Micro Focus Security ArcSight Connectors

SmartConnector for Windows Event Log – Native: Microsoft Sysmon Logs

Supplemental Configuration Guide

Document Release Date: September 19, 2019
Software Release Date: September 19, 2019

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) 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. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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

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.

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
09/19/2019	First edition of this Configuration Guide, for initial support of these events.

Contents

SmartConnector for Microsoft Windows Event Log – Native: Microsoft Sysmon Logs

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Sysmon 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

The *SmartConnector for Microsoft Windows Event Log – 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 Microsoft Remote Access.

Product Overview

Microsoft Sysmon Logs is a network service in Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, and Windows Server 2016 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

Microsoft Sysmon Logs Configuration

For complete information about Microsoft's Reporting and Microsoft Sysmon Logs, 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 Microsoft Sysmon Logs, 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 – 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 Sysmon Logs

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Sysmon'
Device Version	'Unknown'

Event 1

ArcSight Field	Vendor Field
Name	'Process Created'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Device Process Id	__safeToInteger(ProcessId)
Source Process Name	Image
Message	Description
File Name	OriginalFileName
Device Custom String1	CommandLine
Old File Path	CurrentDirectory
Source Nt Domain	__extractNTDomain(User)
Source User Name	__extractNTUser(User)
Destination User Id	LogonGuid
Source User Id	LogonId
Device Custom String 4	IntegrityLevel

ArcSight Field	Vendor Field
File Hash	Hashes
Old File Id	ParentProcessGuid
Destination Process Id	ParentProcessId
Destination Process Name	ParentImage
Device Custom String 5	ParentCommandLine
Device Action	'Process Create'

Event 2

ArcSight Field	Vendor Field
Name	'File creation time changed'
File Id	ProcessGuid
Message	'File creation time changed'
Device Receipt Time	UtcTime
Device Process Id	__safeToInteger(ProcessId)
Source Process Name	Image
File Path	TargetFilename
File Create Time	CreationUtcTime
Old File Create Time	PreviousCreationUtcTime
Device Action	'File creation time changed'

Event 3

ArcSight Field	Vendor Field
Name	'Network connection detected'
Message	'Network connection detected'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Device Process Id	__safeToInteger(ProcessId)
Source Process Name	Image
Source Nt Domain	__extractNTDomain(User)
Source User Name	__extractNTUser(User)

ArcSight Field	Vendor Field
Transport Protocol	Protocol
Device Action	__concatenate("Initiated :",Initiated)
Source Address	__stringToIPv6Address(SourceIp)
Source Host Name	SourceHostname
Source Port	__safeToInteger(SourcePort)
Source Port Name	SourcePortName
DestinationAddress	__stringToIPv6Address(DestinationIp)
Destination Host Name	DestinationHostname
Destination Port	__safeToInteger(DestinationPort)

Event 4

ArcSight Field	Vendor Field
Name	'Sysmon service state changed'
Message	'Sysmon service state changed'
Device Receipt Time	UtcTime
Device Action	State
Additionaldata.schemaVersion	SchemaVersion

Event 5

ArcSight Field	Vendor Field
Name	'Process Terminated'
Message	'Process Terminated'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Device Process Id	__safeToInteger(ProcessId)
Source Process Name	Image
Device Action	'Process Terminated'

Event 7

ArcSight Field	Vendor Field
Name	'Image Loaded'
Message	Description
Device Receipt Time	UtcTime
Device Process Id	__safeToInteger(ProcessId)
File Id|	ProcessGuid
Source Process Name	Image
Device Custom String1	ImageLoaded
File Hash	Hashes
File Name	OriginalFileName
File Type	Signed
File Permission	SignatureStatus
Device Action	'Image Loaded'

Event 9

ArcSight Field	Vendor Field
Name	'RawAccessRead detected'
Message	'RawAccessRead detected'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Device Process Id	__safeToInteger(ProcessId)
Source Process Name	Image
Device Custom String5	Device
Device Action	'RawAccessRead detected'

Event 10

ArcSight Field	Vendor Field
Name	'Process accessed'
Message	'Process accessed'
Device Receipt Time	UtcTime
File Id	SourceProcessGUID
Device Process Id	__safeToInteger(SourceProcessId)
additionaldata.sourceThreadId	SourceThreadId
Source Process Name	SourceImage
Old File Id	TargetProcessGUID
Destination Process Id	__safeToInteger(TargetProcessId)
Destination Process Name	TargetImage
Device Custom String1	GrantedAccess
Old File Path	CallTrace
Device Action	'Process accessed'

Event 11

ArcSight Field	Vendor Field
Name	'File created'
Message	'File created'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Device Process Id	ProcessId
Source Process Name	Image
File Path	TargetFilename
File Create Time	CreationUtcTime
Device Action	'File Created'

Event 12

ArcSight Field	Vendor Field
Name	'Registry object added or deleted'
Message	'Registry object added or deleted'
DeviceReceiptTime	UtcTime
FileId	ProcessGuid
DeviceProcessId	ProcessId
SourceProcessName	Image
FilePath	TargetObject
DeviceAction	'Registry object added or deleted'

Event 13

ArcSight Field	Vendor Field
Name	'Registry value set'
Message	'Registry value set'
DeviceReceiptTime	UtcTime
FileId	ProcessGuid
DeviceProcessId	__safeToInteger(ProcessId)
SourceProcessName	Image
FilePath	TargetObject
Device Custom String4	Details
DeviceAction	'Registry value set'

Event 15

ArcSight Field	Vendor Field
Name	'File stream created'
Message	'File stream created'
DeviceReceiptTime	UtcTime
FileId	ProcessGuid

ArcSight Field	Vendor Field
DeviceProcessId	__safeToInteger(ProcessId)
SourceProcessName	Image
FilePath	TargetFilename
File Create Time	CreationUtcTime
File Hash	Hash
DeviceAction	'File stream created'

Event 16

ArcSight Field	Vendor Field
Name	'Sysmon config state changed'
Message	'Sysmon config state changed'
SourceProcessName	Configuration
File Hash	ConfigurationFileHash
DeviceAction	'Sysmon config state changed'
DeviceReceiptTime	UtcTime

Event 17

ArcSight Field	Vendor Field
Name	'Create Pipe'
Message	'Create Pipe'
DeviceReceiptTime	UtcTime
File Id	ProcessGuid
DeviceProcessId	__safeToInteger(ProcessId)
SourceProcessName	Image
Device Custom String6	PipeName
DeviceAction	'Pipe Created'

Event 18

ArcSight Field	Vendor Field
Name	'Pipe Connected'
Message	'Pipe Connected'
DeviceReceiptTime	UtcTime
File Id	ProcessGuid
DeviceProcessId	__safeToInteger(ProcessId)
SourceProcessName	Image
Device Custom String6	PipeName
DeviceAction	'Pipe Connected'

Event 22

ArcSight Field	Vendor Field
Name	'Dns query'
Message	'Dns query'
DeviceReceiptTime	UtcTime
File Id	ProcessGuid
DeviceProcessId	__safeToInteger(ProcessId)
SourceProcessName	Image
Device Host Name	QueryName
Device Custom String4	QueryResults
DeviceAction	'Dns query'

Event 255

ArcSight Field	Vendor Field
Name	'Error report'
SourceProcessName	ID
Message	'Description
DeviceReceiptTime	UtcTime
DeviceAction	__stringConstant("Level : Error")

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!