Micro Focus Security ArcSight Connectors

SmartConnector for Windows Event Log – Native: Microsoft Windows BITS Client Logs

Supplemental Configuration Guide

Document Release Date: June 18, 2020
Software Release Date: June 18, 2020

Legal Notices

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

https://www.microfocus.com

Copyright Notice

Trademark Notices

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
06/18/2020	First edition of this Configuration Guide to provide support for Microsoft Windows BITS client logs.

Contents

SmartConnector for Microsoft Windows Event Log – Native: Microsoft Windows BITS Client Logs

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Windows BITS Client 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
- Microsoft Windows Server 2019 (*)

Product Overview

Microsoft Windows Background Intelligent Transfer Service (BITS) helps programmers and system administrators to download files from or upload files to HTTP web servers and share files using Server Message Block (SMB) protocol. BITS will take the cost of the transfer into consideration, as well as the network usage so that the user's foreground work has as little impact as possible. It also handles network interruptions, pausing, and automatically resuming transfers, even after a reboot. BITS includes `PowerShell cmdlets` for creating and managing transfers as well as the BitsAdmin command-line utility.

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 **Custom Logs** field and enter **Microsoft-Windows-Bits-Client/Operational**.

Mappings for Microsoft Windows BITS Client Logs

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows BITS Client'

Event ID 3

ArcSight Field	Vendor Field
Destination Nt Domain	string2
Destination User Name	string2
Device Custom String 4	string
Device Custom String 4 Label	"Job Title"
Message	All of("The BITS service created a new job: ",string," , with owner ",string2)
Name	"The BITS service created a new job"

Event ID 4

ArcSight Field	Vendor Field
Device Custom Number 1	fileCount
Device Custom Number 1 Label	"File count"
Device Custom String 4	jobTitle
Device Custom String 4 Label	"Job Title"
Device Custom String 5	jobId
Device Custom String 5 Label	"Job ID"
Device Custom String 6	jobOwner
Device Custom String 6 Label	"Job Owner"
Message	All of("The transfer job is complete.User: ",User,", Transfer job: ",jobTitle,", Job ID: ",jobId,", Owner: ",jobOwner,", File count: ",fileCount)

ArcSight Field	Vendor Field
Name	"The transfer job is complete"
Source Nt Domain	User
Source User Name	User

Event ID 59

ArcSight Field	Vendor Field
Bytes In	bytesTransferredFromPeer
Bytes Out	bytesTransferred
Destination Host Name	peer
Device Custom Number 1	bytesTotal
Device Custom Number 1 Label	"Total Bytes"
Device Custom String 1	transferId
Device Custom String 1 Label	"Transfer ID"
Device Custom String 4	name
Device Custom String 4 Label	"Job Title"
Device Custom String 5	Id
Device Custom String 5 Label	"Job ID"
File Create Time	fileTime
File Path	url
File Size	fileLength
Message	All of("BITS started the ",name," transfer job that is associated with the ",url," URL")
Name	"BITS started the transfer for job"

Event ID 60

ArcSight Field	Vendor Field
Bytes In	bytesTransferredFromPeer
Bytes Out	bytesTransferred
Destination Host Name	peer
Device Custom Number 1	bytesTotal

ArcSight Field	Vendor Field
Device Custom Number 1 Label	"Total Bytes"
Device Custom String 1	transferId
Device Custom String 1 Label	"Transfer ID"
Device Custom String 4	name
Device Custom String 4 Label	"Job Title"
Device Custom String 5	Id
Device Custom String 5 Label	"Job ID"
File Create Time	fileTime
File Path	url
File Size	fileLength
Message	All of("BITS stopped the ",name," transfer job that is associated with the ",url," URL. The status code is 0x",hr)
Name	"BITS stopped transferring for job"
Old File Name	Both("Proxy :",proxy)
Old File Path	Both("Bandwidth Limit :",bandwidthLimit)
Reason	Both ("0x",hr)

Event ID 61

ArcSight Field	Vendor Field
Bytes Out	bytesTransferred
Destination Host Name	peer
Device Custom Number 1	bytesTotal
Device Custom Number 1 Label	"Total Bytes"
Device Custom String 1	transferId
Device Custom String 1 Label	"Transfer ID"
Device Custom String 4	name
Device Custom String 4 Label	"Job Title"
Device Custom String 5	Id
Device Custom String 5 Label	"Job ID"
File Create Time	fileTime

ArcSight Field	Vendor Field
File Path	url
File Size	fileLength
Message	All of("BITS stopped the ",name," transfer job that is associated with the ",url," URL. The status code is 0x",hr)
Name	"BITS stopped transferring the job"
Old File Name	Both("Proxy :",proxy)
Reason	Both("0x",hr)

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 7.15.0)

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!