



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Microsoft DNS DGA Trace Log Multiple Server File SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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>

Contents

- Configuration Guide for Microsoft DNS DGA Trace Log Multiple Server File SmartConnector 4
- Product Overview 5
 - Supported Version 5
- Configuration 6
 - Using Server Debug Logging Options 6
- Installing the SmartConnector 9
 - Preparing to Install the SmartConnector 9
 - Installing the SmartConnector 9
 - Map Files 10
- Device Event Mapping to ArcSight Fields 12
 - Microsoft DNS DGA Trace Log Multiple Server File Mappings to ArcSight ESM Fields 12
- Send Documentation Feedback 14

Configuration Guide for Microsoft DNS DGA Trace Log Multiple Server File SmartConnector

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

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for 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.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

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

For information about DNS Monitoring, see [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 can also 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

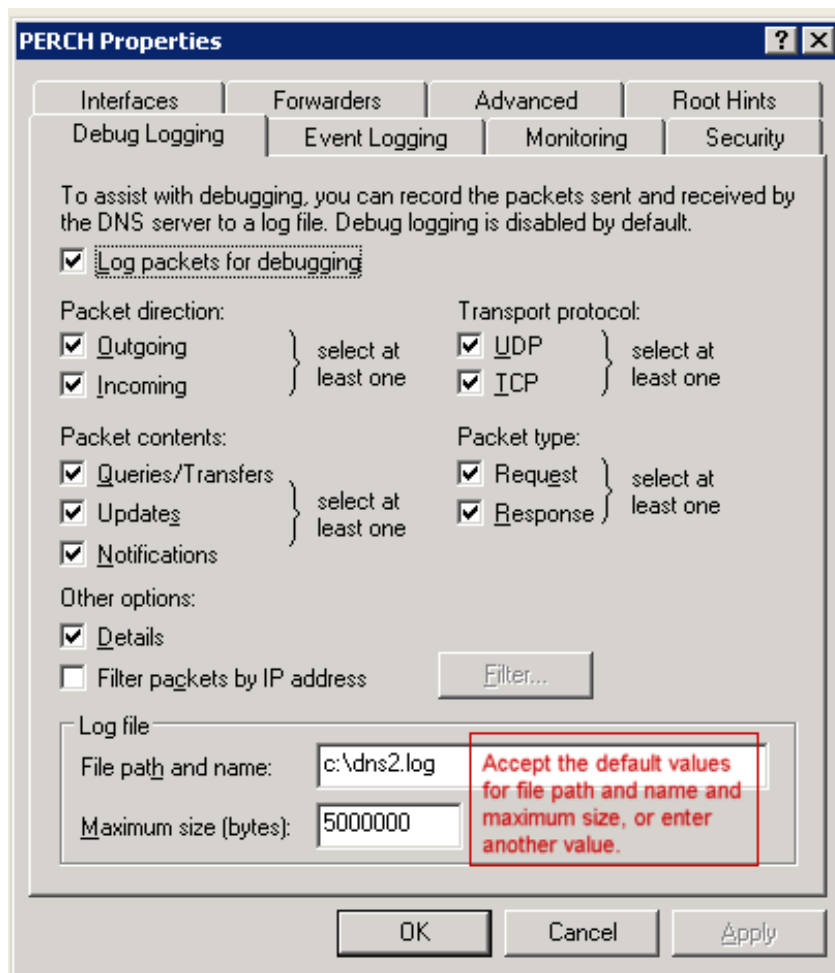
File path and name

Allows you to specify the name and location of the DNS server log file. *Log file maximum size limit* enables you to set the maximum file size for the DNS server log file.

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

1. To open DNS, go to **Control Panel > System and Security > Administrative Tools**, then 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:



5. 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.

Installing 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.

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText 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 the SmartConnector

The installation steps described in this section are specific to the Microsoft DNS DGA Trace Log Multiple Server File SmartConnector. For detailed installation steps or for manual installation steps, see [SmartConnector Installation and User Guide](#).

To install and configure 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. From the **Type** drop-down list, select **Microsoft DNS DGA Trace Log Multiple Server File** as the type of connector, then click **Next**.

5. Enter the following device details to configure the SmartConnector and 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".

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (Conditional) 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 then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

9. Select whether you want to install 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 [Installation and User Guide for SmartConnector](#).

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.
- The domains are whitelisted based on the top-level domain. The domains that do not follow the Internet Assigned Numbers Authority (IANA) standard will not be processed.

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
Device Direction	Snd=Outbound, Rcv=Inbound

Configuration Guide for Microsoft DNS DGA Trace Log Multiple Server File SmartConnector Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
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 Configuration Guide for Microsoft DNS DGA Trace Log Multiple Server File SmartConnector (SmartConnectors 8.4.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!