ArcSight Platform 2.3.0
Technical Requirements

July 2020

About These Technical Requirements

The ArcSight Platform (the Platform) is not a licensed product. Rather, it serves as the structure that enables you to deploy a combination of security, user, and entity solutions into a single Container Deployment Foundation (CDF) environment. A common layer called Fusion provides the core services for this CDF environment, including the Dashboard, user management, and single sign-on configuration. This document describes the common hardware and software requirements for the Fusion layer that you deploy with a product solution such as ArcSight Recon.

Micro Focus recommends the fully tested and certified platforms described in this document. However, customers running on other platforms or with untested configurations will be supported until the point Micro Focus determines that the root cause is the uncertified platform or configuration. Issues that can be reproduced on the certified platforms will be prioritized and fixed according to standard defect-handling policies.

- Chapter 1, "Available Product Versions and Upgrade Paths," on page 7
- Chapter 2, "Software Requirements," on page 9
- Chapter 3, "Hardware Requirements," on page 11
- Chapter 4, "Network File System," on page 13
- Chapter 5, "Ports Used," on page 15

For more information about support polices, see Support Policies.

Additional Documentation

The ArcSight Platform documentation library includes the following resources:

- *Release Notes for ArcSight Platform*, which provides information about the latest release and information that applies to all products that you can deploy in the Platform
- *User Guide for Fusion*, which is embedded in the product to provide both contextual Help and conceptual information
- Administrator Guides for the products that you can deploy in the Platform, which provide information about deploying, configuring, and maintaining the product

For the most recent version of this guide and other 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/.

Contents

1 Available Product Versions and Upgrade Paths

This version of the Platform supports the following deployed products and their upgrade paths. For more information about the products that you can deploy, see their respective Release Notes posted on the documentation site for ArcSight Platform.

Product	Supported Version	Upgrade from Version
ArcSight Enterprise Security Manager	7.3.0	7.2.1 7.2.0
ArcSight Interset SE	6.1.0	none
ArcSight Recon	1.0.0	ArcSight Investigate 3.1.0
ArcSight Transformation Hub	3.3.0	3.2.0
NetIQ Identity Intelligence	1.1.2	1.1.1

2 Software Requirements

This section lists the common minimum software requirements for the Fusion component that you deploy with most product solutions in this version of the Platform. The individual products likely have additional requirements which you can access from the documentation site for ArcSight.

Minimum Software Requirements

Category	Minimum Requirement
Operating systems	A **minimal** installation of one of the following: ◆ Red Hat Enterprise Linux 8.1 (x86, x64) ◆ Red Hat Enterprise Linux 7.8 or later (x86, x64) ◆ Red Hat Enterprise Linux 7.7 or later (x86, x64) ◆ CentOS 8.1 (x86, x64) ◆ CentOS 7.8 (x86, x64)
File systems	One of the following: ◆ EXT3 ◆ EXT4 (recommended) ◆ Logical Volume Manager (LVM) ◆ XFS
Browser	◆ Google Chrome ◆ Mozilla Firefox **NOTE:** Browsers should not use a proxy to access CDF ports 5443 or 3000 applications because this might result in inaccessible web pages.

3 Hardware Requirements

These guidelines apply to the requirements for deploying Fusion in the ArcSight Platform on a single node. You might have other components deployed to that node, such as ESM Command Center or Recon, which have additional requirements. These hardware requirements are based on dedicated resources allocations. In virtual environments, where there is a risk of over-subscription of the physical hardware, ensure that your ArcSight Platform environment meets these hardware requirements to avoid installation and functionality issues.

If you install Fusion on the same node as another deployed capability, such as Recon, you should keep some unused resource capacity on the node. For more information, see the *Technical Requirements* and the *Administrator's Guide* for the products that you want to deploy.

- ◆ "System Sizing" on page 11
- ◆ "Disk Space" on page 11

System Sizing

This section provides guidance for node requirements needed to run Fusion in the ArcSight Platform. Each capability that you deploy with Fusion will have requirements. Please review the *Technical Requirements* for those specific products.

Category	Requirement
Worker nodes	1
vCores (per node)	8
RAM (per node)	32 GB
Disk space (per node)	50 GB

Disk Space

This section lists the minimum disk space needed to run Fusion in the ArcSight Platform. Each capability that you deploy with Fusion will have additional disk space requirements. Please review the *Technical Requirements* for those specific products.

Partition	Disk Space
/opt	200 GB
swap	16 GB
/home	50 GB

4 Network File System

The Platform supports several options for a network file system (NFS) for your deployed products.

- ◆ "Required File Systems" on page 13
- ◆ "Minimum Directory Sizes for the NFS" on page 13

Required File Systems

Category	Minimum Requirement
NFS Types	◆ Amazon EFS ◆ HPE 3PAR File Persona ◆ Linux-based NFS ◆ NetApp
NFS Server Versions	◆ NFSv4 ◆ NFSv3

Minimum Directory Sizes for the NFS

The following table lists the minimum required size for each of the NFS installation directories.

Directory	Minimum Size
{NFS_VOLUME_DIRECTORY}/itom-vol	130 GB
{NFS_VOLUME_DIRECTORY}/itom-vol/db-single-vol	Depends, but start with 10 GB
{NFS_VOLUME_DIRECTORY}/itom-vol/db-backup-vol	Depends, but start with 10 GB
{NFS_VOLUME_DIRECTORY}/itom-vol/itom-logging-vol	Depends, but start with 40 GB
{NFS_VOLUME_DIRECTORY}/arcsight-vol	10 GB

5 Ports Used

Fusion uses specific firewall ports. Therefore, ensure that these ports are available.

- "CDF Management Portal" on page 15
- "CDF" on page 15
- "Kubernetes" on page 16
- "NFS" on page 17

CDF Management Portal

All ports use TCP protocol.

Ports	Node	Description
3000	Master	Used only for accessing the CDF Management portal during CDF installation from a web browser. Web clients must be able to access this port during the installation of CDF. After installation, web clients use port 5443 to access the CDF Management portal.
5443	Master	Used for accessing the CDF Management portal post CDF deployment from a web browser. Web clients must be able to access this port for administration and management of CDF.
5444	Master	Used for accessing the CDF Management portal post CDF deployment from a web browser, when using two-way (mutual) SSL authentication. Web clients must be able to access this port for administration and management of CDF, when using two-way (mutual) SSL authentication.

CDF

All ports use TCP protocol.

Ports	Node	Description
8200	Master	Used by the `itom-vault` service which provides a secured configuration store. All cluster nodes should be able to access this port for the client connection.

Ports	Node	Description
8201	Master	Used by the `itom-vault` service which provides a secured configuration store. All cluster nodes should be able to access this port for peer member connections.

Kubernetes

All ports use TCP protocol, unless otherwise noted.

Ports	Node	Description
2380	Master	Used by the `etcd` component which provides a distributed configuration database. All the master nodes should be able to access this port for the `etcd` cluster communication.
4001	Master	Used by the `etcd` component which provides a distributed configuration database. All cluster nodes should be able to access this port for the client connection.
5000	Master	Used by `kube-registry` component which handles the management of container image delivery. All cluster nodes should be able to access this port to communicate with the local container registry.
7443	Master	*(Conditional)* Used by the Kubernetes API server when you perform one of the following methods of installation: ◆ Use the provided scripts ◆ Install manually and on the same node as Fusion All cluster nodes should be able to access this port for internal communication.
8443	Master	*(Conditional)* Used by the Kubernetes API server when you manually install and the installation is not on the same node as Fusion. All cluster nodes should be able to access this port for internal communication.
8472	All nodes	*Uses UDP protocol* Used by the Flannel service component which manages the internal cluster networking. All cluster nodes should be able to access this port for internal communication.
10250	All nodes	Used by the Kubelet service which functions as a local node agent that watches pod specifications through the Kubernetes API server. All cluster nodes should be able to access this port for internal communications and worker node Kubelet API for exec and logs.

Ports	Node	Description
10251	All nodes	Used by `Kube-scheduler` component that watches for any new pod with no assigned node and assigns a node to the pod.
		All cluster nodes should be able to access this port for internal communication.
10252	All nodes	Used by `kube-controller-manager` component that runs controller processes which regulate the state of the cluster.
		All the cluster nodes should be able to access this port for internal communication.
10256	All nodes	Used by the `Kube-proxy` component, which is a network proxy that runs on each node, for exposing the services on each node.
		All the cluster nodes should be able to access this port for internal communication.

NFS

All ports use TCP protocol.

Ports	Node	Description
111	NFS server	Used by `portmapper` service.
		All cluster nodes should be able to access this port.
2049	NFS server	Used by `nfsd` daemon.
		All the cluster nodes should be able to access this port.
		NOTE: This port must be open even during a single-node deployment.
20048	NFS server	Used by `mountd` daemon.
		All the cluster nodes should be able to access this port.