Micro Focus Security ArcSight Connectors

SmartConnector for Windows Event Log – Native: Microsoft DNS Server Analytics Logs

Supplemental Configuration Guide

Document Release Date: May 21, 2020
Software Release Date: May 21, 2020

Legal Notices

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

https://www.microfocus.com

Copyright Notice

© Copyright 2010-2020 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:

ArcSight Product Documentation on the Micro Focus Security Community

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

Revision History

Date	Description
05/21/2020	First edition of this Configuration Guide to provide support for DNS analytic events.

Contents

SmartConnector for Microsoft Windows Event Log – Native: Microsoft DNS Server Analytic Logs

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft DNS Server Analytic Logs and its event mappings to ArcSight data fields.

Supported Versions:

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Product Overview

Microsoft DNS Server Analytic Logs is a Windows system service and device driver that enables the Microsoft Windows Event Log – Native (WiNC) SmartConnector to monitor and collect the analytic events / logs from the DNS Server.

It provides information about operational events such as dynamic updates, zone transfers, and DNSSEC zone signing and unsigning.

Microsoft DNS Server Analytic Logs Configuration

For information about Microsoft's DNS Logging and Microsoft DNS analytic events logs configuration, see Microsoft's DNS Logging and Diagnostics.

Connector Installation and Configuration

Follow the installation and configuration procedures in the *SmartConnector Configuration Guide for Microsoft Windows Event Log – Native*, selecting **Microsoft Windows Event Log – Native** as the connector to be configured. During installation, select **true** for the **System Logs** field for system events to be collected.

Mappings for Microsoft DNS Server Analytic Logs

General

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'DNS Server Analytic'
Device Version	'Unknown'

Event ID 256

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
File Hash	AdditionalInfo
Name	"QUERY_RECEIVED"
Old File Id	RD

Event ID 257

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP

ArcSight Field	Vendor Field
Device Custom Number 1 Label	"TCP"
Device Custom Number 2	DNSSEC
Device Custom Number 2 Label	"DNSSEC"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 5	PolicyName
Device Custom String 5 Label	"Policy Name"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
File Size	BufferSize
File Hash	AdditionalInfo
Name	"RESPONSE_SUCCESS"
Old File Id	AA,AD
Request Context	Zone
Request Cookies	"Lookup"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event ID 258

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags

ArcSight Field	Vendor Field
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 5	PolicyName
Device Custom String 5 Label	"Policy Name"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
File Size	BufferSize
File Hash	AdditionalInfo
Name	"RESPONSE_FAILURE"
Reason	Reason
Request Context	Zone
Request Cookies	"Lookup"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event ID 259

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 5	PolicyName

ArcSight Field	Vendor Field
Device Custom String 5 Label	"Policy Name"
Device Direction	Inbound/Outbound
File Hash	AdditionalInfo
Name	"IGNORED_QUERY"
Reason	Reason
Request Context	Zone
Request Cookies	"Lookup"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event ID 260

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 5	PolicyName
Device Custom String 5 Label	"Policy Name"
Device Direction	Inbound/Outbound
File Size	BufferSize
File Hash	AdditionalInfo
Name	"RECURSE_QUERY_OUT"
Old File Id	RD
Old File Hash	RecursionScope,CacheScope

ArcSight Field	Vendor Field
Request Cookies	"Recursive query"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event ID 261

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
File Hash	AdditionalInfo
Name	"RECURSE_RESPONSE_IN"
Old File Id	AA,AD
Old File Hash	RecursionScope,CacheScope
Request Cookies	"Recursive query"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event ID 262

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Hash	AdditionalInfo
Name	"RECURSE_QUERY_TIMEOUT"
Old File Hash	RecursionScope,CacheScope
Request Cookies	"Recursive query"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event ID 263

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 2	Secure
Device Custom Number 2 Label	"SECURE"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 4	XID

ArcSight Field	Vendor Field
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"DYN_UPDATE_RECV"
Request Cookies	"Dynamic update"
Request Url	QNAME
Source Port	Port
Source Address	Source

Event ID 264

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 5	PolicyName
Device Custom String 5 Label	"Policy Name"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"DYN_UPDATE_RESPONSE"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Dynamic update"
Request Url	QNAME
Source Address	InterfaceIP

Event ID 265

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"IXFR_REQ_OUT"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event ID 266

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"IXFR_REQ_RECV"
Old File Hash	ZoneScope
Request Context	Zone

ArcSight Field	Vendor Field
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event ID 267

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"IXFR_RESP_OUT"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	InterfaceIP

Event ID 268

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"

ArcSight Field	Vendor Field
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"IXFR_RESP_RECV"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	InterfaceIP

Event ID 269

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"AXFR_REQ_OUT"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event ID 270

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"AXFR_REQ_RECV"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event ID 271

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
Name	"AXFR_RESP_OUT"
Old File Hash	ZoneScope
Request Context	Zone

ArcSight Field	Vendor Field
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	InterfaceIP

Event ID 272

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
Name	"AXFR_RESP_RECV"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	InterfaceIP

Event ID 273

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"XFR_NOTIFY_RECV"
Old File Hash	ZoneScope
Request Context	Zone

ArcSight Field	Vendor Field
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event ID 274

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"XFR_NOTIFY_OUT"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event ID 275

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"XFR_NOTIFY_ACK_IN"
Old File Hash	ZoneScope
Request Cookies	"Zone XFR"
Source Address	Source

Event ID 276

ArcSight Field	Vendor Field
Destination Address	Destination
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"XFR_NOTIFY_ACK_OUT"
Request Context	Zone
Request Cookies	"Zone XFR"
Source Address	InterfaceIP

Event ID 277

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
Name	"DYN_UPDATE_FORWARD"
Request Context	Zone
Request Cookies	"Dynamic update"
Source Address	ForwardInterfaceIP

Event ID 278

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
Name	"DYN_UPDATE_RESPONSE_IN"
Request Context	Zone

ArcSight Field	Vendor Field
Request Cookies	"Dynamic update"
Request Url	QNAME
Source Address	Source

Event ID 279

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"INTERNAL_LOOKUP_CNAME"
Old File Id	RD
Request Cookies	"Lookup"
Request Url	QNAME
Source Port	Port
Source Address	Source

Event ID 280

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"

ArcSight Field	Vendor Field
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"INTERNAL_LOOKUP_ADDITIONAL"
Old File Id	RD
Request Cookies	"Lookup"
Request Url	QNAME
Source Port	Port
Source Address	Source

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 Supplemental Configuration Guide (Connectors)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!