Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for NetApp ONTAP XML File SmartConnector

Document Release Date: February 2022
Software Release Date: February 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 SmartConnector for NetApp ONTAP 9

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

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.

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.

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.

Creating 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

Installing the SmartConnector

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

Preparing to Install Connector

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. Select **NetApp ONTAP XML file** from the **Type** drop-down, then click **Next**.
5. Specify the absolute path to the folder containing the XML log files in the **Log Folder** field, then click **Next**.
6. Select a destination and configure parameters.
7. Specify a name for the connector.
8. 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.

9. Select whether you want to run the connector as a service or in the standalone mode.
10. Complete the installation.
11. 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 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
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 for NetApp ONTAP XML File SmartConnector (SmartConnectors 8.3.0)

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!