Micro Focus Security ArcSight Connectors

SmartConnector for NetApp ONTAP

Configuration Guide

Document Release Date: July 31, 2020
Software Release Date: July 31, 2020

Legal Notices

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

https://www.microfocus.com

Copyright Notice

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, “commercial computer software” is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation (“FAR”) and its successors. If acquired by or on behalf of any agency within the Department of Defense (“DOD”), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement (“DFARS”) and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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:

ArcSight Product Documentation on the Micro Focus Security Community

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

Revision History

Date	Description
07/31/2020	First edition of this guide. Added support for NetApp ONTAP version 9.3 patch 8.

Contents

SmartConnector for NetApp ONTAP 9

This guide provides information for installing SmartConnector for NetApp ONTAP event log collection.

NetAppONTAP version x is supported.

Product Overview

NetApp® ONTAP® 9 unifies data management across flash, disk and cloud to simplify your storage environment. It bridges current enterprise workloads and new emerging applications and builds the foundation for your data fabric, making it easy to move your data where it is needed across flash, disk, and cloud resources.

Audit records are initially stored in binary staging files on individual nodes. If auditing is enabled on an SVM, every member node maintains staging files for that SVM. Periodically, they are consolidated and converted to user-readable event logs, which are stored in the audit event log directory for the SVM.

This connector collects and parses audit event logs in XML file formats.

Create Auditing Configuration

Prerequisites

- You must create the auditing configuration on the storage virtual machine (SVM).
- If you plan on creating an auditing configuration for central access policy staging, a CIFS server must exist on the SVM.
- Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the CIFS server, central access policy staging events are generated only if Dynamic Access Control is enabled.
- Dynamic Access Control is enabled through a CIFS server option. It is not enabled by default.
- If the arguments of a field in a command is invalid, for example, invalid entries for fields, duplicate entries, and non-existent entries, then the command fails before the audit phase. Such failures do not generate an audit record.
- If the SVM is an SVM disaster recovery source, the destination path cannot be on the root volume.

To create Auditing Configuration

1. Using the information in the planning worksheet, create the auditing configuration to rotate audit logs based on log size or a schedule:

If you want to rotate audit logs by...	Enter...
Log size	`vserver audit create -vserver vserver_name -destination path -events [{file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-account|security-group|authorization-policy-change}] [-format {xml}] [-rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]`
A schedule	`vserver audit create -vserver vserver_name -destination path -events [{file-ops|cifs-logon-logoff|cap-staging}] [-format {xml}] [-rotate-limit integer] [-rotate-schedule-month chron_month] [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-day chron_dayofmonth] [-rotate-schedule-hour chron_hour] -rotate-schedule-minute chron_minute` Note: The -rotate-schedule-minute parameter is required if you are configuring time-based audit log rotation.

For more information, see NetApp ONTAP 9 Documentation Center

Prepare to Install Connector

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

For complete product information, read the Administrator's Guide as well as the Installation and Configuration guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the ArcSight Management Center Administrator's Guide for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

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

Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the SmartConnector Product and Platform Support document, available from the Micro Focus SSO and the Micro Focus Security Community website.

1. Download the SmartConnector executable for your operating system from the Micro Focus SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

   Follow the wizard through the following folder selection tasks and installation of the core connector software:

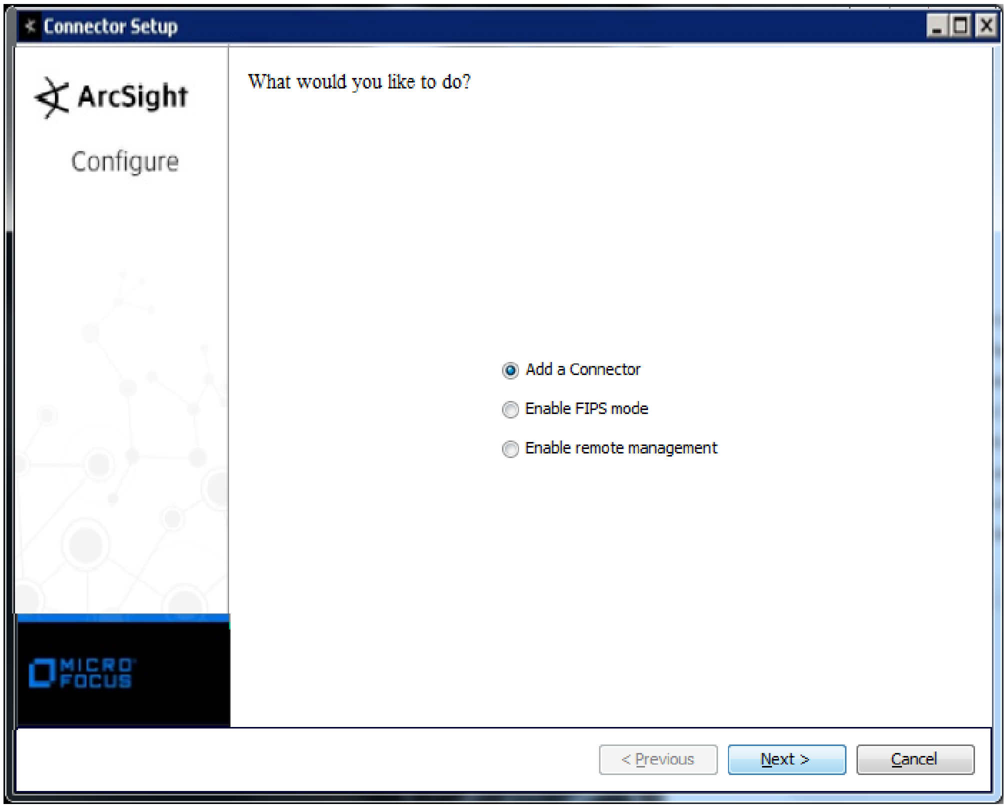
   Introduction

   Choose Install Folder

   Choose Shortcut Folder

   Pre-Installation Summary

   Installing...
3. When the installation of SmartConnector core component software is finished, the following window is displayed:



What would you like to do?

● Add a Connector

○ Enable FIPS mode

○ Enable remote management

Set Global Parameters (optional)

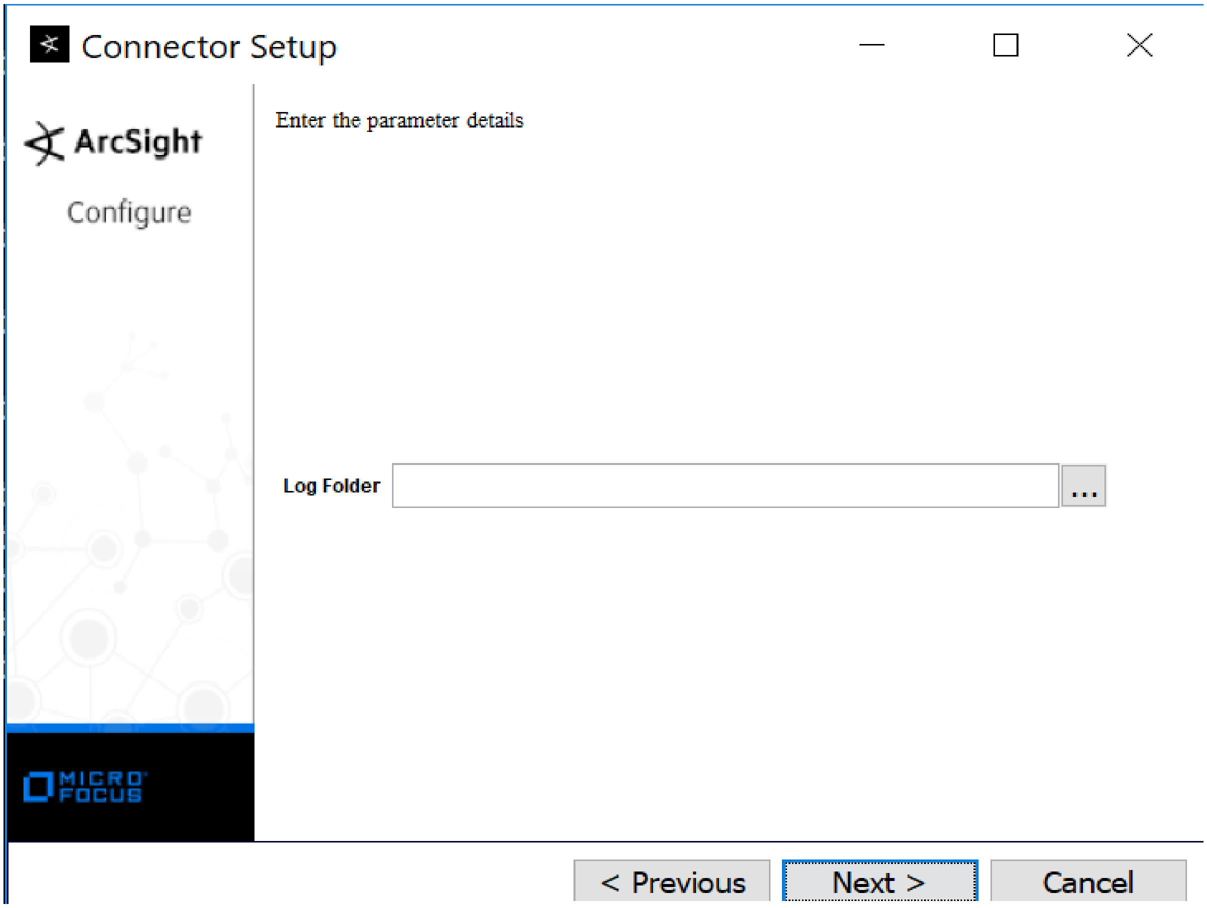
If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4
The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the Micro Focus SecureData Architecture Guide for more information.	
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting ‘Enabled’ to encrypt the fields identified in ‘Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector .
Format Preserving Policy URL	Enter the URL where the Micro Focus SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The Micro Focus SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus SecureData to use for encryption.
Event Fields to Encrypted	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
2. Select **NetApp ONTAP XML file** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click Next.



Enter the parameter details

Log Folder

Parameter	Description
Log Folder	Absolute path to the folder containing the XML log files.

Select a Destination

1. The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the ArcSight SmartConnector User Guide.
2. Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.
3. Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.
4. 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.

Complete Installation and Configuration

1. Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.
2. The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.
3. If you chose to run the connector as a service, with **Install as a servic**e selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.
4. Click Next on the summary window.
5. To complete the installation, choose **Exit** and Click **Next**.

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

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the ArcSight SmartConnector User Guide.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file

`$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

NetApp ONTAP 9.x Event Mappings to ArcSight ESM Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the ArcSight Console User's Guide for more information about the ArcSight data fields.

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	AccessList
Device Custom String 2	ComputerUUID
Device Custom String 3	SubjectUserSid
Device Custom String 4	SubjectUserIsLocal
Device Custom String 5	Version
Device Custom String 6	Result
Device Custom Number 1	Level
Device Custom Number 2	Gid
Device Event Class Id	EventId
Device Receipt Time	TimeCreated
Name	EventName
Application Protocol	Source
Destination Address	SubjectIP
Destination Nt Domain	SubjectDomainName

ArcSight ESM Field	Device-Specific Field
Destination Host Name	Computer
Destination User Id	Uid
Device Event Category	Channel
File Path	ObjectName
File Type	ObjectType
File Name	Object Server
File Id	HandleID
Request Context	InformationRequested
Device Vendor	NetApp
Device Product	ONTAP

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 (Connectors 8.0.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!