Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.2

Configuration Guide for VMware ESXi Syslog SmartConnector

Document Release Date: June 2022
Software Release Date: June 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

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

Contents

Configuration Guide for VMware ESXi Syslog SmartConnector

Configuration Guide for VMware ESXi Syslog SmartConnector

This guide provides information for installing the SmartConnector for VMware ESXi Syslog and configuring the device for event collection. For supported devices and versions, see Technical Requirements.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectors to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

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

Contact Information

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

For specific product issues, contact Micro Focus Customer Care.

Configuration

VMware ESXi Server versions 5.5, 6.0, 6.5, and 7.0 are supported. The following table lists the supported modules by version:

Module Name	5.5	6.0	6.5	7.0
#024			X	
additionaldata.eventType			X	
addVob			X	
apiForwarder				X
amesiac			X	
amshelper			X	
bootstop		X	X	
cfgAgent				X
cimslp	X	X		
Clomd				X
create-statsstore			X	
dcbd		X	X	
DCUI			X	
dhclient	X	X		
dhclient-uw			X	
EPSecMux	X			
ESXShell			X	
esxtokend				X
esxupdate	X		X	
fdm				X
hostd	X		X	X
hostd-probe	X	X	X	X
hostd-icm			X	
hotdCgiServer			X	
hp-ams	X			

Module Name	5.5	6.0	6.5	7.0
ImageConfigManager	X	X	X	
iofilterd-vmwarecrypt			X	
iofiltered-spm			X	
iofilterdvpd			X	
jumpstart			X	
kmxa				X
localcli				X
mark			X	
nfsgssd			X	
nestdb-server				X
nsxavim				X
nsx-exporter				X
nsx-opsagent				X
nsx-sfhc				X
nsx-proxy				X
nsx-sha				X
ntpd_intres	X			
openwsmand		X		
osfsd				X
PyVmomiServer			X	
rabbitmqproxy			X	
Rhttpproxy	X	X	X	X
rhttpproxy-upgrade-config			X	
sdrsInjector			X	
sensord			X	X
sfcbd	X	X		
sfcbd-init			X	
sfcbd-config			X	
sfcb-CIMXML-Processor	X		X	
sfcb-hhrc	X			

Module Name	5.5	6.0	6.5	7.0
sfcb-ProviderManager	X			
sfcb-sfcb			X	
sfcb-vmware_base,sfcbd	X	X		
sfcb-vmware_init			X	
sfcb-*			X	
slpd		X	X	
smartd			X	X
sntp			X	
swapobjd			X	
storageRM			X	
Unknown	X			
usbarb			X	
usbarbitrator			X	
vfcd			X	
vitd			X	
VITLOADER			X	
vmauthd	X		X	
vmfstracegd			X	
vmkdevmgr			X	
vmkernel	X	X	X	X
vmkeventd			X	
vmkwarning			X	X
vmsvc		X		
vmware-hostd	X	X		
VMware[init]	X	X		
VMware[shutdown]			X	
VMware[startup]			X	
vobd			X	
vpxa	X		X	X
vsansystem			X	X

Module Name	5.5	6.0	6.5	7.0
vsantraced		X		
VSANMGMTSVC				X
VVold			X	
watchdog	X	X		
watchdog-dcbd		X		
watchdog-hostdCgiServer			X	
watchdog-iofiltervpd			X	
watchdog-net-lacp			X	
watchdog-net-lbt			X	
watchdog-nfcd			X	
watchdog-nfsgssd			X	
watchdog-nscd		X		
watchdog-ntpd			X	
watchdog-rabbitmqproxy			X	
watchdog-rhttpproxy			X	
watchdog-sdrsInjector			X	
watchdog-sensord			X	
watchdog-smartd		X		
watchdog-storageRM		X		
watchdog-swapobjd		X		
watchdog-usbarbitrator			X	
watchdog-vmfstracegd		X		
watchdog-vmkeventd			X	
watchdog-vmtoolsd		X		
watchdog-vpxa		X		
watchdog-vsantraced		X		
watchdog-vsantracedUrgen		X		
watchdog-vvold			X	

Product Overview

VMware ESXi provides the foundation for building and managing a virtualized IT infrastructure. Processor, memory, storage and networking resources are abstracted into multiple virtual machines that run unmodified operating systems and applications.

Installing the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the Micro Focus ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on ArcSight Documentation for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and Configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant Global Parameters, when prompted.
4. Do one of the following depending on your requirement:

- Select **Syslog Daemon** from the **Type** drop-down:
  a. Click **Next**, the specify the following paramenters:

Parameters	Description
Network port	The SmartConnector for Syslog Daemon listens for syslog events from this port.
IP Address	The SmartConnector for Syslog Daemon listens for syslog events only from this IP address, apart from the default (ALL) to bind to all available IP addresses.
Protocol	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Forwarder	This option applies to Batch Mode only. Specify **None**, **Rename**, or **Delete** as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value **None**.

  b. **Click Next.**

- Select **Syslog File** from the **Type** drop-down:

a. Click **Next**, the specify the following paramenters:

Parameters	Description
Pipe Absolute Path Name	Specify an absolute path to the pipe, or accept the default value: `/var/tmp/syspipe`.
File Absolute Path Name	Specify the full path name for the file from which this connector will read events. The following are default values: • **Solaris:** `\var\adm\messages` • **Linux:** `\var\log\messages` You can use a wildcard pattern in the file name. In the real-time mode, rotation can occur only if the file is over-written or removed from the folder. The real-time processing mode assumes the following external rotation: • **Date format log rotation:** The device creates a new log at a specified time in the with the naming convention `filename.timestamp.log`. The connector detects the new log and terminates the reader thread to the previous log after the processing is complete. The connector then creates a new reader thread to the new `filename.timestamp.log` and begins processing that file. To enable this log rotation, specify timestap in `yyyy-MM-dd` date format. For example, `filename.yyyy-MM-dd.log` • **Index log rotation:** The device writes to indexed files in the following format: `filename.log.001, filename.log.002, filename.log.003`, and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example:`filename'%d,1,99,true'.log;` Specifying `true` indicates that the index can be skipped. For example, if 5 appears before 4, processing proceeds with 5 and will not read 4. Use of `true` is optional.
Reading Events Real Time or Batch	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Action Upon Reaching EOF	This option applies to Batch Mode only. Specify **None**, **Rename**, or **Delete** as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value **None**.
File Extension If Rename Action	This option applies to Batch Mode only. Specify the extension to be added to the file name if the action on reaching the end of file is specified as **Rename**. The default value is **Processed**, which adds a `.processed` extension.

b. Click **Next.**

5. Select a destination and configure parameters.
6. Specify a name for the connector.
7. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.
8. Select whether you want to run the connector as a service or in the standalone mode.
9. Complete the installation.
10. Run the SmartConnector.

For instructions about upgrading the connector or modifying parameters, see SmartConnector Installation and User Guide.

Device Event Mapping to ArcSight Fields

The following table lists the mapping of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

For some UNIX-like messages, the Device Product and Device Vendor fields may contain 'Unix.'

VMware ESXi Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = ALERT, alert; High = error, Error, ERROR; Medium = verbose, warn, warning, WARNING, Warning; Low = info, INFO, DEBUG, lowest
Device Custom String 2	opID
Device Custom String 4	PID
Device Custom String 5	sourcePool
Device Event Class ID	Module
Device Host Name	hostname
Device Process Name	Module
Device Product	'ESX'
Device Severity	one of(severity, severity_v6, sourcePool)
Device Vendor	'VMware'
Device Version	5.5/6.0/6.5/7.0
External ID	One of (logID,logID_v6)
Message	Message
Name	All of ('VMware ESX', Module, 'events')
Source Process Id	processid
Source Service Name	One of (serviceContent, serviceContent_v6)
Source User Name	UserName

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for VMware ESXi Syslog SmartConnector (SmartConnectors 8.3.2)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!