Micro Focus Security ArcSight Connectors

SmartConnector for Zeek IDS NG File

Configuration Guide

September 17, 2020

Configuration Guide

SmartConnector for Zeek IDS NG File

September 17, 2020

Legal Notices

Micro Focus

The Lawn

22-30 Old Bath Road

Newbury, Berkshire RG14 1QN

UK

https://www.microfocus.com.

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:

https://community.microfocus.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Revision History

Date	Description
09/17/2020	This document has been renamed from SmartConnector for Bro IDS NG File Configuration Guide to SmartConnector for Zeek IDS NG File Configuration Guide.
08/20/2020	Added support to the following Zeek 3.1.3 modules: -Conn, Dns, files,Http, ssl, weird, and x509. Added mappings for Support for Ja3 and Hash MD5 Hashes.
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/15/2015	Updated parameters screenshot and table to describe Bro IDS Host Name parameter. Removed host name configuration from the Configuration section.
03/31/2015	Corrected errors in parameters table. Added support for v2.3. Added the following mappings tables: dhcp, files, known_certs, known_hosts, known_services, loaded scripts, and x509.
02/14/2014	Updated parameter screen image.
09/30/2013	Updated mappings.
06/28/2013	Updated HTTP mappings table.
03/29/2013	First edition of this Configuration Guide.

SmartConnector for Zeek IDS NG File

This guide provides information for installing the SmartConnector for Zeek IDS NG File and configuring the device for event collection. Bro IDS Versions 2.1, 2.3 and Zeek 3.1.3 are supported.

Product Overview

Zeek is a Unix-based Network Intrusion Detection System (IDS). Zeek monitors network traffic and detects intrusion attempts based upon the traffic characteristics and content.

Zeek detects intrusions by comparing network traffic against rules describing events that are deemed troublesome. These rules might describe activities (for example, certain hosts connecting to certain services), what activities are worth alerting (for example, attempts to a given number of different hosts constitutes a "scan"), or signatures describing known attacks or access to known vulnerabilities.

If Zeek detects something of interest, it can be instructed either to issue a log entry or to initiate the execution of an operating system command.

Configuration

The Zeek configuration files are `networks.cfg`, `node.cfg` and `zeekctl.cfg`. To reconfigure Zeek, run `$ZEEKHOME/scripts/ZEEK_config`. This updates your Zeek configuration (`$ZEEKHOME/usr/local/zeek/etc/zeek.cfg`) file. You can also edit this file using your favorite editor.

The directory in which log files are located is:

```
$ZEEKHOME/opt/zeek/logs/current
```

The Zeek logs take the form:

```
type.hostname.start_date/time-end_date/time
```

where `type` is the log file type.

The following log types are supported by the Zeek IDS NG SmartConnector:

Log Type	Description
communication	A record of every communication Zeek performs.
conn	A record of every connection Zeek detects.
dhcp	DHCP-related alerts.
dns	DNS-related alerts.
dpd	DPD-related alerts.
files	file-related alerts.

Log Type	Description
ftp	All session activity involving the ftp control port.
http	All session activity involving the http ports.
known_certs	All session activity involving recognized certificates.
known_hosts	All session activity involving recognized hosts.
known_services	All session activity involving recognized services.
loaded_scripts	All session activity involving loaded scripts.
notice	Network occurrences that are determined to be of nominal importance.
packet_filter	All session activity involving packet filtering.
reporter	All session activity generating reports.
smtp	All session activity involving the smtp port.
software	All session activity involving software.
ssh	SSH-related alerts.
ssl	SSL-related alerts.
tunnel	All session activity involving tunnels.
weird	A record of instances of network traffic that simply should not happen.
x509	All session activity involving module X509.

Loading Policy Scripts

The following policy scripts included with Zeek for generating log files are on by default:

conn, ftp, http, smtp, weird, notice

> The Zeek distribution includes a number of standard Notices, controlled by a number of different policies. To get a list of all notices that your Zeek configuration might generated, enter `'sh . $ZEEKHOME/etc/zeek.cfg; zeek -z notice $ZEEK_HOSTNAME.zeek'`

The following policy scripts are not loaded by default. You should add these to your $ZEEKHOME/site/zeekhost.zeek policy file for the log files to be generated.

communication, dns, dpd, packet_filter, reporter, software, ssh, ssl, tunnel

Install the SmartConnector

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

> Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector.

Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

Prepare to Install Connector

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

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. 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 at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

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

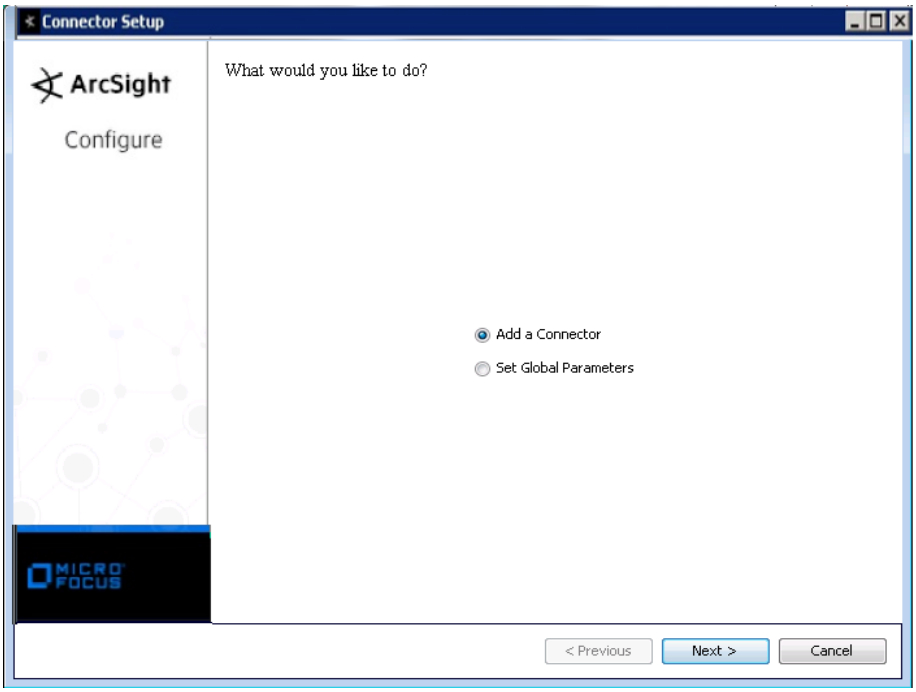
Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the Micro Focus SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

   Follow the wizard through the following folder selection tasks and installation of the core connector software:

   Introduction
   Choose Install Folder
   Choose Shortcut Folder
   Pre-Installation Summary
   Installing...
3. When the installation of SmartConnector core component software is finished, the following window is displayed:



Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

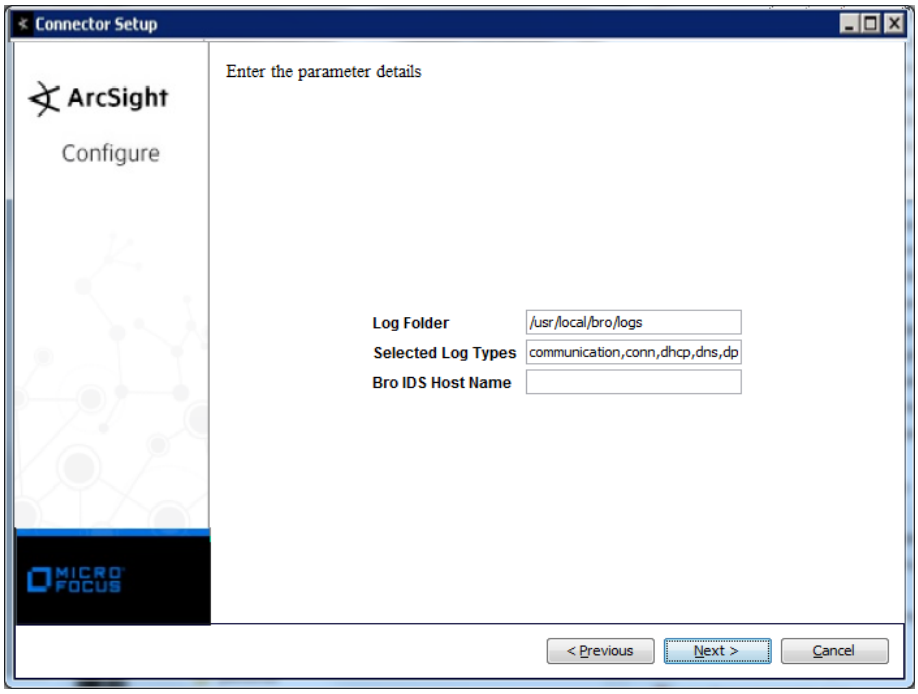
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the Micro Focus SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.

Parameter	Setting
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The Micro Focus SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
2. Select **Zeek IDS NG File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



When a new log file is inserted in the log folder, the connector alphabetically sorts all the logs in the log folder and then reads the last file. If the new log is the last file of the folder, the connector will process it, if not, it is not processed.

Parameter	Description
Log Folder	Enter the location of the directory in which log files are kept, or accept the default value of $ZEEKHOME/opt/zeek/logs/current.
Selected Log Types	Select any or all of the following SmartConnector-supported log types: communication, conn, dhcp, dns, dpd, files, ftp, http, known_certs, known_hosts, known_services, loaded_scripts, notice, packet_filter, reporter, smtp, ssh, ssl, tunnel, weird, x509. Note that the policies for DNS, SSH, and SSL are not automatically loaded by default; you must load them manually for their log files to be generated. See "Loading Policy Scripts."
Zeek IDS Host Name	Enter host name of the machine containing the Zeek IDS File logs. This value is mapped to the event.deviceHostName field.

Select a Destination

1. The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2. Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3. Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1. Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2. The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3. If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4. Click **Next** on the summary window.

5 To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

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.

Zeek IDS Communication Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = error; Medium = warning; Low = info
Device Custom String 2	src_name
Device Custom String 4	peer
Device Event Category	communication
Device Event Class Id	communication
Device Product	Zeek
Device Receipt Time	ts
Device Severity	level
Device Vendor	Zeek
Message	message
Name	communication

Zeek IDS Conn Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	medium = REJ; low = S0, S1, SF, S2, S3, RSTO, RSTR, RSTOS0, RSTRH, SH, SHR, OTH
Application Protocol	service
Bytes In	resp_bytes
Bytes Out	orig_bytes
Destination Address	id.resp_h
Destination Port	id.resp_p
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Missed bytes
Device Custom Number 2	Original IP bytes
Device Custom Number 3	Responder IP Bytes
Device Custom String 3	Connection ID
Device Custom String 4	Connection Duration
Device Event Category	conn
Device Event Class Id	conn_state
Device Product	Zeek
Device Receipt Time	ts
Device Severity	conn_state
Device Vendor	Zeek
Name	conn
Source Address	id.orig_h
Source Port	id.orig_p
Transport Protocol	proto

Zeek IDS DHCP Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Destination Address	id.resp_h
Destination Port	id.resp_p
Device Address	assigned_ip
Device Custom Number 1	Transaction ID
Device Custom String 3	Connection ID
Device Custom String 4	Lease Time
Device Event Category	dhcp
Device Event Class Id	DHCP Lease
Device Product	Zeek
Device Receipt Time	ts
Device Severity	Low
Device Vendor	Zeek
Name	DHCP Lease
Source Address	id.orig_h

ArcSight ESM Field	Device-Specific Field
Source MAC Address	mac
Source Port	id.orig_p

Zeek IDS DNS Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Destination Address	id.resp_h
Destination DNS Domain	query
Destination Port	id.resp_p
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Transaction ID
Device Custom String 1	Query Type Name
Device Custom String 2	rtt
Device Custom String 3	uid
Device Custom String 4	qclass_name
Device Event Category	dns
Device Event Class Id	qtype
Device Product	Zeek
Device Receipt Time	ts
Device Severity	Low
Device Vendor	Zeek
Event Outcome	rejected
Message	All of (answers, Domain Name System Events, answers)
Name	One of (qtype_name, DNS - No Query)
Source Address	id.orig_h
Source Port	id.orig_p
Transport Protocol	proto

Zeek IDS DPD Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Application Protocol	analyzer
Destination Address	id.resp_h
Destination Port	id.resp_p
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom String 3	Connection ID
Device Event Category	'dpd'
Device Event Class Id	All of ('dpd:', analyzer)
Device Product	Zeek
Device Receipt Time	ts

ArcSight ESM Field	Device-Specific Field
Device Severity	Low
Device Vendor	Zeek
Message	failure_reason
Name	All of ('dpd:', analyzer, 'Analyzer')
Source Address	id.orig_h
Source Port	id.orig_p
Transport Protocol	proto

Zeek IDS Files Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Bytes In	total_bytes
Bytes Out	overflow_bytes
Destination Host Name	rx_hosts
Device Custom String 2	Parent File ID
Device Custom String 3	Connection ID
Device Custom String 4	File Analysis Duration
Device Custom String 5	Analyzers
Device Event Category	files
Device Event Class Id	Files Analysis
Device Product	Zeek
Device Receipt Time	ts
Device Severity	extracted
Device Vendor	Zeek
File Hash	sha1
File ID	fuid
File Name	extracted
File Path	source
File Size	extracted_size
File Type	mime_type
Name	Files Analysis
Old File Size	extracted_cutoff
Source Host Name	tx_hosts

Zeek IDS FTP Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Destination Address	One of (id.resp_h, data_channel.resp_h)
Destination Port	id.resp_p
Device Action	command
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	Data Channel Response Port
Device Custom String 3	Connection ID
Device Event Category	ftp
Device Event Class Id	reply_code
Device Product	Zeek
Device Receipt Time	ts
Device Severity	Low
Device Vendor	Zeek
Event Outcome	data_channel.passive
File ID	fuid
File Size	file_size
File Type	mime_type
Message	reply_msg
Source Address	One of (id.orig_h, data_channel.orig_h)
Source Port	id.orig_p
Source User Name	user

Zeek IDS HTTP Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	high = 400 – 599; Medium = 300 – 399; Low = 0 – 299
Bytes In	request_body_len
Bytes Out	response_body_len
Destination Address	id.resp_h
Destination Port	id.resp_p
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom String 2	Origin File Unique Identifier
Device Custom String 3	Connection ID
Device Custom String 4	Referrer
Device Custom String 5	User Agent
Device Custom String 6	Response File Unique Identifier
Device Event Category	'http'
Device Event Class Id	Both("http:",method)
Device Product	Zeek
Device Receipt Time	ts
Device Severity	One of (status_code, 0)
Device Vendor	Zeek
File Name	filename
File Permission	resp_filenames
File Type	One of (orig_mime_types,resp_mime_types)
Message	status_msg
Name	Both('http:', status_msg)
Old File Name	orig_filenames

ArcSight ESM Field	Device-Specific Field
Old File Permission	version
Request Client Application	user-agent
Request Context	referrer
Request Method	method
Request Protocol	http
Request URL Authority	All of (username, password, host, id.resp_h, id.resp_p)
Request URL File Name	uri
Request URL Host	One of (host, id.resp_h)
Request URL Port	id.resp_p
Request URL Query	uri
Source Address	id.orig_h
Source Port	id.orig_p
Source User Name	username

Zeek IDS Known Certificates Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Device Custom String 3	Issuer Subject
Device Custom String 4	Certificate Serial Number
Device Event Category	known_certs
Device Event Class Id	Certificates Information
Device Product	Zeek
Device Receipt Time	ts
Device Severity	Low
Device Vendor	Zeek
Message	subject
Name	Certificates Information
Source Address	host
Source Port	port_num

Zeek IDS Known Hosts Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Device Event Category	known_hosts
Device Event Class Id	TCP Handshakes Host
Device Product	Zeek
Device Receipt Time	ts
Device Severity	Low
Device Vendor	Zeek
Name	TCP Handshakes Host
Source Address	host

Zeek IDS Known Services Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Application Protocol	service
Device Event Category	known_services
Device Event Class Id	Service Tracking
Device Product	Zeek
Device Receipt Time	ts
Device Severity	Low
Device Vendor	Zeek
Name	Service Tracking
Source Address	host
Source Port	port_number
Transport	port_proto

Zeek IDS Loaded Scripts Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Device Event Category	loaded_scripts
Device Event Class Id	Loaded Script
Device Product	Zeek
Device Severity	Low
Device Vendor	Zeek
File Name	name
Message	name
Name	Loaded Script

Zeek IDS Notice Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Destination Address	id.resp_h
Destination Port	id.resp_p
Device Custom Floating Point 1	Suppress Time
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Policy Items
Device Custom String 3	Connection ID
Device Custom String 4	Peer
Device Custom String 5	File Description
Device Event Category	'notice'
Device Event Class Id	actions
Device Product	Zeek
Device Receipt Time	ts

ArcSight ESM Field	Device-Specific Field
Device Severity	Low
Device Vendor	Zeek
File ID	fuid
File Type	file_mime_type
Message	msg
Name	note
Source Address	id.orig_h
Source Port	id.orig_p
Transport Protocol	proto

Zeek IDS Packet Filter Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Device Custom String 4	Node
Device Event Category	'packet_filter'
Device Event Class Id	All of ('PacketFilter::', ' init', init,' success', success)
Device Product	Zeek
Device Receipt Time	ts
Device Severity	Low
Device Vendor	Zeek
Message	filter
Name	All of ('Filter init', init, ' filter applied', success)

Zeek IDS Reporter Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	high = ERROR; medium = WARNING; low = INFO
Device Event Category	reporter
Device Event Class Id	level
Device Product	Zeek
Device Receipt Time	ts
Device Severity	level
Device Vendor	Zeek
File Name	location
File Path	location
Message	level
Name	Message

Zeek IDS SMTP Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Destination Address	id.resp_h

ArcSight ESM Field	Device-Specific Field
Destination Port	id.resp_p
Destination User Name	rcptto
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Transaction Depth
Device Custom String 2	Time To Live Service
Device Custom String 3	Connection ID
Device Custom String 4	Network Path
Device Custom String 5	Unique File Identifier
Device Event Category	smtp
Device Event Class Id	last_reply
Device Product	Zeek
Device Receipt Time	ts
Device Severity	Low
Device Vendor	Zeek
Message	last_reply
Source Address	id.orig_h
Source Port	id.orig_p
Source User Name	mailfrom

Zeek IDS Software Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom String 3	Version Major
Device Custom String 4	Version Minor
Device Custom String 5	Version Addition
Device Event Category	software
Device Event Class Id	software_type
Device Product	Zeek
Device Receipt Time	ts
Device Severity	Low
Device Vendor	Zeek
Message	unparsed_version
Name	name
Source Address	host
Source Port	host_p

Zeek IDS SSH Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Bytes Out	resp_size

ArcSight ESM Field	Device-Specific Field
Destination Address	id.resp_h
Destination Port	id.resp_p
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	version
Device Custom Number 2	auth_attempts
Device Custom String 3	Connection ID
Device Custom String 4	Server Software
Device Custom String 5	Client Software
Device Direction	direction
Device Event Category	ssh
Device Event Class Id	All of ('ssh:', direction, status, __simpleMap(auth_success,"T=success","F=Failure"),'Unknown')
Device Product	Zeek
Device Receipt Time	ts
Device Severity	Low
Device Vendor	Zeek
Event Outcome	one Of (__simpleMap(auth_success,"T=success","F=Failure"),'Unknown')
File Hash	hassh
File Id	compression_alg
File Path	cipher_alg
File Type	host_key_alg
Name	All of ('ssh:', direction, status, __simpleMap(auth_success,"T=success","F=Failure"),'Unknown')
Old File Hash	hasshServer
Old File Id	kex_alg
Old File Path	mac_alg
Old File Type	host_key
Source Address	id.orig_h
Source Port	id.orig_p

Zeek IDS SSL Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Application Protocol	next_protocol
Destination Address	id.resp_h
Destination Host Name	subject (Common Name)
Destination Port	id.resp_p
Device Custom Date 1	Server Certificate Start Time
Device Custom Date 2	Server Certificate End Time
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom String 1	Client Issuer
Device Custom String 2	SSL/TLS Version

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Connection ID
Device Custom String 4	SSL/TLS Cipher Suite
Device Custom String 5	Validation Status
Device Custom String 6	Organizational Unit
Device Event Category	ssl
Device Event Class ID	SSL Session
Device Product	Zeek
Device Receipt Time	ts
Device Severity	Low
Device Vendor	Zeek
Event Outcome	established
Event Outcome	__simpleMap(established,"T=Success","F=Failure")
External ID	session_id
File Hash	ja3
File Id	__simpleMap(resumed,"T=True","F=False")
File Path	subject (Common Name)
Message	subject
Name	SSL Session
Old File Hash	ja3s
Source Address	id.orig_h
Source Port	id.orig_p
Source User Name	client_subject

Zeek IDS Tunnel Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Destination Address	id.resp_h
Destination Port	id.resp_p
Device Action	action
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom String 3	Connection ID
Device Event Category	'tunnel'
Device Event Class Id	action
Device Product	Zeek
Device Receipt Time	ts
Device Severity	Low
Device Vendor	Zeek
Name	tunnel_type
Source Address	id.orig_h
Source Port	id.orig_p

Zeek IDS Weird Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Destination Address	id.resp_h
Destination Event Category	weird
Destination Port	id.resp_p
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom String 3	Connection ID
Device Custom String 4	Peer
Device Event Class Id	name
Device Product	Zeek
Device Receipt Time	ts
Device Severity	Low
Device Vendor	Zeek
Message	name
Name	name
Source Address	id.orig_h
Source Port	id.orig_p

Zeek IDS x509 Module Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	low = Low
Destination Event Category	x509
Device Custom Date 1	Certificate is not valid before
Device Custom Date 2	Certificate is not valid after
Device Custom String 3	certificate.issuer (Certificate Issuer)
Device Event Class Id	x509
Device Product	Zeek
Device Receipt Time	ts
Device Severity	Low
Device Vendor	Zeek
File ID	id
Message	certificate.subject
Name	x509