Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Windows Event Log – Unified: Microsoft Remote Access

Supplemental Configuration Guide

May 15, 2014

Supplemental Configuration Guide

SmartConnector for Windows Event Log – Unified: Microsoft Remote Access

May 15, 2014

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 Package 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 Package 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 Package Enterprise Development LP copyrights, trademarks and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026.

Revision History

Date	Description
05/15/2014	GA support for Windows 2012 R2.
03/31/2014	Added beta support for Windows 2012 R2.
05/15/2013	Updated mappings for event 20169.
03/29/2013	Added support for Windows 2012/Windows 8.
09/28/2012	First edition of this guide.

Contents

SmartConnector for Microsoft Windows Event Log – Unified: Remote Access

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Unified: Remote Access Service and its event mappings to ArcSight data fields. Microsoft Windows 2008 R2, Windows 2012, Windows 8, and Windows 2012 R2 are supported with the SmartConnector for Microsoft Windows Event Log – Unified.

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 Microsoft Remote Access.

Product Overview

Routing and Remote Access is a network service in Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, Windows Server 2003, and Windows 2000 Server that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

Remote Access Configuration

For complete information about Microsoft's Reporting and Remote Access Service, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)":

http://technet.microsoft.com/en-us/library/hh831416

When configuring the Remote Access Log, specify **system** as the event log type for Microsoft Remote Access.

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

General

ArcSight Field	Vendor Field
Source Service Name	EventSource
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 20088

ArcSight Field	Vendor Field
Name	Remote Access Server acquired IP Address
Destination Address	Assigned Address

Event 20106

ArcSight Field	Vendor Field
Name	Unable to add interface
Device Outbound Interface	Interface
Application Protocol	Protocol

Event 20184

ArcSight Field	Vendor Field
Name	Interface is unreachable
Device Inbound Interface	Interface

Event 20249

ArcSight Field	Vendor Field
Name	Failed to authenticate
Device Custom String 4	Correlation-ID
Source User Name	Connected User
Source NT Domain	Domain of Connected User
Application Protocol	Protocol
Source Port	Port

Event 20252

ArcSight Field	Vendor Field
Name	Authentication process did not complete
Device Custom String 4	Correlation-ID
Application Protocol	Protocol
Source Port	Port

Event 20255

ArcSight Field	Vendor Field
Name	Connection was prevented
Device Custom String 4	Correlation-ID
Source User Name	Connected User
Source NT Domain	Domain of Connected User
Application Protocol	Protocol
Source Port	Port

Event 20258

ArcSight Field	Vendor Field
Name	Account does not have Remote Access privilege
Device Custom String 4	Correlation-ID
Source User Name	Connected User
Source NT Domain	Domain of Connected User
Application Protocol	Protocol
Source Port	Port

Event 20266

ArcSight Field	Vendor Field
Name	Successfully authenticated
Device Custom String 4	Correlation-ID
Source User Name	Connected User
Source NT Domain	Domain of Connected User
Application Protocol	Protocol
Source Port	Port

Event 20271

ArcSight Field	Vendor Field
Name	Failed an authentication attempt
Device Custom String 4	Correlation-ID
Source User Name	Connected User
Source NT Domain	Domain of Connected User
Source Address	Address
Reason	Reason

Event 20272

ArcSight Field	Vendor Field
Name	User connected and disconnected
Device Custom String 4	Correlation-ID
Source User Name	Connected User
Source NT Domain	Domain of Connected User
Application Protocol	Protocol
Source Port	Port
Start Time	Connected time
End Time	Disconnected time
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds
Bytes Out	Bytes Out
Bytes In	Bytes In
Additional data	disconnectingReason
Additional data	tunnel
Additional data	quarantineState

Event 20274

ArcSight Field	Vendor Field
Name	User connected and has been assigned address
Device Custom String 4	Correlation-ID
Source User Name	Connected User
Source NT Domain	Domain of Connected User
Application Protocol	Protocol
Source Port	Port
Destination Address	Assigned Address

Event 20275

ArcSight Field	Vendor Field
Name	User disconnected
Device Custom String 4	Correlation-ID
Source Address	Address

Windows 2012/Windows 2012 R2/Windows 8

General

ArcSight Field	Vendor Field
Source Service Name	EventSource
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

20088

ArcSight Field	Vendor Field
Name	'Remote Access Server acquired IP Address'
Message	'The Remote Access Server acquired IP Address to be used on the Server Adapter.'
Destination Address	Assigned Address

20106

ArcSight Field	Vendor Field
Name	'Unable to add interface'
Message	'Unable to add the interface with the Router Manager for the protocol. The following error occurred:'
Device Outbound Interface	Interface
Application Protocol	Protocol
Device Custom String 5	Routing Domain ID

20184

ArcSight Field	Vendor Field
Name	'Interface is unreachable'
Message	'Interface is unreachable because it is not currently connected to the network'
Device Inbound Interface	Interface
Device Custom String 5	Routing Domain ID

20249

ArcSight Field	Vendor Field
Name	'Failed to authenticate'
Message	'The user has connected and failed to authenticate on port. The line has been disconnected.'
Device Custom String 4	Correlation-ID
Source User Name	Connected User
Source NT Domain	Domain of Connected User
Application Protocol	Protocol
Source Port	Port

20252

ArcSight Field	Vendor Field
Name	'Authentication process did not complete'
Message	'The user connected to port has been disconnected because the authentication process did not complete within the required amount of time.'
Device Custom String 4	Correlation-ID
Application Protocol	Protocol
Source Port	Port

20255

ArcSight Field	Vendor Field
Name	'Connection was prevented'
Device Custom String 4	Correlation-ID
Application Protocol	Protocol
Source Port	Port
Source User Name	Connected User
Source NT Domain	Domain of Connected User
Message	Message Text

20258

ArcSight Field	Vendor Field
Name	'Account does not have Remote Access privilege'
Message	'The account for user connected on port does not have Remote Access privilege. The line has been disconnected.'
Device Custom String 4	Correlation-ID
Source User Name	Connected User
Source NT Domain	Domain of Connected User
Application Protocol	Protocol
Source Port	Port

20266

ArcSight Field	Vendor Field
Name	'Successfully authenticated'
Message	'The user has connected and has been successfully authenticated on port. Data sent and received over this link is strongly encrypted.'
Device Custom String 4	Correlation-ID
Device Custom String 5	Routing Domain ID
Source User Name	Connected User
Source NT Domain	Domain of Connected User
Application Protocol	Protocol
Source Port	Port

20271

ArcSight Field	Vendor Field
Name	'Failed an authentication attempt'
Device Custom String 4	Correlation-ID
Source User Name	Connected User
Source NT Domain	Domain of Connected User
Source Address	Address
Message	'The user connected but failed an authentication attempt'
Reason	Reason

20272

ArcSight Field	Vendor Field
Name	'User connected and disconnected'
Message	"The user connected and disconnected'
Device Custom String 4	Correlation-ID
Device Custom String 5	Routing Domain ID
Source User Name	Connected User
Source NT Domain	Domain of Connected User
Application Protocol	Protocol
Source Port	Port
Start Time	Start Time
End Time	End Time
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds
Bytes Out	Bytes Out
Bytes In	Bytes In
Additional data	disconnectingReason
Additional data	tunnel
Additional data	quarantineState

20274

ArcSight Field	Vendor Field
Name	'User connected and has been assigned address'
Message	'The user connected on port has been assigned address'
Device Custom String 4	correlation-ID
Device Custom String 5	Routing Domain ID
Source User Name	Connected User
Source NT Domain	Domain of Connected User
Application Protocol	Protocol
Source Port	Port
Destination Address	Assigned Address

20275

ArcSight Field	Vendor Field
Name	'User disconnected'
Message	'The user with ip address has disconnected'
Device Custom String 4	Correlation-ID
Device Custom String 5	Routing Domain ID
Source Address	Address

20169

ArcSight Field	Vendor Field
Name	'Unable to contact a DHCP server'
Message	'The Automatic Private IP Address will be assigned to dial-in clients. Clients may be unable to access resources on the network.'
Source Address	Address