent containers on the labeled nodes. The starting of services might take 15 minutes or more to complete. For more information about labeling, see "Understanding Labels and Pods" on page 453

Labels required for AWS nodes include the following:

Capability	Required Labels
ArcSight ESM Command Center	`fusion=yes`
ArcSight Layered Analytics	`fusion=yes`
ArcSight Recon	`fusion=yes`

Capability	Required Labels
Core	`fusion=yes`

Intelligence	`fusion=yes`
	`intelligence=yes`
	`intelligence-datanode=yes`
	`intelligence-spark=yes`
	`intelligence-namenode=yes`
	Applies only if you are upgrading Intelligence with the ArcSight Platform. Not applicable for a fresh installation of the ArcSight Platform.
	Select a node on which you need to place the `intelligence-namenode=yes` label. Ensure that you specify the selected node's Fully Qualified Domain Name (FQDN) in the **HDFS NameNode** field under the **OMT Management Portal** > **Configure/Deploy** page > **Intelligence** > **Analytics Configuration** section.

Transformation Hub	`kafka=yes`
	`zk=yes`
	`th-processing=yes`
	`th-platform=yes`
	`fusion=yes`

Perform the following steps to label your worker nodes:

1. Retrieve a list of worker nodes by running the following command:

   ```
   kubectl get nodes
   ```

2. Label the first worker node by running the following command:

   ```
   kubectl label node <node_name> <label_1> <label_2> <label_3> ... <label_n>
   ```

   For example:

   ```
   kubectl label node <node_name> zk=yes kafka=yes th-processing=yes th-platform=yes fusion=yes
   ```

3. Repeat Step 2 for each worker node.

Installing ArcSight in AWS

You can deploy any combination of the Intelligence, ESM Command Center, and Recon products. However, you must include the Core components and Transformation Hub capability. The Layered Analytics capability needs Intelligence, ESM Command Center, or both.

Perform the tasks shown here in the listed order.

Connecting to the OMT

With the OMT bootstrap procedure completed, the next step in installing OMT and the ArcSight Platform is to connect to the OMT web installation UI, then proceed through the installation wizard.

Accessing the OMT Installation UI

At the end of the OMT bootstrap process, you were prompted to connect to the URL `https://<external access host>:3000`, which is part of the standard OMT installation procedure.

The OMT installation port 3000 is now accessible through the chosen Route 53 record set, but only within the VPC. The VPC and any resources inside it are isolated from access from the internet (except for the bastion host, which is accessible on port 22, the SSH port).

You cannot access the created DNS record outside the VPC, since that DNS record will resolve to one of the three private subnet IP addresses which are hidden (and, in our case, in a private A-class IP range).

There are two methods for connecting a browser to the OMT port 3000: forwarding `DISPLAY` and forwarding local ports.

Forwarding DISPLAY

Prerequisite: An operating system capable of running X-server, such as *nix, linux, or MacOS.

For connection to the bastion, the easiest and fastest option is to connect to the bastion using SSH with the `-X` or `-Y` switch. This will set the remote DISPLAY accordingly, so the process running remotely will render its UI on the local X-server. The bastion host you configured earlier has the Mozilla Firefox browser installed.

> The drawback of this method is that only one user can be connected and use the web browser, and the browser response might be quite slow. Any subsequent user will receive a message that the browser is already running, and results in significant lag while in the browser. However, the browser is used only for installation and configuration tasks, which are typically done once and by a single user, so the impact will likely be small.

To connect with this method:

1. Using SSH, connect to the bastion host with the additional parameters for `dbus`. Example command:

```
ssh -i /{path to ssh key} /aws.pem -X centos@54.188.142.125 'firefox
https://srgdemo.arcsight-dev.com:3000'
```

2. Browse to the URL that OMT returned at the end of its CLI installation. For example:

```
https://srgdemo.arcsight-dev.com:3000
```

Forwarding local ports

Prerequisite: Ability to execute SSH with command line switches, as well as the Web UI ability to edit the system file `/etc/hosts` or the corresponding file.

To connect with this method, connect to the bastion host, adding the `-L` parameter. Example:

```
ssh -i .ssh/srgdemo.pem -L 3000:srgdemo.arcsight-dev.com:3000
centos@3.120.237.11
```

The `-L` parameter opens local port 3000 and connects each request to the `srgdemo.arcsight-dev.com port 3000` on the remote side. So, the bastion resolves `srgdemo.arcsight-dev.com` and opens a connection to it on port 3000.

The second part of this approach is to edit `/etc/hosts`, and add your domain to the line containing `localhost`. Example: `127.0.0.1 localhost srgdemo.arcsight-dev.com.`

> When editing your `etc/hosts` file, ensure that the IP address specified each host is unique and not duplicated across hosts. A single IP address can be associated with multiple hostnames, but the same IP address may not be used for multiple hosts.

To execute the following steps,open your preferred browser and direct it to the address that OMT output at the end of its CLI installation. For example: `https://srgdemo.arcsight-dev.com:3000.`

Deploying the ArcSight Capabilities

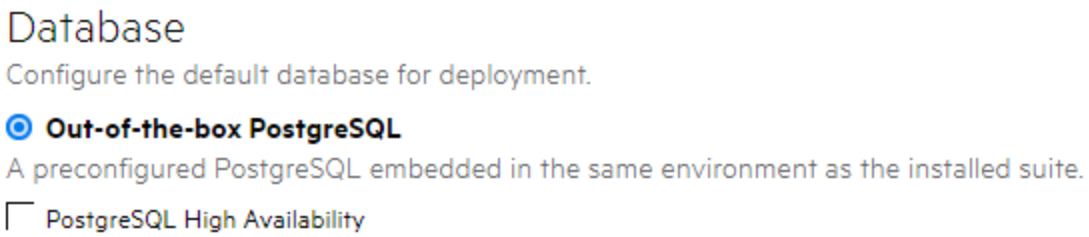
> **Tip:** The registry credentials have an expiration deadline of 12 hours after creation. If more time than that has elapsed, make sure to refresh the credentials before running this procedure.
>
> See "Refreshing the ECR Credentials in Kubernetes" on page 661.

1. On the **End User License Agreement** page:
   a. Review the End User License Agreement.
   b. To accept the agreement, select the **I agree...** check box.

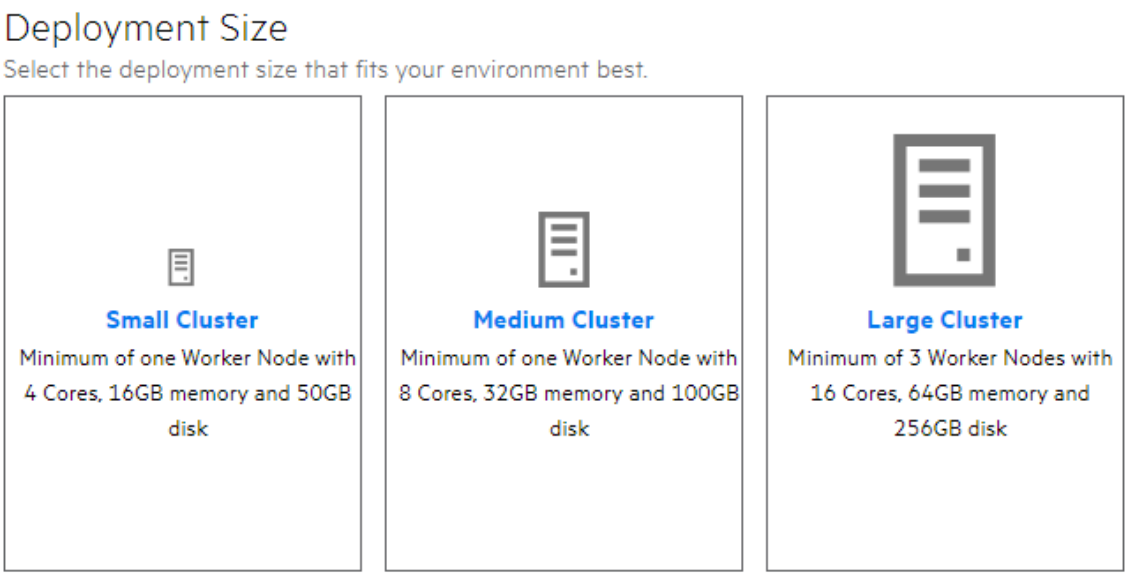
   c. (Optional) To have information passed to OpenText, select the **I authorize...** check box.
   d. Click **Next**.
2. From the **Suite Metadata Upload** screen, select the metadata file versions for the release you will be installing. For more information about those files, please refer to the *Release Notes for ArcSight Platform 24.2*.
3. On the **Capabilities** page:
   a. Select the checkboxes corresponding to the capabilities you wish to install. For example, to install ArcSight Recon, select the **ArcSight Recon** check box. The list of capabilities shown depends on products purchased by your organization, but can include Transformation Hub, Core, ArcSight Recon, ArcSight Intelligence, and ArcSight ESM Command Center.

      > Other products might require Transformation Hub or other capabilities as prerequisites. You can view any such requirements in the pull-down text associated with the capability.

   b. To show additional information associated with the capabilities, click the **>** (greater than) arrow.
   c. Click **Next**.
4. On the **Database** page:
   a. Ensure the **PostgreSQL High Availability** box is *unselected*. This database is not used by ArcSight capabilities.
   b. To continue, click **Next**.

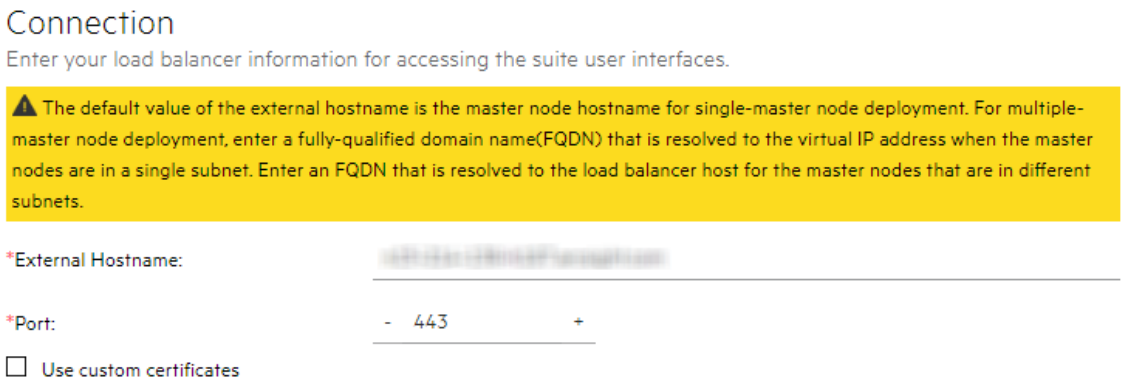


5. On the **Deployment Size** page:
   a. Based on your planned implementation, select a size for your deployment. (You can configure additional nodes, each running on their own host systems, in subsequent steps.)



b. Click **Next**.

6. On the **Connection** page:
   a. In **External Hostname**, the deployment populates an external hostname automatically from the value provided in the `--external-access-host` parameter, specified earlier during the installation of OMT.
   b. Confirm the port is correct.
   c. To continue, click **Next**.

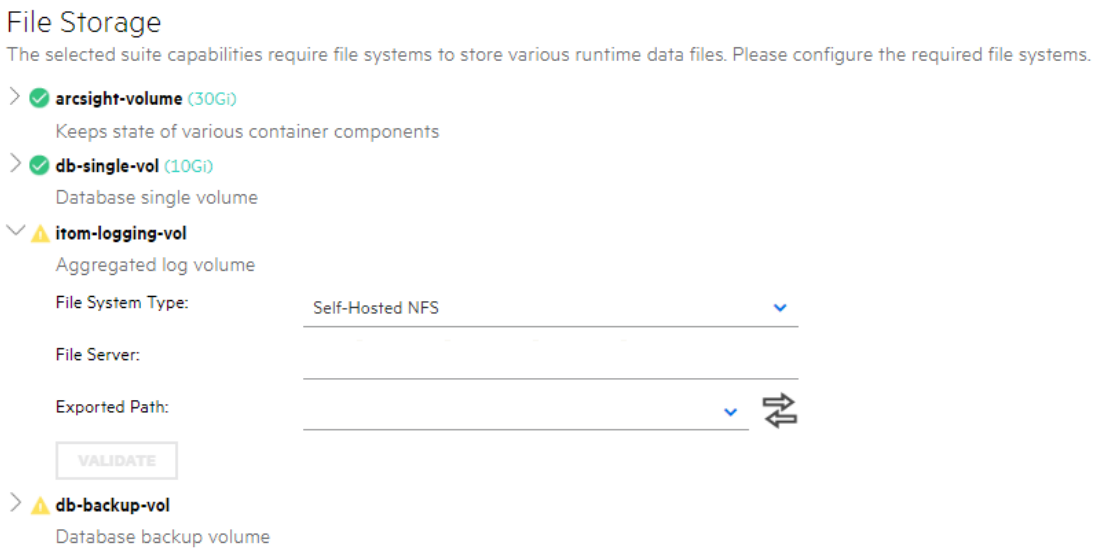


7. On the **File Storage** page, for each NFS volume to configure:
   a. In the **File System Type** drop-down, ensure **Managed NFS** is selected.
   b. In **File Server,** specify the IP address or FQDN for the NFS server.
   c. From the **Exported Path** drop-down, select the appropriate volume. For example, when using NetApp, specify the path manually instead: `/nfs/arcsight-volume`,

`/nfs/db-backup-vol, /nfs/db-single-vol, /nfs/itom-logging-vol itom-vol`. Filling out the volume path for `arcsight-volume`, and clicking the auto-fill slider (in the upper right corner) will fill out the remaining paths.

d. Click **Next**. All volumes must validate successfully to continue with the installation. The following volumes must be available on your NFS server.

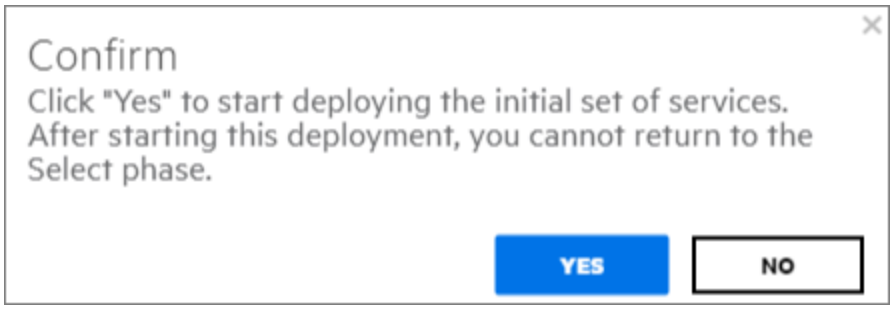
OMT NFS Volume Claim	Your NFS volume
`itom-vol`	`<NFS_ROOT_FOLDER>/itom_vol`
`db-single-vol`	`<NFS_ROOT_FOLDER>/db-single-vol`
`itom-logging-vol`	`<NFS_ROOT_FOLDER>/itom-logging-vol`
`arcsight-volume`	`<NFS_ROOT_FOLDER>/arcsight-volume`



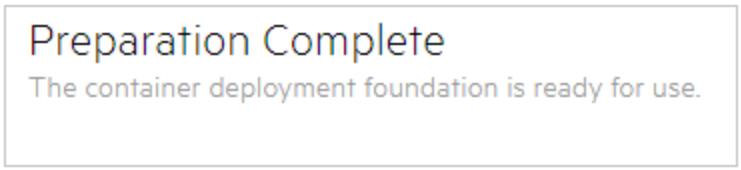
e. Click **Next**.

After you click **Next**, the infrastructure implementation is deployed. *Please ensure that your infrastructure choices are adequate to your needs.* An incorrect or insufficient configuration might require a reinstall of all capabilities.

8. On the **Confirm** dialog, to start deploying the nodes, click **Yes**.



After all nodes have been configured, and all services have been started on all nodes, the **Preparation Complete** page displays. You are now ready to configure product-specific installation attributes.



If the installation of the products seems to stall, check the logs with this command:

```
kubectl logs -n core  <pod_name>  -c suite-conf-pod-arcsight-installer
```

Where:

`<pod_name>`: `is suite-conf-pod-arcsight-installer-XXXXX`, where the Xs represent your version

If the following message is found in the logs:

```
mkdir: cannot create directory 'data/pg-data-backup/log': Permission
denied
```

You will need to manually reassign the NetApp volumes permissions by running these commands:

```
cd  <NFS_ROOT_FOLDER>
```

```
chown -R 1999:1999 itom-vol
```

After the permissions have been reassigned, the `itom-pg-backup` pod will start running and the suite deployment will finish successfully.

Configuring the Deployed Capabilities

For guidance on configuring your deployment, see "System Performance Benchmarks for Sizing and Tuning" in the *Technical Requirements for ArcSight Platform 24.2* for your workload. It might specify additional settings beyond what is described below.

You are now ready to deploy and then configure your deployed capabilities. The *Pre-Deployment Configuration* page displays instructions to configure the products and capabilities chosen at the start of the installation process. This section explains the process of configuring deployed capabilities on a supported platform.

- "Reviewing Settings that Must Be Configured During Deployment" below
- "Transformation Hub" below
- "Core components" on the next page
- "ArcSight Database" on page 233
- "Intelligence" on page 234

Reviewing Settings that Must Be Configured During Deployment

This section describes configuration settings that must be set during deployment. Additional settings can be modified after deployment by logging in to the OMT Management Portal.

> For more information on a setting, hover over the setting to display the setting tooltip, then set the values accordingly.

The following products require configuration settings to be set during deployment.

- "Transformation Hub" below
- "Core components" on the next page
- "ArcSight Database" on page 233
- "Intelligence" on page 234

Transformation Hub

If you deployed Transformation Hub, in the **Transformation Hub** tab, ensure the following are set to the number of Kafka worker nodes in your deployment or what is specified in the *Technical Requirements for ArcSight Platform 24.2* for your workload.

- # of Kafka broker nodes in the Kafka cluster (th-kafka-count)
- # of ZooKeeper nodes in the ZooKeeper cluster (th-zookeeper-count)
- # of replicas assigned to each Kafka Topic (th-init-topicReplicationFactor) (This setting must be set to 1 for a single worker deployment, and 2 for a 3-node environment.)

On the **Transformation Hub** tab, configure the following security settings based on how you planned to secure communications as described in the Securing Communication Among OpenText Components section.

> FIPS, Client Authentication, and Allow Plain Text connections to Kafka settings are available during installation and deployment only.

- Allow plain text (non-TLS) connections to Kafka (th-kafka-allow-plaintext)
- Enable FIPS 140-2 Mode (th-init-fips)

- Connection to Kafka uses TLS Client Authentication (th-init-client-auth)
- # of message replicas for the __consumer_offsets Topic (th-init-kafkaOffsetsTopicReplicationFactor)
- Schema Registry nodes in the cluster (th-schema-registry-count)

If you are deploying ESM, configure your Enrichment Stream Processor Group source Topic according to the scope for which you want to leverage ESM's event enrichment capability. For more information, refer to Enrichment Stream Processors.

Core components

If you're deploying Core, on the **Core** tab:

- Single Sign-on Configuration: Modify the Client ID (sso-client-id) and Client Secret (sso-client-secret) to a unique value for your environment.
- If you are deploying Transformation Hub, you can enrich the ingested data, such as adding a Global Event ID. You must also assign a sufficient range of IDs for the ArcMC Generator ID Manager, thus allowing the Enrichment Stream Processor to request IDs from ArcMC in the same cluster as needed for its processing. A range of 100 IDs should be sufficient for common scenarios with a comfortable buffer. However, you could also make the range larger if you have configured a large number of Enrichment Stream Processor instances or other components that use Generator IDs from this ArcMC instance.

  To enable the Core ArcMC Generator ID Manager:

  - Set **Enable Generator ID Manager** (arcmc-generator-id-enable) to **True** (this is the default value)
  - For the Enrichment Stream Processor, set **# of Enrichment Stream Processor Group instances to start** (`enrichment-processor1-replicas`) to a value greater than zero (default is 2)
  - Specify values for **Generator ID Range Start** (arcmc-generator-id-start) and **Generator ID Range End** (arcmc-generator-id-end) to provide a range of at least 100 between them

> It is important to choose a range that does not overlap with the Generator ID Manager range configured in any other ArcMC instances in your organization, otherwise different events with duplicate Globally Unique Event IDs could be created.

- **Maximum Search Results:** This value specifies number of results that a search can return. Maximum limit is 10 million events.
- **Maximum Number of Searches:** This value specifies the maximum number of searches that can exist in the system at any point. The default maximum search limit is 1,000, but you can change it to any number between 100 and 10,000. Any value above 10,000 or

below 100 will display the following error message: "The value should be a number in the range of >=100 and <=10000."

- To change the maximum search limit:
  i. Log in to the Management Portal.
  ii. Click **Deployment**.
  iii. Select **Deployments**.
  iv. Click the **Three Dots** icon (Browse) on the right side of the screen. Then, select **Reconfigure**.
  v. Select **Core**.
  vi. Scroll down to the **Search Configuration** section.
  vii. Change the value in the **Maximum Number of Searches** field to any number between 100-10,000.

> The higher the number of searches, the more storage space will be consumed.

ArcSight Database

If you deployed the ArcSight Database and you configure SmartConnectors to use the CEF format when you send events to the Transformation Hub, in the **Transformation Hub** tab, ensure the # of CEF-to-Avro Stream Processor instances to start is set to at least 1 or what is specified in *Technical Requirements for ArcSight Platform 24.2* for your workload.

On the **Database Configuration**, ensure that you set these configuration settings for your environment:

- Enable Database
- Database Host

> The host list of the database node's IP, that is node1-IP, node2-IP,..., upto nodeN-IP.

- Database Application Admin User Name
- Database Application Admin User Password
- Search User Name
- Search User Password
- Database Certificate(s)

> Copy the complete contents of the file generated-db-ca.crt, created from "Creating the Database Server Key and Certificate" in "Installing and Configuring the Database Server" on page 180.

- Database Host Name(s)

Intelligence

If you deployed Intelligence, on the Intelligence tab, ensure you set these configuration settings for your environment:

- HDFS NameNode (interset-hdfs-namenode)

  In the **OMT Management Portal** > **Configure/Deploy** page > **Intelligence** > **Analytics Configuration** section, ensure that you specify the Fully Qualified Domain Name (FQDN) of the node in the **HDFS NameNode** field.

- Elasticsearch Index Replicas Count (interset-elasticsearch-index-replicas-count)

  Ensure you change default passwords to have a unique value in your environment.

- H2 Password (interset-h2-password)

  You can set this password only at the time of deployment.

- KeyStore Password
- Elasticsearch Password (interset-elasticsearch-password)

You must enable **Enable Secure Data Transfer with HDFS Cluster** to encrypt communication between the HDFS cluster and the database. For more information, see Configuring HDFS Security in OMT.

Consider the following:

- If the topic name specified for the Avro Event Topic field is not the default topic, then use Transformation Hub's Avro routing rules using ArcMC 2.96 or later to filter Avro events from the default topic. Create a routing rule with the source topic as mf-event-avro-enriched and destination topic as the topic name you have provided in the Avro Event Topic field. For more information, see Creating a Route.
- For **Analytics Configuration-Spark**, set the values based on the data load. For information about the values for Spark, see System Hardware Sizing and Tuning Guidelines in the *Technical Requirements for ArcSight Platform 24.2* for your workload.
- For the **Data Identifiers to Identify Machine Users** field, if you need to consider only human users for licensing, ensure that you provide appropriate values to identify and filter out the machine users from licensing. For more information, contact OpenText Customer Support.

If you are specifying details under the **Hadoop File System (HDFS) Security** section, consider the following:

- The Kerberos details that you provide in **Kerberos Domain Controller Server**, **Kerberos Domain Controller Admin Server**, **Kerberos Domain Controller Domain**, and **Default Kerberos Domain Controller Realm** will be considered only if you select **kerberos** in **Enable Authentication with HDFS Cluster**. They are not valid if you select **simple**.

Checking Deployment Status

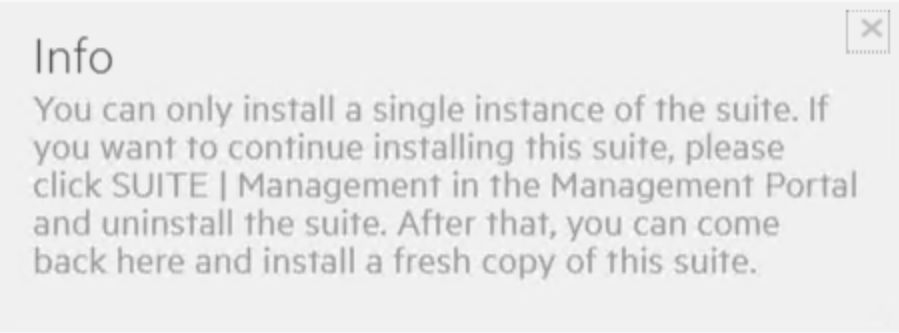
When the **Configuration Complete** page displays, the pod deployment is finished.

- Pods will remain in the *Pending* state until proper labels have been assigned to the worker nodes
- For a pod that is not in the *Running* state, you can find out more details on the pod by running the following command:

```
kubectl describe pod <pod name> -n <namespace>
```

The `Events` section in the output provides detailed information on the pod status.

If you see the following error when you attempt to log in to the OMT Management Portal on port 3000, this typically means that the OMT installation process has completed, port 3000 is no longer required, and has been closed. Instead of port 3000, log in to the Management Portal on port 5443.



Checking Cluster Status

To verify the success of the deployment, check the cluster status and make sure all pods are running.

You might need to wait 10 minutes or more for all pods to be in a *Running* or *Completed* state.

To check cluster status:

1. Connect to the cluster by doing the following:
   - For cloud installations, connect to the bastion host
2. Run the command:

```
kubectl get pods --all-namespaces
```

3. Review the output to determine the status of all pods.

> If the Elasticsearch and Logstash pods enter into a CrashLoopBackOff state, refer to "(Conditional – Intelligence) If Pods are in CrashLoopBackOff State" below and " (Conditional – Intelligence) Getting Logstash to Running State when Using Self-signed Certificates" below for the workarounds.

(Conditional – Intelligence) If Pods are in CrashLoopBackOff State

When preparing the EFS for deploying Intelligence in AWS, even after setting the permissions in the `arcsight-volume` folder to 1999:1999, the Elasticsearch and Logstash pods enter into a CrashLoopBackOff state from a **Running** state. This procedure enables you to workaround the problem of the pods being in the CrashLoopBackOff state.

1. Log in to the bastion host.
2. Navigate to the following directory and set the permissions to 1999:1999 again:

```
cd /mnt/efs/<parent_folder_name>
sudo chown -R 1999:1999 arcsight-volume
```

3. Wait for the Elasticsearch and Logstash pods to come up.
4. If the pods enter into a Running state and then into a CrashLoopBackOff state, keep repeating steps 2 and 3 until the pods are stable. That is, they don't switch from the `Running` state to the `CrashLoopBackOff` state anymore.

(Conditional – Intelligence) Getting Logstash to Running State when Using Self-signed Certificates

In an AWS deployment of Intelligence, when data is ingested, the Logstash pod enters into a CrashLoopBackOff state from a Running state. This issue occurs if you have configured OMT in the cloud (AWS) environments with self-signed certificates.

Perform the following steps:

1. Connect to Bastion.
2. Execute the following command to scale down the Logstash nodes:

```
kubectl -n $(kubectl get namespaces | grep arcsight | cut -d ' ' -f1)
scale statefulset interset-logstash --replicas=0
```

3. Execute the following command to modify the logstash-config-pipeline configmap:

```
kubectl -n $(kubectl get namespaces | grep arcsight | cut -d ' ' -f1)
edit configmaps logstash-config-pipeline
```

4. Update the value of the verify_mode field from "verify_peer" to "verify_none".
5. Save the configmap.
6. Execute the following command to scale up the Logstash nodes:

```
kubectl -n $(kubectl get namespaces | grep arcsight | cut -d ' ' -f1)
scale statefulset interset-logstash --replicas=<number_of_replicas>
```

Tuning Your Deployment for Recon or Intelligence

This section describes tuning your deployment for Recon. Skip this section if you have not deployed Recon.

Verifying Recon `cron` Jobs

After deployment, check Recon to verify that the corresponding `cron` jobs are running, as follows:

1. In Recon, browse to **INSIGHT >Data Timeseries and Source Agents and Hourly Event Volume**. If there is no information displayed after an hour, the `cron` job `events_quality.sh` is not running.
2. Go to **DASHBOARD > Data Processing monitoring** and **Health and Performance Monitoring**. If there is no information displayed after an hour, the `cron` job `events_hourly_rate.sh` is not running.

If either of these `cron` jobs is not running, then restart `fusion-db-adm-schema-mgmt`, as follows:

1. Connect to the Bastion Host.
2. Run the following commands:

```
PODS=`kubectl get pods -A | grep fusion-db-adm-schema-mgmt | awk '{print
$1, $2}'`
kubectl delete pods -n $PODS
```

Updating Event Topic Partition Number

Refer to the *Technical Requirements for ArcSight Platform 24.2*, section entitled *System Hardware Sizing and Tuning Guidelines* to determine an appropriate event topic partition number for your workload.

To update the topic partition number from the master node1:

Select one of the following commands, based on your encryption and authentication configuration:

Note: The commands contain two variables that will need to be replaced before the execution:

- `{topic_to_update}`: replace with `th-arcsight-avro`, `mf-event-avro-esmfiltered`, `th-cef` and `mf-event-avro-enriched` and for each iteration of the command
- {number_of_partitions}: For Recon - database node count * 12

For example, for a 3 nodes database cluster, the partition number would be = 3 * 12 = 36

For FIPS (or non-FIPS) Encryption with Client Authentication:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}') --
sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=$STORES_
SECRET/" /etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --alter --topic {topic_to_
update} --partitions {number_of_partitions} --command-config
/etc/kafka/client.properties'
```

After executing the above, **Copy** and then execute the following command block:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}') --
sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=/"
/etc/kafka/client.properties'
```

For FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}') --
sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreProvider=BCFIPS " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreType=BCFKS " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --alter --topic {topic_to_
update} --partitions {number_of_partitions} --command-config
/etc/kafka/client2.properties'
```

For non-FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}') --
sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --alter --topic {topic_to_
update} --partitions {number_of_partitions} --command-config
/etc/kafka/client2.properties'
```

Copy the selected command (or commands in case of **For FIPS (or non-FIPS) Encryption with Client Authentication**) and execute it 4 times according to the following table:

Command Execution	Replace the `{topic_to_update}` variable with:	Replace the `{number_of_partitions}` variable with:
First	`th-arcsight-avro`	A number of partitions that will comply with your Recon requirements
Second	`mf-event-avro-esmfiltered`	Use the same number as in the first execution of the command
Third	`th-cef`	Use the same number as in the first execution of the command
Fourth	`mf-event-avro-enriched`	Use the same number as in the first execution of the command

> Standard Kafka topics settings only permit increasing the number of partitions, not decreasing them.

5. Use the Kafka manager to verify that the partition number for the `th-cef`, `th-arcsight-avro`, `mf-event-avro-enriched` and `mf-event-avro-esmfiltered` topics have been updated to the desired partition number.

Performing Post Installation Network Configuration

During the installation of the OMT infrastructure, the system created new services providing OMT management and reconfiguration. These services listen on different ports than the OMT installation interface. OMT management listens on port 5443 and reconfiguration on port 443. In this section we will perform network configuration for these ports.

Get OMT Ingress Service Node Port for Port 5443

To get the ingress service node port for port 5443:

1. Run the following command:

```
kubectl get svc -n core | grep portal-ingress-controller-svc
```

Example output:

```
portal-ingress-controller-svc        NodePort       172.20.26.194    <none>
     5443:31704/TCP,5444:32558/TCP   170m
```

2. Record the ingress service node port for port 5443 (in the example, 31704) in the AWS worksheet.

Get Product Ingress Service Node Port for Port 443

To get the ingress service node port for port 5443:

1. Run the following command:

```
kubectl get svc -n $(kubectl get namespace --no-headers -o custom-
columns=":metadata.name" | grep arcsight-installer) | grep nginx-ingress-
controller-svc
```

Example output:

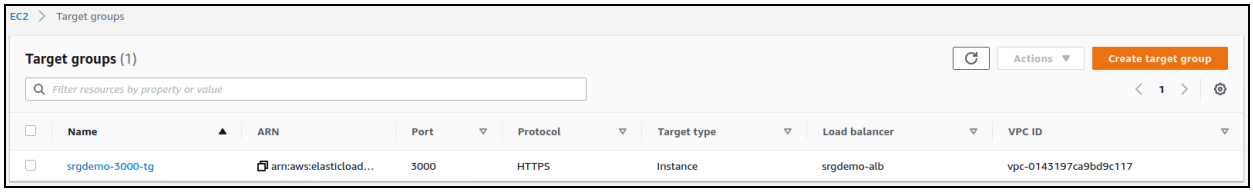
```
nginx-ingress-controller-svc           NodePort       172.20.3.220     <none>
                              443:31480/TCP                51m
```

2. Record the ingress service node port for port 443 (in the example, 31480) in the AWS worksheet.

Creating a Target Group for Port 5443 and 443

To create the target group for port 5443 using the web UI:

1. Using the Find Services search tool, locate and browse to the EC2 dashboard.
2. In the left navigation panel, under **Load Balancing**, click **Target Groups**.
3. On the **Target Groups** management page, click **Create target group.**



4. On the **Specify group details** page, enter values for the following:
   a. Under **Choose a target type,** select **Instances**.
   b. **Target group name:** Choose a descriptive name for easier identification; for example, *srgdemo-5443-tg*
   c. **Protocol:** change to HTTPS
   d. **Port:** 5443
   e. **VPC:** select your VPC
   f. **Tags:** Optionally, add descriptive tags as desired.
   g. **Health Checks:** Under **Health check protocol,** select HTTPS. For path, specify */th/cmak.*

EC2 > Target groups > Create target group

Step 1
Specify group details

Step 2
Register targets

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Choose a target type

- (●) **Instances**
  A target group consisting of instances:
  - Supports load balancing to instances within a specific VPC.
- ( ) **IP addresses**
  A target group consisting of IP addresses:
  - Supports load balancing to VPC and on-premises resources.
  - Facilitates routing to multiple IP addresses and network interfaces on the same instance.
  - Offers flexibility with microservice based architectures, simplifying inter-application communication.
- ( ) **Lambda function**
  A target group consisting of a Lambda function:
  - Facilitates routing to a single Lambda function.
  - Accessible to Application Load Balancers only.

Target group name

srgdemo-5443-tg

Up to 32 alphanumeric characters, including hyphens. Must not begin or end with a hyphen.

Protocol : Port

HTTPS : 5443

VPC

Select the VPC containing the instances you want to choose from for inclusion in this target group.

srgdemo-vpc
vpc-0143197ca9bd9c117
IPv4: 10.0.0.0/16

Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol

HTTPS

Health check path

Use the default path of "/" to ping the root, or specify a custom path if preferred.

/

Up to 1024 characters allowed.

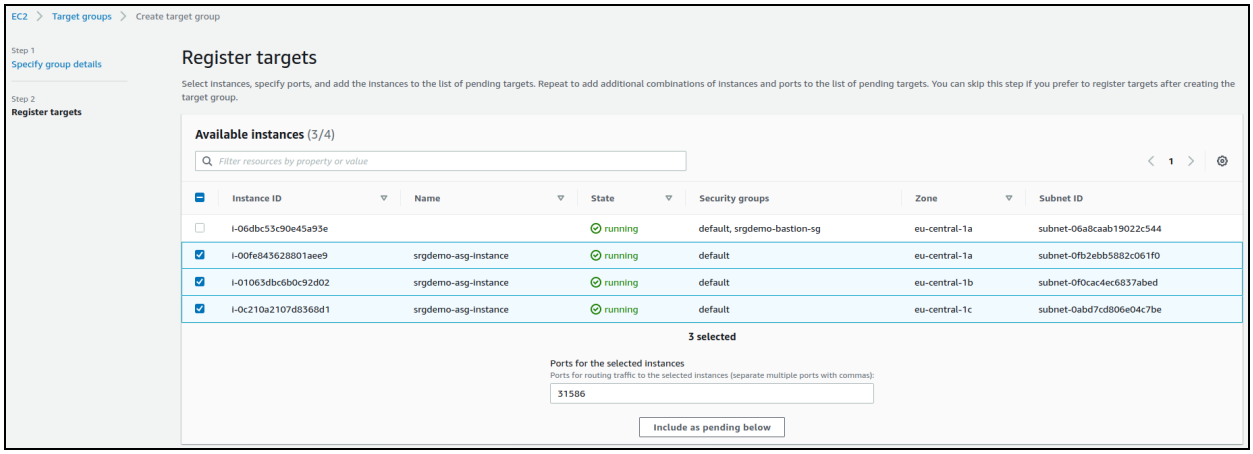
▶ **Advanced health check settings**

▶ **Tags - *optional***

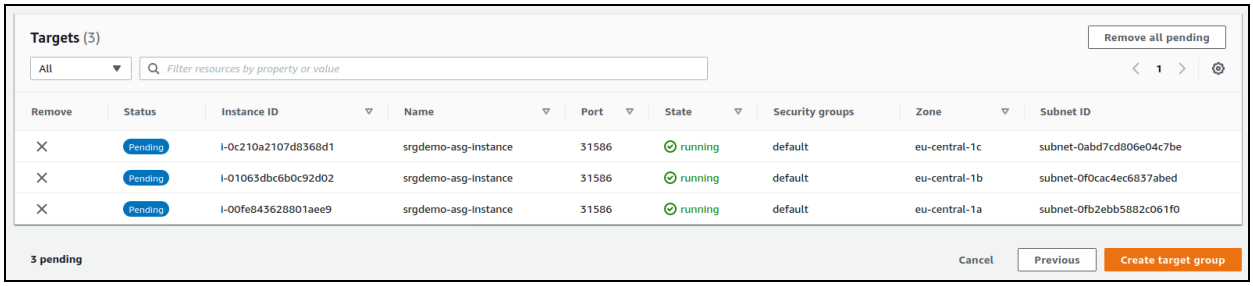
Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

Cancel Next

5. Click **Next**.
6. On the **Register Targets** page, set values for the following:
   a. **Available instances:** Select your worker node instances **only**.
   b. **Ports for the selected instances:** For the selected instances, use the value you retrieved previously and recorded on the AWS worksheet as `Node Port for Port` 5443.



7. Click **Include as pending below.** All marked instances will be added to the list of pending instances.



8. Click **Create target group.**
9. You will be redirected back to the target group management page. From the list, select the newly created target group. From the bottom of the page, record its ARN in the AWS worksheet.
10. Repeat the steps above for port 443.

To create the target group for port 5443 using the CLI:

1. Run the following command:

```
# aws elbv2 create-target-group \
--name <Target group 5443 Name>
--protocol HTTPS \
--port 5443 \
--vpc-id <VPC ID> \
--health-check-protocol HTTPS \
--target-type instance
```

Parameters:

<Target group 5443 Name>: Choose some descriptive name, such as `srgdemo-<PORT_NUMBER>-tg` and record the value in the AWS worksheet

<VPC ID>: The ID of your VPC as recorded in your AWS worksheet

Example input and output:

```
# aws elbv2 create-target-group \
--name srgdemo-5443-tg \
--protocol HTTPS \
--port 5443 \
--vpc-id vpc-0143197ca9bd9c117 \
--health-check-protocol HTTPS \
--target-type instance
```

```
{
   "TargetGroups":[
      {
         "TargetGroupArn":"arn:aws:elasticloadbalancing:eu-central-
\1:115370848038:targetgroup/srgdemo-3000-tg/c0684be94405b6b7",
         "TargetGroupName":"srgdemo-5443-tg",
         "Protocol":"HTTPS",
         "Port":5443,
         "VpcId":"vpc-0143197ca9bd9c117",
         "HealthCheckProtocol":"HTTPS",
         "HealthCheckPort":"traffic-port",
         "HealthCheckEnabled":true,
         "HealthCheckIntervalSeconds":30,
         "HealthCheckTimeoutSeconds":5,
         "HealthyThresholdCount":5,
         "UnhealthyThresholdCount":2,
         "HealthCheckPath":"/",
         "Matcher":{
            "HttpCode":"200"
         },
```

```
        "TargetType":"instance"
      }
   ]
}
```

2. From the output, record the value of `TargetGroupArn` in your AWS worksheet.
3. Repeat the steps above for port 443.

Tagging the Target Group (CLI)

Optionally, you can tag the target group for easier identification.

To tag the target group using the CLI:

1. Run the following command:

```
# aws elbv2 add-tags \
--resource-arns <Target group 5443 ARN> \
--tags Key=owner,Value=<owner>
```

Example output:

```
# aws elbv2 add-tags \
--resource-arns arn:aws:elasticloadbalancing:eu-central-
1:115370848038:targetgroup/srgdemo-5443-tg/c0684be94405b6b7 \
--tags Key=owner,Value=srgdemo
```

Adding Targets to the Target Group for Port 5443 and 443

To add targets to the target group:

1. Run the following command:

```
# aws elbv2 register-targets \
--target-group-arn <Target group 5443 ARN> \
--targets Id="<Instance 1 ID<,Port=<Node port for 5443>" Id="<Instance 2
ID>,Port=<Node port for 5443>" Id="<Instance 3 ID>,Port=<Node port for
5443>"
```

Where:

`<Instance x ID>`: Use the instance IDs you gathered for instances of the Auto Scaling group. Refer to the AWS worksheet.

`<Target group 5443 ARN>`: The ARN of the target group you just created.

`<Node port for 5443>`: Use the `node port number for 5443` from the AWS worksheet.

Example:

```
# aws elbv2 register-targets \
--target-group-arn arn:aws:elasticloadbalancing:eu-central-
1:115370811111:targetgroup/srgdemo-5443-tg/a096cb67c2f9144d \
--targets Id="i-05662f9ef84c182ca,Port=31704" Id="i-07cfcd6716e9890b5,Port=31704"
Id="i-08d819b5ccabe83cb,Port=31704"
```

2. Repeat the step above for port 443.

Adding a Listener for Port 5443 and 443 to the ALB

Similarly to the method used to add a listener for port 3000, here we will create a path for requests on port 5443 and 443 to be routed to the Kubernetes `portal-ingress-controller-svc` service through the target group created above.

To add a listener for port 5443 to the ALB using the web UI:

1. Using the Find Services search tool, locate and browse to the EC2 Dashboard.
2. In the left navigation panel, under **Load Balancing**, click **Load Balancers.**
3. From the list of load balancers, select your previously created Application Load Balancer (ALB).
4. On the **Listeners** tab, click **Add Listener** and set values for the following:
   a. **Protocol: port:** Change to *HTTPS* and *5443*.
   b. **Default action(s):** Choose the action **Forward to...**, then choose your target group for port 5443.
   c. **Default SSL certificate:** Choose the SSL certificate that you created previously.
5. Click **Save.**
6. Repeat the steps above for port 443.

To add a listener for port 5443 to the ALB using the CLI:

1. Run the following command:

```
# aws elbv2 create-listener \
--load-balancer-arn <ALB ARN> \
--protocol HTTPS \
--port 5443 \
--certificates CertificateArn=<Certificate ARN> \
--default-actions Type=forward,TargetGroupArn=<Target group 5443 ARN>
```

Parameters:

`<ALB ARN>`: Use the value of `ALB ARN` recorded in the AWS worksheet.

`<Certificate ARN>`: Use the value of `certificate ARN` recorded in the AWS worksheet.

`<Target group 5443 ARN>`: Use the value for `target group for port 5443 ARN` recorded in the AWS worksheet.

Example input and output:

```
# aws elbv2 create-listener \
--load-balancer-arn arn:aws:elasticloadbalancing:eu-central-
1:115370811111:loadbalancer/app/srgdemo-alb/8718b24107ef591b \
--protocol HTTPS --port 5443 \
--certificates CertificateArn=arn:aws:acm:eu-central-
1:115370811111:certificate/691ec232-98ff-45ed-8e69-1d15c0447538 \
--default-actions
Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:eu-central-
1:115370811111:targetgroup/srgdemo-5443-tg/a096cb67c2f9144d
```

```
Listener for port 5443 description
```

```
{
   "Listeners":[
      {
         "ListenerArn":"arn:aws:elasticloadbalancing:eu-central-
1:115370811111:listener/app/srgdemo-
alb/8718b24107ef591b/98e4aa47242b3d49",
         "LoadBalancerArn":"arn:aws:elasticloadbalancing:eu-central-
1:115370811111:loadbalancer/app/srgdemo-alb/8718b24107ef591b",
         "Port":5443,
         "Protocol":"HTTPS",
         "Certificates":[
            {
               "CertificateArn":"arn:aws:acm:eu-central-
1:115370811111:certificate/691ec232-98ff-45ed-8e69-1d15c0447538"
            }
         ],
         "SslPolicy":"ELBSecurityPolicy-2016-08",
         "DefaultActions":[
            {
               "Type":"forward",
               "TargetGroupArn":"arn:aws:elasticloadbalancing:eu-central-
1:115370811111:targetgroup/srgdemo-5443-tg/a096cb67c2f9144d",
               "ForwardConfig":{
                  "TargetGroups":[
                     {

"TargetGroupArn":"arn:aws:elasticloadbalancing:eu-central-
```

```
1:115370811111:targetgroup/srgdemo-5443-tg/a096cb67c2f9144d",
                        "Weight":1
                     }
                  ],
                  "TargetGroupStickinessConfig":{
                     "Enabled":false
                  }
               }
            }
         ]
      }
   ]
}
```

2. Repeat the step above for port 443.

Completing the Database Kafka Scheduler Setup - AWS

This section details the process for completing the database and Kafka Scheduler setup.

- Gathering Certificates for the Kafka Scheduler Setup
- Enabling the Database to Ingest Events from Transformation Hub

Gathering Certificates for the Kafka Scheduler Setup

The database and deployed capabilities need to establish a trusted connection. To do so, generate the key pair for the Kafka Scheduler.

> This step is required even if you use non-SSL communication between the Kafka Scheduler and Transformation Hub, because the schema registry is always SSL-enabled.

1. Run these commands on your database node1 to generate the Kafka Scheduler private key file `kafkascheduler.key.pem` and the certificate signing request file `kafkascheduler.csr.pem`:

   ```
   cd <yourOwnCertPath>/
   ```

   > If you installed using the ArcSight Platform Installer, the default location is `/opt/arcsight-db-tools/cert/`

```
openssl req -nodes -newkey rsa:2048 -keyout kafkascheduler.key.pem -out
kafkascheduler.csr.pem -subj "/C=US/ST=State/L=City/O=Company
Inc./OU=IT/CN=kafkascheduler"
```

2. Copy the certificate signing request `kafkascheduler.csr.pem` to your cluster, bastion host, or jump host.
3. Run the following commands on your cluster or your bastion host to sign the certificate signing request using your cluster RE certificate:

```
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o json
2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n core
-o json 2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-cbc -
md sha256 -a -d -pass pass:"${PASSPHRASE}")
export COMMON_NAME=kafkascheduler
export CSR=$(cat ${COMMON_NAME}.csr.pem)
```

```
WRITE_RESPONSE=$(kubectl exec -it -n core ${VAULT_POD} -c vault -- bash -
c "VAULT_TOKEN=$VAULT_TOKEN vault write -tls-skip-verify -format=json
RE/sign/coretech csr=\"${CSR}\"") && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .certificate" > ${COMMON_
NAME}.crt.pem && \
echo "${WRITE_RESPONSE}" | jq -r ".data | if .ca_chain then .ca_chain[]
else .issuing_ca end" > issue_ca.crt
```

4. Copy the RE signed certificate file `kafkascheduler.crt.pem` to database node1 <*yourOwnCertPath*>.
5. Copy the `issue_ca.crt` to database node1 <*yourOwnCertPath*>.
6. Change to your certificate location:

```
cd <yourOwnCertPath>/
```

7. For chained CAs, run the following commands to split the CAs into individual files:

```
cat issue_ca.crt | awk 'BEGIN {c=0;} /BEGIN CERT/{c++} { print > "issue_
ca_part." c ".crt"}'
```

```
chown -R <dbadmin_username>:<dbadmin_username> <yourOwnCertPath>
```

8. Run the following commands on database `node1` to update the database `SSL` configuration:

```
cd /opt/arcsight-db-tools
```

```
./db_ssl_setup --disable-ssl
```

If this update attempt fails, drop the certificate manually by running the three commands below:

```
sudo su - dbadmin
```

```
vsql -U <dbadminuser> -w <dbadminpassword> -c "ALTER TLS CONFIGURATION
server CERTIFICATE NULL;"
```

```
vsql -U <dbadminuser> -w <dbadminpassword> -c "DROP CERTIFICATE IF EXISTS
server CASCADE;"
```

Enable database SSL for a single issue CA or chained issue CAs:

- For a single issue CA, run this command:

  ```
  ./db_ssl_setup --enable-ssl --vertica-cert-path
  <yourOwnCertPath>/generated-db-server.crt --vertica-key-path
  <yourOwnCertPath>/generated-db-server.key --vertica-ca-path
  <yourOwnCertPath>/generated-db-ca.crt --client-ca-path
  <yourOwnCertPath>/issue_ca.crt
  ```

- For chained issue CAs, run this command, specifying each CA certificate in the chain one by one, separated by a comma in the `client-ca-path` parameter:

  ```
  ./db_ssl_setup --enable-ssl --vertica-cert-path
  <yourOwnCertPath>/generated-db-server.crt --vertica-key-path
  <yourOwnCertPath>/generated-db-server.key --vertica-ca-path
  <yourOwnCertPath>/generated-db-ca.crt --client-ca-path
  <yourOwnCertPath>/issue_ca_part.1.crt,<yourOwnCertPath>/issue_ca_
  part.2.crt[,...]
  ```

Enabling the Database to Ingest Events from Transformation Hub

The database uses an event consumer, the **Kafka scheduler**, to ingest events from Transformation Hub's Kafka component. Follow these steps when configuring the Kafka Scheduler for a new installation of the ArcSight Database:

> Before you perform these steps, ensure that you have enabled SSL for the database. For information, see Completing the Database Kafka Scheduler Setup - AWS.

1. Log in to the database node1 as root.
2. Change to the database tools directory:

```
cd /opt/arcsight-db-tools/
```

3. Run the following command on database node1 to configure the schema registry server setting:

```
./schema_registry_setup <FQDN of ArcSight Platform Virtual IP for HA,
single master node or cloud DNS name for your cluster>
<yourOwnCertPath>/issue_ca.crt <yourOwnCertPath>/kafkascheduler.crt.pem
<yourOwnCertPath>/kafkascheduler.key.pem
```

You must provide the absolute path to the certificate.

4. Configure the SSL setup:

   On database node1, configure the SSL setting for the Kafka Scheduler by using one of the following methods, plain text or SSL:

   Plain Text (non-SSL)

   This method requires that you first enable **Allow plain text (non-TLS)** connections to Kafka. For more information, see Configuring the Deployed Capabilities.

   Run this command to disable SSL for the Kafka scheduler:

```
./sched_ssl_setup --disable-ssl
```

   SSL

   This method uses the crt and key files gathered or generated in earlier steps. The `issue_ca.crt` file should contain all chained CAs. For the Kafka scheduler to use SSL, run the following command:

```
./sched_ssl_setup --enable-ssl --sched-cert-path
<yourOwnCertPath>/kafkascheduler.crt.pem --sched-key-path
<yourOwnCertPath>/kafkascheduler.key.pem --vertica-ca-key
<yourOwnCertPath>/generated-db-ca.key --vertica-ca-path
<yourOwnCertPath>/generated-db-ca.crt --kafka-ca-path
<yourOwnCertPath>/issue_ca.crt
```

5. Run this command on database node1 to create the Kafka Scheduler:
   - If the Kafka Scheduler was configured to use plain-text in the previous step, use port 9092:

```
./kafka_scheduler create <th_kafka_nodename1>:9092,<th_kafka_
nodename2>:9092[,...]
```

- If SSL was enabled for the Kafka Scheduler in the previous step, use port 9093:

```
./kafka_scheduler create <th_kafka_nodename1>:9093,<th_kafka_
nodename2>:9093[,...]
```

> Do not include spaces between Kafka brokers.

6. Add microbatch:

```
./kafka_scheduler add
```

7. Start the Kafka Scheduler and checker on database node1:

```
./kafka_scheduler messages
./kafka_scheduler events
```

> The dbadmin user has access to all the certificate/keys files.

Enabling Pod Logs in AWS

You can enable the ArcSight products application (pod) logs in AWS, which includes a cluster logging functionality called Fluentd.

To enable Fluentd in AWS, replace the values for cluster-name and cluster-region with your own values, and execute this command:

```
curl https://raw.githubusercontent.com/aws-samples/amazon-cloudwatch-
container-insights/latest/k8s-deployment-manifest-templates/deployment-
mode/daemonset/container-insights-monitoring/quickstart/cwagent-fluentd-
quickstart.yaml | sed "s/{{cluster_name}}/cluster-name/;s/{{region_
name}}/cluster-region/" | kubectl apply -f -
```

In this example, example values are used for `cluster name` and `cluster region name`.

```
curl https://raw.githubusercontent.com/aws-samples/amazon-cloudwatch-
container-insights/latest/k8s-deployment-manifest-templates/deployment-
mode/daemonset/container-insights-monitoring/quickstart/cwagent-fluentd-
quickstart.yaml | sed "s/{{cluster_name}}/test_cluster/;s/{{region_name}}/us-
west-2/" | kubectl apply -f -
```

For more information, see the AWS documentation here.

Chapter 4: Adding Additional Capabilities to an Existing Cluster

You can deploy additional capabilities, such as Recon , to an existing ArcSight Platform cluster in your environment. Reusing an existing cluster reduces costs and system management effort compared to deploying these capabilities in a new cluster.

Prerequisites and Considerations for Adding Capabilities

Before deploying additional capabilities to an existing cluster, review and, if necessary, perform the following tasks.

- Ensure that your existing cluster has the supported version of the Platform required to deploy the additional capabilities. If your deployment does not have the supported version, you must upgrade the Platform using the instructions in Upgrading Your Environment. For information about the supported version of the ArcSight Platform, see the *Technical Requirements for ArcSight Platform 24.2*.
- Recon requires the ArcSight Database. If you are adding this capability and your deployment does not already have the database, you will need to install the database using the instructions in this section.
- Check the system size of your existing ArcSight Platform Kubernetes cluster and, if applicable, ArcSight Database and ensure that it can handle the additional workload of the capabilities you want to add. If your existing cluster cannot handle the additional workload, scale the Kubernetes cluster or database as needed before deploying the additional capabilities. For information about host sizing for the Platform, see the *Technical Requirements for ArcSight Platform 24.2*.

Deploying Additional Capabilities to an Existing Cluster

You can add capabilities, such as Recon, to an existing cluster in your deployment.

> ✔ Ensure that you review the capability-specific prerequisites listed in Configuring Elasticsearch Settings.

1. (Conditional) If you are adding Recon to your deployment, you will need to have the ArcSight Database installed first. Choose your type of deployment from the list and follow the installation instructions.

- AWS

2. (Conditional) Log in to the appropriate node or host, based on your environment:
   - **For an AWS deployment:** Log in to the bastion host.
3. Create a directory for the image files that you will download in the next step:

   ```
   mkdir /tmp/download
   ```

   This directory must contain only the image files and nothing else.
4. Download the images for the capabilities that you want to add.

   For more information about images, see *Downloading ArcSight Platform Installation Files* in the *Release Notes for ArcSight Platform 24.2*.
5. Validate the digital signature of each file.

   For a complete list of files and file versions to be downloaded, consult the *Release Notes for ArcSight Platform 24.2*.

   Do not untar the files.
6. Change to the following directory.

   ```
   cd ${CDF_HOME}/scripts/
   ```

   For example:

   ```
   cd /opt/arcsight/kubernetes/scripts/
   ```
7. To upload the images to the Container Registry of your environment:
   - AWS
8. Log in to the OMT Management Portal with the following credentials:

   User name: admin

   Password: *<the password you provided during OMT installation>*
9. Click ⋮, then click **Change**.
10. On the **Capabilities** page, select the additional capabilities to deploy.

    If you are deploying the Core components on AWS, ensure that you have already configured a listener and target group for port 32080 prior to the Core components deployment. This port is required to add Transformation Hub to Core ArcMC.
11. Click the arrow next to each capability checkbox to view the description of the each capability to deploy, and determine if it requires additional capabilities. For example,

deployment of ArcSight Recon requires the deployment of Transformation Hub and the Core components.

12. Click **Next** until you reach the **Configure/Deploy** page.
13. See Configuring the Deployed Capabilities, then return to this page to continue.
14. Click **Next**. On the **Configuration Complete** page, wait until the deployment is complete. The deployment process might take several minutes to complete.

    > Some of the pods in the **Configuration Complete** page might remain in a Pending state until the product labels are applied on worker nodes.

15. Continue with labeling the nodes according to your deployment:
    - AWS
16. (Conditional) If you deployed the database in the first step, follow the instructions in: "Completing the Database Kafka Scheduler Setup - AWS" on page 248
17. Continue to Performing Post-deployment Configuration.

Chapter 5: Post-deployment Configuration

This section provides information about the post-installation configuration tasks you must perform.

To enable Multi-tenancy after the upgrade, see "Enabling Multi-tenancy " on page 442.

Installing Your License Key

ESM, ArcMC, Transformation Hub, Intelligence, Recon, and SOAR all require license keys. Each product ships with a 90-day instant-on evaluation license, which will enable functionality for a 90 day evaluation period after installation. In order for a product to continue functioning past the initial evaluation period, you will need to apply a valid license key. For more information about license keys, see the Understanding License Keys section.

To ensure continuity of functionality and event flow, make sure you apply your product license **before** the evaluation license has expired.

To install your license:

1. Log in to the Management Portal (`https://<<OMT_masternode_hostname or virtual_IP_hostname>>:5443`).
2. Click **APPLICATION**.
3. Click **License**.

   For more information about license management capabilities, see AutoPass License Management documentation.

4. Click **License > Install.**
5. Click **ADD FILE(S).**
6. Browse to the location of your license file.
7. Click **Next**.
8. Optionally, select the **I authorize OpenText to collect suite and product data...** check box to send usage data to OpenText to help improve the product.
9. Follow the prompts to apply your license.

10. Apply all of the licenses required for your deployed capabilities.
11. (Conditional) If you just installed a Transformation Hub license, restart each Kafka pod in the cluster, one at a time, as follows:
    a. For each of the Kafka pods from 0 to x, restart the selected Kafka pod with the command:
    ```
    # kubectl delete pod th-kafka-(x) -n arcsight-installer-XXX
    ```
    b. Watch the logs and ensure that each Kafka pod is up and running by running this command:
    ```
    # kubectl logs th-kafka-(x) -n arcsight-installer-XXX
    ```
    c. After the selected broker node is up and running, only then proceed to restart the next node.
    d. You can also check the status of the restarted broker node using the Transformation Hub Kafka Manager.
12. (Conditional) If you just installed an ArcSight Management Center (ArcMC) the ArcMC pod needs to be restarted after uploading the license, by running the following command:

    ```
    # kubectl delete pod fusion-arcmc-web-app-XXX -n arcsight-installer-XXX
    ```

Report and SOAR capabilities with an ESM License

The report and SOAR capabilities with an ESM license must be enabled by performing the following steps:

1. Browse to the OMT management portal `https://<OMT_masternode_hostname or virtual_IP hostname>:5443` and log in.
2. Go to the **Reconfigure** section.
3. In SOAR, go to the **ESM License Configuration for SOAR & Reporting Portal** section
4. Enable the **Use ESM License** option.
5. Enter the URL of the ESM.
6. Input the **ESM Username** and **ESM Password** and save them.

Once these steps are performed, the SOAR-web-app and reporting-web-app processes will be stopped, and these pods will be restarted again.

Configuring the Database with HDFS for Intelligence

> Applies only if you have upgraded Intelligence with the ArcSight Platform. Not applicable for a fresh installation of the ArcSight Platform.

After deploying Intelligence, you must configure the database with HDFS for the database to receive the Intelligence Analytics results data from Spark through HDFS. In addition, if **Enable Authentication with HDFS Cluster** is selected as kerberos, ensure you configure the Kerberos Authentication. For more information, see Enabling and Configuring Kerberos Authentication.

The following topics are discussed here:

- Prerequisites
- Configuring the database with unsecured HDFS
- Configuring the database with secured HDFS

Prerequisites

For a manual deployment of Intelligence, ensure that you install the firewall and open the firewall ports on the nodes before you proceed with configuring the database with HDFS:

1. Log in to a Kubernetes node labeled as intelligence-namenode:yes as a root user.
2. Execute the following commands to install and enable the firewall:

   ```
   yum -y install firewalld
   systemctl enable firewalld
   ```

3. Execute the following command to ensure NAT is configured:

   ```
   firewall-cmd --add-masquerade --permanent
   ```

4. (Conditional) Execute the following commands to open the Intelligence firewall ports on the node labeled as intelligence-namenode:yes:

   ```
   firewall-cmd --permanent --add-port=30820/tcp
   firewall-cmd --permanent --add-port=30070/tcp
   ```

   > For a secured HDFS, the port number is 30071.
   > For an unsecured HDFS, the port number is 30070.

5. (Conditional) Execute the following commands to open the Intelligence firewall ports on the node labeled as intelligence-datanode:yes.

```
firewall-cmd --permanent --add-port=30210/tcp
firewall-cmd --permanent --add-port=30010/tcp
```

6. Execute the following commands to avoid a firewall restart and to ensure that the Kubernetes services do not stop running on the node:

```
iptables -I IN_public_allow -j ACCEPT -p tcp --dport 30820 -m conntrack -
-ctstate NEW,UNTRACKED
iptables -I IN_public_allow -j ACCEPT -p tcp --dport 30210 -m conntrack -
-ctstate NEW,UNTRACKED
iptables -I IN_public_allow -j ACCEPT -p tcp --dport 30070 -m conntrack -
-ctstate NEW,UNTRACKED
iptables -I IN_public_allow -j ACCEPT -p tcp --dport 30010 -m conntrack -
-ctstate NEW,UNTRACKED
```

> For a secured HDFS, the port number is 30071.
> For an unsecured HDFS, the port number is 30070.

7. Repeat steps 1 to 5 on all nodes labeled as intelligence-datanode:yes.

Configuring the database with unsecured HDFS

> This procedure applies only if **Enable Secure Data Transfer with HDFS Cluster** is disabled in the **Intelligence** tab in the OMT Management Portal.

1. (Conditional) For a cloud deployment, do the following:
   - For AWS, connect to the bastion.
2. Execute the following command to retrieve the namespace:

```
export NS=$(kubectl get namespaces |grep arcsight|cut -d ' ' -f1)
```

3. Execute the following command to retrieve the RPC port and the web port:

```
kubectl -n $NS get svc |grep hdfs-namenode
```

   An example of the output is:

```
hdfs-namenode-svc ClusterIP None <none> 30820/TCP,30070/TCP 4h32m
```

   The first TCP port number (30820) is the RPC port and the second TCP port number (30070) is the web port.
4. Log in to a database node as a root user.
5. (Conditional) Create the `/etc/hadoop/conf/` directory, if it does not already exist.

6. (Conditional) Create the **core-site.xml** file if it does not already exist, then update the **fs.defaultFS** and **dfs.-namenode.http-address** properties along with the ports you retrieved in Step 3. Ensure that the `NAMENODE_HOST` value matches the hostname or IP address you provided in the **HDFS NameNode** field in the OMT Management Portal, **Configure/Deploy > Intelligence.**

```
cat /etc/hadoop/conf/core-site.xml
<configuration>
<property>
<name>fs.defaultFS</name>
<value>hdfs://<NAMENODE_HOST>:<NAMENODE_RPC_PORT>/</value>
</property>
<property>
<name>dfs.namenode.http-address</name>
<value><NAMENODE_HOST>:<NAMENODE_WEB_PORT></value>
</property>
</configuration>
```

For example:

```
cat /etc/hadoop/conf/core-site.xml
<configuration>
<property>
<name>fs.defaultFS</name>
<value>hdfs://vlab012345.interset:30820/</value>
</property>
<property>
<name>dfs.namenode.http-address</name>
<value>vlab12345.interset:30070</value>
</property>
</configuration>
```

7. Create the **hdfs-site.xml** file as follows if it does not already exist:

```
<configuration>
</configuration>
```

8. Repeat steps 5 to 8 on all database nodes.
9. Verify whether the database and HDFS configuration is successful:
   a. Change to the following directory:

   ```
   cd /opt/vertica/bin/
   ```

   b. Log in as a dbadmin:

```
su dbadmin
```

c. Log in to vsql and specify the password when prompted:

```
vsql
[password prompt]
```

d. (Optional) Clear the cache after configuring the database with HDFS:

```
SELECT CLEAR_HDFS_CACHES();
```

e. Execute the following commands:

```
SELECT VERIFY_HADOOP_CONF_DIR();
```

```
SELECT node_name, node_address, export_address FROM nodes;
```

The expected output is:

```
Welcome to vsql, the Vertica Analytic Database interactive terminal.

Type: \h or \? for help with vsql commands
\g or terminate with semicolon to execute query
\q to quit

dbadmin=> SELECT VERIFY_HADOOP_CONF_DIR();
VERIFY_HADOOP_CONF_DIR
-----------------------------------------------------------------------
-----
Validation Success
v_fusiondb_node0001: HadoopConfDir [/etc/hadoop/conf] is valid

(1 row)

dbadmin=> SELECT node_name, node_address, export_address FROM nodes;
node_name | node_address | export_address
-------------------------------------------------------------
v_fusiondb_node0001 | <IP1> | <IP1>
v_fusiondb_node0002 | <IP2> | <IP2>
v_fusiondb_node0003 | <IP3> | <IP3>
(3 rows)
```

Configuring the database with secured HDFS

> This procedure applies only if **Enable Secure Data Transfer with HDFS Cluster** is enabled and **Enable Authentication with HDFS Cluster** is simple in the **Intelligence** tab in the OMT Management Portal. It is not applicable if **Enable Authentication with HDFS Cluster** is kerberos.

1. (Conditional) For a cloud deployment, do the following:
   - For AWS, connect to the bastion.
2. Execute the following command to retrieve the namespace:

   ```
   export NS=$(kubectl get namespaces |grep arcsight|cut -d ' ' -f1)
   ```

3. Execute the following command to retrieve the RPC port and the web port:

   ```
   kubectl -n $NS get svc |grep hdfs-namenode
   ```

   An example of the output is:

   ```
   hdfs-namenode-svc ClusterIP None <none> 30820/TCP,30071/TCP 4h32m
   ```

   The first TCP port number (30820) is the RPC port and the second TCP port number (30071) is the web port.
4. Log in to a database node as a root user.
5. (Conditional) Create the `/etc/hadoop/conf/` directory, if it does not already exist.
6. Create the **hdfs-site.xml** file as follows if it does not already exist:

   ```
   <configuration>
    <property>
     <name>dfs.http.policy</name>
     <value>HTTPS_ONLY</value>
    </property>
   </configuration>
   ```

7. Create the **core-site.xml** file if it does not already exist, then update the **fs.defaultFS** and **dfs.-namenode.https-address** properties along with the ports you retrieved in Step 4. Ensure that the `NAMENODE_HOST` value matches the hostname or IP address you provided in the **HDFS NameNode** field in the OMT Management Portal, **Configure/Deploy > Intelligence.**

   ```
   <configuration>
    <property>
     <name>fs.defaultFS</name>
     <value>hdfs://<NAMENODE_HOST>:30820/</value>
    </property>
   ```

```
 <property>
  <name>dfs.namenode.https-address</name>
  <value><NAMENODE_HOST>:30071</value>
 </property>
</configuration>
```

8. Repeat steps 5 to 8 on all database nodes.
9. Verify whether the database and HDFS configuration is successful:
   a. Change to the following directory:

      ```
      cd /opt/vertica/bin/
      ```

   b. Log in as a dbadmin:

      ```
      su dbadmin
      ```

   c. Log in to vsql and specify the password when prompted:

      ```
      vsql
      [password prompt]
      ```

   d. Clear the cache after configuring the database with HDFS:

      ```
      SELECT CLEAR_HDFS_CACHES();
      ```

   e. Execute the following commands to verify that the database configuration is valid:

      i. ```
         SELECT VERIFY_HADOOP_CONF_DIR();
         ```

      ii. ```
         SELECT HDFS_CLUSTER_CONFIG_CHECK();
         ```

10. If you have a non-collocated database cluster and **Enable Secure Data Transfer with HDFS Cluster** is enabled, perform the following steps:
    a. Execute the following command in the master node:

       ```
       /opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/re_ca.cert.pem
       ```

    b. Execute the following commands in each database node:

       ```
       scp root@<master_node_FQDN>:/tmp/re_ca.cert.pem /etc/pki/ca-
       trust/source/anchors/
       ```

       ```
       update-ca-trust
       ```

    c. Execute the following command to verify that there is a trust relationship with the CA from each database node:

```
curl https://<WORKER_RUNNING_HDFS_NAMENODE>:30071
```

You should not encounter any certificate errors after executing the above command.

> The **Enable Secure Data Transfer with HDFS Cluster** field is enabled by default to encrypt communication between the HDFS cluster and the database. However, this increases the run time of the analytics jobs.

Creating the First System Admin User

> This procedure applies only when you deploy a capability that requires the Core components.

To create the first user in the System Admin role:

1. Open a supported web browser.
2. Specify the following URL to log in to the application:
   `https://<OMT_masternode_hostname or virtual_ip hostname>/mgmt`
3. Specify the required information to create a System Admin user.

   > **Important**: It is strongly recommended that you use a valid email address for the user, so that it can be used to recover access to the account if the password is forgotten. There is no practical way to recover the account when the password is forgotten if the email address is not valid.

4. After the account is created, log in with the credentials you just created.
5. (Optional) Log in to the application with the Email ID and password you just created.

Enabling Integration with AWS Transformation Hub

> This procedure applies only when you have deployed to AWS.

For proper integration with AWS Transformation Hub, after you set up your AWS deployment architecture, you must complete the applicable procedure for the ArcSight product (SmartConnectors, Logger, or ESM) you are integrating. You must complete the procedure before you can configure the product to consume events from or send events to Transformation Hub.

Completing Additional Procedures for SmartConnectors, Logger, or ESM

Obtain the cluster worker node (Kafka broker node) host names using one of the following procedures.

From the bastion host:

1. From the bastion host, run the following command:

```
# kubectl get nodes
```

2. Copy the node host names. You will need these names when configuring the product to produce events from or send events to Transformation Hub.

From AWS:

1. In the AWS user interface, go to your Auto Scaling Group.
2. To see the instance IDs, select the **Instance Management** tab.
3. To view the details of the corresponding instance, click the first instance ID.
4. Note the private DNS name for the instance.
5. Repeat Step 3 and Step 4 for each instance ID.
6. After determining these values, ensure that your SmartConnector, Logger, or ESM instance is added to the AWS Transformation Hub Cluster Security Group with rules allowing access to ports 32080 and 9093.

You can now configure the product to consume events from or, if the functionality is available, send events to Transformation Hub:

- Configuring Logger and SmartConnectors as a Transformation Hub Consumer
- Configuring ESM as a Transformation Hub Consumer
- Configuring ESM as a Transformation Hub Producer in Distributed Correlation Mode

Configuring ArcMC Parser Upgrades

Perform the steps below to configure ArcMC parser upgrades.

Access ArcSight Marketplace Through a Proxy Server

To access the ArcSight Marketplace through a proxy server when performing parser upgrades:

1. Log in to the OMT Management Portal. See "Accessing the OMT Management Portal" on page 507 for more information.
2. From the left menu select **Deployment > Deployments**.
3. Click **... (Browse)** on the far right and choose **Reconfigure**. A new screen will open in a separate tab.
4. Select the **Core** tab.
5. Scroll down to the **ArcMC Parser Upgrades** section, then specify the desired value for the parameters:
   a. Proxy Server for Parser Upgrades
   b. Proxy Port for Parser Upgrades
   c. Proxy Username for Parser Upgrades (if the proxy server needs authentication)
   d. Proxy Password for Parser Upgrades (if the proxy server needs authentication)
6. Click **Save**. The ArcMC pod will be restarted.

Change the Number of Parser Upgrade Versions Displayed

To select the number of parser upgrade versions retrieved from the ArcSight Marketplace:

1. Follow steps 1 through 4 in "Access ArcSight Marketplace Through a Proxy Server" on the previous page
2. Scroll down to the **ArcMC Parser Upgrades** section and select the desired value for the **Display Marketplace Parser Upgrade Versions** parameter.
3. Click **Save**. The ArcMC pod will be restarted.

Disable the Marketplace Connection

1. Follow steps 1 through 4 in "Access ArcSight Marketplace Through a Proxy Server" on the previous page
2. Scroll down to the **ArcMC Parser Upgrades** section and disable the **Enable Marketplace** option.
3. Click **Save**. The ArcMC pod will be restarted.

If you disable the connection to the ArcSight Marketplace you will not be able to see the available parser upgrade versions. In addition, the containers under **Node Management > Containers tab**, will not display the Parser Out of Date status in the Parser Version column.

Checklist: Performing Regular Maintenance

Use the following checklist to perform regular maintenance of the Platform infrastructure.

Frequency	Task	See...
Every 1-3 Days	Check the Health and Performance Dashboard for status or errors.	Using the Health and Performance Monitoring Dashboard
Every 1-3 Days	Check the Kubernetes Dashboard for status and errors.	"Checking Kubernetes Dashboard for Status and Errors" on page 510
Every week	Check automatic backup jobs for status and errors. **NOTE:** See the link to the right for procedures to enable automatic backup jobs. After the jobs are enabled, they will run automatically on schedule unless an error is encountered.	Backing Up and Restoring
Every 1-3 Days	Run CDF Doctor for status and errors.	Using the CDF Doctor Utility
Every 90 Days	Reset the expiring OMT Management Portal admin account password. The registry-admin password used when uploading capability images during system upgrade is initially set to the same password as the admin user for the OMT Management Portal during installation when configuring and installing OMT; however, later changing the OMT Management Portal admin password does not change the registry-admin password as it is managed separately. The registry-admin password does not automatically expire.	Resetting the OMT Administrator Password
Every 11 Months	Renew any expiring OMT certificates (default expiration is 1 year).	"Maintaining Certificates" on page 524

Configuring Intelligence Analytics Targeted Events

This topic and the procedure that follows are applicable only if you are deploying both the ArcSight Intelligence and ArcSight Recon capabilities with the ArcSight Platform.

Elasticsearch filtering enables Intelligence analytics resources to be focused on the events that are most valuable for Intelligence analytics capabilities.

Through extensive research, ArcSight data scientists have identified a targeted set of events proven to be the best inputs into threat detection analytic models.

Other events, useful for different purposes (such as investigating all stages of a threat life-cycle), are not used as input into the Intelligence analytics capabilities.

In some deployments (especially when ArcSight Recon and Intelligence are both deployed), and depending on the ingested data, applying the correct filter can free up significant storage, CPU and memory resources in each server.

This procedure installs the Logstash-based event filter to limit what is stored in the Intelligence Elasticsearch component to those identified valuable events.

Once the filter is configured, the Intelligence Elasticsearch component will only ingest from Transformation Hub filtered events that are useful with Intelligence analytics.

To install the filter for Intelligence Elasticsearch:

1. Log in to the master node of the OMT cluster.
2. Edit the `logstash-config-pipeline` file using the following command:

```
kubectl -n $(kubectl get namespaces | grep arcsight | cut -d ' ' -f1)
edit configmaps logstash-config-pipeline
```

3. Locate the code block below and add a line break at the end:

```
if [destinationUserName] =~ "\$" {
   mutate {

replace => {
         "did" => "1"
      }
   }
}
```

4. Add the following code block after the line break, while respecting code indentation:

```
if [destinationUserName] and [externalId] in
['4624','4625','4648','4768','4769','4771','4776','4777'] {
}
else if [categoryDeviceGroup] =~ "/Network Equipment" and
[categoryDeviceType] =~ "Network Monitoring" {
}
else if [sourceusername] and [externalId] in ['Squid','Microsoft','Blue
Coat'] and [deviceProduct] in ['Proxy SG','Squid Web Proxy Server','ISA
```

```
Server'] {
}
else if [categoryDeviceType] =~"Repository" and [destinationUserName] and
[deviceAction] and [deviceCustomString1] {
}
else if [destinationUserName] and [categoryOutcome] and [fileName] and
[deviceProduct] in ['','WORKGROUP','NT SERVICE','NT AUTHORITY'] {
}
else if [type] == 2 {
}
else if [categoryObject] =~ "/Host/Application/Service" {
}
else {
      drop {}
}
```

5. Run the following command:

```
kubectl -n $(kubectl get namespaces | grep arcsight | cut -d ' ' -f1)
scale statefulset interset-logstash --replicas=0
```

6. After allowing time for the process to finish, validate that pods are successfully scaled down by running:

```
kubectl -n $(kubectl get namespaces | grep arcsight | cut -d ' ' -f1) get
pods | grep logstash
```

   You will know the process is finished when no pods are shown.

7. Run the following command to complete the filter installation:

```
kubectl -n $(kubectl get namespaces | grep arcsight | cut -d ' ' -f1)
scale statefulset interset-logstash --replicas=X
```

   Were X stands for the number of Logstash instances you want to run across the cluster and generally equals the number of worker nodes.

Chapter 6: Integrating the Platform Into Your Environment

Transformation Hub integrates with many ArcSight products, and is managed and monitored by ArcSight Management Center. After you install and configure Transformation Hub you can use SmartConnectors to produce and publish data to the Transformation Hub, and to subscribe to and consume that data with Logger, ESM, ArcSight Recon, Apache Hadoop, or your own custom consumer.

> Currently, cloud clusters only support other ArcSight products which are in the cloud. Integration with Off-cloud products is not supported for cloud-based Transformation Hub.

Transformation Hub supports both Common Event Format (CEF) versions (0.1 and 1.0), as well as Avro and binary data formats. Transformation Hub third-party integration and other product features are explained in detail in the following sections.

Connecting to Your SMTP Server

To ensure that Core users receive email notifications, configure the connection to your SMTP server. For example, if you do not use external authentication (such as LDAP or SAML), users will need notifications to help reset their forgotten passwords.

> **Note: AWS SES SMTP prerequisites:** If you are deploying Core with AWS, complete these prerequisites before configuring SMTP for Core. AWS SES SMTP requires TLS to be enabled.
>
> - For the AWS SES SMTP service, ensure that your private security group allows SMTP on the ports specified in AWS documentation.
> For more information, see *Connecting to an Amazon SES SMTP endpoint*.
> - Review the list of AWS SMTP protocol endpoints. For more information, see Amazon SES.
> - Download the Starfield Services Root CA from https://good.sca0a.amazontrust.com/.
> - Make sure your Cloud administrator enables outbound traffic on your SMTP service ports.

To configure SMTP for Core:

1. Log in to the OMT Management Portal.
2. Click **DEPLOYMENT**, and select **Deployments**.
3. Select **Reconfigure** in the **Three Dots** menu and navigate to **Core > User Management Configuration**.
4. Configure SMTP:

a. SMTP TLS Enable (Enable it for TLS, or disable it for non-TLS.)
b. Add the certificate for the SMTP service.
c. Add the SMTP host URL.
d. Add the SMTP port number.
e. Enter the SMTP Admin name.
f. Enter the SMTP Admin password.
g. Add the SMTP Admin email address.
h. Click **Save** to activate the configuration changes.

   This will automatically restart application pods that offer email service.

If an installed certificate expires, its path changes or a fresh one is generated. When this happens, you must re-import it using the same process above.

If you connect to an SMTP server as an anonymous user or do not have a user name and password configured, you must add a dummy password and save.

Important: Message size constraints are applied according to the message size policy for your SMTP Service. Emailing report assets is one example that increases message size. If you encounter message limit or size warnings, or other errors, contact your SMTP administrator.

Example warning (AWS default):

AWS SES SMTP email attachments cannot exceed 10 MB. Contact your cloud administrator. See https://docs.aws.amazon.com/ses/latest/dg/quotas.html.

Core ArcMC SMTP

To configure SMTP for Core ArcMC follow the steps in "SMTP" on page 957.

Configuring an External Identity Provider

Password-based authentication requires users to specify their User ID and Password when logging in. You can select the built-in authentication or external authentication, such SAML or LDAP.

- "Configuring LDAP Authentication" on the next page
- "Configuring SAML Authentication" on page 276

Configuring LDAP Authentication

The identity provider (IDP) user and password has governance over the platform; therefore, the user must exist in both systems, but the password is validated only in LDAP. This section details LDAP authentication steps when TLS is enabled and disabled. The following table lists LDAP property names and related values:

S.No	LDAP Property Name	Related Value
1.	LDAP Admin DN	LDAP User DN
2.	LDAP Admin Password	Base64 Encoded LDAP Admin Password
3.	LDAP Host	LDAP Host IP Address
4.	LDAP Use TLS Setting	True or False
5.	LDAP Port	LDAP Environment Port
6.	AS Naming Attribute	Active Directory Attribute
7.	AS User’s Container DN	LDAP Base DN

To use LDAP authentication when TLS is disabled:

1. Create at least one LDAP user to log in into the platform using LDAP authentication.
2. Log in to the OMT server and navigate to the SSO default configuration folder at:

   ```
   <arcsight_nfs_vol_path>/sso/default
   ```

   where `<arcsight_nfs_vol_path>` is the NFS volume used for OMT installation; for example: `/opt/NFS_volume/arcsight-volume.`

3. Open the SSO configuration file (sso-configuration.properties), and review the LDAP parameters.

   ```
   ##### The following LDAP confgs are not utilized at this time
   # com.microfocus.sso.default.ldap.enabled = true
   # com.microfocus.sso.default.login.method = np-ldap
   # com.microfocus.sso.default.ldap.admin-dn = CN=bind_
   user,cn=Users,dc=ospad,dc=test
   # com.microfocus.sso.default.ldap.admin-pwd = password
   # com.microfocus.sso.default.ldap.host = xxx.xx.xx.xx
   # com.microfocus.sso.default.ldap.use-tls = false
   # com.microfocus.sso.default.ldap.port = 389
   #---- uncomment these if the LDAP server is Active Directory rather than
   eDirectory
   # com.microfocus.sso.default.ldap.dir-type = AD
   # com.microfocus.sso.default.as.naming-attr = sAMAccountName
   # com.microfocus.sso.default.as.users-container-dn = cn=Users,dc=ospad,dc=test
   ```

```
## uncomment these to configure URL when LDAP user forgets password
# com.microfocus.sso.default.ldap.forgotten-pwd-url =
# com.microfocus.sso.default.ldap.login.forgotten-password-target = _blank
# com.microfocus.sso.default.ldap.login.forgotten-password-text-res-id =
# com.microfocus.sso.default.ldap.login.forgotten-password-title-res-id =
```

4. Update the SSO configuration file (sso-configuration.properties) for your LDAP log in method by uncommenting (removing the #) of these lines in the sso-configuration.properties file, and completing the information for your LDAP environment.

```
com.microfocus.sso.default.ldap.enabled = true
com.microfocus.sso.default.login.method = np-ldap
com.microfocus.sso.default.ldap.admin-dn = provide your LDAP User DN here
com.microfocus.sso.default.ldap.admin-pwd = provide your Base64 encoded LDAP Admin
password here
com.microfocus.sso.default.ldap.host = provide your LDAP host here
com.microfocus.sso.default.ldap.use-tls = true (this corresponds to your LDAP TLS setting,
true or false. However, a "false" value will fail to enable a TLS LDAP connection)
com.microfocus.sso.default.ldap.port = 636 (your LDAPS Environment port may differ - change
accordingly)
```

5. For Active Directory rather than eDirectory:
   a. Update the SSO configuration file (sso-configuration.properties) to enable AD by uncommenting these lines in the sso-configuration.properties file, and completing the information for your LDAP environment.

```
com.microfocus.sso.default.ldap.dir-type = AD
com.microfocus.sso.default.as.naming-attr = provide your AD attribute here
com.microfocus.sso.default.as.users-container-dn = provide your LDAP Base DN here
```

   b. Save the SSO configuration file (sso-configuration.properties).

To configure the system to require users to login with an email address (recommended), set `com.microfocus.sso.default.as.naming-attr` to 'mail'. Otherwise, to require users to login with their Active Directory username, set `com.microfocus.sso.default.as.naming-attr` to 'sAMAccountName'.

6. For URL configuration when an LDAP user forgets the password:
   a. Update the SSO configuration file (sso-configuration.properties) to enable *forgot password* for the LDAP user by uncommenting these lines in the sso-configuration.properties file, and completing the information for your LDAP environment.

```
com.microfocus.sso.default.ldap.forgotten-pwd-url = provide your LDAP url for
forgotten password here
com.microfocus.sso.default.ldap.login.forgotten-password-target = provide the
```

```
target here
com.microfocus.sso.default.ldap.login.forgotten-password-text-res-id = provide
the text to be shown here
com.microfocus.sso.default.ldap.login.forgotten-password-title-res-id = provide
the title to be shown here
```

b. Save the SSO configuration file (sso-configuration.properties).

7. Restart the fusion-single-sign-on pod.

   a. Get the fusion-single-sign-on pod information:

   ```
   kubectl get pods --all-namespaces | grep single-sign
   ```

   b. Restart the fusion-single-sign-on by deleting the currently running pod:

   ```
   kubectl delete pod fusion-single-sign-on-xxxxxxxxxx-xxxxx -n arcsight-
   installer-xxxxx
   ```

8. Log in using your LDAP credentials.

To use LDAP authentication when TLS is Enabled:

1. Create at least one LDAP user to log in into the platform using LDAP authentication.
2. Log in to the OMT server and navigate to the SSO default configuration folder at:

   ```
   <arcsight_nfs_vol_path>/sso/default
   ```

   where `<arcsight_nfs_vol_path>` is the NFS volume used for OMT installation; for example: `/opt/NFS_volume/arcsight-volume.`

3. Open the SSO configuration file (sso-configuration.properties), and review the LDAP parameters.

   ```
   ##### The following LDAP confgs are not utilized at this time
   # com.microfocus.sso.default.ldap.enabled = true
   # com.microfocus.sso.default.login.method = np-ldap
   # com.microfocus.sso.default.ldap.admin-dn = CN=bind_
   user,cn=Users,dc=ospad,dc=test
   # com.microfocus.sso.default.ldap.admin-pwd = password
   # com.microfocus.sso.default.ldap.host = xxx.xx.xx.xx
   # com.microfocus.sso.default.ldap.use-tls = true
   # com.microfocus.sso.default.ldap.port = 636
   #---- uncomment these if the LDAP server is Active Directory rather than
   eDirectory
   # com.microfocus.sso.default.ldap.dir-type = AD
   # com.microfocus.sso.default.as.naming-attr = mail
   # com.microfocus.sso.default.as.users-container-dn = cn=Users,dc=ospad,dc=test
   ## uncomment these to configure URL when LDAP user forgets password
   ```

4. Update the SSO configuration file (sso-configuration.properties) for your LDAP log in method by uncommenting (remove the #) these lines in the sso-configuration.properties file, and completing the information for your LDAP environment.

```
com.microfocus.sso.default.ldap.enabled = true
com.microfocus.sso.default.login.method = np-ldap
com.microfocus.sso.default.ldap.admin-dn = provide your LDAP User DN here
com.microfocus.sso.default.ldap.admin-pwd = provide your Base64 encoded LDAP Admin
password here
com.microfocus.sso.default.ldap.host = provide your LDAP host here
com.microfocus.sso.default.ldap.use-tls = true provide your LDAP TLS setting here
(true/false)
com.microfocus.sso.default.ldap.port = 636 provide your LDAP port here
```

5. Create and copy the PEM formatted CA LDAP server certificate into the Core single-sign-on pod:

```
kubectl cp /opt/ldapCA.cer arcsight-installer-xxxx/fusion-single-sign-on-
xxxxxxx-xxxx:/tmp -c fusion-single-sign-on
```

6. Log in to the into the fusion-single-sign-on:

```
kubectl exec -it fusion-single-sign-on-xxxxxxx-xxxx -n arcsight-
installer-xxxx -c fusion-single-sign-on -- sh
```

7. Navigate to the Core truststore directory:

```
cd /usr/local/tomcat/conf/default/
```

8. Install the PEM formatted CA LDAP server certificate into the fusion-single-sign-on truststore:

```
keytool -importcert -storepass $KEYSTORE_PASSWORD -destkeystore sso.bcfks
-alias ldapCA -file /tmp/okta.cert -storetype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
/usr/local/openjdk-8/jre/lib/ext/bc-fips-1.0.2.1.jar
```

9. Verify the list of certificates in the fusion-single-sign-on trustore:

```
keytool -list -v -alias ldapCA -keystore sso.bcfks -storepass $KEYSTORE_
PASSWORD
```

10. Close the Terminal session to the pod:

```
exit
```

11. Restart the Corefusion-single-sign-on:

```
kubectl delete pod -n arcsight-installer-xxxx fusion-single-sign-on-
xxxxxxx-xxxx
```

Configuring SAML Authentication

This section provides the steps to integrate SSO with an external SAML 2.0 IDP solution, such as NetIQ Advanced Authentication, Keycloak or Okta. One reason to integrate the two is to utilize a SAML provider's multi-factor authentication (MFA) or other advanced authentication capabilities.

> Core SSO and external SAML 2.0 IDP should be time-synchronized to the same NTP server. In the configuration UI, the session timeout must be set up with the same value that the external IDP has configured for user session timeouts.

- "Describing Information Regarding the Trusted Provider Metadata" below
- Configuring an External SAML Provider
- "Integrating with an External SAML Provider" on the next page

Describing Information Regarding the Trusted Provider Metadata

The metadata document for a trusted SAML provider with which a SSO defined provider interacts must be obtained in a provider-specific manner. While not all providers do so, many supply their metadata documents via URL.

After the trusted provider's metadata document (or the URL-accessible location of the document) is obtained, you must configure the SSO provider that will interact with the trusted provider's metadata.

In the document, modify the `<Metadata>` element within the `<AccessSettings>` element under either the `<TrustedIDP>` element or the `<TrustedSP>` element.

For example:

```
com.microfocus.sso.default.login.saml2.mapping-attr = email
```

The email attribute refers to the email attribute name from the SAML 2.0 IDP.

Configuring an External SAML Provider

Use the metadata URL of Core SSO to derive the specific single sign-on and single log-out URLs to configure an external SAML 2.0 IDP. These URLs include the following:

- Core metadata URL: `https://<FQDN of ArcSight Platform Virtual IP for HA or single master node>/osp/a/default/auth/saml2/spmetadata`
- Core Entity ID or Issuer: `https://<FQDN of ArcSight Platform Virtual IP for HA or single master node>/osp/a/default/auth/saml2/metadata`
- Core single sign-on: https://<FQDN of ArcSight Platform Virtual IP for HA or single master node>/osp/a/default/auth/saml2/spassertion_consumer
- Core single log-out: https://<FQDN of ArcSight Platform Virtual IP for HA or single master node>/osp/a/default/auth/saml2/spslo

> A user present in the external SAML 2.0 IDP solution must also exist in Core to proceed with integration.

Integrating with an External SAML Provider

1. On the NFS server, open the `sso-configuration.properties` file, located by default in the `<arcsight_nfs_vol_path>/sso/default` directory.

   `<arcsight_nfs_vol_path>` is the nfs volume used for OMT installation.

   For Example:

   ```
   /opt/NFS_volume/arcsight-volume/sso/default
   ```

2. Open the *sso-configuration.properties* file and add the following properties:

   ```
   com.microfocus.sso.default.login.method = saml2
   ```

   ```
   com.microfocus.sso.default.saml2.enabled = true
   ```

3. To specify the address where the IDP supplies its metadata document, complete one of the following actions:

   - Add the following property to the file:

   ```
   com.microfocus.sso.default.login.saml2.metadata-url = <IDP SAML metadata URL>
   ```

- An example of an Okta server URL could be:

```
https://<youraccount>.okta.com/app/<appid>/sso/saml/metadata
```

- An example of a Keycloak server URL could be:

```
https://<KeycloakServer>/auth/realms/<YourRealm>/protocol/saml/descriptor
```

> The IDP certificates need to be imported to the Core SSO keystore for HTTPS to work properly. See Step 5 for more details.

- Alternatively, you can convert the metadata xml file to base64 string and set the following variable:

```
com.microfocus.sso.default.login.saml2.metadata = <base64 encoded metadata
xml>
```

4. Save the changes to the `sso-configuration.properties` file.
5. (Conditional) If you specified the metadata URL in Step 3, complete the following steps to import the IDP certificate to the SSO keystore:
   a. Copy the IDP certificate to the following location.

   ```
   arcsight_nfs_vol_path/sso/default
   ```

   b. Get the pod information.

   ```
   kubectl get pods --all-namespaces | grep single-sign-on
   ```

   c. Open a terminal in the currently running pod:

   ```
   kubectl exec -it fusion-single-sign-on-xxxxxxxxxx-xxxxx -n arcsight-
   installer-xxxxx -c fusion-single-sign-on bash
   ```

   d. Import the IDP certificate:

      i.
      ```
      cd /usr/local/tomcat/conf/default/
      ```

      ii.
      ```
      keytool -importcert -storepass $KEYSTORE_PASSWORD -destkeystore \
      sso.bcfks -alias AliasName -file CertificateFileName -storetype \
      BCFKS -providerclass \
      org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider \
      -providerpath /usr/local/openjdk-8/jre/lib/ext/bc-fips-1.0.2.jar
      ```

      - `CertificateFileName` represents the name of the certificate file that you copied to <arcsight_nfs_vol_path>/sso/default/, which automatically displays in your current directory:

```
/usr/local/tomcat/conf/default/
```

- `AliasName` represents the new alias name that you want to assign to the certificate in the SSO keystore.

6. Restart the pod:
   a. Get the pod information.

   ```
   kubectl get pods --all-namespaces | grep fusion-single-sign-on
   ```

   b. Delete the current running pod.

   ```
   kubectl delete pod fusion-single-sign-on-xxxxxxxxxx-xxxxx -n arcsight-
   installer-xxxxx
   ```

7. Retrieve the Core SSO SAML service provider metadata from the server.

   ```
   https://<FQDN of ArcSight Platform Virtual IP for HA or single master
   node>/osp/a/default/auth/saml2/spmetadata
   ```

8. Use the SSO SAML service provider metadata to configure your IDP. For detailed instructions, see the IDP software documentation.
9. To establish a trust relationship between Core SSO and your IDP software, create certificates for your IDP software. For detailed instructions on how to create and import certificates in your IDP software, see the IDP software documentation.

Integrating ESM Data and Users

Core components allows you to integrate users and data from ESM. With single sign-on (SSO) supported between the two, users can easily access the ArcSight Console, ArcSight Command Center, ESM Command Center, and REST APIs with the same login.

For more information see, "Planning to Integrate Tenants from ArcSight ESM" on page 74.

Understanding How ESM Users Access Core

Rather than manually adding users to Core, we recommend you create users in ESM first, then import them into Core.

For the imported ESM users to log in to Core and be able to access ESM data, the following conditions apply:

- You must enable SSO access for ESM and Core users.
- Users must have an account in both ESM and Core.

- You must configure the **External User ID** and E-mail fields in the ESM accounts to comply with the *name@domain.com* format.

  The **External User ID** for ESM is the same as the **Core User ID**.

- Users must log in to Core with the **External User ID/Core User ID** from their ESM account.
- If your environment does not use external authentication (such as SAML or LDAP), ensure you have configured the SMTP server settings for Core. Users imported from ESM might need to set a password the first time they log in, which requires those users to initiate the Forgot Password function and receive an email notification.

Importing Users

You can import users that are already authorized. You need to have at least one role available in Core to assign to these users.

Importing ESM users puts them ALL into the preselected Core roles. You cannot downselect ESM users once you proceed. Only users with a filled e-mail address in ESM get imported.

1. In the ArcSight Console, ensure that the **External User ID/Core User ID** and E-mail fields for each account comply with the following format.

   ```
   name@domain.com
   ```

2. To log in to Core, use the following URL:

   ```
   https://<OMT_masternode_hostname>
   ```

3. Click **ADMIN** > **Account Groups** > **Import Users**.
4. Select the role that you want to assign to the imported users.
5. Ensure you have a valid ESM Root CA certificate in the **Core User Management TrustStore**.

As you add more users to ESM, you can run the import process again. Core ignores duplicates of user accounts that have been imported previously.

Describing Authentication Details

One SSO Provider (OSP) client only authentication allows ArcSight capabilities to use an existing OSP (for example, from the Platform) for authentication.

Password-based authentication requires users to enter their User ID and Password when logging in. You can select built-in authentication or external authentication, such as SAML or LDAP.

Importing Certificates

Import Root CA certificates from the Platform (Off-cloud or Cloud, for e.g. ESM or AWS) and into the **Core User Management TrustStore** for mutual authentication.

The following steps apply to import and install a Root CA certificate:

1. Export the certificate from your browser and into the fusion-user-management pod.

   ```
   kubectl cp /opt/certificates/caroot.cer arcsight-installer-xxxx/fusion-
   user-management-xxxxxxxxx-xxxxx:/tmp -c hercules-management
   ```

2. Open terminal in the currently running pod:

   ```
   kubectl exec -it fusion-user-management-xxxxxxxxx-xxxxx -n arcsight-
   installer-xxxx -c hercules-management sh
   ```

3. Change directory to where the keytool command is located:

   ```
   cd /usr/lib/jvm/zulu-8/bin
   ```

4. Install the certificate:

   ```
   ./keytool -importcert -storepass $KEYSTORE_PASSWORD -destkeystore
   /usr/local/hercules/crt/mgmtTrustStore.bcfks -alias caroot -file
   /tmp/caroot.cer -storetype BCFKS -providerclass
   org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
   /usr/lib/jvm/zulu-8/lib/ext/bc-fips-1.0.2.jar
   ```

5. Restart the fusion-user-management pod.

If an installed certificate expires, it's path changes or a fresh one is generated, you must reimport it.

AA

1. Export the certificate from your browser and into the fusion-user-management pod:

   ```
   kubectl cp /opt/AACert.cer arcsight-installer-xxxx/saasum-fusion-user-
   management-xxxxxxxxx-xxxxx:/tmp -c saasum-fusion-user-management
   ```

2. Open terminal in the currently running pod:

   ```
   kubectl exec -it saasum-fusion-user-management-xxxxxxxxx-xxxxx -n
   arcsight-installer-xxxx -c saasum-fusion-user-management sh
   ```

3. Change directory to where the keytool command is located:

   ```
   cd /usr/lib/jvm/zulu-8/bin
   ```

4. Install the certificate:

```
./keytool -importcert -storepass $KEYSTORE_PASSWORD -destkeystore
/usr/local/hercules/crt/mgmtTrustStore.bcfks -alias aas -file
/tmp/AACert.cer -storetype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
/usr/lib/jvm/zulu-8/lib/ext/bc-fips-1.0.2.jar
```

5. Restart the fusion-user-management pod.

SAML Authentication

For SAML authentication, see Configuring SAML Authentication.

LDAP Authentication

For LDAP authentication, see Configuring LDAP Authentication.

Signing the External Communication Certificate with Your Certificate Authority

At the center of the Platform is a Kubernetes cluster where communication occurs between pods within the cluster and with non-containerized ArcSight components outside of the cluster. In order to ensure secure trusted communication between pods within the cluster and components outside of the cluster, encrypted communication with client certificate authentication is configured by default.

> This page describes the approach of signing a CSR for an intermediate certificate authority generated on the ArcSight Platform. An alternative to this approach is having your PKI team provide an intermediate CA (both key and certificate) that you install into the ArcSight Platform. For more information on this alternate approach, see "Maintaining Certificates" on page 524

- "Understanding Signed Certificate Authorities" below
- "Signing the External Communication Certificate with Your Trusted Certificate Authority" on the next page
- "Restarting Pods" on page 287

Understanding Signed Certificate Authorities

During installation, three self-signed Certificate Authorities (CA) are created automatically, two for signing certificates used exclusively for pod to pod communication within the cluster (RIC

and RID CA) and the other for signing certificates for each pod that performs communication external to the cluster (RE CA). Only pods that perform external communication have a certificate that is signed by the external CA.

External cluster communication occurs not only with ArcSight components, but also with user web browsers and, in some cases, user clients of ArcSight APIs (such as REST API). By default, when the user connects to the cluster, they will be presented with a certificate that has been signed by the self-signed external CA. Since the external CA is self-signed, the user's connection will not automatically trust the certificate because it will not be verifiable using a certificate chain that is already in the user's trust store.

To give users confidence they are connecting to the trusted cluster, we recommend signing the certificates that are presented to the user with a CA that is trusted by the user's trust store. The only pods that perform external cluster communication with the user are the following (see "Understanding Labels and Pods" on page 453):

- nginx-ingress-controller - All user connections to ArcSight capability web UIs and APIs (default port 443) use this pod. This pod accepts the user's connection and then relays requests to other pods within the cluster using cluster internal communication, which utilizes the internal CA.
- OMT Management Portal - This is an administrator only portal (default port 5443) in the Platform used to manage the Kubernetes cluster and the capabilities running within it.

Signing the External Communication Certificate with Your Trusted Certificate Authority

In order to sign the external communication certificate with your trusted CA, you need to create a certificate signing request (CSR) from vault, take it to your organization, sign it, and return back signed CSR plus all the public chain of certificates used to sign it.

1. Export the following access token dependencies, which you can remove later if not needed.

```
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o json
2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n core -o json
2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-cbc -md
sha256 -a -d -pass pass:"${PASSPHRASE}")
```

2. Ask vault to generate the CSR by running the following command. (**Important:** When you execute this command, please proceed expeditiously through steps 3 and 4, as your cluster will not be able to issue external certificates while it waits for the CSR to be signed.)

```
/opt/arcsight/kubernetes/bin/vault write -tls-skip-verify -format=json \
-address=https://<FQDN>:8200 RE/intermediate/generate/internal  \
common_name="none-MF CDF RE CA on <FQDN>" \
| jq -r '.data.csr' > /tmp/pki_intermediate.csr
```

<FQDN> is the FQDN of virtual IP address (also known as the External Access Hostname) for a multi-master type of installation or for a single master/single box use the FQDN of master/node. For cloud deployments, installs use the IP address of the master accessible from the jumphost.

3. Use the CSR file to sign it with your certificate authority, and save the result into the intermediate.cert.pem.
   For a basic example with openssl:

```
openssl ca -keyfile  your-rootca-sha256.key -cert your-rootca-sha256.crt
-config  your-openssl-configuration file -extensions v3_ca -notext -md
sha256 -in /tmp/pki_intermediate.csr -out intermediate.cert.pem
```

   Make sure v3_ca extension is enabled and new certificate is useable as certificate authority on its own. Otherwise in next step you will receive a warning that given certificates is not marked for CA use.

4. Create a chain from your intermediate.cert.pem and place into it certificate authority you used to sign the intermediate certificate request. If you got more levels in certificate chain, make sure they go on after another in the file, starting first with signed CSR, later intermediate certificate autority and last be your highest root certificate autority).

```
cp intermediate.cert.pem intermediate.chain.pem
cat your-rootca-sha256.crt >> intermediate.chain.pem
```

5. Import the bundle to vault.

```
/opt/arcsight/kubernetes/bin/vault write -tls-skip-verify -format=json \
RE/intermediate/set-signed certificate=@intermediate.chain.pem
```

   If Vault returns error 400: no data found in PEM block, it means RFC in which certificate is formatted is not supported. Run "sed -i '/^$/d' intermediate.chain.pem" command and try again importing the file to vault.

6. Locate the RE_ca.crt (part of configuration map).
   a. Replace the certificate content in BEGIN and END of CERTIFICATE headers with the content of the new certificate you imported to vault (make sure you are using just signed certificate from intermediate.cert.pem, note whole chain intermediate.chain.pem).

b. Save your changes, and exit.

c. See the issue commands below.

```
kubectl edit configmap -n core public-ca-certificates
kubectl edit configmap -n arcsight-installer-xxxx public-ca-certificates
```

7. Run the following command, which displays the output including the "private_key" and "certificate" data section.

> If you need to set additional SANs (Subject Alternative Names) in the generated certificate, use following syntax: common_ name=YOUR_ EXTERNAL_ ACCESS_ HOST alt_ names=arcsight.com,pkiadmin@arcsight.com. The list of parameters accepted while requesting certificate to be generated can be found in Vault documentation - PKI engine - Generate Certificate - Parameters.

```
/opt/arcsight/kubernetes/bin/vault write -tls-skip-verify \
RE/issue/coretech common_name=YOUR_EXTERNAL_ACCESS_HOST
```

a. For creating the nginx.KEY, locate the "private_key" data section and copy all the contents from `-----BEGIN RSA PRIVATE KEY-----` until the end of `-----END RSA PRIVATE KEY-----` into the nginx.KEY file.

b. For creating the nginx.CRT, locate the "certificate" data section and copy all the contents from -----BEGIN CERTIFICATE----- until the end of -----END CERTIFICATE----- into the nginx.CRT file.

c. You can place ca_chain certificates *after* the "certificate" into nginx.CRT file with keeping the headers as well to propagate them to browser as well.

8. Use the command below to apply a new nginx key and certificates.

> The "dry-run" flag here is for creating yaml definition but not submitting it to kubernetes for creation - this part is done after pipe with apply command and namespace clarification

```
kubectl create secret generic "nginx-investigate-secret" --from-
file=tls.crt=./nginx.CRT \
--from-file=tls.key=./nginx.KEY --dry-run -o yaml \
| kubectl --namespace="arcsight-installer-xxxxx" apply -f -
```

```
kubectl create secret generic "nginx-default-secret" --from-
file=tls.crt=./nginx.CRT \
--from-file=tls.key=./nginx.KEY --dry-run -o yaml \
| kubectl --namespace="core" apply -f -
```

9. Retrieve the pod information.

```
kubectl get pods --all-namespaces | grep single-sign-on
```

10. Delete the pod to initialize it with a new certificate.

```
kubectl delete pod fusion-single-sign-on-xxxxxxxxxx-xxxxx -n arcsight-
installer-xxxxx
```

11. Retrieve the new pod names.

```
kubectl get pods --all-namespaces | grep single-sign-on
kubectl get pods --all-namespaces | grep user-management
```

12. Store root-ca and sub-root-ca in separate files then copy the certs to the new pods.

```
kubectl cp root-ca.crt arcsight-installer-xxxxx/fusion-single-sign-on-
xxxxxxxxxx-xxxxx:/tmp -c hercules-osp
kubectl cp sub-root-ca.crt arcsight-installer-xxxxx/fusion-single-sign-
on-xxxxxxxxxx-xxxxx:/tmp -c hercules-osp
kubectl cp root-ca.crt arcsight-installer-xxxxx/fusion-user-management-
xxxxxxxxxxx-xxxxx:/tmp -c hercules-user-management
kubectl cp sub-root-ca.crt arcsight-installer-xxxxx/fusion-user-
management-xxxxxxxxxxx-xxxxx:/tmp -c hercules-user-management
```

13. Launch a terminal in the currently active `single-sign-on` pod, then Import the new RE certificate and chain to `single-sign-on truststore - sso.bcfks`.

```
kubectl exec -it fusion-single-sign-on-xxxxxxxxxx-xxxxx -n arcsight-
installer-xxxxx -c hercules-osp -- bash
```

```
cd /usr/local/tomcat/conf/default/
```

```
keytool -importcert -storepass $KEYSTORE_PASSWORD -destkeystore sso.bcfks
-alias updatedreca    -file /vault-crt/trustedCAs/RE_ca.crt -storetype
BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
/usr/local/openjdk-8/jre/lib/ext/bc-fips-1.0.2.jar
```

```
keytool -importcert -storepass $KEYSTORE_PASSWORD -destkeystore sso.bcfks
-alias updatedrechain1 -file /tmp/root-ca.crt -storetype BCFKS -
providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -
providerpath /usr/local/openjdk-8/jre/lib/ext/bc-fips-1.0.2.jar
```

```
keytool -importcert -storepass $KEYSTORE_PASSWORD -destkeystore sso.bcfks
-alias updatedrechain2 -file /tmp/sub-root-ca.crt -storetype BCFKS -
providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -
providerpath /usr/local/openjdk-8/jre/lib/ext/bc-fips-1.0.2.jar
```

```
exit
```

14. Launch a terminal in the currently active `fusion-user-management` pod, then Import the chain to `fusion-user-management truststore - mgmtTrustStore.bcfks`

```
kubectl exec -it fusion-user-management-xxxxxxxxxxx-xxxxx -n arcsight-
installer-xxxxx -c hercules-user-management -- sh
```

```
cd /usr/local/hercules/crt/
```

```
keytool -importcert -storepass $KEYSTORE_PASSWORD -destkeystore
mgmtTrustStore.bcfks -alias updatedrechain1 -file /tmp/root-ca.crt -
storetype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
/usr/local/openjdk-8/jre/lib/ext/bc-fips-1.0.2.jar
```

```
keytool -importcert -storepass $KEYSTORE_PASSWORD -destkeystore
mgmtTrustStore.bcfks -alias updatedrechain2 -file /tmp/sub-root-ca.crt -
storetype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
/usr/local/openjdk-8/jre/lib/ext/bc-fips-1.0.2.jar
```

```
exit
```

15. Restart the `fusion-single-sign-on-xxxxx` and `fusion-user-management-xxxxx` pods to get them initialized with the new ceritificates.

```
kubectl get pods --all-namespaces | grep -E "single-sign-on|user-
management"
```

```
kubectl delete pod -n arcsight-installer-xxxxx fusion-single-sign-on-
xxxxxxxxxx-xxxxx fusion-user-management-xxxxxxxxxxx-xxxxx
```

16. Make sure to import the certificate to your browser's trust store for proper functionality of both **Management** and Core portals.

Restarting Pods

Pods of deployed capabilities that rely on the external certificates for communication will continue to use the existing certificate until they are restarted.

To restart pods:

1. The pods need to be gently scaled to 0 and later scaled back to original values. E.g. for transformation-hub, note the current amount of replicas by issuing (where here and now on xxxxx should correspond to unique suffix of your deployment):

```
kubectl get replicaset -n arcsight-installer-xxxxx
```

> The unique name of th-schemaregistry-xxxxxx and th-web-service-xxxxxx replicasets and amount of replicas you are currently running for them.

2. Scale them down to zero, by commands below. Make sure to repeat above commands to confirm they were scaled to zero and not running in terminating state.

```
kubectl scale --replicas=0 statefulset/th-kafka -n arcsight-installer-
xxxxx
kubectl scale --replicas=0 replicaset/th-schemaregistry-xxxxxx -n
arcsight-installer-xxxxx
kubectl scale --replicas=0 replicaset/th-web-service-xxxxxx -n arcsight-
installer-xxxxx
```

3. You can repeat commands afterward and increase replicas value to the normal state from before the procedure. Other capabilities also have pods that rely on certificates:

```
kubectl scale --replicas=x replicaset/itom-data-ingestion-loader-
xxxxxxxxx -n arcsight-installer-xxxxx
kubectl scale --replicas=x replicaset/fusion-db-search-engine-xxx -n
arcsight-installer-xxxxx
```

Apply the mentioned scaling procedure to all in exactly the same way.

Enabling SSO with ESM

You must configure ESM to use **OSP Client Only Authentication**. If your ESM environment currently uses external client authentication, you must delegate the Core SSO provider to connect to the external authentication client.

If you do not use external authentication, see "Connecting to Your SMTP Server" on page 270 for information on supporting forgotten password activity.

- "Configuring SSO with ESM" below
- "Importing the Core Certificate to the Console Keystore" on page 290
- "Configuring the SSO Proxy" on page 290

Configuring SSO with ESM

This procedure assumes you have ESM installed or upgraded.

1. Change the authentication settings for the ESM Manager service:
   a. On the ESM server, start the configuration wizard by changing to the following directory and entering the following.
      Directory

      ```
      /opt/arcsight/manager/bin/
      ```

      Command

      ```
      arcsight managersetup -i console
      ```

   b. Advance through the wizard until you reach the authentication settings.
   c. Select **OSP Client Only Authentication**, then click **Next**.
   d. To specify the host and port for the OSP server, use the following format:

      ```
      domain_name:port
      ```

      For example, Core by default installs OSP on port 443. So, when you are using Core, specify the format as:

      ```
      <Core host>:443
      ```

   e. Specify a **Tenant Name for OSP**. If you are using a typical installer for Core, specify `default`.
   f. Click **Next** until you complete your changes in the wizard.
   g. Restart the ESM Manager service using the following commands:

      ```
      /etc/init.d/arcsight_services stop manager
      ```

      ```
      /etc/init.d/arcsight_services start manager
      ```

2. Change the authentication settings for the ArcSight Console (the Console):
   a. From the Console's `/bin` directory, specify one of the following commands:
      Windows

      ```
      arcsight.bat consolesetup
      ```

      Linux

      ```
      ./arcsight consolesetup
      ```

   b. Advance through the wizard until you reach the authentication settings.
   c. Select **OSP Client Only Authentication**.
   d. Click **Next** until you complete your changes in the wizard.

Importing the Core Certificate to the Console Keystore

1. Obtain the Core CA certificate in Base-64 encoded X.509 format.
2. From the Console's `/bin` directory, specify one of the following commands. Replace `<Core CA certificate file path>` and `<alias_name>` with the correct information for your system.

   Windows

   ```
   arcsight.bat keytool -store clientcerts -import -file  <Core CA certificate file path> -alias <alias_name>
   ```

   Linux

   ```
   ./arcsight keytool -store clientcerts -import -file  <Core CA certificate file path> -alias <alias_name>
   ```

3. Ensure that when you run the keytool command that the `JAVA_HOME` value listed in the output of the command is pointing to the ArcSight JRE location of your Console to ensure the certificate is imported into the correct keystore.

Configuring the SSO Proxy

If your ArcSight Platform installation is running as a cluster or using a VIP for access, you must configure the SSO proxy settings before ESM and other external clients can access Core.

1. Log in to the OMT server and navigate to the SSO default configuration folder:

   ```
   <arcsight_nfs_vol_path>/sso/default/WEB-INF/conf/current/default
   ```

   Replace `<arcsight_nfs_vol_path>` with the NFS volume used for your OMT installation. For example: `/opt/NFS_volume/arcsight-volume`

2. Open the `tenantcfg.xml` file and locate the `HTTPInterface` sections:

   ```
   <HTTPInterface
          id="default-http-domain"
          displayName="Hercules HTTP"
          path="/osp"
          anyLocalInterface="true"
          proxyPort="443"
          proxyTls="true"
   ```

```
      proxyDomain="${HTTP_INTERFACE_DOMAIN}"
      />
```

3. Update the `tenantcfg.xml` file and and modify the proxyDomain line as shown in the following example.
   Replace `<your.domain.name>` with your VIP or the FQDN of the master node if you are not using a VIP.

```
<HTTPInterface
       id="default-http-domain"
       displayName="Hercules HTTP"
       path="/osp"
       anyLocalInterface="true"
       proxyPort="443"
       proxyTls="true"
       proxyDomain="<your.domain.name>"
       />
```

4. Save the `tenantcfg.xml` file.
5. Restart the fusion-single-sign-on pod.
   a. Get the fusion-single-sign-on pod information:

```
kubectl get pods --all-namespaces | grep single-sign
```

   b. Restart the fusion-single-sign-on by deleting the currently running pod:

```
kubectl delete pod fusion-single-sign-on-xxxxxxxxxx-xxxxx -n arcsight-
installer-xxxxx
```

Integrating Data from ESM

To view ESM data in the Dashboard, update the settings in the OMT Management Portal. Core components manage the Dashboard functions.

1. Open a new tab in a supported web browser. For a list of supported web browsers, see *Technical Requirements for ArcSight Platform 24.2*.
2. Specify the URL for the OMT Management Portal:

```
https://<OMT_masternode_hostname>:5443
```

   Use the fully qualified domain name of the host that you specified in the Connection step during the OMT configuration. Usually, this is the master node's FQDN.
3. Log in to the OMT Management Portal with the credentials of the administrative user that you provided during installation.

4. Select **Reconfigure**.
5. On the **Configuration** page, select **Core**.
6. In the **ArcSight ESM Host Configuration** section, complete the following steps:
   a. For **ESM host**, specify the fully-qualified host name or IP address of the server that hosts ESM.
   b. For **ESM port**, specify the port associated with the **ESM host**. The default value is 8443.

Configuring ESM as a Transformation Hub Producer in Distributed Correlation Mode

Distributed event forwarding is available when ESM is installed in distributed correlation mode. The feature allows you to forward events from ESM to Transformation Hub at a high rate. Distributed event forwarding leverages the distributed infrastructure of ESM to allow ESM to spread the work of event forwarding across the cluster, similar to how ESM distributes event correlation. This allows event forwarding to scale horizontally.

Events that ESM forwards to Transformation Hub can subsequently be read by another ESM instance or multiple ESM instances. Those ESM instances do not have to be installed in distributed correlation mode in order to read events from Transformation Hub.

If you need to forward events from ESM to Transformation Hub at a high rate (generally higher than 10K events per second) OpenText recommends that you use ESM in distributed correlation mode and use distributed event forwarding.

Note: Distributed Forwarding does not support SSL client- side authentication with Transformation Hub.

Distributed event forwarding requires the following:

- CA certificate of the Transformation Hub cluster
- ESM filter that determines which events to forward

  You can create a filter or use one that is installed with ESM.
- List of broker socket addresses (in the form host:port) of the Transformation Hub cluster to which you want to forward events

  The Transformation Hub documentation refers to these as "worker nodes."
- Transformation Hub topic name to which you want to publish events

Note: Perform the configuration steps that are described below on the persistor node of the ESM cluster.

Obtaining and Importing the Transformation Hub CA Certificate

Transformation Hub maintains its own certificate authority (CA) to issue certificates for individual nodes in the Transformation Hub cluster. ESM needs that CA certificate in its truststore so that it will trust connections to Transformation Hub. For information about obtaining the certificate, see the information about viewing and changing the certificate authority. You might need to contact the Transformation Hub administrator to obtain the CA certificate if you do not have sufficient privileges to access the Transformation Hub cluster.

If you have root access to the Transformation Hub cluster (version 3.x or later), you can obtain the CA certificate as follows:

```
master=<master node host name or IP address>
```

```
ssh root@$master env K8S_HOME=/opt/arcsight/kubernetes
/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh >
/opt/arcsight/manager/th.ca.crt
```

The command copies the CA certificate to the file `/opt/arcsight/manager/th.ca.crt`. You must then import that certificate into the ESM cluster using the certadmin tool in the *ESM Administrator's Guide*.

To import the Transformation Hub CA certificate to ESM:

1. Run the following command to ensure that the ESM cluster is running:

   ```
   /etc/init.d/arcsight_services status
   ```

   If it is not, run the following command:

   ```
   /etc/init.d/arcsight_services start
   ```

   Wait for the cluster to completely start.
2. Import the Transformation Hub CA certificate:

   ```
   bin/arcsight certadmin -importcert /opt/arcsight/manager/th.ca.crt
   ```

   Note the alias that is reported in the output.
3. Run the following command and verify that the alias that was reported in the output from the previous command is listed as an approved certificate:

```
bin/arcsight certadmin -list approved
```

If the alias is not listed, re-import the Transformation Hub CA certificate.

Configuring the Filter and Destination

After you import the Transformation Hub CA certificate to ESM, configure a filter and the destination properties. You specify the destination properties in a file that is used as input to the configure-event-forwarding command, as seen in the *ESM Administrator's Guide*.

To configure the filter and destination:

1. Create a filter to select the events that you want to forward or use a filter that is installed with ESM.

   For more information about creating event filters, see the information about filtering events in the ArcSight Console User's Guide.

2. Edit `forwarding.properties` in `/opt/arcsight/manager/config/` with the following information:

   - Name of the filter that you want to use to select the events to be forwarded.
   - Comma separated list of socket addresses of the worker nodes of the Transformation Hub cluster. Each socket address should be in the form host:port.

   > **Note:** Optionally, you can copy `forwarding.properties` to a different file and edit that file. If so, you must specify the file name when running the `configure-event-forwarding` utility. Otherwise, `configure- event- forwarding` will read the default `forwarding.properties` file.

   The properties file is in the following format:

```
# Provide the filter that determines which events to forward.
# The filter may be specified by ID or by Name.
# If name is used then it can be the simple name or the fully qualified URI.
#
# e.g. filterID=2jq5Og-sAABCAFyopCdLChw==
# or
# filterName=Non-ArcSight Internal Events
# or
# filterName=/All Filters/ArcSight System/Event Types/Non-ArcSight Internal Events
filterName=Non-ArcSight Internal Events
```

```
# List the socket addresses of the destination worker nodes
hostPortCSV=host1.example.com:9093,host2.example.com:9093,host3.example.com:9093
# Specify the destination topic name
topicName=esm-forwarded-events
```

3. Run the following command to validate the settings in the properties file:

```
bin/arcsight configure-event-forwarding -validate <file>
```

> **Note:** If you do not specify a file name, `<ARCSIGHT_HOME>/config/forwarding.properties` is the default file.

The command output indicates whether the filter and connections to the forwarding destination are valid.

4. If the settings in `forwarding.properties` are valid, run the following command to set the configuration and save it in the information repository:

```
bin/arcsight configure-event-forwarding -commit <file>
```

> **Note:** If you do not specify a file name, `<ARCSIGHT_HOME>/config/forwarding.properties` is the default file.

5. When you are ready to actively filter and forward events, run the following command to enable event forwarding:

```
bin/arcsight configure-event-forwarding -enable
```

To disable event forwarding, run the following command:

```
bin/arcsight configure-event-forwarding -disable
```

> **Note:** ESM does not cache events when you disable distributed event forwarding. Events that ESM ingests while forwarding is disabled will not be forwarded, even when you subsequently enable forwarding. Events that ESM ingests after you enable forwarding will be forwarded.

6. To view the current settings for distributed event forwarding, including whether it is enabled or disabled, run the following command:

```
bin/arcsight configure-event-forwarding -print
```

Modifying the Filter and Configuration

The properties file is only used to validate and commit the configuration. The information repository stores the configuration itself. If you need to modify the configuration, it is not sufficient to simply edit the file. You must edit the file and then run `bin/arcsight configure-event-forwarding -validate <file>` and `bin/arcsight configure-event-forwarding -commit <file>` again to overwrite the old configuration. It is not necessary to stop and start the ESM cluster to modify the configuration. Distributed event forwarding will automatically detect the updated configuration. You can run `bin/arcsight configure-event-forwarding -print` to view the configuration that is currently in use.

If you modify the filter that distributed event forwarding uses, event forwarding automatically detects the updated filter and begins using it to select events for forwarding as soon as you save the filter update. Therefore, be cautious when modifying the filter.

Instead of modifying the filter, you can create a new filter and test it before you commit to using it. When you are sure that the filter is correct, specify the new filter in the properties file, then run `bin/arcsight configure-event-forwarding -validate <file>` and `bin/arcsight configure-event-forwarding -commit <file>` to apply the change to the current configuration.

Troubleshooting Event Forwarding Throughput

The maximum rate at which events can be forwarded depends on many factors, including the following:

- Amount of other work that distributed correlation must do to support all of the rules, data monitors, and other content that you have defined
- File input/output contention
- CPU contention
- Memory contention
- Network contention, especially the network between distributed correlation nodes and the Transformation Hub worker nodes
- Maximum rate at which Transformation Hub can accept messages

It might be that the maximum throughput of event forwarding is not enough to support the number of events that need to be forwarded in a given period of time. When that happens, events yet to be forwarded will build up inside message bus. This buildup of unforwarded events is called **lag**. If the lag is too high, the ESM cluster will stop ingesting events to reduce the lag. When this happens it is called **backpressure**.

The Acceptable Lag value in the Cluster View dashboard of Command Center defines the amount of lag that can occur before backpressure is applied. For more information, see the information about using the Cluster View dashboard in the ArcSight Command Center User's Guide.

Distributed event forwarding leverages the ESM distributed infrastructure to gain horizontal scalability. The correlator does the work of event forwarding. You might be able to add event forwarding throughput by adding correlator(s), either on an existing node or on a new distributed correlation node. However, this will only increase throughput if it is the correlators that are causing the bottleneck (for example, because of CPU or memory limitations). If the network or Transformation Hub is causing the bottleneck, adding correlators might not have any effect. For information about adding correlators, see Adding Correlators and Aggregators.

Optionally, you can disable backpressure that might occur as a result of unforwarded events, but you should only use this option if you accept that some events might never be forwarded. To disable backpressure, run the following command:

```
bin/arcsight configure-event-forwarding -backpressure disable
```

Note: When you disable backpressure, ESM will not slow the ingestion of events. If event forwarding cannot keep up with the rate at which events are being filtered for forwarding, the lag might build up inside the message bus to the point where the oldest yet-to-be-forwarded events are dropped and therefore not forwarded at all.

To enable backpressure, run the following command:

```
bin/arcsight configure-event-forwarding -backpressure enable
```

Configuring ESM as a Transformation Hub Consumer

Note: For cloud Transformation Hub, you must complete the configuration procedures detailed in:

- Completing Integration with AWS Transformation Hub

before you perform the procedures in this section.

This section describes how to configure ESM to consume events from Transformation Hub in both FIPS and non-FIPS mode, including setting up SSL client-side authentication in both modes:

- Configuring ESM as a Transformation Hub Consumer – Non-FIPS Mode
- Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - Non-FIPS Mode

- Configuring ESM as a Transformation Hub Consumer - FIPS Mode (Server Authentication Only)
- Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - FIPS Mode

For ESM in distributed correlation mode, you can also configure ESM to send events to Transformation Hub. For more information, see Configuring ESM as a Transformation Hub Producer in Distributed Correlation Mode.

Configuring ESM as a Transformation Hub Consumer – Non-FIPS Mode

This procedure uses the CA certificate that is embedded in Transformation Hub.

To complete the configuration, complete the following tasks:

1. Obtain the Transformation Hub CA certificate.
2. On the ESM server, configure ESM to consume from Transformation Hub.

The steps for each task are outlined below.

Obtaining the Transformation Hub CA Certificate

Transformation Hub maintains its own certificate authority (CA) to issue certificates for individual nodes in the Transformation Hub cluster. ESM needs that CA certificate in its truststore so that it will trust connections to Transformation Hub. For information about obtaining the certificate, see the information about viewing and changing the certificate authority. You might need to contact the Transformation Hub administrator to obtain the CA certificate if you do not have sufficient privileges to access the Transformation Hub cluster.

If you have `root` access to the Transformation Hub cluster (version 3.x or later), you can obtain the CA certificate as follows:

```
master=<master node host name or IP address>
```

```
ssh root@$master env K8S_HOME=/opt/arcsight/kubernetes
/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh >
/opt/arcsight/manager/th.ca.crt
```

The command copies the CA certificate to the file `/opt/arcsight/manager/th.ca.crt`.

Configuring ESM to Consume from Transformation Hub

1. Run the following command:

```
/opt/arcsight/manager/bin/arcsight managersetup -i console
```

2. In the wizard, press **Enter** until the wizard asks whether you want to read events from Transformation Hub. Select **Yes**, then provide the following information:

   a. Host name and port information for the worker nodes in Transformation Hub. Use a comma-separated list (for example: <host>:<port>,<host>:<port>) and specify the FQDN of the worker nodes.

   > **Note:** You must specify the host name and *not* the IP address.
   >
   > Transformation Hub can only accept IPv4 connections from ESM.
   >
   > If the Kafka cluster is configured to use SASL/PLAIN authentication, ensure that you specify the port configured in the cluster for the SASL_SSL listener.

   b. Topics in Transformation Hub from which you want to read. These topics determine the data source.

   > **Note:** You can specify up to 25 topics using a comma-separated list (for example: topic1,topic2). ESM will read Avro-format events from any topic where the name contains "avro" in lower case. For example, `th-arcsight-avro`.

   c. Path to the Transformation Hub root certificate (`/opt/arcsight/manager/th.ca.crt`).

   d. Leave the authentication type as None.

   e. Leave the user name and password as empty.

   f. If you specified an Avro topic, specify the host name and port for connecting to the Schema Registry in the format <host name:port>.

   > **Note:** The default port for connecting to the Schema Registry is 32081.

   Transformation Hub runs a Confluent Schema Registry that producers and consumers use to manage compatibility of Avro-format events.

   The wizard uses this information to connect to the Schema Registry, read the Avro schemas for the Avro topic that you specified, and verify that the topic contains Avro events that are compatible with ESM. If ESM cannot retrieve the Avro schemas for the Avro topic that you specified and compare it to the event schema that is packaged with ESM, or if incompatible schemas are detected, the wizard generates warning messages

but allows you to continue. In some cases, you might already know that Transformation Hub will use a compatible schema when the Manager is running.

g. If you choose to configure the Forwarding Connector to forward CEF events to Transformation Hub and then configure Transformation Hub to filter Avro events, use filters to ensure that ESM does not receive duplicate events. You might want to use filters to accomplish the following:

- Filter out desired events from Connectors so that ESM does not process them.
- Filter out ESM's correlation events that were forwarded (CEF events that the Forwarding Connector sent to `th-cef`) so that ESM does not re-process its own events.

  If you do *not* configure filtering, ESM must consume from the `th-arcsight-avro` topic. If you configure filtering, ESM must consume from the `mf-event-avro-esmfiltered` topic. For more information, see configuring filters and local and global event enrichment.

After providing the information, specify **Yes** and complete the remaining sections of the wizard.

3. After you complete the wizard, restart the Manager services:

In compact mode:

```
/etc/init.d/arcsight_services stop manager
```

```
/etc/init.d/arcsight_services start manager
```

In distributed mode:

```
/etc/init.d/arcsight_services stop all
```

```
/etc/init.d/arcsight_services start all
```

4. Verify that the connection was successful:

```
grep -rnw '/opt/arcsight/var/logs/manager/' -e 'Transformation Hub
service is initialized' -e 'Started kafka readers'
```

The output should be similar to the following:

```
/opt/arcsight/var/logs/manager/default/server.std.log:5036:2021-07-13
09:51:36 =====> Transformation Hub service is initialized (49 s) <=====
/opt/arcsight/var/logs/manager/default/server.log:11664:[2021-07-13
09:51:36,656][INFO ][default.com.arcsight.common.messaging.events.aa]
Started kafka readers in PT0.115S
```

```
/opt/arcsight/var/logs/manager/default/server.log:11665:[2021-07-13
09:51:36,657][INFO ][default.com.arcsight.server.NGServer] Transformation
Hub service is initialized (49 s)
```

Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - Non-FIPS Mode

ArcSight Platform maintains its own certificate authority (CA) to issue certificates for individual nodes in the Transformation Hub cluster and external communication. ESM needs the signed certificates in its truststore so that it will trust connections to the ArcSight Platform and Transformation Hub. You might need to contact the ArcSight Platform administrator to obtain the signed certificates if you do not have sufficient privileges to access them and run the necessary commands.

> **Note:** When configuring Transformation Hub access, you must specify the FQDN of the ArcSight Platform virtual IP for HA or single master node and *not* the IP address.

To complete the configuration, complete the following tasks:

- Enable client-side authentication between Transformation Hub and ESM
- Configure ESM to consume from Transformation Hub.

Enabling Client-side Authentication Between Transformation Hub and ESM:

1. Verify that Transformation Hub is functional and that client authentication is configured.
2. As user `arcsight`, stop the ArcSight Manager:

   ```
   /etc/init.d/arcsight_services stop manager
   ```

3. If `/opt/arcsight/manager/config/client.properties` does not exist, create it using an editor of your choice.
4. Change the store password for the keystore, `keystore.client`, which has an empty password by default. This empty password interferes with the certificate import:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -storepasswd
   -storepass ""
   ```

5. Run the following command to update the empty password of the generated key `services-cn` in the keystore to be the same password as that of the keystore itself. When prompted, specify the same password that you entered for the store password:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -keypasswd -
keypass "" -alias services-cn
```

6. Run the following command to update the password in `config/client.properties`:

```
/opt/arcsight/manager/bin/arcsight changepassword -f
config/client.properties -p ssl.keystore.password
```

7. Generate the keypair and certificate signing request (`.csr`) file. When generating the keypair, specify the fully qualified domain name of the ArcSight Manager host as the common name (CN) for the certificate.

   Run the following commands:

```
export COMMON_NAME=<your ESM host's fully qualified domain name>
```

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -genkeypair
-dname "cn=${COMMON_NAME}, ou=<your organization>, o=<your company>,
c=<your country>" -keyalg rsa -keysize 2048 -alias ebkey -startdate -1d -
validity 366
```

```
/opt/arcsight/manager/bin/arcsight keytool -certreq -store clientkeys -
alias ebkey -file  ${COMMON_NAME}.csr
```

   where `${COMMON_NAME}.csr` is the output file where the `.csr` is stored.

8. To sign the ESM certificate signing request, perform the following steps in the ArcSight Platform. For a cloud deployment, perform the steps on the Bastion host.

   a. Create a temporary folder to store the generated certificates:

```
mkdir –m 700 /tmp/esm
```

   b. Move the certificate signing request (`.csr`) file from the ESM host to the temporary folder that you created.

   c. Set the environment variables:

```
export CA_CERT=re_ca.cert.pem
```

```
export COMMON_NAME=<your ESM host's fully qualified domain name>
```

```
export TH=<FQDN of the ArcSight Platform virtual IP for HA or single
master node>_<Kafka TLS-enabled port>
```

   Note: For `COMMON_NAME`, use the same host FQDN as you used for the ESM client key pair.

d. Run the following commands to sign the ESM certificate signing request:

```
cd /tmp/esm
```

```
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o
json 2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n
core -o json 2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-
cbc -md sha256 -a -d -pass pass:"${PASSPHRASE}")
```

```
export CSR=$(cat ${COMMON_NAME}.csr)
```

```
WRITE_RESPONSE=$(kubectl exec -it -n core ${VAULT_POD} -c vault --
bash -c "VAULT_TOKEN=$VAULT_TOKEN vault write -tls-skip-verify -
format=json RE/sign/coretech csr=\"${CSR}\"") && \
echo "$WRITE_RESPONSE" | jq -r ".data | .certificate" > ${COMMON_
NAME}.signed.crt && \
echo "$WRITE_RESPONSE" | jq -r ".data | .issuing_ca" > ${COMMON_
NAME}.issue_ca.crt && \
echo "$WRITE_RESPONSE" | jq -r ".data | .certificate, if .ca_chain
then .ca_chain[] else .issuing_ca end" > ${COMMON_
NAME}.signed.cert.with.ca.crt
```

The signed certificate is in the file `${COMMON_NAME}.signed.crt`. The issuing CA is in the file `${COMMON_NAME}.issue_ca.crt`. The signed certificate with the CA chain is in the file `${COMMON_NAME}.signed.cert.with.ca.crt`.

9. Retrieve the RE certificates:

   For a cloud deployment:

```
cd <path to OMT installer>/cdf-deployer/scripts/
```

```
./cdf-updateRE.sh > /tmp/esm/${CA_CERT}
```

10. Copy the following files from the Transformation Hub `/tmp/esm` folder to an ESM host folder (for example, `/opt/arcsight/tmp`):

    `/tmp/esm/${COMMON_NAME}.signed.cert.with.ca.crt`

    `/tmp/esm/${CA_CERT}`

    Remove the files from `/tmp/esm` after you copy them.

11. On the ESM server, import the RE certificate from file ${CA_CERT} into the ESM client truststore:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientcerts -alias
<alias for the certificate> -importcert -file <absolute path to
certificate file>
```

For example:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientcerts -alias
thcert -importcert -file /opt/arcsight/tmp/re_ca.cert.pem
```

> **Note:** You might receive the following message:
>
> ```
> Certificate already exists in keystore under alias <alias1>
> Do you still want to add it? [no]:
> ```
>
> It is not necessary to add an existing certificate.

12. On the ESM server, run the following command to import the signed certificate:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -alias
<alias for the key> -importcert -file <path to signed cert> -trustcacerts
```

For example:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -alias ebkey
-importcert -file /opt/arcsight/tmp/${COMMON_NAME}.signed.cert.with.ca.crt
–trustcacerts
```

> **Note:** You might see the following warning:
>
> ```
> ...
> Top-level certificate in reply:
> ...
> ... is not trusted. Install reply anyway? [no]:
> ```
>
> This is because the root certificate of the RE CA is not in the ESM truststore. This does not affect the functionality of ESM. Enter **yes** to allow the new certificate to be imported.

Configuring ESM to Consume from Transformation Hub

1. Run the following command:

```
/opt/arcsight/manager/bin/arcsight managersetup -i console
```

2. In the wizard, press **Enter** until the wizard asks whether you want to read events from Transformation Hub. Select **Yes**, then provide the following information:
   a. Host name and port information for the worker nodes in Transformation Hub. Use a comma-separated list (for example: <host>:<port>,<host>:<port>) and specify the

FQDN of the worker nodes.

> **Note:** You must specify the host name and *not* the IP address.
>
> Transformation Hub can only accept IPv4 connections from ESM.
>
> If the Kafka cluster is configured to use SASL/PLAIN authentication, ensure that you specify the port configured in the cluster for the SASL_SSL listener.

b. Topics in Transformation Hub from which you want to read. These topics determine the data source.

> **Note:** You can specify up to 25 topics using a comma-separated list (for example: topic1,topic2). ESM will read Avro-format events from any topic where the name contains "avro" in lower case. For example, `th-arcsight-avro`.

c. Leave the path to the Transformation Hub root certificate empty, as you already imported the certificates.

d. Leave the authentication type as None.

e. Leave the user name and password empty.

f. If you specified an Avro topic, specify the host name and port for connecting to the Schema Registry in the format <FQDN of the ArcSight Platform virtual IP for HA or single master node:port>.

> **Note:** The default port for connecting to the Schema Registry is 32081.

Transformation Hub runs a Confluent Schema Registry that producers and consumers use to manage compatibility of Avro-format events.

The wizard uses this information to connect to the Schema Registry, read the Avro schemas for the Avro topic that you specified, and verify that the topic contains Avro events that are compatible with ESM. If ESM cannot retrieve the Avro schemas for the Avro topic that you specified and compare it to the event schema that is packaged with ESM, or if incompatible schemas are detected, the wizard generates warning messages but allows you to continue. In some cases, you might already know that Transformation Hub will use a compatible schema when the Manager is running.

g. If you choose to configure the Forwarding Connector to forward CEF events to Transformation Hub and then configure Transformation Hub to filter Avro events, use filters to ensure that ESM does not receive duplicate events. You might want to use filters to accomplish the following:

- Filter out desired events from Connectors so that ESM does not process them.
- Filter out ESM's correlation events that were forwarded (CEF events that the Forwarding Connector sent to `th-cef`) so that ESM does not re-process its own

events.

If you do *not* configure filtering, ESM must consume from the `th-arcsight-avro` topic. If you configure filtering, ESM must consume from the `mf-event-avro-esmfiltered` topic. For more information, see configuring filters and local and global event enrichment.

After providing the information, specify **Yes** and complete the remaining sections of the wizard.

3. Start the ArcSight Manager:

   In compact mode:

   ```
   /etc/init.d/arcsight_services start manager
   ```

   In distributed mode:

   ```
   /etc/init.d/arcsight_services stop all
   ```

   ```
   /etc/init.d/arcsight_services start all
   ```

   Ensure that all services started:

   ```
   /etc/init.d/arcsight_services status
   ```

4. Verify that the connection was successful:

   ```
   grep -rnw '/opt/arcsight/var/logs/manager/' -e 'Transformation Hub
   service is initialized' -e 'Started kafka readers'
   ```

   The output should be similar to the following:

   ```
   /opt/arcsight/var/logs/manager/default/server.std.log:5036:2021-07-13
   09:51:36 =====> Transformation Hub service is initialized (49 s) <=====
   /opt/arcsight/var/logs/manager/default/server.log:11664:[2021-07-13
   09:51:36,656][INFO ][default.com.arcsight.common.messaging.events.aa]
   Started kafka readers in PT0.115S
   /opt/arcsight/var/logs/manager/default/server.log:11665:[2021-07-13
   09:51:36,657][INFO ][default.com.arcsight.server.NGServer] Transformation
   Hub service is initialized (49 s)
   ```

Configuring ESM as a Transformation Hub Consumer - FIPS Mode (Server Authentication Only)

This section describes how to configure ESM to access Transformation Hub when FIPS mode is enabled. FIPS 140-2 is the only supported FIPS mode.

To configure ESM access to Transformation Hub in FIPS Mode:

1. As user `arcsight`, stop the ArcSight Manager:

```
/etc/init.d/arcsight_services stop manager
```

2. From the Transformation Hub server, copy the certificate from `/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/ca.crt` to a location on the ESM server.
3. Use the `keytool` command to import the root CA certificate into the ESM client truststore:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert
-file <absolute path to certificate file> -alias <alias for the
certificate>
```

   For example:

   `/opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert -file /tmp/ca.crt -alias alias1`

4. As user `arcsight`, run the following command from the `/opt/arcsight/manager/bin` directory to start the `managersetup` wizard:

```
./arcsight managersetup -i console
```

5. Provide the following information:

   Note: You do not need to provide the path to the Transformation Hub root certificate, as it has already been imported.

   a. Specify the host name and port information for the nodes in Transformation Hub. Include the host and port information for all nodes and not just the master node. Use a comma-separated list (for example: <host>:<port>,<host>:<port>).

      Note: You must specify the host name and *not* the IP address.

      Transformation Hub can only accept IPv4 connections from ESM.

      If the Kafka cluster is configured to use SASL/PLAIN authentication, ensure that you specify the port configured in the cluster for the SASL_SSL listener.

   b. Specify the topics in Transformation Hub from which you want to read. These topics determine the data source.

      Note: You can specify up to 25 topics using a comma-separated list (for example: topic1,topic2). ESM will read Avro-format events from any topic where the name contains "avro" in lower case. For example, `th-arcsight-avro`.

c. Leave the authentication type as None.

d. Leave the user name and password as empty.

e. If you specified an Avro topic, specify the host name and port for connecting to the Schema Registry in the format <host name:port>.

> **Note:** The default port for connecting to the Schema Registry is 32081.

Transformation Hub runs a Confluent Schema Registry that producers and consumers use to manage compatibility of Avro-format events.

The wizard uses this information to connect to the Schema Registry, read the Avro schemas for the Avro topics that you specified, and verify that the topics contain Avro events that are compatible with ESM. If ESM cannot retrieve the Avro schemas for the Avro topics that you specified and compare them to the schema that is packaged with ESM, or if incompatible schemas are detected, the wizard generates warning messages but allows you to continue. In some cases, you might already know that Transformation Hub will use a compatible schema when the Manager is running.

f. If you choose to configure the Forwarding Connector to forward CEF events to Transformation Hub and then configure Transformation Hub to filter Avro events, use filters to ensure that ESM does not receive duplicate events. You might want to use filters to accomplish the following:

- Filter out desired events from Connectors so that ESM does not process them
- Filter out ESM's correlation events that were forwarded (CEF events that the Forwarding Connector sent to `th-cef`) so that ESM does not re-process its own events.

If you do *not* configure filtering, ESM must consume from the `th-arcsight-avro` topic. If you configure filtering, ESM must consume from the `mf-event-avro-esmfiltered` topic. For more information, see configuring filters and local and global event enrichment.

6. Advance through the wizard and complete the configuration.

7. As user `arcsight`, restart the ArcSight Manager:

In compact mode:

```
/etc/init.d/arcsight_services start manager
```

In distributed mode:

```
/etc/init.d/arcsight_services stop all
```

```
/etc/init.d/arcsight_services start all
```

8. Verify that the connection was successful:

```
grep -rnw '/opt/arcsight/var/logs/manager/' -e 'Transformation Hub
service is initialized' -e 'Started kafka readers'
```

The output should be similar to the following:

```
/opt/arcsight/var/logs/manager/default/server.std.log:5036:2021-07-13
09:51:36 =====> Transformation Hub service is initialized (49 s) <=====
/opt/arcsight/var/logs/manager/default/server.log:11664:[2021-07-13
09:51:36,656][INFO ][default.com.arcsight.common.messaging.events.aa]
Started kafka readers in PT0.115S
/opt/arcsight/var/logs/manager/default/server.log:11665:[2021-07-13
09:51:36,657][INFO ][default.com.arcsight.server.NGServer] Transformation
Hub service is initialized (49 s)
```

Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - FIPS Mode

ArcSight Platform maintains its own certificate authority (CA) to issue certificates for individual nodes in the Transformation Hub cluster and external communication. ESM needs the signed certificates in its truststore so that it will trust connections to the ArcSight Platform and Transformation Hub. You might need to contact the ArcSight Platform administrator to obtain the signed certificates if you do not have sufficient privileges to access them and run the necessary commands.

Note: When configuring Transformation Hub access, you must specify the FQDN of the ArcSight Platform virtual IP for HA or single master node and *not* the IP address.

To complete the configuration, complete the following tasks:

- Enable client-side authentication between Transformation Hub and ESM
- Configure ESM to consume from Transformation Hub.

Enabling Client-side Authentication Between Transformation Hub and ESM:

1. Verify that Transformation Hub is functional and that client authentication is configured.
2. As user `arcsight`, stop the ArcSight Manager:

```
/etc/init.d/arcsight_services stop manager
```

3. Generate the keypair and certificate signing request (`.csr`) file. When generating the keypair, specify the fully qualified domain name of the ArcSight Manager host as the common name (CN) for the certificate.

   Run the following commands:

```
export COMMON_NAME=<your ESM host's fully qualified domain name>
```

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -genkeypair
-dname "cn=${COMMON_NAME}, ou=<your organization>, o=<your company>,
c=<your country>" -keyalg rsa -keysize 2048 -alias ebkey -startdate -1d -
validity 366
```

```
/opt/arcsight/manager/bin/arcsight keytool -certreq -store clientkeys -
alias ebkey -file  ${COMMON_NAME}.csr
```

   where `${COMMON_NAME}.csr` is the output file where the `.csr` is stored.

4. To sign the ESM certificate signing request, perform the following steps in the ArcSight Platform. For a cloud deployment, perform the steps on the Bastion host.

   a. Create a temporary folder to store the generated certificates:

```
mkdir –m 700 /tmp/esm
```

   b. Move the certificate signing request (`.csr`) file from the ESM host to the temporary folder that you created.

   c. Set the environment variables:

```
export CA_CERT=re_ca.cert.pem
```

```
export COMMON_NAME=<your ESM host's fully-qualified domain name>
```

```
export TH=<FQDN of the ArcSight Platform virtual IP for HA or single
master node>_<Kafka TLS-enabled port>
```

   > **Note:** For `COMMON_NAME`, use the same host FQDN as you used for the ESM client key pair.

   d. Run the following commands to sign the ESM certificate signing request:

```
cd /tmp/esm
```

```
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o
```

```
json 2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n
core -o json 2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-
cbc -md sha256 -a -d -pass pass:"${PASSPHRASE}")
```

```
export CSR=$(cat ${COMMON_NAME}.csr)
```

```
WRITE_RESPONSE=$(kubectl exec -it -n core ${VAULT_POD} -c vault --
bash -c "VAULT_TOKEN=$VAULT_TOKEN vault write -tls-skip-verify -
format=json RE/sign/coretech csr=\"${CSR}\"") && \
echo "$WRITE_RESPONSE" | jq -r ".data | .certificate" > ${COMMON_
NAME}.signed.crt && \
echo "$WRITE_RESPONSE" | jq -r ".data | .issuing_ca" > ${COMMON_
NAME}.issue_ca.crt && \
echo "$WRITE_RESPONSE" | jq -r ".data | .certificate, if .ca_chain
then .ca_chain[] else .issuing_ca end" > ${COMMON_
NAME}.signed.cert.with.ca.crt
```

The signed certificate is in the file `${COMMON_NAME}.signed.crt`. The issuing CA is in the file `${COMMON_NAME}.issue_ca.crt`. The signed certificate with the CA chain is in the file `${COMMON_NAME}.signed.cert.with.ca.crt`.

5. Retrieve the RE certificates:

   For a cloud deployment:

```
cd <path to OMT installer>/cdf-deployer/scripts/
```

```
./cdf-updateRE.sh > /tmp/esm/${CA_CERT}
```

6. Copy the following files from the Transformation Hub `/tmp/esm` folder to an ESM host folder (for example, `/opt/arcsight/tmp`):

   `/tmp/esm/${COMMON_NAME}.signed.cert.with.ca.crt`

   `/tmp/esm/${CA_CERT}`

   Remove the files from `/tmp/esm` after you copy them.

7. On the ESM server, import the RE certificate from file ${CA_CERT} into the ESM client truststore:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientcerts -alias
<alias for the certificate> -importcert -file <absolute path to
certificate file>
```

   For example:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientcerts -alias
thcert -importcert -file /opt/arcsight/tmp/re_ca.cert.pem
```

> **Note:** You might receive the following message:
>
> ```
> Certificate already exists in keystore under alias <alias1>
> Do you still want to add it? [no]:
> ```
>
> It is not necessary to add an existing certificate.

8. On the ESM server, run the following command to import the signed certificate:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -alias
   <alias for the key> -importcert -file <path to signed cert> -trustcacerts
   ```

   For example:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -alias ebkey
   -importcert -file /opt/arcsight/tmp/${COMMON_NAME}.signed.cert.with.ca.crt
   -trustcacerts
   ```

   > **Note:** You might see the following warning:
   >
   > ```
   > ...
   > Top-level certificate in reply:
   > ...
   > ... is not trusted. Install reply anyway? [no]:
   > ```
   >
   > This is because the root certificate of the RE CA is not in the ESM truststore. This does not affect the functionality of ESM. Enter **yes** to allow the new certificate to be imported.

To complete the configuration, configure ESM to consume from Transformation Hub.

Configuring Logger as a Transformation Hub Consumer

> **Note:** For cloud Transformation Hub, you must complete the configuration procedures detailed in:
>
> - Completing Integration with AWS Transformation Hub
>
> before you perform the procedures in this section.

The procedure for configuring a Logger as a Transformation Hub consumer will depend on which configuration you are using. Follow the configuration that matches your environment.

Configuring Logger as a Transformation Hub Consumer – Client Authentication in FIPS Mode

Follow these steps to configure Logger to consume from Transformation Hub with client authentication in FIPS Mode

- Enabling FIPS and Preparing the Logger Server
- Generating and Signing the Certificate Signing Request

Enabling FIPS and Preparing the Logger Server

Follow these steps to enable FIPS mode on Logger and to prepare the Logger server:

1. Sign-in to the Logger Console and enable FIPS mode.

   For more information, see "Enabling and Disabling FIPS Mode on Logger" in the *Logger 7.3 Administrator's Guide*.
2. Navigate to the Logger server's `/tmp/` directory and create a logger directory if it does not already exist.

   ```
   mkdir -p logger
   ```
3. Change to the Logger directory:

   ```
   cd /tmp/logger
   ```
4. Set the environment variables for static values used by `th_cert_tool.sh` script.

   ```
   export TH=<transformation.hub.fqdn>
   ```

Generating and Signing the Certificate Signing Request

Follow these steps to generate and sign the certificate signing request (CSR).

1. Run these commands to generate the CSR and copy it to the Transformation Hub Logger directory:

   ```
   sudo /opt/arcsight/current/arcsight/logger/bin/scripts/th_cert_tool.sh --generate-csr --th-host ${TH} --key-length 2048
   ```

   ```
   mv csr.csr /tmp/logger/
   ```
2. Run the following commands to sign the Logger certificate signing request in Transformation Hub:

```
cd /tmp/logger
export CA_CERT=re_ca.cert.pem
export COMMON_NAME=<logger.fqdn>
```

```
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o json
2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n core
-o json 2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-cbc -
md sha256 -a -d -pass pass:"${PASSPHRASE}")
mv csr.csr ${COMMON_NAME}.csr
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o json
2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n core
-o json 2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-cbc -
md sha256 -a -d -pass pass:"${PASSPHRASE}")
export CSR=$(cat ${COMMON_NAME}.csr)
```

```
WRITE_RESPONSE=$(kubectl exec -it -n core ${VAULT_POD} -c vault -- bash -
c "VAULT_TOKEN=$VAULT_TOKEN vault write -tls-skip-verify -format=json
RE/sign/coretech csr=\"${CSR}\"") && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .certificate" > ${COMMON_
NAME}.signed.crt && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .issuing_ca" > ${COMMON_
NAME}.issue_ca.crt && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .certificate, if .ca_chain then
.ca_chain[] else .issuing_ca end" > ${COMMON_
NAME}.signed.cert.with.ca.crt
```

3. Retrieve the RE certificate:

```
/<TH Home Path>/scripts/cdf-updateRE.sh > /tmp/logger/${CA_CERT}
```

Example:

```
/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh >/tmp/logger/${CA_CERT}
```

> **Note:** For a cloud installation, log in to the bastion or jump host and run the `cdf-updateRE.sh` script:
>
> arcsight-platform-cloud-installer/cdf-deployer/scripts/cdf-updateRE.sh

4. Move the following files from the Transformation Hub to the Logger `/tmp/logger` directory:
   - `/tmp/logger/${COMMON_NAME}.signed.cert.with.ca.crt`
   - `/tmp/logger/${CA_CERT}`
5. Run the following commands in Logger:

```
export TH=<transformartion.hub.fqdn>
export COMMON_NAME=<Logger.fqdn>
export CA_CERT=re_ca.cert.pem
export ARCSIGHT_HOME=/opt/arcsight/current/arcsight/logger
/opt/arcsight/current/arcsight/logger/bin/scripts/th_cert_tool.sh --
import-cert --th-host ${TH} --cert-path /tmp/logger/${COMMON_
NAME}.signed.cert.with.ca.crt
${ARCSIGHT_HOME}/bin/scripts/keytool_util.sh receiver delete mykey
/opt/arcsight/current/arcsight/logger/bin/scripts/keytool_util.sh
receiver importcert /tmp/logger/${CA_CERT}
```

6. When adding the receiver in the Logger Console, configure the following settings:
   - `Use SSL/TLS = TRUE`
   - `Use Client Authentication = TRUE`

Configuring Logger as a Transformation Hub Consumer – Client Authentication in non-FIPS Mode

Follow these steps to configure Logger to consume from Transformation Hub with client authentication in non-FIPS Mode

- Preparing the Logger Server
- Generating and Signing the Certificate Signing Request

Preparing the Logger Server

Follow these steps to prepare the Logger server:

1. Navigate to the Logger server's `/tmp/` directory and create a logger directory if it does not already exist.

```
mkdir -p logger
```

2. Change to the Logger directory:

```
cd /tmp/logger
```

3. Set the environment variables for static values used by `th_cert_tool.sh` script.

```
export TH=<transformation.hub.fqdn>
```

Generating and Signing the Certificate Signing Request

Follow these steps to generate and sign the certificate signing request (CSR).

1. Run these commands to generate the CSR and copy it to the Transformation Hub Logger directory:

```
sudo /opt/arcsight/current/arcsight/logger/bin/scripts/th_cert_tool.sh --
generate-csr --th-host ${TH} --key-length 2048
```

```
mv csr.csr /tmp/logger/
```

2. Run the following commands to sign the Logger certificate signing request in Transformation Hub:

```
cd /tmp/logger
export CA_CERT=re_ca.cert.pem
export COMMON_NAME=<logger.fqdn>
```

```
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o json
2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n core
-o json 2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-cbc -
md sha256 -a -d -pass pass:"${PASSPHRASE}")
mv csr.csr ${COMMON_NAME}.csr
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o json
2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n core
-o json 2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-cbc -
md sha256 -a -d -pass pass:"${PASSPHRASE}")
export CSR=$(cat ${COMMON_NAME}.csr)
```

```
WRITE_RESPONSE=$(kubectl exec -it -n core ${VAULT_POD} -c vault -- bash -
c "VAULT_TOKEN=$VAULT_TOKEN vault write -tls-skip-verify -format=json
RE/sign/coretech csr=\"${CSR}\"") && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .certificate" > ${COMMON_
```

```
NAME}.signed.crt && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .issuing_ca" > ${COMMON_
NAME}.issue_ca.crt && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .certificate, if .ca_chain then
.ca_chain[] else .issuing_ca end" > ${COMMON_
NAME}.signed.cert.with.ca.crt
```

3. Retrieve the RE certificate:

```
/<TH Home Path>/scripts/cdf-updateRE.sh > /tmp/logger/${CA_CERT}
```

Example:

```
/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh >/tmp/logger/${CA_CERT}
```

> **Note:** For a cloud installation, log in to the bastion or jump host and run the `cdf-updateRE.sh` script:
>
> arcsight-platform-cloud-installer/cdf-deployer/scripts/cdf-updateRE.sh

4. Move the following files from the Transformation Hub to the Logger `/tmp/logger` directory:
   - `/tmp/logger/${COMMON_NAME}.signed.cert.with.ca.crt`
   - `/tmp/logger/${CA_CERT}`
5. Run the following commands in Logger:

```
export TH=<transformartion.hub.fqdn>
export COMMON_NAME=<Logger.fqdn>
export CA_CERT=re_ca.cert.pem
export ARCSIGHT_HOME=/opt/arcsight/current/arcsight/logger
/opt/arcsight/current/arcsight/logger/bin/scripts/th_cert_tool.sh --
import-cert --th-host ${TH} --cert-path /tmp/logger/${COMMON_
NAME}.signed.cert.with.ca.crt
${ARCSIGHT_HOME}/bin/scripts/keytool_util.sh receiver delete mykey
/opt/arcsight/current/arcsight/logger/bin/scripts/keytool_util.sh
receiver importcert /tmp/logger/${CA_CERT}
```

6. When adding the receiver in the Logger Console, configure the following settings:
   - `Use SSL/TLS = TRUE`
   - `Use Client Authentication = TRUE`

Configuring Logger as a Transformation Hub Consumer – No Client Authentication in FIPS Mode

Follow these steps to configure Logger to consume from Transformation Hub without client authentication in FIPS Mode.

- Enabling FIPS and Preparing the Logger Server
- Signing the Certificate in Transformation Hub
- Importing the Certificate into Logger
- Retrieving the Certificate on Transformation Hub

Enabling FIPS and Preparing the Logger Server

Follow these steps to enable FIPS mode on Logger and to prepare the Logger OBC:

1. Sign-in to the Logger Console and enable FIPS mode.

   For more information, see "Enabling and Disabling FIPS Mode on Logger" in the *Logger 7.3 Administrator's Guide*.
2. Run the following commands in Logger:

```
<install dir>/logger/bin/scripts/th_cert_tool.sh --generate-csr --th-host
<MASTER_IP> --key-length 2048
```

```
scp <install dir>/logger/user/logger/th_certs/<MASTER_IP>/csr.csr <MASTER_
IP>:/tmp/
```

Signing the Certificate in Transformation Hub

Run this command to sign the certificate in Transformation Hub:

```
openssl x509 -req -CA ca.crt -CAkey ca.key -in /tmp/csr.csr -out
/tmp/signedLoggerCert.pem -days 3650 -CAcreateserial -passin pass:arcsight -
sha256
```

Importing the Certificate into Logger

Run these commands to import the certificate into Logger:

```
scp masterhost:/tmp/signedLoggerCert.pem /tmp
```

```
<install dir>/logger/bin/scripts/th_cert_tool.sh --import-cert --th-host
<MASTER_IP> --cert-path /tmp/signedLoggerCert.pem
```

Retrieving the Certificate on Transformation Hub

Follow these instructions to retrieve the certificate on Transformation Hub.

- Cloud deployment. Follow these steps:
  a. Log in to the bastion or jump host and run the script `cdf-updateRE.sh`:

     ```
     arcsight-platform-cloud-installer/cdf-deployer/scripts/cdf-updateRE.sh
     ```

  b. Run the following commands in Logger:

     ```
     scp <MASTER_IP>:/tmp/RE.crt /tmp/export ARCSIGHT_HOME=<install
     dir>/logger/$ARCSIGHT_HOME/bin/scripts/keytool_util.sh receiver delete
     mykey
     ```

     ```
     $ARCSIGHT_HOME/bin/scripts/keytool_util.sh receiver importcert
     /tmp/RE.crt
     ```

     ```
     <install dir>/logger/bin/loggerd restart receivers
     ```

     ```
     watch -n 1 '/opt/current/arcsight/logger/bin/loggerd status'
     ```

  c. When adding the receiver in the Logger Console, configure the following setting:

     `Use SSL/TLS = TRUE`

Configuring Logger as a Transformation Hub Consumer – No Client Authentication in non-FIPS Mode with TLS

Configuring Logger to consume from Transformation Hub without client authentication in non-FIPS Mode using TLS only requires retrieving the RE certificate on the Transformation Hub, and the steps to follow depend on your type of deployment:

- Cloud deployment:
  a. Log in to the bastion or jump host and run the script `cdf-updateRE.sh`:

     ```
     arcsight-platform-cloud-installer/cdf-deployer/scripts/cdf-updateRE.sh
     ```

  b. Run the following commands in Logger:

     ```
     scp <MASTER_IP>:/tmp/RE.crt /tmp/export ARCSIGHT_HOME=<install
     dir>/logger/$ARCSIGHT_HOME/bin/scripts/keytool_util.sh receiver delete
     mykey
     ```

```
$ARCSIGHT_HOME/bin/scripts/keytool_util.sh receiver importcert
/tmp/RE.crt
```

```
<install dir>/logger/bin/loggerd restart receivers
```

```
watch -n 1 '/opt/current/arcsight/logger/bin/loggerd status'
```

c. When adding the receiver in the Logger Console, configure the following setting:

   `Use SSL/TLS = TRUE`

Configuring Logger as a Transformation Hub Consumer – No Client Authentication in non-FIPS Mode without TLS

Follow these steps to configure Logger to consume from Transformation Hub without client authentication in non-FIPS Mode and without TLS.

1. Sign in to the Logger Console and create a Logger Transformation Hub receiver.

   For more information, see "*Working with Receivers*" in the Logger 7.3 Administrator's Guide.

2. Configure the Transformation Hub receiver with the following values:
   - Transformation Hub host(s) and port = IP address or host name followed by semicolon and port 9092.

     For example: *your.th.ip.address*:9092
   - Use SSL/TLS Key = FALSE
   - Use SSL/TLS Client Authentication = FALSE
3. Fill in other fields with applicable values, and save the changes.

Configuring Logger as a Transformation Hub Producer

You can configure a Logger with a Transformation Hub destination with the encrypted security mode that you require.

Configuring Logger with a Transformation Hub Destination – Client Authentication in FIPS Mode

Follow these steps to configure a Logger Transformation Hub destination with client authentication in FIPS mode.

- Enabling FIPS and Preparing the Logger OBC
- Creating a Keystore on the Logger Onboard Connector
- Signing the Logger OBC Certificate Signing Request on Transformation Hub
- Updating the Keystore and Creating a Truststore on the Logger OBC
- Creating a Logger Transformation Hub Destination in the Console

Enabling FIPS and Preparing the Logger OBC

Follow these steps to enable FIPS mode on Logger and to prepare the Logger OBC:

1. Sign-in to the Logger Console and enable FIPS mode.

   For more information, see "Enabling and Disabling FIPS Mode on Logger" in the Logger 7.3 Administrator's Guide.

2. Navigate to the Logger OBC's `current` directory:

   ```
   cd <install dir>/connector/current
   ```

3. Set the environment variables for the static values used by `keytool`:

   ```
   export CURRENT=<full path to this "current" folder>
   ```

   ```
   export BC_OPTS="-storetype BCFKS -providername BCFIPS -J-
   Djava.security.egd=file:/dev/urandom -providerpath
   ${CURRENT}/lib/agent/fips/bc-fips-1.0.2.jar -providerclass
   org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider"
   ```

   ```
   export TH=<Transformation Hub hostname>_<Transformation Hub port>
   export STORES=${CURRENT}/user/agent/stores
   export STORE_PASSWD=changeit
   export CA_CERT=re_ca.cert.pem
   export COMMON_NAME=<LoggerFQDN>
   ```

4. Create the `${CURRENT}/user/agent/stores` directory if it does not already exist.

   ```
   mkdir -p ${STORES}
   ```

5. Apply the following workaround for a Java `keytool` issue:

   a. Create a new file, `agent.security`:

      ```
      ${CURRENT}/user/agent
      ```

   b. Add the following content to the newly created file, and then save it:

```
security.provider.1=org.bouncycastle.jcajce.provider.BouncyCastleFipsP
rovider
security.provider.2=com.sun.net.ssl.internal.ssl.Provider BCFIPS
security.provider.3=sun.security.provider.Sun
```

c. Move the `${CURRENT}/lib/agent/fips/bcprov-jdk15on-168.jar` file to the `current` directory.

Creating a Keystore on the Logger Onboard Connector

Follow these steps to create the OBC keystore:

1. Create the keystore for the OBC:

```
cd ${STORES}
```

```
$CURRENT/jre/bin/keytool -keystore ${TH}.keystore.bcfips -genkeypair -
dname "cn=logger.fqdn, ou=ArcSight, o=Micro Focus, c=US" -keyalg rsa -
keysize 2048 -alias ${TH} -startdate -1d -validity 365 -storepass
${STORE_PASSWD} -keypass ${STORE_PASSWD} ${BC_OPTS}
```

2. Create the certificate signing request (CSR) for the Logger OBC:

```
$CURRENT/jre/bin/keytool -certreq -alias ${TH} -keystore
${TH}.keystore.bcfips -file ${COMMON_NAME}.csr -storepass ${STORE_PASSWD}
${BC_OPTS}
```

3. Copy the CSR file `${COMMON_NAME}.csr` to the Transformation Hub `/tmp` folder:

```
cp ${COMMON_NAME}.csr /tmp/
```

Signing the Logger OBC Certificate Signing Request on Transformation Hub

1. Set the environment:

```
export CA_CERT=re_ca.cert.pem
export COMMON_NAME=<LoggerFQDN>
export TH=<Transformation Hub hostname>_<Transformation Hub port>
```

Note: Use the same values that you specified for the Logger OBC.

2. Run these commands to sign the Logger certificate signing request:

```
mkdir /tmp/logger
mv ${COMMON_NAME}.csr /tmp/logger/
cd /tmp/logger
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o json
2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n core
-o json 2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-cbc -
md sha256 -a -d -pass pass:"${PASSPHRASE}")
export CSR=$(cat ${COMMON_NAME}.csr)
```

```
WRITE_RESPONSE=$(kubectl exec -it -n core ${VAULT_POD} -c vault -- bash -
c "VAULT_TOKEN=$VAULT_TOKEN vault write -tls-skip-verify -format=json
RE/sign/coretech csr=\"${CSR}\"") && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .certificate" > ${COMMON_
NAME}.signed.crt && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .issuing_ca" > ${COMMON_
NAME}.issue_ca.crt && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .certificate, if .ca_chain then
.ca_chain[] else .issuing_ca end" > ${COMMON_
NAME}.signed.cert.with.ca.crt
```

The signed certificate is in file `${COMMON_NAME}.signed.crt`.

The issuing CA is in file `${COMMON_NAME}.issue_ca.crt`.

The signed certificate with CA chain is in file `${COMMON_NAME}.signed.cert.with.ca.crt`.

3. Retrieve the RE certificate.

```
/<TH Home Path>/scripts/cdf-updateRE.sh > /tmp/logger/${CA_CERT}
```

Example: `/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh >/tmp/logger/${CA_CERT}`

> **Note:** For a cloud installation, log in to the bastion or jump host and run the `cdf-updateRE.sh` script:
>
> arcsight-platform-cloud-installer/cdf-deployer/scripts/cdf-updateRE.sh

Move the following files from the Transformation Hub to the Logger OBC `STORES` directory:

- `/tmp/logger/ ${COMMON_NAME}.signed.crt`
- `/tmp/logger/${COMMON_NAME}.issue_ca.crt`

- `/tmp/logger/${COMMON_NAME}.signed.cert.with.ca.crt`
- `/tmp/logger/${CA_CERT}`

Updating the Keystore and Creating a Truststore on the Logger OBC

Follow these steps to update the keystore and to create a truststore on the Logger OBC:

1. Update the Logger OBC keystore with a signed certificate.

   ```
   cd ${STORES}/
   ```

   ```
   $CURRENT/jre/bin/keytool -importcert -alias ${TH} -keystore
   ${TH}.keystore.bcfips -trustcacerts -file ${COMMON_
   NAME}.signed.cert.with.ca.crt -storepass ${STORE_PASSWD} ${BC_OPTS}
   ```

   Verification: Run the following command to verify the keystore, and ensure that it has only one entry in the keystore.

   ```
   $CURRENT/jre/bin/keytool -v -list -keystore ${TH}.keystore.bcfips -
   storepass ${STORE_PASSWD} ${BC_OPTS} |grep -i alias
   ```

2. Create the Logger OBC truststore.

   ```
   cd ${STORES}/
   ```

   ```
   $CURRENT/jre/bin/keytool -importcert -alias reca -trustcacerts -file
   ${CA_CERT} -keystore ${TH}.truststore.bcfips -storepass ${STORE_PASSWD}
   ${BC_OPTS}
   ```

   When prompted, specify **yes** to trust the certificate.

Creating a Logger Transformation Hub Destination in the Console

Follow these steps to create a Logger Transformation Hub destination in the Console:

1. Run the following commands, and note the keystore and truststore paths:

   ```
   echo ${STORES}/${TH}.keystore.bcfips
   echo ${STORES}/${TH}.truststore.bcfips
   ```

2. Sign-in to the Logger Console to create a TH destination.

   For more information, see "Transformation Hub Destinations" in the Logger 7.3 Administrator's Guide.

3. Create the Transformation Hub destination with the following values:

- Kafka Broker on SSL/TLS = TRUE
- SSL/TLS Truststore File Path = <*truststorePath*>
- SSL/TLS Truststore Password = STORE_PASSWD
- Use SSL/TLS Client Authentication = TRUE
- SSL/TLS Keystore File Path = <*keystoreFilePath*>
- SSL/TLS Keystore Password = STORE_PASSWD
- SSL/TLS Key Password = STORE_PASSWD

4. Fill in other fields with applicable values, and save the changes.

Configuring Logger with a Transformation Hub Destination – Client Authentication in non-FIPS Mode

Follow these steps to configure a Logger with a Transformation Hub (TH) destination with client authentication, in non-FIPS mode.

- Preparing the Logger Onboard Connector
- Creating the Keystore for Logger's Onboard Connector
- Signing the Logger OBC Certificate Signing Request on Transformation Hub
- Updating the Keystore and Creating a Truststore on the Logger OBC
- Creating a Logger Transformation Hub Destination in the Console

Preparing the Logger Onboard Connector

1. Navigate to the Logger OBC's current directory:

```
cd <install dir>/connector/current
```

2. Set the environment variables for the static values used by `keytool`:

```
export CURRENT=<full path to this "current" folder>
export TH=<Transformation Hub hostname>_<Transformation Hub port>
export STORES=${CURRENT}/user/agent/stores
export STORE_PASSWD=changeit
export CA_CERT=re_ca.cert.pem
export COMMON_NAME=<LoggerFQDN>
```

3. Create the `${CURRENT}/user/agent/stores` directory if it does not already exist.

```
mkdir -p ${STORES}
```

Creating the Keystore for Logger's Onboard Connector

Follow these steps to create the OBC keystore:

1. Create the keystore for the OBC:

```
cd ${STORES}
```

```
$CURRENT/jre/bin/keytool -keystore ${TH}.keystore.bcfips -genkeypair -
dname "cn=Logger.fqdn, ou=yourOU, o=yourCompany, c=US" -keyalg rsa -
keysize 2048 -alias ${TH} -startdate -1d -validity 365 -storepass
${STORE_PASSWD} -keypass ${STORE_PASSWD}
```

2. Create the certificate signing request (CSR) for the Logger OBC:

```
$CURRENT/jre/bin/keytool -certreq -alias ${TH} -keystore
${TH}.keystore.jks -file ${COMMON_NAME}.csr -storepass ${STORE_PASSWD}
```

3. Copy the CSR file `${COMMON_NAME}.csr` to the Transformation Hub `/tmp` folder:

```
cp ${COMMON_NAME}.csr /tmp/
```

Signing the Logger OBC Certificate Signing Request on Transformation Hub

1. Set the environment:

```
export CA_CERT=re_ca.cert.pem
export COMMON_NAME=<LoggerFQDN>
export TH=<Transformation Hub hostname>_<Transformation Hub port>
```

Note: Use the same values that you specified for the Logger OBC.

2. Run these commands to sign the Logger certificate signing request:

```
mkdir /tmp/logger
mv ${COMMON_NAME}.csr /tmp/logger/
cd /tmp/logger
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o json
2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n core
-o json 2>/dev/null | jq -r '.data."root.token"')
```

```
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-cbc -
md sha256 -a -d -pass pass:"${PASSPHRASE}")
export CSR=$(cat ${COMMON_NAME}.csr)
```

```
WRITE_RESPONSE=$(kubectl exec -it -n core ${VAULT_POD} -c vault -- bash -
c "VAULT_TOKEN=$VAULT_TOKEN vault write -tls-skip-verify -format=json
RE/sign/coretech csr=\"${CSR}\"") && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .certificate" > ${COMMON_
NAME}.signed.crt && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .issuing_ca" > ${COMMON_
NAME}.issue_ca.crt && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .certificate, if .ca_chain then
.ca_chain[] else .issuing_ca end" > ${COMMON_
NAME}.signed.cert.with.ca.crt
```

The signed certificate is in file `${COMMON_NAME}.signed.crt`.

The issuing CA is in file `${COMMON_NAME}.issue_ca.crt`.

The signed certificate with CA chain is in file `${COMMON_NAME}.signed.cert.with.ca.crt`.

3. Retrieve the RE certificate.

```
/<TH Home Path>/scripts/cdf-updateRE.sh > /tmp/logger/${CA_CERT}
```

Example: `/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh >/tmp/logger/${CA_CERT}`

> **Note:** For a cloud installation, log in to the bastion or jump host and run the `cdf-updateRE.sh` script:
>
> arcsight-platform-cloud-installer/cdf-deployer/scripts/cdf-updateRE.sh

Move the following files from the Transformation Hub to the Logger OBC `STORES` directory:

- `/tmp/logger/ ${COMMON_NAME}.signed.crt`
- `/tmp/logger/${COMMON_NAME}.issue_ca.crt`
- `/tmp/logger/${COMMON_NAME}.signed.cert.with.ca.crt`
- `/tmp/logger/${CA_CERT}`

Updating the Keystore and Creating a Truststore on the Logger OBC

Follow these steps to update the keystore and to create a truststore on the Logger OBC:

1. Update the Logger OBC keystore with a signed certificate.

```
cd ${STORES}/
```

```
$CURRENT/jre/bin/keytool -importcert -alias ${TH} -keystore
${TH}.keystore.jks -trustcacerts -file ${COMMON_
NAME}.signed.cert.with.ca.crt -storepass ${STORE_PASSWD}
```

   When prompted, specify **yes** to trust the certificate.

   Verification: Run the following command to verify the keystore, and ensure that it has only one entry in the keystore.

```
$CURRENT/jre/bin/keytool -v -list -keystore ${TH}.keystore.jks -storepass
${STORE_PASSWD} |grep -i alias
```

2. Create the Logger OBC truststore.

```
cd ${STORES}/
```

```
$CURRENT/jre/bin/keytool -importcert -alias CARoot -trustcacerts -file
${CA_CERT} -keystore ${TH}.truststore.jks -storepass ${STORE_PASSWD}
```

   When prompted, specify **yes** to trust the certificate.

3. Run the following commands, and take note of the truststore path:

```
echo ${STORES}/${TH}.keystore.jks
echo ${STORES}/${TH}.truststore.jks
```

Creating a Logger Transformation Hub Destination in the Console

Follow these steps to create a Logger TH destination in the Console:

1. Run the following commands, and note the keystore and truststore paths:

```
echo ${STORES}/${TH}.keystore.bcfips
echo ${STORES}/${TH}.truststore.bcfips
```

2. Sign-in to the Logger Console to create a TH destination.

   For more information, see "Transformation Hub Destinations" in the Logger 7.3 Administrator's Guide.

3. Create the Transformation Hub destination with the following values:
   - Kafka Broker on SSL/TLS = TRUE
   - SSL/TLS Truststore File Path = <*truststorePath*>

- SSL/TLS Truststore Password = <*changeit*>
- Use SSL/TLS Client Authentication = TRUE
- SSL/TLS Keystore File Path = <*keystoreFilePath*>
- SSL/TLS Keystore Password = <*changeit*>
- SSL/TLS Key Password = <*changeit*>

4. Fill in other fields with applicable values, and save the changes.

Configuring Logger with a Transformation Hub Destination – No Client Authentication in FIPS Mode

Follow these steps to configure a Logger Transformation Hub destination without client authentication in FIPS mode.

- Enabling FIPS and Preparing the Logger OBC
- Creating a CA CERT File on Transformation Hub
- Creating a Truststore on the Logger OBC
- Creating a Logger Transformation Hub Destination in the Console
- Cleaning up the Certificate File

Enabling FIPS and Preparing the Logger OBC

Follow these steps to enable FIPS mode on Logger and to prepare the Logger OBC:

1. Sign-in to the Logger Console and enable FIPS mode.

   For more information, see "Enabling and Disabling FIPS Mode on Logger" in the Logger 7.3 Administrator's Guide.

2. Navigate to the Logger OBC's `current` directory:

   ```
   cd <install dir>/connector/current
   ```

3. Set the environment variables for the static values used by `keytool`:

   ```
   export CURRENT=<full path to this "current" folder>
   ```

   ```
   export BC_OPTS="-storetype BCFKS -providername BCFIPS -J-
   Djava.security.egd=file:/dev/urandom -providerpath
   ${CURRENT}/lib/agent/fips/bc-fips-1.0.2.jar -providerclass
   org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider"
   ```

```
export TH=<Transformation Hub hostname>_<Transformation Hub port>
export STORES=${CURRENT}/user/agent/stores
export STORE_PASSWD=changeit
export CA_CERT=re_ca.cert.pem
```

4. Create the `${CURRENT}/user/agent/stores` directory if it does not already exist.

```
mkdir -p ${STORES}
```

5. Apply the following workaround for a Java `keytool` issue:
   a. Create a new file, `agent.security`:

   ```
   ${CURRENT}/user/agent
   ```

   b. Add the following content to the newly created file, and then save it:

   ```
   security.provider.1=org.bouncycastle.jcajce.provider.BouncyCastleFipsP
   rovider
   security.provider.2=com.sun.net.ssl.internal.ssl.Provider BCFIPS
   security.provider.3=sun.security.provider.Sun
   ```

   c. Move the `${CURRENT}/lib/agent/fips/bcprov-jdk15on-168.jar` file to the `current` directory.

Creating a CA CERT File on Transformation Hub

Follow these steps to create a `${CA_CERT}` file with the content of the root CA certificate:

1. Set the environment:

```
export CA_CERT=re_ca.cert.pem
```

2. Create a certificate:

```
/<TH Home Path>/scripts/cdf-updateRE.sh > /tmp/${CA_CERT}
```

Example:

`/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/${CA_CERT}`

> **Note:** For a cloud installation, log in to the bastion or jump host and run the `cdf-updateRE.sh` script:
>
> arcsight-platform-cloud-installer/cdf-deployer/scripts/cdf-updateRE.sh

3. Move this file from Transformation Hub to the connector STORES directory.

Creating a Truststore on the Logger OBC

Run this command to create a truststore on the Logger OBC:

```
$CURRENT/jre/bin/keytool -noprompt -importcert -storepass ${STORE_PASSWD} -
destkeystore ${STORES}/${TH}.truststore.bcfips -alias reca -file ${CA_CERT} -
storetype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
${CURRENT}/lib/agent/fips/bc-fips-1.0.2.jar
```

When prompted, specify **yes** to trust the certificate.

Creating a Logger Transformation Hub Destination in the Console

1. Run the following command, and note the truststore path:

   ```
   echo ${STORES}/${TH}.keystore.bcfips
   ```

2. Sign-in to the Logger Console to create a TH destination.

   For more information, see "Transformation Hub Destinations" in the Logger 7.3 Administrator's Guide.

3. Create the Transformation Hub destination with the following values:
   - Kafka Broker on SSL/TLS = TRUE
   - SSL/TLS Truststore File Path = <*truststorePath*>
   - SSL/TLS Truststore Password = <*STORE_PASSWORD*>
   - Use SSL/TLS Client Authentication = FALSE
   - SSL/TLS Keystore File Path = <*keystoreFilePath*>
   - SSL/TLS Keystore Password = <*keystorePassword*>
   - SSL/TLS Key Password = <*keyPassword*>
4. Fill in other fields with applicable values, and save the changes.

Cleaning up the Certificate File

Run the following command to delete the certificate file:

> **Caution:** The following file should be deleted to prevent the distribution of security certificates that could be used to authenticate against the Transformation Hub. These files are very sensitive and must not be distributed to other machines.

```
rm ${STORES}/${CA_CERT}
```

Configuring Logger with a Transformation Hub Destination – No Client Authentication in non-FIPS Mode

Follow these steps to configure Logger with a Transformation Hub destination without client authentication in non-FIPS mode. This is the default security mode configuration when installing Transformation Hub.

- Preparing the Logger Onboard Connector
- Creating a CA CERT File on Transformation Hub
- Importing the CA Certificate on the Logger OBC
- Creating a Logger Transformation Hub Destination in the Console

Preparing the Logger Onboard Connector

Follow these steps to prepare the Logger Onboard Connector.

1. Navigate to the Logger Onboard Connector's (OBC) current directory:

   ```
   cd <install dir>/connector/current
   ```

2. Run the following commands to set the environment variables for the static values used by keytool:

   ```
   export CURRENT=<full path to this "current" folder>
   ```

   Example: `export CURRENT=/opt/arcsight/connector/current`

   ```
   export TH=<Transformation Hub hostname>_<Transformation Hub port>
   export CA_CERT=re_ca.cert.pem
   export STORE_PASSWD=changeit
   export STORES=${CURRENT}/user/agent/stores
   ```

3. Create the directory if it does not already exist.

   ```
   mkdir -p ${STORES}
   ```

Creating a CA CERT File on Transformation Hub

Follow these steps to create a `${CA_CERT}` file with the content of the root CA certificate:

1. Set the environment:

   ```
   export CA_CERT=re_ca.cert.pem
   ```

2. Create a certificate:

```
/<TH Home Path>/scripts/cdf-updateRE.sh > /tmp/${CA_CERT}
```

Example:

```
/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/${CA_CERT}
```

> **Note:** For a cloud installation, log in to the bastion or jump host and run the `cdf-updateRE.sh` script:
>
> arcsight-platform-cloud-installer/cdf-deployer/scripts/cdf-updateRE.sh

3. Move this file from Transformation Hub to the connector STORES directory.

Importing the CA Certificate on the Logger OBC

1. Import the CA certificate to the trust store in the `${CURRENT}` folder.

```
$CURRENT/jre/bin/keytool -importcert -file ${STORES}/${CA_CERT} -alias
CARoot -keystore ${STORES}/${TH}.truststore.jks -storepass ${STORE_
PASSWD}
```

2. When prompted, specify **yes** to trust the certificate.
3. Run the following command and note the trust store path:

```
echo ${STORES}/${TH}.truststore.jks
```

4. Run the following command to delete the certificate file:

> The following file should be deleted to prevent the distribution of security certificates that could be used to authenticate against the Transformation Hub. These files are very sensitive and should not be distributed to other machines.

```
rm ${STORES}/${CA_CERT}
```

Creating a Logger Transformation Hub Destination in the Console

You need to sign-in to the Logger Console to create a Transformation Hub destination. For more information, see "Transfomation Hub Destinations" in the Logger 7.3 Administrator's Guide.

After logging into the console, create the Transformation Hub destination with the following values:

- Kafka Broker on SSL/TLS = TRUE
- SSL/TLS Truststore File Path = <*truststorePath*>

- SSL/TLS Truststore Password = STORE_PASSWD
- Use SSL/TLS Client Authentication = FALSE
- SSL/TLS Keystore File Path = <*keystoreFilePath*>
- SSL/TLS Keystore Password = <*keystorePassword*>
- SSL/TLS Key Password = <*keyPassword*>

Fill in other fields with applicable values, and save the changes.

Configuring SmartConnector as a Transformation Hub Producer

Follow the steps in this section to configure a SmartConnector with a Transformation Hub destination with the encrypted security mode that you require. These procedures are provided with the following assumptions:

- You use the default password. To set a non-default password, see **Password Management** in the ArcSight SmartConnectors 24.2 documentation.
- You are using a command window to specify Windows commands. **Do not use Windows PowerShell for these commands.**

> For AWS installations, the FQDN of the application load balancer; and `<th_port>` refers to either port 9092 (plain text) or 9093 (TLS)

Configuring a SmartConnector with a Transformation Hub Destination without Client Authentication in non-FIPS Mode

Follow these steps to configure a SmartConnector with a Transformation Hub destination without client authentication in non-FIPS mode. This is the default security mode configuration when installing Transformation Hub.

This procedure enables SSL/TLS on the connector.

- "Preparing the SmartConnector Server" on the next page
- "Creating a CA CERT File on Transformation Hub" on page 336
- "Importing the CA Certificate on the Connector" on page 337

Preparing the SmartConnector Server

1. Prepare the SmartConnector:
   - **If the connector is not yet installed:**
     a. Run the installer.
     b. After the core software is installed, do the following in the window that opens: select **Select Global Parameters** > **Set FIPS Mode**, and set the FIPS Mode to **Disabled**.
   - **If the connector is already installed:**
     a. Run the installer.
     b. Select **Set Global Parameters** > **Set FIPS Mode**, and set the FIPS Mode to **`Disabled`**.
2. Navigate to the `current` directory of the Connector:

   Linux command:

   ```
   cd <install dir>/current
   ```

   Windows command:

   ```
   cd <install dir>\current
   ```

3. Run the following commands to set the environment variables for the static values used by keytool:

   Linux commands:

   ```
   export CURRENT=<full path to this "current" folder>
   ```

   Example:`export CURRENT=/opt/CONNECTORS/TA003/current`

   ```
   export TH=<Transformation Hub hostname>_<Transformation Hub port>
   ```

   Example:`export TH=15.214.***.**`

   ```
   export CA_CERT=re_ca.cert.pem
   export STORE_PASSWD=changeit
   export STORES=${CURRENT}/user/agent/stores
   ```

Windows commands:

```
set CURRENT=<full path to this "current" folder>
set TH=<Transformation Hub hostname>_<Transformation Hub port>
set STORES=%CURRENT%\user\agent\stores
set STORE_PASSWD=changeit
set CA_CERT=re_ca.cert.pem
```

4. Create the directory if it does not already exist.

   Linux command:

   ```
   mkdir -p ${STORES}
   ```

   Windows commands:

   ```
   mkdir -p %STORES%
   ```

Creating a CA CERT File on Transformation Hub

Follow these steps to create a ${CA_CERT} file with the content of the root CA certificate:

1. Set the environment:

   ```
   export CA_CERT=re_ca.cert.pem
   ```

2. Create a certificate:

   ```
   /<TH Home Path>/scripts/cdf-updateRE.sh > /tmp/${CA_CERT}
   ```

   Example:/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/${CA_CERT}

   > **Note:** For a cloud installation, log in to the bastion or jump host and run the cdf-updateRE.sh script:
   >
   > arcsight-platform-cloud-installer/cdf-deployer/scripts/cdf-updateRE.sh

3. Move this file from the Transformation Hub to the connector STORES directory.

Importing the CA Certificate on the Connector

1. Import the CA certificate to the trust store in the ${CURRENT} folder.

   Linux command:

   ```
   $CURRENT/jre/bin/keytool -importcert -file ${STORES}/${CA_CERT} -alias
   CARoot -keystore ${STORES}/${TH}.truststore.jks -storepass $STORE_PASSWD
   ```

   Windows command:

   ```
   %CURRENT%\jre\bin\keytool -importcert -file %STORES%\%CA_CERT% -alias
   CARoot -keystore %STORES%\%TH%.truststore.jks -storepass $STORE_PASSWD
   ```

2. When prompted, specify **yes** to trust the certificate.
3. Run the following command and note the trust store path:

   Linux command:

   ```
   echo ${STORES}/${TH}.truststore.jks
   ```

   Windows command:

   ```
   echo %STORES%\%TH%.truststore.jks
   ```

4. Navigate to the bin directory and run the agent setup script to install a connector with Transformation Hub as the destination.

   Linux commands:

   ```
   cd <installation dir>/current/bin
   ```

   ```
   ./runagentsetup.sh
   ```

   Windows commands:

   ```
   cd <installation dir>\current\bin
   ```

   ```
   runagentsetup.bat
   ```

5. Set **Use SSL/TLS** to **true**.
6. Set **Use SSL/TLS Authentication** to **false**.

7. When completing the Transformation Hub destination fields, use the value noted from **step 3** for the trust store path and the password used earlier (For example: `STORE_PASSWD=changeit`) for the trust store password.
8. Run the following command to delete the certificate file:

> **Caution:** The following file must be deleted to prevent the distribution of security certificates that might be used to authenticate against the Transformation Hub. These files are very sensitive and must not be distributed to other machines.

Linux command:

```
rm ${STORES}/${CA_CERT}
```

Windows command:

```
del %\STORES%\%CA_CERT%
```

Configuring a SmartConnector with a Transformation Hub Destination with Client Authentication in FIPS Mode

Follow these steps to configure a SmartConnector with a Transformation Hub (TH) destination with client authentication in FIPS mode.

> You will need to supply an intermediate certificate and key.

- Preparing the SmartConnector Server
- Creating Keystore for SmartConnector on the SmartConnector Server
- Signing a SmartConnector Certificate Signing Request on Transformation Hub
- Updating Keystore and Creating Truststore on the SmartConnector Server
- Running the SmartConnector Setup

Preparing the SmartConnector Server

1. Prepare the SmartConnector:
   - **If the connector is not yet installed:**
     a. Run the installer.

b. After the core software is installed, do the following in the window that opens: select **Select Global Parameters** > **Set FIPS Mode**, and set the FIPS Mode to **Disabled**.

- **If the connector is already installed:**
  a. Run the installer.
  b. Select **Set Global Parameters** > **Set FIPS Mode**, and set the FIPS Mode to **Enabled**.

2. Navigate to the Connector's `current` directory:

Linux command:

```
cd <install dir>/current
```

Windows command:

```
cd <install dir>\current
```

3. Set the environment variables for the static values used by `keytool`:

Linux commands:

```
export CURRENT=<full path to current folder>
```

Example: `export CURRENT=/opt/CONNECTORS/TA003/current`

```
export BC_OPTS="-storetype BCFKS -providername BCFIPS -J-
Djava.security.egd=file:/dev/urandom -providerpath
${CURRENT}/lib/agent/fips/bc-fips-1.0.2.jar -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider"
```

```
export TH=<Transformation Hub hostname>_<Transformation Hub port>
export STORES=${CURRENT}/user/agent/stores
export STORE_PASSWD=changeit
export TH_HOST=<TH master host name>
export CA_CERT=ca.cert.pem
export FIPS_CA_TMP=/opt/fips_ca_tmp
export COMMON_NAME=<your.connector.fqdn>
```

Windows commands:

```
set CURRENT=<full path to this folder>
```

```
set BC_OPTS="-storetype BCFKS -providername BCFIPS -J-
Djava.security.egd=file:/dev/urandom -providerpath
${CURRENT}/lib/agent/fips/bc-fips-1.0.2.jar -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider"
```

```
set TH=<Transformation Hub hostname>_<Transformation Hub port>
set STORES=%CURRENT%\user\agent\stores
set STORE_PASSWD=changeit
set TH_HOST=<TH master host name>
set CA_CERT=C:\Temp\ca.cert.pem
set FIPS_CA_TMP=C:\Temp\fips_ca_tmp
set COMMON_NAME=<your.connector.fqdn>
```

4. Create the `${CURRENT}/user/agent/stores` directory if it does not already exist.

   Linux command:

   ```
   mkdir -p ${STORES}
   ```

   Windows command:

   ```
   mkdir -p %STORES%
   ```

5. Apply the following workaround for a Java `keytool` issue:
   a. Create a new file, `agent.security`, in the applicable location for Linux or Windows:
      - **Linux:** `${CURRENT}/user/agent`
      - **Windows:** `%CURRENT%\current\user\agent`
   b. Add the following content to the newly created file, and then save it:

      ```
      security.provider.1=org.bouncycastle.jcajce.provider.BouncyCastleFipsP
      rovider
      security.provider.2=com.sun.net.ssl.internal.ssl.Provider BCFIPS
      security.provider.3=sun.security.provider.Sun
      ```

   c. Move the `${CURRENT}/lib/agent/fips/bcprov-jdk15on-168.jar` file to the `current` directory.

Creating a Keystore for SmartConnector on the SmartConnector Server

Follow the applicable steps according to your platform type, Windows or Linux.

Linux platform:

1. Create the keystore for SmartConnector:

```
cd ${STORES}
```

```
$CURRENT/jre/bin/keytool -keystore ${TH}.keystore.bcfips -genkeypair -
dname "cn=<your.connector.fqdn>, ou=<yourOU>, o=<yourCompany>, c=US" -
keyalg rsa -keysize 2048 -alias ${TH} -startdate -1d -validity 366 -
storepass ${STORE_PASSWD} -keypass ${STORE_PASSWD} ${BC_OPTS}
```

2. Create the certificate signing request (CSR) for SmartConnector:

```
$CURRENT/jre/bin/keytool -certreq -alias ${TH} -keystore
${TH}.keystore.bcfips -file ${COMMON_NAME}.csr -storepass ${STORE_PASSWD}
${BC_OPTS}
```

3. Copy the CSR file `${COMMON_NAME}.csr` to the Transformation Hub `/tmp` folder:

```
cp ${COMMON_NAME}.csr /tmp/
```

Windows platform:

1. Create the keystore for SmartConnector:

```
cd %STORES%
```

```
%CURRENT%\jre\bin\keytool %BC_OPTS% -genkeypair -alias %TH% -keystore
%STORES%\%TH%.keystore.bcfips -dname "cn=WIN-FO37IMBPNOI,OU=ArcSight,O=MF
,L=<location>,ST=<state(XX format)>,C=US" -keyalg rsa -keysize 2048 -
alias %TH% -startdate -1d -validity 366 -storepass %STORE_PASSWD% -
keypass %STORE_PASSWD%
```

2. Create the certificate signing request (CSR) for SmartConnector:

```
%CURRENT%\jre\bin\keytool -certreq -alias %TH% -keystore
%STORES%\%TH%.keystore.bcfips -file %STORES%\%TH%-cert-req -storepass
password
```

3. Copy the CSR file `${COMMON_NAME}.csr` to the Transformation Hub `/tmp` folder:

```
cp ${COMMON_NAME}.csr /tmp/
```

Signing a SmartConnector Certificate Signing Request on Transformation Hub

1. Set the environment:

```
export CA_CERT=ca.cert.pem
export COMMON_NAME=<your.connector.fqdn>
export TH=<Transformation Hub hostname>_<Transformation Hub port>
```

> It is mandatory to use the same values that you specified in the SmartConnector server.

2. Run the following commands to sign the SmartConnector certificate signing request:

```
mkdir /tmp/smartconnector
mv ${COMMON_NAME}.csr /tmp/smartconnector/
cd /tmp/smartconnector
```

```
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o json
2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n core
-o json 2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-cbc -
md sha256 -a -d -pass pass:"${PASSPHRASE}")
```

```
export CSR=$(cat ${COMMON_NAME}.csr)
```

```
WRITE_RESPONSE=$(kubectl exec -it -n core ${VAULT_POD} -c vault -- bash -
c "VAULT_TOKEN=$VAULT_TOKEN vault write -tls-skip-verify -format=json
RE/sign/coretech csr=\"${CSR}\"") && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .certificate" > ${COMMON_
NAME}.signed.crt && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .issuing_ca" > ${COMMON_
NAME}.issue_ca.crt && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .certificate, if .ca_chain then
.ca_chain[] else .issuing_ca end" > ${COMMON_
NAME}.signed.cert.with.ca.crt
```

The signed certificate is available in the file: `${COMMON_NAME}.signed.crt`.
The issuing CA is available in the file: `${COMMON_NAME}.issue_ca.crt`.
The signed certificate with CA chain is available in the file: `${COMMON_NAME}.signed.cert.with.ca.crt`.

3. Retrieve the RE certificate:

```
/<TH Home Path>/scripts/cdf-updateRE.sh > /tmp/smartconnector/${CA_CERT}
```

Example: `/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh >/tmp/smartconnector/${CA_CERT}`

> **Note:** For a cloud installation, log in to the bastion or jump host and run the `cdf-updateRE.sh` script:
>
> arcsight-platform-cloud-installer/cdf-deployer/scripts/cdf-updateRE.sh

4. Move the following files from Transformation Hub to the SmartConnector STORES directory:
   - `/tmp/smartconnector/ ${COMMON_NAME}.signed.crt`
   - `/tmp/smartconnector/${COMMON_NAME}.issue_ca.crt`
   - `/tmp/smartconnector/${COMMON_NAME}.signed.cert.with.ca.crt`
   - `/tmp/smartconnector/${CA_CERT}`

Updating the Keystore and Creating a Truststore on the SmartConnector Server

1. Update SmartConnector keystore with signed certificate:

   Linux commands:

   ```
   cd ${STORES}/
   ```

   ```
   $CURRENT/jre/bin/keytool -importcert -alias ${TH} -keystore
   ${TH}.keystore.bcfips -trustcacerts -file ${COMMON_
   NAME}.signed.cert.with.ca.crt -storepass ${STORE_PASSWD} ${BC_OPTS}
   ```

   Verification: Run this command to verify the keystore. It must only have one entry in the key store.

   ```
   $CURRENT/jre/bin/keytool -v -list -keystore ${TH}.keystore.bcfips -
   storepass ${STORE_PASSWD} ${BC_OPTS} |grep -i alias
   ```

   Windows commands:

   ```
   cd %STORES%\
   ```

```
%CURRENT%\jre\bin\keytool -importcert -alias %TH% -keystore
%TH%.keystore.bcfips -trustcacerts -file %COMMON_
NAME%.signed.cert.with.ca.crt -storepass %STORE_PASSWD% %BC_OPTS%
```

Verification: Run this command to verify keystore. It must only have one entry in the key store.

```
%CURRENT%\jre\bin\keytool -v -list -keystore %TH%.keystore.bcfips -
storepass %STORE_PASSWD% %BC_OPTS% |grep -i alias
```

2. Create the SmartConnector truststore:

Linux commands:

```
cd ${STORES}/
```

```
$CURRENT/jre/bin/keytool -importcert -alias reca -trustcacerts -file
${CA_CERT} -keystore ${TH}.truststore.bcfips -storepass ${STORE_PASSWD}
${BC_OPTS}
```

When prompted, specify **yes** to trust the certificate.

Windows commands:

```
cd %{STORES}%/
```

```
%CURRENT\jre\bin\keytool -importcert -alias reca -trustcacerts -file %CA_
CERT% -keystore %TH%.truststore.bcfips -storepass %STORE_PASSWD% %BC_
OPTS%
```

When prompted, specify **yes** to trust the certificate.

Running the SmartConnector Setup

1. Run the following commands and note the keystore and truststore paths:

Linux commands:

```
echo ${STORES}/${TH}.keystore.bcfips
echo ${STORES}/${TH}.truststore.bcfips
```

Windows commands:

```
echo %STORES%\%TH%.keystore.bcfips
echo %STORES%\%TH%.truststore.bcfips
```

2. Navigate to the `bin` directory and run the agent setup script to install a connector with Transformation Hub as the destination.

   Linux commands:

   ```
   cd <installation dir>/current/bin
   ```

   ```
   ./runagentsetup.sh
   ```

   Windows commands:

   ```
   cd <installation dir>\current\bin
   ```

   ```
   runagentsetup.bat
   ```

3. Set **Use SSL/TLS** to **true**.
4. Set **Use SSL/TLS Authentication** to **true**.
5. When completing the Transformation Hub destination fields, use the value noted from step 2 for the truststore paths and the password used above for the truststore passwords.

Configuring a SmartConnector with Transformation Hub Destination with Client Authentication in Non-FIPS Mode

Follow these steps to configure a SmartConnector with a Transformation Hub (TH) destination with client authentication, in non-FIPS mode.

> You will need to supply an intermediate certificate and key.

Preparing the SmartConnector Server

1. Prepare the SmartConnector:
   - **If the connector is not yet installed:**
     a. Run the installer.
     b. After the core software is installed, do the following in the window that opens: select **Select Global Parameters** > **Set FIPS Mode**, and set the FIPS Mode to **Disabled**.

- **If the connector is already installed:**
  a. Run the installer.
  b. Select **Set Global Parameters** > **Set FIPS Mode**, and set the FIPS Mode to **Disabled**.

2. Navigate to the Connector's `current` directory:

   Linux command:

   ```
   cd <install dir>/current
   ```

   Windows command:

   ```
   cd <install dir>\current
   ```

3. Set the environment variables for the static values used by `keytool`:

   Linux commands:

   ```
   export CURRENT=<full path to this "current" folder>
   ```

   Example:`export CURRENT=/opt/CONNECTORS/TA003/current`

   ```
   export TH=<Transformation Hub hostname>_<Transformation Hub port>
   ```

   Example:`export TH=15.214.***.**`

   ```
   export CA_CERT=re_ca.cert.pem
   ```

   Example:`export CA_CERT=re_ca.crt.pem`

   ```
   export STORE_PASSWD=changeit
   export STORES=${CURRENT}/user/agent/stores
   export COMMON_NAME=<your.connector.fqdn>
   ```

   Windows commands:

   ```
   set CURRENT=<full path to this "current" folder>
   set TH=<Transformation Hub hostname>_<Transformation Hub port>
   set STORES=%CURRENT%\user\agent\stores
   set STORE_PASSWD=changeit
   ```

4. Create the `${CURRENT}/user/agent/stores` directory if it does not already exist.

   Linux command:

   ```
   mkdir -p ${STORES}
   ```

Windows command:

```
mkdir -p %STORES%
```

Creating the Keystore for SmartConnector on the SmartConnector Server

Follow the applicable steps according to your platform type, Windows or Linux

1. Create the keystore for SmartConnector:

   Linux commands:

   ```
   cd ${STORES}
   ```

   ```
   $CURRENT/jre/bin/keytool -keystore ${TH}.keystore.jks -genkeypair -dname
   "cn=your.connector.fqdn, ou=ArcSight, o=Micro Focus, c=US" -keyalg rsa -
   keysize 2048 -alias ${TH} -startdate -1d -validity 366 -storepass
   ${STORE_PASSWD} -keypass ${STORE_PASSWD}
   ```

   Window commands:

   ```
   cd %STORES%
   ```

   ```
   %CURRENT%\jre\bin\keytool -keystore %TH%.keystore.jks -genkeypair -dname
   "cn=your.connector.fqdn, ou=ArcSight, o=Micro Focus, c=US" -keyalg rsa -
   keysize 2048 -alias %TH% -startdate -1d -validity 366 -storepass %STORE_
   PASSWD% -keypass %STORE_PASSWD%
   ```

2. Create the certificate signing request (CSR) for SmartConnector:

   Linux command:

   ```
   $CURRENT/jre/bin/keytool -certreq -alias ${TH} -keystore
   ${TH}.keystore.jks -file ${COMMON_NAME}.csr -storepass ${STORE_PASSWD}
   ```

   Windows command:

   ```
   %CURRENT%\jre\bin\keytool -certreq -alias %TH% -keystore
   %TH%.keystore.jks -file %COMMON_NAME%.csr -storepass %STORE_PASSWD%
   ```

3. Copy the CSR file `${COMMON_NAME}.csr` to the Transformation Hub `/tmp` folder:

   ```
   cp ${COMMON_NAME}.csr /tmp/
   ```

Signing the SmartConnector Certificate Signing Request on Transformation Hub

1. Set the environment:

```
export CA_CERT=re_ca.cert.pem
export COMMON_NAME=<your.connector.fqdn>
export TH=<Transformation Hub hostname>_<Transformation Hub port>
```

> **Note:** Use the same values that you specified in the smartconnector server.

2. Sign the smartconnector certificate signing request:

```
mkdir /tmp/smartconnector
mv ${COMMON_NAME}.csr /tmp/smartconnector/
cd /tmp/smartconnector
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o json
2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n core
-o json 2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-cbc -
md sha256 -a -d -pass pass:"${PASSPHRASE}")
export CSR=$(cat ${COMMON_NAME}.csr)
```

```
WRITE_RESPONSE=$(kubectl exec -it -n core ${VAULT_POD} -c vault -- bash -
c "VAULT_TOKEN=$VAULT_TOKEN vault write -tls-skip-verify -format=json
RE/sign/coretech csr=\"${CSR}\"") && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .certificate" > ${COMMON_
NAME}.signed.crt && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .issuing_ca" > ${COMMON_
NAME}.issue_ca.crt && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .certificate, if .ca_chain then
.ca_chain[] else .issuing_ca end" > ${COMMON_
NAME}.signed.cert.with.ca.crt
```

The signed certificate is in file `${COMMON_NAME}.signed.crt`.

The issuing CA is in file `${COMMON_NAME}.issue_ca.crt`.

The signed certificate with CA chain is in file `${COMMON_NAME}.signed.cert.with.ca.crt`.

3. Retrieve the RE certificate.

```
/<TH Home Path>/scripts/cdf-updateRE.sh > /tmp/${CA_CERT}
```

Example: `/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh >${CA_CERT}`

> **Note:** For a cloud installation, log in to the bastion or jump host and run the `cdf-updateRE.sh` script:
>
> arcsight-platform-cloud-installer/cdf-deployer/scripts/cdf-updateRE.sh

Move the following files from the Transformation Hub to the connector `STORES` directory:

- `/tmp/smartconnector/ ${COMMON_NAME}.signed.crt`
- `/tmp/smartconnector/${COMMON_NAME}.issue_ca.crt`
- `/tmp/smartconnector/${COMMON_NAME}.signed.cert.with.ca.crt`
- `/tmp/smartconnector/${CA_CERT}`

Updating the Keystore and Create a Truststore on the SmartConnector Server

1. Update the SmartConnector keystore with a signed certificate.

   Linux commands:

   ```
   cd ${STORES}/
   ```

   ```
   $CURRENT/jre/bin/keytool -importcert -alias ${TH} -keystore
   ${TH}.keystore.jks -trustcacerts -file ${COMMON_
   NAME}.signed.cert.with.ca.crt -storepass ${STORE_PASSWD}
   ```

   When prompted, specify **yes** to trust the certificate.

   Verification: Run the following command to verify the keystore, and ensure that it has only one entry in the keystore.

   ```
   $CURRENT/jre/bin/keytool -v -list -keystore ${TH}.keystore.jks -storepass
   ${STORE_PASSWD} |grep -i alias
   ```

   Windows commands:

   ```
   cd %STORES%\
   ```

   ```
   %CURRENT%\jre\bin\keytool -importcert -alias %TH% -keystore
   %TH%.keystore.jks -trustcacerts -file %COMMON_
   NAME%.signed.cert.with.ca.crt -storepass %STORE_PASSWD%
   ```

   Verfication: Run the following command to verify the keystore, and ensure that it has only one entry in the keystore.

```
%CURRENT%\jre\bin\keytool -v -list -keystore %TH%.keystore.jks -storepass
%STORE_PASSWD% |grep -i alias
```

2. Create the SmartConnector truststore.

   Linux commands:

   ```
   cd ${STORES}/
   ```

   ```
   $CURRENT/jre/bin/keytool -importcert -alias CARoot -trustcacerts -file
   ${CA_CERT} -keystore ${TH}.truststore.jks -storepass ${STORE_PASSWD}
   ```

   When prompted, specify **yes** to trust the certificate.

   Windows command:

   ```
   %CURRENT%\jre\bin\keytool -importcert -alias CARoot -trustcacerts -file
   %CA_CERT% -keystore %TH%.truststore.jks -storepass %STORE_PASSWD%
   ```

   When prompted, specify **yes** to trust the certificate.

Run the SmartConnector Setup

1. Run the following command and note the trust store path:

   Linux commands:

   ```
   echo ${STORES}/${TH}.keystore.jks
   ```

   ```
   echo ${STORES}/${TH}.truststore.jks
   ```

   Windows commands:

   ```
   echo %STORES%\%TH%.keystore.jks
   ```

   ```
   echo %STORES%\%TH%.truststore.jks
   ```

2. Navigate to the bin directory, and run agent setup script to install a connector with Transformation Hub as the destination.

   Linux commands:

   ```
   cd <installation dir>/current/bin
   ```

```
./runagentsetup.sh
```

Windows commands:

```
cd <installation dir>\current\bin
```

```
runagentsetup.bat
```

3. Set **Use SSL/TLS** to **true**.
4. Set **Use SSL/TLS Authentication** to **true**.
5. When completing the Transformation Hub destination fields, use the value noted from Step 1 for the key store and trust store paths and the password used above for the store password.

Configuring a SmartConnector with a Transformation Hub Destination without Client Authentication in FIPS Mode

Follow these steps to configure a SmartConnector with a Transformation Hub destination without client authentication in FIPS mode.

Preparing the SmartConnector Server

1. Prepare the SmartConnector:
   - **If the connector is not yet installed:**
     a. Run the installer.
     b. After the core software is installed, do the following in the window that opens: select **Select Global Parameters** > **Set FIPS Mode**, and set the FIPS Mode to **Disabled**.
   - **If the connector is already installed:**
     a. Run the installer.
     b. Select **Set Global Parameters** > **Set FIPS Mode**, and set the FIPS Mode to **Enabled**.
2. Navigate to the Connector's `current` directory:

   Linux command:

   ```
   cd <install dir>/current
   ```

Windows command:

```
cd <install dir>\current
```

3. Set the environment variables for the static values used by `keytool`:

Linux commands:

```
export CURRENT=<full path to this "current" folder>
```

```
export BC_OPTS="-storetype BCFKS -providername BCFIPS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
${CURRENT}/lib/agent/fips/bc-fips-1.0.2.jar -J-
Djava.security.egd=file:/dev/urandom"
```

For Connector 8.0, use `bc-fips-1.0.0.jar` in the command above.

```
export TH=<Transformation Hub hostname>_<Transformation Hub port>
export STORES=${CURRENT}/user/agent/stores
export STORE_PASSWD=changeit
export TH_HOST=<TH master host name>
export CA_CERT=re_ca.cert.pem
export FIPS_CA_TMP=/opt/fips_ca_tmp
```

Windows commands:

```
set CURRENT=<full path to this "current" folder>
```

```
set BC_OPTS="-storetype BCFKS -providername BCFIPS -J-
Djava.security.egd=file:/dev/urandom -providerpath
${CURRENT}/lib/agent/fips/bc-fips-1.0.2.jar -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider"
```

```
set TH=<Transformation Hub hostname>_<Transformation Hub port>
set STORES=%CURRENT%\user\agent\stores
set STORE_PASSWD=changeit
set TH_HOST=<TH master host name>
set CA_CERT=C:\Temp\ca.cert.pem
set INTERMEDIATE_CA_CRT=C:\Temp\intermediate.cert.pem
set FIPS_CA_TMP=C:\Temp\fips_ca_tmp
```

4. Create the `${CURRENT}/user/agent/stores` directory if it does not already exist.

Linux command:

```
mkdir -p ${STORES}
```

Windows command:

```
mkdir -p %STORES%
```

5. Apply the following workaround for a Java `keytool` issue:
   a. Create a new file, `agent.security`, in the applicable location for Linux or Windows:
      - **Linux:** `${CURRENT}/user/agent`
      - **Windows:** `%CURRENT%\current\user\agent`
   b. Add the following content to the newly created file, and then save it:

      ```
      security.provider.1=org.bouncycastle.jcajce.provider.BouncyCastleFipsP
      rovider
      security.provider.2=com.sun.net.ssl.internal.ssl.Provider BCFIPS
      security.provider.3=sun.security.provider.Sun
      ```

   c. Move the `${CURRENT}/lib/agent/fips/bcprov-jdk15on-168.jar` file to the `current` directory.

Creating a CA CERT File on Transformation Hub

Follow these steps to create a `${CA_CERT}` file with the content of the root CA certificate:

1. Set the environment:

   ```
   export CA_CERT=re_ca.cert.pem
   ```

2. Create a certificate:

   ```
   /<TH Home Path>/scripts/cdf-updateRE.sh > /tmp/${CA_CERT}
   ```

   Example: `/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/${CA_CERT}`

   > **Note:** For a cloud installation, log in to the bastion or jump host and run the `cdf-updateRE.sh` script:
   >
   > arcsight-platform-cloud-installer/cdf-deployer/scripts/cdf-updateRE.sh

3. Move this file from Transformation Hub to the connector STORES directory.

Creating Truststore on the SmartConnector Server

Create truststore by running the following command:

Linux command:

```
$CURRENT/jre/bin/keytool -noprompt -importcert -storepass ${STORE_PASSWD} -
destkeystore ${STORES}/${TH}.truststore.bcfips -alias reca -file ${CA_CERT} -
storetype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
${CURRENT}/lib/agent/fips/bc-fips-1.0.2.jar
```

When prompted, specify **yes** to trust the certificate.

Windows command:

```
%CURRENT%\jre\bin\keytool -noprompt -importcert -storepass %STORE_PASSWD% -
destkeystore %STORES%\%TH%.truststore.bcfips -alias reca -file %CA_CERT% -
storetype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
%CURRENT%\lib\agent\fips\bc-fips-1.0.2.jar
```

When prompted, specify **yes** to trust the certificate.

Running the SmartConnector Setup

1. Run the following command and note the keystore and truststore paths:

   Linux command:

   ```
   echo ${STORES}/${TH}.truststore.bcfips
   ```

   Windows command:

   ```
   echo %STORES%\%TH%.truststore.bcfips
   ```

2. Navigate to the bin directory and run the agent setup script to install a connector with Transformation Hub as the destination.

   Linux commands:

   ```
   cd <installation dir>/current/bin
   ```

   ```
   ./runagentsetup.sh
   ```

Windows commands:

```
cd <installation dir>\current\bin
```

```
runagentsetup.bat
```

3. Set **Use SSL/TLS** to **true**.
4. Set **Use SSL/TLS Authentication** to **false**.
5. When completing the Transformation Hub destination fields, use the value noted from Step 2 for the truststore paths and the password used above for the truststore passwords.

Cleaning up the Certificate File

Run the following command to delete the certificate file:

> **Caution:** The following file should be deleted to prevent the distribution of security certificates that could be used to authenticate against the Transformation Hub. These files are very sensitive and must not be distributed to other machines.

Linux command:

```
rm ${STORES}/${CA_CERT}
```

Windows command:

```
del %\STORES%\%CA_CERT%
```

Configuring ArcMC to Manage a Transformation Hub

> **Note:** For cloud Transformation Hub, you must complete the configuration procedures detailed in:
>
> - Completing Integration with AWS Transformation Hub
>
> before you perform the procedures in this section.

The following instructions apply only to the standalone version of ArcMC. You do not need to configure the ArcMC capability deployed in the ArcSight Platform to manage Transformation Hub in the same cluster because the system automatically configures the capability.

> **For AWS deployments only - in case Transformation Hub is not automatically managed by the ArcSight Platform ArcMC:** After the deployment, verify that the Target Groups and Listeners for ports 443 and 32080 have been created, and then execute the procedure below to manually configure the ArcMC management of Transformation Hub.

ArcMC serves as the management UI for Transformation Hub. In order for ArcMC to manage a Transformation Hub, the Transformation Hub must be added as a managed host to ArcMC.

This process will include these steps, which are explained below:

Standalone ArcMC Instructions

- "Retrieving the ArcMC certificate " below
- "Configuring the OMT cluster" below
- "Configuring ArcMC:" on the next page

Standalone ArcMC Instructions

Retrieving the ArcMC certificate

1. Log into ArcMC.
2. Click **Administration > System Admin > SSL Server Certificate > Generate Certificate.**
3. On the **Enter Certificate Settings** dialog, specify the required settings. In **Hostname**, your certificate settings must match the FQDN of your ArcMC.
4. Click **Generate Certificate.**
5. Once the certificate is generated, click **View Certificate** and copy the full content from `--BEGIN cert to END cert--` to the clipboard.

Configuring the OMT cluster

1. Log in to the OMT management portal.
2. Select **Deployment > Deployments.**
3. Click **...** (Browse) on the far right and choose **Reconfigure**. A new screen will be opened in a separate tab.
3. Scroll down to the Management Center Configuration section. Then, specify values as described for the following:
   - **Username:** `admin`
   - Password: Use your Transformation Hub password.
   - Enter the ArcMC hostname and port 443 (for example, `arcmc.example.com:443`). If ArcMC was installed as a non-`root` user, specify port 9000 instead.

- **ArcMC certificates:** Paste the text of the generated OMT server certificates for Core ArcMC (or Standalone ArcMC generated certificate) you copied to the clipboard as described above.

4. Click **Save**. Web services pods in the cluster will be restarted

Configuring ArcMC:

1. Log in to the ArcMC.
2. Click **Node Management > View All Nodes.**
3. In the navigation bar, click Default (or the ArcMC location where you wish to add Transformation Hub). Then click **Add Host,** and specify the following values:
   - **Type:** Select Transformation Hub - Container Deployment Foundation (CDF) (former name for the OMT)
   - **Hostname:** Virtual IP of the Transformation Hub for an HA environment, or master node hostname for any single-master node environment.
   - **Port**: 32080
   - **Cluster Port:** 443
   - **Cluster Username:** admin
   - **Cluster Password:** <use OMT Management Portal password>
   - **Cluster Certificate:** Paste the contents of the OMT certificate you copied earlier.
4. Click **Add**. The Transformation Hub is added as a managed host.

Understanding How Data is Produced and Consumed

Transformation Hub's publish-subscribe messaging system uses SmartConnectors to produce event data, and supports Logger, Recon, and ESM, as well as Apache Hadoop and other third-party consumers.

While Transformation Hub can support a very high event flow (millions of events per second), the event rate for each producer and consumer will generally be much smaller (tens of thousands of events per second). Actual event flow will depend on your specific implementation and tuning applied, as well as server resources available, such as memory and CPU.

Producing Events with SmartConnectors

SmartConnectors can publish events to Transformation Hub topics. In order to publish events, you must configure your SmartConnectors to use the Transformation Hub destination. To send

events to multiple topics, you can configure multiple concurrent destinations with the same Transformation Hub using different topics.

Once configured with a Transformation Hub destination, the SmartConnector sends events to Transformation Hub's Kafka cluster, which can then further distribute events to real-time analysis and data warehousing systems. Other applications, including Recon, ESM, Logger, and any third-party application that supports retrieving data from Kafka can receive them, for example, Apache Hadoop.

Transformation Hub balances incoming events between nodes, by distributing them evenly between the partitions in the configured topic.

Acknowledgments ("acks") ensure that Transformation Hub has received the event before the SmartConnector removes it from its local queue. You can disable acknowledgments, require acknowledgment only from the primary replica, or require every replica to acknowledge the event.

> Acknowledgments do not indicate that consumers, such as Logger, have received the event data, only that Transformation Hub itself has.

Supported SmartConnector versions encode their own IP address as meta-data in the Kafka message for consumers that require that information such as Logger Device Groups.

- For information on supported SmartConnector versions, see the SmartConnectors 24.2 Grand List (A-Z).
- For more information about SmartConnectors and how to configure a Transformation Hub destination, refer to the **CEF Destinations** chapter of the **SmartConnect Install and User Guide** in ArcSight SmartConnectors 24.2 documentation.

Legacy OpenText documentation is available for download from the OpenText support community.

Consuming Events with ESM

ESM agents are the consumers for Transformation Hub's publish-subscribe messaging system. An ESM agent can connect to Transformation Hub and consume all events in binary or Avro format for the topics to which it is subscribed.

Additionally, ESM provides data monitors to monitor Transformation Hub health.

- For information on supported versions of ESM and SmartConnectors, see the SmartConnectors 24.2 Grand List (A-Z)
- For instructions on configuring a supported version of ESM as a consumer, see the *ESM Administrator's Guide*.

Consuming Events with Logger

To subscribe to Transformation Hub topics with Logger, you must configure a receiver on a supported Logger version to receive the Transformation Hub events. Logger's Transformation Hub receivers are consumers for Transformation Hub's publish-subscribe messaging system. They receive events in Common Event Format (CEF) from Transformation Hub topics. A Logger Transformation Hub receiver connects to Transformation Hub and consumes all events for the topics it subscribes to.

When configuring a Logger Transformation Hub receiver, specify the worker node FQDNs, topics to consume from, and consumer group name. You can configure multiple Loggers to consume from the same topic as a part of a consumer group.

For more information about Logger and how to configure a Transformation Hub receiver, refer to the Logger 7.3 Administrator's Guide.

> Kafka consumers can take up to 24 hours for the broker nodes to balance the partitions among the consumers. Check the Transformation Hub Kafka Manager **Consumers** page to confirm all consumers are consuming from the topic.

Sending Transformation Hub Data to Logger

For a Logger to be able to consume Transformation Hub events, the Logger must have a Transformation Hub receiver configured with the Transformation Hub worker nodes, consumer group, and event topic list. SmartConnectors that send data to Transformation Hub must have a Transformation Hub destination.

A group of Loggers, called a pool, can be configured to receive and distribute events between themselves. This works similarly to the Logger pool created by using the Logger Smart Message Pool destination on SmartConnectors. The difference is that when the SmartConnectors have a Logger Smart Message Pool destination, the event load is balanced by each SmartConnector, but when the SmartConnectors have a Transformation Hub destination, the event load is balanced by the Loggers.

Additional Loggers can be added to the pool simply by configuring the same Transformation Hub worker nodes, consumer group, and event topic list in the new Logger's Transformation Hub receivers, without having to reconfigure either the existing Loggers or any SmartConnectors.

The events retrieved by the Logger pool are distributed among the Loggers in the pool. If one Logger is down, new events are rebalanced among existing Loggers. When a Logger is added or removed from the Consumer Group, the event load is distributed across the pool of Loggers.

To send events from a group of SmartConnectors to a pool of Loggers, configure their Transformation Hub destinations to send events to the topic from which the Logger pool is consuming.

To configure Logger to subscribe to event data from specific SmartConnectors, you can do either of the following:

- Configure all the SmartConnectors to publish events to the same topic. Configure the Logger's Transformation Hub receiver to subscribe to this event topic.
- Configure each SmartConnector to publish events to different topics and then configure the Transformation Hub receiver on the Logger to subscribe to multiple event topics.

> **Tip:** Loggers in the same Logger pool do not consume the same events, since they are in the same Consumer Group. In high availability situations, you need events to be stored on two different Loggers. To store the same events on two Loggers, configure the Loggers to have different Consumer Group names, but subscribe them to the same event topic.

The number of Loggers in a Logger pool is restricted by the number of event topic partitions configured on the Container Deployment Foundation. For example, if there are only five partitions configured, only five Loggers will receive the events. If you have more than five Loggers configured in the same Consumer Group, some Loggers will not normally receive events, but will be available as hot spares. When adding receivers, be sure to increase the number of event topic partitions. See Managing Topics for more information.

Procedure to Send Transformation Hub Data to Logger

1. Configure the SmartConnector:
   - Set up a SmartConnector to publish to a particular Transformation Hub topic. Connectors can only send to a single topic for each destination. Additional destinations need to be configured if each event needs to go to multiple topics. Note the number of partitions in the topic.
   - For more information about SmartConnectors and how to configure a Transformation Hub destination, refer to the **CEF Destinations** chapter in the ArcSight SmartConnectors 24.2 documentation.
2. Configure Logger:
   - Create a Transformation Hub receiver on each Logger in the Logger pool.
   - Configure each receiver to subscribe to the topics to which the SmartConnectors are publishing data. To subscribe to multiple topics, indicate the topics by specifying them in the Event Topic List parameter (a list of comma-separated values) while configuring the Transformation Hub receiver.
   - Configure each receiver to be in the same Consumer Group.

Example Setup with Multiple Loggers in a Pool

You can set up your Logger pools to subscribe to events from a particular device type, such as "Firewall." To do this, you would:

1. In ArcMC, create a Kafka topic named *Firewall*.
2. Configure all the SmartConnectors that handle firewall events to publish these events to topic "Firewall."
3. Configure the Loggers in the Logger pool:
   - Create a Transformation Hub Receiver on each Logger in the pool.
   - Configure the receivers to subscribe to the event topic “Firewall,” and include them in the “Logger_Firewall” Consumer Group.

Once the configuration is set up properly, the Logger pool will subscribe to device type *Firewall*.

> This example assumes that the Transformation Hub is being managed by an ArcSight Management Center for topic creation. Topics can also be managed through the Kafka Manager UI.

Consuming Events with Third-Party Applications

Transformation Hub is designed with support for third-party tools. You can create a standard Kafka consumer and configure it to subscribe to Transformation Hub topics. By doing this you can pull Transformation Hub events into your own data lake.

> Custom consumers must use Kafka client libraries of version 0.11 or later.

- All Transformation Hub nodes, consumers, and producers must be properly configured for forward and reverse DNS lookup, and be time-synchronized, using a time server such as NTP.
- Events are sent in standard CEF (CEF text), binary (exclusively for ESM consumption), or Avro format. Any software application that can consume from Kafka and handle the event format can process events.
- You can set up multiple consumer groups, and each group will get a copy of every event. Therefore you can have Logger and Apache Hadoop configured to consume from the same topic and each will get a copy of every event. This enables fanning out multiple copies of events without reconfiguring SmartConnectors or using additional CPU or network resources for them.

Consuming Transformation Hub Events with Apache Hadoop

Apache Hadoop is a software framework that enables the distributed processing of large data sets across clusters of computers. You can send Transformation Hub events to Hadoop by using Apache Flume.

This section describes how to set up the Apache Flume agent to transfer Common Event Format (CEF) events from an Transformation Hub Kafka cluster to Hadoop Distributed File System (HDFS).

Architecture for Kafka to Hadoop Data Transfer

Apache Flume uses a source module to read a Kafka topic containing CEF events, and it then transfers the events using a memory channel, and persists them to HDFS using a sink module. The CEF files are stored on HDFS by time, in a year/month/day/hour directory structure.

Using Apache Flume to Transfer Events to Hadoop

One of the applications you could use to transfer Transformation Hub events into your data lake is Apache Flume. Flume is designed to push data from many sources to the various storage systems in the Hadoop ecosystem, such as HDFS and HBase. This section describes how to use Apache Flume as a data transfer channel to transfer events from Transformation Hub to Apache Hadoop or other storage systems.

Prerequisites

- Transformation Hub installed.
- Flume installed: For information on how to install and configure Flume, refer to the *Flume documentation*.
- Storage system installed: Refer to your storage system documentation.

Procedure

Flume is controlled by an agent configuration file. You must configure Transformation Hub as the source agent, your storage system as the sink agent, and ZooKeeper as the channel agent in this file.

To configure Transformation Hub as the source:

Edit the agent configuration file to include the required properties, as in the table below. Configure other properties as needed for your environment.

Required Kafka Source Configuration

Property	Description
`type`	Set to `org.apache.flume.source.kafka.KafkaSource`.
`topic`	The Event Topic from which this source reads messages. Flume supports only one topic per source.

To configure the sink:

The required configuration varies. Refer to the Flume documentation for details on your storage system. The section Consuming Events with Apache Flume provides an example of how to configure Apache Hadoop as the sink.

Setting Up Flume to Connect with Hadoop

In the simplest deployment model, you need to deploy the Apache Flume agent on a Hadoop node server to pull events, and send them to Hadoop Distributed File System (HDFS).

Hadoop must be installed before you can connect it with Flume. If you do not already have your own Hadoop deployment, you can deploy Hadoop on a Red Hat Enterprise Linux 7.2 host. For more information, see Securing HDFS for Intelligence.

For a detailed discussion of connecting Apache Flume with Hadoop, consult the *Apache Documentation*.

Sample Flume Configuration File

Before starting Apache Flume, create a configuration file based on the template below.

The configuration file should reside in `bin/flume/conf/`. This file is called *kafka.conf* in our example. You can name your own configuration file whatever is appropriate.

```
#####################################################
```

```
#Sample Flume/Kafka configuration file
```

```
#####################################################
```

```
#defines Kafka Source, Channel, and Destination aliases
```

```
tier1.sources = source1
```

```
tier1.channels = channel1
```

```
tier1.sinks = sink1
```

```
#Kafka source configuration
tier1.sources.source1.type = org.apache.flume.source.kafka.KafkaSource
tier1.sources.source1.kafka.bootstrap.servers= kafkaIP1:9092, kafkaIP2:9092,…
tier1.sources.source1.kafka.topics = th-cef
tier1.sources.source1.kafka.consumer.group.id = flume
tier1.sources.source1.channels = channel1
tier1.sources.source1.interceptors = i1
tier1.sources.source1.interceptors.i1.type = timestamp
tier1.sources.source1.kafka.consumer.timeout.ms = 150
tier1.sources.source1.kafka.consumer.batchsize = 100
#Kafka Channel configuration
tier1.channels.channel1.type = memory
tier1.channels.channel1.capacity = 10000
tier1.channels.channel1.transactionCapacity = 1000
#Kafka Sink (destination) configuration
tier1.sinks.sink1.type = hdfs
tier1.sinks.sink1.channel = channel1
tier1.sinks.sink1.hdfs.path = hdfs://localhost:9000/opt/\
hadoop/cefEvents/year=%y/month=%m/day=%d
tier1.sinks.sink1.hdfs.rollInterval = 360
tier1.sinks.sink1.hdfs.rollSize = 0
tier1.sinks.sink1.hdfs.rollCount = 0
```

```
tier1.sinks.sink1.hdfs.fileType = DataStream
```

```
tier1.sinks.sink1.hdfs.filePrefix = cefEvents
```

```
tier1.sinks.sink1.hdfs.fileSuffix = .cef
```

```
tier1.sinks.sink1.hdfs.batchSize = 100
```

```
tier1.sinks.sink1.hdfs.timeZone = UTC
```

Setting Up Hadoop

This is an overview of the steps necessary to install Apache Hadoop 2.7.2 and set up a one-node cluster. For more information, refer to the *Hadoop Documentation* for your version.

To install Hadoop:

1. Be sure that your environment meets the operating system and Java prerequisites for Hadoop.
2. Add a user named 'hadoop'.
3. Download and unpack Hadoop.
4. Configure Hadoop for pseudo-distributed operation.
   - Set the environment variables.
   - Set up passphraseless SSH.
   - Optionally, set up Yarn. (You will not need Yarn if you want to use Hadoop only for storage and not for processing.)
   - Edit the Hadoop configuration files to set up a core location, a Hadoop Distributed File System (HDFS) location, a replication value, a NameNode and a DataNode.
   - Format the Name node.
5. Start the Hadoop server using the tools provided.
6. Access Hadoop Services in a browser and login as the user "hadoop."
7. To create the Hadoop cefEvents directory, run the following command:

   ```
   hadoop fs -mkdir /opt
   hadoop fs -mkdir /opt/hadoop
   hadoop fs -mkdir /opt/hadoop/cefEvents
   ```

8. To grant permissions for Apache Flume to write to this HDFS, run the following command:

```
hadoop fs -chmod 777 -R /opt/hadoop
hadoop fs -ls
```

9. To check Hadoop system status, run the following command:

```
hadoop dfsadmin -report
```

10. To view the files transferred by Flume to Hadoop, run the following command:

```
hadoop fs -ls -R /
```

Configuring Consumers and Producers for High Availability

Configure the Transformation Hub Kafka cluster endpoint to avoid single points of failure in both the producers sending data to Transformation Hub (such as SmartConnectors), and the consumers subscribing to data from the Transformation Hub (such as Logger and ESM).

For Producers

Configure the **Initial Host:Port(s)** parameter field in the Transformation Hub Destination to include all Kafka broker (worker) nodes as a comma-separated list.

Provide all Kafka broker (worker) nodes for a producer and a consumer configuration to avoid a single point of failure. For example, broker_hostname1:9093, broker_hostname2:9093, broker_hostname3:9093.

For more information about how Kafka handles this using bootstrap.servers, see the *Kafka Documentation*.

For Consumers

Configure the **Transformation Hub host(s) and port** parameter field in the Receiver to include all Kafka cluster nodes as a comma-separated list.

For more information about how Kafka handles this using bootstrap servers, see the *Kafka Documentation*.

Understanding Data Compression

Transformation Hub compression settings affect data in two general places, communication and storage. Specifically, this refers to data stored on disk, in Kafka topic partitions, and data that is in transit.

- All external producers such as connectors and internal producers, like routing and CEF2Avro processors, compress data before sending it.

- For data in transit, data compression is controlled by the producer's configuration.

Data Consumers

There is no property that controls data compression on consumers. Consumers read metadata from each message, which indicates the correct decompression algorithm to use. Since this is evaluated on a message-by-message basis, the consumer's behavior does not depend on which topic it is consuming from. A single topic might contain messages which have been compressed with different compression algorithms (also referred to as compression types or codecs).

Data Storage (Data at Rest)

The algorithm used to compress stored data is determined by the topic configuration. All Transformation Hub topics, except `th-arcsight-avro` and `mf-event-avro-enriched`, currently use the default compression type, which is the same as that used by `producer`. This configuration choice means the topic will retain the original compression algorithm set by the producer. By leaving this as producer-defined, there is flexibility for the producer to send either compressed (using any supported codec) or uncompressed data.

The `mf-event-avro-enriched` topic is an exception because the database scheduler reads from this topic, but does not yet have support for reading messages encoded with the ZStandard (zstd) compression algorithm. Therefore, there is a specific, out-of-the-box value for this topic, to insure that the database scheduler can read it, no matter what over-the-wire compression was used.

Topic	Compression Type	Transformation Hub Version Support
All topics except `th-arcsight-avro` and `mf-event-avro-enriched`	producer (default)	3.4.0 and earlier (3.5.0 and earlier for `mf-event-avro-enriched`)
`th-arcsight-avro`	gzip	3.4.0 and 3.3.0
`th-arcsight-avro`	uncompressed	3.2.0 and earlier
`mf-event-avro-enriched`	gzip	3.5.0

Configuring Compression

There are two places in the Kafka architecture where compression can be configured: the producer and the topic.

- Producer-level compression is set on the producer; for example, in SmartConnector Transformation Hub destination parameters. For producers that reside inside Transformation Hub, such as routing and stream processors, the compression algorithm is

configured on the Transformation Hub configuration page, during deployment.

- Topic-level compression can be set with Kafka Manager (using **Topic > Update Config Menu**); however, it is strongly recommended that settings be left at default values.

Compression Types

While Kafka supports a handful of compression types, Transformation Hub implements only two types: gzip and zstd.

- **gzip:** By default, gzip is used for Transformation Hub routing and stream processors, as well as for SmartConnectors. This is for backward compatibility and might change in a future release.
- **zstd:** Testing has shown that zstd uses less bandwidth, storage, and CPU resources than gzip. For bandwidth constrained networks, higher EPS is typically seen when using zstd; however actual results are unique to each environment. Third-party Java producers should use kafka-clients version 2.1.0 or later, for zstd support. ArcSight consumers compatible with zstd include Logger 7.0, ESM 7.2, IDI 1.1, or later.

Pushing JKS files from ArcMC

You can push JKS (Java Keystore) files to multiple managed SmartConnectors in ArcMC. First, you will upload the files to a file repository in ArcMC, then push them out to their destination SmartConnectors. You must then configure and enable the Kafka destination on all SmartConnectors.

To upload the Java Keystore files:

1. Prepare the .jks files you want to push and store them in a secure network location.
2. In ArcMC, click **Administration > Repositories > New Repository.**
3. In **Name, Display Name**, and **Item Display Name**, specify KAFKA_JKS
4. Enter other required details as needed, then click **Save**.
5. Click **Upload to Repository.**
6. Follow the prompts in the upload wizard and browse to the first .jks file. Make sure to choose the individual file option.
7. Upload as many files as needed by repeating the upload wizard.

To push the files to multiple SmartConnectors:

1. In ArcMC, browse to the file repository for the `.jks` files.
2. Click the **Upload** arrow.

3. Follow the prompts in the wizard and select your destination SmartConnectors.
4. The files are pushed to the managed SmartConnectors and stored in the designated SmartConnector folder.

To configure the Kafka destination on all SmartConnectors:

In ArcMC, click **Node Management > Connectors** tab.

1. Select the SmartConnectors to be configured.
2. Choose **Add a destination** and pick the Kafka destination type.
3. Add the destination details along with the `.jks` path and password, and save the changes.

Integrating Intelligence with ESM

Not applicable for a fresh installation of the ArcSight Platform.

To enable ESM to receive the analysed entities and alerts information from Intelligence, you need to install and configure the ArcSight REST FlexConnectors.

The REST FlexConnector provides a configurable method to collect events from Intelligence and send them to ESM. Intelligence's Alerts and Entities APIs serve as the REST API endpoints from which the REST FlexConnectors collect data.

The REST FlexConnectors use the OAuth2 authentication to get permission to receive events from Intelligence. The events collected by the FlexConnectors are in JSON format.

With the help of one JSON parser file each for Alert data and Entities data, these events are converted into a format that can be understood and received by ESM.

Using the JSON Parser Files

The parser file that is used for alerts data is **alerts.jsonparser.properties**.

```
trigger.node.location=/data
token.count=14
token[0].name=alertId
token[0].type=String
token[0].location=alertId

token[1].name=datasource
token[1].type=String
token[1].location=datasource

token[2].name=alertTime
```

```
token[2].type=Long
token[2].location=timestamp

token[3].name=risk
token[3].type=Integer
token[3].location=risk

token[4].name=contribution
token[4].type=Integer
token[4].location=contribution

token[5].name=significance
token[5].type=String
token[5].location=significance

token[6].name=threat
token[6].type=String
token[6].location=templates/threat

token[7].name=family
token[7].type=String
#token[7].format=__uri()
token[7].location=templates/family

token[8].name=teaser
token[8].type=String
token[8].location=templates/teaser

token[9].name=alert
token[9].type=String
token[9].location=templates/alert

token[10].name=anomalyTypes
token[10].type=String
token[10].location=anomalyTypes

token[11].name=numAnomalies
token[11].type=Integer
token[11].location=numAnomalies

token[12].name=category
token[12].type=String
token[12].location=category

token[13].name=scrollId
token[13].type=String
token[13].location=/scrollId
```

```
#(End Of Token Definitions)

#tokens

event.externalId=alertId
event.deviceCustomNumber1=risk
event.deviceCustomNumber1Label=__stringConstant("RiskScore")
event.deviceCustomNumber2=contribution
event.deviceCustomNumber2Label=__stringConstant("Contribution")
event.deviceCustomNumber3=__safeToLong(__regexToken(alert,.?risk=([^\\s]+)
.*))
event.deviceCustomNumber3Label=__stringConstant("Entity Risk Score")

event.fileName=__regexToken(alert,.?entity name="([^"]+)".*)
event.fileHash=__regexToken(alert,.?hash="([^"]+)".*)
event.fileType=__regexToken(alert,.?type="([^"]+)".*)

event.message=alert
event.reason=teaser
event.aggregatedEventCount=numAnomalies
event.deviceEventCategory=category
event.deviceReceiptTime=__createLocalTimeStampFromSecondsSinceEpoch
(alertTime)

#tags
#event.destinationUserId=id
#event.deviceCustomString5=tags
#event.destinationUserName=otherName
#event.deviceCustomString2=source
#event.message=desc

#Other Mappings
event.name=family
event.deviceEventClassId=threat
event.deviceVendor=__stringConstant("Micro Focus")
event.deviceProduct=__stringConstant("Interset")
event.deviceSeverity=significance

#Agent Severity
severity.map.veryhigh.if.deviceSeverity=9,10
severity.map.high.if.deviceSeverity=7,8
severity.map.medium.if.deviceSeverity=4,5,6
severity.map.low.if.deviceSeverity=2,3
severity.map.verylow.if.deviceSeverity=0,1

#Conditional mappings
conditionalmap.count=1
```

```
conditionalmap[0].field=event.fileType
conditionalmap[0].mappings.count=3

conditionalmap[0].mappings[0].values=user
conditionalmap[0].mappings[0].event.destinationUserName=__regexToken
(alert,.?entity name="([^"]+)".*)

conditionalmap[0].mappings[1].values=ip
conditionalmap[0].mappings[1].event.destinationAddress=__
regexTokenAsAddress(alert,.?entity name="([^"]+)".*)

conditionalmap[0].mappings[2].values=machine
conditionalmap[0].mappings[2].event.destinationHostName=__regexToken
(alert,.?entity name="([^"]+)".*)
```

The parser file that is used for entities data is **entities.jsonparser.properties**.

```
trigger.node.location=/data

token.count=12

token[0].name=entityHash
token[0].type=String
token[0].location=entityHash

token[1].name=entityType
token[1].type=String
token[1].location=entityType

token[2].name=entityName
token[2].type=String
token[2].location=entityName

token[3].name=risk
token[3].type=Integer
token[3].location=risk

token[4].name=riskChange
token[4].type=Integer
token[4].location=riskChange

token[5].name=storyCount
token[5].type=Integer
token[5].location=storyCount

token[6].name=lastActivity
token[6].type=String
```

```
token[6].location=lastActivity

token[7].name=tags
token[7].type=String
token[7].format=__uri()
token[7].location=tags

token[8].name=otherName
token[8].type=String
token[8].location=../../tags/name

token[9].name=source
token[9].type=String
token[9].location=../source

token[10].name=desc
token[10].type=String
token[10].location=../tags/description

token[11].name=scrollId
token[11].type=String
token[11].location=/scrollId

#(End Of Token Definitions)

#tokens

event.fileHash=entityHash
event.fileType=entityType
event.fileName=entityName
event.deviceCustomNumber1=risk
event.deviceCustomNumber1Label=__stringConstant("RiskScore")
event.deviceCustomNumber2=riskChange
event.deviceCustomNumber2Label=__stringConstant("RiskChange")
event.deviceCustomString3=lastActivity
event.deviceCustomString3Label=__stringConstant("LastActivity")
#event.deviceCustomDate1=lastActivity
#__parseMutableTimeStampSilently(start)

#tags
#event.destinationUserId=id
event.deviceCustomString5=tags
#event.destinationUserName=otherName
#event.deviceCustomString2=source
#event.message=desc

#nextUrl?
event.deviceCustomString6=scrollId
```

```
#Other Mappings
event.name=__stringConstant("Interset Risky User Information")
event.deviceEventClassId=__stringConstant("IRU")
event.deviceVendor=__stringConstant("Micro Focus")
event.deviceProduct=__stringConstant("Interset")
event.deviceSeverity=2

#Agent Severity
severity.map.low.if.deviceSeverity=2
```

Installing and Configuring the FlexConnectors

You need to install two REST FlexConnectors: one to collect and parse the Alerts data, and another to collect and parse the Entities data.

> The following section has been verified with the installation of REST FlexConnectors on the Windows 10 platform.

Prerequisites

Complete the following steps before you begin with the REST FlexConnector installation and configuration:

1. Create the `OAuth2.properties` file for using the OAuth2 authentication with Intelligence as follows and save it in the desired location (For example, `C:\Users\Administrator\Desktop\`):

   ```
   client_id= <The client_id value. Click here to identify the client_id
   value.>
   client_secret=<The client_secret value. Click here to identify the
   client_secret value.>
   redirect_uri=http://localhost:8081/oauth2callback
   auth_url=https://<FQDN of ArcSight Platform Virtual IP for HA or single
   master node>/osp/a/default/auth/oauth2/grant
   token_url=https://<FQDN of ArcSight Platform Virtual IP for HA or
   single master node>/osp/a/default/auth/oauth2/grant
   scope=
   timestamp_format_of_api_vendor=
   ```

   To identify the client_id and client_secret values, do the following:

   a. Login to the Management portal as the administrator.

      https://<virtual_FQDN>:5443

b. Click **CLUSTER** > **Dashboard**. You will be redirected to the **Kubernetes Dashboard**.

c. Under **Namespace**, search and select the `arcsight-installer-xxxx` namespace.

d. Under **Config and Storage**, click **Config Maps**.

e. Click the filter icon, and search for `investigator-default-yaml`.

f. Open the `investigator-default-yaml` file and look for the client_id and client_secret values in the **OAuth2 Authentication with OSP** section.

2. Do the following to register the callback URL in OSP. The callback URL is the URL where the OSP directs the user after a successful authentication.

   a. Launch a terminal session and log in to the node where NFS is present.

   b. Change to the following directory:

```
cd <NFS_root_DIRECTORY>/arcsight-volume/sso/default/WEB-
INF/conf/current/default/services/
```

   c. Execute the following command to open the authcfg.xml:

```
vi authcfg.xml
```

   d. Add `<Url>http://localhost:8081/oauth2callback</Url>` within:

```
<RedirectUrlList>
<Url>${EXTERNAL_URI:http://localhost:9191}/mgmt/callback</Url>
<Url>${OSP_CLIENT_REDIRECT_URI_
1:http://localhost:9191/mgmt/callback}</Url>
<Url>${OSP_CLIENT_REDIRECT_URI_
2:http://localhost:9191/mgmt/callback}</Url>
<!-- For InetSoft Reporting Engine -->
<!-- <Url>${EXTERNAL_
URI:http://localhost:8181}/report/openid/login</Url> -->
<Url>${EXTERNAL_URI}/report/openid/login</Url>
<Url>${EXTERNAL_URI}:443/report/openid/login</Url>
<!-- Endpoint to receive authcode -->
<Url>${EXTERNAL_
URI:http://localhost:9090}/interset/api/actions/login/oauth2/callback<
/Url>
<!-- Endpoint required while logout, this will set in target -->
<Url>${EXTERNAL_URI:http://localhost:3002}/interset/</Url>
<!-- For ArcSight SOAR -->
<Url>${EXTERNAL_URI}/soar/oauth-callback</Url>
</RedirectUrlList>
```

e. Execute the following commands to restart OSP by deleting the fusion-single-sign-on container:

```
kubectl get pods --all-namespaces|grep fusion-single-sign-on
kubectl delete pod <fusion-single-sign-on-xxxxxxxxxx-xxxxx> -n
<arcsight-installer-xxxxx>
```

Install and Configure the REST FlexConnector

To install and configure a REST FlexConnector, see ArcSight FlexConnector REST Developer Guide in ArcSight SmartConnectors 24.2 documentation.

Ensure the following when you install and configure the REST FlexConnector:

- Select **ArcSight FlexConnector REST** as the **Connector Type**.
- When adding the parameters information, specify the following:
  - For the Configuration File field, specify only alerts if the FlexConnector is for collecting and parsing alerts data, else specify only entities if the FlexConnector is for collecting and parsing entities data.
  - The **Events URL** depends on the use assigned to the FlexConnector.

    If the FlexConnector is for collecting and parsing alerts data, specify the **Events URL** as:

    https: //<FQDN of ArcSight Platform Virtual IP for HA or single master node>/interset/api/search/0/alerts?sort=timestamp&sortOrder=desc&riskSort=maximum
    If the FlexConnector is for collecting and parsing entities data, specify the **Events URL** as:
    https: //<FQDN of ArcSight Platform Virtual IP for HA or single master node>/interset/api/search/0/topRisky?count=100
  - For the **Authentication Type** field, select **OAuth2**.
  - For the **OAuth2 Client Properties File** field, browse to the location where you have created and saved the **OAuth2.properties** file, then select the file.
- Import the OSP Certificate in the REST FlexConnector.
- When configuring the destination, select either ArcSight Manager (encrypted) or Transformation Hub as the destination. For more information, see **SmartConnector Installation and User Guide** in the ArcSight SmartConnectors 24.2 documentation. When adding the parameters information, specify the following if you have selected Transformation Hub as the destination:
  - For the **Content type** field, select **ESM**.
  - For the **Topic (hover for recommendations)** field, specify either **th-binary_esm** or avro topics.

- For the **For ESM topic, the ESM version** field, select **7.2.x** or above versions.
- To install the FlexConnector as a standalone application (recommended), select **install as a standalone application**, else to install the FlexConnector as a service, select **install as a service.**

Importing the OSP Certificate in the REST FlexConnector

To import the OSP certificate in the REST FlexConnector:

1. Launch a terminal session and log in to any of the Kubernetes nodes.
2. Execute the following command:

```
kubectl exec -it th-kafka-0 -n <namespace> bash
```

3. Navigate to the following directory where the `issue_ca.crt` certificate file is present. This certificate is the OSP Issuer Certificate (CA).

```
cd /vault-crt/RE
```

4. Copy the contents of the `issue_ca.crt` file in a new file, name the file as `issue_ca.cer`, and save it in the desired location (for example, C:\Users\<user_name>\Desktop\).
5. Do the following to import the OSP CA certificate to the FlexConnector truststore cacerts:
   a. Open a command window and navigate to the following location:

```
cd $ARCSIGHT_HOME/current/jre/bin/
```

   b. Execute the following command:

```
./keytool -importcert -file /opt/issue_ca.cer -keystore
"/root/ArcSightSmartConnectors_
Alerts/current/jre/lib/security/cacerts" -storepass changeit
```

   c. When you run this command, you are prompted to provide your input for the following message: “Trust this certificate [no]:” Specify Yes.

Performing FlexConnector Post-Installation Tasks

After you install and configure the FlexConnector and before you run the FlexConnector, copy the desired JSON parser files in the **ARCSIGHT_HOME\user\agent\flexagent** location.

Installing ESM and Configuring Transformation Hub with ESM

Installing ESM

To install ESM and ArcSight Console to leverage Intelligence entities and alerts information, see Installation Guide for ESM.

Configuring Transformation Hub with ESM

To configure Transformation Hub with ESM, see Configuring ESM as a Transformation Hub Consumer

Sending Data to Transformation Hub From Intelligence

To send data to Transformation Hub from Intelligence, you need to start the FlexConnector. You can run the FlexConnector in standalone mode or as a service, depending on the mode you selected during installation.

Running in Standalone Mode

If you have installed the FlexConnector in the standalone mode, you need to start it manually (periodically or as per your requirement). Also, you need to start the FlexConnector whenever the host on which it is installed is restarted, because the FlexConnector is not automatically active when the host is restarted.

Perform the following steps to start the FlexConnector agent so that it can send the entities and alerts information from Intelligence to the configured topic.

1. Navigate to:

   ```
   cd $ARCSIGHT_HOME\current\bin\
   ```

2. Execute the following command:

   ```
   ./arcsight agents
   ```

Running as a Windows Service

To start or stop the FlexConnector installed as a service on the Windows platform:

1. Right-click **My Computer**, then select **Manage** from the **Context** menu.
2. Expand the **Services and Applications** folder and select **Services**.

3. Right-click the FlexConnector service name and select **Start** to run the FlexConnector or **Stop** to stop the service.

To verify that the FlexConnector service has started, view the following file:

```
$ARCSIGHT_HOME/logs/agent.out.wrapper.log
```

To reconfigure the FlexConnector as a service, run the FlexConnectorConfiguration Wizard again. Open a command window on $ARCSIGHT_HOME/current/bin and run:

```
./runagentsetup
```

Viewing the Intelligence Entities and Alerts Information in the ArcSight (ESM) Console

Perform the following steps to view the Intelligence entities and alerts information in the ArcSight (ESM) Console:

1. Download the **Interset_Sample_Content.arb.zip** file from the OpenText Marketplace. and save it in a desired location (For example, C:/Desktop/Interset_Sample_Content.arb.zip).
2. Extract the downloaded file:

   ```
   unzip Interset_Sample_Content.arb.zip
   ```

3. Log in to the ArcSight Console.
4. Click the **Packages** tab in the left pane, then click **Import**.
5. Browse to the location where you extracted the **Interset_Sample_Content.arb.zip** file.
6. Click **Install**. The installation process starts.
7. After the installation is successful, click the **Resources** tab in the left pane.
8. Navigate to **Active Channels** > **Shared** > **All Active Channels** > **Interset**.
9. Double-click **Interset** or **Interset Anomalies** to view the Intelligence entities and alerts information.
10. Navigate to **Dashboards** > **Shared** > **All Dashboards** > **Interset**.
11. Double-click **Interset Overview** to view a summary of the Intelligence entities and alerts information.

Integrating SOAR with ESM

ESM **CustomerUri** field is critical for Tenant Integration. Make sure that the Tenant Key Value used in ArcSight tenant and the ESM tenant are same.

SOAR integrates with ESM to log and forward detailed reporting on every single incident to facilitate prioritization and investigation of alerts as well as the remediation of incidents.

SOAR ingests correlated events from ESM and converts them into an alert. When an alert is generated, a new incident is created on SOAR's Incident Management Service Desk. Analyst can then investigate the incident and take remedial actions.

The ESM and SOAR integrations presents following capabilities to:

- Ingest Correlated Alerts
- Retrieve Base Events
- Create Case
- Update Case
- Search Cases
- Get Case Details
- Query Active List
- Add Entries to Active List
- Delete Entries from Active List

The bidirectional integration of ESM and SOAR requires configuration at both the platforms.

Understanding the Prerequisites for ESM and SOAR Integration

Complete the following steps before you begin the ESM and SOAR integration:

- Download the ESM-SOAR integration content from Marketplace.

  > **Note:** You need to download the ESM-SOAR integration content only if you are using ESM 7.5. For ESM 7.6 you do not need to import arb file for ESM-SOAR integration.

- Import the integration content to the ArcSight Console.

  > **Note:** You need to follow this step only if you are using ESM 7.5. For ESM 7.6 you do not need to import the integration content to ArcSight Console.

- Allow network traffic from ESM to SOAR towards port 32200/TCP. The ArcSight SOAR listener for correlated event data (alerts) is accessible from this port.

  Run the following command on ESM to verify network traffic from ESM to SOAR:

  ```
  openssl s_client -connect <OMT HOST>:32200
  ```

- Open REST API port 8443/TCP at ESM to allow HTTPS traffic. SOAR connects with the ESM REST API on this port.

  Run the following command on SOAR to verify HTTPS traffic:

  ```
  openssl s_client -connect <Address of the ESM Manager>:8443
  ```

- Configure a SOAR user account to connect with the ESM API.
- Set the parameter **ArcSightListenerProtocol** in SOAR at **Configuration** > **Parameters** as **tls**.
- Enable the parameter **ArcSightListenerEnabled** in SOAR at **Configuration** > **Parameters** before configuring the forwarding destination on the connector.

  > **Note:** If the parameter **ArcSightListenerEnabled** is not enabled, an error message is displayed as connection refused.

- Install a forwarding connector on ESM and configure it to forward events from ESM to SOAR.

To install a forwarding connector:

1. **Create a forwarding connector**: To create a forwarding connector, see Forwarding Correlation Events. For this example, you can create the forwarding connector for ESM and SOAR integration with the following values:
   - User ID: forwardSOAR
   - User Type: Forwarding Connector
2. **Install and configure the forwarding connector package**: Install the forwarding connector package on ESM. Then complete the following steps for configuration:
   To add the local connector certificate:

   a. From the bastion, run the following command:

   ```
   export VAULT_POD=$(kubectl get pods -n core -o custom-
   columns=":metadata.name"| grep itom-vault)
   CA_CHAIN=$(kubectl exec -n core ${VAULT_POD} -c vault -- bash -c
   "vault read -tls-skip-verify -field=certificate RE/cert/ca_chain"); if
   [ -n "$CA_CHAIN" ]; then echo "$CA_CHAIN" > /tmp/cdf-soar.cert; else
   kubectl exec -n core ${VAULT_POD} -c vault -- bash -c "vault read -
   tls-skip-verify -field=certificate RE/cert/ca" > /tmp/cdf-soar.cert;
   fi
   ```

   b. Copy the cdf-soar.cert certificate to the following path on the forwarding connector:

   ```
   /opt/arcsight/MicroFocus_
   ArcSightSmartConnectors/SuperConnector/current/jre/lib/security
   ```

c. Navigate to the following keytool path:

```
cd /opt/arcsight/MicroFocus_
ArcSightSmartConnectors/SuperConnector/current/jre/bin/
```

d. Run the following command to import the connector certificate:

```
./keytool -importcert -file ../lib/security/cdf-soar.cert -keystore
../lib/security/cacerts -alias "CDF-cert"
```

Note: Keystore password is **changeit**.

e. In the **Connector Setup Wizard**, select the **Add a Connector** option, then the **ArcSight Forwarding Connector (Enhanced)** option to configure the connector as a forwarding connector.

f. Enter the parameter details as follows:

- **ArcSight Source Manager Host Name[localhost]**: <Specify local host IP>
- **ArcSight Source Manager Port**: 8443
- **ArcSight Source Manager User Name**: <Specify the user name that you have created for ESM>
- **ArcSight Source Manager Password**: <Specify the password that you have created>

g. Select **Yes**, if the values are correct.

To configure the forwarding connector for forwarding events from ESM to SOAR:

a. To set up the ArcSight Agent, run the following command:

```
cd /opt/arcsight/MicroFocus_
ArcSightSmartConnectors/SuperConnector/current/bin
```

```
./runagentsetup.sh
```

b. In the **Connector Setup Wizard**, select **Select the type of destination**, and then select **CEF Syslog**.

c. Specify the parameter details as follows:

- IP/Host: <Specify the FQDN corresponding to the Node where SOAR pods are running. Run the following command to obtain the value:

  ```
  kubectl get pods -o wide|grep soar
  ```

- **Port**: SOAR 32200

- **Protocol**: TLS
- **Forwarder**: False

> Note: If ArcSight Platform is installed on AWS and ESM capability is not installed in the same VPC, you must use a network load balancer (NLB) instead of an application load balancer (ALB) on AWS since ALB does not support the TCP communication channel required for sending correlated events from ESM to SOAR.

d. Select **Yes**, if the values are correct.

After you have met the prerequisites, complete the integration in SOAR.

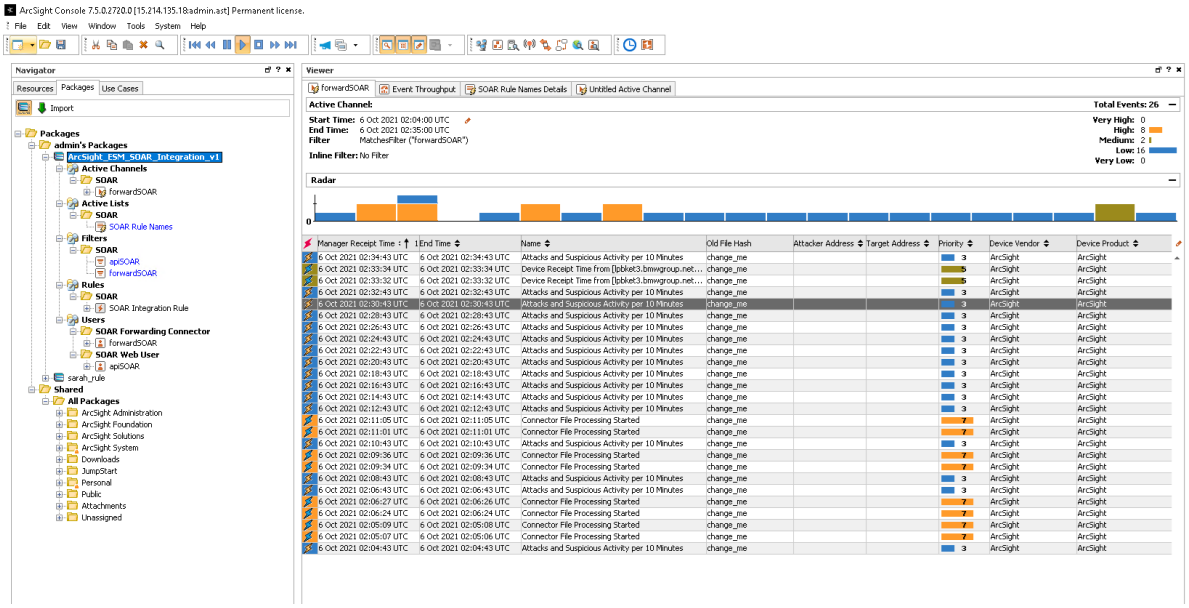
Importing the ESM-SOAR Integration Content

After you download the ESM-SOAR integration content from Marketplace, import it to the ArcSight Console and configure it.

> **Note:** You need to download the ESM-SOAR integration content and import it to ArcSight Console and configure it, only if you are using ESM 7.5. For ESM 7.6 you do not need to import arb file for ESM-SOAR integration.

1. Import the integration content to the ArcSight Console.

   The following shows the content imported to the console:



2. Reset the password for the SOAR Forwarding Connector user, **forwardSOAR**.
3. Reset the password for the SOAR Web user, **apiSOAR**.

4. Add the correlation rule names that you want to forward from ESM to SOAR to the **SOAR Rule Names** active list.
5. The integration content adds **change_me** as the default value for the **Old File Hash** field.

   This value is used during the process of adding ESM as an alert source for SOAR. The default value of the **Old file Hash** field is specified on the **Key** textbox in the **Alert Source Editor**.
6. Open **ACL Editor** for **apiSOAR** user on ESM console and add read and write permissions for all active lists for this user. Now you can access all the active lists on ESM from SOAR side.

   > You can change the value of the **Old File Hash** field on the SOAR Integration Rule action tab in the ArcSight Console. If you are changing the Old file Hash value, please remember to update the same value in ESM filter **forwardSOAR** in path /All Filters/ArcSight Foundation/SOAR/forwardSOAR and key value of ESM alert source configuration of SOAR.

Completing the Integration in SOAR

The ESM and SOAR integration requires some configuration in SOAR. You must add the credentials for the Web User account that you created in ESM to SOAR. This user account is used to read, write, and access the active list in ESM. This account is also responsible for accessing all of the required events, including the base events in ESM. To listen to the events, you must configure ESM as an alert source in SOAR. After you configure ESM as an alert source, SOAR can pull the events from ESM and convert them into alerts for investigation purposes.

Adding Credentials

To support ESM and SOAR integration, you must add the credentials for the ESM SOAR Web user to SOAR. SOAR uses this account to fetch and update events as well as to invoke other supported actions.

To add the credentials to SOAR:

1. In SOAR, navigate to **Configuration** > **Credentials**.
2. Click **Create Credential** to view the **Credential Editor** window.
3. Specify the following values in the **Credential Editor** window:

   For Internal Credential:

   - **Type**: Internal credential
   - **Name**: <Display name of credential set>

     For example: ArcSight ESM Credentials
   - **Username**: <User name created for the SOAR Web user in ESM>

- **ESM Password**: <Password of the SOAR Web user>
- **Private Key**: <Empty>

Configuring ESM as an Alert Source

The active list in ESM has correlated events that ESM passes to SOAR. SOAR converts these events to alerts and performs investigation and response procedures. To receive alerts in SOAR, you must configure ESM as an alert source to SOAR.

To configure ESM as an alert source to SOAR :

1. In SOAR, navigate to **Configuration** > **Alert Source**.
2. Click **Create Alert Source Configuration** and specify the following values in the **Create Alert Source Configuration** window:
   - **Name**:< Display name of the ESM alert source in SOAR >
   - **Type**: OpenText ArcSight ESM
   - **Address**: <Address of the ESM Manager>

     For example, https://192.168.5.5:8443.
   - **Key**: <Specify the name of the key from the ESM pre-persistence rule>
   - **Alert Severity**: <Specify the alert severity values mapping, with SOAR incident severity>
   - **Configuration**: Specify the following parameters:

Parameter Name	Parameter Description	Parameter Usage
CEF field **[severity.field]**	Used as severity value when mapping severity value to SOAR incident severity. You can set this parameter for priority, severity, flexString1 and flexNumber 1	severity.field=priority
CEF-extension **[severity.field]**	Used as rule name value.	

Parameter Name	Parameter Description	Parameter Usage
Scope fields: **[src]**	a. The value of scope field is extracted from correlated event. src:NETWORK_ ADDRESS:OFFENDER, dst:NETWORK_ ADDRESS:IMPACT, request:URL:OFFENDE R fields are always extracted by default. b. This parameter can also specify additional fields to be extracted:	a. (field1:CATEGORY:ROLE, (field2:CATEGORY:ROLE, ...) CATEGORY is any EMAIL_ADDRESS, HASH, HOST, MAC_ADDRESS, NETWORK_ADDRESS, COMPUTER_ NAME, UNKNOWN, URL, USERNAME, PROCESS ROLE is any OFFENDER, IMPACT, RELATED b. correlated.scope=s_ user:USERNAME:OFFENDER, dvc:NETWORK_ADDRESS:RELATED correlated.scope=src:NETWORK_ ADDRESS:OFFENDER, dst:NETWORK_ ADDRESS:IMPACT, request:URL:OFFENDER
Additional Scope Field: **[baseevent.scope]**	These values are extracted from base events (field1:CATEGORY:ROLE) and use JSON pointer notation. See the correlated.scope property for Category and Role values details. This parameter can specify additional fields to be extracted, and will not override the default behavior.	Example: baseevent.scope=/device/address:NETWOR K_ADDRESS:RELATED # baseevent.scope=
[cache.reusing.duration]	Used to configure how far (in minutes) into the past this enrichment is checked.	cache.reusing.duration=20
enable/disable **[enable.baseevent.activit y]**	Used to enable/disable base events activity in the incident timeline.	enable.baseevent.activity=false

Note: To collect information for MITRE Attack, you can add `mitre.id.field` in the configuration pane with the default value as `cs6`.

3. Click **Save** to complete the ESM and SOAR integration.
4. Click **Test** to test the integration. A **Test Alert Source** pop-up is displayed to confirm that you have entered the valid credentials and address.
5. Navigate to **Configuration** > **Parameters** and set the value of following parameters:

- **ArcSightListenerEnabled** to **true**.
- **ArcSightListenerProtocol** to **tls**.

> **Note**: Ensure that the **Forwarding Connector** for the SOAR connection protocol is set to **TLS**.

Configuring ESM as an Integration

ESM must be configured in SOAR as an integration for executing SOAR actions and enrichment capabilities.

To configure ESM as an integration:

1. In SOAR, navigate to **Configuration** > **Integrations**.
2. Click **Create Integration** to view the **Configuration** window.
3. Specify the following values in the **Configuration** window:
   - **Name**: <Display name of the ESM integration in SOAR>
   - **Type**: OpenText ArcSight ESM
   - **Address**: <Address of the ESM Manager>

     For example, https://192.168.5.5:8443
   - **Configuration**: #proxy.id=5422
   - **Credential**: <Name of the credential set created>

     For example, ArcSight ESM Credentials
   - **Trust Invalid SSL Certificates**: <Select this option if the server certificate is self-signed or not recognized by the browsers>
   - **Require Approval From**: <Select users that can provide approval before executing actions on this integration>
   - **Notify**: <Select users to be notified when SOAR performs an action on this integration>
4. Click **Save** to complete the integration.
5. Click **Test** to test the integration. A **Test Alert Source** pop-up is displayed to confirm that you have entered the valid credentials and address.

Tuning ESM and SOAR Integration

The ESM and SOAR integration can be customized as per your requirements. The following parameter values can be tuned to suit your environment:

Consult with ArcSight SOAR Field Engineering Team if tuning is required.

Parameter Name	Parameter Description	Default Value
ArcSightAutoEnrichEnabled	Enable ArcSight auto-enrichment with base-event data	False
ArcSightListenerEnabled	Enable ArcSight Listener	False
ArcSightListenerKeyField	ArcSight listener key field for alert source identification	oldFileHash
ArcSightListenerProtocol	ArcSight listener protocol	tcp
ArcSightListenerThreadPoolCoreSize	ArcSight listener thread pool core pool size (0 = unlimited)	0
ArcSightListenerThreadPoolKeepAlive	ArcSight listener thread pool keep-alive seconds (ignored if core pool size = 0)	60
ArcSightListenerThreadPoolMaxSize	ArcSight listener thread pool maximum size (ignored if core pool size = 0)	20
ArcSightListenerThreadPoolQueueCapacity	ArcSight listener thread pool queue capacity (ignored if core pool size = 0)	1000

To enable receiving MITRE Attack for specific incidents, you can tune the following parameters:

Parameter	Description
MITREAttackControllerFixedDelay	The frequency for SOAR to update the MITRE data, the default value is 86400 (in seconds).
MITREAttackUrl	Represents the source from where to fetch the MITRE details.
MITREAttackControllerProxyIntegrationId	Supports proxy integration, the default value is -1, implying no proxy usage.

Please make sure that to be able to extract scope items from correlated event (the initial event) you need to provide only the CEF key name. For extracting scope items from base events (multiple events fetched from ESM related with correlated event) you need to provide full path of the parameter.
Example: For destination port:
In correlated events: CEF Key name of "dpt" is required.
In base events: Full path of destination port "/destination/port" is required.

Integrating SOAR with Intelligence

Not applicable for a fresh installation of the ArcSight Platform.

OpenText ArcSight Intelligence uses unsupervised machine learning to calculate probabilistic risk assessments based on behavioral analytics from millions of events, ultimately generating a short list of high value targets to allow security teams to detect, investigate, and respond to threats that might hide in the enterprise before any case occurs.

SOAR has the following integration capabilities with Intelligence:

- Ingest Anomalies as Alert
- Get Entity Details

Use Cases

Use Case #1: Prioritizing Cases

SOAR is integrated with Intelligence, to help prioritization and investigation of cases as well as remediation of cases. When an alert is received, a new case is created in the Case Management Service Desk of SOAR. SOAR then automatically checks the risk scores of entities and prioritizes the case based on these risk scores. Get Entity Details enrichment results return latest 1000 records maximum.

Use Case #2: Mitigating Account Compromise

SOAR ingests anomaly data from Intelligence and creates case tickets in the Case Management Service Desk. With its broad integration portfolio, orchestration, and automation capabilities, SOAR investigates, ascertains the case, and takes necessary actions to prevent the compromise.

The bidirectional integration of Intelligence and SOAR requires configuration at both the capabilities.

Configuration

Prerequisites

- SOAR connects to OpenText ArcSight Intelligence API via HTTPS. By default, the interface works on 443/tcp port. Make sure that you have access permission to this port.
- A user account for SOAR to connect to the Intelligence API.

Configuring ArcSight Intelligence

No specific configuration is needed on Intelligence.

Configuring SOAR

1. Click **Configuration** > **Credentials** > **Create Credential**.
2. If the **use.basic.authentication** configuration parameter value is **False**, then get the **Client id** and **Client secret** from Intelligence to ensure that the Intelligence Alert Source and Intelligence Integration work as expected.

   Note: The default value of **use.basic.authentication** parameter is **False**.

   To get the Client ID and Client Secret for OpenText Intelligence open a command prompt and:

   a. Specify the name of the server on which Intelligence works.

   b. Run the following command to get **Client ID** and **Client Secret** from Intelligence:

   ```
   osp-client-id and osp-client-secret : kubectl get secret osp-secret -n
   arcsight-installer-tyoib -o yaml
   ```

   The output is displayed in the following format:

   ```
   data:
   osp-client-id: NTZjODkyYWE3NDMzZThiOTYzZGVkMjE5ZGIzODU3ZDg=
   osp-client-secret:

   ZjRiZDUzODBiZjQ2NTY5MWQ4NDAzMTFhZTJmMjY1ZGJlZGRjOWU0NDhlZmE3ZDhjN2Q5Yz
   JlY2VjMDkzMmExNw==
   ```

   c. Run the following command to decode the **Client ID** and **Client Secret**:

   ```
   echo 'NTZjODkyYWE3NDMzZThiOTYzZGVkMjE5ZGIzODU3ZDg=' | base64 --decode
   echo
   'ZjRiZDUzODBiZjQ2NTY5MWQ4NDAzMTFhZTJmMjY1ZGJlZGRjOWU0NDhlZmE3ZDhjN2Q5Y
   zJlY2VjMDkzMmExNw==' | base64 --decode
   ```

   d. Run the following command to add the **Client ID** to the Alert Source / Integration configuration on Intelligence.

   ```
   # Client id that defined in OSP
   client.id=id
   ```

3. Specify the following parameter values in the **Credential Editor**:

Parameter	Value
Type	Internal Credential
Name	Display name of credential set (For example, Intelligence Credentials)
Username	Name of the SOAR user created on Intelligence.
Password	Password of the SOAR user created on Intelligence.
Private Key	Client secret that has been defined in OSP

Configuring Intelligence as an Alert Source

1. Click **Configuration** > **Integrations** > **Create Alert Source**.
2. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Intelligence Alert Source on SOAR.
Type	OpenText ArcSight Intelligence.
Address	Address of the Intelligence server (the format must be https://172.16.11.9).

Configuration	Specify the following configuration parameters:
	`tenant.id=`
	`# ID of the proxy integration to use when connecting to current source.`
	`# If not provided, ArcSight SOAR will try to use a direct connection.`
	`#proxy.id=123`
	`# configure how far (in minutes) into the past this enrichment will look.`
	`#cache.reusing.duration=20`
	`# Base path of the OpenText Intelligence. SOAR adds it to end of the URL to access OpenText Intelligence.`
	`interset.context.path=/interset`
	`# Client id that defined in OSP`
	`client.id=id`
	Note: By default,Intelligence uses 0 for tenant id. However, Intelligence - SOAR integration supports different tenants.

Credential	Name of the credential set you have created (For example, OpenText ArcSight Credentials)
Trust Invalid SSL Certificates	Select this if Web UI's certificate is self-signed or is not recognized by browsers
Visible Alert Fields	You might define the alarm fields that will be displayed on the Case Management Service Desk

3. Click **Save** to complete the integration.
4. Click **Test** to test the integration.

Configuring Intelligence as Integration

1. Click **Configuration** > **Integrations** > **Create Integration**.
2. Specify the following parameter values in the **Configuration** form:

Parameter	Value
Name	Display name of Intelligence integration on SOAR.
Type	OpenText ArcSight Intelligence.
Address	Address of the Intelligence server (the format must be https://172.16.11.9).

Configuration	Specify the following configuration parameters:
	`tenant.id=`
	`# ID of the proxy integration to use when connecting to current source.`
	`# If not provided, ArcSight SOAR will try to use a direct connection.`
	`#proxy.id=123`
	`# configure how far (in minutes) into the past this enrichment will look.`
	`#cache.reusing.duration=20`
	`# Base path of the OpenText Intelligence. SOAR adds it to end of the URL to access OpenText Intelligence.`
	`interset.context.path=/interset`
	`# Client id that defined in OSP`
	`client.id=id`

Credential	Name of the credential set you have created (For example, OpenText ArcSight Credentials)
Trust Invalid SSL Certificates	Select this if Web UI's certificate is self-signed or is not recognized by browsers
Require Approval From	Select user(s) from the list to request for approval before executing actions on this integration. Because SOAR only executes enrichments on Intelligence, leave it empty.
Notify	Select user(s) from the list to notify when SOAR performs an action on this integration. Because SOAR only executes enrichments on Intelligence, leave it empty.

3. Click **Save** to complete the integration.
4. Click **Test** to test the integration.

Additional Notes

- The following configuration parameters can be used for fine tuning the integration. You must consult the SOAR field engineering team before editing them:

- MicroFocusIntelligenceListenerMaxRetrySeconds OpenText Interset listener queue max message retry in seconds 1800
- MicroFocusIntelligenceListenerQueueConcurrency Upper limit of OpenText Interset Listener consumer thread count 3
- MicroFocusIntelligenceSyncPeriod Period in seconds to sync OpenText Interset anomalies 60

Capabilities

1. **Get Details**

   Enrichment capability to get the risk score of a given entity and related alert details.

   The following table presents the **Get Details** capability details:

Input Parameter	Description	Type	Scope Rescticted (Yes/No)	Required (Yes/No)
Integration	Name of the third party integration.	Integration	N/A	Yes
Entity	Entity to be queried on ArcSight Intelligence.	Network Address Host File Name URL	Yes	Yes
Do not use cache	SOAR does not use cached results if this box is checked.	Checkbox	N/A	No

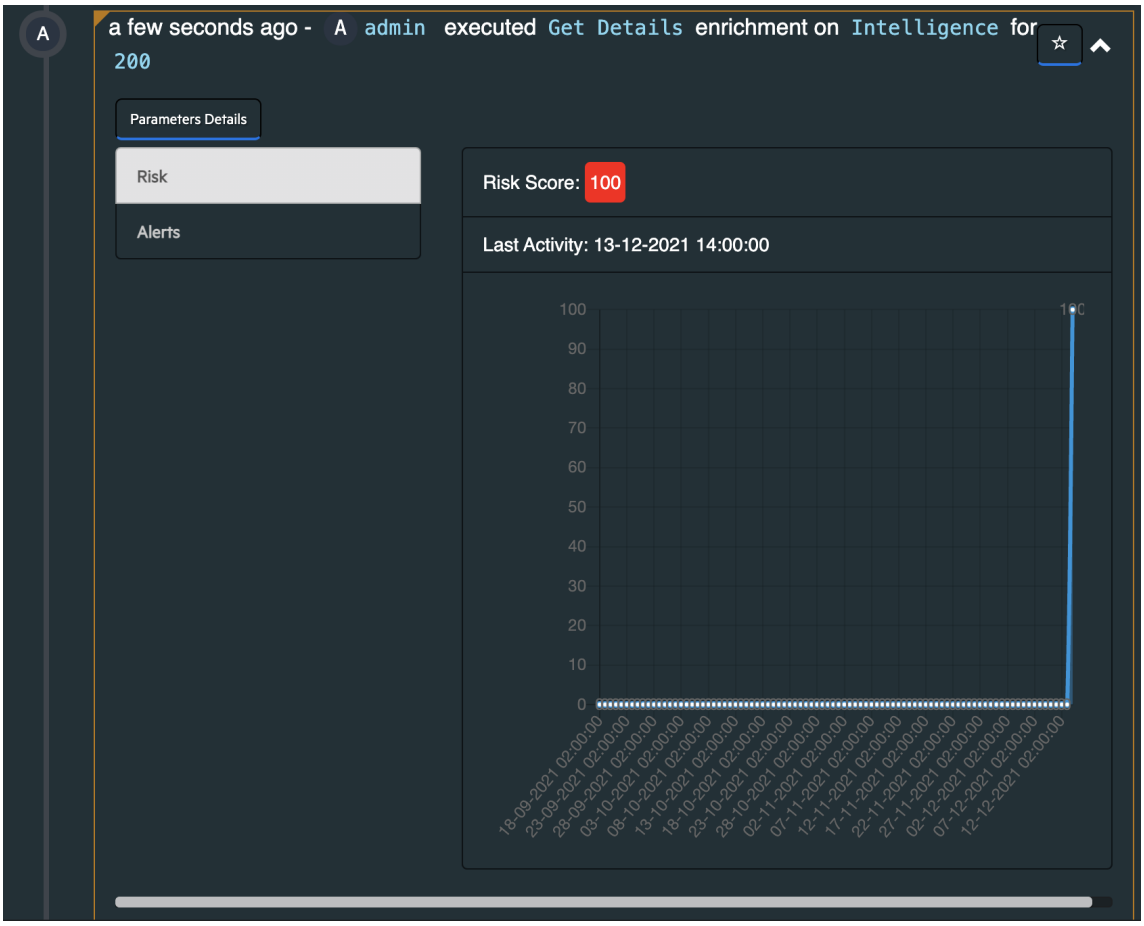
   Output:

   Case Scope:

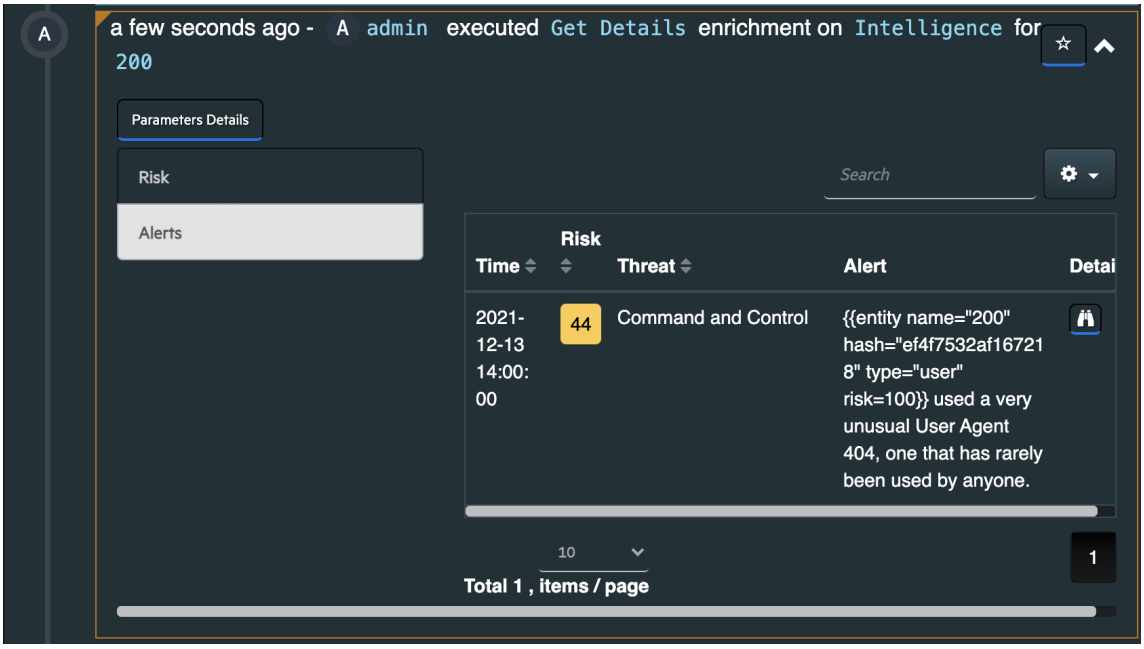
Action	Type	Category/ Value
Add Scope Item Property	Integer	OpenText Intelligence Entity Risk
Add Scope Item Property	TEXT	OpenText Intelligence Entity Hash
Add Scope Item Property	TEXT	OpenText Intelligence Entity Type

   Human Readable Output:

a. Risk tab:



b. Alerts tab:



Chapter 7: Upgrading Your Environment

If Intelligence is deployed on the ArcSight Platform, there is no provision to enable multi-tenancy on the platform. Consider the following scenarios for enabling multi-tenancy in the upgraded platform:

1.**Enabling multi-tenancy during the platform upgrade**:Before you start with the upgrade, ensure that you uninstall the Intelligence capability and remove any artifacts related to it.
2.**Enabling multi-tenancy after the upgrade without Intelligence**: If you have already upgraded the ArcSight Platform with neither Intelligence upgraded nor multi-tenancy enabled, you can enable multi-tenancy from the **Reconfigure** tab in the OMT portal.
3.**Enabling multi-tenancy after the upgrade with Intelligence**: If you have already upgraded Intelligence with the ArcSight Platform and you need to enable multi-tenancy on the upgraded platform at a later stage, you must first uninstall Intelligence, and then enable multi-tenancy from the **Reconfigure**tab in the OMT portal.
4. Once you uninstall Intelligence and enable multi-tenancy in the platform, you cannot reinstall Intelligence.

This section provides information about upgrading your environment. Several options for upgrading your environment are available.

Upgrading an AWS Installation

To ensure a successful upgrade, be sure to follow the tasks in "Checklist: Upgrading Your AWS Cluster" on the next page.

Before you perform this upgrade, ensure that you have a correct version of ArcSight Platform already installed in your environment. For more information about the hardware and software requirements and tuning guidelines for the ArcSight Database, see the *Technical Requirements for the ArcSight Platform*. For more information, see the *ArcSight Platform Upgrade Paths* documentation. To identify the product versions, files to download, and known issues related to installation, see the *Release Notes for ArcSight Platform 24.2*.

Before you begin the upgrade process, you must enable the database to receive SSL connections and to configure deployed capabilities to use SSL for the database connection. For information about configuring capabilities to use SSL, see Enabling the Database to Receive SSL Connections in the *Administrator's Guide for the ArcSight Platform - AWS Deployment*.

Beginning with ArcSight Platform 24.2, the system will also use SSL for connections between the deployed capabilities and the ArcSight Database.

Checklist: Upgrading Your AWS Cluster

Use this checklist to complete the upgrade tasks in the listed order.

Throughout the rolling upgrade process, services not actively being upgraded will continue to be available. Services that utilize the ArcSight Database, such as event ingestion and search, will be interrupted during the Database upgrade phase, but any in-flight data would be cached and processed as soon as the Database upgrade completes.

If you deployed and configured your system for high availability, during the rolling Kubernetes worker node upgrade process, services delivered by pods on the affected worker node will be restarted on another worker node. Similarly, the upgrade of Kubernetes pods is performed in a rolling manner, so there will be a brief pod-level service pause as pods are restarted to perform the upgrade. Some services, such as Transformation Hub, can be configured for high availability with pod replicas so that there are no service pauses during the rolling upgrade.

	Task	See
❑	1. Ensure that you are upgrading from and to the correct version of ArcSight Platform.	*ArcSight Platform Upgrade Paths*
❑	2. Identify the product versions, files to download, and known issues related to the upgrade.	*Release Notes for ArcSight Platform 24.2*
❑	3. Upgrade all prerequisites	"Upgrade Prerequisites " on the next page
❑	4. Ensure that SSL communication is enabled between the deployed capabilities and the ArcSight Database.	Configuring the Deployed Capabilities
❑	5. Download the installation packages.	"Downloading the Upgrade Packages for an AWS Deployment" on page 398
❑	6. (Conditional) If your deployment includes Intelligence or Recon, upgrade the Database.	"Upgrading the Database in AWS" on page 399
❑	7. Upgrade the OMT infrastructure.	" Running the ArcSight Platform OMT Upgrade (AWS)" on page 403
❑	8. Upgrade the deployed capabilities.	"Upgrading Deployed Capabilities in AWS" on page 413
❑	9. Configure the Load Balancer for capabilities.	"Configure the Load Balancer for capabilities" on page 418

❑	10. Upgrade Kubernetes version of the control plane and worker nodes.	"Upgrading EKS" on page 419
❑	11. Recover and restore the Elasticsearch Data.	Recovering and Restoring Elasticsearch Data
❑	12. Complete any post-upgrade tasks.	"Completing Post-Upgrade Tasks" on page 438
❑	13. (Conditional) If your environment includes ESM, you should upgrade to the latest version.	"Upgrading ESM" on page 440
❑	14. (Conditional) If you have purchased licenses for additional capabilities, deploy them to your environment	"Adding Additional Capabilities to an Existing Cluster" on page 253

Upgrade Prerequisites

Verify the following before performing the upgrade:

- The packages for upgrade have been downloaded following this procedure:
  - To identify the files to download to your secure network location, see **Downloading the files** in the *Release Notes for ArcSight Platform 24.2*.
  - From a secure network location, download the installation packages for the OMT Installer and the products of your choice from the Software Licenses and Downloads portal.

  Note: This secure network location must be able to access your instance of AWS.

- Root access to the bastion VM is granted
- The kubernetes command line tool `kubectl` is installed on your bastion and connected to your cluster
- Any existing suite-upgrade-pod-arcsight-installer deployment has been deleted using this command:

```
kubectl delete deployments suite-upgrade-pod-arcsight-installer -n
$(kubectl get namespaces | grep arcsight-installer | awk ' {print $1} ')
```

  Note: The command will return an error if no upgrade has been done previously.

- Check that your **EFS throughput configuration** is the correct one to manage the amount of data going through. See EFS Throughput modes for more information. Making sure your configuration is correct will also prevent environment performance issues during regular operation.

- (Conditional) If you are using custom data identifiers for Intelligence, ensure that you back up the `logstash-config-pipeline` config map that is accessible through the Kubernetes dashboard.
- All pods are running, verify with this command:

```
kubectl get pods -A
```

Downloading the Upgrade Packages for an AWS Deployment

Use this procedure to download the packages for installation or upgrade:

1. To identify the files to download to your secure network location, see "Downloading and Installing the ArcSight Platform Installation Files" in the *Release Notes for ArcSight Platform 24.2*.
2. From a secure network location, download the installation packages for the OMT Installer and the products of your choice, along with their signature files (.sig).

   Note: This secure network location must be able to access your instance of AWS.

   Important: Before proceeding with the next step, verify the GPG digital signatures of the downloaded files as the per this knowledge base article.

3. Extract the `arcsight-platform-cloud-installer-XX.X.X.XXX.zip` file.
4. Review the following table to understand the utility scripts and some templates used during the AWS deployment of ArcSight Platform. The utility scripts and templates are located in the `aws_scripts/scripts` directory.

Script	Description
`generate_aws_secrets`	Generates new Kubernetes Secrets for connecting from the cluster to the Elastic Container Registry (ECR). **Important:** The generated credentials and secrets are valid only 12 hours after generation. If the credentials and secrets have expired, use this script following the instructions in Refresh the ECR credentials in the K8s.
`init_efs`	Creates the required folder structure on the Elastic File Storage (EFS) and assigns correct ownership and permissions. You will use this script when configuring EFS for the ArcSight Suite. Parameters for this script are discussed in the following sections. **Note:** Execute this script without parameters to display the help.

Script	Description
`upload_images_to_ECR`	Uploads the OMT and product images to the ECR to make them accessible to K8s. The script performs tasks in the background required specifically by the AWS ECR. Parameters for this script are discussed in the following sections. **Note:** Execute this script without parameters to display the help.
`workernodes-userdata`	The installation uses this script indirectly for enabling worker nodes to join the Kubernetes cluster.

Upgrading the Database in AWS

Please be patient and give the upgrade sufficient time to confirm completion. If you start the product before the Database upgrade is complete, you might experience performance issues and errors.

For more information about upgrade paths see, ArcSight Platform Install and Upgrade Paths.

Follow the "Checklist: Upgrading Your AWS Cluster" on page 396 to ensure a successful upgrade.

To upgrade the Database:

1. Back up the Database before proceeding.
2. (Conditional) If the installation is passwordless, generate the SSH public key using the command, `ssh-keygen`.
3. Choose one of the following:
   a. In a `FIPS` enabled environment, upgrade your `OS` to `RHEL 9.2` **before** attempting the ArcSight Platform Database upgrade.
   b. In a non-FIPS enabled environment, you can proceed with the ArcSight Platform Database upgrade without first upgrading your `OS`.

   For more information, see **Software Requirements** in the *Technical Requirements for ArcSight Platform 24.2*.
4. Log in to the bastion where you downloaded the files.
5. Copy the `db-installer_x.x.x-x.tar.gz` file to the Database cluster node 1.
   The file is located by default in the `{unzipped-installer-dir}/database/` directory, where *`{unzipped-installer-dir}`* represents the folder that contains the downloaded installation files.
6. Log in to Database cluster node 1.

7. Create a directory to extract the `db-installer_x.x.x-x.tar.gz` file into. We will refer to this directory as {*unzipped-db-installer-dir*}.

   > Do not use the directories `/root`, `/opt/vertica`, or the existing database installer directory (default is `/opt/arcsight-db-tools`). The files in `/opt/arcsight-db-tools` will be upgraded by the database upgrade tool.

8. To change to the directory, run the following command:

```
cd {unzipped-db-installer-dir}
```

9. Extract (untar) the `db-installer_x.x.x-x.tar.gz` file into the directory using the following command:

```
tar xvfz  db-installer_x.x.x-x.tar.gz
```

10. Execute the following command to start the upgrade of the schema and database tools.

```
./db_upgrade -c upgrade-utilities
```

The output of the command will look similar to the following:

```
Stopping cronjob. Please wait.
Stopping cronjob. Please wait.
All cronjobs are stopped.



Upgrade related changes cannot be rolled back, do you want to continue
with the upgrade (Y/N): y
Starting upgrade...



******************** Start of Database Upgrade *****************
Enter previous installed location (/opt/arcsight-db-tools):
Running Pre-Upgrade checks
Checking all database nodes are UP
All database nodes are UP
Replacing files in installed location
Upgrading script and config files.
Creating backup directory: /opt/arcsight-db-tools/oldVersion
Backing up: /opt/arcsight-db-tools/udfs
Backing up: /opt/arcsight-db-tools/sched_ssl_setup
Backing up: /opt/arcsight-db-tools/kafka_scheduler
Backing up: /opt/arcsight-db-tools/scripts
Backing up: /opt/arcsight-db-tools/db_installer
```

```
Backing up: /opt/arcsight-db-tools/db_upgrade.py
Backing up: /opt/arcsight-db-tools/data
Backing up: /opt/arcsight-db-tools/lib
Backing up: /opt/arcsight-db-tools/db_ssl_setup
Backing up: /opt/arcsight-db-tools/schema_registry_setup
Backing up: /opt/arcsight-db-tools/upgrade
Backing up: /opt/arcsight-db-tools/db.properties
Backing up: /opt/arcsight-db-tools/db_upgrade
Backing up: /opt/arcsight-db-tools/copyright.txt
Upgrading: /opt/arcsight-db-tools/udfs
Upgrading: /opt/arcsight-db-tools/sched_ssl_setup
Upgrading: /opt/arcsight-db-tools/kafka_scheduler
Upgrading: /opt/arcsight-db-tools/db-upgrade.log
Upgrading: /opt/arcsight-db-tools/scripts
Upgrading: /opt/arcsight-db-tools/db_installer
Upgrading: /opt/arcsight-db-tools/db_upgrade.py
Upgrading: /opt/arcsight-db-tools/data
Upgrading: /opt/arcsight-db-tools/lib
Upgrading: /opt/arcsight-db-tools/db_ssl_setup
Upgrading: /opt/arcsight-db-tools/schema_registry_setup
Upgrading: /opt/arcsight-db-tools/upgrade
Upgrading: /opt/arcsight-db-tools/db.properties
Upgrading: /opt/arcsight-db-tools/db_upgrade
Upgrading: /opt/arcsight-db-tools/copyright.txt
Successfully updated the db_backup setting.
Version specific upgrade methods
******************** Database Upgraded Complete. Version is 4.0.0
******************
```

11. Disable the watchdog with this command:

```
/opt/arcsight-db-tools/scripts/watchdog.sh disable
```

12. Stop the database:

```
/opt/arcsight-db-tools/db_installer stop-db
```

13. At this point in the upgrade, depending on your deployment's FIPS mode, you might need to upgrade your OS:
    - In a FIPS enabled deployment: upgrade your OS to `RHEL 9.2` before proceeding with the next step.
    - In a FIPS disabled deployment: upgrading your OS is optional, you can proceed with the database upgrade without it.

14. Execute the following command to start the database binaries upgrade:

```
./db_upgrade -c upgrade-db-rpm
```

- The output of the command will look similar to the following if the `rpm` update is not performed (when `rpm` it's already in the current version)

```
Stopping cronjob. Please wait.
Stopping cronjob. Please wait.
All cronjobs are stopped.



Upgrade related changes cannot be rolled back, do you want to continue
with the upgrade (Y/N): y
Starting upgrade...



******************** Start of Database Upgrade *****************
Enter previous installed location (/opt/arcsight-db-tools):
Running Pre-Upgrade checks
Checking all database nodes are UP
All database nodes are UP
******************** Start of db rpm Upgrade *****************
Pre Upgrade check for 23.3.0-2
Current database rpm version is: 23.3.0-2
Database is up to date with the current version 23.3.0-2
```

15. Start the database with this command:

```
/opt/arcsight-db-tools/db_installer start-db
```

16. Start the scheduler:

```
/opt/arcsight-db-tools/kafka_scheduler start
```

17. Enable the watchdog:

```
/opt/arcsight-db-tools/scripts/watchdog.sh enable
```

18. (Optional) Start the firewall service.

Running the ArcSight Platform OMT Upgrade (AWS)

The 24.2 release requires upgrading the underlying infrastructure of the ArcSight Platform to version (the new OPTIC Management Toolkit, abbreviated OMT). This process can take a significant amount of time, depending on the number of master and worker nodes that need to be updated, so please select the most convenient (less busy) time to perform the upgrade.

All commands should be performed from the bastion host.

Ensure the latest version of the AWS CLI is installed on the bastion. Refer to Installing or updating the latest version of the AWS CLI for instructions.
If the AWS CLI version needs to be updated, execute the following command to update the configuration **after** the AWS CLI update is finished:

```
aws eks update-kubeconfig --name <eks_cluster_name> --region <your_region>
```

1. Log in to the secure network location where you stored the ArcSight Platform Cloud Installers. Move the downloaded files into the bastion, and perform the commands listed in this procedure from the bastion.
2. Unzip the `arcsight-platform-cloud-installer-<VERSION>.zip` OMT installer file with this command:

   ```
   cd /tmp
   unzip arcsight-platform-cloud-installer-<VERSION>.zip
   ```

3. On the bastion, verify that all pods in core namespaces are in status *Running* or *Completed* by running this command:

   ```
   kubectl get pods -n core
   ```

   Output example:

   ```
   cdf-apiserver-7965dcf689-4qvkx                          2/2     Running
    0          145m
   ```

   ```
   fluentd-7q4dw                                           2/2     Running
    0          136m
   ```

   ```
   fluentd-kkf2p                                           2/2     Running
    0          136m
   ```

```
fluentd-mwqh8                                          2/2     Running
 0          136m

idm-77b4f9fbfb-cfwkg                                   2/2     Running
 0          136m

idm-77b4f9fbfb-g5pcb                                   2/2     Running
 0          136m

itom-cdf-deployer-2020.05-2.2-2.3-3.1-tncp8            0/1     Completed
 0          137m

itom-cdf-deployer-xg6cw                                0/1     Completed
 0          147m

itom-cdf-ingress-frontend-56c9987b7-bvrsn              2/2     Running
 0          145m

itom-cdf-ingress-frontend-56c9987b7-n8tbc              2/2     Running
 0          145m

itom-logrotate-deployment-6cf9546f8b-rbcvs             1/1     Running
 0          136m

itom-postgresql-default-77479dfbff-t87tv               2/2     Running
 0          137m

itom-vault-6f558dc6cc-bz52l                            1/1     Running
 0          146m

kubernetes-vault-67f8698568-csd54                      1/1     Running
 0          145m

mng-portal-7cfc584db5-hcmjf                            2/2     Running
 0          133m

nginx-ingress-controller-6f6d4c95b9-7fhbs              2/2     Running
 0          133m

nginx-ingress-controller-6f6d4c95b9-nv2zw              2/2     Running
 0          133m

suite-conf-pod-arcsight-installer-86c9687b69-kctjz     2/2     Running
 0          132m
```

```
suite-db-68bfc4fbd5-v6nvm                                 2/2     Running
 0          145m
```

```
suite-installer-frontend-6f49f88797-msb7j                 2/2     Running
 0          145m
```

4. Also on the bastion, check that all nodes are in *Ready* state by running this command:

```
kubectl get nodes
```

5. Switch to the AWS scripts installer directory:

```
cd arcsight-platform-cloud-installer-<VERSION>
```

6. Unzip `aws-scripts.zip`:

```
unzip aws-scripts.zip
```

7. Switch to the scripts directory:

```
cd aws-scripts/scripts
```

8. Run the following command with your credentials from the ECR:

```
./upload_images_to_ECR -o $(kubectl get cm -n core base-configmap --
output=jsonpath={.data.REGISTRY_ORGNAME}) -F arcsight-platform-cloud-
installer-<VERSION>.zip/cdf-byok-images.tar -c 4
```

   Adjust the value of the `-c` parameter (4 in the instruction above) to up to half your CPU cores in order to increase the speed of the upload (default value is 8).

9. Change directory to `/tmp` directory:

```
cd /tmp/
```

10. Unzip cdf-deployer.zip:

```
unzip cdf-deployer.zip
```

11. Change to the cdf-deployer directory:

```
cd cdf-deployer/
```

12. Run the upgrade script with the following command, and follow the prompts:

```
./upgrade.sh -u
```

Output example:

```
**********************************************************************
**********
```

```
WARNING: This step is used to upgrade CDF components to  release.
```

```
The upgrade process is irreversible. You can NOT roll back.
```

```
Make sure that all nodes in your cluster are in Ready status.
```

```
Make sure that all Pods and Services are Running.
```

```
**********************************************************************
**********
```

```
Please confirm to continue (Y/N): y
```

```
** Pre-checking before upgrade ...
```

```
[1]  Checking K8S version ...
```

```
     Passed
```

```
[2]  Checking HA Default DataBase ...
```

```
     Passed
```

```
[3]  Checking Prometheus ...
```

```
     Passed
```

```
[4]  Checking SAN in certificates ...
```

```
     Passed
```

```
[5]  Checking connectivity to registry ...
```

```
     Passed
```

```
[6]  Checking OS version for bastion node ...
```

```
     Passed
```

```
** Common upgrade check ...
[1]  Checking cluster endpoints status ...
     Passed
[2]  Checking chart releases status ...
     Passed
** Prerequisite tasks for Apphub components upgrade ... (Step 1/4)
     Setting BYOK environment files ...
     Copying itom-cdf.sh to HOME folder ...
     Copying Scripts ...
** Updating Kubernetes RBAC ... (Step 2/4)
     RBAC update successfully.
     Updating yaml-templates configmap ...
** Start to upgrade Apphub add-on charts ... (Step 3/4)
     Apphub add-on charts have been successfully updated.
** Start to upgrade Apphub chart ... (Step 4/4)
     Apphub chart has been successfully updated.
Successfully completed Apphub components upgrade process.
```

> The command `upgrade.sh -u` may return an error message on Apphub. If this occurs, run the following command:
> `helm rollback apphub 1 -n core`
> After the command has executed, re-run the upgrade.

13. When the upgrade completes, check that all pods are *Running* or *Completed* with this command:

```
kubectl get pods -A
```

Once the OMT upgrade is complete, the new platform version can be checked by clicking the ? icon in the upper right corner of the OMT UI

Configuring Controller Services

After the ArcSight Platform upgrade, the values for **frontend-ingress-controller-svc** and **portal-ingress-controller-svc** may have changed. Since you previously created a target group for ports 3000 and 5443 using the original ingress-controller-svc value, you must change the targets to match the new values.

To do this, in the target groups previously created for ports 3000 and 5443, de-register the targets. Then, create new target groups with the new port values for **frontend-ingress-controller-svc** and **portal-ingress-controller-svc** using the backend ports and add the node as targets as explained in the next step.

Creating a Target Group for Controller Service Ports

Execute the following commands to obtain the new ingress service ports.

For the new **frontend-ingress-controller-svc**:

```
kubectl get svc -n core | grep frontend-ingress-controller-svc
```

Example output:

```
frontend-ingress-controller-svc LoadBalancer 172.20.150.202 <none>
3000:30058/TCP 18h
```

Where 30058 is the new ingress service node port for port 3000, and must be recorded.

For the new **portal-ingress-controller-svc**:

```
kubectl get svc -n core | grep portal-ingress-controller-svc
```

Example output:

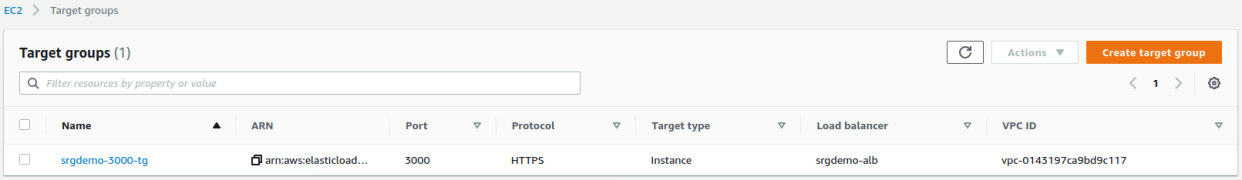
```
portal-ingress-controller-svc NodePort 172.20.26.194 <none>
5443:31704/TCP,5444:32558/TCP 170m
```

Where 31704 is the new ingress service node port for port 5443, and must be recorded.

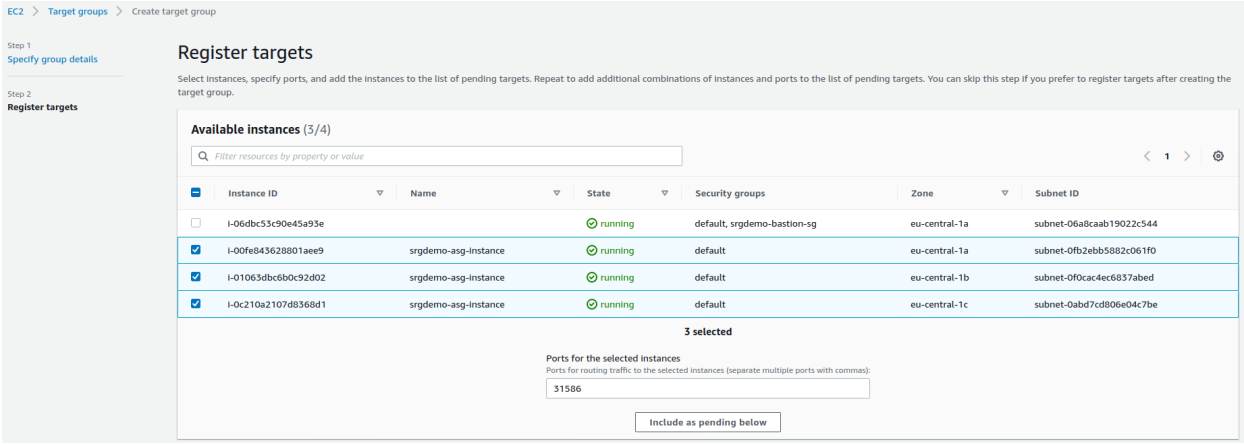
To create the target group for the port values for frontend-ingress-controller-svc and portal-ingress-controller-svc using the web UI:

> This process must be performed twice, once for **frontend-ingress-controller-svc** and once for **portal-ingress-controller-svc**.

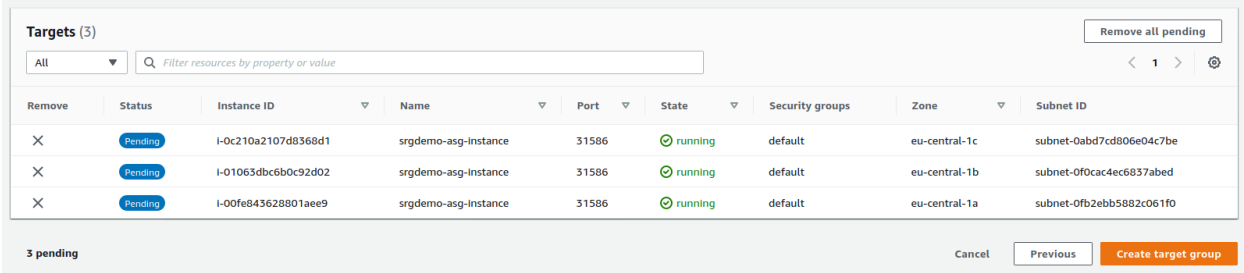
1. Using the Find Services search tool, locate and browse to the EC2 dashboard.
2. In the left navigation panel, under **Load Balancing**, click **Target Groups**.
3. On the **Target Groups** management page, click **Create target group.**



4. On the **Specify group details** page, enter values for the following:
   a. Under **Choose a target type,** select **Instances**.
   b. **Target group name:** Choose a descriptive name for easier identification; for example, *srgdemo-5443-tg*
   c. **Protocol:** change to HTTPS
   d. **Port:**the port value for **frontend-ingress-controller-svc** or **portal-ingress-controller-svc, which you recorded above in** **"Creating a Target Group for Controller Service Ports" on the previous page**
   e. **VPC:** select your VPC
   f. **Tags:** Optionally, add descriptive tags as desired.
5. Click **Next**.
6. On the **Register Targets** page, set values for the following:
   a. **Available instances:** Select your worker node instances **only**.
   b. **Ports for the selected instances:** For the selected instances, use the port value for **frontend-ingress-controller-svc** or **portal-ingress-controller-svc, which you recorded above in** **"Creating a Target Group for Controller Service Ports" on the previous page**.



7. Click **Include as pending below.** All marked instances will be added to the list of pending instances.



8. Click **Create target group.**
9. You will be redirected back to the target group management page. From the list, select the newly created target group. From the bottom of the page, record its ARN in the AWS worksheet.

To create the target group for the port values for frontend-ingress-controller-svc and portal-ingress-controller-svc using the CLI:

1. Run the following command:

```
# aws elbv2 create-target-group \
--name <port values for frontend-ingress-controller-svc and portal-ingress-controller-svc>
\
--protocol HTTPS \
--port <port values for frontend-ingress-controller-svc and portal-ingress-controller-svc>
\
--vpc-id <VPC ID> \
--health-check-protocol HTTPS \
--target-type instance
```

Parameters:

< port values for **frontend-ingress-controller-svc** and **portal-ingress-controller-svc>**: Choose some descriptive name, such as `srgdemo-<PORT_NUMBER>-tg` and record the value in the AWS worksheet.

<VPC ID>: The ID of your VPC as recorded in your AWS worksheet.

Example input and output:

```
# aws elbv2 create-target-group \
   --name srgdemo-5443-tg \
   --protocol HTTPS \
   --port 5443 \
   --vpc-id vpc-0143197ca9bd9c117 \
   --health-check-protocol HTTPS \
   --target-type instance
```

```
{
      "TargetGroups":[
         {
            "TargetGroupArn":"arn:aws:elasticloadbalancing:eu-central-
   \1:115370848038:targetgroup/srgdemo-3000-tg/c0684be94405b6b7",
            "TargetGroupName":"srgdemo-5443-tg",
            "Protocol":"HTTPS",
            "Port":5443,
            "VpcId":"vpc-0143197ca9bd9c117",
            "HealthCheckProtocol":"HTTPS",
            "HealthCheckPort":"traffic-port",
            "HealthCheckEnabled":true,
            "HealthCheckIntervalSeconds":30,
            "HealthCheckTimeoutSeconds":5,
            "HealthyThresholdCount":5,
            "UnhealthyThresholdCount":2,
            "HealthCheckPath":"/",
            "Matcher":{
               "HttpCode":"200"
            },
            "TargetType":"instance"
         }
      ]
   }
```

2. From the output, record the value of `TargetGroupArn` in your AWS worksheet.

Tagging the Target Group (CLI)

Optionally, you can tag the target group for easier identification.

To tag the target group using the CLI:

1. Run the following command:
   ```
   # aws elbv2 add-tags \
   --resource-arns <Target group values for frontend-ingress-controller-svc and portal-ingress-controller-svc ARN> \
   --tags Key=owner,Value=<owner>
   ```

```
# aws elbv2 add-tags \
--resource-arns arn:aws:elasticloadbalancing:eu-central-1:115370848038:targetgroup/srgdemo-5443-tg/c0684be94405b6b7 \
--tags Key=owner,Value=srgdemo
```

Adding Targets to the Target Group for Controller Services

To add targets to the target group:

1. Run the following command:
   ```
   # aws elbv2 register-targets \
   --target-group-arn <Target group values for frontend-ingress-controller-svc and portal-ingress-controller-svc ARN> \
   --targets Id="Instance 1 ID,Port=<new ingress service node port>" Id="Instance 2 ID,Port=<new ingress service node port>" Id="Instance 3 ID,Port=<new ingress service node port>"
   ```

Where:

`<Instance x ID>`: Use the instance IDs you gathered for instances of the Auto Scaling group. Refer to the AWS worksheet.

<Target group values for frontend-ingress-controller-svc and portal-ingress-controller-svc ARN>: The ARN of the target group you just created.

`<New ingress service node port>`: Use the `node port number` you just created.

Example:

```
# aws elbv2 register-targets \
--target-group-arn arn:aws:elasticloadbalancing:eu-central-1:115370811111:targetgroup/srgdemo-5443-tg/a096cb67c2f9144d \
--targets Id="i-05662f9ef84c182ca,Port=31704" Id="i-07cfcd6716e9890b5,Port=31704" Id="i-08d819b5ccabe83cb,Port=31704"
```

Modifying Listeners on Ports 3000 and 5443

1. Using the **Find Services** search tool, locate and browse to the EC2 Dashboard.
2. In the left navigation panel, under **Load Balancing**, click **Load Balancers**.
3. From the list of load balancers, select your **Application Load Balancer** (ALB).
4. On the **Listeners** tab, look for the listeners for ports 3000 and 5443, and edit each one individually, selecting the newly created target group corresponding to the port under **Listener details**.

Upgrading Deployed Capabilities in AWS

> **Tip:** The registry credentials have an expiration deadline of 12 hours after creation. If more time than that has elapsed, make sure to refresh the credentials before running this procedure.
>
> See "Refreshing the ECR Credentials in Kubernetes" on page 661.

As part of the upgrade process, you must upgrade your deployed capabilities using the OMT Management Portal. Perform these steps in order:

1. "Understanding the Upgrade Prerequisites" below
2. "Upload the Upgrade File" on the next page
3. "Verifying the Certificate Validation" on the next page
4. "Considerations for Upgrading Intelligence" on the next page
5. "Upgrading Deployed Capabilities" on page 415

Understanding the Upgrade Prerequisites

Before upgrading the Suite, ensure these requirements are met:

- Ability to access the management portal on port 5443
- The AWS client is configured on the bastion
- The Kubernetes command line tool (`kubectl`) is installed on the bastion and connected to your cluster
- Ensure all pods are running with this command:

  ```
  kubectl get pods -A
  ```

- Verify you have performed all the required tasks and obtained all installation packages as discussed in "Upgrade Prerequisites " on page 397.

Upload the Upgrade File

1. Upload the metadata file for the upgrade version to your bastion host, the name of which follows this format: `arcsight-suite-metadata-uv.x.tar.gz`

   For example: `arcsight-suite-metadata-23.2-cloud.tar`
2. Upload offline images of the upgrade version to your bastion host, which follow this format: `{product}-uv.x.tgz`

   For example: `transformationhub-3.5.4.4-cloud.tar`

Verifying the Certificate Validation

Verify that your certificate has been validated. Do the following:

1. On the OMT Management Portal, click **DEPLOYMENT**, and then select **Deployments.**
2. Click the **Three Dots** (Browse) on the far right and then choose **Reconfigure**.

   > **Note:** If you are unable to access the OMT Management Portal Reconfigure Page during the upgrade process, perform the steps detailed in "Accessing the OMT Management Portal Reconfigure Page" on page 509 before continuing with this procedure.
3. (Optional) Any new parameters for upgraded capabilities are presented. You can set values for them, if desired, or leave the defaults in place.
4. If your certificate has not yet been validated, you are prompted to accept the certificate. Do so now. If you are not prompted, then your certificate has already been validated and no action needs to be taken.
5. Ensure the certificate of the browser you intend to use for the capability upgrade is validated before the upgrade process is initiated.

Considerations for Upgrading Intelligence

If you are upgrading Intelligence and do not need the upgraded platform to be multi-tenant enabled, consider performing the following steps on the NFS:

- Ensure that you move your SQL loader scripts from: `/<arcsight_efs_vol_path>/arcsight-volume/interset/analytics/vertica_loader_sql/0/<existing_folder_name>` to

  `/<arcsight_efs_vol_path>/arcsight-volume/interset/analytics/vertica_loader_sql/0/1.<existing_folder_name>`
- If you are using custom data identifiers, ensure that you back up the `logstash-config-pipeline` config map that is accessible through the Kubernetes dashboard.

Upgrading Deployed Capabilities

Important: DO NOT CLOSE YOUR BROWSER at any time during this process. If you inadvertently close the browser, use this method to recover.

Perform all of the following steps from the bastion to which you downloaded the upgrade files.

1. Delete any pre-existing upgrade pods by running the following command from the master node:

```
kubectl delete deployments suite-upgrade-pod-arcsight-installer -n
$(kubectl get namespaces | grep arcsight-installer | awk ' {print $1} ')
```

   The above command might return a spurious error message. It can be ignored and you can proceed to the next step.

2. Change to the following directory:

```
cd arcsight-platform-cloud-installer-<VERSION>.zip/aws-scripts/scripts
```

3. Run the following commands to upload the images to the Elastic Container Registry (ECR). Use the `-F <image file>` option on the command line multiple times for each image to upload. Adjust the value of the `-c` parameter (8 in the instruction below) to up to half your CPU cores in order to increase the speed of the upload.

```
./upload_images_to_ECR  -o $(kubectl get cm -n core base-configmap --
output=jsonpath={.data.REGISTRY_ORGNAME}) -c 8 -F arcsight-platform-cloud-
installer-<VERSION>.zip/images/Core-x.x.x.x.tar -F {unzipped-installer-
dir}/images/recon-x.x.x.x.tar
```

   Upload the Intelligence tar file only if you are upgrading Intelligence with the ArcSight Platform and do not need the upgraded platform to be multi-tenant enabled.

4. Add new metadata.

   Make sure to copy the `arcsight-suite-metadata-x.x.x.x.tar` to the system where your web browser is running before performing the process below.

5. Browse to the management portal at `https://<virtual_FQDN>:5443`.
   a. Click **DEPLOYMENT>Metadata** and click **+ Add**.
   b. Select `arcsight-suite-metadata-x.x.x.x.tar` from your system, and click **Ok**. The new metadata is added to the system.
6. Start the upgrade process.

> While the upgrade process is running, if you cannot complete it for any reason, make sure to cancel it before you navigate away from it.

a. Go to **DEPLOYMENT > Deployments**. Notice the number **1** in the red circle in the Update column.

> Minor version changes do not display like regular updates (for example: 22.1.0.15 -> 22.1.0.16.)

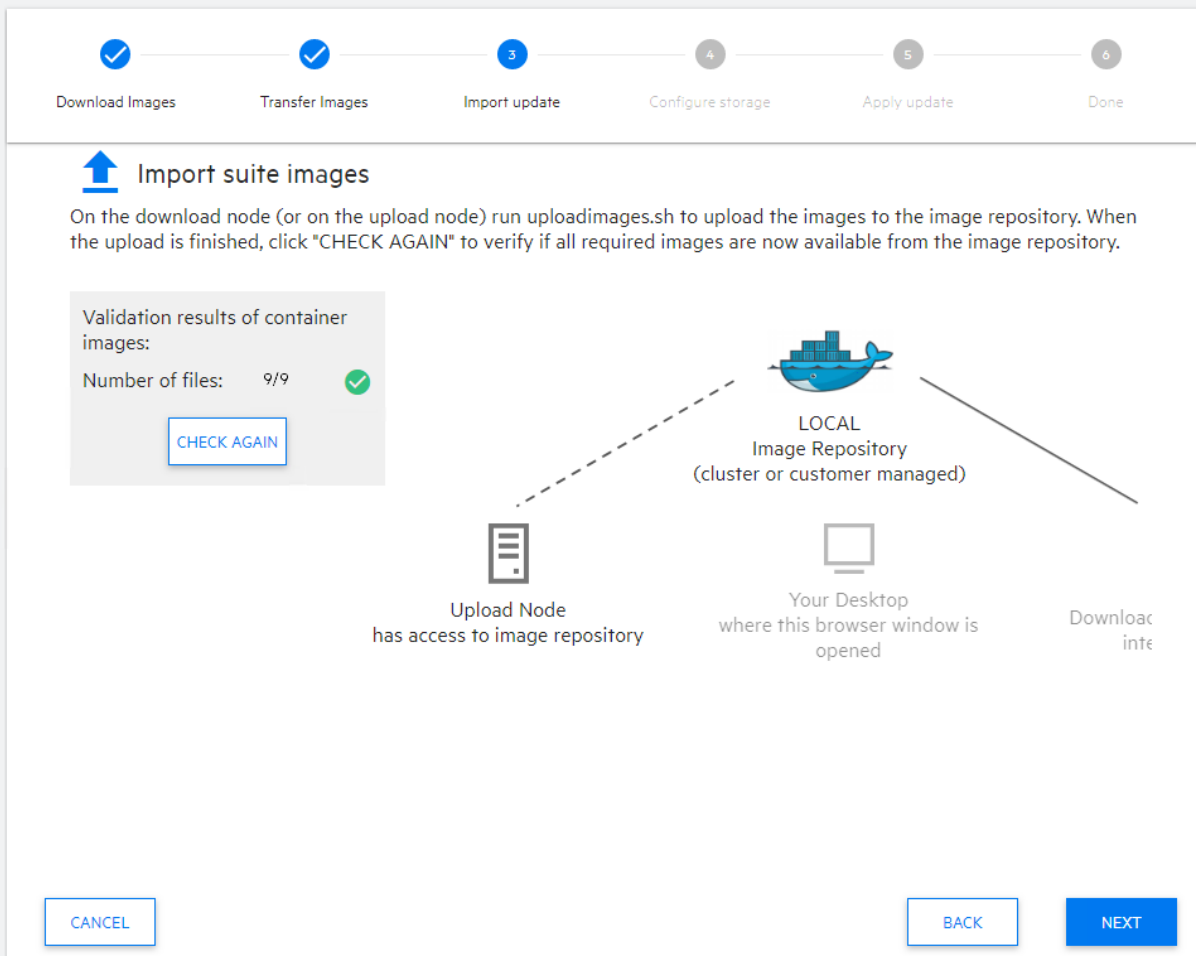
b. Click the red circle and select your recently added metadata to initiate the upgrade.

7. From the **Update to** page, click **NEXT** until you reach the **Import suite images** page.

> When prompted to download or transfer images, you can simply click Next to skip the steps. You performed these steps earlier.

8. Ensure that the validation results of container images show a complete number of files.

> When you arrive at the **Import suite images** page, the images should already be imported, as you performed these steps earlier.



9. Click **NEXT** until you reach the **Upgrade Complete** page.

> **Note:** In the rare event of upgrade failure, consult the log for errors at `/tmp/autoUpgrade/upgradeLog/upgrade-<timestamp>.log`.

Resetting Update Status Using Swagger

If you have inadvertently closed the browser during an upgrade, you will need to reset the status of the pending upgrade using apiserver in the Swagger UI in order to recover and be able resume the upgrade. Do the following:

1. On the bastion, run this command:

   ```
   kubectl edit deployment cdf-apiserver -n core
   ```

2. Locate ENABLE_SWAGGER and change its value from `false` to `true`. Save the change.
3. After the `cdf-apiserver` pod restarts automatically, log in as admin to the OMT Management Portal.
4. Launch a second window and open Swagger:

   `https://VIP_FQDN:5443/suiteInstaller/swagger-ui/`
5. In the OMT Management Portal, on the **Deployments** page, press the F12 key.
6. Switch to the **Network** tab.
7. Refresh the page. Copy and paste each of the following to a text file:
   - From the response section, the `deploymentUuid`
   - From the headers section, the x-auth-token: for example,
     `eyJ0eXAiOiJKV1MiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiIyYzkwODQ4NTdkN2E0NzM0MDE3ZDdhNDc0ODdhMDEwZSIsImlzcyI6IklkTSAxLjMyLjEtYnVpbGQuMjc5IiwiY29tLmhwZS5pZG06dHJ1c3RvciI6bnVsbCwiZXhwIjoxNjM4NDYyODE2LCJjb20uaHAuY2xvdWQ6dGVuYW50Ijp7ImlkIjoiMmM5MDg0ODU3ZDdhNDczNDAxN2Q3YTQ3NDcyYzAwYjciLCJuYW1lIjoiUHJvdmlkZXIiLCJlbmFibGVkIjp0cnVlfSwicHJuIjoiYWRtaW4iLCJpYXQiOjE2Mzg0NjEwMTYsImp0aSI6Ijc0MzhiZDYzLWNkNTYtNDRiNC05MWUyLTBkMTZlZGI4MmI0YyJ9.fd_qxCmeEsbIPc2m04phnQ07MGPFwLW56m127qIE5Tw`
8. In Swagger, verify in the top right that you are in **Public API** section.
   a. Select the csrf-token controller, and click the blue **GET** button.
   b. In the resulting dropdown, click **Try it out.** Paste the x-auth-token you previously copied and execute.
   c. Note the value of `csrfToken` from the Response body, for example: `41d6355f-a0a5-4aa3-80d6-cf1bb09ae7ab`.
   d. Copy and paste this value to your text file.

9. In the top right, switch from the **Public API** section to **Internal API** section, and expand the `kube-upgrade-service-controller` section.
10. On `/suiteInstaller/urest/v1.1/deployment/{deploymentUuid}/upgrade/cancel` (the second line in the Controller selections), click **POST**.
11. Click **Try it out** and provide values for the x-auth-token, csrf-token, and deployment ID from your text file.
12. Click **Execute** to cancel the upgrade.
13. Return to the OMT Management Portal page and retry the installation or upgrade.

    Note: It can take a few minutes for the previous upgrade process to terminate. Please be patient and allow the termination time to complete.

14. Repeat the upgrade process again.
15. To disable swagger, repeat the commands in step 1 and 2. The `cdf-apiserver` will restart automatically. Swagger is disabled by default for security reasons, but is not accessible if no active login session to the management portal on port 5443 is found.

Configure the Load Balancer for capabilities

Changes in the deployed services require updating the target port registered in the 443 target group.

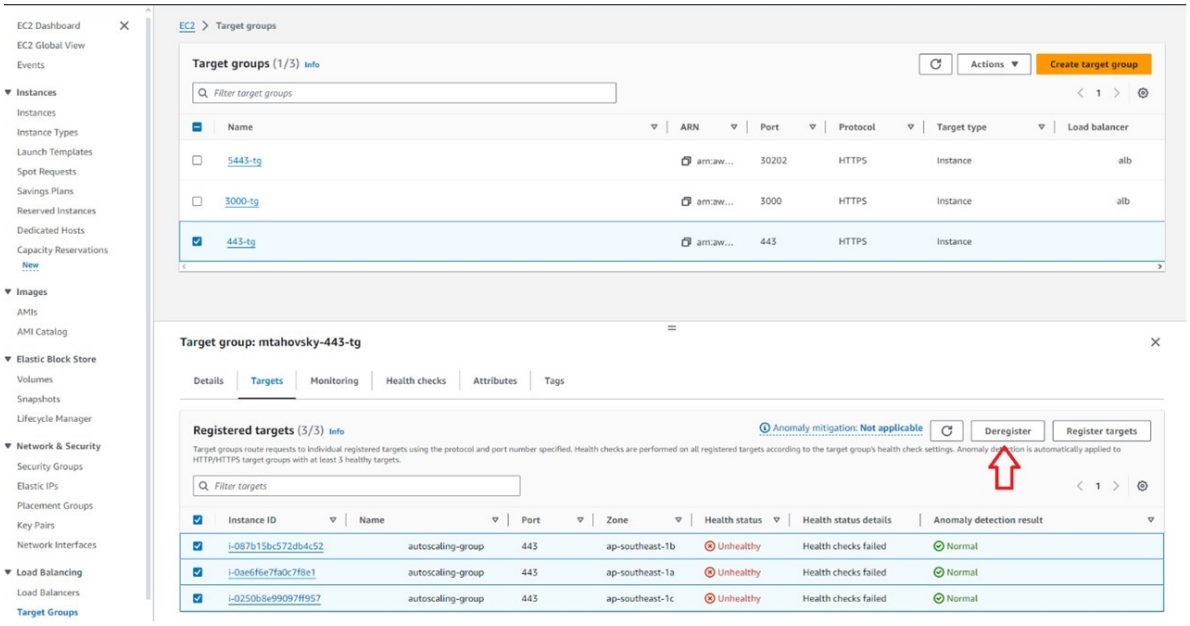
1. Execute the following command to obtain the new ingress service ports.

   ```
   kubectl get svc -A | grep nginx-ingress-controller-svc
   ```

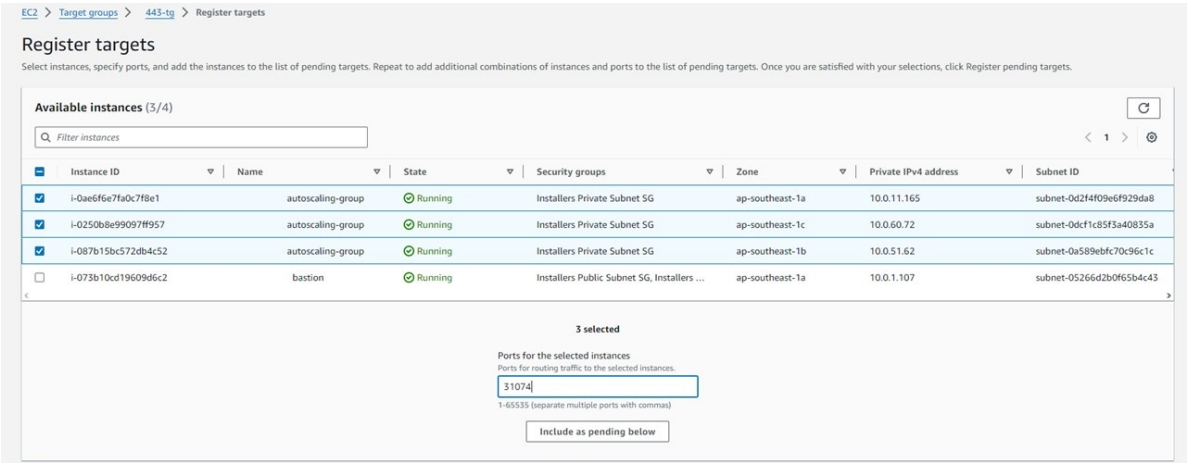
   Example output:

   ```
   arcsight-installer-wjlal   nginx-ingress-controller-svc NodePort
   172.20.116.136 <none> 443:31074/TCP
   ```

   Where **31074** is the new ingress service node port for port 443, and must be recorded in the AWS worksheet.
2. Go to the **Find Services** search tool and use it to locate and browse to the **EC2 Dashboard**.
3. In the left navigation panel, under **Load Balancing**, click **Target Groups**.
4. Select the target group for port 443 and click the **Deregister** button to deregister all targets:



5. On the same page, click **Register targets** and for **Ports for the selected instances**, use the value obtained here.



6. Click the **Include as pending below** button and then click **Register pending targets**.

Upgrading EKS

Prerequisites for the EKS Upgrade

This procedure will upgrade the existing control plane and worker nodes from their present Kubernetes version to a currently supported version of EKS (look for **Hybrid Cloud Support** in the *Technical Requirements for ArcSight Platform 24.2*). As the EKS version can be upgraded only one version number at a time, you must repeat this procedure for each incremental version until the cluster is at the required version.

During each stage of the upgrade, system replaces the worker nodes one at a time with the newer EKS version, so as to avoid data loss or excessive cluster downtime.

Determine EKS AMIs

Determine the EKS AMIs required for each EKS upgrade stage. You will incrementally upgrade from your current version, to a currently supported version. See **Hybrid Cloud Support** in the *Technical Requirements for ArcSight Platform 24.2*.

1. For each incremental upgrade, run the following command:

   ```
   aws ec2 describe-images \--filters "Name=architecture,Values=x86_64"
   "Name=name,Values=amazon-eks-node-<Kubernetes version>*" | jq '.Images |
   map(select((.Description!=null) and (.Description | contains("GPU") |
   not) and (.ImageLocation | contains("gpu") | not))) | sort_by
   (.CreationDate) | [last]'
   ```

   where `<Kubernetes version>` is your current version.

2. Make note of each AMI image ID that the system returns each time. You will need this information in the next step in the upgrade process.

   For example:

   ```
   $ aws ec2 describe-images \--filters "Name=architecture,Values=x86_64"
   "Name=name,Values=amazon-eks-node-1.26*" | jq '.Images | map(select
   ((.Description!=null) and (.Description | contains("GPU") | not) and
   (.ImageLocation | contains("gpu") | not))) | sort_by(.CreationDate) |
   [last]'|grep "ImageId"
   "ImageId": "ami-0aa4096ec49a62235",
   ```

   ```
   $ aws ec2 describe-images \--filters "Name=architecture,Values=x86_64"
   "Name=name,Values=amazon-eks-node-1.27*" | jq '.Images | map(select
   ((.Description!=null) and (.Description | contains("GPU") | not) and
   (.ImageLocation | contains("gpu") | not))) | sort_by(.CreationDate) |
   [last]'|grep "ImageId"
   "ImageId": "ami-00cf63b12c53803a5",
   ```

Open topic with navigation

Create Launch Templates

Create the required launch templates for each of the EKS upgrade versions. Launch settings, featured in prior AWS versions, has been deprecated and replaced by launch templates.

For information on how to convert an existing launch configuration into a launch template, see Migrating a Launch Configuration to a Launch Template. ArcSight recommends you migrate to launch templates as soon as possible.

These launch templates use the previously-determined AMIs, which you noted. Do the following:

1. Log into the AWS console and browse to the **Launch templates** management page.
2. Select your current launch template.
3. Click **Actions > Modify template (Create new version)** to create a copy of the selected configuration. It's helpful do add a description that includes the EKS version contained, so as to tell one version from the others easily.
4. In **Application and OS Images (Amazon Machine Image)**, paste the name of the new AMI for the EKS version you're upgrading to in the **Search our full catalog…** box. Click **enter**.

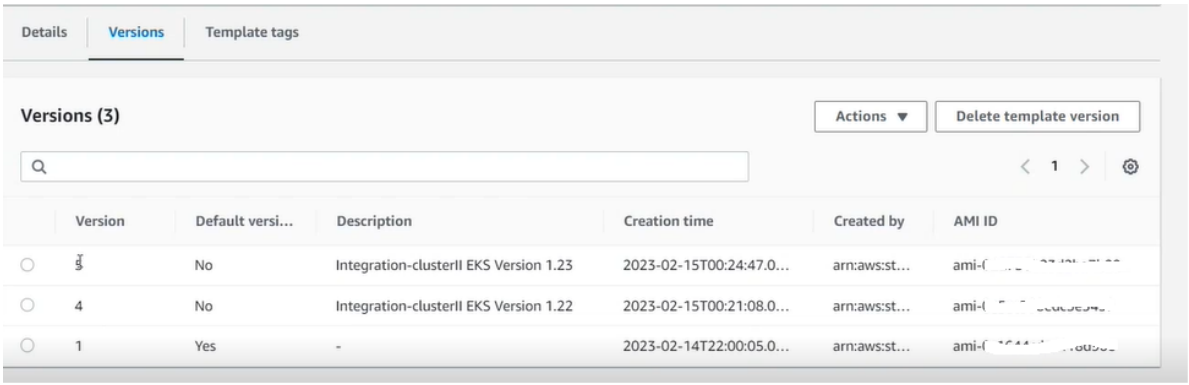
   This will take you to the **Quickstart AMIs**, **My AMIs**, **AWS Marketplace AMIs** or **Community AMIs** tabs. Choose the one that correspond for your case, and select your AMI from it.

   This will bring a pop up message stating that **Some of your current settings will be changed or removed if you proceed**. Click **Confirm changes** to proceed, since this will only apply to the version of the template you're actually editing.

   > Leave the rest of the settings at their default value, except for **Storage (volumes) -> EBS Volumes -> Size (GiB)**. This value defaults to 20, and before proceeding you must change it to reflect the same storage value of the previous launch template.

   Under **Advanced details**, the only verification due would be to check that the **User data – optional** box contains the same user data as the original template. If there was no user data in the original, there's no need to change anything.

   Clicking on **Create template version** will open the newly created template version:

   The description added on step 3 will guide you regarding the version of EKS that should be chosen.
5. Repeat steps 2 through 4 to create a new launch template for the next EKS version, using the corresponding AMI which you previously determined.

Except for the name and AMI image ID, all launch template parameters must be the same as the original. This includes:

- Any desired notifications
- Tags contained in the original group
- Same VPC and all private Availability Zones

Prepare the Environment

You must prepare your environment for the upgrade by doing the following:

- To maintain connection to the Kafka Manager throughout the process, run the following command to patch the th-kafkamgr-svc service:

```
kubectl patch svc -n $(kubectl get ns|awk '/arcsight/ {print $1}') th-
kafkamgr-svc -p '{"spec": { "type": "NodePort", "ports": [ { "nodePort":
32090, "port": 9000} ] } }'
```

- Create a Target Group for port 32090 which uses HTTPS and includes all nodes (old and new). Modify the Health Check path and add: `/th/cmak`.
- Create a listener on the ALB for port 32090 which uses HTTPS and forwards to the new Target Group.
- The resulting URL for accessing Kafka Manager for your cluster after you complete these preparations is: `https://<your cluster DNS name>:32090/th/cmak`

Next Step - **If you have Intelligence in your deployment**: "Enable the search-manager" on the next page

Next Step - **If you don't have Intelligence in your deployment**:"Performing the EKS Upgrade" on page 424

Backing Up the Elasticsearch Data

If Intelligence is deployed in your platform, performing a Elasticsearch data backup will ensure you can restore the data in case there are any issues during the upgrade process. Follow the steps below to backup your data.

1. "Enable the search-manager" on the next page
2. "Scale down logstash" on the next page
3. "Elasticsearch data backup" on the next page
4. "Verify the job status" on page 424

Enable the search-manager

1. Specify the following URL to log in to the OMT Management Portal: https://<CLUSTER FQDN>:5443.
2. Select **Deployment** > **Deployments**.
3. Click **...** (Browse) on the far right and choose **Reconfigure**. A new page will be opened in a separate tab.
4. Click **Intelligence**.
5. Toggle the **Enable Search Manager** button under **Upgrade Configurations**.

Scale down logstash

Execute the following command from the bastion to scale down `logstash`:

```
kubectl -n $(kubectl get ns |awk '/arcsight/ {print $1}') scale statefulset
interset-logstash --replicas=0
```

To ensure that the `logstash` pods have effectively been scaled down, run the following command:

```
kubectl -n $(kubectl get ns |awk '/arcsight/ {print $1}') get pods -A | grep
logstash
```

Also verify no logstash pods are running.

Elasticsearch data backup

1. Login with system-admin role to the interset UI `https://<CLUSTER FQDN>/interset`
2. Click on the gear icon on the top right corner and select **Search Manager**.
3. Click on the **Job History** list box.
4. Select **Submit a Job**.
5. Click on the **Job type** list box and select **Snapshot**.
6. Enter 0 for the **Customer to apply Snapshot to** field.
7. Click the **SUBMIT JOB** button.

Verify the job status

Go to the **Job history** page and check the **Snapshot** job ID status. Click the **REFRESH** button until the status becomes either **COMPLETED_SUCCESS** or **COMPLETED_FAILED**.

If the final status is **COMPLETED_FAILED**, execute this command:

```
kubectl logs  -n $(kubectl get ns |awk '/arcsight/ {print $1}')
elasticsearch-master-0 -c  elasticsearch | grep snapshot
```

The output of this command should include a **[SUCCESS]** message in the output. Repeat the command if the **[SUCCESS]** message does not appear.

> Depending on the amount of data, it may take some time for the **[SUCCESS]** message to appear.

If still unsuccessful after multiple attempts, do not proceed with the upgrade procedure and reach out to customer support for help.

Output examples for successful attempts:

```
{"type": "server", "timestamp": "2022-12-07T15:07:13,016Z", "level": "INFO",
"component": "o.e.s.SnapshotsService", "cluster.name": "interset",
"node.name": "elasticsearch-master-0", "message": "snapshot [repository_
0:snapshot_0_698fee7c-60f4-45e5-bfee-7c06e0f8c415/f5CXpkRpSx6ltB-mIS_TaA]
started", "cluster.uuid": "0Kef4EV2RRaVPQiJHxQQiw", "node.id":
"l6zdkuvgTvq1KZJJQmd-xA" }
```

```
{"type": "server", "timestamp": "2022-12-07T15:07:19,076Z", "level": "INFO",
"component": "o.e.s.SnapshotsService", "cluster.name": "interset",
"node.name": "elasticsearch-master-0", "message": "snapshot [repository_
0:snapshot_0_698fee7c-60f4-45e5-bfee-7c06e0f8c415/f5CXpkRpSx6ltB-mIS_TaA]
completed with state [SUCCESS]", "cluster.uuid": "0Kef4EV2RRaVPQiJHxQQiw",
"node.id": "l6zdkuvgTvq1KZJJQmd-xA" }
```

> If the snapshot job continues to remain in the **Pending** state for a prolonged period of time, restart the `searchmanager-engine-xxxxxxxxxx-xxxxx` pod.

Open topic with navigation

Performing the EKS Upgrade

During the upgrade of EKS, you will first upgrade the EKS control plane, and then upgrade the EKS version on each of the worker nodes. You must upgrade EKS to version 1.26, one version of EKS at a time.

To perform the EKS control plane and worker node upgrade:

1. Browse to the EKS console, then click **Clusters**.
2. From the cluster list, select the cluster to be upgraded and click **Update now.**

   > If your cluster is at EKS version 1.22, attempting the next update will prompt a warning message, stating that: "**if you are using EBS volumes in your cluster, then you must install the Amazon EBS CSI driver before updating your cluster to version 1.23 to avoid interruptions to your workloads**". You can ignore this message and proceed with the update without installing the EBS CSI driver.

3. Select the new Kubernetes version, which must be one version number higher than the current version. For example, 1.22 to 1.23.
4. Click **Update**.

   > It's normal for this process to take around 20 minutes. Once finished, the control plane will have been upgraded.
   > **Do not proceed** until this process has completed successfully.

5. After the EKS control plane upgrade is completed, browse to the **Auto Scaling groups** page and create a new Auto Scaling group for Kafka workers. The new Auto Scaling group contains the same number of nodes (and the same roles) as the current Auto Scaling group, but using the newly-created launch template for the Kubernetes version to which you are upgrading.
   a. In **Choose launch template or configuration**, look for the name of the one just created, and then select the version that contains the right EKS upgrade.
   b. Select the same VPC and all private Availability Zones.
   c. In **Configure advanced options**, for the **Load balancing - optional** value, check **Attach to an existing load balancer**.

      From the **Attach to an existing load balancer** menu, check **Choose from your load balancer target groups**. This will allow you to select the load balancer target groups created for this cluster (3000, 443, 5443, 32080, 32081, 32090, 32101-32150 for the CTH pods, etc) from a list box.

      > You can start writing the name of the groups on the **Existing load balancer target groups** box, and click each of them to add it. You cannot make multiple selections, since the list box will close each time one is chosen, but it can be reopened to enter the rest of the groups

      This selection will automatically register the **Auto Scaling group** nodes to the target groups.

Leave all other advanced options at default values.

d. Ensure group sizes for desired, minimum and maximum are the same as the original Auto Scaling group.

e. Add any desired notifications.

f. Add the same tags contained in the original group. Make sure that the EKS cluster name appears in the tags.

g. Review the new configuration and click **Create Auto Scaling group**. This process will create three new nodes.

> Following the completion of the worker node upgrade, the Kafka broker IDs (as seen in the Kafka Manager UI under **Brokers**) will all be incremented by 1 from their starting values. This is expected.

See Creating the AWS Auto Scaling Group for more information.

6. Get the cluster node names by running the following command, and then record the node names returned:

```
kubectl get nodes
```

Example output:

```
NAME                                          STATUS   ROLES    AGE
VERSION
```

```
ip-10-0-10-253.example.com   Ready    <none>   10m    v1.23.14-eks-
ba74326
```

```
ip-10-0-10-61.example.com    Ready    <none>   3d1h   v1.23.15-eks-
ba74326
```

```
ip-10-0-13-119.example.com   Ready    <none>   3d1h   v1.23.15-eks-
ba74326
```

```
ip-10-0-13-40.example.com    Ready    <none>   10m    v1.23.14-eks-
ba74326
```

```
ip-10-0-14-238.example.com   Ready    <none>   10m    v1.23.14-eks-
ba74326
```

```
ip-10-0-15-193.example.com   Ready    <none>   3d1h   v1.23.15-eks-
ba74326
```

> Repeat the following sequence consisting of steps 7 through 12 on each of the original Kafka worker nodes, cycling throughout the nodes one by one, until the sequence has been performed on all worker nodes. Proceed to Step 13 only after the sequence has been performed on each original Kafka worker node..

7. Select a worker node and drain it by running the following command.

```
kubectl drain <FQDN of selected node> --force --delete-emptydir-data --ignore-
daemonsets --timeout=180s
```

> If the `intelligence-namenode=yes` label has been applied to any node, then drain that node **last** among all nodes.

Wait for the command to complete and for all pods to return to the Running state before proceeding to the next step. **The drain/cordon process can take several minutes for all pods to return to the Running state. Please be patient and allow the process time to complete and all pods to return to Running state.**

> If a **CrashLoopBackOff** or **error** status appears during this process, it can be ignored

8. Log in to Kafka Manager (cmak) at `https://<CLUSTER FQDN>:32090/th/cmak` and re-assign Kafka partitions for the node with these commands:

   a. Click **Generate Partition Assignments** and select all topics (default)

   b. Click **Run Partition Assignments** (use default settings for broker IDs)

   c. Click **Go** to reassign partitions and refresh the page until the *Completed* field shows a data and time of completion.

9. (Conditional) If your deployment includes ArcSight Intelligence, then monitor the ES replication process by logging into the pod and executing this command:

```
kubectl exec -n $(kubectl get ns |awk '/arcsight/ {print $1}')
elasticsearch-master-0 -c  elasticsearch -it bash
```

Monitor the **ES replication** process using the following command:

```
curl -k -XGET 'https://elastic:<password>@localhost:9200/_
cat/health?v=true'
```

Example command and output:

```
curl -k -XGET 'https://elastic:changeme@localhost:9200/_
cat/health?v=true'
```

```
epoch      timestamp cluster  status node.total node.data shards pri relo
init unassign pending_tasks max_task_wait_time active_shards_percent
1671118161 15:29:21  interset green           6         3   1128 583    0
   0        0             0                  -                100.0%
```

> At the completion of the Elasticsearch replication, the status of all nodes should be "green". A "yellow" status indicates that the replication has not yet completed.
>
> However, if the Elasticsearch recovery is not progressing and the `active_shards_percent` does not reach 100%, or its status is **red**, you may disregard the pods not returning to running state and proceed with the EKS upgrade (this applies to **intelligence** and **searchmanager** pods). This is because, after cordoning the node, some interset pods might remain in `init` state, but this can be ignored.

10. In Kafka Manager, check that the topic partition table data returns to normal. There should be no under-replication of data, and broker leader skew values should return to 0%. Do the following:
    a. Select a Kafka pod and log into it.
    b. **Check for under-replication:** Select one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line. The command block will return no result if there is no under-replication.

    For FIPS (or non-FIPS) Encryption with Client Authentication:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=$STORES_
SECRET/" /etc/kafka/client.properties && \sed -ir "s/^
[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=$STORES_
SECRET/" /etc/kafka/client.properties && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --describe --topic
th-cef --under-replicated-partitions --command-config
/etc/kafka/client.properties'
```

    After executing the above, **Copy** and then paste the following command block:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=/"
/etc/kafka/client.properties && \
```

```
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=/"
/etc/kafka/client.properties'
```

For FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'KAFKA_OPTS+=" -
Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-kafka.truststore " &&
\
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreProvider=BCFIPS " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreType=BCFKS " && \
kafka-topics --bootstrap-server th-kafka-svc:9093  --describe --topic
th-cef --under-replicated-partitions --command-config
/etc/kafka/client2.properties'
```

For non-FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'KAFKA_OPTS+=" -
Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-kafka.truststore " &&
\
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
kafka-topics --bootstrap-server th-kafka-svc:9093  --describe --topic
th-cef --under-replicated-partitions --command-config
/etc/kafka/client2.properties'
```

Whether or not there's a result to the command, each of them will return the following warning messages, which can be ignored:

WARNING: An illegal reflective access operation has occurred

WARNING: Illegal reflective access by org.bouncycastle.jcajce.provider.ProvSunTLSKDF (file:/opt/th/libs/bc- fips- 1.0.2.3.jar) to constructor sun.security.internal.spec.TlsPrfParameterSpec (javax.crypto.SecretKey,java.lang.String,byte[],int,java.lang.String,int,int)

WARNING: Please consider reporting this to the maintainers of org.bouncycastle.jcajce.provider.ProvSunTLSKDF

WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations

WARNING: All illegal access operations will be denied in a future release

c. **Check for broker leader skew:** As in the last step, select one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line. Verify that the number of times each broker is listed is equal to the `replicationFactor` value.

   For FIPS (or non-FIPS) Encryption with Client Authentication:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=$STORES_
SECRET/" /etc/kafka/client.properties && \
sed -ir "s/^
[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=$STORES_
SECRET/" /etc/kafka/client.properties && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --describe --topic
th-cef --command-config /etc/kafka/client.properties'
```

After executing the above, **Copy** and then paste the following command block:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=/"
/etc/kafka/client.properties'
```

For FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'KAFKA_OPTS+=" -
Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-kafka.truststore " &&
\
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreProvider=BCFIPS " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreType=BCFKS " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --describe --topic
th-cef --command-config /etc/kafka/client2.properties'
```

For non-FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'KAFKA_OPTS+=" -
Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-kafka.truststore " &&
\
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --describe --topic
th-cef --command-config /etc/kafka/client2.properties'
```

Example output from the above command blocks:

```
Topic: th-cef   PartitionCount: 6       ReplicationFactor: 2
Configs:
cleanup.policy=delete,segment.bytes=1073741824,message.format.version=
2.5-IV0,retention.bytes=6442450944
```

```
Topic: th-cef   Partition: 0    Leader: 1005    Replicas: 1005,1004
 Isr: 1004,1005
```

```
Topic: th-cef   Partition: 1    Leader: 1006    Replicas: 1006,1005
 Isr: 1005,1006
```

```
Topic: th-cef   Partition: 2    Leader: 1004    Replicas: 1004,1006
 Isr: 1004,1006
```

```
Topic: th-cef   Partition: 3    Leader: 1005    Replicas: 1005,1006
 Isr: 1005,1006
```

```
Topic: th-cef   Partition: 4    Leader: 1006    Replicas: 1006,1004
 Isr: 1004,1006
```

```
Topic: th-cef   Partition: 5    Leader: 1004    Replicas: 1004,1005
 Isr: 1004,1005
```

The example output shown above is a final, successful result. It will take time to achieve it, depending on the amount of data, the number of partitions and replication factors.

As well, it might require several executions of the command to reach this point, where all partitions are listed and there are two instances of each leader value.

If this output is not achieved after several executions of the command, please go back to the `cmak` login step and execute parts **a** and **b**. Then come back and execute this command block again.

> Kafka will automatically advertise the new node to the connectors.

11. **Repeat steps 6 through 10 for each additional node in the cluster. When you have completed the steps on each node, only then proceed to Step 10.**
12. (Conditional) If the `intelligence-namenode=yes` label was applied to the node being drained, proceed to Performing the EKS Upgrade - (Conditional) Step 11 - For Intelligence Only

    If not, you can proceed to Step 13 below directly.
13. Delete the old **Auto Scaling group** (you created its replacement as above). Wait until all

nodes from the old **Auto Scaling group** are deleted and all pods have returned to the **Running** state before proceeding to the next step.

> A message may be returned that pods are still running. This message may be ignored.

14. Your next step depends on the EKS version you have reached:
    - If your cluster has been configured for Kubernetes 1.26 already, the upgrade is complete, and you may proceed with the next steps.
    - If your cluster is configured for a Kubernetes version earlier than 1.26, then repeat the entire process above for the next Kubernetes version, beginning with Step 1.

(Conditional) If the ArcSight Database has been deployed, log into the database master node and run these commands:

```
./kafka_scheduler stop
./kafka_scheduler start
```

Verify that Kafka Scheduler has the correct new node IP addresses by running this command:

```
./kafka_scheduler status
```

Verify that Event Table Status events count is increasing by running this command:

```
./kafka_scheduler events
```

Next Step - **If Step 7 failed for your Intelligence deployment**: Recovering and Restoring Elasticsearch Data

Next Step - **If you don't have Intelligence in your deployment**: Continue with the rest of the upgrade checklist.

Performing the EKS Upgrade - (Conditional) Step 11 - For Intelligence Only

If the `intelligence-namenode=yes` label was applied to the node being drained, perform these two steps:

- Add the `intelligence-namenode=yes` label to one of the new nodes and update the node FDQN in the **Reconfigure** page of the OMT (**HDFS NameNode** under the **Intelligence** tab)
- Log into each of the database nodes and replace the **HDFS NameNode** value from the previous step to the `Core-site.xml` file located in the `/etc/hadoop/conf/` directory.

  Select the option that applies to your configuration:

  - If **Enable Secure Data Transfer with HDFS Cluster** is disabled in the **Intelligence** tab of the OMT Management portal, in the `/etc/hadoop/conf` directory, add the following configurations:

In the `hdfs-site.xml` file:

```
<configuration>
</configuration>
```

In the `core-site.xml` file:

```
<configuration>
  <property>
   <name>fs.defaultFS</name>
   <value>hdfs://<namenode>:30820/</value>
  </property>
  <property>
   <name>dfs.namenode.http-address</name>
   <value><namenode>:30070</value>
  </property>
</configuration>
```

- If **Enable Secure Data Transfer with HDFS Cluster** is enabled in the **Intelligence** tab of the OMT Management portal, in the `/etc/hadoop/conf` directory.

  > If Kerberos Authentication is enabled, reconfigure it by following the "Enabling and Configuring Kerberos Authentication" on page 620 procedure before proceeding.

  Navigate to the `/etc/hadoop/conf` directory and add the following configurations:

  In the `hdfs-site.xml` file:

```
<configuration>
  <property>
   <name>dfs.http.policy</name>
   <value>HTTPS_ONLY</value>
  </property>
  <property>
   <name>dfs.encrypt.data.transfer</name>
   <value>true</value>
  </property>
</configuration>
```

  In the `core-site.xml` file:

```
<configuration>
  <property>
   <name>fs.defaultFS</name>
   <value>hdfs://<namenode>:30820/</value>
  </property>
  <property>
   <name>dfs.namenode.https-address</name>
   <value><namenode>:30070</value>
```

```
  </property>
</configuration>
```

Change to the following directory:

```
cd /opt/vertica/bin/
```

Log in as a dbadmin:

```
su dbadmin
```

Log in to vsql and specify the password when prompted:

```
vsql
[password prompt]
```

Next, run the following commands:

```
SELECT CLEAR_HDFS_CACHES();
SELECT VERIFY_HADOOP_CONF_DIR();
SELECT node_name, node_address, export_address FROM nodes;
```

The expected output is:

```
Welcome to vsql, the Vertica Analytic Database interactive terminal.

Type: \h or \? for help with vsql commands
\g or terminate with semicolon to execute query
\q to quit

fusiondb=>
fusiondb=> SELECT CLEAR_HDFS_CACHES();
CLEAR_HDFS_CACHES
-----------------------------------------------------------------------
Cleared
(1 row)

fusiondb=> SELECT VERIFY_HADOOP_CONF_DIR();
VERIFY_HADOOP_CONF_DIR
--------------------------------------------------------------------------
Validation Success
v_fusiondb_node0001: HadoopConfDir [/etc/hadoop/conf] is valid
v_fusiondb_node0002: HadoopConfDir [/etc/hadoop/conf] is valid
v_fusiondb_node0003: HadoopConfDir [/etc/hadoop/conf] is valid

(3 rows)

fusiondb=> SELECT node_name, node_address, export_address FROM nodes;
```

```
node_name | node_address | export_address
---------------------------------------------------------------------
v_fusiondb_node0001 | <IP1> | <IP1>
v_fusiondb_node0002 | <IP2> | <IP2>
v_fusiondb_node0003 | <IP3> | <IP3>
(3 rows)
```

Next Step - **Proceed with the rest of the EKS upgrade steps (resume from Step 12 on)**: "Performing the EKS Upgrade" on page 424

Recovering and Restoring Elasticsearch Data

If you have deployed the Intelligence capability, follow the instructions provided in this section.

- Elasticsearch Monitoring Action Fails During EKS Upgrade
  - Deleting Unassigned Shards
  - Restoring Elasticsearch Data
- Elasticsearch Monitoring Action Succeeds During EKS Upgrade
- If Analytics Run Fails

Elasticsearch Monitoring Action Fails During EKS Upgrade

If the Elasticsearch monitoring actions fails for the Intelligence pods (this could have happened either in step 9 of the "Performing the EKS Upgrade" on page 424 procedure, or step 5 of the "Performing the Nodes Update/Replacement" on page 493 procedure), you must delete the unassigned shards that might impede the recovery process:

- Deleting Unassigned Shards
- Restoring Elasticsearch Data

Deleting Unassigned Shards

1. Run the following command, being sure to replace the <password> value with yours:

```
kubectl exec -it -n $(kubectl get ns |awk '/arcsight/ {print $1}')
elasticsearch-master-0 -c  elasticsearch -- curl -k -XGET
https://elastic:<password>@localhost:9200/_cat/shards | grep UNASSIGNED |
awk {'print $1'} | xargs -i curl -k -XDELETE
'https://elastic:<password>@localhost:9200/{}'
```

2. To monitor the delete progress, run the following command:

```
kubectl exec -n $(kubectl get ns |awk '/arcsight/ {print $1}')
elasticsearch-master-0 -c  elasticsearch -it -- curl -k -XGET
'https://elastic:<password>@localhost:9200/_cat/health?v=true'
```

Example output:

```
epoch      timestamp cluster  status node.total node.data shards pri relo
init unassign pending_tasks max_task_wait_time active_shards_percent
1671118161 15:29:21  interset green           6         3   1128 583    0
   0        0             0                  -                100.0%
```

In the example above, the value has reached a 100% and the status is green.

Restoring Elasticsearch Data

1. If the result of the command is a yellow status, and a value under 100%, apply the following procedure:
   a. Login with system-admin role to the interset UI https://<CLUSTER FQDN>/interset
   b. Click on the gear icon on the top right corner and select **Search Manager**.
   c. Click on the **Job History** list box.
   d. Select **Submit a Job**.
   e. Click on the **Job type** list box and select **Restore**.
   f. Enter 0 for the **Customer to apply Snapshot to** field.
   g. Click the **SUBMIT JOB** button.
2. To verify the job status, complete the following steps:
   a. On the **Job history** page, check the **Snapshot** job ID status.
   b. Click the **REFRESH** button until the status becomes either **COMPLETED_SUCCESS** or **COMPLETED_FAILED**.
   c. If the final status is **COMPLETED_FAILED**, execute the following commands to monitor the health:

      ```
      kubectl exec -n $(kubectl get ns |awk '/arcsight/ {print $1}')
      elasticsearch-master-0 -c  elasticsearch -it curl -k -XGET
      'https://elastic:<password>@localhost:9200/_cat/health?v=true'
      ```

      Example command and output:

      ```
      curl -k -XGET 'https://elastic:changeme@localhost:9200/_
      cat/health?v=true'
      ```

```
epoch      timestamp cluster  status node.total node.data shards pri
relo init unassign pending_tasks max_task_wait_time active_shards_
percent
1671118161 15:29:21  interset green           6         3   1128 583
 0    0        0             0                  -
100.0%
```

In the example above, the value has reached a 100% and the status is green.

d. If the result of the command is a yellow status, and a value under 100%, you could wait 5 minutes and then repeat the command until the green status is achieved.

3. Scale up logstash using the following command:

```
kubectl -n $(kubectl get ns |awk '/arcsight/ {print $1}') scale
statefulset interset-logstash --replicas=<replica count>
```

Now, run analytics on demand.

Elasticsearch Monitoring Succeeds During EKS Upgrade

If the Elasticsearch monitoring actions in step 9 of the "Performing the EKS Upgrade" on page 424 procedure, or step 5 of the "Performing the Nodes Update/Replacement" on page 493 procedure succeeds for the Intelligence pods, run analytics on demand.

If Analytics Run Fails

Follow the workaround, if you encounter any of the following issues:

Issue: If Analytics were to fail after the EKS upgrade, there are two things you can check to remedy it:

Workaround: Perform the following steps:

- Review the logs for the following error:

```
Suppressed: org.elasticsearch.client.ResponseException: method [POST],
host [https://elasticsearch-svc:9200], URI [/_aliases?master_
timeout=30s&timeout=30s],
status line [HTTP/1.1 503 Service Unavailable]{"error":{"root_cause":
[{"type":"not_master_exception",
"reason":"no longer master. source: [index-aliases]"}],"type":"master_
not_discovered_exception",
"reason":"NotMasterException[no longer master. source: [index-aliases]]",
"caused_by":{"type":"not_master_exception","reason":"no longer master.
source: [index-aliases]"}},"status":503}
```

- If this error is found, execute the following commands:

```
kubectl -n $(kubectl get ns |awk '/arcsight/ {print $1}') scale
statefulset elasticsearch-master --replicas=0
```

```
kubectl -n $(kubectl get ns |awk '/arcsight/ {print $1}') scale
statefulset elasticsearch-data --replicas=0
```

```
kubectl -n $(kubectl get ns |awk '/arcsight/ {print $1}') scale
statefulset elasticsearch-master --replicas={replica_count}
```

```
kubectl -n $(kubectl get ns |awk '/arcsight/ {print $1}') scale
statefulset elasticsearch-data --replicas={replica_count}
```

Issue: If Analytics fails after the EKS upgrade because the HDFS namenode has entered safe mode.

Workaround: Perform the following steps:

1. Execute the following command to restart the HDFS pods:

```
kubectl delete pods -n $(kubectl get ns |awk '/arcsight/ {print $1}')
$(kubectl get pods -n $(kubectl get ns |awk '/arcsight/ {print $1}') -o
wide |  grep "hdfs-" | cut -d ' ' -f1)
```

2. Execute the following command:

```
kubectl exec -n $(kubectl get ns |awk '/arcsight/ {print $1}') hdfs-
namenode-0 -c  hdfs-namenode -it bash
```

```
hdfs dfsadmin -safemode leave
```

3. Run Analytics on demand.

Completing Post-Upgrade Tasks

This section describes tasks that must be completed after the upgrade.

To enable Multi-tenancy after the upgrade, see "Enabling Multi-tenancy " on page 442.

Enable the ArcSight Database to Receive SSL Connections

In the Platform 24.2 release, enabling the ArcSight Database to receive SSL connections is mandatory. If you have not already enabled the Database to receive SSL connections, follow the steps in "Completing the Database Kafka Scheduler Setup - AWS" on page 248 to enable it now.

Post-Upgrade Tasks for Intelligence

If you have upgraded Intelligence, you must also perform the following post-upgrade tasks:

- If you have been using custom SQL loader scripts in the previous versions of Intelligence, you need to apply the custom SQL loader scripts.
- If you have been using custom data identifiers, then you need to update the `logstash-config-pipeline` config map. For more information, see Updating the Logstash ConfigMap for Custom Data Identifiers.

Applying Custom SQL Loader Scripts

Note: Applies if Intelligence has been upgraded.

1. Run Analytics to start the next analytics run. For more information, see Running Analytics on Demand.
2. During the analytics run, the 1.14.0.4 folder is created in the following directory with the default SQL loader scripts:

   ```
   cd <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_
   sql/0/1.14.0.4
   ```

3. (Conditional) If you have been using custom SQL loader scripts from previous releases, then the SQL loader scripts with inconsistent md5 sums between the current and previous versions are displayed in the Analytics logs. Perform the following steps to review and modify the SQL loader scripts:

   a. Execute the following command to check the logs of the analytics pod:

   ```
   export NS=$(kubectl get namespaces |grep arcsight|cut -d ' ' -f1)
   pn=$(kubectl get pods -n $NS | grep -e 'interset-analytics' | awk '
   {print $1}')
   kubectl logs -f $pn -n $NS -c interset-analytics
   ```

   b. Review and add the necessary modifications to the new SQL loader scripts present in the following directory:

   ```
   cd <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_
   sql/0/1.14.0.4
   ```

      i. If you are upgrading from 23.2, execute the following command:

      ```
      cd <arcsight_nfs_vol_path>/interset/analytics/vertica_loader_
      sql/0/1.12.4.27
      ```

ii. Update the md5 files with the md5 sums corresponding to the modified SQL loader scripts.

Analytics is triggered automatically after all the SQL loader scripts with inconsistent md5 sums are updated.

Upgrading ESM

If ESM is deployed, you should perform the following:

> For cloud deployments, the OMT upgrade causes the FQDN (fully qualified domain name) of the Kafka nodes to change. This invalidates the ESM event ingestion configuration from Transformation Hub.
>
> Therefore, after the ESM upgrade, the configuration of both ESM and Transformation Hub must be rectified by running the ESM `managersetup` utility and updating the Kafka nodes in the Transformation Hub connection settings.

- Change your ESM enrichment configuration and Transformation Hub topic routing, as described under Local and Global ESM Event Enrichment.
- Upgrade ESM: **be aware that for platform 24.2, ESM requires an upgrade to version 7.7.1 to guarantee ECC compatibility**. See the Upgrade Guide for ESM.

> **Note:** The ESM 7.7 documentation applies to both ESM 7.7 and ESM 7.7.1.

Chapter 8: Maintaining the Platform and Deployed Capabilities

This section describes the maintenance activities that you should perform for the Platform capabilities deployed in your environment.

Changing ArcSight Platform Configuration Properties

> Reconfiguring properties causes the capabilities related to the property to stop and restart and this might cause operations underway to fail. Therefore, ensure that effected capabilities that cannot be easily retried are not running when you reconfigure any of these properties. For example, check the pod logs to see what operations are underway.

To change ArcSight Platform configuration properties:

1. Open a certified web browser.
2. Specify the following URL to log in to the OMT Management Portal: https://<OMT_masternode_hostname or virtual_ip hostname>:5443.
3. Select **Deployment > Deployments.**
4. Click **...** (Browse) on the far right and choose **Reconfigure**. A new screen will be opened in a separate tab.
5. (Optional) Enable Multi-tenancy and required configurations.

> You cannot disable this function after it has been enabled.

6. Update configuration properties as needed.
7. Click **Save.**

All services in the cluster affected by the configuration change will be restarted (in a rolling manner) across the cluster nodes.

Managing a Multi-tenant Environment

> Ensure that you read the "Planning for Multi-tenancy" on page 70 section before you enable Multi-tenancy in your Arcsight Platform environment.

The procedure to create providers and onboard tenants might vary depending on whether you will be or are already using ESM. The following steps provide a high-level overview of setting up multi-tenancy:

1. "Enabling Multi-tenancy " below.
2. Onboard a Provider Profile.
3. (Optional) Integrate tenants and users that exist in your ArcSight ESM deployment.
4. Onboard Tenants.
5. Tune Tenant Topic Settings
6. Provision Tenants.
7. Configure Tenant Topics in Kafka Scheduler.
8. Configure Customer URI in SmartConnectors.
9. Tune the Ingest Pool Concurrency Value.
10. (Optional) Configure ingestion of alerts from ArcSight ESM.

For more information, see Setting Up Multi-tenancy in the *User's Guide for ArcSight Platform.*

Enabling Multi-tenancy

In case of a cloud deployment or upgrade, enable Multi-tenancy from the Core tab of the OMT Management Portal.

> After you have enabled Multi-tenancy, when you log in for the first time, the system prompts you to configure the provider profile and onboard tenants. In case of an upgrade, if any non-System Administrator users log in to ArcSight Platform before the provider and tenants are configured, they see a message that Multi-tenancy migration is in progress.

Create a Database User for the Provider

Applies only when the Multi-tenancy feature is enabled. Not available to customers in the ArcSight SaaS environment..

To create a read-only database user with the db_installer utility, do the following:

1. Log in to the ArcSight database cluster node1 server as root.
2. Navigate to the ArcSight database tools directory. For example: */opt/arcsight-db-tools*.
3. Run the command to create the database user for the Provider:

```
./db_installer create-provider-user
```

> The database user for the provider has permissions to read all the tenant schemas and provide aggregated views on alerts and insights across tenants.

Create a Database Schema and Users for a Tenant

Applies only when the Multi-tenancy feature is enabled. Not available to customers in the ArcSight SaaS environment.

To provision ArcSight Database resources and schema for a tenant, run the *db_installer utility* on the database node. For each tenant, you assign an App Admin user, a Search user, and their Tenant Key. The **App Admin user** has elevated permissions to perform operations on the database for managing the tenant schema. The **Search user** has restricted permissions to perform event search operations for the tenant only. The **Tenant Key** serves as the unique identifier for a tenant. You will use the key again, in the **Create** page, when you onboard that tenant. For more information about onboarding tenants, see the Help while logged into the ArcSight Platform.

In the procedure below, the links for the *Administrator's Guide for ArcSight Platform* direct you to the off-cloud deployment version of the guide. You can find the same topics in the guides corresponding to the following deployment environments:

- AWS
- Azure
- Google Cloud

1. To create the schema for the tenant, complete the following steps:
   a. Log in to the ArcSight Database cluster node1 server as root.
   b. Navigate to the ArcSight Database tools directory, located by default at */opt/arcsight-db-tools*.
   c. To create the database schema for the tenant, run the following command:

      ```
      ./db_installer create-tenant <tenant key>
      ```

      where `<tenant key>` represents the Tenant Key that you want to assign to the tenant. For example, `south_29_test6`. The key must meet the following criteria:

      - 3 to 16 characters
      - Begin with a letter
      - Any combination of letters, numbers, and underscores
      - Case-insensitive
2. Specify credentials for the App Admin user. For more information, see Installing and Configuring the Database Server.

3. Specify credentials for the Search user. For more information, see Installing and Configuring the Database Server.
4. Repeat these steps for each tenant that you want to add to the system.

Tune Tenant Topic Settings

By default, when tenants are provisioned, tenant specific topics are created in Transformation Hub routing rules defined in ArcSight Management Center (ArcMC).

> If a tenant is disabled and the associated SmartConnectors continue to send events, they follow the default route in ArcMC, instead of the tenant specific one. For more information, see Manage Tenant Details.

To facilitate event routing you must configure sufficient number of routing stream processor instances in the OMT Management Portal. For more information, see "Stream Processor Groups" on page 691.

When to Tune

The tuning process is not mandatory, and depends on each tenant's planned event ingestion rate requirements.

For example, a tenant with an expected ingestion of `10 K EPS` would require a high partition and high retention size, while for tenants with lower ingestion rates the default values might be suitable, requiring no tuning.

The procedures below can be applied either to the default topic (`mf-event-avro-enriched-default`), or to the tenant-specific topics, which follow this nomenclature:

```
mf-event-avro-enriched-<tenantKey>
```

See "Configure Tenant Topics in Kafka Scheduler" on page 450 for information on how to identify a tenant’s key.

To tune tenant topic settings based on the event ingestion rate and the retention policy, complete the following steps:

Tuning the Retention Settings for Topics

Kafka topics occupy storage space on worker nodes where you apply the 'kafka:yes' label. To ensure that the nodes have enough storage space for each topic and other components that use storage on these nodes, you must tune the settings for topic retention. Please note that this procedure does not interrupt the flow of events through the system.

1. Log in to an ArcSight master node as root.
2. To determine the current topic retention storage size for a topic, select one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line and **replace {topic name} with the topic in question**.

For FIPS (or non-FIPS) Encryption with Client Authentication:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=$STORES_
SECRET/" /etc/kafka/client.properties && \
sed -ir "s/^
[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --describe --topic
{topic name}  --command-config /etc/kafka/client.properties | grep
retention.bytes'
```

After executing the above, **Copy** and then paste the following command block:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=/"
/etc/kafka/client.properties'
```

For FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreProvider=BCFIPS " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreType=BCFKS " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --describe --topic
{topic name} --command-config /etc/kafka/client2.properties | grep
retention.bytes'
```

For non-FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --describe --topic
{topic name} --command-config /etc/kafka/client2.properties | grep
retention.bytes'
```

3. To set the retention size for a topic, select one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line, **replacing {topic name} with the topic in question, and {retention size in bytes} with the new retention size in bytes**.

For FIPS (or non-FIPS) Encryption with Client Authentication:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=$STORES_
SECRET/" /etc/kafka/client.properties && \
sed -ir "s/^
[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --alter --topic {topic
name} --add-config retention.bytes={retention size in bytes} --command-
config /etc/kafka/client.properties'
```

After executing the above, **Copy** and then paste the following command block:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=/"
/etc/kafka/client.properties'
```

For FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreProvider=BCFIPS " && \
```

```
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreType=BCFKS " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --alter --topic {topic
name} --add-config retention.bytes={retention size in bytes} --command-
config /etc/kafka/client2.properties'
```

For non-FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --alter --topic {topic
name} --add-config retention.bytes={retention size in bytes} --command-
config /etc/kafka/client2.properties'
```

Tune Tenant Topic Partition Settings

Kafka partitions or breaks topics into fractions and stores them on different worker nodes where you apply the 'kafka:yes' label to improve scalability. To ensure topics have enough partitions to scale, you must tune topic partition settings. Please note that this procedure does not interrupt the flow of events through the system.

If you increase topic partitions, you cannot decrease them later.

Select your tuning instructions from one of the following scenarios:

- FIPS (or non-FIPS) Encryption with Client Authentication
- FIPS Encryption without Client Authentication
- non-FIPS Encryption without Client Authentication

Each procedure is detailed below.

For FIPS (or non-FIPS) Encryption with Client Authentication:

1. Log in to an ArcSight master node as root.
2. To determine the current partition count for a topic, select one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line and replace {topic name} with the topic in question.

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=$STORES_
SECRET/" /etc/kafka/client.properties && \
```

```
sed -ir "s/^
[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
kafka-configs --bootstrap-server th-kafka-svc:9093 --describe --topic
{topic name}  --command-config /etc/kafka/client.properties | grep
PartitionCount'
```

After executing the above, **Copy** and then paste the following command block:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=/"
/etc/kafka/client.properties'
```

3. To set the partition count for a topic, select one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line, replacing {topic name} with the topic in question, and {partition count} with the newpartition count.

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=$STORES_
SECRET/" /etc/kafka/client.properties && \
sed -ir "s/^
[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
kafka-topics--bootstrap-server th-kafka-svc:9093 --alter --topic {topic
name} --partitions {partition count} --command-config
/etc/kafka/client.properties'
```

After executing the above, **Copy** and then paste the following command block:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=/"
/etc/kafka/client.properties && \
```

```
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=/"
/etc/kafka/client.properties'
```

For FIPS Encryption Without Client Authentication:

1. Log in to an ArcSight master node as root.
2. To determine the current partition count for a topic, select one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line and replace {topic name} with the topic in question.

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreProvider=BCFIPS " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreType=BCFKS " && \
kafka-configs --bootstrap-server th-kafka-svc:9093 --describe --topic
{topic name} --command-config /etc/kafka/client2.properties | grep
PartitionCount'
```

3. To set the partition count for a topic, select one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line, replacing {topic name} with the topic in question, and {partition count} with the newpartition count.

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreProvider=BCFIPS " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreType=BCFKS " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --alter --topic {topic
name} --partitions {partition count} --command-config
/etc/kafka/client2.properties'
```

For non-FIPS Encryption Without Client Authentication:

1. Log in to an ArcSight master node as root.
2. To determine the current partition count for a topic, select one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line and replace {topic name} with the topic in question.

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
kafka-configs --bootstrap-server th-kafka-svc:9093 --describe --topic
{topic name} --command-config /etc/kafka/client2.properties | grep
PartitionCount'
```

3. To set the partition count for a topic, select one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line, replacing {topic name} with the topic in question, and {partition count} with the newpartition count.

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --alter --topic {topic
name} --partitions {partition count} --command-config
/etc/kafka/client2.properties'
```

Configure Tenant Topics in Kafka Scheduler

The ArcSight Database uses an event consumer namely, Kafka Scheduler to ingest events from Transformation Hub's Kafka component. Kafka Scheduler is installed and configured as part of ArcSight Platform deployment.

> In a single tenant environment, the Kafka Scheduler ingests events from the Kafka topic, *"mf-event-avro-enriched"*, but when Multi-tenancy is enabled, it must read and ingest events from *"mf-event-avro-enriched-default"*.

You must configure tenants to ingest events from a tenant specific Kafka topic as source and the tenant schema in the ArcSight Database as the destination to process a tenant's events. Perform the following steps to do so:

1. Log in to the ArcSight database cluster node1 server as root.
2. Navigate to the ArcSight database tools directory. For example: */opt/arcsight-db-tools*.
3. Perform the following steps to change the default source topic for Kafka Scheduler:
   a. To verify the default source topic configured in Kafka Scheduler (or to print the source topic being consumed), run the following command :

   ```
   ./kafka_scheduler status
   ```

> You can perform this change upon onboarding the very first tenant in the user interface.

i. If the source topic is configured to read from *"mf-event-avro-enriched-default"*, skip to step 4.

ii. If the source topic is not configured to read from *"mf-event-avro-enriched-default"*, run the following command to purge the existing Kafka Scheduler configuration and then change the default source topic:

```
./kafka_scheduler disable
```

```
./kafka_scheduler purge
```

iii. Enable Kafka Scheduler to read from *"mf-event-avro-enriched-default"*:

```
./kafka_scheduler add -t default
```

```
./kafka_scheduler enable -t default
```

iv. To verify the default source topic configured in Kafka Scheduler, run the following command:

```
./kafka_scheduler status
```

4. Onboard the tenant in Kafka Scheduler.

> A tenant key is assigned when a tenant is created; you can retrieve this from the Tenant List page in the user interface.

a. To use the tenant key identifier to create an ingest process in Kafka Scheduler, run the following command:

```
./kafka_scheduler add -t <tenantKey>
./kafka_scheduler enable -t <tenantKey>
```

b. To verify the default source topic configured in Kafka Scheduler, run the following command:

```
./kafka_scheduler status -t <tenantKey>
```

c. Verify Kafka Scheduler is now configured to ingest data for a specific tenant.

Configure Customer URI in SmartConnectors

> If **ArcSight Suite** is integrated with **ArcSight Enterprise Security Manager** (ESM), customer tagging should have been already performed.

You must tag both managed and unmanaged **ArcSight SmartConnectors** configured for given tenants with tenant keys. This ensures that all events from a single SmartConnector are tagged with a specific tenant. The steps to configure the Customer URI of managed or unmanaged ArcSight SmartConnectors are listed below.

1. For **ArcSight SmartConnectors** managed by **ArcSight Management Console** (ArcMC):
   a. Log on to the ArcMC.
   b. Click **Node Management**.
   c. In the navigation tree, browse to the container where the connector resides.
   d. In the management panel, click the **Connectors** tab.
   e. From the list of connectors, select all connectors for which you want to edit destination runtime parameters.
   f. Click **Runtime Parameters** to open the wizard and edit the parameters as follows:
      i. Select the destinations whose runtime parameters you want to modify.
      ii. Select the configurations to be affected.
      iii. Select **Network**.
      iv. Modify the **Customer URI** parameter.

      > The Customer URI parameter must be of format, *"/<tenantkey>"* for routing events to the tenant specific Kafka topic in Transformation Hub.

2. For unmanaged ArcSight SmartConnectors:
   a. Navigate to your SmartConnector installation path; locate the *runagentsetup* script file and run it.
   b. Select **Modify** Connector, then click **Next**.
   c. Select **Add**, **Modify**, or **Remove** destinations, then click **Next**.
   d. Select the destination for which you want to configure batching, then click **Next**.
   e. Select **Modify** destination settings, then click Next.
   f. Select **Network**, then click **Next**.
   g. Specify the **Customer URI** setting, then click **Next**.

> The Customer URI parameter must be of format, *"/<tenantKey>"* for routing events to the tenant specific Kafka topic in Transformation Hub.

h. Select **Done** with editing destination settings, then click **Next**.

i. Click **Exit**.

Tune the Ingest Pool Concurrency Parameter in ArcSight Database

When ArcSight platform is configured to run in the Multi-tenancy mode, the planned concurrency value for ingest resource pool must be set to a minimum of 12.

You can set this value in the config.yaml file during installation. If you have not modified the value during installation, you must complete the following steps as a root user on the ArcSight Database node:

1. On the Database cluster node1 server, browse to the ArcSight Database tools installation path:

   ```
   cd <ARCSIGHT_DATABASE_TOOLS_PATH>
   ```

   ```
   For example, cd /opt/arcsight-db-tools
   ```

2. To tune the planned concurrency parameter by using the `tuning_util.sh` utility, execute the following command:

   ```
   ./scripts/tuning_util.sh -c 12
   ```

3. To verify if the ingest pool concurrency value is set to 12, execute the following command:

   ```
   grep ^ingest_pool_planned_concurrency config/resource_pools.properties
   ```

Understanding Labels and Pods

During installation, you apply labels, which are associated with the deployed capabilities, to the worker nodes in the Kubernetes cluster. The labels indicate to Kubernetes the various types of

workloads that can run on a specific host system. Based on the labels, Kubernetes then assigns pods to the nodes to provide functions, tasks, and services. Each pod belongs to a specific namespace in the OMT Management portal. On occasion, you might need to restart pods or reconfigure the environment by moving labels to different nodes, thus reassigning the workload of the pods.

> When using the OMT Management Portal, the label format is `<label name>:yes`. However, when using the kubectl command line the label format is `<label name>=yes`.

- "Adding Labels to Worker Nodes" below
  - "fusion:yes" on the next page
  - "intelligence:yes " on page 457
  - "intelligence-datanode:yes" on page 459
  - "intelligence-namenode:yes" on page 459
  - "intelligence-spark:yes" on page 459
  - "kafka:yes" on page 460
  - "th-platform:yes" on page 460
  - "th-processing:yes" on page 461
  - "zk:yes " on page 461
- "Understanding the Pods that Do Not Have Labels" on page 462
- "Understanding Pods that Run Master Nodes" on page 462

Adding Labels to Worker Nodes

Depending on the capabilities that you deploy, you must to assign certain a set of labels to the Worker Nodes. Each of the following sections defines the pods and their associated capabilities that get installed per assigned label.

To avoid issues caused by conflicting label assignments, review the following considerations.

- **Labeling for the Intelligence capability**
  - The HDFS NameNode, which corresponds with the `intelligence-namenode:yes` label, should run on one worker node only. The worker node must match the hostname or IP address that you provided in the **HDFS NameNode** field in the **OMT Management Portal** > **Configure/Deploy** page > **Intelligence**.
  - Assign the label for Spark2, `intelligence-spark:yes`, to the same worker nodes where you placed the `intelligence-datanode:yes` label.

- For Transformation Hub's Kafka and ZooKeeper, make sure that the number of the nodes you have labeled corresponds to the number of worker nodes in the Kafka cluster and the number of worker nodes running Zookeeper in the Kafka cluster properties from the pre-deployment configuration page. The default number is 3 for a Multiple Worker deployment.
- Although ESM Command Center, Recon, Intelligence, and SOAR all require Core, you do not need to assign the label for Core to more than one worker node.

fusion:yes

Core components include many of the core services needed for your deployed products, including the Dashboard and user management; all deployed capabilities require Core. Add the `fusion:yes` label to the Worker Nodes where you want to run the associated pods. For high availability, add this label to multiple worker nodes.

Pod	Description	Namespace	Associated Capability
esm-acc-web-app	Manages the user interface for ESM Command Center. The interface connects to an ESM Manager server running outside the Kubernetes cluster.	arcsight-installer	ESM Command Center
esm-web-app	Manages how ESM Command Center links to main navigation of the Platform user interface.	arcsight-installer	ESM Command Center
esm-widgets	Manages the dashboards and widgets that are designed to incorporate data from ESM. The widgets connect to an ESM Manager server running outside of the Kubernetes cluster. For example, when you start this pod, it installs the provided *How is my SOC running?* dashboard.	arcsight-installer	ESM Command Center
fusion-arcmc-web-app	Manages the user interface for ArcSight Management Center. A `fusion-arcmc-web-app:yes` label can optionally be applied to one or more worker nodes to control where this pod runs. Otherwise, it falls back to running on a node where the `fusion:yes` label is applied.	arcsight-installer	Core
fusion-common-doc-web-app	Provides the context-sensitive user guides for Core (the Platform), Recon, and Reporting.	arcsight-installer	Core
fusion-metadata-web-app	Manages the REST API for the metadata of the Dashboard feature.	arcsight-installer	Core
fusion-dashboard-web-app	Manages the framework, including the user interface, for the Dashboard feature.	arcsight-installer	Core

Pod	Description	Namespace	Associated Capability
fusion-db-monitoring-web-app	Manages the REST API for the database monitoring function.	arcsight-installer	Core
fusion-db-search-engine	Provides APIS to access data in the ArcSight Database. NOTE: This pod requires communication outside of the Kubernetes cluster.	arcsight-installer	Core
fusion-metadata-rethinkdb	Manages the RethinkDB database, which stores information about a user's preferences and configurations.	arcsight-installer	Core
fusion-single-sign-on	Manages the SSO service that enables users to log in to any of the deployed capabilities and the consoles for ArcSight Intelligence, SOAR, and ESM Command Center.	arcsight-installer	Core
fusion-ui-services	Manages the framework, including the user interface, for the primary navigation functions in the user interface.	arcsight-installer	Core
fusion-user-management	Manages the framework, including the user interface, for the user management function.	arcsight-installer	Core
interset-widgets	Manages the widgets that are designed to incorporate data from ArcSight Intelligence. The widgets connect to an Intelligence server running outside of the Kubernetes cluster.	arcsight-installer	Intelligence
layered-analytics-widgets	Manages and installs the widgets that can incorporate data from multiple capabilities. For example, the provided *Entity Priority* widget connects to ESM Command Center and Intelligence servers outside the Kubernetes cluster to display entity data.	arcsight-installer	Layered Analytics
recon-analytics	Manages the backend of Outlier Analytics; the user interface for Outlier Analytics is managed by the fusion-search-web-app pod.	arcsight-installer	Recon
fusion-search-web-app	Manages lookup lists, Data Quality Dashboard and Outlier UI capabilities. Also hosts the APIs used for search.	arcsight-installer	Core
fusion-reporting-web-app	Manages the REST API and user interface for the Reporting feature. NOTE: This pod requires communication outside of the Kubernetes cluster.	arcsight-installer	Core
fusion-search-and-storage-web-app	Manages the Search and Storage Groups and capabilities	arcsight-installer	Core

Pod	Description	Namespace	Associated Capability
fusion-db-adm-schema-mgmt	Manages installation, upgrade, and maintenance of the <tenant>_secops_adm schema and data	arcsight-installer	Core
fusion-arcsight-configuration-service	A secure, shared configuration repository for ArcSight capabilities	arcsight-installer	Core
soar-message-broker	Manages SOAR events	arcsight-installer	SOAR
soar-web-app	Manages SOAR backend services	arcsight-installer	SOAR
soar-db-init	Manages the SOAR DB schema lifecycle	arcsight-installer	SOAR
soar-jms-migration	Manages SOAR JMS migration	arcsight-installer	SOAR
soar-widgets	Manages SOAR widget deployment	arcsight-installer	SOAR
soar-frontend	Manages SOAR user interface services	arcsight-installer	SOAR
soar-gateway	Manages SOAR user requests	arcsight-installer	SOAR
th-enrichment-processor-group	Manages the instances that process events coming from the selected source topic (by default, th-arcsight-avro) by executing enrichment tasks , which include generating a Global ID. Events are then routed to the topic mf-event-avro-enriched. The default is 2 instances running Out-of-the-box.	arcsight-installer	Transformation Hub

intelligence:yes

Add the `intelligence:yes` label to Worker Nodes where you want to run the pods that manage functions and services for the ArcSight Intelligence capability. For high availability, add this label to multiple worker nodes.

Pod	Description	Namespace	Associated Capability
elasticsearch-data	Manages the Elasticsearch functions that store all raw events for Intereset Analytics and provide all data that drives the user interface.	arcsight-installer	Intelligence
elasticsearc-master	Manages the Elasticsearch services.	arcsight-installer	Intelligence

Pod	Description	Namespace	Associated Capability
h2	Stores user identities required to authenticate and authorize users.	arcsight-installer	Intelligence
interset-analytics	Determines the individual baselines , then discovers and ranks devisions from those baselines for the Intelligence Analytics feature. This pod requires communication outside of the Kubernetes cluster.	arcsight-installer	Intelligence
interset-api	Manages the REST API that the Intelligence user interface uses to gather the Intelligence Analytics results. This pod requires communication outside of the Kubernetes cluster.	arcsight-installer	Intelligence
interset-exports	Generates the PDF reports of organization risks and the users involved in risky behaviors.	arcsight-installer	Intelligence
interset-logstash	Manages Logstash, which collects raw events from Transofrmation Hub and sends them to Elasticsearch for indexing.	arcsight-installer	Intelligence
interset-spark-config-file-server	Hosts a file server to provide configuration files for Spark3 to consume.	arcsight-installer	Intelligence
interset-ui	Manages the user interface that displays the Intelligence Analytics results and the raw data in the Intelligence dashboard	arcsight-installer	Intelligence
intelligence-arcsightconnector-api	Manages APIs related to licensing support and provides Core menu registration for Intelligence.	arcsight-installer	Intelligence
intelligence-tuning-api	Manages APIs that tune the Intelligence Analytics metadata that can change the Intelligence Analytics results. This pod requires communication outside of the Kubernetes cluster.	arcsight-installer	Intelligence
intelligence-tenant-control	Manages tenant configurations and secrets for Intelligence.	arcsight-installer	Intelligence
searchmanager-api	Manages APIs that provide administrative tools related to Elasticsearch and the search capability in general.	arcsight-installer	Intelligence
searchmanager-engine	Manages jobs that provide administrative tools related to Elasticsearch and the search capability in general. This pod requires communication outside of the Kubernetes cluster.	arcsight-installer	Intelligence

intelligence-datanode:yes

Add the `intelligence-datanode:yes` label to Worker Nodes where you want to run the pods that manage HDFS services for the ArcSight Intelligence capability.

Pod	Description	Namespace	Associated Capability
hdfs-datanode	Manages how HDFS stores the results of Intelligence Analytics searches before transferring them to the ArcSight database. The HDFS Datanodes contain blocks of HDFS files.	arcsight-installer	Intelligence

intelligence-namenode:yes

Add the `intelligence-namenode:yes` label to a Worker Node for the HDFS NameNode.

Place this label on one worker node only. The worker node and the hostname or IP address in the **HDFS NameNode** field in the **Intelligence** tab of the **OMT Management Portal** must match.

Pod	Description	Namespace	Associated Capability
hdfs-namenode	Manages how the HDFS NameNode stores the location of all HDFS files distributed across the cluster.	arcsight-installer	Intelligence

intelligence-spark:yes

Add the `intelligence-spark:yes` label to Worker Nodes where you want to run the Analytics services for the ArcSight Intelligence capability. For high availability, add this label to multiple worker nodes. To reduce network traffic, add the label to the same worker nodes where you placed the `intelligence-datanode:yes` label.

Pod	Description	Namespace	Associated Capability
Spark2	Launches when users run the Intelligence Analytics feature. Spark2 generates multiple pods, changing the names of the pods according to the different phases of the analytics tasks.	arcsight-installer	Intelligence

kafka:yes

Add the `kafka:yes` label to Worker Nodes where you want to run the Kafka Broker functions and services for the Transformation Hub capability.

> Ensure that you assign this label to the same quantity of nodes that you specified for the `# of Kafka broker nodes in the Kafka cluster` setting in the **OMT Management Portal** > **Configure/Deploy** > **Transformation Hub** > **Kafka and Zookeeper Configuration**. The default number is 3.

Pod	Description	Namespace	Associated Capability
th-kafka	Manages the Kafka Broker, to which publishers and consumers connect so they can exchange messages over Kafka. NOTE: This pod requires communication outside of the Kubernetes cluster.	arcsight-installer	Transformation Hub

th-platform:yes

Add the `th-platform:yes` label to Worker Nodes where you want to run the Kafka Manager, schema registry, and WebServices for the Transformation Hub capability. For high availability, add this label to multiple worker nodes.

Pod	Description	Namespace	Associated Capability
th-kafka-manager	Provides the user interface that allows the Kafka Manager to manage the Kafka Brokers.	arcsight-installer	Transformation Hub
th-schemaregistry	Provides the scheme registry that is used for managing the schema of data in Avro format. NOTE: This pod requires communication outside of the Kubernetes cluster.	arcsight-installer	Transformation Hub
th-web-service	Manages the WebServices module of Transformation Hub. WebServices provides the API that ArcMC uses to retrieve data. NOTE: This pod requires communication outside of the Kubernetes cluster to receive client requests from and initiate connections to ArcMC.	arcsight-installer	Transformation Hub

th-processing:yes

Add the `th-processing:yes` label to Worker Nodes where you want to run services that manage processing for the Transformation Hub capability. For high availability, add this label to multiple worker nodes.

Pod	Description	Namespace	Associated Capability
th-c2av-processor	Manages the instances that convert CEF messages on the topic th-cef to Avro on the topic th-arcsight-avro. The quantity of instances depends on the number of partition in the th-cef topic and load. The default is 0 instances.	arcsight-installer	Transformation Hub
th-cth	Manages up to 50 instances of connectors in Transformation Hub that distribute the load of data received from collectors by creating a consumer group that is based on the source top and destination and topic names.	arcsight-installer	Transformation Hub
th-c2av-processor-esm	Manages the instances that convert CEF messages on the topic mf-event-cef-esm-filtered to Avro on the topic mf-event-avro-emsfiltered. The quantity of instances depends on the number of partition in the th-cef topic and load. The default is 0 instances.	arcsight-installer	Transformation Hub
th-routing-processor-group	Manages the routing rules for topics. Use ArcMC to configure the rules.	arcsight-installer	Transformation Hub

zk:yes

Add the `th-zookeeper:yes` label to Worker Nodes where you want to Kafka Zookeeper for the Transformation Hub capability.

Ensure that you assign this label to the same quantity of nodes that you specified for the `# of Zookeeper nodes in the Zookeper cluster` setting in the **OMT Management Portal** > **Configure/Deploy** > **Transformation Hub** > **Kafka and Zookeeper Configuration**. The default number is 3.

Pod	Description	Namespace	Associated Capability
th-zookeeper	Manages Kafka Zookeeper, which stores metadata about partitions and brokers.	arcsight-installer	Transformation Hub

Understanding the Pods that Do Not Have Labels

The Platform includes several pods that are not associated with a deployed capability and thus do not require a label. The installation process automatically creates these pods.

Pod	Description	Namespace
autopass-lm	Manages the Autopass service, which tracks license keys.	arcsight-installer
itom-pg-backup	Performs backup of the PostgreSQL database.	arcsight-installer
suite-reconf-pod-arcsight-intaller	Manages the Reconfiguration features in the OMT Management Portal.	arcsight-installer

Understanding Pods that Run Master Nodes

The Platform includes pods that run master nodes.

Pod	Description	Namespace
itom-postgresql-default	Manages the PostgreSQL database, which stores information for SOAR, ArcMC, OMT status, and license keys.	
idm	Manages user authentication and authorization for the OMT Management Portal.	core
nginx-ingress-controller	Provides the proxy web server that end-users need to connect to the deployed capabilities. By default, server uses HTTPS and port 443. NOTE: This pod requires communication outside of the Kubernetes cluster.	arcsight-installer

Managing OMT Logs

OMT uses Fluentd to collect and gather logs for OMT system components, containers, and Kubernetes. After collection, OMT exports the logs to a remote destination that you configure before OMT installation.

This section contains the following topics:

- About OMT Logs
- Log Retention
- Log Rotation and Deletion
- Changing the Log Rotation or Deletion
- Additional ConfigMap Parameters
- Configuring the Automatic Log Cleanup Settings
- Configuring the System Log Settings
- Installation Logs
- Log Rotation of Docker Services
- Log and Trace Model
- Accessing Pod Logs

About OMT Logs

The OMT logs consist of the following:

- **Container logs:** Logs for all Kubernetes workloads.
- **System logs:** Logs for the journal, including logs from `kubelet.service`.
- **Application logs:** Logs for all applications. The applications must write their logs to a shared volume, which is mounted to the `itom-logging-vol` persistent volume.

A Kubernetes Daemon Set fluentd pod runs as an instance of the Fluentd collector and forwarder on each node. Each Fluentd pod gets its configuration from fluentd in the ConfigMap. By default, Fluentd collects local log files and saves them to the `itom-logging-vol` persistent volume.

Log Retention

By default, OMT retains logs (both on the cluster nodes and on the `itom-logging-vol` persistent volume) for two days. To change the log retention, follow these steps:

1. Set an environment variable to define whether you will change the log retention on the cluster nodes or on the itom-logging-vol persistent volume. To do this, run one of the following commands:

- To configure the retention of logs on cluster nodes:

```
cm_name=logrotate-node-level
```

- To configure the retention of logs on the itom-logging-vol persistent volume:

```
cm_name=itom-logrotate
```

2. Run the following command to set the log retention period:

```
kubectl patch cm ${cm_name} -n core -p "{\"data\":
{\"logrotate.properties\":$(kubectl get cm ${cm_name} -n core -o json | jq
'.data."logrotate.properties"' | sed -e 's/-mtime +[0-9]\{1,\}/-mtime
+<retention_days>/')}}"
```

where `<retention_days>` is the number of days for which you want to retain logs. For example, to retain logs for 10 days, run the following command:

```
kubectl patch cm ${cm_name} -n core -p "{\"data\":
{\"logrotate.properties\":$(kubectl get cm ${cm_name} -n core -o json | jq
'.data."logrotate.properties"' | sed -e 's/-mtime +[0-9]\{1,\}/-mtime
+10/')}}"
```

Log Rotation and Deletion

Logs are either rotated or deleted, depending on the logging mechanism of the components. Files in directories which are defined by OMT will be deleted after a certain period according to the log retention configuration. These files and directories include:

- `$<CDF_HOME>/log`
- Directories that are mounted to the `itom-logging` persistent volume

> Configurations listed below prefixed by “SCRIPT_DELETE_*” control the log deletion strategy of the above directories.

Run the following commands to determine the NFS server and NFS path to which the itom-logging persistent volume is mounted:

```
kubectl get pv itom-logging -o json|$<CDF_HOME>/bin/jq -r '.spec.nfs.server'
kubectl get pv itom-logging -o json|$<CDF_HOME>/bin/jq -r '.spec.nfs.path'
```

Some system log files in the `/var/log/` directory will be rotated after a certain period according to the log rotation configuration. By default, OMT only rotates the `/var/log/messages` log file.

> The configurations that start with “SYSLOG_*” listed below controls the log-rotation strategy of the `/var/log` directories.

Changing the Log Rotation or Deletion

The log rotate configurations are specified in the `itom-logrotate` ConfigMap file for the logs stored under the `itom-logging-vol` persistent volume and in the `logrotate-node-level`

ConfigMap for the logs stored locally on each of the cluster nodes.

> Before proceeding, please verify that you are able to access the logs stored on the `itom-logging-vol` persistent volume from within the `itom-logrotate-deployment` pod. To do this, run the following command:
> `kubectl exec -n core itom-logrotate-deployment-xxxxxxxxx-yyyyy -- ls -altrh /cdf-log-location/container`
> Make sure to use the correct pod name. The command returns the contents of `itom-logging-vol` volume's container directory. Select any log not necessary for retention and try removing it, for example:
> `kubectl exec -n core itom-logrotate-deployment-xxxxxxxxx-yyyyy -- rm -f /cdf-log-location/container/coredns-xxxx_kube-system_coredns-973f75a8ff12f74f128b7749d608d73d2b92a4dc4abcb1ab3edb3c32d9e67910.log.20221001.log`
> Repeat the first command to list the container directory contents again and verify that the the log file is gone. If it is still present or the first command failed, verify your permissions and ownership of the files. Alternatively, you can setup a cronjob which will change permissions and ownership before logrotation runs.

To change the log rotation or deletion:

1. Set an environment variable to define whether you will change the log retention on the cluster nodes or on the itom-logging-vol persistent volume. To do this, run one of the following commands:

- To configure the retention of logs on cluster nodes:

```
cm_name=logrotate-node-level
```

- To configure the retention of logs on the `itom-logging-vol` persistent volume:

```
cm_name=itom-logrotate
```

2. Run the following command to change the default log rotate configuration:

```
kubectl edit cm ${cm_name} -n core
```

The new log rotate configuration takes effect automatically in about 2 minutes.

Additional ConfigMap Parameters

Some of the parameters listed below may not exist in the `itom-logrotate` and `logrotate-node-level` ConfigMaps. However, you can add them to the ConfigMaps to configure some log rotate functions. Below are the details for the parameters in the `itom-logrotate` and `logrotate-node-level` ConfigMap instances:

Parameter	Description
SCRIPT_DELETE_INSTALL_UPGRADE	Delete the logs files of OMT install and upgrade. By default, this parameter is set to `false`. That means the log files of OMT install and upgrade will be retained. OpenText suggests that you use the default value for this parameter because these log files require little space and are useful for your troubleshooting.
SCRIPT_DELETE_LOG_SURVIVAL	Files will be removed if it meets the configured rule. For example, `-mtime +2` means logs will be removed that last for more than 2 days. `-size +51200k` means logs will be removed whose size is larger than 51200 KB. For format, refer to Linux command `find`.

SCRIPT_DELETE_CRONINTERVAL	The interval of file check for delete. The supported formats: `@hourly, @daily, @weekly, @monthly @yearly`, or in the cron job format: `0 0 * * * *`. A brief explanation of the format is shown here.
	`# ┌──────────── second (0 - 59)`
	`# | ┌──────────── minute (0 - 59)`
	`# | | ┌──────────── hour (0 - 23)`
	`# | | | ┌──────────── day of the month (1 - 31)`
	`# | | | | ┌──────────── month (1 - 12)`
	`# | | | | | ┌──────────── day of the week (0 - 6) (Sunday to Saturday; 7 is also Sunday on some systems)`
	`# | | | | | |`
	`# | | | | | |`
	`# | | | | | |`
	`# * * * * * * command to execute`
	Refer to https://godoc.org/github.com/robfig/cron for more details.

SCRIPT_DELETE_FILE_ENDINGS	The file with specified endings will be deleted immediately on each checking for delete. For example, `txt tmp` means every log file named `*.txt` or `*.tmp` will be deleted, no matter if they meet the configured `SCRIPT_DELETE_LOG_SURVIVAL` rule or not.
SYSLOG_ROTATE_FILES	Files that need to be rotated under `/var/log`. Each file name must be separated by a white-space character. Default value: `messages`.
SYSLOG_ROTATE_INTERVAL	The rotate interval of the system log files. Supported values: `every hourly, daily, weekly, monthly, yearly`. Default value: `daily`.
SYSLOG_MAX_SIZE_OF_FILE	Log files are rotated when the files are larger than the specified size, or before the system logs are rotated within the specified time interval. Default value: `500M`
SYSLOG_MAX_ROTATE_OF_FILE	The log rotated time before the files are being removed. Value must be 0 or 1. 0: old versions are removed rather than rotated. 1: (default) old versions are rotated.
SYSLOG_ROTATE_MODE	The rotate mode of the log file. Default value: `copytruncate`
SYSLOG_ROTATE_PARAMETERS	The `logrotate` command line parameters. Supported values: `v`: Verbose. `d`: Debug (Logrotate will be emulated but never executed). `f`: Force.

Parameter	Description
SYSLOG_MIN_SIZE_OF_FILE	The minimum size of log files to be rotated.
SYSLOG_ROTATE_DATEFORMAT	Specify the date text extension for rotated logs using the notation similar to `strftime` function. Only `%Y` `%m` `%d` `%H` and `%s` specifiers are allowed. The default value is `-%Y%m%d` except hourly, which uses `-%Y%m%d%H` as its default value.
SYSLOG_ROTATE_MAXAGE	The maximum time for the logs to be removed. This parameter is only checked if the log file is about to be rotated.
SYSLOG_ROTATE_COMPRESS	Compress rotated log files using gzip. The supported values are: `compress` and `nocompress` (default value).

Configuring the Automatic Log Cleanup Settings

The log automatic log cleanup settings are specified by the following parameters in the itom-logrotate ConfigMap file on the itom-logging-vol persistent volume and in the logrotate-node-level ConfigMap on cluster nodes.
SCRIPT_DELETE_FILE_ENDINGS
SCRIPT_DELETE_INSTALL_UPGRADE
SCRIPT_DELETE_LOG_SURVIVAL
SCRIPT_DELETE_CRONINTERVAL

To configure the automatic log cleanup settings, follow these steps:

1. Set an environment variable to define whether you will change the log retention on the cluster nodes or on the itom-logging-vol persistent volume. To do this, run one of the following commands:

- To configure the retention of logs on cluster nodes:

```
cm_name=logrotate-node-level
```

To configure the retention of logs on the itom-logging-vol persistent volume:

```
cm_name=itom-logrotate
```

2. Run the following command to configure the parameter settings:

```
kubectl edit cm ${cm_name} -n core
```

Below is an example of the parameter settings in the itom-logrotate and logrotate-node-level ConfigMaps:

```
SCRIPT_DELETE_FILE_ENDINGS=""
SCRIPT_DELETE_INSTALL_UPGRADE="false"
SCRIPT_DELETE_LOG_SURVIVAL="-mtime +2"
SCRIPT_DELETE_CRONINTERVAL="@daily"
```

Configuring the System Log Settings

You can configure the log settings of the `/var/log/` system log directory by using the following parameters in the `itom-logrotate` and `logrotate-node-level` ConfigMaps:

```
SYSLOG_ROTATE_FILES
SYSLOG_ROTATE_INTERVAL
SYSLOG_MAX_SIZE_OF_FILE
SYSLOG_MAX_ROTATE_OF_FILE
SYSLOG_ROTATE_MODE
SYSLOG_ROTATE_PARAMETERS
SYSLOG_MIN_SIZE_OF_FILE
SYSLOG_ROTATE_DATEFORMAT
SYSLOG_ROTATE_MAXAGE
SYSLOG_ROTATE_COMPRESS
```

The following is an example of the parameter settings in the `itom-logrotate` and `logrotate-node-level` ConfigMaps:

```
SYSLOG_ROTATE_FILES="messages"
SYSLOG_ROTATE_INTERVAL="daily"
SYSLOG_MAX_SIZE_OF_FILE="500M"
SYSLOG_MAX_ROTATE_OF_FILE=1
SYSLOG_ROTATE_MODE="copytruncate"
SYSLOG_ROTATE_PARAMETERS="v"
SYSLOG_MIN_SIZE_OF_FILE="1M"
SYSLOG_ROTATE_DATEFORMAT="-%Y%m%d%H"
SYSLOG_ROTATE_MAXAGE=7
SYSLOG_ROTATE_COMPRESS="nocompress"
```

Installation Log Locations

During OMT installation, all the installation logs are located under the `$TMP_FOLDER`. When the installation is complete, the installation logs are under `$<CDF_HOME>/log/scripts/install`. Otherwise, the logs are under `$TMP_FOLDER`. An example of an installation log filename: `install-20200316234235.log`.

For an `arcsight-install` installation, all the installation logs are located under the `$TMP_FOLDER`. When a silent installation is complete, the logs are located under `$<CDF_HOME>/log/scripts/install` (for OMT installation) and `$<CDF_HOME>/log/scripts/silent-install` (for ArcSight Suite installation and node extension). An example of the silent installation log filename would be: `silent-install-20200317104001.log`. Otherwise, the logs are located under the `$TMP_FOLDER`.

Log and Trace Model

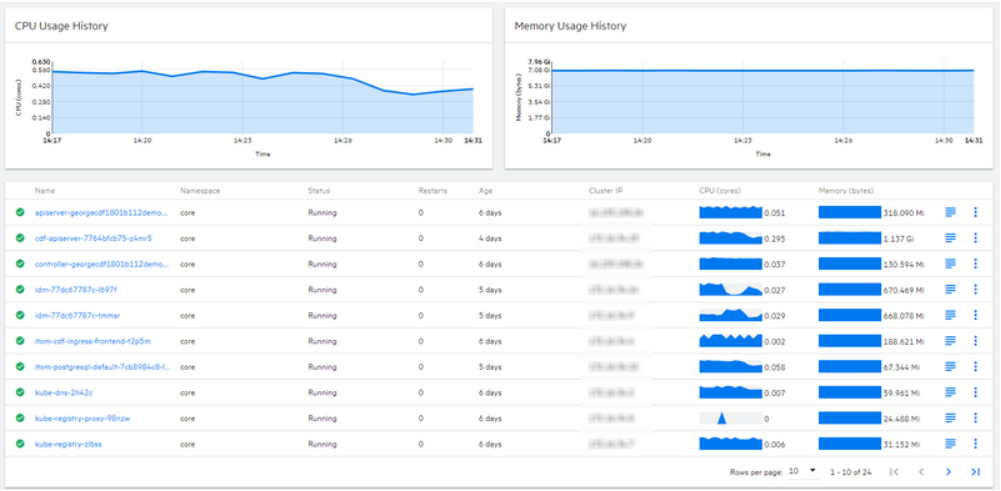
The following is recommended for the log and trace model.

- Pay attention to the log level, and don't unnecessarily enable tracing or debug parameters.
- Pay attention to log rotation and switching.

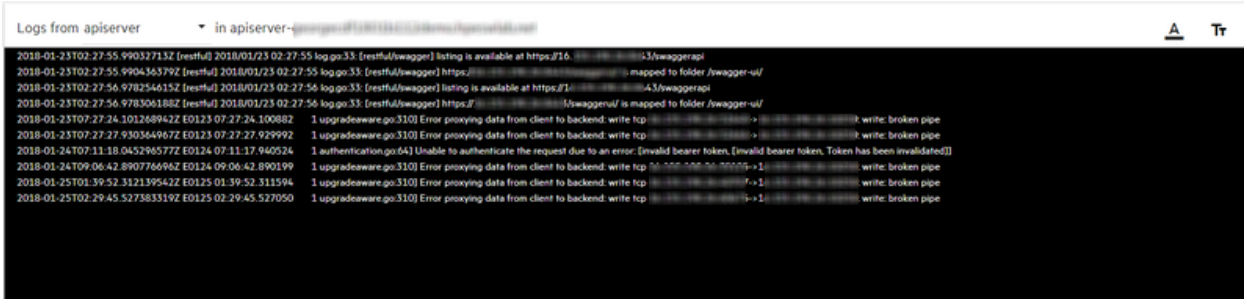
Accessing Pod Logs

To access the log for a particular pod, do the following:

1. In the OMT Management Portal, click **CLUSTER > Dashboard > Workloads > Pods**.
2. In the list of pods, click the pod for which you wish to view logs.



3. In the Pod area, click **View logs**. A page that resembles the following is displayed:



All suite logs are stored within a persistent volume, so that logs will persist even if the pods go down.

Configuring Log Levels

You can configure the log level as desired for troubleshooting purposes.

To change the log level:

1. Browse to the management portal at https://<virtual_FQDN>:5443, or at https://<master_node1_FQDN>:5443.
2. Click **DEPLOYMENT**, and select **Deployments.**
3. Click the **Three Dots** (Browse) on the far right and choose **Reconfigure**. A new screen will be opened in a separate tab.
4. Under the appropriate capability tabs there are log level configuration options for each component. Select the appropriate value to update the Log Levels. The change goes into effect automatically.

Uninstalling and Reinstalling the Platform

This section describes Platform uninstall and reinstall activities in your environment.

Undeploying a Capability

It's possible that you might want to undeploy, or remove, one or more capabilities without uninstalling the ArcSight Platform. For example, you might want to remove Intelligence to resolve an issue with its environment. You can redeploy the capability later.

Prior to undeploying the Core components, you should back up the Core secrets for later restoration. For more information, see "FBacking Up and Restoring Core Secrets" on page 718.

1. To remove the capabilities that you want to undeploy, complete the following steps:
   a. Log in to the OMT Management Portal.
   b. Navigate to **Deployment** > **Deployments**.
   c. In the menu, select **Change**.
   d. Uncheck the capabilities you want to remove.

   > Be aware that most capabilities require Core and Transformation Hub. Thus, if you remove these two capabilities, the capabilities that depend on them cannot function appropriately.

> You must back up Core secrets before you attempt to undeploy and redeploy Core; restore backed up Core secrets after too.

e. Click **Next**, and then follow the wizard to complete the process (continue clicking **Next**).

2. (Conditional) If you have unchecked Intelligence and if you do not need to retain data related to it, do the following:
   a. On every worker node, delete the contents present in *<k8s path>/k8s-hostpath-volume/interset*.
   b. On the NFS server, delete the contents present in *<NFS_root_DIRECTORY>/arcsight-volume/interset*.
3. To check that all pods are in Running status, run the following command:

```
kubectl get pods --all-namespaces
```

Uninstalling Installed Products and OMT from AWS

You have several options for uninstalling OMT and your installed products from AWS. Each of these options is explained in detail below.

- You can uninstall any or all installed products.
- In addition to uninstalling installed products, you can also uninstall OMT but leave your cluster resources in place. Perform this option if you plan to re-use the cluster and re-install OMT later.
- You can uninstall products and OMT as above, and then destroy all resources created during platform setup. Only perform this option when the cluster is no longer needed.

To uninstall OMT from your AWS installation:

1. On the bastion and all worker nodes:
   a. Execute the uninstall command from `/opt/cdf`:

```
# ./uninstall.sh
```

   b. (Conditional) If not already, manually delete the `/opt/cdf` directory.
2. On the bastion, uninstall the ArcSight Database:
   a. Execute the uninstall command from `/opt/arcsight-db-tools`:

```
./db_installer uninstall
```

3. On each ArcSight Database node:

a. Execute the following command to remove the `/opt/arcsight-db-tools` directory as follows:

```
# rm -rf /opt/arcsight-db-tools
```

b. (Conditional) Execute the following command to remove `.ssh/` directory from `/root`:

```
# rm -rf /root/.ssh/
```

You can now proceed to uninstall your installed products.

To uninstall installed products:

If you are also uninstalling OMT, then prior to uninstalling your products, perform the uninstallation of OMT first , and then return here to proceed with uninstalling your products.

1. Log in to the bastion and become `root`.
2. Get the names of all namespaces by running the command:
   `kubectl get namespaces`

For example:

```
kubectl get namespaces
```

```
NAME                        STATUS   AGE
```

```
arcsight-installer-blk62   Active   41m
```

```
core                        Active   48m
```

```
default                     Active   84m
```

```
kube-public                 Active   84m
```

```
kube-system                 Active   84m
```

3. Delete the product namespaces you wish to delete, and the core namespace by running the command:
   `kubectl delete namespace <namespace name>`

For example:

```
kubectl delete namespace arcsight-installer-blk62
```

```
namespace "arcsight-installer-blk62" deleted
```

```
kubectl delete namespace core
```

```
namespace "core" deleted
```

Your own product namespace will have the name format `arcsight-installer-XXXXX`.

4. Wait for the selected namespaces to be deleted before continuing.
5. Get the names of all PVs (persistent volumes) by running the command:
   `kubectl get pv`

For example:

```
kubectl get pv
```

```
NAME                                        CAPACITY   ACCESS MODES   RECLAIM
POLICY   STATUS
```

```
arcsight-installer-blk62-arcsight-volume   30Gi       RWX            Retain
        Released
```

```
arcsight-installer-blk62-db-backup-vol     1Mi        RWX            Retain
        Released
```

```
db-single                                  10Gi       RWX            Retain
        Released
```

```
itom-logging                               1Mi        RWX            Retain
        Released
```

```
itom-vol                                   5Gi        RWX            Retain
        Released
```

6. Delete all PVs by running the following command for each PV:
   `kubectl delete pv <PV_name>`

```
kubectl delete pv arcsight-installer-blk62-arcsight-volume
```

```
persistentvolume "arcsight-installer-blk62-arcsight-volume" deleted
```

```
kubectl delete pv arcsight-installer-blk62-db-backup-vol
```

```
persistentvolume "arcsight-installer-blk62-db-backup-vol" deleted
```

```
kubectl delete pv db-single
```

```
persistentvolume "db-single" deleted
```

```
kubectl delete pv itom-logging
```

```
persistentvolume "itom-logging" deleted
```

```
kubectl delete pv itom-vol
```

```
persistentvolume "itom-vol" deleted
```

7. Clear the data from your NFS volumes by connecting with SSH and clearing (but **not** deleting) all exported directories.

> If you deleted the SSH inbound rule, you will need to add it again to be able to SSH to your NFS.

Disposal of Cluster Resources

The procedures detailed above will leave your cluster resources intact. OMT and applications can be re-installed again on the cluster, either now or in the future, without having to re-create these resources.

If instead the cluster is no longer needed, you can safely destroy all resources created earlier for OMT and your installed applications. Consult the AWS documentation for details on how to destroy resources.

> If you installed the ArcSight Platform 23.1 (or later) Database, then delete the files at the communal location manually to completely uninstall the Database.

Reinstalling the Platform

If you uninstalled the Platform and plan to reinstall it in the same cluster along with the deployed capabilities, perform the following steps before reinstalling Platform and Intelligence:

1. Launch a terminal session and as a root user, log in to the node where NFS is present.
2. Delete the NFS directory:

   ```
   rm -rf /opt/arcsight-nfs
   ```

3. Launch a terminal session and then log in to the node where the Kubernetes hostpath is present.
4. Navigate to the following directory:

   ```
   cd /opt/arcsight/
   ```

5. Delete the following directory:

```
rm -rf k8s-hostpath-volume
```

6. Repeat Step 4 and Step 5 on all OMT worker nodes.
7. Launch a terminal session and then log in to a database node.
8. Navigate to the following directory:

```
cd /[database_install_directory]/
```

9. Stop the Kafka Scheduler:

```
./kafka_scheduler stop
```

10. (Conditional) If you have the ArcSight database installed), complete the following steps as a dbadmin user:
    a. Execute the following command and specify your dbadmin password:

    ```
    /opt/vertica/bin/vsql
    Password:<password>
    ```

    b. Execute the following command to delete the data in the default_secops_adm.events table:

    ```
    DELETE FROM default_secops_adm.events;
    ```

    c. Execute the following command to delete the default_secops_intelligence schema:

    ```
    drop schema default_secops_intelligence cascade;
    ```

11. Continue with reinstalling the Platform and deploying the capabilities. Complete one of the following actions:
    a. Deploy the capabilities manually. For more information, see Performing a Manual Deployment.
    b. Deploy the capabilities by using the ArcSight Platform Installer.

Using REST APIs

To start using ArcSight REST APIs, you must set up access, authenticate, and call the REST endpoints. To do this, you must configure a Client ID and Secret to authenticate with the REST APIs. After establishing a secret, you can update it according to your password rotation policies.

Note: If you update the secret, you must update all REST API clients to reflect the change.

- Setting up Access to REST APIs
- Authenticating to and Calling the REST API
- Links to REST API Documentation

Setting up Access to REST APIs

To start using ArcSight REST APIs, you must set up access, authenticate, and call the REST endpoints. To do this, you must configure a Client ID and Secret to authenticate with the REST APIs. After establishing a secret, you can update it according to your password rotation policies. Follow the procedures for the types of endpoints in your environment.

- **For endpoints other than SOAR**
- **For SOAR Endpoints**

Setting up Access for endpoints other than SOAR

You can use OpenSSL to generate a random Client ID and Secret values that are more secure.

1. Enter the following command to generate Client ID:

```
openssl rand -hex 16
```

2. Enter the following command to generate Client Secret:

```
openssl rand -hex 32
```

3. Log in to the OMT Management Portal.
4. Click the browse icon on the far right, then select **Reconfigure**.
5. In the **Single Sign-on Configuration** section, specify values for **Client ID** and **Client Secret**.
6. Click **Save.**

Setting up Access for SOAR Endpoints

To generate a Client ID and Secret for SOAR endpoints, complete the following procedure:

1. Log in to ArcSight as an admin user.
2. Navigate to **RESPOND** > **Configuration** > **REST Clients**.
3. Click the **Create REST Client** button to create a new REST Client.
4. In the **REST Client Editor** window, specify details for the following fields, then click **Save.**

Value	Description
Client ID	This value will be automatically generated.
Description	Specify the description of the REST client.

A client secret is generated for the REST client. Note down the REST client secret along with the credentials as you will be asked to specify this detail whenever you call the SOAR application using the REST API.

> If you lose the Client ID and Client Secret that you created for the REST client, then you cannot call the SOAR application using the respective REST API. In such cases, you must create the REST Client credentials along with the Client Secret again.

Authenticating to and Calling REST APIs

Follow the procedures for the types of endpoints in your environment

- **For Endpoints Other than SOAR**
- **For SOAR Endpoints**

For Endpoints Other than SOAR

To authenticate and call endpoints other than SOAR, you must generate access tokens, session tokens and refresh tokens. The REST API client uses these tokens when you call the REST API server.

To generate access and refresh tokens and access the REST API, complete the following procedure:

1. Generate the access token in your API client:
   a. Use the following URL with POST method:

      ```
      https://<OMT_masternode_hostname or virtual_ip
      hostname>/osp/a/default/auth/oauth2/grant
      ```

      where <OMT_masternode_hostname or virtual_ip hostname> represents your ArcSight product.

   b. Select and specify the *Header* and *Body* information as follows:

      Authorization

      - Authorization type as **OAuth2**
      - Client_ID:Client_Secret as **base64 encoded**

      Header

- Content-Type as **application/x-www-form-urlencoded**
- Accept as **application/json**

Body

- Enter **grant_type** as OMT password
- Enter **Username** as OMT User ID
- Enter **password** as the password of the UserID

For example:

```
curl -k --location --request POST 'https://<OMT_masternode_hostname or
virtual_ip hostname>/osp/a/default/auth/oauth2/grant' \
--header 'Accept: application/json' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic
MDM0YzE2MzU1N2I0OTUxOWE5ZjRlYjVlNDBkOGJiZGQ6ZGEzMzA2NzBiMGQ0YWIzN2JjOG
RhMzgyNDBiMjM2NzVlZDVkMjUwNTBkNzIzZmNjNDhmNDUxNGJjYzY0NTUwZA==' \
--data-urlencode 'grant_type=password' \
--data-urlencode 'username=*****' \
--data-urlencode 'password=*****'
```

> The server replies with the access_token, the expires_in number of seconds for the access_token validity, and a refresh_token to generate a new access token when the access token expires. To understand how to generate a new access token using the refresh_token, see Refresh Access Tokens

2. Generate a session token using the access token in your API client:
   a. Use the following URL with GET method:

   ```
   https://<OMT_masternode_hostname or virtual_ip
   hostname>/mgmt/users/me/details
   ```

   For example:

   ```
   https://<OMT_masternode_hostname or virtual_ip
   hostname>/mgmt/api/users/me/details
   ```

   b. Select and specify the Header and Body information as follows:

   Authorization

   - Authorization type as **OAuth2**
   - Specify the Access token generated in step 1

   For example:

```
curl -k -v --location --request GET 'https://<OMT_masternode_hostname
or virtual_ip hostname>/mgmt/users/me/details'\
--header 'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZ
SI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36P
Ok6yJV_adQssw5c'
```

To review the documentation for REST API endpoints, see Links to REST API Documentation

3. Access your REST API endpoint with the session token generated in step 2 as a cookie.

   For example, to search all the dashboards owned by the logged in user ID, and the dashboards that are being shared with the logged in user ID's role, you might use the following content:

```
curl -k --location --request GET '<OMT_masternode_hostname or virtual_ip
hostname>/metadata/api/v1/dashboards'\
--header 'Cookie: SESSIONTOKEN=1E4C45F0B8DC821FF251EC17558B1ABF'
```

4. (Optional) Generate the access token again with the refresh token in your API client:

   a. Use the following URL with POST method:

```
https://<OMT_masternode_hostname or virtual_ip
hostname>/osp/a/default/auth/oauth2/token
```

   b. Select and specify Header and Body information as follows, where:

      Authorization

      - Authorization type as **OAuth2**
      - Client_ID:Client_Secret as **base64 encoded**

      Header

      - Content-Type as **application/x-www-form-urlencoded**
      - Accept as application/json
      - Authorization type as OAuth2

      Body

      - Set **grant_type** as **refresh_token**
      - Set **refresh_token** as generated in step 1

      For example:

```
curl -k --location --request POST 'https://<OMT_masternode_hostname or
virtual_ip hostname>/osp/a/default/auth/oauth2/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
```

```
--header 'Accept: application/json' \
--header 'Authorization: OAuth2 Q2xpZW50SWQ6Q2xpZW50U2VjcmV0' \
--data-urlencode 'grant_type=refresh_token' \
--data-urlencode 'refresh_token=IWmk3ugO-KI-XlM16EXSS0WJKBeN08pGh3o'
```

For SOAR Endpoints:

ArcSight SOAR requires specific REST client credentials to start using SOAR REST APIs.

Before calling the SOAR REST API, make sure you have access to the ArcSight SOAR REST API details (Swagger) page, where you can find all available endpoints and parameter details.

To call the SOAR REST API, complete the following procedure:

1. Navigate to the following URL:

   https://<OMT_masternode_hostname or virtual_IP hostname>/soar-api/api/v1/rest-api-docs

2. Specify the following REST client definitions:

   Username: Enter the Client ID

   Password: Enter the Client Secret

3. Click **Sign in**.

4. To familiarize yourself with the REST API, use the following URL to access the SOAR REST API details (Swagger) page:

   https://<OMT_masternode_hostname or virtual_IP hostname>/soar-api/api/v1/openapi.yaml

   You can access functionalities such as creating scope items, updating cases, creating cases with or without scope items, creating case comments and creating case comment attachments.

5. The following is a sample curl request to create a SOAR case:

   > The Authorization request header contains the Base64-encoded username/client id and password/client secret, separated by a colon. When handling the request, the server decodes the login details and checks if the user can access the requested content.

```
curl -k -v 'https://<OMT_masternode_hostname or virtual_ip
hostname>/soar-api/api/v1/case' \
-H 'authorization: Basic
ODI5ODE4NjctODA1NC00M2YxLWE2MTQtNzgzNTUyMzg1NGUwOmY7Si9Tc1xCZlZFP0FCUS5bd
EJ5cmQ3aUZjNy9eV04w' \
-H 'accept: application/json' \
-H 'content-type: application/json' \
```

```
--data-raw '{"external_id":"54","rulename":"Action
failed","subject":"Example subject","description":"Example
description","creation_
time":1647441423000,"severity":"Urgent","scopeItems":
[{"role":"RELATED","value":"example@example.com","category":"EMAIL_
ADDRESS"}]}' \
```

Links to REST API Documentation

Unless otherwise specified, the following REST API Documentation below can be accessed by any user who is authenticated and authorized to access the system:

Name	REST API Endpoint Documentation
ArcMC and Core ArcMC	`https://<master_FQDN or IP>/arcmc/rest-api-docs`
ArcSight Configuration Service (ACS)	`https://<master_FQDN or IP>/acs/rest-api-docs`
Database Monitoring	`https://<master_FQDN or IP>/db-mon/rest-api-docs`
ESM	`https://<master_FQDN or IP>/detect-api`
Intelligence	Developer's Guide to ArcSight Intelligence 24.2
Search	`https://<master_FQDN or IP>/re/rest-api-docs`
Event integrity, scheduled search	`https://<master_FQDN or IP>/rec/rest-api-docs`
System Metadata	`https://<master_FQDN or IP>/metadata/rest-api-docs`
SOAR **Note**: Accessing this document requires SOAR specific REST Client credentials.	`https://<master_FQDN or IP>/soar-api/api/v1/rest-api-docs`

Retrieving the OMT Root CA

You can retrieve the OMT root CA from a supported web browser or by using the command line.

Retrieving the OMT Root CA from a Browser

This procedure assumes you are using Google Chrome.

1. Specify the following URL in the browser:

```
https://<master_node_FQDN>:5443
```

2. Click the icon next to the left of the URL, and then click **Certificate**.
3. Click **Certification Path**.
4. Double-click the CA certificate. A pop-up window displays.
   a. In the pop-up window, click **Details**, and then click **Copy to File...**.
   b. Click **Next**.
   c. Select **Base-64 encoded X.509 (.CER)** and click **Next**.
   d. Specify a file name (for example, ca.cer) and click **Next**.
   e. Click **Finish** and close the pop-up window.
5. (Conditional) If you have multiple CA certificates, repeat Step 4 for each CA certificate in the certificate chain.

Retrieving the OMT Root CA Using Command Line

1. Log in to the initial master node of the cluster.
2. Execute the following command to retrieve the OMT CA certificate:

```
${CDF_HOME}/scripts/cdf-updateRE.sh read > ca.cer
```

Understanding License Keys

ArcSight Platform products ship with an evaluation license, which you can change to a valid license during or after installation. Many ArcSight Platform features are common across your deployed products, but some features might be restricted to a specific license or limited in scope depending on your license.

- "Understanding the Types of Licenses" on the next page
- "How Your License Affects Available Features" on page 485
- "How Your License Affects Data Storage Policies" on page 487
- "How Data Ingestion Affects Your License" on page 488

Considerations for Product Licensing

- If you use an evaluation license, ensure that you apply your product license **before** the license expires to avoid disruption to event flow and functionality.

- Your Intelligence license is based on the number of users that you want Intelligence to run analytics on. The license policy is violated when the number of users exceeds the maximum limit. Renew your license before its validity expires or if the license policy has been violated.
- For a Transformation Hub license, you can use a legacy ArcMC ADP license key or a more recent Transformation Hub license.
- If you install multiple term or permanent licenses for a product or function, the expiration date matches the date for the license that expires first.
- When used with an ArcSight product that requires the ArcSight Database, the storage capacity for the ArcSight Database is license limited to 976 PB. If your ArcSight Database storage utilization exceeds 976 PB, contact technical support for assistance.
- Starting 30 days before a license expires, ArcSight Platform displays a warning about the coming expiration date. However, if your deployment includes an MSSP license, the system does not display this warning.
- Several product licenses include the use of common features, such as Search or Reporting. In general, when you have deployed multiple products, you only need one valid license for the feature to function.
- Your product license might affect the maximum value that you can set for the data retention policy. For example, with a Recon license you can configure stored data to never expire.
- If the calculated MMEPS value exceeds your licensed events per second (EPS) capacity, ArcSight Platform displays a warning until the data ingestion rate normalizes. For example, the warning might display when data ingestion into the ArcSight Database is higher than your licensed EPS.
- When a license expires or is missing, ArcSight Platform redirects users to an invalid license page and disables the functionality associated with the license. To resolve this issue, you can install a valid license or troubleshoot licensing issues.
- You can check the status of an installed license.

Understanding the Types of Licenses

ArcSight products allow a short evaluation period before requiring a long-term license. Your products could have the following types of licenses:

- 90-day Instant-on License for Evaluation
- Long-term Licenses

- MSSP License

90-day Instant-on License for Evaluation

ArcSight products ship with an **instant-on** evaluation license, which enables functionality for 90 days after you install the product. To continue using the product for a longer term, you must install a valid license key. Installing a term or permanent license will override the instant-on license.

> To ensure continuity of functionality and event flow, apply your valid product license **before** the evaluation license has expired.

Long-term Licenses

Most valid product licenses cover a specific period of time (a **term** license) or are a permanent license. If you install multiple term or permanent licenses for a product or function, the expiration date matches the date for the license that expires last.

MSSP License

An MSSP license grants you access to all functions and features available in the Intelligence and Recon capabilities, regardless of the non-MSSP licenses that you might also have installed.

You can purchase an MSSP license, a non-MSSP license, or both to meet your requirements. If you have both licenses, the system responds in the following ways upon expiration:

- If the MSSP license expires and the non-MSSP license is still valid, there is no impact in the accessibility and usage of the product with the non-MSSP license. However, your users will not be able to access any additional features that the MSSP license grants. Renew your license or licenses before the non-MSSP license expires or if its license policy is violated.
- If the non-MSSP license expires or its license policy is violated and the MSSP license is still valid, there is no impact in the accessibility and usage of the product. Renew your license or licenses before the MSSP license expires.

> If you have purchased the MSSP license, ensure that you add an MSSP contract and create an MSSP profile in Core. For more information, see the Help for **Admin** > **Contract & Usage**.

How Your License Affects Available Features

When a user logs in to the ArcSight Platform or attempts to access a function that requires a special license, the system checks the licenses associated with the deployed products.

The common features such as the Reports Portal and SOAR are enabled if at least one license to enable them is valid. For example, the Transformation Hub license on its own does not enable the Reports Portal, but does if the Recon license is also deployed. Both the Recon and Intelligence licenses enable the Reports Portal. Therefore if your Intelligence license were to expire but the Recon license remains valid, the Reports Portal remains enabled on account of the valid Recon license.

The following table shows the functionality available per product license:

	ESM	Intelligence	MSSP	Recon
Data Quality Dashboard		✔	✔	✔
Event Integrity Check			✔	✔
Multi-tenancy	✔		✔	✔
Outlier Analytics			✔	✔
Reports Portal	✔	✔	✔	✔
ArcMC	✔	✔	✔	✔
Transformation Hub	✔	✔	✔	✔
Search		✔	✔	✔
Storage Groups		✔	✔	✔
SOAR	✔	✔	✔	✔

Data Quality Dashboard

The Data Quality Dashboard provides detailed information about the gap between Device Receipt Time from the raw event itself versus the Normalized Event Time and Database Receipt Time. The dashboard identifies the sources that have a gap. Based on the information analyzed through the dashboard, you can accurately mitigate the problem. This feature also provides history of your data over time. For more information about using this feature, see the Help for **Insights** > **Data Quality**.

Event Integrity Check

The Event Integrity Check enables you to validate that the event information in your database matches the content sent from SmartConnectors, helping you check whether

event data might be compromised. In addition to reviewing the raw event data received from SmartConnectors, you can enable Transformation Hub to generate verification events for more than 20 parsed fields to include in the check. By expanding the number of fields within an event that the check examines, you reduce the opportunities for malicious users to hide their activity. For more information about using this feature, see the Help for **Admin** > **Event Integrity**. You can also view the topic "Configuring Event Integrity Checks" on page 646.

Multi-tenancy

To help you create and manage multiple tenants in your environment, the Multi-tenancy feature allows you be more efficient, secure, cost effective with greater opportunities for growth. This feature is applicable to both of the ArcSight license types, Enterprise and MSSP. The concept of tenancy revolves around two major entities, a Provider and Tenant where the provider is a customer of OpenText that has purchased the license to use the ArcSight Platform, and the tenant is a customer of the provider. For more information see,

- "Enabling Multi-tenancy " on page 442
- Help in the product or the following sections in the *User's Guide for ArcSight Platform*,
  - Managing Your Provider Account
  - Managing Tenants

> Multi-tenancy does not apply for a deployment of ArcSight Intelligence on the ArcSight Platform.

Outlier Analytics

To help you identify anomalous behavior, the Outlier Analytics feature allows you to compare incoming EventCount, BytesIn, and BytesOut values to typical values for your environment. The `EventCount`, `BytesIn` and `BytesOut` values are aggregations over certain time periods for each host/IP address. Outlier Analytics can create and persist a baseline of host behavior. To derive outliers, you compare this baseline with aggregations over new time periods. Basically, the lower the anomaly score, the more likely the event is anomalous. For more information about using this feature, see the Help for **Insights** > **Outliers**.

Reports Portal

To help you hunt for undetected threats and vulnerabilities, the Reports Portal includes a set of built-in dashboards and reports associated with industry security standards such as the Cloud Security Alliance and OWASP. Additional reports and dashboards focus on fundamental security issues, such as monitoring firewalls and malware. For more information about using this feature, see the Help for **Reports**.

Search

The Search feature enables you to look for and investigate events that meet specified criteria so you can detect anomalies that point to security threats. Each search consists of specifying query input, search result fields, and the time period for which you want to search events. Commonly available Search features include fieldsets, lookup lists, and scheduled searches. Users can save their search results, search queries, or queries plus search criteria. For more information about using this feature, see the Help for **Search**.

Storage Groups

You can divide data into storage groups, which allows you to partition the incoming events data and provide different retention periods, based on the query filter. Because you can set data retention policies per storage group, you can retain certain high volume events for a short time period and other important events for longer time period. For more information about using this feature, see the Help for **Configuration** > **Storage**.

Depending on your license, storage retention might be limited.

SOAR

ArcSight SOAR provides a secure orchestration, automation, and response solution where customers can automate a lot of their incident management activities so analysts can perform more in-depth threat hunting and case response. When a user acceses SOAR features, the system checks for an active ESM, Recon, or Intelligence license. SOAR also supports manual/legacy ESM license types. For example, customers using ESM 6.11 and later can also use the SOAR capability. For more information about using this feature, see the *ArcSight SOAR User Guide*.

How Your License Affects Data Storage Policies

You can divide data into **storage groups**, which enables you to partition the incoming events data and provide different retention periods, based on the query filter. To preserve space in the database and improve data retrieval from storage groups, you can configure the database to remove events older than a certain number of months. Your product license affects the maximum value that you set for the data retention policy. If you have deployed multiple capabilities in the ArcSight Platform, the term or permanent license with the highest maximum retention value takes precedence over the maximum allowed value of other licenses. For example, a Recon term or permanent license provides the longest retention time.

Product License	Maximum retention value
Intelligence	30 days

Recon – Instant On	90 days
Recon	Never Expire

For more information about setting the data retention policy, see the Help for **Configuration** > **Storage**.

How Data Ingestion Affects Your License

Your product license specifies the maximum number of events per second that your system can ingest, based on the moving **median events per second (MMEPS)** value. To calculate MMEPS, the system performs the following actions:

1. **Calculate Events Per Day (EPD)**

   Events Per Day is the total number of events ingested into database in a twenty-four hour period. For Day1, the system calculates the EPD based from the time you install the product until GTM+0 hours. The time frame is based on GTM+0 hours starting at 00:00:00 and ending at 23:59:59, regardless of any local times that might be in use.

2. **Calculate Sustained EPS (SEPS)**

   Sustained EPS is the “constant” events per second that the system sustained within the 240-hour period. For Day1, the system calculates the EPD based from the time you install the product until GTM+0 hours. It normalizes peaks and valleys to give a better indication of use. The formula used for this calculation is (EPD/((60*60)*24)).

3. **Calculate MMEPS for the last 45 days**

   Using the SEPS information recorded per day, the system calculates a moving median EPS value using the data set from the last 45-days. After the first 45 days, the system adjusts the calculation window one day every24 hours. The official clock for calculation purposes is defined by GTM+0 hours starting at 00:00:00 to 23:59:59 regardless of local time.

Your product license remains in compliance as long as the MMEPS value remains at the limit or below the purchased license capacity. If three or more consecutive MMEPS value indicators exceed their capacity based on the purchased license, the license is considered to be out of compliance. ArcSight Platform displays a warning until the data ingestion rate normalizes.

Creating Widgets for the Dashboard

The license for your deployed application also grants you access to the **Widget Software Development Kit** (the Widget SDK), which you can download to your local production or test

environment. The Widget SDK enables you to build new widgets or modify existing widgets for deployed applications.

- "Using the Widget SDK" below
- "Considerations for Updating the Widget Store" below

Using the Widget SDK

The Widget SDK requires nodejs 12.7.0, at a minimum, which comes with yarn version 1.16.0.

1. Extract the contents of the `widget-sdk-n.n.n.tgz` file to your developer workstation.
2. Follow the steps in the Getting Started section of the included *ReadMe*.
3. After you compile the new or modified widget, add it to the widget store for use in the Dashboard.
4. (Optional) To allow additional Core users to incorporate your custom widget into their environment, submit the widget to the ArcSight Marketplace.

Considerations for Updating the Widget Store

Review the following considerations before modifying or creating new widgets:

- Widgets provided with a deployed application are included in the default widget store directory.

  ```
  /opt/arcsight-nfs/arcsight-volume/fusion/widget-store
  ```

- Each new widget must have a unique name.
- You cannot edit an out-of-the-box widget. However, you can use the widget as a template for creating a new one. To prevent the modified widget from being erased or overwritten by a product upgrade, give the widget a non-default name.

Updating resources in the worker nodes (AWS only)

The procedure detailed in the following topics allows for the update of node instance type resources (such as CPU and memory). The procedure involves restarting AWS worker nodes, and therefore must be performed only when an EKS update is necessary (see "Upgrading EKS" on page 419), or when the resources require changing.

Checklist: Updating AWS Node Resources

Use this checklist to complete the tasks in the listed order.

	Task	See
❑	1. Launch templates	"Create Launch Templates" below
❑	2. Environment Preparation	"Prepare the Environment " on the next page
❑	3. Elasticsearch Data Backup	"Backing Up the Elasticsearch Data" on the next page
❑	4. Node Update or Replacement	"Performing the Nodes Update/Replacement" on page 493
❑	5. Backing Up the Elasticsearch data	Backing Up Elasticsearch Data

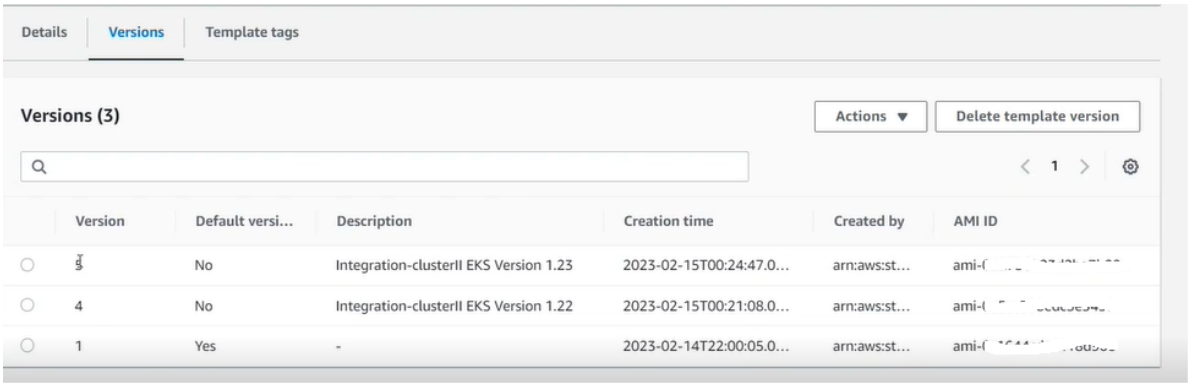
Create Launch Templates

Create a new launch template that uses the desired instance type as follows:

1. Log into the AWS console and browse to the **Launch templates** management page.
2. Select your current launch template.
3. Click **Actions > Modify template (Create new version)** to create a copy of the selected configuration. It's helpful to add a description that includes the new instance type version contained, so as to tell one version from the others easily.
4. In **Application and OS Images (Amazon Machine Image)**, select the same image as used previously, and click enter.
5. Select the new instance type to be used. You can either click **Manually select instance type** and search for the desired type, or click **Specify instance type attributes** and select the `minimum` and `maximum` values for both CPUs and memory size.
6. Leave the rest of the settings at their default value, including **Storage (volumes) -> EBS Volumes -> Size (GiB)**.

   Under **Advanced details**, the only verification due would be to check that the **User data – optional** box contains the same user data as the original template. If there was no user data in the original, there's no need to change anything.

   Clicking on **Create template version** will open the newly created template version:



The description added on step 3 will guide you to the API version be chosen.

Except for the name and AMI image ID, all launch template parameters must be the same as the original. This includes:

- Any desired notifications
- Tags contained in the original group
- Same VPC and all private Availability Zones

Prepare the Environment

You must prepare your environment for the upgrade by doing the following:

- To maintain connection to the Kafka Manager throughout the process, run the following command to patch the th-kafkamgr-svc service:

```
kubectl patch svc -n $(kubectl get ns|awk '/arcsight/ {print $1}') th-
kafkamgr-svc -p '{"spec": { "type": "NodePort", "ports": [ { "nodePort":
32090, "port": 9000} ] } }'
```

- Create a Target Group for port 32090 which uses HTTPS and includes all nodes (old and new). Modify the Health Check path and add: `/th/cmak`.
- Create a listener on the ALB for port 32090 which uses HTTPS and forwards to the new Target Group.
- The resulting URL for accessing Kafka Manager for your cluster after you complete these preparations is: `https://<your cluster DNS name>:32090/th/cmak`

Backing Up the Elasticsearch Data

If Intelligence is deployed in your platform, performing a Elasticsearch data backup will ensure you can restore the data in case there are any issues during the upgrade process. Follow the steps below to backup your data.

1. "Enable the search-manager" below
2. "Scale down logstash" below
3. "Elasticsearch data backup" below
4. "Verify the job status" on the next page

Enable the search-manager

1. Specify the following URL to log in to the OMT Management Portal: https://<CLUSTER FQDN>:5443.
2. Select **Deployment** > **Deployments**.
3. Click **...** (Browse) on the far right and choose **Reconfigure**. A new page will be opened in a separate tab.
4. Click **Intelligence**.
5. Toggle the **Enable Search Manager** button under **Upgrade Configurations**.

Scale down logstash

Execute the following command from the bastion to scale down `logstash`:

```
kubectl -n $(kubectl get ns |awk '/arcsight/ {print $1}') scale statefulset
interset-logstash --replicas=0
```

To ensure that the `logstash` pods have effectively been scaled down, run the following command:

```
kubectl -n $(kubectl get ns |awk '/arcsight/ {print $1}') get pods -A | grep
logstash
```

Also verify no logstash pods are running.

Elasticsearch data backup

1. Login with system-admin role to the interset UI `https://<CLUSTER FQDN>/interset`
2. Click on the gear icon on the top right corner and select **Search Manager**.
3. Click on the **Job History** list box.
4. Select **Submit a Job**.
5. Click on the **Job type** list box and select **Snapshot**.
6. Enter 0 for the **Customer to apply Snapshot to** field.
7. Click the **SUBMIT JOB** button.

Verify the job status

Go to the **Job history** page and check the **Snapshot** job ID status. Click the **REFRESH** button until the status becomes either **COMPLETED_SUCCESS** or **COMPLETED_FAILED**.

If the final status is **COMPLETED_FAILED**, execute this command:

```
kubectl logs  -n $(kubectl get ns |awk '/arcsight/ {print $1}')
elasticsearch-master-0 -c  elasticsearch | grep snapshot
```

The output of this command should include a **[SUCCESS]** message in the output. Repeat the command if the **[SUCCESS]** message does not appear.

> Depending on the amount of data, it may take some time for the **[SUCCESS]** message to appear.

If still unsuccessful after multiple attempts, do not proceed with the upgrade procedure and reach out to customer support for help.

Output examples for successful attempts:

```
{"type": "server", "timestamp": "2022-12-07T15:07:13,016Z", "level": "INFO",
"component": "o.e.s.SnapshotsService", "cluster.name": "interset",
"node.name": "elasticsearch-master-0", "message": "snapshot [repository_
0:snapshot_0_698fee7c-60f4-45e5-bfee-7c06e0f8c415/f5CXpkRpSx6ltB-mIS_TaA]
started", "cluster.uuid": "0Kef4EV2RRaVPQiJHxQQiw", "node.id":
"l6zdkuvgTvq1KZJJQmd-xA" }
```

```
{"type": "server", "timestamp": "2022-12-07T15:07:19,076Z", "level": "INFO",
"component": "o.e.s.SnapshotsService", "cluster.name": "interset",
"node.name": "elasticsearch-master-0", "message": "snapshot [repository_
0:snapshot_0_698fee7c-60f4-45e5-bfee-7c06e0f8c415/f5CXpkRpSx6ltB-mIS_TaA]
completed with state [SUCCESS]", "cluster.uuid": "0Kef4EV2RRaVPQiJHxQQiw",
"node.id": "l6zdkuvgTvq1KZJJQmd-xA" }
```

> If the snapshot job continues to remain in the **Pending** state for a prolonged period of time, restart the `searchmanager-engine-xxxxxxxxxx-xxxxx` pod.

Open topic with navigation

Performing the Nodes Update/Replacement

1. Browse to the **Auto Scaling groups** page and create a new Auto Scaling group for Kafka workers. The new Auto Scaling group contains the same number of nodes (and the same roles) as the current Auto Scaling group, but using the newly-created launch template.

a. In **Choose launch template or configuration**, look for the name of the one just created, and then select the version that contains the desired new type.

b. Select the same VPC and all private Availability Zones.

c. In **Configure advanced options**, for the **Load balancing - optional** value, check **Attach to an existing load balancer**.

   From the **Attach to an existing load balancer** menu, check **Choose from your load balancer target groups**. This will allow you to select the load balancer target groups created for this cluster (3000, 443, 5443, 32080, 32081, 32090, 32101-32150for the CTH pods, etc) from a list box.

   > You can start writing the name of the groups on the **Existing load balancer target groups** box, and click each of them to add it. You cannot make multiple selections, since the list box will close each time one is chosen, but it can be reopened to enter the rest of the groups.

   This selection will automatically register the **Auto Scaling group** nodes to the target groups.

   Leave all other advanced options at default values.

d. Ensure group sizes for desired, minimum and maximum are the same as the original Auto Scaling group.

e. Add any desired notifications.

f. Add the same tags contained in the original group. Make sure that the EKS cluster name appears in the tags.

g. Review the new configuration and click **Create Auto Scaling group**. This process will create three new nodes.

> Following the completion of the worker node upgrade, the Kafka broker IDs (as seen in the Kafka Manager UI under **Brokers**) will all be incremented by 1 from their starting values. This is expected.

See Creating the AWS Auto Scaling Group for more information.

2. Get the cluster node names by running the following command, and then record the node names returned:

```
kubectl get nodes
```

Example output:

```
NAME                                          STATUS    ROLES     AGE
VERSION
```

```
ip-10-0-10-253.example.com   Ready    <none>   10m    v1.23.14-eks-
ba74326
```

```
ip-10-0-10-61.example.com    Ready    <none>   3d1h   v1.23.15-eks-
ba74326
```

```
ip-10-0-13-119.example.com   Ready    <none>   3d1h   v1.23.15-eks-
ba74326
```

```
ip-10-0-13-40.example.com    Ready    <none>   10m    v1.23.14-eks-
ba74326
```

```
ip-10-0-14-238.example.com   Ready    <none>   10m    v1.23.14-eks-
ba74326
```

```
ip-10-0-15-193.example.com   Ready    <none>   3d1h   v1.23.15-eks-
ba74326
```

> Repeat the following sequence consisting of steps 3 through 8 on each of the original Kafka worker nodes, cycling throughout the nodes one by one, until the sequence has been performed on all worker nodes. Proceed to Step 13 only after the sequence has been performed on each original Kafka worker node.

3. Select a worker node and drain it by running the following command.

```
kubectl drain <FQDN of selected node> --force --delete-emptydir-data --ignore-
daemonsets --timeout=180s
```

> If the `intelligence-namenode=yes` label has been applied to any node, then drain that node **last** among all nodes.

Wait for the command to complete and for all pods to return to the Running state before proceeding to the next step. **The drain/cordon process can take several minutes for all pods to return to the Running state. Please be patient and allow the process time to complete and all pods to return to Running state.**

> If a **CrashLoopBackOff** or **error** status appears during this process, it can be ignored

4.

Log in to Kafka Manager (cmak) at `https://<CLUSTER FQDN>:32090/th/cmak` and re-assign Kafka partitions for the node with these commands:

a. Click **Generate Partition Assignments** and select all topics (default)

b. Click **Run Partition Assignments** (use default settings for broker IDs)

5. c. Click **Go** to reassign partitions and refresh the page until the *Completed* field shows a data and time of completion.

(Conditional) If your deployment includes ArcSight Intelligence, then monitor the ES replication process by logging into the pod and executing this command:

```
kubectl exec -n $(kubectl get ns |awk '/arcsight/ {print $1}')
elasticsearch-master-0 -c  elasticsearch -it bash
```

Monitor the **ES replication** process using the following command:

```
curl -k -XGET 'https://elastic:<password>@localhost:9200/_
cat/health?v=true'
```

Example command and output:

```
curl -k -XGET 'https://elastic:changeme@localhost:9200/_
cat/health?v=true'
```

```
epoch      timestamp cluster  status node.total node.data shards pri relo
init unassign pending_tasks max_task_wait_time active_shards_percent
1671118161 15:29:21  interset green           6         3   1128 583    0
   0        0             0                  -                100.0%
```

> At the completion of the Elasticsearch replication, the status of all nodes should be "green". A "yellow" status indicates that the replication has not yet completed.
>
> However, if the Elasticsearch recovery is not progressing and the `active_shards_percent` does not reach 100%, or its status is **red**, you may disregard the pods not returning to running state and proceed with the EKS upgrade (this applies to **intelligence** and **searchmanager** pods). This is because, after cordoning the node, some interset pods might remain in `init` state, but this can be ignored.

6. In Kafka Manager, check that the topic partition table data returns to normal. There should be no under-replication of data, and broker leader skew values should return to 0%. Do the following:
   a. Select a Kafka pod and log into it.
   b. **Check for under-replication:** Select one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line. The command block will return no result if there is no under-replication.

   For FIPS (or non-FIPS) Encryption with Client Authentication:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'sed -ir "s/^
```

```
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=$STORES_
SECRET/" /etc/kafka/client.properties && \sed -ir "s/^
[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=$STORES_
SECRET/" /etc/kafka/client.properties && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --describe --topic
th-cef --under-replicated-partitions --command-config
/etc/kafka/client.properties'
```

After executing the above, **Copy** and then paste the following command block:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=/"
/etc/kafka/client.properties'
```

For FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'KAFKA_OPTS+=" -
Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-kafka.truststore " &&
\
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreProvider=BCFIPS " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreType=BCFKS " && \
kafka-topics --bootstrap-server th-kafka-svc:9093  --describe --topic
th-cef --under-replicated-partitions --command-config
/etc/kafka/client2.properties'
```

For non-FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'KAFKA_OPTS+=" -
Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-kafka.truststore " &&
\
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
kafka-topics --bootstrap-server th-kafka-svc:9093  --describe --topic
th-cef --under-replicated-partitions --command-config
/etc/kafka/client2.properties'
```

> Whether or not there's a result to the command, each of them will return the following warning messages, which can be ignored:
>
> WARNING: An illegal reflective access operation has occurred
>
> WARNING: Illegal reflective access by org.bouncycastle.jcajce.provider.ProvSunTLSKDF (file:/opt/th/libs/bc- fips- 1.0.2.3.jar) to constructor sun.security.internal.spec.TlsPrfParameterSpec (javax.crypto.SecretKey,java.lang.String,byte[],int,java.lang.String,int,int)
>
> WARNING: Please consider reporting this to the maintainers of org.bouncycastle.jcajce.provider.ProvSunTLSKDF
>
> WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
>
> WARNING: All illegal access operations will be denied in a future release

c. **Check for broker leader skew:** As in the last step, select one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line. Verify that the number of times each broker is listed is equal to the `replicationFactor` value.

For FIPS (or non-FIPS) Encryption with Client Authentication:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=$STORES_
SECRET/" /etc/kafka/client.properties && \
sed -ir "s/^
[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=$STORES_
SECRET/" /etc/kafka/client.properties && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --describe --topic
th-cef --command-config /etc/kafka/client.properties'
```

After executing the above, **Copy** and then paste the following command block:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=/"
/etc/kafka/client.properties'
```

For FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'KAFKA_OPTS+=" -
Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-kafka.truststore " &&
\
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreProvider=BCFIPS " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreType=BCFKS " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --describe --topic
th-cef --command-config /etc/kafka/client2.properties'
```

For non-FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print
$1}') -- sh -c 'KAFKA_OPTS+=" -
Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-kafka.truststore " &&
\
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --describe --topic
th-cef --command-config /etc/kafka/client2.properties'
```

Example output from the above command blocks:

```
Topic: th-cef   PartitionCount: 6       ReplicationFactor: 2
Configs:
cleanup.policy=delete,segment.bytes=1073741824,message.format.version=
2.5-IV0,retention.bytes=6442450944
```

```
Topic: th-cef   Partition: 0    Leader: 1005    Replicas: 1005,1004
 Isr: 1004,1005
```

```
Topic: th-cef   Partition: 1    Leader: 1006    Replicas: 1006,1005
 Isr: 1005,1006
```

```
Topic: th-cef   Partition: 2    Leader: 1004    Replicas: 1004,1006
 Isr: 1004,1006
```

```
Topic: th-cef   Partition: 3    Leader: 1005    Replicas: 1005,1006
 Isr: 1005,1006
```

```
Topic: th-cef   Partition: 4    Leader: 1006    Replicas: 1006,1004
 Isr: 1004,1006
```

```
Topic: th-cef   Partition: 5    Leader: 1004    Replicas: 1004,1005
 Isr: 1004,1005
```

The example output shown above is a final, successful result. It will take time to achieve it, depending on the amount of data, the number of partitions and replication factors.

As well, it might require several executions of the command to reach this point, where all partitions are listed and there are two instances of each leader value.

If this output is not achieved after several executions of the command, please go back to the `cmak` login step and execute parts **a** and **b**. Then come back and execute this command block again.

> Kafka will automatically advertise the new node to the connectors.

7. **Repeat steps 2 through 6 for each additional node in the cluster. When you have completed the steps on each node, only then proceed to the next step.**
8. (Conditional) If the `intelligence-namenode=yes` label was applied to the node being drained, proceed to For Intelligence Only - Steps for nodes with the intelligence-namenode=yes label.

   If not, you can proceed to the step below directly.
9. Delete the old **Auto Scaling group** (you created its replacement as above). Wait until all nodes from the old **Auto Scaling group** are deleted and all pods have returned to the **Running** state before proceeding to the next step.

   > A message may be returned that pods are still running. This message may be ignored.
10. Verify that the 3000 and 5443 ports are using the **frontend-ingress-controller-svc** and **portal-ingress-controller-svc** internal port values respectively after the final node update. In case they're not, follow the procedure described in Configuring Controller Services.

(Conditional) If the ArcSight Database has been deployed, log into the database master node and run these commands:

```
./kafka_scheduler stop
./kafka_scheduler start
```

Verify that Kafka Scheduler has the correct new node IP addresses by running this command:

```
./kafka_scheduler status
```

Verify that Event Table Status events count is increasing by running this command:

```
./kafka_scheduler events
```

If Step 5 failed for your Intelligence deployment: For Intelligence Only - Steps for nodes with the intelligence-namenode=yes label

For Intelligence Only - Steps for nodes with the `intelligence-namenode=yes` label

If the `intelligence-namenode=yes` label was applied to the node being drained, perform these two steps:

- Add the `intelligence-namenode=yes` label to one of the new nodes and update the node FDQN in the **Reconfigure** page of the OMT (**HDFS NameNode** under the **Intelligence** tab)
- Log into each of the database nodes and replace the **HDFS NameNode** value from the previous step to the `Core-site.xml` file located in the `/etc/hadoop/conf/` directory.

  Select the option that applies to your configuration:

  - If **Enable Secure Data Transfer with HDFS Cluster** is disabled in the **Intelligence** tab of the OMT Management portal, in the `/etc/hadoop/conf` directory, add the following configurations:

    In the `hdfs-site.xml` file:

    ```
    <configuration>
    </configuration>
    ```

    In the `core-site.xml` file:

    ```
    <configuration>
      <property>
       <name>fs.defaultFS</name>
       <value>hdfs://<namenode>:30820/</value>
      </property>
      <property>
       <name>dfs.namenode.http-address</name>
       <value><namenode>:30070</value>
      </property>
    </configuration>
    ```

  - If **Enable Secure Data Transfer with HDFS Cluster** is enabled in the **Intelligence** tab of the OMT Management portal, in the `/etc/hadoop/conf` directory.

    > If Kerberos Authentication is enabled, reconfigure it by following the "Enabling and Configuring Kerberos Authentication" on page 620 procedure before proceeding.

    Navigate to the `/etc/hadoop/conf` directory and add the following configurations:

    In the `hdfs-site.xml` file:

    ```
    <configuration>
      <property>
       <name>dfs.http.policy</name>
    ```

```
    <value>HTTPS_ONLY</value>
   </property>
   <property>
    <name>dfs.encrypt.data.transfer</name>
    <value>true</value>
   </property>
</configuration>
```

In the `core-site.xml` file:

```
<configuration>
  <property>
   <name>fs.defaultFS</name>
   <value>hdfs://<namenode>:30820/</value>
  </property>
  <property>
   <name>dfs.namenode.https-address</name>
   <value><namenode>:30070</value>
  </property>
</configuration>
```

Change to the following directory:

```
cd /opt/vertica/bin/
```

Log in as a dbadmin:

```
su dbadmin
```

Log in to vsql and specify the password when prompted:

```
vsql
[password prompt]
```

Next, run the following commands:

```
SELECT CLEAR_HDFS_CACHES();
SELECT VERIFY_HADOOP_CONF_DIR();
SELECT node_name, node_address, export_address FROM nodes;
```

The expected output is:

```
Welcome to vsql, the Vertica Analytic Database interactive terminal.

Type: \h or \? for help with vsql commands
\g or terminate with semicolon to execute query
\q to quit

fusiondb=>
```

```
fusiondb=> SELECT CLEAR_HDFS_CACHES();
CLEAR_HDFS_CACHES
-----------------------------------------------------------------------
Cleared
(1 row)

fusiondb=> SELECT VERIFY_HADOOP_CONF_DIR();
VERIFY_HADOOP_CONF_DIR
--------------------------------------------------------------------------
Validation Success
v_fusiondb_node0001: HadoopConfDir [/etc/hadoop/conf] is valid
v_fusiondb_node0002: HadoopConfDir [/etc/hadoop/conf] is valid
v_fusiondb_node0003: HadoopConfDir [/etc/hadoop/conf] is valid

(3 rows)

fusiondb=> SELECT node_name, node_address, export_address FROM nodes;
node_name | node_address | export_address
--------------------------------------------------------------------------
v_fusiondb_node0001 | <IP1> | <IP1>
v_fusiondb_node0002 | <IP2> | <IP2>
v_fusiondb_node0003 | <IP3> | <IP3>
(3 rows)
```

Recovering and Restoring Elasticsearch Data

If you have deployed the Intelligence capability, follow the instructions provided in this section.

- Elasticsearch Monitoring Action Fails During EKS Upgrade
  - Deleting Unassigned Shards
  - Restoring Elasticsearch Data
- Elasticsearch Monitoring Action Succeeds During EKS Upgrade
- If Analytics Run Fails

Elasticsearch Monitoring Action Fails During EKS Upgrade

If the Elasticsearch monitoring actions fails for the Intelligence pods (this could have happened either in step 9 of the "Performing the EKS Upgrade" on page 424 procedure, or step 5 of the "Performing the Nodes Update/Replacement" on page 493 procedure), you must delete the unassigned shards that might impede the recovery process:

- Deleting Unassigned Shards
- Restoring Elasticsearch Data

Deleting Unassigned Shards

1. Run the following command, being sure to replace the <password> value with yours:

```
kubectl exec -it -n $(kubectl get ns |awk '/arcsight/ {print $1}')
elasticsearch-master-0 -c  elasticsearch -- curl -k -XGET
https://elastic:<password>@localhost:9200/_cat/shards | grep UNASSIGNED |
awk {'print $1'} | xargs -i curl -k -XDELETE
'https://elastic:<password>@localhost:9200/{}'
```

2. To monitor the delete progress, run the following command:

```
kubectl exec -n $(kubectl get ns |awk '/arcsight/ {print $1}')
elasticsearch-master-0 -c  elasticsearch -it -- curl -k -XGET
'https://elastic:<password>@localhost:9200/_cat/health?v=true'
```

   Example output:

```
epoch      timestamp cluster  status node.total node.data shards pri relo
init unassign pending_tasks max_task_wait_time active_shards_percent
1671118161 15:29:21  interset green           6         3   1128 583    0
   0        0             0                  -                100.0%
```

   In the example above, the value has reached a 100% and the status is green.

Restoring Elasticsearch Data

1. If the result of the command is a yellow status, and a value under 100%, apply the following procedure:
   a. Login with system-admin role to the interset UI https://<CLUSTER FQDN>/interset
   b. Click on the gear icon on the top right corner and select **Search Manager**.
   c. Click on the **Job History** list box.
   d. Select **Submit a Job**.
   e. Click on the **Job type** list box and select **Restore**.
   f. Enter 0 for the **Customer to apply Snapshot to** field.
   g. Click the **SUBMIT JOB** button.
2. To verify the job status, complete the following steps:
   a. On the **Job history** page, check the **Snapshot** job ID status.
   b. Click the **REFRESH** button until the status becomes either **COMPLETED_SUCCESS** or **COMPLETED_FAILED**.

c. If the final status is **COMPLETED_FAILED**, execute the following commands to monitor the health:

```
kubectl exec -n $(kubectl get ns |awk '/arcsight/ {print $1}')
elasticsearch-master-0 -c  elasticsearch -it curl -k -XGET
'https://elastic:<password>@localhost:9200/_cat/health?v=true'
```

Example command and output:

```
curl -k -XGET 'https://elastic:changeme@localhost:9200/_
cat/health?v=true'
```

```
epoch      timestamp cluster  status node.total node.data shards pri
relo init unassign pending_tasks max_task_wait_time active_shards_
percent
1671118161 15:29:21  interset green           6         3   1128 583
 0    0        0             0                  -
100.0%
```

In the example above, the value has reached a 100% and the status is green.

d. If the result of the command is a yellow status, and a value under 100%, you could wait 5 minutes and then repeat the command until the green status is achieved.

3. Scale up logstash using the following command:

```
kubectl -n $(kubectl get ns |awk '/arcsight/ {print $1}') scale
statefulset interset-logstash --replicas=<replica count>
```

Now, run analytics on demand.

Elasticsearch Monitoring Succeeds During EKS Upgrade

If the Elasticsearch monitoring actions in step 9 of the "Performing the EKS Upgrade" on page 424 procedure, or step 5 of the "Performing the Nodes Update/Replacement" on page 493 procedure succeeds for the Intelligence pods, run analytics on demand.

If Analytics Run Fails

Follow the workaround, if you encounter any of the following issues:

Issue: If Analytics were to fail after the EKS upgrade, there are two things you can check to remedy it:

Workaround: Perform the following steps:

- Review the logs for the following error:

```
Suppressed: org.elasticsearch.client.ResponseException: method [POST],
host [https://elasticsearch-svc:9200], URI [/_aliases?master_
timeout=30s&timeout=30s],
status line [HTTP/1.1 503 Service Unavailable]{"error":{"root_cause":
[{"type":"not_master_exception",
"reason":"no longer master. source: [index-aliases]"}],"type":"master_
not_discovered_exception",
"reason":"NotMasterException[no longer master. source: [index-aliases]]",
"caused_by":{"type":"not_master_exception","reason":"no longer master.
source: [index-aliases]"}},"status":503}
```

- If this error is found, execute the following commands:

```
kubectl -n $(kubectl get ns |awk '/arcsight/ {print $1}') scale
statefulset elasticsearch-master --replicas=0
```

```
kubectl -n $(kubectl get ns |awk '/arcsight/ {print $1}') scale
statefulset elasticsearch-data --replicas=0
```

```
kubectl -n $(kubectl get ns |awk '/arcsight/ {print $1}') scale
statefulset elasticsearch-master --replicas={replica_count}
```

```
kubectl -n $(kubectl get ns |awk '/arcsight/ {print $1}') scale
statefulset elasticsearch-data --replicas={replica_count}
```

Issue: If Analytics fails after the EKS upgrade because the HDFS namenode has entered safe mode.

Workaround: Perform the following steps:

1. Execute the following command to restart the HDFS pods:

```
kubectl delete pods -n $(kubectl get ns |awk '/arcsight/ {print $1}')
$(kubectl get pods -n $(kubectl get ns |awk '/arcsight/ {print $1}') -o
wide |  grep "hdfs-" | cut -d ' ' -f1)
```

2. Execute the following command:

```
kubectl exec -n $(kubectl get ns |awk '/arcsight/ {print $1}') hdfs-
namenode-0 -c  hdfs-namenode -it bash
```

```
hdfs dfsadmin -safemode leave
```

3. Run Analytics on demand.

Managing the OMT Infrastructure

For information about OMT infrastructure, see " Understanding the OMT Infrastructure " on page 22

This section provides information about managing the OMT infrastructure.

Accessing the OMT Management Portal

The OMT Management Portal enables management, deployment, and configuration of OMT and OMT-based products.

To open the management portal for an AWS-based cluster:

1. On the bastion host, use either the forwarding display or forwarding local ports methods to browse to `http://<Route 53>:5443`.
2. Enter the username *admin* and the password.

Managing OMT Management Portal Access

At times, you may be unable to log in to the OMT Management Portal with the admin user. When this situation occurs, you can unlock the user's account or reset the user's password.

- "Resetting the OMT Administrator Password" below
- "Unlocking the OMT Management Portal User Account" on the next page
- "Resetting the User's Password" on the next page
- "Accessing the OMT Management Portal Reconfigure Page" on page 509

Resetting the OMT Administrator Password

You can reset the administrator password on a OMT installation.

1. Browse to OMT Management Portal.
2. Log in using admin USERID and the password you specified during the platform installation in the command line argument. (This URL is displayed at the successful completion of the OMT installation shown earlier.)
3. In the left navigation page, click **IDM Administration.**

4. In the main panel, click **SRG**.
5. In the left navigation bar, click **Users**.
6. In the list of users on the right, select *Admin* and click **Edit**.
7. In the bottom right, click **Remove Password.**
8. Click **Add Password.**
9. Enter a new admin password, then click **Save**.

Unlocking the OMT Management Portal User Account

1. Log in to a master node as root.
2. To access the shell of the `idm` container, run the following command:

```
 kubectl exec -it $(kubectl get pod -n core -ocustom-
columns=NAME:.metadata.name |grep idm|head -1) -n core sh -c idm
```

3. To unlock the user, run the following command:

```
sh /idmtools/idm-installer-tools/idm.sh databaseUser unlockUser -org
Provider -name admin
```

Resetting the User's Password

1. Log in to a master node as root.
2. Run the following command to access the `idm` pod:

```
kubectl exec -it $(kubectl get pod -n core -ocustom-
columns=NAME:.metadata.name |grep idm|head -1) -n core sh idm
```

3. Run the following command to reset the password to a temporary value. (Replace `<new_tmp_password>` with your new temporary password.)

```
sh /idmtools/idm-installer-tools/idm.sh databaseUser resetPassword -org
Provider -name "admin" -plainPwd "<new_tmp_password>"
```

> If the user account is locked due to too many failed login attempts, run unlock, as described above in "Unlocking the OMT Management Portal User Account" above.

4. Log into the OMT Management Portal with the new temporary password, then set the new non-temporary password on the password reset page.
5. Log in to the OMT Management Portal with the new password.

Accessing the OMT Management Portal Reconfigure Page

At times, you might not be able to access the OMT Management Portal Reconfigure page. For example, this issue might occur when you are trying to perform an upgrade.

In that case, follow the steps below to remedy the issue:

1. Verify the status of the `nginx-ingress-controller` DaemonSet :

```
NS=$(kubectl get namespaces | awk '/arcsight/{print $1}');kubectl get
daemonset nginx-ingress-controller -n $NS
```

2. Create a new `nginx-ingress-controller.yaml` file:

```
cd ${K8S_HOME};kubectl get daemonset nginx-ingress-controller -n `kubectl
get namespaces | grep arcsight-installer | awk '{print $1}'` -o yaml > \
nginx-ingress-controller.yaml
```

3. Ensure that the saved `nginx-ingress-controller.yaml` file exist in the `${K8S_HOME}` home directory (`/opt/arcsight/kubernetes`) and contains definitions in yaml format.
4. Delete the current `nginx-ingress-controller` configuration:

```
kubectl delete -f ./nginx-ingress-controller.yaml
```

5. Apply the new `nginx-ingress-controller` configuration:

```
kubectl apply -f ./nginx-ingress-controller.yaml
```

6. Wait until the `nginx-ingress-controller` pods are up and running:

```
kubectl get pods -n $NS --watch | grep nginx-ingress-controller
```

7. Verify the `nginx-ingress-controller` controller daemonset status:

```
kubectl get daemonset nginx-ingress-controller -n $NS
```

Changing the IP Address of a Master or Worker Node

You can assign a master or worker node a new IP address by deleting the node, and then re-adding the node with the new FQDN.

To change the IP address of a master or worker node:

1. Note the FQDN, current IP address, and new IP address of the node for which you wish to assign a new IP address.

2. Log in to the OMT Management Portal (`https://<ha-address>:5443`).
3. Click **Cluster > Nodes.**
4. Click **+ Add.**
5. Next to the node for which you plan to change the IP address, in the **Operations** column, click **Delete**.
6. Enter the username and password/keyphrase to confirm node deletion. Remain on the page and verify that the node has been deleted. Give the process time to complete.
7. Outside of OMT, perform the necessary changes within your network administration or host settings to change the old IP address of the node to the new IP address.
8. In the OMT Management Portal, on **Cluster > Nodes.**
9. Click **+ Add.**
10. Enter the FQDN of the node which you are re-adding.
11. Enter values for the pop-up dialog as prompted. For host name, use the new (existing) FQDN of the node you deleted in Step 5.
12. Click **ADD**, and then wait for the confirmation that new node has been added to the cluster.
13. Ensure that you add the appropriate labels to the node that you re-added.

Checking Kubernetes Dashboard for Status and Errors

1. Log in to the OMT Management Portal.
2. Navigate to **Cluster** > **Dashboard** to access the Kubernetes Dashboard.
3. In Kubernetes Dashboard change Namespace to arcsight-installer-*.
4. Navigate to **Workloads** > **Pods**.
5. View the status of pods. For more information about each pod, see Understanding Labels and Pods.
6. Clicking a pod reveals more status details of that pod.
   a. Logs for the pod can be viewed by clicking on the View Logs button on the right side of the blue banner near the top.
   b. Each pod may contain multiple containers, so when viewing logs, be sure to use the Logs from <container> to view the logs for the specific container you need to view.
   c. Logging levels can be modified as described at here.

Maintaining the RE Certificate

Use the information provided in the sections below to update or maintain the RE External Communication Certificate for the ArcSight Platform.

Securing External Communication with the RE Certificate

At the center of the Platform is a Kubernetes cluster where communication occurs between pods within the cluster and with non-containerized ArcSight components outside of the cluster. In order to ensure secure trusted communication between pods within the cluster and components outside of the cluster, encrypted communication with client certificate authentication is configured by default.

- Understanding the ArcSight Platform Certificate Authorities
- Using an RE External Communication Certificate Signed by Your Trusted Certificate Authority

Understanding the ArcSight Platform Certificate Authorities

During installation, three self-signed Certificate Authorities (CA) are created automatically, two for signing certificates used exclusively for pod to pod communication within the cluster (RIC and RID CA), and the other for signing certificates for each pod that performs communication external to the cluster (RE CA). Only pods that perform external communication have a certificate that is signed by the external CA.

External cluster communication occurs not only with ArcSight components, but also with user web browsers and, in some cases, user clients of ArcSight APIs (such as the REST API). By default, when the user connects to the cluster, they will be presented with a certificate that has been signed by the self-signed external CA. Since the external CA is self-signed, the user's connection will not automatically trust the certificate because it will not be verifiable using a certificate chain that is already in the user's trust store.

To give users confidence they are connecting to the trusted cluster, we recommend signing the certificates that are presented to the user with a CA that is trusted by the user's trust store. There are two approaches to doing this that are described in the documentation below. These approaches are:

Method 1 - Signing the RE External Communication Certificate with Your Trusted Certificate Authority

This is the recommended approach, because it is theoretically more secure than the other approach, in that it only involves transferring a CSR and public certificate between systems,

which does not put any private secrets at risk.

Method 2 - Importing an Externally Created Intermediate CA

This approach involves creating an Intermediate CA (key and certificate pair) in a system outside of the ArcSight Platform, and then importing it into the ArcSight Platform. While this approach does work, it is theoretically less secure than the other approach, because it involves transferring a CA private key between systems, which potentially exposes it to unintended parties.

Use only one of the two approaches above.

Using an RE External Communication Certificate Signed by Your Trusted Certificate Authority

Use only one of the two approaches below. The first one, "Signing the RE External Communication Certificate with Your Trusted Certificate Authority" approach is recommended for the reasons described in Understanding the ArcSight Platform Certificate Authorities.

Method 1 - Signing the RE External Communication Certificate with Your Trusted Certificate Authority

Signing the RE External Communication Certificate with Your Trusted Certificate Authority approach is recommended for the reasons described in Understanding the ArcSight Platform Certificate Authorities.

In order to sign the RE external communication certificate with your trusted CA, you need to (1) create a certificate signing request (CSR) from vault, (2) take it to your organization, (3) sign it, and (4) return the signed CSR and all the public chain-of-certificates used to sign it.

1. Export the following access token dependencies (you can remove these later if not needed):

```
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o json
2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n core
-o json 2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-cbc -
md sha256 -a -d -pass pass:"${PASSPHRASE}")
```

2. Delete the existing vault secrets by running the following command:

```
kubectl exec -it -n core ${VAULT_POD} -- bash -c "VAULT_TOKEN=$VAULT_
TOKEN vault secrets disable -tls-skip-verify RE" && kubectl exec -it -n
core ${VAULT_POD} -- bash -c "VAULT_TOKEN=$VAULT_TOKEN vault secrets
enable -tls-skip-verify -max-lease-ttl=87600h -path=RE pki"
```

3. Ask vault to generate the CSR by running the following command:

   Important: When you execute this command, proceed expeditiously through steps 3 and 4, as your cluster will not be able to issue external certificates while it waits for the CSR to be signed.

```
kubectl exec -it -n core ${VAULT_POD} -c vault -- bash -c "VAULT_
TOKEN=$VAULT_TOKEN vault write -tls-skip-verify -format=json
RE/intermediate/generate/internal common_name=\"none-MF CDF RE CA on
<FQDN of ArcSight Platform Virtual IP for HA or single master node>\"
country=<Country> locality=<Locality> province=<Province>
organization=<Organization> ou=<Organizational Unit>" | jq -r '.data.csr'
> /tmp/pki_intermediate.csr
```

   Note: The `common_name` in the command above is an example common name. Substitute your own values for the common name to fit your environment. Additionally, your trusted certificate authority might require additional parameters in the CSR besides common_name. Ask your PKI team for what the required CSR parameters are and add the appropriate parameters to the command (similar to how the parameter common_name is specified). The parameter names for the vault command used above are documented at https://www.vaultproject.io/api-docs/secret/pki#generate-intermediate

4. Sign the CSR file with your trusted certificate authority, and save the result into the `intermediate.cert.pem` file.

   Example only. A basic example is provided below. Your environment will likely be different.

```
openssl ca -keyfile your-rootca-sha256.key -cert your-rootca-sha256.crt -
config your-openssl-configuration-file -extensions v3_ca -notext -md
sha256 -in /tmp/pki_intermediate.csr -out intermediate.cert.pem
```

   Make sure the `v3_ca` and `authorityKeyIdentifier` extensions are enabled and a new certificate is useable as a certificate authority on its own. Otherwise, you will receive a warning in the next step that given certificates are not marked for CA use.

5. Create an `intermediate.chain.pem` file that includes the combination of the `intermediate.cert.pem`, the public certificate of your trusted certificate authority, and all intermediate public certificates in the chain between them so that `intermediate.chain.pem` includes the full trust chain.

```
cp intermediate.cert.pem intermediate.chain.pem
cat [parent-intermediate1.crt] [parent-intermediate2.crt] [...] your-
rootca-sha256.crt >> intermediate.chain.pem
```

> If you have intermediate certificates between your `intermediate.cert.pem` and your trusted certificate authority, you must add the certificates in the specific order of the sequence of the chain, with the last certificate being the certificate of the root trusted CA.

6. Import the `intermediate.chain.pem` file into the cluster vault:

```
chaincerts=$(cat intermediate.chain.pem) && kubectl exec -it -n core
${VAULT_POD} -c vault -- bash -c "VAULT_TOKEN=$VAULT_TOKEN vault write -
tls-skip-verify -format=json RE/intermediate/set-signed
certificate=\"${chaincerts}\""
```

   Re-create the vault coretech role by running the following command:

```
kubectl exec -it -n core ${VAULT_POD} -- bash -c "VAULT_TOKEN=${VAULT_
TOKEN} vault write -format=json -tls-skip-verify RE/roles/coretech allow_
any_name=true allow_ip_sans=true max_ttl=87600h ttl=8760h"
```

7. Update `ConfigMap RE_ca.crt` by running these commands:

```
reCrtForJson=$(sed -E ':a;N;$!ba;s/\r{0,1}\n/\\n/g'
intermediate.chain.pem) && kubectl patch configmap -n core public-ca-
certificates -p "{\"op\": \"replace\", \"data\":{\"RE_
ca.crt\":\"${reCrtForJson}\"}}"
```

```
ARCSIGHT_NS=$(kubectl get namespaces --no-headers -o custom-
columns=":metadata.name" | grep arcsight-installer)
```

```
if [ -n "$ARCSIGHT_NS" ];then reCrtForJson=$(sed -E ':a;N;$!ba;s/\r
{0,1}\n/\\n/g' intermediate.chain.pem); kubectl patch configmap -n
$ARCSIGHT_NS public-ca-certificates -p "{\"op\": \"replace\", \"data\":
{\"RE_ca.crt\":\"${reCrtForJson}\"}}";fi
```

8. (Conditional) If you already deployed ArcSight Capabilities onto the OMT, update the ArcSight Capabilities to use the updated RE external communication certificate, by following the instructions in Configuring ArcSight Kubernetes Pods to Use the Updated RE External Communication Certificate.

   If you deployed OMT but have not yet deployed any ArcSight Capabilities, you can skip those instructions.

Method 2 - Importing an Externally Created Intermediate CA

This is an alternate approach for signing certificates to connect to the trusted cluster. Before choosing this approach, ensure that you understand the other approach recommended in Understanding the ArcSight Platform Certificate Authorities.

1. Obtain an intermediate CA (key and certificate pair) from your trusted certificate authority.
   a. Name the certificate files as follows:
      - key file: `intermediate.key.pem`
      - certificate file: `intermediate.cert.pem`
   b. Obtain the root CA certificate (including chain), and put it in a file named ca.cert.pem.
   c. Create an `intermediate.cert.chain.pem` file that includes the combination of the `intermediate.cert.pem`, and the root CA certificate (including chain) `ca.cert.pem`. This way, `intermediate.chain.pem` includes the full trust chain.

      ```
      cat intermediate.cert.pem ca.cert.pem >> intermediate.cert.chain.pem
      ```

2. Replace the existing RE CA in the ArcSight Platform with the intermediate CA you obtained in the step above.
   a. Change the directory:
      - For a cloud deployment, run these commands:

        ```
        cd <path to OMT installer>/cdf-deployer/scripts/
        ```

   b. Run the following command to replace the existing RE CA:

      ```
      ./cdf-updateRE.sh write --re-crt=/pathto/intermediate.cert.chain.pem --re-key=/pathto/intermediate.key.pem
      ```

3. (Conditional) If you already deployed ArcSight Capabilities onto OMT, proceed to the next section to update the ArcSight Capabilities to use the updated RE external communication certificate, Configuring ArcSight Kubernetes Pods to Use the Updated RE External Communication Certificate.

   However, if you have only deployed OMT, but have not deployed ArcSight Capabilities yet, you can skip that section.

Configuring ArcSight Components to Use the Updated RE External Communication Certificate

After signing the RE External Communication Certificate for a new or upgraded ArcSight installation, you need to configure the Kubernetes pods and the ArcSight Database to use the updated certificate. The sections below provide the instructions to configure those components for the updated certificate. For information about signing the RE certificate, see "Method 1 - Signing the RE External Communication Certificate with Your Trusted Certificate Authority" on page 512.

- Configuring ArcSight Kubernetes Pods to Use the Updated RE External Communication Certificate
- Configuring the ArcSight Database to Use the Updated RE External Communication Certificate

Configuring ArcSight Kubernetes Pods to Use the Updated RE External Communication Certificate

Following this procedure will restart ArcSight Kubernetes pods so that they immediately refresh their trust stores to use an updated RE external communication certificate chain. This will result in temporary downtime of the services these pods provide while the pods are restarting.

1. Restart the following ArcSight pods, so they can use the new RE certificate:
   a. Commands for all deployments:

```
ARCSIGHT_NS=$(kubectl get namespaces --no-headers -o custom-
columns=":metadata.name" | grep arcsight-installer)
labels=autopass-lm-apps,soar-web-app,soar-
frontend,osp,management,reporting,search-engine,arcmc,web-
service,schema-registry,kafka,zookeeper,c2av-stream-
processor,enrichment-processor,kafka-manager,c2av-
esmprocessor,routing-processor,ceb,searchmanager-engine,interset-
api,interset-analytics,intelligence-tuning-api,hdfs-namenode,hdfs-
datanode,interset-logstash,arcsightconnector-api,soar-alert-
dispatcher,visualization-api-service,fusion-tenant-lifecycle-manager
```

```
kubectl delete pods -n $ARCSIGHT_NS -l "name in (suite-reconf-sel-
arcsight-installer)"
```

```
kubectl delete pods -n $ARCSIGHT_NS -l "app in ($labels)"
```

> Some pods may not return to running state after restart due to the certificate change while trying to connect to database. For example, `intelligence-tuning-api`, `interset-analytics`, and `interset-api`. These pods should return to running state once you update database certificates.

b. (Conditional) Run the following command only if Multi-tenancy is enabled:

```
ARCSIGHT_NS=$(kubectl get namespaces --no-headers -o custom-
columns=":metadata.name" | grep arcsight-installer)
SOAR_WEB_APP_PODS=$(kubectl get pods -n $ARCSIGHT_NS --no-headers |
awk '{if ($1 ~ "soar-web-app") print $1}')
kubectl delete pods -n $ARCSIGHT_NS $SOAR_WEB_APP_PODS
```

2. Update the ArcSight Platform's embedded reverse proxy `Nginx` to use the updated RE external communication certificate chain, by running the commands below:

   a. Change the directory:

      - For a cloud deployment, run:

```
cd <path to OMT installer>/cdf-deployer/scripts/
```

   b. Run the `cdf-updateRE` script:

```
./cdf-updateRE.sh renewPortals
```

3. (Conditional) If you deployed the ArcSight Database, update the ArcSight Database to use the updated RE external communication certificate by following the instructions in Configuring the ArcSight Database to Use the Updated RE External Communication Certificate.

Create or Update Route 53 Certificates (AWS Only)

A user-provided self-signed or CA-signed certificate is required for creating the Application Load Balancer (ALB). In this section, you will:

- Create a configuration file for the certificate signing request (CSR)
- Sign the CSR
- Create a chained file for import
- Import the self-signed certificate into Amazon Certificate Manager (ACM)

1. Create or update Route 53 certificates:
   a. Run the applicable command on a secure machine to generate the Route 53 certificate:
      - For a current version of SSL, run this command:

```
openssl req -nodes -newkey rsa:2048 -keyout
<your.route53dnsRecordsetName>.key.pem -out
<your.route53dnsRecordsetName>.csr.pem -subj
"/C=US/ST=State/L=City/O=Company
Inc./OU=IT/CN=<your.route53dnsRecordsetName>" -addext
"subjectAltName = DNS:<your.route53dnsRecordsetName>"
```

      - If your operating system does not support `-addext` for SSL, run this command:

```
openssl req -newkey rsa:2048 -sha256 -nodes -keyout
your.route53dnsRecodsetName.key.pem -out
your.route53dnsRecodsetName.csr.pem -subj
"/C=US/ST=CA/L=SU/O=MF/OU=IT/CN=<your.route53dnsRecordsetName>" -
extensions san -config <(echo '[req]'; echo 'distinguished_
name=req';echo 'req_extensions=san';echo '[san]'; echo
'subjectAltName=DNS:your.route53dnsRecodsetName')
```

> `your.route53dnsRecordsetName` is your route53 record set name tracked in your AWS configuration worksheet. This command will create the private key file `<your.route53dnsRecordsetName>.key.pem` and the certificate signing request file `<your.route53dnsRecordsetName>.csr.pem`.

   b. Copy the certificate signing request `<your.route53dnsRecordsetName>.csr.pem` to your bastion or jump host machine.
   c. Run the following commands to sign the certificate signing request using your cluster RE certificate:

```
export COMMON_NAME=<your.route53dnsRecordsetName>
```

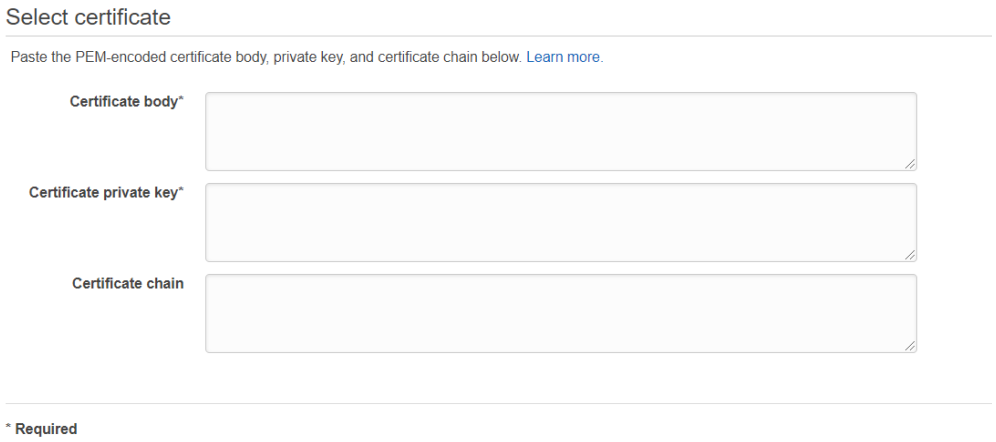
```
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o
json 2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n
core -o json 2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-
cbc -md sha256 -a -d -pass pass:"${PASSPHRASE}")
```

```
export CSR=$(cat ${COMMON_NAME}.csr.pem)
```

```
export WRITE_RESPONSE=$(kubectl exec -it -n core ${VAULT_POD} -c vault
-- bash -c "VAULT_TOKEN=$VAULT_TOKEN vault write -tls-skip-verify -
format=json RE/sign/coretech csr=\"${CSR}\"") && \
echo ${WRITE_RESPONSE} | jq -r ".data | .certificate" > ${COMMON_
NAME}.signed.crt.pem && \
echo ${WRITE_RESPONSE} | jq -r ".data | if .ca_chain then .ca_chain[]
else .issuing_ca end" > ${COMMON_NAME}.ca_chain.pem
```

The RE signed certificate is in file `${COMMON_NAME}.signed.crt.pem`. The certificate chain is in file `${COMMON_NAME}.ca_chain.pem`.

2. Import or update the certificate in Amazon Certificate Manager (ACM).
   a. Import the self-signed certificate into ACM (for a fresh installation):
      i. Log in to the AWS Console.
      ii. Browse to the Amazon Certificate Manager (ACM).
      iii. Click **Import a certificate**, and then complete the fields as follows:
         - **Certificate body:** Specify the contents of the signed certificate you created earlier. For example, `<your.route53dnsRecordsetName>.crt.pem`
         - **Certificate private key:** Specify the contents of the private key created by the CSR request creation. For example, `<your.route53dnsRecordsetName>.key.pem`
         - **Certificate chain:** Specify the contents of the chain file. For example, `<your.route53dnsRecordsetName>.ca.pem`



   b. To update the certificate in ACM (for a current running installation):
      i. Log in to the AWS Console.
      ii. Browse to the Amazon Certificate Manager (ACM).

iii. Search for your certificate Domain name or ID.

iv. Select your Certificate ID, and click **Reimport**.

v. Complete the fields as follows:

- **Certificate body:** Specify the contents of the new signed certificate you created earlier. For example, `<your.route53dnsRecordsetName>.crt.pem`
- **Certificate private key:** Specify the new contents of the private key created by the CSR request creation. For example, `<your.route53dnsRecordsetName>.key.pem`
- **Certificate chain:** Specify the new contents of the chain file. For example, `<your.route53dnsRecordsetName>.ca.pem`

For more details, see https://docs.aws.amazon.com/acm/latest/userguide/import-reimport.html

3. Click **Next**. Optionally, add any tags you wish to the import.
4. Click **Next**, and then, click **Import**.

   After the import, click the arrow next to the certificate ARN value. Note the value to your AWS worksheet for later use. For example:

Imported at	2021-04-01T00:11:48UTC
Not after	2022-04-11T00:06:47UTC
Expires in	374 Days
Public key info	RSA 2048-bit
Signature algorithm	SHA256WITHRSA
ARN	arn:aws:acm:us-west-2:115370848038:certificate/9a03c730-0923-4b2d-8a0d-ea7868917377
Validation state	None

Configuring the ArcSight Database to Use the Updated RE External Communication Certificate

If you deployed the ArcSight Database with your platform, you need to follow these instructions to update the RE External communication certificate.

1. Run these commands on your database node1 to generate the Kafka Scheduler private key file `kafkascheduler.key.pem` and the certificate signing request file `kafkascheduler.csr.pem`:

```
cd <yourOwnCertPath>/
```

> If you installed using the ArcSight Platform Installer, the default location is `/opt/arcsight-db-tools/cert/`

```
rm -fr kafkascheduler.*.pem issue_ca* *.0
```

```
openssl req -nodes -newkey rsa:2048 -keyout kafkascheduler.key.pem -out
kafkascheduler.csr.pem -subj "/C=US/ST=State/L=City/O=Company
Inc./OU=IT/CN=kafkascheduler"
```

2. Copy the certificate signing request `kafkascheduler.csr.pem` to your cluster or your bastion or jump host.
3. Run the following commands on your cluster or your bastion host to sign the certificate signing request using your cluster RE certificate:

```
export VAULT_POD=$(kubectl get pods -n core -o custom-
columns=":metadata.name"| grep itom-vault)
export PASSPHRASE=$(kubectl get secret vault-passphrase -n core -o json
2>/dev/null | jq -r '.data.passphrase')
export ENCRYPTED_ROOT_TOKEN=$(kubectl get secret vault-credential -n core
-o json 2>/dev/null | jq -r '.data."root.token"')
export VAULT_TOKEN=$(echo ${ENCRYPTED_ROOT_TOKEN} | openssl aes-256-cbc -
md sha256 -a -d -pass pass:"${PASSPHRASE}")
```

```
export COMMON_NAME=kafkascheduler
export CSR=$(cat ${COMMON_NAME}.csr.pem)
```

```
WRITE_RESPONSE=$(kubectl exec -it -n core ${VAULT_POD} -c vault -- bash -
c "VAULT_TOKEN=$VAULT_TOKEN vault write -tls-skip-verify -format=json
RE/sign/coretech csr=\"${CSR}\"") && \
echo "${WRITE_RESPONSE}" | jq -r ".data | .certificate" > ${COMMON_
NAME}.crt.pem && \
echo "${WRITE_RESPONSE}" | jq -r ".data | if .ca_chain then .ca_chain[]
else .issuing_ca end" > issue_ca.crt
```

4. Copy the RE signed certificate file `kafkascheduler.crt.pem` and certificate chain file `issue_ca.crt` to database node1 <*yourOwnCertPath*>.
5. Update the Database SSL Configuration.
   a. If you have not already done so, move the following files to database node1 <*yourOwnCertPath*> as root:

```
cd <yourOwnCertPath>/
ls <yourOwnCertPath>/
```

The output should have the following files:

- `generated-db-ca.crt`
- `generated-db-server.crt`
- `generated-db-server.key`
- `generated-db-ca.key`
- `generated-db-ca.srl`
- `generated-db-server.csr`
- `issue_ca.crt`
- `kafkascheduler.crt.pem`
- `kafkascheduler.key.pem`

> If you have not set up the database for SSL mode before and you want to enable SSL now, you may need to generate `generated-db-*.*`. To do so, continue with substeps 5. b-c. Otherwise, skip to Step 6.

b. For chained CAs, run these commands to split the CAs into individual files:

```
cat issue_ca.crt | awk 'BEGIN {c=0;} /BEGIN CERT/{c++} { print >
"issue_ca_part." c ".crt"}'
```

```
chown -R dbadmin:dbadmin <yourOwnCertPath>
```

c. (Conditional) If your database is SSL enabled, run the following commands on database node1 to update the database SSL configuration:

```
cd /opt/arcsight-db-tools
```

```
./db_ssl_setup --disable-ssl
```

NOTE: If the attempt fails, drop the certificate manually by running these commands:

```
sudo su - dbadmin
```

```
vsql -U <dbadminuser> -w <dbadminpassword> -c "ALTER TLS CONFIGURATION
server CERTIFICATE NULL;"
```

```
vsql -U <dbadminuser> -w <dbadminpassword> -c "DROP CERTIFICATE IF
EXISTS server CASCADE;"
```

i. Enable database SSL for a single issue CA or chained issue CAs:

- For a single issue CA, run this command:

```
./db_ssl_setup --enable-ssl --vertica-cert-path
<yourOwnCertPath>/generated-db-server.crt --vertica-key-path
<yourOwnCertPath>/generated-db-server.key --vertica-ca-path
<yourOwnCertPath>/generated-db-ca.crt --client-ca-path
<yourOwnCertPath>/issue_ca.crt
```

-or-

- For chained issue CAs, run this command, specifying each CA certificate in the chain one by one, separated by a comma in the `client-ca-path` parameter:

```
./db_ssl_setup --enable-ssl --vertica-cert-path
<yourOwnCertPath>/generated-db-server.crt --vertica-key-path
<yourOwnCertPath>/generated-db-server.key --vertica-ca-path
<yourOwnCertPath>/generated-db-ca.crt --client-ca-path
<yourOwnCertPath>/issue_ca_part.1.crt,
<yourOwnCertPath>/issue_ca_part.2.crt[,...]
```

6. Update the Kafka Scheduler configuration.

a. On database node1, stop the Kafka Scheduler:

```
cd /opt/arcsight-db-tools/
./kafka_scheduler stop
```

b. Run the following command on database node1 to configure the schema registry server setting:

```
./schema_registry_setup <FQDN of ArcSight Platform Virtual IP for HA
or single master node> <yourOwnCertPath>/issue_ca.crt
<yourOwnCertPath>/kafkascheduler.crt.pem
<yourOwnCertPath>/kafkascheduler.key.pem
```

c. (Conditional) If the Kafka Scheduler and database are both SSL enabled, update the Kafka Scheduler SSL setup:

i. On database node1, delete the Kafka Scheduler:

```
cd /opt/arcsight-db-tools/
./kafka_scheduler delete
```

ii. On all database nodes, remove the existing Kafka Scheduler SSL configuration.

```
rm -fr /opt/arcsight-db-tools/ssl_default /opt/arcsight-db-
tools/wrk
```

iii. On database node1, configure the SSL setting for the Kafka Scheduler.

This method uses the crt and key files gathered or generated in earlier steps. The `issue_ca.crt` file should contain all chained CAs. For the Kafka Scheduler to use SSL, run the following command:

```
./sched_ssl_setup --enable-ssl --sched-cert-path
<yourOwnCertPath>/kafkascheduler.crt.pem --sched-key-path
<yourOwnCertPath>/kafkascheduler.key.pem --vertica-ca-key
<yourOwnCertPath>/generated-db-ca.key --vertica-ca-path
<yourOwnCertPath>/generated-db-ca.crt --kafka-ca-path
<yourOwnCertPath>/issue_ca.crt
```

iv. Run the following command on database node1 to create the Kafka Scheduler:

```
./kafka_scheduler create <aks_nodename1>:9093,<aks_
nodename2>:9093,<aks_nodename3>:9093
```

7. Start the Kafka Scheduler and checker on database node1:

```
./kafka_scheduler start
./kafka_scheduler messages
./kafka_scheduler events
```

Maintaining Certificates

Certificates and their Certificate Authority (CA) have an expiration date; therefore, they need to be renewed prior to expiring in order for the cluster to operate properly.

To better understand the CAs in the cluster, see "Method 1 - Signing the RE External Communication Certificate with Your Trusted Certificate Authority" on page 512

> In this section, `$<CDF_HOME>` refers to:
>
> Cloud: `$<OMT-deployer path>`

- "Viewing the CA Validity Dates" on the next page
- "Renewing Internal CAs" on the next page
- "Renewing External CAs" on page 526

Viewing the CA Validity Dates

Review the content below for information about viewing CA validity dates.

- Internal CA (RIC and RID CA) is reported in the beginning of each `kube-status` run with time/date and days remaining till expiration.
- To view the external CA (RE CA) validity dates, execute the following command:
  - On the jump host or bastion for a cloud deployment

```
${CDF_HOME}/scripts/cdf-updateRE.sh read | openssl x509 -noout -issuer -subject -dates
```

Renewing Internal CAs

> This information for is for pod communication within the cluster and not for certificates used for external pod communication.
>
> To check if your Internal Certificate Authority is close to expiration, login into the OMT Management Portal, which will show a warning if less than 30 days are left till expiration.
>
> Alternatively, you can run the `kube-status.sh` script from `/opt/arcsight/kubernetes/bin` (installation path by default). Expiration date will be reported as the first line in the script output.

To renew internal CAs and dependent certificates:

1. Execute `renewCert`. This action also distributes the renewed CA between the nodes.

```
${CDF_HOME}/scripts/renewCert --renew -t internal -V 730
```

2. Follow the on-screen prompts to:
   a. Generate new certificates.
   b. Distribute them between the nodes using `scp`.
   c. Apply certificates by restarting nodes one by one.

Renewing External CAs

> This procedure updates the certificates used by the OMT Management Portal as well as ArcSight capabilities. Changing the certificate by way of the OMT Management Portal, **Administration > Certificate**, only changes the certificate used by the OMT Management Portal.

To renew external CAs, request that your PKI team generates an intermediate certificate and matching key. Be sure to obtain any higher root certificate authority or a whole chain if more that one level used.

If you cannot get a key from your PKI team, see "Using an RE External Communication Certificate Signed by Your Trusted Certificate Authority" on page 512.

1. Execute `cdf-updateRE.sh`.

   ```
   ${CDF_HOME}/scripts/cdf-updateRE.sh write --re-key={New Intermediate Key Name}.pem --re-crt={New Intermediate Certificate Name}.crt
   ```

   > If your intermediate certificate is signed by a higher root certificate authority, provide a chain of root CA certificate and intermediate certificate concatenated in one file (keeping the headers) to the "re-crt" parameter. Make sure the intermediate certificate is first in the file, and the root CA certificate is last in the file.

2. Pods of the deployed ArcSight capabilities that perform external communication continue to use the certificates generated by the platform on the pod start up until the pod is restarted.

   > To understand the pods that perform external communication, see "Understanding Labels and Pods" on page 453.

Renewing External Certificate of Management Portal and Core Single-Sign-On Portal

To renew the certificate for portals:

1. Log in to database node1.
2. Follow these steps to stop the Kafka Scheduler and Watchdog:
   a. Change to the database tools directory:

      ```
      cd /opt/arcsight-db-tools
      ```

   b. Stop the Kafka Scheduler:

```
./kafka_scheduler stop
```

c. Disable watchdog:

```
scripts/watchdog.sh disable
```

3. Restart the ArcSight pods:

```
kubectl delete pods --all -n $(kubectl get namespaces --no-headers -o
custom-columns=":metadata.name" | grep arcsight-installer)
```

4. Run this command to update the `nginx` certificate:

```
${CDF_HOME}/scripts/cdf-updateRE.sh renewPortals
```

> The second command generates the `nginx` certificate and updates the `nginx-invesitgate-secret` and `nginx-default-secret`.

5. Continue to the next step to update the database certificates: Configuring the ArcSight Database to Use the Updated RE External Communication Certificate.

Diagnose and Repair the OMT Infrastructure (CDF Doctor Utility)

The CDF Doctor utility, supported for both Off-cloud and BYOK OMT installations, can be used to diagnose and repair OMT and CDF (previous version of the OMT) issues. You can request a newer version of CDF Doctor through OpenText Support channels to have enhanced diagnostic and logging capabilities.

CDF Doctor is located at `{CDF_HOME}/tools/cdf-doctor`.

Running CDF Doctor

For maximum visibility into issues, run CDF Doctor on each problematic node.

To run the CDF Doctor on a problematic node:

1. Enter the following commands:
```
cd $CDF_HOME/tools/cdf-doctor/
./cdf-doctor cluster check
```

2. When prompted for login credentials:
   a. For username use `admin`
   b. For password, use your password for the OMT management portal (that is, at `https://<your high availability FQDN>:5443`)

> You can run CDF Doctor on a failed master node by adding the `--master` parameter to the `cluster check` run command.

Types of Diagnostic Checks

When run, CDF Doctor will perform an array of diagnostic checks by default. Some checks permit CDF Doctor to repair an issue as soon as it is detected. Default diagnostic checks run by CDF Doctor will check the following components.

- OMT components
- Kube-system (`etcd`)

Default diagnostic checks are compatible with all CDF and OMT versions 2020.08 and later.

Component	Checks...
Container Runtime	Container Runtime status
`kubelet`	• `kubelet` status • whether policy is loaded when SELinux is enforcing • whether `kubelet` runtime data directory is missing • whether `kubelet` certificate files's permission is incorrect • whether `kubelet` certificate is expired • whether swap is off • whether swap is enabled
`Etcd`	`etcd` status
`cdf-apiserver`	`cdf-apiserver` status
`dashboard`	`dashboard` status
`db-backup`	`db-backup` status
`idm`	`idm` status
`mng-portal`	`mng-portal` status
`nginx-ingress`	`nginx-ingress-controller` status
`node`	cluster node status

Component	Checks...
pv	persistent volume status
registry	registry status
suite-config	FQDN in suite-conf-cm- FQDN in suite-conf-ing- FQDN in suite-conf-pod-
suite-frontend-ingress	suite-frontend-ingress status
suite-frontend-ui	suite-frontend-ui status
suite-update	• FQDN in suite-upgrade-cm- • FQDN in suite-upgrade-ing-
Vault	• Vault component status • whether node NTP service is enable and synced • cluster nodes time difference • suite metadata folder permission • whether vault policy incorrect (automated fix) • whether pullsecret exists • whether can login to registry • whether registry contains jdbc image • FQDN in nginx-ingress-controller deployment • FQDN in idm deployment and ingress • whether suite parameter file is missing • PV info in suite parameter file (fix provided after user confirmation) • FQDN in ingress • FQDN in mng-portal deployment and ingress • FQDN in frontend-ingress deployment • check FQDN in suite-installer-frontend deployment • FQDN in itom-k8s-dashboard deployment and ingress • FQDN in itom-pg-backup-config configmap • FQDN in itom-ingress-pg-backup ingress

Dump File

The dump file provides a quick way to gather information about nodes where OMT is deployed. The file can be used to quickly gather and encrypt information to provide for support investigation of issues.

To generate a dump file with check results, run CDF Doctor with the `--encrypt-password` parameter. You can also provide a username and password to get additional dump data from the OMT Management Portal.

The dump file contains the following information:

File Section	Description
OS commands output	Refer to `$CDF_HOME/tools/support-tool/conf/supportdump.config`
Directory content	Refer to `$CDF_HOME/tools/support-tool/conf/supportdump.config`
Files content	Refer to `$CDF_HOME/tools/support-tool/conf/supportdump.config`
Kube-Info	• CRI version and installation status • `kubelet` version and Installation status • Current node infomation Current node information: • Containers on current node • Container images on current node's docker runtime Cluster info: • namespace, pv, pvc, nodes, deployment, service,pod,ingress Pod container information: • pod name • pod namespace • node pod is running on • images pod uses Suite info: • manage portal accessibility • selected features Deployment information • CRI journal logs • Container images details collected from Docker inspection • cluster dump info collected from `kubectl` cluster dump • pod description • suite-db data • suite metadata

Managing the ArcSight Database

This section provides information about managing the ArcSight database.

Monitoring the ArcSight Database

You can monitor the ArcSight Database by using commands, or the out-of-the-box Health and Performance Monitoring dashboard included in the component.

- "Understanding the ArcSight Database Watchdog" below
- "Monitoring the ArcSight Database Status" below
- "Monitoring Scheduler Status, Events, and Messages" below
- "Using the Health and Performance Monitoring Dashboard" on the next page
- "Removing Rejected Events" on the next page

Understanding the ArcSight Database Watchdog

The ArcSight Database includes a watchdog, which is configured as a cron job to automatically run once an hour to monitor the database and perform the following operations:

- When it detects a database cluster node is in down state, it will try to restart the node.
- Create the database event ingestion process (Kafka Scheduler) if it is missing.
- Start the database event ingestion process (Kafka Scheduler) if it is stopped.
- Unless there is a policy in place, do not use watchdog to delete reject events.

Monitoring the ArcSight Database Status

Monitor the ArcSight database status by using the following command:

```
/opt/arcsight-db-tools/db_installer status
```

Monitoring Scheduler Status, Events, and Messages

Monitor the scheduler's status by using the following command:

```
/opt/arcsight-db-tools/kafka_scheduler status
```

Monitor scheduler events by using the following command:

```
/opt/arcsight-db-tools/kafka_scheduler events
```

Monitor scheduler messages by using the following command:

```
/opt/arcsight-db-tools/kafka_scheduler messages
```

Using the Health and Performance Monitoring Dashboard

You can also monitor the status of the ArcSight database by using the out-of-the-box Health and Performance Monitoring dashboard included in the component. The dashboard includes the following widgets.

Database Event Ingestion Timeline

The Database Event Ingestion Timeline widget represents the rate of event ingestion into the ArcSight database. This widget measures when the database receives the event data.

As a SOC Manager or an IT Administrator you want to monitor the event ingestion rate into the database. Due to differences in how quickly an event from different sources arrive at the database for storage, the moment when a database stores an event differs from when the event occurred. In this widget, you can monitor when the database receives the event data.

In the Database Event Ingestion widget, you can set the Upper and Medial Threshold values. Yellow represents the EPS values occurring in between the Medial and Upper Thresholds, and red represents the values occurring above the Upper Threshold. Green represents the EPS values occurring below the Medial Threshold.

Removing Rejected Events

For default tenants, use this procedure to ensure there are no rejected events. If `/opt/vertica/data/fusiondb/v_fusiondb_node000*_data/RejectionTableData` is not empty, then reject event exists and you need to take action immediately.

A high volume of rejected events impacts the query performance and occupies disk space, which retention policy cannot reduce. The rejected events will continue to occur until the root cause is resolved.

> If you are using watchdog to delete rejected events, be sure a policy is in place, such as *if the reject events utilization is > 1% of the storage then delete the reject events*.

1. Analyze the content of reject_event_file to determine the root cause or save the reject_event_file for further analysis. Without resolving the root cause, the reject event creation will continue.
2. Delete reject events after completed analysis by using the following command:

```
rm -rf /opt/vertica/data/fusiondb/v_fusiondb_node000*_
data/RejectionTableData*
```

Understanding the ArcSight Database Installer Options

To specify an option:

Type `./db_installer <Option_Name>`.

Option Name	Description
install	Installs the ArcSight database
uninstall	Uninstalls the ArcSight database and deletes data and users
create-schema	Creates the database schema for Recon/ Intelligence
delete-schema	Deletes the Recon/ Intelligence database schema
start-db	Starts the database with the `dba_password` specified in `db_credentials.properties`
stop-db	Stops the database
status	Prints the database cluster status

Configuring the Policy for Retaining Data

ArcSight Platform allows you to configure a policy for retaining raw events in the ArcSight database. The policy for retaining data uses a script, which runs in the primary database node.

Consider the following example to understand how the policy for retaining data works:

If you run the data retention script on 6/30/2019 and the data retention period is set as 90 days, then data older than 04/01/2019 will be deleted.

Configuring Data Retention with Recon and Intelligence Deployed

- "Configuring Analytics Data Retention" below
- "Configuring Event Data Retention" on the next page

Configuring Analytics Data Retention

In Intelligence, you can set a desired event retention period, which should range from 1 to 365 days.

To set the event retention period:

1. In the OMT Management Portal, select **Deployment** > **Deployments**.
2. Click ... (Browse) on the far right and choose **Reconfigure**. A new screen will be opened in a separate tab.

3. Click **Intelligence**.
4. Under **Analytics Configuration**, specify the value for **Analytics Data Retention Period**.

   Note: The default value for **Analytics Data Retention Period** is 90 days.

5. Click **Save**.

Deleting Old Data

For information about deleting old data, see **Delete Old Data** in the User's Guide for ArcSight Platform 24.2.

Configuring Event Data Retention

For information about using storage groups to organize and retain data, follow the *Use Storage Groups to Organize and Retain Data* section in the User's Guide for ArcSight Platform 24.1.

Configuring Event Retention with Only Intelligence Deployed

- "Configuring Analytics Data Retention" below
- "Configuring Event Data Retention" below

Configuring Analytics Data Retention

In Intelligence, you can set a desired event retention period, which should range from 1 to 365 days.

To set the event retention period:

1. In the OMT Management Portal, select **Deployment** > **Deployments**.
2. Click ... (Browse) on the far right and choose **Reconfigure**. A new screen will be opened in a separate tab.
3. Click **Intelligence**.
4. Under **Analytics Configuration**, specify the value for **Analytics Data Retention Period**.

   Note: The default value for **Analytics Data Retention Period** is 90 days.

5. Click **Save**.

Configuring Event Data Retention

To enable event retention when only Intelligence is deployed:

1. Login to the primary ArcSight database node.
2. Use a `vsql` or `db sql` tool of your choice and run the following query:

```
update default_secops_adm.storage_groups set deleteAfter = <number_of_
month_to_keep>;  commit;
```

> **Note**: In the above query, replace `<number_of_month_to_keep>` by a desired value, which should be greater than 0 or -1.
> The default value for `<number_of_month_to_keep>` is -1, which stores the events forever.

Setting the Maximum Number of Storage Groups for Tenants

Available only when the Multi-tenancy feature is enabled.

Storage groups in the ArcSight Database allow your tenants to partition the incoming event data based on a query filter per storage group. Each storage group can have a specific retention period policy, allowing tenants to retain certain high volume events for a short time period and other important events for longer time periods. After you enable the multi-tenancy feature, the system automatically creates a *Default Storage Group* for each tenant. You can then specify the maximum number of additional storage groups that each tenant can create.

Before you allow more than the *Default Storage Group*, consider the number of tenants and events that your system might ingest. If you let tenants create custom storage groups, you must consider the impact that the additional groups would have on the stability of data ingestion for the system. Also consider how the additional storage needs will affect your hardware configuration. Higher volumes of event data require more storage space. By default, the maximum time allowed for retaining events in the *Default Storage Group* is 12 months. However, the license for your deployed product might require a lower maximum value, such as 30 days. For guidance on revising your system's configuration, please contact OpenText Customer Care.

> Reducing the maximum number of storage groups will not affect the groups already created. For example, if you have four storage groups, then change the limit to two, you continue to have the four storage groups. However, you will not be able to create any new groups.

To change the maximum number of storage groups:

1. Browse to the OMT Management Portal.
2. Select **DEPLOYMENT** > **Deployments**.
3. In the **Three Dots** menu, select **Reconfigure**.
4. In the left navigation page, click **Infrastructure** > **Database**.

5. In the main panel, specify a value for **Maximum Number of Storage Groups per Tenant**.

   The minimum value is one, representing the *Default Storage Group*.

To create storage groups, log in to ArcSight Platform, then view Use Storage Groups to Organize and Retain Data in the Help.

Rebooting the ArcSight Database Cluster

1. Log in to ArcSight Database node 1.

```
cd /opt/arcsight-db-tools
```

2. Run the following command to disable the watchdog:

```
./scripts/watchdog.sh disable
```

3. Run the following command:

```
./db_installer stop-db
```

4. Reboot all cluster nodes.
5. Log in to ArcSight Database node 1.

```
cd /opt/arcsight-db-tools
```

6. Run the following command:

```
./db_installer start-db
```

7. Execute the following command:

```
./kafka_scheduler start
```

8. Enable the watchdog again with the following command:

```
./scripts/watchdog.sh enable
```

Configuring the ArcSight Database for MinIO Storage (Examples Only)

Note: The information on this page is provided for illustrative purpose only, is not verified for production use, and no support is provided by OpenText for this information. Please utilize MinIO official support resources to assist you with deploying and configuring MinIO.

The setup examples below incorporated MinIO version Release.2021-10-13T00-23-17Z.

The procedures in this section for setting up the MinIO storage solution using MinIO Gateway in NFS mode are for example purposes only. Additionally, the procedures are not necessarily contiguous and provide more than one way of configuring MinIO. For example, the type of certificate used or setting up with or without TLS.

As you proceed with your own MinIO setup, ensure that you thoroughly run the processes that you configure in a test environment before deploying to your operational system. For more information, see "Understanding Object Storage Options for the ArcSight Database" on page 41.

Server addresses and the like are from our test environment and should not be taken literally.

- Configuring the ArcSight Database for MinIO Storage (Examples Only)
- Setting Up MinIO Using a TLS-Signed Certificate
- Setting Up MinIO Using a TLS Self-Signed Certificate
- Creating a Bucket and Folder in MinIO
- Yaml Configuration File Example
- Configuring MinIO TLS Mode for ArcSight Database Back Up and Restore
- Configuring the ArcSight Database for Backup

Setting Up MinIO - Non-TLS

Example for setting up MinIO without TLS on the NFS server.

1. Log in to the MinIO Server and create the `start-minio.sh` script:

```
start-minio.sh
```

```
#!/bin/bash

MINIO_DIR=/opt/minIO
```

```
DATA_DIR=$MINIO_DIR/data

mkdir -p $DATA_DIR
chown -R 1999:1999 $DATA_DIR

echo ========================================
echo "$DATA_DIR has been created"
echo "Data will be placed in $DATA_DIR"
echo "Check output for more information"
echo ========================================

export MINIO_ROOT_USER=minio-user
export MINIO_ROOT_PASSWORD=change_me

./minio server $DATA_DIR --console-address :42497 &
```

Port 42497 is an example. You need to configure your own unused port. You also need to get your own Minio binary code.

2. Run the `start.minio.sh` script:

```
./start.minio.sh
```

Output example:

```
Output:
========================================
/opt/minIO/data has been created
Data will be placed in /opt/minIO/data
Check output for more information
========================================
```

```
API: http://10.000.000.000:9000 http://192.168.122.1:9000
http://127.0.0.1:9000
RootUser: access_key
RootPass: change_me
```

```
Console: http://10.000.000.001:42497 http://192.168.122.1:42497
http://127.0.0.1:42497
RootUser: access_key
RootPass: change_me
```

```
Command-line: https://docs.min.io/docs/minio-client-quickstart-guide
$ mc alias set myminio http://10.000.000.001:9000 access_key change_me
```

```
Documentation: https://docs.min.io
```

3. Create the `stop-minio.sh` script:

```
stop-minio.sh
```

```
#!/bin/bash

MINIO_DIR=/opt/minIO
DATA_DIR=$MINIO_DIR/data

ps -ef | grep minio | awk '{print $2}' | xargs kill -9

echo ========================================
echo "$DATA_DIR still contains data"
echo "Clean them if needed"
echo "rm -rf $DATA_DIR"
echo ========================================
```

4. Run the `stop-minio.sh` script:

```
./stop-minio.sh
```

Output example:

```
Output:

========================================
/opt/minIO/data still contains data
Clean them if needed
rm -rf /opt/minIO/data
========================================
```

Setting Up MinIO Using a TLS-Signed Certificate

Example for configuring a TLS-signed certificate for MinIO.

1. Log in to the MinIO server and create the Sign-CA directory:

```
mkdir Sign-CA
cd Sign-CA
```

2. Generate the self-signed certificate:

```
openssl req -newkey rsa:4096 -sha256 -keyform PEM -keyout ca.key -x509 -
days 3650 -outform PEM -out ca.crt -subj
"/C=<country>/ST=<state>/L=<locality>/O=<organization>/OU=<organizational
unit>/CN=RootCA/emailAddress=<admin@myCompany.com>" -nodes
```

3. Generate a private key for MinIO:

```
openssl genrsa -out private.key 4096
```

4. Update the MinIO server's IP address and FQDN:

```
create openssl.conf ### Update minio server's IP and FQDN
[req]
distinguished_name = req_distinguished_name
x509_extensions = v3_req
prompt = no
```

```
[req_distinguished_name]
C = <country>
ST = <XX>
L = <locality>
O = <organization>
OU = <organizational unit>
CN = <fqdn>
[v3_req]
subjectAltName = @alt_names
[alt_names]
IP.1 = <IP-address>
DNS.1 = <fqdn>
```

5. Create the MinIO signing request:

```
#minio server IP: 10.000.000.001
```

```
openssl req -new -key private.key -out minio.csr -config openssl.conf -
nodes
```

6. Sign the CSR:

```
openssl x509 -req -in minio.csr -CA ca.crt -CAkey ca.key -CAcreateserial
-extensions server -days 3650 -outform PEM -out public.crt -sha256 -
extensions v3_req -extfile openssl.conf
```

7. Run the `start-minio.sh` script:

```
./start-minio.sh
```

```
cp public.crt private.key /root/.minio/certs
cp ca.crt /root/.minio/certs/CAs
```

8. Stop and restart MinIO:

```
./stop-minio.sh
```

```
./start-minio.sh
```

Example output:

```
Output:
========================================
/opt/minIO/data has been created
Data will be placed in /opt/minIO/data
Check output for more information
========================================
[root@n10-000-000-h001 minio]#
```

```
API: https://10.000.000.001:9000 https://192.168.122.1:9000
https://127.0.0.1:9000
RootUser: access_key
RootPass: change_me
```

```
Console: https://10.000.000.001:42497 https://192.168.122.1:42497
https://127.0.0.1:42497http://127.0.0.1:42497
RootUser: access_key
RootPass: change_me
```

```
Command-line: https://docs.min.io/docs/minio-client-quickstart-guide
$ mc alias set myminio http://10.000.000.000:9000 access_key change_me
```

```
Documentation: https://docs.min.io
```

9. Connect to the ArcSight database server:

```
scp ca.crt <All-database-nodes>:/tmp
```

10. Run this command on all ArcSight database nodes:

```
cp /tmp/ca.crt /etc/pki/ca-trust/source/anchors;update-ca-trust
```

Setting Up MinIO Using a TLS Self-Signed Certificate

Example for setting up MinIO without TLS self-signed certificate/

1. Log in to the MinIO server and create the self-sign directory:

```
mkdir self-sign
cd self-sign
```

2. Update the MinIO server's IP address and FQDN:

```
create openssl.conf ### Update minio server's IP and FQDN
[req]
distinguished_name = req_distinguished_name
x509_extensions = v3_req
prompt = no
```

```
[req_distinguished_name]
C = <country>
ST = <XX>
L = <locality>
O = <organization>
OU = <organizational unit>
CN = <fqdn>
```

```
[v3_req]
subjectAltName = @alt_names
```

```
[alt_names]
IP.1 = <IP-address>
DNS.1 = <fqdn>
```

3. Generate the self-signed certificate:

```
openssl req -newkey rsa:4096 -sha256 -keyform PEM -keyout private.key -
x509 -days 3650 -outform PEM -out public.crt -config openssl.conf -nodes
```

4. Run the `start-minio.sh` script:

```
./start-minio.sh
```

```
cp public.crt private.key /root/.minio/certs
cp public.crt /root/.minio/certs/CAs
```

5. Stop and restart MinIO:

```
./stop-minio.sh
```

```
./start-minio.sh
```

Example output:

```
Output:
========================================
/opt/minIO/data has been created
Data will be placed in /opt/minIO/data
Check output for more information
```

```
========================================
[root@n10-000-000-h001 minio]#
```

```
API: https://10.000.000.001:9000 https://192.168.122.1:9000
https://127.0.0.1:9000
RootUser: access_key
RootPass: change_me
```

```
Console: https://10.000.000.001:42497 https://192.168.122.1:42497
https://127.0.0.1:42497http://127.0.0.1:42497
RootUser: access_key
RootPass: change_me
```

```
Command-line: https://docs.min.io/docs/minio-client-quickstart-guide
$ mc alias set myminio http://10.000.000.000:9000 access_key change_me
```

```
Documentation: https://docs.min.io
```

6. Connect to the ArcSight database:

```
scp public.crt <All-database-nodes>:/tmp
```

7. Run this command on all ArcSight database nodes:

```
cp /tmp/public.crt /etc/pki/ca-trust/source/anchors;update-ca-trust
```

Creating a Bucket and Folder in MinIO

These are the basic steps for creating a bucket and folder in MinIO:

1. Log in to the MinIO console. For example:
   a. Enter the console address in a browser. For example (http://10.000.000.000:42497).
   b. Enter MinIO credentials (access key and password).
2. Create the bucket.

> To see how the Yaml configuration corresponds to the MinIO bucket, see Yaml Configuration File Example

Yaml Configuration File Example

The following is an example of the Yaml configuration file used for the MinIO setup. For more information, see Using the Configuration Files.

Non-TLS:

```
s3:
 type: preconfigured
 server: <fqdn>
 port: 9000
 url: s3://<bucketName>/<folderName>
 access-key: <access_key>
 tls-enabled: False
 region: <region>
```

TLS:

```
s3:
 type: preconfigured
 server: <fqdn>
 port: 9000
 url: s3://<bucketName>/<folderName>
 access-key: <access_key>
 tls-enabled: True
 region: <region>
```

Configuring MinIO TLS Mode for ArcSight Database Back Up and Restore

These sections have instructions for configuring MinIO TLS mode to back up and restore the ArcSight database using a TLS-signed certificate and self-signed certificate:

- Configuring the MinIO Backup Server Using a TLS-Signed Certificate
- Configuring the MinIO Backup Server Using a TLS Self-Signed Certificate

Configuring the MinIO Backup Server Using a TLS-Signed Certificate

Follow these steps to configure the MinIO backup server using a TLS-signed certificate:

1. Log in to the MinIO source server.
2. Change to the Certificate directory:

   ```
   cd Sign-CA
   ```

3. Generate the private key for MinIO's backup server:

   ```
   openssl genrsa -out backup_minio_private.key 4096
   ```

4. Create the `backup_minio_openssl.conf` file:

```
[req]
distinguished_name = req_distinguished_name
x509_extensions = v3_req
prompt = no
[req_distinguished_name]
C = <country>
ST = <XX>
L = <locality>
O = <organization>
OU = <organizational unit>
CN = <MinIOBackupfqdn>
[v3_req]
subjectAltName = @alt_names
[alt_names]
IP.1 = <MinioBackupIP-address>
DNS.1 = <MinIOBackupfqdn>
```

5. Create the MinIO backup server signing request:

```
openssl req -new -key backup_minio_private.key -out backup_minio.csr -
config backup_minio_openssl.conf -nodes
```

6. Sign the certificate sign-request using ca.crt from the MinIO source server:

```
openssl x509 -req -in backup_minio.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -extensions server -days 3650 -outform PEM -out backup_
minio_public.crt -sha256  -extensions v3_req -extfile backup_minio_
openssl.conf
```

7. Run this command on the MinIO backup server:

```
./start-minio.sh
```

8. Run these commands on the MinIO server:

```
cd Sign-CA
scp backup_minio_public.crt <backup_minio_server_
IP>:/root/.minio/certs/public.crt
scp backup_minio_private.key <backup_minio_server_
IP>:/root/.minio/certs/private.key
scp ca.crt <backup_minio_server_IP>:/root/.minio/certs/CAs
scp ca.crt <backup_minio_server_IP>:/tmp
```

9. Stop and start the MinIO backup server:

```
./stop-minio.sh
./start-minio.sh
```

10. Log into the Console and create a bucket and folder on MinIO backup server. For more information, see Creating a Bucket and Folder in MinIO.

Configuring the MinIO Backup Server Using a TLS Self-Signed Certificate

Follow these steps to configure the MinIO backup server using a TLS self-signed certificate:

1. Log in to the MinIO backup server and create the self-sign directory:

```
mkdir self-sign
cd self-sign
```

2. Create the `backup_minio_openssl.conf` file:

```
[req]
distinguished_name = req_distinguished_name
x509_extensions = v3_req
prompt = no
[req_distinguished_name]
C = <country>
ST = <XX>
L = <locality>
O = <organization>
OU = <organizational unit>
CN = <MinIOBackupfqdn>
[v3_req]
subjectAltName = @alt_names
[alt_names]
IP.1 = <MinioBackupIP-address>
DNS.1 = <MinIOBackupfqdn>
```

3. Generate the self-signed certificate:

```
openssl req -newkey rsa:4096 -sha256 -keyform PEM -keyout backup_
private.key -x509 -days 3650 -outform PEM -out backup_public.crt -config
backup_minio_openssl.conf -nodes
```

4. Start MinIO:

```
./start-minio.sh
```

5. Copy the `backup_private.key` and `backup_public.crt` files to the certificate directory:

```
cp backup_private.key backup_public.crt /root/.minio/certs
cp backup_public.crt /root/.minio/certs/CAs/ca.crt
```

6. Stop and restart MinIO:

```
./stop-minio.sh
./start-minio.sh
```

7. Log into the Console and create a bucket and folder on MinIO backup server. For more information, see Creating a Bucket and Folder in MinIO.
8. Connect to the ArcSight database:

```
scp backup_public.crt <All-database-nodes>:/tmp
```

9. Run this command on all ArcSight database nodes:

```
cp /tmp/backup_public.crt /etc/pki/ca-trust/source/anchors;update-ca-
trust
```

Configuring the ArcSight Database for Backup

Run these commands on ArcSight database node1 to configure the ArcSight database for backup:

```
cd /opt/acsight-db-tools/config
vi backup_restore_cloud_storage_base.ini
change
; cloud_storage_ca_bundle = /home/user/ssl_folder/ca_bundle.pem
to
cloud_storage_ca_bundle = /etc/pki/tls/certs/ca-bundle.crt
```

You are now ready to proceed with the backup procedures.

Specifying Kafka Scheduler Options

Type `./kafka_scheduler <Option_Name>`.

Option Name	Description
update	Updates the scheduler
start	Starts the scheduler and begins copying data from all registered Kafka brokers
stop	Stops the scheduler and ends copying data from all registered Kafka brokers
delete	Deletes all registered Kafka instances from the scheduler. This operation will cause the ArcSight database to discard Kafka topic offsets. When the scheduler is created again, it will start reading data added to the topic after the scheduler creation, instead of at the old offset, which is likely to result in some data on the topic being skipped.

Option Name	Description
status	Prints the following information and log status for a running or stopped scheduler: • Current Kafka cluster assigned to the scheduler • Name and ArcSight database host where the active scheduler is running • Name, ArcSight database host, and process ID of every running scheduler (active or backup)
events	Prints event copy progress for the scheduler
messages	Prints scheduler messages

Managing Search

This section provides guidance for managing Search functions and features within the deployment.

- "Making Searches Case-insensitive" below
- "Performing a Keyword Search on Raw Event Data" below
- "Understanding the Schema for Events" on page 550

Making Searches Case-insensitive

By default, Search queries are case-sensitive for full-text searches and field-based ones. You can modify the database to make Search insensitive to case.

As the dbadmin user in the ArcSight Database, execute the following command:

```
 – ALTER DATABASE investigate set DefaultSessionLocale = ‘en_
US@colstrength=secondary’
```

Case-insensitive searches tend to slow Search performance.

Performing a Keyword Search on Raw Event Data

The system adds a **rawEvent** field, or a subset of event fields, to a text index for use in free-form text search. Users can perform a free-form text search for values only in event fields that are indexed.

- "Understanding Indexed Fields for Free-form Search" on the next page
- "Indexing Event Fields Before Installing the Database" on page 550

- "Indexing Event Fields After Installing the Database" on the next page

Understanding Indexed Fields for Free-form Search

If the **rawEvent** field has a value, the database will tokenize the field's content and store it as indexed text. If the **rawEvent** field is null, search allows you to perform a full-text search on the following columns:

agentDnsDomain	deviceCustomNumber3Label	filePermission
agentHostName	deviceCustomString1	fileType
agentTranslatedZoneURI	deviceCustomString1Label	flexDate1Label
agentZoneURI	deviceCustomString2	flexString1
applicationProtocol	deviceCustomString2Label	flexString1Label
categoryDeviceGroup	deviceCustomString3	flexString2
categoryDeviceType	deviceCustomString3Label	flexString2Label
categoryObject	deviceCustomString4	message
categoryOutcome	deviceCustomString4Label	name
categorySignificance	deviceCustomString5	oldFileId
categoryTechnique	deviceCustomString5Label	oldFileName
cryptoSignature	deviceCustomString6	oldFilePath
destinationDnsDomain	deviceCustomString6Label	oldFilePermission
destinationGeoLocationInfo	deviceDnsDomain	oldFileType
destinationHostName	deviceDnsDomain	rawEvent
destinationNtDomain	deviceDomain	reason
destinationProcessName	deviceEventCategory	requestClientApplication
destinationServiceName	deviceEventClassId	requestContext
destinationTranslatedZoneURI	deviceExternalId	requestCookies
destinationUserId	deviceFacility	requestMethod
destinationUserName	deviceHostName	requestUrl
destinationUserPrivileges	deviceInboundInterface	requestUrlFileName
destinationZoneURI	deviceNtDomain	requestUrlQuery
deviceAction	deviceOutboundInterface	sourceDnsDomain
deviceAssetId	devicePayloadId	sourceGeoLocationInfo

deviceCustomDate1Label	deviceProcessName	sourceHostName
deviceCustomDate2Label	deviceProduct	sourceNtDomain
deviceCustomFloatingPoint1Label	deviceSeverity	sourceProcessName
deviceCustomFloatingPoint2Label	deviceTranslatedZoneURI	sourceServiceName
deviceCustomFloatingPoint3Label	deviceVendor	sourceTranslatedZoneURI
deviceCustomFloatingPoint4Label	deviceVendor	sourceUserId
deviceCustomIPv6Address1Label	deviceZoneURI	sourceUserName
deviceCustomIPv6Address2Label	eventOutcome	sourceUserPrivileges
deviceCustomIPv6Address3Label	externalId	sourceGeoPostalCode
deviceCustomIPv6Address4Label	fileId	sourceGeoRegionCode
deviceCustomNumber1Label	fileName	sourceZoneURI
deviceCustomNumber2Label	filePath	transportProtocol

Indexing Event Fields Before Installing the Database

Before installing the database, you can index event fields that would not otherwise be indexed when the rawEvent field is null. To do so, contact Support Services so they can assist you in modifying the `superschema_vertica.sql` file in the installer.

Indexing Event Fields After Installing the Database

After installing the database, you can index event fields that would not otherwise be indexed when the rawEvent field is null. If there are events in the database, you must drop the text index and recreate it. The reindexing process might take time, depending on the number of events in the system.

Understanding the Schema for Events

The following table describes the columns of the **default_sec_ops_adm.Events** table:

Column Name	Data Type	Description
agentAddressBin/agentAddress	Binary(16)	The IP address of the ArcSight connector that processed the event.
agentHostName	Varchar(1023)	The hostname of the ArcSight connector that processed the event.
agentNtDomain	Varchar(255)	
agentSeverity	Varchar(9)	
agentType	Varchar(63)	The agent type of the ArcSight connector that processed the event.
agentZoneURI	Varchar(2048)	Specify hourly, daily, weekly, or monthly.
applicationProtocol	Varchar(40)	Application level protocol, example values are HTTP, HTTPS, SSHv2, Telnet, POP, IMPA, IMAPS, and so on.
baseEventCount	Integer	A count associated with this event. How many times was this same event observed? Count can be omitted if it is 1.
bytesIn	Integer	Number of bytes transferred inbound, relative to the source to destination relationship, meaning that data was flowing from source to destination.
bytesOut	Integer	Number of bytes transferred outbound relative to the source to destination relationship. For example, the byte number of data flowing from the destination to the source.
categoryBehavior	Varchar(1023)	The action or behavior associated with the event.
categoryDeviceGroup	Varchar(1023)	The type of events for the device.

Column Name	Data Type	Description
categoryObject	Varchar(1023)	The type of the object.
categoryOutcome	Varchar(1023)	The outcome of the event.
categorySignificance	Varchar(1023)	The significance of the event.
categoryTechnique	Varchar(1023)	
destinationAddressBin/destinationAddress	Binary(16)	Identifies the destination address that the event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”
destinationDnsDomain	Varchar(255)	The DNS domain part of the complete fully qualified domain name (FQDN).
destinationHostName	Varchar(1023)	Identifies the destination that an event refers to in an IP network. The format should be a fully qualified domain name (FQDN) associated with the destination node, when a node is available. Examples: “host.domain.com” or “host”.
destinationMacAddressBin/ destinationMacAddress	Binary(16)	Six colon-separated hexadecimal numbers. Example: “00:0D:60:AF:1B:61”
destinationNtDomain	Varchar(255)	The Windows domain name of the destination address.
destinationPort	Integer	The valid port numbers are between 0 and 65535.
destinationProcessName	Varchar(1023)	The name of the event’s destination process. Example: “telnetd” or “sshd”.
destinationServiceName	Varchar(1023)	The service targeted by this event. Example: “sshd”
destinationTranslatedAddressBin/ destinationTranslatedAddress	Binary(16)	

Column Name	Data Type	Description
destinationUserId	Varchar(1023)	Identifies the destination user by ID. For example, in UNIX, the root user is generally associated with user ID 0.
destinationUserName	Varchar(1023)	Identifies the destination user by name. This is the user associated with the event's destination. Email addresses are often mapped into the UserName fields. The recipient is a candidate to put into this field.
destinationUserPrivileges	Varchar(1023)	The typical values are "Administrator", "User", and "Guest". This identifies the destination user's privileges. In UNIX, for example, activity executed on the root user would be identified with destinationUser Privileges of "Administrator".
destinationZoneURI	Varchar(2048)	The URI for the Zone that the destination asset has been assigned to in ArcSight.
deviceAction	Varchar(63)	Action taken by the device.
deviceAddressBin/deviceAddress	Binary(16)	Identifies the device address that an event refers to in an IP network. The format is an IPv4 address. Example: "192.168.10.1".
deviceCustomDate1	Integer	One of two timestamp fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.

Column Name	Data Type	Description
deviceCustomDate1Label	Varchar(1023)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomDate2	Integer	One of two timestamp fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
deviceCustomDate2Label	Varchar(1023)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomNumber1	Integer	One of three number fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
deviceCustomNumber1Label	Varchar(1023)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomNumber2	Integer	One of three number fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
deviceCustomNumber2Label	Varchar(1023)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.

Column Name	Data Type	Description
deviceCustomNumber3	Integer	One of three number fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
deviceCustomNumber3Label	Varchar(1023)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomString1	Varchar(4000)	One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
deviceCustomString1Label	Varchar(1023)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomString2	Varchar(4000)	One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
deviceCustomString2Label	Varchar(1023)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomString3	Varchar(4000)	One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.

Column Name	Data Type	Description
deviceCustomString3Label	Varchar(1023)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomString4	Varchar(4000)	One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
deviceCustomString4Label	Varchar(1023)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomString5	Varchar(4000)	One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
deviceCustomString5Label	Varchar(1023)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomString6	Varchar(4000)	One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
deviceCustomString6Label	Varchar(1023)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.

Column Name	Data Type	Description
deviceEventCategory	Varchar(1023)	Represents the category assigned by the originating device. Devices often use their own categorization schema to classify event. Example: “/Monitor/Disk/Read”
deviceEventClassId	Varchar(100)	Unique code assigned to an event.
deviceExternalId	Varchar(255)	A name that uniquely identifies the device generating this event.
deviceHostName	Varchar(100)	The format should be a fully qualified domain name (FQDN) associated with the device node, when a node is available. Example: “host.domain.com” or “host”.
deviceInboundInterface	Varchar(128)	Interface on which the packet or data entered the device.
deviceOutboundInterface	Varchar(128)	Interface on which the packet or data left the device.
deviceProduct	Varchar(100)	The device product of the client.
deviceReceiptTime	Integer	The time at which the event related to the activity was received. The format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1st 1970)
deviceSeverity	Varchar(63)	The HTTP response status.
deviceVendor	Varchar(100)	The device vendor of the client.
deviceVersion	Varchar(31)	The device version.
deviceZoneURI	Varchar(2048)	The URI for the Zone that the device asset has been assigned to in ArcSight.

Column Name	Data Type	Description
endTime	Integer	The time at which the activity related to the event ended. The format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1st1970). An example would be reporting the end of a session.
eventId	Integer	This is a unique ID that ArcSight assigns to each event.
externalId	Varchar(40)	The ID used by an originating device. They are usually increasing numbers, associated with events.
fileName	Varchar(1023)	Name of the file only (without its path).
filePath	Varchar(1023)	Full path to the old file, including the file name itself. Examples: c:\Program Files\ WindowsNT\Accessories \wordpad.exe or /usr/bin/zip
flexDate1	Integer	A timestamp field available to map a timestamp that does not apply to any other defined timestamp field in this dictionary. Use all flex fields sparingly and seek a more specific, dictionary supplied field when possible. These fields are typically reserved for customer use and should not be set by vendors unless necessary.
flexDate1Label	Varchar(128)	The label field is a string and describes the purpose of the flex field.
flexNumber1	Integer	
flexNumber1Label	Varchar(128)	

Column Name	Data Type	Description
flexNumber2	Integer	
flexNumber2Label	Varchar(128)	
flexString1	Varchar(1023)	One of four floating point fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible. These fields are typically reserved for customer use and should not be set by vendors unless necessary.
flexString1Label	Varchar(128)	The label field is a string and describes the purpose of the flex field.
flexString2	Varchar(1023)	One of four floating point fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible. These fields are typically reserved for customer use and should not be set by vendors unless necessary.
flexString2Label	Varchar(128)	The label field is a string and describes the purpose of the flex field.
globalEventId	Integer	
message	Varchar(1023)	An arbitrary message giving more details about the event. Multi-line entries can be produced by using \n as the new line separator.
name	Varchar(1023)	
requestClientApplication	Varchar(1023)	The User-Agent associated with the request.

Column Name	Data Type	Description
requestContext	Varchar(2048)	Description of the content from which the request originated (for example, HTTP Referrer)
requestMethod	Varchar(1023)	The method used to access a URL. Possible values: “POST”, “GET”, etc.
requestUrl	Varchar(2048)	In the case of an HTTP request, this field contains the URL accessed. The URL should contain the protocol as well. Example: “http://www/secure.com”
requestUrlFileName	Varchar(2048)	
requestUrlQuery	Varchar(2048)	
sourceAddressBin/sourceAddress	Binary(16)	Identifies the source that an event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”.
sourceHostName	Varchar(1023)	Identifies the source that an event refers to in an IP network. The format should be a fully qualified domain name (FQDN) associated with the source node, when a mode is available. Examples: “host” or “host.domain.com”.
sourceMacAddressBin/sourceMacAddress	Binary(16)	Six colon-separated hexadecimal numbers. Example: “00:0D:60:AF:1B:61”
sourceNtDomain	Varchar(255)	The Windows domain name for the source address.
sourcePort	Integer	The valid port numbers are 0 to 65535.
sourceProcessName	Varchar(1023)	The name of the event’s source process.

Column Name	Data Type	Description
sourceServiceName	Varchar(1023)	The service that is responsible for generating this event.
sourceTranslatedAddressBin/sourceTranslatedAddress	Binary(16)	Identifies the translated source that the event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”.
sourceUserId	Varchar(1023)	Identifies the source user by ID. This is the user associated with the source of the event. For example, in UNIX, the root user is generally associated with user ID 0.
sourceUserName	Varchar(1023)	Identifies the source user by name. Email addresses are also mapped into the UserName fields. The sender is a candidate to put into this field.
sourceUserPrivileges	Varchar(1023)	The typical values are “Administrator”, “User”, and “Guest”. It identifies the source user’s privileges. In UNIX, for example, activity executed by the root user would be identified with “Administrator”.
sourceZoneURI	Varchar(2048)	The URI for the Zone that the source asset has been assigned to in ArcSight.
startTime	Integer	The time when the activity the event referred to started. The format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1st 1970)
transportProtocol	Varchar(31)	Identifies the Layer-4 protocol used. The possible values are protocols such as TCP or UDP.

Column Name	Data Type	Description
type	Varchar(1023)	0 means base event, 1 means aggregated, 2 means correlation, and 3 means action. This field can be omitted for base events (type 0).
agentDnsDomain	Varchar(255)	The DNS domain name of the ArcSight connector that processed the event.
agentId	Varchar(40)	The agent ID of the ArcSight connector that processed the event.
agentMacAddressBin	Binary(16)	
agentReceiptTime	Integer	The time at which information about the event was received by the ArcSight connector.
agentTimeZone	Varchar(255)	The agent time zone of the ArcSight connector that processed the event.
agentTranslatedAddressBin	Binary(16)	
agentTranslatedZoneExternalID	Varchar(200)	
agentTranslatedZoneURI	Varchar(2048)	
agentVersion	Varchar(31)	The version of the ArcSight connector that processed the event.
agentZoneExternalID	Varchar(200)	
categoryDeviceType	Varchar(1023)	The events generated by a device type irrespective of the device group the events belong to.
cryptoSignature	Varchar(512)	
customerExternalID	Varchar(200)	
customerURI	Varchar(2048)	
destinationGeoCountryCode	Varchar(1023)	
destinationGeoLatitude	Float	The latitudinal value from which the destination’s IP address belongs.

Column Name	Data Type	Description
destinationGeoLocationInfo	Varchar(1023)	
destinationGeoLongitude	Float	The longitudinal value from which the destination's IP address belongs.
destinationGeoPostalCode	Varchar(1023)	
destinationGeoRegionCode	Varchar(1023)	
destinationProcessId	Integer	Provides the ID of the destination process associated with the event. For example, if an event contains process ID 105, "105" is the process ID.
destinationTranslatedPort	Integer	Port after it was translated; for example, a firewall. Valid port numbers are 0 to 65535.
destinationTranslatedZoneExternalID	Varchar(200)	
destinationTranslatedZoneURI	Varchar(2048)	
destinationZoneExternalID	Varchar(200)	
deviceAssetId	Varchar(40)	
deviceCustomDescriptorId	Varchar(1023)	
deviceCustomFloatingPoint1	Float	One of four floating point fields available to map fields that do not apply to any other in this dictionary.
deviceCustomFloatingPoint1Label	Varchar(1023)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomFloatingPoint2	Float	One of four floating point fields available to map fields that do not apply to any other in this dictionary.
deviceCustomFloatingPoint2Label	Varchar(1023)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.

Column Name	Data Type	Description
deviceCustomFloatingPoint3	Float	One of four floating point fields available to map fields that do not apply to any other in this dictionary.
deviceCustomFloatingPoint3Label	Varchar(1023)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomFloatingPoint4	Float	One of four floating point fields available to map fields that do not apply to any other in this dictionary.
deviceCustomFloatingPoint4Label	Varchar(1023)	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
deviceCustomIPv6Address1Bin	Varbinary(16)	
deviceCustomIPv6Address1Label	Varchar(1023)	
deviceCustomIPv6Address2Bin	Varbinary(16)	
deviceCustomIPv6Address2Label	Varchar(1023)	
deviceCustomIPv6Address3Bin	Varbinary(16)	
deviceCustomIPv6Address3Label	Varchar(1023)	
deviceCustomIPv6Address4Bin	Varbinary(16)	
deviceCustomIPv6Address4Label	Varchar(1023)	
deviceDirection	Varchar(1023)	Any information about what direction the observed communication has taken. The following values are supported: “0” for inbound or “1” for outbound.
deviceDnsDomain	Varchar(255)	The DNS domain part of the complete fully qualified domain name (FQDN).
deviceDomain	Varchar(1023)	

Column Name	Data Type	Description
deviceFacility	Varchar(1023)	The facility generating this event. For example, Syslog has an explicit facility associated with every event.
deviceMacAddressBin	Binary(16)	
deviceNtDomain	Varchar(255)	The Windows domain name of the device address.
deviceProcessId	Integer	Provides the ID of the process on the device generating the event.
deviceProcessName	Varchar(1023)	Process name associated with the event. An example might be the process generating the syslog entry in UNIX.
deviceTimeZone	Varchar(255)	The timezone for the device generating the event.
deviceTranslatedAddressBin	Binary(16)	
deviceTranslatedZoneExternalID	Varchar(200)	
deviceTranslatedZoneURI	Varchar(2048)	The URI for the Translated Zone that the device asset has been assigned to in ArcSight.
deviceZoneExternalID	Varchar(200)	
eventOutcome	Varchar(63)	Displays the outcome, usually as ‘success’ or ‘failure’.
fileCreateTime	Integer	Time when the file was created.
fileHash	Varchar(255)	Hash of a file.
fileId	Varchar(1023)	An ID associated with a file could be the inode.
fileModificationTime	Integer	Time when the file was last modified.
filePermission	Varchar(1023)	Permissions of the file.
fileSize	Integer	Size of the file.

Column Name	Data Type	Description
fileType	Varchar(1023)	Type of file (pipe, socket, etc.)
id	Integer	
locality	Varchar(1023)	
normalizedEventTime	Integer	
oldFileCreateTime	Integer	Time when old file was created.
oldFileHash	Varchar(255)	Hash of the old file.
oldFileId	Varchar(1023)	
oldFileModificationTime	Integer	Time when old file was last modified.
oldFileName	Varchar(1023)	Name of the old file.
oldFilePath	Varchar(1023)	Full path to the old file, including the file name itself. Examples: c:\Program Files\ WindowsNT\Accessories \wordpad.exe or /usr/bin/zip
oldFilePermission	Varchar(1023)	Permissions of the old file.
oldFileSize	Integer	Size of the old file.
oldFileType	Varchar(1023)	Type of the old file (pipe, socket, etc.)
originator	Varchar(1023)	
persistedTime	Integer	
rawEvent	Varchar(4000)	
reason	Varchar(1023)	The reason an audit event was generated. For example “bad password” or “unknown user”. This could also be an error or return code. Example: “0x1234”
requestCookies	Varchar(1023)	Cookies associated with the request.
severity	Integer	

Column Name	Data Type	Description
sourceDnsDomain	Varchar(255)	The DNS domain part of the complete fully qualified domain name (FQDN).
sourceGeoCountryCode	Varchar(1023)	
sourceGeoLatitude	Float	
sourceGeoLocationInfo	Varchar(1023)	
sourceGeoLongitude	Float	
sourceGeoPostalCode	Varchar(1023)	
sourceGeoRegionCode	Varchar(1023)	
sourceProcessId	Integer	The ID of the source process associated with the event.
sourceTranslatedPort	Integer	A port number after being translated by, for example, a firewall. Valid port numbers are 0 to 65535.
sourceTranslatedZoneExternalID	Varchar(200)	
sourceTranslatedZoneURI	Varchar(2048)	The URI for the Translated Zone that the destination asset has been assigned to in ArcSight.
sourceZoneExternalID	Varchar(200)	
version	Varchar(10)	
priority	Integer	
base_event_ids	Varchar(8000)	
correlated_event_id	Integer	
extraFields	Varchar(8192)	

Managing ArcMC

This section provides information about managing ArcMC.

Managing Repositories

Certain management operations require a specific upgrade or content update (`.enc`) file, or a certificate. Other operations, such as viewing logs, require you to load the logs to a Log

repository. ArcMC can also maintain centralized repositories for files needed for host configuration and management.

By default, a number of pre-defined repositories are provided. However, you can create more repositories to suit your needs. Any repositories you create are referred to as *user-defined* repositories.

The following controls are used for repository functions:

- **Retrieve Container Files** copies a file from one or more managed hosts to the repository.
- **Upload to Repository** sends a file from your local computer (the computer running the browser) or a network host accessible from your local computer to the repository.
- **Retrieve** downloads a file from the repository.
- **Upload** copies a file from the repository to one or more managed nodes.

You can perform these operations using repositories:

- Manage logs in the Logs repository
- Manage CA certificates in the CA Certs repository
- Upgrade a connector using an upgrade file available in the Upgrade repository
- Apply a Content ArcSight Update Pack (AUP) on one or more connectors
- Maintain centralized repositories of files for connector configuration and management

The following topics are discussed here.

Logs Repository

To view logs, you need to first **Load** the logs of the container that contains the connector to the Logs repository, and then **Retrieve** the logs to view them.

Note: If a container contains more than one connector, logs for all connectors are retrieved.

For information on loading, retrieving, and deleting container logs, see "Viewing Container Logs" on page 851.

Uploading a File to the Logs Repository

Uploading a file into the Log repository is useful for sharing annotated log or other files with other users. An uploaded file needs to be in `.zip` format.

To upload a ZIP file:

1. Click **Administration > Repositories.**
2. Click **Logs** from the left panel.

3. Click **Upload** from the management panel.
4. Enter the local file path or click **Browse** to select the ZIP file.
5. Click **Submit** to add the specified file to the repository or **Cancel** to quit.

> **Note:** Due to a browser limitation in Internet Explorer 11, the progress of the file upload will not be shown.

CA Certs Repository

Connectors require a Certificate Authority (CA) issued or self-signed SSL certificate to communicate securely with a destination. The CA Certs repository (shown below) enables you to store CA Certs files (that contain one or multiple certificates) and single CA certificates. When certificates are stored in the CA Certs repository, you can add the certificates to a container so that the connectors in the container can validate their configured destinations.

You can add a single certificate to a container that is in FIPS or non-FIPS mode. You can only add a CA Certs file to a container that is in non-FIPS mode.

To associate a CA certificate to a connector, you need to:

- Upload the CA certificate or CA Certs file to the CA Certs repository, as described below.
- Add a CA certificate from the CA Certs repository to the container that contains the connector, as described in "Managing Certificates on a Container" on page 855.

Uploading CA Certificates to the Repository

You can upload a CA Certs file or a single certificate to the CA Certs repository.

> **Tip:** Before you upload a single CA certificate, change the name of the certificate on the local computer to a name that you can recognize easily. This helps you distinguish the certificate when it is displayed in the Certificate Management wizard.

To upload certificates to the repository:

1. Click **Administration > Repositories.**
2. Click **CA Certs** in the left panel.
3. Click **Upload** in the management panel.
4. Enter the local path for the CA Certs file or the certificate, or click **Browse** to select it.
5. Click **Submit** to add the specified CA Certs file or the certificate to the repository, or **Cancel** to quit.

The CA Certs Repositories tab shows all the CA Certs files and single certificates that have been uploaded. The Type column shows CERTIFICATE for a single certificate and CACERT for a CA Certs file.

Removing CA Certificates from the Repository

When you delete a CA Certs file or a single certificate from the repository, it is deleted from ArcMC.

> **Note:** When you delete a CA Certs file or a single certificate from the CA Certs repository, containers are not affected; the connectors continue to use the certificates, which are located in a trust store after being added to a container. For information about adding a CA certificate to a container, see "Managing Certificates on a Container" on page 855.

To remove a certificate from the repository:

1. Click **Administration > Repositories.**
2. Click **CA Certs** in the left panel.
3. Identify the certificate or the CA Certs file you want to remove and click the **Remove** button (✕).

Upgrade Files Repository

The Upgrade files repository enables you to maintain a number of connector upgrade files. You can apply any of these upgrade files to containers when you need to upgrade to a specific version. As a result, all connectors in a container are upgraded to the version you apply to the container.

> **Note:** Logger ENC files are required for the remote upgrade of a Logger Appliance. For more information, see "Upgrading a Logger " on page 843.

About the AUP Upgrade Process

> **Note:** The process discussed in this section only applies to upgrading connectors and to upgrading a remotely-managed Connector Appliance. If you are upgrading the local ArcMC (localhost), use an ENC file instead.

To upgrade a connector or to upgrade a remotely-managed Connector Appliance, you need to:

- Upload the appropriate `.aup` upgrade file to the Upgrade Files repository, as described below.

- Apply the `.aup` upgrade file from the Upgrade Files repository to the container (see "Upgrading All Connectors in a Container" on page 849).

Uploading an AUP Upgrade File to the Repository

To upload AUP upgrade files to the repository:

1. Download the upgrade files for the connector or the remote Connector Appliance from the ArcSight Customer Support site at https://www.microfocus.com/en-us/support to the computer that you use to connect to the browser-based interface.
2. Log in to the browser-based interface.
3. Click **SetupConfiguration** > **Administration** > **Repositories.**
4. Click **Upgrade AUP** from the left panel.
5. Click **Upload** from the management panel.
6. Click **Browse** and select the file you downloaded earlier.
7. Click **Submit** to add the specified file to the repository or click **Cancel** to quit.
8. You can now use the AUP upgrade file to upgrade a container to a specific version. For instructions, see "Upgrading All Connectors in a Container" on page 849.

Removing a Connector Upgrade from the Repository

You can remove a connector upgrade file from the repository when you no longer need it. When you remove a connector upgrade file from the repository, it is deleted from ArcMC.

To remove a Connector upgrade from the repository:

1. Click **SetupConfiguration** > **Administration** > **Repositories.**
2. Click **Upgrade AUP** from the left panel.
3. Locate the upgrade file that you want to delete and click the associated ✕ icon.

Content AUP Repository

ArcSight continuously develops new connector event categorization mappings, often called *content*. This content is packaged in ArcSight Update Packs (AUP) files. All existing content is included with major product releases, but it is possible to stay completely current by receiving up-to-date, regular content updates through ArcSight announcements and the Customer Support site. The AUP files are located under Content Subscription Downloads.

The ArcSight Content AUP feature enables you to apply an AUP file to applicable connector destinations that you are managing. Only the event categorization information can be applied to the connectors using this feature.

You can maintain a number of Content AUP files in the Content AUP repository. When an AUP file with a version number higher than the ones already in the repository is loaded, it is automatically pushed out to the connector destinations being managed. However, these connectors or connector destinations are skipped:

- Connectors that are unavailable at the time of the AUP file push
- Connectors whose current version does not fall in the range of versions that the Content AUP supports
- The ESM destination on a connector
- All destinations of a connector that have an ESM destination with the AUP Master flag set to Yes

Also, when a new connector is added, the highest number Content AUP is pushed automatically to its destinations.

Applying a New Content AUP

You can add a new content AUP file to the repository and push it automatically to all applicable managed nodes.

To apply a new Content AUP:

1. Download the new Content AUP version from the support site at https://softwaresupport.softwaregrp.com/ to the computer that you use to connect to the browser-based interface.
2. Log in to the browser-based interface.
3. Click **Administration > Repositories.**
4. Click **Content AUP** from the left panel.
5. Click **Upload** from the management panel.
6. Click **Browse** and select the file you downloaded earlier.
7. Click **Submit** to add the specified file to the repository and push it automatically to all applicable connectors, or **Cancel** to quit.

You can verify the current Content AUP version on a connector by performing either of these steps:

- Run the `GetStatus` command on the node destination and check that the value for aup `[acp].version` is the same as the AUP version you applied. For information about running a command on a connector destination, see "Sending a Command to a Connector" on

page 873.

- Hover over a host name to see the AUP version applied to all destinations of that connector.

Applying an Older Content AUP

If you need to apply an older Content AUP from the Content AUP repository, delete all versions newer than the one you want to apply in the repository. The latest version (of the remaining AUP files) is pushed automatically to all applicable connectors.

To delete a Content AUP from the Content AUP repository:

1. Click **Administration > Repositories.**
2. Click **Content AUP** from the left panel.
3. Locate the AUP file that you want to delete and click the associated ✕ icon. Repeat for multiple files.

User-Defined Repositories

A *user-defined repository* is a user-named collection of settings that control upload and download of particular files from connectors to the repository. Each repository uses a specified path, relative to `$ARCSIGHT_HOME/user/agent`, for files to be uploaded or downloaded. ArcSight connectors use a standard directory structure, so map files, for example, are always found in `$ARCSIGHT_HOME/user/agent`, (that is, the root directory, `$ARCSIGHT_HOME`, of the installation path) in a folder called `map/`.

After they are created, user-defined repositories are listed on the left-side menu, under the **New Repository** heading, and appear with the user-specified display name.

User-defined repositories should be grouped by file type and purpose, such as log files, certificate files, or map files. Each user-defined repository has a name, a display name, and an item display name, which are described under the repository **Settings** tab.

Files viewed in a user-defined repository can be bulk processed with specified hosts and can be exchanged with the user’s browser host.

Creating a User-Defined Repository

You can create a new repository at any time.

The repository requires correct directory paths. Your file will be applied to the wrong directory if the entered path contains errors, such as extra spaces or incorrect spellings. You can verify your directory paths by accessing the Directory.txt file, which lists the directory structure for

every entered path. View the Directory.txt file by accessing your container logs and finding the Directory.txt file.

To create a new user-defined repository:

1. Click **Administration > Repositories.**
2. Click **New Repository** under the **Repositories** section in the left panel.
3. For the new repository, enter the parameters listed in the following table.

Parameter	Description
Name	A unique name for the repository, typically based on the type of files it contains.
Display Name	The name that will be displayed on the left-side menu and for tabs: Process *names*, View *names*, Settings for *names*. Typically plural.
Item Display Name	The name used to describe a single item.
Recursive	Check to include sub-folders.
Sort Priority	-1 by default
Restart Connector Process	Check to restart the connector process after file operations.
Filename Prefix	An identifying word that is included in the names of retrieved files. For example, map files are identified by `Map` in the file name: `localhost_Container_-1.Map-2009-04-06_12-22-25-607.zip`
Relative path (Download)	The path for download, relative to `$ARCSIGHT_HOME`, for example, `user/agent/map` or `user/agent/flexagent`. Leave this field blank to specify files in `$ARCSIGHT_HOME`. **Note**: The relative path is used for download only.
Include Regular Expression	A description of filenames to include. Use `.*` to specify all files. The following example selects properties files that consist of `map`. followed by one or more digits, followed by `.properties`: `map\.[0-9]+\.properties$`
Exclude Regular Expression	A description of filenames to exclude. The following example excludes all files with a certain prefix or in the `agentdata` folder. `(agentdata/|cwsapi_fileset_).*$`
Delete Before Upload	Check to delete earlier copies before upload. **CAUTION**: If you check **Delete Before Upload** and do not specify a Relative path (Upload), all files and folders in `current/user/agent` will be deleted.
Delete Groups	Whether to delete folders recursively in `$ARCSIGHT_HOME/user/agent/map directory`.
Relative path (Upload)	The path for upload, relative to `$ARCSIGHT_HOME/current/user/agent/flexagent/`<*connectorname*>

Parameter	Description
Delete Relative Path	Whether the directory specified in **Relative Path (Upload)** and its contents should be removed when a file is uploaded from the repository.
Delete Include Regular Expression	Typically the same as the Include Regular Expression.
Delete Exclude Regular Expression	Typically the same as the Exclude Regular Expression.

4. Click **Save** at the bottom of the page.

   The new repository displays under the **New Repository** heading in the left-side window panel.

Retrieving Container Files

The **Retrieve Container Files** button copies a file from one or more containers to a repository. The specific files that are retrieved depend on the settings of the repository.

To retrieve a container file:

1. Click **Administration > Repositories.**
2. In the left panel, under **Repositories**, click the name of the repository to which you want to copy connector files.
3. Click **Retrieve Container Files** in the management panel.
4. Follow the instructions in the Retrieve Container Files wizard.

Uploading Files to a Repository

To upload files to a repository:

1. Click **Administration > Repositories.**
2. In the lower left panel (under **Repositories**), click the name of the repository to which you want to upload files.
3. Click **Upload To Repository** from the management panel.
4. Follow the instructions in the Repository File Creation wizard. Select **Individual files** to create a ZIP file with appropriate path information.

   Caution: Be sure **not** to change the default sub-folder name `lib` in the **Enter the sub folder where the files will be uploaded** page of the Repository File Creation wizard.

Deleting a User-Defined Repository

To delete a user-defined repository:

1. Click **Administration > Repositories.**
2. From the left panel, click the name of the repository you want to delete.
3. Click **Remove Repository** from the management panel.

Updating Repository Settings

To update the settings of a user-defined repository:

1. Click **Administration > Repositories.**
2. In the left panel, click the name of the repository whose settings you want to update.
3. Click the **Settings for *Repository_Name*** tab from the management panel.
4. Update the settings.
5. Click **Save** at the bottom of the page.

Managing Files in a Repository

Retrieving a File from the Repository

To retrieve a file from the repository:

1. Click **Administration > Repositories.**
2. From the left panel, click the name of the repository in which the file exists.
3. Click ✕ from the management panel for the file that you want to retrieve.
4. Follow the file download instructions to copy the file to your local computer.

Uploading a File from the Repository

To upload a file from the repository:

1. Click **Administration > Repositories.**
2. In the left panel, click the name of the repository in which the file exists.
3. In the management panel, click **Upload to Repository** for the file that you want to upload.
4. Follow the Upload Container Files wizard instructions to upload the file to the containers of your choice.

5. Verify that the file was uploaded correctly:
   - If you have SSH access to the connectors, connect to them and check the file structure.
   - Obtain the connector logs and check the contents of the `Directory.txt` file for each connector.

Removing a File from the Repository

To remove a file from the repository:

1. Click **Administration > Repositories.**
2. In the left panel, click the name of the repository in which the file exists.
3. In the management panel, click ✕ for the file that you want to delete.

Pre-Defined Repositories

You can define repositories for any connector-related files. The following repositories are pre-defined:

- **Backup Files**: connector cloning (see " Backup Files " on page 581).
- **Map Files**: enrich event data
- **Parser Overrides**: customize the parser (see "Adding Parser Overrides" on page 582)
- **FlexConnector Files**: user-designed connector deployment
- **Connector Properties**: `agent.properties`; subset of cloning
- **JDBC Drivers**: database connectors

To view the settings for a pre-defined repository, click the name of the repository and then click the **Settings** tab in the management panel. Settings for a pre-defined repository are read-only.

Settings for Map Files

This table lists the default settings for map files.

Map File Settings

Name	Default Setting
Name	map
Display Name	Map Files
Item Display Name	Map File
Recursive	Deselected (No)

Map File Settings , continued

Name	Default Setting
Sort Priority	5
Restart Connector Process	Deselected (No)
Filename Prefix	Map
Download Relative Path	map
Download Include regular expression	map\.[0-9]+\.properties$
Download Exclude regular expression	
Delete before upload	Selected (Yes)
Delete groups	Deselected (No)
Upload Relative Path	
Delete Relative Path	map
Delete Include regular expression	map\.[0-9]+\.properties$
Delete Exclude regular expression	

Settings for Parser Overrides

This table lists the default settings for parser overrides.

Parser Override Settings

Name	Default Setting
Name	parseroverrides
Display Name	Parser Overrides
Item Display Name	Parser Override
Recursive	Selected (Yes)
Sort Priority	10
Restart Connector Process	Selected (Yes)
Filename Prefix	Parsers
Download Relative Path	fcp
Download Include regular expression	.*
Download Exclude regular expression	
Delete before upload	Selected (Yes)
Delete groups	Selected (Yes)
Upload Relative Path	

Parser Override Settings , continued

Name	Default Setting
Delete Relative Path	fcp
Delete Include regular expression	.*
Delete Exclude regular expression	

Settings for FlexConnector Files

This table lists the default settings for FlexConnector files.

FlexConnector Settings

Name	Default Setting
Name	flexconnectors
Display Name	FlexConnector Files
Item Display Name	FlexConnector File
Recursive	Selected (Yes)
Sort Priority	15
Restart Connector Process	Selected (Yes)
Filename Prefix	FlexConnector
Download Relative Path	flexagent
Download Include regular expression	.*
Download Exclude regular expression	
Delete before upload	Selected (Yes)
Delete groups	Selected (Yes)
Upload Relative Path	
Delete Relative Path	flexagent
Delete Include regular expression	.*
Delete Exclude regular expression	

Settings for Connector Properties

Connector Default Property Settings

Name	Default Setting
Name	connectorproperties
Display Name	Connector Properties

Connector Default Property Settings , continued

Name	Default Setting
Item Display Name	Connector Property File
Recursive	Deselected (No)
Sort Priority	20
Restart Connector Process	Selected (Yes)
Filename Prefix	ConnectorProperties
Download Relative Path	
Download Include regular expression	agent\.*
Download Exclude regular expression	
Delete before upload	Deselected (No)
Delete groups	Deselected (No)
Upload Relative Path	
Delete Relative Path	
Delete Include regular expression	agent\.*
Delete Exclude regular expression	

Settings for JDBC Drivers

This table lists the default settings for JDBC Drivers.

JDBC Driver Settings

Name	Default Setting
Name	jdbcdrivers
Display Name	JDBC Drivers
Item Display Name	Connector JDBC Driver File
Recursive	Deselected (No)
Sort Priority	25
Restart Connector Process	Selected (Yes)
Filename Prefix	
Download Relative Path	lib
Download Include regular expression	
Download Exclude regular expression	
Delete before upload	Deselected (No)

JDBC Driver Settings , continued

Name	Default Setting
Delete groups	Deselected (No)
Upload Relative Path	
Delete Relative Path	lib
Delete Include regular expression	
Delete Exclude regular expression	

Backup Files

Using the **Backup Files** repository, you can quickly copy a container to other containers. As a result, all connectors in the source container are copied to the destination container. This process is called *cloning* a container configuration. You can clone a container to several containers at once. The contents of the source container replace the existing contents of the destination container.

> **Caution:** Containers on ArcMC are pre-installed with the latest connector release. Do not clone older, software-based connectors (such as build 4.0.8.4964) to containers with newer connector builds (such as 4.0.8.4976 or later).
>
> *Cloning* a connector using the Backup repository only works if the connector version numbers are the same.

To clone a container using the Backup Files repository:

1. Click **Node Management > View All Nodes.**
2. Click the **Containers** tab to list the containers and determine the source and destination for cloning.
3. Click **Administration > Repositories.**
4. Click **Backup Files** under the **Repositories** section in the management panel.
5. If the backup file that you need to use for cloning exists in the repository, go to the next step. Otherwise, follow the instructions in "Retrieving a File from the Repository" on page 576 to retrieve the container's backup file to the Backup repository.

   The retrieved file is named in `<connector name>` ConnectorBackup `<date>` format.
6. Follow the instructions in "Uploading a File from the Repository" on page 576 to upload the backup file to one or more containers.

   The destination containers are unavailable while the backup file is applied and the connectors are restarted.

> **Note:** The backup file does not include the container certificates. You have to re-apply the certificates to the container after you upload the backup file.
>
> After applying the certificates, check the status of the destination container to make sure it is available.

Adding Parser Overrides

A parser override is a file provided by ArcSight used to resolve an issue with the parser for a specific connector, or to support a newer version of a supported device where the log file format changed slightly or new event types were added.

To use parser overrides, you need to:

- Upload a parser override file to the **Parser Overrides** repository.
- Download the parser override file to the container that contains the connector that will use the parser override.

Follow the steps below.

To upload a parser override file:

1. Click **Administration > Repositories.**
2. Click **Parser Overrides** under the **Repositories** section in the management panel.
3. On the **Parser Overrides** tab, click the **Upload To Repository** button.
4. Follow the wizard to upload the file. When prompted by the wizard, make sure you:
   - Select the **Individual Files** option from the **Select the type of file that you want to upload** field.
   - Add a slash (/) after fcp before adding the folder name in the **Enter the sub folder where the files will be uploaded** field. For example, `fcp/multisqlserverauditdb`.

     > **Note:** The folder name may only contain letters and numbers. Do not include special characters such as (,), <, or >.

     When the upload is complete, the parser override file is listed in the table on the **Parser Overrides** tab.

To download the parser override file to a container:

1. Click **Administration > Repositories.**
2. Click **Parser Overrides** under the **Repositories** section in the management panel.

3. In the table on the **Parser Overrides** tab, locate the parser override file you want to download and click the up arrow next to the file.
4. Follow the wizard to select the container to which you want to add the parser overrides.

   When the wizard completes, the parser overrides are deployed in the selected container.

   > **Note:** You can download a parser override file from ArcSight Marketplace. For more information, refer to "Sharing Connectors in ArcSight Marketplace" on page 877.

To verify that the parser override has been applied successfully, issue a Get Status command to the connector. See "Sending a Command to a Connector" on page 873. In the report that appears, check for the line starting with `ContentInputStreamOverrides`.

Audit Logs

The following topics are discussed here.

Audit Event Types

You can forward ArcMC application audit events, which are in Common Event Format (CEF), to a destination of your choice.

Several types of audit events are generated by ArcMC:

- **Application events:** related to ArcMC functions and configuration changes
- **Platform events:** related to the ArcMC system
- **System health events:** related to ArcMC health.

Audit Event Information

An ArcMC audit event contains information about the following prefix fields.

- Device Event Class ID
- Device Severity
- Name
- Device Event Category (`cat`)

See Audit Logs for details on how to generate audit logs.

> **Note:** If no Syslog Daemon connector is installed or configured on your local host, then no audit events will be visible.

Application Events

Application Events

Signature	Severity	Description	deviceEventCategory
Connector			
connector:101	1	Register connector successful	/Connector/Add/Success
connector:102	1	Connector removed successfully	/Connector/Delete
connector:103	1	Update connector parameters successful	/Connector/Parameter/Update/ Success
connector:104	1	AUP Package create successful	/Connector/AUP Package/Create/Success
connector:105	1	AUP Package deploy successful	/Connector/AUP Package/Deploy/Success
connector:201	1	Connector add failed	/Connector/Add/Fail
connector:202	1	Connector delete failed	/Connector/Delete/Fail
connector:203	1	Connector parameters update failed	/Connector/Parameter/Update/ Fail
ArcMC			
arcmc:101	1	ConfigurationBackupScheduler add success	/BackupScheduler/Add/Success
arcmc:102	1	ConfigurationBackupScheduler update successful	/BackupScheduler/Update/ Success
arcmc:103	1	ConfigurationBackupScheduler delete success	/BackupScheduler/Delete/ Success
arcmc:104	1	Scheduled Backup triggered	/Backup/Scheduled/Trigger
arcmc:105	1	Scheduled Backup completed	/Backup/Scheduled/Complete/Success
arcmc:106	1	Manual Backup completed	/Backup/Manual/Complete/ Success
arcmc:107	1	Local Backup completed	/Backup/Local/Complete/ Success

Application Events, continued

Signature	Severity	Description	deviceEventCategory
arcmc:108	1	You have exceeded the maximum number of managed connectors allowed by your license	/RemotelyManagedConnectors/Exceeded
arcmc:110	1	You have attempts to exceed the maximum number of managed products allowed by your license	/managedproducts/exceeded
arcmc:111	1	Reboot command launched successfully	Node/reboot/launched/Success
arcmc:112	1	New configuration created successfully	/Configuration/Add/Success
arcmc:113	1	Edit configuration succesful	/Configuration/Edit/Success
arcmc:114	1	Delete configurations successful	/Configuration/Delete/Success
arcmc:115	1	Push configuration successful	/Configuration/Push/Success
arcmc:116	1	Import configuration successful	/Configuration/Import/Success
arcmc:117	1	Add subscriber to configuration successful	/Configuration/Subscribe/Success
arcmc:118	1	Unsubscribe node for configuration successful	/Configuration/Unsubscribe/Success
arcmc:119	1	Check compliance of configuration successful	/Configuration/Check Compliance/Success
arcmc:120	1	Configuration set successfully	/Node/Set/Configuration/Success
arcmc:121	1	Configuration appended successfully	/Node/Append/Configuration/Success
arcmc:122	1	Agent install success	/ArcMCAgent/Install/Success
arcmc:123	1	Upgrade agent successfully	/ArcMCAgent/Upgrade/Success
arcmc:124	1	Add/Push Logger Peers Successful	/Logger/AddPeers/Success

Application Events, continued

Signature	Severity	Description	deviceEventCategory
arcmc:125	1	Remove Logger Peers Successful	/Logger/RemovePeers/Success
arcmc:127	1	Create/Import Logger Peer Group Successful	/Logger/AddPeerGrp/Success
arcmc:128	1	Delete Logger Peer Group Successful	/Logger/DeletePeerGrp/Success
arcmc:129	1	Edit Logger Peer Group Successful	/Logger/EditPeerGrp/Success
arcmc:130	1	Import Initial Configuration Successful	/Logger/ImportInitConfig/Success
arcmc:131	1	Pushed Initial Configuration	/Logger/PushInitConfig/Success
arcmc:132	1	Deleted Initial Configuration	/Logger/DelInitConfig/Success
arcmc:133	1	Host upgrade started.	/Node/Upgrade/Start
arcmc:134	1	Host upgrade successful.	/Node/Upgrade/Success
arcmc:138	1	Update rule/s	/ArcMC/UpdateRules/Success
arcmc142	1	Rule add success	/ArcMC/AddRule" + SUCCESS
arcmc143	1	Rule delete success	/ArcMC/DeleteRule" + SUCCESS
arcmc:201	1	ConfigurationBackupScheduler add failed	/BackupScheduler/Add/Fail
arcmc:202	1	ConfigurationBackupScheduler update failed	/BackupScheduler/Update/Fail
arcmc:203	1	ConfigurationBackupScheduler delete failed	/BackupScheduler/Delete/Fail
arcmc:205	1	Scheduled Backup failed	/Backup/Scheduled/Complete/Fail
arcmc:206	1	Manual Backup failed	/Backup/Manual/Complete/Fail
arcmc:212	1	New configuration creation failed	/Configuration/Add/Fail
arcmc:213	1	Edit configuration failed	/Configuration/Update/Fail
arcmc:214	1	Configuration deletion failed	/Configuration/Delete/Fail
arcmc:215	1	Push configuration failed	/Configuration/Import/Fail

Application Events, continued

Signature	Severity	Description	deviceEventCategory
arcmc:216	1	Import configuration failed	/Backup/Local/Push/Fail
arcmc:217	1	Add subscriber to configuration failed	/Configuration/Subscribe/Fail
arcmc:218	1	Unsubscribe node for configuration failed	/Configuration/Unsubscribe/Fail
arcmc:219	1	Check compliance of configuration failed	/Configuration/Check Compliance/Success
arcmc:220	1	Configuration set failed	/Node/Set/Configuration/ Fail
arcmc:221	1	Configuration append failed	/Node/Append/Configuration/ Fail
arcmc:222	1	Agent install failed	/ArcMCAgent/Install/Failure
arcmc:223	1	Upgrade agent failed	/ArcMCAgent/Upgrade/Fail
arcmc:224	1	Add/Push Logger Peers Failed	/Logger/AddPeers/Fail
arcmc:225	1	Remove Logger Peers Failed	/Logger/RemovePeers/Fail
arc mc:226	1	Alert message payload	/ArcMCMonitor/Breach
arcmc:230	1	Import Initial Configuration Failed	/Logger/ImportInitConfig/Fail
arcmc:234	1	Host upgrade failed.	/Node/Upgrade/Fail
arcmc:250	1	Push user assignment <assignment name>	/ArcMCUM/Push
arcmc:251	1	Decommission user <UserName>	/ArcMCUM/DeleteUser
arcmc:252	1	Add user <UserName>	/ArcMCUM/AddUser
Destination			
destination:102	1	Update destination successful	/Connector/Destination/Update/Success
destination:103	1	Remove destination successful	/Connector/Destination/Delete/Success
destination:104	1	Update destination configuration successful	/Connector/Destination/ Configuration/Update/Success

Application Events, continued

Signature	Severity	Description	deviceEventCategory
destination:105	1	Register destination successful	/Connector/Destination/Registration/Success
destination:106	1	Create destination configuration successful	/Connector/Destination/Configuration/Add/Success
destination:107	1	Destination configuration delete successful	/Connector/Destination/Configuration/Delete/Success
destination:202	1	Destination update to a connector failed	/Connector/Destination/Update/Fail
destination:203	1	Destination delete from a connector failed	/Connector/Destination/Delete/Fail
destination:204	1	Destination configuration update failed	/Connector/Destination/Configuration/Update/Fail
destination:205	1	Register destination failed	/Connector/Destination/Registration/Fail
destination:206	1	Destination configuration add failed	/Connector/Destination/Configuration/Add/Fail
destination:207	1	Destination configuration delete failed	/Connector/Destination/Configuration/Delete/Fail
Container			
container:101	1	Container upgrade successful	/Container/Upgrade/Success
container:102	1	Push user file successful	/Container/UserFiles/Push/Success
container:103	1	User file delete from container	/Container/UserFiles/Delete
container:104	1	CA cert push to a container successful	/Container/CACert/Push/Success
container:105	1	Container demo CA enable successful	/Container/DemoCA/Enable/Success
container:106	1	Container demo CA disable successfu	/Container/DemoCA/Disable/Success
container:109	1	Delete property from a container successful	/Container/Property/Delete/Success
container:110	1	Modify properties successful	/Container/Property/Update/Success

Application Events, continued

Signature	Severity	Description	deviceEventCategory
container:111	1	Container password update successful	/Container/Password/Update/Success
container:112	1	Container add successful	/Container/Add/Success
container:113	1	Container edit	/Container/Update
container:114	1	Remove container	/Container/Delete
container:115	1	Add certificate for a container successful	/Container/Certificate/Add/Success
container:116	1	Removing certificates successful [addtrust class 1ca]	/Container/Certificate/Delete/Success
container:117	1	Enabling FIPS mode successful	/Container/FIPS/Enable/Success
container:118	1	Disabling FIPS mode successful	/Container/FIPS/Disable/Success
container:119	1	Upgrade was triggered for container that resides on end of life appliance model	Container/FromEndOfLifeModel/Upgrade/Triggered
container:123	1	Emergency restore failed	/Container/EmergencyRestore/Fail
container:201	1	Container upgrade failed	/Container/Upgrade/Fail
container:202	1	User file push to a container failed	/Container/UserFiles/Push/Fail
container:204	1	CA cert push to a container failed	/Container/CACert/Push/Fail
container:205	1	Enable demo CA for a container failed	/Container/DemoCA/Enable/Fail
container:206	1	Disable demo CA for a container failed	/Container/DemoCA/Disable/Fail
container:209	1	Delete property from a container failed	/Container/Property/Delete/Fail
container:210	1	Update property to a container failed	/Container/Property/Update/Fail
container:211	1	Container password update failed	/Container/Password/Update/Fail
container:212	1	Container add failed	/Container/Add/Fail

Application Events, continued

Signature	Severity	Description	deviceEventCategory
container:215	1	Add certificate for a container failed	/Container/Certificate/Add/Fail
container:216	1	Delete certificate for a container failed	/Container/Certificate/Delete/Fail
container:217	1	Enable FIPS on a container failed	/Container/FIPS/Enable/Fail
container:218	1	Disable FIPS on a container failed	/Container/FIPS/Disable/Fail
container:219	1	SSL Certificate downloaded successfully	/Container/Certificate/Download/Success
container:220	1	SSL Certificate download failed	/Container/Certificate/Download/Fail
container:221	1	SSL Certificate imported successfully	/Container/Certificate/Import/Success
container:222	1	SSL Certificate import failed	/Container/Certificate/Import/Fail
container:226	1	Emergency restore successful	/Container/EmergencyRestore/Success
container:301	1	Container upgrade started	/Container/Upgrade/Start
Transformation Hub			
eventbroker:146	1	Transformation Hub Add Topic succesful	/EventBroker/Topic/Add/Success
eventbroker:147	1	Transformation Hub delete route/s successful	/EventBroker/Route/Add/Success
eventbroker:148	1	Transformation Hub Add Route/s successful	/EventBroker/Route/Add/Success
eventbroker:149	1	Transformation Hub Update Route successful	/EventBroker/Route/Update/Success
eventbroker:241	1	Transformation Hub Add Topic failed	/EventBroker/Topic/Add/Fail
eventbroker:242	1	Transformation Hub delete route/s failed	/EventBroker/Route/Add/Fail
eventbroker:243	1	Transformation Hub Add Route failed	/EventBroker/Route/Add/Fail

Application Events, continued

Signature	Severity	Description	deviceEventCategory
eventbroker:244	1	Transformation Hub Update Route failed	/EventBroker/Route/Update/Fail
Location			
location:101	1	Location add successful	/Location/Add/Success
location:102	1	Location edit	/Location/Update
location:103	1	Remove location	/Location/Delete
location:201	1	Location add failed	/Location/Add/Fail
Host			
host:101	1	Host add successful	/Host/Add/Success
host:103	1	Remove host	/Host/Delete
host:105	1	Host certificate download and import successful	/Host/Certificate/Download /Import/Success
host:201	1	Host add failed	/Host/Add/Fail
host:205	1	Host certificate download and import failed	/Host/Certificate/Download Import/Fail
host:363	1	Move Host Success	/Host/Move/Success
host:364	1	Move Host Fail	/Host/Move/Fail
Marketplace			
marketplace:150	1	Successfully saved Marketplace user in ArcMC	/Marketplace/User/Add/Success
marketplace:245	1	Failed to save Marketplace user in ArcMC	/Marketplace/User/Add/Fail
Deployment Templates			
deploymenttemplates: 151	1	Successfully deleted template instance(s) in ArcMC	/DeploymentTemplates/TemplateInstance/Delete /Success
deploymenttemplates: 246	1	Failed to delete template instance(s) in ArcMC	/DeploymentTemplates/TemplateInstance/Delete /Fail
deploymenttemplates: 152	1	Successfully added template instance in ArcMC	/DeploymentTemplates/TemplateInstance/Add/S uccess

Application Events, continued

Signature	Severity	Description	deviceEventCategory
deploymenttemplates:247	1	Failed to add template instance in ArcMC	/DeploymentTemplates/TemplateInstance/Add/Fail
deploymenttemplates:153	1	Successfully updated template instance in ArcMC	/DeploymentTemplates/TemplateInstance/Update/Success
deploymenttemplates:248	1	Failed to update template instance in ArcMC	/DeploymentTemplates/TemplateInstance/Update/Fail
Generator ID			
generatorid:157	1	Generate ID create successful	/GeneratorID/Add/Success
generatorid:251	1	Generate ID create failed	/GeneratorID/Add/Fail
generatorid:158	1	Generate ID edit successful	/GeneratorID/Update/Success
generatorid:158	1	Generate ID edit failed	/GeneratorID/Update/Fail
generatorid:159	1	Generate ID delete successful	/GeneratorID/Delete/Success
generatorid:159	1	Generate ID delete failed	/GeneratorID/Delete/Fail

Platform Events

Platform Events

Signature	Severity	Definition	Category
platform:200	7	Failed password change	/Platform/Authentication/PasswordChange/Failure
platform:201	7	Failed login attempt	/Platform/Authentication/Failure/Login
platform:202	5	Password changed	/Platform/Authentication/Password
platform:203	7	Login attempt by inactive user	/Platform/Authentication/InactiveUser/Failure
platform:205	7	Automated password reset attempt made for admin account	/Platform/Authentication/PasswordChange/AdminFailure

Platform Events, continued

Signature	Severity	Definition	Category
platform:206	7	Failed automated password reset attempt for user	/Platform/Authentication/PasswordChange/Failure
platform:207	7	Automated password reset attempted for non-existent user	/Platform/Authentication/PasswordChange/UnknownUser
platform:213	7	Audit forwarding modified	/Platform/Configuration/Global/AuditEvents
platform:220	5	Installed certificate	/Platform/Certificate/Install
platform:221	7	Certificate mismatch failure	/Platform/Certificate/Mismatch
platform:222	1	Created certificate signing request	/Platform/Certificate/Request
platform:224	5	Re-generate self-signed certificate	/Platform/Certificate/Regenerate
platform:226	7	Uploaded update file damaged or corrupt	/Platform/Update/Failure/CorruptPackage
platform:227	5	Update installation success	/Platform/Update/Applied
platform:228	7	Update installation failure	/Platform/Update/Failure/Installation
platform:230	3	Successful login	/Platform/Authentication/Login
platform:234	7	Failed login attempt (LOCKED)	/Platform/Authentication/Failure/LOCKED
platform:239	1	User logout	/Platform/Authentication/Logout
platform:240	3	Added user group	/Platform/Groups/Add
platform:241	3	Updated user group	/Platform/Groups/Update
platform:242	5	Removed all members from group	/Platform/Authorization/Groups/Membership/Update/Clear
platform:244	3	Deleted user group	/Platform/Groups/Remove
platform:245	3	Added user	/Platform/Users/Add
platform:246	3	Updated user	/Platform/Users/Update
platform:247	3	Deleted user	/Platform/Users/Delete
platform:248	3	Session expired	/Platform/Authentication/Logout/SessionExpiration

Platform Events, continued

Signature	Severity	Definition	Category
platform:249	7	Account locked	/Platform/Authentication/AccountLocked
platform:250	3	Added remote mount point	/Platform/Storage/RFS/Add
platform:251	5	Edited remote mount point	/Platform/Storage/RFS/Edit
platform:252	7	Failed to create remote mount point	/Platform/Storage/RFS/Failure
platform:253	5	Removed remote mount point	/Platform/Storage/RFS/Remove
platform:260	5	Static route modified	/Platform/Configuration/Network/Route/Update
platform:261	5	Static route removed	/Platform/Configuration/Network/Route/Remove
platform:262	5	Appliance time modified	/Platform/Configuration/Time
platform:263		NIC settings modified	/Platform/Configuration/NIC
platform:264		NTP server settings modified	/Platform/Configuration/NTP
platform:265	5	DNS settings modified	/Platform/Configuration/Network/DNS
platform:266	5	Hosts file modified	/Platform/Configuration/Network/Hosts
platform:267	5	SMTP settings modified	/Platform/Configuration/SMTP
platform:268	5	Static route added	/Platform/Configuration/Network/Route/Add
platform:269	5	Updated Platform Settings	/Platform/Configuration
platform:280	7	Appliance reboot initiated	/Appliance/State/Reboot/Initiate
platform:281	3	Appliance reboot canceled	/Appliance/State/Reboot/Cancel
platform:282	9	Appliance poweroff initiated	/Appliance/State/Shutdown
platform:284	5	Enabled SAN Multipathing	/Platform/Storage/Multipathing/Enable
platform:285	5	Disabled SAN Multipathing	/Platform/Storage/Multipathing/Disable

Platform Events, continued

Signature	Severity	Definition	Category
platform:300	5	Installed trusted certificate	/Platform/Certificate/Install
platform:301	5	Installed certificate revocation list	/Platform/Certificate/Revocation/Install
platform:302	5	Deleted trusted certificate	/Platform/Certificate/Delete
platform:303	5	Deleted certificate revocation list	/Platform/Certificate/Revocation/Delete
platform:304	7	Failed installing trusted certificate	/Platform/Certificate/Install/Failure
platform:305	7	Failed installing certificate revocation list	/Platform/Certificate/Revocation/Install/Failure
platform:306	5	Start process	/Platform/Process/Start
platform:307	5	Stop process	/Platform/Process/Stop
platform:308	5	Restart process	/Platform/Process/Restart
platform:310	5	Enabled FIPS mode	/Platform/Configuration/FIPS/Enable
platform:311	7	Disabled FIPS mode	/Platform/Configuration/FIPS/Disable
platform:312	7	Web server cipher strength changed	/Platform/Configuration/WebServer/CipherStrength
platform:313	5	Enable SSH	/Platform/Configuration/SSH/Enable
platform:314	7	Disable SSH	/Platform/Configuration/SSH/Disable
platform: 315	7	Enable SSH only during startup/reboot	/Platform/Configuration/SSH/StartupOnly
platform:316	7	Enable SSH only for 8 hours	/Platform/Configuration/SSH/Enable8Hours
platform: 320	3	Appliance poweroff canceled	/Appliance/State/Shutdown/Cancel
platform:371	5	Restarted OS service	/Platform/Service/Restart
platform:400	1	Ran diagnostic command	/Platform/Diagnostics/Command
platform:407	7	SSL certificate expiration warning	/Platform/Certificate/SSL/Expiration
platform:408	5	Appliance startup completed	/Appliance/State/Startup

Platform Events, continued

Signature	Severity	Definition	Category
platform:409	3	Configure login warning banner	/Platform/Configuration/LoginBanner
platform:410	3	Network settings modified	
platform:411	5	Automated password reset	/Platform/Authentication/PasswordChange
platform:412	3	Set locale	/Platform/Configuration/Locale
platform:440	3	SNMP configuration modified	Platform/Configuration/SNMP
platform:450	3	FTP service enabled	
platform:451	3	FTP service disabled	
platform:454	3	FTP service configuration changed	
platform:455	3	Added sub directory	
platform:456	3	Removed sub directory	
platform:460	3	NIC alias added	/Platform/Network/Alias/Add
platform:462	3	NIC alias removed	/Platform/Network/Alias/Remove
platform:500	5	Remove member from group	/Platform/Authorization/Groups/Membership/Remove
platform:501	5	Group member added	/Platform/Authorization/Groups/Membership/Add
platform:502	5	User removed from group	/Platform/Authorization/Users/Groups/Remove
platform:503	5	User added to group	/Platform/Authorization/Users/Groups/Add
platform:530	5	Authentication Session settings successfully changed	/Platform/Configuration/Authentication/Sessions/Success
platform:540	5	Password Lockout settings successfully updated	/Platform/Configuration/Authentication/Password/Lockout/Success
platform:550	5	Password Expiration settings successfully updated	/Platform/Configuration/Authentication/Password/Expiration/Success

Platform Events, continued

Signature	Severity	Definition	Category
platform:560	5	Password Validation settings successfully updated	/Platform/Configuration/Authentication/Password/Validation/Success
platform:570	5	Allow Automated Password Reset settings successfully changed	/Platform/Configuration/Authentication/Password/AutomatedReset/Success
platform:590	5	RADIUS authentication settings successfully changed	/Platform/Configuration/Authentication/RADIUS/Success
platform:600	5	LDAP authentication settings successfully changed	/Platform/Configuration/Authentication/LDAP/Success
platform:610	5	Global authentication settings successfully changed	/Platform/Configuration/Authentication/Global/Success

System Health Events

System health events provide four status indicators:

- OK
- Degraded
- Rebuilding
- Failed

An **OK** event, indicating normal system behavior, is generated once every ten minutes (six events per hour, per sensor). For a status other than **OK** (**Degraded**, **Rebuilding**, or **Failed**), the event is sent every minute until the sensor returns an **OK** status.

SNMP Related Properties

The following list provides the event fields for system health events sent via SNMP traps. For detailed instructions on setting up SNMP traps, see SNMP.

• event.deviceReceiptTime	• event.endTime
• event.deviceVendor	• event.deviceProduct
• event.deviceVersion	• event.deviceEventClassId
• event.name	• event.deviceSeverity

• event.deviceEventCategory	• event.deviceCustomNumber1
• event.deviceCustomNumber1Label	• event.deviceCustomString1
• event.deviceCustomString1Label	• event.deviceCustomString2
• event.deviceCustomString2Label	• event.deviceCustomString3
• event.deviceCustomString3Label	• event.deviceCustomString4
• event.deviceCustomString4Label	• event.deviceCustomString5
• event.deviceCustomString5Label	• event.deviceCustomString6
• event.deviceCustomString6Label	• event.destinationAddress
• event.deviceAddress	

The **snmp.mib.version** is set to 5.0.

System Health Events

Signature	Severity	Definition	Category
CPU			
cpu:100	1	CPU Usage	/Monitor/CPU/Usage
cpu:101	1	Health statistics per CPU	/Monitor/CPU*n*/Usage
Disk			
disk:101	1	Root Disk Space Remaining	/Monitor/Disk/Space/Remaining/Data
disk:102	1	Disk bytes read	/Monitor/Disk/*drive*/Read
disk:103	1	Disk bytes written	/Monitor/Disk/*drive*/Write
disk:104	1	Disk Space Remaining	/Monitor/Disk/Space/Remaining/Root
Hardware			
hardware:101	1	Electrical (Current) OK	/Monitor/Sensor/Current/Ok**
hardware:102	5	Electrical (Current) Degraded	/Monitor/Sensor/Current/Degraded**
hardware:103	8	Electrical (Current) Failed	/Monitor/Sensor/Current/Failed**
hardware:111	1	Electrical (Voltage) OK	/Monitor/Sensor/Voltage/Ok**
hardware:112	1	Electrical (Voltage) Degraded	/Monitor/Sensor/Voltage/Degraded**
hardware:113	1	Electrical (Voltage) Failed	/Monitor/Sensor/Voltage/Failed**
hardware:121	1	Battery OK	/Monitor/Sensor/Battery/Ok**
hardware:122	5	Battery Degraded	/Monitor/Sensor/Battery/Degraded **
hardware:123	8	Battery Failed	/Monitor/Sensor/Battery/Failed**
hardware:131	1	Fan OK	/Monitor/Sensor/Fan/Ok

System Health Events, continued

Signature	Severity	Definition	Category
hardware:132	5	Fan Degraded	/Monitor/Sensor/Fan/Degraded
hardware:133	8	Fan Failed	/Monitor/Sensor/Fan/Failed
hardware:141	1	Power Supply OK	/Monitor/Sensor/PowerSupply/Ok
hardware:142	5	Power Supply Degraded	/Monitor/Sensor/PowerSupply/Degraded
hardware:143	8	Power Supply Failed	/Monitor/Sensor/PowerSupply/Failed
hardware:151	1	Temperature OK	/Monitor/Sensor/Temperature/Ok
hardware:152	1	Temperature Degraded	/Monitor/Sensor/Temperature/Degraded
hardware:153	1	Temperature Failed	/Monitor/Sensor/Temperature/Failed
Memory			
memory:100	1	Platform memory usage	/Monitor/Memory/Usage/Platform
memory:101	1	Health statistics for JVM memory	/Monitor/Memory/Usage/Jvm
memory:102	1	Health statistics for platform buffers memory	/Monitor/Memory/Usage/Platform/Buffers
memory:103	1	Health statistics for platform cached memory	/Monitor/Memory/Usage/Platform/Cached
memory:104	1	Health statistics for platform free memory	/Monitor/Memory/Usage/Platform/Free
memory:105	1	Health statistics for JVM heap memory	/Monitor/Memory/Usage/Jvm/Heap
memory:106	1	Health statistics for JVM non-heap memory	/Monitor/Memory/Usage/Jvm/NonHeap
Network			
network:100	1	Network usage—Inbound	/Monitor/Network/Usage/*iface*/In
network:101	1	Network usage—Outbound	/Monitor/Network/Usage/*iface*/Out
network:200	1	Number of Apache connections	
NTP			
ntp:100	1	NTP synchronization	
RAID			
raid:101	1	RAID Controller OK	/Monitor/RAID/Controller/OK
raid:102	5	RAID Controller Degraded	/Monitor/RAID/Controller/Degraded
raid:103	8	RAID Controller Failed	/Monitor/RAID/Controller/Failed

System Health Events, continued

Signature	Severity	Definition	Category
raid:111	1	RAID BBU OK	/Monitor/RAID/BBU/Ok
raid:112	5	RAID BBU Degraded	/Monitor/RAID/BBU/Degraded
raid:113	8	RAID BBU Failed	/Monitor/RAID/BBU/Failed
raid:121	1	RAID Disk OK	/Monitor/RAID/DISK/Ok
raid:122	5	RAID Disk Rebuilding	/Monitor/RAID/DISK/Rebuilding
raid:123	8	RAID Disk Failed	/Monitor/RAID/DISK/Failed

Managing Intelligence

All the topics in this section apply only if you have upgraded Intelligence with the ArcSight Platform.

This section provides guidance for managing Intelligence functions and features within the deployment.

Enabling Windowed Analytics

By default, Intelligence is configured to run Analytics in batch mode. When new data is ingested, Analytics is run on both the new and the existing data. Although this process is beneficial when you first deploy Intelligence (for testing and validation purposes), running Analytics on the entirety of your data on an ongoing basis unnecessarily uses system resources. Instead, you can enable Windowed Analytics.

When you enable Windowed Analytics, you configure Intelligence to run Analytics only on newly ingested data as determined by the date of the last Analytics run and the timestamp of the data. Intelligence identifies the data it has already analyzed, then runs Analytics only on the new data. These results are then aggregated with the existing results to produce updated, current Analytics results for the entire data set.

Windowed Analytics has a positive impact on performance and stability because it allows the system to analyze and aggregate smaller, more consistently sized quantities of data than batch mode, particularly as the total amount of data in your system continues to grow.

Important: After you have validated the initial data ingest and Analytics run for your Intelligence cluster, you might need to ingest and analyze historical data. In this scenario, you must continue to run Analytics in batch mode to ensure that all data is included.

To enable Windowed Analytics:

1. Open a certified web browser.
2. Specify the following URL to log in to the OMT Management Portal: https://<OMT_masternode_hostname or virtual_ip hostname>:5443.
3. Select **Deployment** > **Deployments**.
4. Click ... (Browse) on the far right and choose **Reconfigure**. A new screen will be opened in a separate tab.
5. Click **Intelligence** and disable **Batch Processing**.
6. Click **Save**.

> The first Windowed Analytics run performs a full batch run to establish the baseline for the system going forward. The second and subsequent runs occur as Windowed Analytics.

Configuring the 'Peek-Back' Window for Windowed Analytics

The 'peek-back' window is a best-effort buffer that ensures that delayed or out-of-order data is not missed between Windowed Analytics runs. For more information on configuring the peek-back window, see the *Configuring the 'Peek-Back' Window for Windowed Analytics* section in the ArcSight Intelligence 24.2 User's Guide.

Running Analytics on Demand

Before you run Analytics on Demand, do the following:

1. To ensure that Analytics is not currently running, run the following command on any worker or master node to confirm:

```
ANALYTICS_POD=$(kubectl get pods -n $(kubectl get namespaces | awk
'/arcsight/ {print $1}') |awk '/interset-analytics/ {print $1}') ;
kubectl exec -it -n $(kubectl get namespaces | awk '/arcsight/ {print
$1}') ${ANALYTICS_POD} -c interset-analytics -- ls -l /tmp/interset_lock/
```

2. If Analytics is currently running, the output of this command will be:

```
=> tenant_0.lock
```

   In this case, wait for Analytics to complete running before proceeding. The command can be run periodically to monitor the status of Analytics.

3. If the previous Analytics execution failed, check whether the properties in the Intelligence tab are set correctly. If this does not solve the issue, contact OpenText Customer Support.

To run Analytics on demand:

1. Launch a terminal session and log in to the NFS node.
2. Navigate to the following directory:

```
cd <NFSVolume>/interset/analytics
```

3. (Conditional) Delete the `blackhawk_down` file, if present. This is an error file and it is generated if the previous Analytics execution fails.

```
rm blackhawk_down
```

4. When prompted whether you want to delete the file, enter yes.
5. Execute the following command to delete the latest `AnalyticsStarted.mk` and `AnalyticsCompleted` files:

```
rm -rf AnalyticsStarted-0-<Today's_date>.mk AnalyticsCompleted-0-
<Today's_date>.mk
```

6. When prompted whether you want to delete the files, enter yes.

   After 30 seconds of deletion of the files, Analytics is triggered automatically.

Changing Passwords for a Secure Environment

You can change the passwords for the components during deployment and also at any point after deployment, as needed.

1. Open a certified web browser.
2. Specify the following URL to log in to the OMT Management Portal: https://<OMT_ masternode_hostname or virtual_ip hostname>:5443.
3. Select **Deployment** > **Deployments**.
4. Click ... (Browse) on the far right and choose **Reconfigure**. A new screen will be opened in a separate tab.
5. Click **Intelligence** and modify the passwords.
6. Click **Save**.

Changing the Elasticsearch Node Data Path

To change the Elasticsearch node data path, perform the following steps:

1. Launch a terminal session and as a root user, log in to a worker node labeled as **intelligence:yes**.
2. Execute the following commands to scale down the Elasticsearch master node and Elasticsearch data nodes:

```
export NS=$(kubectl get namespaces |grep arcsight|cut -d ' ' -f1)
kubectl -n $NS scale statefulset elasticsearch-master --replicas=0
kubectl -n $NS scale statefulset elasticsearch-data --replicas=0
```

3. (Conditional) To create an Elasticsearch data directory in the NFS server, log in to the server.
4. (Conditional) To create a new Elasticsearch data directory in a worker node labeled as **intelligence:yes**, log in to the node.
5. Execute the following commands to create a new directory:

```
cd <path to create the new directory>
mkdir <new directory in the path>
```

> If you are creating a new directory in the NFS server, ensure that the directory is accessible or mounted on all the worker nodes labeled as **intelligence:yes**. The Elasticsearch data directory in the NFS server might impact the system performance.

6. Execute the following command to copy data from the existing directory to the new directory:
   - To copy the data to a worker node labeled as **intelligence:yes**:

     ```
     cp -rf <existing_directory_path> <new_directory_path>
     ```

     For example:

     ```
     cp -rf /opt/arcsight/k8s-hostpath-volume/interset
     /opt/arcsight/testpath/
     ```

     In this example, the existing directory path `/opt/arcsight/k8s-hostpath-volume/interset` and the new directory path is `/opt/arcsight/testpath/`.

   - To copy the data to the NFS server:

     ```
     scp -rf <existing_directory_path> root@<ip address or hostname of
     the NFS server>:<new_directory_path>
     ```

7. Execute the following command to change the permissions of the new directory:

```
chown 1999:1999* <new_directory_path>
```

For example:

```
chown 1999:1999* /opt/arcsight/testpath/
```

8. If you have created a new Elasticsearch directory in a worker node labeled as **intelligence:yes**, then repeat Steps 4 to 7 on all the worker nodes labeled as **intelligence:yes**.
9. Open a certified web browser.
10. Specify the following URL to log in to the OMT Management Portal: https://<OMT_masternode_hostname or virtual_ip hostname>:5443.
11. Select **Deployment** > **Deployments**.
12. Click ... (Browse) on the far right and choose **Reconfigure**. A new screen will be opened in a separate tab.
13. Click **Intelligence** and provide the new value of the Elasticsearch directory path in the **Elasticsearch Node Data Path to persist data to** field.
14. Click **Save**.
15. Launch a terminal session and as a root user, log in to a worker node labeled as **intelligence:yes**.
16. Execute the following commands to scale up the Elasticsearch master node and Elasticsearch data nodes:

```
export NS=$(kubectl get namespaces |grep arcsight|cut -d ' ' -f1)
kubectl -n $NS scale statefulset elasticsearch-master --replicas=1
kubectl -n $NS scale statefulset elasticsearch-data --replicas=<number_
of_replicas>
```

17. Execute the following curl command on any Kubernetes node and verify the status of the Elasticsearch cluster:

```
curl -k "https://<Elasticsearch_username:Elasticsearch_password>@<ip
address or hostname of the OMT>:31092/_cluster/health"
```

Enabling Elasticsearch to Start on Limited Hardware Sizing

If Elasticsearch is not able to start because of a lack of CPU resources, you can modify the **Elasticsearch Minimum Cores** field in the OMT Management Portal to enable Elasticsearch to start.

1. Open a certified web browser.
2. Specify the following URL to log in to the OMT Management Portal: https://<OMT_masternode_hostname or virtual_ip hostname>:5443.
3. Select **Deployment** > **Deployments**.
4. Click ... (Browse) on the far right and choose **Reconfigure**. A new screen will be opened in a separate tab.
5. Click **Intelligence**.
6. In the **Elasticsearch Configuration** section, modify the value of the **Elasticsearch Minimum Cores** field.

   For example, for a 0.5 CPU, you can specify the corresponding value in any of the following formats:

   - 500m
   - 0.5
7. Click **Save**.

Updating the Logstash Config Map for Custom Data Identifiers

If you are using custom data identifiers (dids) to identify a specific data type or machine users, then you must update the `logstash-config-pipeline` config map with custom data identifiers so that you can view the events or explore the raw events corresponding to the anomalies of the custom dids.

1. Open a certified web browser.
2. Specify the following URL to log in to the **OMT Management Portal**: https://<OMT_masternode_hostname or virtual_ip hostname>:5443.
3. Navigate to **Cluster > Dashboard** to access the Kubernetes Dashboard.
4. Under **Namespace**, search and select the **arcsight-installer-xxxx** namespace.
5. Under **Config and Storage**, click **Config Maps**.
6. Click the filter icon, then search for `logstash-config-pipeline`.
7. Click and select **Edit**.
8. Add the required mapping corresponding to custom did under the 'filter' section of `logstash-config-pipeline`. For example:

```
if [destinationNtDomain] {
 if [destinationNtDomain] in ['','WORKGROUP','NT SERVICE','NT AUTHORITY']
```

```
 {
     mutate {
        replace => {
           "did" => "1"
        }
     }
 }
}
if [destinationUserName] =~ "\$$" {
 mutate
    replace => {
      "did" => "1"
     }
 }
}
```

> If you have upgraded Intelligence, you can update the logstash config map with the custom did mappings used in the previous version of Intelligence, if required. To update, copy the necessary mappings from the logstash-config-pipeline config map that you had backed up prior to the upgrade.

9. Click **Update**.
10. Restart the `interset-logstash` pods:
    a. Launch a terminal session and log in to the master or worker node.
    b. Execute the following command to retrieve the namespace:

    ```
    export NS=$(kubectl get namespaces | grep arcsight|cut -d ' ' -f1)
    ```

    c. Execute the following commands to restart the interset-logstash pods:

    ```
    kubectl -n $NS scale statefulset interset-logstash --replicas=0
    kubectl -n $NS scale statefulset interset-logstash --replicas=3 (set
    as per the environment)
    ```

For more mapping instances for custom dids, contact OpenText Customer Support.

Enabling Custom Model Support

This section provides guidance for enabling custom model support in Intelligence.

Introduction

Intelligence provides support for custom machine learning (ML) models. This support enables you to import trained ML models into Intelligence. Intelligence can then use these models to

run analytics on the incoming data, that is, detect anomalies and generate risk scores for the associated entities, and display the analytics results in the Intelligence dashboard.

The introduction of this feature enables you to enhance Intelligence with models that provide analytics tailored to your unique environments. It also provides a method for extending Intelligence analytics to address new use cases such as the detection of new patterns of unusual behavior.

Important: Intelligence accepts only those custom models that are in the Predictive Model Markup Language (PMML) format and are based on the data types supported by Intelligence.

Supported Algorithms

The following types of algorithms are supported by Intelligence:

- Classification Algorithms
- Anomaly Detection Algorithms

Classification Algorithms

Intelligence supports those classification algorithms that can be stated as classification problems with two classes of output as follows:

- Anomalous
- Non anomalous

The classes can take any name. A classification algorithm must provide a probability for each class.

You must provide one of the two classes in the **targetClass** parameter while **registering the model** (see the ArcSight Intelligence 24.2 User's Guide). This class is used to filter the events that will be considered for determining anomalies.

The following classification algorithms are supported by Intelligence:

- General Regression
- Naïve Bayes
- Neural Network
- Regression
- Rule Set
- Support Vector Machine
- Tree

Anomaly Detection Algorithms

Anomaly Detection algorithms output two values:

- A score on the event.
- A Boolean value indicating if the score is anomalous or not.

These anomaly detection algorithms do not measure the anomalousness of an event, but they give a Boolean value indicating whether the event is anomalous or not. Intelligence interprets a Boolean value of true as an anomalous event and a Boolean value of false as a non anomalous event while calculating the risk scores for the entities associated with the anomalous events.

You must provide one of the two Boolean values in the **targetClass** parameter while **registering the model** (see the ArcSight Intelligence 24.2 User's Guide). This value is used to filter the events that will be considered for determining anomalies.

Supported Data Types

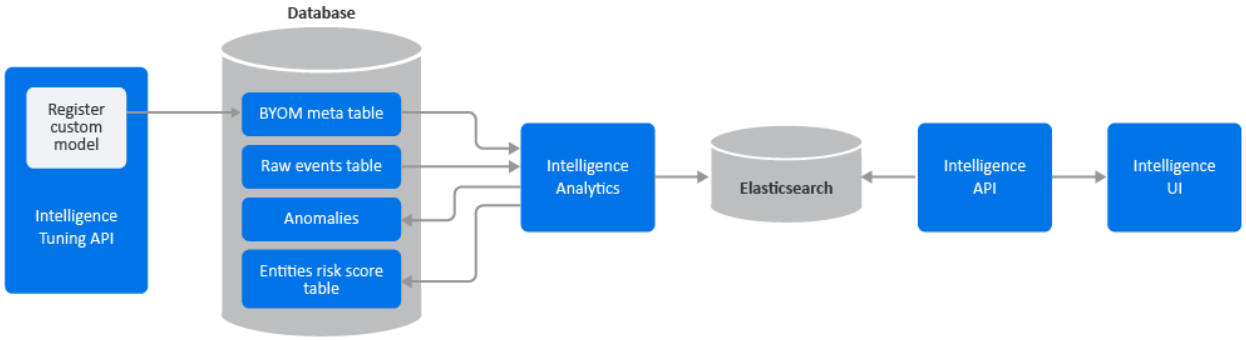
Intelligence supports the ingestion and analysis of data of the following data types:

- **Access**
  The Access schema represents events collected from Identity and Access Management (IAM) solutions where users access resources such as servers or fileshares. For more information on the Access schema, see Access in Intelligence Data Types and Schemas.
- **Active Directory**
  The Active Directory schema represents events collected from Identity and Access Management (IAM) solutions that identify successful and failed logins to authentication targets. These authentication targets include domain controllers/servers, resources, and file shares. For more information on the Active Directory schema, see Active Directory in Intelligence Data Types and Schemas.
- **VPN**
  The VPN schema represents events collected from Identity and Access Management (IAM) solutions or from other VPN devices such as Pulse Secure that identify VPN events. For more information on the VPN schema, see VPN in Intelligence Data Types and Schemas.
- **Web Proxy**
  Web Proxy data are raw events that capture network traffic, primarily Web surfing, from a collection of human users. For more information on the Web Proxy schema, see Web Proxy in Intelligence Data Types and Schemas.
- **Repository**
  Repository data are raw events collected from a source control (repository) system. For more information on the Repository data type, see Repository in Intelligence Data Types and Schemas.

For the supported data types, there are corresponding SmartConnectors and FlexConnectors. For more information, see the **Supported Data Types and Supported SmartConnectors/FlexConnectors Types** section in the *Technical Requirements for ArcSight Platform 24.2*. In addition, for the supported data types, Intelligence provides support for new devices which provide data of relevance to the Intelligence analytics models. For more information, see Adding Support for New Devices. You can also refer to the Ingesting Sample CSV Data section to get an understanding of data ingest.

The Custom Model Support Architecture

The following diagram helps you understand the custom model support architecture:



The following table describes the components involved in the custom model support architecture:

Component	Description
Intelligence Tuning API	API that provides a way of registering a custom model with Intelligence. By registering the model, you are importing the model into Intelligence. This API also allows for the management of the custom models.
Database	When a model is registered through the Intelligence Tuning API, the PMML file and the other metadata of the model are stored in the BYOM_meta table of the database. The database also stores the raw events (incoming data from different data sources) in the Raw events table. In addition to events, the database stores the Intelligence analytics data in the Anomalies table and the Entities risk score table.
Intelligence Analytics	Performs the vital task of determining individual behavioral baselines, then discovering and ranking deviations from those baselines. It reads data from the Raw events table and uses the model with the help of the model data in the BYOM meta table to generate the analytics data, that is, anomalies in the Anomalies table and entities' scores in the Entities risk score table. It also stores the analytics data in Elasticsearch.

Component	Description
Elasticsearch	Elasticsearch is an open source, broadly-distributable and easily-scalable enterprise-grade search engine. Elasticsearch houses all the Intelligence analytics results and raw events, and it provides all the data that drives the user interface.
Intelligence API	Intelligence API reads data from Elasticsearch and provides the REST API from which Intelligence UI gathers the Intelligence analytics results and raw events.
Intelligence UI	Provides a rich user interface that allows you to visually explore the Intelligence analytics results and raw events in the Intelligence dashboard.

Understanding the Custom Model Support Process

The end-to-end Custom Model Support process is as follows:

- **Identify your use case** - Identify the use case on which you need to build your custom model. Intelligence supports the Classification and Anomaly Detection algorithms. For more information, see Supported Algorithms.
- **Identify input data columns** - Before you build your model, ensure that the feature column names of the model match the column names present in the **default_secops_adm.events** input data table. This ensures that all the column names in your sample data set on which you are training your custom model match at least a subset of the columns in the **default_secops_adm.events** table. When analytics is run on the incoming data, only the selected column values are considered for arriving at the results. For more information on the event's table column information, see Understanding the Schema for Events.
- **Create and train your model** - Create your model using your data set and the identified column values. Train the model using the selected data set and create a PMML model file that can represent the derived model.
- **Register a custom model** - Import a custom model into Intelligence by registering it through the API. Registering provides a way to import the model's PMML file and provide other metadata associated with the model. You must provide one of the two classes in the **targetClass** parameter while registering the model. This class is used to filter the events that will be considered to determine anomalies. For more information, see the *Registering a Custom Model* section in the ArcSight Intelligence User's Guide.
- **Run analytics** - The registered model is used in analytics and results are derived for it when analytics is run on the next scheduled time or when you run analytics on demand. For more information on running analytics, see Running Analytics on Demand.
- **View the analytics results on the Intelligence dashboard** – Next, you can view the analytics results and explore the underlying raw events in the Intelligence Dashboard. For

more information, see the *Understanding the Intelligence Dashboard* section in the ArcSight Intelligence User's Guide.

- **Download CSV and PDF reports** - You can view reports that provide you with further insight into risky entities and their behaviors. For more information, see the *Viewing Reports* section in the ArcSight Intelligence User's Guide.

Additional Tasks on Custom Models

You can perform additional tasks with respect to custom models in Intelligence as follows:

- **Manage the custom models** - You can manage the custom models such as activate or deactivate a model, or tune a model. For more information, see Managing Custom Models.
- **Manage alert templates** - An alert template provides a way to describe an anomaly in the Intelligence UI by using the textual information provided as part of the alert template's meta data. You can customize the alert templates associated with a custom model. For more information, see Managing Alert Templates.

Input Data Table Schema

The custom model that you develop for an Intelligence supported data type must be based on the input data table schema of the database. Before you build your model, ensure that the feature column names of the model match the column names present in the input data table. You can refer to the **default_secops_adm.events** input data table present in Understanding the Schema for Events to identify the columns in the events table that must be used for that model. This ensures that all the column names in your sample data set on which you are training your custom model match at least a subset of the columns in the **default_secops_adm.events** table. When analytics is run on the incoming data and a custom model is used, only the selected column values are considered for arriving at the results.

Before You Proceed

Before you register your models and manage them in Intelligence, ensure the following:

- The models are in the PMML format.
- The models are based on the algorithms supported by Intelligence. For more information on the supported algorithms, see Supported Algorithms.
- The models are based on the data types supported by Intelligence. For more information on the data types supported, see Supported Data Types.
- The models are based on the input data table schema. For more information, see Input Data Table Schema.
- The models are trained.

- SmartConnectors and FlexConnectors are configured for data collection. For more information about data collection, see **SmartConnector Installation and User Guide**, **SmartConnector Configuration Guides**, and **ArcSight FlexConnector Developer's Guide** in the ArcSight SmartConnectors 24.2 documentation site. You can also refer to the Ingesting Sample CSV Data section to get an understanding of data ingest.

Managing Custom Models

You can import a custom model into Intelligence by registering it through the API. After registering models, you can also manage them.

For more information, see the Managing Custom Models section in the ArcSight Intelligence 24.2 User's Guide.

Managing Alert Templates

An alert template provides a way to describe an anomaly in the Intelligence UI by using the textual information provided as part of the alert template's meta data. It also helps in associating an anomaly with all the events that triggered it. When you register a model with Intelligence, an anomaly type and an alert template are automatically created for the model. You can customize the created alert templates to suit your needs, create new alert templates, and so on.

For more information, see the **Managing Alert Templates** section in the ArcSight Intelligence 24.2 User's Guide.

Appendix: Ingesting and Exporting Input Data

This section provides guidance on the following:

- Ingesting sample CSV data to the database input data table.
- Exporting data from the database tables to the CSV format.

Ingesting Sample CSV Data to the Input Data Table

SmartConnectors are applications that collect events from different devices, process them, and send them to the desired destinations.

If SmartConnectors are not available for a particular device of an Intelligence-supported data type, you can create FlexConnectors that can read and parse information from the devices and map that information to ArcSight's event schema. FlexConnectors are custom connectors you define to gather security events from log files, databases, and other software and devices. For every FlexConnector that you create, you need to create a corresponding configuration file. A

configuration file is a text file containing properties (name, value pairs) that describe how the FlexConnector parses event data.

This section provides guidance on ingesting sample CSV data of a supported data type (for example, Active Directory) to the **default_secops_adm.events** database input data table with the help of FlexConnectors.

> **Note**:
> - This section goes on the assumption that SmartConnectors are not available for collecting the sample CSV data and that you must create a FlexConnector.
> - This section is intended only for a sample CSV data of the Active Directory data type. If you need to add a new device for any of the Intelligence supported data types, see Adding Support for New Devices.

Configuration File

The configuration file provided in this section is designed only for the sample data set provided here for the Active Directory data type. This configuration file is used by the FlexConnector to parse the CSV data and convert it to the CEF format. The configuration file must be in this format - **<file_name>.sdkfilereader.properties**. For example, **testdata.sdkfilereader.properties**.

Sample CSV Data of the Active Directory Data Type

```
destinationUserName,categoryOutcome,externalId,destinationHostName,deviceRece
iptTime,deviceCustomString5
bennett.merry,Success,4659,OTTAWADC.interset.com,2016-04-01T08:00:04-05:00,
pamila.dankert,Success,4659,NFMC.interset.com,2016-04-01T08:00:18-05:00,
pamila.dankert,Failure,4777,NFMC.interset.com,2016-04-01T08:00:20-05:00,
lakendra.danielson,Success,4634,NFMC.interset.com,2016-04-01T08:00:27-05:00,3
```

Configuration File for the Sample CSV Data

```
delimeter=,
text.qualifier="
comments.start.with=\#
trim.tokens=true
contains.empty.tokens=true

token.count=6

token[0].name=destinationUserName
token[0].type=String
token[1].name=categoryOutcome
token[1].type=String
token[2].name=externalId
```

```
token[2].type=String
token[3].name=destinationHostName
token[3].type=String
token[4].name=deviceReceiptTime
token[4].type=String
token[5].name=deviceCustomString5
token[5].type=String

event.destinationNtDomain=__stringConstant("WIN-MP0VNBBQVSI")
event.categoryBehavior=__stringConstant("/Authentication/Verify")
event.categoryObject=__stringConstant("/Host/Operating System")
event.deviceProduct=__stringConstant("Microsoft Windows")
event.deviceVendor=__getVendor("Microsoft")
event.deviceReceiptTime=__createOptionalTimeStampFromString
(deviceReceiptTime,"YYYY-MM-DDThh:mm:ss.SSSX")
event.destinationUserName=destinationUserName
event.categoryOutcome=categoryOutcome
event.externalId=externalId
event.destinationHostName=destinationHostName
event.deviceCustomString5=deviceCustomString5
```

You can also create or customize the configurations files for other data sets of the supported data types. For more information, see the **FlexConnector Developer's guide** in the ArcSight SmartConnectors 24.2 documentation.

FlexConnector Installation and Configuration

To install and configure a FlexConnector, see the **FlexConnector Developer's guide** in the ArcSight SmartConnectors 24.2 documentation.

Ensure the following when you install and configure the FlexConnector:

- Select **ArcSight FlexConnector File** as the **Connector Type**.
- When adding the parameters information, specify the following:
  - Select **Log Unparsed Events** as **False**.
  - Provide the absolute path and the CSV file name that the FlexConnector needs to read in the **Log File Name** field.
    For example, c:\temp\sample_data.csv.
  - For the **Configuration File** field, specify only the file name that you used in the configuration file.
    For example, if the configuration file is in this format - **testdata.sdkfilereader.properties**, then specify only **testdata**. The suffix

.sdkfilereader.properties is appended automatically. The configuration file name now is **testdata.sdkfilereader.properties**.

- When configuring the destination, select either **CEF File** or **Transformation Hub** as the destination. For more information, see the **SmartConnector Installation and User Guide** in the ArcSight SmartConnectors 24.2 documentation.

Post-Installation Tasks

After you install and configure the FlexConnector and before you run the FlexConnector, copy the configuration file in the **ARCSIGHT_HOME\user\agent\flexagent** location.

Sending Data to the Input Data Table

To send data to the input data table, you need to start the SmartConnector/FlexConnector. You can run the SmartConnector/FlexConnector in standalone mode or as a service, depending on the mode you selected during installation.

Running in Standalone Mode

If you have installed the SmartConnector/FlexConnector in the standalone mode, you need to start it manually (periodically or as per your requirement). Also, you need to start the SmartConnector/FlexConnector whenever the host on which it is installed is restarted, because the SmartConnector/FlexConnector is not automatically active when the host is restarted.

Perform the following steps to start the SmartConnector/FlexConnector agent so that it can send the CSV data to the Transformation Hub topic and which will then be loaded to the database events table.

1. Change to the following directory:

```
cd $ARCSIGHT_HOME\current\bin\
```

2. Execute the following command:

```
./arcsight agents
```

Running as a Windows Service

To start or stop the SmartConnector/FlexConnector installed as a service on the Windows platform:

1. Right-click **My Computer**, then select **Manage** from the **Context** menu.
2. Expand the **Services and Applications** folder and select **Services**.
3. Right-click the SmartConnector/FlexConnector service name and select **Start** to run the SmartConnector/FlexConnector or **Stop** to stop the service.

To verify that the SmartConnector/FlexConnector service has started, view the following file:

```
$ARCSIGHT_HOME/logs/agent.out.wrapper.log
```

To reconfigure the SmartConnector/FlexConnector as a service, run the SmartConnectorConfiguration/FlexConnectorConfiguration Wizard again. Open a command window on $ARCSIGHT_HOME/current/bin and run:

```
./runagentsetup
```

Exporting Data from the Database Tables to the CSV Format

You can export data from the database tables to the CSV format by using VSQL and its output format options. These options can be set either from within an interactive vsql session, or through command-line arguments to the vsql command (making the export process suitable for automation through scripting). After setting VSQL options so it outputs the data in a format your target system can read, you can run a query and capture the result in a CSV file. The procedure mentioned here is for some of the VSQL output format options. To know more about the available output format options, see the **Database Documentation** in the ArcSight Database 24.1 Guide.

To export data from the database tables:

1. Launch a terminal session and log in to a database node.
2. Change to the following directory:

   ```
   cd /opt/vertica/bin/
   ```

3. Log in as a dbadmin:

   ```
   su dbadmin
   ```

4. (Conditional) To create an output file directly from the command line by passing parameters to vsql, execute the following commands:

   ```
   vsql -U username -F ',' -At -o <outputfile_name> -c "SELECT * FROM
   <table_name>;"
   ```

   where:
   - F is used to set the field separator. In this case, because the output is a CSV file, the field separator is ','.
   - At is used to disable the padding and show only the table's tuples in the output file. If you want to show the table headings and the row counts, do not specify t.
   - o is used to send the output to the output file.

- <outputfile_name> is the output file name you need to provide to save the data to, for example, **test.csv**. Ensure that you have write permissions to the output file.
- c is used to run the SQL query
- <table_name> is the table whose data you want to export, for example, **default_secops_adm.events**.

```
[password prompt]
```

5. (Conditional) To create an output file within an interactive vsql session, do the following.
   a. Log in to vsql and specify the password when prompted.

   ```
   vsql
   ```

   ```
   [password prompt]
   ```

   b. Execute the following command to disable padding so as to align the output:

   ```
   \a
   ```

   c. (Optional) Execute the following command to export only the table tuples to the output file:

   ```
   \t
   ```

   d. Execute the following command to set the field separator to export data in the CSV format:

   ```
   \pset fieldsep ','
   ```

   e. Execute the following command to save the output to a file:

   ```
   \o <outputfile_name>
   ```

   where <outputfile_name> is the output file name you need to provide to save the data to, for example, **test.csv**. Ensure that you have write permissions to the output file.

   f. Execute the following command to export data from a database table to the output file you specified in the previous step:

   ```
   select * from <table_name>;
   ```

   where <table_name> is the table whose data you want to export, for example, **default_secops_adm.events**.

   g. Execute the following command to view the data in the output file:

   ```
   \! cat <outputfile_name>
   ```

Adding Support for New Devices

Intelligence supports the ingestion and analysis of data of the following data types:

- Access
- Active Directory
- VPN
- Web Proxy
- Repository

For the supported data types, Intelligence also provides support for new devices that provide data of relevance to the Intelligence analytics models. This section provides information on supporting new devices.

Checklist: Implementation

To add the support for new devices, perform the following tasks in the listed order.

	Task	See
❑	(Conditional) If SmartConnectors are available for the new device, install and configure SmartConnectors for data collection.	SmartConnectors
❑	(Conditional) If SmartConnectors are not available for the new device, install and configure FlexConnectors for data collection.	FlexConnectors
❑	(Conditional) If you have installed and configured FlexConnectors, perform data engineering.	Data Engineering
❑	(Conditional) If you have installed and configured FlexConnectors, perform event categorization.	Event Categorization
❑	Generate SQL Loader Scripts.	SQL Loader Scripts
❑	Update the Intelligence tables required for relations.	Intelligence Tables

SmartConnectors

SmartConnectors are applications that collect events from different devices, process them, and send them to the desired destinations. SmartConnectors are available for the following data types supported by Intelligence:

- Access
- Active Directory
- VPN
- Web Proxy

For more information about the SmartConnectors for the supported data types, see the Supported Data Sources and SmartConnectors/FlexConnectors section. If a new device needs to be supported for any of these data types for which there are corresponding SmartConnectors, then you can configure the SmartConnector for data collection. For more information, see **SmartConnector Installation and User Guide** and **SmartConnector Configuration Guides** in the ArcSight SmartConnectors 24.2 documentation.

FlexConnectors

If there are no SmartConnectors for a new device of the supported data types, you can create FlexConnectors that can read and parse information from the devices and map that information to ArcSight's event schema. FlexConnectors are custom connectors you define to gather security events from log files, databases, and other software and devices. For the data of repository type, that is, GitHub Enterprise, Bitbucket Server, and Perforce, you can create FlexConnectors to collect the data. For every FlexConnector that you create, you need to create a corresponding configuration file. A configuration file is a text file containing properties (name, value pairs) that describe how the FlexConnector parses event data. For more information about FlexConnectors and the configuration files, see the **FlexConnector Developer's guide** in the ArcSight SmartConnectors 24.2 documentation.

Data Engineering

When a new device is supported and a FlexConnector is configured for it, you must identify data fields that are required, on which Intelligence must run analytics. Data engineering is the process of selecting the fields/columns that are required for Intelligence Analytics. This also entails cleansing the data and filtering it from unwanted information, such as noise.

Perform the following steps for data engineering:

1. Clean up data.
2. Filter data.
3. Normalize data. Perform the following as part of normalizing data:
   a. Ensure that the username is in lowercase.
   b. Set the depth value for filepath.
   c. Perform entity mapping.

For more details on data engineering, contact OpenText Customer Support.

Event Categorization

When a new device is supported and a FlexConnector is configured for it, you must perform event categorization. Event Categorization is the process of identifying the type and nature of events and categorizing them into groups. Categorizing events is helpful when customizing SQL Loader Scripts to filter specific types of events. For more information, see **Event Categorization WhitePaper** in the ArcSight SmartConnectors 24.2 documentation.

SQL Loader Scripts

To support a new device of the supported data types, you must update the corresponding loader scripts. For more information, contact OpenText Customer Support.

Intelligence Tables

The support of a new device necessitates updating the Intelligence schema tables so that Intelligence analytics can run on the data from the new device. For more information, contact OpenText Customer Support.

Securing HDFS for Intelligence

HDFS (Apache Hadoop Distributed File System) is a distributed file system, which is deployed on the worker nodes of the OMT cluster by default. The Intelligence analytics platform uses HDFS as a temporary storage to push analytics data to the ArcSight database. HDFS stores analytics data only when the write process is active.

Intelligence now allows you to secure access to HDFS with SASL (Simple Authentication and Security Layer). To secure HDFS, you can enable and configure Kerberos authentication services. When you configure HDFS to run in a secure mode, Kerberos authenticates each HDFS service and user. For authentication, Intelligence uses the Kerberos protocol, which is built on a trusted third-party encryption server, known as **Key Distribution Center (KDC)**.

> The secure data transfer between HDFS and the database is enabled by default. However, this increases the run time of the analytics jobs.

Enabling and Configuring Kerberos Authentication

This section provides information on enabling and configuring kerberos authentication for securing HDFS. Perform the tasks in the listed order:

	Task	See
❑	(Conditional) For Linux, configure the Kerberos Key Distribution Centre.	Configuring Kerberos Key Distribution Centre in Linux
❑	(Conditional) For Windows, set up your environment to configure Kerberos KDC.	Setting Up Your Windows Environment to Configure Kerberos KDC
❑	(Conditional) For Windows, create service and user principals for Kerberos ticket generation.	Creating Service and User Principals for Kerberos Ticket Generation in Windows
❑	Configure HDFS services to use keytabs.	Configuring HDFS Services to Use Keytabs

Configuring Kerberos Key Distribution Centre in Linux

To configure Kerberos Key Distribution Centre (KDC):

1. Install MIT Kerberos on any of the Kubernetes nodes in the OMT cluster. Refer to the open source documentation to perform this step.
2. As a root user, log in to the node where MIT Kerberos is installed, then create a service principal for HDFS:

```
$kadmin.local
$addprinc hdfs/<DATANODE_HOST>
```

3. Generate the keytab for the service principal created in **step 2**:

```
$kadmin.local
$ktadd -k hdfs_<DATANODE_HOST>.keytab hdfs/<DATANODE_HOST>
```

4. As a root user, log in to the node where MIT Kerberos is installed, then create a service principal for http:

```
$addprinc http/<DATANODE_HOST>
```

5. Generate the keytab for the service principal created in **step 4**:

```
$kadmin.local
$ktadd -k http_<DATANODE_HOST>.keytab http/<DATANODE_HOST>
```

6. Repeat steps 2 to 5 for all nodes where HDFS datanodes are active.
7. As a root user, log in to the node where MIT Kerberos is installed, then create a user principal for HDFS:

```
$kadmin.local
$addprinc hdfs
```

Setting Up Windows Environment to Configure Kerberos KDC

The steps provided in this section have been verified on the Windows 2016 server.

To set up your Windows environment to configure Kerberos KDC, do the following:

1. If you have not deployed the Active Directory Domain Controller in your environment, then deploy a Windows server and promote the server as the Active Directory Domain Controller. Refer to the Microsoft documentation to perform this activity.
2. If you have deployed the Active Directory Domain Controller and Intelligence in the same domain, proceed to step 4.
3. If you have deployed the Active Directory Domain Controller and Intelligence in different domains, add the Active Directory Domain Controller DNS entry in the Kubernetes environment:
   a. Log in to the node in the OMT cluster as a root user and run the following command to edit the `DNS-hosts-configmap` file:

      ```
      kubectl edit cm dns-hosts-configmap -n kube-system
      ```

      Your terminal looks as follows:

      ```
      apiVersion: v1
      data:
        dns-hosts-key: ""
      kind: ConfigMap
      metadata:
        creationTimestamp: 2018-10-19T05:28:05Z
        name: dns-hosts-configmap
        namespace: kube-system
      ```

   b. Update the DNS entries and save the file. This change will take effect in 20 seconds automatically.

      For example, add the following DNS entries:

      ```
      dns-hosts-key: |
       192.0.2.0 myhost.mydomain.com
       192.0.2.1 myhost.mydomain2.com
      ```

c. Your terminal looks as follows:

```
apiVersion: v1
 data:
  dns-hosts-key: |
   192.0.2.0 myhost.mydomain.com
   192.0.2.1 myhost.mydomain.com
 kind: ConfigMap
 metadata:
   creationTimestamp: 2018-10-19T05:28:05Z
```

4. (Recommended) Perform the following steps to ensure that you select strong encryption algorithm types for Kerberos in the Active Directory Domain controller:

   a. In **Local Group Policy Editor**, navigate to the following location:

      Local Computer Policy > **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.

   b. Select **Network Security: Configure encryption types allowed for Kerberos**.

   c. Right-click **Network Security: Configure encryption types allowed for Kerberos** and click **Properties**.

   d. In the pop-up window, under the **Local Security Setting** tab, select the following check boxes:

      - AES128_HMAC_SHA1
      - AES256_HMAC_SHA1
      - Future encryption types

   e. Click **Apply** and then click **OK**.

   f. Launch the command prompt in the Active Directory Domain Controller and execute the following command to update the global policy:

```
/gpupdate
```

Creating Service and User Principals for Kerberos Ticket Generation in Windows

To create service and user principals for Kerberos ticket generation:

1. Create a service principal account for **HDFS** in the Windows Active Directory domain controller:

   a. Click **Active Directory Users and Computers** > **domain name (example: intelligence.lab)** > right-click **Users** > **New** > **User**.

   b. In **New Object - User**, specify your first, last, and full name.

   c. Specify **User logon name** as `hdfs/<DATANODE_HOST>` and click **Next**.
   d. Specify and confirm your password. Ensure that you select **Password Never Expires** and click **Next**.
   e. Click **Active Directory Users and Computers** > **domain name (example: intelligence.lab)** > right-click **Users (The user created in the above steps)** > **Properties**.
   f. Click **Account**, and under **Account Options:**, select all of the following:
      - This account supports Kerberos AES 128 bit encryption.
      - This account supports Kerberos AES 256 bit encryption.
      - Do not require Kerberos preauthentication.
   g. Click **Apply** and then click **OK**.
2. Create a service principal account for **HTTP** in the Windows Active Directory domain controller:
   a. Click **Active Directory Users and Computers** > **domain name (example: intelligence.lab)** > right-click **Users** > **New** > **User**.
   b. In **New Object - User**, specify your first, last, and full name.
   c. Specify **User logon name** as `http/<DATANODE_HOST>` and click **Next**.
   d. Specify and confirm your password. Ensure that you select **Password Never Expires** and click **Next**.
   e. Click **Active Directory Users and Computers** > **domain name (example: intelligence.lab)** > right-click **Users (The user created in the above steps)** > **Properties**.
   f. Click Account, and under **Account Options**, select all of the following:
      - This account supports Kerberos AES 128 bit encryption.
      - This account supports Kerberos AES 256 bit encryption.
      - Do not require Kerberos preauthentication.
   g. Click **Apply** and then click **OK**.
3. Repeat steps 1 to 2 for all the worker nodes where HDFS datanodes are active.
4. Create a user principal for **HDFS** in the Windows Active Directory domain controller:
   a. Click **Active Directory Users and Computers** > **domain name (example: intelligence.lab)** > right-click **Users** > **New** > **User**.
   b. In **New Object - User**, specify your first, last, and full name.
   c. For **User logon name**, specify either a new user name or the default user name of hdfs, and then click **Next**.
   d. Specify and confirm your password. Ensure that you select **Password Never Expires** and click **Next**.

e. Click **Active Directory Users and Computers** > **domain name (example: intelligence.lab)** > right-click **Users (The user created in the above steps)** > **Properties**.

f. Click **Account**, and under **Account Options:**, select all of the following:

- This account supports Kerberos AES 128 bit encryption.
- This account supports Kerberos AES 256 bit encryption.
- Do not require Kerberos preauthentication.

g. Click **Apply** and then click **OK**.

5. For the service principal account created for **HDFS**, generate the keytabs by running the following commands in the Windows command prompt:

```
ktpass /out hdfs_<DATANODE_HOST>.keytab /princ hdfs/<DATANODE_
HOST>@<Domain name of domain controller> /mapuser <DATANODE_HOST without
domain name>@<Domain name of domain controller> /pass <password> /crypto
all /ptype KRB5_NT_PRINCIPAL
```

6. For the service principal account created for **HTTP**, generate the keytabs by running the following commands in the Windows command prompt:

```
ktpass /out http_<DATANODE_HOST>.keytab /princ http/<DATANODE_
HOST>@<Domain name of domain controller> /mapuser <DATANODE_HOST without
domain name>@<Domain name of domain controller> /pass <password> /crypto
all /ptype KRB5_NT_PRINCIPAL
```

7. Repeat steps 4 and 5 for all the worker nodes where HDFS datanodes are active.

Configuring HDFS Services to Use Keytabs

To configure HDFS services to use keytabs:

1. **For Datanode**

   a. Launch a terminal session and log in to the Kubernetes worker node where the HDFS datanode is active.

   b. Copy the `http_<DATANODE_HOST>.keytab` and `hdfs_<DATANODE_HOST>.keytab` keytab files from the Windows Active Directory domain controller and paste them in the `/opt/arcsight/k8s-hostpath-volume/interset/hdfs/keytabs` directory of the Kubernetes worker node where the HDFS datanode is active, then rename them as `http.keytab` and `hdfs.keytab`.

   c. Repeat **step a** and **step b** for all the HDFS datanodes that are active in the Kubernetes cluster.

   d. For all the keytab files present in the HDFS datanodes of the Kubernetes cluster, provide the permissions of the users who have privilege to NFS, then navigate to the

`/opt/arcsight/k8s-hostpath-volume/interset/hdfs/keytabs` directory and set:

```
chmod 600 *
chown UID:GID *
```

For example:

```
chmod 600 hdfs.keytab
chown 1999:1999 hdfs.keytab
```

2. **For Namenode**
   a. Launch a terminal session and log in to the Kubernetes node where NFS is created.
   b. Copy the `http_<DATANODE_HOST>.keytab` and `hdfs_<DATANODE_HOST>.keytab` keytab files from the Windows Active Directory domain controller and paste them in the `/opt/arcsight-nfs/arcsight-volume/interset/hdfs/namenode/keytabs` directory of the Kubernetes node where NFS is created, then rename them as `http.keytab` and `hdfs.keytab`:

   > You must generate the above keytab files for the Kubernetes worker node labeled as `intelligence-namenode:yes`.

   c. Repeat **step a** and **step b** for all the namenodes active in the Kubernetes cluster.
   d. For all the keytab files present in the HDFS datanodes of the Kubernetes cluster, provide the permissions of the users who have privilege to NFS, then navigate to the `/opt/arcsight/k8s-hostpath-volume/interset/hdfs/keytabs` directory and set:

   ```
   chmod 600 *
   chown UID:GID *
   ```

   For example:

   ```
   chmod 600 hdfs.keytab
   chown 1999:1999 hdfs.keytab
   ```

Creating Service Principals for Kerberos Ticket Generation in Windows

To create service principals for Kerberos ticket generation:

1. Create a service principal account for **HDFS** in the Windows Active Directory domain controller:
   a. Click **Active Directory Users and Computers** > **domain name (example: intelligence.lab)** > right-click **Users** > **New** > **User**.
   b. In **New Object - User**, specify your first, last, and full name.

   c. Specify **User logon name** as `hdfs/<DATANODE_HOST>` and click **Next**.
   d. Specify and confirm your password. Ensure that you select **Password Never Expires** and click **Next**.
   e. Click **Active Directory Users and Computers** > **domain name (example: intelligence.lab)** > right-click **Users (The user created in the above steps)** > **Properties**.
   f. Click **Account**, and under **Account Options:**, select all of the following:
      - This account supports Kerberos AES 128 bit encryption.
      - This account supports Kerberos AES 256 bit encryption.
      - Do not require Kerberos preauthentication.
   g. Click **Apply** and then click **OK**.
2. Create a service principal account for **HTTP** in the Windows Active Directory domain controller:
   a. Click **Active Directory Users and Computers** > **domain name (example: intelligence.lab)** > right-click **Users** > **New** > **User**.
   b. In **New Object - User**, specify your first, last, and full name.
   c. Specify **User logon name** as `http/<DATANODE_HOST>` and click **Next**.
   d. Specify and confirm your password. Ensure that you select **Password Never Expires** and click **Next**.
   e. Click **Active Directory Users and Computers** > **domain name (example: intelligence.lab)** > right-click **Users (The user created in the above steps)** > **Properties**.
   f. Click Account, and under **Account Options**, select all of the following:
      - This account supports Kerberos AES 128 bit encryption.
      - This account supports Kerberos AES 256 bit encryption.
      - Do not require Kerberos preauthentication.
   g. Click **Apply** and then click **OK**.
3. Repeat steps 1 and 2 for all the worker nodes where HDFS datanodes are active.
4. For the service principal account created for **HDFS**, generate the keytabs by running the following commands in the Windows command prompt:

```
ktpass /out hdfs_<DATANODE_HOST>.keytab /princ hdfs/<DATANODE_
HOST>@<Domain name of domain controller> /mapuser <DATANODE_HOST without
domain name>@<Domain name of domain controller> /pass <password> /crypto
all /ptype KRB5_NT_PRINCIPAL
```

5. For the service principal account created for **HTTP**, generate the keytabs by running the following commands in the Windows command prompt:

```
ktpass /out http_<DATANODE_HOST>.keytab /princ http/<DATANODE_
HOST>@<Domain name of domain controller> /mapuser <DATANODE_HOST without
domain name>@<Domain name of domain controller> /pass <password> /crypto
all /ptype KRB5_NT_PRINCIPAL
```

6. Repeat steps 4 and 5 for all the worker nodes where HDFS datanodes are active.

Configuring HDFS Security in OMT

This section provides steps to configure or reconfigure HDFS security in the OMT.

> You need not perform this procedure if you already enabled Kerberos Authentication at the time of deploying Intelligence and do not intend to modify the Kerberos details.
> Perform this procedure for any of the following scenarios:
> - If you are enabling Kerberos Authentication for the first time.
> - If you need to modify the Kerberos details in the Intelligence tab. In this case, ensure that you first enable and configure Kerberos Authentication with the new Kerberos details before proceeding with this procedure.

To configure or reconfigure HDFS security in OMT:

1. Open a certified web browser.
2. Specify the following URL to log in to the OMT Management Portal: https://<OMT_masternode_hostname or virtual_ip hostname>:5443.
3. Select **Deployment** > **Deployments**.
4. Click ... (Browse) on the far right and choose **Reconfigure**. A new screen will be opened in a separate tab.
5. Click **Intelligence** and specify details under the **Hadoop File System (HDFS) Security** section.

   > The **Enable Secure Data Transfer with HDFS Cluster** field is enabled by default to encrypt communication between the HDFS cluster and the database. However, this increases the run time of the analytics jobs.

   - If you have a non-collocated database cluster and **Enable Secure Data Transfer with HDFS Cluster** is enabled, perform the following steps:
     a. Execute the following command in the master node:

     ```
     /opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/re_
     ca.cert.pem
     ```

     b. Execute the following commands in each database node:

```
scp root@<master_node_FQDN>:/tmp/re_ca.cert.pem /etc/pki/ca-
trust/source/anchors/
```

```
update-ca-trust
```

c. Execute the following command to verify that there is a trust relationship with the CA from each database node:

```
curl https://<WORKER_RUNNING_HDFS_NAMENODE>:30071
```

You should not encounter any certificate errors after executing the above command.

- The Kerberos details that you provide in **Kerberos Domain Controller Server**, **Kerberos Domain Controller Admin Server**, **Kerberos Domain Controller Domain**, and **Default Kerberos Domain Controller Realm** will be considered only if you select **kerberos** in **Enable Authentication with HDFS Cluster**. They are not valid if you select **simple**.

6. Click **Save**.
7. The following containers restart:
   - `interset-analytics-xxxxx-xxx`
   - `hdfs-namenode-x`
   - `hdfs-datanode-xxx`
8. (Conditional) After modifying the value of **Enable Secure Data Transfer with HDFS Cluster**, if HDFS namenode enters the safe mode when you run analytics, perform the following steps:
   a. Do the following to bring the HDFS namenode up:
      i. Launch a terminal session and log in to the NFS server.
      ii. Navigate to the directory where NFS is created.

      (Conditional) If you have used the ArcSight Platform Installer, navigate to the following NFS directory:

```
/opt/arcsight-nfs/arcsight-volume/interset/hdfs/namenode
```

      (Conditional) If you have used the manual deployment method, navigate to the following NFS directory:

```
/<arcsight_nfs_vol_path>/interset/hdfs/namenode
```

      for example:

```
/opt/arcsight/nfs/volumes/itom/arcsight/interset/hdfs/namenode
```

iii. Delete the name folder under the namenode directory.

b. Do the following to bring the HDFS datanodes up:

i. Navigate to the following directory:

(Conditional) If you have used the ArcSight Platform Installer, navigate to the following directory:

```
/opt/arcsight/k8s-hostpath-volume/interset/hdfs
```

(Conditional) If you have used the manual deployment method, navigate to the following directory:

```
<arcsight_k8s-hostpath-volume>/interset/hdfs
```

ii. Delete the data folder under the hdfs directory.

iii. Repeat steps i and ii on all the datanodes.

c. Restart the HDFS datanode and namenode containers.

Setting an Encoding Option for the URL

For better data security, Intelligence provides options to encode the Intelligence URL string. Based on your requirement, you can set the limit for the URL string length and then select a preferred URL encoding option.

The supported URL encoding options are:

- **plain**: Does not encode and/or compress the URL string.
- **base64**: Compresses the URL string with **zLib** and encodes the string to **base64**.
- **hash**: Stores the encoded **base64** URL string as **JSON** in **localstorage**. Then, it uses a **hash** of the **base64** encoded URL string as the key values.
- **limitLength**: The URL string uses the **plain** and then **base64** encoding options if either of the encoding options have lesser characters than **urlLimit**. The URL string uses the **hash** encoding option if both the **plain** and **base64** encoding options are above **urlLimit**.

  > **urlLimit** is an integer, which sets the maximum URL length (in characters) for encoding options before using **localstorage**. **urlLimit** is only available for the **limitLength** and **limitAndObscure** encoding options.

- **limitAndObscure**: The URL string uses the **base64** encoding option if it has lesser characters than **urlLimit**. The URL uses the **hash** encoding option if it has more characters than **urlLimit**.

> If you do not specify an encoding option, the default encoding option is set as plain.

To set an encoding option for the URL string:

1. Login to the Management portal as the administrator.
   `https://<virtual_FQDN>:5443`
2. Click **CLUSTER** > **Dashboard**. You will be redirected to the **Kubernetes Dashboard**.
3. Under **Namespace**, search and select the `arcsight-installer-xxxx` namespace.
4. Under **Config and Storage**, click **Config Maps**.
5. Click the filter icon, and search for `investigator-default-yaml`.
6. Click ⋮ and select **Edit**.
7. In the **YAML** tab, specify the preferred URL encoding option in **`urlEncoding`** and the preferred URL string length limit in **`urlLimit`**.
8. Click **Update**.
9. Restart the `interset-api` pods:
   a. Launch a terminal session and log in to the master or worker node.
   b. Execute the following command to retrieve the namespace:
      ```
      export NS=$(kubectl get namespaces | grep arcsight|cut -d ' ' -f1)
      ```
   c. Execute the following commands to restart the `interset-api` pods:
      ```
      kubectl -n $NS scale deployment interset-api --replicas=0
      kubectl -n $NS scale deployment interset-api --replicas=2
      ```

Intelligence Data Types and Schemas

This section provides detailed information about each data type, Intelligence supports and how they are used in analytics. For each given data type, a description, supported SmartConnectors and associated schema are included:

Access

Access data sources: sh (Fileshare), rs (Resource)

The Access schema represents events collected from Identity and Access Management (IAM) solutions where users access resources such as servers or fileshares.

Examples of access events include:

- A user fails to access a network share object `VPM-CFDB01.data.int`
- A user attempts to access shared drive `Network Shares/HR/HR-Policies/`

Examples of IAM products include: Active Directory

The Intelligence Access data type best supports Windows Security Log (or Active Directory) event data.

The Microsoft Windows Security Log contains records of login/logout activity, as well as other security-related events specified in the system's Audit Policy. A System Administrator must enable the Windows Audit feature to allow events to be recorded in the Security Log.

Supported SmartConnectors

The following SmartConnectors are used for the collection and ingestion of Access events:

- SmartConnector for Microsoft Windows Event Log – Native Application and System Event Support

Access Schema

The following table describes the default_secops_adm.Events table columns for Access data.

Column Name	Data Type	Required (Y/N)	Description	Example
deviceReceiptTime	Integer	Y	The time at which the event related to the activity was received.	1592839336200 Equivalent GMT - 2020-06-22 15:22:00
destinatonUserName	Varchar	Y	The user involved in authentication.	john.legget
destinationHostName	Varchar	N	The server handling the authentication.	
filePath	Varchar	N	Path, project, or tag that the resource belongs to.	
fileType	Varchar	N	Type of collection that the resource belongs to, for example, shr	
fileName	Varchar	N	File, ID, or Object that the resource is mapped to.	
externalId	Varchar	N	Usually a Windows event code (for example, **5140**, **4664**,and so on), but Analytics can be configured to accept other values, including **-1**.	4663
categoryOutcome	Varchar	N	An indicator of whether the authentication was successful. Usually either **success** or **failure** , however, Analytics can be configured to accept other values.	failure

Active Directory

Active Directory data sources: ad

The Active Directory schema represents events collected from Identity and Access Management (IAM) solutions that identify successful and failed logins to authentication targets. These authentication targets include domain controllers/servers, resources, and file shares.

Examples of authentication events include:

- A user fails to log in to YOURDC.yourcompany.com
- A user attempts to access shared drive DEV_102_share

Examples of IAM products include:

- Active Directory

The Intelligence Authentication data type best supports Windows Security Log (or Active Directory) event data.

The Microsoft Windows Security Log contains records of login/logout activity, as well as other security-related events specified in the system's Audit Policy. A System Administrator must enable the Windows Audit feature to allow events to be recorded in the Security Log.

Supported SmartConnectors

The SmartConnector for Microsoft Active Directory Windows Event Log Native is used for the collection and ingestion of Active Directory data.

Active Directory Schema

The following table describes the default_secops_adm.Events table columns for Active Directory data.

Column Name	Data Type	Required (Y/N)	Description	Example
destinationUserName	Varchar	Y	The user involved in authentication. Primary entity for ad data source.	john.legget
categoryOutcome	Varchar	Y	The outcome of the event. One of success or failure.	success

Column Name	Data Type	Required (Y/N)	Description	Example
destinationHostName	Varchar	Y	The target involved in the authentication. Typically the domain controller to which the user is authenticating. The secondary entity for an ad data source.	CONTROLLER3.interset.com
externalId	Varchar	Y	Usually a Windows event code (e.g., 4624, 4771, etc.), but Analytics can be configured to accept other values, including -1.	4624
deviceReceiptTime	Integer	Y	The time at which the event related to the activity was received.	1592839336200 Equivalent GMT -2020-06-22 15:22:00
destinationNTDomain	Varchar	N	The domain that contains the user that is affected by the event.	interset
categoryObject	Varchar	N	The type of the object.	/Host/Operating System
categoryBehavior	Varchar	N	The action or behavior associated with the event.	Authentication/Verify
deviceCustomString4	Varchar	N	The string that further explains why the user failed to authenticate. Usually a hexadecimal code, but can be any string.	0xc0000064
sourceGeoLocationInfo	Varchar	N	Combination of the latitude and longitude values separated by a comma.	45.1234, -74.4321

VPN

VPN data source: vpn

The VPN schema represents events collected from Identity and Access Management (IAM) solutions or from other VPN devices such as Pulse Secure that identify VPN events.

Examples of VPN events include:

- A Network Policy Server granted full access to a user
- A user failed to authenticate with a Network Policy Server

Examples of IAM products include:

- Active Directory

The Intelligence Authentication data type best supports Windows Security Log (or Active Directory) event data. It also supports login success and failure event data from the supported VPN devices.

The Microsoft Windows Security Log contains records of login/logout activity, as well as other securityrelated events specified in the system's Audit Policy. A System Administrator must enable the Windows Audit feature to allow events to be recorded in the Security Log.

Supported SmartConnectors

The following SmartConnectors are used for the collection and ingestion of VPN data:

- SmartConnector for Microsoft Network Policy Server File
- SmartConnector for Pulse Secure Pulse Connect Secure Syslog
- SmartConnector for Citrix NetScaler Syslog
- SmartConnector for Nortel Contivity Switch Syslog

VPN Schema

The following table describes the default_secops_adm. Events table columns for VPN data.

Column Name	Type	Required (Y/N)	Description	Example
deviceReceiptTime	Integer	Y	The time at which the event related to the activity was received.	1592839336200 Equivalent GMT - 2020-06-22 15:22:00
sourceUserName	Varchar	Y	The user involved in authentication for Citrix NetScaler device. Primary entity for vpn data source.	john.legget
destinationUserName	Varchar	Y	The user involved in authentication. Primary entity for **vpn** data source.	john.legget
sourceAddressBin	Binary	N Exception: required for IPbased VPN models.	The IP address of the VPN user. Secondary entity	172.1.193.87

Column Name	Type	Required (Y/N)	Description	Example
sourceGeoCountryCode	Varchar	N Exception: required for countrybased VPN models.	The country the user is authenticating from. Secondary entity	Canada
sourceGeoLatitude	Float	N	The latitude where the VPN connection is initiated.	45.1234
sourceGeoLongitude	Float	N	The longitude where the VPN connection is initiated.	-74.4321
externalId	Varchar	Y	Unique code assigned to a Network Policy Server events. Typically a Windows event code or -1. Analytics can be configured to accept other values.	6272
deviceEventClassId	Varchar	Y	Unique code assigned to a Pulse Secure or Citrix NetScaler event.	AUT24326
deviceAction	Varchar	Y	Unique code assigned to a Nortel event.	OK
categoryOutcome	Varchar	Y	The outcome of the event. One of success or failure. For Citrix NetScaler, the outcome is attempt.	success
categoryBehavior	Varchar	Y	The action or behavior associated with the event.	/Authentication/Verify
categoryDeviceGroup	Varchar	Y	The type of events for the device. It is used for Pulse Secure, Citrix NetScaler, and Nortel events.	/VPN
categoryDeviceType	Varchar	Y	The events generated by a device type irrespective of the device group the events belong to. It is used for Citrix NetScaler and Nortel events.	VPN for Nortel Network-based IDS/IPC for Citrix NetScaler
deviceCustomString4	Varchar	N	The string that further explains why the user failed to authenticate. Usually a hexadecimal code, but can be any string. It is used for NPS events with externalId 6273.	18

Web Proxy

Web Proxy data source: pxy

Web Proxy data are raw events that capture network traffic, primarily Web surfing, from a collection of human users.

Examples

- A user accessed the Web site **https://yourcompany.com**
- A user received data from a web destination, **vap3iad3.lijit.com**

Examples of Web Proxy products include:

- Microsoft Internet Security and Acceleration Server (ISA)
- Squid
- Blue Coat Secure Web Gateway

Supported SmartConnectors

The following SmartConnectors are used for the collection and ingestion of Web Proxy data:

- SmartConnector for Microsoft Forefront Threat Management Gateway File
- SmartConnector for Squid Web Proxy Server File
- SmartConnector for Blue Coat Proxy SG Multiple Server File

Web Proxy Schema

The following table describes the default_secops_adm. Events table columns for Web Proxy data.

Column Name	Data Type	Required (Y/N)	Description	Example
deviceReceiptTime	Integer	Y	The time at which the event related to the activity was received.	1592839336200 Equivalent GMT -2020-06- 22 15:22:00
requestMethod	Varchar	Y	The HTTP method of the request.	GET
deviceSeverity	Varchar	Y	The HTTP response status.	400
bytesIn	Integer	Y	Bytes returned to the client in the response.	410235

Column Name	Data Type	Required (Y/N)	Description	Example
sourceUserName	Varchar	N	The name associated with the client making the request.	john.legget
destinationHostName	Varchar	N	The name of the host the client is trying to connect to.	a-0001.a-msedge.net
bytesOut	Integer	N	The number of bytes the client sent in its request.	690235
requestClientApplication	Varchar	N	The agent string of the Blue Coat devices.	Mozilla/5.0 (Windows NT 5.1; rv:8.0) Gecko/20100101 Firefox/8.0
deviceCustomString1	Varchar	N	The agent string of the Microsoft devices.	Windows Update Agent
deviceVendor	Varchar	N	The device vendor of the client.	Microsoft
deviceProduct	Varchar	N	The device product of the client.	ISA Server

Repository

Repository data source: rp

Repository data comprises raw events collected from a source control (repository) system.

Examples:

- A user fetched files from a directory **/project_files/linux/tools/**
- A user added files to a directory **/depot/project5/java_source/**

Information in this section pertain to the following repository systems and their versions:

Repository System	Version
GitHub Enterprise	2.21.0
Bitbucket Server	7.5.0
Perforce	2020.1

The repository systems store audit information in log files. The ArcSight FlexConnectors are installed and configured on the repository systems where they read the log files, filter the messages, tokenise them, and then populate them in the default_secops_adm.Events table. For each of the repository systems and the specified versions, there is a corresponding configuration file (also referred to as a parser). The configuration file is a text file containing properties (name, value pairs) that describe how the FlexConnector parses event data.

The FlexConnector type that is used to process and parse the repository log files is the ArcSight FlexConnector Regex File.

Configuration Files

The configuration files provided in this section are designed only for the specified versions of the repository systems.

Configuration File for GitHub Enterprise 2.21.0

The configuration file that is used for GitHub Enterprise 2.21.0 is **git.sdkrfilereader.properties**.

```
text.qualifier="
comments.start.with=\#
trim.tokens=true
contains.empty.tokens=true

line.include.regex=(.+)"committer_date":"([^ ]+)(.+)"hostname":"([^,]+)"
(.+)"program":("upload-pack"|"run-hook-postreceive")(.+)"
real_ip":"([^,]+)"(.+)"repo_name":"([^,]+)"(.+)"user_login":"([^,]+)"(.+)
regex=(.+)"committer_date":"([^ ]+)(.+)"hostname":"([^,]+)"(.+)"program":"
([^,]+)"(.+)"real_ip":"([^,]+)"(.+)"repo_
name":"([^,]+)"(.+)"user_login":"([^,]+)"(.+)
token.count=13

token[0].name=CONSTANT1
token[0].type=String
token[1].name=EVENTTIME
token[1].type=Long
token[2].name=CONSTANT2
token[2].type=String
token[3].name=HOSTNAME
token[3].type=String
token[4].name=CONSTANT2
token[4].type=String
token[5].name=PROGRAM
token[5].type=String
token[6].name=CONSTANT3
token[6].type=String
token[7].name=REALIP
token[7].type=String
token[8].name=CONSTANT4
token[8].type=String
token[9].name=REPONAME
token[9].type=String
token[10].name=CONSTANT5
token[10].type=String
token[11].name=USERNAME
```

```
token[11].type=String
token[12].name=CONSTANT6
token[12].type=String

event.deviceVendor=__getVendor("GitHub")
event.deviceProduct=__stringConstant("GitGub Enterprise")
event.deviceVersion=__stringConstant("2.21.0")

event.deviceReceiptTime=__createLocalTimeStampFromSecondsSinceEpoch
(EVENTTIME)
event.destinationUserName=USERNAME
event.deviceCustomString1=__toLowerCase(REPONAME)
event.deviceCustomString1Label=__stringConstant("RepositoryName")
event.deviceAction=__ifThenElse(PROGRAM,"run-hook-post-receive","receive-
pack","upload-pack")
event.sourceAddress=__oneOfAddress(REALIP)
event.destinationHostName=__oneOfHostName(HOSTNAME)
event.name=__ifThenElse(PROGRAM,"run-hook-post-receive","receive-
pack","upload-pack")
event.bytesOut=__safeToInteger(__regexToken(CONSTANT5,".+uploaded_bytes.:
([^,]+)"))
#event.requestMethod=
#event.protocol=
#event.request=

event.categoryObject=__stringConstant("/Host/Resource")
event.categoryBehavior=__stringConstant("/Access")
event.categoryOutcome=__stringConstant("/Attempt")
event.categorySignificance=__stringConstant("/Informational")
event.categoryDeviceGroup=__stringConstant("Application")
event.categoryDeviceType=__stringConstant("Repository")
```

Configuration File for Bitbucket Server 7.5.0

The configuration file that is used for Bitbucket Server 7.5.0 is **bitbucket.sdkrfilereader.properties**.

```
text.qualifier="
comments.start.with=\#
trim.tokens=true
contains.empty.tokens=true

line.include.regex=(.+)\\|(.+)\\|(.+)\\|([^-]+)\\|(.+)\\|(.+git-upload-
pack.+|.+git-receive-pack.+)\\|(.+)\\|(.+)\\|
(.+)\\|(.+)\\|(.+)\\|(.+)\\|(.+)\\|(.*)
regex=(.+)\\|(.+)\\|(.+)\\|(.*)\\|(.+)\\|(.*)\\|(.+)\\|(.+)\\|(.+)\\|
```

```
(.+)\\|(.+)\\|(.+)\\|(.+)\\|(.*)

token.count=14

token[0].name=REALIP
token[0].type=String
token[1].name=PROTOCOL
token[1].type=String
token[2].name=REQUESTID
token[2].type=String
token[3].name=USERNAME
token[3].type=String
token[4].name=EVENTTIME
token[4].type=String
token[5].name=ACTION
token[5].type=String
token[6].name=REQUESTINFO
token[6].type=String
token[7].name=STATUS
token[7].type=String
token[8].name=BYTESREAD
token[8].type=String
token[9].name=BYTESWROTE
token[9].type=String
token[10].name=EXTRAINFO1
token[10].type=String
token[11].name=EXTRAINF02
token[11].type=String
token[12].name=EXTRAINF03
token[12].type=String
token[13].name=EXTRAINF04
token[13].type=String

event.deviceVendor=__getVendor("BitBucket")
event.deviceProduct=__stringConstant("BitBuket Server")
event.deviceVersion=__stringConstant("7.5.0")

event.deviceReceiptTime=__createOptionalTimeStampFromString
(EVENTTIME,"yyyy-MM-dd HH:mm:ss,sss")
event.destinationUserName=USERNAME
event.deviceCustomString1=__toLowerCase(__regexToken(__regexToken(__split
(ACTION," ",2),"(.*)\\.git(.+)"),".*\/(.+)"))
event.deviceCustomString2=__regexToken(__split(ACTION," ",2),"(\/.+)(\/git-
upload-pack|\/git-receive-pack)")
event.deviceCustomString2Label=__stringConstant("RepositoryName")
event.name=__regexToken(__split(ACTION," ",2),".+\/(.+)")
event.sourceAddress=__oneOfAddress(REALIP)
event.sourceHostName=__oneOfHostName(REALIP)
```

```
event.deviceAction=__regexToken(__split(ACTION," ",2),".+\/(.+)")
event.bytesIn=__safeToInteger(BYTESREAD)
event.bytesOut=__safeToInteger(BYTESWROTE)
event.requestMethod=__ifThenElse(__contains
(ACTION,"POST"),"true","POST","GET")
event.requestUrl=__split(ACTION," ",2)

event.categoryObject=__stringConstant("/Host/Resource")
event.categoryBehavior=__stringConstant("/Access")
event.categoryOutcome=__ifThenElse(STATUS,"200","/Success",__ifThenElse
(STATUS,"401","/Denied","/Attempt"))
event.categorySignificance=__stringConstant("/Informational")
event.categoryDeviceGroup=__stringConstant("Application")
event.categoryDeviceType=__stringConstant("Repository")
```

Configuration File for Perforce 2020.1

The configuration file that is used for Perforce 2020.1 is **perforce.sdkrfilereader.properties**.

```
text.qualifier="
comments.start.with=\#
trim.tokens=true
contains.empty.tokens=true

regex=(.+)\\s(.+)\\s(.+)\\s(.+)\\s(.+)\\s(.+)

token.count=6

token[0].name=EVENTDATE
token[0].type=String
token[1].name=EVENTTIME
token[1].type=String
token[2].name=USER
token[2].type=String
token[3].name=CLIENTIP
token[3].type=String
token[4].name=ACTION
token[4].type=String
token[5].name=RESOURCE
token[5].type=String

event.deviceVendor=__getVendor("Perforce")
event.deviceProduct=__stringConstant("Perforce")
event.deviceVersion=__stringConstant("2020.1")

event.deviceReceiptTime=__createOptionalTimeStampFromString(__concatenate
(EVENTDATE,EVENTTIME),"yyyy/MM/ddHH:mm:ss")
```

```
event.destinationUserName=USER

#######################################################################
#1.\/\/([^\/]+)\/([^\/]+)\/([^\/]+).*","/","//","")
# will return max of depth 4
# __regexTokenFindAndJoin(RESOURCE,"\/\/([^\/]+)?\/?([^\/]+)?\/?
([^\/]+)?","/","//","")
# eg //csvr/A/B/C
# //csrv/main/null
# //csrv/null/null
# //csrv/A/master
#2.\/\/(.*)(?=\/main$|\/null$|\/rel$|\/master$)
#__regexToken(__regexTokenFindAndJoin(RESOURCE,"\/\/([^\/]+)?\/?
([^\/]+)?\/?([^\/]+)?","/","//",""),"\/\/(.*)
(?=\/main$|\/null$|\/rel$|\/master$)")
#eg.returns all info nothign with main/null/rel/master
#3. remove version if any
#__regexToken(__ifGreaterOrEqual(__length(__regexToken(__
regexTokenFindAndJoin(RESOURCE,"\/\/([^\/]+)?\/?([^\/]+)?\/?
([^\/]+)?","/","//",""),"\/\/(.*)
(?=\/main$|\/null$|\/rel$|\/master$)")),"1",__regexToken(__
regexTokenFindAndJoin
(RESOURCE,"\/\/([^\/]+)?\/?([^\/]+)?\/?([^\/]+)?","/","//",""),"\/\/(.*)
(?=\/main$|\/null$|\/rel$|\/master$)"),__
regexTokenFindAndJoin(RESOURCE,"\/\/([^\/]+)?\/?([^\/]+)?\/?
([^\/]+)?","/","//",""))","(.*)[#\/][\\d.]+")
#eg.//crsv/A/12.3
# //crsv/A#1.2
#######################################################################

event.deviceCustomString1=__ifGreaterOrEqual(__length(__regexToken(__
ifGreaterOrEqual(__length(__regexToken(__
regexTokenFindAndJoin(RESOURCE,"\/\/([^\/]+)?\/?([^\/]+)?\/?
([^\/]+)?","/","//",""),"(\/\/.*)
(?=\/main$|\/null$|\/rel$|\/master$)")),"1",__regexToken(__
regexTokenFindAndJoin(RESOURCE,"\/\/([^\/]+)?\/?([^\/]+)?\/?
([^\/]+)?","/","//",""),"(\/\/.*)(?=\/main$|\/null$|\/rel$|\/master$)"),__
regexTokenFindAndJoin(RESOURCE,"\/\/
([^\/]+)?\/?([^\/]+)?\/?([^\/]+)?","/","//",""))","(.*)[#\/][\\d.]+")),"1",_
_regexToken(__ifGreaterOrEqual(__length(__
regexToken(__regexTokenFindAndJoin(RESOURCE,"\/\/([^\/]+)?\/?([^\/]+)?\/?
([^\/]+)?","/","//",""),"(\/\/.*)
(?=\/main$|\/null$|\/rel$|\/master$)")),"1",__regexToken(__
regexTokenFindAndJoin(RESOURCE,"\/\/([^\/]+)?\/?([^\/]+)?\/?
([^\/]+)?","/","//",""),"(\/\/.*)(?=\/main$|\/null$|\/rel$|\/master$)"),__
regexTokenFindAndJoin(RESOURCE,"\/\/
([^\/]+)?\/?([^\/]+)?\/?([^\/]+)?","/","//",""))","(.*)[#\/][\\d.]+"),__
```

```
ifGreaterOrEqual(__length(__regexToken(__
regexTokenFindAndJoin(RESOURCE,"\/\/([^\/]+)?\/?([^\/]+)?\/?
([^\/]+)?","/","//",""),"(\/\/.*)
(?=\/main$|\/null$|\/rel$|\/master$)")),"1",__regexToken(__
regexTokenFindAndJoin(RESOURCE,"\/\/([^\/]+)?\/?([^\/]+)?\/?
([^\/]+)?","/","//",""),"(\/\/.*)(?=\/main$|\/null$|\/rel$|\/master$)"),__
regexTokenFindAndJoin(RESOURCE,"\/\/
([^\/]+)?\/?([^\/]+)?\/?([^\/]+)?","/","//",""))
event.deviceCustomString2=RESOURCE
event.deviceAction=ACTION
event.sourceAddress=__oneOfAddress(CLIENTIP)
event.sourceHostName=__oneOfHostName(CLIENTIP)
event.name=ACTION

event.categoryObject=__stringConstant("Host/Resource")
event.categoryBehavior=__stringConstant("Access")
event.categoryOutcome=__stringConstant("/Attempt")
event.categorySignificance=__stringConstant("/Informational")
event.categoryDeviceGroup=__stringConstant("Application")
event.categoryDeviceType=__stringConstant("Repository")
```

You can also create or customize the configurations files for other versions of the repository systems. For more information, see ArcSight FlexConnector Developer's Guide in ArcSight SmartConnectors 24.2 documentation.

FlexConnector Installation and Configuration

To install and configure a FlexConnector, see ArcSight FlexConnector Developer's Guide in ArcSight SmartConnectors 24.2 documentation.

Ensure the following when you install and configure the FlexConnector:

- Select **ArcSight FlexConnector Regex** File as the **Connector Type**.
- When adding the parameters information, specify the following:
  - Select **Log Unparsed Events** as **False**.
  - Provide the absolute path and the repository log file name that the FlexConnector needs to read in the **Log File Name** field.

    For example:
    c:\temp\sample_data.log
  - For the **Configuration File** field, depending on the repository on which you are installing the FlexConnector, specify only **git**, **bitbucket**, or **perforce**.

For example, for the GitHub Enterprise repository, you must specify only git. The suffix **.sdkrfilereader.properties** is appended automatically. The configuration file name now is **git.sdkrfilereader.properties**.

- When configuring the destination, select either **CEF File** or Transformation Hub as the destination. For more information, see SmartConnector Installation and User Guide in ArcSight SmartConnectors 24.2 documentation.

Post-Installation Tasks

After you install and configure the FlexConnector and before you run the FlexConnector, copy the desired configuration (parser) files in the **ARCSIGHT_HOME\user\agent\ flexagent** location.

Repository Schema

The following table describes the default_secops_adm.Events table columns for Repository data.

Column Name	Type	Required (Y/N)	Description	Example
deviceAction	Varchar	Y	The action performed on the device.	upload-pack
deviceCustomString1	Varchar	Y	The device involved in the event. Typically a file path. Can be any string identifying a repository. Secondary entity for the rp data source	dev3/rel/hydra
deviceReceiptTime	Integer	Y	The time at which the event related to the activity was received.	1592839336200 Equivalent GMT - 2020-06-22 15:22:00
destinationUserName	Varchar	Y	The user involved in the event. Primary entity.	john.legget
deviceVendor	Varchar	Y	The device vendor of the client.	GitHub
deviceProduct	Varchar	N	The device product of the client.	GitHub Server
deviceVersion	Integer	N	The device version.	2.21.0
categoryObject	Varchar	N	The type of the object.	Host/Resource
categoryBehavior	Varchar	N	The action or behavior associated with the event.	/Access
categoryOutcome	Varchar	Y	The outcome of the event.	/Attempt
cateorySignificance	Varchar	N	The significance of the event.	/Informational
categoryDeviceGroup	Varchar	Y	The type of events for the device.	Application

Column Name	Type	Required (Y/N)	Description	Example
categoryDeviceType	Varchar	N	The events generated by the device type irrespective of the device group the events belong to.	Repository
sourceAddressBin	Varchar	N	The IP address of the user involved in the event.	78.1.198.82
bytesOut/bytesIn	Integer	N	The size of data (in bytes) related to the action performed on the project.	2203

Managing Recon

This section provides guidance for managing Recon functions and features within the deployment.

- "Configuring Event Integrity Checks" below

Configuring Event Integrity Checks

To validate that the event information in your database matches the content sent from SmartConnectors, run an **Event Integrity Check**. When you run the check, Recon searches the database for verification events received within the specified date range, then runs a series of checks to compare content in the database with information supplied by the verification event. The results of an Event Integrity Check help you identify whether event data might be compromised. In addition to reviewing the *raw event data* received from SmartConnectors, you can enable Transformation Hub to generate more than 20 *parsed fields* to include in the check.

- "Configuring a SmartConnector to Include a Verification Event for Raw Events" below
- "Enabling Transformation Hub to Generate Verification Events for Parsed Fields" on the next page

For more information about verification events and running integrity checks, see the Help.

Configuring a SmartConnector to Include a Verification Event for Raw Events

For a SmartConnector to support event integrity checks, you must enable it to include a verification event for each batch of events. This configuration ensures that the connector generates a verification event for the **Raw Event** field in an event at the moment that your environment captures it.

For this setting...	Enter...
Preserve Raw Event	Yes **NOTE**: When you enable this setting, the size of each event increases, which will require more storage space in your database.
Event Integrity Algorithm	MD5, SHA-1, or SHA-256
Check Event Integrity Method	Recon

For more information about configuring SmartConnectors, see the following topics:

- "Configuring Processing" in the *Installation Guide for ArcSight SmartConnectors* (ArcSight SmartConnectors 24.2 documentation)
- "Destination Runtime Parameters " on page 945

Enabling Transformation Hub to Generate Verification Events for Parsed Fields

The Event Integrity Check can verify the integrity of multiple fields within an event. You must enable Transformation Hub to generate verification events for the parsed fields received from the SmartConnectors. You can configure this setting as you deploy Transformation Hub or at any time after deployment, such as an upgrade.

It's important to tune the number of partitions of the enrichment stream processor source topic before enabling Transformation Hub to generate verification events for parsed fields. If you change the number of partitions of the source topic after enabling it, you must browse to Kafka Manager's Topics section and do the following:
1. Adjust and match the number of partitions of the Integrity events Enrichment changelog with the source topic number of partitions. The internal topic is named with the following format and pattern: `com.arcsight.th.AVRO_ENRICHMENT_1-integrityMessageStore-changelog.`
2. Restart the TH Web services pod by running the following command:
`kubectl delete pod th-web-service-xxxxxxxxx-yyyyy -n arcsight-installer-yyyyy`

1. Log in to the Management Portal.
2. Navigate to **Transformation Hub** > **Stream Processors and Routers**.
3. Enable **Generate verification events for parsed field integrity checks**. Default value is false. If true, a verification event is generated that accompanies a batch of events for checking the integrity of parsed fields in each event. Recon uses this verification event to check event integrity. If true, then specify a value for Verification event batch size as described below.
4. For **Verification event batch size**, specify the number of events that you want to be associated with a verification event. Default value is 256. A lower value indicates fewer associated events need to be included in the batch for integrity checks. However, a lower value will also result in higher resource consumption by generating more verification events.

This process generates an internal topic named with the following format and pattern com.arcsight.th.AVRO_ ENRICHMENT_ 1- integrityMessageStore- changelog. The setting "# of replicas assigned to each Kafka Topic" setting also applies to it.

If the flow of events is not consistent, and there are long intervals between the reception of events, the feature will check every hour (60 mins) for a summary event that hasn't reached the verification event batch size. If it hasn't been sent for more than 4 hours (240 mins), then it will be sent with the aggregated info of the previous number of events, regardless of whether it reached the verification event batch size.

Migrating Reports and Data From ArcSight Logger

To help you switch to ArcSight platform from ArcSight Logger, the system enables you to migrate the event data and reports that you regularly accessed in Logger.

This section helps you understand the prerequisites and processes required for the migration.

Migrating Logger Reports to the ArcSight Platform

This procedure guides you through the process of importing your Logger reports into the ArcSight platform.

1. From your terminal, open a bash shell to your reporting container.

   Tip: Opening a Bash Shell to the Reporting Container

   # Determine the namespace and id of your reporting pod:

   ```
   kubectl get pods --all-namespaces|grep reporting-web-app
   ```

   # Use your reporting pod id with "kubectrl exec" to open a bash shell:

   ```
   kubectl exec -c reporting-web-app -n <YOUR_NAMESPACE> -it <YOUR_POD_ID>
   /bin/bash
   ```

   Example:

   ```
   kubectl exec -c reporting-web-app -n arcsight-installer-2rjic -t fusion-
   reporting-web-a[[-c8c85f885-5xmfp /bin/bash
   ```

2. From your reporting pod bash shell, change to the `/var/lib/inetsoft/config` directory.
3. Extract the `mf-logger-converter-tool.tar` file to create the `/var/lib/inetsoft/config/logger` directory:

```
[root@n15-214-136-h8 config]# cd /var/lib/inetsoft/config
/opt/arcsight/nfs/vol/arcsight/reporting/config
[root@n15-214-136-h8 config]# tar xvf mf-logger-converter-tool.tar
logger/
logger/groovyInetSoft/
logger/groovyInetSoft/logger.groovy
logger/groovyInetSoft/options.json
logger/groovyInetSoft/setEnv.sh
logger/groovyInetSoft/dashboard2f.zip
logger/example_logger_dashboards/
logger/example_logger_dashboards/dashboards.29.A10 - Insufficient Logging
AND Monitoring_Attacks And Suspicious Activity.xml
logger/example_logger_dashboards/dashboards.228.Vulnerabilities_Injection
Vulnerabilities.xml
logger/example_logger_dashboards/dashboards.106.Denial of Service_DoS
Activity.xml
logger/example_logger_dashboards/dashboards.20.A 3 - Sensitive Data
Exposure_All Information Leakage events.xml
logger/example_logger_dashboards/dashboards.107.DNS_DGA Overview.xml
logger/example_logger_reports/
logger/example_logger_reports/reports.46.Anti-Virus_Top Infected
Systems.xml
logger/example_logger_reports/reports.4.3 - Unauthorized Changes to Users
Groups and Services_SANS Top 5 -3- User Account Creations.xml
logger/example_logger_reports/reports.9.5 - Suspicious or Unauthorized
Network Traffic Patterns_SANS Top 5 -5- Alerts from IDS.xml
```

```
logger/example_logger_reports/reports.49.Anti-Virus_Virus Activity by
Hour.xml
logger/example_logger_reports/reports.156.NetFlow Monitoring_Daily
Bandwidth Usage.xml
```

Note: Ensure the new logger directory has write and execute permissions: chmod -R 777 logger

4. Transfer the Logger `Report.xml` files that are to be converted into a directory within your reporting pod, such as:

```
/var/lib/inetsoft/config/logger/dashboards
```

or

```
/var/lib/inetsoft/config/logger/reports
```

Tip: Transferring Logger Reports to your Reporting Pod

To transfer a file to the reporting pod, you can use commands similar to this in your terminal:

Determine the namespace and id of your reporting pod:

```
kubectl get pods --all-namespaces|grep reporting-web-app
```

Use your reporting pod namespace and id with "kubectrl cp" to copy the file into your pod:

```
kubectl cp ./my- report.xml <YOUR_ NAMESPACE>/<YOUR_ POD_
ID>:/var/lib/inetsoft/config/logger/reports/my-report.xml
```

If using the "kubectl cp" command to transfer files to the pod, some systems might require the use of the --container=reporting-web-app --no-preserve=true flags:

Example 1:

```
kubectl cp ./my-report.xml arcsight-installer-2rjic/fusion-reporting-web-
app-c8c85f885-5xmfp:/var/lib/inetsoft/config/logger/reports/my-report.xml
```

Example 2:

```
kubectl cp ./m- report.xml secops/fusion- reporting- web- app- c8c85f885-
5xmfp:/var/lib/inetsoft/config/logger/reports/my- report.xml - -
container=reporting-web-app --no-preserve=true
```

5. From your terminal connected to the reporting pod's bash shell (Step 1 above), change to the directory where the converter script is located:

```
cd /var/lib/inetsoft/config/logger/groovyInetSoft/
```

6. Set the `INETSOFT_LICENSE_KEY` variables:

```
export INETSOFT_LICENSE_KEY=`echo $INETSOFT_LICENSE | base64 --decode`
export INETSOFT_LICENSE=`echo $INETSOFT_LICENSE | base64 --decode`
```

7. Run the `logger.groovy` script to convert the Logger reports.

   usage:

```
inetsoft-shell.sh logger.groovy options.json <target.zip> <source dir>
```

   where:

```
inetsoft-shell.sh is the full path to the shell script (typically:
/usr/local/inetsoft/shell/bin/inetsoft-shell.sh)
```

   - logger.groovy is the name of the converter script.
   - options.json is the name of the options file (pre-set).
   - <target.zip> is the full path and zip file name of where the converted reports will be written to.
   - <source dir> is the full path to the directory where the Logger Report .xml files to be converted are located (from STEP 6 above).

   Example:

```
/usr/local/inetsoft/shell/bin/inetsoft-shell.sh logger.groovy
options.json /var/lib/inetsoft/config/logger/groovyInetSoft/my-converted-
reports.zip /var/lib/inetsoft/config/logger/example_logger_reports
```

8. Import the converted report .zip file.
   a. Launch the Enterprise Manager from the **Content** tab.
   b. Create a directory called "Logger" under the **Standard Content** folder.

   > It is necessary to create the Logger directory under either the **Custom Content** folder or the **Standard Content** folder because users will not have permission to create a top level Logger directory.

   > The Logger reports have their own built-in date prompts. If is preferred to install the Logger reports under the **Standard Content** folder because this folder is "whitelisted." Using this method will prevent you from seeing two date prompts (one prompt for the global parameter provider and a second prompt for their own built-in date prompt). Alternately, if you choose to place the Logger reports the **Custom Content** folder, you might see two date prompts.

   c. Select the **Import Assets** icon.

d. Select the .zip file you want to import and select the newly created folder on the **Import Assets** page.

> NOTE: Be sure that the "Overwrite assets of the same name." is **not** selected. (This ensures you do not accidentally overwrite any common or required assets.

The imported reports now display in the new **Standard Content** Logger folder.

When you run the tool on a system with SSL enabled, you might see various *"IOException while communicating with server"* exceptions. These are messy but can be ignored.

> **Note:** The following is a passage from the InetSoft's original converter tool instructions that can be found in **LoggerConverter.pdf**:
>
> The custom InetSoft instance and Vertica datasource are secured with FIPS mode and SSL, the JVM options used to secure the instance for the inetsoft server need to be added to the inetsoft-shell.sh file to avoid the errors connecting to the datasource. However, these errors do not cause issues with the export but may result in issues with the datasource dependency export. Therefore, when importing the export into EM, uncheck the dependent datasourse to prevent import.

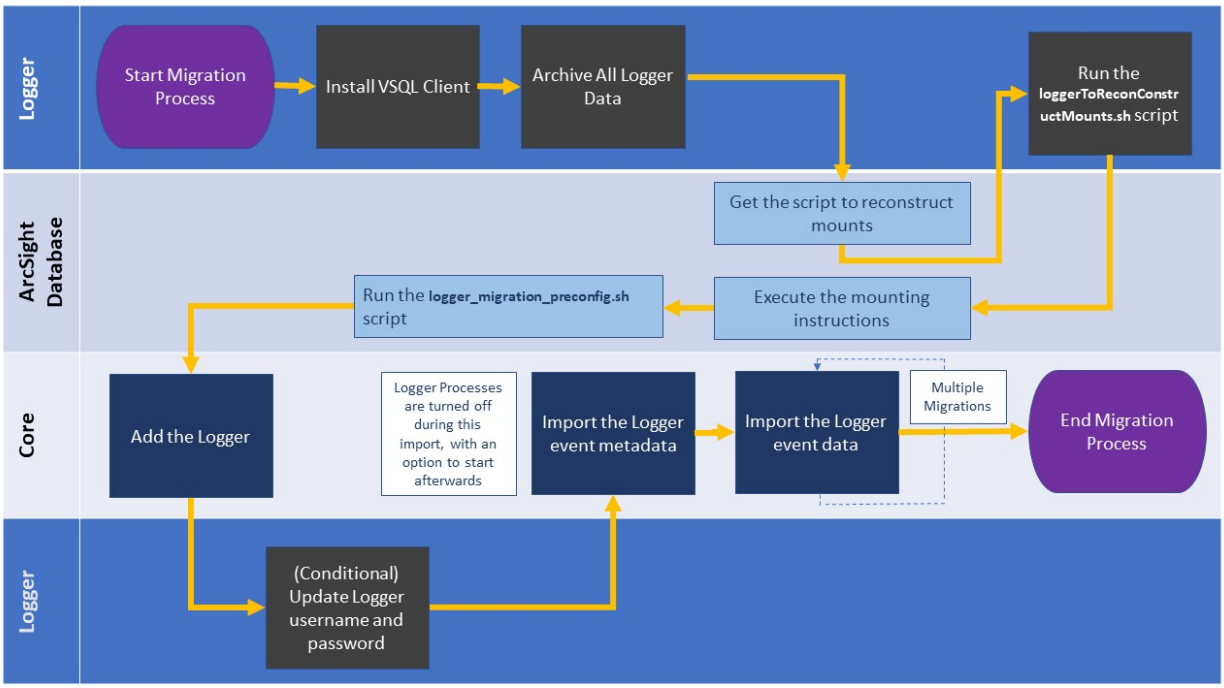
Migrating Logger Data to the ArcSight Database

> The procedure and steps described in this section have been tested with Logger and ArcSight Platform installed on two different machines

The Core Search functionality is able to not only encompass events received from sources such as SmartConnectors, but also imported from ArcSight Logger archives. To take advantage of this feature, you must first make the archived Logger events available to Core by importing them into the ArcSight Database.

This section guides you through the process of preparing your Logger metadata and then its corresponding archived events to be imported to the ArcSight Database.

To start the procedure, please follow the "Checklist: Migrating Logger Data" on the next page.



Checklist: Migrating Logger Data

Does not apply in a SaaS environment.

Use the following checklist to migrate event data from Logger. You must perform the tasks in the listed order.

	Task	See
❑	1. Ensure that you have read the considerations and can comply with the prerequisites for importing Logger data	"Prerequisites and Considerations for Importing Logger Data" on the next page
❑	2. Install VSQL Client Driver in Logger	"Install VSQL Client Driver" on page 655
❑	3. Archive all live data in Logger	"Archive Live Logger Data" on page 656
❑	4. Get the `loggerToReconConstructMounts.sh` script from ArcSight Database	"Obtain the Construct Mounts Instructions Script" on page 658

❑	5. Run the script to get archives mounting instructions	"Execute the Construct Mounts Instructions Script" on page 659
❑	6. Run the mounting instructions and `logger_migration_preconfig.sh` script in the ArcSight Database. If Multi-tenancy is enabled, run the `logger_migration_preconfix.sh -t <tenantKey>` script in the ArcSight Database. Notice that the -t parameter is optional and the value `<tenantKey>` represents the tenant key for an onboarded tenant.	"Execute the Instructions in ArcSight Database " on page 659
❑	7. From Core, import the Logger events	Importing Logger Data to the ArcSight Database (non-SaaS)

Prerequisites and Considerations for Importing Logger Data

Does not apply in a SaaS environment.

Since this process involves different ArcSight products interacting with each other, ensure that you have the correct credentials and requirements for all of them before you proceed.

- "Considerations for Importing Logger Data" below
- "Prerequisites for Logger" below
- "Prerequisites for the ArcSight Platform" on the next page

Considerations for Importing Logger Data

Please review the following considerations that affect how you can migrate data from Logger to the ArcSight Database.

- The process **imports only the archived events from the current Logger instance**. The process does not migrate content, configuration, and data from Logger peers.
- Logger event ingestion can continue up until the Import Metadata for Logger Events step. At that point, the recommendation would be to:
  - Stop all Logger event ingestion
  - Switch connectors to send events to the ArcSight Database
  - Archive all the existing events in Logger before importing the Logger metadata
- You can perform only one migration at a time. If you plan to migrate data from different Loggers, run the migrations sequentially.

Prerequisites for Logger

- Admin user with SSH credentials.

- The username and password that you use to import Logger data must match the OS credentials set in Logger.
- The system directory must have enough space. For more information, see the Release Notes for ArcSight Logger 7.3.
- The Logger host will need to have the **VSQL Client Driver** installed (as explained in Step 1 of the procedure).

Prerequisites for the ArcSight Platform

- Admin user with ArcSight Database credentials.
- The system directory must have enough space. For more information, see the *Technical Requirements for ArcSight Platform 24.2*.
- The ArcSight Platform capabilities must be reachable from the Logger instance (on port 5433).
- ArcSight Database version 11.1, or more recent
- For the migration process, the user must have the *Logger Data Migration* permission assigned in Core (check **View Available Permissions** in the *User guide for ArcSight Platform 24.2*). This is assigned by default to the *System Admin* role, but the user could have a custom role that includes the permission.
- For search execution after the data has been imported, users must have either the *Default Role* or a role with appropriate Search permissions.

Install VSQL Client Driver

Does not apply in a SaaS environment.

The Logger host requires the VSQL client to perform the data migration procedure. If client is not present yet, follow these steps to install the VSQL Client driver.

1. Download the TAR version of the driver.

   This feature requires, at a minimum, version 11.1 of the ArcSight Database

   Tip: Micro Focus recommends to use the same version for database server and TAR driver. Refer to the Technical Requirements for Arcsight Platform for details on the supported version.

2. To extract the TAR from the directory, run the following command:

   ```
   tar xvfz vertica-client-[version] [OS].tar.gz -C /
   ```

3. From your home directory, add the PATH:

```
cd ~
```

4. Open the file:

```
vi .bashrc
```

5. On the PATH variable located at the **/opt/vertica/bin** file, add the vsql path:

```
export PATH-$ANT_HOME/bin:$JAVA_HOME/bin:$PATH:$P4_
HOME/bin:/opt/vertica/bin
```

If the PATH variable is not found, create it:

```
PATH=$PATH:/opt/vertica/bin
```

6. Save the changes:

```
:wq
```

7. Press **Enter**.
8. Refresh the .bashrc file:

```
source .bashrc
```

9. To verify VSQL has been installed, run the following command:

```
vsql --version
```

Archive Live Logger Data

Does not apply in a SaaS environment.

The steps listed in this procedure must be performed on your ArcSight Logger

All live data in Logger must be archived before you attempt the migration process.

- "Configure the Archive Storage Setting" below
- "Add an Event Archive" on the next page

Configure the Archive Storage Setting

Required only if you have not previously configured this setting

If you are using the Logger Appliance, create the NFS or CIFS mount point. For more information, see the Storage and Remote File System sections in Chapter 6 of the *Administrator's Guide to ArcSight Logger*. If you are using Software Logger and intend to use an

NFS or CIFS mount point, ensure that the external storage point is mounted on the machine on which Logger is installed. For more information, see your system's operating system documentation.

1. Go to **Configuration** > **Storage** > **Archive Storage Settings**.
2. Specify a mount location and an archive path for each storage group. You can specify a different path for each storage group, thus enabling Logger to archive events to a different location for each storage group.

   You can configure settings for all storage groups on the **Archive Storage Settings** page even if you do not intend to archive all of them. Logger enables you to only save the storage group paths that have a mount configured and ignore the empty fields.

   - On a Logger Appliance L7700: Select (from the list box) a path in the Archive Path field appended to the path specified in the mount location. This location can be an NFS mount, CIFS mount, which is configured using the Logger user interface.

     For example, if the mount location you selected refers to the path `/opt/ARCHIVES`, and the archive directory in that location is `archivedir`, then specify `archivedir` in the **Archive Path** field.
   - In a Logger Software or a Logger Appliance L8000, enter a complete path where the archive file will be written in the **Archive Path** field. This path could be a local directory or a mount point already established on the Logger host.

   Tip: On Software Loggers, the **Mount Location** field does not exist.

3. Click **Save**.

   If all fields are blank or without any changes, Logger will display the message *No changes have been made*. Otherwise, Logger will acknowledge the configuration with the message *Archive Storage Settings saved successfully*.

Add an Event Archive

1. Select **Configuration** > **Storage**.
2. Select **Event Archives**.
3. Click **Add**.
4. For **Name**, enter a meaningful name for the new **Event Archive**.
5. Specify the **Start** and **End** dates in the `m/dd/yy` format, where m is month number, dd is the day of the month (with a leading zero if necessary), and yy is the two-digit year number.

When the **Start** and **End** dates are different, one archive file per storage group, for each specified day is created. For example, that will be the case when you specify the following **Start** and **End** dates:

Start Date: 8/12/19

End Date: 8/13/19

> Note: If a day's events have already been archived, you will not be able to archive them again. If you try to archive the same day's events twice, Logger will display a message with the already archived day or dates. If you are archiving a range of dates and some of them have been archived, the archive process will complete, skipping any days already archived, and a message will display the

And, if you configure both storage groups—**Internal Event Storage Group** and **Default Storage Group**, four archive files will be created as a result of this archive operation—two files per storage group for the specified two days.

The **Event Archives table** (in the **Event Archives** page) lists the archives by an alias in this format:

```
<archive_name> [<yyyy-m-dd>] [<storage_group_name>]
```

6. Select the names of the storage groups that need to be included in the archive.
7. Click **Save** to start archiving events, or **Cancel** to quit.

> Note: You can cancel an in-progress archive operation at any time using the Cancel link that displays on top of the Event Archives page.

> If corruption cases have been detected before, please see the instructions for how to sanitize an Event Archive in Chapter 5 of the Administrator's Guide for ArcSight Logger.

Obtain the Construct Mounts Instructions Script

Does not apply in a SaaS environment.

To obtain the instructions for mounting the archives in the ArcSight Database, complete the following steps:

1. Navigate to the scripts folder in the ArcSight Database server, by default `/opt/arcsight-db-tools/scripts/`.

   This is where the `loggerToReconConstructMounts.sh` script is located.
2. To move the script to the Logger Server from which you want to import Logger Archive events, execute the following command:

```
scp /opt/arcsight-db-tools/scripts/loggerToReconConstructMounts.sh
root@<LOGGER IP>/opt/
```

Execute the Construct Mounts Instructions Script

Does not apply in a SaaS environment.

To generate instructions for the mounting of the data, complete the following steps:

> The output instructions are for guidance purposes only. They can be used as-are in Logger Appliances, but for Software Loggers, which can save data locally or externally, you must make sure that the path contained in the instructions corresponds to the NFS mount you created when configuring archive storage. See "Archive Live Logger Data" on page 656.

1. Give the execute right to the script that you just copied on the Logger Server:

   ```
   chmod +x ./loggerToReconConstructMounts.sh
   ```

2. Execute the script:

   ```
   ./loggerToReconConstructMounts.sh $<INSTALL LOGGER PATH>
   ```

3. The instructions generated will consist of the **mkdir** command to create a directory, and the **mount** command to perform the actual mounting, for example:

   ```
   Getting the instructions for /opt/mnt/ARCH-141-203
   mkdir -p /opt/LOGGER_15214141203/opt/mnt/ARCH-141-203
   mount -t nfs 15.214.129.238:/opt/shared|nfs4 /opt/LOGGER_15214141203/opt/mnt/ARCH-141-203
   ```

   These instructions will be generated for each of the mounts to be migrated.

Copy these instructions to execute them in ArcSight Database.

If the process fails to find archives that can be migrated, no instructions will be generated, and you will be notified by a UI message.

Execute the Instructions in ArcSight Database

Does not apply in a SaaS environment.

You must configure the ArcSight Database to receive the Logger migrated data.

> The following instructions need to be run as **root** user, or a user with sudo credentials

1. To mount the archives on the ArcSight Database nodes, from your Linux command line, execute the commands that you copied or came up with during the procedure in "Execute

the Construct Mounts Instructions Script" above.

2. Run the `logger_migration_preconfig.sh` script located by default in the `/opt/arcsight-db-tools/scripts/` directory.

Managing Transformation Hub

This section provides guidance for managing Transformation Hub functions and features within the deployment.

Maintaining a Deployment on AWS

Maintenance of an AWS deployment is performed through the bastion host.

Enabling Access to Kafka Manager

Kafka Manager is the management tool for maintenance, management, and monitoring of topics, partitions, consumers, and Kafka brokers. It is integrated with the Core UI and it supports Single Sign-On (SSO). The Core `Manage Kafka` permission is required for a user to access Kafka Manager.

> The Manage Kafka permission is included by default in the System Operations Administrator and System Admin roles, and it is not included in the Admin role. If needed, you can manually add the Manage Kafka permission to the Admin role.

To access Kafka Manager using the default Core admin user with the Manage Kafka permission:

1. Follow the steps documented in the Core capability section: Creating the First System Admin User.

To access Kafka Manager using a non-default Core admin user with the Manage Kafka permission:

> **Note:** Before proceeding, request the default admin to assign the Manager Kafka permission to the non-default admin user.

1. Log in to the bastion.
2. Browse to `https://<cdf_external_hostname>/th/cmak`.
3. Log in using the user credentials.

4. Log out by browsing to the Core home page: `https://<cdf_masternode_hostname or virtual_ip hostname>/`

Refreshing the ECR Credentials in Kubernetes

During the initial OMT installation, the credentials and the URL for the ECR (Elastic Container Repository) are passed through environment variables `ECR_USER_NAME`, `ECR_USER_PASSWORD` and `ECR_URL`. All of these values are then stored inside Kubernetes as **Secrets** for use in OMT during installation as well by your ArcSight Suite products.

The security policy on `AWS ECR` requires that the `ECR_USER_PASSWORD` is valid for 12 hours after creation. The following scenarios require a refresh of the password used to access the Docker images stored in the ECR when:

- The bootstrap of OMT was performed on port 3000 more than 12 hours before installation
- You need to add a new capability to the suite, images are uploaded but not registered on OMT
- You are performing a suite upgrade

In such cases, replace the stored user password with a freshly generated one

To refresh the credentials:

1. On the bastion, change directory to `arcsight-platform-cloud-installer-23.2.X/aws-scripts/scripts`.
2. Generate a new `ecr_credentials` snippet by running the command:

   ```
   ./upload_images_to_ECR --get-ecr-credentials
   ```

3. Add the retrieved values to the environment:

   ```
   source ecr_credentials
   ```

4. Run the following script to create a set of JSON files to be applied to the cluster:

   ```
   ./generate_aws_secret
   ```

   > The script has no output, except when one or more required environment variables (`ECR_USER_NAME`, `ECR_USER_PASSWORD` or `ECR_URL`) are empty. This procedure though generates several new files named `secret_xxxx.json` in the directory where you ran the `generate_aws_secret` script.

5. Execute the following command to apply all generated files to Kubernetes:

   ```
   kubectl apply -f secret_core.json
   ```

6. Verify in the OMT, if all required or missing images are available when uploaded to the ECR correctly.

Installing the Kubernetes Metrics Server

The Kubernetes Metrics Server is a service running inside the Kubernetes cluster, which collects various utilization and performance data later used by the ArcSight Management Center (ArcMC).

A detailed guide on how to install Kubernetes Metrics Server service is provided by AWS. It is expected that the version of Kubernetes Metrics Server will evolve as the time goes by.

Removing the Cluster

You can remove the cluster to make it possible to perform a fresh installation of OMT and the ArcSight Suite. As part of the removal, you will remove or clean some cluster-specific resources. However, some of your existing resources are reusable.

Reusable Resources

Many of the resources created during your OMT and ArcSight Suite installation are reusable, and do not need to be removed during the cluster removal. You might find it useful to keep such resources on hand for use with other product suites.

- Launch template is not dependent on the OMT installation and is not bound to a VPC. Other users performing installation in the same region could re-use an already existing launch template.
- Bastion instance is bound to the VPC created for OMT, and can be used only within this VPC. However, a bastion is a highly re-usable resource for installing and managing other clusters or product suites.
- The Route 53 record set, with its certificate, is not dependent on the installation.

Cluster Removal

As part of removing the cluster, you will perform the following tasks:

- Removal of the Auto Scaling group
- Removal of the EKS control plane
- Cleaning or deleting the EFS/NFS

Each of these procedures is explained below.

Removing the Auto Scaling Group

The AWS Auto Scaling group holds the worker nodes instances. Accordingly, in order to delete the worker nodes, you must delete the Auto Scaling group.

To delete the Auto Scaling group:

1. Run the following command:
   ```
   aws autoscaling delete-auto-scaling-group --force-delete --auto-scaling-group-name <auto-scaling group name from AWS worksheet>
   ```
2. The command has no output, and in the background the deletion instances will start. Check the presence of the Auto-Scaling group by running the following command:
   ```
   aws autoscaling describe-auto-scaling-groups \
   | jq -r '.AutoScalingGroups[] | select(.AutoScalingGroupName=="<auto-scaling group name>") | .AutoScalingGroupName'
   ```

> If the group name is returned, the Auto Scaling group and its instances are not fully deleted including its instances. The process can take around 5 minutes to complete.

3. Once the auto-scaling group and worker nodes are removed, you can check the pods by executing this command on the bastion:
   ```
   kubectl get pods -A -o wide
   ```

All pods are shown in the Pending state, as they do not have a host to run on, but the Kubernetes control plane still has the cluster definition.

If desired, you can create another Auto Scaling group with a different launch template. All the pods will be deployed and started on the new worker nodes. Remember to add respective targets to Target Groups. Any new worker nodes will receive new instance IDs.

Removing the EKS Control Plane

The Kubernetes control plane holds the definitions of services, daemons, deployments, pods, and other resources, including the fully qualified identifier of Docker images in the registry. To clean the AWS infrastructre for a new installation, this control plane needs to be removed as well.

To remove the EKS control plane:

1. Run the following command:
   ```
   aws eks delete-cluster --name <cluster name from AWS worksheet>
   ```

> The command output is very verbose. An example is given below.

2. Verify the cluster has been deleted by running the command:
   `aws eks list-clusters | jq -r '.clusters[] | select(.=="<cluster name from AWS worksheet>")'`

   An empty output indicates that the cluster has been deleted.

Example output of a cluster in the process of being deleted:

```
{
   "cluster":{
      "name":"srgdemo-cluster",
      "arn":"arn:aws:eks:eu-central-1:115370811111:cluster/srgdemo-cluster",
      "createdAt":"2020-08-10T12:13:31.748000+02:00",
      "version":"1.26",
      "endpoint":"https://90842F339FC27B9BE1DD0554E508B914.gr7.eu-central-
1.eks.amazonaws.com",
      "roleArn":"arn:aws:iam::115370811111:role/ARST-EKS-Custom-Role",
      "resourcesVpcConfig":{
         "subnetIds":[
            "subnet-0fb2ebb5882c061f0",
            "subnet-0abd7cd806e04c7be",
            "subnet-0f0cac4ec6837abed"
         ],
         "securityGroupIds":[
            "sg-0ce3c569f73737b77"
         ],
         "clusterSecurityGroupId":"sg-0263ae0d4c33decc4",
         "vpcId":"vpc-0143197ca9bd9c117",
         "endpointPublicAccess":false,
         "endpointPrivateAccess":true,
         "publicAccessCidrs":[

         ]
      },
      "logging":{
         "clusterLogging":[
            {
               "types":[
                  "api",
                  "audit",
                  "authenticator",
                  "controllerManager",
                  "scheduler"
               ],
               "enabled":false
            }
         ]
      },
```

```
      "identity":{
         "oidc":{
            "issuer":"https://oidc.eks.eu-central-
1.amazonaws.com/id/90842F339FC27B9BE1DD0554E508B914"
         }
      },
      "status":"DELETING",
      "certificateAuthority":{

"data":"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUN5RENDQWJDZ0F3SUJBZ0lCQURBT
kJna3Foa2lHOXcwQkFRc0ZBREFWTVJNd0VRWURWUVFERXdwcmRXSmwKY201bGRHVnpNQjRYRFRJd0
1EZ3hNREV3TWpFd01sb1hEVE13TURnd09ERXdNakV3TWxvd0ZURVRNQkVHQTFVRQpBeE1LYTNWaVp
YSnVaWFJsY3pDQ0FTSXdEUVlKS29aSWh2Y05BUUVCQlFBRGdnRVBBRENDQVFvQ2dnRUJBSnZXCnUy
MDVNZFJkWUV1VkliQU1yeFJzKzFSMmtyRlhWUmpZd0ZXQUdIRUY2WmJ6V1F2L2Y0d052MmlxaFM0Q
0lJa2wKVTVvTmtaTzFBaU9USk9Ja1l3UFAwdjRGQkNyVFlvU3BldW1xelhqVFBHU2JFUVJ4OXFVM0
ttTkorUXlSZEhJeQpaTHV6b2tXbXJXSG1TVlRLNUxkZUppN3Z4enoweU1TNzczL01GK3FkcVNML2o
1dHJTNEt2cU5ObVRKMEVVY0hwCjdWNklENnFaSEVxZXdKQjl2cmhPdGFlc05TMFdhVWwwUFU4d3pW
aFVUWUlEMllFTU8rOXFsZEdVQVlWTmo3cVIKMUdXVVNVZVVIUWJqNEViMHg4VGhjcDNPYi9oZUNQW
WZ1Rno5MVRWUUR5enRxaDZtUDQvNXFZaW1QeklkaFh5LwpIdDltVmZ3M0tVemlzMURtNk9VQ0F3RU
FBYU1qTUNFd0RnWURWUjBQQVFIL0JBUURBZ0trTUE4R0ExVWRFd0VCCi93UUZNQU1CQWY4d0RRWUp
Lb1pJaHZjTkFRRUxCUUFEZ2dFQkFDU2pyZG5Xb0N1WTA4c3pqVU5BSHdnbnFtMDgKZlhydkxtVkxz
SHZiZHFSTmorUTJQMFQvVCtFZFRVWFg5SGNia1JwQU5QNTRkNzRQRmJGbzA0K0dmaTYrTHE5UAoyY
lBzZ2o3Mmo4WWx0V0twVHJiNFpKMnhyZXFsWnZ4MVFZNHpZWUhKdDdKZ1RRaU4xQ2JjaFZLR0V6K0
9nQ3ZTClZGMWE2OEJJajlUMFFDNXgzTTJncHdDa1JMOHArbXkzbkp0Z281Q0JHanhGU2ZHNnN3M0Z
MRXdlRHQyc2dOc1UKV2hpQWZGQmtPdUl2OENmMmlwMUZYQ2toWjJxTXdYanU4UzFFc3Z3bUcrSy9v
d3NiOUFLZG5TaVRQVXJSQWdGbwpsVjBrSGVaK1FpSG5wK0t3a1NpbkoyMVpXRUFMVG5GRjBCR3hYM
DhpU1cwM25Kcy9XemRFdTVFWWhUYz0KLS0tLS1FTkQgQ0VSVElGSUNBVEUtLS0tLQo="
      },
      "platformVersion":"eks.1",
      "tags":{
         "user":"user"
      }
   }
}
```


Cleaning or deleting NFS/EFS

Your NFS/EFS is a partially reusable resource. For the EFS you created, you have the following options:

- Leave the existing EFS folder structure intact. A new installation will use a parallel structure. No action needs to be taken.
- Delete and re-create the folder structure during a new installation. The procedure is

discussed below.

- Delete the EFS instance completely. The procedure is discussed below.

To delete the folder structure:

1. Log on to the bastion host.
2. Unmount the EFS file system by running the following command:
   `sudo umount -f /mnt/efs`
3. As a `sudo` user, open the file `/etc/fstab` in a text editor.
4. Locate the following line:
   `fs-5df66605.efs.eu-central-1.amazonaws.com:/ /mnt/efs nfs4 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,_netdev 0 0`
5. Uncomment the line and then save the file.
6. Mount EFS to the bastion by running the following command:
   `sudo mount -a`
7. Change your current working directory to the mount point, in our case `/mnt/efs`.
8. Delete the whole folder structure by running the following command:
   `sudo rm -Rf <parent folder from AWS worksheet>`

To delete the EFS instance (not required for re-installing the OMT bootstrap):

1. Delete the mount targets by running the following command on each configured mount target:
   ```
   aws efs delete-mount-target \
   --mount-target-id <mount target id from AWS worksheet>
   ```
2. Verify the deletion by running the following command:
   ```
   aws efs describe-mount-targets \
   --file-system-id <filesystem Id from AWS worksheet>
   ```

Example output:

```
{
   "MountTargets":[

   ]
}
```

3. Delete the filesystem by running the command:
   `aws efs delete-file-system --file-system-id <filesystem Id from AWS worksheet>`

Next Steps

At this point the filesystem has been deleted. As explained above, some reusable resources will remain.

- The Application Load Balancer, its listeners, and target groups are not dependent on installation. For a new installation, you will need to add new targets to all target groups.
- The VPC tag marking the EKS cluster has been removed, and the required tag `kubernetes.io/cluster/<cluster name>` has been removed as well. Remember to add it before new installation.

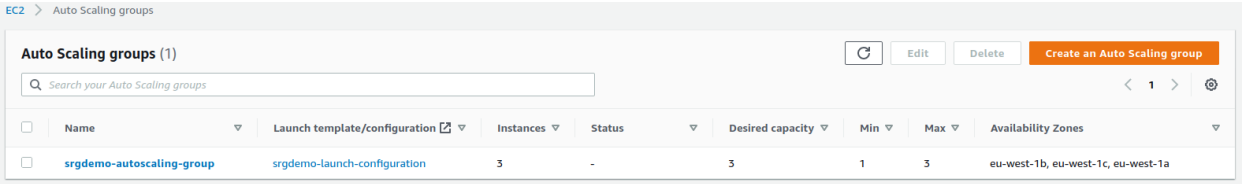
You can now perform a clean installation of a new cluster.

Scaling Up an AWS Cluster

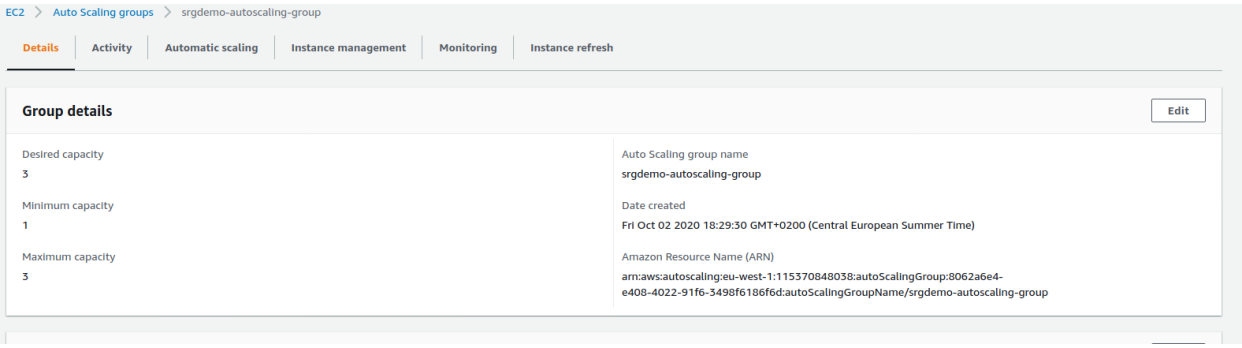
The process of scaling up a cluster involves adding nodes, labeling them as required, and performing some additional configuration. In an AWS cluster, instances are managed by Auto Scaling groups, which include the current number of nodes, as well the upper and lower limits of the nodes for the cluster, and these values must be adjusted to accomodate new instances.

To scale up a cluster using the Web UI:

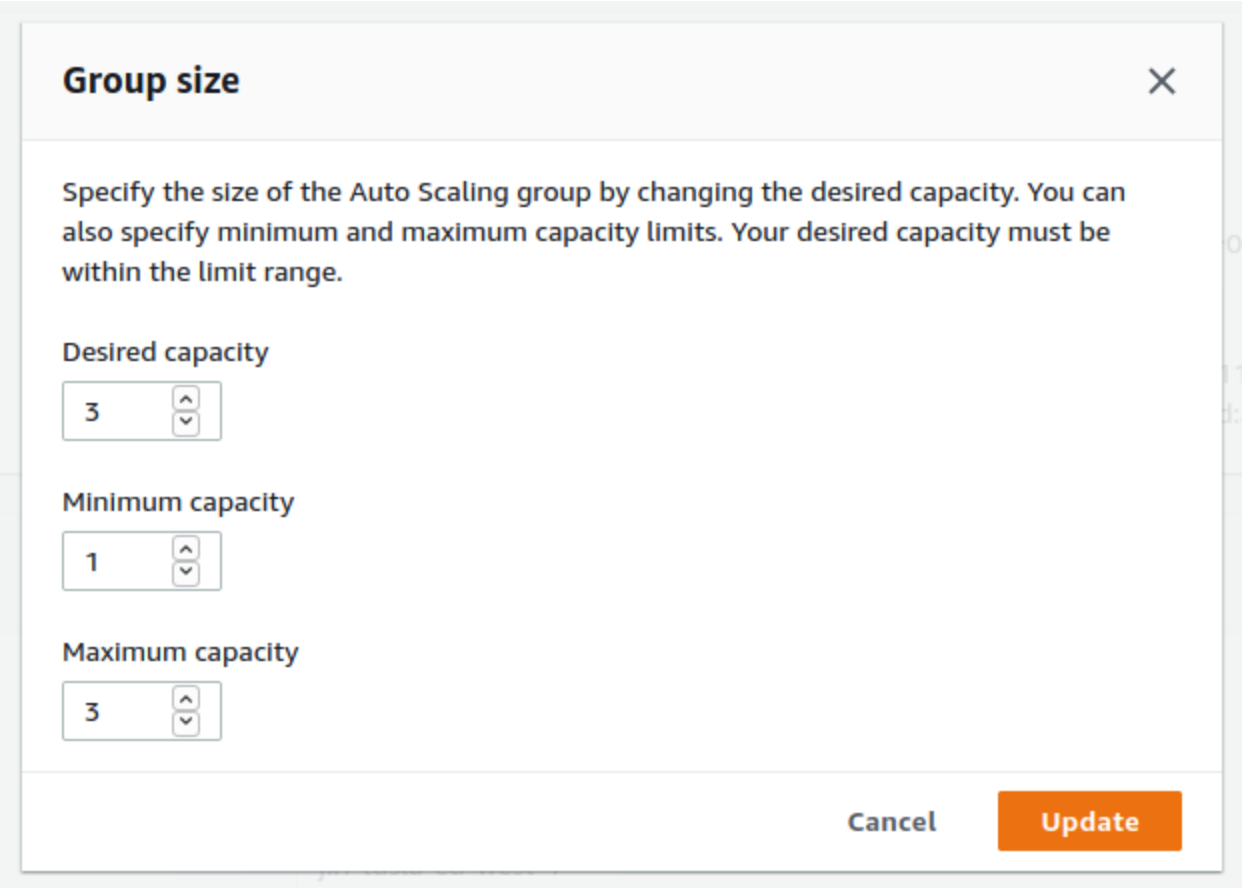
1. Using the Find Services search tool, locate and browse to the EC2 Dashboard.
2. In the left navigation panel, under **Auto Scaling,** click **Auto Scaling Groups**.
3. From the list of **Auto Scaling groups**, click the Auto Scaling group that you previously created.



4. On the **Details** tab, under **Group Details**, click **Edit**.



5. On the **Group Size** dialog, specify values for the cluster's desired, minimum, and maximum capacities.
6. Click **Update**.



7. You are returned to the Auto Scaling group details. The group status is shown as *Updating capacity.*

To scale an AWS cluster up using the CLI:

1. Verify that the new number of nodes will fit into the existing limits set on your Auto Scaling group. Run the following command:
   ```
   aws autoscaling describe-auto-scaling-groups --auto-scaling-group-names
   <your auto-scaling group name> \
   | jq -r '.AutoScalingGroups[0] | "MaxSize: " + (.MaxSize |
   tostring),"DesiredSize: " + (.DesiredCapacity | tostring),"MinSize: " +
   (.MinSize | tostring)'
   ```

Example input and output:

```
aws autoscaling describe-auto-scaling-groups --auto-scaling-group-names
srgdemo-autoscaling-group \
| jq -r '.AutoScalingGroups[0] | "MaxSize:         " + (.MaxSize |
tostring),"DesiredCapacity: " + (.DesiredCapacity | tostring),"MinSize:
  " + (.MinSize | tostring)'
```

```
MaxSize:         3
```

```
DesiredCapacity: 3
```

```
MinSize:         1
```

In this example, both the `DesiredCapacity` as well as the `MaxSize` must be increased.

2. Increase the number of nodes in the Auto Scaling group by running this command (command has no output):
   ```
   aws autoscaling update-auto-scaling-group \
   --auto-scaling-group-name <your auto-scaling group name> \
   --max-size <new maximum size of the cluster> \
   --desired-capacity <desired new number of nodes>
   ```

Example:

In this example, the number of active nodes in our example group `srgdemo-autoscaling-group` is raised to 5, and at the same time the group capacity is increased to 7. The command has no output.

```
aws autoscaling update-auto-scaling-group \
--auto-scaling-group-name srgdemo-autoscaling-group \
--max-size 7 \
--desired-capacity 5
```

3. To verify the updated values, repeat the command shown in Step 1 above.
4. To verify creation of the new nodes, on the bastion host, run the following command until the desired number of nodes is shown in the Ready state:
   `kubetlc get nodes`

Labeling New Nodes

You might need to label the new nodes after they are added and ready to use.

- You will not need to add new labels to new nodes if you have previously extended the set of labels for the Launch template.
- Otherwise, proceed to "Labeling Cloud (AWS) Worker Nodes " on page 223.

To verify labels on new nodes:

Run the following command:

```
kubectl get nodes --show-labels
```

Extending Targets in Target Groups

Your newly created nodes are now labeled. Kubernetes might migrate pods used for installation, management and re-configuration to these new nodes as part of cluster operations. You will now need to perform some tasks for the new nodes that you have previously performed for the old nodes.

1. Retrieve instance IDs from auto-scaling group: Retrieve the IDs of all instances in your cluster. Identify the new instances by comparing with existing list of instance IDs. Note any new instance IDs to your AWS worksheet.
2. Repeat the steps listed in Target Group 3000 - Get OMT Ingress service node port for 3000 and Add targets to target group 3000 to extend routing for installation portal.
3. Repeat the steps in chapter Configure access to OMT management - Get OMT Ingress service node port for 5443 and "Adding Targets to the Target Group for Port 5443 and 443" on page 245 to extend routing for management portal.
4. Repeat the step in chapter Configure access to re-configuration - Add targets to target group 443.

You might use the web UI or CLI to perform these tasks, as desired. Only apply these procedures to your new nodes.

Additional Steps

For Transformation Hub, see the following procedures:

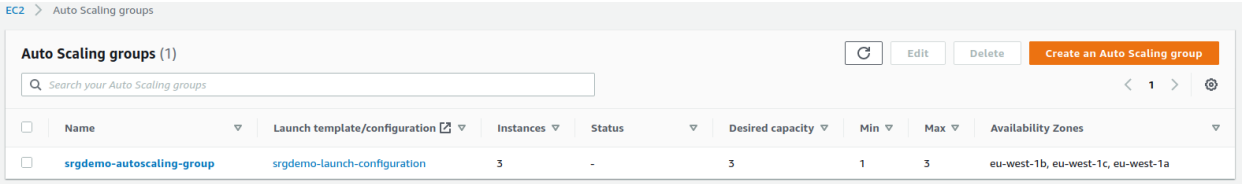
- Adding a Kafka Broker Instance
- Adding a ZooKeeper Instance

Scaling Down an AWS Cluster

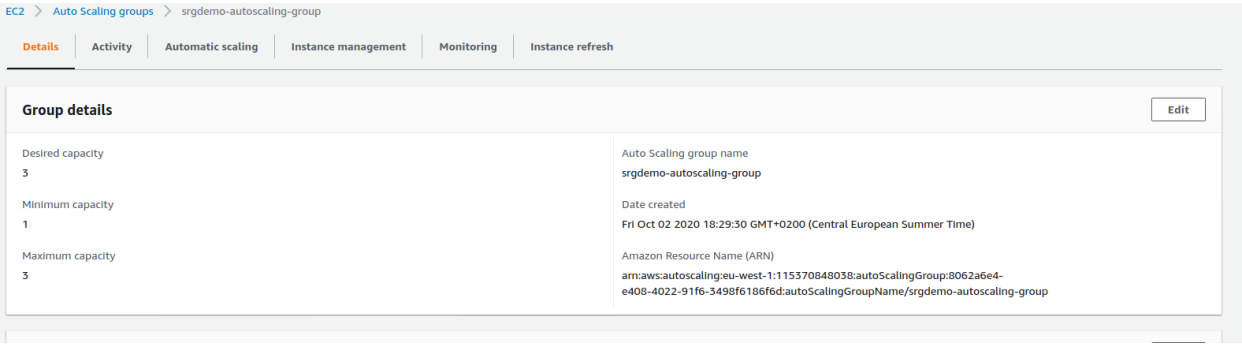
In an AWS cluster, instances are managed by Auto Scaling groups, which include the current number of nodes, as well the upper and lower limits of the nodes for the cluster.

To scale down a cluster using the Web UI:

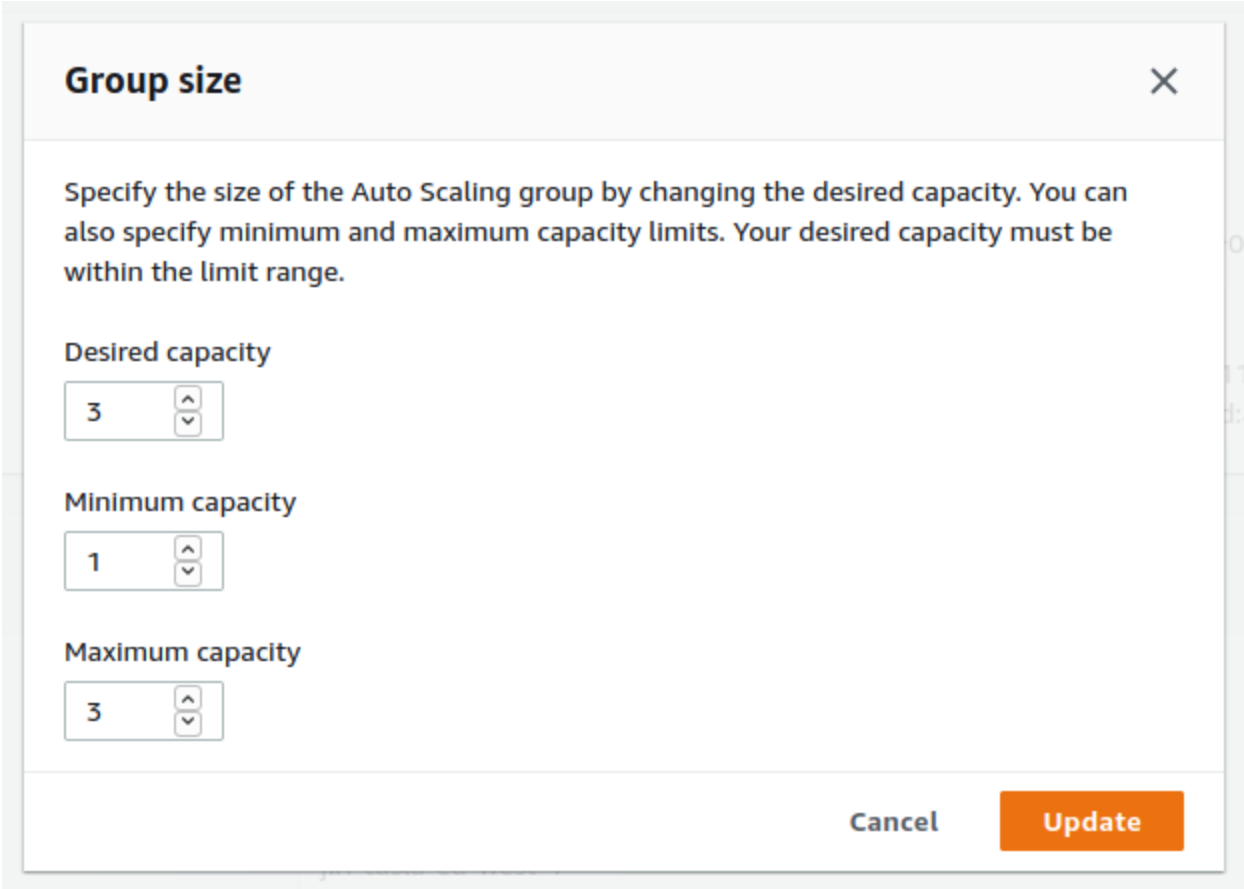
1. Using the Find Services search tool, locate and browse to the EC2 Dashboard.
2. In the left navigation panel, under **Auto Scaling,** click **Auto Scaling Groups**.
3. From the list of **Auto Scaling groups**, click the Auto Scaling group that you previously created.



4. On the **Details** tab, under **Group Details**, click **Edit**.



5. On the **Group Size** dialog, specify new values for the cluster's desired, minimum, and maximum capacities.



6. Click **Update**.
7. You are returned to the Auto Scaling group details. The status is shown as *Updating capacity*.

To scale down the number of nodes in an AWS cluster using the CLI:

1. Verify the existing limits set on your Auto Scaling group. Run the following command:
```
aws autoscaling describe-auto-scaling-groups \
--auto-scaling-group-names <your auto-scaling group name> \
| jq -r '.AutoScalingGroups[0] \
| "MaxSize: " + (.MaxSize | tostring),"DesiredSize: " + (.DesiredCapacity
| tostring),"MinSize: " + (.MinSize \
| tostring)'
```

Example input and output:

```
aws autoscaling describe-auto-scaling-groups \
--auto-scaling-group-names srgdemo-autoscaling-group \
| jq -r '.AutoScalingGroups[0] \
| "MaxSize:         " + (.MaxSize \
```

```
| tostring),"DesiredCapacity: " + (.DesiredCapacity \
| tostring),"MinSize:         " + (.MinSize | tostring)'
```

```
MaxSize:         5
```

```
DesiredCapacity: 5
```

```
MinSize:         1
```

In this example, it would be possible to scale down to 3 nodes without any other configuration changes.

2. Decrease the number of nodes in the Auto Scaling group by running the command (command has no output):
   ```
   aws autoscaling update-auto-scaling-group \
   --auto-scaling-group-name <your auto-scaling group name> \
   --desired-capacity <desired new number of nodes>
   ```
3. To verify the updated values, repeat the command shown in Step 1 above.

The AWS will then gracefully stop the removed nodes (2 in our example) and destroy their VMs.

Understanding the Transformation Hub Kafka Manager

The Transformation Hub Kafka Manager enables you to monitor and manage your clusters, topics, and partitions, and perform the following tasks:

- Viewing and managing cluster states, including topics, consumers, offsets, broker nodes, replica distribution, and partition distribution.
- Creating and updating topics.
- Generating partitions and adding partitions to a topic.
- Reassigning partitions to other broker nodes, such as replacing a failed node with a new one.
- Reassigning partition leaders to their preferred broker node after a node temporarily leaves the cluster (for example, in case of a reboot).
- Managing JMX polling for broker-level and topic-level metrics.

Enabling Access to Kafka Manager

Kafka Manager is the management tool used for maintenance, management, and monitoring of topics, partitions, consumers, and Kafka brokers. See **Assigning Permissions to Roles** in the

User guide for ArcSight Platform 24.2. The **Manage Kafka** permission is required to access the Kafka Manager.

> The Manage Kafka permission is included by default in the System Operations Administrator and System Admin roles, and it is not included in the Admin role. If needed, you can manually add the Manage Kafka permission to the Admin role.

To access Kafka Manager:

1. Browse to `https://<cdf_masternode_hostname or virtual_ip hostname>/th/cmak`
2. Log in with a user account with the Manage Kafka permission and perform the required task.
3. Log out by browsing to the Core home page: `https://<cdf_masternode_hostname or virtual_ip hostname>/`

Managing the Kafka Cluster

The **Clusters** page is the Transformation Hub Manager's home page. From here you can modify, disable or delete a cluster from view in the Transformation Hub Manager (the cluster itself is not deleted), or drill down into the cluster for more information.

Location: Clusters

Click the *Cluster Name* link. The Transformation Hub Manager displays the **Cluster Summary** page. For more information, see Viewing Information About a Cluster.

To edit the cluster:

1. Click **Modify**. The Transformation Hub Manager displays the **Update Cluster** page.
2. Update the appropriate fields, and click **Save**.

> Editing the cluster is an advanced operation, and normally the cluster should never be edited.

To disable the cluster:

Click **Disable**. Once a cluster has been disabled, a **Delete** button is displayed.

To delete the cluster:

After disabling the cluster, click **Delete**.

Viewing Information About a Cluster

On the **Summary** page, you can view the ZooKeeper processes in your cluster and drill down into its topics and broker nodes for more information.

Location: Clusters > *Cluster Name* > Summary

- "Viewing Information" below
- "Viewing or Editing the Topics" below
- "Viewing or Editing the Broker Nodes" below

Viewing Information

To view information about your cluster:

- If the cluster is not yet open, click **Cluster > List** in the navigation bar. Then click the *Cluster Name* link.
- If the cluster is already open, click **Clusters > *Cluster Name* > Summary**

Viewing or Editing the Topics

To view or edit the topics in your cluster:

Click the **Topics** hyperlink (number of topics) to show the topics in the cluster. For more information, see Managing Topics.

Viewing or Editing the Broker Nodes

To view or edit the broker nodes in your cluster:

Click the **Brokers** hyperlink (number of broker nodes) to show the broker nodes in the cluster. For more information, see Managing Brokers.

Managing Brokers

On the **Brokers** page, you can see an overview of all of your Worker nodes and drill down into a node for more information.

> The term *Brokers* refers to nodes running Kafka services (that is, Kubernetes worker nodes, but not master nodes).

Location: Clusters > *Cluster Name* > Brokers

To view the broker nodes in your cluster:

Click **Brokers** in the navigation bar. The **Brokers** page opens.

To see more information about a specific broker:

Click the broker's *Id* link. The *Broker Name* ID opens. For more information, see "Managing Brokers" on the previous page

Viewing Broker Details

You can view detailed information about a broker from the *Broker Name* details page.

Location: Clusters > *Cluster Name* > Brokers > *Broker Name*

To view information on a specific broker:

1. Click **Brokers** in the navigation bar.
2. Click the *Broker Name* link. The *Topic Name* page opens.

The following data is displayed.

Summary

In the **Summary** section, you can see an overview of your broker, including the number of topics and partitions located on it.

Metrics

In the **Metrics** section, you can view information about the data flow.

Messages count

In the **Messages** section, you can view a message view chart.

Per Topic Detail

In the **Per Topic Detail** section, you can view topic replication and partition information and drill down to view more information about each topic.

To see more information about a specific topic:

Click the *Topic Name* link in the **Per Topic Details** section. See Viewing Topic Details

Managing Topics

On the **Topics** page, you can run or generate partition assignments, add a new partition, and drill down into individual topics for more information.

To view the complete lists of Topics:

Click **Location: Clusters >Cluster Name> Topic> List**

Note: The following default topics are used internally by Transformation Hub and should not be deleted, modified, or used by external data producers or consumers.

```
__consumer_offsets
```

```
 _schemas
```

```
th-arcsight-json-datastore
```

```
th-arcsight-avro-sp_metrics
```

```
th-syslog
```

```
th-arcsight-avro
```

```
mf-event-avro-enriched
```

```
mf-event-avro-esmfiltered
```

```
mf-event-cef-esmfiltered
```

```
th-cef
```

To manage the topics in your cluster:

Click **Topic > List** in the navigation bar.

To view information on a topic:

Click the *Topic Name* link. The **Topic Name** page displays the topic's summary, metrics, consumers, operations and partitions. See Viewing Topic Details.

To generate partition assignments:

1. Click **Generate Partition Assignments**.
2. Select the topics and broker nodes to reassign.
3. Click **Generate Partition Assignments**.

To assign partitions as generated:

1. Click **Run Partition Assignments**.
2. Select the topics to reassign.

3. Click **Run Partition Assignments**.

To add a partition:

1. From the Topics Summary page, click **Add Partition**.
2. Enter the new number of partitions.
3. Select the topics and broker nodes.
4. Click **Add Partitions**.

Default Topics

> The CTH and Collectors were deprecated as of SmartConnector 8.4 release. The deployment of CTH and Collectors is now removed in SmartConnector CE 24.2 release. There will be limited support for customers already using CTH and Collectors, until the end of support date for the ArcSight SmartConnector CE 24.1 release, which is Jan 31, 2027.

Transformation Hub manages the distribution of events to topics, to which consumers can subscribe and receive events from.

Transformation Hub includes the following default topics:

Topic Name	Event Type	Producers For This Topic
mf-event-avro-esmfiltered	Filtered Avro events for consumption by ESM, Vertica, or Intelligence, depending on the enrichment scenario.	Transformation Hub, ESM
mf-event-cef-esmfiltered	Filtered CEF events for consumption by ESM.	SmartConnector, Connector in Transformation Hub (CTH).
mf-event-avro-enriched	Event data in Avro format that has been enriched by the Enrichment Stream Processors.	Transformation Hub
th-arcsight-avro	For ArcSight product use only. Event data in Avro format.	Transformation Hub, SmartConnector, Connector in Transformation Hub (CTH) or ESM
th-arcsight-avro-sp_metrics	For ArcSight product use only. Routing stream processor operational metrics data.	
th-arcsight-json-datastore	For ArcSight product use only. Transformation Hub dynamic configuration data.	
th-binary_esm	Binary security events, a format consumed by ArcSight ESM.	SmartConnector

Topic Name	Event Type	Producers For This Topic
th-cef	CEF event data.	SmartConnector, Connector in Transformation Hub (CTH).
th-cef-other	CEF event data destined for a non-ArcSight subscriber.	
th-syslog	The Connector in Transformation Hub (CTH) feature sends raw syslog data to this topic using a Collector.	Should only be configured as Collector or CTH destination.

In addition, using ArcSight Management Center, you can create new custom topics to which your SmartConnectors can connect and send events.

Topic Data Preservation

Topic data is preserved across Transformation Hub restarts, reinstalls, and upgrades.

- When a Transformation Hub reinstall is performed, all data in a Kafka topic is preserved. No data is lost.
- When the consumer resumes data collection from the topics, the consumer re-starts where it last left off. No data is lost.

Creating Topics

> This method of creating topics does not permit you to specify topic type. As a result, it is strongly recommended that you use ArcMC to create new topics in Transformation Hub.

You can create a new topic on the **Create Topic** page.

Location: Clusters > *Cluster Name***Topics > Create Topics**

To open the Add Topic page:

Click **Topic > Create** in the navigation bar.

To create a new topic:

1. Fill in values for the **Topic Name,** number of **Partitions**, and **Replication Factor** fields
2. Click **Create**.

For a discussion of field values, consult the Kafka documentation.

The number of custom topics you can create will be limited by Kafka, as well as performance and system resources needed to support the number of topics created.

Creating Routes for Topics

You can use ArcMC to view and create topics , as well as to create *routes*, which direct events into appropriate topics.

A *route* is a rule that directs Transformation Hub to duplicate events that meet certain criteria (filter) from a source topic to the route's destination topic. Rules are defined using event field names and expected values. Only CEF and Avro format events can be routed; binary security events in the `th-binary_esm` topic cannot be routed.

Using ArcMC, you can view, create, edit and delete routes based on CEF fields or Avro schema fields and event metadata. You must create destination topics before you can route events to them. For more information, see "Creating a Route" on page 929.

> As a general guideline, `th-arcsight-avro` is no longer a recommended source topic for Avro routing; use `mf-event-avro-enriched` instead.

Tuning the Retention Settings for Topics

Kafka topics occupy storage space on worker nodes where you apply the 'kafka:yes' label. To ensure that the nodes have enough storage space for each topic and other components that use storage on these nodes, you must tune the settings for topic retention. Please note that this procedure does not interrupt the flow of events through the system.

1. Log in to an ArcSight master node as root.
2. To determine the current topic retention storage size for a topic, select one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line and **replace {topic name} with the topic in question**.

   For FIPS (or non-FIPS) Encryption with Client Authentication:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=$STORES_
SECRET/" /etc/kafka/client.properties && \
sed -ir "s/^
[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --describe --topic
```

```
{topic name}  --command-config /etc/kafka/client.properties | grep
retention.bytes'
```

After executing the above, **Copy** and then paste the following command block:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=/"
/etc/kafka/client.properties'
```

For FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreProvider=BCFIPS " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreType=BCFKS " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --describe --topic
{topic name} --command-config /etc/kafka/client2.properties | grep
retention.bytes'
```

For non-FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --describe --topic
{topic name} --command-config /etc/kafka/client2.properties | grep
retention.bytes'
```

3. To set the retention size for a topic, select one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line, **replacing {topic name} with the topic in question, and {retention size in bytes} with the new retention size in bytes**.

For FIPS (or non-FIPS) Encryption with Client Authentication:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=$STORES_
SECRET/" /etc/kafka/client.properties && \
```

```
sed -ir "s/^
[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --alter --topic {topic
name} --add-config retention.bytes={retention size in bytes} --command-
config /etc/kafka/client.properties'
```

After executing the above, **Copy** and then paste the following command block:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=/"
/etc/kafka/client.properties'
```

For FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreProvider=BCFIPS " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreType=BCFKS " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --alter --topic {topic
name} --add-config retention.bytes={retention size in bytes} --command-
config /etc/kafka/client2.properties'
```

For non-FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
kafka-topics --bootstrap-server th-kafka-svc:9093 --alter --topic {topic
name} --add-config retention.bytes={retention size in bytes} --command-
config /etc/kafka/client2.properties'
```

Deleting a Topic

In order to delete a topic, you must first enable topic deletion.

Note: Topic deletion is no longer supported in Kafka Manager.

To enable topic deletion:

1. If it has not been defined previously, define the environment variable `arcsight_namespace` by running the following command:
   `export arcsight_namespace=$(kubectl get ns | grep "arcsight" | awk '{print $1}')`
2. Edit the Kafka stateful set by running the following command:
   `kubectl edit sts -n $arcsight_namespace th-kafka`
3. Add a new environment variable to the environment section after `SSL_CLIENT_AUTH_ENABLED` for the `th-kafka` container definition in the stateful set.
   - name: `KAFKA_DELETE_TOPIC_ENABLE`
   value: "true"
4. Save the *sts (stateful set)* configuration and exit. The Kafka pods will restart.

Topic deletion can also be enabled by overriding `KAFKA_DELETE_TOPIC_ENABLE=true` through Transform

To delete a topic:

1. Perform the deletion by selecting one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line, replacing {topic name} with the actual topic name before executing.

   For FIPS (or non-FIPS) Encryption with Client Authentication:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=$STORES_
SECRET/" /etc/kafka/client.properties && \
sed -ir "s/^
[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
kafka-topics --topic {topic name} --bootstrap-server th-kafka-svc:9093 --
delete --command-config /etc/kafka/client.properties'
```

   After executing the above, **Copy** and then paste the following command block:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=/"
/etc/kafka/client.properties && \
```

```
sed -ir "s/^[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=/"
/etc/kafka/client.properties'
```

For FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreProvider=BCFIPS " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreType=BCFKS " && \
kafka-topics --topic {topic name} --bootstrap-server th-kafka-svc:9093 --
delete --command-config /etc/kafka/client2.properties'
```

For non-FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}')
-- sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
kafka-topics --topic {topic name} --bootstrap-server th-kafka-svc:9093 --
delete --command-config /etc/kafka/client2.properties'
```

2. Verify deletion by selecting one of the following command blocks to use, depending on your security mode. Click **Copy** to copy the selected command block and then paste it into your command line.

For FIPS (or non-FIPS) Encryption with Client Authentication:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}') --
sh -c 'sed -ir "s/^
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=$STORES_
SECRET/" /etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=$STORES_SECRET/"
/etc/kafka/client.properties && \
kafka-topics --list --bootstrap-server th-kafka-svc:9093 --command-config
/etc/kafka/client.properties'
```

After executing the above, **Copy** and then paste the following command block:

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}') --
sh -c 'sed -ir "s/^
```

```
[#]*\s*ssl.truststore.password=.*/ssl.truststore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.keystore.password=.*/ssl.keystore.password=/"
/etc/kafka/client.properties && \
sed -ir "s/^[#]*\s*ssl.key.password=.*/ssl.key.password=/"
/etc/kafka/client.properties'
```

For FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}') --
sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreProvider=BCFIPS " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStoreType=BCFKS " && \
kafka-topics --list --bootstrap-server th-kafka-svc:9093 --command-config
/etc/kafka/client2.properties'
```

For non-FIPS Encryption Without Client Authentication

```
kubectl exec th-kafka-0 -n $(kubectl get ns|awk '/arcsight/ {print $1}') --
sh -c 'KAFKA_OPTS+=" -Djavax.net.ssl.trustStore=/etc/kafka/secrets/th-
kafka.truststore " && \
KAFKA_OPTS+="-Djavax.net.ssl.trustStorePassword=$STORES_SECRET " && \
kafka-topics --list --bootstrap-server th-kafka-svc:9093 --command-config
/etc/kafka/client2.properties'
```

Viewing Topic Details

You can see details about a topic, including information about the summary, metrics, consumers, and partitions from the *Topic Name* details page.

Location: Clusters > *Cluster Name* Topics > *Topic Name*

To view information on a specific topic:

1. Click **Topic > List** in the navigation bar.
2. Click the *Topic Name* link. The *Topic Name* page opens.

The following data is displayed.

Topic Summary

In the **Topic Summary** section, you view information on the topic's replicas, partitions, and broker nodes.

Metrics

In the **Metrics** section, you can view information about the data flow.

Operations

In the **Operations** section, you can perform a variety of tasks on broker nodes.

To reassign partitions:

Click **Reassign Partitions**.

To update a topic's configuration:

1. Click **Update Config**.
2. Edit the configuration fields.
3. Click **Update Config**.

To specify partition assignments:

1. Click **Manual Partition Assignment**.
2. Select the desired assignments.
3. Click **Save Partition Assignment**.

Partitions by Broker

In the **Partitions by Broker** section, you can see topic partition information and drill down to see details for each broker.

To view details on a broker:

Click the **Broker** link. The **Topic Summary** page displays information on the topic's lag, partitions, and consumer offset.

In Transformation Hub Kafka Manager, users will see different offset values between CEF (such as Logger) topics and binary (ESM) topics. In CEF topics, the offset value can generally be associated with number of events that passed through the topic. Each message in a CEF topic is an individual event. However, that same association cannot be made for the ESM topic, as several events are batched into each message.

Consumers consuming from this topic

In the **Consumers consuming from this topic** section, you can drill down to see details on each consumer.

> New consumers can take some time to display properly. Give the process time to populate the view with the correct data.

To view details on a consumer:

Click the *Topic Name* link. The Topic Summary page displays information on the topic's lag, partitions, and consumer offset.

Partition Information

In the **Partition Information** section, you can view information about the topic's partitions and drill down for more information about each leader.

To view details on a leader:

Click the **Leader** link. The *Broker Name* ID page displays the broker's summary, metrics, message count, and topic details. See Viewing Broker Details.

Data Redundancy and Topic Replication

When configuring a Transformation Hub, you can specify the number of copies (replicas) of each topic which Transformation Hub should distribute.

Kafka brokers automatically distribute each event in a topic to the number of broker nodes indicated by the topic replication level specified during the Transformation Hub configuration. While replication does decrease throughput slightly, ArcSight recommends that you configure a replication factor of at least 2.

You need at least one node for each replica. For example, a topic replication level of 5 requires at least five nodes; one replica would be stored on each node. The following table illustrates how the replication factor provides redundancy in case of unavailable nodes.

Replication Factor	Number of brokers receiving the event	If one node becomes unavailable...
1	1	Data is lost
2 (or more)	Same as replication factor	• Copies of the event data are still present on other node. • Data is restored to an unavailable node when it becomes available again. • No data is lost unless all nodes become unavailable simultaneously.

When you add new consumers, you don't need to update your producers. The distribution and replication is handled for you. Refer to the Kafka documentation for more information.

Filtering Events for ESM

Transformation Hub is capable of filtering and routing from a source topic of type event-avro to a destination topic of type event-avro. This capability can be used to filter events from a source topic such as `mf-event-avro-enriched` to a destination topic which ESM can consume from, such as `mf-event-avro-esmfiltered`. Both of these are default topics described here.

1. Use ArcSight Smart Connectors or any producer that supports sending Avro formatted events to send the events directly to an event-avro topic. Smart Connectors by default will send Avro formatted events to the `th-arcsight-avro` topic.
2. Filter the events using Transformation Hub's Avro routing rules using ArcMC 2.96 or later. Create a routing rule with an event-avro topic as source topic (such as `mf-event-avro-enriched`) and an event-avro topic as destination topic (such as `mf-event-avro-esmfiltered`). For more information, please refer to the **Routing** section in the ArcMC Administration Guide.

   > Earlier versions of Transformation Hub that did not yet support Avro routing rules required using a combination of CEF routing rules and CEF-to-Avro conversion. Using Avro routing rules is the recommended way to filter events for ESM.

   > As a general guideline, `th-arcsight-avro` is no longer a recommended source topic for Avro routing; use `mf-event-avro-enriched` instead. For more information, see About Routes.

Managing Consumers

On the **Consumers** page, you can see a list of consumers, view their type, the topics they consume, and drill down into each consumer and topic for more information.

Location: Clusters > *Cluster Name* > Consumers

- "Viewing the Consumers in Your Cluster" below
- "Viewing Details on a Specific Consumer" on the next page
- "Viewing Details on the Topic it Consumes" on the next page

Viewing the Consumers in Your Cluster

Click **Consumers** in the navigation bar.

Viewing Details on a Specific Consumer

Click the *Consumer Name* link. The *Consumer Name* page displays details about the consumer. You can drill down further for more information, including Consumed Topic Information (such as Partitions Covered % and Total Lag).

Viewing Details on the Topic it Consumes

Click the *Topic Name* link. The *Topic Name* page displays details about the topic. You can drill down further for more information including Consumer Lag, and Consumer Offset and LogSize data by Partition.

Managing Preferred Replicas

You can update the replicas for each cluster on the **Preferred Replica Election** page.

Location: Clusters > *Cluster Name* > Preferred Replica Election

- "Opening the Preferred Replica Election Page" below
- "Running the Preferred Replica Election for Your Topic" below

Opening the Preferred Replica Election Page

Click **Preferred Replica Election** in the navigation bar.

Running the Preferred Replica Election for Your Topic

Click **Run Preferred Replica Election**.

Managing Partitions

You can reassign partitions for your cluster on the **Reassign Partitions** page.

Location: Clusters > *Cluster Name* > Reassign Partitions

- "Opening Reassigned Partitions" below
- "Reassigning the Partitions" on the next page
- "Configuring Topic Partitions Based on Number of Consumers" on the next page

Opening Reassigned Partitions

To open the Reassign Partitions page, click **Reassign Partitions** in the navigation bar.

Reassigning the Partitions

To reassign the partitions for your topic, click **Reassign Partitions**.

Configuring Topic Partitions Based on Number of Consumers

You can scale the consumption rate for a consumer of a topic by adding more consumers to the consumer group. However, when adding new consumers to the consumer group, please consider the topic partition count of the topic you are consuming from. The following table shows the relationship between the number of consumers in a consumer group and data consumption from each partition.

Number of Consumers in Group is...	Consumption from Partitions
A single consumer	Consumer consumes from all partitions in the source topic.
Lower than partition count	Each consumer consumes from a subset of the topic partitions.
Equals partition count	Each consumer consumes from one topic partitions.
Exceeds partition count	Each consumer consumes from each of the topic partitions; additional consumers stay idle until new partitions are added to the source topic.

If you change the number of partitions in the source topic to match the consumer group size (same or a multiple) for a given consumer group consumption rate, or add additional consumers in the consumer to match the topic partition count, then the Transformation Hub will automatically re-balance the consumer groups.

Stream Processor Groups

Transformation Hub implements three types of stream processors to process events: routing stream processors, transforming stream processors, and enrichment stream processors.

- "Routing Stream Processors" on the next page
- "Transforming Stream Processors" on the next page
- Enrichment Stream Processors
- "Generate Verification Events for Parsed Field Integrity Checks (ArcSight Recon)" on page 693
- Local and Global ESM Event Enrichment
- "Describing Routing" on page 695
- "Tuning Stream Processor Groups" on page 695
- "Best Practices for Routing Stream Processors" on page 695

Routing Stream Processors

Event data is processed and sent to its destination by Routing stream processors, based on Transformation Hub routing rules specified in ArcSight Management Center. There are two types of routing stream processors:

- CEF-to-CEF routing stream processing is supported in Transformation Hub 3.7.0 and all previous versions.
- In Transformation Hub 3.4.0 and later versions, Avro-to-Avro routing stream processing occurs between two ArcSight Avro topics. To use an Avro topic, it should be of the type `ArcSight Avro`. You can configure a topic with this type in two ways:
    - Create the topic with type `ArcSight Avro` using ArcMC 2.9.6 or later and Transformation Hub 3.4.0 or later.
    - Change the type of an existing topic with no topic type to Arcsight Avro using ArcMC 2.9.6 or later.

> As a general guideline for routing stream processors, stream processor configurations and routes are refreshed every 60 seconds. Consider this factor when adding, deleting, or editing routing rules using ArcMC.

Transforming Stream Processors

From ArcSight SmartConnector 8.1 on, the SmartConnector is capable of sending events to Transformation Hub in the Avro event format from which they can be consumed by Avro formatted event consumers, such as ESM and Database. Earlier versions of the SmartConnector were not capable of this and, as such, would send CEF formatted events to Transformation Hub that then needed to be transformed to Avro format in order to be consumed by Avro formatted event consumers. The following default CEF to Avro or C2AV transforming stream processors work to transform CEF data in the CEF source topic and route it to the dedicated Avro destination topic for use by Avro consumers.

1. The CEF-to-Avro stream processor transforms events from the th-cef topic to the th-arcsight-avro topic.
2. The CEF-to-Avro ESM Filtered Stream Processor transforms events from the mf-event-cef-esmfiltered topic to the mf-event-avro-esmfiltered topic. For more information about filtering events for ESM, see "Filtering Events for ESM" on page 689.

Enrichment Stream Processors

Introduced in Transformation Hub 3.5.0, an enrichment stream processor processes events coming from the selected source topic (by default, `th-arcsight-avro`) by executing enrichment tasks , which include generating a Global ID. Events are then routed to the topic `mf-event-avro-enriched`.

> If you are enabling enrichment stream processors, ensure that the Generator ID Manager is enabled.

Use the OMT Management Portal to configure the following aspects of the enrichment stream processor.

Number of enrichment stream processor groups: By default, Transformation Hub has 1 enrichment stream processor group with 2 instances enabled.

Source topic: Choose one of the following source topics according to your deployment needs.

- `th-arcsight-avro:` (default source topic) Use this topic for local ESM event enrichment when ESM is deployed.
- `mf-event-avro-esmfiltered`: Use this topic for global ESM event enrichment when ESM is deployed.

For more information on local and global ESM event enrichment, see below.

Global Event ID Enrichment: Transformation Hub ensures that all the events that passes through the Enrichment Stream processor have a global ID. If the event's global ID value is missing, then a new global ID is assigned to it.

> Global Event ID generation enrichment is always enabled. You can also enable Event Integrity enrichment.

Generate Verification Events for Parsed Field Integrity Checks (ArcSight Recon)

ArcSight Recon can check the integrity of event data to provide assurance that event data sent by Connectors and other producers through the ingestion pipeline is not modified, and that events are not subsequently lost or deleted.

To achieve this objective, Transformation Hub provides *generate verification events for parsed field integrity checks* that publishes summary events (such as M1 or agent:040 Connectors events), about messages that pass through the enrichment source topic. Each summary event

will contain a calculated hash of data, a list of fields used to generate the hash, and list of the global event IDs of each message that is summarized.

Configuring Event Integrity Enrichment: For information about configuring this setting, see the Configuring Event Integrity Checks section.

For more information about verifying event data, see **Checking the Integrity of Event Data** in the User's Guide for ArcSight Platform 24.1.

Local and Global ESM Event Enrichment

ESM event enrichment can be configured locally or globally.

Local ESM Event Enrichment: With local ESM event enrichment (the default setting), ArcSight capabilities such as Recon and Intelligence can benefit from ESM Correlation. When local ESM event enrichment is configured:

- ESM reads the topic `mf-event-avro-esmfiltered`, enriches events found there, and stores them in ESM.
- ESM can be configured to send Correlation events to the `th-arcsight-avro` topic.
- Transformation Hub's Event Enrichment Stream Processor reads events from the `th-arcsight-avro` topic, enriches them, and sends them to `mf-event-avro-enriched` for Recon and Intelligence to read.

Global ESM Event Enrichment: With global event enrichment, events enriched by ESM are shared with all other ArcSight capabilities, including Recon and Intelligence. When global ESM event enrichment is configured:

- ESM reads the topic `th-arcsight-avro`, enriches events found there, and stores them in ESM.
- You must configure ESM to send all enriched events and Correlation events to the `mf-event-avro-esmfiltered` topic.
- Transformation Hub's Event Enrichment Stream Processor reads events from `mf-avro-esmfiltered`, enriches them, and sends them to `mf-event-avro-enriched` for Recon and Intelligence to read.

Configuring ESM Event Enrichment: For local ESM event enrichment, no configuration is needed by default for the enrichment processor. However, for this mode to work as intended, the user must do the following:

- Manually create a route from ArcMC that performs filtering and routing between `mf-event-avro-enriched` and `mf-event-avro-esmfiltered` topics. At a minimum, the filtering (besides any other desired rule) should exclude the ESM correlation events. Typically, you can do this by adding the rule type != 2.

- In the OMT Management Portal, manually enable a new routing stream processor group to pick up the newly-created route.

For global ESM event enrichment, in the OMT Management Portal, set the source topic for Enrichment Stream Processors to the `mf-event-avro-esmfiltered` topic.

Describing Routing

Each stream processor includes six processing threads. All routes with the same source topic are processed by one *routing stream processor group*. You can scale a processor group independently as load increases by adding more routing processor instances to the group.

You configure routing in ArcMC.

- The number of routing stream processor groups should match the number of source topics they are processing.
- Each routing stream processor group can contain multiple routing stream processors.
- You can configure up to 10 routing stream processor groups on Transformation Hub in the OMT Management Portal, allowing Transformation Hub to support up to 10 source topics.

Tuning Stream Processor Groups

The performance of stream processors is critical to Transformation Hub performance. In general, you can follow these guidelines for tuning stream processors and drive better performance.

- Since all routes which use the same source topic share the same routing stream processor group, adding more source topics can speed up processing.
- Increase the number of source topic partitions to handle high EPS throughput, depending on the CPU and memory resources of each worker node. For example, when the partition number is increased to 60, up to 10 routing (or C2AV) process instances can be used. Each stream processor uses 6 threads by default.
- Where possible, limit the number of routing rules per route.
- If stream processors display a `TimeoutException` in logs, consider overriding the application properties by slightly increasing the following settings, until the exceptions are no longer returned in logs:
  - `arcsight.th.sp.MAX_BLOCK_MS` (default is 60000 milliseconds)
  - `arcsight.th.sp.DELIVERY_TIMEOUT_MS`(default is 120000 milliseconds)

Best Practices for Routing Stream Processors

The following best practices apply to management of routing stream processors.

- By default, Transformation Hub has 1 routing stream processor group. Accordingly, if you create 2 or more routes with different source topics, then make sure to enable more stream processor groups according to the number of source topics used in such routes (this applies to both type of routings: CEF-to-CEF or Avro-to-Avro).
- To enable and increase the number of instances of routing stream processor groups, in the OMT Management Portal, browse to the **Reconfigure** page. Identify the desired group number; and to enable it, just increase it from 0 to the desired value.
- To support high availability, routing stream processor groups can scale out and down partially. Once a group is enabled, you can increase or decrease the number of instances. However, it might never be reduced to 0, or the source topic mapped to that service group will no longer route until you increase the number of instances above 0.
- Always consider the available resources when enabling more routing stream processor groups.
- C2AV and routing stream processing in Transformation Hub are Kafka Streams applications. By default, Kafka Streams are using at-least-once processing guarantees in the presence of failure. This means that if the stream processing application fails, no data records are lost or will fail to be processed, but some data records maybe re-read and therefore reprocessed. Therefore, C2AV and routing stream processing is using an at-least-once processing guarantees configuration. In this case, when C2AV/Routing pods are killed abnormally and restarted, the user might see duplicated events.

Stream Processor Deployment Guidelines

Effective stream processor (SP) deployment is based on workload and some other considerations. Each SP requires CPU and memory, so the more SPs are deployed, the more system resources are used.

- If no stream processors are needed, then none should be deployed, in order to conserve resources.
- Do not deploy more than one C2AV/Routing SP per node on small and medium nodes and no more than 3 C2AV/Routing SPs per node on large nodes, in co-located mode.

The table shows recommendations for deployment of SPs. These are recommendations and not requirements, but following the recommendations will avoid overloading a given system and still enable processing of the intended EPS:

Node type	EPS per Enrichment SP	Enrichment SP per worker node (Co-located)	Enrichment SP per worker node (Dedicated)	EPS per Routing SP	Routing SP per worker node (Co-located)	Routing SP per worker node (Dedicated)
Small (VM, 4 cores, 8cpus, 16G RAM)	Up to 10K	0	2	Up to 10K	0	2
Medium (VM, 8 cores, 16 vCPUs, 32G RAM)	Up to 35K	1	3	Up to 50K	1	3
Large (Appliance, 24 cores, 48 vCPUs, 188G RAM)	Up to 70K	4	4	Up to 90K	4	4

The EPS values shown on the table are based on the hardware mentioned on the **Node Type** column. Values shown here may vary depending on the actual performance of the VM/appliance, and the EPS performance of the stream processors may vary.

- On small nodes, we recommend deploying the enrichment SP and routing SP on dedicated nodes, as deploying them in a co-located fashion affects the overall EPS IN capacity of a small cluster.
- On medium nodes, avoid putting more than 1 enrichment SP in the same node. This will depend on how much EPS each enrichment SP has to process. The more EPS, the more CPU consumption there will be.
  - If using the default 2 enrichment SPs, they will be automatically assigned to different nodes.
  - If another SP instance is needed, then assign it to another node where no enrichment nor Routing SP is running.
- On medium nodes, the number of routing SPs deployed in a node follows the same logic as the enrichment SP mentioned above. There is a slight difference when it comes to performance. The more a routing SP needs to filter events, the more CPU consumption there will be. You may find a situation where a routing SP processing less than 1K might use more CPU than a routing SP processing 10K. This will depend on the size of the events, structure of the rule expressions, the number of field tests in rules, and system load of the cluster, among other factors that might affect the overall performance of the routing SP instances.
- On medium nodes, if another enrichment SP/routing SP instance needs to be deployed on a co-located node, then make sure the target node is not running another enrichment SP/routing SP. You can ignore this recommendation for the enrichment SP, but only if the already running enrichment SP is processing less than 10K. Otherwise, just stick to 1 enrichment SP/Routing SP per co-located node.

Dedicated nodes (not running Kafka, Zookeeper or Core) enable deploying more enrichment SP and Routing SP instances.

Overriding Application Properties

Each Transformation Hub module (Kafka, Zookeeper, and so on) has many additional properties available, and a system administrator might be required to override the default values for some of these properties. This section covers how to override these property values.

Property values (for properties that support overrides) are set by injecting environment variables in the respective container's start-up environment. These variables are read from a user-supplied properties file, in a specific location on the Network File Server (NFS). To see the available properties for override, consult the respective module's published documentation.

Note that in most cases, this feature is not required for normal operation of Transformation Hub, and most likely will be used at the direction of technical support. Not all properties support overrides; please check with technical support before making any changes to your configuration.

- For Kafka, ZooKeeper, and Schema Registry properties, consult the appropriate Confluent documentation.
- The properties for routing processor, stream processor and web service modules are detailed below.

> **Note**: Legacy properties suffixed with `arcsight.eventbroker` will continue to function as they did in previous versions, but as explained below, newly added properties must be suffixed with `arcsight.th`. If two properties of the same name are set with different suffixes, the property with `arcsight.th` will supersede the other one.

- "Routing Processor and Stream Processor Properties" below
- "Web Service Properties" on page 700
- "Configuring the Values" on page 700
- "Changing Value Examples" on page 700

Routing Processor and Stream Processor Properties

As explained in "Configuring the Values" on page 700, prefix these properties with `arcsight.th.sp.` to create an override.

Property Name	Default Value	Description
RETRIES	2147483647	The number of retries for broker requests that return a retry-able error.
RETRY_ BACKOFF_MS	100	The amount of time (milliseconds), before a request is retried. This applies if the retries parameter is configured to be greater than 0.
RECEIVE_ BUFFER_BYTES	65536	The size of the TCP receive buffer to use when reading data. If the value is -1, the OS default will be used.
MAX_ PARTITION_ FETCH_BYTES	1048576	The maximum amount of data per-partition the server will return. Records are fetched in batches by the consumer.
MAX_REQUEST_ SIZE	1048576	The maximum size of a request in bytes.
BUFFER_MEMORY	33554432	The total bytes of memory the producer can use to buffer records waiting to be sent to the server.
BATCH_SIZE	16384	The default batch size in bytes when batching multiple records sent to a partition
LINGER_MS	100	The producer will wait for up to the given delay to allow other records to be sent so that the sends can be batched together
HEARTBEAT_ INTERVAL_MS	1000	The expected time (milliseconds) between heartbeats to the consumer coordinator when using Kafka's group management facilities. Heartbeats are used to ensure that the consumer's session stays active and to facilitate rebalancing when new consumers join or leave the group.
MAX_POLL_ INTERVAL_MS	3600000	The maximum delay (milliseconds) between invocations of poll() when using consumer group management
MAX_POLL_ RECORDS	100	The maximum number of records returned in a single call to poll().
SESSION_ TIMEOUT_MS	180000	The timeout (milliseconds) used to detect client failures when using Kafka's group management facility
REQUEST_ TIMEOUT_MS	305000	The configuration controls the maximum amount of time (milliseconds) the client will wait for the response of a request.
CONNECTIONS_ MAX_IDLE_MS	540000	The maximum amount of time (milliseconds) before idle connections are closed.
TH_NUM_ THREADS	6	The number of threads to execute stream processing.
MAX_BLOCK_MS	60000 (milliseconds)	Controls how long the KafkaProducer's send(), partitionsFor(), initTransactions (), sendOffsetsToTransaction(), commitTransaction() and abortTransaction() methods will block.
DELIVERY_ TIMEOUT_MS	120000 (milliseconds)	An upper bound on the time to report success or failure after a call to send() returns. This limits the total time that a record will be delayed prior to sending, the time to await acknowledgement from the broker (if expected), and the time allowed for retriable send failures.

Web Service Properties

As explained in "Configuring the Values" below, prefix the names of these properties with `arcsight.th.web-service.` to create an override.

Property Name	Default Value	Description
`WS_AUTH_ARCMC_CONNECTION_TIMEOUT`	30000	The amount of time (milliseconds) before a request to connect to ArcMC is retried due to ArcMC timeout.
`WS_AUTH_ARCMC_CONNECTION_NUM_RETRIES`	2	The number of times that TH retries to connect ArcMC due to ArcMC timeout.

Configuring the Values

1. Create a file named `arcsight-env-override.properties` under the folder `<NFS_root_DIRECTORY>/transformationhub/config`.

   The `<NFS_root_DIRECTORY>` path is described in this guide as the NFS root folder (usually `/opt/arcsight/nfs/volumes`). For more information, refer to the section Creating the NFS Shares.

2. Add properties to the file. To each property, add the module prefix from the table below.

Module	Prefix
Kafka	`arcsight.th.kafka.`
Schema Registry	`arcsight.th.schema-registry.`
ZooKeeper	`arcsight.th.zookeeper.`
Routing/C2AV/Enrichment Processor	`arcsight.th.sp.`
Web Services	`arcsight.th.web-service.`

3. Delete the pods for which properties were defined, or, alternatively, redeploy Transformation Hub.
4. To verify the changes, search the log file (after the container's status is back to Running) for matching properties.

Changing Value Examples

To change the value of `ZOOKEEPER_MAX_CLIENT_CNXNS` to 65, in ZooKeeper, and to change the value of `SCHEMA_REGISTRY_KAFKASTORE_TIMEOUT_MS` in the Schema Registry, create a file, `<NFS Volume mount>/transformationhub/config/arcsight-env-override.properties`, and add the following lines:

```
arcsight.th.zookeeper.ZOOKEEPER_MAX_CLIENT_CNXNS=65
```

```
arcsight.th.schema-registry.SCHEMA_REGISTRY_KAFKASTORE_TIMEOUT_MS=20000
```

Example of verifying the change by searching the log:

```
kubectl -n transformationhub1 logs th-zookeeper-0 | grep ZOOKEEPER_MAX_CLIENT_
CNXNS
Environment override script set: ZOOKEEPER_MAX_CLIENT_CNXNS=65
ZOOKEEPER_MAX_CLIENT_CNXNS=65
```

Transformation Hub Liveness Probes

A *liveness probe* is a Kubernetes feature that can be configured to detect problematic pods. Once detected, Kubernetes will take action to restart a problematic pod. Liveness probes help ensure higher availability of pods as well as a more robust cluster environment. Consult the Kubernetes documentation for a more detailed explanation of liveness probes. Transformation Hub supports these liveness probe types:

- TCP/IP port-socket connection
- HTTP request
- Log scanning

Each container or pod supports the listed liveness probes, with their default parameter values shown.

Container/Pod	Probe	initialDelaySeconds	periodSeconds	timeoutSeconds	failureThreshold
Kafka	tcp socket :9093 and log scanning	240	60	30	3
Zookeeper	tcp socket :2182 and log scanning	240	60	30	3
Web Service	https GET :8080 and log scanning	240	300	30	3
Schema Registry	https GET :8081 config and log scanning	240	300	30	3
Kafka Manager	https GET :9000 and log scanning	240	600	30	3
Routing/Enrichment Processor	log scanning	240	60	30	3
C2AV (CEF-to-Avro) Processor	log scanning	240	60	30	3

Probe parameters are defined as follows:

Parameter	Definition
`initialDelaySeconds`	Number of seconds after the container has started before liveness probes are initiated. The first probe execution after startup is not until initialDelaySeconds + periodSeconds.
`periodSeconds`	How often to perform the probe.
`timeoutSeconds`	Number of seconds after which the probe times out.
`failureThreshold`	When a Pod starts and the probe fails, Kubernetes will try failureThreshold times before giving up and restarting the pod.

Managing Liveness Probes

To check if a pod has a liveness probe configured:

1. Run:
   `kubectl -n <namespace> describe pod <podname>`
2. Review the output. Look (or `grep`) for the line starting with the string `Liveness...`This will show some of the probe's configuration.

To check for probe failures:

1. Run:
   `kubectl get pods --all-namespaces`
2. If any pod shows 1 or more restarts, run:
   `kubectl -n <namespace> describe pod <podname>`
3. Review any list of events at the end of the output. Liveness probe failures will be shown here.

Configuring Liveness Probes

The default values for liveness probes can be overriden by changing the values of the appropriate properties on the Configuration page.

1. Log in to the OMT Management Portal.
2. Click **DEPLOYMENT > Deployments**.
3. Click the **...** (Browse) icon to the right of the main window.
4. From the drop-down, click **Reconfigure**. The post-deployment settings page is displayed.
5. Browse the configuration properties list to find the desired property, and specify the new value.
5. Click **Save**.

Configuring Log Scanning Liveness Probes

Log scanning probes scan the application's output for a match to a configured pattern, such as a known error message. If the pattern is found, the pod is restarted.

In addition to the four parameters described in the table above, log scanning probes have two additional properties:

literal	A literal expression for matching against the application's log output.
regex	A regular expression for matching against the application's log output.

- The *literal* property specifies a literal (exact match) search string. If the value matches a portion of the log text, the liveness probe, on its next periodic check, will report a failure and restart the pod.
- The *regex* property is similar, except that a regular expression can be specified for the match. This regex must conform to Java regex rules. To specify a regex escape value within the regex, use 2 backslashes to escape it (`\\`).
- Multiple search patterns can be specified per property, separated by 4 vertical bars (`||||`). A match on any of the patterns will trigger the probe failure.
- There are no default values for these parameters. Log scanning is disabled in the default configuration.
- Matching across multiple rows is not supported. The match must occur on one log line.
- For example, to restart the CEF-to-Avro Routing Stream Processor pod when the value, `Setting stream threads to d` (where `d` could be any single digit), is found in the log, change the configuration property "CEF-to-Avro Routing Stream Processor liveness probes regular expression" to the following value .

```
  Setting stream threads to \\d
```

Verification

To verify that log scanning is configured as intended, review the pod's log and look for entries containing `InputStreamScanner`.

For example, to view the c2av-processor pod log, run:

```
kubectl -n <namespace> logs th-c2av-processor-0 | more
```

For the previous property example, the corresponding log line would be:

```
InputStreamScanner: Will scan for RegEx pattern [Setting stream threads to
\d]
```

Migrating the NFS Server to a New Location

The process given here explains how to migrate your NFS server and paths to another location (including changing paths within the same NFS server). During the move, some of the exported path pods from the core namespace will incur downtime as they are scaled to zero or temporarily removed. The OMT Management Portal (and all of its features) will not be available during such downtime.

Data will be copied before being transferred, so that the original location should remain as a backup until the procedure is complete and the cluster successfully back to operation, with pods restarted with new paths and the new NFS server.

This procedure will be executed on your primary master node, with access to the`kubectl` command and the contents of `/opt/arcsight/kubernetes`.

The procedures uses the `volume_admin.sh` script located in `/opt/arcsight/kubernetes/scripts`

Usage:

```
./volume_admin.sh <Operation> <Persistent Volume> <Options>
```

Where the options include:

- `reconfigure`: Reconfigures a persistent volume
- `search`: Finds persistent volume consumers
- `down`: Scales down resources using a persistent volume
- `up`: Scales up resources using a persistent volume by reverting the “down” command inner operations.

> The `up` command requires the `down` command to have been executed beforehand, which generates the necessary information for the resources scale up (such as numbers of replicas, yaml definitions)

Using the `volume_admin.sh` script for a migration is recommended, as it speeds up the process and makes it less vulnerable to user errors.

> Do not use `volume_admin.sh` to scale resources up or down for `PV arcsight-installer-xxxxx-arcsight-volume`

Use the following steps to migrate a `PV` using `volume_admin.sh`:

1. Display a list of the PV consumers:

```
./volume_admin.sh search pv_name
```

2. Scale down or delete the resources consuming the PV:

```
./volume_admin.sh down pv_name
```

3. Ensure all consumers are removed from the PV users list (as compared to the list from step 1):

```
./volume_admin.sh search pv_name
```

4. Copy the data of the concerned volume from the old NFS/path to the new one.
5. Compare both volumes for any permissions discrepancies. The output of the following command should be identical for both:

```
ls -l pv_name
```

6. To authorize the PV change:

```
./volume_admin.sh reconfigure pv_name -t nfs -s <new_nfs_FQDN_or_IP> -p
/<new_nfs_path>/pv_name
```

7. Verify the PV change:

```
kubectl get pv pv_name -o yaml
```

8. Scale up or recreate resources consuming the PV:

```
./volume_admin.sh up pv_name
```

9. Verify that all resources have been restored (as compared to the list from step 1):

```
./volume_admin.sh search pv_name
```

10. Verify that all pods are up again:

```
kubectl get pods -A
```

11. Check the OMT status:

```
/opt/arcsight/kubernetes/bin/kube-status.sh
```

Preparation

1. Verify that all pods are running correctly with the following command:

```
kubectl get pods --all-namespaces -o wide | awk -F " *|/" '($3!=$4 ||
$5!="Running") && $5!="Completed" {print $0}'
```

2. Verify status of OMT installation with the following command:

```
/opt/arcsight/kubernetes/bin/kube-status.sh
```

3. Prepare the new NFS volumes with the same permission set as the existing volumes.
   - If you are using a software-controlled NFS, make sure the export policy is configured in the correct order. For example, for `NetApp NFS`, the `RO/RW` Access rules are None, Superuser Security types are None, User ID to which anonymous users are mapped equals 1999 (or whatever value you used during initial install).
   - For using `NFSv4` and later versions, make sure ID mapping (configured in (`/etc/idmapd.conf`) on both the NFS server and all NFS clients (that is, your cluster nodes) uses the same domain.
   - Verify that `UID/GID` is correct by manually mounting new NFS mount points and touching a file. Permission should be the same as for touching the file on the old NFS mount points.
   - Note that for any changes on the NFS Server to take effect, all mount points still pending mounting should be closed.
4. Get an overview of persistent volumes for your installation with the following command:

```
kubectl get pv
```

Migration Procedures

The recommended order in which migration should be executed on your persistent volumes is as follows:

1. `arcsight-installer-xxxxx-arcsight-volume`
2. `db-single`
3. `itom-logging`
4. `itom-monitor`
5. `itom-vol`

In any of the following commands, `<old_nfs_mount>` and `<new_nfs_mount>` refer to manually-mounted NFS for copying or maintenance procedures, and `<new_nfs_path>` refers to the real path on the NFS server of the mount point for the PV change command.

> If any PV change fails, roll back any changes to the old NFS location until the issue is resolved. **Do not leave your cluster in a change-pending state.**

This section contains the following topics:

Migrate `itom-logging` PV

We describe both a manual approach and a more automated one using the `volume_admin.sh` script.

Manual approach

1. Determine the services using the `itom-logging` PV by running the following command. Note down the number of replicas running, to scale back after the NFS migration:

   ```
   /opt/arcsight/kubernetes/scripts/volume_admin.sh search itom-logging
   ```

   Example output:

   ```
   Namespace    Kind          Name
   core         DaemonSet     itom-fluentbit-infra
   core         Deployment    itom-idm
   core         Deployment    itom-logrotate-deployment
   core         Deployment    itom-pg-backup
   core         Deployment    itom-prometheus-grafana
   ```

2. Scale down other services by running these commands:

   ```
   kubectl scale --replicas=0 -n core deployment/itom-idm
   kubectl scale --replicas=0 -n core deployment/itom-logrotate-deployment
   kubectl scale --replicas=0 -n core deployment/itom-pg-backup
   kubectl scale --replicas=0 -n core deployment/itom-prometheus-grafana
   ```

> **Note:** For `itom-fluentbit-infra`, save its `yaml` definition temporarily to be able to delete the `daemonset`:
>
> ```
> kubectl get ds itom-fluentbit-infra -n core -o yaml > itom-fluentbit-infra.yaml
> ```
>
> And recreate it after you authorize the PV change to the new NFS server/path:
>
> ```
> kubectl delete ds itom-fluentbit-infra -n core
> ```

3. Verify all pods of interest are deleted by running this command:

   ```
   /opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
   awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
   ```

4. Verify that consumers have been removed from the PV users list:

   ```
   /opt/arcsight/kubernetes/scripts/volume_admin.sh search itom-logging
   ```

5. Copy the NFS data to the new mount point:

   ```
   cp -rfp /<old_nfs_mount>/itom-logging-vol /<new_nfs_ mount>/itom-logging-
   vol
   ```

   Or to copy to a new server:

   ```
   rsync -az --progress --rsync-path="sudo rsync" /<old_nfs_mount>/itom-
   logging-vol/ user@<new_nfs_FQDN_or_IP >:/<new_nfs_mount>/itom-logging-
   vol/
   ```

6. Check the content of the mount for any permissions discrepancies. The output of these commands must be identical:

   ```
   ls -l /<old_nfs_mount>/itom-logging-vol
   ```

   ```
   ls -l /<new_nfs_mount>/itom-logging-vol
   ```

7. Authorize the PV change by running this command:

   ```
   /opt/arcsight/kubernetes/scripts/volume_admin.sh reconfigure itom-logging
   -t nfs -s <new_nfs_FQDN_or_IP> -p /<new_nfs_path>/itom-logging-vol
   ```

8. Verify the new NFS path in the configuration by running the following command:

   ```
   kubectl get pv itom-logging -o yaml
   ```

9. For the previous command, locate the `nfs:` section of the output. It should list the new server and volume.

10. Repeat all the commands you used to scale down or destroy the pods, to scale up all replicas or start up the related `daemonsets`.
11. Recreate the `daemonset` from the `YAML` with these commands.

    Note that this will still be the old path until `itom_volPV` is migrated

    ```
    kubectl apply -f itom-fluentbit-infra.yaml
    kubectl scale --replicas=<value> -n core deployment/itom-idm
    kubectl scale --replicas=<value> -n core deployment/itom-logrotate-
    deployment
    kubectl scale --replicas=<value> -n core deployment/itom-pg-backup
    kubectl scale --replicas=<value> -n core deployment/itom-prometheus-
    grafana
    ```

12. Verify that the consumers have been restored with this command:

    ```
    /opt/arcsight/kubernetes/scripts/volume_admin.sh search itom-logging
    ```

13. Verify that all the pods are running:

    ```
    /opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
    awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
    ```

14. If all pods are running, verify the OMT status:

    ```
    /opt/arcsight/kubernetes/bin/kube-status.sh
    ```

Automated approach

To migrate `itom-logging` PV using the `volume_admin.sh` script, run the following commands in this set order:

For a description of what each command does see the "Usage:" on page 704 section

1. Determine the services using the `itom-loggingPV` by running the following command:

   ```
   /opt/arcsight/kubernetes/scripts/volume_admin.sh search itom-logging
   ```

2. Scale down other services by running this command:

   ```
   /opt/arcsight/kubernetes/scripts/volume_admin.sh down itom-logging
   ```

3. Verify that consumers have been removed:

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh search itom-logging
```

4. Copy the NFS data to the new mount point:

```
cp -rfp /<old_nfs_mount>/itom-logging-vol/<new_nfs_ mount>/itom-logging-
vol
```

Or, if copying to a new server:

```
rsync -az --progress --rsync-path="sudo rsync" /<old_nfs_mount>/itom-
logging-vol/ user@<new_nfs_FQDN_or_IP >:/<new_nfs_mount>/itom-logging-
vol/
```

5. Compare both volumes for any permissions discrepancies.

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh reconfigure itom-logging
-t nfs -s <new_nfs_FQDN_or_IP> -p /<new_nfs_path>/itom-logging-vol
```

6. Check the PV change:

```
kubectl get pv itom-logging -o yaml
```

7. Scale back up:

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh up itom-logging
```

8. Verify that consumers have been restored with this command:

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh search itom-logging
```

9. Verify that all pods are up again:

```
kubectl get pods -A
```

10. If all pods are running, verify the OMT status:

```
/opt/arcsight/kubernetes/bin/kube-status.sh
```

Migrate `itom-monitor` PV

1. Determine the services using the `itom-monitor PV` by running the following command. Note down the number of replicas running, to scale back after the NFS migration:

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh search itom-monitor
```

Example output:

```
Namespace    Kind           Name
core         StatefulSet    prometheus-itom-prometheus-prometheus
```

2. Scale down deployments with these commands. Make sure you have noted down the original number of replicas for each deployment.

```
kubectl scale --replicas=0 -n core statefulset/prometheus-itom-
prometheus-prometheus
```

3. Verify if all Pods are deleted and not in terminating state by running this command:

```
/opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
```

4. Then, make sure that the PV consumers list is returned empty:

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh search itom-monitor
```

5. Copy the NFS data to a new mount point:

```
cp -rfp /<old_nfs_mount>/itom-monitor-vol /<new_nfs_mount>/itom-monitor-
vol
```

Or to copy to a new server:

```
rsync -az --progress /<old_nfs_mount>/itom-monitor-vol/ user@<new_nfs_
FQDN_or_IP >:/<new_nfs_mount>/itom-monitor-vol/
```

6. Check the mount content for any permissions discrepancies. The output of these commands must be identical:

```
ls -l /<old_nfs_mount>/itom-monitor-vol
```

```
ls -l /<new_nfs_mount>/itom-monitor-vol
```

7. Authorize the PV change:

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh reconfigure itom-monitor
-t nfs -s <new_nfs_FQDN_or_IP> -p /<new_nfs_path>/itom-monitor-vol
```

8. Repeat all the commands you used to scale down or destroy the pods to scale all replicas up, or start up the related `daemonsets`.

```
kubectl scale --replicas=<value> -n core statefulset/prometheus-itom-
prometheus-prometheus
```

To perform this process using `volume_admin.sh`, the steps are identical to the migration of `itom-logging PV`. Replace `itom-logging` and `itom-logging-vol` with `itom-monitor` and `itom-monitor-vol` in each commands.

Migrate `itom-vol` PV

1. Determine the services using the `itom-vol PV` by running the following command. Note down the number of replicas running, to scale back after the NFS migration:

   ```
   /opt/arcsight/kubernetes/scripts/volume_admin.sh search itom-vol
   ```

   Example output:

   ```
   Namespace    Kind          Name
   core         Deployment    apphub-apiserver
   core         Deployment    cdf-apiserver
   core         Deployment    cdfapiserver-postgresql
   core         Deployment    itom-cloudserver
   core         Deployment    itom-frontend-ui
   core         Deployment    itom-idm
   core         Deployment    itom-mng-portal
   core         Deployment    itom-pg-backup
   core         Deployment    itom-vault
   core         Deployment    kube-registry
   core         Deployment    suite-conf-pod-arcsight-installer
   ```

2. Scale down deployments with these commands. Make sure you have noted down the original number of replicas for each deployment.

   ```
   kubectl scale --replicas=0 -n core deployment/cdf-apiserver
   kubectl scale --replicas=0 -n core deployment/itom-idm
   kubectl scale --replicas=0 -n core deployment/itom-vault
   kubectl scale --replicas=0 -n core deployment/itom-mng-portal
   kubectl scale --replicas=0 -n core deployment/kube-registry
   kubectl scale --replicas=0 -n core deployment/suite-conf-pod-arcsight-
   installer
   kubectl scale --replicas=0 -n core deployment/apphub-apiserver
   kubectl scale --replicas=0 -n core deployment/cdfapiserver-postgresql
   kubectl scale --replicas=0 -n core deployment/itom-cloudserver
   kubectl scale --replicas=0 -n core deployment/itom-frontend-ui
   kubectl scale --replicas=0 -n core deployment/itom-pg-backup
   ```

> **Note:** Any consumer jobs displayed during the listing are just temporary one-time actions and can be deleted with:
>
> ```
> kubectl delete pod -n core <job_name>
> ```

3. Verify if all Pods are deleted and not in terminating state by running this command:

```
/opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
```

4. Then, make sure that the PV consumers list is returned empty:

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh search itom-vol
```

5. Copy the NFS data to a new mount point:

```
cp -rfp /<old_nfs_mount>/itom_vol /<new_nfs_mount>/itom_vol
```

Or to copy to a new server:

```
rsync -az --progress /<old_nfs_mount>/itom-vol/ user@<new_nfs_FQDN_or_IP
>:/<new_nfs_mount>/itom-vol/
```

6. Check the mount content for any permissions discrepancies. The output of these commands must be identical:

```
ls -l /<old_nfs_mount>/itom-vol
```

```
ls -l /<new_nfs_mount>/itom-vol
```

7. Authorize the PV change:

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh reconfigure itom-vol -t
nfs -s <new_nfs_FQDN_or_IP> -p /<new_nfs_path>/itom_vol
```

8. Repeat all the commands you used to scale down or destroy the pods, to scale up all replicas or start up the related `daemonsets`.

```
#kubectl scale --replicas=<value> -n core deployment/cdf-apiserver
```

```
kubectl scale --replicas=<value> -n core deployment/itom-idm
```

```
kubectl scale --replicas=0 -n core deployment/cdf-apiserver
kubectl scale --replicas=0 -n core deployment/itom-idm
kubectl scale --replicas=0 -n core deployment/itom-vault
kubectl scale --replicas=0 -n core deployment/itom-mng-portal
```

```
kubectl scale --replicas=0 -n core deployment/kube-registry
kubectl scale --replicas=0 -n core deployment/suite-conf-pod-arcsight-
installer
```

```
kubectl scale --replicas=<value> -n core deployment/apphub-apiserver
```

```
kubectl scale --replicas=<value> -n core deployment/cdfapiserver-
postgresql
```

```
kubectl scale --replicas=<value> -n core deployment/itom-cloudserver
```

```
kubectl scale --replicas=<value> -n core deployment/itom-frontend-ui
```

```
kubectl scale --replicas=<value> -n core deployment/itom-pg-backup
```

9. To restore the path services, use this command:

```
kubectl create -f <PATH>
```

10. Verify that the consumers have been restored with this command:

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh search itom-vol
```

11. Verify that all the pods are running:

```
/opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
```

12. If all pods are running, verify the OMT status:

```
/opt/arcsight/kubernetes/bin/kube-status.sh
```

To perform this process using `volume_admin.sh`, the steps are identical to the migration of `itom-logging PV`. Replace `itom-logging` and `itom-logging-vol` with `itom-vol` and `itom-vol` in each commands.

Migrate `db-single PV`

1. Determine the services using the `db-single PV` by running the following command. Note down the number of replicas running, to scale back after the NFS migration:

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh search db-single
```

Example output:

```
Namespace    Kind          Name
core         Deployment    itom-postgresql
```

2. Scale down the necessary deployments:

```
kubectl scale --replicas=0 -n core deployment/itom-postgresql-default
```

3. Verify pods are not stuck in terminating state, and that afterwards no consumers are displayed:

```
/opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
```

```
#/opt/arcsight/kubernetes/scripts/volume_admin.sh search db-single
```

4. Copy the NFS data to a new mount point:

```
cp -rfp /<old_nfs_mount>/db-single-vol /<new_nfs_mount>/db-single-vol
```

Or to copy to a new server:

```
rsync -az --progress /<old_nfs_mount>/db-single-vol/ user@<new_nfs_FQDN_
or_IP >:/<new_nfs_mount>/db-single-vol/
```

5. Check the mount content for any permissions discrepancies. The output of these commands must be identical:

```
ls -l /<old_nfs_mount>/db-single-vol
```

```
ls -l /<new_nfs_mount>/db-single-vol
```

6. Authorize the PV change by running this command:

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh reconfigure db-single  -
t nfs -s <new_nfs_FQDN_or_IP> -p /<new_nfs_path>/itom/db
```

7. Repeat all the commands you used to scale down or destroy the pods, to scale up all replicas.
8. Verify that the consumers have been restored with this command:

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh search db-single
```

9. Verify that all the pods are running:

```
/opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
```

10. If all pods are running, verify the OMT status:

```
/opt/arcsight/kubernetes/bin/kube-status.sh
```

> To perform this process using `volume_admin.sh`, the steps are identical to the migration of `itom-logging PV`. Replace `itom-logging` and `itom-logging-vol` with `db-single` and `db-single-vol` in each commands.

Migrate `arcsight-installer-xxxxx-arcsight-volume PV`

1. Determine the services using the `arcsight-installer-xxxxx-arcsight-volume PV` by running the following command. Note down the number of replicas running, to scaleback after the NFS migration:

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh search arcsight-
installer-xxxxx-arcsight-volume
```

2. Scale down the necessary deployments with the following commands, **in the listed order**. Your list may vary depending on your `Transformation Hub` configuration.

> Note that between each scale down command, you will run a `get pods` command as shown to make sure the scale down has finished successfully, before proceeding to the next consumer.

```
kubectl scale --replicas=0 -n arcsight-installer-xxxxx deployment/th-
kafka-manager
/opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
```

```
kubectl scale --replicas=0 -n arcsight-installer-xxxxx deployment/th-
schemaregistry
/opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
```

```
kubectl scale --replicas=0 -n arcsight-installer-xxxxx deployment/th-web-
service
/opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
```

```
kubectl scale --replicas=0 -n arcsight-installer-xxxxx sts/th-routing-
processor-group1
/opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
```

```
kubectl scale --replicas=0 -n arcsight-installer-xxxxx
deployment/autopass-lm
/opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
```

Note: Scaling down can take some time. Please be patient, as this is normal behavior.

3. Run these commands in the listed order:

```
kubectl scale --replicas=0 -n arcsight-installer-xxxxx sts/th-kafka
/opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
#kubectl scale --replicas=0 -n arcsight-installer-xxxxx sts/th-zookeeper
/opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
```

4. Verify that no consumers are displayed for the PV by running the following command:

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh search arcsight-
installer-xxxxx-arcsight-volume
```

5. Copy the NFS data to a new mount point:

```
cp -rfp /<old_nfs_mount>/arcsight-volume /<new_nfs_mount>/ arcsight-
volume
```

Or to copy to a new server:

```
rsync -az --progress /<old_nfs_mount>/arcsight-volume/ user@<new_nfs_
FQDN_or_IP >:/<new_nfs_mount>/arcsight-volume/
```

6. Check the mount content for any permissions discrepancies. The output of these commands must be identical:

```
ls -l /<old_nfs_mount>/arcsight-volume
```

```
ls -l /<new_nfs_mount>/arcsight-volume
```

7. Authorize the PV change:

```
/opt/arcsight/kubernetes/scripts/volume_admin.sh reconfigure arcsight-
installer-xxxxx-arcsight-volume -t nfs -s <new_nfs_FQDN_or_IP> -p /<new_
nfs_path>/arcsight-volume
```

8. Verify that the new server and volume are listed under the `nfs:` section in the configuration:

```
kubectl get pv arcsight-installer-xxxxx-arcsight-volume -o yaml
```

9. Run the scale up commands in the order shown. After each scale up, you will run the `get pods` command as shown to make sure nothing is in the crashing state:

```
kubectl scale --replicas=<value> -n arcsight-installer-xxxxx
deployment/autopass-lm
/opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
kubectl scale --replicas=<value> -n arcsight-installer-xxxxx sts/th-
zookeeper
#/opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
kubectl scale --replicas=<value> -n arcsight-installer-xxxxx sts/th-kafka
/opt/arcsight/kubernetes/bin/kubectl get pods --all-namespaces -o wide |
awk -F " *|/" '($3!=$4 || $5!="Running") && $5!="Completed" {print $0}'
```

10. When all `th-zookeeper` and `th-kafka` nodes are in the running state, run these commands to scale up the rest of the PV consumers.

> Note that this list may vary depending on your configuration

```
kubectl scale --replicas=<value> -n arcsight-installer-xxxxx
deployment/th-kafka-manager
kubectl scale --replicas=<value> -n arcsight-installer-xxxxx
deployment/th-schemaregistry
kubectl scale --replicas=<value> -n arcsight-installer-xxxxx
deployment/th-web-service
kubectl scale --replicas=<value> -n arcsight-installer-xxxxx sts/th-
routing-processor-group1
```

11. Log into Kafka manager and verify topic assignment between brokers, and if all brokers are up and running.

Backing Up and Restoring

The ArcSight Platform includes several components that should be backed up on a regular schedule, as well as before you upgrade your environment.

FBacking Up and Restoring Core Secrets

Before you undeploy the Core components, back up the Core secrets for later restoration.

Backing Up Core Secrets

To back up Core secrets before you undeploy Core, use the following commands to locate and save them:

```
echo $(kubectl get secret rethink-secret -n $( kubectl get namespaces | grep
arcsight | cut -d ' ' -f1) -o json | jq '.data["rethink-password"]' | sed
's/"//g' ) > rethink-secret-bkp
```

```
echo $(kubectl get secret reporting-secret -n $( kubectl get namespaces |
grep arcsight | cut -d ' ' -f1) -o json | jq '.data["reporting-password"]' |
sed 's/"//g' ) > reporting-secret-bkp
```

```
echo $(kubectl get secret acs-secret-db -n $( kubectl get namespaces | grep
arcsight | cut -d ' ' -f1) -o json | jq '.data["dbuser-pwd"]' | sed 's/"//g'
) > acs-db-secret-bkp
```

```
echo $(kubectl get secret acs-svc-secret -n $( kubectl get namespaces | grep
arcsight | cut -d ' ' -f1) -o json | jq '.data["acs-svc-password"]' | sed
's/"//g' ) > acs-svc-secret-bkp
```

Restoring Backed-Up Core Secrets

To restore previously backed-up Core secrets after you redeploy Core, complete the following steps:

1. Locate the secrets that you backed up previously.
2. To restore the secrets, run the following commands on the master node:

   ```
   export RETHINK_SECRET=$(cat rethink-secret-bkp); echo $(kubectl get
   secret rethink-secret -n $( kubectl get namespaces | grep arcsight | cut
   -d ' ' -f1) -o json | jq '.data["rethink-password"]=env.RETHINK_SECRET' |
   kubectl apply -f -)
   ```

   ```
   export REPORTING_SECRET=$(cat reporting-secret-bkp); echo $(kubectl get
   secret reporting-secret -n $( kubectl get namespaces | grep arcsight |
   cut -d ' ' -f1) -o json | jq '.data["reporting-password"]=env.REPORTING_
   SECRET' | kubectl apply -f -)
   ```

   ```
   export ACS_DB_SECRET=$(cat acs-db-secret-bkp); echo $(kubectl get secret
   acs-secret-db -n $( kubectl get namespaces | grep arcsight | cut -d ' ' -
   f1) -o json | jq '.data["dbuser-pwd"]=env.ACS_DB_SECRET' | kubectl apply
   -f -)
   ```

```
export ACS_SVC_SECRET=$(cat acs-svc-secret-bkp); echo $(kubectl get
secret acs-svc-secret -n $( kubectl get namespaces | grep arcsight | cut
-d ' ' -f1) -o json | jq '.data["acs-svc-password"]=env.ACS_SVC_SECRET' |
kubectl apply -f -)
```

Backing Up and Restoring Configuration Data for Deployed Capabilities

For more information on backing up and restoring Event Data, see Backing Up and Restoring the ArcSight Database

Certain components deployed on the ArcSight Platform use NFS (or EFS when deployed to AWS) to store some of their data, such as Core credentials, dashboard widgets, and search preferences. You can configure automatic backups of NFS or EFS as a protection in the event of data corruption or loss. You can restore the backed up data at any time to the same system or a separate one per your requirements. In the event of data corruption or loss, you can use the backed up data and roll back to an available and known good restore point. Backups are carried out at two levels: pod and NFS.

Because data stores are mounted to *`/<Server mount path>/arcsight-volume`*, do not use this same storage device for your NFS backups. Use a local folder on the system or a remote location.

The following table lists the impacted pods for each capability:

Capability Name	Pod Name
Core	• fusion-metadata-rethinkdb-*-* • fusion-user-management-*-* • fusion-single-sign-on-*-* • fusion-dashboard-web-app-*-* • fusion-metadata-web-app-*-* • fusion-arcmc-web-app-*-* • soar-web-app -*-* • soar-message-broker -*-*

Intelligence	• h2-*-* • intelligence-arcsightconnector-api-*-* • intelligence-tenant-control-*-* • intelligence-tuning-api-*-* • interset-analytics-*-* • interset-api-*-* • interset-ui-*-* • searchmanager-api-*-* • searchmanager-engine-*-*
Transformation Hub	• th-c2av-processor-*.* • th-c2av-processor-esm-*.* • th-enrichment-processor-group*-* • th-kafka-*.* • th-kafka-manager-*-* • th-routing-processor-group*-* • th-schemaregistry-*-* • th-web-service-*-* • th-zookeeper-*.*

- "Backing Up and Restoring Configuration Data for Deployed Capabilities" on the previous page
- "NFS Level Backup" below

Understanding How Pod-level Backup Occurs

Each pod backs up its own data on an hourly basis, placing the data in a **backup staging directory** related to the pod's mount location under `/<Server mount path>/arcsight-volume`. This automated backup process ensures that the pod stores a backup of its data in a complete state. The pod retains a maximum of 24 backups in the staging directory. At any given hour, the oldest backup is deleted and a fresh one created. Because the pod backup is stored in the same NFS volume as the pod content, this pod-level backup does not protect you against data loss or corruption of the volume. Thus, you should configure an NFS level backup to ensure data continuity.

Automated pod backups apply to Core and Intelligence capabilities only.

NFS Level Backup

You must configure an NFS level backup to store the pod-level backup in a reliable, external storage system. For the backup, you must configure a scheduled job to back up the backup

staging directory updated by the pod-level backups. The schedule should be less frequent than the hourly interval for pod-level backups.

To set up the NFS level backup or to restore the data, see the following sections based on your environment:

- Backing Up and Restoring Configuration Data On AWS

Backing Up and Restoring for AWS Deployments

To backup or restore configuration data for deployed capabilities , use the following procedures:

- "Backing Up Configuration Data " below
- "Restoring Configuration Data " below

> The new NFS server requires the prerequisites to be met before attempting any backup or restore. Please browse to here for instructions on creating the NFS shares.

Backing Up Configuration Data

You can back up the configuration data for the deployed capabilities and ArcSight Platform components.

1. Log in to the AWS Backup console at https://console.aws.amazon.com/backup.
2. Attach the *AWSBackupFullAccess* policy to your IAM role.

   For more information, see *Managed policies for AWS Backup* in the AWS documentation.
3. Create an AWS backup plan for the EFS that you created during installation.

   For more information, see *Creating a backup plan* in the AWS Documentation.
4. Follow the onscreen prompts to complete the backup plan for backups at intervals of your choice with appropriate retention periods.
5. After backup creation, in the left-hand pane select **Protected resources** to view a list of Resource IDs and Resource Types.
6. To view associated backups available, click a Resource ID.

Restoring Configuration Data

When restoring data stores, retain the original directory structure and the pod-level sub-directory structure:

```
<efs_server mount path>/arcsight-volume
```

> The default EFS server mount path is /mnt/efs/*<efs parent folder>* .

1. Ensure that you have a valid AWS backup.
2. Log in to the AWS Backup console at https://console.aws.amazon.com/backup.
3. In the left-hand pane, select **Protected resources** to view a list of resources designated by Resource Type and Resource ID.
4. To view the available Recovery point IDs, select a given Resource ID.
5. Select a Recovery point ID and then click **Restore**.
6. Keep default values on the page and then click **Restore backup**.
7. In the left-hand pane, drill down to **Jobs** > **Restore Jobs** to view the restore job status.

   The Restore Job creates a new Recovery directory off of the root of the EFS with the recovered contents preserving the original path hierarchy.
8. On the bastion host used for your AWS setup, navigate to the following location where the restore script resides:

   ```
   cd <INSTALLER_LOCATION>/aws-scripts/scripts
   ```

   > Ensure to replace the <INSTALLER_LOCATION> variable, with a specific value, before you run the command.
9. To view the restore script options, execute the following command:

   > The `nfs-arcsight-volume-restore.sh` script must be run as root

   ```
   ./nfs-arcsight-volume-restore.sh -h
   ```

   Use the following parameters:

   -o | --older-backup
   Available pod backups. This parameter is optional.

   -r | --restore-dir
   Specify the AWS restore directory name created in the mount location. This parameter is mandatory.

   -p | --path
   Specify the EFS mount path. This parameter is mandatory.

   -h | --help
   Displays the command options.
10. (Conditional) To restore to the latest EFS backup, execute the following command:

The `nfs-arcsight-volume-restore.sh` script must be run as root

```
./nfs-arcsight-volume-restore.sh  -r <restore_dir_in_mount_location> -p
<mount_path>
```

Replace the `<restore_dir_in_mount_location>` and `<mount_path>` variables, with specific values, before you run the command.

For example:

```
./nfs-arcsight-volume-restore.sh -r aws-backup-restore_<TIMESTAMP> -p
arcsight
```

To restore to an earlier pod backup, use the -o parameter from the Usage Options.

11. To complete the restore process, follow the onscreen instructions.

After following the configuration data restoration process, opening Core ArcMC from the Core dashboard can produce a 503 Service temporarily unavailable error. To resolve this issue, use the workaround described here.

12. (Conditional) If Transformation Hub is deployed, complete the following steps:
    a. Mount and navigate to the EFS backup location.
    b. Navigate to the Transformation Hub directory.

       For example:

       ```
       /<efs mount location>/arcsight-volume/transformationhub/config/
       ```

    c. Ensure that the *arcsight-volume* is mounted, then navigate to `/transformationhub/config/`.
    d. (Conditional) If the file `arcsight-env-override.properties` exists in the backup location (Step 12b), copy it to the *arcsight-volume* directory (Step 12c), and then remove any file properties that do not apply to the restored environment.
13. To get the names of pods to restart, execute the following command:

```
for pod in $(kubectl get pods --no-headers -n $( kubectl get namespaces |
awk '/arcsight/ {print $1}')|awk '// {print $1}'); do echo -n "${pod} ";
done
```

Compare the output with the impacted pods listed in this table to know pods names.

14. To restart pods listed in this table, execute the following command:

```
kubectl delete pods -n $( kubectl get namespaces | grep arcsight | cut -d ' ' -
f1) <space separated impacted pod names>
```

> Ensure to replace the <space separated pod names> variable, with specific values, before you run the command.

For example:

```
kubectl delete pods -n $( kubectl get namespaces | grep arcsight | cut -d
' ' -f1) fusion-user-management-56497c76bb-mdmmz fusion-dashboard-web-
app-7b864467d5-d2c8v fusion-metadata-rethinkdb-5c69c77756-hxxzg
```

15. Remove the recovery directory restored from AWS to the default mount location in step 7 above.

```
cd <default mount path>
```

```
sudo rm -rf aws-backup-restore_<TIMESTAMP>
```

> Ensure to replace the <default mount path> and <TIMESTAMP> variables, with specific values respectively, before you run the command.

16. Ensure that all Pods display a running status:

```
kubectl get pods --all-namespaces
```

17. To verify restored data stores, log in to the associated application.

> **Note:** Performing the Capabilities Restore operation might require restoring the permissions in the EFS ArcMC folder. If the ArcMC login from the ArcSight Platform dashboard fails with the message: **503 Service Temporarily Unavailable**, execute the following steps:
>
> From the bastion, change to the `arcsight-volume` folder:
>
> ```
> cd /mnt/efs/<efs parent folder>/arcsight-volume
> ```
>
> Change the permissions on the arcmc folder to 1999:1999:
>
> ```
> sudo chown -R  1999:1999 arcmc
> ```
>
> The `fusion-arcmc-web-app` pod will be restarted automatically after this.

Backing Up and Restoring the ArcSight Database

You can configure automatic backups of the ArcSight Database to protect against data loss or corruption. The backed up data can be restored anytime to the same or separate system as per your requirement.

The database uses a single communal storage location for all data and for the catalog (metadata). Communal storage is the database's centralized storage location, shared among the database nodes. When you perform a backup, data gets copied to a backup communal storage location that replicates the live communal storage.

- Backing Up the Database
- Restoring the Database
- Managing Your Backups
- Preparing for a Database Recovery

Backing Up the ArcSight Database

You can manually create or automatically schedule a database backup before upgrading the ArcSight Platform. Follow this section to successfully back up the database.

- Understanding the Database Backup Process
- Preparing the Backup Configuration File
- Backing Up the Database
- Scheduling Automatic Backups

Understanding the Database Backup Process

This section provides an introduction to the backup process:

- Backup Overview
- Backup Terminology
- Prerequisites to Configuring Database Backup

Backup Overview

You can perform a full backup, which is a complete copy of the database catalog, its schemas, tables, and other objects. It provides a snapshot of the database at the time of backup. You can use it for disaster recovery or to restore a damaged or an incomplete database. You can also restore individual objects from a full backup.

If a full backup already exists, then the database backup utility tool backs up new or changed data from the time the full backup was created. You can specify the number of backup snapshots to retain.

Backup Terminology

- Backups are stored in the following folders in the backup location:
  - **Object Folder:** Consists of database objects files, which contain the actual data stored in the database. Repeated backups copy the new objects that are not in the backup location.
  - **Snapshot folder**: Contains a snapshot of the full catalog of the database at the time of the backup. Catalog contains metadata which is smaller in size than the actual data in the database. Catalog keeps track of all the database objects that were present in the database at the time of the backup snapshot. Many Catalog snapshots will refer to the same object files as the backups are performed more often than the lifespan of the object file. This avoids storing duplicates of object files for each backup. The backup_snapshot portion is defined by the .ini file and the date time strings are automatically appended by the database backup process.
- **Restore point:** Each backup operation records the state of the database at the time of the backup and stores it in the backup archive as a restore point. You can restore to a specific restore point using the `-archive` argument.
- **Restore point limit:** Specifies the number of previous backups that you want to retain in addition to the most recent backup.
- In the backup utility configuration file, you can specify the number of backup snapshots to be retained using **Specify the number of historical backups to retain in addition to the most recent backup**, so that the expired snapshots can be groomed out. When a backup snapshot is groomed out, all associated object files that was being referenced by the snapshot will also be groomed out.

(Conditional) Prerequisites to Configuring Database Backup

If you have a cloud deployment, ensure your cloud administrator creates the communal storage backup location before you configure the database backup.

AWS Environment

For an AWS-based deployment, the backup communal storage location must be in the same region as the live database communal storage. The database supports connecting to S3 buckets in AWS using IAM roles. IAM roles are the default access control method for AWS

resources. The database uses this method if you do not configure the legacy access control session parameters.

To use an IAM role, the bucket must be in the same region as the node's database cluster and the role needs to be set with the proper permissions for reading and writing to the S3 bucket. For more information about creating Amazon S3 buckets, see the AWS documentation, Creating a bucket. For more information about IAM roles, see the AWS documentation, IAM Roles for Amazon EC2 and Creating a role to delegate permissions to an AWS service.

Preparing the Backup Configuration File

A database backup utility is provided to be used to perform backup and restore procedures. To use this utility, it must first be configured. Once configured, it can be used to perform the complete lifecycle of scheduling backups, backup on-demand, managing the backup archive, and restoring from backup.

You must create an S3 bucket or a Blob storage backup folder before configuring the database backup utility.

Run this tool as a root user.

1. On database node1, execute the following command from the database scripts directory, located by default at `/opt/arcsight-db-tools/scripts`:

   ```
   ./db_backup.sh config
   ```

2. Select the communal storage.
3. Specify the values for the fields based on your storage type.
   - For S3 storage:

Scenario	Fields
Using IAM role	a. Specify your S3 server: b. Specify S3 server port [443]: c. Is TLS enabled(y/n): d. Specify your S3 backup bucket: e. Specify your S3 backup folder path: f. Specify your locking system path [/tmp]: g. Specify the number of historical backups to retain in addition to the most recent backup: Are the values correct? (y/n):

Backing Up the Database

To back up the ArcSight Database, complete the following steps:

1. Prepare the backup configuration file.
2. Run the following command from the database scripts directory, located by default at `/opt/arcsight-db-tools/scripts`:

```
./db_backup.sh backup
```

Scheduling Automatic Backups

OpenText recommends that you schedule backups to run every hour. To schedule a backup, use the following command from the database scripts directory, located by default at `/opt/arcsight-db-tools/scripts`:

```
./db_backup.sh schedule '<crontab_expression>'
```

where `<crontab_expression>` represents the time that you want to set for the scheduled backup.

For example:

```
./db_backup.sh schedule '0 * * * *'
```

Restoring the Database

You can use the following information to restore a backed up database. This section has the following topics:

- Prerequisites for Restoring the Database
- Restoring a Backup

Prerequisites for Restoring the Database

Before restoring a backup, make a note of the following requirements:

- The database name must match the database name in the backup.
- The number of nodes in the primary subcluster must be equal to the number of nodes that were present in the primary subcluster at the time the backup was taken.
- Database node names must match the names of nodes in the backup.
- Use the same catalog directory location that was used in the database when the backup was taken.

- Use the same port numbers that were used by the database when the backup was taken.
- For object restore, have the same shard subscriptions. If the shard subscriptions have changed, then you can only perform full restore. Shard subscriptions can change when you add or remove nodes or rebalance the cluster.
- The database cannot be restored while it is still running. Run *db_installer* to stop, start, or check the status of the database. If you must stop the database, also run *./scripts/watchdog.sh disable* to disable the watchdog.

> You must stop the database to perform a full restore. Run `db_installer stop-db` to stop the database. However, the database must be running to perform an object restore. Run `db_installer start-db` to start the database.

Restoring a Backup

You can restore a full or object backup of a database that has primary and secondary subclusters to a new (target) database. The target database can have both primary and secondary subclusters. However, the backup is restored only to the primary subclusters of the target database.

To restore a backup, use following command from the database scripts path (`/opt/arcsight-db-tools/scripts`):

```
./db_backup.sh restore
```

You can use the following parameters:

`--archive=<timestamp_value>`	To specify a timestamp of the backup that you want to restore. For example: `./db_backup.sh restore --archive=20211006_205934`
`--restore-objects=<objects>`	To specify the individual objects you want to restore from a full or object-level backup. If you are using wildcards, then use `--include-objects` and `--exclude-objects` instead. For example: `./db_backup.sh restore --restore-objects=default_secops_adm` This parameter is invalid in combination with parameters `--include-objects` and `--exclude-objects`.

`--include-objects=<objects>`	To specify database objects or pattern of objects to restore from a full or object-level backup. Use comma to delimit multiple objects and wildcard patterns. For example: `./db_backup.sh restore --include-objects=default_secops_adm` You cannot use this parameter with `--restore-objects` parameter.
`--exclude-objects=<objects>`	Used along with `--include-objects` option, to specify database objects or pattern of objects you want to remove from the set. Use comma to delimit multiple objects and wildcard patterns. For example: `./db_backup.sh restore --include-objects=default_adm --exclude-objects=default_secops_adm` You cannot use this parameter with `--restore-objects` parameter.

After restore completes, execute the restart commands:

```
./db_installer start-db
```

```
./kafka_scheduler start
```

```
./scripts/watchdog.sh enable
```

After the database is restored, it takes some time before all data is populated in the Core dashboard.

Managing Your Backups

You can use the following information to manage your backups. This section has the following topics:

- Viewing Available Backups
- Quick-Check Backup
- Full-Check Backup
- Deleting a Backup
- Disabling Scheduled Automatic Backups

Viewing Available Backups

To view all the available backups, use the following command from the database scripts path (/opt/arcsight-db-tools/scripts):

```
./db_backup.sh list
```

Quick-Check Backup

You can collect all backup metadata from the backup location specified in the configuration file and compare that metadata to the backup manifest using the following command from the database scripts path (/opt/arcsight-db-tools/scripts):

```
./db_backup.sh quick-check
```

Full-Check Backup

Verify all objects listed in the backup manifest against the filesystem metadata using the following command from the database scripts path (/opt/arcsight-db-tools/scripts):

```
./db_backup.sh full-check
```

Available options:

`--report-file=<path or a file name>`

Full-Check also includes the steps of Quick-Check.

Deleting a Backup

To delete a backup, use the following command from the database scripts path (`/opt/arcsight-db-tools/scripts`):

```
./db_backup.sh remove --archive=<timestamp>
```

Required parameter:

`--archive=<timestamp>`: To specify a timestamp of the backup you want to remove. Replace `<timestamp>` with the timestamp of the archive.

For example:

```
./db_backup.sh remove --archive=20211006_205934
```

Required options:

Disabling Scheduled Automatic Backups

To remove a job that runs scheduled backup, use following command from the database scripts path (/opt/arcsight-db-tools/scripts):

```
./db_backup.sh unschedule
```

Preparing for a Database Recovery

In the event your database is lost, you must work with a Support Technician to recover the ArcSight Database. Before doing so, you must prepare your environment for the recovery process. This process is separate from restoring the database as you are preparing to rebuild the database in this scenario.

NOTE: You must complete this process with the ArcSight Platform Installer. If you use a manual install, it will be difficult to access the necessary files needed in this process.

1. To install the database, run the ArcSight Platform Installer.

   NOTE: The following installation commands must be completed with no exceptions:

   - `./arcsight-install -c /opt/my-install-config.yaml --cmd preinstall`
   - `./arcsight-install -c /opt/my-install-config.yaml --cmd install`
   - `./arcsight-install -c /opt/my-install-config.yaml --cmd postinstall`
2. After installation is complete, ensure that the events collected by SmartConnectors can be copied to the database.

   This step ensures the events are flowing properly into the database and that the installation was successful.
3. Configure the database backup. This process generates the following backup-related file:
   - `/opt/arcsight-db-tools/scripts/db_backup.sh config`
4. Perform a backup of the database. This process generates the following backup-related file:

   `. /opt/arcsight-db-tools/scripts/db_backup.sh backup`

   This steps ensures that the backup process is working without error.
5. Execute the following commands on database node1 to create separate directories:
   - `mkdir /opt/db-saved`
   - `mkdir /opt/db-saved/db-cert`
   - `mkdir /opt/db-saved/db-config`
6. Execute the following commands on database node1:
   - `cd /opt/arcsight-db-tools`
   - `cp db-remote-install.properties /opt/db-saved`
   - `cp cert/* /opt/db-saved/db-cert`
   - `cd /opt/arcsight-db-tools/config`
   - `cp db_credentials_default.properties /opt/db-saved/db-config`
   - `cp db_user.properties /opt/db-saved/db-config`

- `cp backup_restore_cloud_storage.ini /opt/db-saved/db-config`
- `cp backup_restore_cloud_storage_test.ini /opt/db-saved/db-config`
- `cp db_backup.properties /opt/db-saved/db-config`
- `cp password.ini /opt/db-saved/db-config`

7. Save the `/opt/db-saved` directory from step 7 to a location outside of the database.
8. Save the following S3 storage credentials to a location outside of the database:
   - AWS: Access key| Secret
   - minIO: MINIO_ROOT_USER | MINIO_ROOT_PASSWORD
   - S3 certs/keys, if available

Backing Up and Restoring the Postgres Database

Some components that are deployed on the ArcSight Platform utilize an embedded Postgres database that is also deployed on the platform. You can configure backups of the Postgres database to protect from data loss or corruption. The backed up data can be restored anytime to the same or separate system as per your requirement.

Registering the Deployed Capabilities

Before backing up the configuration data, you should ensure that your capabilities have been registered.

> **Note:** You must register the capability only once. You do not need not to repeat the registration each time you perform the backup.

Register the capabilities and functionalities listed in the following table. Some are registered automatically and indicated so in the table. Do not register any that are registered automatically.

Name	When to register	Application Name	PostgreSQL Server Container Hostname	DB Name	DB User	DB Password Key	Pod/ Deployment Names for Restore Instructions
Autopass	Always	Specified by user during registration	itom-postgresql.core	defaultdbapsdb	postgres	ITOM_DB_DEFAULT_PASSWD_KEY	autopass-lm
CDF Data and Deployments	N/A, registered automatically. DO NOT REGISTER.	apphub-cdfapiserver-postgresql	cdfapiserver-postgresql.core	cdfapiserverdb	postgres	ITOM_DB_API_PASSWD_KEY	cdfapiserver-postgresql
CDF Identity Manager	N/A, registered automatically. DO NOT REGISTER.	apphub-idm-postgresql	itom-postgresql.core	cdfidmdb	postgres	ITOM_DB_DEFAULT_PASSWD_KEY	itom-idm
Core ArcMC	N/A, registered automatically. DO NOT REGISTER.	arcsight-fusion-arcmc	itom-postgresql.core	arcmc_rwdb	postgres	ITOM_DB_DEFAULT_PASSWD_KEY	fusion-arcmc-web-app
ArcSight Configuration Service (ACS)	When the Core components is deployed	Specified by user during registration	itom-postgresql.core	arcsight_configuration_service	postgres	ITOM_DB_DEFAULT_PASSWD_KEY	fusion-arcsight-configuration-service
SOAR	When the Core components is deployed	Specified by user during registration	itom-postgresql.core	soar	postgres	ITOM_DB_DEFAULT_PASSWD_KEY	soar-web-app

To register the capability, complete the following steps:

1. "Generate the IDM Token " below
2. "Verifying Application Registration" on the next page
3. "Registering a Capability" on page 738

Generate the IDM Token

The backup service requires an IDM token to authorize the capabilities that you want to register.

Note: Use curl with --noproxy '*' option if there are proxy-related errors.

1. SSH to the OMT master node, bastion, or jump host.
2. Use **integration_admin** as username and run the following command to fetch the password:

```
kubectl exec -it -n core $(kubectl get pods -n core | grep itom-
postgresql | awk '{print $1}') -c itom-postgresql -- get_secret idm_
integration_admin_password | cut -d '=' -f2-
```

3. Connect to the `itom-pg-bacpkup` pod:

```
kubectl exec -it -n core $(kubectl get pods -n core --no-headers -o
custom-columns=":metadata.name" | grep itom-pg-backup) -c itom-pg-backup
-- /bin/sh
```

Note: The X-Auth-Token expires after 30-min. after which the user will need to generate a new token.

4. Run the following commands to get the authorization token and store it in the `TOKEN` environment variable.

```
TOKEN=$(curl -k -sS -X POST --data '{
"passwordCredentials": {
"password": "<password>",
"username": "<username>"
},
"tenantName": "provider"
}' -H 'content-type:application/json' https://portal-ingress-controller-
svc:5443/suiteInstaller/urest/v1.1/tokens | jq -r .token)
```

where <password> is the password obtained in step 2 and <username> is `integration_admin`.

5. Validate the TOKEN environment variable with this command:

```
echo $TOKEN
```

Example output of above command:


```
eyJ0eXAiOiJKV1MiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiI4YTc0ODI5Mjg5NGU5YzE3MDE4OTRl
OWMzNjE5MDE0ZSIsImlzcyI6Imh0dHBzOi8vYXJjc2lnaHQubXRhaG92c2t5LmNvbTo1NDQzL2lkb
S1zZXJ2aWNlIiwiY29tLmhwZS5pZG06dHJ1c3RvciI6bnVsbCwiZXhwIjoxNjg5MzI2MjM5LCJjb2
0uaHAuY2xvdWQ6dGVuYW50Ijp7ImlkIjoiOGE3NDgyOTI4OTRlOWMxNzAxODk0ZTljMzM2ZjAwZTA
iLCJuYW1lIjoiUHJvdmlkZXIiLCJlbmFibGVkIjp0cnVlfSwicHJuIjoiYWRtaW4iLCJpYXQiOjE2
ODkzMjQ0MzksImp0aSI6IjE2YTc4ZmI4LTg5NmQtNDg0NS04ZWRkLTUzMGQxY2M0NmExYiJ9.npKt
pAbNp-XqrYKE2djW08Ub03uidKczjgjk-OIOkik
```


Verifying Application Registration

Stay connected to `itom-pg-backup` pod.

You do not have to re-register the application if it is currently registered. To check which capabilities have been registered, run the following command:

```
curl -k -sS -H "Accept: application/json" --header \
"X-Auth-Token: $TOKEN" -X \
GET https://localhost:8443/backupd/api/v1/registry/applications | jq
```

> Use curl with the --noproxy '*' option if there are proxy-related errors. Also, ensure to replace the *<Token>* variable with a specific value before you run the command.

Example Output:

```
{
  "_links": {
    "self": {
      "href": "/backupd/api/v1/registry/applications",
      "class": "collection"
    },
    },
    "items": [
      {
        "href": "/backupd/api/v1/registry/applications/apphub-cdfapiserver-
postgresql",
        "title": "apphub-cdfapiserver-postgresql"
      },
      {
        "href": "/backupd/api/v1/registry/applications/apphub-cdfapiserver-
postgresql",
        "title": "apphub-idm-postgresql"
      },
      {
        "href": "/backupd/api/v1/registry/applications/arcsight-fusion-
arcmc",
```

```
        "title": "arcsight-fusion-arcmc"
      }
    ]
  }
}
```

Registering a Capability

If the capabilities are not displayed in the registered capabilities list "Verifying Application Registration" on the previous page, then you must register the capability.

1. Stay connected into itom-pg-backup pod. If needed get authorization token and store it in TOKEN environmental variable.
2. Run and input the requested information as shown below:

```
curl -k -sS -X PUT --data '
{
"services":{
"<postgresql-server-container-hostname>":{
"userName":"<application-db-owner-username>",
"passwordKey":"<application-db-owner-passwordKey-on Vault>",
"port":"5432",
"dbName":"<application-db-name>",
"type":"backup.type.postgres",
"secure":true}}}' \
-H 'content-type:application/json' -H "Accept: application/json" -H "X-Auth-
Token: \
$TOKEN"
https://localhost:8443/backupd/api/v1/registry/applications/<application-
name> | jq
```

Note: Ensure that you replace the *<postgresql-server-container-hostname>, <application-db-owner-username>, <application-db-owner-passwordKey-on Vault>, <application-db-name>, <IDM Token>, <itom-pg-backupd-pod-IP>* and *<application-name>* variables, with specific values, before you run the command.

Use curl with --noproxy '*' option if there are proxy-related errors. Also, ensure to replace the *<Token>* variable with a specific value before you run the command.

Where:

- **PostgreSQL Server Container Hostname:** Hostname of the PostgreSQL server container used by the application.

- **Application Database Owner Username:** Application database user name. If the application's database password is not kept in the vault, "postgres" can be used.
- **Application Database Owner PasswordKey on Vault:** Application database password key name in the vault. If the application's database password is not kept in the vault, "defaultdb_user_password" can be used.
- **Application Database Name:** Name of the application database.
- **Secure:** When set to true, the connection to the PostgreSQL service is in secure mode. This is an optional parameter but it should always be set to true to ensure security.
- **Application Name:** Descriptive name of the application.

The following example shows the process of registration for the Autopass capability.

```
curl -k -sS -X PUT --data '
{
"services":{
"itom-postgresql.core":{
"userName":"postgres",
"passwordKey":"ITOM_DB_DEFAULT_PASSWD_KEY",
"port":"5432",
"dbName":"defaultdbapsdb",
"type":"backup.type.postgres",
"secure":true}}}' \
-H 'content-type:application/json' -H "Accept: application/json" -H "X-Auth-
Token: \
$TOKEN" https://localhost:8443/backupd/api/v1/registry/applications/autopass
| jq
```

Validation of registration running:

```
curl -k -sS -H "Accept: application/json" --header \
"X-Auth-Token: $TOKEN" -X \
GET https://localhost:8443/backupd/api/v1/registry/applications | jq
```

Typical output:

```
{
  "_links": {
    "self": {
      "href": "/backupd/api/v1/registry/applications",
      "class": "collection"
    },
    },
    "items": [
      {
        "href": "/backupd/api/v1/registry/applications/apphub-cdfapiserver-
postgresql",
```

```
        "title": "apphub-cdfapiserver-postgresql"
      },
      {
        "href": "/backupd/api/v1/registry/applications/apphub-cdfapiserver-
postgresql",
        "title": "apphub-idm-postgresql"
      },
      {
        "href": "/backupd/api/v1/registry/applications/arcsight-fusion-
arcmc",
        "title": "arcsight-fusion-arcmc"
      },
      {
        "href": "/backupd/api/v1/registry/applications/autopass",
        "title": "autopass"
      }
    ]
  }
}
```

Backing up the Capability Configuration Data

You can back up configuration data for ArcSight capabilities on a regular basis. The backed-up data can be restored when needed.

Starting the Backup

Use the `db_admin.sh` backup and restore script, located in the `${CDF_HOME}/tools/postgres-backup/` directory to back up data.

> **Note:** Before you back up the configuration data for a capability, ensure that the capability is running and accessible, and has been registered. For more information, see Registering the Deployed Capabilities.

Understanding the backup and restore script

The following are the `db_admin.sh` script options and parameters:

```
./db_admin.sh [Options][Parameters]
```

Options	backup	Start database backup
	status	Obtain database backup status
	restore	Start database restore

Parameters	-t|--type	Perform backup/restore operation
	-l|--location	Identify specific backup/restore operation
	-a|--app	Specifies the appName that want to restore

Running the backup script:

1. Run the following command to get the `backupdApiToken` to be used when running the `db_admin.sh` script:

```
./getRestoreToken
```

2. Run the following command:

```
./db_admin.sh backup
```

3. The backup file is stored on the NFS server under this folder:
   `<NFS Server>/itom-vol/pg-data/backupd/backups`
4. Verify the backup status:

```
./db_admin.sh status -l <location> -t backup
```

> **Note:** Replace `<location>` with the associated value before you run the command.

5. To see the data backup for all ArcSight capabilities, run the following command from the NFS server:

```
ls -lh <NFS Server>/itom-vol/pg-data/backupd/backups
```

> **Note:** Replace `<NFS Server>` with the associated value before you run the command.

The example output below shows the data backup for all ArcSight capabilities:

```
total 0
drwxr-x---. 3 arcsight arcsight 44 Mar 25 17:04 2023-03-25T17:04:43.807Z
drwxr-x---. 2 arcsight arcsight 27 Mar 25 17:37 2023-03-25T17:37:24.907Z
drwxr-x---. 2 arcsight arcsight 27 Mar 29 08:24 2023-03-29T08:24:14.530Z
drwxr-x---. 2 arcsight arcsight 27 Mar 29 09:36 2023-03-29T09:36:19.605Z
drwxr-x---. 2 arcsight arcsight 27 Mar 29 09:54 2023-03-29T09:54:01.232Z
drwxr-x---. 3 arcsight arcsight 44 Mar 29 13:05 2023-03-29T13:05:46.311Z
drwxr-x---. 4 arcsight arcsight 56 Mar 29 14:12 2023-03-29T14:12:58.071Z
drwxr-x---. 4 arcsight arcsight 56 Mar 30 06:48 2023-03-30T06:48:57.245Z
drwxr-x---. 4 arcsight arcsight 56 Apr  2 14:34 2023-04-02T14:34:55.128Z
```

```
drwxr-x---. 4 arcsight arcsight 56 Apr 16 12:17 2023-04-16T12:17:27.006Z
-rw-r-----. 1 arcsight arcsight  0 Mar 25 17:04 backupd.lock
```

The backup data is saved in directories with timestamps (for example, 2023-03-25T17:37:24.907Z). The data stored here is used during the restore procedure.

Restoring a Capability's Configuration Data

You can restore the backed up configuration data for any capability. Use the **db_admin.sh** backup-restore script, located by default in the `${CDF_HOME}/tools/postgres-backup/` directory.

The app deployment names are different from the capability names, refer to "Registering the Deployed Capabilities" on page 734 for the pod deployment names.

1. Stop the running application:

   Note: In case of an Multi-tenancy instance, repeat this step for each soar-web-app deployment.

   ```
   kubectl scale --replicas=0 deployment <app-deployment-name> -n
   <namespace>
   ```

   Note: You must wait until the pod related to the deployment terminates.

   Note: Do not scale down the deployment cdfapiserver-postgresql that corresponds to the CDF Data and Deployments application when restoring this capability.

   Note: Do not scale down the deployment itom-idm that corresponds to the CDF Identity Manager when restoring this capability.

2. Run the following command:

   ```
   ./db_admin.sh restore -l <location> -a <application name>
   ```

   Note: Ensure you run the getRestoreToken script to obtain the authorization token before you run the `db_admin.sh` command.

3. Check the restore status:

   ```
   ./db_admin.sh status -l <restore location>  -t restore
   ```

> **Note:** Make sure to differentiate the `<restore location>` in the status check from the `<backup location>` in the restore command, as these do not correspond to the same location.

4. If the application's database password is kept in the vault, skip this step. If it is not and it has been backed up with a user other than the database owner (like 'postgres'), you need to run the following commands in the PostgreSQL console.

   > **Note:** This procedure needs to be done for the SOAR database.

   a. Log in to the PostgreSQL container console:

   ```
   kubectl exec -it itom-postgresql-xxxxxxxxxx-xxxxx -n core -c itom-postgresql -
   - /bin/bash
   ```

   b. Get the database user password on the vault:

   ```
   get_secret <vault-key>
   (postgres user default vault-key=ITOM_DB_DEFAULT_PASSWD_KEY)
   ```

   c. Run the following command and paste the password value in step b.

   ```
   psql -h 127.0.0.1 -U postgres <app-db-name>
   ```

   d. To grant usage privilege to `postgres` user for the `soar_default` schema, run the following command:

   > **Note**: For Multi-tenancy,replace **soar_default** with **soar_tenantkey** and repeat the steps for each tenant schema in the following steps.

   ```
   GRANT USAGE ON SCHEMA soar_default TO postgres;
   ```

   e. To grant create privilege to `postgres` user for the `soar_default` schema, run the following command:

   ```
   GRANT CREATE ON SCHEMA soar_default TO postgres;
   ```

   f. To grant usage privilege to app-db-owner-user for the `soar_default` schema, run the following command:

   ```
   GRANT USAGE ON SCHEMA soar_default TO app-db-owner-user;
   ```

   For example:

   ```
   soar=# GRANT USAGE ON SCHEMA soar_default TO soar_default;
   ```

g. To grant create privilege to app-db-owner-user for the `soar_default` schema, run the following command:

```
GRANT CREATE ON SCHEMA soar_default TO app-db-owner-user;
```

5. Restart the application:

> **Note**: In case of an Multi-tenancy instance, repeat this step for each soar-web-app deployment.

```
kubectl scale --replicas=1 deployment <app-deployment-name> -n arcsight-installer-xxxxx
```

Checking Backup and Restore Status

Use the `db_admin.sh` backup and restore script, located in the `${CDF_HOME}/tools/postgres-backup/` directory, to check the status of backup and restore procedure of all ArcSight capabilities.

Checking backup/restore status:

1. Run the following command to view the backup and restore status:

```
./db_admin.sh status -l <location>  -t <backup/restore>
```

Where:

`<Location>`: The encoded directory with timestamps, for example 2021-03-25T17:37:24.907Z.

`<Type>`: The type of operation to be performed, for example, backup or restore.

For example:

```
./db_admin.sh status -l 2021-03-30T07%3A05%3A02.183Z -t restore
```

2. Specify the IDM token that you received in the Fetching the IDM Token for backupd service section, when prompted.

The following example output shows the in-progress restore status for ArcSight capabilities:

```
[INFO] 2021-03-30 07:05:41 :
{
"version": "1",
"user": "admin",
"mode": "full",
"applications": {
```

```
"soar": {
"itom-postgresql.core": {
"status": "IN_PROGRESS"
}
}
},
"status": "IN_PROGRESS"
}
```

Chapter 9: Managing Your ArcSight Infrastructure with ArcMC

ArcSight Management Center (ArcMC) is a centralized security management center that manages large deployments of ArcSight solutions such as Transformation Hub, ArcSight Logger, ArcSight SmartConnectors (Connectors), ArcSight FlexConnectors, and ArcSight Connector Appliance (ConApp) through a single interface.

Whether you have a large deployment of ArcSight or a small shop, ArcMC automates log collection and log management. ArcSight Management Center helps you with centralized management of ArcSight solution, automation of change management, reduction of the resource requirement for security information and event management (SIEM), easy management of large deployments, reduction of the administrative overhead, efficient log traffic management, bandwidth optimization for log collection, support of IT operational analytics. ArcMC also manages the ArcSight deployment through a unified interface.

The following topics are discussed here:

The User Interface

This chapter provides a general overview of the ArcMC interface. ArcMC uses a browser-based user interface. Refer to the ArcMC Release Notes for the latest information on supported browsers.

The following topics are discussed here.

The Menu Bar

The menu bar provides access to the main functional components of ArcMC. It includes the **Dashboard**, **Node Management, Configuration Management, User Management** and **Administration** menus.

Monitoring Summary

The Monitoring Summary page displays information on all monitored products.

- The aggregated health status for products of each type is displayed in pie graph format, showing total number of nodes, as well as the number corresponding to each status. A summary table shows the same data in percentage format.
- The management panel displays the **Monitoring Summary** table, showing all products which are currently reporting issues.

- The navigation panel enables you to display a monitoring summary for individual product types in the management panel. Click the product type to display the product's monitoring summary.

For more information on viewing and configuring monitoring, see "Dashboard " on page 752.

Node Management

Use **Node Management** to manage any of the following node types:

- Connectors
- Hardware or Software Connector Appliances
- Hardware or Software Loggers
- Hardware or Software ArcSight Management Centers
- Transformation Hub

For more information on adding and managing nodes, see "Managing Nodes " on page 793. From the same menu, you can also perform selected management tasks on managed ArcSight products. See "Managing ArcSight Products " on page 835.

Configuration Management

Use **Configuration Management** to create and manage node configurations, synchronization (pushing) of configurations across multiple nodes, and expedite the initial configuration of Loggers. You can manage any of these configuration types:

- Subscriber configurations for:
  - ArcMC
  - Connectors
  - Connector Appliances
  - Destinations
  - Loggers
  - System administration
- Other configurations are also managed here:
  - Logger Initial configurations
  - Logger event archives
  - Management of Logger peers
  - Management of Transformation Hub
  - Bulk Operations

- Generator ID Management
- Management of Deployment Templates

For more information on subscriber configuration management, see "Managing Configurations" on page 882.

For more information on initial configurations, see "Logger Initial Configuration Management" on page 918.

User Management

User management enables you to manage users across all of your managed nodes. You can create and edit users, user lists, their associations, and roles. You can also check to see if each node complies with a list of authorized users on the managing .

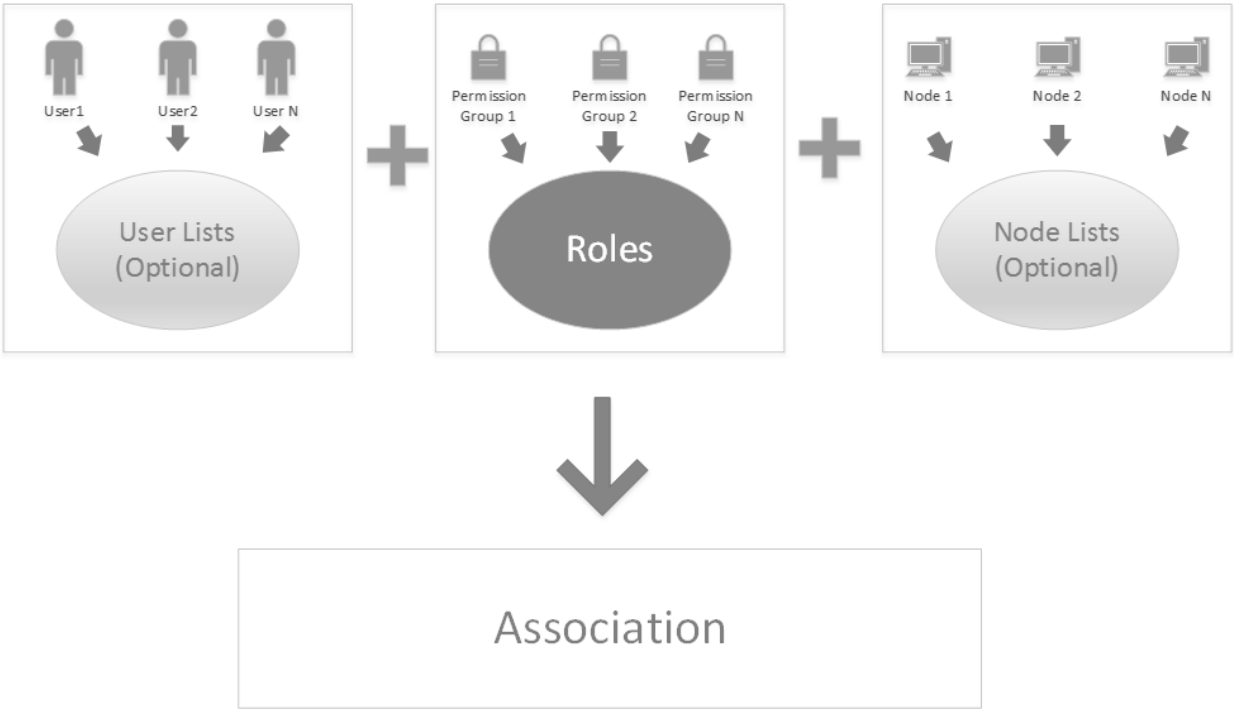
For more information about user management, see "User Management Workflow" on the next page.

Overview

Role-based access control (RBAC) user management enables you to manage product user access with custom roles across specified nodes.

> Previous versions of ArcMC included user management across nodes as part of Configuration Management (where user information was defined in a Users configuration). In ArcMC 2.1, user management across nodes is now a separate, greatly improved RBAC (role-based access control) functionality.

User Management Workflow



User management in ArcSight Management Center follows this workflow:

1. Create users in ArcSight Management Center, or import them from managed nodes.
2. Optionally, group users into user lists for ease of organization and management.
3. Create (or import) permission groups to enable administrative privileges.
4. Create roles by assigning permission groups to grant functional access to products.
5. Optionally, create node lists to ease the organization of sets of nodes.
6. Create associations to associate users (or user lists), nodes (or node lists), and roles.
7. Push associations to nodes to enable access for users included in the association, with privileges appropriate for the role and access only to the desired nodes.
8. Check compliance of users on managed nodes with the managing ArcMC.

Administration

The **Administration** menu contains these items:

- **Backup:** Enables you to back up your current ArcSight Management Center configuration. For more information, see Managing Backups and Restores.

> This function isn't available when you deploy ArcMC in the containerized ArcSight Platform.

- **Repositories:** Enables you to manage repositories that store files, such as logs, certificates, and drivers. For more information, see "Managing Repositories " on page 567.
- **Snapshot:** Enables you to take a snapshot image of ArcSight Management Center, to produce logs that are useful in troubleshooting. For more information, see Creating Snapshots, on page 1.
- **Restore:** Enables you to restore your configuration from a saved backup. For more information, see Managing Backups and Restores.

> This function isn't available when you deploy ArcMC in the containerized ArcSight Platform.

- **System Admin:** Describes the system administration tools that enable you to create and manage users and user groups, and to configure security settings for your system. For more information, see "System Administration " on page 953.
- **Consumption Report:** Generates a report on Logger data consumption for selected managed nodes.

ArcMC Name

To assign ArcMC a name, add the property `arcmc.instance.name=<arcmc_instance_name>` to the `logger.properties` file.

You can set a name for your ArcMC during the OMT deployment for Core ArcMC.

A valid ArcMC name must meet the following criteria:

- Is a non-empty string
- Is equal to or less than 32 characters long
- It contains characters: A-Za-z0-9 _-

For more information on how to edit the `logger.properties` file, please refer to the "Modifying logger.properties " on page 800 section.

Stats (EPS In/Out)

The **Stats** menu item shows the total Events Per Second (EPS) in and out from all managed connectors (standalone SmartConnectors and connectors running on managed hosts).

Job Manager

The Job Manager shows all deployment jobs processed in a specified time frame. Using the Job Manager, you can identify issues that occurred during deployments.

The Job Manager shows the following for each job:

- **Name of the Job:** The job name (must be smaller than 255 characters).
- **Started By:** The user who ran the job.
- **Type:** Type of job.
- **Start/End Time:** The start and end time of the job.
- **Status:** Job status. If the job has a status of *Failed*, click **Retry** to re-run the job.
- **Details:** Job details.

Hover over any field to display details about the field in a tooltip. Click the Up/Down arrows at the top of any column to sort data by the selected parameter.

To view the Job Manager:

1. On the menu bar, click the Job Manager (notepad) icon. By default, the Job Manager displays all deployment jobs for the last 5 days. A red numeral on the Job Manager icon, if any, indicates the number of jobs currently in the In-Progress state.

- To change the time frame for job data displayed, specify the date criteria in the date boxes in the upper right corner, then click **Show Results.** You may specify any time frame in the last 180 days (6 months).
- To search for a specific job, specify the search criteria in the **Search** box.
- If a job is in progress, you can click **Refresh** on the menu bar to refresh the display.

Site Map

For ease of accessibility and convenience, the Site Map links to all pages in the ArcMC UI.

To access the site map: on the main toolbar, click **Site Map.** Select the desired link to navigate.

History Management

History management enables you to quickly and easily access previously-navigated pages. History management is available for Node Management, Configuration Management, User Management pages, and for some Administration pages.

In Node Management, the navigation tree shows the full path for any item selected on the tree. Click any node in the path to navigate directly to the corresponding page.

You also can return to any previously-browsed page by clicking the corresponding link in the breadcrumb trail.

In addition, you can use your browser's **Back** and **Forward** buttons to navigate to previously visited pages.

Dashboard

Using ArcMC, you can monitor the health status of all managed nodes. You can also configure warnings and alerts for issues of importance to you.

> **Note:** In order for products to be monitored, they must be added as nodes to ArcMC. For more information on managing nodes, see "Managing Nodes " on page 793.

Monitoring is displayed on the **Dashboard > Monitoring Summary** page. ArcMC automatically monitors all managed nodes.

You can also configure notifications (email, SNMP, and through audit forwarding) about the status of managed nodes.

Monitoring Managed Nodes

ArcMC monitoring, on the **Dashboard > Monitoring Summary** page, displays the current health history of all managed nodes, both software and hardware.

- Monitored metrics for software nodes (such as Software Logger) include such software parameters as CPU usage, event flow, and disk usage statistics.
- Monitored metrics for hardware appliances (such as Logger Appliance) include both software as well as hardware-related attributes, such as remaining disk space and hardware status.
- Device health related information:
  - Devices have severity associated with them instead of status. Up is equivalent to "HEALTHY" and Down to "FATAL".
  - Sunburst Chart and corresponding breakdown table is enhanced to show the severity instead of status.

You can view a complete list of monitored parameters in "Monitoring Rules Parameters " on page 766 , and use them in creating your own custom rules. These rules breaches will also be displayed on the Health History and Hardware Status panels. Note that the layout and selection of the data panels in the Monitoring Summary is not customizable.

Configuring Properties for Monitoring Managed Nodes

The default properties values for node monitoring are set to work on most customer environments. If ArcMC has a heavy inventory and metrics are not being shown correctly, you may wish to configure these properties with custom values.

Configuration property	Description	Default	Type
`monitoring.node.status.taskBatchSize`	Number of tasks to add to the thread pool at once. It will optimum to set a value equal or half of corePoolSize.	20	Number
`monitoring.node.status.timeout`	Timeout in seconds for a batch of tasks to complete	120	Number
`monitoring.node.status.corePoolSize`	Size of the thread pool for executing tasks.	50	Number
`monitoring.node.status.maxPoolSize`	Max size of the thread pool. This limit overrides corePoolSize when the value is greater than maxPoolSize. The maximum value is 300.	100	Number
`monitoring.node.status.trackCancelledEntities`	Logged cancelled entities after reaching max set attempts.	false	Boolean
`monitoring.node.status.evaluateCancelledAttempts`	Increments the cancelled counter on the entity after x number of attempts.	5	Number
`monitoring.node.status.cancelledPollThreshold`	Log when an entity reaches its cancelled poll threshold.	2	Number

To configure monitoring properties:

1. In a text editor, open the file In a text editor, open the file `.../userdata/arcmc/logger.properties`. If the file does not exist, follow the steps outlined here.
2. Change the values of one or more properties listed above as needed.
3. Save the file.
4. Restart the ArcMC web processes.

The Monitoring Summary Dashboard

The Monitoring Summary includes a variety of panels that display monitoring information on the health and status of your managed products.

To view the monitoring summary, click **Dashboard > Monitoring Summary**.

Total Number of Nodes

Each tile in the **Total Number of Nodes** panel displays the count of managed nodes of the specified type. These types are defined as follows.

Tile	Count
Devices	Devices which are forwarding events.
ArcMC/CHA	Includes managed ArcMCs and Connector Hosting Appliances, in both hardware and software form factors.
Connectors	Managed Connectors.
Loggers	Managed Loggers (hardware and software form factors).
Nodes	Nodes on the managed Transformation Hub. (Note that if Transformation Hub is upgraded, the Monitoring Summary will not reflect the correct Transformation Hub information until you import the new Transformation Hub certificate into ArcMC. See "Downloading and Importing Host Certificates" on page 943 for more information.) **Note:** To display Transformation Hub Processing Data users need to turn on the C2AV pod on the Transformation Hub, for more information see Managing Transformation Hub through ArcMC. **Event Parsing Error**, **Stream Processing EPS**, and **Stream Processing Lag** are the metrics that will be available after the C2AV pod is turned on, otherwise only **CPU Usage** and **Memory** under **Broker's Health** will be displayed. **Note:** The stream processors metric name format has changed to SP_Name(SP_Type).

To see the details of a node type, click the title corresponding to the node type. For example, to view the details of all Connectors, click **Connectors**.

Devices by Device Type

The **Devices by Device Type** display shows a color-coded sunburst of the various device types in use across your network. The table shows the total number of active and inactive devices by device product.

The inner ring of the sunburst shows the total devices.

The outer ring of the sunburst shows the total number of device types. For clarity of display, if the number of device types exceeds 1000, the outer ring is not shown.

The **Devices Information for All Device Types** table breaks down the information to display Device Type, Severity (Fatal, Critical, Warning, Healthy), and Total Devices.

To see the details of a device type, click the corresponding tile in the wheel, or its entry in the table.

> **Note:** ArcMC 2.6 and 2.7 Device Monitoring function supports only Connectors 7.3 - 7.7. ArcMC 2.8 and later support Connectors 7.3 and later for Device Monitoring.

Device Configuration for Device Type

The Device Configuration for Device Type page allows you to modify the **Device Product time-out Interval**, **Device age-out Interval**, and **Disable Device Tracking.**

Device Product time-out Interval

The default value is set to 20 minutes, this can be modified. If the selected device type does not send events to the connector during the last 20 minutes, the device type will be marked as Inactive.

Device age-out Interval

The default value is set to 14 days, this can be modified. If the selected device type remains inactive for 14 days, the device type records will be purged from the system.

Disable Device Tracking.

This box can be checked to disable the selected device product family.

> **Note:** If device product monitoring is re-enabled X days later while **Disable Device tracking** is enabled, the aged-out internal should be set to Y days, in which Y comes after X days. This will prevent the selected disable tracking product family device records from being removed of the ArcMC system.

Device Health Metrics

The dashboard displays device health information as severity. The Sunburst Chart shows the Severity as "HEALTHY", "FATAL", "WARNING", or "CRITICAL".

> **Note:** The selection and layout of the panels on the Monitoring Summary is not customizable. You can, however, customize the issues reported for a given node type by creating custom breach rules, which can be viewed on the Severity Issue Summary. See "Monitoring Rules" on page 760

Drilling Down

You can view the details of problematic nodes, and then take action to rectify any issues.

To view all details of a problematic node, select it in the upper table. The lower table shows issues associated with that node. Each issue is shown with these identifiers:

- **Metric Type:** Metric assigned to the issue.
- **Metric Name:** Name of the metric.
- **First Occurrence:** Local time of the issue's first occurrence.
- **Last Occurrence:** Local time of the issue's last occurrence.
- **Severity:** Issue severity.
- **Description:** Brief description of the issue.

To view details of nodes by severity:

1. On the menu bar, click **Dashboard > Monitoring Summary**.
2. Click the ring meter corresponding to any of the monitored product types, in the portion of the meter corresponding to the severity you wish to view. (For example, to view all nodes currently with Warning status, click the Warning, or yellow, part of the ring.) The corresponding **Severity Issue Summary** is displayed.
3. On the **Severity Issue Summary** page:

   The upper table shows a list of all problematic nodes, with the following identifiers:

   - **Name:** Node name.
   - **Path:** Path to the node.
   - **Type:** Type of node.
   - **Lead/Breach:** Short summary of the most severe issue reported by the node. The node may be experiencing less severe issues as well.

   ### Details and Health History

   To view further health details of a problematic node, including history and status, click **Details**. The data tables show the detailed parameters of the selected node.

   The Health History panel will show any rules breaches, including custom rules you have created yourself.

   > **Note:** The layout of the panels and selection of the displayed parameters is not customizable.

Data Charts

Each data chart represents values of the parameter over time. Use the drop-down list to change the interval shown from the last 4 hours, the last day, or the last week. Data charts can include any of the metrics shown under the Valid Values for Metric Types table.

Click the data legend to toggle display of the corresponding line from the chart. Hiding some lines may be helpful to clarify a chart with many lines.

ADP License Usage for the Last 30 Days

Your ADP license entitles you to a specified number of managed products and amount of managed traffic. The **ADP License Usage for the Last 30 Days** panel shows your ADP data usage for the previous month.

The graph shows all traffic in your ADP environment.

- Green (the default) indicates that data usage is within your licensed limit.
- Amber indicates periods when your data usage approached your licensed traffic limit.
- Red indicates periods when your data usage exceeded your licensed traffic limit.

The **Active Loggers** indicate the number of ADP Loggers the data from which contributes to the license monitoring report. For more details, you can export the license report to PDF format, which includes data on the last 365 days.

If your ArcMC is enabled as a License Server, the Daily Usage bar chart displays the overall ADP license consumption on a daily basis. The daily license usage is calculated from the managed connectors (version of 7.3.0 or later) and managed ADP loggers based on the following:

- If a Connector is managed by ArcMC, then ArcMC will include its event ingestion from all non-ADP or non-managed source devices in the ADP daily license usage calculation. If a source is also a managed ADP component, the event flow from this source to the managed Connector will not be tracked.
- If an ADP Logger is managed by ArcMC, then ArcMC will include its event ingestion from all non-ADP or non-managed source devices in the ADP daily license usage calculation. If a source is also a managed ADP component, the event flow from this source to the managed ADP Logger will not be tracked.

Each day, ArcMC collects the daily ingestion information from each Connector and ADP Logger. Connectors and Loggers give an accumulated ingestion total when not reachable by ArcMC at the time of ingestion collection (daily at 1:00:00 ArcMC local time by default). This scenario could be caused by any of the following:

- The ADP Logger or Connector was down.
- The ADP Logger or Connector’s server certificate has changed.

- The ADP Logger or Connector was not managed by the ArcMC.

If any managed nodes (Connector, ADP Logger) are not reachable during ingestion collection time, the daily consumption of these nodes will be counted and reflected in the consumption number on a daily report, when ArcMC license server has successfully pulled the consumption data from the affected nodes.

> **Note:** Daily ingestion collection only applies to License Server ArcMCs and ArcMCs that are managed by the License Server.

The ingestion report on an individual ADP Logger includes its previous day's ingestion during the time window of [00:00:00 – 23:59:59] GMT. For license usage calculation, ArcMC collects the previous ADP Logger's ingestion during the time window of [01:00:00 – 24:59:59] ArcMC local time. The time window used for individual Logger ingestion tracking and ingestion calculation are different; hence, it is not recommended to compare these two reports because they will report different numbers.

To enable the display of ADP license usage:

1. Enable ArcMC as an ADP license server. In the ArcMC toolbar, click **ADP License Server,** then click **Yes**.
2. Upload a valid capacity license to the ArcMC on the **License and Upgrade** page.

To export the license report to PDF format:

1. Click **Export License Report.**
2. The PDF is downloaded to your local system.

EPS License Reporting

The customer is considered to be in compliance with the license agreement as long as the MMEPS value indicators remain at the limit or below the purchased license capacity. If 3 or more consecutive MMEPS value indicators exceed their capacity based on the purchased license, they are considered to be out of compliance.

> **Note:** ArcMC will only report events from the managed EPS licensed Loggers.

You can download up to one year license reports in PDF format.

Keystones:

1. **Events per Day (EPD):** Is the total number of events generated in a 24 hour clock period. The clock is calculated based on UTC time starting at 00:00:00 and ending at 23:59:59,

regardless of the local times used.

2. **Sustained EPS (SEPS):** Is the event “constant” per second supported by the system within the 24 hour clock period. It stabilizes peaks and valleys and gives a better indication of use
3. **Moving Median EPS (MMEPS):** Is the license usage. It uses the 45 day period SEPS data shifting the calculation window 1 day every 24 hours after the first 45 days. The clock is calculated based on UTC time starting at 00:00:00 and ending at 23:59:59, regardless of the local times used.
4. **License Limit:** Corresponds to the amount of EPS acquired in the license.
5. **Baselining:** The baselining period begins when an EPS licensed product is detected in ArcMC for the first time (day 1), and it continues for the next 45 days. Once ArcMC detects an EPS licensed product, the baseline is set, and it does not change even if the license is redeployed. During this period, the usage will be calculated as the median of the SEPS values available at that moment. MMEPS values are truncated to benefit the customer. For example:

   MMEPS Calculation

   Day 1: SEPS of day 1

   Day 2: Truncated median of SEPS of days 1 and 2.

   Day 3: Truncated median of SEPS of days 1, 2, and 3.

   Day 45: Truncated median value of SEPS of days 1 through 45

EPS License Usage Calculation

The usage will be collected from each managed Loggers and ArcMCs once a day.

- **Moving Median Events Per Second (MMEPS):** The median value over the last 45 days.
- **Baselining:** The usage will be calculated as the median of the SEPS values available at that moment. MMEPS values are truncated to benefit the customer.

Host Status Exceptions

This feature lists all the managed nodes that are in either Fatal, Critical or Warning status. To access the monitoring metric details view of a managed node, click **Dashboard > Host Status Exceptions.**

The following fields are displayed in the host status exceptions page:

- Host name: Name of the host.
- Status: Status of the host (Fatal, Critical, Warning).
- Cause: Root cause for hosts to be unhealthy (usually due to being unreachable or triggering a specific rule).

- Type: Type of host.
- Logical Group Path: Host location within ArcMC.

Monitoring Rules

Monitoring rules are defined to generate monitoring warnings for each managed product type. ArcMC includes many preset monitoring rules for your use. You can use these rules as written, or customize them for your own use. In addition, you can create your own custom monitoring rules.

A monitoring rule comprises a set of logical, performance, health, or other criteria. All criteria in the rule are evaluated together to determine the rule's total effect, which generates an alert from ArcMC.

Rules breaches will be displayed in the Warning Severity Issue Summary, which you can view by clicking one of the ring meters on the Monitoring Dashboard.

For example, a rule could check for the number of *input events per second* (criterion #1) that reach a *certain type of device* (criterion #2). Should this number *exceed* (criterion #3) a specified *level* (criterion #4), then a *warning* (*alert*) should be returned.

Breach Function

The breach function checks the backend monitor metric data table. The metric data table is updated every 3 minutes, and the breach check function runs every four minutes at the 45th second. Reducing the rule's time range to a smaller number (e.g. 1 or 2) could result in an undetected breach.

Alerts can be delivered by email or by SNMP, or can be recorded in audit logs. Only when there is new breach detected (i.e. not found on the previous run), ArcMC sends the notification/alert if the notification option is enabled. If the breach keeps coming on the subsequent calls, the alert will only be sent the first time.

For more information on managing and creating rules, see "Managing Rules " on page 765.

Preset Rules

ArcSight Management Center includes preset rules to assist in monitoring. You can use these preset rules as written or customize them as needed for your own use. You can also create custom rules of your own.

By default, ArcMC preset rules are disabled. You must enable a preset rule in order for it to apply and trigger alerts.

Note: For customers with previous versions of ArcMC and who already have a list of existing rules, preset rules included in ArcMC are appended to your existing rules.

To review preset rules:

1. Click **Dashboard > Rules.** The Monitoring Rules summary is shown.
2. To view a rule's settings in detail, in the **Name** column, click the rule name.
3. To enable a disabled preset rule, under **Status**, select **Enable.**

Preset Rules Description

Name	Description	Products			
MM_DD_YYYY_RAID_BATTERY_Failed_ArcMC_ConApp_Logger	Displays a critical alert when the Raid Battery has failed during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_POWER_SUPPLY_Failed_ArcMC_ConApp_Logger	Displays a critical alert when the Power supply has failed during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_TEMPERATURE_Failed_ArcMC_ConApp_Logger	Displays a critical alert when the temperature reaches a certain level during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_POWER_SUPPLY_Degraded_ArcMC_ConApp_Logger	Sends a warning when the power supply has been degraded during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_VOLTAGE_Failed_ArcMC_ConApp_Logger	Displays a critical alert when the voltage levels have been failing during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_FAN_Failed_ArcMC_ConApp_Logger	Displays a critical alert when the fan has failed during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_HARD_DRIVE_Rebuilding_ArcMC_ConApp_Logger	Sends a warning when the hard drive has been rebuilding during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_RAID_CONTROLLER_Failed_ArcMC_ConApp_Logger	Displays a critical alert when the RAID controller has failed during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_CURRENT_Degraded_ArcMC_ConApp_Logger	Sends a warning when the current has been degraded during the last 5 minutes.	ArcMC	ConApp	Logger	

Name	Description	Products			
MM_DD_YYYY_RAID_CONTROLLER_Degraded_ArcMC_ConApp_Logger	Sends a warning when the raid controller has been degraded during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_VOLTAGE_Degraded_ArcMC_ConApp_Logger	Sends a warning when the voltage has been degraded during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_ALL_EPS_OUT_ArcMC_ConApp_Logger	Displays a critical alert when all outgoing events per second have failed during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_HARD_DRIVE_Failed_ArcMC_ConApp_Logger	Displays a critical alert when the hard drive has failed during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_Queue Files Accumulated	Displays a critical alert when files have accumulated in queue during the last 5 minutes.				Connector
MM_DD_YYYY_Full GC	Sends a warning when the garbage collection count is higher than 7 during the last 60 minutes.				Connector
MM_DD_YYYY_Caching	Sends a warning when the connector caching is higher than 100 during the last 5 minutes.				Connector
MM_DD_YYYY_Receiver Down	Sends a warning when the receiver has been down during the last 5 minutes.			Logger	
MM_DD_YYYY_Events Dropped from Cache	Displays a fatal alert when the connector events dropped from cache have been down during the last 5 minutes.				Connector
MM_DD_YYYY_Files Dropped From Cache	Displays a critical alert when the connector files dropped from cache have been down during the last 5 minutes.				Connector
MM_DD_YYYY_Logger Not Receiving Data	Displays a fatal alert when logger hasn't recevied data during the last 30 minutes.			Logger	
MM_DD_YYYY_Storage Disk Usage above 85%	Sends a warning when the storage limit goes over 85% during the last 5 minutes.			Logger	
MM_DD_YYYY_JVM_MEMORY_ArcMC_ConApp_Logger	Sends a warning when the jvm memory reaches 800 GB during the last 5 minutes.	ArcMC	ConApp	Logger	

Name	Description	Products			
MM_DD_YYYY_Connector Restart	Sends a warning when the connector has restarted more than 5 times during the last 5 minutes.				Connector
MM_DD_YYYY_Memory Red Zone	Displays a critical alert when the Connector JVM memory has gone over 90% during the last 5 minutes.				Connector
MM_DD_YYYY_Memory Yellow Zone	Sends a warning when the Connector JVM memory has gone over 80% during the last 5 minutes.				Connector
MM_DD_YYYY_Events Dropped From Queue	Displays a fatal alert when more than 100 Connector queue events dropped during the last 5 minutes.				Connector
MM_DD_YYYY_Files Dropping From Queue	Displays acritical alert when Connector files dropped from queue during the last 5 minutes.				Connector
MM_DD_YYYY_RAID_ BATTERY_Degraded_ ArcMC_ConApp_Logger	Sends a warning when the raid battery has been degraded during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_ TEMPERATURE_ Degraded_ArcMC_ ConApp_Logger	Sends a warning when the temperature has been degraded during the last 5 minutes in	ArcMC	ConApp	Logger	
MM_DD_YYYY_EPS_OUT_ Connector	Displays a critical alert when the outgoing events per second have been degraded during the last 5 minutes.				Connector
MM_DD_YYYY_FAN_ Degraded_ArcMC_ ConApp_Logger	Sends a warning when the fan's RPMS have failed during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_HARD_ DRIVE_Degraded_ArcMC_ ConApp_Logger	Sends a warning when the hard drive has been degraded during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_ALL_EPS_ IN_ArcMC_ConApp_ Logger	Displays a critical alert when all incoming events per second have failed during the last 5 minutes.	ArcMC	ConApp	Logger	

Name	Description	Products			
MM_DD_YYYY_CPU_USAGE_ArcMC_ConApp_Logger	Sends a warning when the cpu usage has exceeded 50% during the last 5 minutes.	ArcMC	ConApp	Logger	
MM_DD_YYYY_QUEUE_DROP_COUNT_Connector	Sends a warning when Objects droppped from file Queue during the last 5 minutes.				Connector
MM_DD_YYYY_CURRENT_Failed_ArcMC_ConApp_Logger	Displays a critical alert when the current has failed during the last 5 minutes.	ArcMC	ConApp	Logger	

Managing Rules

To create a custom rule:

1. Click **Dashboard > Rules.**
2. In the toolbar, click **Add New Rule.**
3. Select values for the rule parameters.
4. Click **Save.**

To edit an existing rule:

1. Click **Dashboard > Rules.**
2. Under **Monitoring Rules**, select the rule you wish to edit.
3. Click **Edit Rule.**
4. Select new values for the rule parameters, as needed.
5. Click **Save.** Alternatively, click **Save As** to save the edited rule with a new name.

When creating or editing rules, the only characters that are allowed for naming them are the following:

- Letters (a-z and/or A-Z)
- Numbers and spaces
- Symbols (only restricted to): **%** _ and -

To export all rules to a text file:

1. Click **Dashboard > Rules.**
2. In the toolbar, click **Export.** Your rules are exported to a local text file called `monitor_breach_rules.properties.` and downloaded locally.

> **Caution:** Do not partially delete a rule from the exported breach rules file. The rules file to be uploaded should have all the properties for all the rules in the file. Before uploading a new breach rules file create a backup of the existing file.

To import a rule:

1. Click **Dashboard > Rules.**
2. In the toolbar, click **Import.** A new window will pop-up, click **Browse**, find the location of the file, select it, and click **Import.**

Global Settings

1. Click **Dashboard > Rules.**
2. In the toolbar, click **Global Settings.** The following settings are displayed: **SNMP Notifications**, **Email Notifications**, and **Audit Notifications.** These settings enable or disable notifications to be sent by ArcMC.

To enable (or disable) a rule:

1. Click **Dashboard > Rules.**
2. In the management panel, under **Monitoring Rules**, select the rule to enable or disable.
3. In the **Rule Name** column, click the rule name.
4. Under **Status**, toggle the status to **Enable** (or **Disable**).
5. Click **Save.**

To delete a rule:

1. Click **Dashboard > Rules.**
2. Under **Monitoring Rules**, select the rule you wish to delete.
3. Click **Delete.**
4. Click **OK** to confirm deletion.

Monitoring Rules Parameters

Monitoring rules are defined by rule parameters. The following table describes monitoring rules parameters and their valid values.

Monitoring Rules Parameters

Parameter	Description
Name	Name of the rule. (Max. length 50 characters)
Metric Type	Criterion being measured. For valid values of Metric Type, see the **Valid Values for Metric Type** table, below. Each metric type has a Value Type constraining the kind of value which may be assigned to it.
Product Type(s)	Managed product type (or types) to which the rule applies. These are automatically selected based on the Metric Type. For example, if you selected a metric type that applied only to hardware, such as Voltage, only products with hardware form factors would be available for selection. You can also deselect types to which to apply the rule, as applicable.

Monitoring Rules Parameters, continued

Parameter	Description
Specific Node Selector	Click **View/Choose**, and then select one or more specific nodes to which the rule applies. If none are chosen, then the rule applies to all nodes of the selected Product Types.
Severity	Breach severity. Valid values are Healthy, Warning, Critical and Fatal. Thresholds for each of these values are defined by the administrator.
Aggregation	Aggregation function applied to Metric Type data points. Valid values: • ANY: any value • AVG: average value (numeric values only) • MIN: minimum value (numeric values only) • MAX: maximum value (numeric values only) • SUM: addition of values (numeric values only)
Measurement	A comparison between two criteria. Valid values: • GREATER: One field is greater than the other • LESS: One field is less than the other • EQUAL: One field is equal to the other • NOT_EQUAL: Two fields are unequal
Value	Threshold value for comparison. Valid values are dependent on Metric Type. • Percentage: Number from 1-100 (with no %-sign). • Numeric: Numeric string. • Boolean: true/false (case-insensitive) • Literal Status: Status of the appliance component, and can be one of the following values: *Ok, Degraded, Rebuilding, Failed, Unavailable*.
Notify Me	Select one or more notification mechanisms for alerts about the rule (Email, SNMP, or Audit Forwarding).
Status	If **Enabled**, the rule will apply and produce alerts, as specified in **Notify Me.** (ArcMC rule presets are Disabled by default.)
Time Range	Evaluation interval, in hours and minutes. The total of hours and minutes must not exceed 168 hours (7 days).

Note: Compound rules (AND/OR) are not supported.

Valid Values for Metric Type

Value	Description	Value Type
Description	Brief description of the rule. (Max. length 300 characters.)	What kind of value this is.
For Connector Appliances or Loggers only		
CPU Usage	CPU usage, as a percentage.	Percentage
JVM Memory	Memory of Java Virtual Machine.	Numeric
Disk Read	Number of reads of the disk.	Numeric
Disk Write	Number of writes to the disk.	Numeric
All EPS In	Total Events Per Second in.	Numeric
All EPS Out	Total Events Per Second out.	Numeric
For Connectors only		
Events/Sec (SLC)	Events Per Second (EPS) in (Since Last Checked)	Numeric
EPS In	Events Per Second (EPS) in.	Numeric
EPS Out	Events Per Second (EPS) out.	Numeric
Events Processed	Number of events processed.	Numeric
Events Processed (SLC)	Events processed (Since Last Checked).	Numeric
FIPS Enabled	1= FIPS enabled, 0=FIPS disabled.	Boolean
Command Responses Processed	Number of command responses processed.	Numeric
Queue Drop Count	Queue drop count.	Numeric
Queue Rate (SLC)	Queue rate (Since Last Checked).	Numeric
Active Thread Count	Active thread count.	Numeric
For hardware form factor products only		
Fan	Hardware fan status.	Literal Status
Disk Space	Hardware disk space status. Disk space will be reported as "degraded" if storage reaches 75% of its capacity. Other statuses are not used.	Literal Status
Voltage	Hardware voltage status.	Literal Status
Current	Hardware current status.	Literal Status
Temperature	Hardware temperature status.	Literal Status
Power Supply	Hardware power supply status.	Literal Status

Valid Values for Metric Type, continued

Value	Description	Value Type
RAID Controller	RAID controller status.	Literal Status
RAID Battery	RAID battery status.	Literal Status
Hard Drive	Hard drive status.	Literal Status
For Loggers Only		
Storage Group Usage	Current storage group usage, in bytes.	Numeric
Storage Group Capacity	Current storage group capacity, in bytes.	Numeric
For Transformation Hubs Only		
Transformation Hub All Bytes In	All bytes received by the Transformation Hub cluster.	Numeric
Transformation Hub All Bytes Out	All bytes transmitted by the Transformation Hub cluster. Note that due to the replication of each topic, Bytes Out will always exceed Bytes In.	Numeric
Transformation Hub Disk Usage	Disk usage of Transformation Hub's individual nodes.	Numeric
Transformation Hub Memory Usage	Memory usage of Transformation Hub's individual nodes.	Numeric
Transformation Hub SP EPS	Count of events per second received by Transformation Hub's Stream Processor.	Numeric
Transformation Hub SP Error	Count of events per second wating to be processed received by Transformation Hub's Stream Processor which produced an error.	Numeric
Transformation Hub SP Lag	Count of events per second waiting to be received by Transformation Hub's Stream Processor.	Numeric

Rule Verification

It is possible to create syntactically valid rules that return confusing or meaningless alerts. For example, you could create a syntactically valid rule to trigger an alert if CPU usage is below 101%, but this rule would not return useful alerts (since it would alert you constantly).

Always verify your rules to ensure that they return meaningful values, to help you best detect problems and issues.

Note: Custom Polling Intervals: ArcSight Management Center uses three polling intervals (4 hours, 1 day, and 1 week) associated with metric data archive types across ArcSight products. These intervals can be adjusted for proper usage, if required.

It is strongly recommended that you adjust these intervals only if you fully understand the impact of the changes.

Polling intervals can be specified in the file `logger.properties` using a text editor.

- 4-hour data (minimum allowed interval 1 minute):

  `monitoring.data.poll.4hour.cron=10 0/3 * * * ?`

  This property indicates a poll at 3 minute intervals.
- 1-day data (minimum allowed interval 5 minutes):

  `monitoring.data.poll.1day.cron=15 0/10 * * * ?`

  This property indicates a poll at 10 minute intervals.
- 1-week data (minimum allowed interval 1 hour):

  `monitoring.data.poll.1week.cron=20 2 */2 * * ?`

  This property indicates a poll at 2 hour intervals.

After making the changes and saving the edited file, a server restart is required for the changes to take effect.

Custom Rules Examples

Shown here are examples of custom monitoring rules.

Example 1: Warning Breach

This example specifies the following Warning condition:

"Generate a Warning breach if the average CPU usage of any ArcMC in the past 30 minutes is greater than 70%."

Name: ArcMC Warning

Metric Type: CPU Usage

Product Type: ArcMCs

Severity: Warning

Aggregation: AVG

Measurement: GREATER

Value: 70

Timespan: 30 minutes

Example 2: Critical Breach

Example 2 specifies the following Critical condition:

"Generate a Critical breach if the Power Supply fails on any Logger Appliance in the past hour."

Name: *Logger Warning*

Metric Type: Power Supply

Product Type: Loggers

Severity: Critical

Aggregation: ANY

Measurement: EQUAL

Value: Failed

Timespan: 60 minutes

Device Rule Management

Device Rule Management involves creating, editing and deleting rules specifically for devices. The operation of creating, editing and deleting rules is different than what is done for other entities. Rules are created on the Device List page. The contents of the rule are the same as those of the exiting rule.

The Device List page is where you manage rules. This page has two tabs: Devices and Manage Rules.

Device Inactive Notification

When ArcMC detects an inactive device, (time out value can be defined by the customer on the Device UI page, default vale is set to 20 minutes), the internal defined device inactive rule is triggered, and an alert is sent out via snmp, email, and audit log.

There are two options for users who don't want to receive device inactive notifications:

1. Keep the device on "active" status: Review the connector's device event status and configure a proper interval value for Device Product time-out interval on **Dashboard > Monitoring Summary> Devices UI** page.
2. Contact support to disable device inactive notifications.

Managing Devices

About

From the Devices page you can add one or more devices to a new rule or add one or more devices to an existing rule.

The Lead Breach column describes the Lead Breach for a device. The Severity column describes the severity of a device. Severity is defined when creating a rule. The # of Rules column describes the number of rules applied to the devices.

Procedure

Location: Dashboard > Monitoring summary > Devices count indicator > Devices page

To add one or more devices to a new rule

1. Select the desired device or devices.
2. Click **Add New Rule**.
3. From the Add New Rule dialog, specify the necessary information.

   Device rules support "EPS out" and "Bytes out" measurements.

To add one or more devices to an existing rule

1. Select the desired device or devices.
2. Click **Add to Existing Rule**.
3. From the Add to Existing Rule dialog, specify the existing rule.

See also

- "Device Rule Management " on the previous page
- "Managing Device Rules" on the next page

Managing Device Rules

About

The Manage Rules page lists of all the rules and options: Disable, Enable, Delete and Edit an existing rule. The multi-selection option is available for Disable, Enable and Deleting the Rules. You can Edit one rule at a time.

A device that has stopped sending events will be marked as "Fatal" and there is no rule to change that. The timeout value for each device product is configurable and documented.

Procedure

Location: Dashboard > Monitoring summary > Devices count indicator > Manage Rules tab

1. Click **Manage Rules**.
2. From the Rules Details page, specify the desired management option.

See also

- "Device Rule Management " on page 771
- "Managing Devices" on page 771

Configuring Email Notifications

Email notifications will inform recipients about monitored nodes being down or out of communications.

> **Note:** Email alerts do not include issues with Connectors. However, containers may be the subject of email alerts.

Before configuring email notifications, ensure that values are specified for your SMTP settings under **Administration > System Admin > System > SMTP.** For more information on SMTP settings, see "SMTP" on page 957.

Once configured, email notifications must be configured for each of the notification rules you wish to trigger an alert.

To configure email notifications:

1. In a text editor, open the file `.../userdata/arcmc/logger.properties.` (If the file does not exist, you can create it in a text editor. When creating the file, ensure that it is owned by the non-root user.)

2. Add a new line with the new property named `monitoring.notification.emails` and a value equal to a comma-separated list of email addresses of all administrators you intend to receive notifications. For example, this value would send email alerts to address1@example.com and address2@example.com:

   ```
   monitoring.notification.emails=address1@example.com,
   address2@example.com
   ```

3. Save the modified `logger.properties` file.
4. Restart the ArcMC web process.
5. In the rules editor, open the notification rule you wish to trigger an email alert, and under **Notify Me,** select *Email*.

Example Email Notification

An example of the email sent to recipients is shown here.

`<URI>` refers to the URI of a problematic node.

NodeN is the hostname of a problematic node.

This information is found on the **Hosts** tab under Node Management.

```
Subject: <Email title>
The following nodes are either down or not reachable from ArcSight Management
Center:
```

`//Default/<URI>/<Node1>`

`//Default/<URI>/<Node2>`

Defining Email Notification Lists Using a CSV File

Email notifications lists can be enabled using a CSV file to create a customized notification broadcast.

To enable notifications using a CSV file:

1. In a text editor, open the file `.../userdata/arcmc/logger.properties.`
2. Add a new line with the new property named `monitoring.notification.emails.file` and a value equal to your intended CSV's fully qualified path and file name. This CSV file must reside in the directory `<ArcMC_INSTALL_DIR>/userdata/arcmc`. For example:

```
monitoring.notification.emails.file=/opt/arcmc/userdat/arcmc/notification
s/notification_emails.csv
```

```
monitoring.notification.emails.file=/opt/arcmc/userdat/arcmc/notification
s/section_1/notification_emails.csv
```

3. Create the CSV file at the location you specified in Step 2. When creating the file, ensure that it is owned by the non-root user, or the non-root user has at least read access.

> Without both the new property from Step 2 and the CSV file from Step 3, email notifications will not function. Ensure you configure both.

4. Use the CSV file to define the notification rules and the email addresses. The email list can be configured by device type, location name, and monitoring rule name.

   • The CSV file must be separated by commas (,), and the first line must correspond to the header:

```
Device Type, Location Name, Rule Name, Emails.
```

• Each line of the file is considered a notification rule. It can be configured by device type, location, and monitoring rule.

```
Connector, Location-1, EPS_OUT_Connector, address1@example.com
```

• If the notification rule applies for any Device Type, Location, or Rule the value must be (ANY).

```
Connector,(ANY),(ANY),address1@example.com / This email list is for the
Connector device type,
no matter the location or monitoring rule.
```

• When sending a notification, ArcMC checks that there is an email address assigned to the Device Type, Location, or Rule. If not, ArcMC will use the value of `monitoring.notification.emails` as the default email address. For example:

```
monitoring.notification.emails=admin@email.com
```

```
monitoring.notification.emails.file=/opt/arcmc/userdat/arcmc/notifications/no
tification_emails.csv
```

The possible device type values for managed products are: ArcMC, Connector, Logger, Transformation Hub.

• For the devices (Unmanaged products), the device type corresponds to the Device Product Name. For example: ArcSight, JUNOS.

• For the devices (Unmanaged product), the location name must be empty, since these devices do not belong to any location.

```
ArcSight, (ANY),address1@example.com / This email list is for the ArcSight
devices,
no matter the monitoring rule.
```

• The email value could be equal to list of semi-colon delimited email addresses, for example:

```
Connector, (ANY), (ANY), address1@example.com; address2@example.com
```

• Each notification rule (line) is evaluated independently, regardless of the order in the file. For example:

```
(ANY),(ANY),(ANY), all@mycompany.com / All alerts are sent to this email
address.

Logger,(ANY), (ANY), logger@mycompany.com / All alerts for any Logger are
sent to this email address.

Logger, Loc-a, (ANY), logger.loca@mycompany.com / All alerts for any Logger
in location Loc-a are sent to
this email address.

Logger, Loc-b, Rule Name 1, logger.locb.rule@mycompany.com / All alerts for
any Logger in location Loc-b for
Rule Name 1 are sent to this email.

Connector, (ANY), (ANY), connector@mycompany.com / All alerts for any
connector are sent to this email address.

Connector, Loc-a, (ANY), connector.loca@mycompany.com / All alerts for any
connector in location Loc-a are
sent to this email address.

Connector, Loc-b, Rule Name 1, connector.locb.rule@mycompany.com / All alerts
for any connector in location
Loc-b for Rule Name 1 are sent to this email address.
```

• ArcMC issues an alert when nodes are down or unreachable. To route these emails, a notification rule should be created, the reserved word (NODE) must be used instead of device type, and the rule name must be blank.

```
(NODE), location-a, node.location.a@email.com / If a node in the location-a
is down, an alert is sent to
this email address.
```

```
(NODE), location-b, node.location.b@email.com / If a node in the location-b
is down, an alert.
```

Note: The CSV entries "(ANY)" and "(NODE)" for Device Type or Location, respectively, are read as reserved keywords rather than user-configured values, which may result in unexpected behaviors.

• If there is no email list assigned to the device type, location or monitoring rule, the monitoring.notification.emails property is used as default.

5. Save the changes in the CSV file.

6. Restart the ArcMC web process.

7. In the rule editor, open the notification rule you wish to trigger an email alert, and under Notify Me, select Email.

Note: It is not necessary to restart the ArcMC web process when the CSV file is modified, since the changes are automatically detected.

Configuring SNMP Notifications

SNMP notifications will send SNMP traps about monitored nodes being down or out of communications.

To configure SNMP notifications on ArcMC appliance:

1. Under **Administration > System Admin > System > SNMP**, enable SNMP. Then, specify values for port, SNMP version, and other required settings for your SNMP environment.
2. In the rules editor, open the notification rule you wish to trigger an SNMP alert, and under **Notify Me,** select *SNMP*. Repeat for each rule you wish to trigger an SNMP alert.

Enabling SNMP on Software

Software ArcMC does not include UI controls for SNMP configuration. Instead, take these steps to configure Software ArcMC for SNMP notifications and monitoring.

To enable SNMP notifications on a software host:

1. Make sure following RPM packages are installed on the system: `net-snmp, net-snmp-utils, net-snmp-libs, lm_sensors-libs.`

2. Enable the SNMP service by entering: `chkconfig snmpd on`

3. Start the SNMP service by entering: `service snmpd start`

4. In a text editor, create a file `/opt/arcsight/userdata/platform/snmp.properties` with the following parameters, Items in angle brackets <> indicate you should substitute values appropriate for your own environment.

```
snmp.enabled=true
```

```
snmp.version=V3
```

```
snmp.port=161
```

```
snmp.v3.authprotocol=SHA
```

```
snmp.v3.authpassphrase=<password>
```

```
snmp.v3.privacyprotocol=AES128
```

```
snmp.v3.privacypassphrase=<password>
```

```
snmp.user=<SNMP username>
```

```
snmp.community=public
```

```
snmp.system.location=<SNMP location>
```

```
snmp.system.name=ArcMC Node 247
```

```
snmp.system.contact=<your support email address>
```

```
snmp.trap.enabled=true
```

```
snmp.trap.version=V3
```

```
snmp.trap.port=162
```

```
snmp.trap.nms=<IP address of NNMI>
```

```
snmp.trap.user=<SNMP trap user name>
```

```
snmp.trap.community=public
```

```
snmp.trap.v3.authprotocol=SHA
```

```
snmp.trap.v3.authpassphrase=<password>
```

```
snmp.trap.v3.privacyprotocol=AES128
```

```
snmp.trap.v3.privacypassphrase=<password>
```

---

5. Give the file permission: 644 and owner: arcsight.

6. Copy the file `ARCSIGHT-EVENT-MIB.txt` file from `$ARCSIGHT_HOME/current/arcsight/aps/conf/` to location `/usr/share/snmp/mibs`. Give the file permission: 644 and owner: root:root.

7. Run the script `arcsight_snmpconf` script as a root user, as follows:

```
<ArcSight_Home>/current/arcsight/aps/bin/arcsight_snmpconf <ArcSight_Home>
/userdata/platform/snmp.properties trap
```

8. Run the script a second time, as follows:

```
<ArcSight_Home>/current/arcsight/aps/bin/arcsight_snmpconf <ArcSight_Home>
/userdata/platform/snmp.properties poll
```

This script will setup `/etc/snmp/snmpd.conf` file and restart the SNMP service.

9. Restart SNMP services: `service snmpd restart`

> **Note:** To preserve the `SNMP V3 Trap oldEngineID` persistent in software ArcMC, set the `$ARCMC_HOME/userdata/platform/snmp_persist/snmpapp.conf` file to be immutable: `#chattr +i $file_path_of_snmpapp.conf`
> Follow the steps below to create the `snmpapp.conf` file if it does not exist in the snmp_persist folder:

a) In a text editor, create a file `<ARCSIGHT_HOME>/userdata/platform/snmp_persist/snmpapp.conf` with the following entry: `oldEngineID $VALUE`

$VALUE: copy the value from the `oldEngineID` entry to `/var/lib/net-snmp/snmpd.conf`
For example: `oldEngineID 0x80001f888011b5336c8d41895f00000000`

b) Give the file permission 600:
`chmod 600 <ARCSIGHT HOME>/userdata/platform/snmp_persist/snmpapp.conf`

c) Set the owner:
If arcmc is installed as root user: `# chown root:root <ARCSIGHT_HOME>/userdata/platform/snmp_persist/snmpapp.conf`

If arcmc is installed as arcsight user: `#chown arcsight:arcsight <ARCSIGHT_HOME>/userdata/platform/snmp_persist/snmpapp.conf`

d) Set immutable:

```
chattr +i <ARCSIGHT_HOME>/userdata/platform/snmp_persist/snmpapp.conf
```

10. In the rules editor, open the notification rule you wish to trigger an SNMP alert, and under **Notify Me,** select *SNMP*. Repeat for each rule you wish to trigger an SNMP alert.

Topology View

The Topology View displays your end-to-end data flow in browseable format. Shown are the logical relationships between network devices (event producers), Connectors, and their destinations in each of your ArcMC locations.

As your environment scales to thousands of source devices, you can use logical groupings (locations) to model subsystems, and datacenters can quickly trace issues and drill down on details.

To display the Topology View, click **Dashboard > Topology View.**

The left column highlights the current topology view. The available views are based on the locations defined in ArcMC.

Each of monitor icons represents a Device Product type, and the bubbles on the left of each monitor icon indicate the number of devices for each Device Product type.

The severity status of each item in the topology view is indicated by its color. Item status may be Healthy (green), Fatal (red), Critical (amber), Warning (yellow), or Unknown (gray).

The status indicates the severity as reported by the managed product. Hovering over the device product show more details of the severity status. Clicking on any of the severity levels opens the device details filtered by that product type and severity combination.

The **Devices** area shows any devices which are forwarding events in your network.

- To view the EPS (events per second) traffic to and from a device, mouse over the device.

The **Connectors** area shows Connectors in the current topology view, specific to the location.

- To view the EPS (events per second) traffic to and from a connector, and get an overview of the connector status, mouse over the connector. Also shown are name, Device Type, Status, Path, Rule Violation (if any), Version, and ArcMC Managed.
- To drill down and view the health of the connector in detail, including health history, click the connector.
- In some cases, such as immediately following adding a connector node, an unmanaged connector may be displayed. This will be replaced with the connector data within a few collection cycles as data from the new connector is collected.

- Connectors displayed with the symbol are included in a different location from the one currently selected for viewing.

> **Note:** Transformation Hub drill-down mode is ArcMC-location specific.

The **Destinations** area shows connector destinations.

- To drill down and view the health of an ArcMC-managed destination in detail, click the destination.

The Topology View refreshes automatically once per minute. (You can toggle automatic data refresh with the **Auto Refresh** control.) To refresh the view manually, click **Refresh** in the toolbar.

The **Export** button allows users to export the devices list, status, last reported, eps, event size, connector, and customer URI into a CSV file.

When exporting the devices list, users can choose between **Use stored data** and **Real time device query** information. These options are displayed from a drop-down after clicking the **Export** button.

> **Note:** The **Real time device query** option might take some time to be completed.

You can also toggle the display of legends for the graphic with the **Legends** control.

Click **Deployment View** to show your environment's Deployment View.

> **Note:** If any are present, unmanaged connectors (or other nodes) in your network are noted as such in the Topology View. ArcMC will have no visibility into unmanaged connectors, nor any visibility of traffic from those nodes. Various scenarios for such views, and the results of each scenario, are detailed here. To get the most complete and accurate picture of your network, you are strongly encouraged to use ArcMC to manage all connectors which are part of your logical topology.

Deployment View

The Deployment View shows the physical relationships between network devices (event producers), connectors, their hosts, and their destinations in each of your ArcMC locations.

To display the Deployment View, click **Dashboard > Deployment View.**

The left column highlights the current deployment view. The available views are based on the physical hosts.

Each of the monitor icons represents a Device Product type, and the bubbles on the left of each monitor icon indicate the number of devices for each Device Product type.

The severity status of each item in the topology view is indicated by its color. Item status may be Healthy (green), Fatal (red), Critical (amber), Warning (yellow), or Unknown (gray).

The status indicates the severity as reported by the managed product. Hovering over the device product shows more details of the severity status. Clicking on any of the severity levels opens the device details filtered by that product type and severity combination.

The **Devices** area shows any devices which are forwarding events in your network.

- To view the EPS (events per second) traffic to and from a device, mouse over the device.

  The **Connectors** area shows Connectors in the current topology view.
- To view the EPS (events per second) traffic to and from a connector, and get an overview of the connector status, mouse over the connector. Also shown are name, Device Type, Status, Path, Rule Violation (if any) and ArcMC Managed.
- To drill down and view the health of the connector in detail, including health history, click the connector.
- In some cases, such as immediately after adding a connector node, an unmanaged connector may be displayed. This will be replaced with the connector data within a few collection cycles as data from the new connector is collected.
- Connectors displayed with the symbol are included in a different location from the one currently selected for viewing.

  The **Destinations** area shows connector destinations.
- To drill down and view the health of an ArcMC-managed destination in detail, click the destination.

The Topology View refreshes automatically once per minute. (You can toggle automatic data refresh with the **Auto Refresh** control.) To refresh the view manually, click **Refresh** in the toolbar.

The **Export** button allows users to export the devices list, status, last reported, eps, event size, connector, and customer URI into a CSV file.

When exporting the devices list, users can choose between **Use stored data** and **Real time device query** information. These options are displayed from a drop-down after clicking the **Export** button.

Note: The **Real time device query** option might take some time to be completed.

You can also toggle the display of legends for the graphic with the **Legends** control.

Click **Topology View** to show the topological relationships in your environment.

Prerequisites for Instant Connector Deployment

The following are prerequisites for Instant Connector Deployment.

- You must set up one or more deployment templates.
- Instant Connector Deployment is supported for accounts using SSH key authentication, but not supported for SSH with passphase authentication. To enable SSH key authentication, the SSH key needs to be set up between a non-root user of ArcMC and a user of the remote host that will be used for deployment.
- In addition, it is strongly suggested you consult the Configuration Guide for the connector you plan to deploy before deployment, to understand any special considerations or features of the connector being installed.
- For more information regarding Connector destinations, please see the Smart Connectors User's Guide.
- The below prerequisites are not present by default on Linux 8.x, unlike in previous Linux versions (e.g. Linux 6.x and 7.x). Perform the following steps for RHEL 8.1 on the host where the ArcMC is or will be installed, and in the target Linux host (the VM where the Connector will be deployed):

  a. Install python2:

     For RHEL 7.x:
     ```
     sudo yum install -y python2
     ```

     For RHEL 8.x:
     ```
     sudo dnf install -y python2
     ```

  b. Create a symlink:

     ```
     sudo ln -s /usr/bin/python2 /usr/bin/python
     ```

  c. Install libselinux-python package:

     For RHEL 7.x:
     ```
     sudo yum install -y libselinux-python
     ```

     For RHEL 8.x:
     ```
     sudo dnf install -y libselinux-python
     ```

     > **Note:** If the `yum/dnf` command fails when installing `libselinux-python` on RHEL, follow the steps below:
     > - Download `libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm`
     > - Install the package:
     > `rpm -i libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm`

Additional Requirements For Windows Platforms

The following additional items are required for Instant Connector Deployment on Windows platforms.

- Only the local admin account is supported for deployment.
- The following preparatory steps are required when deploying on a Windows VM.

1. Enable PowerShell 4.0 or later.

https://www.microsoft.com/en-us/download/details.aspx?id=40855

2. Enable and configure PowerShell Remoting, with CredSSP authentication.

- Download the "ConfigureRemotingForAnsible.ps1" file:
  - https://github.com/ansible/ansible/blob/devel/examples/scripts/ConfigureRemotingForAnsible.ps1
- Open Power Shell as Administrator and run the following command:
  - `ConfigureRemotingForAnsible.ps1 -EnableCredSSP`

3. Enable TLS 1.2.

Instant Connector Deployment

Instant Connector Deployment enables rapid installation of connectors where you need them in your environment. You perform Instant Connector Deployment right from the Deployment View.

Before proceeding, ensure you have met all the prerequisites for performing Instant Connector Deployment.

To instantly deploy a connector:

1. Click **Dashboard > Deployment View.**
2. In the **Connectors** column label, click **+**, then select **Add Connector.**
3. On the **Add Connector** dialog, specify values for the connector to be added. Any fields marked with an asterisk (*) are required. Note that your selected deployment template may populate some fields automatically, but you may overwrite the values in these fields, if needed, for a particular deployment. **Exception:** you may only use the latest version of the connector you have uploaded to the repository when you set up deployment templates. You can add multiple destinations for each connector if needed.
4. To add multiple hosts to the Host list, in the Host drop-down, click **Add Host**, and then select or specify the name of each host.

- **ArcSight SecureData Add-On Enablement:** To enable the ArcSight SecureData Add-on during deployment, under **Global Fields**, set **Format Preserving Encryption** to *Enabled*. For more information on enabling the SecureData Add-On, see "SecureData Encryption " on page 792.

4. To add multiple connectors of the same type, click **Clone**. Then specify the information unique to the new connector. When deploying multiple connectors, if any specified parameters (such as port number) are invalid, the deployment of all connectors in the job will fail.
4. Click **Install.** The Connector is deployed. Alternatively, click **Add** to add more connectors to the deployment job.

Note: Instant Connector Deployment is not supported from RHEL 6.9 to a remote Windows host.

You can track and manage deployment jobs and issues using the Job Manager.

Note: If you later connect to a host where Connectors were installed through Instant Deployment, and run the Connector setup wizard from the command line, you should run agent setup from `$ARCSIGHT_HOME/current/bin` by setting the mode with option, `-i`, such as: `./runagentsetup.sh -i console` or `./runagentsetup.sh -i swing`, where options are swing, console, silent, and so on. For more information on options, see the **Smart Connectors User's Guide** in ArcSight SmartConnectors 24.2 documentation.

Deployment on Linux Platform Using Non-root User

Follow these steps to install a Connector using non-root user through instant deployment feature.

Step 1

Option 1: Provide blanket sudo rights to non-root users:

1. Edit the sudoers file on the remote host where the Connector will be deployed:

- Open the sudoers file:

```
# visudo
```

- Locate the following lines in the file:

```
## Allow root to run any commands anywhere root ALL=(ALL) ALL
```

2. Provide blanket sudo rights to non-root user below the previously mentioned line.

```
<non-root-user> ALL= (ALL) NOPASSWD:ALL
```

3. Save the file.
4. Specify this non-root user and password in the instant deployment job.

Option 2: Provide rights to non-root user to execute specific set of commands as mentioned below:

1. Edit the sudoers file on the remote host where the Connector will be deployed:

- Open the sudoers file:

```
# visudo
```

- Locate the following lines in the file:

```
## Allow root to run any commands anywhere root ALL=(ALL) ALL
```

2. Add special rights to the non-root user below the previously mentioned line:

```
<non-root-user> ALL=(ALL) NOPASSWD: /bin/chown root\:root <connector_install_dir>/current/config/agent/arc_<service_internal_name>, /bin/mv <connector_install_dir>/current/config/agent/arc_<service_internal_name> /etc/init.d/, /bin/chmod 755 /etc/init.d/arc_<service_internal_name>, /bin/rm -rf /etc/init.d/arc_<service_internal_name>
```

Note:`<connector_install_dir>` and `<service_internal_name>` should match exactly what the user will be entering in the instant deployment job. Provide these 4 commands in the sudoers for every Connector installation that will be done from ArcMC through this non-root user.

3. Save the file.
4. Specify this non-root user and password in the instant deployment job.

Step 2

Option 1: Use the Home user path.

The folder will be automatically created.

Option 2: Use an alternative path.

For non-root installation, users need to create the folder:

```
mkdir <path to folder>
```

Grant full permissions:

```
chmod 777 <path to folder>
```

If the SSH certificate changes...

If the connector VM is redeployed, its SSH certificate will change and will no longer be able to use Instant Connector Deployment to deploy connectors to the VM. In this case, take the following steps to re-enable Instant Connector Deployment to the re-deployed VM.

1. Connect to the ArcMC's VM.
2. Change to the directory `/home/<non root user>/.ssh`
3. Open the file `known_hosts`.
4. Delete the line with the IP or hostname of the Connector's VM.
5. Save the file.

Deploying a Connector in Transformation Hub (CTH) (Standalone ArcMC)

> The CTH and Collectors were deprecated as of SmartConnector 8.4 release. The deployment of CTH and Collectors is now removed in SmartConnector CE 24.2 release. There will be limited support for customers already using CTH and Collectors, until the end of support date for the ArcSight SmartConnector CE 24.1 release, which is Jan 31, 2027.

A Connector in Transformation Hub (CTH) moves the security event normalization, categorization, and enrichment of connectors processing to the Docker containers environment of Transformation Hub, while reducing the work done by the Collector.

Transformation Hub can have a maximum of 50 CTHs.

> **Note:** CTHs cannot be configured with SecureData encryption. By default, CTH is set as TLS + CA.

To update the CTH port range:

1. Open `logger.properties` for editing.

   Create the file if it does not exist.

   ```
   /opt/arcmc/userdata/arcmc/logger.properties
   ```

   ```
   chown <non-root user>:<non-root user> logger.properties
   ```

   ```
   chmod 660 logger.properties
   ```

2. Add the following information to `logger.properties`.

```
# ==============================================================
```

```
# CTH port range
```

```
# ==============================================================
```

```
configuration.cth.end.port=39050
```

For Transformation Hub 3.3 and later use:

```
configuration.cth.end.port.post.th.32=32150
```

3. Restart the web process.

To deploy a CTH:

> **Note:** To use the Global ID feature, Generator ID Manager has to be enabled in the ArcMC so that Generator ID can be set on the CTH.

1. Click **Dashboard > Deployment View.**
2. In the **Transformation Hub** column, click the managed Transformation Hub, then click the **+** icon.
3. On the **Deploy CTH** dialog, in **CTH Name**, specify a name for the CTH.

   The name must be smaller than 256 characters.
4. Under Acknowledgment mode, click the down arrow, then select the Acknowledgment mode for this CTH. (none/leader/all)

   The mode you select affects the safety of stored events in case of immediate system failure.

Acknowledgment Mode	Description
none	Acknowledgment off The producer will not wait for any acknowledgment from the server. The record will be immediately added to the socket buffer and considered sent. No guarantee can be made that the server has received the record in this case, and the retries configuration will not take effect (as the client won't generally know of any failures). The offset given back for each record will always be set to -1.
leader	Leader mode on The leader will write the record to its local log but will respond without awaiting full acknowledgment from all followers. In this case, if the leader fails immediately after acknowledging the record but before the followers have replicated it, the record will be lost.
all	All acknowledgments on The leader will wait for the full set of in-sync replicas to acknowledge the record; guaranteeing that the record will not be lost if at least one in-sync replica remains alive (strongest available guarantee). This is equivalent to the `acks=-1` setting.

5. Under **Destination Topics**, click the down arrow, then select one or more destination topics (CEF, Avro, or binary) for the CTH.
6. Select the corresponding ESM version. This is required for CTH to support Global ID when sending events to ESM 7.2
7. Click **Deploy**.

   Note: Please allow a few minutes after deploying or updating the CTH for the new values to be displayed.

   The CTH deployment job status can be viewed in Job Manager.

Once deployed, the CTH displays in Node Management on the Connectors tab, and in the Topology and Deployment View drill-down under the source topic.

Note: Destination topics must always be grouped the same for multiple CTHs. For example, if a CTH is sending events to both th-cef and th-esm topics, then any other CTH that sends events to one of these topics must also send events to the other topic, or events will be duplicated.

Editing a CTH

The CTH and Collectors were deprecated as of SmartConnector 8.4 release. The deployment of CTH and Collectors is now removed in SmartConnector CE 24.2 release. There will be limited support for customers already using CTH and Collectors, until the end of support date for the ArcSight SmartConnector CE 24.1 release, which is Jan 31, 2027.

To edit a CTH:

1. Click **Dashboard > Deployment View.**
2. In the **Transformation Hub** column, click the managed Transformation Hub, and then click the edit (pencil) icon.
3. On the **CTH Parameters** dialog, modify the name or destination topics, as needed.
4. Click **Redeploy**. The CTH is re-deployed. The job progress can be viewed in Job Manager.

Undeploying CTHs

> The CTH and Collectors were deprecated as of SmartConnector 8.4 release. The deployment of CTH and Collectors is now removed in SmartConnector CE 24.2 release. There will be limited support for customers already using CTH and Collectors, until the end of support date for the ArcSight SmartConnector CE 24.1 release, which is Jan 31, 2027.

To undeploy one or more CTHs:

1. Click **Dashboard > Deployment View.**
2. Click on the Transformation Hub box to drill down.
3. Click the edit (pencil) icon.
4. On the **CTH Parameters** dialog, click **X** next to any CTHs to be undeployed.
5. Click **Redeploy**. The job progress can be viewed in Job Manager.

Deploying Collectors

This section provides information about deploying Collectors, Non-TLS, TLS, and FIPS deployment.

1. Under **Dashboard > Deployment View**, click the icon next to the **Collectors** label and click **Add Collector.**
2. From the **Add Collector** window, under add collector details select the collector template.

Non-TLS Collectors Deployment

For Non-TLS Collector deployment:

1. Follow the steps in "Deploying Collectors" above section, and select the Syslog Daemon Collector template.
2. Scroll down to **Destination > Destination Template** and select the TH Collector Template.

3. Under **Kafka Broker Host(s):Port(s)**, confirm that port number is 9092, otherwise, change it accordingly.
4. Set the **Kafka Broker on SSL/TLS** flag to false.
5. Click **Install**.

TLS Collectors Deployment

For TLS Collector deployment:

1. Follow the steps in "Deploying Collectors" on the previous page section, and select the Syslog NG Daemon Collector template.
2. Scroll down to **Destination > Destination Template** and select the TH Collector Template.
3. Under **Kafka Broker Host(s):Port(s)** confirm that port number is 9093, otherwise, change it accordingly.
4. Set the **Kafka Broker on SSL/TLS** flag to true.
5. Click **Install**.

FIPS Collectors Deployment

FIPS can be enabled on Collectors either during the deployment of the Collector or while creating the Collector Configuration Template.

1. Follow the steps in "Deploying Collectors" on the previous page section.
2. From the **Add Collector** window, under add collector details select the collector template. Scroll down to the **Global Fields** section, and select **Enabled** from the **Enable FIPS mode** drop-down.
3. Replicate steps 2 through 4 in the "TLS Collectors Deployment" above section.
4. Click **Install**.

Post Deployment Collector Property Update

FIPS

1. Go to **Configuration Management > Bulk Operations.**
2. Click on the **Collector** tab, select one of the Collectors from the Manage Collectors table, and click **Properties.**
3. In the **Collector Property Update** window, click the icon next to **Property List** and search for `fips.enable`.
4. Click **Edit** and set the Value to `true`.

> **Note:** When setting the `fips.enable` property to true, you need to modify the property's `agents[0].destination[0].params` bootstraphosts parameter port value to 9093, as well as change the usessl parameter (SSL/TLS) value to `true`.

5. Click **Save**.

Non-TLS and TLS

For Non-TLS and TLS the process remains the same for steps 1 to 2 listed in "Post Deployment Collector Property Update" on the previous page In the **Collector Property Update** window, click the icon next to Property List and search for the `agents[0].destination[0].params` property. See the table below for the correct values.

Property	Parameter	Non-TLS	TLS
agents[0].destination[0].params	bootstraphosts	port value: 9092	port value: 9093
agents[0].destination[0].params	usessl	false	true

SecureData Encryption

To enable SecureData encryption, you must provide the SecureData server details in the Deployment Template for a connector.

> **Note:** CTHs cannot be configured with SecureData encryption.

If any proxy settings are required, these must also be provided in the Deployment Template.

To explicitly specify that no proxy be used for the SecureData client, no parameters are needed in the Deployment Template. In addition, edit the file `/etc/profile.d/proxy.sh` (or its equivalent on Windows VM) and add/edit the line "export no_proxy and export NO_PROXY" with your SecureData server details.

If your SecureData client needs a certificate, then upload the valid certificate to ArcMC's cacerts repository when creating the deployment template.

After all settings are configured, and a connection is ensured from the connector host to the SecureData server, you can deploy the connector using the Instant Connector Deployment process.

> **Warning:** SecureData settings may only be updated once. Once encryption is turned on, it may not be turned off. Make sure you wish to use encryption before activating it.

Managing Nodes

A *node* is a networked ArcSight product that can be centrally managed through ArcSight Management Center. Each node is associated with a single networked host which has been assigned a hostname, an IP address, or both.

Node types can include any of the following ArcSight products:

Management of Core ArcMC is not supported.

- Connector Appliances or Software Connector Appliances
- Logger Appliances or Software Loggers
- Containers or connectors
- Other ArcSight Management Centers, either software or Connector Hosting Appliances
- Transformation Hub

A single host, such as a single deployed Transformation Hub, can comprise multiple nodes for management purposes. In addition, a node can be in a parent or child relationship with other nodes.

You can perform any of the following node management tasks:

- View managed nodes by location, by host, or by node type.
- Add, view, edit, and delete locations for hosts.
- Add nodes from a host, import hosts from a CSV file, view and delete hosts, view all hosts in a location, update software on hosts, move hosts to different locations, and scan hosts for new connectors or containers.

For more information on adding hosts, see "About Adding a Host" on page 813.

The following topics are discussed here.

Node Management

To manage nodes, on the menu bar, click **Node Management > View All Nodes.** The Node Management UI displays. The Node Management UI comprises two panels:

- The left side displays the navigation tree.
- The right side displays the management panel, enabling you to perform management operations on items selected in the navigation tree.

The Navigation Tree

The navigation tree organizes managed nodes into a hierarchy, and comprises the following:

- **System**: Displays the entire set of nodes managed by ArcMC.
- **Location**: Individual locations are displayed under **System**, listed in the order in which they were added. Locations are logical groupings you can use to organize a list of hosts. For more information, see "Locations" on page 811.
- **Host**: Each location branch shows all hosts assigned to that location, listed by hostname, in the order in which they were added. For more information, see "Hosts" on page 813.
- *Node Types*: Each host branch shows all managed nodes associated with that host. A node can be any of the following types:
- **Connector Appliance or Software Connector Appliance:** Each Connector Appliance (hardware or software) is shown as a separate node.
- **Logger Appliance or Software Logger:** Each Logger (hardware or software) is shown as a separate node.
- **ArcSight Management Center:** Each ArcSight Management Center (hardware or software) is shown as a separate node.
- **Container:** If the host includes any containers, each is shown as a node.
- **Connector**: If a container node contains a connector, the connector is shown under the container node in which it is contained.
- **Transformation Hub:** A managed Transformation Hub is shown as a node.

Since items in the tree are organized hierarchically, each item in the tree includes all branches displayed below it. For example, a **Location** branch includes all hosts assigned to that location. Click the wedge icon to toggle the view of any branch and any items included in the branch.

The Management Panel

Select an item in the navigation tree to display its details on one of the tabs in the central management panel. For example, to display the details of a host shown in the navigation tree, select the host in the tree. The management panel to the right of the tree will display details and controls pertaining to selected host.

Management Tabs

The tabs displayed in the management panel depend on the type of item selected in the navigation tree. The management tabs displayed will show detailed information associated with the selected item, depending on its position in the hierarchy.

Selected Item Type in Navigation Tree	Tabs Shown in Management Panel
System	Locations, Hosts, Containers, Connectors, ConApps, Loggers, ArcMCs, TH Nodes
Location	Hosts, Containers, Connectors, ConApps, Loggers, ArcMCs, TH Nodes
Host	Containers, Connectors,ConApps, Loggers, ArcMCs, TH Nodes
Node	Connectors, ConApps, Loggers, ArcMCs, TH Nodes

For example, if you selected a location item from the navigation tree, the **Hosts, Containers**, **Connectors, ConApps**, **Loggers ArcMCs** and **TH Nodes** tabs would be shown. Each tab would display the items of the named type associated with the selected location, including details on those items.

Working with Items in the Management Panel

Selecting One or Multiple Items: To select an item from a list of items in the management panel, click the item. Use Shift+Click to select multiple adjacent list items, or Ctrl+Click to select multiple non-adjacent items.

Column Settings: Click the gear icon to change column settings:

- **Sorting:** To sort data by a column, select either **Sort Ascending** or **Sort Descending**.
- **Column Display:** To change the columns displayed in a table, select **Columns**. Then toggle one or more columns to display.
- **Filter:** To filter a list of items, select **Filters**. Then enter one or more filter criteria to display items matching those criteria.

Refreshing a List: To refresh the data in a list, click **Refresh** in the upper right corner.

Tab Controls

These controls are commonly displayed on all tabs in the management panel:

- **Toolbar Buttons:** Toolbar buttons enable operations related to the items on the tab.
- **Items Table:** Items corresponding to the tab header are displayed in a table. For example, locations are listed in tabular format on the Locations tab.
- **Bulk Operations Buttons:** On most tabs, bulk operations buttons enable you to perform operations on one or more items. Choose one or multiple items in the list, and then click the button to perform the indicated operation. For example, to delete multiple items such as hosts, select one or more hosts on the **Hosts** tab, and then click **Delete**. The selected hosts would be deleted.

In addition, each tab may have controls individual to that item type. For example, the **Connectors** tab includes controls related to the management of connectors (see "Managing Connectors" on page 860).

The Locations Tab

The **Locations** tab displays all locations defined in ArcMC. The **Locations** tab includes these buttons:

Add Location	Adds a new location. For more information, see "Adding a Location" on page 812
Delete	Deletes one or more selected locations from ArcMC. For more information, see "Deleting a Location" on page 813

The **Locations** table displays these parameters for each location.

- **Name:** Location name.
- **Number of Hosts:** Number of hosts assigned to the location.
- **Action:** Drop-down includes a control for editing a location. For more information on editing a location, see "Editing a Location" on page 812.

For more information on managing locations, see "Locations" on page 811.

The Hosts Tab

The **Hosts** tab displays all hosts associated with the location selected in the navigation tree. The **Hosts** tab includes these buttons:

Add Host	Adds a host. Available on the **Hosts** tab when a location is selected in the navigation tree. For more information on adding a host, see "About Adding a Host" on page 813.
Move	Moves selected hosts to a new location. For more information, see "Moving a Host to a Different Location" on page 945
Update Agent	Updates the ArcMC Agent on selected hosts. If the Agent is not currently installed, this button will install the Agent. For more information, see "Updating (or Installing) the ArcMC Agent " on page 799.
Delete	Deletes selected hosts from ArcMC. For more information, see "Deleting a Host" on page 945

The **Hosts** table displays these parameters for each host:

- **Hostname:** Fully qualified domain name (FQDN) or the IP address of the host. The hostname must match the hostname in the host's SSL certificate. If IP address was used to add the host, then the certificate will match the IP address used.

- **Path:** Path to the host.
- **Agent Version:** Version number of the ArcMC Agent running on the host.
- **Issues:** Status of any issues associated with the host. Possible indicators include:
  - *None:* No issues are associated with the host.
  - *Internet connection Not Present:* The host is currently not reachable by internet connection. Displayed when ArcMC is not able to connect to the Marketplace for retrieving parser upgrade versions. If the user environment needs a proxy server for an internet connection, configure the logger.properties file. If the user environment is an appliance, save the DNS settings on the **System Admin > Network** page.
  - *Valid Marketplace Certificate Not Found in ArcMC*: Displayed when the Marketplace certificate does not match the one found in ArcMC's trust store.
  - *Host Certificate Mismatch:* The hostname does not match the hostname in the SSL certificate. For instructions on downloading and importing certificates for the host, see "Downloading and Importing Host Certificates" on page 943. If this issue is displayed for the localhost, and the certificate cannot be downloaded, please restart the web service on the localhost.
  - *ArcMC Agent Out of Date:* The host's Agent version cannot be upgraded from the managing ArcMC, or the ArcMC cannot communicate with the ArcMC Agent on the managed node. You may need to manually install the ArcMC Agent. For requirements and instructions, see "Installing the ArcMC Agent" on page 802.
  - *ArcMC Agent Stopped:* The Agent process on the host has been stopped.
  - *ArcMC Agent Upgrade Recommended:* The host's Agent version is older than the one on the managing ArcMC. An Agent upgrade is recommended.
  - *ArcMC Agent Uninstalled:* The Agent on the host has been uninstalled.
  - *ArcMC Agent Down:* The Agent on the host is not running.
  - *Update the authentication credentials on the localhost, then install the ArcMC Agent:* For a localhost added for remote management, authentication credentials need to be updated to ensure authentication, then the ArcMC Agent needs to be installed to enable management. Take both of these steps to correct this issue.
  - *Error in REST Authentication*: The Transformation Hub node lacks the ArcMC certificate, ArcMC session ID, or ArcMC URL and port. To resolve this issue:
    - Make sure the user has the permission rights for the Transformation Hub operations.
    - Make sure the valid ArcMC certificate (with FQDN and .crt extension) is present in the Transformation Hub's location: /opt/arcsight/k8s-hostpath-volume/th/arcmccerts

    - Make sure that the ArcMC URL is updated with correct FQDN and port in ArcSight Installer > Transformation Hub Configuration > ArcMC_Monitoring field.
    - Note that each time the user replaces the ArcMC certificate to the TH's location, the TH's webservice pod has to be restarted for the new certificate to be read and updated in the trust store.
- **Model**: If the host is an appliance, this shows the ArcSight model number of the appliance. If the host is not an appliance, the label *Software* is shown.
- **Type**: Type of installation, either ArcMC Appliance or Software.
- **Version:**Version number of the software on the host.
- **Action:** Drop-down shows controls for executing host management tasks, which include:
    - Scanning a host
    - Downloading certificate details
    - Updating host credentials

For more information on host management, see "Hosts" on page 813.

Updating (or Installing) the ArcMC Agent

Hosts running an outdated version of the ArcMC Agent can be quickly upgraded to the latest version.

Agent installation or upgrade is supported on all versions of ArcMC Appliance, Connector Appliance (hardware) and Logger Appliance, Software Logger 6.0 or later, and software ArcMC 2.1 or later.

> **Tip:** Check the version of the Agent on each host by clicking the **Hosts** tab and reviewing the **Agent Version** column.

To upgrade or install the Agent on one or more hosts:

1. Click **Node Management**.
2. In the navigation tree, click **System**, and then click the **Hosts** tab.
3. Select one or more hosts to update.
4. Click **Update Agent**. The Agent Upgrade wizard launches. Follow the prompts to complete the Agent Upgrade wizard.

Modifying logger.properties

To enable or modify some functionality, you may need to edit the file <install_dir>/userdata/arcmc/logger.properties with additional parameters in any text editor.

General Editing Procedure

If <install_dir>/userdata/arcmc/logger.properties does not exist, then create one in a text editor. This file must be owned by a non-root user. For an ArcMC appliance, use the 'arcsight' user, and for software ArcMC, use the non-root account used to install the ArcMC.

The logger.properties file may not be readable and writable by all users. Apply the following commands to the file.

```
chown <non-root user>:<non-root user> logger.properties
```

```
chmod 660 logger.properties
```

Finally, *restart the web process* after making any edits to logger.properties.

Uploading Files Larger Than 100 MB under Repository

Modify the <install_dir>/userdata/arcmc/logger.properties by adding:

```
connectorappliance.file.maxupload=400
```

After adding the previous line, owner and permissions need to be changed:

```
chown <non-root user>:<non-root user> logger.properties
```

```
chmod 660 logger.properties
```

Finally, restart the web process after making any edits to logger.properties.

For Parser Upgrades Through a Proxy Server

If performing parser upgrades, and your environment connects to the Marketplace through a proxy server, you will need to modify the <install_dir>/userdata/arcmc/logger.properties file with the proxy details.

```
proxy.server=<server address>
```

```
proxy.port=<server port>
```

```
#Enter the proxy server credentials if the proxy server needs authentication
```

```
proxy.username=<username>
```

```
proxy.password=<password>
```

For the Number of Parser Upgrade Versions Displayed

You can control the number of parser upgrade versions displayed in the parser upgrade drop-down list. In `logger.properties`, set the parameter

```
marketplace.parser.update.latest.versions.count = <number of parser upgrade
versions to be retrieved from Marketplace>
```

To Disable the Marketplace Connection

To disable ArcMC's Marketplace connection, in `logger.properties`, set the parameter

```
marketplace.enable=false
```

If set to false, you will not be able to see the available parser upgrade versions from the Marketplace. In addition, the containers under **Node Management > Containers** tab, will not display the *Parser Out of Date* status in the **Parser Version** column.

Installing the ArcMC Agent

The ArcMC Agent runs on managed hosts and enables their management by ArcMC. Whether you need to install the ArcMC on a managed host depends on the host's form factor, which is summarized in the table and explained in detail below.

Host Type	ArcMC Agent Required?	Agent Installation
ArcMC, Logger, or Connector Appliance hardware form factor (all versions)	Yes	Automatically performed when adding host.
Software Connector Appliance (all versions)	Yes	Manual installation required; perform before adding host.
Software Logger (before version 6.0)	Yes	Manual installation required; perform before adding host.
Software Logger (version 6.0 or later)	Yes	Automatically performed when adding host.
Software ArcMC (before version 2.1)	Yes	Manual installation required; perform before adding host.
Software ArcMC (version 2.1 or later)	Yes	Automatically performed when adding host.
Connector (any)	No	None. ArcMC Agent is not required.
Transformation Hub	No	None. ArcMC Agent is not required.

Automatic Installation

The ArcMC Agent is *automatically* installed when adding any of the following host types to ArcMC:

- Any hardware appliance (ArcSight Management Center Appliance, Connector Appliance, or Logger Appliance)
- Software Logger 6.0 or later
- Software ArcMC 2.1 or later

As part of the Add Host process, ArcMC automatically pushes the ArcMC Agent installer to the added host, installs the Agent, then starts the service. The host is then ready to manage in ArcSight Management Center. You will not need to take any manual installation steps. For more information about the Add Host process, see "About Adding a Host" on page 813.

> **Note:** Perl is required for the automatic installation of the ArcMC Agent. Ensure that Perl is installed on the host prior to attempting to add the host to ArcMC.

Manual Installation

You must perform a *manual* installation of the ArcMC Agent on any of these host types *prior to* adding them to ArcMC for management:

- Software ArcSight Management Center (before version 2.1)
- Software Logger (before version 6.0)
- Software Connector Appliance (all versions)

An ArcMC used to manage products must have an Agent installed with the same version number as the ArcMC. For example, if your ArcMC 3.1.0 will be used to manage products, then the ArcMC Agent running on that ArcMC must also be version 3.1.0.

To manually install the ArcMC Agent:

1. In the directory to where you transferred the installer, run these 2 commands:
   - `chmod +x ArcSight-ArcMCAgent-.<agent_installer_build_number>.0.bin`
   - `./ArcSight-ArcMCAgent-.<agent_installer_build_number>.0.bin LAX_VM <install_dir>/current/local/jre/bin/java`

     where `<agent_installer_build_number>`is the build number of the latest installer and `<install_dir>` is the installation directory of the software product.

The installation wizard starts.

2. Review the dialog box, then click **Next.** The required installation path is the install directory (that is, the same directory where Software Connector Appliance or Software Logger is installed).
3. Follow the prompts to complete the installation. The ArcMC Agent is automatically started upon completion of the installation process.

   > **Note:** If the ArcMC Agent fails to install on the localhost, localhost management will not be enabled. To verify correct installation of the Agent, check on the **Hosts** tab under **Issues**. Follow the instructions shown in the tooltip to install the Agent properly and resolve any issues shown.

Connectors and Transformation Hub

Connectors and Transformation Hub do not require the installation of the ArcMC Agent in order to be managed by ArcMC.

The Containers Tab

The **Containers** tab displays all containers associated with the item selected in the navigation tree. For example, if you selected a location in the tree, since locations include hosts, the **Containers** tab would display all containers associated with all hosts in the selected location. The **Containers** tab includes these buttons:

Properties	This operation previously performed on this tab, is now performed on the new **Bulk Operations** page.
Certificates	Manage certificates on selected containers. For more information, see "Managing Certificates on a Container" on page 855.
FIPS	Enable or disable FIPS on selected containers. For more information, see "Enabling FIPS on a Container" on page 852.
Upgrade	Upgrades all connectors in selected containers. For more information, see "Upgrading All Connectors in a Container" on page 849.
Credentials	Manage credentials on selected containers. For more information, see "Changing Container Credentials" on page 848.
Logs	Manage logs on selected containers. For more information, see "Viewing Container Logs" on page 851.
Restart	Restart all connectors in selected containers. For more information, see "Restarting a Container " on page 851.
Delete	Deletes the selected containers from ArcMC. For more information, see "Deleting a Container" on page 848.

The **Containers** table includes the following columns:

- **Name:** Name of the container.
- **Path:** Path to the container.
- **Issues:** Status of any issues associated with the container.
- **Port:** Port number through which the container is communicating.

- **Framework Ver:** Framework version number of the container.
- **Parser Ver:** Parser version number of the container.
- **Status:** Status of the container. Possible values for container status are:
  - *Improper configuration: Initial default state.*
  - *Initializing connection:* The connector has a resolvable URL, but ArcMC has not logged in to the connector yet.
  - *Down*: There was an exception trying to execute the login command.
  - *Unauthorized:* The login command was executed, but login has failed.
  - *Connecting:* The login is in progress.
  - *Connected:* The login was successful.
  - *Empty:* Login successful, but the container doesn't have connectors.
  - *Initialized:* Login successful and the container has connectors.
  - *Unknown:* No information on status. To resolve, manually SSH to the system and restart the container.
- **Last Check:** Date and time of last status check.
- **Action:** Drop-down shows a variety of controls for executing container management tasks, which include:
  - Edit Container
  - Send Container Command
  - Add Connector
  - Run Logfu
  - Download Certificate
  - Display Certificates
  - Deploy (to ArcSight Marketplace)
  - Run FlexConnector Wizard

For more information on container management, see "Upgrading All Connectors in a Container" on page 849

The Connectors Tab

The **Connectors** tab displays all connectors associated with the item selected in the navigation tree. For example, if you selected a container in the navigation tree, the **Connectors** tab would show all connectors in the selected container. For the details on managing connectors, see "Managing Connectors" on page 860.

The Connectors tab will also show any deployed CTHs.

The **Connectors** tab includes these buttons, which perform operations on one or more selected connectors:

Add Connector	(Only shown when a container is selected in the navigation tree.) Adds a connector to the selected container.
Runtime Parameters	Edit the runtime parameters on selected connectors. For more information, see "Editing Connector Parameters " on page 862.
Destinations	Sets the destinations of selected connectors. For more information, see "Managing Destinations" on page 865.
Parameters	Sets parameters for selected connectors. For more information, see "Editing Connector Parameters " on page 862.
Delete	Deletes connectors from ArcSight Management Center. For more information, see "Deleting a Connector " on page 872.

The **Connectors** table displays the following parameters for each connector:

- **Name:** Name of the connector.
- **Path:** Path to the connector.
- **Group Name:** Name of the group for the connectors and CTHs. For connectors that have not been assigned to any group and older connector types no group name will be displayed.
- **Type:** Type of connector.
- **EPS In:** Events per second received by the connector.
- **EPS Out:** Events per second sent by the connector to its destination.
- **Cache:** Connector cache size. For more information on cache files, see the **Smart Connectors User Guide** in ArcSight SmartConnectors 24.2 documentation.
- **Last Check:** Date and time of the last status check.
- **Action:** Drop-down shows a variety of controls for executing connector management tasks. These include:
  - Send Connector Command
  - Share a connector to ArcSight Marketplace
  - Edit a FlexConnector

For more information on connector management, see "Managing Connectors" on page 860.

The Connector Summary Tab

To view a single connector in detail, click the connector in the navigation tree. The toolbar on the summary tab includes the following buttons for operations on the connector:

Connector Command	Sends a command to the connector. For more information, see "Sending a Command to a Connector" on page 873.
Remove Connector	Removes the connector. For more information, see "Deleting a Connector " on page 872.
Run Logfu	Run Logfu diagnostics on the connector. For more information, see "Running Logfu on a Connector" on page 873.
Share	Shares the connector through the ArcSight Marketplace. For more information, see "Sharing Connectors in ArcSight Marketplace" on page 877.

Tables below the toolbar show connector specifics, including basic connector data, parameters, and connector destinations. These tables include the following columns:

Connector Data

- **Type:** Type of connector.
- **Status:** Connector status.
- **Input Events (SLC):** Total number of events received by the connector since it was last checked (generally once per minute).
- **Input EPS (SLC):** Events per second received by the connector since it was last checked (generally once per minute).
- In addition, the columns to the right include tools for editing a connector, editing runtime parameters, adding a failover destination, and sending a destination command.

Connector Parameters

Click **Connector Parameters** to toggle display of this table. The **Connector Parameters** table includes:

- Click to edit parameters.
- **Parameters:** Parameters can include connector network port, IP address , protocol, and other information.
- **Value:** Parameter value.

Table Parameters (WUC Connectors Only)

WUC connectors (only) display these parameters.

- **Domain Name:** Connector domain name.
- **Host Name:** Connector host name.
- **User Name:** Connector user name.
- **Security Logs:** Indicates whether security events are collected.
- **System Logs:** Indicates whether system events are collected.

- **Application:** Indicates whether application events are collected from the Common Application Event Log.
- **Custom Log Names:** List of custom application log names, if any.
- **Microsoft OS Version:** Microsoft operating system for the connector.
- **Locale:** Connector locale.

Destinations

Click **Destinations** to toggle display of this table. The **Destinations** table includes:

- Click + to add additional destinations.
- **Name:** Destination name.
- **Output Events (SLC):** Total number of events output by the connector to the destination since it was last checked (generally once per minute).
- **Output EPS (SLC):** Events per second output by the connector to the destination since it was last checked (generally once per minute).
- **Cached:** Total number of events cached to be transmitted to the destination.
- **Type:** Destination type. Destination types are described in the SmartConnector User's Guide.
- **Location:** Location of the destination.
- **Device Location:** Location of the device on which the destination is located.
- **Comment:** Comments on the destination.
- **Parameters:** Destination-specific parameters, such as IP address , port, and protocol.
- **Action Buttons:** Action buttons enable destination management tasks, such as editing the destination, editing the runtime parameters, adding a new failover destination, sending destination commands and removing the destination.

For more information on managing connectors, see "Managing Connectors" on page 860.

The ConApps Tab

The **ConApps** tab displays all hardware and software Connector Appliances associated with the item selected in the navigation tree. For example, if you selected **System** in the navigation tree, the **Connector Appliances** tab would display all Connector Appliances in ArcMC; if you selected a Location, the tab would display all Connector Appliances in the selected location.

The **Connector Appliances** tab includes the following button, which operates on one or more selected Connector Appliances:

Set Configuration	Sets the configuration for selected Connector Appliances. For more information, see "Setting a Configuration on ConApps" on page 837

The **Connector Appliances** table displays these parameters for each Connector Appliance:

- **Name:** Name of the Connector Appliance.
- **Path:** Path to the Connector Appliance.
- **Port:** Port number through which the Connector Appliance is communicating.
- **Version:** Software version of the Connector Appliance.
- **Status:** Status of the Connector Appliance.
- **Last Check:** Date and time of last status check.
- **Action:** Drop-down shows a variety of controls for executing Connector Appliance management tasks, including the following:
  - Rebooting
  - Shutting down
  - Editing or removing a configuration

For more information on Connector Appliance management, see "Managing Connector Appliances (ConApps) " on page 835.

The Loggers Tab

The **Loggers** tab displays all hardware and software Loggers associated with the item selected in the navigation tree. For example, if you selected **System** in the navigation tree, the **Loggers** tab would display all Loggers in ArcMC; while if you selected a Location, you would see all Loggers in that location.

The **Loggers** tab includes the following buttons, which perform operations on one or more selected Loggers:

Set Configuration	Sets the configuration for selected Loggers. For more information, see "Setting a Configuration on Loggers" on page 846.
Upgrade Logger	Upgrades selected Loggers. For more information, see "Upgrading a Logger " on page 843

The **Loggers** table displays these parameters for each Logger:

- **Name:** Name of the Logger.
- **Path:** Path to the Logger.
- **Port:** Port number through which the Logger is communicating.
- **Version:** Software version of the Logger.
- **Top Storage Use:** Displays the most used storage group and its percentage of storage.
- **Status:** Status of the Logger.
- **Last Check:** Date and time of last status check.

- **Action:** Shows controls for executing Logger management tasks, including the following:
  - Rebooting
  - Shutting down
  - Editing or removing a configuration

The ArcMCs Tab

The **ArcMCs** tab displays all Software ArcSight Management Centers and ArcSight Management Center Appliances associated with the item selected in the navigation tree. For example, if you selected **System** in the navigation tree, the **ArcMCs** tab would display all managed ArcSight Management Centers; while if you selected a Location, you would see all ArcMCs in that location.

The **ArcMCs** tab includes the following buttons, which perform operations on one or more selected ArcMCs:

Set Configuration	Sets the configuration for selected ArcMCs. For more information, see "Setting a Configuration on Managed ArcMCs" on page 840
Upgrade ArcMC	Upgrades selected ArcMCs. For more information, see "Upgrading ArcMC " on page 839

The **ArcMCs** table displays these parameters for each ArcMC:

- **Name:** Name of the ArcMC.
- **Path:** Path to the ArcMC.
- **Port:** Port number through which the ArcMC is communicating.
- **Version:** Software version of the ArcMC.
- **Status:** Status of the ArcMC.
- **Last Check:** Date and time of last status check.
- **Action:** Shows controls for executing ArcMC management tasks, including the following:
  - Rebooting
  - Shutting Down
  - Editing a configuration

For more information on managing other ArcSight Management Centers in ArcMC, see "Managing Other ArcSight Management Centers" on page 837.

The TH Nodes Tab

ArcMC can only manage a single Transformation Hub. However, the single managed Transformation Hub may have any number of Transformation Hub nodes, each of which can be

managed and monitored by ArcMC. When you add a Transformation Hub as a host to ArcMC, you add all of its nodes.

The **TH Nodes** tab displays all Transformation Hub nodes present in the managed Transformation Hub. For example, if you selected **System** in the navigation tree, the **TH Nodes** tab would display all managed Transformation Hub nodes; while if you selected a location, you would see all Transformation Hub nodes in that location.

The tab displays these parameters for each managed Transformation Hub node:

- **Name:** Name of the Transformation Hub node.
- **Port:** Port number through which the Transformation Hub node is communicating.
- **Type:** Type of Transformation Hub node.
- **Last Check:** Date and time of last status check.

For more information on managing Transformation Hub in ArcMC, see "Managing Transformation Hub" on page 927.

The Collectors Tab

The **Collectors** tab displays all Collectors associated with the item selected in the navigation tree. For example, if you selected a container in the navigation tree, the **Collectors** tab would show all Collectors in the selected container.

The **Collectors** table displays the following parameters for each connector:

- **Name:** Name of the Collector.
- **Port:** Collector port.
- **Type:** Type of Collector.
- **Syslog Lines Received:** Events Received.
- **Custom Filtering:** Messages filtered out.
- **Status:** Collector status.
- **Last Check:** Date and time of the last status check.

For the details on managing Collectors, see "Bulk Operations" on page 933.

Locations

A *location* is a logical grouping of hosts. The grouping can be based on any criteria you choose, such as geographical placement or organizational ownership. Locations are a useful way to organize a set of hosts.

For example, you could group all hosts in New York separately from hosts in San Francisco and assign them to locations named “New York” and “San Francisco”. Similarly, you could group hosts in a location named “Sales” and others in the location “Marketing”.

A location can contain **any number** of hosts. For information on adding hosts to locations, see "About Adding a Host" on the next page.

> **Note:** ArcMC includes one location by default (called *Default*) but you may add any number of locations. The name of the Default location may be edited, and the location itself may be deleted.

Adding a Location

You can add any number of locations.

To add a location:

1. Click **Configuration Management > Bulk Operations**.
2. In the navigation tree, click **System** and click the **Location** tab.
3. Click **Add.**
4. Enter the name of the new location, and click **Save**.

Editing a Location

You can edit the name of a location.

To edit a location:

1. Click **Configuration Management > Bulk Operations**.
2. In the navigation tree, click **System**, and then click the **Location** tab.
3. On the **Locations** tab, choose a location to rename.
4. Click **Edit**.
5. Enter the new name of the location, and click **Save**. The location is renamed.

Viewing All Locations

You can see all the locations that exist in ArcMC.

To view all locations:

1. Click **Node Management**.
2. In the navigation tree, click **System**, and then click the **Locations** tab to view all locations.

Deleting a Location

When you delete a location from ArcMC, any hosts in the location (and their associated nodes) are also deleted.

> **Tip:** If you want to delete a location but still want to keep its hosts in ArcMC, relocate the hosts before deleting the location. See "Moving a Host to a Different Location" on page 945.

To delete a location:

1. Click **Configuration Management** > **Bulk Operations**.
2. In the navigation tree, click **System**, and then click the **Location** tab.
3. On the **Location** tab, choose one or more locations to delete.
4. Click **Delete**.
5. Click **Yes** to confirm deletion. The selected locations are deleted.

Hosts

A *host* is a networked system associated with a unique IP address or hostname. A host can be an ArcSight appliance, or a system running an ArcSight software product, such as Software Logger.

For information on adding hosts to manage, see "About Adding a Host" below.

About Adding a Host

After a host is added to ArcMC, ArcSight products on the host becomes *nodes,* and can be managed. For example, adding a host running Connector Appliance with 4 containers would add 5 nodes to ArcMC: the Connector Appliance itself, and each container.

> **Note:** In ArcMC 2.2 and later, the ArcMC localhost is added automatically for remote management. You will be able to manage the localhost as you would any other node (see Overview).

Prerequisites for Adding a Host (for each Host Type)

Connection Information for Adding a Host

Host Type	Required Information
Appliance with Local Connectors (includes ArcSight Management Center Appliance, Connector Appliance, or Logger Appliance (L7700))	• Hostname (FQDN) or IP address. Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. If hostname is used, the hostname entered must match the hostname from the host's SSL certificate. If the FQDN fails to resolve, restart the web service. • Authentication credentials (username and password) for logging into the host. If the host is configured for external authentication, such as LDAP or RADIUS, use the external authentication credentials, if possible, or use the fall back credentials. **Note:** See "Node Authentication Credentials " on page 820 for more information about authentication credentials.
	• Authentication credentials (username and password) for any local containers. If the appliance includes multiple containers, then the credentials for each container must be identical. For example, if the username and password for one container managed by a Connector Appliance is *myusername* and *mypassword*, then *myusername* and *mypassword* must be the credentials for all local containers managed by the same Connector Appliance.
Appliance without Local Connectors (includes Logger Appliance (non-L7700))	• Hostname (FQDN) or IP address. Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. If hostname is used, the hostname entered must match the hostname from the host's SSL certificate. If the FQDN fails to resolve, restart the web service. • Authentication credentials (username and password) for logging into the host. If the host is configured for external authentication, such as LDAP or RADIUS, use the external authentication credentials, if possible, or use the fall back credentials. **Note:** See "Node Authentication Credentials " on page 820 for more information about authentication credentials.
Software Form Factor (includes Software ArcSight Management Center, Software Connector Appliance, or Software Logger)	• Hostname (FQDN) or IP address. Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. If hostname is used, the hostname entered must match the hostname from the host's SSL certificate. If the FQDN fails to resolve, restart the web service. • Authentication credentials (username and password) for logging into the host. If the host is configured for external authentication, such as LDAP or RADIUS, use the external authentication credentials if possible, or use the fall back credentials. **Note:** See Node Authentication Credentials for more information about authentication credentials. • Port number assigned to the product.

Connection Information for Adding a Host, continued

Host Type	Required Information
Connector (includes SmartConnectors of all types)	• Hostname (FQDN) or IP address. Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. If the FQDN fails to resolve, restart the web service. • Authentication credentials (username and password) for the connector. **Note:** See Node Authentication Credentials for more information about authentication credentials. • Optionally, specify an inclusive port range separated by a hyphen (such as 9004-9008) to scan a port range for all connectors. **Note:** If the port range includes multiple connectors, then the credentials for each connector in the range must be identical. For example, if the username and password for one connector in the range was *myusername* and *mypassword*, then *myusername* and *mypassword* must be the credentials for every connector in the port range. **Note:** Prior to adding a software-based SmartConnector as a host, you must prepare the Smart Connector as explained in SmartConnectors on ArcMC.
Transformation Hub - Non-Containerized Deployment	• Hostname (FQDN) or IP address. Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. If the FQDN fails to resolve, restart the web service. • Port number for the Transformation Hub (default 32080) • In order to add Transformation Hub as a host, the active user must belong to an ArcMC permission group with rights to do so. By default, the admin user has such rights. **Note:** Prior to performing the Add Host process, you need to generate the ArcMC certificate with complete FQDN and download the .crt file, then copy the certificate file to your Kubernetes master node. See Preparing to Add Transformation Hub as a Host for details on this process.

Transformation Hub - OPTIC Management Toolkit (OMT)	• Virtual FQDN or Virtual IP (VIP) address.
	VIP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for a VIP address. If the FQDN fails to resolve, restart the web service.
	• Port number for the Transformation Hub (default 32080)
	• The following Kubernetes cluster parameters:
	  • Cluster Port (default 443)
	  • Cluster Username and Password
	  • Contents of the certificate file. For more details, see here.
	• In order to add Transformation Hub as a host, the active user must belong to an ArcMC permission group with rights to do so. By default, the admin user has such rights.

- **An SSL Certificate:** An SSL certificate must be generated for any of the following host types to be managed:
  - Connector Appliance or Software Connector Appliance
  - Logger Appliance or Software Logger
  - Transformation Hub (any version)

- ArcSight Management Center Appliance or Software ArcSight Management Center

  The hostname in the certificate must match the hostname you are adding to ArcMC. For more information on generating certificates for these host types, consult the ArcSight Administrator's Guide for each product. If a host to be added already has a certificate installed, you can use the existing certificate, as long as the hostname on the certificate matches the hostname of the host you are adding.

  > **Note:** If the hostname does not match the hostname in the SSL certificate, you can regenerate a matching certificate by doing one of the following:
  >
  > - For a hardware appliance, in **System Admin > Network**, click the **NICS** tab. Under **Host Settings**, note the entry in the Hostname field. This is the value you should use to add the host to ArcMC. Click **Restart Network Service.** Then, in the navigation menu, under **Security**, pick **SSL Server Certificate**. Click **Generate Certificate**. A new certificate will be generated that matches the hostname from the **NICS** tab.
  > - For software form factor, in **System Admin > SSL Server Certificate**, under **Enter Certificate Settings**, verify that the hostname from the NICS tab noted previously is entered in the **Hostname** field. Then, click **Generate Certificate**. A new certificate will be generated that matches the hostname from the **NICS** tab.

- **Check for Agent Installation:** Check the table under "Installing the ArcMC Agent" on page 802 to determine if the ArcMC Agent needs to be installed on a host prior to adding it to ArcMC. For some host types, the Agent will be installed automatically upon adding a host.

  > **Note:** Perl is required for the automatic installation of the ArcMC Agent. Ensure that Perl is installed on the host prior to attempting to add the host to ArcMC.

Permission Groups

A *permission group* is a set of access privileges. Access privileges are organized functionally, enabling you to assign different functions or different product access across users.

Permission groups are the building blocks of roles. In themselves, permission groups do not enable access for any users. Permission groups can be bundled into roles, and when users are assigned to those roles, they will gain the privileges which the individual permission groups grant them.

Permission groups can be created, imported from managed nodes, edited, and deleted in ArcMC.

You can create permission groups of the following types in ArcMC.

Group Type	Grants access to...
System Admin	System admin and platform settings.
Logger Rights	Logger general functionality. Does not include Logger Reports and Logger Search permissions.
Logger Reports	Logger report functionality.
Logger Search	Logger search functionality.
Conapp Rights	Connector Appliance general functionality.
ArcMC Rights	ArcMC general functionality. Note that ArcMC rights *View options* and *Edit, save and remove options* can only be granted to groups with either *View management* or *Edit, save, and remove management rights.*

You can create different permission groups to reflect different management access levels. For example, you could create two System Admin permissions groups, one with access to reboot and update privileges, and the other with access to global settings. However, a role can only be assigned one permission group per group type.

To create a permission group:

1. Select **User Management > Permission Groups.**
2. On the **Permission Groups** page, click **New**.
3. In **Group Name**, enter a name for the new group.
4. Select a type from the **Group Type** drop-down list.
5. In **Description**, enter a brief description of the permission group.
6. In the **Rights** list, select the rights to which the permission group controls. (Click **Select All**

to select all rights in the list.)

7. Click **Save**.

To import one or more permission groups from a managed node:

> **Note:** Only US ASCII characters are supported for import.

1. Select **User Management > Permission Groups.**
2. On the **Permission Groups** page, click **Import**.
3. From the list of managed nodes, select the node from which to import a group, and then click Next.
4. The **Available Permission Group(s)** column shows available permission groups on the managed node. Select one or more groups, and then use the Add button to move them to the **Selected Permission Group(s)** column. (Note that permission groups already present in ArcMC will be shown as disabled and unavailable for selection.)
5. Click **Import**. The groups are imported into ArcMC.

To edit a permission group:

1. Select **User Management > Permission Groups.**
2. From the list of groups, click the name of the group you wish to edit.
3. Enter values or select rights as needed.
4. Click **Save**. (Click **Save As** to save the group under a new name.)

To delete a permission group:

> You can only delete a permission group that is not currently assigned to any roles, nor is part of any Filter configuration.
> To delete a permission group that is part of a role, delete the role first.
> To delete a permission group that is part of a Filter configuration, remove it from the configuration.

1. Select **User Management > Permission Groups.**
2. From the list of groups, select the group you wish to delete.
3. Click **Delete**.
4. Click **Yes** to confirm deletion.

Preparing to Add Transformation Hub 2.01 or Earlier as a Host

Before you can add Transformation Hub (version 2.01 or earlier) as a managed host, you will need to generate the ArcMC certificate with complete FQDN and download the .crt file, and then copy the certificate file to your Kubernetes master node.

To prepare for adding Transformation Hub as a host:

1. In ArcMC, click **Administration > System Admin.**
2. Under **Security > SSL Server Certificate**, under Hostname, enter the FQDN of the ArcMC.
3. Click **Generate Certificate.**
4. Save the certificate locally.
5. Connect to your Kubernetes master node.
6. Copy the previously generated certificate to `/opt/arcsight/k8s-hostpath/th/arcmccerts.`
7. Launch the ArcSight Installer.
8. Click **Configuration > ArcSight Transformation Hub.**
9. On the **ArcMC Monitoring** tab, in **ArcMC URL**, enter the FQDN and port number of the managing ArcMC.

Preparing to Add Transformation Hub as a Host (Standalone ArcMC)

In order to add Transformation Hub as a managed host, you will need to generate the ArcMC certificate with complete FQDN and copy it to the ArcMC monitoring tab of the ArcSight installer.

To prepare for adding Transformation Hub as a host:

1. In ArcMC, click **Administration > System Admin.**
2. Under **Security > SSL Server Certificate**, under Hostname, specify the FQDN of the ArcMC.
3. Click **Generate Certificate.**
4. Once the certificate is generated, click **View Certificate** and copy the full content from --BEGIN cert to END cert--
5. Access the ITOM Management Portal: https://<TH-VIP>:5443
6. From the left menu click **DEPLOYMENT > Deployments.**
7. Click the three dots on the right **> Reconfigure.**
8. Scroll down to **Management Center Configuration.**
9. Type the ArcMC username in the **Transformation Hub Administrator Username** field.
10. Type the ArcMC password in the **Transformation Hub Administrator Password** field.
11. Add the FQDN and port number in the **Management Center host names and ports managing this cluster** field.
12. Paste the previously generated certificate from the ArcMC View Server Certificate page into the **Management Center Certificates** field and click **Save.**

In ArcMC, you can now follow the process outlined under Adding Transformation Hub as a Host.

Node Authentication Credentials

ArcSight Management Center authenticates to each managed node each time it communicates with the node, using the node's authentication credentials—that is, username and password—you supply when first adding the host. If the host includes connectors or containers, then authentication credentials must also be supplied for these as well. (Exception: Transformation Hub does not require authentication credentials for individual nodes.) As a result, valid credentials for each node are required when adding a host.

Determining a Node's Credentials:

Consult the system administrator for each managed node to determine its current login credentials. Each ArcSight product ships with a default set of credentials. However, for optimal security, it is expected that the default credentials are changed as soon as possible by the administrator, so the default credentials may no longer be valid for authentication.

- For default credentials for ArcSight products, consult the relevant product administrator's guide. (For SmartConnector default credentials, consult the SmartConnector User's Guide, available from the OpenText Community.)
- Some products can be configured by administrators to use external authentication, in which case the external authentication credentials or fallback credentials should be provided when adding the host to ArcMC. (SmartConnectors may not be configured for external authentication.)

Changed or Expired Credentials

If the username or password on a node are changed (or expire) any time after the node is added to ArcSight Management Center, then the node will no longer be managed. However, it will still appear in the list of managed nodes. For example, on some hosts, passwords are set to expire automatically after some time period, which would prevent successful authentication by ArcMC using the node's initial credentials. To avoid this issue, you may wish to use node credentials that do not expire. To continue management of node on which the credentials have changed or expired, use the Update Host Credentials feature.

Dynamic Credentials

If authentication credentials are configured to change dynamically (such as with RADIUS one-time passwords), then instead of providing external authentication credentials, you can provide the credentials of a local user on the managed node who is permitted to use fallback authentication. ArcMC will then try to authenticate to the managed node using the external authentication method first, and if this fails, it will try to authenticate to the managed node using the local user credentials.

Managing SmartConnectors on ArcMC

ArcMC can remotely manage previously-installed, software-based SmartConnectors; however, the remote management feature is disabled on software SmartConnectors by default.

You can install several SmartConnectors on a single host if supported by the hardware. ArcSight certifies a maximum of 4 SmartConnectors on Windows hosts and 8 on Linux hosts.

To manage software-based SmartConnectors with , you need to enable remote management on each connector, as follows:

1. In a text editor, in the installation directory for the SmartConnector, open the file `/<install_dir>/user/agent/agent.properties.`
2. Add the line: `remote.management.enabled=true`
3. If desired, customize the connector's listening port. The default is 9001. To change this value, add the line: `remote.management.listener.port=<port_number>`, where `<port_number>` is the new port number.
4. Save the file.
5. Restart the SmartConnector for changes to take effect.

Adding a Host

Before adding a host, ensure that you have the required information for the host on hand. For more information, see "Prerequisites for Adding a Host (for each Host Type)" on page 814.

To add a host to ArcMC:

1. Click **Node Management**.
2. In the navigation tree, select a location to which you plan to add the host.
3. On the **Hosts** tab, click **Add Host.**
4. On the **Add a new Host** dialog, in **Hostname/IP,** enter either the hostname or IP address of the host.
5. In **Type,** select the type of node from the drop-down list.
6. Enter values for the required settings. (See About Adding a Host for the specific information required, based on the different type of nodes.)
   - In **Host Credentials** or **Connector Credentials**, enter the username and password required for authentication.
   - In **Port**, if required, enter the value of the port on which ArcMC will connect to the host.
7. Click **Add**. The host is added to ArcMC.

Note: You can quickly deploy a Connector directly to a host in the ArcMC Deployment View. For more information, see "Instant Connector Deployment" on page 784.

Adding a Host with Containers

When you add a host that includes containers (such as Connector Appliance), ArcMC also attempts to retrieve the SSL certificates from any containers that reside on the host, and add each container as a separate node. Containers on the remote host can be managed only if ArcMC can authenticate using the certificates and supplied credentials. When the certificates are retrieved, you are prompted to import them into ArcMC.

Note: On ArcMC Appliance, all local containers are added automatically as hosts of type Software Connector.

Adding Transformation Hub Non-Containerized (THNC) as a Host

To add THNC as a managed host:

In the THNC server:

1. During the THNC setup script, add the arcmc host when the option is prompted. For example: hostname:443.
2. Get a copy of the ArcMC server certificate, with the extension *.crt from the system where ArcMC is running.
3. Copy the ArcMC certificate file and paste it on /opt/arcsight/th/current/cert/webservice/ directory.
4. Restart the THNC services.

In ArcMC:

1. Go to **Node Management > View All nodes**
2. From the left navigation tree, select the location where you want to add the THNC.
3. Click **Add Host**.
4. In the **Hostname/IP** field, type the fully qualified name of the THNC.
5. In the **Type** field, select **Transformation Hub - Non-Containerized Deployment.**
6. In the **Port** field, type 8080 and click **Add**.

Importing Multiple Hosts

To quickly and easily add multiple hosts in bulk, you can import a comma-separated values (CSV) file that lists the names and required attributes of the hosts to be added.

Prerequisites for Importing Multiple Hosts

The following prerequisites apply to importing hosts.

- **Add Host Prerequisites:** Any prerequisites for the Add Host process also apply to importing multiple hosts by a CSV file. See "Prerequisites for Adding a Host (for each Host Type)" on page 814.
- **Valid CSV File:** Ensure the values in your CSV file are valid and correct. An import hosts job will fail immediately upon receiving an invalid or incorrect value. The CSV file format is described under "CSV File Format" below.
- **Stop the Agent 1.0 Process:** In addition, if any of the hosts to be imported are running the ArcMC 1.0 Agent, stop the Agent process on each such host before the import. (This is not needed for later versions of the ArcMC Agent.)

CSV File Format

The CSV (comma-separated value) file requires the following header line to be its first line:

```
location,hostname,type,host username,host password,connector
username,connector password,connector container name,port/port range,connector
username,connector password, connector port/port range
```

Each subsequent line represents one host to be imported. Each line must include values for the following comma-separated fields for each host:

```
<Location>, <Hostname>,<Host Type>,<Host Username>,<Host Password>,
<Connector Username>,<Connector Password>,<Connector Container
Name>,<Port/Port Range>
```

Note: The column `connector container name` (for instances in which users edit a container) has been added to the CSV file when importing or exporting hosts. If users don't want to import the values of this field, they can leave it blank. This applies for ArcMC versions 2.9.4 and later.

Some host types require values for all fields, and some are optional. An optional field with no value specified must still include a comma to represent the empty field.

Note: Only US ASCII characters are supported for import.

Host Field Values

Valid values for host fields are detailed in the following table. An asterisk (*) indicates a required field. An optional field with no value specified must still include a comma to represent the empty field.

Field	Description
Location*	Location to which the host will be assigned.
Hostname*	Hostname (FQDN) or IP address of the host. • FQDN or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. • If hostname is used, the hostname entered must match the hostname from the host's SSL certificate. • For a hardware appliance, DNS must be configured on the managing appliance (**System Admin > DNS**).
Host Type*	Host type. Valid (case-insensitive) values are: • `appliance_with_local_connectors:` includes ArcSight Management Center Appliance, Connector Appliance and Logger Appliance (L77XX) • `appliance_without_local_connectors:` includes Logger Appliance (non-L77XX). • `software_form_factor:` includes Software ArcSight Management Center, Software Connector Appliance or Software Logger. • `software_connector:` includes all Connectors.
Host Username/ Password*	User name and password used to authenticate to the host. **Note:** See "Node Authentication Credentials " on page 820 for more information about authentication credentials.

Field	Description
Connector Username/ Password	Username and password used to authenticate to the connector. Required for hosts of type Appliance with Local Connector and Software Connector; otherwise optional. **Note:** See "Node Authentication Credentials " on page 820 for more information about authentication credentials.
Connector Container Name	Name of the container. For example: Syslog Container or SmartConnector Container.
Port/Port Range	Starting port or port range for connector scan. Valid values: • Port number • Port range • Comma-separated port numbers (for example, 9000,9004,9007) Notes: • *For software form factors*, port is required. • *For appliance form factors*, to add all local containers, leave the field blank. However, if any port numbers are entered, then certificates will be downloaded only for the specified port numbers, and only those containers will be imported. • *For connectors,* either a port or port range is required. If using port range, specify an inclusive port range, using a hyphen between starting and ending port. For example, a specified port range of 9001-9003 would scan ports 9001, 9002, and 9003. **Note:** If the port range includes multiple connectors, then the credentials for each connector in the range must be identical. For example, if the username and password for one connector in the range was *myusername* and *mypassword*, then *myusername* and *mypassword* must be the credentials for every connector in the port range.

An example of a valid import file, importing two hosts, is shown here:

```
location,hostname,type,host_username,password1,connector_
username,password2,port/port range,username,password3,port/port range
```

```
CorpHQ,hostname.example.com,software_connector,username,password,connector__
username,connector_password,9001-9005
```

```
EMEA,hostname2.example.com,appliance_without_local_connectors,
logger_user,logger_pword,,,,,
```

In this example, the first line would represent the required header line, the second line a Software Connector, and the third line would represent a Logger Appliance.

Import Hosts Procedure

Only a single Import Hosts job may be executed at one time.

> **Note:** Importing Transformation Hub host in ArcMC is not supported. Please add Transformation Hub host to ArcMC through the "Adding a Host" on page 822 process.

To import hosts from a CSV file:

> **Note:** Before beginning the import, stop the Agent processes on any hosts running version 1.0 of the ArcMC Agent.

1. Create and save your CSV file in a text editor.
2. Log into ArcMC.
3. Select **Node Management > Import Hosts.** The Import Hosts wizard starts.
4. Click **Browse**, and browse to the location of your hosts CSV file.
5. Click **Import**. The hosts are imported as a background job.

   If the CSV file is valid, connector certificates are retrieved automatically so that ArcMC can communicate with each connector in a container. The Upload CSV wizard lists the certificates. (To see certificate details, hover over the certificate.).

Automatic installation of the ArcMC Agent may increase the time required for the Import Hosts job.

- Select **Import the certificates...**, and then click **Next** to import the certificates and continue.
- Select **Do not import the certificates...**, and then click **Next** if you do not want to import the certificates. The Upload CSV wizard does not complete the upload CSV process.

  > **Note:** The Import Hosts wizard does not complete the upload if certificate upload failed for any of the connectors in a container, or if any of the certificates failed to import into the trust store.

1. The Import Hosts job executes.

Import Hosts Job Logs

ArcMC logs the results of all Import Hosts jobs. Each job produces a new log, named `import_hosts_<date>_<time>.txt`, where `<date>` and `<time>` are the date and time of the import hosts job.

- For Software ArcSight Management Center, logs are located in the directory `<install_dir>/userdata/logs/arcmc/importhosts.`
- For ArcSight Management Center Appliance, logs are located in the directory `opt/arcsight/userdata/logs/arcmc/importhosts.`

Log Format

Each entry in the log will show the success or failure of each host import attempt, in the following format:

```
<User initiating job>, <CSV filename>, <Time of import host job
start>,<Hostname>,<Success/failure result>
```

For example:

```
admin, my_csv_file.csv, Tue Apr 08 14:16:58 PDT 2015, host.example.com, Host
added successfully
```

If the import hosts job has failed due to one or more invlaid entries in the CSV file, the result file will show the parsing error details with the line number and error.

For example:

```
Line [1] has [connector password] field empty. [connector password] field is
required for this host type.
```

Exporting Hosts

Exporting hosts from an ArcMC will create a CSV list of hosts managed by that ArcMC. (Password information is not included in this file.)

After adding passwords for each host to the file, you can then import this list of hosts into another ArcMC, using the Import Hosts feature described under "Importing Multiple Hosts" on page 824

Exporting hosts is most useful when you are reassigning management of hosts from one ArcMC to another.

For example, consider two ArcSight Management Centers, called ArcMC East and ArcMC West. ArcMC East currently manages 50 hosts. However, you are consolidating management of all hosts to the new ArcMC West. To do this quickly and easily, you would export the hosts from ArcMC East into a CSV file. Then, you would add an additional entry for ArcMC East to the CSV file.

After adding in password data for each host, you would import the resulting CSV file into ArcMC West. At the end of the process, all of ArcMC East's hosts, and ArcMC East itself, would be managed by ArcMC West.

To export hosts in ArcMC:

1. Select **Node Management > Export Hosts.**
2. All hosts managed by the ArcMC are exported to the local CSV file (`exporthosts.csv`).
3. Optionally, open the file in a CSV editor. Add the password information for each host to the CSV file, and then save the file.

Viewing All Hosts

You can see all the hosts managed by ArcMC, or view hosts by location.

To view all hosts:

1. Click **Node Management**.
2. In the navigation tree, click **System**. (To view by location, click the location you wish to view.)
3. Click the **Hosts** tab. All managed hosts are displayed.

Viewing Managed Nodes on a Host

You can view all the managed nodes on a host, by host type.

To view managed nodes on a host:

1. Click **Node Management**.
2. In the navigation tree, click the location to which the host is assigned. Then, click the host.
3. Click the appropriate tab to view the node types for the managed host: **Containers, Connectors, Connector Appliances, Loggers,** or **ArcMCs**.

Generator ID Manager

Every event generated by an ArcSight component will have a unique Global Event ID. This will help in identifying the events in case the same event is seen in multiple ArcSight components like Logger, ESM, and Transformation Hub.

- "Generator ID Management" on the next page
- "Setting Up Generator ID Management" on the next page
- "Getting Generator ID for Non-managed Nodes" on the next page
- " Setting Generator IDs on Managed Nodes" on the next page

Generator ID Management

This feature allows users to generate an ID to assign it to a non-managed product. Each assigned Generator ID should be unique for the ArcSight environment.

Setting Up Generator ID Management

1. On the top right side of the screen, click **Generator ID Manager.**
2. Select **Yes** to enable Generator ID Management in ArcMC.
3. Enter the numeric values between 1 and 16383 for the Generator ID range (**Start** and **End**) and click Save. ArcMC will set the generator ids for itself if not set already.
4. Restart all ArcMC processes to continue.

Getting Generator ID for Non-managed Nodes

1. Go to **Configuration Management** and select **Generator ID Management**.
2. Click **Assign a Generator ID.**
3. Select the **Event Producer Type**. Other fields are optional, click **Assign.**
4. Copy the ID by clicking the copy to clipboard icon and Click **OK**. A list of generated IDs will be displayed.

Setting Generator IDs on Managed Nodes

ArcMC will automatically set the generator IDs for each managed node when performing the following actions, if ArcMC is enabled as a Generator ID Manager:

Connectors

- Adding a Host version 7.11 or later.
- Scanning a Host
- Adding a Connector to a Container
- Connector upgrade to version 7.11 or later.
- Instant Deployment

Note: Multiple host deployment is disabled when the Generator ID Manager flag is enabled.

Logger

- Remote Upgrade: Upgrade from and to Logger version 6.7 or later.
- Adding a Host version 6.7 or later.

ArcMC

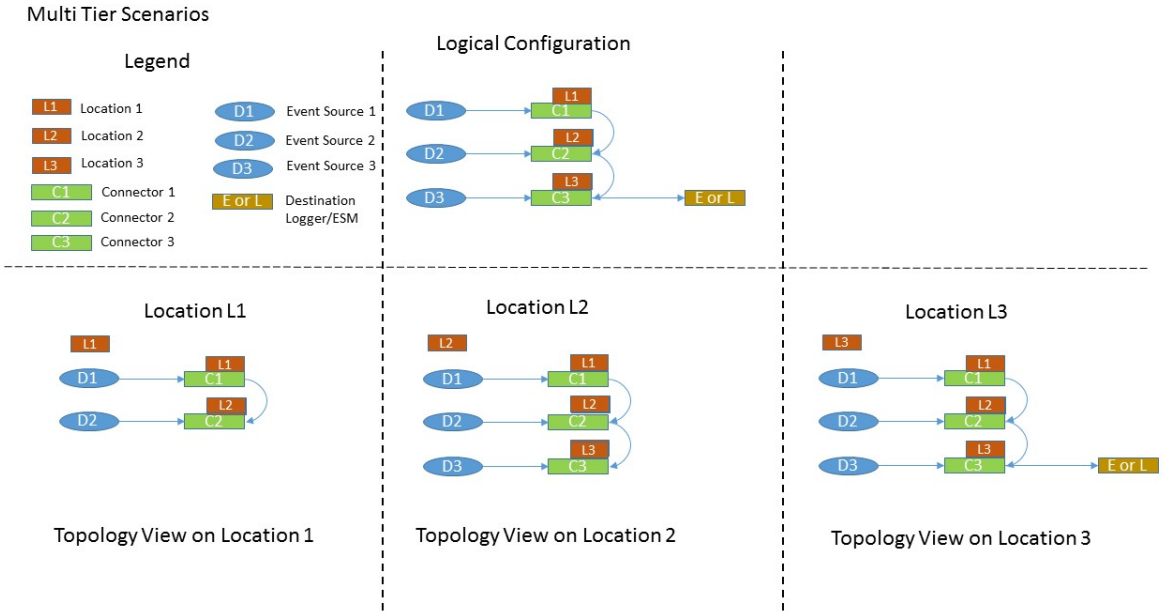
- Remote Upgrade: Upgrade from and to ArcMC version 2.9 or later.
- Adding a Host version 2.9 or later.
- Scanning a Host.
- Setting the Generator IDs on localhost by enabling the Generator ID Manager.

The Topology View and Unmanaged Devices

This section details various scenarios for the inclusion of devices not managed by ArcMC in your network, and the effect of each scenario on the ArcMC Topology View. Particularly when connectors are chained together in a multi-tier configuration, unmanaged products can block the view from their immediate downstream neighbor.

Scenario 1: No Unmanaged Devices

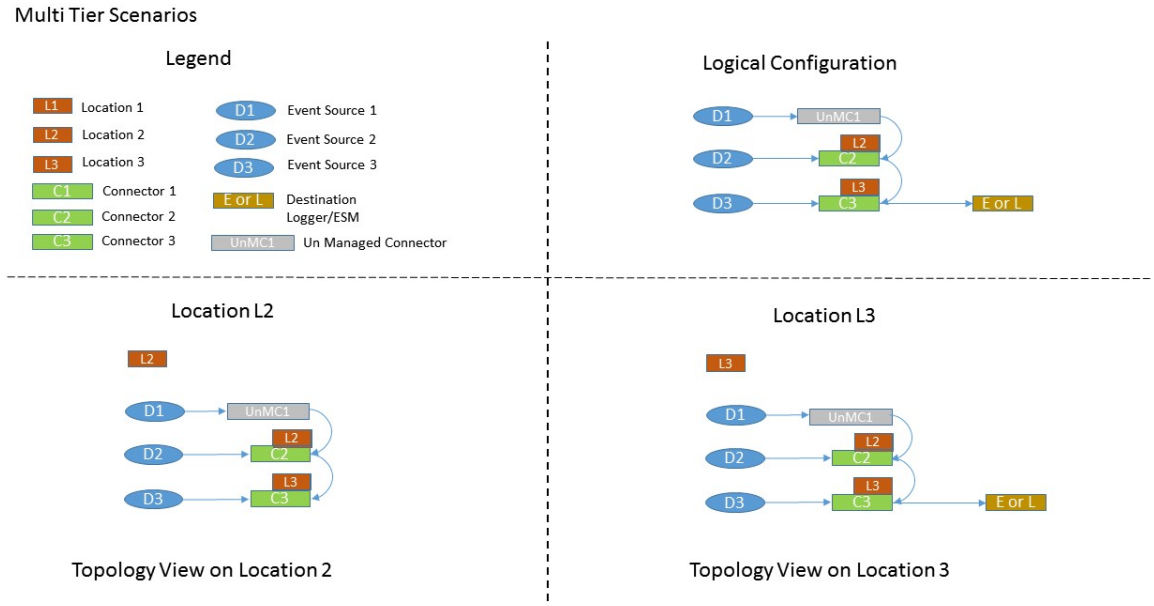
In this scenario, no umanaged products are included in the network. As a result, the ArcMC Topology view is unimpeded and gives an accurate picture of the logical topology as viewed from any location.



Scenario 2: Unmanaged Connector in Location L1

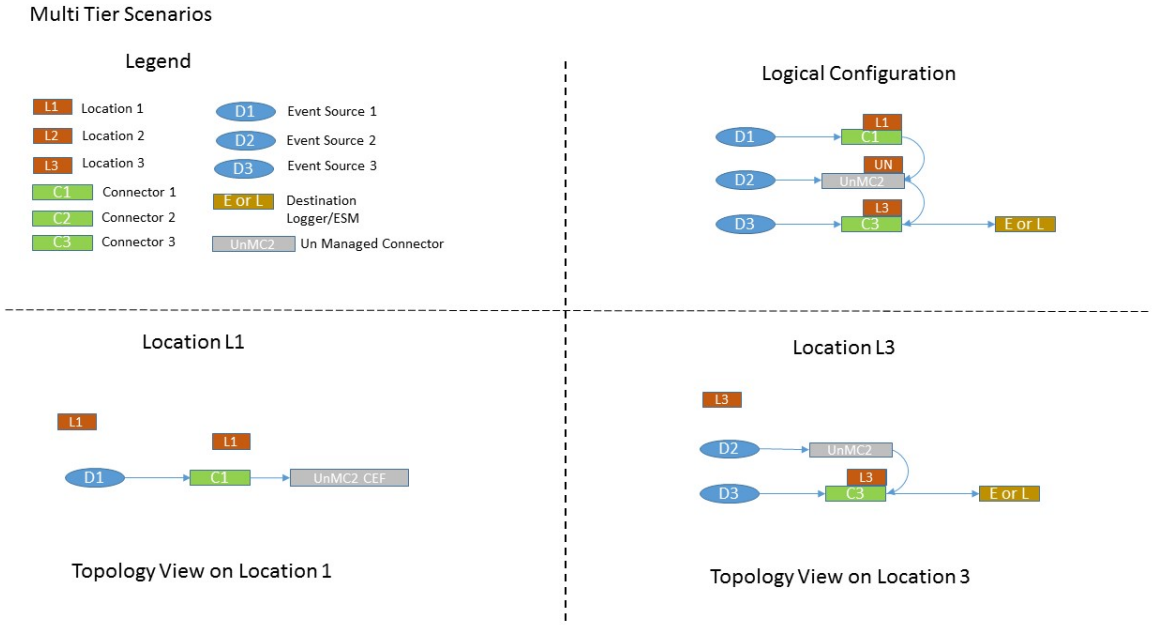
This scenario shows an unmanaged connector in location L1 and the results on the Topology View as seen from locations L2 and L3. No view is seen from L1, since it does not include any

managed nodes. The view at the other downstream locations is as expected.



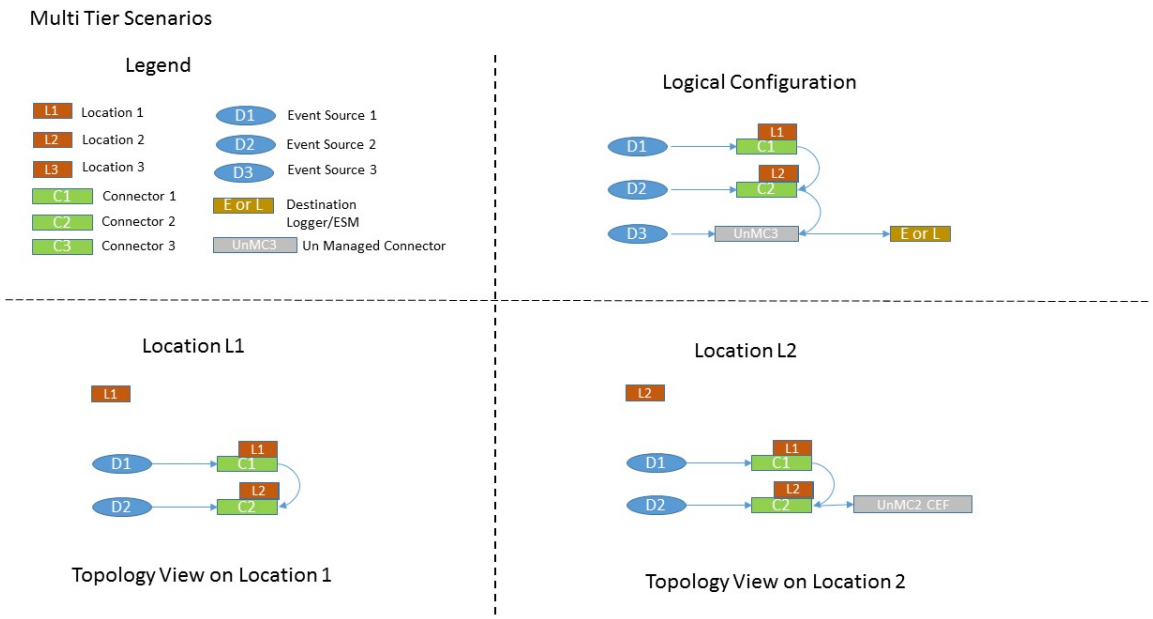
Scenario 3: Unmanaged Connector in Location L2

In this scenario, an unmanaged connector is located in Location L2 and chained to connectors in locations L1 and L2. This blocks the Topology view of L1 as seen from L3. In addition, the destination Logger or ESM shows no traffic from L1.



Scenario 4: Unmanaged Connector in Location L3

In this scenario, an unmanaged connector is in Location L3. This impedes an accurate Topology view of location 3. In fact, no traffic from locations L1 and L2 is shown for the destination Logger/ESM.



To get the most complete and accurate topological view, you are strongly encouraged to use ArcMC to manage all supported connectors included in your logical topology.

Logger Consumption Report

The Logger Consumption Report includes information on your Logger data consumption. You can choose which managed Logger 6.1 (or later) nodes to include in the report.

To generate a Logger Consumption report:

1. Click **Administration > Application > Consumption Report.**
2. Use the **Add** and **Remove** arrows to add or remove nodes from the **Available Nodes** column to the **Selected Nodes** column.
3. Click **Run Report.** The report is generated for the selected nodes.
4. Click **+** to expand the data on any node to view licensing specifics.
5. To export the license report to PDF, click **Export to PDF.**

6. Specify a time range for the report.
7. Click **OK** to exit the report.

Report Data

The report displays the licensed value and actual value for data consumption by managed Loggers.

Value	Description
Licensed Consumption	Shows the data consumption to which your license entitles you. For individual ADP Loggers, the license limit will be shown as *Not Applicable*, since ArcMC tracks the overall data limit, not those of individual Loggers. **Note:** If an ADP Logger is managed by a version of ArcMC earlier than 2.5, then the license limit will be incorrectly shown in the report as *Unlimited*.
Actual Consumption	Shows the current value of data consumption. Click the value to display the Consumption Chart, which shows data consumption in detail.
Status	Click any status hyperlink to view individual Logger data for the last 30 days. Status values are shown as follows: *OK* if the actual value is less than or equal to the license value. *In Violation* indicates that the actual value exceeds the license value, which constitutes a violation of the terms of your license. Your license permits you a number of violations for each 30-day period, which is shown on the *Violations Last 30 Days* line. Click any hyperlink to view individual Logger data for the last 30 days.

Exporting PDF Reports

You can export up to 5 MB of data in PDF reports, this is the default size.

To increase the limit of data to be exported add the following property to the `logger.properties` file (include the new increased value in bytes):

```
pdf.reports.size.limit.content=<new value in bytes)
```

Restart the web process after editing the `logger.properties` file.

For more information, please see "Modifying logger.properties " on page 800.

Follow the steps below to increase the limit of data to be exported perform:

1. Log in to the OMT Management Portal. See "Accessing the OMT Management Portal" on page 507 for more information.
2. From the left menu select **Deployment > Deployments**.

3. Click **... (Browse)** on the far right and choose **Reconfigure**. A new screen will open in a separate tab.
4. Select the **Fusion** tab and scroll down to the **ArcMC Configuration** section to enter the desired value for the "**Maximum Exported PDF Report Size** parameter.
5. Click **Save**. The ArcMC pod will be restarted

Managing ArcSight Products

ArcSight Management Center enables management tasks on a variety of ArcSight products, including the following:

- Hardware and Software Connector Appliances
- Hardware and Software ArcMCs
- Hardware and Software Loggers
- Containers
- Software connectors
- Transformation Hub

This chapter discusses the remote management of these products.

Managing Connector Appliances (ConApps)

You can perform any of the following management tasks on managed Connector Appliances or Software Connector Appliances using ArcMC:

- Reboot or shut down.
- Edit or remove a configuration.
- Set a configuration on one (or multiple) Connector Appliances.

> **Note:** Not all Connector Appliance functionality is manageable through ArcMC. For a complete discussion of Connector Appliance features, see the Connector Appliance Administrator's Guide.

Rebooting a ConApp

To remotely reboot a managed Connector Appliance:

1. Click **Node Management.**
2. In the navigation tree, click **System**.
3. In the management panel, click **ConApps**.

4. In the list of Connector Appliances, locate the Connector Appliance to be rebooted.
5. In the **Action** drop-down of the Connector Appliance, select **Reboot ConApp**.
6. Click **Next** to confirm reboot.
7. The Connector Appliance is rebooted. Click **Done**.

Shutting Down a ConApp

To remotely reboot a managed Connector Appliance:

1. Click **Node Management.**
2. In the navigation tree, click **System**.
3. In the management panel, click **ConApps**.
4. In the list of Connector Appliances, locate the Connector Appliance to be shut down
5. In the **Action** drop-down of the Connector Appliance, select **Shutdown ConApp**.
6. Click **Next** to confirm shutdown.
7. The Connector Appliance is shut down. Click **Done**.

Editing or Removing a Configuration for a ConApp

You can edit a configuration on, or remove property values of a list configuration from, a managed Connector Appliance.

Editing or removing a configuration will overwrite the node's current configuration. This may make the node non-compliant with its current subscriptions.

To edit or remove a configuration on Connector Appliance:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ConApps**.
4. In the list of Connector Appliances, locate the desired Connector Appliance.
5. In the **Action** drop-down of the Connector Appliance, select **Edit/Remove Config.** The Update Configurations wizard is launched.
6. Review the dialog box, and click **Next**.
7. Follow the prompts to complete the wizard.
8. When the wizard is complete, click **Done**.

> **Note:** In order to edit a backup configuration on a Connector Appliance node, the node must have a scheduled backup to begin with.

Setting a Configuration on ConApps

You can set a configuration on one or multiple Connector Appliances using the Set Configuration wizard.

- For list configurations, use the Set Configuration wizard to append property values to an existing configuration on multiple Connector Appliances. Only new values will be appended. For more information on list configurations, see "List Configurations" on page 885.
- For non-list configurations, use the Set Configuration wizard to overwrite the configuration on multiple Connector Appliances.

> **Caution:** Setting a configuration on one or multiple Connector Appliances may make each Connector Appliance node non-compliant with its current subscriptions.

To set a configuration on one or more Connector Appliances:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Connector Appliances**.
4. In the list of Connector Appliances, select one or more Connector Appliances.
5. Click **Set Configuration**. The Set Configuration wizard is launched.
6. Review the dialog box, and then click **Next**.
7. Follow the prompts to complete the wizard.
   - Click **Add Row** to add a new Property to a list configuration, and then enter values as needed.
8. The configuration is set on the selected Connector Appliances. Click **Done**.

Managing Other ArcSight Management Centers

You can perform any of the following management tasks on managed Software ArcSight Management Centers or ArcMC Appliances:

- Reboot or shut down.
- Edit or remove a configuration.

- Remotely upgrade an .
- Set a configuration on one (or multiple) ArcSight Management Centers.

Rebooting an ArcMC

To remotely reboot a managed ArcSight Management Center:

1. Click **Node Management.**
2. In the navigation tree, click **System**.
3. In the management panel, click **ArcMCs**.
4. In the list of ArcSight Management Centers, locate the ArcSight Management Center to be rebooted.
5. In the **Action** drop-down of the ArcMC, select **Reboot ArcMC**
6. Click **Next** to confirm reboot.
7. The ArcSight Management Center is rebooted. Click **Done**.

Shutting Down an ArcMC

To remotely shut down a managed ArcSight Management Center:

1. Click **Node Management.**
2. In the navigation tree, click **System**.
3. In the management panel, click **ArcMCs**.
4. In the list of ArcSight Management Centers, locate the ArcSight Management Center to be shut down.
5. In the **Action** drop-down of the ArcMC, select **Shutdown ArcMC**.
6. Click **Next** to confirm shutdown.
7. The ArcSight Management Center is shut down. Click **Done**.

Editing or Removing a Configuration for ArcMC

You can edit a configuration on, or remove property values of a list configuration from, a managed ArcSight Management Center.

Editing or removing a configuration will overwrite the node’s current configuration. This may make the node non-compliant with its current subscriptions.

To edit or remove a configuration on ArcSight Management Center:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ArcMCs**.
4. In the list of ArcSight Management Centers, locate the desired ArcSight Management Center.
5. In the **Action** drop-down, select **Edit/Remove Config**. The Update Configurations wizard is launched.
6. Review the dialog box, and then click **Next**.
7. Follow the prompts to complete the wizard.
8. When the wizard is complete, click **Done**..

> **Note:** In order to edit a backup configuration on an ArcMC node, the node must have a scheduled backup to begin with.

Upgrading ArcMC

> **Note:** Prior to upgrading a production system, make sure to have a rollback plan to minimize potential production down time. The rollback plan will restore an ArcMC to its working state prior to the upgrade.
> If there are any unexpected issues during or after the upgrade, implement the rollback plan. Restore the configuration backup of production to a staging environment. Test the upgrade in the staging environment to troubleshoot further.

In ArcMC, you can remotely upgrade any of the following managed ArcMC types and versions.

Form Factor	Upgrade File Name	Comments
Appliance	`arcmc-<build number>.enc`	
Software	`arcmc-sw-<build number>-remote.bin`	Remote operating system upgrade is not supported for software ArcMC, and, if required, must be performed manually.

Remote Upgrade Using Node Management

Remote upgrade first requires that you upload the appropriate file to your ArcMC repository first. You can then apply the upgrade file to managed ArcMCs.

To upload the upgrade file to your repository:

1. Download the ArcMC upgrade file for the upgrade version, as outlined in the table above, and store it in a secure network location.
2. Click **Administration > Repositories.**
3. In the navigation tree, pick **Upgrade Files.**
4. In the management panel, click **Upload**.
5. Click **Choose File** and browse to your upgrade file, then click **Submit**. The file is uploaded.

To remotely upgrade one or more managed ArcMCs:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ArcMCs**.
4. In the list of ArcMCs, select one or more ArcMCs for upgrade. (You may select only the form factor appropriate for the upgrade file type, as outlined above.)
5. Click **Upgrade ArcMC**. The Upgrade wizard is launched.
6. Review the dialog box, and then click **Next**.
7. Follow the prompts to complete the wizard.
8. When the wizard is complete, click **Done**.

Setting a Configuration on Managed ArcMCs

You can set a configuration on one or multiple ArcSight Management Centers using the Set Configuration wizard.

- For list configurations, use the Set Configuration wizard to append property values to an existing configuration on multiple ArcSight Management Centers. Only new values will be appended. (For more information on list configurations, see "The Configurations Table" on page 884.).
- For non-list configurations, use the Set Configuration wizard to overwrite the configuration on multiple ArcSight Management Centers.

> **Caution:** Setting a configuration on one or multiple ArcSight Management Centers may make each ArcSight Management Center node non- compliant with its current subscriptions.

To set a configuration on one or more ArcSight Management Centers:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ArcMCs**.
4. In the list of ArcSight Management Centers, select one or more ArcSight Management Centers for which to set a configuration.
5. Click **Set Configuration**. The Set Configuration wizard is launched.
6. Review the dialog box, and then click **Next**.
7. Follow the prompts to complete the wizard.
   - Click **Add Row** to add a new Property to a list configuration, and then enter values as needed.
8. The configuration is set on the selected ArcSight Management Centers. Click **Done**.

Managing SmartConnectors on ArcMC

ArcMC can remotely manage previously-installed, software-based SmartConnectors; however, the remote management feature is disabled on software SmartConnectors by default.

You can install several SmartConnectors on a single host if supported by the hardware. ArcSight certifies a maximum of 4 SmartConnectors on Windows hosts and 8 on Linux hosts.

To manage software-based SmartConnectors with , you need to enable remote management on each connector, as follows:

1. In a text editor, in the installation directory for the SmartConnector, open the file `/<install_dir>/user/agent/agent.properties.`
2. Add the line: `remote.management.enabled=true`
3. If desired, customize the connector's listening port. The default is 9001. To change this value, add the line: `remote.management.listener.port=<port_number>`, where `<port_number>` is the new port number.
4. Save the file.
5. Restart the SmartConnector for changes to take effect.

Managing Loggers

You can perform any of the following management tasks on managed Logger Appliances or Software Loggers using ArcMC.

- Reboot or shut down.
- Edit or remove a configuration.
- Set a configuration on one (or multiple) Loggers.
- Remotely upgrade a Logger.

> **Note:** Not all Logger functionality is manageable through ArcMC. For a complete discussion of Logger features, see the Logger Administrator's Guide.

Rebooting a Logger

To remotely reboot a managed Logger:

1. Click **Node Management.**
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, locate the Logger to be rebooted.
5. In the **Action** drop-down of the Logge, click **Reboot Logger**.
6. Click **Next** to confirm reboot.
7. The Logger is rebooted. Click **Done**.

Shutting Down a Logger

To remotely shut down a managed Logger:

1. Click **Node Management.**
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, select the Logger to be shut down.
5. In the **Action** drop-down of the Logger, select **Shut Down Logger**.
6. Click **Next** to confirm shut down.
7. The Logger is shut down. Click **Done**.

Editing or Removing a Configuration for a Logger

You can edit a configuration on, or remove property values of a list configuration from a managed Logger.

Editing or removing a configuration will overwrite the node's current configuration. This may make the node non-compliant with its current subscriptions.

To edit or remove a configuration on a managed Logger:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, locate the desired Logger.
5. In the **Action** drop-down of the Logger, select**Edit/Remove Config**. The Update Configurations wizard is launched.
6. Review the dialog box, and then click **Next**.
7. Follow the prompts to complete the wizard.
8. When the wizard is complete, click **Done**..

> **Note:** In order to edit a backup configuration on a Logger node, the node must have a scheduled backup to begin with.

Upgrading a Logger

Remote upgrades to Logger 7 require a previous hot-fix to be applied if Logger's versions are any of the following:

• 6.7.0.8242

• 6.7.1.8253

• 6.7.1.8257

• 6.7.1.8262

The hot fix file to be uploaded is **preupgrade-logger-20190924.enc**. The name should be kept as is.

To upload the file from the master ArcMC:

1. Download the hotfix file and store it in a secure network location. The file name should always be preupgrade-logger-20190924.enc depending on the form factor.
2. Click **Administration > Repositories.**
3. Select **Upgrade Files** from the navigation tree.
4. In the management panel, click **Upload.**

5. Click **Choose File** and browse to your hot fix file, then click **Submit.** The file is now uploaded.
6. Continue with the normal procedure outlined in the "To remotely upgrade one or more managed Loggers:" on the next page

In ArcMC, you can remotely upgrade any of the following managed Logger types.

Form Factor	Upgrade File Name	Can Upgrade From Version...	Can Upgrade To Version...	Comments
Appliance	`logger-<build number>.enc`	6.0 or later	6.1 or later	The filename format for the remote upgrade file for Logger Appliance is `logger-<build number>.enc`
Software	`logger-sw-<build number>-remote.enc`	6.0 or later	6.1 or later	• The filename format for the remote upgrade file for software Logger is `logger-sw-<build number>-remote.enc` • Remote operating system upgrade is not supported for software Logger, and, if required, must be performed manually.

Note: Upgrading to Logger version 6.0 requires ArcMC Agent 1167.1 or later to be running on the managed Logger. Upgrade the Agent on the managed Logger before performing the upgrade to Logger 6.0.

To upload the upgrade file to your repository:

1. Download the Logger upgrade file for the upgrade version, as outlined in the table above, and store it in a secure network location.
2. Click **Administration > Repositories.**
3. In the navigation tree, pick **Upgrade Files.**
4. In the management panel, click **Upload.**
5. Click **Choose File** and browse to your upgrade file, then click **Submit**. The file is uploaded.

To remotely upgrade one or more managed Loggers:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, select one or more Loggers. (You may only select one form factor type to upgrade.)
5. Click **Upgrade Logger**. The Upgrade wizard is launched.
6. Review the dialog box, and then click **Next**.
7. Follow the prompts to complete the wizard.
8. When the wizard is complete, click **Done**.

> **Note:** In some cases, after the upgrade of a localhost with an .enc file completes, an empty page is displayed. You may navigate away from this page as normal.

Setting a Configuration on Loggers

You can set a configuration on one or multiple Loggers using the Set Configuration wizard.

- For list configurations, use the Set Configuration wizard to append property values to an existing configuration on multiple Loggers. Only new values will be appended. For example, if you had a common group of users on three Loggers, you could use the Set Configuration wizard to add the same new user to all three Loggers with a single action. (For more information on list configurations, see "The Configurations Table" on page 884.)
- For non-list configurations, use the Set Configuration wizard to overwrite the configuration on multiple Loggers.

> **Caution:** Setting a configuration on one or multiple Loggers may make each Logger node non-compliant with its current subscriptions.

To set a configuration for one or more Loggers:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, select one or more Loggers for which to set a configuration.
5. Click **Set Configuration**. The Set Configuration wizard is launched.
6. Review the dialog box, and click **Next**.
7. Follow the prompts to complete the wizard.
   - Click **Add Row** to add a new Property to a list configuration, and then enter values as needed.
8. The configuration is set on the selected Loggers. Click **Done**.

Managing Containers

A *container* is a single Java Virtual Machine (JVM) that can run up to four connectors. The exact number of connectors depends on your current service agreement and the type of connector.

Containers may run on ArcMCs, on Connector Appliances, and on L77XX model Loggers. The number of containers that can be run at one time is based on the product license. Check under **System Admin > License & Update** for this information.

Scanning a managed host will ensure all currently running containers on the host (and the connectors associated with them) are accurately inventoried. For more information, see "Scanning a Host" on page 943.

Note: A connector of any of the following types must be the single connector running in its container:

- Trend Micro Control Manager (TMCM)
- Syslog
- Windows Unified Connector (WUC)

Note: For Microsoft Windows Event Log (WINC), only one connector can be created on an ArcMC appliance.

Viewing All Containers

You can view all containers managed in ArcMC.

To view all containers:

1. Click **Node Management**
2. In the navigation tree, click **System**. (Alternatively, to view containers on a specific host, select the host from the navigation tree.)
3. Click the **Containers** tab to display the containers.

Viewing Connectors in a Container

You can see all the connectors in a container.

To view connectors in a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the container whose connectors you wish to view.
3. Click the tree branch corresponding to the container.
4. Click the **Connectors** tab. The connectors in the container are displayed.

Editing a Container

The default name for a container is *Container N*, where N is a sequential number that indicates the order in which the container was added. However, you can edit a container's default name.

To edit a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host with container you wish to rename.
3. In the list of containers, locate the container you wish to edit.
4. In the **Action** drop-down of the container, click **Edit Container.**
5. In **Name,** enter the new container name, and then click **Next**.
6. Click **Done**. The container is renamed.

Deleting a Container

When you delete a container, the connectors that it contains are also deleted.

To delete a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to delete.
5. Click **Delete**.
6. Click **OK** to confirm deletion. The selected containers are deleted.

Note: Containers on appliances can't be deleted.

Changing Container Credentials

You can change the user name and password associated with each container.

Caution: A container's default user name is `connector_user` and the default password is `change_me`. ArcSight strongly recommends that for optimal security, you should change each container's credentials to a non-default value before deploying it to production.

To change container credentials:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers for which to change the credentials.

5. Click **Credentials**.
6. Follow the instructions in the wizard to update the credentials for the selected containers.

Sending a Command to a Container

You can run commands on a container to configure memory settings, pull an OPSEC certificate, generate a key, or restart the container.

To run a command on a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. In the **Action** drop-down of the container, click **Send Container Command.** The Send Command wizard starts.
5. From the drop-down list, select the command you want to send, and then click **Next**.
6. Enter appropriate values for the parameters and then click **Done**.

Upgrading All Connectors in a Container

You can upgrade all connectors in a container to a specific parser or framework version number.

Before Performing the Upgrade

Prior to performing a container upgrade, you will need to follow the steps below:

For connectors running 32-bit with version < 7.11, it is required to perform 32-bit to-64 bit migration before upgrading to a connector running >=7.11.

32-bit to 64-bit container migration.

1. Upgrade the appliance you currently have (a G8 migrated from conapp to ArcMC) to the latest ArcMC build.
2. Back up the container using the repositories page.
3. Emergency restore the container to the 64 bit connector AUP.
4. Restore the backup to the container using the repositories page.
    - **Case #1:** G8 appliances: model >= 6500 and restoreToVersion >= 7.9.0.8084 OR if connector is restored to any version less than 7.9.0, the connector will get restored to 32 bit, if connector is restored to any version greater than 7.9.0, the connector will get

restored to 64 bit.

- **Case #2:** G9 appliances: model >= 6600 and restoreToVersion >= 7.2.1.7714.0 if connector is restored to any version less than 7.2.1 - restore should not be allowed, if connector is restored to any version greater than 7.2.1, the connector will get restored to 64 bit.

> **Note:** The above Emergency Restore to perform 32-bit to 64 bit connector migration does not support Appliances running on C5500 model.

To upload a version file to your repositories.

You can use a connector AUP file of the new parser or framework version in your ArcMC repository. If you opt to use this method, you will need to upload the version file to your repository as follows:

1. Click **Administration > Repositories.**
2. In the navigation tree, pick **Upgrade Files.**
3. In the management panel, click **Upload**.
4. Click **Choose File** and browse to your connector AUP file, then click **Submit**. The file is uploaded.

- Alternatively, instead of using a parser AUP file from the repository, you can download and use parser files from the ArcSight Marketplace. (Framework files are not available from the Marketplace.) Create your administrative account on the ArcSight Marketplace. If you have not created your Marketplace account, you will be given an opportunity to sign up for an account during the parser upgrade process.

To perform the parser or framework upgrade on all connectors in a container:

1. Click **Node Management.**
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to upgrade.
5. Click **Upgrade**.
6. On the upgrade page, under **Select Upgrade Type,** choose either **Parser upgrade** or **Framework upgrade.**
7. Under **Select Upgrade Version,** from the drop-down list, choose the version to which you want to upgrade the selected containers. (You can control the number of parser upgrade versions displayed in the drop-down, as described in Modifying logger.properties.)(You can select the number of parser upgrade versions displayed in the drop-down as described in

"Configuring ArcMC Parser Upgrades" on page 265)

a. For a parser upgrade, if the selected parser version is from the Marketplace and not the local repository, save your Marketplace credentials in ArcMC. This is a one-time task unless you wish to update these credentials.

8. Click **Upgrade**. The upgrade is performed on all containers.

> **Note:** If you are performing parser upgrades through a proxy server, additional configuration is required. See Modifying logger.properties for more information.

Restarting a Container

Restarting a container will restart all the connectors in the container. You can restart multiple containers in bulk.

To restart one or more containers:

1. Click **Node Management.**
2. In the navigation tree, navigate to the host on which a container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to restart.
5. Click **Restart**.
6. Click **Yes** to confirm restart. The selected containers are restarted.

Viewing Container Logs

You can retrieve and view the log files for one or more containers. The log files are in `.zip` format.

Container logs must be uploaded to the Logs repository before they can be viewed. For instructions on how to upload logs, see "Uploading a File to the Logs Repository" on page 568.

To retrieve and view container logs:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers for which to view logs.
5. Click **Logs**.

6. Click **Next** to begin the **Retrieve Container Logs** process. When complete, click **Done**.
7. Click **Administration** > **Repositories.**
8. In the left panel, click **Logs**.
9. In the management panel, click to retrieve the log files (in `.zip` format) you want to view.

Deleting a Container Log

You can delete unneeded container logs as necessary.

To delete a container log file:

1. Click **Administration > Repositories.**
2. In the left panel, click **Logs**.
3. In the management panel, on the list of logs, click next to the log file you want to delete.
4. Click **OK** to confirm deletion.

Enabling FIPS on a Container

FIPS mode is supported on local, and remote Connectors running version 4.7.5 or later, but certain connectors do not support FIPS mode. For information about which connectors do not support FIPS mode, see the Installing FIPS-Compliant SmartConnectors document at ArcSight SmartConnectors 24.2 documentation. Before enabling FIPS on a container that contains connectors running as a service, review the caveats listed in that document.

FIPS is disabled by default on ArcSight Management Center, but can be enabled as described under FIPS 140-2. After FIPS is enabled on the appliance, you can enable FIPS on a container. Any FIPS-compliant connector in that container (or one which is added later) will automatically communicate in FIPS mode.

- If the connector destination is ArcSight Manager, Connector Management automatically imports the ArcSight Manager certificate into its trust store and applies it to the container.
- However, if the connector destination is Logger, the Logger certificate must be uploaded manually and applied to the container.

A FIPS Suite B certificate must be uploaded manually, regardless of the connector destination, as described in under “Enabling FIPS Suite B on a Container”, below.

You enable or disable FIPS using the same procedure.

To enable or disable FIPS mode on a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers for which to enable FIPS.
5. Click **FIPS**.
6. Follow the instructions in the wizard to update FIPS status.

Check that the appropriate CA certificates are in the trust store so that the connectors in the container can validate their configured destinations successfully. If necessary, add the appropriate certificates to the container.

> **Note:** A 32-bit FIPS connector enabled cannot be remotely managed if it is installed on a 64-bit Linux system.

Enabling FIPS Suite B on a Container

Managed connectors can communicate in FIPS Suite B mode with their destination. A FIPS Suite B certificate must be imported manually and applied to the container, regardless of the connector destination.

Before you perform the following procedure, make sure FIPS mode is enabled on ArcSight Management Center, as described in FIPS 140-2.

To enable FIPS Suite B on a container:

1. Export the certificate for the connector destination (either ArcSight Manager or Logger) to a temporary directory. For example, on ArcSight Manager, from $ARCSIGHT_HOME/current/bin, specify the following command: `./arcsight runcertutil -L -n mykey -r -d /opt/arcsight/manager/config/jetty/nssdb -o /tmp/managercert.cer`
2. Upload the certificate from the temporary directory to the CA Certs Repository, as described in "CA Certs Repository " on page 569.
3. Enable FIPS on the container as described above.
4. Add the certificate on the container, as described in "Managing Certificates on a Container" on page 855 .
5. Click **Node Management**.
6. In the navigation tree, navigate to the host on which the container resides.
7. Click the **Containers** tab.

8. On the **Containers** tab, select one or more containers for which to enable FIPS Suite B.
9. Click **FIPS**.
10. Follow the instructions in the wizard to update FIPS Suite Bstatus.

Adding a Connector to a Container

Each container may hold up to 4 connectors.

To add a connector to a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the container to which you wish to add a connector.
3. On the **Connectors** tab, click **Add Connector**. The **Connector Setup** wizard starts.
4. Click **Next**, and then follow the prompts to set up the new connector.

> **Note:** Always change the default credentials of any new connector to non-default values. For more information, see "Changing Container Credentials" on page 848.

Running Logfu on a Container

The **Logfu** utility is a diagnostic tool that parses ArcSight logs to generate an interactive visual representation of the information contained within the logs. When event flow problems occur, it can be useful to have a visual representation of what happened over time.

To run Logfu on a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, locate a container on which to run Logfu.
5. In the **Action** drop-down of the container, click **Run Logfu.**
6. The Logfu progress window is displayed as system data logs are retrieved and analyzed. Data is then displayed by **Group**, **Field**, and **Chart**.
   - In the **Group** box, choose which type of data you would like to view. The **Group** box lists all connectors within the chosen container, plus many other types of data such as memory usage and transport rates.
   - Then, choose one of the Group box **data points**. Depending on which data point you chose, a list of fields appears in the Field box below.

- Choose a **field** to view. A graphic chart appears in the Chart box, providing rate and time information. The key at the bottom of the Chart box defines the data points mapped in the chart.
- To choose a different data point for analysis, click **Reset Data**.

7. When complete, close the display window.

Managing Certificates on a Container

Connectors require a Certificate Authority (CA) issued or self-signed SSL certificate to communicate securely with a destination. The Certificate Management wizard, available from the **Containers** tab, helps you add and remove certificates on a container. Using the wizard, you can:

- Add a certificate to a container.
- Add certificates in bulk, enabling multiple containers at once.
- Enable or disable a demo certificate on a container that is in non-FIPS mode only.
- Add a CA Certs file on a container that is in non-FIPS mode only.
- Remove a certificate from a container.

From the **Containers** tab and the **Connectors** tab, you can view details about the certificates applied to a container. See "Viewing Certificates on a Container" on page 858.

For information about resolving invalid certificates, see "Resolving Invalid Certificate Errors" on page 859.

Adding CA Certificates to a Container

You can add a single CA certificate to a container that is in FIPS mode or non-FIPS mode.

> **Note:** Whenever you enable or disable FIPS mode on a container, check that the required certificates are present in the trust store and add them if necessary.
>
> Click the icon next to the container name to see the type of certificate applied to it. Click **Display Certificates** from the action drop down to see the list of available certificates on the container.

Before you perform the following procedure, make sure the certificate you want to add is loaded in the CA Certs repository.

To add a single CA certificate to a container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.

4. On the **Containers** tab, select one or more containers to which you wish to add certificates.
5. Click **Certificates**. The Certificate Management wizard starts.
6. Review the dialog box, and then click **Next**.
7. Under **Choose an Action**, select **Add Certificate**, and then click **Next**.
8. Follow the instructions in the wizard to add the certificate.

   If a container is down or a connector is running an older build, the wizard reports errors in the progress bar and on the Summary page.

Removing CA Certificates from a Container

You can remove CA certificates from a container when they are no longer needed. When you remove a CA certificate, the certificate is removed from the container's trust store; but it is **not** deleted from the repository.

> **Caution:** Use caution when deleting certificates. When you delete a certificate on a container but the connector destination is still using that certificate, the connector can no longer communicate with the destination.

To remove CA certificates from a container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to which you wish to remove certificates.
5. Click **Certificates**. The **Certificate Management** wizard starts.
6. Review the dialog box, and then click **Next**.
7. Under **Choose an Action,** select **Remove certificate**, and then click **Next**.
8. Select one or more certificates from the certificate list, and then click **Next**. The certificates are removed from the list of certificates and no longer used. When you remove a certificate from a container in FIPS mode, the container restarts automatically.
9. The Certificate Management wizard displays the certificates that are removed successfully in a comma-separated list. Certificates that cannot be removed are shown in a comma-separated list together with a reason why the certificate removal failed.

Adding a CA Certs File to a Container

You can add a CA Certs file to any container that is in non-FIPS mode.

Caution: When you apply a CA Certs file, the entire trust store on the container is overwritten. All previously-added certificates are overwritten.

Before you follow the procedure below, make sure that the CA Certs file you want to add is loaded in the CA Certs repository.

To add a CA Certs file to a non-FIPS mode container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, Select one or more non-FIPS mode containers to which you wish to add a CA Certs file.
5. Click **Certificates**. The **Certificate Management** wizard starts.
6. Review the dialog box, and then click **Next**.
7. Under **Choose an Action,** select **CA Cert (Legacy)**.
8. Follow the instructions in the wizard.

   After the CA Certs file has been added to a container, the container restarts automatically.

Enabling or Disabling a Demo Certificate on a Container

You can use the demo certificate on a container for testing purposes. By default, the demo certificate on a container is disabled. You can enable the demo certificate temporarily for testing purposes on a container that is non-FIPS mode.

Note: Enable a *demo* certificate on a container in non-FIPS mode for testing purposes only. Using a demo certificate in a production environment is a serious security issue because the demo certificate is not unique.

To enable or disable a demo certificate on a non-FIPS mode container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, Select one or more non-FIPS mode containers for which you wish to enable or disable a CA Certs file.
5. Click **Certificates**. The **Certificate Management** wizard starts.
6. Review the dialog box, and then click **Next**.

7. Under **Choose an Action**, select **Demo CA (Legacy)**, and then click **Next**.
8. Follow the instructions in the Certificate Management wizard.

   After you add the demo certificate on a container, the container restarts automatically.

Adding Multiple Destination Certificates to a Container

You can add multiple destination certificates to a container, whether in FIPS mode or not.

> **Note:** Whenever you enable or disable FIPS mode on a container, check that the required certificates are present in the trust store and add them if necessary.
>
> Click the icon to display a list of the certificates available on the container.

> **Note:** In the event that importing destination certificates for Transformation Hub fails due to changes in the certificate, please proceed to **remove** and then **add** the destination from the Connector as explained in "Removing Destinations" on page 868 and "Adding a Primary Destination to a Connector" on page 865.

To apply multiple destination certificates to a container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, containers for which you wish to add multiple destination certificates.
5. Click **Certificates**. The **Certificate Management** wizard starts.
6. Review the dialog box, and then click **Next**.
7. Under **Choose an Action**, select **Import destination certificates** to add a certificate.
8. Follow the instructions in the wizard to complete the process.

Viewing Certificates on a Container

You can display a list of the CA certificates applied to a container and view the details for a particular certificate in the list. To view certificates on a container,

- On the **Containers** tab, in the **Action** drop-down for the container whose certificates you want to view, select **Display Certificates.**
- On the **Connectors** tab, click **Certificates** at the top of the page.

The Certificate List wizard displays the certificates applied to a container. To see details of a certificate, select the certificate, and then click **Next** at the bottom of the page.

Resolving Invalid Certificate Errors

If no valid CA certificates exist for the connectors in the container, resolve the invalid certificate error as follows:

To resolve the invalid certificate error:

1. Select the container in the navigation tree.
2. Click the **Containers** tab. The error message is displayed.
3. In the **Action** drop-down of the container showing the issue, select **Download Certificates.**
4. Follow the instructions in the wizard to download and import the valid certificates.

Running Diagnostics on a Container

You can run diagnostics on a container.

> **Note:** Diagnostic tools are also provided under **Administration** > **System Admin**.

To run diagnostics on a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers for which to run diagnostics.
5. In the **Action** drop-down, click **Run Logfu**. The Diagnostics wizard starts.
6. Select the action you want to take on the selected container:
   - Select **Edit a configuration file** to edit a file in the `user/agent` folder on the container with the extension `.properties`, `.csv`, or `.conf`.
   - Select **Edit a user file** to edit any file (except binary files, such as `.zip`, `.jar`, or `.exe`) in the `user/agent` folder on the container.
7. From the list of available files, select the file you want to edit. The file displays in the Edit File panel. Make your edits, and then click **Next** to save your edits and restart the container.

   > **Note:** When you click **Next**, ArcMC saves the updated file in the `user/agent` folder on the container. The original file is overwritten.

8. Click **Done** to close the Diagnostics wizard.

Managing Connectors

A *connector* (also known as a *SmartConnector*) is an ArcSight software component that collects events and logs from various sources on your network. A connector can be configured on ArcMC, on a Logger platform with an integrated Connector Appliance, or installed on a computer on your network, managed remotely. When a connection is managed by ArcMC, runagentsetup can no longer be used to handle that connector. For a complete list of supported connectors, go to the ArcSight Customer Support site.

Procedures for managing connectors are described below.

Viewing All Connectors

You can see all currently managed connectors.

To view all connectors:

1. Click **Node Management**.
2. Click **System** in the navigation tree.
3. In the management panel, click the **Connectors** tab. All connectors display on the **Connectors** tab in the management panel.

Adding a Connector

Prerequisites

Before you add a connector, review the following important information.

- Make sure that the container, host, and location to which you want to add the connector exist in ArcMC. If any of these elements do not exist, create them.
- Follow the configuration best practices described in "Configuration Suggestions for Connector Types " on page 881.
- For more information see SmartConnectors 24.2 Grand List (A-Z)
- If you are adding a software-based connector, make sure that the username and password for the connector match the username and password for the container to which you are adding the connector. If necessary, refer to "Changing Container Credentials" on page 848.

> **Caution:** Each connector's default user name is `connector_user` and the default password is `change_me`. A connector with these default values still in place should be considered non-secure. ArcSight strongly recommends that for optimal security, you should change each connector's credentials to non-default values before deploying the connector to production.

- File-based connectors use the Common Internet File System (CIFS) or Network File System (NFS). These stipulations apply when creating a local connector to run as part of ArcMC.
  - On a Windows system, a CIFS share needs to be configured before you add a file-based connector.
  - For all other connectors, an NFS mount needs to be established before a file-based connector can be added. In addition, when entering the connector parameters, enter the configuration file name without an extension in the **Configuration File** field. The extension `.sdkrfilereader.properties` is appended automatically.
- For detailed information about individual connector parameters, refer to the specific ArcSight SmartConnector Configuration Guide for the type of connector chosen. The configuration guide also describes how to set up the source device for use with the connector

To add a connector:

> **Tip:** If you are adding a connector for the Check Point FW-1/VPN-1 system, see a more detailed procedure in "Configuring the Check Point OPSEC NG Connector" on page 1.

1. Click **Node Management**.
2. In the navigation tree, browse to the host on which the connector will reside.
3. In the management panel, click the **Containers** tab.
4. On the **Containers** tab, locate the container where you will assign the connector.
5. In the **Action** drop-down, click **Add Connector.** The Connector Setup wizard starts.
6. Review the dialog box, and then click **Next**.
7. Select a connector type from the pull-down list of available types, and then click **Next**.
8. Enter basic parameters for the connector. Parameters vary based on the connector type. (Hover over a field for more information on a field.) When all fields have been entered, click **Next**.

   > **Note:** When entering parameters that include a file path, enter the path in POSIX format (for example, `/folder/filename`).

For file-based connectors on Windows systems, specify the name of the CIFS mount point you created for the connector. (You need to specify `/opt/mnt/CIFS_share_name`.)

Some connectors include table parameters. For example, the Microsoft Windows Event Log includes parameters for each host in the domain and one or more log types (security, application, system, directory service, DNS, file replication, and so on). You can import table parameters from a CSV file that was exported from another connector, as long as you export it and import it from the same containers. If the CSV file was exported from a different container, you need to change the secret parameters, such as the password, which appear in obfuscated format in the CSV file to plain text before you import the CSV file.

> **Note:** For connectors that query Microsoft Active Directory to detect devices, if the "Network Security: LDAP Server Signing Requirements" policy is set to "Signing Required" on the Domain Controller, ArcMC will be unable to connect to the Active Directory or browse for devices. You see an error when selecting **Windows Host Browser** as the connector device browser type.

9. Choose a primary destination for the connector and enter destination-specific parameters on the following page(s), and then click **Next**.

   - > **Note:** FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.
     >
     > To see certificate details, hover over the certificate.
     >
     > - Select **Import the certificate to the connector from the destination**, and then click **Next** to import the certificate and continue.
     > - Select **Do not import the certificate to the connector from the destination, and then click Next** if you do not want to import the certificate. The destination will not be added.

10. Enter connector details:

Parameter	Description
Name	A descriptive name for this connector.
Location	The location of the connector (such as the hostname).
Device Location	The location of the device that sends events to the connector.
Comment	Additional comments.

11. When complete, click **Done**.

Editing Connector Parameters

ArcSight supports a large number of connector types to gather security events from a variety of sources, including syslog, log files, relational databases, and proprietary devices. Accordingly,

configuration parameters vary widely depending on the type of connector being configured.

You can edit parameters (simple and table) for a specific connector, or for multiple connectors of the same type at the same time.

Updating Simple Parameters for a Connector

The following procedure describes how to update simple parameters for a specific connector.

To update parameters for a specific connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector you wish to update.
3. In the management panel, the **Connector** summary tab displays.
4. On the **Connector** tab, next to **Connector Parameters,** click .
5. Modify parameters as necessary, and then click **Next**.

   Note: When editing parameters that include a file path, enter the path in POSIX format (for example, `/folder/filename`).

6. When complete, click **Done**. The updated parameters display in the **Connector Parameters** table of the Connector summary tab.

Updating Table Parameters for a Connector

Certain connectors, such as the Microsoft Windows Event connector, have table parameters. You can update the table parameters for a specific connector when necessary.

To update table parameters for a specific connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector you wish to update. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, next to **Table Parameters,** click .
4. Modify parameters as necessary and then click **Next**.
   - To add more rows of parameter information, click the **Add Row** link.
   - You can use an Excel-compatible program to prepare a comma-separated values text file with the information and click the **Import File** button to load the entire table at once. The file needs to be in the same format as the rows shown on the Update Table Parameters page, and it needs to include a header row with parameter labels in the

order shown on that page. For fields that require checkbox values, enter True or False as the value. An example is shown below.

	A	B	C	D	E	F
1	Domain Name	Host Name	User Name	Password	Security Logs	System Logs
2	test	1.1.1.1	admin	password	TRUE	FALSE
3	test2	1.1.1.1.1	admin	password	TRUE	FALSE

5. When complete, click **Done**. The updated table parameters display in the Table Parameters section of the Connector page.

> **Note:** You can import a CSV file that was exported from another connector as long as you export and import the CSV file from the same container. If the CSV file was exported from a different container, you need to change the secret parameters, such as the password, which appear in obfuscated format in the CSV file to plain text before you import the CSV file.

Updating Simple and Table Parameters for Multiple Connectors

If you have multiple connectors of the same type, you can change the simple and table parameters for all the connectors at the same time.

To edit parameters for multiple connectors of the same type:

1. Click **Node Management**.
2. In the navigation tree, select the host where the connectors reside.
3. In the management panel, select the connectors whose parameters you want to update.
4. Click **Parameters**. The Update Connect Parameters wizard starts.
5. Review the dialog box, and then click **Next**.
6. Follow the instructions in the wizard.
   - You can choose to modify the simple parameters for all the selected connectors at once or modify the simple parameters per connector.
   - If the connectors have table parameters, the table parameters are displayed so that you can modify them. If you have many table parameters to modify for multiple connectors, you can import the parameters from a CSV file. You can also export the table parameters to a CSV file for use as a backup or to import on another Connector Appliance.

     > **Note:** When you update parameters for connectors of different versions, the newer connectors might have additional parameters. In this case, only those parameters shared by all connectors are displayed for updating.
7. Click **Done** when complete.

Managing Destinations

Connectors can forward events to more than one destination, such as ArcSight Manager and ArcSight Logger. You can assign one or more destinations per connector. You can assign multiple destinations to a connector and specify a failover (alternate) destination in the event that the primary destination fails.

The following procedures describe how to perform these actions on a specific connector or for multiple connectors at the same time:

- Add a primary or failover destination
- Edit destination parameters and destination runtime parameters
- Remove destinations
- Re-register destinations
- Manage alternate configurations for a destination
- Send a command to a destination

> **Note:** Compared to the standalone Connector destination list, ArcMC Appliance on-board Connector does not cover the following three options: CEF file, CSV file and Raw Syslog

> **Note:** In the event that the Transformation Hub certificate changes, the Connectors that had that Transformation Hub as a destination will be lost. To re-enable them follow the steps under ----new section---

Adding a Primary Destination to a Connector

When you add a primary destination to a connector, you need to enter details for the destination, such as the destination hostname and port used.

To add a primary destination to a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector to which you wish to add a destination. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, next to **Destinations**, click + . The Add Destination wizard starts.
4. Follow the steps in the wizard. You can either select an existing destination or add a new destination. If you are adding a new destination, select the destination type and enter parameters for the destination. Destination types are described in the SmartConnector

User's Guide.

> **Note:** For containers running 5.1.2.5823 and later, ArcMC retrieves the certificate for the ArcSight Manager destination automatically and displays the certificate summary.
>
> For containers running 5.1.2 and earlier, upload the certificate on the container and then add the destination.
>
> FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.
>
> To see certificate details, hover over the certificate.
>
> - Select **Import the certificate to the connector from the destination**, and then click **Next** to import the certificate and continue.
> - Select **Do not import the certificate to the connector from the destination** and click **Next** if you do not want to import the certificate. The destination will not be added.

5. Click **Done** when complete.

Adding a Failover Destination to a Connector

Each destination can have a failover destination in case the connection with the primary destination fails.

> **Tip:** UDP connections cannot detect transmission failure. Use Raw TCP for CEF Syslog destinations.

To add a failover destination to a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector to which you wish to add a destination. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click . The Add Destination wizard starts.
4. Follow the steps in the wizard to select from available destinations and enter the destination details.

> **Note:** FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.
>
> To see certificate details, hover over the certificate.
>
> - Select **Import the certificate to the connector from the destination**, and then click **Next** to import the certificate and continue.
> - Select **Do not import the certificate to the connector from the destination** and click **Next** if you do not want to import the certificate. The destination will not be added.

5. Click **Done** when complete.

Adding a Primary or Failover Destination to Multiple Connectors

You can add a primary or failover destination to several connectors at the same time.

To add a primary or failover destination to multiple connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors to which you wish to assign a destination.
5. Click + **Destinations. The Manage Destinations wizard launches**.
6. Review the dialog, and then click **Next**.
7. Under **Choose an Option**, select **Add a destination, and then click Next**.
8. Choose between creating a new destination or selecting an existing destination, and then click **Next**.
   - If you choose to **create a new destination**, select the destination type and then provide the destination parameters. Destination types are described in the SmartConnector User's Guide.
   - If you choose to **select an existing destination**, select a destination from the list.

     > **Note:** ArcMC retrieves the ArcSight Manager certificate for the destination automatically and displays the certificate summary.
     >
     > FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.
     >
     > To see certificate details, hover over the certificate.
     >
     > - Select **Import the certificate to the connector from destination**, and then click **Next** to import the certificate and continue.
     > - Select **Do not import the certificate to the connector from the destination** and click **Next** if you do not want to import the certificate. The destination will not be added.
9. Define the destination function by choosing between a primary or failover destination.
   - If you choose **Primary destination**, click **Next** to update the configuration.
   - If you choose **Failover destination**:
     a. Select the primary destination that applies to your failover.
     b. Check the box in the table header to modify all of the displayed connectors.

   c. Click **Next** to update the configuration.

10. Click **Done** when complete.

Removing Destinations

You can remove a destination from a connector at any time. Each connector must have at least one destination; as a result, you may not remove all destinations from a connector.

To remove destinations from one or more connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors to which you wish to remove a destination.
5. Click **Destinations. The Manage Destinations wizard launches**.
6. Review the dialog, and then click **Next**.
7. Under **Choose an Option**, select **Remove a destination, and then click Next**.
8. Follow the instructions in the wizard, and click **Done** when complete.

Re-Registering Destinations

At certain times, you might need to re-register the destinations for one or more connectors; for example, after you upgrade ESM, or if a Logger appliance or ESM appliance becomes unresponsive.

To re-register destinations for one or more connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors to which you wish to assign a destination.
5. Click **Destinations. The Manage Destinations wizard launches**.
6. Review the dialog, and then click **Next**.
7. Under **Choose an Option**, select **Re-register destinations,** and then click **Next**.
8. Follow the instructions in the wizard and click **Done** when complete.

Editing Destination Parameters

The following procedures describe how to edit destination parameters for a specific connector and how to edit destination parameters for multiple connectors.

> **Note:** When enabling the demo CA for one or more connectors, use the Certificate button, instead of editing the ESM destination.

To edit destination parameters for a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector to which you wish to edit destination parameters. In the management panel, the **Connector** summary tab displays.
3. In the **Destinations** table, click next to the destination you want to edit to display the **Edit Destination Parameters** page.
4. Make your changes, and then click **Next**.
5. Click **Done** when complete.

To edit destination parameters for multiple connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors for which you wish to edit destination parameters.
5. Click **Destinations. The Manage Destinations wizard opens.**
6. Review the dialog, and then click **Next**.
7. Under **Choose an Option**, select **Edit a destination**, and then click **Next**.
8. Follow the instructions in the wizard and click **Done** when complete.

Editing Destination Runtime Parameters

The runtime parameters for a destination enable you to specify advanced processing options such as batching, time correction, and bandwidth control. The parameters you can configure are listed in "Destination Runtime Parameters " on page 945. The user interface automatically displays the parameters valid for a destination.

The following procedures describe how to edit the runtime parameters for a specific connector and how to edit the runtime parameters for multiple connectors at the same time.

To edit destination runtime parameters for *a* connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to edit destination runtime parameters. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click next to the destination whose runtime parameters you want to edit.
4. Under **Add Alternate Configurations**, click next to the alternate configuration that you want to edit.

   If you have not set up alternate configurations, click next to the **Default**. For more information about alternate configurations, see "Managing Alternate Configurations " below.
5. Specify or update values for the listed parameters, and then click **Save**.

To edit destination runtime parameters for *multiple* connectors at the same time:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors for which you wish to edit destination runtime parameters.
5. Click **Runtime Parameters** to open the wizard.
6. Follow these steps in the wizard to edit the runtime parameters:
   a. Select the destinations whose runtime parameters you want to modify.
   b. Select the configurations to be affected (default or alternate configurations).
   c. Select the group of parameters you want to modify (for example, batching, cache, network, processing).
   d. Modify the parameters.

Managing Alternate Configurations

An *alternate configuration* is a set of runtime parameters that is used instead of the default configuration during a specified portion of every day. For example, you might want to specify different batching schemes (by severity or size) for different times of a day. You can define more than one alternate configuration per destination, and apply them to the destination for different time ranges during the day. For example, you can define a configuration for 8 a.m. to 5 p.m. time range and another configuration for the 5 p.m. to 8 a.m. time range.

By default, a configuration labeled **Default** is applied to a destination. Any subsequent configurations you define are labeled **Alternate#1**, **Alternate#2**, and so on. The default configuration is used if the time ranges specified for other alternate configurations do not span 24 hours. For example, if you specify an alternate configuration, **Alternate#1** that is effective from 7 a.m. to 8 p.m., the **Default** configuration is used from 8 p.m. to 7 a.m.

If you need to apply the same alternate configuration for multiple destinations, you need to define an alternate configuration (with the same settings) for each of those destinations.

Defining a New Alternate Configuration

The process of defining a new alternate configuration includes first defining the configuration, and then editing it to specify the time range for which that configuration is effective.

To define an alternate configuration:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to edit destination runtime parameters. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click .
4. Under **Add Alternate Configurations,** click **Add**.
5. Specify or update values for the listed parameters.
6. Click **Save**. If this is the first alternate configuration you defined, it is saved as Alternate#1. Subsequent configurations are saved as Alternate#2, Alternate#3, and so on.

   To specify the effective time range for which the configuration you just defined, edit the configuration you just defined using the following procedure, "Editing an Alternate Configuration" below.

Editing an Alternate Configuration

In addition to editing an alternate configuration to change parameter values, you can edit it to specify the time range for which it is effective.

To edit an alternate configuration:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to edit destination runtime parameters. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click .

4. From the list of alternate configurations, select the alternate configuration that you want to edit, and then click .
5. Specify or update values for the listed parameters, including the time range in the From Hour/To Hour.
6. Scroll down to the end of the page and click **Save**.

Editing Alternate Configurations in Bulk

If you need to update the same parameters in multiple alternate configurations, follow the procedure described in "Editing Destination Runtime Parameters" on page 869.

Sending a Command to a Destination

You can send a command to a connector destination.

To send a command to a destination on a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to send a command. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click .
4. Select the command you want to run, and then click **Next**.
5. Enter values for the parameters that the user interface displays, and then click **Finish**.

Deleting a Connector

To delete one or more connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all the connectors you want to delete.
5. Click **Delete**.
6. Click **OK** to confirm deletion.
7. Reboot the Connector Appliance or Logger system that each connector was associated with.

Note: You can also delete a specific connector from its **Connector** summary tab. Click ✕ at the top of the tab to delete the connector.

Sending a Command to a Connector

You can send a command to a connector.

To send a command to a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector to which you wish to send a command. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, click **Connector Command.**
4. From the **Command Type** drop-down list, select the command you want to send to the connector, and then click **Next**.

Running Logfu on a Connector

Run Logfu on a connector to parse ArcSight logs and generate an interactive visual representation of the information contained within the logs.

To run Logfu on a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector to which you wish to run Logfu. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, click **Run Logfu.**
4. The Logfu progress window is displayed as system data logs are retrieved and analyzed. Data is then displayed by **Group**, **Field**, and **Chart**.
   - In the **Group** box, choose a data type to view. The **Group** box lists all connectors within the chosen container, plus many other data types, such as memory usage and transport rates.
   - Next, choose one of the **Group** box **data points**. Depending on which data point you chose, a list of fields appears in the **Field** box below.
   - Choose a **field** to view. A graphic chart appears in the **Chart** box, providing rate and time information. The key at the bottom of the **Chart** box defines the data points

mapped in the chart.

- To choose a different data point for analysis, click **Reset Data**.

5. When complete, close the Logfu display window.

Changing the Network Interface Address for Events

ArcMC has multiple network interfaces. By default, the connector determines which network interface address is used for events displayed in the ArcSight Console or Logger, but typically uses `eth0`.

To use a specific network interface address for events, add the parameter `connector.network.interface.name` to the Connector's `agent.properties` file. For example, to use the IP address for `eth1`, specify the following parameter:

```
connector.network.interface.name=eth1
```

Developing FlexConnectors

FlexConnectors are custom, user-designed *SmartConnector*s that can read and parse information from third-party devices and map that information to ArcSight's event schema.

ArcMC provides a FlexConnector Development wizard that enables you to quickly and easily develop a FlexConnector by creating a parser file, and enables you to test and package your new FlexConnector before deploying it. The wizard generates regular expressions and provides event field mapping suggestions automatically so you do not need to be an expert in regular expression authoring, parser syntax, or ArcSight event schema.

Use the FlexConnector Development wizard to develop FlexConnectors for simple log files. For complex log files, use the FlexConnector SDK (available from the ArcSight Customer Support site)

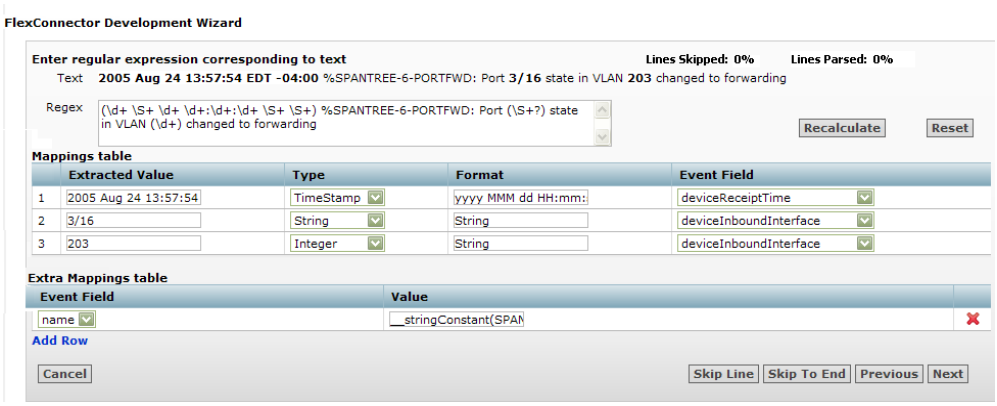
The FlexConnector Development wizard supports Regex Files, Folder Follower, and Syslog (Daemon, File, Pipe) FlexConnectors only.

The FlexConnector Development wizard does not support the extra processors property or multiple sub-messages. If you need these features, use the FlexConnector SDK to create your FlexConnector.

Caution: A FlexConnector that you develop with the FlexConnector Development wizard might perform more slowly than an ArcSight *SmartConnector*.

To develop a FlexConnector:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where you wish to develop the connector.
3. In the management panel, click the **Connectors** tab.
4. On the **Connectors** tab, in the Action drop-down, click **Edit FlexConnector**. The FlexConnector Development wizard is launched.
5. Provide the vendor and product name of the device for which you are creating a FlexConnector, and then click **Next**.
6. Select the data source type, and then click **Next**:
   - Select **Syslog** to create a Syslog FlexConnector to read events from Syslog messages.
   - Select **File** to create a FlexConnector to parse variable-format log files using regular expressions (ArcSight FlexConnector Regex File) or to parse variable-format log files in batch mode (ArcSight FlexConnector Folder Follower).
7. Upload a sample log file for the data source type you selected in the previous step, and then click **Next**.
8. The wizard finds the first unparsed line in the log file, generates a regular expression to match and extract tokens from that line, and displays the suggested field mappings for each extracted token in the Mappings table.



> **Note:** The mappings are displayed in descending order of probability (based on ArcSight training data). You can change the mappings by selecting from the list.
>
> The percentage of parsed lines in the file is shown in the top right of the panel. You can use this percentage to estimate where you are in the log file. The percentage of unparsed lines skipped in the file is also shown in the top right of the panel.

- To change the regular expression in the **Regex** box and recalculate the mappings, edit the expression and then click the **Recalculate** button.You can set the regular expression back to the suggested value by clicking the **Reset** button.

- Field mappings that do not correspond directly to the extracted tokens in the unparsed line of the log file are displayed in the Extra Mappings table. You can change the Event Field and provide a token operation. To add a new Event Field, click **Add Row**.

  You can use extra mappings to:

  - Remap an extracted token to a different Event Field in addition to the existing mapping. For example, you can add an Event Field with the value `$3` where `$3` is the third token in the list of suggested mappings.
  - Map a modified token or combination of tokens to an Event Field. For example, you can add an Event Field with the value `__operation($1,$3)`.
  - Map an Event Field to a constant string or integer. For example, you can add an Event Field with the value `__stringConstant(constant)`.

    For a list of the token operations used when tokens are mapped to ArcSight event fields, refer to the FlexConnector Developer's Guide (available from the ArcSight Customer Support site).

9. Click **Next** to save the mapping to the parser file and display the next unparsed line in the log file.

   After all unparsed lines in the log file have corresponding regular expressions and mappings, the wizard displays the parser file for review.
10. Review the parser file and make changes, if necessary, directly in the Review Parser File panel.
11. Click **Next** to save and package the parser file.
12. Choose how you want to deploy the FlexConnector:
    - Select **Deploy parser to existing connector in container**, and then click **Next** to use the parser file with an existing connector. Click **Done** to close the FlexConnector wizard and re-display the **Container** tab.

      > **Note:** The **Deploy parser to existing connector in container** option displays only if the container already contains a connector of the same type.

    - Select **Add new connector to container,** and then click **Next** to add the parser as a new connector. Follow the steps to add the connector to the container.

You can share FlexConnectors with other users. See "Sharing Connectors in ArcSight Marketplace" on the next page.

Editing FlexConnectors

After you have developed a FlexConnector with the FlexConnector wizard and have deployed it in a container, you can edit the FlexConnector to make changes to the parser file when needed.

The FlexConnector Edit wizard is available on the **Connectors** tab in the **Action** drop-down.

Click **Edit Connector** in the **Action** drop-down for the FlexConnector to open the wizard, then edit the parser file.

Caution: Only edit a FlexConnector that is created with the FlexConnector wizard. Editing manually-created FlexConnectors might produce unpredictable results.

Sharing Connectors in ArcSight Marketplace

You can share FlexConnectors and parser overrides with other users.

A FlexConnector is a custom connector that you define to gather security events from log files, databases, and other software and devices. You can share the following FlexConnector types:

- Syslog FlexConnectors (to read events from syslog messages)
- Log File FlexConnectors (to read fixed-format log files)
- Regular Expression Log File FlexConnectors (to read variable-format log files)
- Regular Expression Folder Follower FlexConnectors (to read variable-format log files recursively in a folder)
- Regular Expression Multiple Folder Follower FlexConnectors (to read events in real time or batch mode from multiple folders)
- XML FlexConnectors (to read events recursively from XML-based files in a folder)

A parser override is a file provided by ArcSight used to resolve an issue with the parser for a specific connector, or to support a newer version of a supported device where the log file format changed slightly or new event types were added. You can share parser overrides for all connector types that use a parser.

To share a FlexConnector or parser override, you need to package and upload it to ArcSight Marketplace on the ArcSight online community or to your local host. You can also download a FlexConnector or parser override that you need from ArcSight Marketplace or from your local host and add it to a container.

Note: ArcSight Marketplace will not be able to reach the ArcSight Community if access is attempted through a proxy server.

Packaging and Uploading Connectors

Before uploading your FlexConnector or parser override to ArcSight Community or to your local computer, you need to package it into a zip file (called an AUP package) using the upload wizard.

A FlexConnector AUP package contains the connector properties file, categorization file, connector parameters, and a manifest file with all the metadata on the package required for successful deployment. Metadata includes information about the AUP package, such as the package type, connector type, connector description, and so on. You can create only one AUP package per connector per device type. You can package a FlexConnector in Basic or Advanced mode. In **Basic** mode:

- The wizard packages the FlexConnector properties file automatically. If the wizard finds more than one properties file, you are prompted to select the file you want to package.
- The wizard packages the categorization file automatically *only* if it can be determined based on the device vendor and product information found in the properties file.
- The wizard does not package connector parameters. You are prompted to configure the connector when it is downloaded and deployed.

In **Advanced** mode:

- The wizard packages the FlexConnector properties file automatically. If the wizard finds more than one properties file, you are prompted to select the file you want to package. (Same as Basic mode.)
- The wizard packages the categorization file automatically if it can be determined based on the device vendor and product information found in the properties file. If the categorization file cannot be determined, you are prompted to select the categorization file you want to package from the list of files found in the container.
- The wizard displays connector parameters so you can configure the ones you want to display and set the default values you want to provide during connector deployment (download). The parameters you do not configure for display are pre-configured with the current values and will not be displayed during connector deployment.

A parser override package contains the parser override properties file and the manifest file only.

Follow the steps below to package and upload a FlexConnector or parser override.

- To upload to ArcSight Marketplace, you must have a valid username and password for ArcSight Community.
- Make sure that you have configured network settings under **Administration** > **System Admin** > **Network** and that ArcMC can communicate with the ArcSight Community server.

To package and upload a FlexConnector or parser override:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to upload a package. In the management panel, the **Connector** summary tab is displayed.

3. On the **Connector** details page, click .The upload wizard is launched.
4. Click **Next** and follow the steps in the wizard to:
   a. Select the type of AUP package you want to create for the selected connector. ArcMC scans the container and displays the relevant files that can be packaged.
   b. For a FlexConnector, select **Basic** to create a default package or select **Advanced** to customize the package to meet your needs.
   c. If the connector contains several properties files, you are prompted to select the properties file you want to package. Certain connectors, for example, syslog connectors, can have more than one parser override folder, in this case, you are prompted to select the folder you want to package.
   d. If you previously selected Advanced mode for a FlexConnector, and the categorization file cannot be determined, you are prompted to select the categorization file you want to package from a list of files found in the container.

      Note: Categorization files are not packaged for parser overrides.

   e. If you previously selected Advanced mode for a FlexConnector, select the configuration parameters you want to display when the connector is deployed and then provide default values for these parameters. Parameters you do not select are pre-configured with the current values.

      If any advanced connector parameters were previously modified from their defaults, the wizard displays these parameters so that you can select which ones you want to be configured automatically during deployment.

      Note: Configuration parameters are not displayed for parser overrides. If the connector has table parameters, they are not displayed during packaging. However, when the connector is downloaded to a container, you are prompted to provide values for all the table parameters.

   f. Provide a description of the AUP package and instructions on how to configure the device used by the connector.
   g. Provide the vendor, product, and version of the device used by the connector.

      If the wizard can determine the vendor, product, and version of the device, the information is displayed in the fields provided. You can change the information to meet your needs.
   h. Upload the created AUP package to ArcSight Marketplace or to your local host. You will require a username and password for the OpenText Community.

Downloading Connectors

You can download a FlexConnector or parser override that is available from ArcSight Marketplace on the OpenText Community or from your local computer. You download a FlexConnector or parser override directly to a container.

You can download only one FlexConnector per container using the download wizard. However, there is no limit to the number of parser overrides you can download to a container.

- When downloading a parser override to a container, the download wizard overwrites any existing parser override with the same name in the container without prompting for confirmation. To avoid overwriting an existing parser override, send a **Get Status** command to the existing parser override to check the parser information before you download a new one. For information on sending a Get Status command, refer to "Sending a Command to a Connector" on page 873.
- Always back up the container to the Backup Files repository before downloading a connector or parser override so you can revert to the previous configuration if the download produces unexpected results.

Follow the steps below to download a FlexConnector or parser override to a container.

To download to ArcSight Marketplace, you must have a valid username and password for ArcSight Community. Also, make sure that you have configured network settings under **Administration** > **System Admin** > **Network** and that the appliance can communicate with the ArcSight Community server.

To download a FlexConnector or parser override:

1. Click **Node Management**.
2. In the navigation tree, browse to the host on which the container resides.
3. In the management panel, click the **Containers** tab.
4. From the list of containers, locate the container into which you want to download the connector. In the **Action** drop-down, select **Run FlexConnector Wizard.**
5. Click **Next** and follow the steps in the wizard to:
   a. Select whether you want to download the connector from ArcSight Marketplace on ArcSight Community or from your local computer.
   b. Select the AUP package you want to download.

      On the OpenText Community, you can search for a parser override or FlexConnector AUP package using a keyword or a combination of keywords.

> **Note:** You can only download a parser override package to a container that has a connector of the same type as the package. You can download only one FlexConnector per container using the download wizard. If the container already contains a FlexConnector of the same type as the one you want to download, you can replace the existing FlexConnector with the one you are downloading, but you cannot create a new one.

c. For a FlexConnector, provide connector configuration parameters, if needed.

   Pre-configured and advanced parameters are deployed automatically with the values that were packaged; you are not prompted to configure these parameters. The configurable parameters are displayed with suggested defaults, which you can modify if necessary. The table parameters are displayed with no configured values, you have to provide the values manually, as needed.

d. Add or select a destination for the connector.

   If you are downloading the connector to a container that has an existing connector of the same type, you are *not* prompted for a destination.

The wizard copies the properties and categorization files to the appropriate locations and also installs the zip file for the AUP package in the `user/agent/deployedaups` folder on ArcMC to keep track of the deployment history.

After a successful download, the container is restarted automatically.

Configuration Suggestions for Connector Types

The following table provides configuration suggestions for different types of Connectors.

Connector Type	Effects of Limited Usage
Syslog	Due to the nature of UDP (the transport protocol typically used by Syslog), these Connectors can potentially lose events if the configurable event rate is exceeded. This is because the connector delays processing to match the event rate configured, and while in this state, the UDP cache might fill and the operating system drops UDP messages. **Note**: Do not use the **Limit CPU Usage** option with these connectors because of the possibility of event loss.
SNMP	Similar to Syslog connectors, when the event rate is limited on SNMP connectors, they can potentially lose events. SNMP is also typically UDP-based and has the same issues as Syslog.
Database	Because connectors follow the database tables, limiting the event rate for database connectors can slow the operation of other connectors. The result can be an event backlog sufficient to delay the reporting of alerts by as much as minutes or hours. However, no events will be lost, unless the database tables are truncated. After the event burst is over, the connector might eventually catch up with the database if the event rate does not exceed the configured limit.

Connector Type	Effects of Limited Usage
File	Similar to database connectors, file-based connectors *follow* files and limiting their event rates causes an event backlog. This can eventually force the connector to fall behind by as much as minutes or hours, depending on the actual event rate. The connectors might catch up if the event rate does not exceed the configured rate.
Asset Scanner	All connectors on run as a service (not as an application). Therefore, asset scanner connectors running onConnector Appliance are *not* supported in Interactive mode. To run the asset scanner connector in Interactive mode, install the connector on a standalone system and manage it as a software-based connector.
Proprietary API	The behavior of these connectors depends on the particular API, (for example, OPSEC behaves differently than PostOffice and RDEP). But in most cases, there will be no event loss unless the internal buffers and queues of the API implementation fill up. These connectors work much like database or file connectors.

Included FlexConnectors

ArcSight ArcMCConnector Applianceincludes these prototype FlexConnectors:

- ArcSight FlexConnector File
- ArcSight FlexConnector ID-based Database
- ArcSight FlexConnector Multiple Database
- ArcSight FlexConnector Regular Expression File
- ArcSight FlexConnector Regular Expression Folder File
- ArcSight FlexConnector Simple Network Management Protocol (SNMP)
- ArcSight FlexConnector Time-based Database
- ArcSight FlexConnector XML File

You can use these prototypes to develop your own FlexConnectors, and these can be shared with other users. Refer to "Sharing Connectors in ArcSight Marketplace" on page 877.

For more information, consult the FlexConnector Developer’s Guide, available from ArcSight Customer Support.

Managing Configurations

A *configuration* is a group of related appliance or software settings and their associated values, which applies to one or more node types. A configuration created for a node can be pushed to nodes of the same type managed by ArcMC, assuring uniformity across a group of nodes.

Configurations come in these kinds:

- A *subscriber* configuration is for the routine management of multiple managed ArcSight products. You can easily assign values to, propagate, and maintain the same settings across multiple nodes of the same type, including connectors, Connector Appliances, Loggers, or other ArcMCs.
- A *initial* configuration is for the rapid, uniform setup of multiple ArcSight Loggers (only). Use an initial configuration to expedite the initial deployment of ArcSight Loggers to a production environment.

Configuration management tasks include:

- *Configuration Creation:* A configuration for a node type can be created (as well as edited or deleted) in ArcMC.
- *Configuration Import:* A configuration can be created directly on a managed node, exported, then imported into ArcMC for sharing with nodes of the same type.
- *Configuration Push:* A configuration can be *pushed* from ArcMC to managed nodes. This copies the configuration from ArcMC and changes the settings on each destination node.
- *Subscriptions:* Managed nodes can be *subscribed* to a subscriber configuration, so they can receive a new or updated configuration pushed from ArcMC.
- *Compliance Checks:* Check whether the settings and their values on a managed node match the ones for a configuration type specified in ArcMC. If so, the node is said to be in *compliance* with the configuration.
- *Comparisons:* Compare two configurations of the same type quickly, with a field by field breakdown of each setting, its value, and any differences. You can compare the values of a configuration on a subscriber node to the values of the baseline or reference configuration on an ArcMC which manages it. You can also compare two configurations of the same type on a single ArcMC.

For example, a typical workflow for a subscriber configuration might work as follows: you can create a suitable DNS configuration for an appliance, specifying primary DNS server, secondary DNS server, and search domains for the appliance. (See "Destination Configuration Types" on page 903.) You can then push your DNS configuration to subscribing appliances, and so ensure that DNS settings for all subscribed nodes are configured identically with a single action.

If you later updated the configuration to use a new primary DNS server, you could push the new configuration to all subscribers, and all of them would be updated for the new DNS server with one action.

At any time, you could verify any managed node's compliance with the configuration to determine if its settings were assigned the desired values.

The following topics are discussed here.

Configuration Management

To create or manage configurations, on the menu bar, click **Configuration Management.** To manage a specific configuration type, select the configuration type from the sub-menu.

For example, to access subscriber configurations for Loggers, click **Configuration Management > Subscriber Configurations > Logger Configurations.**

The Configurations Table

The **Configurations** table lists all currently available subscriber configurations in ArcSight Management Center. Each listed configuration, whether it was created in ArcSight Management Center or imported from an existing node, is considered the baseline copy of that configuration, for pushing to managed nodes. The table includes the following columns.

- **Name:** The name of the configuration.
- **Type:** The type of configuration.
- **Last Edited By:** The most recent user to edit the configuration.
- **Compliance:** An aggregation of the status of the individual subscribers to that configuration.
  - *Compliant* indicates that all subscribers are in compliance.
  - *Non-Compliant* indicates that at least one subscriber is out of compliance.
  - *Unknown* indicates that the compliance status for one or more subscribers cannot be determined (for example, because connectivity to one or more subscribers is not available).

    > **Tip:** You can check the individual compliance of each subscriber on the **Subscribers** tab.

Click any column header to sort the **Configurations** table by that column.

To view the details of any configuration, click its name in the list. The **Details** and **Subscribers** tabs will display additional information.

> **Tip:** To select multiple items from any list, Shift+Click or Ctrl+Click while selecting.

The Details Tab

The **Details** tab shows the specifics of the configuration, including any configured attributes and their values.

Configuration Name

Each configuration has a unique name. A configuration may be up to 255 characters in length.

General

General details describe the basics of the configuration, as follows:

- **Configuration Type:** The type of the configuration. For details of configuration types, see "Subscriber Configuration Types" on page 896.
- **Last Edited By:** The most recent user to edit the configuration.

Properties

A *property* is a group of one or more settings for the configuration. For example, for the NTP Server configuration, the property includes two settings: Enable as NTP Server (a Boolean value indicating whether to enable the product as an NTP server), and NTP Servers (a list of NTP servers).

The specific parameters included in each property are pre-defined for each configuration type. ArcSight Management Center prompts for values of each setting when the property is selected. Each parameter must be assigned a valid value corresponding to its data type. For instance, if the data type is integer, you must specify an integer value. A red asterisk (*) indicates a required parameter.

List Configurations

A configuration type that can include more than one property is known as a *list configuration*. A list configuration represents a configuration with multiple instances of data values of the same kind. Each instance is known as a *property*.

For example, the Connector Map File configuration could include information on multiple map files. Each Property would represent a different map file (with different values for file path and content).

> **Note:** A pushed list configuration will override any existing configuration of the same type on the managed node. To *append* data to an existing configuration, use the bulk management tools (**Set Configuration**)

For a description of supported configuration types, the parameters associated with each type, and their data types, see "The Configurations Table" on the previous page.

The Subscribers Tab

The **Subscribers** list shows all managed nodes currently eligible to receive the configuration. (The list is empty if no hosts have been added yet.)

The tab includes these operations buttons:

Add Subscribers	Adds subscribers to the existing configuration.
Push	Pushes the configuration to one or more selected subscribers.
Check Compliance	Checks the compliance of all subscribers with the baseline configuration.
Unsubscribe	Removes one or more selected subscribers from the subscriber list.

The list includes the following columns:

- **Path:** The path of the subscribing node, consisting of location/hostname/node type.
- **Type:** The type of subscribing node.
- **Last Pushed At:** The time and date of the most recent push to the subscriber.
- **Last Push Status:** The status of the most recent push to the subscriber.
  - *Succeeded*: The configuration push was successful.
  - *Failed*: Hover over the link to determine the reason for the push failure. An error message is displayed to help in remediation of the issue. For more information, see "Push Remediation " on page 893.
  - *Unknown:* Initial status before the subscriber has received any pushes.
- **Last Compliance Check:** The date and time of the most recent compliance check.
- **Compliance:** Whether the node is in compliance with the configuration.
  - *Compliant* indicates the node is in compliance. The values for *all* settings associated with the configuration type match the values from the configuration.
  - *Non-Compliant* indicates the node is out of compliance. One or more values for the settings associated with the configuration type do not match the values from the configuration. Hover over *No* to show the cause of the node's non-compliance.
  - *Unknown* indicates either that the node's compliance could not be determined at the time of the most recent compliance check, or that the node has not yet undergone a compliance check.

Non-Compliance Reports

You can determine why a compliance status is Non-Compliant.

For a compliance status of *Non-Compliant,* click the status to display the **Configuration Comparison** dialog, which compares all setting values for the configuration on ArcMC and on the managed node.

Click **Push Configuration** to push the configuration to the managed node in order to make it Compliant.

Creating a Subscriber Configuration

You can create a subscriber configuration for pushing to any subscribed nodes.

Note: The following subscriber configuration types cannot be created in ArcMC, but can only be imported from managed nodes:

- Logger Storage Group
- Logger Filter
- Logger ESM Forwarder, Connector Forwarder, TCP Forwarder, UDP Forwarder
- Authentication External

For more information on importing a configuration from a managed node, see "Importing a Subscriber Configuration" on page 889.

To create a configuration:

1. Click **Configuration Management > Subscriber Configurations > All Configurations.**

   Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. Under **Configurations**, click **New**.
3. On the **Details** tab, select a configuration type from the **Configuration Type** drop-down list. (Only the appropriate configuration types are shown in the drop-down list.)
4. In **Configuration Name,** enter a name for the configuration. (Configuration names must be unique and may be up to 255 characters in length.)
5. Enter values for any required parameters, which are indicated with a red asterisk (*).

   Note: For a description of valid parameters for each configuration type, and the data type associated with each, see "Subscriber Configuration Types" on page 896.

6. Optionally, add values for any optional parameters.
7. Optionally, to add an additional property for a list configuration: click **Add Property**, and then enter values for the prompted parameters. Repeat adding properties as needed to completely define the configuration.
8. Click **Save**.

Editing a Subscriber Configuration

You can modify or delete values for a subscriber configuration. (You may not edit a configuration currently being pushed.)

To edit a configuration:

1. Click **Configuration Management > Subscriber Configurations > All Configurations.**

   > **Tip:** To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, click the name of the configuration to be edited.
3. On the **Details** tab, click **Edit**.
   - Edit the general settings as needed.
   - Optionally, to add an additional property for a list property, click **Add Property**, then specify values for the prompted parameters. Repeat adding properties as needed to completely define the configuration.
   - Optionally, to delete a property from the configuration, click **Delete Property.**
4. When complete, click **Save**. After saving, if the configuration has any subscribers, you are prompted to push the updated configuration to the subscribers.

Deleting a Subscriber Configuration

A deleted subscriber configuration is no longer available for pushes to subscribers. You may not delete a configuration currently being pushed.

To delete a subscriber configuration:

1. Click **Configuration Management > Subscriber Configurations > All Configurations.**

   > **Tip:** To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, select one or more configurations to be deleted.
3. Click **Delete.**
4. Click **Yes** to confirm deletion.

Importing a Subscriber Configuration

A subscriber configuration created on a managed node may be imported into ArcMC, for editing and pushing to other nodes of the same type.

For example, you can define a configuration on a managed Connector Appliance, then import the configuration into ArcMC. The imported configuration may then be edited and pushed to other managed Connector Appliances, just the same as you would with a configuration you originally created in ArcMC.

Note: If configuration import to the localhost fails, restart the web service on the localhost.

To import a subscriber configuration from a managed node:

1. Click **Configuration Management > Subscriber Configurations > All Configurations.**

   Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. Under **Configurations**, click **Import**.
3. On the **Choose a Node** dialog, select the node from which you wish to import the configuration.
4. Click **Continue**.
5. On the **Import Configuration** dialog:
   a. Select a configuration type for the imported configuration from the **Type** drop-down list. (The entries in the list depend on the configuration types which apply to the node chosen in Step 3.)
   b. In **Name**, specify a name for the imported configuration.
6. Click **Import**. The configuration is imported into ArcMC and is shown in the **Configurations** table.

   Note: In order to import a backup configuration from a Connector Appliance, Logger, or ArcMC node, the node must have a scheduled backup to begin with.

Managing Subscribers

A *subscriber* is a managed node to which a configuration may be pushed. A subscriber to which a configuration is pushed will receive and process the pushed configuration and apply it to the managed node, so that the managed node's settings are the same as the settings specified in the configuration.

Each node can subscribe to *only one* configuration of each configuration type.

For example, a Logger appliance could subscribe to one Logger Storage Group configuration, but the same appliance could also subscribe to a Logger Filter configuration as well as a Logger Transport Receiver configuration.

Viewing Subscribers

To view subscribers for a configuration:

1. Click **Configuration Management > All Configurations.**
2. From the list of configurations, locate the configuration for which you wish to view subscribers.
3. Click the name of the configuration.
4. Click the **Subscribers** tab. The current subscribers are displayed.

Adding a Subscriber

A subscriber (that is, a subscribed node) can receive a pushed configuration.

To subscribe a node to a configuration:

1. Click **Configuration Management > All Subscriber Configurations.**

   Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, click the name of the configuration to which you wish to add subscribers.
3. Click the **Subscribers** tab.
4. Click **Add Subscribers.**
5. On the **Add Subscribers** dialog, select a node to add as a subscriber. The list of potential subscribers is determined by the selected configuration type. To select multiple nodes for subscription, Ctrl+Click each node.

   Note: A node may only subscribe to one configuration of each type; for example, one DNS configuration.

   If you attempt to add a subscriber which is already subscribed to a configuration of the same type, the following message is displayed: *No available subscribers have been found for the selected configuration.*

6. Click **Add Subscribers.**
7. Click **OK** to confirm completion. The subscriber is added to the recipients for the configuration.

Unsubscribing a Subscriber

After being unsubscribed, a node can no longer receive a pushed configuration.

To remove a subscriber from a configuration:

1. Click **Configuration Management > All Subscriber Configurations.**

   Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, click the name of the configuration from which you wish to remove subscribers.
3. Click the **Subscribers** tab.
4. Select one or more subscriber from the list of subscribers.
5. Click **Unsubscribe**.
6. Click **OK** to confirm. The selected subscribers are unsubscribed.

Pushing a Subscriber Configuration

A pushed subscriber configuration synchronizes the configuration from ArcMC to all or a selection of the configuration's subscribers. Pushing must be performed manually.

When selecting subscribers, only valid potential subscribers for the configuration are shown. For example, if pushing a Logger configuration, which only applies to Loggers, only managed Loggers would be shown as potential subscribers, not Connector Appliances or ArcMCs.

Note: If a configuration push to the localhost fails, restart the web service on the localhost.

To push a subscriber configuration to all subscribers:

1. Select **Configuration Management > All Subscriber Configurations.**

   Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, select a configuration to be pushed.
3. Click **Push**.
4. Click **Yes** to confirm the push. The configuration is pushed to all subscribers of the selected configuration. A compliance check is automatically performed on each subscriber.

To push a subscriber configuration to selected subscribers:

1. Select **Configuration Management > Subscriber Configurations > All Configurations.**

   > **Tip:** To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, select a configuration to be pushed, and click the name of the configuration.
3. On the **Configuration Details and Subscribers** page, click the **Subscribers** tab.
4. On the **Subscribers** tab, select one or more subscribers to which to push the configuration.
5. Click **Push**.
6. Click **Yes** to confirm the push. The configuration is pushed to the selected subscribers. A compliance check is automatically performed on each recipient.

Push Validation

During a push to subscribers, the configuration is automatically validated by ArcSight Management Center. Validation ensures that a pushed configuration contains appropriate, meaningful values for all settings. If any configuration values are found to be invalid, the push will fail, and an error message will be returned. Hover over the subscriber's entry on the **Subscribers** tab, in the **Push Status** column, to show the cause of the failed push. In addition, a compliance check is automatically performed after the push.

Common Causes for Push Failure

A push to a subscriber may fail for any number of reasons. These may include:

- **Validation Failure:** A push with invalid content will fail. Verify that your configuration includes valid setting values for the configuration type.
- **Lack of Connectivity:** Network or system issues can cause disrupt connectivity to a subscriber. Verify connectivity with the subscriber.
- **Agent Not Running on Host :** Verify that the ArcMC Agent process is active on the subscribing node. (This does not apply to Connectors, which do not require the Agent.)
- **Privileges on Subscribing Host**: In order to push a subscription, the user (specified by the user credentials) must have privileges to view, edit, or delete configuration settings on the

subscriber nodes.

- **Expired License:** An expired host license will cause a push to the host to fail.

Push Remediation

If a push to a subscriber fails, you may be able to remedy the failure by following these steps:

1. Select the configuration from the **Configurations** table.
2. Click the **Subscribers** tab and choose the subscriber to which the push failed.
3. The **Last Push Status** will show *Failed*. Hover over this link to view the error message associated with the push failure.

After viewing the error message, you can take the appropriate steps on the managed node to address the issue. Resolution may require direct or remote access to the node outside of ArcSight Management Center.

After the issue is resolved, you can retry the failed configuration push.

Checking Subscriber Compliance

A subscribed node is in *compliance* with a configuration if the settings for the node match those assigned to the configuration in ArcSight Management Center.

The configuration listed in the managing ArcSight Management Center is considered the baseline copy of the configuration.

For example, you create an SMTP configuration in ArcSight Management Center named *Sample SMTP Configuration,* with these values assigned:

- Primary SMTP Server: *Mailserver1*
- Secondary SMTP Server: *Mailserver2*
- Outgoing Email Address: *admin@example.com*

A node would be in compliance with this configuration if the values for its primary and secondary SMTP servers, and outgoing email address, matched the values in *Sample SMTP Configuration*.

If any one of these values were different (for example, if a node had a primary SMTP Server of *CorporateMail1*) the node would be out of compliance.

You can manually check the compliance of all subscribers to a configuration.

To manually check subscriber compliance for a configuration:

1. Click **Configuration Management > Subscriber Configurations > All Configurations.**

   > **Tip:** To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. In the **Configurations** table, select the configuration to be checked for compliance.
3. Click **Check Compliance**. All subscribers to the selected configuration are checked for compliance.
   - On the **Configurations** table, the **Compliance** column shows the aggregated compliance of all subscribers.
   - On the **Subscribers** tab for the configuration:
     - The **Last Compliance Check** column is updated to show the most recent check.

       > Automatic compliance checks will run every 12 hours. So this will be the date and time of the latest automatic check.

     - The **Compliance** column indicates the individual compliance of each node.

Comparing Configurations

You can compare two configurations of the same type to verify whether they contain the same settings. The following two comparisons are possible:

- **Comparing two configurations on a single ArcMC.** You can compare two configurations of the same type on a single ArcMC. For example, you could compare the settings for two different SMTP configurations.
- **Comparing the configuration on a subscriber to the same configuration on its managing ArcMC.** You can quickly check to see how the settings for a configuration on a subscribing node differs from the same configuration on its managing ArcMC.

To compare two configurations of the same type on one ArcMC:

1. Click **Configuration Management.**
2. Select **All Configurations.**
3. In the list of configurations, select two configurations.
4. Click **Compare**.

The **Configuration Comparison** dialog shows each setting for the configuration and the current value for each compared item in the **Status** column.

To print the comparison as a PDF report, click **Export to PDF.**

To compare the configuration on a subscriber to the same configuration on its managing ArcMC:

1. Click **Configuration Management.**
2. Select **All Configurations.**
3. In the configurations list, select the configuration you wish to compare between ArcMC and the subscriber.
4. Under **Configuration Details & Subscribers**, click the **Subscribers** tab.
5. In the **Compliance** column, click the status link.

The **Configuration Comparison** dialog shows each setting for the configuration and the current value for each compared item.

Optionally, if the subscriber is Non-compliant with the configuration on its managing ArcMC, click **Push Configuration** to push the configuration to the subscriber (which will make it compliant).

To export the comparison as a PDF report, click **Export to PDF.**

Configuration Management Best Practices

Configuration management is a powerful tool for managing multiple ArcSight products. You can easily implement configurations across managed products with just a few actions.

- **Node management versus Configuration Management:** Use ArcSight Management Center's node management tools for the administration of individual nodes and their day-to-day operations. However, for consistent and wide-ranging changes to the data or settings of managed nodes, use configuration management if the appropriate configuration exists. For example, to change DNS settings across multiple managed nodes, it would be faster and easier to create the configuration in ArcMC and push it out to managed nodes, than to individually change the settings across multiple devices.
- **Implementing data settings across multiple appliances or products in bulk:** Use the Bulk Management (**Set Configuration**) tools to implement data settings across multiple appliances or products. For example, you can quickly configure all of your appliances to use the same hardware settings (such as SMTP server) with a single platform (in this case, SMTP) configuration applied to managed nodes. (Pushing will overwrite any existing data.)
- **Compliance versus Non-Compliance:** If configuration compliance is not relevant to your configuration management, use the bulk management tools under Node Management to manage your node settings. A bulk push can also be performed under Configuration Management.

Subscriber Configuration Types

The following section lists the available subscriber configuration types, the parameters associated with each, their data types, and a brief description of what the parameter represents. When assigning values to parameters:

- Each parameter's value must be of the data type indicated (for example, the String data type indicates that you must enter a string for the value).
- *Required* parameters are marked with an asterisk (*) and must be assigned a value. A configuration missing a value for a required parameter cannot be saved or pushed.
- *Read-only* parameters cannot be edited in .
- For security reasons, all password parameters are displayed with obfuscation.

> **Tip:** For details of each entry field, in edit mode, hover over the field label and view its descriptive tooltip.

Connector Configuration Types

Connector configurations set values for settings on containers, or connectorss. The available connector configuration types are listed here.

BlueCoat Connector Configuration

A BlueCoat Connector configuration defines settings for one or more BlueCoat connectors. The configuration is only pushed to a target if a BlueCoat connector exists.

To push a BlueCoat Connector configuration from to a managed node that already has values defined for all fields listed here, then specify values for all fields in the pushed configuration. Default values may be used if necessary.

BlueCoat Connector Configuration Parameters

Parameter	Data Type	Description
Row Number*	Integer	Row number of the table parameter to which the configuration is pushed.
Log File Wildcard*	String	Log file wildcard.
Log File Type*	String	Log file type. Valid values are: • `main` • `im` • `ssl` • `streaming`

BlueCoat Connector Configuration Parameters, continued

Parameter	Data Type	Description
Processing Mode	String	Processing mode. Valid values are Batch and Real time.
Post-Processing Mode	String	Post-processing mode. Valid values are: • `RenameFileInTheSame Directory` • `PersistFile` • `DeleteFile`
Mode Options	String	Mode options. Required if Post-Processing Mode is chosen as `RenameFileInTheSame Directory`
Processing Threshold	Integer	Interval, in hours, after which the log file will be marked as processed.
Processing Limit	Integer	Number of files that can be read in the directory at the same time.

FIPS Configuration

A FIPS configuration enables or disables FIPS mode on a container.

Note: After pushing a FIPS configuration, the destination container will be restarted.

FIPS Configuration Parameters

Parameter	Data Type	Description
Enabled*	Boolean	If **Yes**, FIPS is enabled on the container.

Map File Configuration

A map file configuration defines the path and content of one or more container map files. Each Path/Content pair represents a single map file. To include multiple files, add multiple Properties to the configuration.

- When pushed, the configuration deletes all `*.properties` files in the `\map` directory on the target, then adds the list of map files to the target, replacing any existing map files.
- If the configuration contains an empty list, all `*.properties` files are deleted.

Note: If importing and uploading a map configuration file, convert the downloaded CSV file into a .properties file before uploading.

Uploading Map Files Larger Than 1 MB

a. Log in to the OMT Management Portal. See "Accessing the OMT Management Portal" on page 507 for more information.
b. From the left menu select **Deployment > Deployments.**
c. Click **... (Browse)** on the far right and choose **Reconfigure**. A new screen will open in a separate tab.
d. Select the **Fusion** tab
e. Scroll down to the **ArcMC Configuration** section, and enter the desired value for the **Maximum In-memory Buffer Size** parameter.
f. Click **Save**. The ArcMC pod will be restarted.

If `<install_dir>/userdata/arcmc/logger.properties` does not exist, then create one in a text editor. This file must be owned by a non-root user. For an ArcMC appliance, use the 'arcsight' user, and for software ArcMC, use the non-root account used to install the ArcMC.

Modify the `<install_dir>/userdata/arcmc/logger.properties` by adding:

```
configuration.max.inmemory.mb=2
```

> **Note:** 2097152 = 2 * 1024 * 1024

After adding the previous line, owner and permissions need to be changed:

```
chown <non-root user>:<non-root user> logger.properties
chmod 660 logger.properties
```

Finally, restart the web process after making any edits to `logger.properties.`

Map File Configuration Parameters

Parameter	Data Type	Description
Path*	String	Path to the map file.
Content*	String	Content of the map file.

Parser Override Configuration

A parser override configuration defines the path and content of one or more container parser override files.

Each Path/Content pair represents a single parser override file. To include multiple files, add multiple Properties to the configuration.

- When pushed, the configuration deletes all `*.properties` files in the `\fcp` directory on the target, then adds the list of parser override files to the target, replacing any existing

parser override files.

- If the configuration contains an empty list, all `*.properties` files are deleted.

Parser Override Configuration Parameters

Parameter	Data Type	Description
Path*	String	Path to the parser override file.
Content*	String	Content of the parser file.

Syslog Connector Configuration

A Syslog connector configuration defines values for one or more Syslog connectors. The configuration is only pushed to the target node if a Syslog connector exists.

Syslog Connector Configuration Parameters

Parameter	Data Type	Description
Port*	Integer	Syslog connector port.
Protocol*	Enum	Protocol of the syslog connector (either UDP or Raw TCP).

Windows Unified Connector (WUC) External Parameters Configuration

A WUC External Parameters connector configuration defines the external parameters for one or more WUC connectors. The configuration is only pushed to the target node if a WUC connector exists.

Limitations to WUC External Parameters Configurations

A WUC external parameters configuration has the following limitations:

- Domain user password is not supported as a WUC configuration parameter. Instead, domain user password must be managed individually for each WUC host.
- WUC connectors are not FIPS-compliant.
- If you wish to push a WUC configuration from ArcMC to a managed node that already has values defined for all fields listed here, then you must specify values for all fields in the pushed configuration. Default values may be used if necessary.

WUC External Parameters Configuration Parameters

Parameter	Data Type	Description
Domain Name*	String	Windows domain name.
Domain User*	String	Windows domain user name.

WUC External Parameters Configuration Parameters, continued

Parameter	Data Type	Description
Active Directory Host	String	Hostname for the Active Directory server, if one is used. ◦ If specified, values for User, User Password, Base DN, Protocol, and Port must be specified in subsequent entries.
Active Directory Use	String	Username for the AD server. ◦ Required if a value is provided for Active Directory Host.
Active Directory User Password	String	Password for AD server. ◦ Required if a value is provided for Active Directory Host.
Active Directory Base DN	String	Base DN of the Active Directory. ◦ Required if a value is provided for Active Directory Host.
Active Directory Protocol	String	Protocol for Active Directory. ◦ Required if a value is provided for Active Directory Host.
Active Directory Port	String	Port for Active Directory. ◦ Required if a value is provided for Active Directory Host.
Global Catalog Server	String	Hostname for the Global Catalog server, if one is used. ◦ If specified, values for User Name, User Password, and Base DN must be specified in subsequent entries.
Global Catalog User Name	String	Username for the GC server. ◦ Required if a value is provided for Global Catalog server.
Global Catalog User Password	String	Password for the GC server. ◦ Required if a value is provided for Global Catalog server.
Global Catalog Base DN	String	Base DN of the GC server. ◦ Required if a value is provided for Global Catalog server.
WEF Collection*	String	Indicates if Windows Event Format collection is enabled. Valid values are: ◦ Disabled ◦ Enabled (use Active Directory for sources) ◦ Enabled (do not use Active Directory for sources) **Note:** WEF collection is only supported for Connector versions 6.0.6 or later. Otherwise, compliance checks for checks for WUC External Parameters configurations will always fail.

Windows Unified Connector (WUC) Internal Parameters Configuration

A WUC Internal Parameters connector configuration defines the internal parameters for one or more WUC connectors. The configuration is only pushed to the target if a WUC connector exists.

Limitations to WUC Internal Parameters Configurations

A WUC internal parameters configuration has the following limitations:

- Domain user password is not supported as a WUC configuration parameter. Instead, domain user password must be managed individually for each WUC host.
- WUC connectors are not FIPS-compliant.
- If you wish to push a WUC configuration from ArcMC to a managed node that already has values defined for all fields listed here, then you must specify values for all fields in the pushed configuration. Default values may be used if necessary

WUC Internal Parameters Configuration Parameters

Parameter	Data Type	Description
Enable GUID Translation*	Boolean	If true, Globally Unique Identifier translation is enabled.
Enable SID Translation*	Boolean	If true, Security Identifier translation is enabled.
Enable SID Translation Always*	Boolean	If true, SID translation is used even for events Windows does not translate.
FCP Version	Integer	File Control Protocol version number.
Global Catalog Port	Integer	Port used by Global Catalog server.
Global Catalog Security Protocol	Enum	Security protocol used by Global Catalog server.
Host Browsing Threads Sleep Time	Integer	Time in milliseconds between host browsing queries.
Inactivity Sleep Time	Integer	Time in milliseconds to sleep if no events are retrieved from the configured hosts
Log Rotation Check Interval	Integer	Time in milliseconds to wait before checking for log rotation.
Reconnect Interval	Integer	Time in milliseconds after which the connection to a previously down host is to be retried.
Rotation Retry Count	Integer	Number of times to check that log has been rotated.

WUC Internal Parameters Configuration Parameters, continued

Parameter	Data Type	Description
Rotation Retry Interval	Integer	Interval in milliseconds for rotation retry.
Sleep Time	Integer	Time, in milliseconds, to sleep before collecting more events from hosts (-1 means disable sleep time).
Thread Count	Integer	Number of threads to use for the connector.

ArcMC/Connector Appliance Configuration Types

ArcMC/Connector Appliance configurations set values for settings on Software ArcSight Management Centers, ArcSight Management Center Appliances, and hardware or software Connector Appliances. The currently available ArcMC/Connector Appliance configuration type is listed here.

ArcMC/Connector Appliance Configuration Backup Configuration

An ArcMC/Connector Appliance Configuration Backup configuration sets values for scheduled configuration backups of ArcSight Management Center or Connector Appliance. Backup content includes all backup data.

After a push, the web process is automatically restarted on the subscriber.

For this configuration type, no automatic compliance checks will be performed. You must check compliance manually. The following limitation applies:

- This Configuration is not supported if the Backup Server platform is CentOS 7.4.

Note: You can neither create nor import settings related to a one-time configuration backup.

ArcMC/Connector Appliance Configuration Backup Parameters

Parameters	Data Type	Description
Backup Server IP Address*	String	IP address of the remote system where the backup will be saved.
Port*	Integer	Port of the remote system. Default value is 22.
Base Remote Directory*	String	Destination directory on the remote system. Must be manually created on remote system prior to push. After a push, the destination host name is appended to this, to give it a unique value across all nodes.
User*	String	User name on destination.

ArcMC/Connector Appliance Configuration Backup Parameters, continued

Parameters	Data Type	Description
Password*	String	Password on the destination. (Obfuscated.)
Days of the Week*	List of comma-separated strings	Comma-delimited list of days of the week on which the backup will be performed. Valid values are *Su, M, T, W, Th, F, Sa*.
Hours of Day*	List of comma-separated integers	Comma-delimited list of hours of the day at which the backup will be performed. Valid values are integers from 0 to 23, where 0 is 12:00 midnight. For example, a value of 14 would correspond to 2 PM.

Destination Configuration Types

A destination configuration sets values for ESM destination settings. The available destination configuration types are listed here.

Destination Configuration Parameters

A Destination Configuration Parameters configuration defines values and behavior for destination configuration parameters.

> **Note:** Destination Configuration Parameters configurations can only be imported from managed Connectors, not created in ArcMC. See "Importing a Subscriber Configuration" on page 889 for more information.

For a description of the parameters for this configuration type, see "Destination Runtime Parameters " on page 945.

Networks and Zones

A Networks and Zones configuration defines values and behavior for ArcSight ESM networks and zones. For more information on ESM networks and zones, consult the ArcSight Console documentation. For Connector Network and Zone Configuration information see the Smart Connector's User Guide at ArcSight SmartConnectors 24.2 documentation.

> **Note:** So as not to interfere with ESM connector management, ArcMC will not push Network and Zones AUPs to a connector's ESM destination folder.

Networks and Zones Configuration Parameters

Parameter	Data Type	Description
Configuration Name*	String	Name of the configuration.

Networks CSV Content*	CSV	Comma-separated Value (CSV) file. Click **Upload** to upload a valid CSV file, or click **Download** to download an existing file.
		Creating a CSV File
		The CSV must include the literal header line:
		`#Type,Name,Parent Group URI,Customer URI`
		Then, each line describes a Network. Each line must comprise values for the following fields, and end with a hard return (no white spaces). Begin the first of these network lines with the # character before Type.
		`<Type>,<Name>,<Parent Group URI>,<Customer URI>`
		For a complete detailed description of the requirements of this file, see ArcMC Network Models.

Zones CSV Content*	CSV	Comma-separated Value (CSV) file. Click **Upload** to upload a valid CSV file, or click **Download** to download an existing file.
		Creating a CSV File
		The CSV must include the literal header line:
		`#Name,Start Address,End Address,Parent Group URI,Network URI`
		Then, each line describes a Zone. Each line must comprise values for the following fields, and end with a hard return (no white spaces). Begin the first of these zone lines with the # character before Name.
		`<Name>,<Start Address>,<End Address>,<Parent Group URI>,<Network URI>`
		For a complete detailed description of the requirements of this file, see ArcMC Network Models.

Logger Configuration Types

Logger configurations set values for settings on hardware and software Loggers. The available Logger configuration types are listed here.

Logger Configuration Backup Configuration

A Logger configuration backup configuration sets values for scheduled configuration backups of hardware and software Logger to a remote system. The following limitation applies:

- This Configuration is not supported if the Backup Server platform is CentOS 7.4.

Note: You can neither create nor import settings related to a one-time configuration backup.

Logger Configuration Backup Configuration Parameters

Parameter	Data Type	Description
SCP Port*	String	Port of the remote system. Default value is 22.
Backup Server IP Address*	String	IP address of the remote system where the backup will be saved.
Username*	String	User name on destination.
Password*	String	Password on destination. (Obfuscated.)
Base Remote Directory*	String	Destination directory on the remote system. After a push, the destination host name is appended to this, to give it a unique value across all nodes. When using a Logger appliance, some settings need to be configured in the `/etc/hosts` file. For more information, please refer to the *Configuring Hosts for the Appliance* chapter in the Logger Installation Guide.
Days of the Week*	List of comma-separated strings	Comma-delimited list of days of the week on which the backup will be performed. Valid values are *Su, M, T, W, Th, F, Sa*.
Hours of Day*	List of comma-separated integers	Comma-delimited list of hours of the day at which the backup will be performed. Valid values are integers from 0 to 23, where 0 is 12:00. For example, a value of 14 would correspond to 2 PM.
Backup Content*	String	Type of content to be included in the backup. Valid values are: • *All:* includes all backup data. • *Report_Content_Only*: includes only report data.

Logger Connector Forwarder Configuration

A Logger Connector Forwarder configuration sets values for one or more connector forwarders on a Logger (version 6.1 or later). Each forwarder in the configuration is represented by a different Property.

Note: Logger Connector Forwarder configurations can only be imported from managed Loggers, not created in ArcMC. See "Importing a Subscriber Configuration" on page 889 for more information.

Logger Connector Forwarder Configuration Parameters

Parameter	Data Type	Description
Forwarder Name*	String	Display name of the forwarder
Filter Type*	Enum	Filter type that was selected while creating a forwarder on logger. Valid types are *Unified* or *Regex*.
Query	String	Used to filter events that the forwarder will forward.
Unified Query Filters	String	Select from the default and user-defined Unified filters on the source Logger. Only visible if Filter Type is Unified.
Regular Expression Filters	String	Select from the default and user-defined Regex filters on the source Logger. Only visible if Filter Type is Regex.
Start Time	DateTime	Optional start of time range for selection.
End Time	DateTime	Optional end of time range for selection.
IP/Host*	String	IP address or host name of the destination that will receive forwarded events.
Port*	Integer	Port number on the destination that will receive forwarded events. Ensure this port is open on the destination.
Enable*	Boolean	If **Yes**, the forwarder is enabled.
Connection Retry Timeout*	Integer	Time, in seconds, to wait before retrying a connection.
Source Type*	Integer	Source Type. Valid values: • Apache HTTP Server Access • Apache HTTP Server Error • IBM DB2 Audit • Juniper Steel-Belted Radius • Microsoft DHCP Log • Other

Logger ESM Forwarder Configuration

A Logger ESM Forwarder configuration sets values for one or more ESM destinations on a Logger (version 6.1 or later). Each destination in the configuration is represented by a different Property.

Note: Logger ESM Forwarder configurations can only be imported from managed Loggers, not created in ArcMC. See "Importing a Subscriber Configuration" on page 889 for more information.

Logger ESM Forwarder Parameters

Parameter	Data Type	Description
Parameter	Data Type	Description
Forwarder Name*	String	Display name of the forwarder
Filter Type*	Enum	Filter type that was selected while creating a forwarder on logger. Valid types are *Unified* or *Regex*.
Query	String	Used to filter events that the forwarder will forward.
Unified Query Filters	String	Select from the default and user-defined Unified filters on the source Logger. Only visible if Filter Type is Unified.
Regular Expression Filters	String	Select from the default and user-defined Regex filters on the source Logger. Only visible if Filter Type is Regex.
Start Time	DateTime	Start of time range for selection.
End Time	DateTime	End of time range for selection.
IP/Host*	String	IP address or host name of the destination that will receiveforwarded events.
Port*	Integer	Port number on the destination that will receive forwarded events. Ensure this port is open on the destination.
Enable	Boolean	If **Yes**, the forwarder is enabled.

Logger Filter Configuration

A Logger Filter configuration sets values for one or more saved searches on a Logger.

Each filter in the configuration is represented by a different Property.

Note: Logger Filter configurations can only be imported from managed Loggers, not created in ArcMC. See "Importing a Subscriber Configuration" on page 889 for more information.

Logger Filter Configuration Parameters

Parameter	Data Type	Description
Filter Name*	String (Read-only)	Name of the filter.
Filter Category	String	Category of filter. Valid values are **Shared**, **System** and **SearchGroup**.

Logger Filter Configuration Parameters, continued

Parameter	Data Type	Description
Filter Type*	String	Type of filter. Valid values are **RegexQuery** or **UnifiedQuery**.
Query*	String	Query string.
Permission Group	String	Permission group which with the Logger filter is associated. When the configuration is pushed: • If the permission group is not present on the target Logger, the permission group will be created during the push. • If the permission group of the same name is already present on the target, but has different rights, the rights of the permission group on the target Logger will not be overwritten, and the association between the filter and the permission group will be removed.

Logger SmartMessage Receiver Configuration

A Logger SmartMessage Receiver sets values for one or more for SmartMessage Receivers.

A SmartMessage Receiver configuration pushed to a target overwrites any existing SmartMessage receivers on the target; other types of receivers such as UDP and TCP are not affected.

Logger SmartMessage Receiver Configuration Parameters

Parameter	Data Type	Description
Receiver Name*	String	Name of the receiver.
Enabled*	Boolean	If **Yes**, SmartMessage reception is enabled.
Encoding*	String	Encoding type. Valid values are: • `UTF-8` • `US-ASCII`

Logger Storage Group Configuration

A Logger Storage Group configuration sets values for one or more Logger storage groups.

Note: Logger Storage Group configurations can only be imported from managed Loggers, not created in ArcMC. See "Importing a Subscriber Configuration" on page 889 for more information.

Logger Storage Group Configuration Parameters

Parameter	Data Type	Description
Storage Group Name*	String (Read-only)	Name of the storage group. • The pushed configuration must contain the same number of storage groups as configured on the Logger. • The names of the storage groups in the pushed configuration must match the names of storage groups on the Logger.
Maximum Age (Days)*	Integer	Maximum age of events in storage, in days.
Maximum Size (GB)*	Integer	Maximum size of the storage group, in gigabytes. • The cumulative size of all storage groups must not be greater than the storage volume size on the Logger.

Logger TCP Forwarder Configuration

A Logger Connector Forwarder configuration sets values for one or more TCP forwarders on a Logger (version 6.1 or later). Each forwarder in the configuration is represented by a different Property.

Note: Logger TCP Forwarder configurations can only be imported from managed Loggers, not created in ArcMC. See "Importing a Subscriber Configuration" on page 889 for more information.

Logger TCP Forwarder Configuration Parameters

Parameter	Data Type	Description
Forwarder Name*	String	Display name of the forwarder
Filter Type*	Enum	Filter type that was selected while creating a forwarder on logger. Valid types are *Unified* or *Regex*.
Query	String	Used to filter events that the forwarder will forward.
Unified Query Filters	String	Select from the default and user-defined Unified filters on the source Logger. Only visible if Filter Type is Unified.
Regular Expression Filters	String	Select from the default and user-defined Regex filters on the source Logger. Only visible if Filter Type is Regex.
Start Time	DateTime	Optional start of time range for selection.
End Time	DateTime	Optional end of time range for selection.
IP/Host*	String	IP address or host name of the destination that will receive forwarded events.
Port*	Integer	Port number on the destination that will receive forwarded events. Ensure this port is open on the destination.
Enable*	Boolean	If **Yes**, the forwarder is enabled.

Logger TCP Forwarder Configuration Parameters, continued

Parameter	Data Type	Description
Preserve System Timestamp*	Boolean	If **Yes**, the timestamp showing original event receipt time is preserved.
Preserve Original Syslog Sender*	Boolean	If **Yes**, event is sent as is, without inserting Logger's IP address in the hostname (or equivalent) field of the syslog event.
Connection Retry Timeout*	Integer	The time, in seconds, to wait before retrying a connection.

Logger Transport Receiver Configuration

A Logger Transport Receiver configuration sets values for one or more UDP, TCP, CEF UDP, or CEF TCP receivers.

Note: In Logger documentation, a *Transport Receiver* is referred to as simply a *Receiver*.

A pushed Transport Receiver type configuration will overwrite any existing UDP, TCP, CEF UDP, or CEF TCP receiver. Any other type of receivers, such as SmartMessage receivers, are not affected.

Logger Transport Receiver Configuration Parameters

Parameter	Data Type	Description
Receiver Name*	String	Name of the receiver.
Receiver Type*	String	Receiver type. Valid values are: • UDP • TCP • CEF UDP • CEF TCP
Receiver Name*	String	Name of the receiver.

Logger Transport Receiver Configuration Parameters, continued

Parameter	Data Type	Description
Port*	Integer	Port number. Must be a non-zero positive number. Ensure this port is open on the destination.
Enabled*	Boolean	If **Yes**, transport reception is enabled.
Encoding*	String	Encoding type. Valid values are: • `UTF-8` • `Shift_JIS` • `EUC-JP` • `EUC-KR` • `US-ASCII` • `GB2312` • `UTF-16BE` • `Big5` • `GB18030` • `ISO-8859-1` • `Windows-1252` For CEF UDP and CEF TCP receivers, only UTF-8 and US-ASCII apply. **Caution:** Selection of the wrong encoding for a CEF receiver will cause a push failure.

Logger UDP Forwarder Configuration

A Logger Connector Forwarder configuration sets values for one or UDP forwarders on a Logger. Each forwarder in the configuration is represented by a different Property.

Note: Logger UDP Forwarder configurations can only be imported from managed Loggers, not created in ArcMC. See "Importing a Subscriber Configuration" on page 889 for more information.

Logger UDP Forwarder Configuration Parameters

Parameter	Data Type	Description
Forwarder Name*	String	Display name of the forwarder
Filter Type*	Enum	Filter type that was selected while creating a forwarder on logger. Valid types are *Unified* or *Regex*.
Query	String	Used to filter events that the forwarder will forward.
Unified Query Filters	String	Select from the default and user-defined Unified filters on the source Logger. Only visible if Filter Type is Unified.

Logger UDP Forwarder Configuration Parameters, continued

Parameter	Data Type	Description
Regular Expression Filters	String	Select from the default and user-defined Regex filters on the source Logger. Only visible if Filter Type is Regex.
Start Time	DateTime	Optional start of time range for selection.
End Time	DateTime	Optional end of time range for selection.
IP/Host*	String	IP address or host name of the destination that will receive forwarded events.
Port*	Integer	Port number on the destination that will receive forwarded events. Ensure this port is open on the destination.
Enable*	Boolean	If **Yes**, the forwarder is enabled.
Preserve System Timestamp*	Boolean	If **Yes**, the timestamp showing original event receipt time is preserved.
Preserve Original Syslog Sender*	Boolean	If **Yes**, event is sent as is, without inserting Logger's IP address in the hostname (or equivalent) field of the syslog event.

SecureData Configuration

A SecureData configuration sets values for the SecureData encryption client on a managed Logger.

SecureData Configuration Parameters

Parameter	Data Type	Description
Server*	String	SecureData server IP address.
Port*	String	SecureData server port.
Auth Identity*	String	SecureData authentication identity
Shared Secret*	String	SecureData shared secret
Event Fields*	String	Comma-separated list of event fields to be encrypted. Default data for event fields will be populated from the connector bin file uploaded in the repository. If there is no such file, then the default field will be defined by ArcMC.

System Admin Configuration Types

System Admin configurations set values for system administrative settings. The available System Admin configuration types are listed here.

Authentication External

An Authentication External configuration defines values and behavior for a hardware or software system requiring authentication to an external server, such as LDAP or RADIUS.

After changing the Authentication Method on a host, you must delete the host from ArcMC, then re-add it using Node Management.

> **Note:** Authentication External configurations can only be imported from managed Loggers, not created in ArcMC. See "Importing a Subscriber Configuration" on page 889 for more information.

Authentication External Configuration Parameters

Parameter	Data Type	Description
Authentication Method*	String	System authentication method.
Allow Local Password Fallback for Default Admin Only*	Boolean	If **Yes**, the authentication server will fall back to local passwords for authentication for administrators.
Allow Local Password Fallback for All Users*	Boolean	If **Yes**, the authentication server will fall back to local passwords for authentication for all users.
LDAP Server Hostname[port]*	String	LDAP server hostname and port.
LDAP Backup Server Hostname [port]	String	LDAP backup server hostname and port.
LDAP Server Request Timeout (seconds)	Integer	LDAP server request timeout, in seconds.
RADIUS Server Hostname[port]	String	RADIUS server hostname and port.
RADIUS Backup Server Hostname [port]	String	RADIUS backup server hostname and port.
RADIUS Shared Authentication Secret	String	RADIUS authentication shared secret.
RADIUS Server NAS IP Address	String	RADIUS server Network Access Server IP address .
RADIUS Request Timeout (seconds)	Integer	RADIUS server request timeout, in seconds.
RADIUS Retry Request	Integer	Number of times to retry RADIUS server requests.
RADIUS Protocol	String	Type of RADIUS protocol.

Authentication Local Password

An Authentication Local Password configuration defines a hardware or software system's local password options and behavior.

Authentication Local Password Configuration Parameters

Parameter	Data Type	Description
Enable Account Lockout*	Boolean	If **Yes**, account lockouts are enabled after an incorrect password entry.
Lock Out Account after N Failed Attempts*	Integer	Number of failed attempts before lockout.
Remember Failed Attempts For (seconds)*	Integer	Time, in seconds, between failed attempts that will trigger a lockout.
Lockout Account for (minutes)*	Integer	Time, in minutes, that the account will be locked out.
Enable Password Expiration*	Boolean	If **Yes**, password expiration is enabled
Password Expires in (days)*	Integer	Interval, in days, after which a password expires.
Notify User (Days Before Expiration)*	Integer	Days before password expiration that the user is notified.
Users Exempted from Password Expiration Policy	List of comma-separated strings	Comma-separated list of users whose passwords will never expire.
Enforce Password Strength*	Boolean	If **Yes**, password strength is enforced.
Minimum Length (characters)*	Integer	Minimum number of password characters.
Maximum Length (characters)*	Integer	Maximum number of password characters.
Numeric [0-9]*	Integer	Minimum number of numeric password characters.
Upper Case [A-Z]*	Integer	Minimum number of uppercase password characters.
Lower Case [a-z]*	Integer	Minimum number of lowercase password characters
Special [1$^*...]*	Integer	Minimum number of special password characters.
Password Must Be At Least*	Integer	Minimum number of characters a new password must differ from the user's previous password.
Include "Forgot Password" link on Login Screen*	Boolean	If **Yes**, a link is provided where the user can recover a password.

Authentication Session

An Authentication Session configuration defines values for a hardware or software system's authentication sessions.

Authentication Session Configuration Parameters

Parameter	Data Type	Description
Max Simultaneous Logins Per User*	Integer	Maximum number of simultaneous logins per user. If Max Simultaneous Logins/User is set to 1, it is required to have at least another admin user, otherwise the admin user will not be able to log in.
Logout Inactive Session After (seconds)*	Integer	Inactivity session timeout, in seconds.
Disable Inactive Account After (days)*	Integer	Number of days of inactivity after which an account will be disabled.

DNS Configuration

A DNS Configuration defines values for a hardware appliance's Domain Name Service.

DNS Configuration Parameters

Parameter	Data Type	Description
Primary DNS*	String	Primary DNS server.
Secondary DNS	String	Secondary DNS server.
DNS Search Domains	List of comma-separated strings	Comma-separated list of DNS search domains.

FIPS Configuration

A FIPS configuration enables or disables FIPS mode on a managed node.

Note: After pushing a FIPS configuration, the destination node will be restarted.

FIPS Configuration Parameters

Parameter	Data Type	Description
Enabled*	Boolean	If **Yes**, FIPS is enabled on the node.

Network Configuration

A Network Configuration defines values for a hardware appliance's default gateway setting.

Note: Values for these network settings cannot be changed through ArcSight Management Center: hostname, IP addresses for the network interfaces, static routes, /etc/hosts file, and time settings.

Network Configuration Parameters

Parameter	Data Type	Description
Default Gateway*	String	Default network gateway.

NTP Configuration

An NTP Configuration defines values for a hardware appliance's Network Time Protocol.

NTP Configuration Parameters

Parameter	Data Type	Description
Enable as NTP Server*	Boolean	If **Yes**, the system is enabled as an NTP server.
NTP Servers*	List of comma-separated strings	Comma-separated list of NTP servers. Required even if **Enable as NTP Server** is false.

SMTP Configuration

An SMTP Configuration defines values for a hardware or software system's Simple Mail Transfer Protocol.

SMTP Configuration provides for authentication and security. This is implemented through the primary STMP server port, primary username, primary password, primary certificate, backup STMP server port, backup username, backup password, and backup certificate fields, along with the primary STMP server, backup STMP server, and outgoing email address fields.

SMTP Configuration Parameters

Parameter	Data Type	Description
Primary SMTP Server*	String	Primary SMTP server.
Secondary SMTP Server	String	Secondary SMTP server.
Outgoing Email Address*	String	Outgoing email address.
Enable Auth/TLS	Boolean	Enable/Disable secure authenticated mode of communication with SMTP server
Primary SMTP Server Port	Integer	Primary SMTP Server Port. Required if Auth/TLS is enabled.

SMTP Configuration Parameters, continued

Parameter	Data Type	Description
Primary SMTP Server Username	String	Primary SMTP Server Username. Required if Auth/TLS is enabled.
Primary SMTP Server Password	String	Primary SMTP Server Password. Required if Auth/TLS is enabled.
Primary SMTP Server Certificate Content	String	Upload Primary SMTP Server Certificate. Required if Auth/TLS is enabled.
Secondary SMTP Server Port	Integer	Secondary SMTP Server Port. Required if Auth/TLS is enabled.
Secondary SMTP Server Username	String	Secondary SMTP Server Username. Required if Auth/TLS is enabled.
Secondary SMTP Server Password	String	Secondary SMTP Server Password. Required if Auth/TLS is enabled.
Secondary SMTP Server Certificate Content	String	Upload secondary SMTP Server Certificate. Required if Auth/TLS is enabled.

SNMP Poll Configuration

An SNMP Poll Configuration defines values for a hardware appliance's Simple Network Management Protocol monitoring. supports V2c and V3 of SNMP.

SNMP Poll Configuration Parameters

Parameter	Data Type	Description
Status	Boolean	If **Yes**, SNMP polling is enabled.
Port*	Integer	SNMP port.
SNMP Version*	String	Version of SNMP supported.Valid values are v2c and v3.
Community String	String	SNMP community string. Required for V2c only.
Username	String	Authentication username. Required for V3 only.
Authentication Protocol*	String	Authentication protocol. Valid values are MD5 and SHA. Required for V3 only.
Authentication Passphrase	String	Authentication passphrase. Required for V3 only.
Privacy Protocol	String	Privacy protocol. Valid values are DES and AES128. Required for V3 only.
Privacy Passphrase	String	Privacy passphrase. Required for V3 only.
System Name	String	Name of the SNMP system.
Point of Contact	String	Point of contact.
Location	String	System location.

SNMP Trap Configuration

An SNMP Trap Configuration defines values for a hardware appliance's Simple Network Management Protocol notifications. supports V2c and V3 of SNMP.

Note: In previous versions of , an SNMP Trap configuration was known as an SNMP Configuration.

SNMP Trap Configuration Parameters

Parameter	Data Type	Description
Status	Boolean	If **Yes**, SNMP polling is enabled.
NMS IP Address	String	IP address of network management server.
Port*	Integer	SNMP port.
SNMP Version*	String	Version of SNMP supported.Valid values are v2c and v3.
Community String	String	SNMP community string. Required for V2c only.
Username	String	Authentication username. Required for V3 only.
Authentication Protocol*	String	Authentication protocol. Valid values are MD5 and SHA. Required for V3 only.
Authentication Passphrase	String	Authentication passphrase. Required for V3 only.
Privacy Protocol	String	Privacy protocol. Valid values are DES and AES128. Required for V3 only.
Privacy Passphrase	String	Privacy passphrase. Required for V3 only.

Logger Initial Configuration Management

A *Logger initial configuration* is intended for the rapid, uniform setup of multiple ArcSight Loggers of the same model number and software version. Use a Logger initial configuration to expedite the initial deployment of Loggers to a production environment. Initial configuration management is supported on Logger version 6.1 or later.

A Logger initial configuration is not created in ArcMC. Instead, a suitable initial configuration is created on a managed Logger and imported into ArcMC. The configuration may then be pushed to other managed Loggers of the same model and software version number.

The following attributes are shown for each initial configuration:

Attribute	Description
Imported Init-Config Name	Name of the imported initial configuration.
Product Type	Type of Logger to which the configuration may be pushed: either Logger (appliance) or SWLogger (software)
Source Host	IP address of the host from which the configuration was imported.
Imported On	Date of import.
Imported By	User who imported the configuration.
SW Version	Software version of the configuration.
Source Model	For appliances, the model number of the source host Logger. (For software Logger, this is shown as Software.)

You can perform the following initial configuration management tasks:

- Import an Initial Configuration
- Push an Initial Configuration
- View the Initial Configuration Event History
- Delete an Initial Configuration

Importing a Logger Initial Configuration

An initial configuration created on a managed Logger (of version 6.1 or later) may be imported into , for editing and pushing to other Loggers.

ArcMC can store up to 30 initial configurations.

To import an initial configuration from a Logger of version 6.1 or later:

1. Click **Configuration Management > Logger Initial Configurations.**
2. Under **Configurations**, click **Import**.
3. On the **Import Initial Configuration** dialog, in **Name**, specify a name for the configuration you wish to import.
4. Under **Source Host URI**, select the node from which you wish to import the configuration.
5. Click **Import**. The configuration is imported into and is shown in the **Configurations** table.
6. Optionally, if you wish to push the imported configuration to managed nodes, when prompted to push, click **Yes**.

Note: An initial configuration is not created in ArcMC. Instead, create the initial configuration on a managed Logger, then import it into ArcMC for pushing to other managed Loggers.

Pushing a Logger Initial Configuration

You can push a Logger initial configuration to selected managed Loggers of version 6.1 or later. The destination Loggers must be of the same software version (and, for hardware appliances, model number) as the Logger on which the initial configuration was created.

The push process overwrites the settings on the destination Loggers.

Pushing a Logger initial configuration must be performed manually.

> **Note:** Before performing a push, ensure that the destination Logger's storage volume is set up, and that it exceeds that of any source Logger.

To push an initial configuration to one or more managed Loggers of version 6.1 or later:

1. Click **Configuration Management > Logger Initial Configurations.**
2. From the **Configurations** table, select a configuration to be pushed.
3. Click **Push**.
4. On the **Make Selections for Push** dialog, under **Available Nodes**, the nodes eligible for receiving a push are displayed by location. Browse to the recipient node and click **Add**. The selected node is shown under **Selected Nodes.** (To select multiple nodes to receive a push, Ctrl+click each selected node.)
5. Click **Push**.
6. Click **Yes** to confirm the push and change settings on the destinations. The configuration is pushed to the selected destination nodes.

> **Tip:** In order to correctly view push status, click **Refresh**, even if the status is shown as In Progress.

Push Results on a Destination Logger

The results of a push of an initial configuration on a given setting of a destination Logger are dependent on the setting, as shown in the following table.

Setting on Destination	Result After Push
• Archive storage settings • Audit logs • ESM destinations • Event archives • Finished tasks • Forwarders • Peer Loggers	**Blank:** These settings will be blank on the destination, even if they are included in the pushed initial configuration. Also, all configurations on the destination Logger related to these settings will also be blanked.
• Alerts • User-created receivers (RFSFileReceiver, FileTransfer, FolderFollowerReceiver)	**Disabled:** These settings are disabled on the destination Logger, but are editable through the destination Logger's UI.
• Hosts file • Groups • Users	**Copied From Source:** These values are copied from the initial configuration and overwritten on the target. This may include user credentials that the Logger uses to authenticate to ArcMC, which could break the management link between ArcMC and the destination Logger (which requires these credentials). If an overwrite of these credentials occurs, to enable management, delete the host from ArcMC, then re-add the Logger as a host (with the new credentials).
• All other settings	**Copied From Source:** Values are copied from the initial configuration and overwritten on the target.

Deleting a Logger Initial Configuration

A deleted initial configuration is no longer available for pushes. You may not delete a configuration currently being pushed.

To delete an initial configuration:

1. Click **Configuration Management > Logger Initial Configurations.**
2. From the **Logger Initial Configurations** table, select one or more configurations to be deleted.
3. Click **Delete.**
4. Click **Yes** to confirm deletion.

Event History

The **Event History** list records all imports, pushes, and deletes transactions related to initial configuration pushes. Each event in the history displays the following information:

Column	Description
Init-Config Name	Initial configuration's name.
Author	User who performed the action.
Event Type	Type of event recorded for the initial configuration. Event types include Push, Import, and Delete.
Event Occurrence	Local date and time of the event.
Source Host	URI of the host on which the initial configuration was created.
Destination URI for Push	If the event is of type Push, this is the URI of the destination node to which the initial configuration was pushed.
Event Status	Status of the event. Status types include: • In-progress: the transaction is still in progress. • Successful: the transaction succeeded. • Failed: the transaction failed. Click the failed status to view an indication of the failure reason.

To search for a specific event by any of these criteria, click the drop-down in the corresponding column header. Then, in **Filters**, select or specify the specific criterion for which you wish to show events. Only events matching the filter will be displayed in the **Event History** list.

For example, to see all pushes, in the **Event Type** column, click the header drop-down. Then, in **Filters**, select *Push*.

Managing Logger Event Archives

Logger Event Archives enable you to save the events for any day in the past (not including the current day). In , you can view Logger Event Archives on managed Loggers, and perform management tasks including loading, unloading, and indexing archives.

Logger Event Archive management is only available for managed Loggers of version 6.2 or later.

For complete information on managing Logger Event Archives, see the Logger Administrator's Guide.

The following parameters are shown on the Logger Event Archives list:

Parameter	Description
Peers	For Loggers, the number of peers of the Logger. To see the Logger's peers in detail, click the number shown.
Event Status	The status of a current archiving job, where status is one of the following values: • *Loading:* The archive is being loaded on the managed Logger. • *Loaded*: The archive is currently loaded on the managed Logger. • *Unloading*: The archiving job is currently executing. • *Archived*: The archiving job is complete. • *Failed*: The archiving job was not successful.
Index Status	The status of a current indexing job, where status is one of the following values. • *None:* No indexing status is available. • *Pending*: The indexing job is about to begin. A pending job can be canceled by clicking in the **Cancel** column of the table. • *Indexing*: The indexing job is in process. • *Indexed*: The indexing job is complete. • *Failed*: The indexing job was unsuccessful.
Cancel	Click the **X** to cancel a pending indexing job before it begins.

To view Logger event archives:

1. Under **Configuration Management**, select **Logger Event Archive.**
2. On the **Event Archive List** tab, select your criteria to search for Logger Event Archives on managed Loggers.
3. Select a Start and End Date, then select one or more Loggers to search.
4. Click **Search**. All Logger Event Archives matching the search criteria are listed in hierarchical format: by managed Logger, then by Storage Group, and finally by Event Archive.

To toggle the view open or closed, click **Expand** or **Collapse**.

Managing Event Archives

You can perform two management tasks on managed Loggers related to event archives: loading (or unloading) archives, and indexing them.

To load an event archive:

1. On the Event Archive List, select an archive to load.
2. Click **Load Archive**. The selected operation will be performed. The status of the job will be shown in the **Event Status** column.

To index an Event Archive:

1. On the Event Archive List, select an archive to index.
2. Click **Index Archive**. The selected archive will be indexed. The status of the indexing job will be shown in the **Index Status** column.

Viewing Load/Unload History

You can also view your Logger event archive load, unload, and indexing history. This displays the actions taken in ArcMC to view Logger Event Archives.

To view Logger event archive load/unload history:

1. Under **Configuration Management**, select **Initial Configurations > Logger Event Archive.**
2. Click the **Archive Load/Unload History** tab. The activity history is displayed.

Managing Logger Peers

Managed Loggers can be peered with any number of other Loggers. You can manage the peer relationship between Loggers in ArcMC. ArcSight recommends that, if possible, all peer Loggers be managed by ArcMC.

You can view peers; add or remove peers to a Logger; and import, edit, push, and delete peer groups. A *peer group* is a named set of Loggers you can use to organize and administer sets of Loggers more easily.

> **Note:** For more information about Logger peering, please refer to the ArcSight Logger Administrator's Guide.

Viewing Peers or Peer Groups

You can view the peers of a Logger managed by ArcMC, as long as the Logger is version 6.1 or later.

To view peered Loggers in ArcMC:

1. Select **Configuration Management > Logger Peers.** The **Logger Peers** table is displayed with all managed Loggers of version 6.1 or later.
2. To view the Loggers peered to a specific Logger in the list , in the **Peer Loggers** column, click the link indicating the number of peers. The filterable **Peer Loggers** dialog lists all the

Logger's peers.

3. To view peer groups in ArcMC, click **View Peer Groups.**

Adding or Removing Peers

You can add peers to, or remove peers from, a Logger managed by ArcMC, as long as the managed Logger is version 6.1 or later.

> **Note:** If you remove a Logger not managed by ArcMC as a peer, you will not be able to add it back to the group unless you import the peer group including the Logger into ArcMC, or you add the removed Logger to ArcMC management.

To add peers to, or remove peers from, a Logger:

1. Select the Logger whose peers you wish to edit from the **Logger Peers** table.
2. Click **Edit Peers.**
3. All currently peered Loggers are shown.
   a. To add one or more peers, click **Add Peers**. Then, in the **Add Peers** dialog, select the Loggers to be added as peers. Optionally, to create a new peer group in ArcMC, in **Peer Group Name**, enter a name for the peer group. Then, click **Add**.
   b. To remove one or more Loggers as peers, select the Loggers to remove, and click **Remove Peers.** Click **Yes** to confirm removal as peers.

> **Note:** For this release, Logger peering is supported using user name and password, not authorization code.

Importing a Peer Group

You can import Logger peer groups into ArcMC. Importing a peer group is only supported on Loggers version 6.1 or later.

To import a peer group from a Logger (of version 6.1 or later):

1. Select **Configuration Management > Logger Peers.**
2. Click **View Peer Groups.**
3. Click **Import Peers.**
4. On the **Select Peer** dialog, select a managed Logger. (The selected Logger will also be part of the imported peer group.) Then, click **Next**.
5. On the **Select Peer (of the Target)** dialog, select one or more peers to import into ArcMC.

6. In **Peer Group Name**, enter a name for the selected peer group.
7. Click **Import**. The selected peer group is imported into ArcMC.

Edit a Peer Group

You can edit a peer group, including the name, peered Logger hostname, and group members.

To edit a peer group:

1. Select**Configuration Management > Logger Peers.**
2. Click **View Peer Groups.**
3. Click the name of the peer group you wish to edit.
4. On the **Edit Peer Group** dialog, edit the peer group as needed. You can edit the peer group name, and add or remove peers from the group.
5. Click **Save**. Alternatively, click **Save As...** to save the peer group under a new name.

Pushing a Peer Group

You can push a peer group to one or multiple managed Loggers of version 6.1 or later. The Loggers in the group will become peered with the managed Loggers to which you pushed the group.

To push a peer group:

1. Click **Configuration Management > Logger Peers.**
2. Click **View Peer Groups.**
3. From the table, select a peer group to push.
4. Click **Push**.
5. On the **Destination Loggers** dialog, select one or more destination Loggers to which to push the peer group.
6. Click **Push**. The peer group is pushed to the destination Loggers.

Deleting a Peer Group

You can delete a peer group from ArcMC.

To delete a peer group:

1. Click **Configuration Management > Logger Peers.**
2. Click **View Peer Group.**

3. From the list of peer groups, select a group to delete.
4. Click **OK** to confirm deletion.

Managing Transformation Hub

You can use ArcMC to perform management and monitoring of Transformation Hub. These functions include adding topics, managing routes, and status monitoring.

About Topics

A *topic* is a metadata tag that you can apply to events in order to categorize them. Transformation Hub ships with several pre-set topics, and you can define any number of additional topics as needed.

A topic includes these components:

- **Name:** The name of the topic.

  > **Note:** ArcSight Avro is the displayed name for the type name event-avro for the ArcSight avro topic.

- **Topic Type:** The type of topic CEF (routable) ArcSight Avro (routable) BINARY (not routable) RAW (not routable) SYSLOG (not routable).
- **Partition Count:** A segment of a topic. There can be one or more partitions for each topic. The number of partitions limits the maximum number of consumers in a consumer group.
- **Replication Factor:** The number of copies of each partition in a topic. Each replica is created across one Transformation Hub node. For example, a topic with a replication factor of 3 would have 3 copies of each of its partitions, across 3 Transformation Hub nodes.

You can only use ArcMC to add topics (not delete them). The **Edit** option is only available for topics with a *null* topic type (topics not created by ArcMC. e.g. Kafka manager) and it allows the user to modify the **Topic Type** value.

To set the type for existing topics (only for topics not created by ArcMC. e.g. Kafka manager), users can access the **List of Topics** page located in **Configuration Management > Transformation Hub > Topics.** This page will display detailed information for Topic Name, Topic Type, Routable Topic, Partitions Count, and Replication Factor. This option is only available for Transformation Hub 3.4+.

For more information on managing topic partitions and replication, please see "Managing Topics" on page 677.

Adding a Topic

To add a topic:

1. Click **Configuration Management > Transformation Hub.**
2. On the Transformation Hub Configurations page, click **Topics > + Add.**
3. On the Add New Topic dialog, in **Topic Name**, specify a name for the new topic.
4. In **Topic Type**, select the type for the new topic.

> **Note:** For Transformation Hub 3.4 and later users must select the topic type when adding the new topic. This option is disabled for Transformation Hub 3.3 or earlier.

5. In **# of Partitions,** specify the number of partitions the topic will have.
6. In **Replication Factor**, specify the number of copies that will be made for each partition.
7. Click **Save**.

> **Best Practice:** When creating a topic, use a value for replication factor of at least 2. In addition, the number of partitions should be equal to the number of consumers which will be subscribed to the topic (now and in future). If ArcSight Database will be a consumer, the number of partitions should be a multiple of the number of Database nodes.

About Routes

A *route* is a method of retrieving events in a topic that meet certain criteria and then copying them into a new topic. Use routes to filter events into your topics for your own requirements, such as selecting a group of events for more detailed examination.

A route comprises these components:

- **Name:** Name of the route.
- **Routing Rule:** A logical filter that defines criteria by which events will be categorized into topics. The criteria are defined in terms of CEF and Avro fields for Transformation Hub 3.4 and later, and CEF only for Transformation Hub 3.3 and earlier.
- **Source Topic:** The topic being filtered for events which match the routing rule.
- **Destination Topic:** The topic to which a copy of an event matching the routing rule should be copied. (A copy of the event will remain in the source topic.)
- **Description:** A short description of the route.

You can add, edit, or delete routes in ArcMC. Routes only apply to CEF and Avro topics for Transformation Hub 3.4 and later, and CEF only for Transformation Hub 3.3 and earlier. Routes created to or from a binary topic (such as th-binary_esm) will not function.

As a general guideline, th-arcsight-avro is no longer recommended as a source topic for Avro routing, since enrichment stream processors were added as intermediate layer between th-arcsight-avro and mf-event-avro-enriched in Transformation Hub 3.5 . This makes the mf-event-avro-enriched topic the current primary source topic for the platform's database scheduler (replacing th-arcsight-avro). As a result, the routing starting point should start from the mf-event-avro-enriched topic to benefit from event enrichment.

Creating a Route

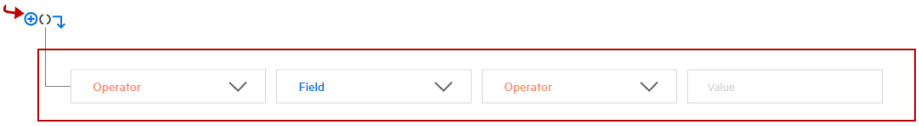
Routes cannot be created until Stream Processors are enabled.
Prior to creating a route, ensure that your source and destination topics already exist. If not, create them before creating a route that uses them.

To create a route:

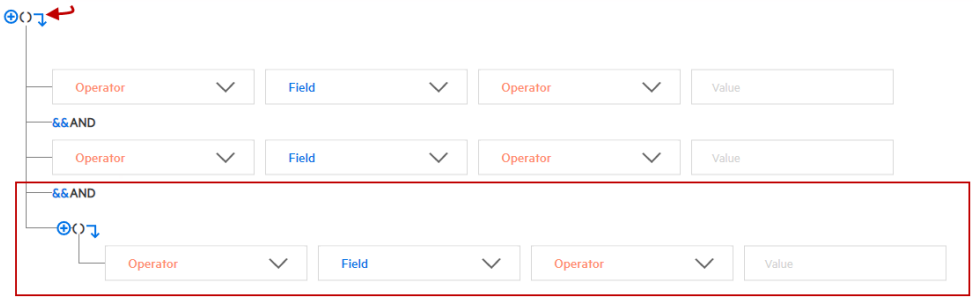
1. Click **Configuration Management > Transformation Hub.**
2. On the Transformation Hub Configurations page, click **Routes > +Add**.
3. In **Route Name**, specify a name for the route.
4. From the **Source Topic** drop-down list, select the topic from which events will be filtered.
5. From the **Destination Topic** drop-down list, select the destination to which events will be copied.
6. In **Description**, specify a short description of the route.
7. Under **Add Routing Rule**, use the Rule Editor to define the criteria for the routing rule.

Note: Only routable topics are displayed in the drop-down list for both **Source Topic** and **Destination Topic** when adding a new route. This option is only available for Transformation Hub 3.4.

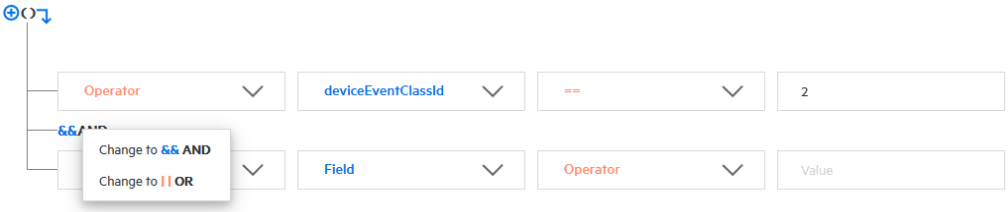
- Define a criterion by using the drop-downs to select a **Field, Operator,** and **Value** as a filter. **Fields** and **Operators** are based on the **Source Topic** type.
- Click + to add a new conjunction (& AND, || OR), or the right arrow to add a dependent conjunction. Then define any new required criteria as needed.



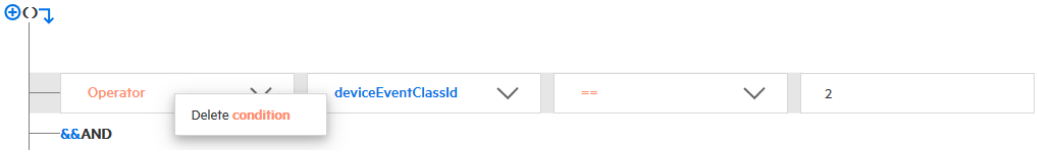
- You can create nested conjunctions by clicking the right arrow at the same level as the current conjunction.



- To change a conjunction, right-click the conjunction and select your choice from the drop-down menu.



- To delete a conjunction, right-click the conjunction and pick Delete. Note that deleting a conjunction will delete all the criteria associated with the deleted conjunction.



The rule is shown in the rule field as you construct it. When the rule is complete, click **Save**.

> The following IP address routing fields are only supported in Avro routing:
> `agentAddressBin`
> `agentTranslatedAddressBin`
> `destinationAddressBin`
> `destinationTranslatedAddressBin`
> `deviceAddressBin`
> `deviceTranslatedAddressBin`
> `sourceAddressBin`
> `sourceTranslatedAddressBin`

Editing a Route

To edit a route:

1. Click **Configuration Management > Transformation Hub > Routes.**
2. On the Transformation Hub Configurations page, select the route to edit, then click **Edit**.
3. Edit the route as needed, then click **Save**.

Deleting a Route

To delete a route:

1. Click **Configuration Management > Transformation Hub > Routes.**
2. On the Transformation Hub Configurations page, select one or more routes to delete, then click **Delete**.
3. Click **Yes** to confirm deletion.

ColleDeployment Templates

A *deployment template* is a pre-set collection of settings and parameters for a connector.

When you deploy that connector type using the Instant Connector Deployment process, and specify a deployment template, all of the settings you have predefined in the template are applied during the deployment.

You may specify any number of deployment templates for each connector type.

> **Note:** During the deployment process, you are prompted to use the predefined template settings, but may choose to overwrite any of the predefined template settings to custom-fit a particular deployment.

Managing Deployment Templates

> You should be familiar with the settings for Connectors before managing deployment templates. These settings are described in detail in the Smart Connector User's Guide at ArcSight SmartConnectors 24.2 documentation.

Prior to managing any deployment templates, first upload the appropriate 64-bit Connector installer file to your ArcMC repository. Only the Linux and Windows 64-bit installers are supported. The installer contains a list of currently supported Connectors and is used in the creation of the Connector list in ArcMC. This upload only needs to be done in preparation to manage deployment templates.

To upload the installer file to ArcMC:

1. Download the Connector installer file to a secure network location.
2. In ArcMC, click **Administration > Application > Repositories.**
3. In the navigation menu, click **Upgrade Files.**
4. Click **Upload**.

5. Under **Upload Upgrade Repository**, click **Choose File.** Then, browse to and select the installer file you previously downloaded.
6. Click **Submit**. The installer file is uploaded to ArcMC.

Additional Files

Note that some connector types may require additional, supplementary files to function correctly, such as Windows DLLs. Such files are not included in the connector installer file.

If additional files are required for a connector type, you must also upload these files to an ArcMC repository before attempting to deploy them using the Instant Connector Deployment process. After uploading the installer file as described, upload additional files (in ZIP format) to the following repositories:

File Type	Repository
SecureData server certificate (Certificate_FPE)	cacert. **Note:** The certificate must be Base 64 encoded. For Linux plarforms (only), it must include the .pem extension.
Windows DLL, JavaLibrary	JDBC Drivers
FlexParsers	Flex Connectors

You will be able to specify the location of these additional files when you create the deployment template.

To create a deployment template:

Click **Configuration Management > Deployment Templates.**

1. In the navigation menu, from the list of supported Connectors, select the type of Connector for which you wish to create a template.
2. In the management panel, click **New**.
3. To clone a template from an existing template of the same type, click **+ New/Clone**.

   To clone a template, select one from the **Copy from** dropdown and the values are populated based on the selected template instance.
4. Enter values for any required settings (marked with an asterisk *), as well as any settings you wish to apply to all Connectors of that type when using Instant Connector Deployment. (**Note:** Spaces in file or path names are not supported.)
5. If additional files are needed for operation, such as a Voltage server certificate, under **File Table Fields**, enter values for file name, type, and any other required fields. If more than 1 additional file is needed, click **Add Row**, and then specify the details of the additional file. Repeat for additional files as needed.
6. Click **Save**.

ArcSight SecureData Add-On Enablement: To enable the ArcSight SecureData Add-on during deployment, under **Global Fields**, set **Format Preserving Encryption** to *Enabled*. Note that only a single instance of the add-on is supported on Windows clients. If you wish to move the add-on to a new location, you must first uninstall the previously installed client before launching Instant Connector Deployment.

To delete a deployment template:

1. In the navigation menu, browse to the template you wish to delete. (Templates are sorted by Connector type.)
2. In the management panel, select the template and click **Delete**. Click **Yes** to confirm deletion.

Bulk Operations

The following topics are discussed here.

Location

The **Location** tab displays all locations defined in ArcMC. The **Location** tab includes these buttons:

Add	Adds a new location. For more information, see "Adding a Location" on page 812
Edit	Edits the name of a location. For more information, see "Editing a Location" on page 812
Delete	Deletes one or more selected locations from ArcMC. For more information, see "Deleting a Location" on page 813

The **Manage Locations** table displays these parameters for each location.

- **Name:** Location name.
- **Number of Hosts:** Number of hosts assigned to the location.

Host Tab

The Host tab displays all hosts associated with the location selected in the navigation tree. The Hosts tab includes these buttons:

Update Credentials	Updates the host's credentials. For more information, see "Updating Host Credentials " on page 942
Download Certificate	Downloads the host's current certificates. For more information, see "Downloading and Importing Host Certificates" on page 943

Scan Host	Scans each port on non-appliance based hosts. For more information, see "Scanning a Host" on page 943
Move	Moves selected hosts to a new location. For more information, see ""Moving a Host to a Different Location" on page 945
Delete	Deletes selected hosts from ArcMC. For more information, see "Deleting a Host" on page 945

The **Hosts** table displays these parameters for each host:

- **Hostname:** Fully qualified domain name (FQDN) or IP address of the host. The hostname must match the hostname in the host's SSL certificate. (If IP address was used to add the host, then the certificate will match the IP address used.)
- **Path:** Path to the host.
- **Agent Version:** Version number of the ArcMC Agent running on the host.
- **Issues:** Status of any issues associated with the host. Possible indicators include:
  - *None:* No issues are associated with the host.
  - *Internet connection Not Present:* The host is currently not reachable by internet connection. Displayed when ArcMC is not able to connect to the Marketplace for retrieving parser upgrade versions. If the user environment needs a proxy server for an internet connection, configure the logger.properties file. If the user environment is an appliance, save the DNS settings on the **System Admin > Network** page.
  - *Valid Marketplace Certificate Not Found in ArcMC*: Displayed when the Marketplace certificate does not match the one found in ArcMC's trust store.
  - *Host Certificate Mismatch:* The hostname does not match the hostname in the SSL certificate. For instructions on downloading and importing certificates for the host, see "Downloading and Importing Host Certificates" on page 943. If this issue is displayed for the localhost, and the certificate cannot be downloaded, please restart the web service on the localhost.
  - *ArcMC Agent Out of Date:* The host's Agent version cannot be upgraded from the managing ArcMC, or the ArcMC cannot communicate with the ArcMC Agent on the managed node. You may need to manually install the ArcMC Agent. For requirements and instructions, see "Installing the ArcMC Agent" on page 802
  - *ArcMC Agent Stopped:* The Agent process on the host has been stopped.
  - *ArcMC Agent Upgrade Recommended:* The host's Agent version is older than the one on the managing ArcMC. An Agent upgrade is recommended.
  - *ArcMC Agent Uninstalled:* The Agent on the host has been uninstalled.
  - *ArcMC Agent Down:* The Agent on the host is not running.
  - *Update the authentication credentials on the localhost, then install the ArcMC Agent:* For a localhost added for remote management, authentication credentials need to be

updated to ensure authentication, then the ArcMC Agent needs to be installed to enable management. Take both of these steps to correct this issue.

- *Error in REST Authentication*: The Transformation Hub node lacks the ArcMC certificate, ArcMC session ID, or ArcMC URL and port. To resolve this issue:
  - Make sure that the OMT Cluster has been configured correctly with the appropriate ArcMC details. For more information, please see "Configuring ArcMC to Manage a Transformation Hub" on page 355.
  - Note that each time the user replaces the ArcMC certificate to the TH's location, the TH's webservice pod has to be restarted for the new certificate to be read and updated in the trust store.

- **Model:** If the host is an appliance, this shows the ArcSight model number of the appliance. If the host is not an appliance, the label *Software* is shown.
- **Type:** Type of installation, either ArcMC Appliance or Software.
- **Version:**Version number of the software on the host.

Container Tab

The Containers tab includes the **Properties** button, it allows you to modify the properties of Containers.

The **Containers** table includes the following columns:

- **Name:** Name of the container.
- **Path:** Path to the container.
- **Issues:** Status of any issues associated with the container.
- **Port:** Port number through which the container is communicating.
- **Framework Ver:** Framework version number of the container.
- **Parser Ver:** Parser version number of the container.
- **Status:** Status of the container. Possible values for container status are:
  - *Improper configuration: Initial default state.*
  - *Initializing connection:* The connector has a resolvable URL, but ArcMC has not logged in to the connector yet.
  - *Down*: There was an exception trying to execute the login command.
  - *Unauthorized:* The login command was executed, but login has failed.
  - *Connecting:* The login is in progress.
  - *Connected:* The login was successful.
  - *Empty:* Login successful, but the container doesn't have connectors.

  - *Initialized:* Login successful and the container has connectors.
  - *Unknown:* No information on status. To resolve, manually SSH to the system and restart the container.
- **Last Check:** Date and time of last status check.

Transformation Hub Tab

The **Transformation Hub** table includes the following columns:

- **Transformation Hub:** Name of the Transformation Hub.
- **Host:** Name of the host.
- **Port:** Port number through which the Transformation Hub is communicating.
- **Last Check:** Date and time of the last status check.

For more information on connector management, see "Managing Connectors" on page 860

Updating Collector Properties

To update Collector properties:

1. Click **Configuration Management > Bulk Operations**.
2. On the **Manage Collectors** page, select the item you wish to manage.
3. Click **Properties**.
4. On the **Property Update** page, click **Edit**
5. Edit the Collector properties as needed.
6. To add a new property, enter the property, a value for the property, and click the check mark.
7. When complete, click **Save**.

Retrieving Collector Logs

To retrieve Collector logs:

1. Click **Configuration Management > Bulk Operations**.
2. On the **Bulk Opeartions** page, select one or more items for which you wish to retrieve logs.
3. Click **Retrieve Logs**.
4. Follow the wizard prompts to zip the selected logs into a single file.
5. To view the logs, on the main menu bar, click **Admin > Repositories.** The log zip file is stored in the *Logs* respository.

Updating Collectors Parameters

To update Collector parameters:

1. Click **Configuration Management > Bulk Operations**.
2. On the **Manage Collectors** page, select one or more items for which you wish to update parameters.
3. Click **Update Parameters**.
4. On the **Collector Parameter Update** page, enter values for the parameters, as needed.
5. Click **Save**. The parameters are updated for the selected items.

Updating Collector Destinations

To update Collector destinations:

1. Click **Configuration Management > Bulk Operations**.
2. On the **Manage Collectors** page, select one or more items for which you wish to update destinations.
3. Click **Update Destinations**.
4. On the **Collector Destination Update** page, enter values for the destinations, as needed.
5. Click **Save**. The destinations are updated for the selected items.

Updating Collector Credentials

To update Collector credentials:

1. Click **Configuration Management > Bulk Operations**.
2. On the **Manage Collectors** page, select one or more items for which you wish to update credentials.
3. Click **Credential**.
4. On the **Collector Credential Update** page, enter values for passwords, as needed. (The username is fixed as *collector*.)
5. Click **Save**. The passwords are updated for the selected Collectors.

Note: Updating Collector credentials from ArcMC does not update the actual credentials, just the credentials ArcMC uses to authenticate.

Restarting Collectors

To restart one or more Collectors:

1. Click **Configuration Management > Bulk Operations.**
2. On the **Manage Collectors** page, select one or more items which you wish to restart.
3. Click **Restart.**
4. Click **Yes** to confirm restart. The Collectors are restarted.

Deleting Collectors

To delete Collectors:

1. Click **Configuration Management > Bulk Operations**.
2. On the **Manage Collectors** page, select one or more items which you wish to delete.
3. Click **Delete**.
4. Click **Yes** to confirm delete. The items are deleted.

Enabling SecureData Encryption on Managed Connectors

SecureData can be enabled as part of the Instant Connector Deployment process. However, you can also enable SecureData encryption on connectors or containers you already manage in ArcMC.

To enable SecureData encryption on connectors or containers you already manage in ArcMC:

1. Ensure that the remote VM can communicate with the SecureData server. If not, edit the hosts file or configure DNS to enable communication.
2. If there is a certificate for the SecureData server, make sure it is successfully imported to the remote VM.
3. Ensure proxy settings allow the SecureData client to communicate with the SecureData server.
4. Install the SecureData client manually on the remote VM where the connectors reside.
5. Finally, in ArcMC, select the connectors or containers. Perform the Modify Property operation and provide the necessary SecureData and proxy details.

Prerequisites for Addition of SecureData Client to Multiple Containers

The following are prerequisites for the addition of the SecureData client to multiple containers.

- The process should be performed by an account with which the Connector was installed.

  > **Note:** If this user was a non-root user, that user must have access to the directory on the destination host with all permissions.

  The process must have a dedicated port numbered higher than 1024.

  Bulk SecureData client install is supported for accounts using SSH key authentication, but not supported for SSH with passphase authentication. To enable SSH key authentication, the SSH key needs to be set up between a non-root user of ArcMC and a user of the remote host.
- You should consult and review the Format Preserving Encryption Environment Setup Guide for proxy settings.
- All the selected container hosts need to have same SSH credentials (username:password).
- The voltage client install path on all the selected containers hosts must be the same.
- You can only push voltage client in bulk to all the container hosts that are on the same platform e.g. all Linux, or all Windows.
- The below prerequisites are not present by default on RHEL 8.x, unlike in previous RHEL versions (e.g. RHEL 7.x). Perform the following steps for RHEL on the host where the ArcMC is or will be installed, and in the target RHEL host (the VM where the Connector will be deployed):

  a. Install python2:

     For RHEL:
     ```
     sudo yum install -y python2
     ```
     For RHEL:
     ```
     sudo dnf install -y python2
     ```

  b. Create a symlink:

     ```
     sudo ln -s /usr/bin/python2 /usr/bin/python
     ```

  c. Install libselinux-python package:

     For RHEL:
     ```
     sudo yum install -y libselinux-python
     ```
     For RHEL:
     ```
     sudo dnf install -y libselinux-python
     ```

> **Note:** If the `yum/dnf` command fails when installing `libselinux-python` on RHEL, follow the steps below:
> - Download `libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm`
> - Install the package: `rpm -i libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm`

Additional Requirements For Windows Platforms

For Windows platforms, only the local admin account is supported for the bulk-addition of the SecureData client.

In addition, the following preparatory steps are required when deploying on a Windows VM.

1. Enable PowerShell 4.0 or later.

https://www.microsoft.com/en-us/download/details.aspx?id=40855

2. Enable and configure PowerShell Remoting, with CredSSP authentication.

- Download the "ConfigureRemotingForAnsible.ps1" file:
  - https://github.com/ansible/ansible/blob/devel/examples/scripts/ConfigureRemotingForAnsible.ps1
- Open Power Shell as Administrator and run the following command:
  - `ConfigureRemotingForAnsible.ps1 -EnableCredSSP`

3. Enable TLS 1.2.

Adding SecureData to Multiple Containers

You can add the SecureData encryption client to multiple containers at once. The following limitations apply:

- The selected containers must meet all prerequisites for adding SecureData.
- All selected container hosts must have the same user credentials (username and password), and must be the same platform (that is, all Windows or all Linux.)
- The SecureData client installation path on all container hosts will be the same.
- If a certificate is needed, upload the required certificate before proceeding to **Repositories > CA Certs.**

To add SecureData encyption to multiple containers:

1. Click **Configuration Management> Bulk Operations**
2. On the **Container** tab, select the containers to which you wish to add SecureData encryption.
3. Click **Properties**.
4. On the Container Property Update dialog, click **Edit**.
5. in the **Property List** column, click the **Settings** icon, then search for any values with `fpe` in the name. Change or specify values for these properties as follows.

Property	Description
`fpencryption.enabled`	If true, SecureData (Format Preserving) Encryption is enabled. Once enabled, encryption parameters cannot be modified. A fresh installation of the connector will be required to make any changes to encryption parameters.
`fpencryption.host.url`	URL of the SecureData server
`https.proxy.host`	Proxy SecureData server (https)
`https.proxy.port`	Proxy port
`fpencryption.user.identity`	SecureData identity
`fpencryption.shared.secret`	SecureData shared secret
`fpencryption.event.fields`	Comma-separated list of fields to encrypt.
`fpencryption.voltage.installdir`	Absolute path where the SecureData client needs to be installed

6. Select Install SecureData Client.
7. To use SSH key-based authentication to Linux container hosts (only), select **SSH Key.**

> **Note:** SSH key applies to Linux hosts only. If the SSH Key check box is selected for Windows hosts, the update will fail.

8. If needed, from the **SecureData Cert** drop-down, select a previously-uploaded certificate for SecureData.
9. In **Username** and **Password**, specify the common user credentials for all selected container hosts. (Password is not needed if SSH is enabled in Step 7.)
10. Click **Save.**

The SecureData client is pushed to the selected containers, and each one is restarted. To see if the encryption properties were updated successfully, wait on this page. The Job Manager shows the status of client installation on the containers.

Updating Transformation Hub Cluster Details in ArcMC

When you upgrade the Transformation Hub cluster to the latest version, and if you choose to manage the whole cluster with ArcMC, you will need to update the cluster details in ArcMC. Doing this enables you to deploy CTHs on the latest version of the Transformation Hub cluster.

> **Note:** Make sure that the **Cluster Username**, **Cluster Password**, and **Certificate** information, correspond to the upgraded version of the Transformation Hub.

To update Transformation Hub Cluster Details in ArcMC:

1. Click **Configuration Management > Bulk Operations**
2. Click the **Host** tab.
3. Select the Transformation Hub host.
4. Click **Update Cluster Details.**
5. In the **Hostname** field, type the fully qualified name of the TH.
6. In the **Cluster Port** field, type **443**.
7. In the **Cluster Username** field type the TH username.
8. In the **Cluster Password** field type the TH password.
9. SSH to the Transformation Hub and go to: `/opt/arcsight/kubernetes/scripts/`
10. Run the following script to generate the certificate: `cdf-updateRE.sh`
11. Copy the certificate name ca.crt (be sure to include from ----- BEGIN CERT to END CERT -----), navigate to the GUI, paste it on the **Cluster Certificate** field and click **Save.**

Updating Host Credentials

 relies on a host's login credentials to connect and authenticate to the managed host. You specify these credentials when adding the host to for management. If these credentials ever change, the management link between and the host will be broken.

However, you can update the credentials uses to authenticate to a managed host, which will prevent the management link from being broken.

Updating host credentials on does not change the actual credentials on the managed host. You will need to change those on the host directly, either immediately before or immediately after performing this operation. Updating credentials will only update the credentials that uses to authenticate to the host.

To update host credentials:

1. Click **Configuration Management > Bulk Operations**.
2. Click the **Host** tab.
3. Select the host you want to update, click **Update Credentials**.
4. In **Username** and **Password**, enter the new credentials that will use to connect to the host.
5. Click **Save.**

Downloading and Importing Host Certificates

In case of a mismatch between the hostname and the hostname in the SSL certificate, you can download and import the host's current certificates.

To download and import host certificates:

1. Click **Configuration Management > Bulk Operations**.
2. Click the **Hosts** tab.
3. Select the desired host.
4. Click **Download Certificate**.
5. Click **Import** in the wizard and then Click **Done**.

Scanning a Host

Scanning a host will inventory all currently running containers on the host and the connectors associated with them.

To ensure accuracy and currency of container inventory, you will need to manually scan for new containers in any of the following circumstances:

- Additional containers or connectors are added to a remote host after it has been added to ArcMC.
- Containers and connectors are removed from a remote host managed in ArcMC.
- Any containers which were down when the initial, automatic scan was performed have since come back up.
- The license for a managed ArcSight Management Center (managed by another ArcSight Management Center) is upgraded to increase the number of licensed containers.

Any host that includes containers is scanned automatically when first added to ArcSight Management Center.

You can manually scan any host types that can run containers. These types include:

- Connector Appliances
- Loggers (L77XX models only)
- ArcSight Management Center Appliances
- Connectors

The Scan Process

A host scan retrieves information on all CA certificates from any running containers on the host. The containers on the remote host can be managed only if ArcMC can authenticate using the certificates and the credentials. You are prompted to import any retrieved certificates into the ArcMC trust store.

A manual scan will be discontinued if any of the following are true:

- Any containers on a scanned Connector Appliance host are down.
- If you choose *not* to import any certificates that are retrieved.
- Authentication fails on any of the containers.

To manually scan a host:

1. Click **Configuration Management > Bulk Operations**.
2. In the navigation tree, select the location to which the host has been assigned.
3. Click the **Host** tab.
4. Select the host you want to scan, click **Scan Host**. The Host Scan wizard starts.
5. Enter values for the parameters in the following table, and then click **Next**.

Parameter	Description
Starting Port	The port number on the host on which ArcMC starts scanning for containers.
Ending Port	The port number on the host on which ArcMC ends scanning for containers.
Connector Username	The Connector user name to authenticate with the host.
Connector Password	The password for the Connector you provided.

6. Connector certificates are retrieved automatically so that the ArcMC can communicate with each connector in a container. The Host Scan wizard lists the certificates. (To see certificate details, hover over the certificate.)
   - To continue the scan, select **Import the certificates**, and then click **Next** to import the certificates and continue.
   - Otherwise, select **Do not import the certificates,** and then click **Next**. The Host Scan wizard discontinues the scan.

Moving a Host to a Different Location

You can assign one or more hosts to a new location. When you move a host, any nodes associated with it are also moved. For example, if you moved a Connector Appliance to a new location, all of its containers and managed connectors would also be moved to the new location.

To move one or more hosts:

1. Click **Configuration Management > Bulk Operations**.
2. Click the **Hosts** tab.
3. Choose one or more hosts to move.
4. Click **Move**.
5. Follow the prompts in the **Host Move** wizard.The selected hosts are reassigned to their new locations.

Deleting a Host

When you delete a host, any nodes associated with the host are also deleted. Deleting a host removes its entry from ArcSight Management Center, but otherwise leaves the host unaffected.

> **Note:** Use caution when deleting a host. Deleting a host will delete its associated nodes from any node list, association, peers listing, or subscribers listing that includes those nodes.

To delete one or more hosts:

1. Click **Configuration Management > Bulk Operations.**.
2. Choose one or more hosts to delete.
3. Click **Delete**.
4. Click **Yes** to confirm deletion. The host (and any associated nodes) are deleted.

Destination Runtime Parameters

The following table describes configurable destination parameters. The parameters listed in the table are not available for all destinations. The user interface automatically displays the parameters valid for a destination. For step-by-step instructions on updating the runtime parameters of a destination, see "Editing Connector Parameters " on page 862.

Parameter	Description
Batching	Connectors can batch events to increase performance and optimize network bandwidth. When activated, connectors create blocks of events and send them when they either (1) reach a certain size or (2) the time window expires, whichever occurs first. You can also prioritize batches by severity, forcing the connector to send the highest-severity event batches first and the lowest-severity event batches later.
Enable Batching (per event)	Create batches of events of this specified size (5, 10, 20, 50, **100**, 200, 300 events).
Enable Batching (in seconds)	The connector sends the events if this time window expires (1, 5, 10, 15, 30, 60).
Batch By	This is **Time Based** if the connector should send batches as they arrive (the default) or **Severity Based** if the connector should send batches based on severity (batches of Highest Severity events sent first).
Time Correction	The values you set for these fields establish forward and backward time limits, that if exceeded, cause the connector to automatically correct the time reported by the device.
Use Connector Time as Device Time	Override the time the device reports and instead use the time at which the connector received the event. This option assumes that the connector will be more likely to report the correct time. (**No** | Yes)
Enable Device Time Correction (in seconds)	The connector can adjust the time reported by the device `Detect Time`, using this setting. This is useful when a remote device's clock isn't synchronized with the ArcSight Manager. This should be a temporary setting. The recommended way to synchronize clocks between Manager and devices is the NTP protocol. The default is **0**.
Enable Connector Time Correction (in seconds)	The connector can also adjust the time reported by the connector itself, using this setting. This is for informational purposes only and allows you to modify the local time on the connector. This should be a temporary setting. The recommended way to synchronize clocks between Manager and connectors is the NTP protocol. The default is **0**.
Set Device Time Zone To	Ordinarily, it is presumed that the original device is reporting its time zone along with its time. And if not, it is then presumed that the connector is doing so. If this is not true, or the device isn't reporting correctly, you can switch this option from Disabled to GMT or to a particular world time zone. That zone is then applied to the time reported. Default: **Disabled**.
Device Time Auto-correction	
Future Threshold	The connector sends the internal alert if the detect time is greater than the connector time by `Past Threshold` seconds.
Past Threshold	The connector sends the internal alert if the detect time is earlier than the connector time by `Past Threshold` seconds.
Device List	A comma-separated list of the devices to which the thresholds apply. The default, `(ALL)`, means all devices.
Time Checking	These are the time span and frequency factors for doing device-time auto-correction.
Future Threshold	The number of seconds by which to extend the connector's forward threshold for time checking. The default is **5 minutes** (300 seconds).

Parameter	Description
Past Threshold	The number of seconds by which to extend the connector's rear threshold for time checking. Default is **1 hour** (3,600 seconds).
Frequency	The connector checks its future and past thresholds at intervals specified by this number of seconds. Default is **1 minute** (60 seconds).
Cache	Changing these settings will not affect the events cached, it will only affect new events sent to the cache.
Cache Size	Connectors use a compressed disk cache to hold large volumes of events when the ArcSight Manager is down or when the connector receives bursts of events. This parameter specifies the disk space to use. The default is **1 GB** which, depending on the connector, can hold about 15 million events, but it also can go down to **5 MB**. When this disk space is full, the connector drops the oldest events to free up disk cache space. (5 MB, 50 MB, 100 MB, 150 MB, 200 MB, 250 MB, 500 MB, 1 GB, 2.5 GB, 5 GB, 10 GB, 50 GB.)
Notification Threshold	The size of the cache's contents at which to trigger a notification. Default is **10,000**.
Notification Frequency	How often to send notifications after the Notification Threshold is reached. (1 minute, 5 minutes, **10 minutes**, 30 minutes, 60 minutes.)
Network	
Heartbeat Frequency	This setting controls how often the connector sends a heartbeat message to the destination. The default is **10 seconds**, but it can go from **5 seconds** to **10 minutes**. Note that the heartbeat is also used to communicate with the connector; therefore, if its frequency is set to **10 minutes**, then it could take as much as 10 minutes to send any configuration information or commands back to the connector.
Enable Name Resolution	The connector tries to resolve IP addresses to hostnames, and hostnames to IP addresses , if required and if the event rate allows. This setting controls this functionality. The Source, Target and Device IP addresses , and Hostnames might also be affected by this setting. By default, name resolution is enabled (**Yes**).
Name Resolution Host Name Only	Default: **Yes**.
Name Resolution Domain From E-mail	Default: **Yes**.
Clear Host Names Same as IP Addresses	Default: **Yes**.
Limit Bandwidth To	A list of bandwidth options you can use to constrain the connector's output over the network. (**Disabled**, 1 kbit/sec to 100 Mbits/sec.)

Parameter	Description
Transport Mode	You can configure the connector to cache to disk all the processed events it receives. This is equivalent to pausing the connector. However, you can use this setting to delay event-sending during particular time periods. For example, you could use this setting to cache events during the day and send them at night. You can also set the connector to cache all events, except for those marked with a very-high severity, during business hours, and send the rest at night. (**Normal** | Cache | Cache (but send Very High severity events).
Address-based Zone Population Defaults Enabled	This field applies to v3.0 ArcSight Managers. This field is not relevant in ESM v3.5 because the system has integral zone mapping. Default: **Yes**.
Address-based Zone Population	This field applies to v3.0 ArcSight Managers. This field is not relevant in ESM v3.5 because the system has integral zone mapping.
Customer URI	Applies the given customer URI to events emanating from the connector. Provided the customer resource exists, all customer fields are populated on the ArcSight Manager. If this particular connector is reporting data that might apply to more than one customer, you can use Velocity templates in this field to conditionally identify those customers.
Source Zone URI	Shows the URI of the zone associated with the connector's source address. Required for ESM v3.0 compatibility.
Source Translated Zone URI	Shows the URI of the zone associated with the connector's translated source address. The translation is presumed to be NAT. Required for ESM v3.0 compatibility.
Destination Zone URI	Shows the URI of the zone associated with the connector's destination address. Required for ESM v3.0 compatibility.
Destination Translated Zone URI	Shows the URI of the zone associated with the connector's translated destination address. The translation is presumed to be NAT. Required for ESM v3.0 compatibility.
Connector Zone URI	Shows the URI of the zone associated with the connector's address. Required for ESM v3.0 compatibility.
Connector Translated Zone URI	Shows the URI of the zone associated with the connector's translated address. The translation is presumed to be NAT. Required for ESM v3.0 compatibility.
Device Zone URI	Shows the URI of the zone associated with the device's address. Required for ESM v3.0 compatibility.
Device Translated Zone URI	Shows the URI of the zone associated with the device's translated address. The translation is presumed to be NAT. Required for ESM v3.0 compatibility.

Parameter	Description
Field Based Aggregation	This feature is an extension of basic connector aggregation. Basic aggregation aggregates two events if, and only if, all the fields of the two events are the same (the only difference being the detect time). However, field-based aggregation implements a less strict aggregation mechanism; two events are aggregated if only the selected fields are the same for both alerts. It is important to note that field-based aggregation creates a new alert that contains only the fields that were specified, so the rest of the fields are ignored. Connector aggregation significantly reduces the amount of data received, and should be applied only when you use less than the total amount of information the event offers. For example, you could enable field-based aggregation to aggregate “accepts” and “rejects” in a firewall, but you should use it only if you are interested in the count of these events, instead of all the information provided by the firewall.
Time Interval	Select a time interval, if applicable, to use as a basis for aggregating the events the connector collects. It is exclusive of Event Threshold (**disabled**, 1 sec, 5 sec, and so on, up to 1 hour).
Event Threshold	Select a number of events, if applicable, to use as a basis for aggregating the events the connector collects. This is the maximum count of events that can be aggregated; for example, if 150 events were found to be the same within the time interval selected (that is, contained the same selected fields) and you select an event threshold of 100, you then receive two events, one of count 100 and another of count 50. This option is exclusive of Time Interval (**disabled**, 10 events, 50 events, and so on, up to 10,000 events).
Field Names	Specify one or more fields, if applicable, to use as the basis for aggregating the events the connector collects. The result is a comma-separated list of fields to monitor. For example, "eventName,deviceHostName" would aggregate events if they have the same event- and device-hostnames. Names can contain no spaces and the first letter must not be capitalized.
Fields to Sum	Specify one or more fields, if applicable, to use as the basis for aggregating the events the connector collects.
Preserve Common Fields	Choosing Yes adds fields to the aggregated event if they have the same values for each event. Choosing **No**, the default, ignores non-aggregated fields in aggregated events.
Filter Aggregation	Filter Aggregation is a way of capturing aggregated event data from events that would otherwise be discarded due to an agent filter. Only events that would be filtered out are considered for filter aggregation (unlike Field-based aggregation, which looks at all events). Connector aggregation significantly reduces the amount of data received, and should be applied only when you use less than the total amount of information the event offers.
Time Interval	Select a time interval, if applicable, to use as a basis for aggregating the events the connector collects. It is exclusive of Event Threshold (**disabled**, 1 sec, 5 sec, and so on, up to 1 hour).
Event Threshold	Select a number of events, if applicable, to use as a basis for aggregating the events the connector collects. This is the maximum count of events that can be aggregated; for example, if 150 events were found to be the same within the time interval selected (that is, contained the same selected fields) and you select an event threshold of 100, you then receive two events, one of count 100 and another of count 50. This option is exclusive of Time Interval (**disabled**, 10 events, 50 events, and so on, up to 10,000 events).
Fields to Sum	(Optional) Select one or more fields, if applicable, to use as the basis for aggregating the events the connector collects.

Parameter	Description
Processing	
Preserve Raw Event	For some devices, a raw event can be captured as part of the generated alert. If that is not the case, most connectors can also produce a serialized version of the data stream that was parsed/processed to generate the ArcSight event. This feature allows the connector to preserve this serialized "raw event" as a field. This feature is disabled by default since using raw data increases the event size and therefore requires more database storage space. You can enable this by changing the **Preserve Raw Event** setting. The default is **No**. If you choose **Yes**, the serialized representation of the "Raw Event" is sent to the destination and preserved in the Raw Event field.
Turbo Mode	You can accelerate the transfer of a sensor's event information through connectors by choosing one of two “turbo” (narrower data bandwidth) modes. The default transfer mode is called **Complete**, which passes all the data arriving from the device, including any additional data (custom, or vendor-specific). **Complete** mode does indeed use all the database performance advances of ArcSight ESM v3.x. The first level of Turbo acceleration is called **Faster** and drops just additional data, while retaining all other information. The **Fastest** mode eliminates all but a core set of event attributes, in order to achieve the best throughput. The specific event attributes that apply to these modes in your enterprise are defined in the self-documented `$ARCSIGHT_HOME/config/connector/agent.properties` file for the ArcSight Manager. Because these properties might have been adjusted for your needs, you should refer to this file for definitive lists. Only scanner connectors need to run in **Complete** mode, to capture the additional data. **Note**: Connector Turbo Modes are superseded by the Turbo Mode in use by the ArcSight Managers processing their events. For example, a Manager set to **Faster** will not pass all the data possible for a connector that is set for the default of **Complete**.

Parameter	Description
Enable Aggregation (in seconds)	When enabled, aggregates two or more events on the basis of the selected time value (**disabled**, 1, 2, 3, 4, 5, 10, 30, 60). The aggregation is performed on one or more matches for a fixed subset of fields: • Agent ID • Name • Device event category • Agent severity • Destination address • Destination user ID • Destination port • Request URL • Source address • Source user ID • Source port • Destination process name • Transport protocol • Application protocol • Device inbound interface • Device outbound interface • Additional data (if any) • Base event IDs (if any) The aggregated event shows the event count (how many events were aggregated into the displayed event) and event type. The rest of the fields in the aggregated event take the values of the first event in the set of aggregated events.
Limit Event Processing Rate	You can moderate the connector's burden on the CPU by reducing its processing rate. This can also be a means of dealing with the effects of event bursts. The choices range from **Disabled** (no limitation on CPU demand) to **1 eps** (pass just one event per second, making the smallest demand on the CPU). Note: The effect of this option varies with the category of connector in use, as described in the connector Processing Categories table below.
Fields to Obfuscate	
Store Original Time in	**Disabled** or Flex Date 1.
Enable Port-Service Mapping	Default: **No**.
Enable User Name Splitting	Default: **No**.

Parameter	Description
Split File Name into Path and Name	Default: **No**.
Generate Unparsed Events	Default: **No**.
Preserve System Health Events	Yes, **No**, or Disabled.
Enable Device Status Monitoring (in minutes)	**Disabled** or 1, 2, 3, 4, 5, 10, 30, 60, or 120 minutes.
Filters	
Filter Out	NA
“Very High Severity” Event Definition	NA
“High Severity” Event Definition	NA
“Medium Severity” Event Definition	NA
“Low Severity” Event Definition	NA
“Unknown Severity” Event Definition	NA
Payload Sampling	When available.
Max. Length	Discard, 128 bytes, **256 bytes**, 512 bytes, 1 kbyte
Mask Non-Printable Characters	Default: **False**.

Special Connector Configurations

Certain connectors require additional configuration when used with ArcMC. This appendix describes the additional configuration. For general information about installing connectors, see "Adding a Connector" on page 860.

The following topics are discussed here:

System Administration

SMTP (Simple Mail Transfer Protocol) is a standard protocol used for sending and receiving email messages over the internet. In order to use SMTP on ArcMC, it is necessary to configure it properly. This chapter describes the system administration tool that enables you to do this:

- "SMTP" on page 957

SSL Server Certificate

Your system uses Secure Sockets Layer (SSL) technology to communicate securely over an encrypted channel with its clients, such as SmartConnectors, when using the SmartMessaging technology and other ArcSight systems. Your system ships with a self-signed certificate so that an SSL session can be established the first time you use the appliance. For more information on this option, see "Generating a Self-Signed Certificate" below.

Although a self-signed certificate is provided for your use, you should use a certificate authority (CA) signed certificate. To facilitate obtaining a CA-signed certificate, your system can generate a Certificate Signing Request. After a signed certificate file is available from the CA, it can be uploaded to your system for use in a subsequent authentication. For detailed instructions, see "Generating a Certificate Signing Request (CSR)" on page 955.

Your system generates an audit event when the installed SSL certificate is going to expire in less than 30 days or has already expired. The event with Device Event Class ID “`platform:407`” is generated periodically until you replace the certificate with one that is not due to expire within 30 days.

Generating a Self-Signed Certificate

Your system ships with a self-signed certificate so that an SSL session can be established the first time you connect. This type of certificate does not require signing from another entity and can be used immediately.

To generate a self-signed certificate:

1. Click **Administration > Setup > System Admin.**
2. Click **SSL Server Certificate** from the **Security** section in the left panel to display the **Generate Certificate/Certificate Signing Request** page.
3. Click the **Generate Certificate** tab.
4. From the **Generate Certificate For Protocol** field, use the **Network Protocol** drop-down menu to choose the appropriate protocol

Parameter	Description
HTTPS	Choose this option to generate a CSR for use with the HTTPS protocol. This is the most commonly used option.
FTPS	Choose this option only when generating a CSR for use with FTPS.

5. From the **Enter Certificate Settings** field, enter new values for the following fields:

Parameter	Description
Country	ISO 3166-1 two-letter country code, such as 'US' for the United States.
State/Province	State or province name, such as 'California.'
City/Locality	City name, such as 'Sunnyvale'.
Organization Name	Company name, governmental entity, or similar overall organization.
Organizational Unit	Division or department within the organization.
Hostname	The host name or IP address of this system. When specifying the host name, make sure that this name matches the name registered in the Domain Name Service (DNS) server for the system. Additionally, this name must be identical to the host name specified in "NICs" on page 1. **Note:** If the host name or IP address of this system changes in the future, you must generate a new self-signed certificate or CSR. After a new certificate is obtained, you must upload it to ensure that the connectors which communicate with the system are able to validate the host name.
Email Address	The email address of the administrator or contact person for this CSR.
Private Key Length	Private key length is 2048 bits.

6. Use the first two buttons to generate a CSR or a self-signed certificate. The **View Certificate** button is only used to view the resulting certificate.

Button	Description
Generate CSR	Click to generate a Certificate Signing Request (CSR).
Generate Certificate	Click to generate a self-signed certificate.
View Certificate	Click to view the generated certificate.

7. Click the **Generate Certificate** button to generate the self-signed certificate.
8. Click **Ok** after the confirmation message appears.
9. Click the **View Certificate** button to view the PEM encoded self-signed certificate.

Generating a Certificate Signing Request (CSR)

The first step in obtaining a CA-signed certificate is to generate a Certificate Signing Request (CSR). The CSR must be generated on the system for which you are requesting a certificate. That is, you cannot generate a CSR for System A on System B or use a third-party utility for generation.

The resulting CSR must be sent to a CA, such as VeriSign, which responds with a signed certificate file.

To generate a certificate signing request:

1. Click **Administration > System Admin.**
2. Click **SSL Server Certificate** from the **Security** section in the left panel to display the **Generate Certificate/Certificate Signing Request** page.
3. Click the **Generate Certificate** tab.
4. From the **Generate Certificate For Protocol** field, use the **Network Protocol** drop-down menu to choose the appropriate protocol. From the **Generate Certificate For Protocol** field, use the **Network Protocol** drop-down menu to choose the appropriate protocol.

Parameter	Description
HTTPS	Choose this option to generate a CSR for use with the HTTPS protocol. This is the most commonly used option.
FTPS	Choose this option only when generating a CSR for use with FTPS.

5. From the **Enter Certificate Settings** field, enter new values for the following fields:

Parameter	Description
Country	A two-letter country code, such as ‘US’ for the United States.
State / Province	State or province name, such as ‘California.’
City / Locality	City name, such as ‘Sunnyvale’.
Organization Name	Company name, governmental entity, or similar overall organization.
Organizational Unit	Division or department within the organization.

Parameter	Description
Hostname	The host name or IP address of this system. When specifying the host name, make sure that this name matches the name registered in the Domain Name Service (DNS) server for the system. Additionally, this name must be identical to the host name specified in "NICs" on page 1. **Note:** If the host name or IP address of this system changes in the future, you must generate a new self-signed certificate or CSR. After a new certificate is obtained, you must upload it to ensure that the connectors which communicate with the system are able to validate the host name.
Email Address	The email address of the administrator or contact person for this CSR.
Private Key Length	Select the length (in bits) of the private key: **1024**, **2048**, **4096**, or **8192**.

6. Use the first two buttons to generate a CSR or a self-signed certificate. The **View Certificate** button is only used to view the resulting certificate.

Button	Description
Generate CSR	Click to generate a Certificate Signing Request (CSR).
Generate Certificate	Click to generate a self-signed certificate.
View Certificate	Click to view the generated certificate.

7. Choose **Generate CSR** to generate a certificate signing request.
8. If the CSR was successfully generated, a pop-up window appears, allowing you to either download the CSR file or to cut-and-paste its content.

   To do so, copy all the lines from `-----BEGIN CERTIFICATE REQUEST-----` to `-----END CERTIFICATE REQUEST-----`.
9. Send the CSR file to your certificate authority to obtain the CA-signed certificate.
10. After the CA-signed certificate file is obtained, continue on to "Importing a Certificate" below.

Importing a Certificate

If you have obtained a certificate from your certificate authority (CA), follow the steps below to import it onto your system.

1. Click **Administration > System Admin.**
2. Click **SSL Server Certificate** under the **Security** section in the left panel.
3. Select the **Import Certificate** tab.
4. From the **Import Certificate For Protocol** field, use the **Network Protocol** drop-down menu to select the appropriate protocol type.

Parameter	Description
HTTPS	Choose to import an HTTPS certificate. (This option may require a reboot).
FTPS	Choose to import an FTPS certificate.

5. Click the **Browse** button to locate the signed certificate file on your local file system.

   Note: The imported certificate must be in **Privacy Enhanced Mail (PEM)** format.

6. Click **Import and Install** to import the specified certificate.
7. If using **HTTPS** and depending on your browser, you may need to close and restart the browser for the new certificate to take effect. If you are unsure of your browser's requirements, close and restart it.

SMTP

Your system uses the Simple Mail Transfer Protocol (SMTP) setting to send email notifications such as alerts and password reset emails.

To add or change SMTP settings:

1. Click **Administration > Setup > System Admin.**
2. Click **SMTP** in the **System** section and specify these settings.

Setting	Description
Enable SMTP Auth Mode	Enable/Disable secure authenticated mode of communication with SMTP server.
Primary SMTP Server	Mandatory. The IP address or hostname of the SMTP server that will process outgoing email.
Primary SMTP Server Port	Primary SMTP Server Port. Required if SMTP Auth Mode is enabled.
Username	Primary SMTP Server Username. Required if SMTP Auth Mode is enabled.
Password	Primary SMTP Server Password. Required if SMTP Auth Mode is enabled.
Upload Cert File SMTP Primary	Upload Primary SMTP Server Certificate. Required if SMTP Auth Mode is enabled.
Backup SMTP Server	Mandatory. The IP address or hostname of the SMTP server that will process outgoing email in case the primary SMTP server is unavailable.
Ba ckup SMTP Server Port	Secondary SMTP Server Port. Required if SMTP Auth Mode is enabled.
Username	Secondary SMTP Server Username. Required if SMTP Auth Mode is enabled.

Setting	Description
Password	Secondary SMTP Server Password. Required if SMTP Auth Mode is enabled.
Upload Cert File SMTP Backup	Upload secondary SMTP Server Certificate. Required if SMTP Auth Mode is enabled.
Outgoing Email Address	The email address that will appear in the From: field of outbound email.

3. Click **Save**.

   For more information on SMTP Configuration, see Connecting to Your SMTP Server.

Troubleshooting Your Cluster

The following troubleshooting tips may be helpful in resolving issues with the OMT cluster.

Issue	Description
Installation of master nodes fails	During installation, installation of Master Nodes can fail with the error: `Unable to connect to the server: context deadline exceeded` Ensure that your `no_proxy` and `NO_PROXY` variables include valid virtual IP addresses and hostnames for each of the master and worker nodes in the cluster, as well as the NFS server.
Installation times out	During installation, the process may time out with the error: `Configure and start ETCD database` Ensure your `no_proxy` and `NO_PROXY` variables include correct Master Node information.
During sudo installation, worker node fails to install	During the Add Node phase, if one or more of the worker nodes fails to install and the log shows the following error message: `[ERROR] : GET Url: https://itom-vault.core:8200/v1/***/PRIVATE_KEY_CONTENT_{hostname}_{sudo user}, ResponseStatusCode: 404` You can take the following steps to rectify the issue: 1. Click **Cancel** to return to the version selection screen. 2. Proceed through the installation screens again (all previous data is preserved). 3. On the **Add Node** screen, where you added the Worker Node data, remove the worker node which failed by clicking on the **Delete** icon. 4. Click **Add Node** and add the node again. 5. Click **Next** and proceed with the installation.

Issue	Description
Worker nodes out of disk space and pods evicted	If the worker nodes run out of disk space, causing the pods on the node to go into Evicted status, try one of the following steps: • Fix the disk space issue by adding an additional drive or contact OpenText support to receive help remove unnecessary files. • On the node where the low disk space occurred, run the following command: `{install dir} /kubernetes/bin/kube-restart.sh` For information on adjusting the eviction threshold, see "Updating the OMT Hard Eviction Policy."

Kafka fails to start up; fails to acquire lock or corrupted index file found	Many scenarios can cause a failure for Kafka to start up and report either `Failed to acquire lock` or `Corrupted index file found.`
	Workaround: To resolve this on the problematic Kafka node:.
	1. Go to the directory:
	`cd /opt/arcsight/k8s-hostpath-volume/th/kafka/`
	2. Find the file `.lock`, and delete it.
	3. Search for all index files:
	`find . -name "*.index" | xargs ls -altr`
	4. Delete all the corrupted index files
	5. Restart the affected Kafka pod.

ArcSight database rejects new sessions because the maximum sessions limit is reached	You might observe the following error in the logs: [Vertica][VJDBC](4060) FATAL: New session rejected due to limit, already 125 sessions active **Workaround:** Do one of the following: • Delete the active open sessions to ensure that the total number of active sessions is within the specified maximum limit. • Refer to the ArcSight Database documentation to **configure the maximum sessions** in the ArcSight Database 24.1 Guide.
ArcSight Dat abase fails to restart	If the database fails to start, you can run a set of commands to recover the last known good set of data and restart the database. For example, the database might not restart after an unexpected shutdown. Please consult your database administrator for the commands to run.

Issue	Description

Multiple node failures	Here are some considerations when handling node failures on 3 or more worker nodes.
	• A cluster with 3 masters and 3 or more worker nodes should have at least 2 or more master and worker nodes running (quorum) to work properly in high availability.
	• As a general rule in terms of data loss prevention, no more than `TOPIC_REPLICATION_FACTOR` minus 1 worker nodes can be down at any time
	• Handling failures and stability if Worker nodes go down:
	  ◦ Resume the stability of the cluster as follows:
	  • Repair or replace any down worker nodes or replace with new ones
	  • Delete any pods which are in “Terminating” state (this is the expected behavior for stateful pods in Kubernetes when nodes are down).
	  ◦ Wait until the pod startup sequence is completed. The cluster should resume normal operation.
	  ◦ Repair any issues on the lost nodes, the cluster should return to Running state

Second upgrade fails or some resources aren't really upgraded after it	In some cases, a second upgrade may fail completely or fail to upgrade resources. If this is encountered, run the following command: `kubectl delete deployment suite-upgrade-pod-arcsight-installer -n `kubectl get namespaces | grep arcsight-installer | awk '{print $1}'` Wait until the suite-upgrade-pod-arcsight-installer is deleted, then begin the second upgrade again.
OMT deployment fails on servers running VMWare V Motion	Installation of OMT may fail on virtual machines running the VMWare product VMotion. If this occurs, run the installation of OMT again but disable VMotion on all OMT virtual machines.
New partition source topics not correctly displayed in Kafka Manager	Changes to the partition source topics in Kafka Manager may take up to 5 minutes to refresh and display correctly.
Certificate Warnings in Logstash Logs	When you view the Logstash logs, you might come across the following warnings: ** WARNING ** Detected UNSAFE options in elasticsearch output configuration!** WARNING ** You have enabled encryption but disabled certificate verification.** WARNING ** To make sure your data is secure change :ssl_certificate_vertification to true. **Workaround**: There is no workaround needed. You can ignore these warnings as there is no impact in the functionality.

Troubleshooting Issues with Your Product License

This section provides guidance on issues that you might encounter related to your product license.

- "System Fails to Recognize a License Change" below
- "Conflicting Indicators about Your License" below
- "Erroneous Warning about Recon License" on the next page

System Fails to Recognize a License Change

When you install or update a license, some components might not recognize the update because of cached data. You should to wait an hour to ensure that the update propagates across the system.

Conflicting Indicators about Your License

It's possible Autopass indicates that your license is valid but the product behaves as if the the license has expired or the pods fail to work. To check the status of a license, you can run the following command:

```
cat /opt/arcsight/k8s-hostpath-volume/<product>/autopass/license.log
```

For example, for Transformation Hub, run:

```
cat /opt/arcsight/k8s-hostpath-volume/th/autopass/license.log
```

The system responds with the following messages:

License status	Message
Valid license	`<product> licensed capacity: <eps number>`
Not installed	`ERROR: No valid license key was found. Please install a valid license key or contact OpenText Customer Support for instructions on how to get one`
Expired	`"<errorMessage>No license is found in Memory ..."`

Erroneous Warning about Recon License

In an ArcSight Platform deployment that has Intelligence with an MSSP license, you will receive the usual notifications that the licenses are about to expire. However, if the MSSP license expires, the Platform erroneously displays a warning that the Recon license has expired even though Recon is not deployed. This issue does not occur when Recon is deployed, with or without the MSSP license.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Administrator's Guide for the ArcSight Platform (AWS) (24.2)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to documentation-feedback@microfocus.com.

We appreciate your feedback!