opentext™

ArcSight SmartConnectors

Software Version: CE 24.2

Configuration Guide Microsoft Azure Monitor Event Hub Connector

Document Release Date: April 2024
Software Release Date: April 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

Trademark Notices

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

Configuration Guide for Microsoft Azure Monitor Event Hub SmartConnector

The Microsoft Azure Monitor Event Hub SmartConnector is a Cloud-native connector that is deployed on the cloud environment.

Microsoft Azure Monitor Event Hub helps you monitor the activities on Microsoft Azure Cloud services.

This connector collects events and logs from Azure Active Directory and Azure Monitor, normalizes the events to Common Event Format (CEF), and then sends the them to either ArcSight Syslog NG Daemon SmartConnector or to ArcSight Load Balancer. The events that are sent to ArcSight Load Balancer, are consequently sent to the Syslog NG Daemon SmartConnector.

Important:

The Microsoft Azure Monitor Event Hub connector has been replaced by the Microsoft Azure Event Hub SmartConnector.

The **Microsoft Azure Monitor Event Hub connector will not be shipped after April 2025**. Therefore, it is highly recommended to switch to the Microsoft Azure Event Hub SmartConnector before April 2025.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- Technical Requirements Guide for SmartConnector, which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- Installation and User Guide for SmartConnectors, which provides detailed information about installing SmartConnectors.
- Configuration Guides for ArcSight SmartConnectors, which provides information about configuring SmartConnectors to collect events from different sources.
- Configuration Guide for SmartConnector Load Balancer, which provides detailed information about installing Load Balancer.

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

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 MFI-Documentation-Feedback@opentext.com.

For specific product issues, contact Open Text Support for Micro Focus products.

Product Overview

Microsoft Azure is an ever-expanding set of cloud services to help your organization meet your business challenges. It is the freedom to build, manage, and deploy applications on a massive, global network using your favorite tools and frameworks.

Azure Event Logs

The Azure Monitor Event Hub connector collects the following event logs from Active Directory, Azure Monitor, and Microsoft Defender for Cloud in Azure:

- **Active Directory Logs**
  - **Audit logs**: Provides records of system activities for compliance.
  - **Sign-in logs:** Provides information related to user logins.

  > **Note:** To export Active Directory sign-in logs, you must have one of P1 or P2 premium editions of Azure Active Directory.

- **Activity Logs**: Provides data related to write operations, such as CREATE, UPDATE, and DELETE that were performed on resources in your subscription. For more information, see Azure Activity log.
- **Resource Log (formerly known as Diagnostic Log)**: Provides data related to operations performed within an Azure resource (the data plane). Example: Getting a secret from a key vault or making a request to a database. The content of resource log varies by the Azure service and resource type.
- **Microsoft Defender for Cloud**
  - **Security alerts**: Provides data related to security actions performed on Microsoft Defender for Cloud in your subscription.
  - **Recommendation logs**: Provides data related to prevention recommendations provided for the resources in your subscription.

Azure event logs such as activity log and resource log are emitted in JSON format. The Azure Monitor Event Hub connector collects these event logs, converts these to CEF using mapping files, and sends these to Syslog NG Daemon SmartConnector or Load Balancer. Every JSON field is mapped to the appropriate CEF key. Each event log type has various categories and each log category has its own schema. Azure logs have schema for various log categories. With the help of these logs schema, the source fields (in JSON) are mapped to appropriate CEF keys.

The Azure Monitor Event Hub connector currently includes mapping files for several log categories of activity, audit, sign-in, and resource log. The Azure documents do not have the schemas for a few categories. Therefore, the mappings for these categories are not available in

the connector. Such events are sent unparsed to the Syslog NG Daemon SmartConnector or to the Load Balancer, and then forwarded to the ArcSight destination.

Related Azure Services

The following services are used when working with Azure Monitor Event Hub connector:

- **Azure Resource Manager**: Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure subscription. You use management features, such as access control, locks, and tags, to secure and organize your resources after deployment. For more information, see Azure Resource Manager.
- **Azure App Service plan**: In App Service, an app runs in an App Service plan. An App Service plan defines a set of compute resources for a web app to run. These compute resources are analogous to the server farm in conventional web hosting. One or more apps can be configured to run on the same computing resources (or in the same App Service plan). For more information, see Azure App Service Plan Overview.
- **Azure Functions**: Azure Functions allows you to run small pieces of code (called "functions") without worrying about application infrastructure. With Azure Functions, the cloud infrastructure provides all the up-to-date servers you need to keep your application running at scale. For more information ,see An introduction to Azure Functions.
- **Storage account**: An Azure storage account contains all of your Azure Storage data objects: blobs, files, queues, tables, and disks. The storage account provides a unique namespace for your Azure Storage data that is accessible from anywhere in the world over HTTP or HTTPS. Data in your Azure storage account is durable and highly available, secure, and massively scalable. For more information, see Storage Account Overview.
- **Azure Event Hubs**: Azure Event Hubs is a big data streaming platform and event ingestion service. It can receive and process millions of events per second. Data sent to an event hub can be transformed and stored by using any real-time analytics provider or batching/storage adapters. For more information, see Azure Event Hubs — A big data streaming platform and event ingestion service.

Azure Event Log Categories

Following tables list the categories for mappings supported by the Azure connector. The mappings are done using the schemas provided in the Azure documents.

Active Directory Log Categories

Categories	Certified
Signin	Yes
Audit	Yes

Activity Log Categories

Categories	Certified	Comments
Administrative	Yes	These are the sub-categories: 1. Action 2. Write 3. Delete For more information, see Azure Activity Log event schema .
Alert	Yes	Azure alerts.
Recommendation	Yes	Recommendation events from Azure Advisor.
Security	No	Same as Microsoft Defender for Cloud log events for Security Alert activity without remediation steps.
ServiceHealth	Yes	Service Health incidents occurred in Azure.

Resource Log Categories

Categories	Resource Type
GatewayLogs	Microsoft.ApiManagement/service
JobLogs	Microsoft.Automation/automationAccounts JobStreams
JobStreams	Microsoft.Automation/automationAccount
CoreAnalytics	Microsoft.Cdn/profiles/endpoints
PipelineRuns	Microsoft.DataFactory/factories
TriggerRuns	Microsoft.DataFactory/factories
Audit	Microsoft.DataLakeAnalytics/accounts
Requests	Microsoft.DataLakeAnalytics/accounts

Categories	Resource Type
Audit	Microsoft.DataLakeStore/accounts
Requests	Microsoft.DataLakeStore/accounts
Connections	Microsoft.Devices/IotHubs
DeviceTelemetry	Microsoft.Devices/IotHubs
C2DCommands	Microsoft.Devices/IotHubs
DeviceIdentityOperations	Microsoft.Devices/IotHubs
FileUploadOperations	Microsoft.Devices/IotHubs
Routes	Microsoft.Devices/IotHubs
D2CTwinOperations	Microsoft.Devices/IotHubs
C2DTwinOperations	Microsoft.Devices/IotHubs
TwinQueries	Microsoft.Devices/IotHubs
JobsOperations	Microsoft.Devices/IotHubs
DirectMethods	Microsoft.Devices/IotHubs
DataPlaneRequests	Microsoft.DocumentDB/databaseAccounts
ArchiveLogs	Microsoft.EventHub/namespaces
OperationalLogs	Microsoft.EventHub/namespaces
AuditEvent	Microsoft.KeyVault/vaults
WorkflowRuntime	Microsoft.Logic/workflows
NetworkSecurityGroupEvent	Microsoft.Network/networksecuritygroups
NetworkSecurityGroupRuleCounter	Microsoft.Network/networksecuritygroups
LoadBalancerAlertEvent	Microsoft.Network/loadBalancers
LoadBalancerProbeHealthStatus	Microsoft.Network/loadBalancers
ApplicationGatewayAccessLog	Microsoft.Network/applicationGateways
ApplicationGatewayPerformanceLog	Microsoft.Network/applicationGateways
ApplicationGatewayFirewallLog	Microsoft.Network/applicationGateways
OperationalLogs	Microsoft.ServiceBus/namespaces
QueryStoreRuntimeStatistics	Microsoft.Sql/servers/databases
QueryStoreWaitStatistics	Microsoft.Sql/servers/databases
Errors	Microsoft.Sql/servers/databases
DatabaseWaitStatistics	Microsoft.Sql/servers/databases
Timeouts	Microsoft.Sql/servers/databases

Categories	Resource Type
Blocks	Microsoft.Sql/servers/databases
Audit	Microsoft.Sql/servers/databases
Execution	Microsoft.StreamAnalytics/streamingjobs
Authoring	Microsoft.StreamAnalytics/streamingjobs
AzureFirewallApplicationRule	Microsoft.Network/AzureFirewalls
AzureFirewallNetworkRule	Microsoft.Network/AzureFirewalls
ServiceLog	Microsoft.Batch/batchAccounts
SQLSecurityAuditEvents	Microsoft.Sql/servers/databases
SQLSecurityAuditEvents	Microsoft.Synapse/workspaces
AutomaticTuning	Microsoft.Sql/servers/databases
Deadlocks	Microsoft.Sql/servers/databases
ActivityRuns	Microsoft.DataFactory/factories
AzureBackupReport	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryEvents	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryJobs	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryProtectedDiskDataChurn	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryRecoveryPoints	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryReplicatedItems	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryReplicationDataUploadRate	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryReplicationStats	Microsoft.RecoveryServices/Vaults
DscNodeStatus	Microsoft.Automation/automationAccounts
Engine	Microsoft.PowerBI
Engine	Microsoft.AnalysisServices/servers
GatewayDiagnosticLog	microsoft.network/p2svpngateways
GatewayDiagnosticLog	microsoft.network/virtualnetworkgateways
GatewayDiagnosticLog	microsoft.network/vpngateways
IkeDiagnosticLog	microsoft.network/p2svpngateways
IkeDiagnosticLog	microsoft.network/virtualnetworkgateways
IkeDiagnosticLog	microsoft.network/vpngateways
Operationlogs	microsoft.loadtestservice/loadtests
Operationlogs	Microsoft.Search/searchServices

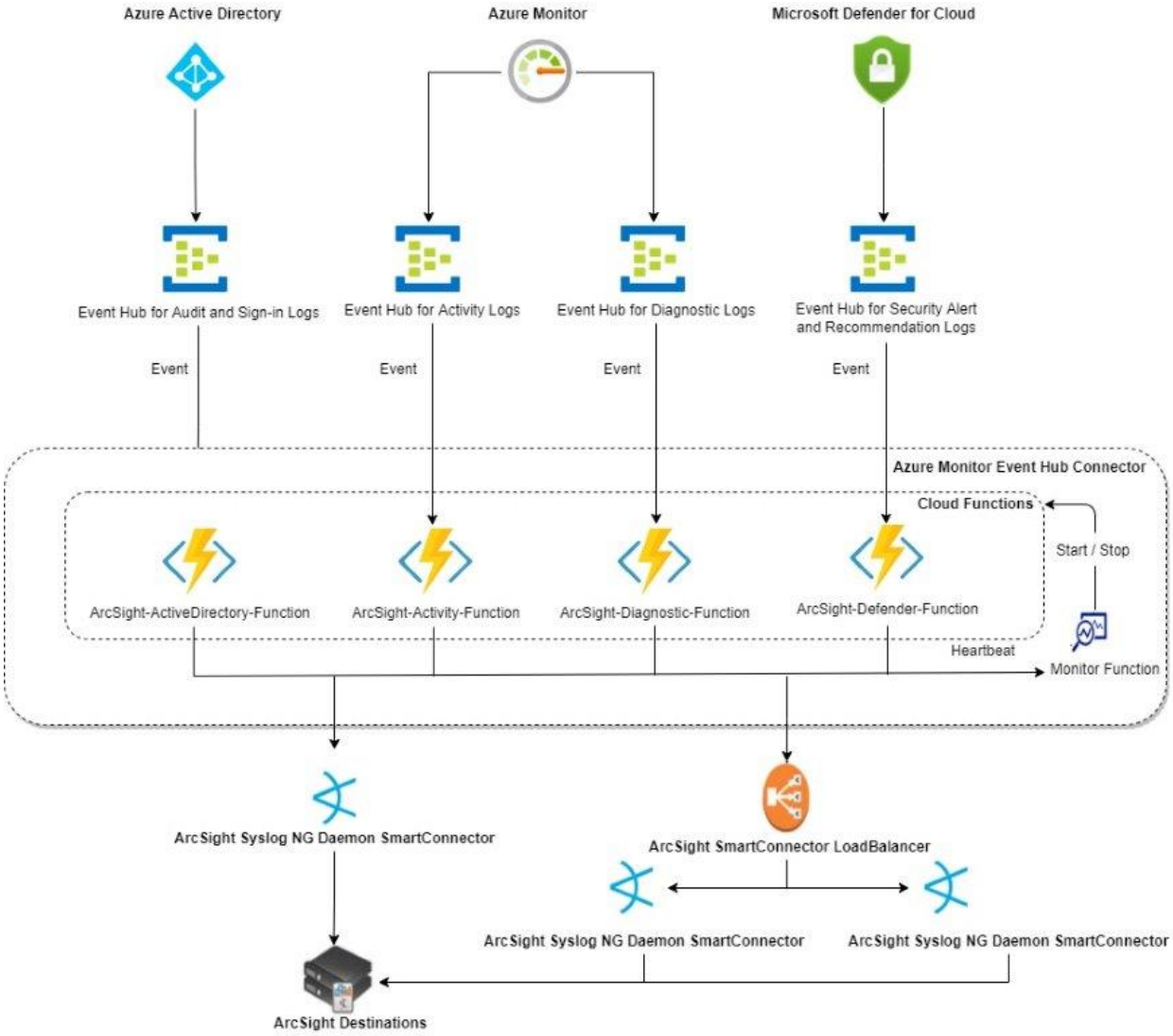
Categories	Resource Type
P2Sdiagnosticlog	microsoft.network/virtualnetworkgateways
P2Sdiagnosticlog	microsoft.network/p2svpngateways
Routediagnosticlog	microsoft.network/virtualnetworkgateways
Routediagnosticlog	microsoft.network/vpngateways
OperationalLogs	Microsoft.NotificationHubs/namespaces
OperationalLogs	Microsoft.ServiceBus/Namespaces
PostGreSQLLogs	Microsoft.DBforPostgreSQL

Microsoft Defender for Cloud Log Categories

Categories	Resource Type	Certified
Securityalerts	All resources	Yes
SecurityRecommendations	All resources	Yes

Understanding Data Collection

The following diagram provides a high-level overview of how the Azure Monitor Event Hub connector collects and sends data to ArcSight's destinations.



Understanding the process flow of data collection

1. After installing, the Azure Monitor Event Hub connector creates event hubs for Active Directory, Azure Monitor, and Microsoft Defender for Cloud.
2. The Azure Monitor Event Hub connector then automatically configures the supported log types to be forwarded to the following event hubs: Active Directory, Activity, Resource, and Microsoft Defender for Cloud. To configure Microsoft Defender for Cloud, see Streaming Logs.
3. The ArcSight Azure Event Processor collects logs in JSON format and then converts these to CEF format.

4. The ArcSight Azure Event Processor then forwards these CEF events to the Syslog NG Daemon SmartConnector or Load Balancer through a secured communication channel using TLS 1.2.
5. The Azure Monitor Event Hub connector establishes a TLS 1.2 connection by accepting a server certificate from the Syslog NG Daemon SmartConnector or ArcSight Load Balancer.
6. The Monitor App continuously monitors the heartbeat of the Syslog NG Daemon SmartConnector or Load Balancer to ensure that it is up and running to receive events. If the Syslog NG Daemon SmartConnector or Load Balancer is down due to an unexpected shutdown of the machine or network issues, this connector stops further processing of events from the event hub. The unprocessed events are sent back to the event hub to avoid data loss. After the Syslog NG Daemon SmartConnector or Load Balancer comes up, the Azure Monitor Event Hub connector continues to send the events to the Syslog NG Daemon SmartConnector. However, the Monitor App will not monitor Syslog NG Daemon SmartConnector connected to the Load Balancer.
7. The Syslog NG Daemon SmartConnector then sends the events to the ArcSight destination.

Preparing to Deploy the Connector

Before you begin deploying the Azure Monitor Event Hub connector, make sure that the following prerequisite tasks are completed:

Setting up VM or System for Deployment

To set up the VM or system for installation, make sure that you have the following prerequisites and prepare the system for deployment:

Prerequisites

Deploying or undeploying the Azure Monitor Event Hub connector can be performed from any on-prem or any cloud hosted virtual machine. Following are the supported environments:

- **Operating System**: Microsoft Windows Server 2012 , 2016, and 2019 (in the cloud with Azure)
- **PowerShell**: 5.0 or higher. Ensure that Windows Powershell is enabled to run scripts on the machine where you want to deploy the connector. For more information see, "Enabling Windows Powershell to Run the Script" on the next page.
- **Az Module**: 6.5.0
- **Az.Resources**: 4.4.0

Note: If a higher version of AZ module is installed, you must downgrade it to 6.5.0 for the installation script to work. For more information see, "Verifying Version of Az Module and Az.Resources" on the next page.

Preparing System for Deployment

This section includes the following information:

Enabling Windows Powershell to Run the Script

PowerShell scripts are now signed in Azure Event Hub SmartConnectors. This allows users to run them in security-enabled environments with an execution policy set to either **RemoteSigned** or **AllSigned**. For more information, see PowerShell Execution Policies. However, signed scripts can still run in unrestricted environments.

To deploy the Azure Monitor Event Hub connector, you must run a script in Windows PowerShell. You must enable the Windows Powershell to run scripts on the machine where you want to deploy the Azure Monitor Event Hub connector.

Note: This procedure needs to be done only once on the machine.

To enable Windows PowerShell to run scripts:

1. Upgrade the Windows PowerShell version to 5.0 or later.
2. Click Start and search for Windows PowerShell. Right-click Windows PowerShell and click **Run as administrator**.
3. Check the current script execution policy:

   `Get-ExecutionPolicy`
4. If the current script execution policy is Restricted, change the script execution policy to one of the following options:
   - `Set-ExecutionPolicy AllSigned`
     a. Enter `Yes to All` when prompted.
     b. Run the `Get-ExecutionPolicy` command to ensure that PowerShell is now `AllSigned`.
     c. Enter `Run Once` or `Always Run` when prompted to trust the publisher while running the script.
   - `Set-ExecutionPolicy RemoteSigned`

a. Enter `Yes to All` when prompted.

b. Run the `Get-ExecutionPolicy` command to ensure that PowerShell is now `RemoteSigned`.

- `Set-ExecutionPolicy unrestricted`

a. Enter `Yes to All` when prompted.

b. Run the `Get-ExecutionPolicy` command to ensure that PowerShell is now `Unrestricted`.

Verifying Version of Az Module and Az.Resources

1. Run the `Get-InstalledModule` command to ensure that "Az" version is 6.5.0 and "Az.Resources" version is 4.4.0.

   If the `Get-InstalledModule` command does not show any results, skip to step 1.b.

   If you have the latest version of "Az" (such as 7.2.0), then perform the following steps to uninstall the current version and reinstall the required version:

   a. Run the following commands to uninstall the higher version of Az:

   ```
   $Modules += (Get-Module -ListAvailable Az.*).Name
   Foreach ($Module in ($Modules | Get-Unique))
   {
   Write-Output ("Uninstalling: $Module")
   Uninstall-Module $Module -Force
   }
   Uninstall-Module Az -Force
   ```

   b. After the product is uninstalled, run the following command to install the supported version: `Install-Module Az -RequiredVersion 6.5.0`

   > **Note:** If you have a slow internet connection, the following might occur:
   >
   > - The download progress might not be displayed while the libraries are downloading and installing the Az module. However, the download is in progress.
   > - The download and installation of the Az module might take up to 40 minutes.

2. Restart your machine.

   > **Note**: If you encounter any issue during the Az module uninstall, then close all the PowerShell windows and try again.

Setting up Azure Environment

Complete the following procedures to set up an Azure environment:

Supported Azure Plans

- **Azure Datacentres with Stamps (Scale Units) with Premium V2 VMs**:

  Only applications running on stamps that support Premium V2 scale units, possess the hardware required to use the VNet Integration (preview) feature.

- **AppService Plan with Basic Pricing Tier Created on a Stamp with Premium V2 VMs**:

  Microsoft Azure Monitor Event Hub Connector requires an AppService plan with basic pricing tier. However, you must ensure that your AppService plan is created in a stamp that supports VNet Integration. VNET integration feature configuration requires a premium V2VM

  It is possible that you have an existing AppService plan that was created in a stamp that does support Premium V2 even for a basic plan and it allows you to use the VNet Integration feature.

  Workaround:

  If you are on a basic plan and are unable to create VNet integration, try the following:

  - You can temporarily upgrade the plan to complete the VNet configuration. After the VNet configuration completes, you scale back to the basic plan to use the VNet Feature.
  - If your AppService plan does not show the feature to scale up to Premium V2, you might not be able to create a new AppService plan in the same Resource Group of the Premium V2 pricing Tier. This happens because the Resource Group sometimes, decides on a particular stamp and creates all resources in there. If you experience this issue, try creating the AppService plan in a different Resource Group.

  Next Step: Setting User Permissions in Azure

Setting User Permissions in Azure

In Azure, users must be associated with a subscription to provide them with access to resources such as virtual machine, storage account, virtual network, and so on. Therefore, you must determine the subscription you want to use for the Azure Monitor Event Hub connector and add users to the required subscription. You must also assign users to a role to define their permission to perform tasks.

Permission Requirements

- **To deploy or upgrade**:

Scope	Description
Azure Active Directory	The users must have the **Application Administrator** and **Security Administrator** roles on the Azure Active Directory.
Resource Group	The users must create a resource group. The users must ensure that they are assigned the **Owner** role on the resource group before deploying both Azure Monitor Function and Cloud Function applications. **Note:** ◦ The users must have the **Owner** role assigned on the resource group so that they can assign the **Contributor** role for the Azure Monitor Function application over the resource group during deployment. ◦ The Azure Monitor Function application requires the **Contributor** role on the resource group to start or stop the Cloud Function application.

- **To run and monitor**: The users must have at least a **Contributor IAM** role on the subscription.

> **Note:** The default value for **identifierUri** is `nsl-test.xyz` in `app.properties`. Ensure that you update with verified domain URI.

Next Step: Installing the Syslog NG Daemon SmartConnector

Installing the Syslog NG Daemon SmartConnector

Because Microsoft Azure Monitor Event Hub is a Cloud-native Connector, you must install the Syslog NG Daemon SmartConnector with TLS protocol to receive events from the Microsoft Azure Monitor Event Hub Connector. For more information, see Installing the Syslog NG Daemon SmartConnector.

Next Step: Opening Ports

Opening Ports

You must ensure that the ports on the server on which you installed the Syslog NG Daemon SmartConnector is accessible from Azure.

Opening Ports on a Non-Virtual Machine

If you installed the Syslog NG Daemon SmartConnector on a physical, non-virtual machine, ensure that the ports on which you installed it are accessible to Azure.

Opening Ports on a Virtual Machine

If you have installed the Syslog NG Daemon SmartConnector on a virtual machine in Azure cloud, ensure that the ports on which you installed Syslog NG Daemon SmartConnector are open in both Azure and the virtual machine.

To open inbound ports on Azure:

1. Log in to Microsoft Azure as a user with administrator privileges.
2. Click **Virtual Machines** > **Virtual machine name** > **Networking** > **Add inbound port**.
3. Enter the same port or port range on which you installed the Syslog NG Daemon SmartConnector.
4. Update other fields and click **Add**.

To open ports in the virtual server:

1. Log in to the virtual Microsoft Windows Server machine.
2. Open Microsoft Windows Server Firewall.
3. Click **Inbound Rules** > **New Rule** > **Port** > **Next** > **TCP** > **Specific local ports**.
4. Enter the same port or port range on which you installed the Syslog NG Daemon SmartConnector.
5. Click **Next** > **Allow the connection** > **Next**> **Profile** > **Next**.
6. Name the rule and click **Finish**.

(Optional) Opening Port to Enable On-premises Connectivity

To connect from an on-premises network to an Azure Virtual Network (VNet), create an incoming port to allow the TCP port number (the default port is 1999) or a range of IP's between 0 and x.

From 00.000.0.000/00 (Azure cloud) to xx.xxx.xxx.xxx (on-premises Arcsight's Syslog SmartConnector).

Next Step: (Optional) Configuring Load Balancer

(Optional) Configuring Load Balancer

In environments where the event load is more than what can be handled by a single Syslog NG Daemon SmartConnector, you can configure Load Balancer to handle large event loads. For more information about configuring Load Balancer, see ArcSight SmartConnector Load Balancer documentation.

Deploying the Connector

This section provides information about deploying the Azure Monitor Event Hub connector to collect and forward events from Azure Cloud Services to the Syslog NG Daemon SmartConnector or Load Balancer, and then the events can be sent to an ArcSight destination.

Complete the following procedures to deploy the Azure Monitor Event Hub connector:

1. "Deploying the Connector in Azure Cloud" below
2. "Updating Keystore Certificate" on page 23
3. "Streaming Logs" on page 24
4. "Configuring Function Apps to Stay Connected" on page 26
5. "Verifying the Deployment in Azure" on page 26

Deploying the Connector in Azure Cloud

Deploying the Azure Monitor Event Hub connector will automatically deploy and configure the required components in your Azure Cloud.

When you deploy the Azure Monitor Event Hub connector against a subscription, you can monitor the events emitted from the services registered to the subscription. If you have multiple subscriptions and you want to monitor the services under all your subscriptions, you must deploy this connector against each of the subscriptions separately. The Azure Monitor Event Hub connector gets deployed directly into the Azure cloud and you do not need to set up a virtual machine in the cloud to deploy the connector.

To deploy the Azure Monitor Event Hub connector:

1. On the machine from where you want to deploy the connector, download the `arcsight-azure-monitor-eventhub-connector-x.x.x.zip`.
2. Extract the `arcsight-azure-monitor-eventhub-connector-x.x.x.zip` files to the desired location.
3. Edit the **app.properties** file.

a. Configure the following application properties of this connector:

Properties	Description
resourceGroupName	Modify the name of the resourceGroupName property. The default value is **arcsight-functions-group**.
FunctionAppName1	Modify the name of the Function App. Function Apps must not contain the period symbol. The default value is **arcsight-cloudfunctions**
FunctionAppName2	Modify the name of the Function App. Function Apps must not contain the period symbol. The default value is **arcsight-monitor-functions**
connectorhostname	Specify the IP address of the Syslog NG Daemon SmartConnector or Load Balancer. The default value is **0.0.0.0**.
connectorport	Specify the port number of the Syslog NG Daemon SmartConnector or Load Balancer. The default value is **1999**.
keyStoreFileName	Specify the keystore file name of the Syslog NG Daemon SmartConnector or Load Balancer. The **`keyStoreFileName`** property is used by the event hub connector application running on Azure to establish a TLS connection over SSL with the client Syslog NG Daemon SmartConnector.
keyStorePassword	Specify the keystore password of the Syslog NG Daemon SmartConnector or Load Balancer The **`keyStorePassword`** property is used by the event hub connector application running on Azure to establish a TLS connection over SSL with the client Syslog NG Daemon SmartConnector.
storageaccountname	Specify a unique storageaccountname. Storage account names must be between 3 and 24 characters in length and might contain numbers and lowercase letters only.
Eventhubnamespace	Specify a unique Eventhubnamespace.
alwaysOn	Ensure to set the default value as **true** before starting a fresh deployment, or else change it to **false** if you would like it to be off.

Note: Copy the keystore file from the Syslog NG Daemon SmartConnector or Load Balancer to cloud. To access the keystore file, log in to Azure and click **Storage Accounts** > <***storage account name***> > **Files** > **Storage container** > <***function app name***> > **`certs`** folder.

b. Specify the Service Plan. You can specify either **Consumptionplan** or **Appserviceplan**. The following table lists the service plans and their default values:

Service Plans	Default Values
servicePlanName	ArcSightPlan
servicePlanTier	Basic
servicePlanNumberofWorkers	1
servicePlanWorkerSize	Small

- An App Service plan handles a fixed event load. You can modify the service plan values as required.
- A Consumption plan is a serverless plan and allows you to scale automatically. It is not mandatory to specify any values for this plan.

c. Specify the location based on the locale of the resources you want to monitor.

d. Save the file.

Note:

- The default identifierUri is **www.example.com** in **app.properties**. Ensure that you update with a verified domain URI.
- Back up the **app.properties** file because you would need to refer to these configurations during uninstallation.

4. The deployment script has an option to enable and disable event hubs for Active Directory, Azure Monitor and Microsoft Defender for Cloud.
5. Open Windows PowerShell as Administrator and run the following command:

   `<extracted path>\DeployFunction.ps1`
6. When prompted, log in to Microsoft Azure as a user with required privileges for the subscription you want to use with Azure.
7. Select the appropriate subscription from the list displayed and click **Yes**.

Note: Ignore warnings displayed while deploying the Azure Monitor Event Hub connector.

Next Step: "Updating Keystore Certificate" below

Updating Keystore Certificate

The Syslog NG Daemon SmartConnector contains a default keystore certificate. Ensure that you associate this default keystore certificate with the new storage account to prevent errors.

Caution: : Do not use the existing resource groups in your Azure environment because this resource group will be deleted when you uninstall this connector.

To update the keystore certificate:

1. Go to `ArcSightSmartConnectors\current\user\agent` and rename the desired keystore certificate that is from the Syslog NG Daemon SmartConnector as **remote_ management.p12**, which is the file name of the default keystore certificate so that the Azure connector identifies the custom keystore.
2. Log in to Microsoft Azure as a user with required privileges for the subscription you want to use with Azure.
3. Select **All services** > **Storage accounts**.
4. In the Storage Accounts window, select the required storage account name.
5. Under the **Data storage** section, select **File shares**.
6. Select the storage container name function.
7. Open the displayed folder.
8. Click **Storage accounts** > <***Storage account name***> > **Data Storage** > **File shares** > <***function app name***> > **certs** folder. The default `certificate, remote_management.p12` certificate is displayed.
9. Delete this default certificate or overwrite the existing file.
10. Upload the certificate, `remote_management.p12`.
    a. Click **Upload**.
    b. In the URL field, browse to the desired location and select `remote_management.p12`.
    c. Click **Upload**.
11. Restart both the function apps:
    a. Click **Function Apps** > <*arcsight cloud function app name*> > **Restart**.
    b. Click **Function Apps** > <*arcsight monitor app name*> > **Restart**.

Note: After restarting the function apps, the Azure Connector is restarted along with the certificate uploaded. If you do not see the folder inside Storage Accounts, start the SyslogNG Connector and restart the `arcsight-monitor-functions` function.

Next Step: "Streaming Logs" below

Streaming Logs

After the installation completes, some logs stream automatically and some need to be configured.

Activity Logs

The install script automatically streams events from activity logs. There is no specific configuration required.

However, if you want to send activity logs from other account manually, complete the following steps:

1. Navigate to **Activity Logs** > **Monitoring** > **Diagnostic Settings**.
2. Add the setting by selecting the appropriate event hub and log categories to be monitored.

Active Directory Logs

The install script automatically streams events from Active Directory logs - audit logs, sign-in logs. There is no specific configuration required.

However, if you want to send Active Directory logs from other account manually, complete the following steps:

1. Navigate to **Activity Logs** > **Monitoring** > **Diagnostic Settings**.
2. Add the setting by selecting the appropriate event hub and log categories to be monitored.

Resource Logs

You must manually add diagnostic settings to configure streaming of these logs. The following procedure provides a brief overview of settings required for streaming Diagnostic Logs. For information, see Azure documentation.

1. Select **Azure Home** > **Monitor** > **Diagnostic Settings**.
2. Select the event hub. The default event hub name is **eh-emitter-arcsight**.
3. When the list of configured diagnostics is displayed, click **Edit** on the desired diagnostic to be updated. Click **Add**, to monitor a new resource.
4. From the Diagnostic settings window, select the **Stream to an event hub** check box or select the event hub.
5. On the Select event hub window:
    a. From the **Select event hub namespace** drop-down list, specify a name of event hub namespace.
    b. From the **Select event hub name** drop-down list, select **insights-diagnostics-logs**.
    c. From the **Select event hub policy name** drop-down list, select **ArcSightAccessKey**.
6. Click **OK**.
7. On the Diagnostic settings window, select the logs you want to stream.

Microsoft Defender for Cloud Event Logs

To send Microsoft Defender for Cloud events to Event Hub, follow these steps:

1. From the left sidebar, select **Microsoft Defender for Cloud**, and then click **Environment Setting**.

2. Select the specific subscription to be used when configuring data export.
3. On the **Subscription** settings, go to the sidebar and select **Continuous Export**.
4. Select the data type to be exported and choose from the filters on each type.
5. From **Export target**, choose the current subscription. Event hub namespace and name are defined in the **app.properties** file when deploying.
6. Go to the Event hub and create a new policy if needed.
7. Save your changes.

Next Step: "Configuring Function Apps to Stay Connected" below

Configuring Function Apps to Stay Connected

On the App Service Plan, function apps are designed to go to an idle state after a default timeout period. Therefore, you must manually configure the function apps to stay connected even if events are not streamed during the timeout period.

Note: For the **Always On** feature, ensure to set the default value as **True** in the **app.properties** before starting a fresh deployment, or else change it to **False** if you would like it to be off.

To configure the function apps to stay connected:

1. Click **Function Apps** > **Function Name** > **Application Settings** > **General Settings**.
2. For the **Always On** feature click **ON** if you want to keep it on or else click **OFF**.

   Ensure that you do this for both `<arcsight cloud function app name>` and `<arcsight monitor function app name>`.

Next Step: "Verifying the Deployment in Azure" below

Verifying the Deployment in Azure

To ensure that the Azure Monitor Event Hub connector installed successfully, verify the following:

1. The following Azure functions are installed in your Azure subscription: <***arcsight cloud function app name***> and <***arcsight monitor app name***>.

   These functions collect events from Azure event hubs and monitor the health of the connection downstream. To view the functions in Azure, click **Function Apps**.
2. The install script automatically streams events from the audit logs, sign-in logs, and activity logs. For Resource Log, you must manually add diagnostic settings to configure streaming of these logs. For more information, see **Step 7** in "Streaming Logs" on page 24.

3. Uploads the application settings listed in the **app.properties** file to Azure. This enables you to add or modify properties from Azure instead of modifying the **app.properties** file and redeploying the Azure Monitor Event Hub connector. To view the properties in Azure, click **Function Apps** > <***function app name***> > **Application Settings**. For more information about modifying these properties, see "Customizing the Connector" on page 28.
4. The Azure Monitor Event Hub Connector converts JSON events to CEF format. To view the default certificates in Azure, click **Storage Accounts** > <***Storage account name***> > **File shares** > ***Storage container*** > <***function app name***> > **certs** folder. The default name of the storage account is **emitterarcsightstorage**.

   Note: The Azure Monitor Event Hub connector supports custom mapping. If you want to modify the current mappings or support a new category, then create a map file.
   To upload the newly created map file to Azure, click **Storage Accounts** > <***Storage account name***> > **File shares** > **Storage container** > <***function app name***> > **maps** folder.
5. An Active Directory application called <***arcsight monitor app name***> is created and the Azure Website Contributor role is assigned to this application.
6. A resource group called <***arcsight functions group name***> is created. This resource group manages the resources of this connector. The default name of the resource group is **arcsightfunctions-group**.
7. An Azure storage account called <***storage account name***> is created. This storage account stores the Azure Monitor Event Hub connector certificate, function logs, and the parser files.

Additional Configurations

Customizing the Connector

You can customize the connector properties as required.

To customize the connector:

1. Log in to Microsoft Azure as a user with required privileges for the subscription you want to use with Azure.
2. Click **Function Apps** > <***arcsight cloud function app name***> or <***arcsight monitor function app name***> > **Platform Features** > **Application Settings**.

   Important: Do not modify any of the settings other than those listed in this procedure as this may cause unpredictable performance or even outages.
3. (Conditional) To modify the connector port and connector name of the Syslog NG Daemon SmartConnector or Load Balancer:
   a. Update the **Connector Port** field.
   b. Update the **Connector Hostname** field with the IP address or hostname.

      Note: Ensure that you do this for both <arcsight cloud function app name> and <arcsight monitor function app name>.
4. (Conditional) You can send the connector logs to a storage account. However, this consumes cloud storage

   In the **logging.storage.enabled** field, enter **true**. The connector now sends logs from the function app to the storage account every 15 minutes.

   To stop sending logs to the storage account, enter **false** in the **logging.storage.enabled** field.
5. Click **Save**.

Scaling Performance

You might need to modify your deployment or change certain configurations to improve the performance.

- Your Azure pricing plan also affects performance scaling.

  A Consumption plan scales automatically and an App Service plan handles a fixed event load. A Consumption plan automatically creates Function App instances to scale up the load. For more information about the event load handled in a App Service plan, see the Azure Documentation.
- You can configure Load balancer in environments where the event load is more than what can be handled by a single Syslog NG Daemon SmartConnector.

Additional Security Configurations

This section has the following information:

Adding Role Assignments

Ensure that you have:

`Microsoft.Authorization/roleAssignments/write` and `Microsoft.Authorization/roleAssignments/delete` permissions, such as User Access Administrator or Owner.

To add a role assignment:

1. Sign into the **Azure** portal.
2. From the search box, search for the **Resource Group** you want to assign roles to.
3. Click the **Resource Group** and navigate to the **Access Control (IAM)** page.
4. Click the **Role Assignments** tab to view the role assignments at this scope.
5. Click **Add** > **Add Role Assignment**.

   The **Add Role Assignment** pane opens.

   Note: If you do not have permissions to assign roles, the **Add Role Assignment** option is disabled.
6. From the role list, search or scroll to find the role that you want to assign and click to select it.
7. Go to the **Assign Access To** list and click to select the type of security principle to assign access to.

   These principles generally are **User**, **Group** or **Service**.

8. If you selected a user-assigned managed identity or a system-assigned managed identity, select the subscription where the managed identity is located.
9. From the **Select** section, search for the security principle by entering a string or scrolling through the list.
10. To assign the role, click **Save**.
11. From the **Role Assignments** tab, confirm that you see the role assignment in the list.

To remove existing role assignments:

1. Open **Access control (IAM)** at a specific scope, such as management group, subscription, resource group, or resource, where you want to remove access.
2. Click the **Role Assignments** tab to view all the role assignments at the scope.
3. From **Role Assignments**, add a check mark next to the security principle with the role assignment you want to remove.
4. Click **Remove**.
5. A message is displayed, click **Yes** to confirm the changes.

Configuring Firewall Settings for Azure Resources

1. Sign into the **Azure** portal.
2. Navigate to the **Azure Resource** that needs to be monitored.
3. Go to **Networking**.
4. Select **Allow Access from Selected Networks**.
5. Add a new virtual network or select an existing network.
6. Under Firewall, enter the IP Address Range that needs to be allowed.

   Additionally, you can select your client's IP address as well.
7. Select the **Resource Type** and the Instance name as **All in this Resource Group**.
8. Under **Exceptions**, check the option **Allow trusted Microsoft services to access this storage account**.
9. Verify if the Network Routing field shows **Microsoft Network Routing** as the default one.
10. Save the changes and refresh the resource modified.
11. Restart the function apps.

Disabling FTP/FTPS when using function apps

By default, FTP/FTPS is enabled when using Function App for TLS communication. You can disable FTP/FTPS if required.

To disable FTP/FTPS:

1. Go to the **Cloud Function App**.
2. Navigate to **Configuration** > **General Settings** > **Platform Settings**.
3. On the **FTP State** field, select **Disabled**.
4. Save the changes and restart the function app.
5. Perform the same steps on the Monitor function app and save changes.

(Optional) Using a Private IP

You can configure Event Hub and Function App to use a private IP. However, if you are on a basic subscription plan, then you must upgrade to a Standard or Premium plan.

To use a private IP:

1. Add a new or an existing VNet to Event Hubs, Storage Account, and Function Apps.

   To add VNet to Event Hubs

   a. From your **Event Hub**, under **Settings**, click **Networking**

   b. Do one of the following:

   - Select **All Networks** to add all networks to access your resources.
   - Click **Selected Networks** to add selected networks to access your resource.

     Add the **Existing virtual network** or **Create new virtual network**.

   To add VNet to Storage Account

   a. From your **Storage Account**, click **Networking**, and then click the **Firewalls and Virtual Networks** tab.

   b. Select one of the followings:

   - **Enabled from all networks** - to add all networks to access your resources.
   - **Enabled from selected virtual networks and IP addresses** - to add selected networks to access your resource.

     Add the **Existing virtual network** or **Add new virtual network**.

   To add VNet to Function Apps

   a. Go to the **Function App** > **Settings** > **Networking** > **Outbound Traffic** > **VNet Integration**, add those to your VNet.

   b. Add or remove network interfaces from your virtual machines, for more information, see Add network interfaces to or remove network interfaces from virtual machines.

2. Enable the Service endpoints of the previously used subnets.

a. From **Virtual networks Service**, select your **VNet** > **Subnets**.

b. Open all the subnets.

c. Select **All Service Endpoints** and save your changes.

3. Check if the Function Apps communicate to the destination (ArcSight Syslog NG Daemon, ArcSight Load Balancer, etc.) through the Private IP.
4. From **Development Tools** > **Console Tool**, execute the `tcpping` command to your VM via private IP.

   `tcpping host:port`

   `host: private IP`

   `port`: you may use port 3389 or the port used in your Function Apps.
5. After successfully executing the command above, from **Function Apps** > **Application Settings**, check if the setting already exists or add a new one:

   APP SETTING NAME: JAVA_OPTS

   VALUE: -Djava.net.preferIPV4Stack=true
6. In the field **connectorhostname**, enter your Private IP.
7. Next, in the field **Port**, enter the port of your Private IP.
8. Restart **Function Apps**.

Note: The VNet integration preview is a preview, if it does not work, you can disable and enable the VNet integration or create another subnet.

Upgrading the Connector

You can only do a binary upgrade of the Azure Monitor Event Hub connector. A binary upgrade upgrades the connector and also enables you to continue using the components and the custom settings created during deployment.

To upgrade the connector:

1. Stop all the connector specific Function App(s).
2. Stop the Syslog NG Daemon SmartConnector.
3. On the machine from where you want to upgrade the connector, download `arcsight-azure-monitor-eventhub-connector-x.x.x.zip`.
4. Extract the `arcsight-azure-monitor-eventhub-connector-x.x.x.zip` files to the desired location.
5. Configure the **app.properties** file. For more information, see Step 3 in **Deploying the Connector**. Ensure that you specify the same Function App names that you specified during deployment.
6. Open Windows PowerShell as Administrator and run the following command:

   ```
   <extracted path>\DeployFunction.ps1
   ```

7. When prompted to enable or disable a specific event hub, press **0** to enable and **1** to disable.

   The event hubs for Active Directory logs, Activity Logs, Resource Logs (formerly known as Diagnostic logs), and Microsoft Defender for Cloud logs are enabled by default. However, you can select to monitor only the specific event hubs.
8. Log in to Microsoft Azure as a user with required privileges for the subscription you want to use with Azure.
9. Select the required subscription.
10. When the script prompts you, select one of the following:
    - **Y**: to verify and update the resources.

      The script first checks whether there is an existing installation of the Connector in the cloud, and then the installation will verify and update the resources.
    - **N**: to exit the script.
11. To configure the Function App(s) to stay connected, click **Function Apps** > <***function name***> > **Application Settings** > **General Settings** and update it to **Always on**.
12. Start all the connector specific Function App(s).
13. Start the Syslog NG Daemon SmartConnector.

Updating Parser Files

First, extract the new parser files from the AUP Extractor Tool:

To extract parser files:

1. Download the `ArcSight-x.x.x.xxxx.0-ConnectorParsers.aup` package from the ArcSight Marketplace.
2. To apply monthly parser updates to Cloud Connectors:
   a. Download the `ArcSight-x.x.x.xxxx.0-aup-extractor.jar` utility from the location where you have downloaded the connector.

      Note: Your system must have Java 1.8.x or later version installed and Java available in the operating system's path to use the aup-extractor.jar utility

   b. Run the following command to use the utility to extract parser files from the package:

      `java -jar aup-extractor.jar <AUP filename>`

      Examples:

      - `java -jar aup-extractor.jar ArcSight-x.x.x.xxxx.0-ConnectorParsers.aup` - When the **.aup** package is in the same directory where the JAR file is present.
      - `java -jar aup-extractor.jar c:\MyFolder\ArcSight-CE 24.2xxxx.0-ConnectorParsers.aup` - When the **.aup** package is present in other directory.

      You can either provide one or both the parameters. If you do not provide any parameters, the utility picks up any available. aup file and creates a new folder named **output** in the directory from where the utility is run and uploads the output files.

      The following folders will be extracted:

      - **aws_cloudwatch**: Contains security parser for AWS Cloudwatch.
      - **aws_securityhub**: Contains security parser for AWS Security Hub.
      - **azure_emitter**: Contains security parser for Azure emitter.

   c. Copy the parser files in the **output/azure_emitter** folder and upload them to the Azure environment.

To override parser files:

1. Stop the Cloud Function app and the Monitor Function app.
2. Go to **Cloud function app** > **App Service Editor (Preview)**> **Developer Tools**.
3. Click **Go**.
4. Right-click the **Maps** folder and click **Upload**.

5. Select the parser files to be overridden and click **OK**.
6. Restart the function apps.
7. Refresh the page by restarting the **App Service Editor (Preview)**.

To store and quick-view parser files:

Go to **Storage Accounts** > **Storage Account Name** > **File Shares** > **Storage Container** > **Function App Directory** >**Maps**.

Undeploying the Connector

Undeploying the Azure Monitor Event Hub connector deletes the Active Directory application (AzADApplication) and all the associated components such as storage account and event hubs created during deployment.

To undeploy the connector:

1. Open Windows PowerShell as Administrator and run the following command:

   ```
   <deployed path>\UndeployFunction.ps1
   ```

2. Log in to Microsoft Azure as a user with the required privileges for the subscription you want to use with Azure.
3. Select the required subscription.
4. Enter **Yes** when prompted to confirm deletion of the installed resources, such as event hubs, storage account, function apps, and AzADApplication. This will undeploy the connector.

Note: The resource group will not be deleted when you undeploy the connector. However, post undeployment, you can delete the resource group if required.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the ArcSight Console User's Guide for more information about the ArcSight data fields.

Event Mappings for Active Directory

Common Event Mapping

ArcSight ESM Field	Device-Specific Field
Name	operationName
Device Event Class ID	operationName
Severity	Level

Sign-in Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Application Protocol	properties/clientAppUsed
Destination Process Name	properties/appDisplayName
Destination User ID	properties/userId
Destination User Name	properties/userDisplayName
Device Custom Date 1	properties/createdDateTime
Device Custom Floating Point 1	properties/location/geoCoordinates/latitude
Device Custom Floating Point 2	properties/location/geoCoordinates/longitude
Device Custom String 1	properties/deviceDetail/operatingSystem
Device Custom String 2	properties/isRisky
Device Custom String 3	properties/location
Device Custom String 4	location
Device Custom String 5	correlationId
Device Custom String 6	properties/userPrincipalName
Device Event Category	category
Device Receipt Time	time
Event Outcome	resultType
External ID	properties/id
Reason	resultDescription
Request Client Application	properties/deviceDetail/browser
Source Address	callerIpAddress

Audit Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	properties/targetResources/userPrincipalName
Device Event Category	properties/category
Device Custom String 1	properties/identityType
Device Custom String 2	properties/operationType
Device Custom String 3	properties/targetResources/modifiedProperties(Role.DisplayName)/displayName (Role.DisplayName)
Device Custom String 5	correlationId
Device Custom String 6	properties/targetResources
Device Receipt Time	time
Event Outcome	resultType
External ID	properties/id
File Hash	properties/targetResources/modifiedProperties(Role.DisplayName)/newValue (Role.DisplayName)
File Name	properties/targetResources/modifiedProperties(Group.DisplayName)/newValue (Group.DisplayName)
File Path	properties/targetResourceName
File Type	properties/targetResourceType
Old File Hash	properties/targetResources/modifiedProperties(Role.DisplayName)/oldValue (Role.DisplayName)
Old File Name	properties/targetResources/modifiedProperties(Group.DisplayName)/oldValue (Group.DisplayName),
Reason	resultDescription
Source Address	callerIpAddress
Source User ID	properties/initiatedBy/user/id,
Source User Name	properties/initiatedBy/user/userPrincipalName

Event Mappings for Microsoft Defender for Cloud

Common Event Mapping

ArcSight ESM Field	Device-Specific Field
Name	AlertDisplayName
Device Event Class ID	AlertType
Severity	Severity

Security Alerts Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	AlertType
Destination Host Name	CompromisedEntity, Entities/HostName
Device Custom Date 1	ProcessingEndTime
Device Custom Number 1	Entities/$id
Device Custom String 1	ExtendedProperties
Device Custom String 2	IsIncident
Device Custom String 3	ResourceIdentifiers
Device Custom String 4	AlertUri

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	Entities/Location/Asn & Entities/Location/CountryCode & Entities/Location/CountryName & Entities/Location/State & Entities/Location/City & Entities/Location/Longitude & Entities/Location/Latitude
Device Receipt Time	TimeGenerated
Device Severity	Severity
End Time	EndTimeUtc
Event Outcome	Status
External ID	SystemAlertId
File Path	AzureResourceId, Entities/AzureID, Entities/ResourceId
File Type	Entities/Type
Message	Description & RemediationSteps
Reason	Intent
Start Time	StartTimeUtc
Source Address	Entities/Address

Security Recommendations Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	type
Device Action	assessmentEventDataEnrichment/action
Device Custom String 1	properties/metadata/policyDefinitionId
Device Custom String 2	properties/metadata/threats
Device Custom String 4	properties/links/azurePortal
Device Severity	properties/metadata/severity
File Name	file
File Path	ID
Message	properties/metadata/description & properties/metadata/remediationDescription

ArcSight ESM Field	Device-Specific Field
Name	properties/displayName
Event Outcome	properties/status/code
Reason	properties/status/cause

Event Mappings for Activity

Common Event Mapping

ArcSight ESM Field	Device-Specific Field
Name	operationName
Device Event Class ID	operationName
Severity	level

Action Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination Port	properties/eventProperties/destinationPort
Destination Host Name	resourceId, properties/eventProperties/machineName
Destination User Name	identity/claims/name
Destination User Privileges	identity/authorization/evidence/role
Device Custom Date 1 Label	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	properties/eventProperties, properties/policies
Device Custom String 3	properties/eventProperties/title
Device Custom String 4	location
Device Custom String 5	correlationId
Device Custom String 6	properties/isComplianceCheck
Device Event Category	category
Device Receipt Time	time
Event Outcome	resultType
External ID	eventDataId

ArcSight ESM Field	Device-Specific Field
File Hash	properties/eventProperties/fileSha256
File Path	resourceId, properties/eventProperties/filePath
File Name	properties/eventProperties/fileName
File Type	resourceType, properties/eventProperties/type
Message	description
Old File Type	properties/eventProperties/resourceType
Reason	properties/eventProperties/cause
Request Client Application	properties/eventProperties/compromisedEntity
Source Address	callerIpAddress
Source Service Name	properties/eventProperties/attackedResourceType
Transport Protocol	properties/eventProperties/protocol

Administrative Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	identity/claims/name
Destination User Privileges	identity/authorization/evidence/role
Device Action	identity/authorization/action
Device Custom Number 1	durationMs
Device Custom String 1	resultSignature
Device Custom String 4	location
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	time
Event Outcome	resultType
File Path	resourceId
Message	identity/claims
Request Client Application	identity/claims/iss
Request URL	identity/claims/aud
Source Address	callerIpAddress

Alert Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	caller
Device Custom Date 1	submissionTimestamp
Device Custom Number 1	properties/Threshold
Device Custom Number 2	properties/WindowSizeInMinutes
Device Custom String 1	properties/RuleUri, subStatus
Device Custom String 2	properties/RuleName
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
Event Outcome	status
External ID	eventDataId
File Path	resourceId
File Type	resourceType
Message	description

Delete Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Privileges	identity/authorization/evidence/role
Destination User Name	identity/claims/name
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	correlationId
Device Custom String 4	location
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
File Type	resourceType
Event Outcome	resultType

ArcSight ESM Field	Device-Specific Field
External ID	eventDataId
Message	description
Source Address	callerIpAddress

Recommendation Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	caller
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	properties/recommendationCategory
Device Custom String 3	properties/recommendationImpact
Device Custom String 4	properties/recommendationRisk
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
Event Outcome	status
External ID	eventDataId
File Path	resourceId
File Type	resourceType
Message	description

Security Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination Process ID	properties/processId
Destination Process Name	properties/processName
Destination NT Domain	properties/domainName
Destination User ID	properties/accountLogonId
Destination User Name	caller, properties/userName
Device Action	properties/ActionTaken

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	properties/UserSID
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
External ID	eventDataId
Event Outcome	status
File Path	resourceId
File Type	resourceType
Message	description

Service Health Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination Service Name	properties/impactedServices
Destination User Name	caller
Device Custom Date 1	submissionTimestamp
Device Custom String 1	properties/trackingId
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
External ID	eventDataId
Event Outcome	status
File Path	resourceId
File Type	resourceType
Message	description
Start Time	properties/impactStartTime
Reason	properties/communication

Write Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	identity/claims/name
Destination User Privileges	identity/authorization/evidence/role
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 4	location
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	time
External ID	eventDataId,
Event Outcome	properties/statusCode
File Path	resourceId
File Type	resourceType
Source Address	callerIpAddress

Event Mappings for Resource Log

Common Event Mapping

Device Event Mapping	ArcSight Fields
Name	operationName
Device Event Class ID	operationName
Severity	Level

Activity Runs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 2	Error

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	correlationId
Device Receipt Time	time
External ID	activityRunId
File ID	pipelineRunId
File Path	resourceId
File Name	pipelineName
Destination Process Name	activityName
Start Time	start
End Time	end
Message	Output

Application Gateway Access Log Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
Device External ID	instanceId
Source Address	properties/clientIP
Source Port	properties/clientPort
Request URL	properties/requestUri
Request Client Application	properties/userAgent
Event Outcome	properties/httpStatus
Bytes In	properties/receivedBytes
Bytes Out	properties/sentBytes
Device Custom Number 1	properties/timeTaken
Device Custom String 1	properties/sslEnabled

Archive Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
External ID	ActivityId
Device Custom String 1	trackingId
Device Custom String 2	archiveStep
File Path	resourceId
File Name	eventHub
Start Time	startTime
Device Custom Number 1	failures
Device Custom Number 2	durationInSeconds
Message	message

Audit Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Event Outcome	resultType
Source Address	callerIpAddress
Destination User ID	identity
Device Custom String 1	properties/JobId
Device Custom String 2	properties/JobRunTime
Device Custom String 5	correlationId
Destination Process Name	properties/JobName
Start Time	properties/StartTime
End Time	properties/EndTime

Authoring Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Event Outcome	status
Device Receipt Time	time
Device Custom String 1	properties/Error
Device Custom String 5	properties/correlationId
Message	properties/Message
Reason	properties/Type

Automatic Tuning Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
File Path	ResourceId

Azure Firewall Application Rule Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceid
Message	properties/smg

Azure Firewall Network Rule Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceid
Message	properties/smg

Azure Site Recovery Jobs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
Event Outcome	properties/resultType
Message	properties/resultDescription
Start Time	properties/startTime
End Time	properties/endTime
Device Custom String 2	properties/affectedResourceType
Device Custom String 3	properties/affectedResourceId
Device Custom String 5	properties/correlationId

Blocks Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup

ArcSight ESM Field	Device-Specific Field
Device Custom String 4	DatabaseName_s
Device Custom Number 1	duration_d
File Path	ResourceId
Destination User Name	resource_owner_type_s

C2D Command , C2D Twin Operations, and D2C Twin Operations Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Device Custom String 1	properties
Device Custom String 2	location
Device Custom Number 1	durationMs
Event Outcome	resultType
Message	resultDescription

Database Wait Statistics Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	delta_wait_time_ms_d
Device Custom Number 2	delta_waiting_tasks_count_d
File Path	ResourceId

Deadlocks Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
Device Custom Number 1	duration_d
File Path	ResourceId
Destination User Name	resource_owner_type_s

Engine Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
File Path	resourceId
Device Event Category	category
Start Time	properties/StartTime
Device Custom String 1	properties/ObjectID
Device Custom String 2	properties/ObjectType
Device Custom String 3	properties/ObjectName
Device Custom String 4	properties/ObjectPath
Device Custom String 5	properties/ObjectReference

ArcSight ESM Field	Device-Specific Field
End Time	properties/EndTime
Event Outcome	properties/Success
Device Custom Number 1	properties/ConnectionID
Device Custom Number 2	properties/SPID
Source NT Domain	properties/NTDomainName
Source Host Name	properties/ClientHostName
Source Process ID	properties/ClientProcessID
Device Custom String 6	properties/ApplicationName
Destination User Name	properties/User
Destination Service Name	properties/ServerName

Errors Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
File Path	ResourceId
Message	Message
Event Outcome	state_d
Reason	error_number_d

Gateway Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
Device Custom Number 1	durationMs
Device Custom String 2	location
Source Address	callerIpAddress
Request URL Method	properties/method
Request URL	properties/url
Event Outcome	properties/responseCode

Job Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	TimeGenerated
File Name	RunbookName_s
Destination User Name	Caller_s
Device Custom String 1	resourceId
Device Custom String 2	resourceGroup
Device Custom String 3	Tenant_g
Device Custom String 5	correlationId
File ID	JobId_g
Event Outcome	ResultType
Device Event Category	category

Jobs Operations Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time

ArcSight ESM Field	Device-Specific Field
File Path	resourceId
Device Custom String 1	properties
Device Custom String 2	location
Device Custom Number 1	durationMs
Event Outcome	resultType
Message	resultDescription

Load Balancer Alert Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
Device Custom String 1	systemId
File Path	resourceId
Reason	properties/eventDescription
Destination Address	properties/eventProperties/public ip address

Network Security Group Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Destination MAC Address	properties/macAddress
Destination Address	properties/primaryIPv4Address
Device Custom String 1	properties/subnetPrefix
Device Custom String 2	properties/ruleName
Device Custom String 3	properties/direction
Device Custom String 4	properties/priority
Device Custom String 5	properties/type
Message	properties/conditions
Transport Protocol	properties/conditions/protocols

Operational Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
File Path	resourceId
Device Custom String 1	subscriptionId
Device Custom String 4	Region
Device Receipt Time	EventTimeString
Message	EventProperties
Event Outcome	Status
Source Process Name	Caller
External ID	ActivityId

P2S Diagonstic Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
Message	properties/message
Device External ID	properties/instance

Postgre SQL Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
Device Custom String 3	ResourceGroup
Device Custom String 2	SubscriptionId
Source Service Name	LogicalServerName
Message	properties/message

Query Store Wait Statistics Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 1	TenantId
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
Device Custom Number 1	total_query_wait_time_ms_d
File Path	ResourceId

Requests Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Event Outcome	resultType
Source Address	callerIpAddress
Destination Use ID	identity
Request Method	properties/HttpMethod
Request URL	properties/Path
Bytes In	properties/RequestContentLength
External ID	properties/ClientRequestId
Start Time	properties/StartTime
End Time	properties/EndTime

Routes Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Device Custom String 1	properties
Device Custom String 2	location
Device Custom Number 1	durationMs
Event Outcome	resultType
Message	resultDescription

Service Log Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	Tenant
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
External ID	properties/id
File Type	properties/imageType

Timeouts Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Receipt Time	TimeGenerated
File Name	Resource

ArcSight ESM Field	Device-Specific Field
File Type	ResourceType
Azure Logical Server Name_s	LogicalServerName_s
Azure Elastic Pool Name_s	ElasticPoolName_s
CS 4 Label	DatabaseName_s
File Path	ResourceId

Trigger Runs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 2	triggerEvent
Device Custom String 5	correlationId
Device Receipt Time	time
External ID	activityRunId
File Path	resourceId
File Name	pipelineName
Destination Process Name	activityName
Start Time	start
End Time	end
File ID	triggerId
File Type	triggerType

Twin Queries Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
Device Custom Number 1	durationMs
Device Custom String 1	properties
Device Custom String 2	location

ArcSight ESM Field	Device-Specific Field
Event Outcome	resultType
File Path	resourceId
Message	resultDescription

Workflow Runtime Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
Reason	code
Event Outcome	properties/status
Start Time	properties/startTime
End Time	properties/endTime
Device Custom String 1	properties/resource/subscriptionId
Device Custom String 2	properties/resource/resourceGroupName
Device Custom String 4	properties/resource/location
Device Action	properties/resource/actionName
File Name	properties/resource/workflowName

Troubleshooting

This section includes:

Error during Installation or Upgrade

The following connection error is displayed while installing or upgrading the connector:
“502 - Web server received an invalid response while acting as a gateway or proxy server.”

Workaround:

You can ignore this error message. Generally, the server tries to reconnect with the connector and the installation or upgrade process continues after the connection is established. However, if the server is unable to establish connection with the connector, the installation or upgrade process fails to proceed, and you are exited from the wizard.

Errors during Deployment

You might receive an error message prompting you to register the subscription <subscription id> with **Microsoft.Insights**.

Workaround:

In this case, you must register your subscription with the **microsoft.insights** provider.

To register:

1. Log in to Microsoft Azure as a user with administrator privileges.
2. Click **All Services** > **Subscriptions**.
3. Select the subscription you want for this connector.
4. Select **Resource Providers**.
5. Click **Register**.

Connection Errors

Connection errors are displayed when the Syslog NG Daemon SmartConnector hostname and port are not reachable from Azure cloud.

Workaround:

To ensure that the Syslog NG Daemon SmartConnector host and port are reachable from Azure cloud:

1. Open the relevant ports. The certificate file is overridden during the deployment of the Azure Monitor Event Hub connector.
2. Replace the remote connection management file in Azure with your remote connection management file.
3. Click **Storage Accounts** > <***Storage account name***> > **Files** > **Storage container** > <***function app name***> > **certs** folder.
4. Replace the **remote_management.p12** file with your **<*customname*>.p12** file.

Parsing Errors

Parsing errors are displayed if the event log categories are not supported by the Azure Monitor Event Hub connector. For a list of the supported categories, see Appendix A, “Azure Event Log Categories".

Workaround:

You can contact technical support in the following scenarios:

- If you want to change the default mappings.
- If you want to add a new log type.
- See parsing errors.

Sharing Logs for Troubleshooting

You might want to share logs with technical support for troubleshooting.

Workaround:

To share logs:

1. Log in to Microsoft Azure as a user with security reader privileges or contributor privileges.
2. From the **Development Tools** menu, click **App Service Editor**.

3. Click **Go**.
4. On the new App Service Editor tab, select **Open Kudo Console** from the top drop-down menu.
5. On the new tab, go to: **site** > **wwwroot** > **logs**.
6. Download the function logs and send them to technical support.

AppService plan is not created in a stamp that supports VNet integration

Microsoft Azure Monitor Event Hub Connector requires an AppService plan with basic pricing tier. However, you must ensure that your AppService plan is created in a stamp that supports VNet Integration. the VNet integration feature configuration requires a premium V2VM.

It is possible that you have an existing AppService plan that was created in a stamp that does support Premium V2 even for a basic plan and it allows you to use the VNet integration feature.

Workaround:

If you are on a basic plan and are unable to create VNet integration, try the following:

You can temporarily upgrade the plan to complete the VNet configuration. After the VNet configuration completes, you scale back to the basic plan to use the VNet Feature.

If your AppService plan does not show the feature to scale up to Premium V2, you might not be able to create a new AppService plan in the same Resource Group of the Premium V2 pricing Tier. This happens because the Resource Group sometimes, decides on a particular stamp and creates all resources in there. If you experience this issue, try creating the AppService plan in a different Resource Group.

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 Configuration Guide Microsoft Azure Monitor Event Hub Connector (SmartConnectors CE 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 MFI-Documentation-Feedback@opentext.com .

We appreciate your feedback!