Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Windows Event Log – Native: Microsoft Network Policy Server

Supplemental Configuration Guide

November 30, 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026

Revision History

Date	Description
11/30/2016	Added Windows Server 2016 support.
02/16/2015	First edition of this configuration guide.

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

SmartConnector for Microsoft Windows Event Log – Native: Microsoft Network Policy Server

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Network Policy Server (NPS) and its event mappings to ArcSight data fields.

Versions supported:

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

The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Microsoft Network Policy Server.

Product Overview

The following information is from Microsoft Windows Server TechNet Library. For complete information, see "RADIUS Accounting -> NPS Events and Event Viewer -> Configure NPS Event Logging" (http://technet.microsoft.com/en-us/library/cc731085(v=ws.10).

Internet Authentication Service (IAS) was renamed Network Policy Server (NPS) starting with Windows Server 2008. The content of this guide applies to both IAS and NPS. Throughout the text, NPS is used to refer to all versions of the service, including the versions originally referred to as IAS.

Windows Server 2008 and Windows Server 2016 are supported.

NPS Logging

NPS logging is also called RADIUS accounting, and should be configured to your requirements whether NPS is used as a RADIUS server, proxy, NAP policy server, or any combination of the three configurations.

To configure NPS logging, you must configure the events logged and viewed with Event Viewer and determine other information you want to log. In addition, you must decide whether you want to log user authentication and accounting information to text log files stored on the local computer or to a SQL Server database on either the local computer or a remote computer.

Using the event logs in Event Viewer, you can monitor Network Policy Server (NPS) errors and other events that you configure NPS to record.

NPS records connection request failure events in the System and Security event logs by default. Connection request failure events consist of requests that are rejected or discarded by NPS. Other NPS authentication events are recorded in the Event Viewer system log on the basis of the settings that you specify in the NPS snap-in. Some events that might contain sensitive data are recorded in the Event Viewer security log.

Use this procedure to configure Network Policy Server (NPS) to record connection request failure and success events in the Event Viewer system log.

Membership in Domain Admins, or equivalent, is the minimum required to complete this procedure.

To configure NPS event logging using the Windows interface:

1. Open the Network Policy Server (NPS) snap-in.
2. Right-click NPS (Local), and then click Properties.
3. On the General tab, select each required option, and then click OK.

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 Windows 2016, 2012, and 8

General

ArcSight ESM Field	Device-Specific Field
Device Vendor	'Microsoft'
Device Product	'NPS'

Event 13

ArcSight ESM Field	Device-Specific Field
Name	'A RADIUS message was received'
Message	Both ('A RADIUS message was received from the invalid RADIUS client IP address',%1)

ArcSight ESM Field	Device-Specific Field
Source Address	%1 (client IP address)

Event 25

ArcSight ESM Field	Device-Specific Field
Name	'The address of remote RADIUS server in remote RADIUS server group resolves to local address will be ignored'
Message	Both ('The address of remote RADIUS server ',%1,' in remote RADIUS server group ',%2,' resolves to local address ',%3,'. The address will be ignored.')
Source Address	%3 (address)
Additional data	%2 (ServerGroup)
Destination Address	%1 (address)

Event 4400

ArcSight ESM Field	Device-Specific Field
Name	'A LDAP connection with domain controller for domain is established'
Message	Both ('A LDAP connection with domain controller ',%1,' for domain ',%2,' is established')
Destination Host Name	%1 (host name)
Destination NT Domain	%2 (domain name)

Event 4402

ArcSight ESM Field	Device-Specific Field
Name	'No Domain controller available for domain'
Message	Both ('There is no domain controller available for domain ',%1)
Destination NT Domain	%1 (domain name)

Event 4405

ArcSight ESM Field	Device-Specific Field
Name	'NPS cannot log accounting information in the primary data store'
Message	Both ('NPS cannot log accounting information in the primary data store (',%1,'). Due to this logging failure, NPS will discard all connection requests. Error information: ',%2)'
Destination NT Domain	%1 (domain name)
Reason	%2 (reason code)

Mappings for Windows 2008 R2

General

ArcSight ESM Field	Device-Specific Field
Device Vendor	'Microsoft'
Device Product	'NPS'

Event 13

ArcSight ESM Field	Device-Specific Field
Name	'A RADIUS message was received'
Source Address	%1 (client IP address)
Message	Both ('A RADIUS message was received from the invalid RADIUS client IP address ','%1)

Event 4400

ArcSight ESM Field	Device-Specific Field
Name	'A LDAP connection with domain controller for domain is established'
Destination Host Name	%1 (host name)
Destination NT Domain	%2 (domain name)
Message	Both (A LDAP connection with domain controller ',%1,' for domain ',%2,' is established)

Event 4402

ArcSight ESM Field	Device-Specific Field
Name	'No Domain controller available for domain'
Message	Both ('There is no domain controller available for domain' ',%1)
Destination NT Domain	%1 (domain name)

Event 4405

ArcSight ESM Field	Device-Specific Field
Name	'NPS cannot log accounting information in the primary data store'
Destination Host Name	%1 (host name)
Reason	%2 (reason code)
Message	Both ('NPS cannot log accounting information in the primary data store (',%1,'). Due to this logging failure, NPS will discard all connection requests. Error information: ',%2')

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 system, 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 arc-doc@hpe.com.

We appreciate your feedback!