ArcSight Command Center for ESM 7.3

Administrator's Guide

July 2020

Legal Notice

Contents

About This Book

This *Administrator's Guide* provides information about deploying, configuring, and managing ArcSight Command Center for ESM (ESM for Fusion). Some applications that are deployed in the ArcSight Platform require Fusion, and their individual installation guides might also include instructions for Fusion deployment.

Intended Audience

This book provides information for IT administrators who are responsible for managing the ESM for Fusion software and its environment. Usually, these individuals have experience in configuring servers and managing SIEM-related applications.

Additional Documentation

The ESM for Fusion documentation library includes the following resources:

- *User Guide for Fusion*, which is embedded in the product to provide both context-sensitive Help and conceptual information
- *Technical Requirements for ArcSight Command Center for ESM*, which provides information about the hardware and software requirements for installing ESM for Fusion
- *Release Notes for ArcSight Enterprise Security Manager*, which provides information about the latest release

For the most recent version of this guide and other Enterprise Security Manager documentation resources, visit the documentation site for ArcSight web page.

Contact Information

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

For specific product issues, contact Micro Focus Customer Care at https://www.microfocus.com/support-and-services/.

1 Understanding Command Center for ESM

Micro Focus provides a platform that enables you to deploy a combination of security, user, and entity solutions into a single Container Deployment Foundation (CDF) environment. The platform's browser-based interface gives users fast access to the ArcSight suite of products that you have deployed. A common layer called **Fusion** provides the core services for this CDF environment, including the Dashboard, user management, and single sign-on configuration. The Dashboard enables users to visualize, identify, and analyze potential threats by incorporating intelligence from the multiple layers of security sources that might be installed in your security environment, such as:

- Real-time event monitoring and correlation with data from ArcSight Enterprise Security Manager (ESM)
- Analyzing end-user behavior with ArcSight Interset
- Performing deep-dive investigations with ArcSight Recon

Deploying **ArcSight Command Center for ESM** (ESM for Fusion) in this platform incorporates the dashboards and some functions of the ArcSight Command Center console. Users will be able to run and review searches, reports, and case management, as well as perform administrative functions for managing active channels, content, connectors, storage, archives, search filters, saved searches, peer configuration, and system logs. For the Dashboard, ESM for Fusion adds several widgets that display data from your ESM sources. If you also deploy the Layered Analytics capability, widgets such as the Active Lists widget can incorporate data from both ESM and Interset for greater insights. If you want to create widgets specific for your organization, you can build them in the Widget SDK.

NOTE: The Command Center console deployed with ESM for Fusion is separate from the Command Center console that you might have installed with previous versions of ESM.

ESM for Fusion scales to match the footprint of your environment. You can install ESM for Fusion on the same server as ESM, if there are enough spare resources on the server, or install on multiple servers.

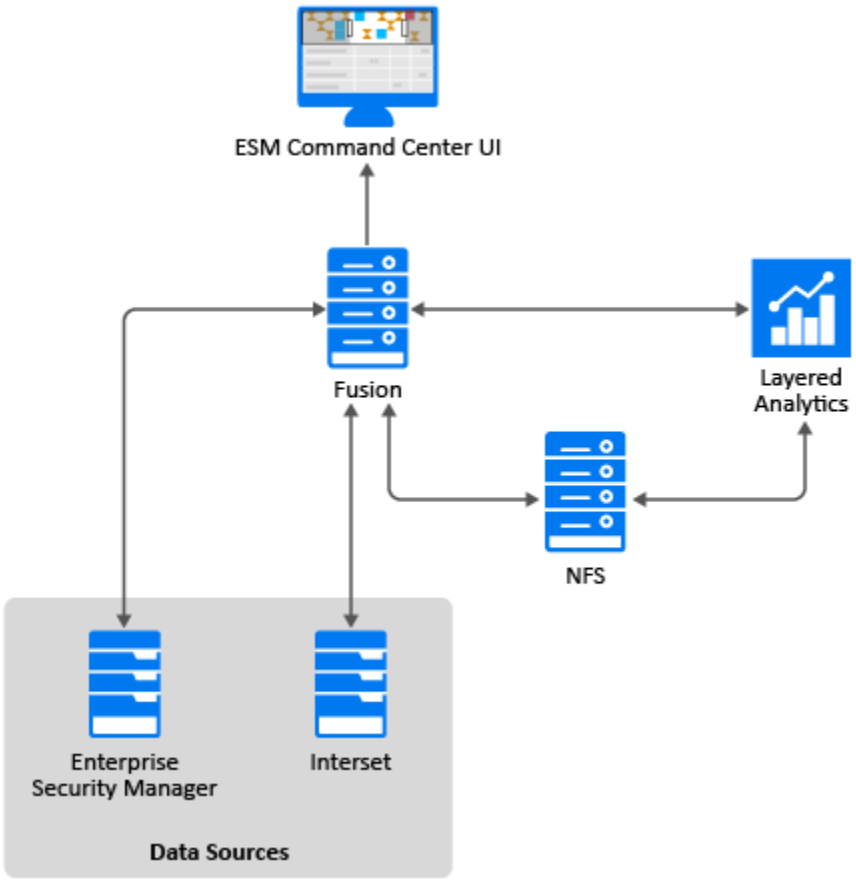
For information about using this product, see the Help embedded in the product or posted with the documentation for Fusion.

- "Understanding the ESM for Fusion Architecture" on page 10
- "Understanding the ESM for Fusion Components" on page 10

Understanding the ESM for Fusion Architecture

The ESM for Fusion environment incorporates several components that enable it to receive and display data from sources such as ESM. The following diagram helps you understand the software and components that comprise your ESM for Fusion environment.

Figure 1-1 *ESM for Fusion Architecture*



Understanding the ESM for Fusion Components

The ESM for Fusion environment incorporates the following components:

Enterprise Security Manager

ArcSight Enterprise Security Manager serves as the primary data source for the the Dashboard and the Command Center console in ESM for Fusion.

Interset

Required if you want to use Layered Analytics

ArcSight Interset is an optional component that you can deploy for access to unsupervised machine learning and probabilistic risk assessments based on behavioral analytics from millions of events.

Data Sources

Provide data to ESM for Fusion for display in the Dashboard and Command Center dashboards and searches.

Fusion

Fusion provides the Dashboard, user management, single sign-on, and other core services that give the deployed components a unified solution experience. Most deployed components require Fusion.

Layered Analytics

Optional

Layered Analytics blends the analytics results from some of the capabilities deployed with ESM for Fusion, thus providing multiple layers of useful data that can lead to actionable insights. To use this capability, you must deploy both ArcSight Interset and ESM for Fusion in the same cluster.

Network File System (NFS)

NFS stores some of the persistent data generated by ESM for Fusion and ArcSight Interset. Container Deployment Foundation (CDF) requires an NFS server to maintain state information about the infrastructure and to store other pertinent data.

Planning Installation and Deployment

This section helps you plan the installation and deployment of ESM for Fusion. Some components must be installed in a specific order because the process requires access to previously installed components.

2 Installation Checklist

As part of your planning process, we recommend that you perform the tasks in this checklist in the order listed below. To upgrade from a previous version of Fusion, see Chapter 17, “Upgrading ESM for Fusion,” on page 81.

	Checklist Items
❑	1. Review the description of the installation process. For more information, see Chapter 3, “Understanding the Installation Process,” on page 17.
❑	2. Ensure that the computers, on which you are installing ESM for Fusion components, meet the specified hardware and software requirements. For more information, see the *Technical Requirements for ArcSight Command Center for ESM*.
❑	3. Review the ports required for the installed and connected components. For more information, see “Ports Used” in the *Technical Requirements for ArcSight Command Center for ESM*.
❑	4. Review the limitations and options associated with the installation. For more information, see Chapter 3, “Understanding the Installation Process,” on page 17.
❑	5. (Conditional) If installing ESM and ESM for Fusion on the same node, add the ESM port to the firewall. For more information, see Chapter 5, “Installing ESM for Fusion and ESM on the Same Node,” on page 23.
❑	6. Download the files for installing ESM for Fusion. For more information, see the *Release Notes for ArcSight Enterprise Security Manager*.
❑	7. (Conditional) Install or upgrade your ESM environment before deploying or upgrading ESM for Fusion. For more information, see the *Installation Guide for ArcSight Enterprise Security Manager*.
❑	8. (Conditional) If installing all components on a single system, run the preparation script. For more information, see Chapter 6, “Preparing Your Environment,” on page 27.
❑	9. Install ESM for Fusion: ◆ Chapter 7, “Installing ESM for Fusion by Using Scripts,” on page 29 ◆ Chapter 8, “Installing ESM for Fusion Manually,” on page 31 ◆ Chapter 9, “Deploying ESM for Fusion in an Existing Cluster,” on page 55
❑	10. Log in to ESM for Fusion to create the first administrative user. For more information, see Chapter 11, “Verifying the Installation,” on page 63.

	Checklist Items
❑	11. Connect ESM for Fusion to your data sources: ◆ Chapter 12, “Integrating Data and Users from Enterprise Security Manager,” on page 67 ◆ Chapter 13, “Integrating Data from Interset,” on page 71
❑	12. Enable users to access ESM for Fusion: ◆ Add or import users and groups ◆ Create roles ◆ Assign permissions For more information, see the *User Guide for Fusion*, which is also the context-sensitive Help in the product.
❑	13. Create and share dashboards. For more information, see the *User Guide for Fusion*, which is also the context-sensitive Help in the product.

3 Understanding the Installation Process

ESM for Fusion is a container-based application. To deploy and manage ESM for Fusion, you must first install the **Container Deployment Foundation (CDF)**, which is a container and management module built on Kubernetes and Docker containers. You can deploy the components for ESM for Fusion either on a single-node or multi-node cluster setup.

If you already have the ArcSight Platform installed, you can deploy ESM for Fusion to the same cluster. Reusing existing clusters allows you to reduce costs and system management effort, when compared to deploying ESM for Fusion in a new cluster.

Components Needed for Deployment

The installation process deploys the following components:

- Command Center
- Fusion
- Layered Analytics (optional)

Methods of Deployment

You can deploy ESM for Fusion on one or more nodes, depending on the anticipated workload, and whether high availability deployment is required. The supported methods of deployment are:

Single-Node Deployment

The single-node deployment method allows you to deploy all of the ESM for Fusion components on a single node. This method of deployment is suitable only for small workloads and where you do not need high availability. You can use the provided scripts, which prepare your environment, install the CDF, and deploy ESM for Fusion.

Multi-Node Deployment

For larger workloads, we recommend deploying ESM for Fusion in a multi-node cluster setup. The multi-node deployment method provides load balancing across several worker nodes and is scalable to handle large workloads. You can add multiple master nodes and worker nodes to scale. A multi-node deployment with three master and three worker nodes can be configured for HA support.

NOTE: Although, you can add worker nodes even after the installation, you can add master nodes only during the installation. Plan your deployment carefully before you start the installation process.

High Availability Deployment

For high availability deployment, you must set up a minimum of three master and three worker nodes, so that even in cases where two nodes are unavailable, the third node is still available. When only two master nodes are used, and the primary master node is offline for maintenance or upgrade, only a single master node remains available, which creates a single point of failure. If the available single master node fails, the cluster stops and cluster orchestration will not be possible until the master is back online.

NOTE: Although, you can add worker nodes even after the installation, you can add master nodes only during the installation. Plan your deployment carefully before you start the installation process.

Securing Communication Between Components

Determine the security mode (TLS/SSL) you want for establishing communication between the infrastructure components. The security mode must be the same across all components. Set up other Micro Focus components with the security mode you intend to use before connecting them.

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

Changing the security mode after the deployment requires system downtime. If you do need to change the security mode after deployment, refer to the appropriate *Administrator's Guide* for the relevant component.

The following table lists Micro Focus components, preparations needed for secure communication with components, security modes, and where to find more information about the component.

Communication	Preparations needed...	Supported security modes
ESM for Fusion to NFS Server	For optimal security, secure all NFS settings to allow only required hosts to connect to the NFS server.	
Web browser to NGINX (proxy)	No action is required.	TLS/SSL

Enabling FIPS in Nginx: No user action is required to enable FIPS for Nginx. The Nginx docker container is FIPS enabled by default. The FIPS-enabled Nginx server accepts TLS 1.2 connections using FIPS-compliant Cipher Suites.

4 Installation Options

You can install ESM for Fusion either by using the provided installation scripts or manually.

Installation Using Scripts

To enable an easier installation, ESM for Fusion provides scripts that automatically take care of all the prerequisites, software installations, and post-installation configurations. The scripts are applicable for single-node deployments where high availability is not needed. However, if you prefer to manually set the configurations and the installations because of your organization's security policies, you can install ESM for Fusion manually in single-node deployments as well. The scripts configure the system to match the settings described for performing a manual installation.

The installation scripts require your environment to be in a specific state. Before deciding to use the installation scripts, review the considerations for installation.

For information about installing ESM for Fusion by using scripts for a single-node deployment, see Chapter 7, "Installing ESM for Fusion by Using Scripts," on page 29.

Manual Installation

In deployments with a larger workload where high availability is a requirement, you must manually perform all the necessary system configurations and software installations. However, you can use some of the installation scripts to make your tasks easier, then complete the rest of the configurations and installations manually.

For information about installing ESM for Fusion manually, see Chapter 8, "Installing ESM for Fusion Manually," on page 31.

Deciding to Use the Scripts or Manual Installation Method

To determine whether to use the installation scripts or perform a manual installation, review the following considerations:

- The scripts install ESM for Fusion on the operating system with a default minimum installation. If you have any customizations on the operating system, we recommend that you perform the prerequisites manually and perform installation and post-installation configuration using scripts.

NOTE: When installing ESM for Fusion on the same machine as the ESM Manager, the installation scripts require that the ESM is installed on the system before running the installation scripts.

- The scripts install ESM for Fusion only on a singled-homed network (one that is connected with a single network link). If you have a dual-homed network (dual or redundant connections to a single Internet Service Provider), we recommend that you use the manual installation process.
- The scripts automatically tune the system for a single-node deployment with a small workload.
- The scripts install the cluster with a single master node and single worker node running on the same system. You can add worker nodes after the installation to scale and enable worker high availability.
- If you use the scripts, you cannot configure high availability for the master node. If you want high availability for the master node, we recommend that you use the manual installation process.
- The scripts disable the option to authorize Micro Focus to collect suite usage data.
- The scripts create NFS shares on the system used by the containers in the cluster. They configure the firewall to disable remote access to this NFS server. If you plan to add additional nodes to the cluster, you must enable remote access to the NFS server in the firewall.
- The scripts use the following paths by default:
  - To install Kubernetes: `/opt/kubernetes`
  - To create NFS shared directories: `/opt/NFS_Volume/`
- If you must use proxy in your environment, you must use the manual installation process.

5 Installing ESM for Fusion and ESM on the Same Node

You can install ESM for Fusion on the same node as ESM, either manually or by using scripts.

1 Install ESM.

NOTE: Always install ESM before installing ESM for Fusion and CDF.

2 Add the ESM https port in iptables using the following commands:

2a To find your active zones, use the following command:

```
firewall-cmd --get-active-zones
```

2b To add the ESM port in iptables, use the following command:

```
firewall-cmd --zone=public --add-port=port_number/tcp --permanent
```

NOTE: This step enables you to access ESM externally (outside the firewall).

2c To reload the firewall so that the changes are applied, use the following command:

```
firewall-cmd --reload
```

3 Install ESM for Fusion.

For more information, see Chapter 7, “Installing ESM for Fusion by Using Scripts,” on page 29 and Chapter 8, “Installing ESM for Fusion Manually,” on page 31.

NOTE: While installing ESM for Fusion, specify a CDF API Server Port that does not use the same port as the ESM server (default 8443). For more information about ESM for Fusion ports, see the *Technical Requirements for ArcSight Command Center for ESM*.

II Installing CDF and Deploying ESM for Fusion

This section provides guidance for installing all components that are required to deploy ESM for Fusion in your environment.

6 Preparing Your Environment

We provide the following script that prepares your environment to install all components on a single system:

```
./prepare-install-single-node-host.sh
```

For more information, see Chapter 7, “Installing ESM for Fusion by Using Scripts,” on page 29.

7 Installing ESM for Fusion by Using Scripts

You can use the installation scripts to install ESM for Fusion on a single node. The installation scripts perform end-to-end installation starting from configuring prerequisites to completing post-installation configurations. For more information on running the scripts successfully, see Chapter 8, "Installing ESM for Fusion Manually," on page 31.

Prerequisites

Ensure that your environment meets the hardware and software requirements described in the *Technical Requirements for Command Center for ESM*.

Understanding the Installation Scripts

The installation scripts automatically take care of all the prerequisites, software installations, and post-installation configurations.

Script	Purpose
`./prepare-install-single-node-host.sh`	Installs all the necessary packages and configures the prerequisites
`./install-single-node.sh`	Installs ArcSight Command Center for ESM
`./install-single-node-post.sh`	Performs post-installation configurations, such as labeling the nodes

Using the Installation Scripts

IMPORTANT: The information in this section applies only when your deployment does not need high availability.

To install ESM for Fusion by using the scripts:

1. Log in to the master node as `root`.
2. Change to the directory where you downloaded the ESM for Fusion installation files. For example:

   ```
   cd /opt
   ```

For information about downloading the ESM for Fusion installation files, see “Downloading Fusion” in the *Release Notes for ArcSight Enterprise Security Manager*.

3 Extract the downloaded ESM for Fusion installation files using the following command:

```
tar zxvf esm-cmd-center-installer-for-fusion-7.3.0.x.tar.gz
```

4 Execute the scripts in the following order:

4a `./prepare-install-single-node-host.sh`

4b `./install-single-node.sh`

4c `./install-single-node-post.sh`

8 Installing ESM for Fusion Manually

This chapter provides information about manually installing ESM for Fusion and the required software.

Preparing Your Environment for CDF

The procedures in this section enable you to configure your environment for a successful installation of the Container Deployment Foundation (CDF).

Configuring the Nodes

For multi-node deployment, consider the following when configuring master and worker nodes:

- Deploy master and worker nodes on virtual machines. Since most of the processing occurs on worker nodes, we recommend that you deploy worker nodes on physical servers.
- Keep the host system configuration identical across master and worker nodes.
- When using virtual machines, ensure that:
  - Resources are reserved and not shared
  - UUID and MAC addresses are static because dynamic addresses cause the Kubernetes cluster to fail

- Install all master and worker nodes in the same subnet.
- Add more worker nodes rather than installing bigger and faster hardware.

  Using more worker nodes enables you to perform maintenance on your cluster nodes with minimal impact to uptime. Adding more nodes also helps with predicting costs due to new hardware.

For high availability, consider the following when configuring master and worker nodes:

- Create a virtual IP that is shared by all master nodes and ensure that virtual IP is under the same subnet. The VIP must not respond when pinged before you install ESM for Fusion.
- Install all master and worker nodes in the same subnet.

Setting System Parameters (Network Bridging)

Ensure that the `br_netfilter` module is installed on all master and worker nodes before changing system settings.

You can either run the following scripts that set system parameters automatically or you can set the system parameters manually:

- `/opt/<ESM_Command_Center_Installer_For_Fusion>/scripts/prereq_sysctl_conf.sh`
- `/opt/<ESM_Command_Center_Installer_For_Fusion>/scripts/prereq_rc_local.sh`

Perform the following steps on all the master and worker nodes to set the system parameters manually.

1. Log in to the master node.
2. Check whether the `br_netfilter` module is enabled:

   ```
   lsmod |grep br_netfilter
   ```
3. If there is no return value and the `br_netfilter` module is not installed, install it:

   ```
   modprobe br_netfilter
   echo "br_netfilter" > /etc/modules-load.d/br_netfilter.conf
   ```
4. Open the `/etc/sysctl.conf` file.
5. Ensure that the following system parameters are set:

   ```
   net.bridge.bridge-nf-call-iptables=1
   net.bridge.bridge-nf-call-ip6tables=1
   net.ipv4.ip_forward = 1
   net.ipv4.tcp_tw_recycle = 0
   kernel.sem=50100 128256000 50100 2560
   ```
6. Save the `/etc/sysctl.conf` file.
7. Apply the updates to the node:

   ```
   /sbin/sysctl -p
   ```
8. Repeat these steps for worker node.

Checking MAC and Cipher Algorithms

To configure MAC and Cipher algorithms manually, ensure that the `/etc/ssh/sshd_config` files on every master and worker node are configured with at least one of the following values, which lists all supported algorithms. Add only the algorithms that meet the security policy of your organization.

- For MAC algorithms: `hmac-sha1,hmac-sha2-256,hmac-sha2-512,hmac-sha1-96`
- For Cipher algorithms: `3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr,arcfour128,arcfour256,blowfish-cbc`

For example, you could add the following lines to the /`etc/ssh/sshd_config` file on all master and worker nodes:

```
MACs hmac-sha2-256,hmac-sha2-512

Ciphers aes128-cbc,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr
```

Checking Password Authentication Settings

If you plan to use a user name and password authentication for adding cluster nodes during the installation, ensure that the `PasswordAuthentication` parameter in the `/etc/ssh/sshd_config` file is set to `yes`. There is no need to check the password authentication setting when you add cluster nodes using a user name and key authentication.

To ensure that the password authentication is enabled, perform the following steps on every master and worker node.

1. Log in to the master node.
2. Open the `/etc/ssh/sshd_config` file.
3. Check whether the `PasswordAuthentication` parameter is set to `yes`. If not, set the parameter to `yes` as follows:

   ```
   PasswordAuthentication yes
   ```

4. Restart the `sshd` service:

   ```
   systemctl restart sshd.service
   ```

5. Repeat these steps for each worker node.

Installing the Required Operating System Packages

Ensure that the packages listed in the following table are installed on appropriate nodes. These packages are available in the standard `yum` repository.

Package	Nodes
`device-mapper-libs`	Master and worker
`java-1.8.0-openjdk`	Master
`libgcrypt`	Master and worker
`libseccomp`	Master and worker

Package	Nodes
libtool-ltdl	Master and worker
net-tools	Master and worker
nfs-utils	Master and worker
rpcbind	Master node, worker node, and NFS server
systemd-libs (version >= 219)	Master and worker
unzip	Master and worker
httpd-tools	Master and worker
conntrack-tools	Master and worker
lvm2	Master and worker
curl	Master and worker
libtool-libs	Master and worker
openssl	Master and worker
socat	Master and worker
container-selinux	Master and worker

You can either run the `/opt/<ESM_Command_Center_Installer_For_Fusion>/scripts/prereq_1_required_packages.sh` script that installs the required OS packages automatically or install the required OS packages manually.

To install the packages manually:

1. Log in to the master or worker nodes.
2. Verify whether the package exists:

   `yum list installed <package name>`
3. (Conditional) If the package is not installed, install the required package:

   `yum -y install <package name>`

Removing Libraries

Remove libraries that prevent Ingress from starting and confirm the removal when prompted:

```
yum remove rsh rsh-server vsftpd
```

Configuring Time Synchronization

You must implement a Network Time Protocol (NTP) to synchronize time on all nodes in the cluster. To implement this protocol, use chrony. Ensure that chrony is running on all nodes in the cluster. By default chrony is installed on some versions of RHEL.

You can either run the `/opt/<ESM_Command_Center_Installer_For_Fusion>/scripts/prereq_synchronize_time.sh` script that synchronizes time automatically or configure the time synchronization manually.

To configure the time synchronization manually:

1. Verify chrony configuration:

   ```
   chronyc tracking
   ```

2. (Conditional) If chrony is not installed, install chrony:

   ```
   yum install chrony
   ```

3. Start and enable chrony:

   ```
   systemctl start chronyd
   systemctl enable chronyd
   ```

4. Synchronize the operating system time with the NTP server:

   ```
   chronyc makestep
   ```

5. Restart the chronyd daemon:

   ```
   systemctl restart chronyd
   ```

6. Check the server time synchronization:

   ```
   timedatectl
   ```

7. Synchronize the hardware time:

   ```
   hwclock -w
   ```

Configuring the Firewall

Ensure that the `firewalld.service` is enabled and running on all nodes.

You can either run the `/opt/<ESM_Command_Center_Installer_For_Fusion>/scripts/prereq_firewall.sh` script that configures the firewall automatically or configure the firewall manually.

When the firewall is enabled, you must also enable the masquerade settings.

To enable masquerade settings:

1. Check whether the masquerade setting is already enabled:

   ```
   firewall-cmd --query-masquerade
   ```

   If the command returns `yes`, then masquerade is enabled.

   If the command returns `no`, then masquerade is disabled.

2 (Conditional) If the masquerade setting is not enabled, enable masquerade:

```
firewall-cmd --add-masquerade --permanent
firewall-cmd --reload
```

Configuring Proxy

Ensure that the cluster should have no access to the Internet and that the proxy settings (`http_proxy`, `https_proxy`, and `no_proxy`) are not set. However, if a connection with the Internet is needed and you already specified a proxy server for http and https connection, you must correctly configure `no_proxy`.

If you have the `http_proxy` or `https_proxy` set, then `no_proxy` definitions must contain at least the following values:

`no_proxy=localhost, 127.0.0.1, <all Master and Worker cluster node IP addresses>,<all cluster node FQDNs>,<HA virtual IP Address>,<FQDN for the HA Virtual IP address>`

For example:

- `export http_proxy="http://web-proxy.example.net:8080"`

  `export https_proxy="http://web-proxy.example.net:8080"`

  ```
  export
  no_proxy="localhost,127.0.0.1,node1.swinfra.net,10.94.235.231,node2.sw
  infra.net,10.94.235.232,node3.swinfra.net,10.94.235.233,node3.swinfra.
  net,10.94.235.233,node4.swinfra.net,10.94.235.234,node5.swinfra.net,10
  .94.235.235,node6.swinfra.net,10.94.235.236,ha.swinfra.net
  10.94.235.200"
  ```

- `export http_proxy="http://web-proxy.eu.example.net:8080"`

  ```
  export
  https_proxy="localhost,127.0.0.1,swinfra.net,10.94.235.231,10.94.235.2
  32,10.94.235.233,10.94.235.233,10.94.235.234,10.94.235.235,10.94.235.2
  36,10.94.235.200"
  ```

NOTE: Incorrect configuration of proxy settings has proven to be a frequent installation problem. To verify that proxy settings are configured properly on all master and worker nodes, run the following command and ensure that the output corresponds to the recommendations:

```
echo $http_proxy, $https_proxy, $no_proxy
```

If the firewall is turned off, the installation process will generate a warning. To prevent the warning, set the CDF install parameter `--auto-configure-firewall` to `true`.

Configuring DNS

Ensure that the host name resolution through Domain Name System (DNS) is working across all nodes in the cluster, including correct forward and reverse DNS lookups. Host name resolution must not be performed through `/etc/hosts` file settings.

You can either run the `<download_directory>/scripts/prereq_disable_ipv6.sh` script that configures DNS automatically or configure DNS manually.

Ensure that all nodes are configured with a Fully Qualified Domain Name (FQDN) and are in the same subnet. Transformation Hub uses the host system FQDN as its Kafka `advertised.host.name`. If the FQDN resolves successfully in the Network Address Translation (NAT) environment, producers and consumers will function correctly. If there are network-specific issues resolving FQDN through NAT, DNS will need to be updated to resolve these issues.

- Transformation Hub supports ingestion of event data that contains both IPv4 and IPv6 addresses. However, its infrastructure cannot be installed in an IPv6-only network.
- `localhost` must not resolve to an IPv6 address, such as, `::1` – this is the default state. The installation process expects only IPv4 resolution to IP address `127.0.0.1`. Comment out any `::1` reference.
- The initial master node host name must not resolve to multiple IPv4 addresses and this includes lookup in `/etc/hosts`.
- "Testing Forward and Reverse DNS Lookup" on page 37
- "Understanding Kubernetes Network Subnet Settings" on page 38

Testing Forward and Reverse DNS Lookup

Test that the forward and reverse lookup records for all servers were properly configured.

To test the forward lookup, run the following commands on every master and worker node in the cluster and on every producer and consumer host system, including:

- All master nodes: $master_1$`.yourcompany.com, …, `$master_n$`.yourcompany.com`
- All worker nodes: $worker_1$`.yourcompany.com, …, `$worker_n$`.yourcompany.com`
- Your ArcMC nodes: $arcmc_1$`.yourcompany.com, ..., `$arcmc_n$`.yourcompany.com`

Use the `nslookup` or `host` commands to verify your DNS configuration.

NOTE: Do not use the `ping` command.

You must run the `nslookup` commands on every server specified in your`/etc/resolv.conf` file. Every server must be able to perform forward and reverse lookup properly and return identical results.

If you have a public DNS server specified in your `/etc/resolv.conf` file, such as the Google public DNS server 8.8.8.8 or 8.8.4.4, you must remove this server from your DNS configuration.

Run the commands as follows. Expected sample output is shown below each command.

- `hostname`

```
master1
```

- `hostname -s`

```
master1
```

- `hostname -f`

```
master1.yourcompany.com
```

- `hostname -d`

```
yourcompany.com
```

- `nslookup master1.yourcompany.com`

```
Server: 192.168.0.53
Address: 192.168.0.53#53
Address: 192.168.0.1
Name: master1.example.com
```

- `nslookup master1`

```
Server: 192.168.0.53
Address: 192.168.0.53#53
Name: master1.example.com
Address: 192.168.0.1
```

- `nslookup 192.168.0.1`

```
Server: 192.168.0.53
Address: 192.168.0.53#53
1.0.168.192.in-addr.arpa name = master1.example.com.
```

Understanding Kubernetes Network Subnet Settings

The Kubernetes network subnet is controlled by the `--POD_CIDR` and `–SERVICE_CIDR` parameters to the Container Deployment Foundation (CDF) installation portal.

The `--POD_CIDR` parameter specifies the network address range for Kubernetes pods. The address range specified in the `--POD_CIDR` parameter must not overlap with the IP range assigned for Kubernetes services, which is specified in the `–SERVICE_CIDR` parameter. The expected value is a Classless Inter-Domain Routing (CIDR) format IP address. CIDR notation comprises an IP address, a slash (/) character, and a network prefix (a decimal number). The minimum useful network prefix is /24 and the maximum useful network prefix is /8. The default value is `172.16.0.0/16`.

For example:

```
POD_CIDR=172.16.0.0/16
```

The `CIDR_SUBNETLEN` parameter specifies the size of the subnet allocated to each host for Kubernetes pod network addresses. The default value is dependent on the value of the `POD_CIDR` parameter, as described in the following table.

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

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

Change the default `POD_CIDR` or `CIDR_SUBNETLEN` values only when your network configuration requires you to do so. You must also ensure that you have sufficient understanding of the flannel network fabric configuration requirements before you make any changes.

Configuring the NFS Server

Container Deployment Foundation (CDF) requires an NFS server to maintain state information about the infrastructure and to store other pertinent data.

For high availability, NFS must run on a highly available external server in the case of a dedicated master deployment having a minimum of three master nodes. For optimal security, secure all NFS settings to allow only required hosts to connect to the NFS server.

- "Prerequisites" on page 39
- "Creating NFS Shared Directories" on page 40
- "Exporting the NFS Configuration" on page 41
- "Verifying NFS Configuration" on page 41
- "Setting Up NFS By Using the Script" on page 42

Prerequisites

The prerequisites for configuring the NFS server are listed below:

- Ensure that the ports 111, 2049, and 20048 are open on the NFS server for communication.
- Enable the `rpcbind` and `nfs-server` package by executing the following commands on your NFS server:

```
systemctl enable rpcbind
systemctl start rpcbind
systemctl enable nfs-server
systemctl start nfs-server
```

- Create and configure the following shared directories:

Directory	Description
<*NFS_VOLUME_DIRECTORY*>/itom-vol	This is the CDF NFS root folder, which contains the CDF database and files. The disk usage will grow gradually.
<*NFS_VOLUME_DIRECTORY*>/db-single-vol	This volume is available only if you did not choose PostgreSQL High Availability (HA) for the CDF database setting. It is for the CDF database. During the installation you will not choose the Postgres database HA option.
<*NFS_VOLUME_DIRECTORY*>/db-backup-vol	This volume is used for backup and restoration of the CDF PostgreSQL database. Its sizing is dependent on the implementation's processing requirements and data volumes.
<*NFS_VOLUME_DIRECTORY*>/itom-logging-vol	This volume stores the log output files of CDF components. The required size depends on how long the log will be kept.
<*NFS_VOLUME_DIRECTORY*>/arcsight-vol	This volume stores the component installation packages.

Creating NFS Shared Directories

1. Log in to the NFS server as `root`.
2. Create the following:
   - **Group:** arcsight with a GID 1999
   - **User:** arcsight with a UID 1999
   - **NFS root directory:** Root directory under which you can create all NFS shared directories.

     Example (NFS_Volume_Directory):`/opt/NFS_Volume`
3. (Conditional) If you have previously installed any version of CDF, you must remove all NFS directories using the following command for each directory:

   `rm -rf <path to NFS directory>`

   For example:

   `rm -rf /opt/NFS_Volume/itom-vol`
4. Create each NFS shared directory using the command:

   `mkdir -p <path to NFS directory>`

   For example:

   `mkdir -p /opt/NFS_Volume/itom-vol`
5. For each NFS directory, set the permission to 755 using the command:

   `chmod -R 755 <path to NFS directory>`

   For example:

   `chmod -R 755 /opt/NFS_Volume/itom-vol`

6 For each NFS directory, set the ownership to UID 1999 and GID 1999 using the command:

```
chown -R 1999:1999 <path to NFS directory>
```

For example:

```
chown -R 1999:1999 /opt/NFS_Volume/itom-vol
```

If you use a `UID/GID` other than `1999/1999`, provide it during the CDF installation in the installation script arguments `--system-group-id` and `--system-user-id`.

Exporting the NFS Configuration

For every NFS volume, run the following set of commands on the External NFS server based on the IP address. You will need to export the NFS configuration with the appropriate IP address for the NFS mount to work properly.

1 For every node in the cluster, you must update the configuration to grant the node access to the NFS volume shares.

For example:

```
/opt/NFS_Volume/arcsight-vol 192.168.1.0/
24(rw,sync,anonuid=1999,anongid=1999,all_squash)

/opt/NFS_Volume/itom-vol 192.168.1.0/
24(rw,sync,anonuid=1999,anongid=1999,all_squash)

/opt/NFS_Volume/db-single-vol 192.168.1.0/
24(rw,sync,anonuid=1999,anongid=1999,all_squash)

/opt/NFS_Volume/itom-logging-vol 192.168.1.0/
24(rw,sync,anonuid=1999,anongid=1999,all_squash)

/opt/NFS_Volume/db-backup-vol 192.168.1.0/
24(rw,sync,anonuid=1999,anongid=1999,all_squash)
```

2 Modify the `/etc/exports` file and run the following command:

```
exportfs -ra
```

If you add more NFS shared directories later, you must restart the NFS service.

Verifying NFS Configuration

1 Create the NFS directory under `/mnt`.

2 Mount the NFS directory on your local system by using the command:

- **NFS v3:** `mount -t nfs 192.168.1.25:/opt/NFS_Volume/arcsight-vol /mnt/nfs`
- **NFS v4:** `mount -t nfs4 192.168.1.25:/opt/NFS_Volume/arcsight-vol /mnt/nfs`

3 After creating all the directories, run the following commands on the NFS server:

```
exportfs -ra

systemctl restart rpcbind

systemctl enable rpcbind
```

```
systemctl restart nfs-server
systemctl enable nfs-server
```

Setting Up NFS By Using the Script

IMPORTANT: The information in this section applies only for non-high-availability and single-node deployments.

You can either run the `/opt/<ESM_Command_Center_Installer_For_Fusion>/scripts/preinstall_create_nfs_share.sh` script that sets up the NFS automatically or set up NFS manually.

To set up NFS manually:

1. Copy `setupNFS.sh` to the NFS server.

   The `setupNFS.sh` file is located on the master node in the `<download_directory>/esm-cmd-center-installer-for-fusion-x.x.x.x/installers/cdf-x.x.x.x/scripts` folder.

2. (Conditional) If you are using the default UID/GID, use the command:

   ```
   sh setupNFS.sh <path_to_nfs_directory>/volumes/volume_name
   ```

3. (Conditional) If you are using a non-default UID/GID, use the command:

   ```
   sh setupNFS.sh <path_to_nfs_directory>/volumes/volume_name true <uid> <gid>
   ```

4. Restart the NFS service:

   ```
   systemctl restart nfs
   ```

Disabling Swap Space

You must disable swap space on all master and worker nodes, excluding the node that has the database.

1. Log in to the node where you want to disable swap space.
2. Run the following command:

   ```
   swapoff -a
   ```

3. In the `/etc/fstab` file, comment out the lines that contain `swap` as the disk type and save the file.

   For example:

   ```
   #/dev/mapper/centos_shcentos72x64-swap swap
   ```

Creating Docker Thinpools

Optionally, to improve performance of Docker processing, set up a thinpool on each master and worker node. Before setting up a thinpool on each node, create a single disk partition on the node, as explained below.

For the thinpool device for Docker (for example, **sdb1**) the minimum physical volume size is 30 GB.

- "Creating a New Partition" on page 43
- "Setting Up a Thinpool for Docker" on page 43

Creating a New Partition

1. Log in to the node.
2. Run the command:

   `fdisk <name of the new disk device that was added>`

   For example:

   `# fdisk /dev/sdb1`
3. Enter `n` to create a new partition.
4. When prompted, enter the partition number, sector, type (`Linux LVM`), and size for the first partition. To select the Linux LVM partition type:
   - Enter `t` to change the default partition type to Linux LVM
   - Type `L` to list the supported partition types
   - Type `8e` to select the Linux LVM type
5. When prompted, enter the partition number, sector, type `(Linux LVM`), and size for the second partition.
6. Type `p` to view the partition table.
7. Type `w` to save the partition table to disk.
8. Type `partprobe`.

Setting Up a Thinpool for Docker

1. Create a physical volume with the following command:

   `# pvcreate [physical device name]`

   For example:

   `# pvcreate /dev/sdb1`
2. Create a volume group with the following command:

   `# vgcreate [volume group name] [logical volume name]`

   For example:

   `# vgcreate docker /dev/sdb1`
3. Create a logical volume (LV) for the thinpool and bootstrap with the following command:

   `# lvcreate [logical volume name] [volume group name]`

For example, the data LV is 95% of the 'Docker' volume group size. (Leaving free space allows for automatic expanding of either the data or metadata if space is running low, as a temporary measure.)

```
# lvcreate --wipesignatures y -n thinpool docker -l 95%VG
# lvcreate --wipesignatures y -n thinpoolmeta docker -l 1%VG
```

4 Convert the pool to a thinpool with the following command:

```
# lvconvert -y --zero n -c 512K --thinpool docker/thinpool --
poolmetadata docker/thinpoolmeta
```

Optionally, you can configure the auto-extension of thinpools using an lvm profile.

4a Open the `lvm` profile.

4b Specify a value for the parameters `thin_pool_autoextend_threshold` and `thin_pool_autoextend_percent`, each of which represents a percentage of the space used.

For example:

```
activation {
thin_pool_autoextend_threshold=80
thin_pool_autoextend_percent=20
}
```

4c Apply the `lvm` profile with the following command:

```
# lvchange --metadataprofile docker-thinpool docker/thinpool
```

4d Verify that the `lvm` profile is monitored with the following command:

```
# lvs -o+seg_monitor
```

4e Clear the graph driver directory with the following command, if Docker was previously started:

```
# rm -rf /var/lib/docker/*
```

4f Monitor the thinpool and volume group free space with the following commands:

```
# lvs
# lvs -a
# vgs
```

4g Check the logs to see the auto-extension of the thinpool when it hits the threshold:

```
# journalctl -fu dm-event.service
```

Enabling Installation Permissions for a sudo User

If you choose to install CDF as a `sudo` user, the root user must grant non-root (`sudo`) users installation permission before they can perform the installation. Ensure that the provided user has permission to execute scripts under temporary directory `/tmp` on all master and worker nodes.

There are two distinct file edits that need to be performed: First on the initial master node only, and then on all remaining master and worker nodes.

- "Edit the `sudoers` File on the Initial Master Node" on page 45
- "Edit the `sudoers` File on the Remaining Master and Worker Nodes" on page 46

Edit the `sudoers` File on the Initial Master Node

Make the following modifications only on the initial master node.

IMPORTANT: In the following commands you must ensure that there no more than a single space character after each comma that delimits parameters. Otherwise, you may get an error similar to this when you attempt to save the file:

```
>>> /etc/sudoers: syntax error near line nn<<<
```

---

1. Log in to the initial master node as the `root` user.
2. Open the `/etc/sudoers` file using Visudo.
3. Add the following `Cmnd_Alias` line to the command aliases group in the `sudoers` file:

   ```
   Cmnd_Alias CDFINSTALL = <CDF_installation_package_directory>/scripts/
   precheck.sh, <CDF_installation_package_directory>/install, <K8S_HOME>/
   uninstall.sh, /usr/bin/kubectl, /usr/bin/docker, /usr/bin/mkdir,/bin/
   rm, /bin/su, /bin/chmod, /bin/tar, <K8S_HOME>/scripts/uploadimages.sh,/
   bin/chown
   ```

   where

   - **CDF_installation_package_directory** represents the directory where you unzipped the installation package. For example:

     `/tmp/cdf-2019.05.0xxx.`

   - **K8S_HOME** represents the Kubernetes directory, by default `/opt/arcsight/kubernetes`.

4. Add the following lines to the wheel users group, replacing <*username*> with your `sudo` user password:

   ```
   %wheel ALL=(ALL) ALL

   cdfuser ALL=NOPASSWD: CDFINSTALL
   ```

   For example:

   ```
   Defaults: root !requiretty
   ```

5. Locate the `secure_path` line in the `sudoers` file and ensure that the following paths are present:

   ```
   Defaults secure_path = /sbin:/bin:/usr/sbin:/usr/bin
   ```

   By doing this, the `sudo` user can execute the `showmount`, `curl`, `ifconfig`, and `unzip` commands when installing CDF.

6. Save the file.

Installing Components Using the sudo User

After completing the modifications to the sudoers file as described above, perform the following steps:

1. Log in to the initial master node as the non-root sudo user to perform the installation.
2. Download the installation files to a directory where the non-root sudo user has write permissions.
3. Run CDF using the sudo command.

Edit the sudoers File on the Remaining Master and Worker Nodes

Make the following modifications only on the remaining master and worker nodes.

IMPORTANT: In the following commands you must ensure that there is, at most, a single space character after each comma that delimits parameters. Otherwise, you may get an error similar to this when you attempt to save the file.

```
>>> /etc/sudoers: syntax error near line nn<<<
```

---

1. Log in to each master and worker node.
2. Open the /etc/sudoers file.
3. Add the following Cmnd_Alias line to the command aliases group in the sudoers file.

   ```
   Cmnd_Alias CDFINSTALL = /tmp/scripts/pre-check.sh,
   <ITOM_Suite_Foundation_Node>/install, <K8S_HOME>/uninstall.sh, /usr/
   bin/kubectl, /usr/bin/docker,/usr/bin/mkdir, /bin/rm, /bin/su, /bin/
   chmod, /bin/tar, <K8S_HOME>/scripts/uploadimages.sh, /bin/chown
   ```

   where

   - **ITOM_Suite_Foundation_Node** represents the directory where you unzipped the installation package. For example:

     ```
     /tmp/ITOM_Suite_Foundation_2019.05.0xxx
     ```

   - **K8S_HOME** represents the Kubernetes directory, by default /opt/arcsight/kubernetes.
4. Add the following lines to the wheel users group, replacing <*username*> with your sudo user password:

   ```
   %wheel ALL=(ALL) ALL
   ```

   ```
   cdfuser ALL=NOPASSWD: CDFINSTALL
   ```

   For example:

   ```
   Defaults: root !requiretty
   ```
5. Locate the secure_path line in the sudoers file and ensure that the following paths are present:

   ```
   Defaults secure_path = /sbin:/bin:/usr/sbin:/usr/bin
   ```

   By doing this, the sudo user can execute the showmount, curl, ifconfig, and unzip commands when installing CDF.
6. Save the file.

Repeat the process for each remaining master and worker node.

Installing the CDF

This section provides guidance for installing the Container Deployment Foundation (CDF).

NOTE: You can install CDF as a root user or `sudo` user. However, if you choose to install as a sudo user, you must first configure installation permissions from the root user.

---

1. Log in to the master node as the `root` or `sudo` user.
2. Change to the directory where you downloaded the installation files. For information about downloading the installation files, see Part II, "Installing CDF and Deploying ESM for Fusion," on page 25.

   ```
   cd <download_directory>/esm-cmd-center-installer-for-fusion-x.x.x.x/
   installers/cdf-<year>.<month>.<build_number>-<version>
   ```

   For example:

   ```
   cd opt/esm-cmd-center-installer-for-fusion-x.x.x.x/installers/cdf-
   2020.02.00120-2.2.0.2
   ```

3. (Conditional) If you are installing CDF on a node where ESM Manager is not installed, use the command:

   ```
   ./install -m <metadata_file_path>
   --k8s-home <cdf_installer_directory>
   --nfs-server <NFS_server_IP_address>
   --nfs-folder <NFS_Volume_file_path>
   --registry-orgname srg
   ```

   For example:

   ```
   ./install -m /opt/esm-cmd-center-installer-for-fusion-x.x.x.x/
   suite_images/arcsight-installer-metadata-x.x.x.x.tar
   --k8s-home /opt/arcsight/kubernetes
   --nfs-server <NFS_server_IP_address>
   --nfs-folder <NFS_Volume_file_path>/itom-vol
   --registry-orgname srg
   ```

4. (Conditional) If you are installing CDF on the same machine as ESM Manager, complete the following action:

   If ESM is installed with the default port (8443), add the following command argument to configure the CDF API server port (default 8443) to use a different port:

   ```
   --master-api-ssl-port 7443
   ```

   For example:

   ```
   ./install -m /opt/esm-cmd-center-installer-for-fusion-x.x.x.x/
   suite_images/arcsight-installer-metadata-x.x.x.x.tar
   --k8s-home /opt/arcsight/kubernetes
   --nfs-server <NFS_server_IP_address>
   --master-api-ssl-port 7443
   --nfs-folder <NFS_Volume_file_path>/itom-vol
   --registry-orgname srg
   ```

5 (Conditional) For high availability, use the following command:

```
./install -m <metadata_file_path>
--k8s-home <NFS_server_IP_address>
--nfs-folder <NFS_Volume_file_path>
--registry-orgname srg
--ha-virtual-ip <HA_virtual_IP_address>
```

For example:

```
./install -m /opt/esm-cmd-center-installer-for-fusion-x.x.x.x/
suite_images/arcsight-installer-metadata-x.x.x.x.tar
--k8s-home /opt/arcsight/kubernetes
--nfs-server <NFS_server_IP_address>
--nfs-folder <NFS_Volume_file_path>/itom-vol
--registry-orgname srg
--ha-virtual-ip <NFS_server_IP_address>
```

6 When prompted, specify the administrator password. This password is required to log in to the CDF Management Portal as an administrator.

The CDF Management Portal enables you to deploy ESM for Fusion and all required software in a cluster.

7 Change the default CA certificate that is generated during the installation. For steps to change the CA certificate, see Changing the CA of CDF.

A self-signed CA certificate is generated during the installation of CDF by default. After deploying Fusion, the pods of the deployed products use the certificates generated by the CA on pod startup. If you change the CA certificate after deployment, you will have to uninstall and reinstall all the software. So, we recommend changing the CA certificate before deploying ESM for Fusion.

8 To deploy ESM for Fusion and all required software, continue with the section "Deploying ESM for Fusion" on page 48.

Deploying ESM for Fusion

This section provides information about using the CDF Management Portal to deploy ESM for Fusion.

Configuring the Cluster

1 Open a new tab in a supported web browser.

2 Specify the URL for the CDF Management Portal:

```
https://<ESM_for_Fusion-server>:3000
```

NOTE: Use port *3000* when you are setting up the CDF for the first time. After the initial setup, use port *5443* to access the CDF Management Portal.

Use the fully qualified domain name of the host that you specified in the **Connection** step during the CDF configuration. Usually, this is the master node's FQDN.

3 Log in to the CDF Management Portal with the credentials of the administrative user that you provided during installation.

4 Select the metadata file version in **version**, and then click **Next**.

5 Read the license agreement, and then select **I agree**.

6 Click **Next**.

7 On the **Capabilities** page, select the following options:

- Fusion
- ArcSight Command Center
- (Optional) ArcSight Layered Analytics

NOTE: To use this capability, you must deploy both ArcSight Interset and ESM for Fusion in the same cluster.

---

8 Click **Next**.

9 On the **Database** page, retain the default values, and then click **Next**.

10 On the **Deployment Size** page, select the required cluster, and then click **Next**.

11 (Conditional) For worker node configuration, select **Medium Cluster**.

12 On the **Connection** page, an external host name is automatically populated. This is resolved from the virtual IP (VIP) specified during the CDF installation (--ha-virtual-ip parameter). Confirm that the VIP is correct and then click **Next**.

13 (Conditional) To set up high availability, complete the following steps:

IMPORTANT: You must configure high availability at this point in the process. You cannot add master nodes and configure high availability after installation.

13a Select **Make master highly available**.

13b On the **Master High Availability** page, add at least two additional master nodes.

13c On the **Add Master Node** page, specify the following details:

Host

Specifies the fully qualified domain name (FQDN) of the node that you are adding.

Ignore Warnings

Specifies whether you want the CDF Management Portal to ignore any warnings that occur during the pre-checks on the server.

If deselected, the add node process will stop and a window will display any warning messages. We recommend that you start with **Ignore Warnings** deselected in order to view any warnings displayed. You may then evaluate whether to ignore or rectify any warnings, clear the warning dialog, and then click **Save** again with the box selected to avoid stopping.

User Name

Specifies the user credential for logging in to the node.

Verify Mode

Specifies whether the verification mode should be **Password** or **Key-based**.

- For **Password**, you must also specify the your password.
- For **Key-based**, you must first specify a user name and then upload a private key file when connecting the node with a private key file.

Thinpool Device

Applies only if you configured a Thinpool for the master node

Specifies the Thinpool Device path that you configured for the master node.

For example: `/dev/mapper/docker-thinpool`

You must have already set up the Docker thin pool for all cluster nodes that need to use thinpools, as described in the *CDF Planning Guide*.

flannel IFace

Applies only if the master node has more than one network adapter

Specifies the flannel IFace value for Docker inter-host communication.

The value must be a single IPv4 address or name of the existing interface.

13d Click **Save**.

13e Repeat these steps for other master nodes.

14 Click **Next**.

15 (Conditional) For multi-node deployment, complete the following steps:

15a Select the **Add Worker Node** page.

15b To add additional worker nodes, click **+** (Add).

15c Specify the required configuration information.

15d Click **Save**.

15e Repeat these steps for each of the worker nodes you want to add.

16 Click **Next**.

17 (Conditional) To run the worker node on the master node, select **Allow suite workload to be deployed on the master node**, and then click **Next**.

NOTE: Before selecting this option, ensure that the master node meets the system requirements specified for the worker node.

---

18 To configure each NFS volume, complete the following steps:

18a Navigate to the **File Storage** page.

18b For **File System Type**, select **Self-Hosted NFS**.

Self-hosted NFS refers to the external NFS that you created while preparing the environment for CDF installation.

18c For **File Server**, specify the IP address or FQDN of the NFS server.

18d For **Exported Path**, specify the following paths for the NFS volumes:

NFS Volume	File Path
arcsight-volume	`<NFS_VOLUME_FOLDER>/arcsight-vol`
itom-vol-claim	`<NFS_VOLUME_FOLDER>/itom-vol`
db-single-vol	`<NFS_VOLUME_FOLDER>/db-single-vol`
itom-logging-vol	`<NFS_VOLUME_FOLDER>/itom-logging-vol`
db-backup-vol	`<NFS_VOLUME_FOLDER>/db-backup-vol`

18e Click **Validate**.

Ensure that you have validated all NFS volumes successfully before continuing with the next step.

19 Click **Next**.

20 To start deploying master and worker nodes, click **Yes** in the **Confirmation** dialog box.

21 Continue with "Uploading Images to the Local Registry" on page 51.

Uploading Images to the Local Registry

For the docker registry to deploy ESM for Fusion, it needs the following images associated with the deployment:

- `fusion-x.x.x.x`
- `esm-x.x.x.x`
- (Optional) `layered-analytics-x.x.x.x`

You must upload these images to the local registry as follows:

1. Launch a terminal session, then log in to the master node as `root` or a `sudo` user.
2. Change to the following directory:

   `cd /<cdf_installer_directory>/scripts/`

   For example:

   `cd /opt/esm-cmd-center-installer-for-fusion-x.x.x.x/installers/cdf-x.x.x-x.x.x.x/scripts/`
3. Upload required images to the local registry. When prompted for a password, use the admin user password for the CDF Management Portal:

   `./uploadimages.sh -d <downloaded_suite_images_folder_path>`

   For example:

   `./uploadimages.sh -d /<download_directory>/esm-cmd-center-installer-for-fusion-x.x.x.x/suite_images`
4. Continue with "Deploying ESM for Fusion" on page 52.

Deploying ESM for Fusion

After you upload the images to the local directory, the CDF uses these images to deploy the respective software in the cluster.

1. Log in to the CDF Management Portal.
2. On the **Download Images** page, click **Next** because all the required packages are already downloaded and uncompressed.
3. After the **Check Image Availability** page displays `All images are available in the registry`, click **Next**.

   If the page displays any missing image error, upload the missing image.
4. (Optional) To monitor the progress of service deployment, complete the following steps:
   - **4a** Launch a terminal session.
   - **4b** Log in to the master node as `root`.
   - **4c** Execute the command:

     ```
     watch 'kubectl get pods --all-namespaces'
     ```
5. After the **Deployment of Infrastructure Nodes** page displays the status of the node in green, click **Next**.

   The deployment process can take up to 15 minutes to complete.
6. (Conditional) If any of the nodes show a red icon on the **Deployment of Infrastructure Nodes** page, click the **retry** icon.

   IMPORTANT: CDF might display the red icon if the process times out for a node. Because the retry operation executes the script again on that node, ensure that you click **retry** only once.

   ---
7. After the **Deployment of Infrastructure Services** page indicates that all the services are deployed and the status indicates green, click **Next**.

   The deployment process can take up to 15 minutes to complete.
8. Click **Next**.
9. Configure the pre-deployment settings in the CDF Management Portal, by making the following changes under **ANALYTICS**:
   - In the **Cluster Configuration** section, select **0** from the **Hercules Search Engine Replicas** drop-down list.

     NOTE: By default, the value for **Hercules Search Engine Replicas** is **1**.

   - In the **Database Configuration** section, disable Database.
   - In the **Single Sign-on Configuration** section, specify the values for **Client ID** and **Client Secret**.
10. To finish the deployment, click **Next**.
11. Copy the Management Portal link displayed on the **Configuration Complete** page.

    Some of the pods on the **Configuration Complete** page might remain in a pending status until the product labels are applied on worker nodes.

12 (Conditional) For high availability and multi-master deployment, after the deployment has been completed, complete the following steps to manually restart the keepalive process:

12a Log in to the master node.

12b Change to the following directory:

```
cd /<k8S_HOME>/bin/
```

For example:

```
cd /opt/arcsight/kubernetes/bin/
```

12c Run the following script:

```
./start_lb.sh
```

13 Continue to the post-installation steps.

9 Deploying ESM for Fusion in an Existing Cluster

If you already have the ArcSight Platform installed, you can deploy ESM for Fusion to the same cluster. Reusing existing clusters would reduce costs and system management effort compared to deploying this software in a new cluster.

Prerequisites

Before installing ESM for Fusion, complete the following tasks:

- Review the Installation Checklist to understand the tasks involved for installing and configuring ESM for Fusion.
- Download the ESM for Fusion installation files and verify the signatures. You need the following files to deploy ESM for Fusion in an existing cluster:
  - `fusion-x.x.x.x`

    You do not have to deploy the Fusion capability if ArcSight Recon or ArcSight Interset has already been deployed.
  - `esm-x.x.x.x`
  - (Optional) `layered-analytics-x.x.x.x`

    NOTE: To use this capability, you must deploy both ArcSight Interset and ESM for Fusion in the same cluster.
  - `arcsight-installer-metadata-x.x.x.x.tar`
- Upgrade the existing cluster to the correct version of the ArcSight Suite in the CDF Management Portal to deploy the current version of ESM for Fusion.

Deploying Fusion to an Existing Cluster

To deploy ESM for Fusion in an existing cluster, perform the following steps:

1. Log in to the CDF Management Portal.
2. Select **Deployment** > **Deployments** > ⋮ > **Change**.
3. On the **Capabilities** page, select the following options:
   - Fusion (if not selected already)
   - ArcSight Command Center

- (Optional) ArcSight Layered Analytics

  NOTE: To use this capability, you must deploy both ArcSight Interset and ESM for Fusion in the same cluster.

4. Click **Next** until you reach the **Import Container Images** page.
5. Launch a terminal session, then log in to the master node as `root` or as a sudo user.
6. Change to the following directory:

   `cd /<fusion_download_directory>/installers/cdf-x.x.x-x.x.x.x/scripts/`

   For example:

   `cd /opt/esm-cmd-center-installer-for-fusion-x.x.x.x/installers/cdf-x.x.x-x.x.x.x/scripts/`
7. Upload required images to the local registry.

   When prompted for a password, use the admin user password for the CDF Management Portal:

   `./uploadimages.sh -d /<fusion_download_directory>/suite_images`

   Repeat this step for the other selected capabilities.
8. Switch to the CDF Management Portal.
9. To ensure that the images have been uploaded, click **CHECK AGAIN**.
10. Click **Next** until you reach the **Configuration Complete** page.
11. After the **Configuration Complete** page displays all the pods in green, click **Next**.
12. Continue to the post-installation steps.

10 Post-Installation Configuration

This chapter provides information about the post-installation configuration you must perform after deploying ESM for Fusion.

Add Dashboard Roles and Permissions to the User Management Pod

Applies only when you deploy ESM for Fusion to an existing cluster

When you deploy ESM for Fusion to an existing cluster, the User Management pod does not automatically incorporate the new roles and permissions for the Dashboard to the **ADMIN** function in the user interface. Without the default roles, not even an administrative user can view the Dashboard. Deleting (restarting) the User Management pod adds the roles and permissions.

To delete the User Management pod:

1. Complete the ESM for Fusion deployment.
2. Enter the following command:

   ```
   kubectl delete pod -n namespace management pod name
   ```

   For example:

   ```
   kubectl delete pod -n arcsight-installer-p2dlt hercules-management-
   7f876b4978-9xkl6
   ```

   When you delete any pod, the pod will start automatically.
3. After the pod restarts, you can log in to the Dashboard.

Labeling Nodes

IMPORTANT: *Does not apply if you used the* `./install-single-node-post.sh` *installation script*

Labeling a node tells Kubernetes what type of application can run on a specific node. It identifies application processing and qualifies the application as a candidate to run on a specific host system. Labeling is required only for worker nodes and not for master nodes.

You can follow the instructions in this section to label the nodes manually for both single-node and multi-node deployment. However, for single node deployment, you can alternatively use the `/opt/<ESM_Command_Center_Installer_for_Fusion>/postinstall_label_master_node.sh` script (present in the scripts folder) to label the node automatically.

To label the nodes in a new cluster:

1. Open a new tab in a supported web browser.
2. Specify the URL for the CDF Management Portal:

   `https://ESM_for_Fusion_server:5443`

   Use the fully qualified domain name of the host that you specified in the **Connection** step during the CDF configuration. Usually, this is the master node's FQDN.
3. Log in to the CDF Management Portal with the credentials of the administrative user that you provided during installation.
4. Select **Administration > Nodes.**
5. In **Predefined Labels**, click **+** to add labels.
6. Specify the following label:

   `fusion:yes`

   NOTE: Labels are case-sensitive. Ensure that you enter the values correctly.
7. (Conditional) For single-node deployment, drag all the newly-added labels to the worker node.
8. (Conditional) For multi-node deployment, drag and drop the new labels from the predefined set to each of the worker nodes based on your workload sharing configuration.

   You might need to click **Refresh** to see the attached labels.

Connecting to an SMTP Server

To ensure that ESM for Fusion users receive email notifications, configure the connection to your SMTP server. For example, if you do not use SAML 2 authentication, users will need notifications to help reset their forgotten passwords.

1. Log in to the CDF Management Portal with the credentials of the administrative user that you provided during installation.
2. Select **FUSION**.
3. Under **User Management Configuration**, configure the SMTP settings.

Integrating Fusion Single Sign-On

The Fusion capability manages single sign-on activity, as well as provides user management functions. You can configure Fusion to establish a trust relationship with your external identity provider. With this authentication method, a user's email address, specified in the 'email' claim value from the SAML2 Identity Provider, maps to the userID for any Fusion user.

NOTE

- You should time-synchronize Fusion and the external SAML 2.0 IDP to the same NTP server. In the configuration UI, ensure that the session timeout matches the same value that the external IDP has configured for user session timeouts.
- **Regarding the Trusted Provider Metadata**, the metadata document for a trusted SAML provider with which an SSO-defined provider interacts must be obtained in a provider-specific manner. While not all providers do so, many supply their metadata documents via URL.

  Once the trusted provider's metadata document (or the URL-accessible location of the document) is obtained, you must configure the SSO provider that will interact with the trusted provider with the trusted provider's metadata. In the document, modify the `<Metadata>` element within the `<AccessSettings>` element under either the `<TrustedIDP>` element or the `<TrustedSP>` element. For example:

  ```
  com.microfocus.sso.default.login.saml2.mapping-attr = email
  ```

  The `email` attribute refers to the email attribute name from the SAML2 IDP.

To integrate with an external SAML provider:

1. On the CDF server, open the `sso-configuration.properties` file, located by default in the `/opt/arcsight/nfs/vol/arcsight/sso/default` directory.
2. Add the following properties to the file:
   - `com.microfocus.sso.default.login.method = saml2`
   - `com.microfocus.sso.default.saml2.enabled = true`
3. To specify the address where the IDP supplies its metadata document, complete one of the following actions:
   - Add the following property to the file:

     `com.microfocus.sso.default.login.saml2.metadata-url = IDP SAML metadata URL`

     For example, a Keycloak server URL could be `https://KeycloakServer/auth/realms/YourRealm/protocol/saml/descriptor`.

     NOTE: For HTTPS to work properly, you must import the IDP certificates to the Fusion single sign-on keystore as described in Step 5.
   - Convert the metadata xml file to a base64 string, then add the following property to the file:

     `com.microfocus.sso.default.login.saml2.metadata = base64 encoded metadata xml`
4. Save the changes to the `sso-configuration.properties` properties file.
5. (Conditional) If you specified the metadata URL in Step 3, complete the following steps to import the IDP certificate to the SSO keystore:

   5a Copy the IDP certificate to following location:

   `/path/to/sso/default/`

5b Get the pod information using the following command:

```
kubectl get pods --all-namespaces | grep osp
```

5c Open a terminal in the currently running `hercules-osp` pod:

```
kubectl exec -it hercules-osp-xxxxxxxxxx-xxxxx -n arcsight-
installer-xxxxx -c hercules-osp -- bash
```

5d Import the IDP certificate file using the following commands:

5d1 `cd /usr/local/tomcat/conf/default/`

5d2 `keytool -importcert -file` *`CertificateFileName`* `-keystore sso.keystore -storepass $KEYSTORE_PASSWORD -alias` *`AliasName`*

where

- **CertificateFileName** represents the name of the certificate file that you want to import.
- **AliasName** represents the new alias name that you want to assign to the certificate in the SSO keystore.

6 Restart the pod by completing the following steps:

6a To get the pod information, enter the following command:

```
kubectl get pods --all-namespaces | grep osp
```

6b To delete the currently running pod, enter the following command:

```
kubectl delete pod hercules-osp-xxxxxxxxxx-xxxxx -n arcsight-
installerxxxxx
```

7 Retrieve the Fusion SSO SAML service provider metadata from the Fusion server:

`https://`*`Fusion_server`*`/osp/a/default/auth/saml2/spmetadata`

where **Fusion_server** represents the host name of the Fusion server.

8 Use the Fusion SSO SAML service provider metadata to configure your IDP.

For more information, see the IDP software documentation.

9 To establish a trust relationship between Fusion SSO and your IDP software, create certificates for your IDP software.

For more information on how to create and import certificates in your IDP software, see the IDP software documentation.

Securing NFS

You must secure the NFS shared directories from external access. This section provides one method for ensuring security while maintaining access to master and worker nodes in the cluster. However, you can use a different approach to adequately secure NFS.

1 Log in to the master node as root.

2 Remove the firewall definition for all NFS ports:

```
NFS_PORTS=('111/tcp' '111/udp' '2049/tcp' '20048/tcp')
for port in "${NFS_PORTS[@]}"; do firewall-cmd --permanent --remove-
port $port; done;
```

3 (Conditional) If you have installed Fusion by using scripts, remove all rich rules:

```
firewall-cmd --list-rich-rules |xargs -I '{}' firewall-cmd --permanent
--remove-rich-rule '{}'
```

4 Reload the new firewall configuration:

```
firewall-cmd --reload
```

5 Restart the nginx pod to apply the new firewall configuration:

```
SUITE_NAMESPACE=$(kubectl get namespaces |grep arcsight|cut -d ' ' -f1)
kubectl delete pod --namespace=$SUITE_NAMESPACE -l app=nginx-ingress-lb
```

6 (Conditional) To expose NFS shares to other hosts such as other master and worker node, complete the following steps:

6a Execute the command:

```
firewall-cmd --add-source="<IP_address or CIDR expression of host or
hosts>" --zone="trusted" --permanent
```

6b Reload the new firewall configuration:

```
firewall-cmd --reload
```

6c Restart the nginx pod to apply the new firewall configuration:

```
SUITE_NAMESPACE=$(kubectl get namespaces |grep arcsight|cut -d ' ' -
f1)
kubectl delete pod --namespace=$SUITE_NAMESPACE -l app=nginx-
ingress-lb
```

11 Verifying the Installation

To determine whether the installation is successful, launch ESM for Fusion. The first time that you connect after deployment, the application prompts you to create credentials for the product administrator.

1. Open a supported web browser.
2. Specify the URL for ESM for Fusion:

   `https://<ESM_for_Fusion-server>/dashboard`

3. Specify credentials for the appropriate administrator, using the following format:

   name@domain.com

4. Specify credentials for the initial administrator.

   NOTE: If your environment includes Interset, review the following requirements for the initial administrative user:

   - For the first-time login, you must enter credentials for the *Interset administrator*, which is the administrative account that was specified during the deployment of Interset. Otherwise, Interset users will not have single sign-on access to the Dashboard.
   - The Interset administrator account cannot access analytics data in Interset because the application automatically assigns it to the *Administrative Tenant* role. So, this role cannot view content in widgets that display data from Interset.
   - Other users created with Dashboard permissions automatically receive the *Default Tenant* status in Interset. These users can view content in widgets that display data from Interset.

   ---

5. Log in with the new credentials.
6. To connect with ESM, continue to Chapter 12, “Integrating Data and Users from Enterprise Security Manager,” on page 67.
7. (Conditional) To connect with Interset, continue to Chapter 13, “Integrating Data from Interset,” on page 71.
8. Create additional Dashboard users.

III Configuring ESM for Fusion

This section provides guidance for configuring ESM for Fusion data sources and users after a successful installation.

12 Integrating Data and Users from Enterprise Security Manager

ESM for Fusion allows you to integrate data from Enterprise Security Manager (ESM). With single sign-on enabled, ESM and ESM for Fusion users can easily access the ArcSight Console, ArcSight Command Center, ESM for Fusion, and the REST APIs. As a convenience, you can import users that are already authorized for ESM.

Understanding How ESM Users Access ESM for Fusion

Rather than manually adding users in ESM for Fusion, we recommend that you create the users in ESM then import them. For the imported ESM users to log in to ESM for Fusion and be able to access ESM data, the following conditions apply:

- You must enable single sign-on (SSO) access for ESM and ESM for Fusion users.
- Users must have an account in both ESM and ESM for Fusion.
- You must configure the **External User ID** and **E-mail** fields in the ESM accounts to comply with the *name@domain.com* format.
- Users must log in to ESM for Fusion with the **External User ID** from their ESM account.
- If your environment does not use SAML 2 authentication, ensure that you have configured the SMTP server settings for ESM for Fusion. Users might need to set a password for ESM for Fusion the first time that they log in. This requires those users to initiate the "Forgot Password" function and receive an email notification.

Importing Users from ESM

You can import users that are already authorized for ESM. You need to have at least one role available in ESM for Fusion to assign to these users.

1. In the ArcSight Console, ensure that the **External User ID** and **E-mail** fields for each account comply with the following format:

   name@domain.com

2. Log in to ESM for Fusion.
3. Click **ADMIN** > **Account Groups** > **Import Users**.

4 Select the role that you want to assign to the imported users.

5 Select **IMPORT USERS**.

As you add more users to ESM, you can run the import process again. ESM for Fusion ignores duplicates of user accounts that have been imported previously.

Enabling Single Sign-on with ESM

You must configure ESM to use **OSP Client Only Authentication**. If your ESM environment currently uses an external SAML 2 client authentication, you must delegate the Fusion SSO provider to connect to the SAML client. If you do not use SAML 2 authentication, you will need to configure SMTP settings for Fusion to support forgotten password activity. The Fusion capability manages single sign-on functions.

This procedure assumes that you have already installed or upgraded ESM.

1 Change the authentication settings for the ESM Manager service:

1a On the ESM server, start the configuration wizard by entering the following command from the `/opt/arcsight/manager/bin/` directory:

```
arcsight managersetup -i console
```

1b Advance through the wizard until you reach the authentication settings.

1c Select **OSP Client Only Authentication**, then click **Next**.

1d To specify the host and port for the OSP server, use the following format:

domain_name:port

For example, Fusion by default installs OSP on port 443. So, when you are using ESM for Fusion, specify the format as `<fusion host>:443`.

1e To specify the host and port for the ArcSight Command Center, use the following format:

domain_name:port

Example:

`<ESM Manager>:8443`

Typically, the host and port are the same as those for the ArcSight Manager.

1f Specify a **Tenant Name for OSP**. If you are using a typical installer for Fusion, enter `default`.

1g Click **Next** until you complete your changes in the wizard.

1h Restart the ESM Manager service using the following commands:

```
/etc/init.d/arcsight_services stop manager
```

```
/etc/init.d/arcsight_services start manager
```

2 Change the authentication settings for the ArcSight Console (the Console):

2a From the Console's `/bin` directory, enter one of the following commands:

On Windows: `arcsight.bat consolesetup`

On Linux: `./arcsight consolesetup`

2b Advance through the wizard until you reach the authentication settings.

2c Select **OSP Client Only Authentication**.

2d Click **Next** until you complete your changes in the wizard.

3 To configure the SSO settings in the CDF Management Portal, complete the following steps:

3a Connect to the Portal:

```
https://ESM_for_Fusion_server:5443
```

3b Log in with the credentials of the administrative user that you provided during installation.

3c Select **FUSION**.

3d Under **Single Sign-on Configuration**, specify the **Client ID** and **Client Secret**.

3e Under **ArcSight ESM Host Configuration**, verify the settings for the ESM host and port that were specified during deployment.

4 (Conditional) To use an external SAML2 authentication method, continue to "Integrating Fusion Single Sign-On" on page 58.

5 (Conditional) If you do not use an external SAML 2 authentication method, ensure that users can receive email notifications to change their Fusion password. Continue to "Connecting to an SMTP Server" on page 58.

Integrating Data from Enterprise Security Manager

To view ESM data in the Dashboard, update the settings in the CDF Management Portal. The Fusion capability manages the Dashboard functions.

1 Open a new tab in a supported web browser.

2 Specify the URL for the CDF Management Portal:

```
https://ESM_for_Fusion_server:5443
```

Use the fully qualified domain name of the host that you specified in the **Connection** step during the CDF configuration. Usually, this is the master node's FQDN.

3 Login to the CDF Management Portal with the credentials of the administrative user that you provided during installation.

4 In the CDF Management Portal, click the ⋮ icon for the installed suite.

5 Select **Reconfigure**.

6 On the **Configuration** page, select **FUSION**.

7 In the **ArcSight ESM Host Configuration** section, complete the following steps:

7a For **ESM host**, specify the fully-qualified host name or IP address of the server that hosts ESM.

7b For **ESM port**, specify the port associated with the ESM host. The default value is 8443.

13 Integrating Data from Interset

You can deploy ESM for Fusion within the same cluster as ArcSight Interset. As an administrator, you do not have to perform any additional configurations in ESM for Fusion to integrate data from Interset.

NOTE: To use the Layered Analytics capability, you must deploy both Interset and ESM for Fusion in the same cluster.

Interset users automatically have single sign-on access as long as the first administrative account for Fusion matches the credentials for the *Interset administrator*, which is the administrative account that was specified during the deployment of Interset. Users with Dashboard permissions automatically receive the *Default Tenant* status in Interset. These users can view content in widgets that display data from Interset. The *User Guide for Fusion*, available as context-sensitive help within ESM for Fusion and posted with the documentation for ArcSight Platform, indicates whether a widget needs data from a specific data source.

14 Creating Widgets for the Dashboard

The license for your deployed application also grants you access to the **Widget Software Development Kit** (the Widget SDK), which you can download to your local production or test environment. The Widget SDK enables you to build new widgets or modify existing widgets for deployed applications such as ESM and Interset.

Using the Widget SDK

Once you unpack the Widget SDK, you have access to its documentation.

1. Extract the contents of the `widget-sdk-n.n.n.tgz` file.
2. Follow the steps in the **Getting Started** section of the included *ReadMe*.
3. After you compile the new or modified widget, add it to the widget store for use in the Dashboard.

Considerations for Updating the Widget Store

Review the following considerations before modifying or creating new widgets:

- Widgets provided with a deployed application are included in the default widget store directory: `/opt/NFS_Volume/arcsight-vol/fusion/widget-store`.
- Each new widget must have a unique name.
- You cannot edit an out-of-the-box widget. To prevent your custom widgets from being erased or overwritten by a product upgrade, do not name them the same as an out-of-the-box widget.

15 Adding Users and Groups to ESM for Fusion

ESM for Fusion allows you to incorporate users either by manually adding them or by importing users and groups from ESM. To assign permissions to these users, you can create roles with specific sets of permissions and add users to those roles.

The Fusion capability supports the user management functions. For more information about assigning permissions to users and roles, see the *User Guide for Fusion* embedded in the product or posted with the documentation for ArcSight Platform.

IV Upgrading Fusion

This section provides information about upgrading a single-node deployment of ESM for Fusion.

16 Upgrade Checklist

Before you upgrade ESM for Fusion, review the following checklist to ensure a successful upgrade.

	Task	See
❑	1. Review any updates to system requirements	*Technical Requirements for Command Center for ESM*
❑	2. Complete the tasks mentioned in prerequisites	"Reviewing the Prerequisites" on page 81
❑	3. Upgrade the CDF You can use the automated process or perform a manual upgrade.	"Upgrading the CDF" on page 81
❑	4. Upgrade ESM for Fusion	"Upgrading ESM for Fusion" on page 86

17 Upgrading ESM for Fusion

This chapter describes how to upgrade ESM for Fusion. Perform the upgrade in the order listed below:

Reviewing the Prerequisites

Before upgrading ESM for Fusion, complete the following tasks:

1. Upgrade ArcSight Enterprise Security Manager to the latest version.
2. Download and untar the installation files, and then verify the signatures.

   You need the following images and files in the ESM for Fusion installer for upgrading:

   - `cdf-xxxx.xx.xxxx`
   - `arcsight-installer-metadata-x.x.x.tar`
   - `fusion-x.x.x.tar`
   - `esm-x.x.x.x.tar`
   - (Optional) `layered-analytics-x.x.x.x.tar`
3. Download the following file to a computer from which you will access the CDF Management Portal:

   `arcsight-installer-metadata-x.x.x.tar`

Upgrading the CDF

You can upgrade the CDF in the following ways:

Manually Upgrading the CDF

This section provides information about upgrading CDF manually.

Preparing for a Manual Upgrade

- Ensure that you have downloaded the ESM for Fusion package on all the CDF nodes. You need the following file in the package for upgrading the CDF:

  `cdf-xxxx.xx.xxxx`

- Ensure that you have minimum 50 GB free space in master node and 30 GB free space in worker node.
- Create a backup directory with minimum 30 GB of space on every node of your cluster:

  `mkdir /tmp/upgrade-backup`

  If you do not create a backup directory, the backup files will be stores in the default location (`\tmp`).
- Install `socat` and `container-selinux` packages on all nodes in the cluster by using the command:

  `yum install <package_name>`
- Ensure that you have appropriate permission to restart nodes. You may need to restart nodes if there is an issue during upgrade.
- Ensure that all nodes are currently running:

  `kubectl get nodes`
- Ensure that all pods are currently running:

  `<K8S_HOME>/bin/kube-status.sh`

Upgrading the CDF Manually

1. Run the following commands on each node:

   `cd <fusion_download_directory>/installers/cdf-xxxx.xx.xxxx`

   `./upgrade.sh -t <path_to_backup_directory> -i`

   Example:

   `cd /opt/esm-cmd-center-installer-for-fusion-x.x.x.x/installers/cdf-2020.05.x.x.x.x`

   `./upgrade.sh -t /tmp/upgrade-backup -i`

   NOTE: If you do not specify `-t <path>`, the backup files will be stored in the default location (`\tmp`).

   ---

2. Run the following commands on one of the master nodes:

   `cd <fusion_download_directory>/installers/cdf-xxxx.xx.xxxx`

   `./upgrade.sh -u`

   Example:

   `cd /opt/esm-cmd-center-installer-for-fusion-x.x.x.x/installers/cdf-2020.05.xxxx`

   `./upgrade.sh -u`

3 (Optional) Clean unused docker daemon images by executing the following command on all the worker and master nodes:

```
cd <fusion_download_directory>/installers/cdf-xxxx.xx.x.x.x.x
./upgrade.sh -c
```

Example:

```
cd /opt/esm-cmd-center-installer-for-fusion-x.x.x.x/installers/cdf-2020.05.x.x.x.x
./upgrade.sh -c
```

4 Ensure that upgrade is successful by verifying the following on all the nodes:

- Check the CDF version by executing the command:

  ```
  cat <K8S_HOME>/version.txt
  ```

  For example:

  ```
  cat /opt/arcsight/kubernetes/100.txt
  ```

- Check the current status of CDF pods by executing the command:

  ```
  <K8S_HOME>/bin/kube-status.sh
  ```

  For example:

  ```
  /opt/arcsight/kubernetes/bin/kube-status.sh
  ```

  NOTE: If the pods are not in running state, execute the following command to recreate main cluster services:

  ```
  <K8S_HOME>/bin/kube-restart.sh
  ```

Troubleshooting a Manual Upgrade

This section provides workarounds for the following problems that might occur during the CDF upgrade:

- If any of the upgrade process fails, complete the following steps:
  1. To ensure that `kubelet` is running, execute the following command:

     ```
     kubectl get pod -all-namespaces
     ```

  2. Rerun the upgrade command.
- If upgrade process timeouts, complete the following steps:
  1. Restart the node.
  2. To ensure that all the pods are in running state, execute the following command:

     ```
     <K8S_HOME>/bin/kube-status.sh
     ```

     For example:

     ```
     /opt/arcsight/kubernetes/bin/kube-status.sh
     ```

  3. Rerun the upgrade command.

Using the Automated Upgrade Process

You can run the CDF **automated upgrade** with a single command, requiring no interaction until completion of each phase. Typically, the upgrade process takes around 1 hour for a 3x3 cluster.

The automated upgrade allows you to upgrade the CDF from any host (known as the upgrade manager). The upgrade manager can be one of the following:

- One of the cluster nodes
- A host outside the cluster in a secure network location

The automated upgrade process generates the following directories:

- `/tmp/autoUpgrade` directory on the upgrade manager. This directory stores the upgrade process steps and logs.
- `/tmp/CDF_xxxx_upgrade`, a backup directory, on every node. This directory is approximately 1.7 GB.
- A working directory on the upgrade manager and every node at the location provided by the ***-d*** parameter. The upgrade package will be copied to this directory. This directory is approximately 9 GB. The automated upgrade process deletes this directory after the upgrade.

NOTE: You can create the working directory manually on upgrade manager and every node, and then pass as ***-d*** parameter to the auto-upgrade script. If you are a non-root user on the nodes inside the cluster, make sure you have permission to this directory.

Preparing for an Automated Upgrade

1. Ensure that you have downloaded the ESM for Fusion installer package to the download directory (<*download_directory*>) on the upgrade manager.

   Verify that you have CDF xxxx.xx upgrade packages in the following location:

   <*fusion_download_directory*>/installers/cdf-xxxx.xx.x.x.x.x/autoUpgrade.sh

   For example:

   ```
   cd /opt/esm-cmd-center-installer-for-fusion-x.x.x.x/installers/cdf-2020.05.x.x.x.x/autoUpgrade.sh
   ```

2. Install `socat` and `container-selinux` packages on all nodes in the cluster by using the command:

   yum install <*package_name*>

3. To configure passwordless SSH communication between the upgrade manager and all the nodes in the cluster, complete the following steps:

   3a To generate key pair, run the following command on the upgrade manager:

   ```
   ssh-keygen -t rsa
   ```

   3b To copy the generated public key to every node of your cluster, run the following command on the upgrade manager:

   ```
   ssh-copy-id -i ~/.ssh/id_rsa.pub root@<node_fqdn_or_ip>
   ```

Upgrading the CDF with the Automated Process

1 Change to the directory where you have downloaded the latest CDF package:

```
cd /<download-directory>/installers/cdf-xxxx.xx.xxxx/
```

2 Run the following command for automatic upgrade:

```
./autoUpgrade.sh -d /path/to/workinig_directory -n
{any_cluster_node_adress_or_ip}
```

For example:

```
./autoUpgrade.sh -d /tmp/upgrade -n pueas-ansi-node1.swinfra.net
```

3 Ensure that upgrade is successful by verifying the following on all the nodes:

- Check the CDF version by executing the command:

  ```
  cat <K8S_HOME>/version.txt
  ```

  For example:

  ```
  cat /opt/arcsight/kubernetes/100.txt
  ```

- Check the current status of CDF pods by executing the command:

  ```
  <K8S_HOME>/bin/kube-status.sh
  ```

  For example:

  ```
  opt/arcsight/kubernetes/bin/kube-status.sh
  ```

  NOTE: If the pods are not in running state, execute the following command to recreate main cluster services:

  ```
  <K8S_HOME>/bin/kube-restart.sh
  ```

4 Delete the auto-upgrade temporary directory and backup directory from the upgrade manager.

The auto-upgrade temporary directory contains the upgrade steps and logs. If you want to upgrade another cluster from the same upgrade manager, remove that directory.

```
rm -rf /tmp/autoUpgrade
rm -rf /tmp/CDF_xxxx_upgrade
```

Troubleshooting an Automated Upgrade

- If the automated upgrade fails, run `autoUpgrade.sh` again as outlined above. The process may take several attempts to succeed.
- In some cases, the automatic upgrade may return an error message about the upgrade process still running and the existence of a `*.lock` file which prevents `autoupgrade.sh` to continue. This file is automatically deleted in a few minutes. Alternatively, you can manually delete this file. Once the file is deleted either automatically or manually, run `autoUpgrade.sh` again.
- If the automated upgrade process is still unsuccessful, continue the process on the failed node using the procedure outlined in Manually Upgrading the CDF.

Uninstalling Analytics

The ESM for Fusion 7.3 release merges the Analytics capability with Fusion. Therefore, before upgrading ESM for Fusion, you must uninstall Analytics.

1. Open a new tab in a supported web browser.
2. Specify the URL for the CDF Management Portal:

   `https://<Fusion-server>:5443`

   Use the fully-qualified domain name of the host that you specified in the **Connection** step during the CDF configuration. Usually, this is the master node's FQDN.
3. Log in to the **CDF Management Portal** with the credentials of the administrative user that you provided during installation.
4. Select **Deployment** > **Deployments** > ⋮ > **Change**.
5. In the **Capabilities** page, deselect **Analytics**.
6. Click **Next** until you reach the **Configuration Complete** page.
7. Click **Next** after all the pods in the **Configuration Complete** page are displayed in green.

Upgrading ESM for Fusion

After upgrading the CDF and ESM, you can upgrade ESM for Fusion.

NOTE: For the upgrade, you must have at least temporary access to the configuration properties on the installed cluster. The upgrade process requires you to accept a certificate for the **Configuration** page in Step 4 on page 86. Otherwise, you might encounter certificate errors during the upgrade.

---

1. Open a new tab in a supported web browser.
2. Specify the URL for the CDF Management Portal:

   `https://<Fusion-server>:5443`

   Use the fully-qualified domain name of the host that you specified in the **Connection** step during the CDF configuration. Usually, this is the master node's FQDN.
3. Log in to the **CDF Management Portal** with the credentials of the administrative user that you provided during installation.
4. To accept the **Configuration** page certificate, complete the following steps:

   4a Select **Deployment** > **Deployments** > ⋮ > **Reconfigure**.

   4b Accept the certificate.
5. Switch to the **CDF Management Portal**.
6. Click **Deployment** > **Metadata**.
7. Click **+ADD** on the top-right and add the installer metadata file.

8 Click **Deployment** > **Deployments**.

Under **Update**, you will see a notification that indicates there are updates available to components in your cluster.

NOTE: If you know that there are updates but the Portal fails to provide a notification, we recommend that you clear the browser cache then refresh the page. Alternatively, you could change to private mode in the browser.

---

9 Click the notification icon, and then click the installer metadata link.

10 Since you have already downloaded the required files for upgrade, continue to click **Next** until you are in the **Import suite images** screen.

11 Launch a terminal session, then log in to the master node as `root` or as a sudo user.

12 Change to the following directory:

```
cd $K8S_HOME/scripts
```

For example:

```
cd /opt/arcsight/kubernetes/scripts
```

13 To upload the required images to the local registry, enter the following command:

```
./uploadimages.sh -d /<fusion_download_directory>/suite_images
```

When prompted for a password, enter the administrator password for the **CDF Management Portal**.

14 To ensure that the images have been uploaded, switch to the CDF Management Portal, then click **CHECK AGAIN**.

15 Click **Next** until you get the **Apply update** screen.

16 To apply the updates under **Fusion**, complete the following steps:

16a In **Cluster Configuration**, change **Search Engine Replicas** to **0**.

16b In **Database Configuration**, disable **Enable Database**.

16c (Conditional) Update the **ArcSight ESM Host Configuration** details if configured before upgrade.

17 Select **Deployment** > **Metadata**, and then delete the metadata file that is not in use.

18 To label the Fusion node, complete the following steps:

18a Select **Cluster** > **Nodes**.

18b In **Predefined Labels**, specify `fusion:yes` label and click **+**.

NOTE: Labels are case-sensitive. Ensure that you enter the values correctly.

18c (Conditional) Remove the obsolete `analytics:yes` label.

NOTE: This label will not be visible in the UI if you installed Fusion 1.0 using the script.

18d (Conditional) For single-node deployment, drag the newly added labels to the worker node.

18e (Conditional) For multi-node deployment, drag-and-drop the new label from the predefined set to each of the worker nodes based on your workload sharing configuration.

19 To configure ArcSight Command Center, complete the following steps:

19a Select **Deployment** > **Deployments** > ⋮ > **Change**.

19b In the **Capabilities** page, select **ArcSight Command Center**.

19c (Conditional) If you are using the **Active List** widget from the Fusion 1.0 release, select **Layered Analytics**.

NOTE: To use this capability, you must deploy both ArcSight Interset and ESM for Fusion in the same cluster.

19d Click **Next** until you reach the **Configuration Complete** page.

19e Click **Next** after all the pods in the **Configuration Complete** page are displayed in green.

20 Check the upgrade status by monitoring the pods' status:

20a Click **Cluster** > **Dashboard**.

20b In the left pane, switch to the *arcsight-installer-<XXXX>* **Namespace**.

20c Go to the **Pods** section and continue reloading the page until you see the status for all the pods as *Running*. On the **Status** column, sort the pod status to see if any pod is not running. Once the status for all the pods is changed to *Running*, the upgrade is complete.

21 To determine whether the upgrade is successful, complete the following steps:

21a Select **Deployment** > **Deployments**.

21b Under the **Version** column, you will see the new version of the suite.

Also, under the **Update** column, you will see zero, which indicates there are no updates available for components in your cluster.

22 To reload CDF images that the upgrade process removed, complete the following steps:

22a Change to the following directory:

```
cd $K8S_HOME/scripts
```

For example:

```
cd /opt/kubernetes/scripts
```

22b Run the following command:

```
./uploadimages.sh -d /<fusion_download_directory>/installers/cdf-2020.05.00100-2.3.0.7/cdf/images/
```

For example:

```
./uploadimages.sh -d /esm-cmd-center-installer-for-fusion-x.x.x.x/installers/cdf-2020.05.00100-2.3.0.7/cdf/images/
```

When prompted for a password, use the administrator password for the CDF Management Portal.

V Managing ArcSight Command Center for ESM

This section provides information about managing ESM for Fusion.

18 Configuring the Dashboard

ESM for Fusion allows you to perform the following configuration:

- Specify the log level for the Dashboard Metadata Web Application service.
- Specify the maximum number of days of data that the Dashboard can collect and display. The default value is **365 days**.

To configure your dashboard:

1. Open a new tab in a supported web browser.
2. Specify the URL for the CDF Management Portal:

   `https://<ESM_for_Fusion-server>:5443`

   Use the fully-qualified domain name of the host that you specified in the **Connection** step during the CDF configuration. Usually, this is the master node's FQDN.
3. Log in to the **CDF Management Portal** with the credentials of the administrative user that you provided during installation.
4. In the CDF Management Portal, click ⋮, and then select **Reconfigure**.
5. On the **Configuration** page, select the **FUSION** tab.
6. Under the **Dashboard Configuration** section, select the log level from the **Metadata Log Level** drop-down list.

   The default value is **info**.
7. In **Maximum Time Range (Days)**, specify the maximum number of days of data that the dashboard can collect and display.

   The default value is 365 days.

19 Using REST APIs with Fusion

The Fusion capability uses REST APIs to manage dashboard configurations, and you can access these APIs directly. For example, you might want to update a particular user's dashboard. You can access the *Dashboard Metadata REST API Documentation* for the Dashboard at the following URL:

```
https://<ESM_for_Fusion Server>/metadata/rest-api-docs
```

NOTE: For single sign-on access to the REST APIs, specify the values for **Client ID** and **Client Secret**, in the **Single Sign-on Configuration** section. For more information, see step 9 in the Deploying Fusion section.

---

20 Restarting Nodes in the Cluster

To restart or shut down any node in the ESM for Fusion cluster, you must stop the Kubernetes services running on the node. Otherwise, the Kubernetes pods will not start after the restart.

You can restart nodes in one of the following ways:

- "Restarting Nodes by Using Scripts" on page 95
- "Restarting Nodes Manually" on page 95

Restarting Nodes by Using Scripts

Applies only if you installed ESM for Fusion by using scripts.

1. Log in to the node that you need to restart.
2. To restart the node, execute the following command:

   `/opt/fusion/bin/single-node-util.sh reboot_node`
3. (Conditional) If restart fails, perform a hard reboot of the node.

Restarting Nodes Manually

Applies only if you installed ESM for Fusion manually.

1. (Conditional) If the node contains CDF, perform the following steps:
   - **1a** Log in as `root` to the node that you need to restart.
   - **1b** Change to the following directory:

     `cd <K8S_HOME>/bin/`

     For example:

     `cd /opt/arcsight/kubernetes/bin/`
   - **1c** Stop the kubernetes services by using the following command:

     `kube-stop.sh`
   - **1d** Unmount Kubernetes volumes by using the following command:

     `kubelet-umount-action.sh`
2. Restart the node using the following command:

   `reboot`
3. (Conditional) If restart fails, perform a hard reboot of the node.
4. (Conditional) After the node restarts, perform the following steps if the node contains CDF:
   - **4a** Log in as `root` to the node.
   - **4b** Change to the following directory:

```
cd <K8S_HOME>/bin/
```

For example:

```
cd /opt/arcsight/kubernetes/bin/
```

4c Check whether all Kubernetes services are running:

```
kube-status.sh
```

4d (Conditional) If any service is not running, start the service by using the command:

```
kube-start.sh
```

21 Resetting the CDF Administrator Password

To change the administrator password of the CDF Management Portal, complete the following steps:

1. Log in to the CDF Management Portal (`https://<Fusion Server>:5443`) using the administrator user ID and password that you specified during the CDF installation.
2. On the main page, click **Application** > **IdM Administration**.
3. Click the **SRG** image.
4. In **Organization**, click **Users**.
5. In the list of users on the right, select **Admin**, and then click **Edit**.
6. Click **Remove Password**.
7. Click **Add Password**.
8. Enter a new administrator password.
9. Click **Save**.

22 Renewing CDF Certificates

The validity of a CDF certificate is one year. If you do not upgrade the CDF certificate within one year, the certificate will expire and you must renew the certificate. The CDF certificates can be renewed before and after expiration.

CDF contains the following certificates:

- Internal certificates, which are used within the cluster nodes, such as `client.crt`, `client.key`, `server.crt`, `server.key`, `kubernetes.crt`, and `kubernetes.key`.
- External certificates, which are used for the ingress service of the CDF Management Portal.

Renewing Certificates Before Expiration

You can renew both internal and external certificates before expiration.

1. Log in to the master node.
2. Change to the following directory:

   `cd <k8s_HOME>`

   For example:

   `cd /opt/arcsight/kubernetes`
3. (Conditional) For internal certificates, run the following command to generate new certificates:

   `./scripts/renewCert --renew -t internal`

   In a multi-node deployment, executing the above command automatically distributes the new certificates to all nodes in the cluster.
4. (Conditional) For external certificates, run the following command to generate new certificates:

   `./scripts/renewCert --renew -t external`

Renewing Certificates After Expiration

You can renew both internal and external certificates after expiration.

1. Log in to the master node.
2. Change to the following directory:

   `cd <k8s_HOME>`

   For example:

   `cd /opt/arcsight/kubernetes`

3 (Conditional) For an internal certificate, complete the following steps:

3a To generate new `client.crt`, `client.key` and `server.crt` certificates, run the following command:

```
./scripts/renewCert --renew -V 365 -t internal
```

3b (Conditional) If you have multiple master nodes, run the following command on all the master nodes:

```
./scripts/renewCert --renew -t internal
```

4 (Conditional) For external certificates, run the following command:

- To generate new external self-signed certificates:

  ```
  ./scripts/renewCert --renew -t external
  ```

- To generate the external custom self-signed certificates:

  ```
  ./scripts/renewCert --renew -t external --tls-cert /<cert file directory>/<cert file> --tls-key <private key directory>/<private key> [--tls-cacert <CA cert directory>/<CA cert file>]
  ```

23 Creating and Adding CDF Certificate Authority

The cluster maintains its own certificate authority (CA) to issue certificates for external communication. A self-signed CA is generated during the installation of CDF by default. Pods of the deployed products use the certificates generated by the CA on pod startup. When configuring SSL, you must create a new CA and add the CA to CDF, which will be used by all the products in the cluster.

IMPORTANT: If you change the CA after deploying ESM for Fusion, you will have to uninstall and reinstall the CDF suite. Uninstalling the CDF suite will also uninstall all the installed capabilities such as Fusion, ArcSight Command Center, and ArcSight Layered Analytics. We recommend that you perform this procedure when you first install ESM for Fusion to avoid downtime and data loss.

To create a new CA and add the CA to CDF:

1 To create a new CA, complete the following steps:

1a Create a directory and configure the directory permissions using the following command:

```
mkdir /root/ca
cd /root/ca
mkdir certs crl newcerts private
chmod 700 private
touch index.txt
echo 1000 > serial
```

1b Open the configuration file in a text editor (`vi /root/ca/openssl.cnf`).

1c Add the following content to the configuration file:

NOTE: The values shown here are examples. You should change parameter values to match your environment.

```
# OpenSSL root CA configuration file.
# Copy to `/root/ca/openssl.cnf`.
[ ca ]
default_ca = CA_default
[ CA_default ]
# Directory and file locations.
dir = /root/ca
certs = $dir/certs
crl_dir = $dir/crl
new_certs_dir = $dir/newcerts
database = $dir/index.txt
serial = $dir/serial
RANDFILE = $dir/private/.rand
# The root key and root certificate.
```

```
private_key = $dir/private/ca.key.pem
certificate = $dir/certs/ca.cert.pem
# For certificate revocation lists.
crlnumber = $dir/crlnumber
crl = $dir/crl/ca.crl.pem
crl_extensions = crl_ext
default_crl_days = 30
# SHA-1 is deprecated, so use SHA-2 instead.
default_md = sha256
name_opt = ca_default
cert_opt = ca_default
default_days = 375
preserve = no
policy = policy_strict
[ policy_strict ]
# The root CA should only sign intermediate certificates that match.
# See the POLICY FORMAT section of `man ca`.
countryName = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
[ policy_loose ]
# Allow the intermediate CA to sign a more diverse range of
certificates.
# See the POLICY FORMAT section of the `ca` man page.
countryName = optional
stateOrProvinceName = optional
localityName = optional
organizationName = optional
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
[ req ]
# Options for the `req` tool (`man req`).
default_bits = 2048
distinguished_name = req_distinguished_name
string_mask = utf8only
# SHA-1 is deprecated, so use SHA-2 instead.
default_md = sha256
# Extension to add when the -x509 option is used.
x509_extensions = v3_ca
[ req_distinguished_name ]
countryName = Country
stateOrProvinceName = State
localityName = Locality
0.organizationName = EntCorp
organizationalUnitName = OrgName
commonName = Common Name
emailAddress = Email Address
# Optionally, specify some defaults.
countryName_default = <your country code>
stateOrProvinceName_default = <your state or province>
localityName_default =
```

```
0.organizationName_default = <your company name>
organizationalUnitName_default =
emailAddress_default =
[ v3_ca ]
# Extensions for a typical CA (`man x509v3_config`).
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, digitalSignature, cRLSign, keyCertSign
[ v3_intermediate_ca ]
# Extensions for a typical intermediate CA (`man x509v3_config`).
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true, pathlen:0
keyUsage = critical, digitalSignature, cRLSign, keyCertSign
[ usr_cert ]
# Extensions for client certificates (`man x509v3_config`).
basicConstraints = CA:FALSE
nsCertType = client, email
nsComment = "OpenSSL Generated Client Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, nonRepudiation, digitalSignature,
keyEncipherment
extendedKeyUsage = clientAuth, emailProtection
[ server_cert ]
# Extensions for server certificates (`man x509v3_config`).
basicConstraints = CA:FALSE
nsCertType = server
nsComment = "OpenSSL Generated Server Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer:always
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
[ crl_ext ]
# Extension for CRLs (`man x509v3_config`).
authorityKeyIdentifier=keyid:always
[ ocsp ]
# Extension for OCSP signing certificates (`man ocsp`).
basicConstraints = CA:FALSE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, digitalSignature
extendedKeyUsage = critical, OCSPSigning
```

1d To generate a CA root key, run the following commands:

```
cd /root/ca
openssl genrsa -out private/ca.key.pem 4096
chmod 400 private/ca.key.pem
```

1e To create a CA cert, run the following command:

```
openssl req -config openssl.cnf -key private/ca.key.pem -new -x509 -
days 375 -sha256 -extensions v3_ca -out certs/ca.cert.pem
```

1f To verify the root CA, run the following commands:

```
chmod 444 certs/ca.cert.pem
openssl x509 -noout -text -in certs/ca.cert.pem
```

2 To add the CA, run the following command:

```
<K8S_HOME>/scripts/cdf-updateRE.sh write --re-key=private/ca.key.pem --
re-crt=certs/ca.cert.pem --re-ca=certs/ca.cert.pem
```

For example:

```
opt/arcsight/kubernetes/scripts/cdf-updateRE.sh write --re-key=private/
ca.key.pem --re-crt=certs/ca.cert.pem --re-ca=certs/ca.cert.pem
```

3 To verify, read the CDF CA file by executing the following command and ensure that it is same as the `ca.cert.pem` file. You must execute the following command on the initial master node:

```
<K8S_HOME>/scripts/cdf-updateRE.sh read
```

For example:

```
opt/arcsight/kubernetes/scripts/cdf-updateRE.sh read
```

24 Configuring the Log Level

The log levels for ESM for Fusion are set to **Info** by default. You can configure the log level as desired for troubleshooting purposes.

To configure the log level:

1. Log in to the CDF Management Portal.
2. Click ⋮ of `arcsight-installer` and click **Reconfigure**.
3. Click **ESM Command Center**.
4. Select the appropriate log level.
5. Click **Save**.

25 Collecting Diagnostic Logs

Diagnostic log files helps in investigating and troubleshooting issues. This section provides information about collecting diagnostic logs for ESM for Fusion.

To collect diagnostic logs:

1. Log in to the CDF master node as `root`.
2. Change to the directory where you installed ESM for Fusion:

   ```
   cd /opt/esm
   ```

   Alternatively, if you have installed manually, you can find the `support_utils` script in the location where you extracted the ESM for Fusion installer. For example, `/opt/esm-x.x.x.x`.
3. Execute the script to generate logs:

   ```
   ./support_utils.sh
   ```
4. If you want to collect the operating system logs, specify `Y` to install the `sos` package. Otherwise, specify `N`.

   The `sos` package is required to generate the operating system logs. Installation of the `sos` package is a onetime activity.
5. Specify the password to encrypt the output file.

   The encrypted log file is stored in the location:

   `/opt/support_util/<ddmmyyyyhhmmss>`

   For example:

   `/opt/support_util/07072020043015`
6. To view the logs, you must decrypt the file as follows:

   6a Change to the directory where the log file is stored.

   For example:

   ```
   cd /opt/support_util/07072020043015
   ```

   6b Execute the command:

   ```
   dd if=<log_file_name> | openssl aes-256-cbc -md sha1 -d -k <Encrypt-Password> | tar zxf -
   ```

   For example:

   ```
   dd if=esm-support-util-20200707043015.aes | openssl aes-256-cbc -md sha1 -d -k <Encrypt-Password> | tar zxf -
   ```

VI Appendices

This section provides additional information for managing your ESM for Fusion environment.

A Understanding the Pods that Manage Deployed Containers

When you deploy ESM for Fusion, Fusion, and Layered Analytics, the process creates several Kubernetes pods to ensure the functionality of the containers that support these products. A **pod** is a group of containers that are deployed and managed together as a single unit. The pods have specifications for running the containers and can share storage and network resources. Pods always runs on a **node**, which is a worker machine in Kubernetes.

Pods for the Deployed Capabilities

The following pods support the functionality of ESM for Fusion, Fusion, and Layered Analytics. Each pod corresponds to a specific label that you apply to the nodes working with the pod.

Pod Name	Description	Deployed with	Label
common-doc-web-app	Contains the Help files for the Fusion features and the REST APIs	Fusion	fusion:yes
dashboard-metadata-web-app	Contains the Dashboard metadata of the REST API	Fusion	fusion:yes
dashboard-web-app	Manages the uer interface for the Dashboard	Fusion	fusion:yes
database-monitoring-web-app	Contains the REST API for database monitoring When this pod starts up, it also installs the **Health and Performance Monitoring** dashboard, as well as the widgets that are in that dashboard	Fusion	fusion:yes
hercules-common-services	Supports the core services, such as the navigation menu capability	Fusion	fusion:yes
hercules-management	Supports the user account and role management, authentication, for the Fusion user interface and the user interfaces that integrate with it. User and role data is stored within an embedded H2 database. Note: This is a separate user population than CDF Management Portal UI, which uses "idm" pod.	Fusion	fusion:yes
hercules-osp	Supports the single sign-on service and authentication	Fusion	fusion:yes
hercules-rethinkDB	Supports the RethinkDB database, which stores user configuration and preference information, such as a user's dashboards and favorites	Fusion	fusion:yes

Pod Name	Description	Deployed with	Label
hercules-search-engine	Provides APIs to access data in database	Fusion	fusion:yes
layered-analytics-widgets	Supports the out-of-the-box widgets and dashboard that blend data from two or more deployed capabilities When this pod starts up, it installs the **Entity Priority** dashboard and the **Active List** widget, which connects to an ESM Manager server running outside of the Kubernetes cluster	ArcSight Layered Analytics	fusion:yes
esm-widgets	Supports the out-of-the-box widgets and dashboards for ESM case management activities When this pod starts up, it installs the **How is my SOC running?** dashboard and the related widgets, which connect to an ESM Manager server running outside of the Kubernetes cluster	ArcSight ESM Command Center	fusion:yes
esm-acc-web-app	Manages the interface for the ESM Command Center console, which connects to an ESM Manager server running outside of the Kubernetes cluster	ArcSight ESM Command Center	fusion:yes

Pods for the CDF Management Portal

The following pods represent functions in the CDF Management Portal, which are common to any deployed capability.

Pod Name	Description
autopass-lm	Supports the service that manages license keys
itom-pg-backup	Supports the backup and restoration of the databases in the suite
nginx-ingress-controller	Provides a proxy server to which end-users connect in web browser on HTTPS port 443
suite-reconf-pod-arcsight-installer	Supports the functions for reconfiguring the CDF Management Portal

B Troubleshooting

Refer to the following section if you are experiencing a problem with ESM for Fusion.

Authentication Failure while accessing ArcSight Command Center

Issue: You detect an authentication failure (an error in validating the access token) while accessing ArcSight Command Center.

Workaround: Configure NTP in the nodes because time synchronization is important for SSO components.

Identifying Location of the Scripts Available in the Installer For ESM for Fusion

Issue: You want to identify the location of the scripts available in the ESM for Fusion installer.

Workaround: The scripts available in the ESM for Fusion installer are present at the following location:

- `/<installer directory>/scripts/`
- `/<K8S_HOME>/bin/`, by default `/opt/arcsight/kubernetes/bin/`

Checking the Log File of a Specific Pod/Container Using Kubernetes Dashboard

Issue: You want to check the log file of a specific pod/container using kubernetes dashboard.

Workaround: Perform the following steps to check the log file of a specific pod/container using Kubernetes dashboard:

1. Open a new tab in a supported web browser.
2. Specify the URL for the CDF Management Portal:

   `https://ESM_for_Fusion_server:5443`

   Use the fully qualified domain name of the host that you specified in the **Connection** step during the CDF configuration. Usually, this is the master node's FQDN.
3. Log in to the **CDF Management Portal** with the credentials of the administrative user that you provided during installation.
4. Click **Cluster** > **Dashboard** > **Namespaces** (select **arcsight-installer-***) > **Pods**.
5. Under **Pods**, click the pod for which you want to see the logs.
6. Click **View Logs**.

Debugging the Old Logs for a Specific Container

Issue: You want to debug the old logs for a specific container.

Workaround: Navigate to the following location to debug the old logs for a specific container:

`</opt/NFS_Volume/>/itom-logging-vol`

For example:

```
/opt/NFS_Volume/itom-logging-vol/container/dashboard-web-app-*_arcsight-installer-*_dashboard-web-app-*.log.20200*
```

Configuring Log Level in the CDF Management Portal for Detailed Logs

Issue: You want to configure the log level in the CDF Management Portal for detailed logs.

Workaround for Dashboard-Web-App:

1. Open a new tab in a supported web browser.
2. Specify the URL for the CDF Management Portal:

   `https://ESM_for_Fusion_server:5443`

   Use the fully qualified domain name of the host that you specified in the **Connection** step during the CDF configuration. Usually, this is the master node's FQDN.
3. Login to the **CDF Management Portal** with the credentials of the administrative user that you provided during installation.

4 Click **Cluster** > **Dashboard** > **Namespaces**.

5 For the namespace, select **arcsight-installer-***.

6 Select **Deployments**.

7 Select **dashboard-web-app**.

8 Click **Edit**.

9 Change the `LOG_LEVEL env variable` value to `debug/warn/trace/error`.

10 Click **Update**.

Workaround for Dashboard-Metadata-Web-App:

1 Open a new tab in a supported web browser.

2 Specify the URL for the CDF Management Portal:

`https://ESM_for_Fusion_server:5443`

Use the fully qualified domain name of the host that you specified in the **Connection** step during the CDF configuration. Usually, this is the master node's FQDN.

3 Log in to the **CDF Management Portal** with the credentials of the administrative user that you provided during installation.

4 In the **CDF Management Portal**, click the ⋮ icon for the installed suite.

5 Select **Reconfigure**.

6 On the **Configuration** page, select **FUSION**.

7 Select a log level from **Dashboard log level** and **Metadata log level**.

8 Click **Save**.

Monitoring the Health of the Nodes and Pods using Kubernetes Dashboard

Issue: You want to monitor the health of the nodes and pods using kubernetes dashboard.

Workaround to monitor the health of the nodes:

1 Open a new tab in a supported web browser.

2 Specify the URL for the CDF Management Portal:

`https://ESM_for_Fusion_server:5443`

Use the fully qualified domain name of the host that you specified in the **Connection** step during the CDF configuration. Usually, this is the master node's FQDN.

3 Login to the **CDF Management Portal** with the credentials of the administrative user that you provided during installation.

4 Select **Cluster** > **Dashboard** > **Cluster** > **Nodes**.

Workaround to monitor the health of the pods:

1. Open a new tab in a supported web browser.
2. Specify the URL for the CDF Management Portal:

   `https://ESM_for_Fusion_server:5443`

   Use the fully qualified domain name of the host that you specified in the **Connection** step during the CDF configuration. Usually, this is the master node's FQDN.
3. Log in to the **CDF Management Portal** with the credentials of the administrative user that you provided during installation.
4. Click **Cluster** > **Dashboard** > **Namespaces** (select **arcsight-installer-***) > **Pods**.

Checking the Status of the Pods for All the Namespaces

Issue: You want to check the status of the pods for all the namespaces.

Workaround: To check the status of all the pods for all the namespaces use the following command:

```
kubectl get pods --all-namespaces
```

Checking the Physical and Internal IP Details of All the Pods

Issue: You want to check the physical and internal IP details of all the pods.

Workaround: To check the physical and internal IP details of all the pods use the following command:

```
kubectl get pods -n arcsight-installer-htzzp -o wide
```

Checking the Log File of a Specific Pod/Container using Command Line

Issue: You want to check the log file of a specific pod/container using command line.

Workaround: To check the log files of the pods of `dashboard-web-app`, `dashboard-metadata-web-app`, `Hercules-management`, use the following command:

```
kubectl logs -f -n <namespace>  <pod_name> -c <container_name>
```

Example:

```
kubectl logs -f -n arcsight-installer-htzzp dashboard-web-app-57f4675759-m6zbk -c dashboard-web-app
```

Encountering an Unsuccessful Installation

Issue: You encounter an unsuccessful installation.

Workaround: If you encounter an unsuccessful installation, use the following command:

`/<k8s-home>/log/scripts`

For example:

`/opt/arcsight/kubernetes/log/scripts`

Understanding which Functionality is Affected if there is an Error in a Container's Log

Issue: You want to understand which functionality is affected if there is an error in a container's log.

Workaround: Check the following information:

- Description of Namespaces
- Description of Pods/Containers

C Uninstalling ESM for Fusion

You can uninstall ESM for Fusion in the following ways.

Uninstalling by Using the Script

You can uninstall ESM for Fusion by using the script only if the installer files are available in the following locations:

- **Kubernetes:** `/opt/arcsight/kubernetes`
- **NFS Volumes:** `/opt/arcsight`

If the installer files are in a different location, you must uninstall manually using the CDF Management Portal. For more information, see "Uninstalling Manually" on page 119.

To uninstall ESM for Fusion with the script:

1. Log in as `root` to the master node.
2. Change to the directory where you extracted the ESM for Fusion installation files:

   `cd <installer_directory>`
3. Execute the script by using the following command:

   `./uninstall-single-node.sh`

Uninstalling Manually

You can choose to remove ESM for Fusion from the CDF, or uninstall the CDF.

Uninstalling ESM for Fusion

This section provides information about uninstalling ESM for Fusion manually.

1. Log in to the CDF Management Portal.
2. Click **Deployment** > **Deployments**.
3. Click the ⋮ icon of `arcsight-installer`.
4. Click **Uninstall**.

Uninstalling the CDF

This section provides information about uninstalling the CDF manually. When you uninstall the CDF, you all remove all deployed capabilities, such as ESM for Fusion.

1. Log in to the CDF master node.
2. Change to the CDF installation directory using the following command.

   ```
   cd <k8s_home>
   ```

   For example:

   ```
   cd opt/arcsight/kubernetes
   ```
3. Uninstall CDF using the following command:

   ```
   ./uninstall.sh -r false
   ```
4. Reboot the server.