Micro Focus Security ArcSight Connectors

SmartConnector for NetApp Filer Event Log

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for NetApp Filer Event Log

June, 2018

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") 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. The information contained herein is subject to change without notice.

Restricted Rights Legend

Trademark Notices

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/15/2015	General content update.
05/15/2012	Added new installation procedure.
02/15/2012	Updated configuration parameters.
05/16/2011	First version of Configuration Guide for Beta support.

SmartConnector for NetApp Filer Event Log

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.

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.

Enable 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.

Install the SmartConnector

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

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 Protect 724 sites.

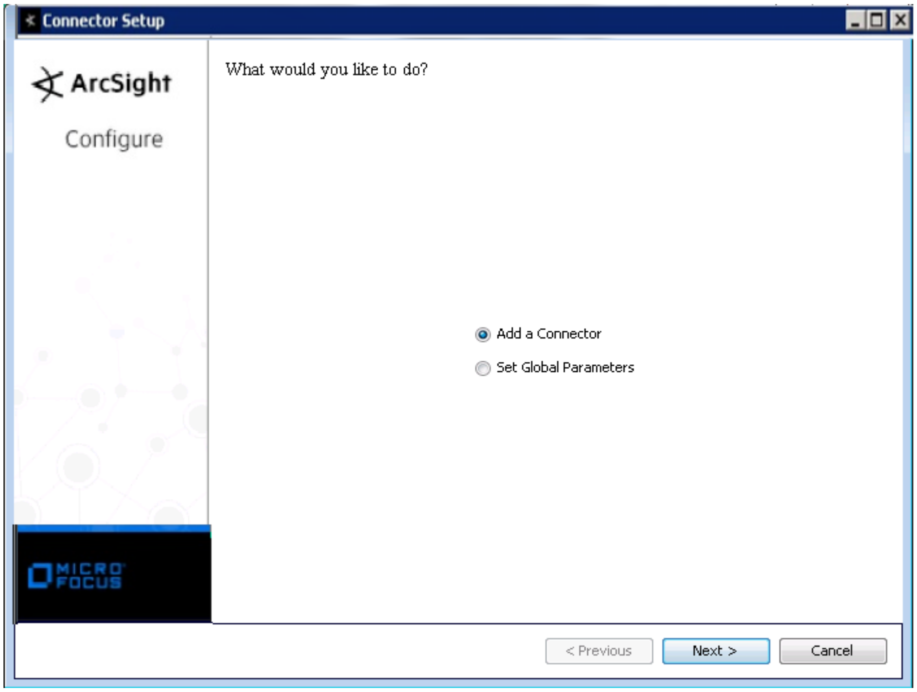
1. Download the SmartConnector executable for your operating system from the Micro Focus SSO site.

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

○ Set Global Parameters

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.

Parameter	Setting
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.

Parameter	Setting
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 Encrypt	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."

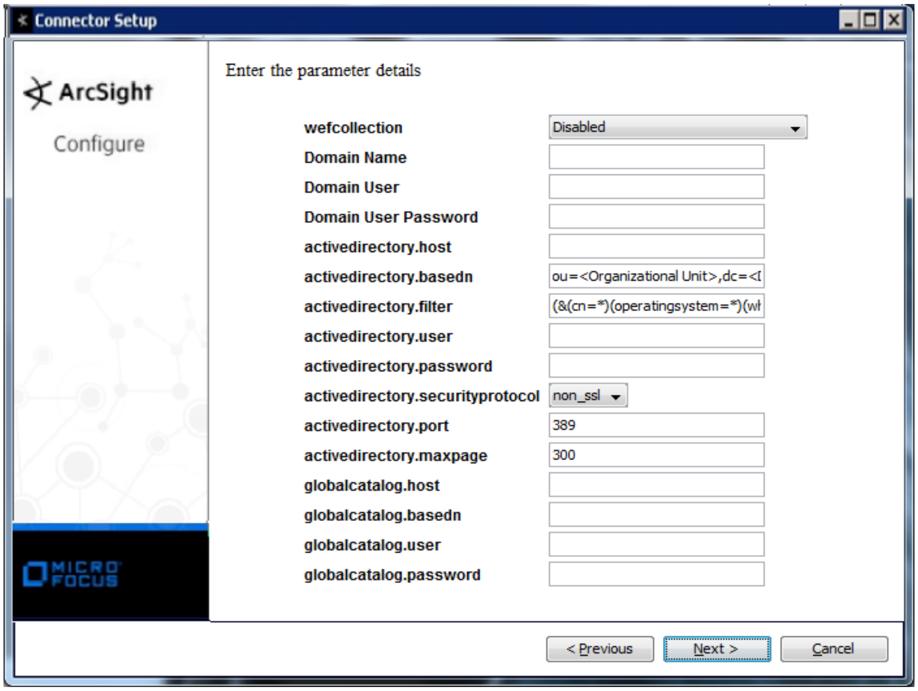
Select Connector and Add Parameter Information

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 Filer Event Log** and click **Next**.

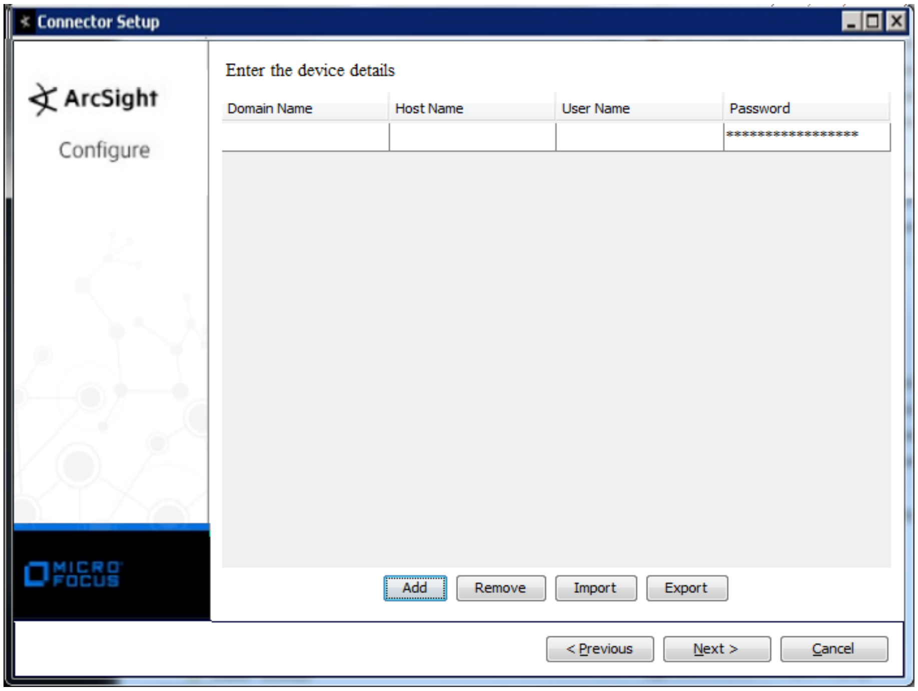
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

   For a complete description of the parameters in the first parameter entry window, see the configuration guide for the SmartConnector for Windows Event Log – Unified.



Enter the parameter details

wefcollection	Disabled
Domain Name	
Domain User	
Domain User Password	
activedirectory.host	
activedirectory.basedn	ou=<Organizational Unit>,dc=<[
activedirectory.filter	(&(cn=*)(operatingsystem=*)(wh
activedirectory.user	
activedirectory.password	
activedirectory.securityprotocol	non_ssl
activedirectory.port	389
activedirectory.maxpage	300
globalcatalog.host	
globalcatalog.basedn	
globalcatalog.user	
globalcatalog.password	



Enter the device details

Domain Name	Host Name	User Name	Password
			******************

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. See "Security Certifications when using SSL"in the SmartConnector Configuration Guide for Microsoft Windows Event Log - Unified for more information.

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

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 service** 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 Filer Event Log Mappings to ArcSight Fields

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