MICRO FOCUS

ArcSight Recon 1.0

Technical Requirements

October 2020

Legal Notice

About These Technical Requirements

Micro Focus recommends the tested platforms listed below. However, customers running on any platforms not provided in this list or with untested configurations will be supported until the point Micro Focus determines that the root cause is the untested platform or configuration. Issues that can be reproduced on the tested platforms will be prioritized and fixed according to standard defect-handling policies.

For more information about support polices, see Support Policies.

For information about installation, see the *Administrator Guide to ArcSight Recon*.

Additional Documentation

The ArcSight Recon documentation library includes the following resources:

- *Release Notes for ArcSight Recon*, which provides information about the current release
- *Administrator Guide to ArcSight Recon*, which provides information about deploying, configuring, and maintaining this product
- *User Guide to ArcSight Recon*, which is embedded in the product to provide both contextual Help and conceptual information

For the most recent version of the system requirements and other Recon documentation resources, visit the documentation for ArcSight Recon.

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 Software Requirements

This section lists the software needed to install and run ArcSight Recon.

Category	Minimum Requirement
Operating systems (**minimal** installation)	For Recon: ◆ Red Hat Enterprise Linux 7.7 (x86, x64) ◆ Red Hat Enterprise Linux 7.8 (x86, x64) ◆ Red Hat Enterprise Linux 8.1 (x86, x64) ◆ CentOS 8.1 (x86, x64) ◆ CentOS 7.8 (x86, x64) ◆ CentOS 7.7 (x86, x64) For the database: ◆ Red Hat Enterprise Linux 7.8 (x86, x64) ◆ Red Hat Enterprise Linux 7.7 (x86, x64) ◆ CentOS 7.8 (x86, x64) ◆ CentOS 7.7 (x86, x64)
File systems	One of the following: ◆ EXT3 ◆ EXT4 (recommended) ◆ Logical Volume Manager (LVM) ◆ XFS
Data Processing	Transformation Hub 3.3.0 **NOTE:** If you have not already deployed Transformation Hub in your environment, the Recon installation package includes the needed image. For documentation, see the Transformation Hub documents.
Fusion	Fusion 1.1.0 **NOTE:** If you have not already deployed Fusion in your environment, the Recon installation package includes the needed image.
Data Collection	SmartConnector 7.14 or later Provided with the ArcSight Recon download

Category	Minimum Requirement
Browser	◆ Google Chrome ◆ Mozilla Firefox **NOTE:** Browsers should not use a proxy to access Container Deployment Foundation (CDF) application because this might result in inaccessible web pages.

2 Hardware Requirements and Tuning Guidelines

The guidelines in this section are for a deployment where you install all of the following software:

- Database
- Transformation Hub
- Fusion
- Recon

The hardware requirements are based on dedicated resource allocations. In virtual environments, where there is a risk of over subscription of the physical hardware, ensure that the ArcSight Recon system meets these hardware requirements to avoid installation and functionality issues.

- "Understanding the Workload for Recon" on page 9
- "System Sizing for a Small Workload" on page 9
- "System Sizing for Medium Workload" on page 11

NOTE: The system sizing was tested in an ArcSight Recon environment without SSL communication.

Understanding the Workload for Recon

The total workload for Recon depends on your data received through SmartConnectors or ArcSight Enterprise Security Manager (ESM) and on the number of events captured by those data sources each day. For example, each day, your environment might have thousands of events. At the same time, someone might be updating details about the events or new information can be coming in about the entities associated with the events. Recon must be able to process all of these types of transactions. Thus, this document lists the requirements for small and medium workloads.

We based these recommendations on the maximum workload achievable while still maintaining stability of the system resources in our labs. It is possible that you might need to further adjust the tuning values for satisfactory peformance in your environment.

System Sizing for a Small Workload

This section helps you in determining whether your environment might meet the requirements for a small workload environment. It provides guidance for hardware requirements and tuning the performance of the workload. You might compare this information with the guidance for medium workloads.

- "Workload Distribution for a Small Workload" on page 10
- "System Sizing for a Small Workload" on page 10

Workload Distribution for a Small Workload

The following table provides an example of how event ingestion activities might occur in a small workload:

Application	Category	Expected Workload
Microsoft Windows	Events per second	375
Fortinet Fortigate	Events per second	375
Infoblox NIOS	Events per second	375
Blue Coat, Check Point, Cisco	Events per second	375
ArcSight Recon	Events per second	1500
	Searches (concurrent)	3

System Sizing for a Small Workload

Category	Requirement
Single node (master and worker)	1
CPU cores (per node)	8
RAM (per node)	32
Disks (per node)	1
Storage per day (1x)	15 GB
Total disk space (1.5 billion Events)	500 GB

Vertica Resource Pools Tuning for a Small Workload

Category	Property	Value
Vertica	active_partitions	8
	tm_concurrency	5
	tm_memory	6,000
Resource pools	ingest_pool_memory_size	30%
	ingest_pool_planned_concurrency	12
Schedule	plannedconcurrency	5
	tm_memory_usage	10,000
	maxconcurrency	7

Transformation Hub Tuning for a Small Workload

Property	Quantity
# of Kafka broker nodes in the Kafka cluster	1
# of ZooKeeper nodes in the ZooKeeper cluster	1
# of Partitions assigned to each Kafka Topic	12
# of replicas assigned to each Kafka Topic	1
# of message replicas for the __consumer_offsets Topic	1
Schema Registry nodes in the cluster	1
Kafka nodes required to run Schema Registry	1
# of CEF-to-Avro Stream Processor instances to start	2

System Sizing for Medium Workload

This section helps you in determining whether your environment meets the requirements for a medium workload environment. It provides guidance for hardware requirements and tuning the performance of the workload. You might compare this information with the guidance for small workload.

Workload Distribution for a Medium Workload

The following table provides an example of how event ingestion activities might occur in a medium workload:

Application	Category	Expected Workload
Fortinet Fortigate	Events per second	7600
Microsoft Windows	Events per second	6000
Infoblox NIOS	Events per second	4000
Blue Coat, Check Point, Cisco	Events per second	1900
ArcSight Recon	Events per second	19500
	Searches (concurrent)	3

System Sizing for a Medium Workload

Category	Requirement
Single node (master and worker)	1 (G10 -L7700)
CPU cores (per node)	48
RAM (per node)	192
Disks (per node)	4 (7500 rpm)
Storage per day (1x)	0.9 TB
Total disk space (12 billion Events)	10.8 TB

Vertica Resource Pools Tuning for a Medium Workload

Category	Property	Value
Vertica	active_partitions	8
	tm_concurrency	5
	tm_memory	6,000
Resource pools	ingest_pool_memory_size	30%
	ingest_pool_planned_concurrency	12
Schedule	plannedconcurrency	5
	tm_memory_usage	10,000
	maxconcurrency	7

Transformation Hub Tuning for a Medium Workload

Property	Quantity
# of Kafka broker nodes in the Kafka cluster	1
# of ZooKeeper nodes in the ZooKeeper cluster	1
# of Partitions assigned to each Kafka Topic	12
# of replicas assigned to each Kafka Topic	1
# of message replicas for the __consumer_offsets Topic	1
Schema Registry nodes in the cluster	1
Kafka nodes required to run Schema Registry	1
# of CEF-to-Avro Stream Processor instances to start	2

3 Network File System

Recon supports several options for a network file system (NFS).

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_ROOT_DIRECTORY}/itom/itom_vol	130 GB
{NFS_ROOT_DIRECTORY}/itom/db	Depends, but start with 10 GB
{NFS_ROOT_DIRECTORY}/itom/db_backup	Depends, but start with 10 GB
{NFS_ROOT_DIRECTORY}/itom/logging	Depends, but start with 40 GB
{NFS_ROOT_DIRECTORY}/arcsight	10 GB

4 Ports Used

Recon uses following firewall ports. Therefore, ensure that the following ports are available.

Database

The database requires several ports to be open on the local network. It is not recommended to place a firewall between nodes (all nodes should be behind a firewall), but if you must use a firewall between nodes, ensure the following ports are available:

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

CDF Management Portal

Ports (TCP)	Direction	Description
3000	Inbound	Used for accessing the CDF management portal during CDF deployment.
5443, 5444	Inbound	Used for accessing the CDF management portal post CDF deployment.

Kubernetes

Ports (TCP)	Direction
2379	
2380	
3000	Inbound
4001	Inbound
4194	
5000	Inbound
8080	Inbound
8088	
8200	Inbound
8201	Inbound
8285	
8443	Inbound
8472	
10250	Inbound
10251	Inbound
10252	Inbound
10256	Inbound

NFS

Ports (TCP/UDP)	Direction	Description
111	Inbound	Used by `portmapper` service
2049	Inbound	Used by `nfs` service
20048	Inbound	Used by `mountd` service

Transformation Hub

Ports (TCP)	Direction	Description
2181	Inbound	Used by ZooKeeper as an inbound port
9092	Inbound	Used by Kafka during non-SSL communication
9093	Inbound	Used by Kafka when TLS is enabled
38080	Outbound	Used by Transformation Hub to send data to ArcMC
32181	Outbound	Used by ZooKeeper as an outbound port
443	Inbound	Used by ArcMC
9000	Inbound	Used by ArcMC
9999, 10000	Inbound	Used by the Transformation Hub Kafka Manager to monitor Kafka
39001, 39050	Outbound	Used by ArcMC to communicate with Connectors in Transformation Hub

ArcMC

Ports	Direction	Description
38080, 9000	Inbound	Used for Transformation Hub and ArcMC communication

SmartConnector

Ports	Direction	Description
◆ 1515 (Raw TCP) ◆ 1999 (TLS)	Inbound	Used by SmartConnector to receive events
◆ 9092 (Non-SSL) ◆ 9093 (SSL)	Outbound	Used by SmartConnector to send data to Transformation Hub

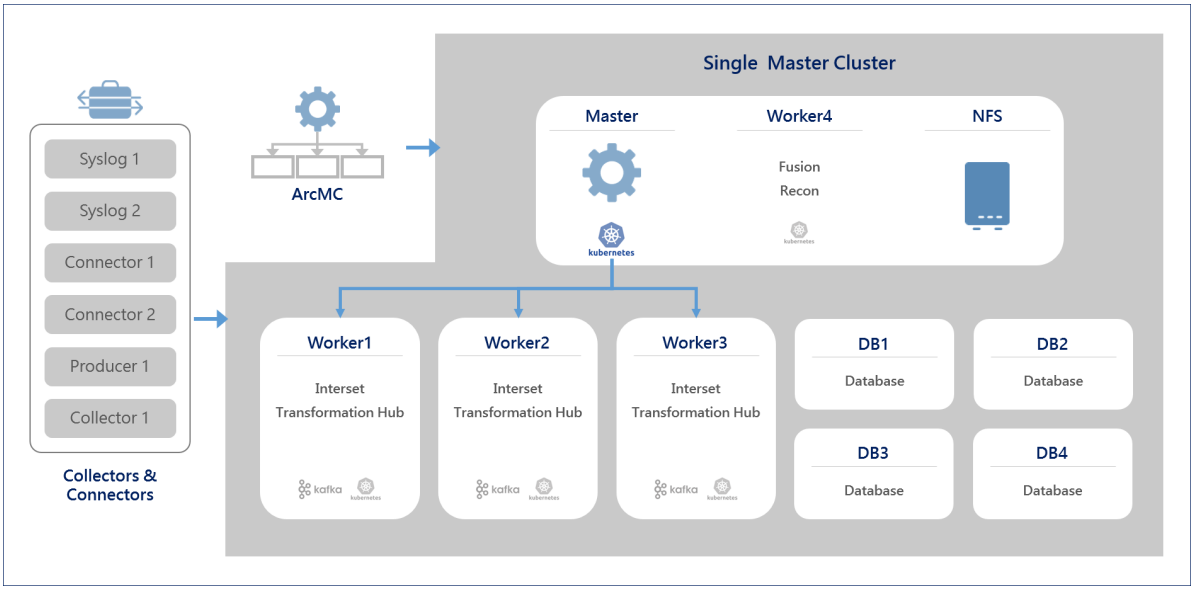
5 Guidance for a Multi-node Setup

The most basic deployment option is an all-in-one system that contains all Recon capabilities on a single node. The single-node deployment is suitable for small workloads or to use as a proof-of-concept environment. For large workloads, you will need a multi-node environment, possibly with multiple masters. For high-availability, you should have multiple masters and nodes. All of these environments require an external server to support NFS.

Single Master, Multiple Nodes

In this example, which deploys Recon and ArcSight Interset, you have a single Master Node connected to three Worker and four Database Nodes. All nodes have the same operating system, such as CentOS 7.8. You can deploy the Master Node, Worker Node 4, and NFS on the same server because of the minimal load that they require. Each Worker Nodes processes events, with failover to another Worker Node if a Worker fails.

Figure 5-1 *Example deployment of Recon and Interset*



The following table provides guidance for deploying the Recon and Interset capabilities across multiple nodes to support a large workload.

Node Name	Description	RAM	CPU Cores	Disk Space	Ports
Master Worker4	CDF Management Portal Fusion Recon	256 GB	32	5 TB	CDF Management Portal Kubernetes NFS
DB1	Database	192 GB	24	28 TB	Database
DB2	Database	192 GB	24	28 TB	Database
DB3	Database	192 GB	24	28 TB	Database
DB4	Database	192 GB	24	28 TB	Database
Worker1	Interset Transformation Hub	256 GB	32	5 TB	Kubernetes Transformation Hub Interset - 30010, 30070, 30820
Worker2	Interset Transformation Hub	256 GB	32	5 TB	Kubernetes Transformation Hub Interset - 30010, 30070, 30820
Worker 3	Interset Transformation Hub	256 GB	32	5 TB	Kubernetes Transformation Hub Interset - 30010, 30070, 30820

For more information about deploying Interset, see the *Deployment Guide for ArcSight Interset Standard Edition*.