Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for TCPdump File

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for TCPdump File

November 30, 2016

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Revision History

Date	Description
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/15/2012	Added new installation procedure.
02/15/2012	Added support for tcpdump versions 3.9 and 4.1.
03/01/2008	Updated installation procedure.
11/12/2007	First edition of this Configuration Guide.

SmartConnector for TCPdump File

This guide provides information for installing the SmartConnector for TCPdump File and configuring the device for event collection. This SmartConnector is supported for installation on Solaris and Linux platforms. Versions 3.8, 3.9, and 4.1 of `tcpdump` are supported.

Product Overview

`tcpdump` is a common computer network debugging tool that runs under the command line. It lets you intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under a permissive free software license, `[1] tcpdump` is free software.

`tcpdump` works on most Unix-like operating systems: Linux, Solaris, BSD, Mac OS X, HP-UX and AIX, among others. (Note that the SmartConnector is supported for installation on Linux and Solaris platforms only.)

In some Unix-like operating systems, a user must have superuser privileges to use `tcpdump` because the packet capturing mechanisms on those systems require elevated privileges. However, you can use the `-Z` option to drop privileges to a specific unprivileged user after capturing has been set up.

In other Unix-like operating systems, the packet capturing mechanism can be configured to allow non-privileged users to use it; if that is done, superuser privileges are not required.

Optionally, you can apply a BPF-based filter to limit the number of packets seen by `tcpdump`; this renders the output more usable on networks with a high volume of traffic.

`tcpdump` is often used to debug applications that generate or receive network traffic. You also can use it for debugging the network setup itself, by determining whether all necessary routing is occurring properly, letting you further isolate the source of a problem.

You also can use `tcpdump` for the specific purpose of intercepting and displaying the communications of another user or computer. A user with the necessary privileges on a system acting as a router or gateway through which unencrypted traffic such as TELNET or HTTP passes can use `tcpdump` to view login IDs, passwords, the URLs and content of websites being viewed, or any other unencrypted information.

Using tcpdump

The easiest way to use `tcpdump` is to run it with just an `-i` switch to specify which network interface should be used. This will dump summary information for every Internet packet received or transmitted on the interface. However, `tcpdump` provides several important options, as well as the ability to specify an expression to restrict the range of packets you want to study.

For complete information about `tcpdump`, see the man page `tcpdump(1)`.

Problems You Might Encounter

No output
: Check to make sure you have specified the correct network interface with the `-i` option. If you are experiencing DNS problems, `tcpdump` might hang while attempting to look up DNS names for IP addresses; try the `-f` or `-n` options to disable this feature. If you still see nothing, check the kernel interface; `tcpdump` might not be configured properly for your system.

Dropped packets
: At the end of its run, `tcpdump` will inform you if any packets were dropped in the kernel. If this becomes a problem, it is likely that your host is unable to keep up with the network traffic and decode it at the same time. Try using `tcpdump`'s `-w` option to bypass the decoding and write the raw packets to a file, then come back later and decode the file with the `-r` switch. You can also try using `-s` to reduce the capture snapshot size.

Messages that end like [|rip] and [|domain]
: Messages ending with [|proto] indicate that the packet couldn't be completely decoded because the capture snapshot size (the so-called "snarf length") was too small. Increase it with the -s switch.

Permissions

Reading packets from a network interface may require that you have special privileges:

Under SunOS 3.x or 4.x with NIT or BPF:
You must have read access to `/dev/nit` or `/dev/bpf*`.

Under Solaris with DLPI:
You must have read/write access to the network pseudo device, for example, `/dev/le`. On at least some versions of Solaris, however, this is not sufficient to let `tcpdump` capture in promiscuous mode; on those versions of Solaris, you must be `root`, or `tcpdump` must be installed `setuid` to `root`, in order to capture in promiscuous mode. Note that, on many (perhaps all) interfaces, if you do not capture in promiscuous mode, you will not see any outgoing packets, so a capture not done in promiscuous mode may not be very useful.

Under HP-UX with DLPI:
You must be `root` or `tcpdump` must be installed `setuid` to `root`.

Under Linux:
You must be `root` or `tcpdump` must be installed `setuid` to `root`.

Under BSD:
You must have read access to `/dev/bpf*`.

Reading a saved packet file does not require special privileges.

Examples

To print all packets arriving at or departing from sundown:

```
tcpdump host sundown
```

To print traffic between helios and either hot or ace:

```
tcpdump host helios and \( hot or ace \)
```

To print all IP packets between ace and any host except helios:

```
tcpdump ip host ace and not helios
```

To print all traffic between local hosts and hosts at Berkeley:

```
tcpdump net ucb-ether
```

To print all ftp traffic through internet gateway snup: (note that the expression is quoted to prevent the shell from (mis-)interpreting the parentheses):

```
tcpdump 'gateway snup and (port ftp or ftp-data)'
```

To print traffic neither sourced from nor destined for local hosts (if you gateway to one other net, this stuff should never make it onto your local net).

```
tcpdump ip and not net localnet
```

To print the start and end packets (the SYN and FIN packets) of each TCP conversation that involves a non-local host.

```
tcpdump 'tcp[13]]& 3 != 0 and not src and dst net localnet'
```

To print IP packets longer than 576 bytes sent through gateway snup:

```
tcpdump 'gateway snup and ip[2:2]> 576'
```

To print IP broadcast or multicast packets that were not sent via ethernet broadcast or multicast:

```
tcpdump 'ether[0] & 1 = 0 and ip[16] >= 224'
```

To print all ICMP packets that are not echo requests/replies (that is, not ping packets):

```
tcpdump 'icmp[0] != 8 and icmp[0] != 0"
```

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). This configuration guide takes you through the installation process with **ArcSight Manager (encrypted)** as the destination.

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

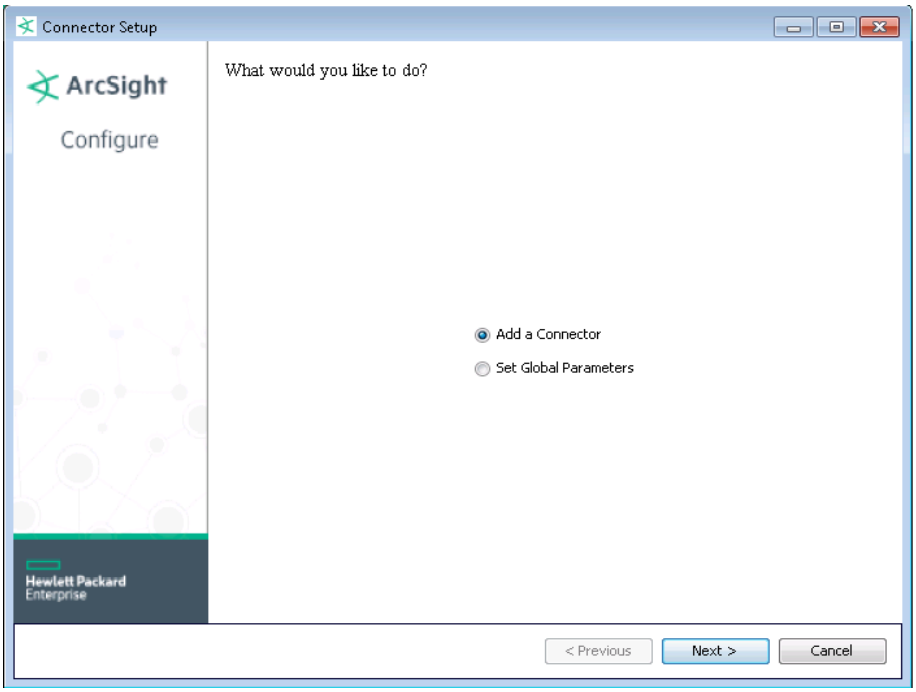
Install Core Software

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 HPE SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the HPE 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. After installing core software, you can set the following parameters:

Global Parameter	Setting
Set FIPS mode	Set to 'Enable' 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 'Disable'.
Set Remote Management	Set to 'Enable' 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 'Disable'.
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	If 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. When both values are present, the initial setting is IPv4.

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 the "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 **TCPDump** and click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
TCPdump command	Enter the command that will invoke TCPdump; for example: 'tcpdump -S -nn -l -e -v -tttt'.

Select a Destination

1 The next window asks for the destination type; make sure **ArcSight Manager (encrypted)** is selected and click **Next**. (For information about this destination or any of the other destinations listed, see the *ArcSight SmartConnector User Guide*.)

2 Enter values for the **Manager Host Name**, **Manager Port**, **User** and **Password** required parameters. This is 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 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 some SmartConnectors, a system restart is required before the configuration settings you made take effect. If a **System Restart** window is displayed, read the information and initiate the system restart operation.

Save any work on your computer or desktop and shut down any other running applications (including the ArcSight Console, if it is running), then shut down the system.

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.

TCPDUMP Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Additional data	Ack
Additional data	ethernetLength
Additional data	FirstSeq
Additional data	group
Additional data	hlim
Additional data	IPTOS
Additional data	ipv4Length
Additional data	LastSeq
Additional data	linkAddress
Additional data	nextHeader
Additional data	options
Additional data	payloadLength
Additional data	reportVersion
Additional data	rtalert
Additional data	seg
Additional data	state
Additional data	TcpPayloadBytes
Additional data	Win
Application Protocol	protocol or (ICPM, Netbios, DHCP, DNS)
Bytes In	LinkLevelLength
Destination Address	destination address
Destination Mac Address	DestMac
Destination Port	destination port

ArcSight ESM Field	Device-Specific Field
Detect Time	Date
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	TTL
Device Custom Number 2	IPID
Device Custom Number 3	IPLength
Device Custom String 1	One of (RequestedIP, CommunityString, GatewayIP, requestedAddress)
Device Custom String 2	One of (RequestedMac, RequestType, DNS response, Failed DNS response)
Device Custom String 3	One of (Fragment, OID)
Device Custom String 4	TCPFlags
Device Custom String 5	Options
Device Custom String 6	IPFlags
Device Process Name	'tcpdump'
Device Product	'tcpdump'
Device Vendor	'Unix'
Source Address	source address
Source Mac Address	SourceMac
Source Port	source port
Transport Protocol	transport protocol