Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for NetApp Filer Event Log SmartConnector

Document Release Date: December 2021
Software Release Date: November 2018

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 NetApp Filer Event Log SmartConnector

This guide provides information for installing the SmartConnector for NetApp Filer Event Log and configuring the device for event collection. Support for NetApp Filer 7.3 is provided.

This guide provides a high level overview of ArcSight SmartConnectors.

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 Filer is a family of network attached storage (NAS) appliances from Network Appliance that are highly scalable to terabytes of data. NetApp Filers are high-performance, mission critical products used by large enterprises and service providers.

Configuration

Event collection is done in near realtime with a maximum delay of one minute. Due to some limitations with NetApp Filer, regular reloads of processed events are required. This can slightly degrade performance. To minimize this issue, you can adjust the value for `agents[0].reload.ratio`.

For example:

- Setting the ratio to 100 results in a full reload of all events in the NetApp Filer. This means up to 4999 duplicate events might be loaded and skipped to reach the first new event.
- The default ratio of 30 results in a reload of approximately 1200 events. There is a risk that if more that 1200 events were created in the last minute, some events might be skipped.

Event recognition is based on the event creation timestamp. So during all reloads, there is a chance of a small number of event duplication due to a safety measure to prevent missing any events.

Enabling Live View

To view the storage system event logs in real time from your Windows client, perform the following procedure:

1. Set options `cifs.audit.liveview.enable` to on.
2. Start the Event Viewer from Administrative Tools or from MMC.
3. From the **Action** menu, select **Connect to Another Computer**.
4. Enter the name of the storage system you want to audit and click **OK**.
5. On the left side of the application, select the **Security** entry.

   The latest audit events are captured and displayed on the right side of the application.

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* guide, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* 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 Filer Event Log** from the **Type** drop-down, then click **Next**.
5. Specify the following parameters, then click **Next**.

Parameter	Description
Domain Name	Enter the name of the domain to which the host belongs. If you are using a Domain User account for a target host, fill in the Domain Name field. If you are using a Local User account for the target host, leave the Domain Name field blank. If the target host is a Workgroup host that does not belong to a domain, leave the Domain Name field blank.
Domain User	Enter the name of the user account with adequate privileges to collect Windows events from the target host. This will be the user name only, without the domain.
Domain User Password	Enter the password for the user specified in Domain User Name.
activedirectory.host	Enter the Active Directory Host Name or IP address required for authentication to the MS Active Directory for the Host Browsing feature.
activedirectory.basedn	Enter the Active Directory Base DN, which is required for automatic host browsing. The Base DN is the starting point in the MS Active Directory hierarchy at which the search is to begin. It can contain Common Names (cn), Organizational Units (ou), and Domain Components (dc).
activedirectory.filter	Enter the Active Directory Filter required for automatic host browsing to filter hosts by name, operating system, and creation time. The filter can contain attributes for Common Names (cn), Operating System (operatingsystem) and Creation Time (whencreated) in 'YYMMDDHHmmSSZ' format, where YY=Last two digits of the year, MM=Month, DD=Date, HH=Hours, mm=Minutes, SS=Seconds in 24-hour format. For more details, see the SmartConnector Configuration Guide for Microsoft Windows Event Log - Unified.
activedirectory.user	Enter the Active Directory User Name for access to Active Directory. This is required for authentication to the MS Active Directory for the Host Browsing feature.
activedirectory.password	Enter the password associated with the Active Directory User Name. This is required for authentication to the MS Active Directory for the Host Browsing feature.
activedirectory.securityprotocol	Select whether the protocol to be used is non_ssl (the default value) or SSL. Note: For SSL protocol, be sure to import the Active Directory security certificate to the connector before starting the connector.

Parameter	Description
activedirectory.port	Enter the port number to which the connector will listen: the default for the non_ssl protocol is 389; the default for the SSL protocol is 636. Note: For SSL protocol, be sure to import the Active Directory security certificate to the connector before starting the connector. See "Import the CA Certificate" in the SmartConnector Configuration Guide for Microsoft Windows Event Log - Unified for more information.
activedirectory.maxpage	Enter a maximum page size for the Active Directory query. This lets the connector read all hosts by repeating query for max page size hosts as many times as needed. The default value is 300.
globalcatalog.host	Global Catalog Server IP or Host Name is required for GUID translation. To use the Active Directory Server as the Global Catalog Server, leave this field empty.
globalcatalog.basedsn	Global Catalog Base DN is required for GUID translation. To use the Active Directory Base DN as the Global Catalog Base DN, leave this field empty.
globalcatalog.user	Global Catalog User name required for GUID translation. This can be a Domain Admin User or even a Standard Domain User. To use the Active Directory User Name and Active Directory User Password as the Global Catalog User Name and Global Catalog User Password, respectively, leave this field empty.
globalcatalog.password	Global Catalog User Password required for GUID translation. To use the Active Directory User Name and Active Directory User Password as the Global Catalog User Name and User Password, respectively, leave the Global Catalog User Name field empty. For Global Catalog user information, to use the same values as specified for Active Directory, leave the Global Catalog parameters empty. To use differing user information for the Global Catalog, in addition to specifying the Server, Base DSN, User Name, and User Password, you can access the connector's advanced parameters to specify Global Catalog Protocol as needed. See "Advanced Configuration Parameters for Global Catalog" later in this guide. The port (3268 for non-ssl) will adjust automatically to standard SSL connection port for Global Catalog, which is 3269.
Domain Name	Enter the name of the domain to which the host belongs.

Parameter	Description
Host Name	Name of the NetApp Filer host.
User Name	User with permission to read events through Live View.
Password	Password for the user.

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. The connector cannot detect the network drive when running as a service on a Windows platform. This problem does not occur when the connector and IIS Server are installed on the same host.
11. Complete the installation.
12. Run the SmartConnector.

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

Device Event Mapping to ArcSight Fields

See ArcSight SmartConnector Mappings to Windows Security Events for Windows Event Log security event mappings.

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 Filer Event Log 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!