
Micro Focus Security ArcSight SmartConnectors

SmartConnector for Amazon Web Services Security Hub

Configuration Guide

Document Release Date: July 31, 2020

Software Release Date: July 31, 2020



Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

© Copyright 2020 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

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.

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
07/24/2020	First edition of this guide. Added support for GuardDuty event collection through AWS EventBridge.

Contents

SmartConnector for Amazon Web Services Security Hub	5
Product Overview	5
Understanding Data Collection	5
Installation	7
Prerequisites	7
SecurityGroup for Lambda Configuration	11
Configuring an EC2 Instance	11
Opening Ports	12
ASFF Keys to ArcSight Fields	18
Header	18
GuardDuty Default	18
GuardDuty AWS_API_CALL	19
GuardDuty DNS_REQUEST	20
GuardDuty NETWORK_CONNECTION	20
GuardDuty PORT_PROBE	21
Resource Header	22
ResourcesDetailsAwsEc2Instance	22
ResourcesDetailsAwsIamAccessKey	22
ResourcesDetailsAwsEc2NetworkInterface	23
ResourcesDetailsAwsEc2SecurityGroup	23
ResourcesDetailsAwsIamRole	23
ResourcesDetailsAwsKmsKey	24
ResourcesDetailsAwsS3Bucket	24
ResourcesDetailsAwsS3Object	24
ResourcesDetailsAwsSnsTopic	25
ResourcesDetailsAwsSqsQueue	25
ResourcesDetailsAwsLambdaFunction	25
Parser Updates/Override	26
Troubleshooting	26
Send Documentation Feedback	28

SmartConnector for Amazon Web Services Security Hub

This guide provides information for installing the SmartConnector for Amazon Web Services Security Hub and configuring the device for GuardDuty event collection through AWS EventBridge.

Product Overview

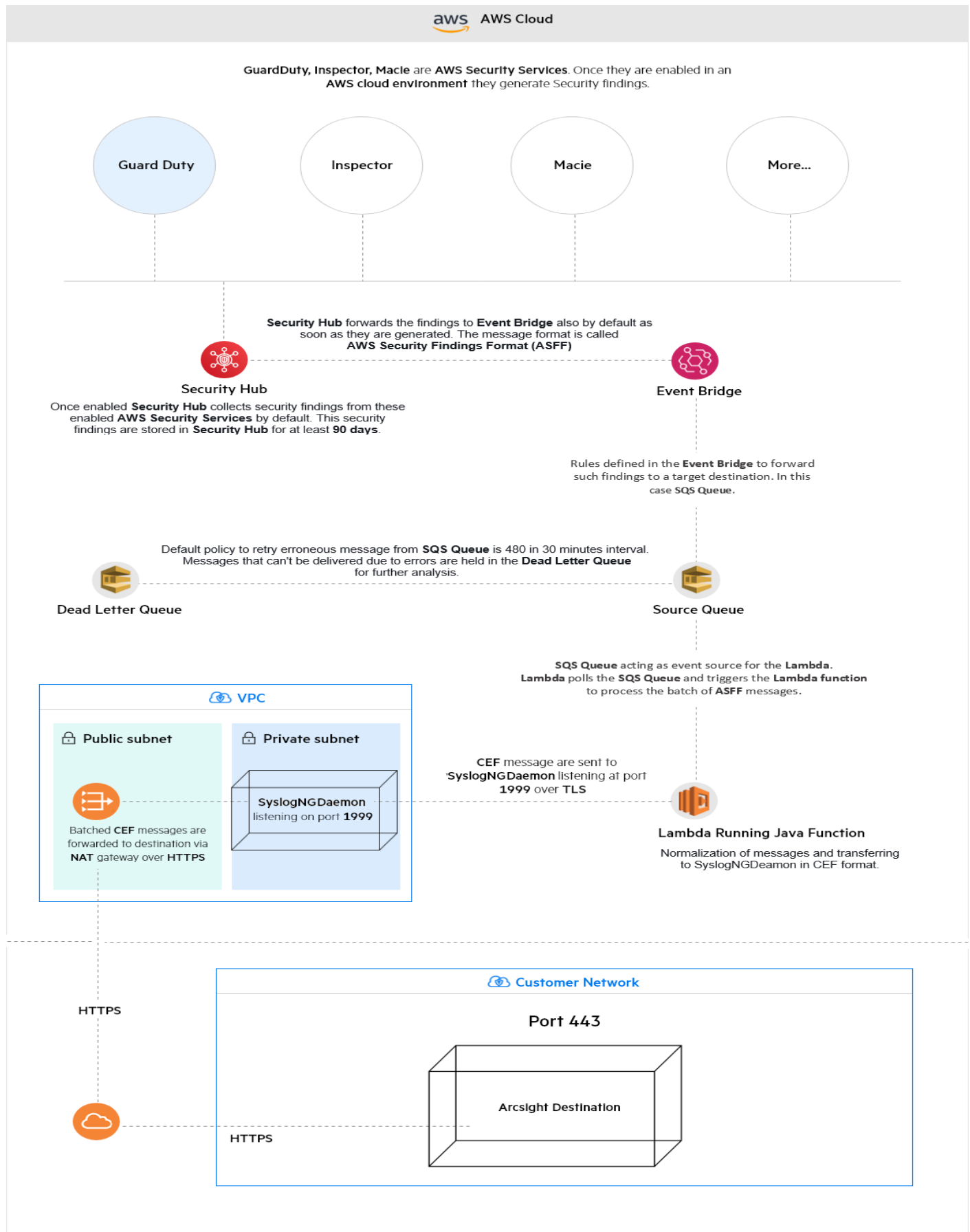
AWS cloud currently supports multiple security services such as Amazon GuardDuty, Amazon Inspector, Amazon Macie etc. These services, when enabled in an AWS cloud environment, generate security findings.

AWS Security Hub is AWS's own security finding aggregator. When enabled in an AWS cloud environment, it aggregates, organizes, and prioritizes these security findings, from multiple AWS security services, and forwards them to AWS EventBridge in ASFF format.

The ArcSightAWS Security Hub connector facilitates security findings collection by integrating it with AWS EventBridge. The AWS Security Hub connector converts the security findings, originally in ASFF format to CEF format, and forwards them to an ArcSight destination. Consequently, enabling other ArcSight destinations, such as ESM or Logger so that they can process these security findings.

Understanding Data Collection

The following diagram provides a high-level overview of how the AWS Security Hub connector collects and sends GuardDuty events through EventBridge to an ArcSight destination.



Permissions to run the CloudFormation Template

The following permissions should be granted:

- AmazonS3FullAccess
- CloudwatchEventsFullAccess
- AmazonSQSFullAccess
- LambdaFullAccess
- CloudwatchFullAccess
- EC2FullAccess

Installation

Prerequisites

1. Enable Guard Duty in your AWS environment.
2. Enable Security Hub in your AWS environment.
3. Make sure you have the AWS permissions to run the Cloud Formation Template.
4. Create an existing VPC with a private and public subnet created.
5. Create an EC2 instance in a private subnet.

SyslogNGDaemon is installed here.

6. Create a EC2 instance in a public subnet.

SSH connects to the EC2 in a private instance where SyslogNGDaemon is installed.

For more information, see ["Configuring an Amazon Virtual Private Cloud \(VPC\) and Subnets " on page 10](#)

7. Create two security groups. One of them is for Lambda and the other one for the EC2 instance. For more information, see ["SecurityGroup for Lambda Configuration" on page 11](#).
8. Create or select an S3 Bucket.
 - a. The external.properties file, maps folder, the ArcSight SmartConnector certificate, the arcsight-aws-securityhub-connector-1.1.0.jar and installer.json are stored here.

Note: The S3 bucket region must be the same in which the AWS Security Hub SmartConnector is supposed to run and collect process data from.

To create a S3 bucket, see [Creating and configuring an S3 bucket](#).

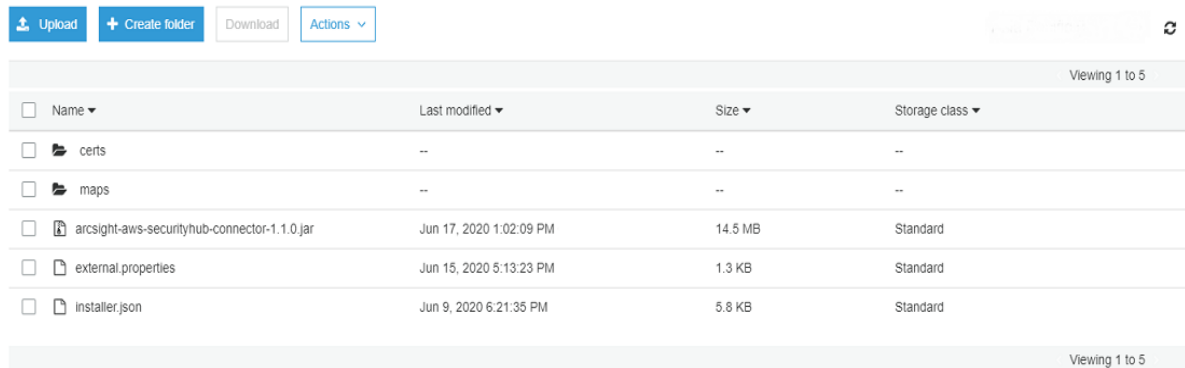
9. Upload the `arcsight-aws-securityhub-connector-1.1.0.jar` file to your S3 bucket.
This file is available in the AWS Security Hub Connector installer zip file.
10. Upload the `installer.json` file to your S3 bucket.
This file is available in the AWS Security Hub Connector installer zip file.
11. Upload the `maps` folder to your S3 bucket. You can create a `maps` folder and upload the content of the map files or copy the `maps` folder itself.
This file is available in the AWS Security Hub Connector installer zip file.
12. Create a `certs` folder and upload the Syslog NG Daemon Connector certificate to your S3 bucket.
The certificate is located in the installation folder of the Syslog NG Daemon SmartConnector.
`$INSTALLATIONFOLDER/current/user/agent/remote_management.p12`.
13. Upload the `external.properties` file to your S3 bucket.
This file is used by a Java function running in Lambda and it calls the SyslogNGDaemon SmartConnector.

To update this file:

```
##
## external properties file to upload to s3
##
##
##Valid properties
##
##Arcsight connector hostname or ip address, required parameter
#host.name=0.0.0.0
##
##Arcsight connector port number, required parameter
#port.number=9999
##
##Arcsight connector certificate bucket location in s3, required parameter
#certificate.bucket=bucket_name
##
##Arcsight connector certificate key location in s3, required parameter
#certificate.key=path/to/file
```

```
##
##Arsight connector certificate password, required parameter
#certificate.password=password
##
##Log Level changes the log level to the specified level
##value can be any of: info debug error all warn fatal trace off
##case insensitive value
##required parameter
#log.level=info debug error all warn fatal trace off
host.name: [IP of the private EC2 instance running SyslogNGDaemon]
port.number:1999
certificate.override.bucket.name: [S3bucket name]
certificate.override.key.file: certs/remote_management.p12
certificate.override.keystore.password:
crY2cvNdo8wpFdYdDrslv8cdMAV9f33A56hC+zXsqK4=
map.override.bucket.name: [S3bucket name]
map.override.bucket.directory: maps
log.level: info
```

Once zip file content is uploaded to the S3 bucket, your S3 bucket structure should look like below:



The screenshot shows the AWS S3 console interface for a bucket. At the top, there are buttons for 'Upload', 'Create folder', 'Download', and 'Actions'. Below these is a table listing the contents of the bucket. The table has columns for 'Name', 'Last modified', 'Size', and 'Storage class'. The contents include two folders, 'certs' and 'maps', and three files: 'arcsight-aws-securityhub-connector-1.1.0.jar', 'external.properties', and 'installer.json'.

Name	Last modified	Size	Storage class
certs	--	--	--
maps	--	--	--
arcsight-aws-securityhub-connector-1.1.0.jar	Jun 17, 2020 1:02:09 PM	14.5 MB	Standard
external.properties	Jun 15, 2020 5:13:23 PM	1.3 KB	Standard
installer.json	Jun 9, 2020 6:21:35 PM	5.8 KB	Standard

14. Additionally, if the private EC2 instance is a Windows machine, open the relevant ports. For more information, see ["Opening Ports " on page 12](#)

This step is not required for Linux EC2 machines.

Configuring an Amazon Virtual Private Cloud (VPC) and Subnets

To configure the existing VPC, you must create a private subnet and associate it with the lambda function.

A private subnet is a subnet with a route table pointing to a NAT gateway.

Elements required:

- A VPC
- A public subnet, a public subnet is a subnet associated with an internet gateway.

To create a public subnet:

1. Create an internet gateway if you don't have one.
2. From the VPC console, go to the navigation pane and choose Subnets.
3. To create a new subnet, choose Create Subnet. Otherwise, choose an existing subnet.
4. Choose the Route Table tab, and then choose Edit.
5. From the Change to: drop-down menu, choose an appropriate route table.

For a public subnet, the default route should point to an internet gateway.

To create a NAT gateway:

1. From the VPC console, go to the navigation panel, choose NAT Gateways, and then choose Create NAT Gateway.
2. In the Subnet field, choose the public subnet already created
3. In the Elastic IP Allocation ID field, choose an existing Elastic IP address, or select Create New EIP, and then choose Create a NAT Gateway.

It can be used as soon as the status changes to **available**.

To create a route table

1. In the VPC console, choose Route Tables, and then choose Create Route Table.
2. In the Name tag field, enter a name that is meaningful to you, select the VPC drop-down menu and choose your VPC, and then choose Yes, Create
3. Select the new route table, and then choose the Routes tab.
4. Choose Edit, and then choose Add another route.

Destination: 0.0.0.0/0

Target: private subnet with the NAT gateway created in the previous step

SecurityGroup for Lambda Configuration

Create a SecurityGroup for Lambda with the following inbound/ outbound rules.

Inbound rules					Edit inbound rules
Type	Protocol	Port range	Source	Description - optional	
No rules found					
This security group has no inbound rules.					

Create a SecurityGroup for the EC2 instance with the following inbound/ outbound rules.

Inbound rules					Edit inbound rules
Type	Protocol	Port range	Source	Description - optional	
SSH	TCP	22	0.0.0.0/0	SSH Management Traffic	
SSH	TCP	22	0.0.0.0/0 (SG_Conn_NGSyslog)	SSH Between EC2 instances	
Custom TCP	TCP	1999	0.0.0.0/0 (SG_Conn_LambdaNGSyslog)	From Lambda	
RDP	TCP	3389	0.0.0.0/0	RDP Traffic	

Note: SSH is enabled to facilitate the Syslog NG Daemon Smartconnector installation in a private EC2 instance on Linux. RDP is enabled to facilitate the Syslog NG Daemon installation in a private EC2 instance on Windows. The Lambda connects to Syslog NG Daemon's port (1999) over TLS as shown in "[Understanding Data Collection](#)" on page 5. Once the Syslog NG Daemon SmartConnector is installed in the EC2 instance, SSH & RDP rules should be removed for security purposes.

Configuring an EC2 Instance

To launch EC2 services from the AWS console:

1. Click Instances.
2. Click Launch Instance.
3. Click Community AML.

A list of operating systems is displayed.

4. If you deploy the EC2 instance on Linux.
5. From Red Hat, select Redhat 7.6 operating system.
6. Select Instance type **t2.micro**.
7. Click **Next: Configure Instance details** and select network **custom_vpc**.
8. Select the subnet.
9. Enable Auto-assign public IP.
10. From the network interface, click **Add IP**, for a secondary IP address.
11. Click **Next: Add Storage** and keep the original values.
12. Click **Next: Add Tags** and enter the key and value details (optional).
13. Click **Next: Add Security Group**.
14. Click **Create a New Security Group** or select an existing group.
15. Click **Review and Launch**.
16. Click **Launch**.
17. Select **Create a New Key Pair**.
18. Enter the keypair name **test.pem**.
19. Click **Download Key Pair**.

Opening Ports

You must ensure that the ports on the server on which you installed the Syslog NG Daemon SmartConnector is accessible from AWS. The procedure to open ports varies based on whether you have installed Syslog NG Daemon SmartConnector on a virtual machine or not.

Opening Ports on a Non-Virtual Machine

If you installed Syslog NG Daemon SmartConnector on a physical, non-virtual machine, ensure that the ports on which you installed it are accessible to AWS.

Opening Ports on a Virtual Machine

If you have installed the Syslog NG Daemon SmartConnector on a virtual machine in AWS, ensure that the ports on which you installed Syslog NG Daemon SmartConnector are open in both AWS and the virtual machine.

To open inbound ports on AWS:

1. Log in to AWS as a user with administrator privileges.
2. Go to **Services** and select **EC2**.

3. Select **Instances**.
4. Choose the EC2 instance to be edited.
5. Click **Launch-Wizard**.
6. Edit the **Inbound** and **Outbound** fields as required.

To open ports in the virtual server:

1. Log in to the virtual AWS machine.
2. Open the AWS Firewall.
3. Click **Inbound Rules < New Rule < Port < Next < TCP < Specific local ports**
4. Enter the same port or port range on which you installed the Syslog NG Daemon SmartConnector.
5. Click **Next < Allow the connection < Next < Profile < Next**.
6. Name the rule.
7. Click Finish.

Note: Linux EC2 instances are not required to follow these steps, only Windows instances.

Security Hub SmartConnector Installation

The overall Security Hub SmartConnector solution, uses AWS cloud resources such as Security Hub, EventBridge (CloudwatchEvent), SQS, and Lambda for sourcing and parsing ASFF messages to CEF messages and then forwarding them to Syslog NG Daemon.

Syslog NG Daemon batches and forwards these CEF messages to an Arcsight destination.

The Security Hub SmartConnector installation is divided in two processes:

Creating AWS Cloud resources using Cloud Formation Template (CFT)

Installing Syslog NG Daemon as a Forwarding Agent.

Installing Syslog NG Daemon as a Forwarding Agent

1. Launch the EC2 Instance in a public subnet and a private subnet.
2. Log in to the public EC2 instance using the key.
You can use either of the following software tools: putty or MobaXterm.
3. Upload the key of the private EC2 instance to the public EC2 instance.
4. From the public EC2 instance, run the command `chmod 600 testprivate.pem`.

5. Ssh to the private instance using the command `ssh ec2-user@private-ip-address -i testprivate.pem`.
6. Upload the Syslog NG Daemon installer to public EC2 instance.
MobaXterm can be used to perform this task.
7. Copy the Syslog NG Daemon installer to the private EC2 instance.
This step can be performed using the command

```
scp -i testprivate.pem ArcSight-7.15.0.8287.0-Connector-Linux64.bin ec2-user@private-ip-address:/home/ec2-user/.
```
8. Configure the Syslog NG Daemon SmartConnector in the private instance.
9. Select 1.0 as the CEF File version.
10. Configure the Protocol as default TLS.
11. Configure the Port 1999.
12. Select CSV File/CSV File as the destination, unless you are using any other ArcSight product like Logger or ESM.
13. Run the SmartConnector as a standalone process or as a service.
14. Once the deployment is complete, upload the certificate `remote_management.p12` file to the S3 bucket certs folder.

Creating AWS Cloud resources using Cloud Formation Template (CFT)

The AWS Security Hub SmartConnector installer is downloaded as a zip file. Inside the zip file, you can find a jar file containing the java function to be deployed in Lambda and a `installer.json` file which is a Cloud Formation Template. The CFT is used to generate the AWS cloud resources (as shown in ["Understanding Data Collection" on page 5](#)).

1. Log in as a user with in AWS Web console with the appropriate permission. For more information, see ["Permissions to run the CloudFormation Template" on page 7](#).
2. From **Find Services**, search **CloudFormation Service**.
3. From the CloudFormation service console, click **Create Stack**.
4. Click **With New Resources (Standard)**.
A screen is displayed.

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready
 ☐ Use a sample template
 ☐ Create template in Designer

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

☒ Amazon S3 URL
 ☐ Upload a template file

Amazon S3 URL

`https://`

Amazon S3 template URL

S3 URL: *Will be generated when URL is provided*

[View in Designer](#)

- From **Amazon S3 URL**, enter the Object URL of the `installer.json` file uploaded to your S3 bucket earlier.

You can get the S3 object url by clicking the `installer.json`.

installer.json Latest version ▾

Overview

Properties

Permissions

Select from

Open

Download

Download as

Make public

Copy path

Owner
5137c50813aa771205d3ed3a945c6a0a2

Last modified
Jun 17, 2020 4:03:09 PM

Etag
b05016bc0b51456e00

Storage class
Standard

Server-side encryption
None

Size
5.6 KB

Key
installer.json

Object URL
[https://\[redacted\].com/installer.json](https://[redacted].com/installer.json)

- Click **Next**.

The screen below is displayed.

The screenshot shows the AWS CloudFormation console interface. On the left, a sidebar lists the steps: Step 2 (Specify stack details), Step 3 (Configure stack options), and Step 4 (Review). The main area is titled 'Stack name' and contains a text input field with the placeholder 'Enter a stack name'. Below this, a note states: 'Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-)'. The 'Parameters' section follows, with a description: 'Parameters are defined in your template and allow you to input custom values when you create or update a stack.' It includes four parameter fields: 'AWSS3BucketName' (text input), 'Region' (text input), 'SecurityGroupID' (dropdown menu), and 'SubnetID' (dropdown menu). At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next' (highlighted in orange).

7. Enter the **Stack Name**.

Note: The stack name must be unique for each region.

8. Enter the S3 bucket name in which the installer.json is.
9. Enter the region code in which you want to install the connector.
It should be same as the S3 bucket region.
10. Select the Security Group created for Lambda.
11. Select the private subnet previously created.
12. Click Next and keep the default values.
13. Select **I acknowledge that AWS CloudFormation might create IAM resources**.
14. Create Stack.

Cloud Formation Service will start deploying all of the resources as per the CFT. Once the status changes to CREATE_COMPLETE, the resources will be successfully deployed.

Security Hub Connector Post-Deployment Configuration

Currently, the SQS queue is configured to re-send failed messages 480 times in a 30 minutes interval for 10 days, considering any network connectivity issue. This setting can be changed by updating the stack.

Note: This step is optional. You can keep the default settings.

To update the stack:

1. From the stack console, click update.
In the next screen, choose **Edit Template in Designer** and click View Designer.
2. Choose **Edit Template in Designer** and click View Designer.
3. Update the **maxReceiveCount** value.
4. Click **Create stack**, continue clicking **Next** and then click **Update Stack**.

Upgrading the Security Hub SmartConnector

1. Update the S3 bucket with the latest jar file, latest installer.json file and the latest map folder.
2. Go to the stack console
3. Click **Update** and choose **Replace Current Template**.
4. From Amazon S3 URL, enter the Object URL of the installer.json file uploaded to your S3 bucket.
5. Continue clicking **Next**.
6. Select **I acknowledge that AWS CloudFormation might create IAM resources**.
7. Create **Update Stack**.

Cloud Formation Service will start deploying all of the resources as per the CFT. Once the status changes to **CREATE_COMPLETE**, the resources will be successfully deployed.

Undeploying the AWS Security Hub SmartConnector

1. Go to CloudFormation console.
2. From the **Filter by Stack name** search box, enter the the stackname.
3. From the stack console, click delete.

A pop-up is displayed, click **Delete Stack**.

4. Delete stack.

All the AWS cloud resources will be deleted. The VPC components and the EC2 instances must be manually deleted as they were manually created.

ASFF Keys to ArcSight Fields

Header

ASFF Key	ArcSight Fields
Version	deviceCustomFloatingPoint1
Id	devicePayloadId
Detail-type	requestMethod
Account	deviceExternalID
Time	deviceReceiptTime
Region	deviceDnsDomain
Resources	requestCookies

GuardDuty Default

ASFF Key	ArcSight Fields
Product Arn	deviceFacility
Types	deviceCustomString2
Description	requestContext
SchemaVersion	deviceCustomDate2
Generator Id	deviceProcessName

ASFF Key	ArcSight Fields
First Observed At	startTime
Created At	fileCreateTime
Record State	oldFileHash
Title	message
Workflow / Status	oldFileId
Last Observed At	endTime
Severity / Normalized	DeviceCustomNumber2
Severity / Label	deviceSeverity
Updated At	fileModificationTime
Aws Account Id	destinationZoneExternalID
Id	oldFilePermission

GuardDuty AWS_API_CALL

ASFF Key	ArcSight Fields
action/actionType, resourceRole	name,deviceEventClassId
action/awsApiCallAction/serviceName	sourceServiceName
action/awsApiCallAction/callerType	requestClientApplication
action/awsApiCallAction/remotepDetails/ipAddressV4	sourceAddress
action/awsApiCallAction/remotepDetails/organization/	deviceCustomString1
action/awsApiCallAction/remotepDetails/country/countryName	deviceCustomString6
action/awsApiCallAction/remotepDetails/city/cityName	
Resource Role	
Additional Info	requestUrl
Archived	filePermission
Count	baseEventCount
aws/securityhub/FindingId	fileId
aws/securityhub/ProductName	productName
aws/securityhub/CompanyName	productVendor

GuardDuty DNS_REQUEST

ASFF Key	ArcSight Fields
action/actionType : resourceRole	name,deviceEventClassId
action/dnsRequestAction/domain	destinationDnsDomain
action/dnsRequestAction/protocol	transportProtocol
action/dnsRequestAction/blocked	deviceAction
Resource Role	deviceCustomString6
Additional Info	requestUrl
evidence/threatIntelligenceDetails:0/threatNames:0	deviceCustomString4
evidence/threatIntelligenceDetails:0/threatListName	
Archived	filePermission
Count	baseEventCount
aws/securityhub/FindingId	fileId

GuardDuty NETWORK_CONNECTION

ASFF Key	ArcSight Fields
action/actionType : resourceRole	name,deviceEventClassId
action/networkConnectionAction/connectionDirection	deviceDirection
action/networkConnectionAction/remotelPDetails/ipAddressV4	sourceAddress
action/networkConnectionAction/remotelPDetails/organization/asn	deviceCustomString1
action/networkConnectionAction/remotelPDetails/organization/asnOrg	
action/networkConnectionAction/remotelPDetails/organization/isp	
action/networkConnectionAction/remotelPDetails/organization/org	
action/networkConnectionAction/remotelPDetails/country/countryName	
action/networkConnectionAction/remotelPDetails/geoLocation/lat	sourceGeoLatitude
action/networkConnectionAction/remotelPDetails/geoLocation/lon	sourceGeoLongitude
action/networkConnectionAction/remotePortDetails/port	sourcePort
action/networkConnectionAction/remotePortDetails/portName	source ServiceName
action/networkConnectionAction/localPortDetails/port	destinationPort
action/networkConnectionAction/localPortDetails/portName	destinationServiceName

ASFF Key	ArcSight Fields
action/networkConnectionAction/protocol	transportProtocol
action/networkConnectionAction/blocked	deviceAction
action/networkConnectionAction/localIpDetails/ipAddressV4	destinationAddress
Resource Role	deviceCustomString6
Archived	filePermission
Count	baseEventCount
aws/securityhub/FindingId	fileId

GuardDuty PORT_PROBE

ASFF Key	ArcSight Fields
action/actionType : resourceRole	name,deviceEventClassId
action/portProbeAction/portProbeDetails:0/localPortDetails/port	sourcePort
action/portProbeAction/portProbeDetails:0/localPortDetails/portName	sourceServiceName
action/portProbeAction/portProbeDetails:0/remotelpDetails/ipAddressV4	sourceAddress
action/portProbeAction/portProbeDetails:0/remotelpDetails/organization/asn	deviceCustomString1
action/portProbeAction/portProbeDetails:0/remotelpDetails/organization/asnOrg	
action/portProbeAction/portProbeDetails:0/remotelpDetails/organization/isp	
action/portProbeAction/portProbeDetails:0/remotelpDetails/organization/org	
action/portProbeAction/portProbeDetails:0/remotelpDetails/country/countryName	
action/portProbeAction/portProbeDetails:0/remotelpDetails/city/cityName	
action/portProbeAction/portProbeDetails:0/remotelpDetails/geoLocation/lat	sourceGeoLatitude
action/portProbeAction/portProbeDetails:0/remotelpDetails/geoLocation/lon	sourceGeoLongitude
action/portProbeAction/blocked	deviceAction
Resource Role	deviceCustomString6
Additional Info	requestUrl
evidence/threatIntelligenceDetails:0/threatNames:0	deviceCustomString4
evidence/threatIntelligenceDetails:0/threatListName	
evidence/threatIntelligenceDetails:1/threatNames:0	

ASFF Key	ArcSight Fields
evidence/threatIntelligenceDetails:1/threatListName	
Count	baseEventCount
aws/securityhub/FindingId	fileId

Resource Header

ASFF Key	ArcSight Fields
Id	filePath
Partition	deviceDomain
Tags	deviceCustomString3
Type	fileType

ResourcesDetailsAwsEc2Instance

ASFF Key	ArcSight Fields
I am Instance Profile Arn	oldFilePath
KeyName	event.oldFileName
Type	fileName
VpcId SubnetId ImageId	oldFileType
IpV6Addresses	deviceCustomString5
IpV4Addresses	deviceCustomString5
Launched At	deviceCustomDate1

ResourcesDetailsAwsIamAccessKey

ASFF Key	ArcSight Fields
User Name	sourceUserName
Created At	deviceCustomDate1
Principal Id	fileHash
Principal Name	oldFileName
Principal Type	oldFileType
Status	deviceCustomString5

ResourcesDetailsAwsEc2NetworkInterface

ASFF Key	ArcSight Fields
Attachment/AttachmentId Attachment/InstanceId	deviceCustomString5
Attachment/AttachTime	deviceCustomDate1
Attachment/DeleteOnTermination SourceDestCheck	oldFileType
Attachment/DeviceIndex	deviceCustomNumber1
Attachment/InstanceOwnerId	sourceUserId
Attachment/Status	fileName
Security Groups	fileHash
Network Interface Id	oldFilePath
SourceDestCheck	oldFileType

ResourcesDetailsAwsEc2SecurityGroup

ASFF Key	ArcSight Fields
Group Id	oldFilePath
Group Name	fileName
Ip Permissions	oldFileName
Ip Permissions Egress	deviceCustomString5
Owner Id	sourceUserId
Vpc Id	oldFileType

ResourcesDetailsAwsIamRole

ASFF Key	ArcSight Fields
Assume Role Policy Document	oldFileName
Create Date	deviceCustomDate1
Max Session Duration	deviceCustomNumber1
Path	oldfilepath
Role Id	destinationUserId
Role Name	destinationUserName

ResourcesDetailsAwsKmsKey

ASFF Key	ArcSight Fields
AWS Account Id	fileHash
Creation Date	deviceCustomDate1
Key Id	oldFileType
Key Manager	fileName
Key State	oldFilePath
Origin	deviceCustomString5

ResourcesDetailsAwsS3Bucket

ASFF Key	ArcSight Fields
Created At	deviceCustomDate1
Owner Id	sourceUserID
Owner Name	sourceUserName
Server Side Encryption Configuration	deviceCustomString5

ResourcesDetailsAwsS3Object

ASFF Key	ArcSight Fields
Content Type	oldFileType
E Tag	deviceCustomString5
Last Modified	deviceCustomDate1
Server Side Encryption	fileName
SSEKMS Key Id	oldFileName
Version Id	oldFilepath

ResourcesDetailsAwsSnsTopic

ASFF Key	ArcSight Fields
KmsMasterKeyId	fileHash
Owner	destinationUserName
Subscription	deviceCustomString5
Topic Name	fileName

ResourcesDetailsAwsSqsQueue

ASFF Key	ArcSight Fields
Dead Letter Target Arn	oldFilePath
Kms Data Key Reuse Period Seconds	deviceCustomNumber1
Kms MasterKey Id	fileHash
Queue Name	fileName

ResourcesDetailsAwsLambdaFunction

ASFF Key	ArcSight Fields
Code	deviceCustomString5
Code Sha 256	fileHash
Dead Letter Config /Target Arn	oldFileType
Environment / Variables	oldFileName
Environment / Error / Error Code	reason
Function Name	fileName
Handler, KmsKeyArn, Layers, RevisionId, Runtime, Timeout, TracingConfigMode, Version, VpcConfig, MasterArn	oldFilePath
Last Modified	deviceCustomDate1
Memory Size	fileSize
Role	destinationUserName

Parser Updates/Override

The ArcSight SmartConnector for AWS Security Hub connector is designed to support parser files updates in the run time without any code changes.

In this way the connector can support extended events of the service supported or add support to new service events. Parser updates are applied on top of the connectors basic installation.

Below are the steps for a successful parser update:

1. Navigate to the AWS S3 bucket as mentioned in the prerequisites.
2. Navigate to the “Maps” folder.
3. Upload the new map file to the Maps folder (new files will get added and existing files will be overwritten with these updates).

Troubleshooting

Amazon Web Services Security Hub

Deleting Error Messages From DLQ (Dead Letter Queue)

Workaround

1. See the Amazon [SQS Standard queues](#) and the Amazon [SQS FIFO \(First-In-First-Out\) queues](#) examples.
2. Set a string that contains JSON-formatted parameters and values for the RedrivePolicy queue attribute:

```
final String redrivePolicy =
"
{\"maxReceiveCount\": \"5\", \"deadLetterTargetArn\": \"arn:aws:sqs:us-east-2:123456789012:MyDeadLetterQueue\"}
";
```

3. Use the CreateQueue or SetQueueAttributesRequest action to configure the RedrivePolicy queue attribute:

```
final SetQueueAttributesRequest queueAttributes = new
SetQueueAttributesRequest();
final Map<String,String> attributes = new HashMap<String,String>();
attributes.put("RedrivePolicy", redrivePolicy);
queueAttributes.setAttributes(attributes);
queueAttributes.setQueueUrl(myQueueUrl);
```

```
sqs.setQueueAttributes(queueAttributes);
```

4. Compile and run your program.

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 8.0.0)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!