
Micro Focus Security ArcSight Micro Focus Security ArcSight Connectors

Software Version: 8.2.0

SmartConnector for Microsoft DNS DGA Trace Log Multiple Server File

Document Release Date: May 2021

Software Release Date: May 2021



Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

© Copyright 2021 Micro Focus or one of its affiliates

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:

<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

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

- SmartConnector for Microsoft DNS DGA Trace Log Multiple Server File 5
 - Product Overview 5
 - Supported Version 6
 - Configuration 6
 - Using Server Debug Logging Options 6
 - Install the SmartConnector 9
 - Prepare to Install Connector 9
 - Install Core Software 9
 - Set Global Parameters (optional)10
 - Select Connector and Add Parameter Information12
 - Select a Destination13
 - Complete Installation and Configuration 13
 - Map Files14
 - Run the SmartConnector15
 - Device Event Mapping to ArcSight Fields16
 - Microsoft DNS DGA Trace Log Multiple Server File Mappings to ArcSight ESM Fields 16
- Send Documentation Feedback18

SmartConnector for Microsoft DNS DGA Trace Log Multiple Server File

This guide provides information for installing the SmartConnector for Microsoft DNS DGA Trace Log Multiple Server File and configuring the device for event collection.

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.

The new feature enables users to apply a Domain Generation Algorithm (DGA) and:

- Whitelist filters on real time
- Filter and drop events prior a license check
- Use the Connector immediately after installation. Required files are pre-configured.
- Populate a dga_whitelist.txt locally or remotely (via ArcMC) to avoid getting events from trusted domains
- Add Map files to /user/agent/map/ to extend connector functionalities

See the section "Map Files" later in this document for more information.

Supported Version

Microsoft's Domain Name Service (DNS) included with Microsoft Windows 2008, Microsoft Windows 2012, Microsoft Windows 2016 and Microsoft Windows 2012 R2 are supported.

Configuration

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

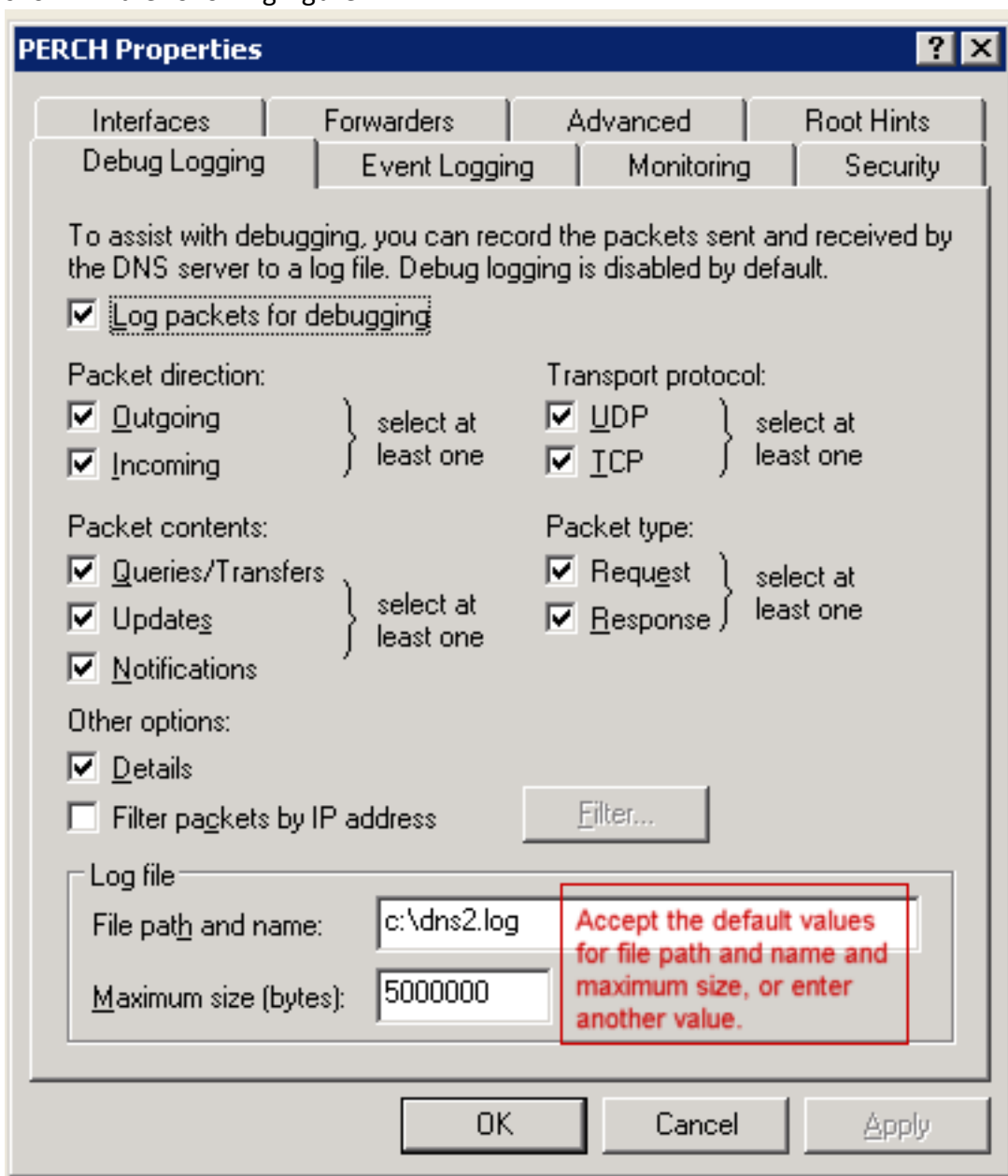
File path and name lets you specify the name and location of the DNS server log file.

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 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

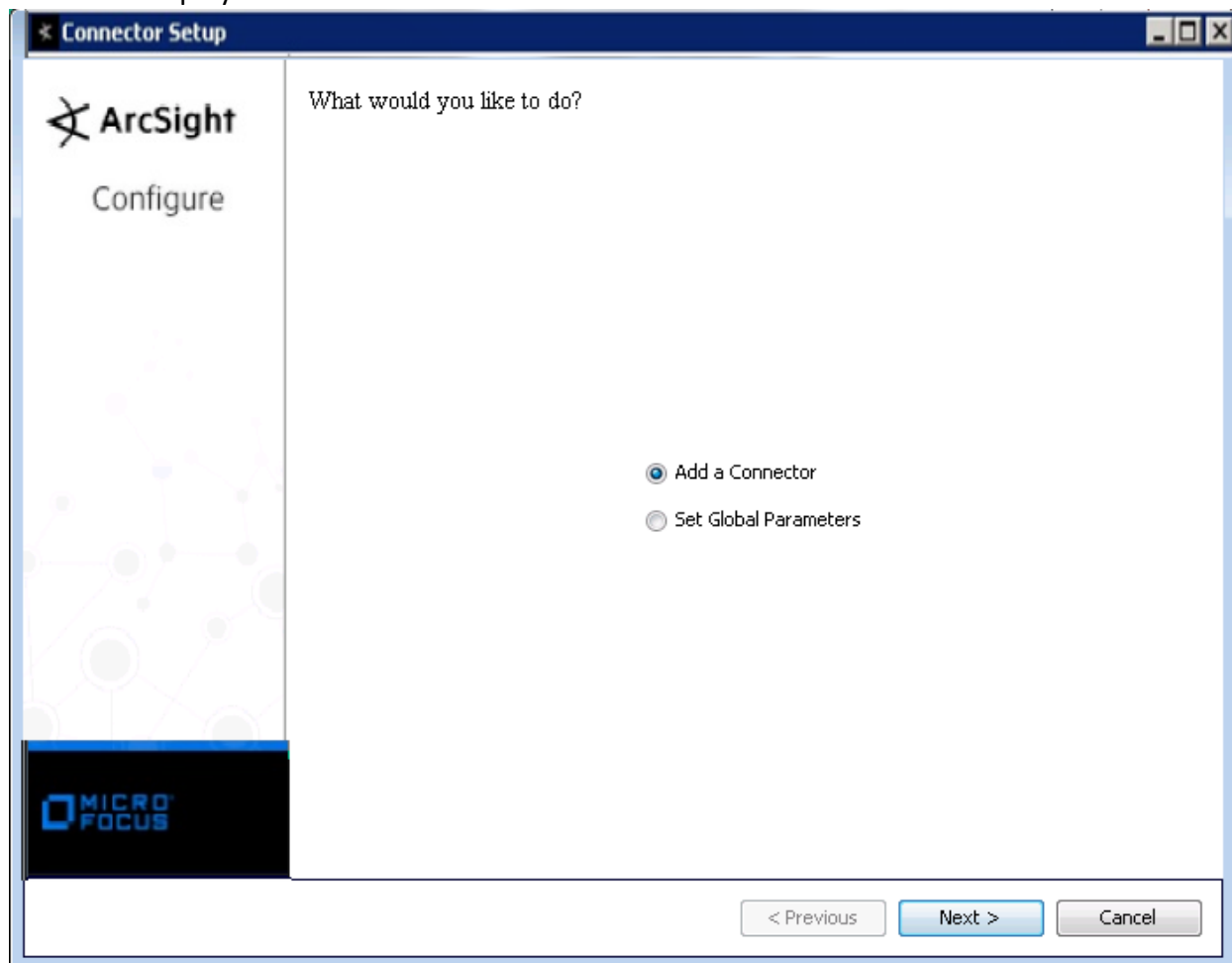
Choose Install Folder

Choose Shortcut Folder

Pre-Installation Summary

Installing...

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



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.
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 **Microsoft DNS DGA Trace Log Multiple Server File** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Folder	Wildcard	Log File Type
	*.log	tracelog

Parameter	Description
Folder	The absolute path to the location of the log files.
	- For Windows platform, use: 'c:\Program Files\DNS_Multi_File\logs'

Parameter	Description
	- 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*.

Map Files

By adding map files, users can increment the functionalities of the Connector.

File	Description	Sample Content
dga_whitelist.txt	White list file. Includes all domains that are not scanned by the DGA detection.	google.com youtube.com facebook.com baidu.com wikipedia.org yahoo.com reddit.com google.co.in qq.com taobao.com amazon.com twitter.com
map.2.properties	Numbered connector map file. It calls the _domainWhitelist operation. This operation is a lookup for whitelisted domains in each event and marks them as WHITELISTED, so they can be dropped by the filter later.	!Flags,Overwrite+set.expr (destinationHostName).event.deviceCustomFloatingPoint2Label __domainWhitelist(destinationHostName)
map.3.properties	Numbered connector map file. It calls the dgaForbiddenTrigrams operation. This operation applies the forbiddenTrigrams DGA classifier in every event and returns 1 or 0 for each.	!Flags,Overwrite+set.expr (destinationHostName).event.deviceCustomNumber1__dgaForbiddenTrigrams(destinationHostName)
map.4.properties	Numbered connector map file. It calls the ForbiddenTrigramsHelper operation. This is a helper function that adds a label to the dga field in CEF.	!Flags,Overwrite+set.expr (deviceCustomNumber1).event.deviceCustomNumber1Label__dgaForbiddenTrigramsHelper (deviceCustomNumber1)
map.5.properties	Numbered connector map file. It sets the event.dropEventFlag based on the value of event.deviceCustomFloatingPoint2Label. It is set to "true" when the value of event.deviceCustomFloatingPoint2Label is WHITELISTED.	event.deviceCustomFloatingPoint2Label,set.event.dropEventFlag, WHITELISTED,true



Note: Adjust the sequence numbers of your new map files based on any existing map files. For example, if the last map file in the connector is number 3, the new DGA map file must be set to 4 and so on.

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 DGA 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 Floating Point 2 Label	WHITELISTED
Device Custom IPv6 Address 2	Source IPv6 address
Device Custom Number 1	0 or 1
Device Custom Number 1 Label	DNS-Analytics
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

ArcSight ESM Field	Device-Specific Field
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)

please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to received events.

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 SmartConnector for Microsoft DNS DGA Trace Log Multiple Server File (Micro Focus Security ArcSight Connectors 8.2.0)

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!