Micro Focus Security ArcSight SmartConnectors

SmartConnector for Amazon S3

Configuration Guide

Document Release Date: November 2022
Software Release Date: November 2022

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:

https://www.microfocus.com/support-and-services/documentation

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://www.microfocus.com/documentation/arcsight/

Contents

Configuration Guide for Amazon S3 SmartConnector

This guide provides information for installing the SmartConnector for Amazon S3 and configuring the device for event collection from an Amazon S3 bucket.

An Amazon S3 bucket receives events in any of the following ways:

- Through a device - A device sends events directly to an Amazon S3, or you can upload events manually.
- Through the Amazon Cloudwatch - Amazon CloudWatch forwards or exports events to an Amazon S3 bucket. For information about exporting logs to Amazon S3, see the Amazon CloudWatch Documentation.

Product Overview

The SmartConnector for Amazon S3 currently supports the following log sources:

Note: The following log sources are also supported through the Amazon S3 SmartConnector. However, you need to make sure that the logs from these log sources are made available in the S3 bucket.

Apache HTTP Server Access Multiple Folder File	Dell EMC Isilon/PowerScale Unity and VNXe Storage	Linux Audit File	Qualys QualysGuard File
Apache HTTP Server Error File	Extreme Networks Dragon Export Tool File	McAfee Web Gateway File_ Access	Rapid7 NeXpose XML File
Apache Tomcat File	Extreme Networks Dragon IDS File	McAfee Web Gateway File_ Access_Denied	SAINT Vulnerability Scanner
AWS CloudTrail	F-Secure Anti-Virus File	McAfee Web Gateway File_ Found_viruses	SAP Real-Time Security Audit Multiple Folder File
Blue Coat Proxy SG Multiple Server File	Google Cloud Platform	McAfee Web Gateway File_ Security	SAP Security Audit File
Box	HPE OM i Web Services	Microsoft 365 Defender	sFlow Devices
CA SiteMinder Single Sign-On File	HPE OM Incident Web Service	Microsoft DHCP File	Snort Multiple File
CA Top Secret for z/OS File_tss_audit_track	HPE OpenVMS File	Microsoft DNS DGA Trace Log Multiple Server File	Squid Web Proxy Server File
CA Top Secret for z/OS File_tss_util_short	HPE UX Audit File	Microsoft DNS Trace Log Multiple Server File	Sun ONE Direct Server/Multi Server File

CEF Format	IBM BigFix REST API	Microsoft Exchange Message Tracking Log Multiple Server File	Sun ONE Web Access Multiple Server file
Check Point OPSEC NG	IBM eServer Audit Journal File_type5	Microsoft Exchange PowerShell	Symantec AntiVirus Corporate Edition File_ 8.x
Cisco IronPort Email Security Appliance File_ Http	IBM eServer iSeries Audit Journal File_type1iSeries	Microsoft Forefront Threat Management Gateway File	Symantec AntiVirus Corporate Edition File_ 9.x
Cisco IronPort Email Security Appliance File_ TextMail	IBM Lotus Domino Web Server File	Microsoft IIS File	Symantec AntiVirus Corporate Edition File_ 10.x
Cisco IronPort Web Security Appliance File	IBM NVAS for z/OS File	MicroSoft IIS Multiple Server File	TCPdump
Cisco Secure IPS SDEE	IBM NVAS Session for z/OS File	Microsoft IIS Multiple Site File	Tenable Nessus .nessus File
Cisco Sourcefire Defense Center eStreamer	IBM RACF for z/OS File	Microsoft Network Policy Server File	Tenable SecurityCenter XML File
Cisco Umbrella - DNS, Proxy, IP Logs	IBM SDSF for z/OS File	Microsoft Office 365 Management Activity	Tripwire IP360 File
CiscoUmbrella-DNSLogs	IBM System Log for z/OS File	NetApp Filer Event Log	Tripwire Manager File
CiscoUmbrella-DNSLogs_ v3	IBM WebSphere File	NetApp ONTAP XML File	UNIX Login/Logout File
CiscoUmbrella-DNSLogs_ v4	IDMEF XML File	NMap XML File	VMware Web Services
CiscoUmbrella-IPLogs	IP Flow (Netflow/J-Flow)	Okta	Windows
CiscoUmbrella-ProxyLogs	IP Flow Information Export (IPFIX)	Oracle WebLogic Server File_ Access	Zeek IDS NG File
CiscoUmbrella-ProxyLogs-v4	JBoss Security Audit File	Oracle WebLogic Server File_ Server	
CloudFront Access CloudFront Real Time	Juniper Steel-Belted Radius File	OVAL XML File	

Syslog sources			
AirMagnet Enterprise Syslog	Cisco Meraki Syslog	Infoblox NIOS Syslog	Proofpoint Enterprise Protection and Enterprise Privacy Syslog
Apache HTTP Server Syslog	Cisco Mobility Services Engine Syslog	Ingrian DataSecure Syslog	Pulse Secure Pulse Connect Secure Syslog

Arbor Networks Peakflow Syslog	Cisco NX-OS Syslog	Intersect Alliance SNARE Syslog	Radware DefensePro Syslog
ArcSight CEF Cisco FireSIGHT Syslog	Cisco Secure ACS Syslog	ISC BIND Syslog	Raw Syslog Daemon
ArcSight CEF Encrypted Syslog (UDP)	Cisco Wireless LAN Controller Syslog	ISC DHCP Syslog	Sabernet NTSyslog
ArcSight Common Event Format Syslog	Citrix NetScaler Syslog	Juniper Firewall ScreenOS Syslog	Sendmail Syslog
Barracuda Email Security Gateway Syslog	Dell SonicWALL Syslog	Juniper IDP Series Syslog	Symantec Messaging Gateway Syslog
Barracuda Firewall NG F-Series Syslog	F5 BIG-IP Syslog	Juniper JUNOS Syslog	Syslog NG Daemon
Barracuda Web Appliance Firewall Syslog	Fortinet Fortigate Syslog	Juniper Network and Security Management Syslog	TippingPoint SMS Syslog
Blue Coat Proxy SG Syslog	HoneyD Syslog	Linux Audit Syslog	TippingPoint SMS Syslog Extended
BroadWeb NetKeeper IDP Syslog	HPE Aruba Mobility Controller Syslog	McAfee Email Gateway Syslog	Top Layer Attack Mitigator Syslog
Brocade BigIron Syslog	HPE c7000 Virtual Connect Module Syslog	McAfee Firewall Enterprise Syslog	Type80 SMA_RT Syslog
Check Point Syslog	HPE H3C Syslog	McAfee Network Security Manager Syslog	UNIX OS Syslog
Cisco ASA Syslog	HPE Integrated Lights-Out Syslog	McAfee Web Gateway Syslog	VarySys PacketAlarm IPS Syslog
Cisco Catalyst OS Syslog	HPE ProCurve Syslog	Microsoft IIS Syslog	VMware ESXi Server Syslog
Cisco IOS Syslog	HPE UX Syslog	NitroSecurity Syslog	Vormetric CoreGuard Syslog
Cisco IronPort Email Security Appliance Syslog	HP Printers Syslog	Nortel Contivity Switch (VPN) Syslog	
Cisco IronPort Web Security Appliance Syslog	IBM AIX Audit Syslog	Oracle Audit Syslog	
Cisco ISE Syslog	IBM Security Access Manager Syslog	Oracle Solaris Basic Security Module Syslog	

However, the connector can support other log sources available in an Amazon S3 bucket. One connector instance can support one log source. To support multiple log sources, install multiple instances of the Amazon S3 connector, and provide specific configurations. With parser

updates, the connector can support extended events of the log sources or a completely new log source.

The supported log formats are: CSV, Json, Regex, Key- value pair, XML, XQuery, and CEF.

Amazon Web Services (AWS) is a collection of remote computing services (also called web services) that make up a cloud computing platform offered by Amazon which provides online services for other websites or client-side applications.

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. You must create a bucket in one of the Amazon regions to upload your data. You can then upload any number of objects to the bucket.

Amazon Simple Queue Service (Amazon SQS) is a fully managed service that works with serverless systems, micro-services, and distributed architectures. It has the capability of sending, storing and receiving messages at scale without dropping message data.

Understanding Data Collection

The following diagram provides a high-level overview on the data collection flow. With the SmartConnector for Amazon S3, you can choose one of the two approaches below to collect events from an S3 bucket. To configure log retrieval, see Configuring Log Retrieval.

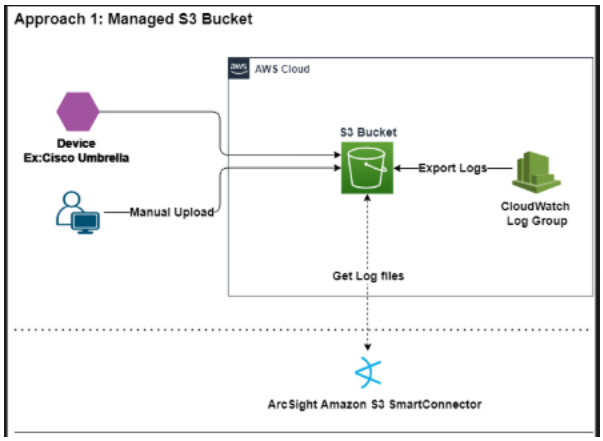
S3 Approach - Poll Approach

This approach is recommended for Vendor Managed S3 Buckets.

In this approach, the connector directly enumerate an S3 bucket for the new files. This approach is recommended when logs are stored in the vendor's Amazon S3 bucket with limited access.

Process Flow

1. A file is enumerated from a specified folder in S3.
2. The log files are collected from S3.
3. The log files are processed.
4. The connector will continue to collect only new and unprocessed files.



SQS Approach - Notification Approach

This approach is recommended for Customer Managed S3 Buckets.

In this approach, the connector polls SQS for S3 notifications and collects log files from an S3 bucket. This approach is recommended when users have control over the AWS account with permissions to create SQS and configure S3 notifications to SQS.

Process Flow

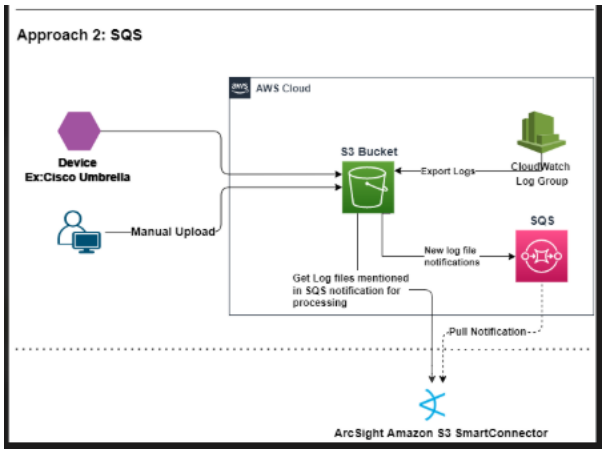
1. Amazon S3 is configured to send notifications from a new file to SQS.

2. The connector reads the SQS notifications.

3. Based on the SQS notifications, the log files are collected from the S3 bucket.

4. The log files are processed.

5. The SQS messages are deleted.



Setting up an AWS Account

If you are using an EC2 role-based credentials, then use an IAM role with AmazonS3ReadOnlyAccess and AmazonSQSFullAccess policies.

If you are using an access key/secret key as credentials, complete the following procedure

1. Create an Amazon Web Services account.
2. In the Welcome to Amazon Web Services window, click **Launch Management Console** .
3. Click **Amazon Web Services** > **Administration & Security** > **Identity & AccessManagement**.
4. On the left side of the console, go to **Dashboard** and select Groups.
5. Create a new group with permissions to access the logs stored in S3 through the API.
6. Click **Create New Group** and enter a **Group Name**, for example, arcsightgroup.
7. Click **Next** to attach two policies to the group.
8. Select the **AmazonS3ReadOnlyAccess** and **AmazonSQSFullAccess** check boxes policies of the arcsightgroup, and then click **Next**.

   The connector can now download logs.
9. Click **Create Group**.

Creating and Adding a User to a Group

To create and add a user who can access the logs stored in S3 through the API to a group:

1. Go to the Amazon Web Services console.
2. On the left pane, go to **Dashboard**.
3. Select **Users** and click **Create New Users**.
4. Enter the user name, for example, arcsight2.
5. Select the **Generate an Access Key** check box for each user and click **Create**.
6. Click the **Download Credentials** and save the .csv file.

   The downloaded Access Key ID and Secret Access Key will used during installation of the connector.
7. Click **Close** and return to the **Dashboard**.
8. Under **Dashboard**, select **Groups** and click the arcsightgroup previously created.
9. Click **Add Users to Group**.
10. Select the check boxes next to the users previously created, and then click **Add Users**.

AWS Credentials

In the configuration window, you can enter the AWS access key and AWS secret key. These parameters are optional and will be used if provided. Otherwise, the Default Credential Provider Chain is used, instead. The Default Credential Provider Chain searches for credentials in the following order, as documented by Class Default AWS Credentials Provider Chain.

1. In the environment variables: AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY (These recommended since they are recognized by all the AWS SDKs and CLI except for .NET), or AWS_ACCESS_KEY and AWS_SECRET_KEY (only recognized by Java SDK).
2. In the Java system properties: aws.accessKeyId and aws.secretKey.
3. In the **Web Identity Token Credentials**, from the environment or container
4. In the default **Credential Profiles** file, the `(~/.aws/credentials)`is shared by all AWS SDKs and the AWS CLI.
5. Credentials delivered through the Amazon EC2 container service if AWS_CONTAINER_ CREDENTIALS_RELATIVE_URI" environment variable is set and security manager has permission to access the variable.
6. In the instance **Profile Credentials**, through the Amazon EC2 metadata service.

Configuring Log Retrieval

S3 Approach - Poll Approach

This approach is highly recommended for users with vendor-managed S3 buckets, although users with customer-managed S3 buckets might also choose the S3 Approach.

You can also consider using this approach if the service provider (in this case, Cisco Umbrella), manages the AWS account and as a user you are not authorized to create AWS resources.

- **For vendor-managed S3 buckets:**
  - Note down the AWS credentials - access key and secret key, the S3 bucket name, the S3 folder name and the S3 region.
  - To enable logging of Cisco Umbrella logs to a Cisco-managed S3 Bucket, see, Enable Logging to a Cisco-managed S3 Bucket.
- **If you manage the AWS account and the S3 bucket:**
  - Set up an AWS account and create an Identity and Access Management (IAM) user or role.
  - Create an S3 bucket and configure it to receive logs.

Note: S3 buckets can either be encrypted or non-encrypted.

SQS Approach - Notification Approach

This is a recommended approach for Customer Managed S3 Buckets.

1. Set up an AWS account and create an Identity and Access Management (IAM) user or role.
2. Create an S3 bucket and configure it to receive logs.
3. Create an SQS queue and configure S3 to send events to SQS on new object creation.

Creating and Configuring an S3 Bucket to Receive Logs

To create a new S3 bucket:

1. Log in to the AWS Management Console and open the **Amazon S3** console.
2. Click **Create bucket**.
3. In the **Create bucket** dialog box, enter the **Bucket Name** of your S3 bucket, for example, arcsights3.

4. Accept or edit the default value settings in the other fields.
5. Click **Create**.

   Your new S3 bucket is now listed under the S3 bucket names.

The configuration to receive DNS, IP or Proxy Logs might change based on the device.

For Cisco Umbrella, see Enable Logging to Your Own S3 Bucket.

Configuring an S3 to Send Events to SQS on a New Object

Creating an SQS Queue for the Connector to Poll

To create a new SQS queue:

1. Log in to the **AWS Management** Console and open the **Amazon SQS** console.
2. Click **Create New Queue**.
3. In the **Create New Queue** dialog box, enter the **Bucket Name** of your S3 bucket, for example, arcsightQueue.
4. Accept or edit the default value settings of the other fields.
5. Click **Create Queue**.

   Your new queue is now listed under the queue names.
6. Select the Queue created.
   a. Click **Permissions**.
   b. Click **Add permission**.
   c. From **Select Effect**, click **Allow**.
   d. Enter Principal.
   e. Select Actions: Delete Message, Receive Message, and Send Message.
   f. Click **Add Permission**.

Configuring S3 to Send Events to SQS

To configure S3 to send events to SQS on a new object, see Amazon Documentation.

1. Log in to the **AWS Management** Console and open the **Amazon S3** console.
2. Select the S3 bucket created to receive logs.
3. Click **Properties** and select **Events**.
4. In the Events dialog, add a notification:

a. Enter the notification Name

b. Click **Events** > **All objects create events**.

   This option is triggered when the events are sent to SQS, for example, all object create events on a specific prefix.

c. Enter a **prefix** (the folder name to receive device logs).

d. Select **Send to as SQS Queue**.

e. Select the **SQS queue** created above.

Installing the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Preparing to Install Connector

Before you install any SmartConnectors, make sure that the Micro Focus ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform* guide, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure from step 3.

Before installing the SmartConnector, ensure that you have the following:

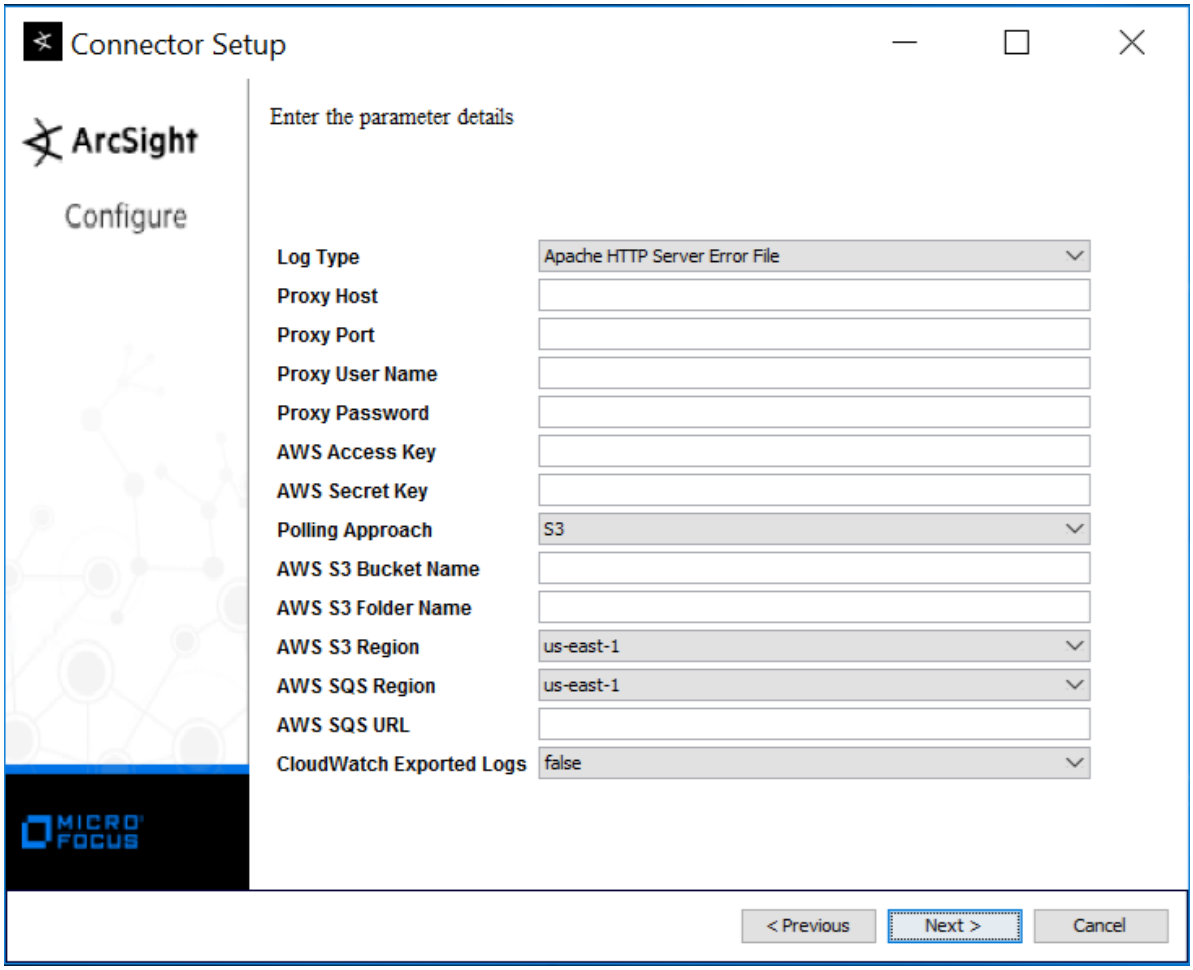
- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and Configuring the SmartConnector by Using the Wizard

The installation steps described in this section are specific to the Amazon S3 Connector. For detailed installation steps or for manual installation steps, see the Installation Guide for ArcSight SmartConnectors.

To install and configure the Amazon S3 Connector:

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant **Global Parameters**, when prompted.
4. From the **Type** drop-down list, select **Amazon S3** as the type of connector, then click **Next**.
5. Enter the following SmartConnector parameters, then click **Next**.



Parameter	Description
Log Type	Specify the Log Type. The default option is **Apache HTTP Server Error File**.
Proxy Host	If proxy is enabled for your machine, the IP address or host name of the proxy server for HTTPS connection. Specify this value only if proxy needs access to internet.
Proxy Port	If proxy is enabled for your machine, the port number of the proxy server for HTTPS connection. Specify this value only if proxy needs access to internet.

Parameter	Description
Proxy User Name	If proxy is enabled for your machine, the user name for the proxy server. This value is optional for additional proxy authentication. If you enter the proxy user name, you must provide the proxy password. Specify this value only if proxy needs access to internet.
Proxy Password	If proxy is enabled for your machine, the password for the proxy server user. Specify this value only if proxy needs access to internet.
AWS Access Key	Enter the AWS access key. This is optional and will be used if provided. If not, the Default Credential Provider Chain will be used. For more information, see AWS Credentials.
AWS Secret Key	Enter the AWS secret key. This is optional and will be used if provided. If not, the Default Credential Provider Chain will be used. For more information, see AWS Credentials.
Polling Approach	**For S3:** provide the S3 bucket name, S3 folder name and S3 region details. **For SQS:** provide SQS URL, SQS region and S3 region.
AWS S3 Bucket Name	Enter the name of the AWS S3 bucket that will be sending logs out.
AWS S3 Folder Name	Enter the folder name in which the logs appear. For example: AWS S3 > bucket-name > folder-name.
AWS S3 Region	Select the S3 region code.
AWS SQS Region	Select the SQS region code.
AWS SQS URL	The SQS URL from where the AWS S3 notifications are received.
CloudWatch Exported Logs	Select **true** if the logs are exported from CloudWatch to Amazon S3.

6. Select a destination and configure parameters.
7. Specify a name for the connector.
8. Select whether you want to run the connector as a service or in the standalone mode.
9. Complete the installation.
10. Run the SmartConnector.

For instructions about upgrading the connector or modifying parameters, see the Installation Guide for ArcSight SmartConnectors.

Performance Tuning

By default, the connector application maximum heap size is set to 1024 MB. If users with higher system configurations, expect higher EPS, update the changes below to improve the performance.

1. Stop the connector.
2. Increase heap size to perform more in memory operations.
   a. To increase the memory size for stand-alone connectors from the command line, change the following line in

      `$ARCSIGHT_HOME\current\bin\scripts\connectors.bat` (Windows)

      `$ARCSIGHT_HOME/current/bin/scripts/connectors.sh (Linux)`

      `ARCSIGHT_MEMORY_OPTIONS=" -Xms1024m -Xmx1024m "`

      to

      `ARCSIGHT_MEMORY_OPTIONS=" -Xms4096m -Xmx4096m "`

   b. To increase the memory size for connectors being run as a service, change the following lines in `user/agent/agent.wrapper.conf` from:

      `wrapper.java.initmemory=1024 wrapper.java.maxmemory=1024`

      to

      `wrapper.java.initmemory=4096 wrapper.java.maxmemory=4096`

   c. To increase the memory size for connectors managed by the Connector Appliance/ArcSight Management Center, increase the heap size by using a container level command.
3. Increase the awsthreadcount in the `<Install path>\current\user\agent\agent.properties` file.

   `Existing: awsthreadcount=1`

   `New: awsthreadcount=5`
4. Start the connector.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the ArcSight Console User's Guide for more information about the ArcSight data fields.

For information about Supported Log Sources for Amazon S3, see "Product Overview" on page 5.

Additional DNS Logs Version 3 Mappings to ArcSight Fields

ArcSight Field	Vendor Field
File Type	Identity Types
Old File Type	Policy Identity Type

Additional DNS Logs Version 4 Mappings to ArcSight Fields

ArcSight Field	Vendor Field
Device Custom String 4	Blocked Categories
Device Custom String 4 Label	Blocked Categories
File Type	Identity Types
Old File Type	Policy Identity Type

Additional Proxy Logs Version 4 Mappings to ArcSight Fields

ArcSight Field	Vendor Field
Device Custom String 4	BlockedCategories
Device Custom String 4 Label	Blocked Categories

Cisco Umbrella DNS Logs Mappings to ArcSight Fields

ArcSight Field	Vendor Field
Device Action	Action
Device Custom String 1	QueryType
Device Custom String 2	Policy Identity
Device Custom String 3	Identities
Device Custom String 5	Categories

ArcSight Field	Vendor Field
Device Custom String 6	ResponseCode
Destination Dns Domain	Domain
Device Event Class Id	ResponseCode: Action
Device Product	Umbrella
Device Severity	ResponseCode
Device Vendor	Cisco
Name	ResponseCode: Action
Source Address	InternalIp
Source Translated Address	ExternalIp
Start Time	DateTime

Cisco Umbrella Proxy Logs Mappings to ArcSight Fields

ArcSight Field	Vendor Field
Device Custom String 2	AVDetections
Device Custom String 2 Label	AV Detections
Device Custom String 3	Identities
Device Custom String 3 Label	Identities
Bytes In	ResponseSize
Bytes Out	RequestSize
Destination Address	DestinationIP
Device Action	Verdict
Device Custom Number 1	AMPScore
Device Custom Number 1 Label	AMP Score
Device Custom String 1	IdentityType
Device Custom String 1 Label	Identity Type
Device Custom String 5	Categories
Device Custom String 5 Label	Categories
Device Custom String 6	PUA
Device Custom String 6 Label	PUA
Device Event Category	Proxy Logs

ArcSight Field	Vendor Field
Device Event Class Id	Proxy: Verdict
Device Product	Umbrella
Device Vendor	Cisco
Event Outcome	StatusCode
File Hash	SHA-SHA256
File Name	AMP Malware Name: AMPMalwareName
File Size	ResponseBodySize
File Type	ContentType
Name	Proxy: Verdict
Old File Type	AMP Disposition: AMPDisposition
Request Client Application	UserAgent
Request Context	Referer
Request Url	URL
Source Address	InternalIp
Source Translated Address	ExternalIp
Start Time	DateTime

Cisco Umbrella IP Logs Mappings to ArcSight Fields

ArcSight Field	Vendor Field
Destination Address	DestinationIP
Destination Port	DestinationPort
Device Custom String 3	Identity
Device Custom String 5	Categories
Device Event Category	"IP Logs"
Device Event Class Id	"IP Logs"
Device Product	"Umbrella"
Device Receipt Time	DateTime
Device Vendor	"Cisco"
Name	"IP Logs"

ArcSight Field	Vendor Field
Source Address	SourceIP
Source Port	SourcePort
Start Time	DateTime

CloudFront Access Logs Mappings to ArcSight Fields

ArcSight Field	Vendor Field
Application Protocol	cs-protocol
Device Custom Number 2	sc-range-start
File Size	sc-content-len
Bytes In	sc-bytes
Bytes Out	safeToInteger(cs-bytes)
Destination Dns Domain	cs(Host)
Device Action	x-edge-result-type
Device Custom Floating Point 1	time-to-first-byte
Device Custom Floating Point 2	time-taken
Device Custom Number 1	fle-encrypted-fields
Device Custom Number 3	sc-range-end
Device Custom String 1	ssl-protocol
Device Custom String 3	x-edge-response-result-type
Device Custom String 4	cs-protocol-version
Device Custom String 5	fle-status
Device Dns Domain	x-host-header
Device Event Class Id	cs-method:sc-status
Device Facility	x-edge-location
Device Product	CloudFront
Device Vendor	Amazon
End Time Ng	date,time,time-taken
Event Outcome	sc-status
External Id	x-edge-request-id
File Hash	ssl-cipher

ArcSight Field	Vendor Field
File Path	cs-uri-stem
File Type	sc-content-type
Name	CloudFront Access
Reason	x-edge-detailed-result-type
Request Client Application	cs(User-Agent)
Request Context	cs(Referer)
Request Cookies	cs(Cookie)
Request Method	cs-method
Request Url Query	cs-uri-query
Source Address	__oneOfAddress(c-ip,X-Forwarded-For)
Source Port	c-port
Start Time Concatenate	date,time

CloudFront Real-time Logs Mappings to ArcSight Fields

ArcSight Field	Vendor Field
Application Protocol	cs-protocol
Bytes In	sc-bytes
Destination Dns Domain	cs-host
Device Action	x-edge-result-type
Device Custom Floating Point 1	time-to-first-byte
Device Custom Floating Point 2	time-taken
Device Custom Floating Point 3	cs-headers-count
Device Custom Number 1	fle-encrypted-fields
Device Custom Number 2	sc-range-start
Device Custom Number 3	sc-range-end
Device Custom String	3 x-edge-response-result-type
Device Custom String 1	ssl-protocol
Device Custom String 4	cs-protocol-version
Device Custom String 5	fle-status
Device Custom String 6	cs-headers

ArcSight Field	Vendor Field
Device Dns Domain	x-host-header
Device Facility	x-edge-location
Device Product	CloudFront
Device Receipt Time	timestamp
Device Vendor	Amazon
Event Outcome	sc-status
External Id	x-edge-request-id
File Hash	ssl-cipher
File Id	c-ip-version
File Path	cs-uri-stem
File Size	sc-content-len
File Type	sc-content-type
Name	CloudFront Real Time
Old File Hash	cs-accept-encoding
Old File Path	cache-behavior-path-pattern
Reason	x-edge-detailed-result-type
Request Client Application	cs-user-agent
Request Context	cs-referer
Request Cookies	cs-cookie
Request Method	cs-method
Request Url Query	cs-uri-query
Source Address	x-forwarded-for
Source Address	c-ip
Source Port	c-port

Adding Parser Files

The connector can support other log sources available in an Amazon S3 bucket. One connector instance can support one log source. Therefore, the default log source configurations will be overridden with the following changes.

With limited support, relying on Cisco Umbrella, and plenty of event source formats, you can build and integrate parsers.

To add new parser files:

1. Create a file in the following location:
   `<installFolder>\current\user\agent\fcp\awss3`
2. Specify the file name as `awss3_parser_configuration.properties`.
3. Add the following properties to the file:

```
#Start
parser.type.count=1
parser.type[0].devicetype=CiscoUmbrella-DNSLogs
parser.type[0].parserfolder=awss3
parser.type[0].parserfile=ciscoumbrella.dnslogs
parser.type[0].parserclasstype=0
parser.type[0].description=Cisco Umbrella DNS Logs
parser.type[0].filetype=csv
#End
```

Properties and description:

Property Name	Description
`parser.type.count`	This is a mandatory field. Set this value to **1**.
`parser.type[0].devicetype`	This is a mandatory field. This property describes a log format. It appears as a new selection in the Connector Installation wizard drop-down list. For example, Cisco DNS Logs.

<table>
<tr><th>Property Name</th><th>Description</th></tr>
<tr><td>parser.type[0].parserfolder</td><td>This is a mandatory field.
Specify the path in which the new parser files are available.
Set this value to the relative path from the fcp folder: <installFolder>\current\user\agent\fcp\.
For example: If you are copying the new parser file into: <installFolder>\current\user\agent\fcp\awss3, set the value as
parser.type[1].parserfolder=awss3</td></tr>
<tr><td>parser.type[0].parserfile</td><td>This is a mandatory field.
Set the parser file name without the file name extension. For example: ciscoumbrella.dnslogs. If there are sub-parser files, refer only to a parent parser file name.
Note: If the log format is CEF, then leave this field blank.</td></tr>
<tr><td>parser.type[0].parserclasstype</td><td>This is a mandatory field.
Select one of the following appropriate values for the desired input log format:<table><tr><th>Values</th><th>Log Formats</th></tr><tr><td>0</td><td>CSV or any common separator</td></tr><tr><td>1</td><td>Needs regular expression to process</td></tr><tr><td>2</td><td>Has syntax as key and value</td></tr><tr><td>3</td><td>XML</td></tr><tr><td>4</td><td>XQuery</td></tr><tr><td>6</td><td>CEF</td></tr><tr><td>7</td><td>JSON</td></tr></table></td></tr>
<tr><td>parser.type[0].description</td><td>This is an optional field.
This property also describes a log format. However, it is not visible in the Connector Installation wizard or other user interfaces.</td></tr>
<tr><td>parser.type[0].filetype</td><td>This is an optional field.
Set the file extension without using a period (.) preceding the file name extension. For example: txt, csv, or json.
This file is for future use.</td></tr>
</table>

Troubleshooting

1. Certificate Issue while Integrating Connector with Third-party Application.

   Because of SNI, the following certificate exception might be displayed while configuring the connector with third-party application:

   ```
   Error[1]: RemoteException: cause[javax.net.ssl.SSLHandshakeException: PKIX path building failed:
   sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
   ```

   To fix this issue, see Certificate Issue while Integrating Connector with Third-party Application.

2. Agent is configured but not generating event.
   a. Check for errors in `<Install path>\current\logs\agent.log`.
   b. If any errors related to AWS permissions are found, refer to "Configuring Log Retrieval" on page 12

3. When using the SQS approach, the configuration may be completed without any errors displayed on the configuration window, even if the IAM user does not have the required permissions. Post-configuration, the IAM user will not be able to process any events.

   In this case, the installer does not control and/or validate the S3 bucket details. Check for errors in `<Install path>\current\logs\agent.log`.

   If any errors related to AWS permissions are found, see "Configuring Log Retrieval" on page 12

4. When noticing frequent AWS API calls, checking for new S3 files or SQS Messages:
   a. If a specific interval was defined to receive new files, set the time interval in connector configuration.

      `<Install path>\current\user\agent\agent.properties`

   b. Replace `pollingfrequencyinsec=10` for `pollingfrequencyinsec=<Defined new file arrival interval in seconds>`

5. When using the S3 approach, how to re-process the log files?
   a. Stop running agent.
   b. Clear the `<Install path>\current\user\agent\ageantdata` folder to discard the intermediate state.
   c. Restart agent.

6. When a file is deleted or the connector is restarted, SQS notifications can get into flight mode.

a. S3 must be configured to send events to SQS on new object creation.
   The connector will delete SQS only if the message is successfully processed.

7. Agent setup displays the following message: "Enter valid AWS Credentials and parameters to retrieve AWS logs."
   a. Ensure you are using valid AWS credentials with valid permissions. For more information, see "Configuring Log Retrieval" on page 12.
   b. If using the SQS approach, make sure these values are correct:
      - AWS SQS URL
      - AWS SQS Region
      - AWS S3 region
   c. If using the S3 approach, make sure these values are correct:
      - AWS S3 bucket name
      - AWS S3 folder name
      - AWS S3 region

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 Configuration Guide (SmartConnectors 8.4)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!