Hewlett Packard Enterprise

HPE Security ArcSight Connectors

SmartConnector for Microsoft DNS Trace Log Multiple Server File

Configuration Guide

July 15, 2017

Configuration Guide

SmartConnector for Microsoft DNS Trace Log Multiple Server File

July 15, 2017

Revision History

Date	Description
07/15/2017	Removed platform support for Windows 2003.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
09/30/2014	First edition of this Configuration Guide.

SmartConnector for Microsoft DNS Trace Log Multiple Server File

This guide provides information for installing the SmartConnector for Microsoft DNS Trace Log Multiple Server File and configuring the device for event collection. Microsoft's Domain Name Service (DNS) included with Microsoft Windows 2008, Microsoft Windows 2012, and Microsoft Windows 2012 R2 are supported.

Product Overview

The Domain Name System (DNS) is a hierarchical distributed database and an associated set of protocols that define a:

■ Mechanism for querying and updating the database

■ Mechanism for replicating the information in the database among servers

■ Schema of the database

With DNS, the host names reside in a database that can be distributed among multiple servers, decreasing the load on any one server and providing the ability to administer this naming system on a per-partition basis. DNS supports hierarchical names and allows registration of various data types in addition to host name to IP address mapping used in HOSTS files.

This ArcSight SmartConnector lets you import events generated by the Microsoft DNS Trace Log Multiple Server File device into the ArcSight System. See the section "Device Event Mapping to ArcSight Data Fields" later in this document for the specific events mapped to fields in the ArcSight database.

Configuration

Detailed information regarding DNS Monitoring can be found at: http://technet.microsoft.com/en-us/library/cc783975(WS.10).aspx.

The primary tool used to manage DNS servers is the DNS console, which can be found in the **Administrative Tools** folder in the **Start** menu's **Programs** folder.

DNS server event messages are separated and kept in their own system event log, the DNS server log. The DNS server log contains events logged by the DNS server service. Most critical DNS server service events are logged here, such as when the server starts but cannot locate initializing data.

You can change the event types logged by DNS servers using the DNS console. You also can use the DNS console to selectively enable additional debug logging options for temporary trace logging to a text-based file of DNS server activity.

Using Server Debug Logging Options

By default, all debug logging options are disabled. When selectively enabled, the DNS Server service can perform additional trace-level logging of selected types of events or messages for general

---

troubleshooting and debugging of the server. `Dns.log` contains debug logging activity. By default, it is located in the `windir\System32\Dns` folder.

The following DNS debug logging options are available:

Packet Direction

Outgoing
> Packets sent by the DNS server are logged in the DNS server log file.

Incoming
> Packets received by the DNS server are logged in the log file.

Packet Content

Queries/Transfers
> Specifies that packets containing standard queries (per RFC 1034) are logged in the DNS server log file.

Updates
> Specifies that packets containing dynamic updates (per RFC 2136) are logged in the DNS server log file.

Notifications
> Specifies that packets containing notifications (per RFC 1996) are logged in the DNS server log file.

Transport Protocol

UDP
> Specifies that packets sent and received over UDP are logged in the DNS server log file.

TCP
> Specifies that packets sent and received over TCP are logged in the DNS server log file.

Packet Type

Request
> Specifies that request packets are logged in the DNS server log file (a request packet is characterized by a QR bit set to 0 in the DNS message header).

Response
> Specifies that response packets are logged in the DNS server log file (a response packet is characterized by a QR bit set to 1 in the DNS message header).

Other Options

Filter packets by IP address
> Provides additional filtering of packets logged in the DNS server log file.

Details
> Specifies that all event details be logged in the DNS server log file.

Log File
> *File path and name* lets you specify the name and location of the DNS server log file. *Log file maximum size limit* lets you set the maximum file size for the DNS server log file.

To select and enable debug logging options on the DNS server:

1   Open DNS. (Click **Start** -> **Control Panel** -> **Administrative Tools**. Double-click **DNS**.)

2   In the console tree, right-click the applicable DNS server, then click **Properties**.

3   Click the **Debug Logging** tab.

4   To set the debug logging options, first select **Log packets for debugging**. To ensure collecting the appropriate information for processing by ArcSight, select the options shown in the following figure.
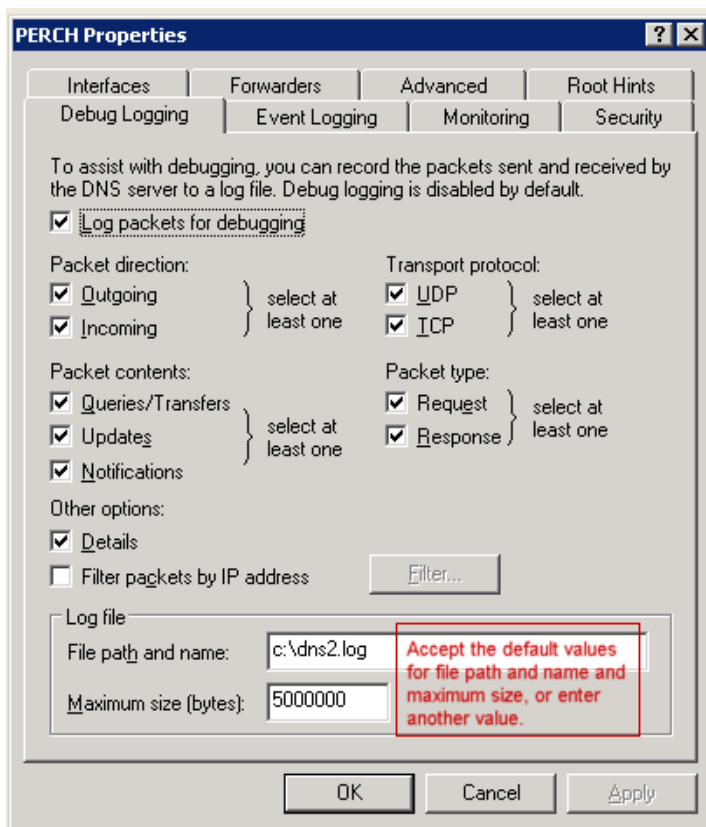
In addition to selecting events for the DNS debug log file, select the default values or specify the file name, location, and maximum file size for the file.

Install the SmartConnector

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

> Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

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 HPE SSO and Protect 724 sites.

1 Download the SmartConnector executable for your operating system from the HPE 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:
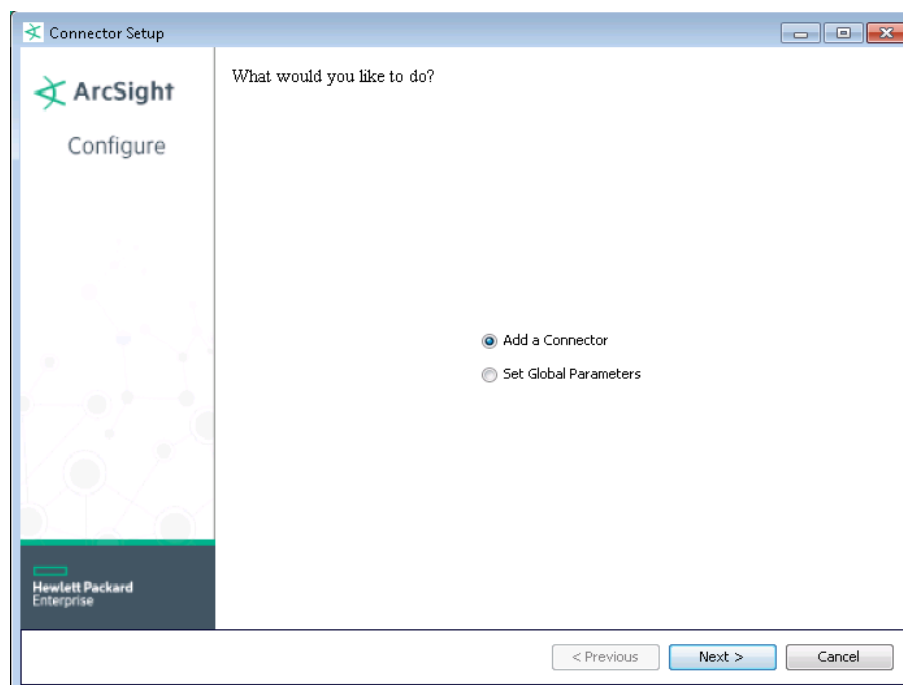
Set Global Parameters (optional)

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:
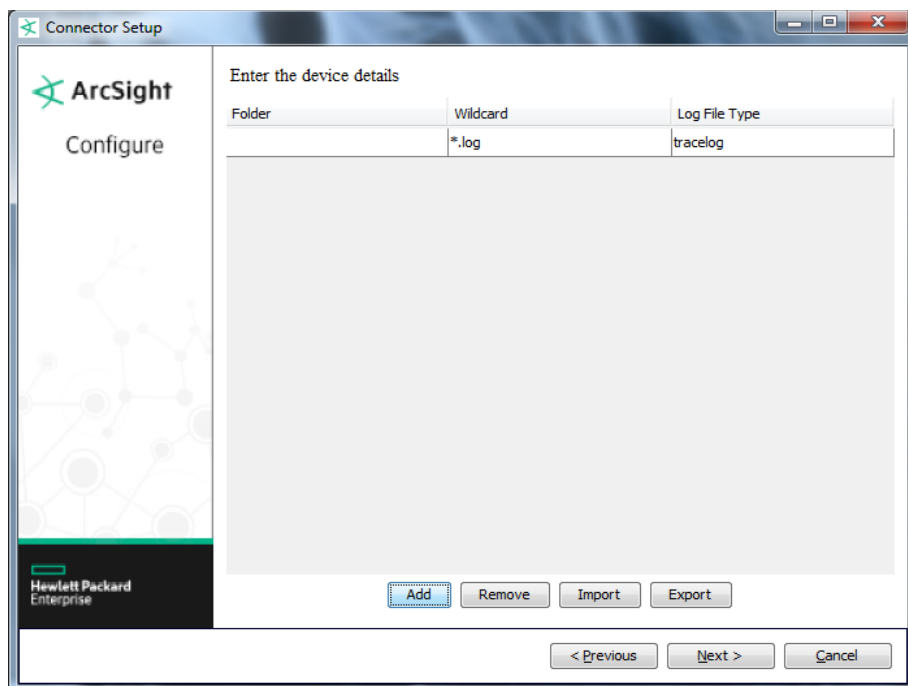
Global Parameter	Setting
Set FIPS mode	Set to 'Enable' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disable'.
Set Remote Management	Set to 'Enable' to enable remote 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 'Disable'.
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	If 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. When both values are present, the initial setting is IPv4.

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 the "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 **Microsoft DNS Trace Log Multiple Server File** and click **Next**.

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

Parameter	Description
Folder	The absolute path to the location of the log files.
	- For Windows platform, use: 'c:\Program Files\DNS_Multi_File\logs\'
	- For Linux platform, use: '/var/log/dnsmultifile/'
	For multiple servers, click Add and enter information about the additional server.
	- For Windows platform, use: \\<servername>\folder\folder.
Wildcard	The log file name ('*.log') has two parts:
	- Part 1: ('*') is the file name
	- Part 2: ('.log') is the file type
	- For example: 'dnsmulti.log'
Log File Type	Accept the default "tracelog".

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.

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.

Microsoft DNS Trace Log Multiple Server File Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 2, 3, 5, 16, SERVFAIL, NXDOMAIN, REFUSED, BADVERS, BADSIG; Medium = 1, 4, 6-10, 17-22, Error, Warning, FORMERR, NOTIMP, YXDOMAIN, YXRRSET, NXRRSET, NOTAUTH, NOTZONE, BADKEY, BADTIME, BADMODE, BADNAME, BADALG, BADTRUNC; Low = 0, 11-15, 23-65535, Information, Success, NOERROR (based on Rcode values at: http://www.networksorcery.com/enp/protocol/dns.htm#Rcode, Return code)
Application Protocol	application protocol
Bytes In	Size, incoming bytes
Destination Address	destination address
Destination DNS Domain	destination DNS domain
Destination Host Name	destination host name
Destination NT Domain	destination NT domain
Device Action	Action taken by the device
Device Custom IPv6 Address 2	Source IPv6 address
Device Custom String 1	Thread Id
Device Custom String 2	OpCode
Device Custom String 3	Flags (character codes)
Device Custom String 4	Reason or error code
Device Direction	Snd=Outbound, Rcv=Inbound
Device Event Category	Context
Device Event Class ID	Event Name
Device Product	'DNS Trace Log'
Device Receipt Time	DateTime
Device Severity	One of (Information, Warning, Error, Success, NOERROR)
Device Vendor	'Microsoft'
File Name	file name
File Path	file path
Message	Rcode description (based on Rcode descriptions at: http://www.networksorcery.com/enp/protocol/dns.htm#Rcode, Return code
Name	Rcode name (based on Rcode name at: http://www.networksorcery.com/enp/protocol/dns.htm#Rcode, Return code
Request URL	Question Name
Source Address	Source network address
Source DNS Domain	sourceDNSDomain
Source Host Name	Source host name
Source Port	Source port
Source Service Name	sourceServiceName
Start Time	startTime
Transport Protocol	transport protocol (UDP)