Micro Focus Transformation Hub Non-Containerized (THNC)

Software Version: 3.0.0

Deployment Guide

Document Release Date: September 13, 2019
Software Release Date: July 31, 2019

Legal Notices

Copyright Notice

Trademark Notices

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Chapter 1: Overview

About Transformation Hub

Transformation Hub is a high-performance message bus and data ingestion application for security events that utilizes Kafka and Micro Focus technology for the deployment and management of applications. It can queue, transform, and route security events to ArcSight and third-party software. Transformation Hub enables products such as Logger and ESM to receive the event stream as it comes, while smoothing event spikes.

Transformation Hub ingests, enriches, normalizes, and then routes data to connections between existing data lakes, analytics platforms, and other security technologies and the multiple systems within the Security Operations Center (SOC). It can seamlessly broker data from any source and to any destination that is able to consume the supported message formats.

The Transformation Hub product is available in two different deployment forms. Choose one that supports your specific needs:

- **Transformation Hub:** Docker container-based deployment package which utilizes Kubernetes, containerized Kafka, containerized ZooKeeper, a Kafka management application, plus support for all Transformation Hub features. See the Transformation Hub Deployment Guide for information about how to install Transformation Hub using this deployment package.
- **Transformation Hub Non-Containerized (THNC):** File-based deployment package that supports a subset of Transformation Hub features, and does not come with Kafka, ZooKeeper, or the Transformation Hub Kafka Manager built-in. This package is intended to be used in environments where a customer wants to deploy Transformation Hub onto an existing Kafka cluster. This document describes how to install the THNC deployment package.

Product Compatibility

The following product versions are compatible with one another.

Transformation Hub Non-Containerized (THNC)	3.0
SmartConnector	7.13
Management Center	2.92
ESM	7.0, 6.11.0

About Transformation Hub Non-Containerized

The Transformation Hub Non-Containerized (THNC) deployment package is intended for environments with an existing installation of Kafka and ZooKeeper, and the customer wants to install Transformation Hub

into that environment.

The THNC deployment package provides only the software components needed to run Transformation Hub. It does not include Kafka, ZooKeeper, or Transformation Hub Kafka Manager which manages the Kafka brokers. THNC is not a container-based deployment, but a set of systemd managed services, one for each software component, that communicate with Kafka and ZooKeeper systems and with each other. Each installed instance of THNC includes the following software components (and service name):

- Schema Registry (arst-sr): Used to define the structure of messages for CEF to AVRO transformation and for the Routing Stream processor.
- Web Service (arst-ws): Provides management, monitoring, and metrics capabilities to ArcMC. Is also responsible for creating the THNC topics in Kafka when you first install THNC.
- Routing Stream Processor (arst-route): Routes CEF events to defined topics based on rules that characterize which subset of events should be routed.
- C2AV Stream Processor (arst-c2av): Transforms messages from CEF to Avro..

Feature Comparison Transformation Hub Non-Containerized (THNC) Versus Transformation Hub

Certain features that are available in Transformation Hub are not available in Transformation Hub Non-Containerized (THNC). The following table summarizes the differences.

Capability	Transformation Hub	Transformation Hub Non-Containerized (THNC)
CEF Event Routing	Supported	Supported
Management and Monitoring through ArcMC	Supported	Limited Support. • Operating System metrics are not collected. • ArcMC connects to one instance of THNC at a time. If that instance fails and you have a highly available deployment topology, you manually connect ArcMC to another running instance
Connectors in Transformation Hub	Supported	Not Supported
Transformation Hub Kafka Manager	Supported	Not Supported
Container-based deployment	Supported	Not Supported

Capability	Transformation Hub	Transformation Hub Non-Containerized (THNC)
Auto restart of failed modules	Supported via the native ability of Kubernetes-managed containers to restart automatically.	Not supported. Services must be monitored, managed, and restarted by the customer.
Security Modes	TLS Supported Client Authentication Supported FIPS Supported	TLS Supported Client Authentication supported FIPS Not Supported

Summary of Deployment Steps

The high-level deployment process for Transformation Hub Non-Containerized (THNC) consists of the following steps.

1. Ensure that you have a fully functional Kafka and ZooKeeper deployment. Kafka brokers in the cluster must be able to accept connection requests; a producer must be able to publish a message to a topic; and consumers must be able to read from that same topic.
2. Plan your Deployment Topology. See Planning the Deployment Topology.
3. Set up the host machines needed for THNC and ArcMC, and collect the information needed during the installation process. See "Installation Prerequisites" on page 9.
4. Download and install the THNC installation package. See "Download and Install Transformation Hub Non-Containerized" on page 14.
5. Configure the THNC services. See Configuring Transformation Hub NC service.
6. Install your customer license to ensure continued functionality and event flow. See "Install Your Customer License" on page 23 for more information.
7. Install ArcMC to connect to THNC. See "Connect ArcMC to Transformation Hub Non-Containerized" on page 24 for more information.

   Start the THNC services. See Starting the Transformation Hub NC service.
8. Ensure the Transformation Hub services are running and are healthy. See Checking the Status of the THNC Services.
9. Set up SmartConnectors to publish events to THNC.
10. As needed, set up ESM or Logger to consume events from THNC.

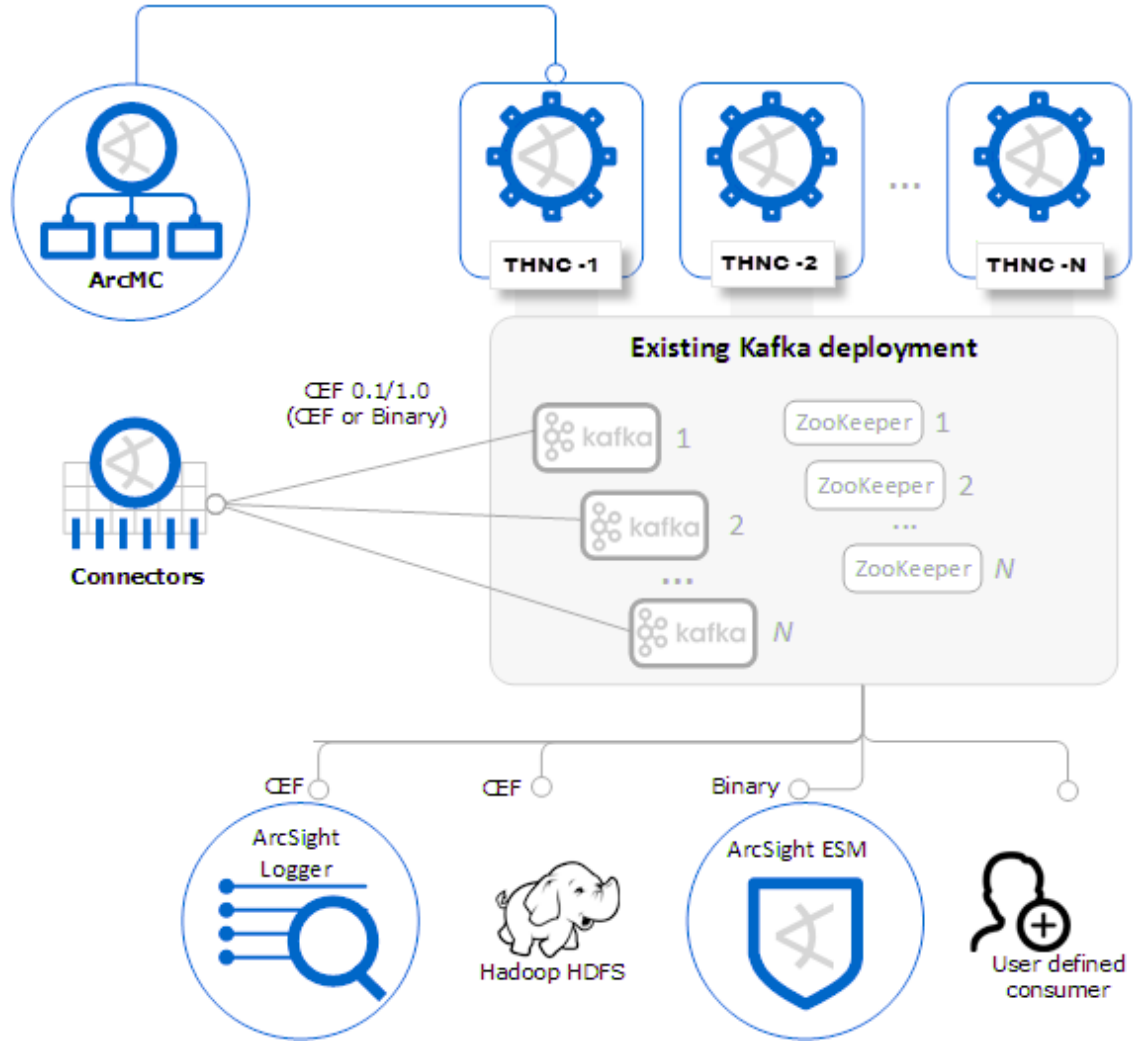
Plan the Deployment Topology

You can deploy one instance of THNC or multiple instances of THNC, each on a separate system. To support a highly-available deployment topology, install at least three THNC instances, with each one on a

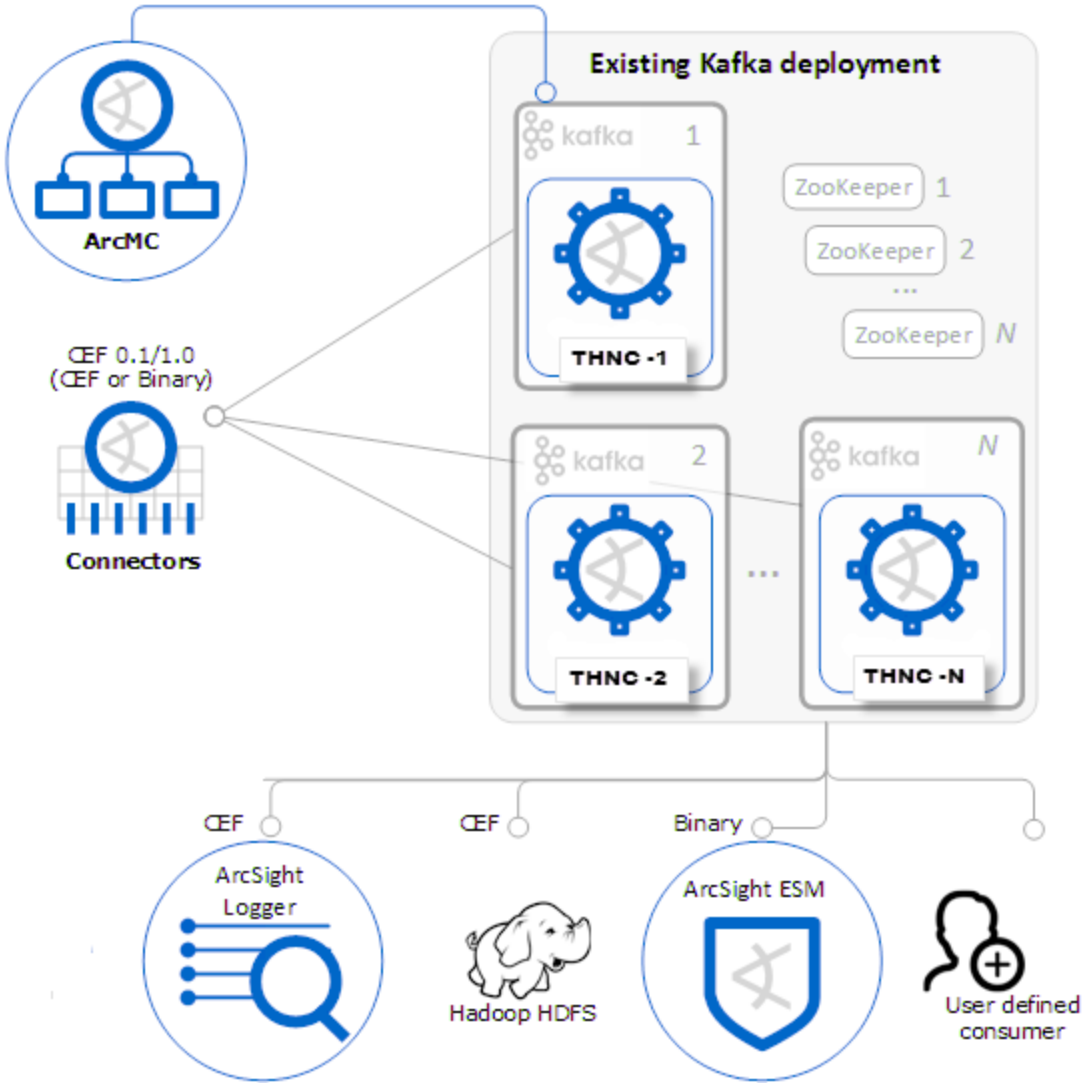
separate server. Each THNC instance can run on a dedicated system, or it can run on the same system where Kafka is installed.

- When you deploy in a multi-node configuration, the Stream Processor services (both CEF to AVRO and Routing) will work as a consumer group providing High Availability (HA) if one THNC instance fails.
- ArcMC connects to Web Service on one of the instances. If that system fails, ArcMC will need to be manually reconfigured to connect to one of the other systems running the THNC Web Service.
- You must install the ArcMC server certificate onto the THNC system that ArcMC connects to. You can import certificates to all systems ahead of time to prepare for the future connections, or you can import the certificate to the individual system only at the time you connect ArcMC to that instance.
- JMX must be enabled on Kafka brokers so that monitoring data can be obtained from the brokers.

Transformation Hub Non-Containerized running on Dedicated Nodes



Transformation Hub Non-Containerized running on Kafka Nodes



Installation Prerequisites

Software and system prerequisites

Make sure that you have the following software installed on each system where THNC will be installed:

Operating system	CentOS 7.5 and 7.6, RHEL 7.5 and 7.6
Kafka and ZooKeeper	Confluent 5.1.0 and Apache Kafka 2.1.0-cp1
OpenSSL	Any version of OpenSSL is sufficient. Make sure that the `openssl` command

	can be called from the command line. OpenSSL is used to generate a certificate during installation .
Python	2.7.5

Configuration prerequisites

Make sure that you perform the following configurations :

- Open port 8080 on each system where you will install Transformation Hub Non-Containerized (THNC) and where you plan to connect ArcMC. This port is used by ArcMC to communicate to Transformation Hub Non-Containerized (THNC) .
- Make sure that JMX is enabled on the Kafka cluster so that the Web Service can retrieve metrics from Kafka.
- If you plan to connect ArcMC to Transformation Hub Non-Containerized (THNC) so that you can manage and monitor the Transformation Hub, you will need a copy the ArcMC server certificate, as a *.crt file.
- By default, the scripts that install THNC, configure services, and manage services must be run as root user. Make sure you can connect to each system with this privilege.
- Alternatively, installation and management may be configured with a non-root userid. For more information, see Installation and Configuration with a Non-Root User.

Information needed before you get started

You will be prompted for information during the installation and the services set up interviews. Gather the following information ahead of time to prepare .

Information Needed	Description
Information about your Kafka Installation	You will need to know the host names and port of each system in the cluster where Kafka brokers are running. You will need the hostname and port of all systems in the cluster where ZooKeeper is running.
Password for Self Signed certificate	The Transformation Hub Non-Containerized (THNC) services communicate with each other securely. Self signed certificates are used for this communication. You will be prompted for a password when this certificate is generated.
Kafka JMX port	If you plan to have ArcMC manage and monitor Transformation Hub Non-Containerized (THNC), you will need to configure JMX on all Kafka brokers so that the Transformation Hub Web Service can retrieve metrics from the cluster. You will need to provide the port that was configured as the JMX_PORT.

Information Needed	Description
Choose an Admin username and password	The Transformation Hub Web Service requires admin credentials.
Information about your ArcMC installation	You will need to know the host name and port of the system where ArcMC will be installed. You will also need to obtain the ArcMC server certificate. It must be copied to the THNC system to which ArcMC will connect.
AutoPass Customer License	Obtain your permanent license. Transformation Hub Non-Containerized (THNC) provides a 90 day trial license. You will need to install your own license to continue operation past the 90 day trial period.

Unset the DISPLAY Variable

Prior to installation, you must unset the **DISPLAY** environmental variable. If the variable is set, the installation will hang.

Use the **echo $DISPLAY** command to see the current setting of the **DISPLAY** environment variable:

```
[root@<hostname>]# echo $DISPLAY

localhost:10.0
```

With this setting here is the result of executing the installer:

```
Preparing to install

Extracting the JRE from the installer archive...

Unpacking the JRE...

Extracting the installation resources from the installer archive...

Configuring the installer for this system's environment...

Launching installer...

PuTTY X11 proxy: unable to connect to forwarded X server: Network error:
Connect ion refused

===============================================================

Installer User Interface Mode Not Supported

Unable to load and to prepare the installer in console or silent mode.

===============================================================
```

To enable the installer to perform the installation, unset the **DISPLAY** environment variable:

```
[root@<hostname>]# unset DISPLAY
[root@<hostname>]# echo $DISPLAY
```

Chapter 2: Install Transformation Hub Non-Containerized (THNC)

This section contains the following topics:

THNC Security Considerations

THNC consists of up to 4 components, as follows:

- A REST API server (webservice), used by ArcMC
- A Kafka Schema Registry (schema-registry)
- Zero or more routing servers (route)
- Zero or more CEF-to-Avro stream processors (c2av)

The customer provides the required Kafka brokers (version 2.1.0).

THNC network connections are as follows:

- ArcMC connects to the web service
- Web service connects to ArcMC, Kafka/ZooKeeper, and Schema Registry
- C2AV processors connect to Kafka/ZooKeeper and Schema Registry
- Routing processors connect to Kafka and webservice
- Schema Registry connects to Kafka/ZooKeeper

Note: Each component that connects to Kafka also connects to ZooKeeper, but ZooKeeper currently doesn't support TLS connections.

Planning

Here are some questions to have answers to before beginning the installation.

Is TLS enabled on your Kafka brokers? If yes:

- Is Client Authentication enabled?
- Are your server certificates signed by a Certificate Authority (CA)? If yes, get the CA certificate file. If no, get the broker server certificate from each broker.

TH will use its own CA to sign its certs. Do you want to sign this cert with yours?

This can be done regardless of whether TLS is enabled on Kafka, but if TLS is enabled, the same CA used by the brokers should sign the Transformation Hub's CA. This will allow, for example, Client Authentication to work without importing certificates on the brokers and restarting them.

Installation

Run the THNC installer and answer the prompts according to the decisions made in regards to the planning section above. For Client Authentication, no separate choice is required; however if the TH CA is not signed, then a message will be displayed about importing the TH CA into the Kafka trust stores.

Installation and Configuration with a Non-Root User

THNC includes these scripts which you may want to run as a non-root user.

- The THNC installer script will run as root user by default, or alternatively, as the non-root user by using the `sudo` command:
  `sudo ./ArcSight-TransformationHub-3.0.0.1018.bin`
- The configuration script, which is run after the installer, will prompt for the username and groupname under which the THNC application will be run, which will enable the admin to specify either a root or non-root user for running THNC.
- By default, the service scripts are configured so that when they start, they will run as a non-root user automatically.

Download and Install Transformation Hub Non-Containerized

The following steps install the Transformation Hub Non-Containerized (THNC) files to the system. If you want high availability for the THNC cluster, you must install it on multiple systems. Repeat the following steps on each system in the cluster that will run THNC. You must perform these steps as root user.

1. Download the THNC 3.0.0.1018 Installer from the Micro Focus software entitlement site to the system where you plan to install it.
2. Change to the directory where you downloaded the file.
3. To run the installer as root, enter the command:

   ```
   ./ArcSight-TransformationHub-3.0.0.1018.bin
   ```

   You will see the message start with:

   ```
   Extracting the JRE from the installer archive...

   Unpacking the JRE...
   ```

This first installation prompt provides an explanation about the installation interview that follows.

Note: The THNC installer script will run as root user by default, or alternatively, as the non-root user by using the `sudo` command:
`sudo ./ArcSight-TransformationHub-3.0.0.1018.bin`.

4. Read the License Agreement and Accept the Terms.
5. You will be prompted to define an Installation folder. It is recommended that you use the default folder:

   ```
   /opt/arcsight/TH
   ```

6. Read and confirm information in the Pre-Installation Summary.
7. When complete you will see the following message, with additional instructions about next steps:

   ```
   Congratulations! Transformation Hub Non-Containerized has been
   successfully installed to: /opt/arcsight/TH/current
   ```

   The next steps are to configure the Transformation Hub Non-Containerized (THNC) services.

Configure the Transformation Hub Non-Containerized Services

The following steps guide you through configuring THNC services so that THNC can communicate with Kafka and ZooKeeper, and enable ArcMC to connect to a Web Service instance. Perform these steps on each system where you installed the THNC., as `root` user.

To launch the configuration tool:

```
cd /opt/arcsight/TH/current/
./bin/setup-th
```

Then follow the interview procedure below corresponding to your security mode: Non-TLS, TLS, or Client Authentication. See the following sections.

Security Mode: Non-TLS

- The configuration tool begins.

  ```
  Transformation Hub configuration tool

  ========================================

  This configuration tool will guide you through configuring
Transformation Hub.
  ```

- The installation tool will prompt for a password for the root CA, generated keys, and key stores. Enter and confirm a password.

```
Please provide a password for the root Certificate Authority (CA)

This password will also be used for generated keys and key stores:

Password:

Confirm Password:
```

- Transformation Hub can use a CA-signed certificate or a self-signed certificate to secure its communications. This includes connecting to Kafka in TLS mode. Enter N to self-sign the CA Transformation Hub CA certificate. If you enter Y here, you will use a CA-signed certificate and then be prompted with additional steps to generate the cert files.

```
Do you want to sign the Transformation Hub CA certificate with your own CA [Y/N]? N
```

- When prompted if your Kafka is in TLS mode, enter N (for non-TLS mode).

```
Is your Kafka in TLS mode? [Y/N]

N

Kafka in non-TLS mode
```

- Enter the Kafka endpoints. Provide a comma-separated list of the host name and port for each system in the cluster that runs Transformation Hub. For example:

```
host1.usa.company.com:9092,host2.usa.company.com:9092,host3.usa.company.com:9092
```

- Enter the ZooKeeper endpoint (host:port). Enter the host name and port of the system that runs ZooKeeper. For example:

```
host3.usa.company.com:2181
```

- Enter Kafka JMX port. Kafka JMX is used by the Web Service to retrieve metrics about the installed Kafka brokers. Enter the port that you configured when you enabled JMX on the Kafka cluster. For example:

```
9999
```

- Enter Transformation Hub WebService Admin Password.
- Enter and confirm the WebService Password.

Note: The admin username and password are only used for authentication during communication between the routing stream processor and the web service. These credentials will not be used by a user for any other purpose.

- If you plan to connect to ArcMC, enter Y.

```
Do you want to provide ArcMC host info? [Y/N]

Y
```

- You will be prompted to review and confirm the information provided:

```
Please review the following information regarding Kafka configuration.
```

- You will be prompted to start the configuration.

```
About to install Transformation Hub services to run on boot as user
root? Enter Y or N.
```

- When the configuration is complete, you will see the message:

```
Transformation Hub services installed.
```

For next steps, see Start the THNC Services.

Security Mode: TLS

- The configuration tool begins.

```
Transformation Hub configuration tool

========================================

This configuration tool will guide you through configuring
Transformation Hub.
```

- The installation tool will prompt for a password for the root CA, generated keys, and key stores. Enter and confirm a password.

```
Please provide a password for the root Certificate Authority (CA)

This password will also be used for generated keys and key stores:

Password:

Confirm Password:
```

- Transformation Hub can use a CA-signed certificate or a self-signed certificate to secure its communications. This includes connecting to Kafka in TLS mode. Enter N to self-sign the CA Transformation Hub CA certificate. If you enter Y here, you will use a CA-signed certificate and then be bprompted with additional steps to generate the cert files.

```
Do you want to sign the Transformation Hub CA certificate with your own
CA [Y/N]?

N
```

- When prompted if your Kafka is in TLS mode, enter Y (for TLS mode).

```
Is your Kafka in TLS mode? [Y/N]

Y

Kafka in TLS mode
```

- Enter the Kafka endpoints. Provide a comma-separated list of the host name and port for each system in the cluster that runs Transformation Hub. For example:

```
host1.usa.company.com:9092,host2.usa.company.com:9092,host3.usa.company.com:9092
```

- Enter the ZooKeeper endpoint (host:port). Enter the host name and port of the system that runs ZooKeeper. For example:

```
host3.usa.company.com:2181
```

- Enter Kafka JMX port. Kafka JMX is used by the Web Service to retrieve metrics about the installed Kafka brokers. Enter the port that you configured when you enabled JMX on the Kafka cluster. For example:

```
9999
```

- Enter Transformation Hub WebService Admin Password.
- Enter and confirm the WebService Password.

Note: The admin username and password are only used for authentication during communication between the routing stream processor and the web service. These credentials will not be used by a user for any other purpose.

- If you plan to connect to ArcMC, enter Y.

```
Do you want to provide ArcMC host info? [Y/N]

Y
```

- Enter Transformation Hub services username. Use root.

```
root
```

- Enter Transformation Hub services group name. Use wheel.

```
wheel
```

Note: These entries will cause the script to run as a root user. Alternatively, you may specify a non-root username and group name to run the configuration script as a non-root user.

- You will be prompted to review and confirm the information provided:

```
Please review the following information regarding Kafka configuration.
```

- Place the indicated certificate files in the specified directory (`opt/arcsight/TH/current/cert/kafka`) as shown. When complete, press ENTER to continue.
- Enter and confirm a password for the trust stores. The certificates are imported and added to the trust stores.
- You will be prompted to start the configuration. Enter Y.

```
About to install Transformation Hub services to run on boot as user
```

```
root? Enter Y or N.
```

When the configuration is complete, you will see the message:

```
Transformation Hub services installed.
```

For next steps, see Start the THNC Services.

Security Mode: Client Authentication

- The configuration tool begins.

```
Transformation Hub configuration tool

========================================

This configuration tool will guide you through configuring
Transformation Hub.
```

- The installation tool will prompt for a password for the root CA, generated keys, and key stores. Enter and confirm a password.

```
Please provide a password for the root Certificate Authority (CA)

This password will also be used for generated keys and key stores:

Password:

Confirm Password:
```

- Transformation Hub can use a CA-signed certificate or a self-signed certificate to secure its communications. This includes connecting to Kafka in TLS mode. Enter N to self-sign the CA Transformation Hub CA certificate. If you enter Y here, you will use a CA-signed certificate and then be prompted with additional steps to generate the cert files. If you do not sign the CA certificate, then the client certificate must be imported to each Kafka broker's trust store and the broker must be restarted.

```
Do you want to sign the Transformation Hub CA certificate with your own
CA [Y/N]?
```

- When prompted if your Kafka is in TLS mode, enter Y (for TLS mode).

```
Is your Kafka in TLS mode? [Y/N]

Y

Kafka in TLS mode
```

- Enter the Kafka endpoints. Provide a comma-separated list of the host name and port for each system in the cluster that runs Transformation Hub. For example:

```
host1.usa.company.com:9093,host2.usa.company.com:9093,host3.usa.company.com:9093
```

- Enter the ZooKeeper endpoint (host:port). Enter the host name and port of the system that runs ZooKeeper. For example:

  ```
  host3.usa.company.com:2181
  ```

- Enter Kafka JMX port. Kafka JMX is used by the Web Service to retrieve metrics about the installed Kafka brokers. Enter the port that you configured when you enabled JMX on the Kafka cluster. For example:

  ```
  9999
  ```

- Enter Transformation Hub WebService Admin Username.
- Enter and confirm the WebService Password.

Note: The admin username and password are only used for authentication during communication between the routing stream processor and the web service. These credentials will not be used by a user for any other purpose.

- If you plan to connect to ArcMC, enter **Y.**

  ```
  Do you want to provide ArcMC host info? [Y/N]
  ```

  ```
  Y
  ```

- Enter Transformation Hub services username. Use **root**.

  ```
  root
  ```

- Enter Transformation Hub services group name. Use **wheel**.

  ```
  wheel
  ```

Note: These entries will cause the script to run as a root user. Alternatively, you may specify a non-root username and group name to run the configuration script as a non-root user.

- You will be prompted to review and confirm the information provided:

  ```
  Please review the following information regarding Kafka configuration.
  ```

- Place the indicated certificate files in the specified directory (**opt/arcsight/TH/current/cert/kafka**) as shown. When complete, press ENTER to continue.
- Enter and confirm a password for the trust stores. The certificates are imported and added to the trust stores.
- You will be prompted to start the configuration. Enter **Y.**

  ```
  About to install Transformation Hub services to run on boot as user root? Enter Y or N.
  ```

- When the configuration is complete, you will see the message:

```
Transformation Hub services installed.
```

For next steps, see Start the THNC Services.

Start the Transformation Hub Non-Containerized Services

You can start all services at the same time or start them individually. Services must start in a specific order:

1. Schema Registry
2. Web Service
3. Either the Routing Stream Processor or CEF-to- Avro Stream Processor

If any dependent service fails to start, the downstream service will not start. You must run these scripts as root user.

Procedure

Start all services using one command

1. Change to the /opt/arcsight/TH/current/bin/ directory:

   ```
   cd /opt/arcsight/TH/current/bin/
   ```

2. Run the following command to start all services:

   ```
   ./manage-service start
   ```

3. You will see a confirmation prompt:

   ```
   Transformation Hub Deployment on Kafka

   ========================================

   About to start Transformation Hub Non-Containerized services as user root.

   Are you sure you want to continue? (type YES)
   ```

4. After you enter YES, you will see status output as the individual services start. If a service fails to start you will see the FAILURE status , and the entire start up process will stop .

   ```
   Starting Schema Registry...

   Starting arst-sr (via systemctl):                          [  OK  ]

   Starting Web Service...

   Starting arst-ws (via systemctl):                          [  OK  ]

   Starting Routing Stream Processor...

   Starting arst-route (via systemctl):                       [  OK  ]

   Starting CEF to AVRO Transforming Stream Processor...
   ```

```
Starting arst-c2av (via systemctl):                        [  OK  ]

Transformation Hub Non-Containerizedservices started.
```

5. Check that the services are running by running the command:

   ```
   ./manage-service status
   ```

Start one service at a time

You can start a single service using the following commands. You must execute these commands as root user.

Command	Description
`systemctl start arst-sr`	Starts the Schema Registry service.
`systemctl start arst-ws`	Starts the Web Service.
`systemctl start arst-c2av`	Starts the CEF to AVRO Stream Processor service
`systemctl start arst-route`	Starts the Routing Stream Processor service

Stop the Transformation Hub Non-Containerized Services

This procedure explains how to stop the Transformation Hub Non-Containerized services. You can stop all services at the same time or stop them individually. You must run these commands as root user.

Stop all services using one command

- Change to the /opt/arcsight/thnc/current/bin/ directory:

  ```
  cd /opt/arcsight/TH/current/bin/
  ```

- Run the following command to stop all services:

  ```
  ./manage-service stop
  ```

Stop one service at a time

You can stop an individual service using the following commands.

Command	Description
`systemctl stop arst-sr`	Stops the Schema Registry service.
`systemctl stop arst-ws`	Stops the Web Service.
`systemctl stop arst-c2av`	Stops the CEF to AVRO Stream Processor service

`systemctl stop arst-route`	Stops the Routing Stream Processor service

<ToDo: add the output>

Check the status of the Transformation Hub Non-Containerized Services

This section explains how to check the status of Transformation Hub Non-Containerized Services. You must run these scripts as `root` user.

View the status of all services using one command

1. Change to the /opt/arcsight/thnc/current/bin/ directory:

   ```
   cd /opt/arcsight/TH/current/bin/
   ```

2. Run the command

   ```
   ./manage-service status
   ```

View the status of an single service

You can view the status of a single service using the following commands.

Command	Description
`systemctl status arst-sr`	View the status of the Schema Registry service.
`systemctl status arst-ws`	View the status of the Web Service.
`systemctl status arst-c2av`	View the status of the CEF to AVRO Stream Processor service
`systemctl status arst-route`	View the status of the Routing Stream Processor service

Install Your Customer License

Transformation Hub Non-Containerized (THNC) comes packaged with a 90-day trial license. ***To ensure continuity of event flow, make sure to install the license you received as part of the license activate process before the 90-day trial period ends.*** The check for a valid license happens during the start up process for the c2av, routing, web service, and schema registry services. All services look for the license file in the same location under the installation directory of that instance.

After you receive your Transformation Hub license file (or if you already have the legacy ADP license file):

1. Rename the file to *license.xml*.
2. Connect to each system that runs Transformation Hub Non-Containerized (THNC) and copy the license file to the `/opt/arcsight/TH/current/config/autopass/` directory. This directory is created when the THNC services are started for the first time. If you do not see the directory,start the Transformation Hub NC services and then recheck for the directory.

   If you have installed multiple THNC instances, copy the license file to each instance under the same installation sub-directory.
3. Restart the c2av, routing, web service, and schema registry services. You must restart the services each time you change the license.

   Note: The THNC license check can be found at `/opt/arcsight/TH/current/logs/license.log`

Connect ArcMC to Transformation Hub Non-Containerized

ArcMC can connect to one system in a THNC cluster at a time. If the system that ArcMC is connected to fails, then you will need to reconfigure ArcMC to connect to another system in the cluster.

Import ArcMC Certificate to the Transformation Hub Non-Containerized (THNC) system

- Get a copy of the ArcMC server certificate , with the extension *.crt from the system where ArcMC is running.
- Copy the ArcMC certificate file to the system where ArcMC will connect, under the /opt/arcsight/TH/current/cert/webservice/ directory.
- Restart the services to apply the certificate.

Connect ArcMC to Transformation Hub Non-Containerized (THNC)

See the ArcMC Administrator Guide for instructions about how to Add a Host in ArcMC.

Adding Transformation Hub Non-Containerized (THNC) as a Host

To add THNC as a managed host:

On 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 in /opt/arcsight/TH/current/cert/webservice/ directory.
4. Restart the THNC services.
5. In ArcMC, go to **Node Management > View All nodes**

6. From the left navigation tree, select the location where you want to add the THNC.
7. Click **Add Host**.
8. In the **Hostname/IP** field, type the fully qualified name of the THNC.
9. In the **Type** field, select **Transformation Hub - Non-Containerized Deployment.**
10. In the **Port** field, type 8080 and click **Add**.

Chapter 3: Managing THNC

The following topics describe the management of THNC. For a more complete description of THNC administration, see the Transformation Hub Administrator's Guide, available from the Micro Focus software community.

This section contains the following topics:

Uninstalling the Transformation Hub Non-Containerized Service

The following steps will uninstall the THNC instance from the system. This process does not remove the Kafka topics created by the web service. To remove Kafka topics, you must manually delete them. See the Apache Kafka documentation for information on deleting topics.

Note: Run the uninstallation script as root user.

To uninstall THNC:

1. Change to the following directory:
   `cd /opt/arcsight/TH/current/UninstallerData/`
2. Remove the services:
   `./manage-service remove`
3. Run the command:
   `./Uninstall_ArcSight_TH`

Troubleshooting the Transformation Hub Non-Containerized instance

This section provides the mechanisms you can use to troubleshoot issues you may encounter with Transformation Hub Non-Containerized (THNC).

There are two mechanisms you can use to investigate issues:

- To check the status of services, see Checking the status of the Transformation Hub NC service.
- You can also view Transformation Hub Non-Containerized (THNC) logs under `/opt/arcsight/TH/current/logs` directory.

Configuring the C2AV (CEF-to-Avro) Stream Processor

For THNC, the configuration properties file for C2AV (CEF to Avro) stream processor is in the `etc/route` directory of the Transformation Hub installation. The properties file name is `stream.properties`.

After installation and setup have been completed, the c2av stream processor has one instance configured. In the `stream.properties` file,v the key/value pair is:

```
service.instance.count=1
```

To change the number of c2av instances configured, edit the file and change the `service.instance.count` value to the desired number of instances. A larger number of instances can handle higher event rates.

Each c2av stream processor has its own log file in the logs directory of the TH installation. The stream processor instance number is part of the file name. For example, if three instances have been configured the following files will be in the logs directory:

```
c2av.1.log

c2av.2.log

c2av.3.log
```

Configuring Stream Processor Groups

For THNC, the configuration properties files for the ten routing stream processor groups are in the `etc/route` directory of the TH installation. The properties files are:

```
th-routing-processor-group1.properties

th-routing-processor-group2.properties

...

th-routing-processor-group10.properties
```

After installation and setup have been completed, the routing group 1 has one instance configured. In the `th-routing-processor-group1.properties` properties file, the key/value pair is:

```
service.instance.count=1
```

For the other groups, no instances are configured. So in the properties file, the key/value pair is:

```
service.instance.count=0
```

To change the number of instances configured for a given group, edit the file and change the `service.instance.count` value to the desired number of instances. A larger number of instances can handle higher event rates.

Configuration of routes and rules can be done in the ArcSight Management Center using the **Configuration Management | Transformation Hub** menu item. A new route is configured by entering

the **Route Name, Source Topic, Destination Topic** and **Description**. The associated routing rules are configured by entering the **Field, Operator and Value.**

To display the configured rules:

```
curl --noproxy 127.0.0.1 -k -u <TH username:password>
https://127.0.0.1:8080/routing/rule
```

To display the configured routes:

```
curl --noproxy 127.0.0.1 -k -u <TH username:password>
https://127.0.0.1:8080/routing/route
```

To display the registry:

```
curl --noproxy 127.0.0.1 -k -u <TH username:password>
https://127.0.0.1:8080/service/registry
```

To display the mappings:

```
curl --noproxy 127.0.0.1 -k -u <TH username:password>
https://127.0.0.1:8080/service/mapping
```

Example output for these commands:

```
[root@host current]#  curl --noproxy 127.0.0.1 -k -u "admin:atlas"
https://127.0.0.1:8080/routing/rule

{

"rules" : [ {

"field" : "cat",

"id" : "RULE_1",

"name" : "Rule One",

"operator" : "contains",

"value" : "Firewall"

}, {

"id" : "RULE_2",

"ruleExpression" : "(cat.contains('Firewall'))"

}, {

"id" : "RULE_3",
```

```
"ruleExpression" : "(deviceVendor == 'Intel')"

}, {

"id" : "RULE_4",

"ruleExpression" : "(deviceProduct == 'A-One')"

} ]

}

[root@<hostname> current]# curl --noproxy 127.0.0.1 -k -u "admin:atlas"
https://127.0.0.1:8080/routing/route

{

"routes" : [ {

"description" : "added via ArcMC",

"id" : "ROUTE_2",

"name" : "Route One",

"rule" : "RULE_2",

"source" : "th-cef",

"target" : "th-cef-other"

}, {

"description" : "My second route added via ArcMC",

"id" : "ROUTE_3",

"name" : "Route Two",

"rule" : "RULE_3",

"source" : "TestTopic-A",

"target" : "TestTopic-B"

}, {

"description" : "Third route added via ArcMC",

"id" : "ROUTE_4",

"name" : "Route Three",

"rule" : "RULE_4",
```

```
"source" : "th-cef",
"target" : "th-cef-other"
} ]
}
[root@<host> current]# curl --noproxy 127.0.0.1 -k -u "admin:atlas"
https://127.0.0.1:8080/service/registry
{
"services" : [ {
"capability" : "ROUTING",
"id" : "SERVICE_1",
"serviceAttributes" : { },
"serviceGroup" : "TH_CEF_TEXT_ROUTING_GROUP_1",
"serviceName" : "TH_CEF_ROUTING_SERVICE_1"
}, {
"capability" : "ROUTING",
"id" : "SERVICE_2",
"serviceAttributes" : { },
"serviceGroup" : "TH_CEF_TEXT_ROUTING_GROUP_2",
"serviceName" : "TH_CEF_ROUTING_SERVICE_2"
}, {
"capability" : "ROUTING",
"id" : "SERVICE_3",
"serviceAttributes" : { },
"serviceGroup" : "TH_CEF_TEXT_ROUTING_GROUP_4",
"serviceName" : "TH_CEF_ROUTING_SERVICE_4"
}, {
"capability" : "ROUTING",
"id" : "SERVICE_4",
```

```
"serviceAttributes" : { },
"serviceGroup" : "TH_CEF_TEXT_ROUTING_GROUP_3",
"serviceName" : "TH_CEF_ROUTING_SERVICE_3"
} ]
}
[root@<host> current]# curl --noproxy 127.0.0.1 -k -u "admin:atlas"
htps://127.0.0.1:8080/service/mapping
{
"mapping" : {
"TH_CEF_TEXT_ROUTING_GROUP_1" : "th-cef",
"TH_CEF_TEXT_ROUTING_GROUP_2" : "TestTopic-A"
},
"mapped" : [ {
"SERVICE_1" : {
"routes" : [ {
"source" : "th-cef",
"target" : "th-cef-other",
"rule" : "(cat.contains('Firewall'))"
}, {
"source" : "th-cef",
"target" : "th-cef-other",
"rule" : "(deviceProduct == 'A-One')"
}, {
"source" : "th-cef",
"target" : "TestTopic-H",
"rule" : "(deviceVendor == 'Intel')"
} ]
}
```

```
}, {
"SERVICE_2" : {
"routes" : [ {
"source" : "TestTopic-A",
"target" : "TestTopic-B",
"rule" : "(deviceVendor == 'Intel')"
} ]
}
} ],
"unmapped" : [ "SERVICE_3", "SERVICE_4" ],
"unmappedSources" : [ ]
}
```

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 Deployment Guide (Transformation Hub Non-Containerized (THNC) 3.0.0)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!