



Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

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

Supplemental Configuration Guide

March 29, 2013

Supplemental Configuration Guide

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

March 29, 2013

Copyright © 2010 – 2013 Hewlett Packard Enterprise Development LP

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 Development LP shall not be liable for technical or editorial 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. Hewlett Packard Enterprise Development LP 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 Development LP 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.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:

<https://www.protect724.hpe.com/docs/DOC-13026>.

Revision History

Date	Description
03/29/2013	Added support for Windows 2012/8 events.
09/28/2012	First edition of this configuration guide.

Contents

Product Overview..... 4

 NPS Logging..... 4

Connector Installation and Configuration 5

 Windows 2008 R2 NPS Event Log Mappings to ArcSight ESM Fields 5

 General 5

 Event 13..... 5

 Event 4400..... 5

 Event 4402..... 5

 Event 4405..... 5

 Windows 2012/8 NPS Event Log Mappings to ArcSight ESM Fields..... 6

 General 6

 Event 13..... 6

 Event 25..... 6

 Event 4400..... 6

 Event 4402..... 6

 Event 4405..... 7

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

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Unified: Microsoft Network Policy Server (NPS) and its event mappings to ArcSight data fields. NPS with Microsoft Windows 2008 R2, Windows 2012, and Windows 8 is supported.

The *ArcSight SmartConnector Mappings to Windows Security Events* 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 – Unified: 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\(v=ws.10\)](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.

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 – Unified](#), selecting **Microsoft Windows Event Log – Unified** as the connector to be configured. During installation, select **true** for the **System Logs** field for system events to be collected.

Windows 2008 R2 NPS Event Log Mappings to ArcSight ESM Fields

General

ArcSight ESM Field	Device-Specific Field
Source Service Name	EventSource
Device Vendor	'Microsoft'
Device Product	'NPS'

Event 13

ArcSight ESM Field	Device-Specific Field
Name	'A RADIUS message was received'
Source Address	client IP address

Event 4400

ArcSight ESM Field	Device-Specific Field
Name	'A LDAP connection with domain controller for domain is established'
Destination Host Name	host name
Destination NT Domain	domain name

Event 4402

ArcSight ESM Field	Device-Specific Field
Name	'No Domain controller available for domain'
Message	'There is no domain controller available for domain'
Destination NT Domain	domain name

Event 4405

ArcSight ESM Field	Device-Specific Field
Name	'NPS cannot log accounting information in the primary data store'
Destination Host Name	host name
Reason	reason code

Windows 2012/8 NPS Event Log Mappings to ArcSight ESM Fields

General

ArcSight ESM Field	Device-Specific Field
Source Service Name	EventSource
Device Vendor	'Microsoft'
Device Product	'NPS'

Event 13

ArcSight ESM Field	Device-Specific Field
Name	'A RADIUS message was received'
Message	'A RADIUS message was received from the invalid RADIUS client IP address'
Source Address	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	'The address of remote RADIUS server in remote RADIUS server group resolves to local address. The address will be ignored.'
Source Address	address
Additional data	ServerGroup
Destination Address	address

Event 4400

ArcSight ESM Field	Device-Specific Field
Name	'A LDAP connection with domain controller for domain is established'
Message	'A LDAP connection with domain controller for domain is established'
Destination Host Name	host name
Destination NT Domain	domain name

Event 4402

ArcSight ESM Field	Device-Specific Field
Name	'No Domain controller available for domain'
Message	'There is no domain controller available for domain'
Destination NT Domain	domain name

Event 4405

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