Cisco Tetration Analytics Installation Guide for the Sensor Agents

First Published: October 11, 2017
Last Updated: August 14, 2018

Contents
Preface ............................................................................................................................................................................... 4
Purpose .......................................................................................................................................................................... 4
Audience ........................................................................................................................................................................ 4
Cisco Product Security Overview ................................................................................................................................... 4
Conventions ................................................................................................................................................................... 4
About the Cisco Tetration Analytics Platform ................................................................................................................... 5
Installation Planning .......................................................................................................................................................... 5
Sensor Type Comparison ............................................................................................................................................... 5
Requirements and Limitations ........................................................................................................................................... 6
  Software Limitations ...................................................................................................................................................... 6
  Hardware Limitations ...................................................................................................................................................... 6
  Supported Software Versions ........................................................................................................................................ 6
  Software Dependencies ................................................................................................................................................. 7
  Software Installation Requirements ................................................................................................................................ 8
Hardware Installation Requirements ...................................................................................................................................... 9
Licensing ........................................................................................................................................................................ 9
  License Accounting for Deployment Options ................................................................................................................... 9
  License Pooling ............................................................................................................................................................. 9
  Licensing for Software Agents ...................................................................................................................................... 9
Software Sensor Agent Installation ......................................................................................................................................... 10
Software Sensor Agent Pre-Installation Tasks .................................................................................................................. 10
  Checking for Deep Visibility Agent Dependencies on RHEL 6.[0-8], 7.[0-3] | CentOS 6.[0-8], 7.[0-3] | SUSE 11.[2-4], 12. [0-1] | Oracle Linux Server 6.[0-8], 7.[0-3] ................................................................. 10
  Checking for Deep Visibility Agent Dependencies on Ubuntu 14.04.x ............................................................................ 11
Preface

Checking for Enforcement Agent Dependencies on Ubuntu 14.04.x | RHEL 6.[0-8], 7.[0-3] | CentOS 6.[0-8], 7.[0-3] | SUSE 11.[4], 12.[0-1] | Oracle Linux Server 6.[0-8], 7.[0-3] ................................................................. 12

Checking for Universal Agent Dependencies on AIX 5.3, 6.1, 7.1, 7.2 ................................................................. 12

Creating the Software Agent Interface Intent ........................................................................................................ 12

Downloading the Software Agent .......................................................................................................................... 12

Software Sensor Agent Installation Tasks .......................................................................................................... 13

Installing the Deep Visibility and Enforcement Agents on RHEL 6.[0-8], 7.[0-3] | CentOS 6.[0-8], 7.[0-3] | SLES 11.[2-4], 12.[0-1] | Oracle Linux Server 6.[0-8], 7.[0-3] ................................................................. 13

Installing the Deep Visibility and Enforcement Agents on Ubuntu 14.04.x | 14.10 .................................................................................. 13

Installing the Deep Visibility and Enforcement Agents on Microsoft Server .......................................................... 13

Installing the Universal Agent AIX 5.3, 6.1, 7.1, or 7.2 ..................................................................................... 13

Software Sensor Agent Post-Installation Tasks .................................................................................................. 14

Verifying the Agent Installation on RHEL 6.[0-8], 7.[0-3] | CentOS 6.[0-8], 7.[0-3] | Ubuntu 14.04.x | 14.10 | SUSE 11.[2-4], 12.[0-1] | Oracle Linux Server 6.[0-8], 7.[0-3] ................................................................. 14

Verifying the Agent Installation on Microsoft Server .............................................................................................. 14

Verifying the Agent Installation on AIX ................................................................................................................... 15

Uninstalling the Software Sensor Agent .............................................................................................................. 15

Uninstalling the Software Agent from Ubuntu 14.04.x | RHEL 6.[0-8], 7.[0-3] | CentOS 6.[0-8], 7.[0-3] | SLES 11[4], 12.[0-1] | SUSE 11.[2-4], 12. [0-1] | Oracle Linux Server 6.[0-8], 7.[0-3] ................................................................. 15

Uninstalling the Software Agent from Microsoft Server .......................................................................................... 15

Uninstalling the Software Agent from AIX .......................................................................................................... 15

Hardware Sensor Agent Installation ...................................................................................................................... 16

Downloading the Hardware Agent ....................................................................................................................... 16

Uploading the Hardware Sensor Agent Firmware .................................................................................................. 16

Creating a Fabric Node Control Policy ................................................................................................................ 16

Creating an Analytics Policy for the Hardware Sensor Agent .............................................................................. 17

Creating a Leaf Switch Policy Group for the Hardware Sensor Agent .................................................................. 17

Creating a Leaf Switch Profile for the Hardware Sensor Agent ............................................................................ 17

Verifying the Hardware Sensor Agent Firmware Installation .................................................................................. 18

Creating Tenants and VRF Instances in Cisco Tetration Analytics ........................................................................ 19

Enabling the Precision Time Protocol ................................................................................................................ 20

Troubleshooting ..................................................................................................................................................... 20

Troubleshooting the Deep Visibility Agent ........................................................................................................ 20

Troubleshooting the Enforcement Agent ........................................................................................................... 21
Troubleshooting on AIX ............................................................................................................................................... 21
Virtual Appliances ............................................................................................................................................................ 21
Cisco Tetration Analytics ERSPAN Virtual Appliance ................................................................................................... 21
  Deploying the Cisco Tetration Analytics ERSPAN Virtual Appliance .............................................................. 21
  Configuring the Source ERSPAN Session ............................................................................................................. 22
Supported ERSPAN Formats ............................................................................................................................................. 22
Performance Considerations When Configuring the ERSPAN Source ................................................................. 23
Security Considerations for the Cisco Tetration Analytics ERSPAN Virtual Appliance ............................................ 23
Troubleshooting Issues with the Cisco Tetration Analytics ERSPAN Virtual Appliance ........................................... 23
Cisco Tetration Analytics NetFlow Virtual Appliance .................................................................................................. 24
  Deploying the Cisco Tetration Analytics NetFlow Virtual Appliance .............................................................. 24
  Configuring NetFlow on the Switch ......................................................................................................................... 25
Security Considerations for the Cisco Tetration Analytics NetFlow Virtual Appliance ............................................ 26
Troubleshooting Issues with the Cisco Tetration Analytics NetFlow Virtual Appliance ........................................... 26
Cisco Tetration Analytics Citrix NetScaler AppFlow Collector Virtual Appliance ......................................................... 27
  Deploying the Cisco Tetration Analytics Citrix NetScaler AppFlow Collector Virtual Appliance .................... 27
  Configuring AppFlow on Citrix NetScaler ............................................................................................................ 27
Security Considerations for the Cisco Tetration Analytics Citrix NetScaler AppFlow Collector Virtual Appliance .. 28
Troubleshooting Issues with the Cisco Tetration Analytics Citrix NetScaler AppFlow Collector Virtual Appliance 28
Cisco Tetration Analytics F5 BIG-IP Collector Virtual Appliance .................................................................................. 29
  Deploying the Cisco Tetration Analytics F5 BIG-IP Collector Virtual Appliance ............................................ 29
  Configuring IPFIX on F5 BIG-IP ................................................................................................................................. 30
Security Considerations for the Cisco Tetration Analytics F5 BIG-IP Collector Virtual Appliance .......................... 31
Troubleshooting Issues with the Cisco Tetration Analytics F5 BIG-IP Collector Virtual Appliance ......................... 31
Reference Information ..................................................................................................................................................... 32
Appendix: Microsoft Server DLLs ..................................................................................................................................... 32
Obtaining Documentation and Submitting a Service Request ........................................................................................ 34
Legal Information ............................................................................................................................................................. 35
Preface

The following sections provide information about this document.

Purpose

This document describes how to install the following software:

- Cisco Tetration Analytics software agents installed from a 2.0.2.20 cluster.

Audience

This installation guide is intended for administrators who are responsible for installing the Cisco Tetration Analytics software.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product, you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at the following URL: http://www.cisco.com/wwl/export/crypto/tool/stqrq.html

If you require further assistance, contact us by sending an email to export@cisco.com.

Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold font</strong></td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><em>italic font</em></td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic</em> font.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><strong>courier font</strong></td>
<td>Terminal sessions and information the system displays appear in <strong>courier</strong> font.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>
About the Cisco Tetration Analytics Platform

Cisco Tetration Analytics is a turnkey data center analytics solution that uses modern big data and machine learning analytics technologies to better understand application behavior inside of the data center. The data collection framework consists of hardware and software agents.

The agent framework consists of agents that provide data collection and streaming of telemetry back to the analytics cluster. The heart of Cisco Tetration Analytics is the analytics cluster, which is a big data platform that is designed to ingest the large volumes of streaming telemetry from the agents for long term retention.

Installation Planning

The following sections provide information about the installation planning:

- Sensor Type Comparison
- Requirements and Limitations
- Licensing

Sensor Type Comparison

The following table provides a comparison of the sensor types:

<table>
<thead>
<tr>
<th>Type</th>
<th>Main Use Case</th>
<th>What is Captured</th>
<th>Latency Info</th>
<th>When to Use</th>
<th>SaaS</th>
<th>Tetration-V</th>
<th>VRF Configuration Behind NAT</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software sensor (deep visibility/enforcement)</td>
<td>Flow search ADM enforcement SW NPMD Forensics analysis</td>
<td>Flow information Inter-packet variation Context details (process ID info)</td>
<td>SRTT Estimated network latency App latency</td>
<td>Always the first option</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Universal Sensor</td>
<td>ADM</td>
<td>Which port is opened Process information No actual packet information</td>
<td>N/A</td>
<td>You are unable to use the software sensor You have old servers or mainframes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ERSPAN Sensor</td>
<td>Flow search ADM</td>
<td>Flow information Inter-packet variation</td>
<td>N/A</td>
<td>You are unable to use the software sensor</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Need OVA deployment Need bandwidth for ERSPAN</td>
</tr>
</tbody>
</table>
Requirements and Limitations

The following sections provide information about the requirements that your system must meet to install the Cisco Tetration Analytics software agent.

Software Limitations

The following limitations apply to the software agent:

- The Visibility and Enforcement software agents are intended to be installed on x86 64-bit systems.
- The Universal agent is intended to be installed on 32-bit and 64-bit systems.

Hardware Limitations

The following limitations apply to the hardware agent:

- Cisco Tetration Analytics is supported only on Cisco Nexus 9000 EX and newer leaf switches.

Supported Software Versions

The following software versions are supported with Release 2.0.2.20:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Full Visibility</th>
<th>Limited Visibility (Universal Agent)</th>
<th>Policy Enforcement</th>
</tr>
</thead>
</table>

Table 2: Software Agent Support Matrix
**Software Dependencies**

Your system must meet the following requirements to install the software agent successfully. Any distributions with packages that are missing or below the minimum version must be remediated.

**Linux Installation Dependencies**

You must meet the following dependencies to install the software agent on Linux:

- **Install Requirements**
  - Root user or privilege is required
  - The correct time zone and system clock settings must be set
  - 64-bit version (universal agents support 32-bit)

- **Deep Visibility Agent**
  - curl: version 7.15 or later
  - dmidecode: version 2.11 or later
  - openssl: we recommend that you upgrade openssl to the latest version that is supported by the Linux distributor (such as RedHat or Oracle)
  - cpio
  - sed
  - lsb_release
  - awk
  - flock
  - lsof
  - rpm (even in Ubuntu/Debian)
Cisco Tetration Analytics Installation Guide for the Sensor Agents

Installation Planning

- Enforcement Agent
  - Linux Install Dependencies

- Deep Visibility Agent dependencies
  - Iptables: version v1.4.7-16 or later
  - ipset: version v6.11-4 or later
- ip6tables services up

Microsoft Server and Desktop Install Dependencies
You must meet the following dependencies to install the software agent on Microsoft Server:

- Installation Requirements
  - Administrator user or privilege is required.
  - The correct time zone and system clock settings must be set.
  - 64-bit version.
  - All required DLLs are installed by installer. See the appendix for more information.

- Deep Visibility Agent
  - Npcap version 0.94 or later
    - If you use the install.cmd script (see below) to install, Npcap version 0.94 will be installed automatically if a version of Npcap is not already installed.
    - If a version of Npcap is installed already and it is not Npcap version 0.94 or later, then the installation script will fail and you will be prompted to upgrade Npcap.

- Enforcement Agent
  - Installation dependencies:
    - Deep Visibility Agent dependencies
    - Windows Firewall enabled

AIX Install Dependencies
You must meet the following dependencies to install the universal software agent on AIX:

- Installation Requirements
  - Root user is required
  - The correct time zone and system clock settings must be set

- Universal Agent
  - crontab
  - install (shell command)

Software Installation Requirements
The entire installation process, excluding pre- and post-installation tasks, takes no more than 5 minutes to execute the required set of commands. The actual installation time can vary depending on your installation process and procedures.
The software agents require the following TCP ports:

### Table 3 TCP ports required by the software agents

<table>
<thead>
<tr>
<th>Port</th>
<th>Purpose</th>
<th>Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Control</td>
<td>On-premises or Cisco Tetration Analytics Virtual</td>
</tr>
<tr>
<td>5640</td>
<td>Visibility</td>
<td>On-premises or Cisco Tetration Analytics Virtual</td>
</tr>
<tr>
<td>5660</td>
<td>Enforcement</td>
<td>On-premises or Cisco Tetration Analytics Virtual</td>
</tr>
<tr>
<td>443</td>
<td>Control, Visibility, Enforcement</td>
<td>Software-as-a-Service</td>
</tr>
</tbody>
</table>

## Hardware Installation Requirements

The entire installation process, excluding pre- and post-installation tasks, takes no more than 5 minutes to execute the required set of commands. The actual installation time can vary depending on your installation process and procedures.

You must meet the following requirements in your Cisco APIC:

- Configure in-band management.
- Use the VRF instance mgmt:inb. This VRF instance is pre-defined in the Cisco Application Policy Infrastructure Controller (APIC) mgmt tenant; you do not need to create the VRF instance manually.
- Use the bridge domain subnet as the gateway of the hardware agent. Because of this requirement, you need an L3Out for Cisco Tetration Analytics cluster reachability. You need an L3Out because a spine switch does not reply to the ARP for the node's in-band mgmt IP address.

The hardware agents require the following TCP ports:

### Table 4 Ports required by the hardware agents

<table>
<thead>
<tr>
<th>Port</th>
<th>Purpose</th>
<th>Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 443</td>
<td>Control</td>
<td>On-premises or Cisco Tetration Analytics Virtual</td>
</tr>
<tr>
<td>UDP 5640</td>
<td>Leaf switch visibility</td>
<td>On-premises or Cisco Tetration Analytics Virtual</td>
</tr>
<tr>
<td>UDP 5641</td>
<td>Spine switch visibility</td>
<td>On-premises or Cisco Tetration Analytics Virtual</td>
</tr>
</tbody>
</table>

## Licensing

The following sections provide information about the licensing requirements for Cisco Tetration Analytics.

### License Accounting for Deployment Options

The license accounting deployment options are based on the software and hardware agents in the Cisco Tetration Analytics platform.

### License Pooling

A Cisco Tetration Analytics software subscription license can be pooled across multiple Cisco Tetration Analytics clusters.

### Licensing for Software Agents

You can deploy the Cisco Tetration Analytics platform and choose to use software agents. In this scenario, license accounting is based on the number of software agents concurrently connected to the platform. These agents can be deployed on virtual machines or bare-metal servers. Information about the number of concurrent agents is available to the administrator through the web GUI.

The subscription duration can be 1, 3, or 5 years with an option for annual billing or prepayment. The software license consists of two components:
Software Sensor Agent Installation

The following sections provide information about installing the software agent.

Software Sensor Agent Pre-Installation Tasks

The following sections provide information about software sensor agent pre-installation tasks.

Checking for Deep Visibility Agent Dependencies on RHEL 6.[0-8], 7.[0-3] | CentOS 6.[0-8], 7.[0-3] | SUSE 11.[2-4], 12.[0-1] | Oracle Linux Server 6.[0-8], 7.[0-3]

The following procedure checks if the deep visibility agent dependencies are met on RHEL, CentOS, SLES, or Oracle Linux Server. If any of the following dependencies are missing, the installation will fail:

1. Check the operating system version. Use one of the following commands that is appropriate for your operating system:
   - `# cat /etc/centos-release`
   - `# cat /etc/redhat-release`
   - `# cat /etc/SuSE-release`
   - `# cat /etc/os-release`

2. Check the kernel version:
   - `# uname -r`

3. Check for the /bin/sh and bash shells:
   - `# cat /etc/shells`

4. Ensure that the rpmlib RPM is installed and that the libraries indicated below exist:
   - `# rpm --showrc | grep 'rpmlib(CompressedFileNames)'
   - `# rpm --showrc | grep 'rpmlib(PayloadFilesHavePrefix)'

5. Check the curl version:
   - `# curl -V`

6. Check the dmidecode version:
   - `# dmidecode -V`

7. Check the openssl version:
   - `# openssl version -a`

8. Check the cpio version:
   - `# cpio --version`

9. Check the sed version:
Checking for Deep Visibility Agent Dependencies on Ubuntu 14.04.x

The following procedure checks if the deep visibility agent dependencies are met on Ubuntu. If any of the following dependencies are missing, the installation will fail:

1. Check the Ubuntu version:
   
   ```
   # lsb_release -a
   ```

2. Check the kernel version:
   
   ```
   # uname -r
   ```

3. Check for the /bin/sh and bash shells:
   
   ```
   # cat /etc/shells
   ```

4. Ensure that the rpmlib RPM is installed and that the libraries indicated below exist:
   
   ```
   # rpm --showrc | grep 'rpmlib(CompressedFileNames)'
   # rpm --showrc | grep 'rpmlib(PayloadFilesHavePrefix)'
   ```

5. Check the curl version:
   
   ```
   # curl -V
   ```

6. Check the dmidecode version:
   
   ```
   # dmidecode -V
   ```

7. Check the openssl version:
   
   ```
   # openssl version -a
   ```

8. Check the cpio version:
   
   ```
   # cpio --version
   ```

9. Check the sed version:
   
   ```
   # sed --version
   ```

10. Check for the lsb_release RPM:
    
    ```
    # dpkg -S lsb_release
    ```

11. Check the awk version:
    
    ```
    # awk --version
    ```
# awk -V

12. Check the flock version:

    # flock -V

13. Check for the libpcap RPM:

    # dpkg -S libpcap

Checking for Enforcement Agent Dependencies on Ubuntu 14.04.x | RHEL 6.[0-8], 7.[0-3] | CentOS 6.[0-8], 7.[0-3] | SUSE 11.[4], 12. [0-1] | Oracle Linux Server 6.[0-8], 7.[0-3]

Check for all of the same dependencies as with deep visibility, plus the following dependencies:

- Check the iptables version:

    # iptables --version

- Check the ipset version:

    # ipset --version

Checking for Universal Agent Dependencies on AIX 5.3, 6.1, 7.1, 7.2

Cisco will package and provide you the .tar.gz file. Check for dependencies. If any of the following dependencies are missing, the installation will fail:

- Run the crontab command to ensure that it is installed:

    # crontab -l

- Run the install command to ensure that it is installed:

    # install

- Check the dmidecode version:

    # dmidecode --V

Creating the Software Agent Interface Intent

The following procedure creates the software agent interface intent on the Cisco Tetration Analytics Cluster:

Create the software agent interface intent on the Cisco Tetration Analytics cluster:

1. Log into the Cisco Tetration Analytics GUI. We recommend that you use Google Chrome.
2. Click the gears icon > Agent Config.
3. Click on the Software Agent tab.
4. Click Create Agent Config Intent.

Downloading the Software Agent

Cisco will provide you with the AIX agents package. The following procedure downloads the software agent from the Cisco Tetration Analytics cluster:

1. Log into the Cisco Tetration Analytics GUI. We recommend that you use Google Chrome.
2. Click the gears icon > Agent Config.
3. Click on the **Software Agent Download** tab.
4. Click the **Download** button for the correct agent that you want to install.

**Software Sensor Agent Installation Tasks**

The following sections provide installation procedures for the software agent.

**Installing the Deep Visibility and Enforcement Agents on RHEL 6[0-8], 7[0-3] | CentOS 6[0-8], 7[0-3] | SLES 11[2-4], 12[0-1] | Oracle Linux Server 6[0-8], 7[0-3]**

The following procedure installs the deep visibility and enforcement agents on RHEL, CentOS, SLES, or Oracle Linux Server:

1. Verify that all dependencies are installed and are the correct version.
2. Install the agent. On the endpoint, run the following command:

   ```
   # rpm -Uvh <agentfile.rpm>
   ```

**Installing the Deep Visibility and Enforcement Agents on Ubuntu 14.04.x | 14.10**

The following procedure installs the deep visibility and enforcement agents on Ubuntu:

1. Verify that all dependencies are installed and are the correct version.
2. Install the agent. On the endpoint, run the following command:

   ```
   # rpm -Uvh <agentfile.rpm> --nodeps
   ```

**Installing the Deep Visibility and Enforcement Agents on Microsoft Server**

The following procedure installs the deep visibility and enforcement agents on Microsoft Server:

2. You can run the `install.cmd` script and stop following this procedure for an automated installation of the deep visibility and enforcement agents on Microsoft Server, or you can manually install the agent by proceeding with this procedure.

   ```
   > install.cmd
   ```

3. Install **Npcap** if it is not installed:

   ```
   > npcap-0.94.exe /S
   ```

   `/S` specifies silent mode.

4. Create the **Agent** directory:

   ```
   > mkdir C:\Program Files\Cisco Tetration\Agent
   ```

5. Copy the `sensor_config` file to the **Agent** directory:

   ```
   > copy sensor_config C:\Program Files\Cisco Tetration\Agent
   ```

6. Copy the `site.cfg` file to the **Agent** directory:

   ```
   > copy site.cfg C:\Program Files\Cisco Tetration\Agent
   ```

7. Create the **cert** directory:

   ```
   > mkdir C:\Program Files\Cisco Tetration\Agent\cert
   ```

8. Copy the `ca.cfg` file to the **cert** directory:
> copy ca.cert C:\Program Files\Cisco Tetration\Agent\cert

9. Run the installer:

> WindowsSensorInstaller.exe /S

/S specifies silent mode. The installation in the GUI displays without the /S argument.

The package can be installed to a non-standard location by using the /D command line parameter. For example:

> WindowsSensorInstaller.exe /D=C:\AgentCustomPath

Once installation completes, all files in the C:\tmp\win_sensor directory will be automatically deleted. The installed path (default or custom) can be found in the registry under the following entry:

HKLM\Software\Tetration\SensorPath

Installing the Universal Agent AIX 5.3, 6.1, 7.1, or 7.2

The following procedure installs the universal agent on AIX:

1. Verify all dependencies are installed and correct version.
2. Unpackage the agent:

    # tar xzvf tet-sensor-lw-2.0.2-x-1-aix-ppc.tar.gz

3. Run the installer:

    # sh install.sh

Software Sensor Agent Post-Installation Tasks

The following sections provide procedures for you to follow after installing the software agent.

Verifying the Agent Installation on RHEL 6.[0- 8], 7.[0-3] | CentOS 6.[0- 8], 7.[0-3] | Ubuntu 14.04.x | 14.10 | SUSE 11.[2-4], 12.[0-1] | Oracle Linux Server 6.[0-8], 7.[0-3]

The following procedure verifies the agent installation on RHEL, CentOS, SLES, or Oracle Linux Server:

1. View the agent status by running one of the following commands as appropriate to your operating system:

    ■ # service tet-sensor status
    ■ # initctl status tet-sensor
    ■ # systemctl status tet-sensor

2. View the enforcer status by running one of the following commands as appropriate to your operating system:

    ■ # service tet-enforcer status
    ■ # initctl status tet-enforcer
    ■ # systemctl status tet-enforcer

3. Check for the Cisco Tetration Analytics aux process:

    # ps aux | grep tet

4. Check for the Cisco Tetration Analytics afx process:

    # ps afx | grep tet
5. View the Cisco Tetration Analytics network statistics:
   
   # netstat -natp | grep -i tet

Verifying the Agent Installation on Microsoft Server

The following procedure verifies the agent installation on Microsoft Server. The installation will create an Uninstall action in the Control Panel.

1. Check if the files are installed in C:\Program Files\Cisco Tetration.
2. View the information about the WindowsTetEngine service:
   
   > sc query WindowsTetEngine
3. Check for the WindowsSensor.exe process:
   
   > tasklist /FI "IMAGENAME eq WindowsSensor.exe"
4. View the information about the WindowsAgentEngine service:
   
   > sc query WindowsAgentEngine
5. Check for the tet_enforcer.exe process:
   
   > tasklist /FI "IMAGENAME eq tet_enforcer.exe"
6. Check for the tet_controller.exe process:
   
   > tasklist /FI "IMAGENAME eq tet_controller.exe"

Verifying the Agent Installation on AIX

The following procedure verifies the agent installation on AIX:

1. Check to see if the agent job is scheduled to run by viewing the crontab:
   
   # crontab -l

Uninstalling the Software Sensor Agent

The following sections provide procedures for uninstalling the software sensor agent.

Uninstalling the Software Sensor Agent from Ubuntu 14.04.x | RHEL 6.[0- 8], 7.[0-3] | CentOS 6.[0- 8], 7.[0-3] | SLES 11[4], 12.[0-1] | SUSE 11.[2-4], 12. [0-1] | Oracle Linux Server  6.[0-8], 7.[0-3]

The following procedure uninstalls the software agent from RHEL, CentOS, SLES, or Oracle Linux Server:

1. Check for name of the installed package:
   
   # rpm -qa | grep tet
2. Remove the package:
   
   # rpm -e <tet-sensor-site.xxx>
3. Remove the tet directory:
   
   # rm -r /usr/local/tet

Uninstalling the Software Agent from Microsoft Server

The following procedure uninstalls the software agent from Microsoft Server:

1. Uninstall action in the Control Panel.
1. Run the `uninstall_all.cmd` script.

Uninstalling the Software Agent from AIX

The following procedure uninstalls the software agent from AIX:

1. Run uninstallation script:

```
# cd /usr/local/tet-light/
# ./uninstall.sh
```

Hardware Sensor Agent Installation

The following sections provide information about installing the hardware agent.

Downloading the Hardware Agent

The following procedure downloads the hardware agent from the Cisco Tetration Analytics cluster:

1. Log into the Cisco Tetration Analytics GUI. We recommend that you use Google Chrome.
2. Click the gears icon > Agent Config.
3. Click on the Hardware Agent Download tab.
4. Click the Download button for the correct agent that you want to install.

Uploading the Hardware Sensor Agent Firmware

The following procedure uploads the hardware sensor agent firmware to the Cisco Application Policy Infrastructure Controller (APIC):

1. Log into the Cisco APIC GUI.
2. On the menu bar, choose Admin > Firmware.
3. In the navigation pane, right-click Download Tasks and choose Upload Firmware to APIC.
4. Browse to the agent firmware file and click Open.
5. Click Submit.
6. To verify that the firmware uploaded successfully, in the navigation pane, choose Firmware Repository and look for the firmware in the work pane.

Creating a Fabric Node Control Policy

You should create a fabric node control policy to enable the analytics priority for consistency. The following procedure creates a fabric node control policy in the Cisco Application Policy Infrastructure Controller (APIC):

1. Log into the Cisco APIC GUI.
3. In the navigation pane, expand Policies > Monitoring.
4. Right-click Fabric Node Controls and choose Create Fabric Node Control.
5. For the Feature Selection, you can choose Analytics Priority, Netflow Priority, or Telemetry Priority. Analytics Priority is Cisco Tetration Analytics.
Creating an Analytics Policy for the Hardware Sensor Agent

You must create an analytics policy to specify the Cisco Tetration Analytics cluster IP address. The following procedure creates an analytics policy in the Cisco Application Policy Infrastructure Controller (APIC):

1. Log into the Cisco APIC GUI.
3. In the navigation pane, choose Policies > Analytics.
4. Right-click Analytics and choose Create Analytics Policy.
5. Enter the information as appropriate for your configuration:
   - Cluster—Enter the Cisco Tetration Analytics cluster name.
   - Name—Enter the name of the policy that you are creating.
   - IP—Enter the IP address of the Cisco Tetration Analytics cluster. However, the hardware agent uses the values in the hardware agent image on TA Cluster. The value that you enter in this field is ignored.
   - Destination Port—Enter the destination port number of the switches. Leaf switches use destination port 5640. Spine switches use destination port 5641.
   - DSCP—The Differentiated Services Code Point (DSCP) value for the policy. Choose VA (voice admit).
6. Click Submit.

Creating a Leaf Switch Policy Group for the Hardware Sensor Agent

The following procedure creates a leaf switch policy group in the Cisco Application Policy Infrastructure Controller (APIC):

1. Log into the Cisco APIC GUI.
3. In the navigation pane, expand Switch > Leaf Switches.
4. Right-click Policy Groups and choose Create Leaf Switch Policy Group.
5. Enter the information as appropriate for your leaf switch:
   - Name—Enter the name of the policy that you are creating.
   - Analytics Policy—Choose the analytics policy that you created previously.
   - Node Control Policy—Choose the fabric node control policy that you created previously.
6. Click Submit.

Creating a Leaf Switch Profile for the Hardware Sensor Agent

The following procedure creates a leaf switch profile in the Cisco Application Policy Infrastructure Controller (APIC):

1. Log into the Cisco APIC GUI.
3. In the navigation pane, expand Switches > Leaf Switches.
4. Right-click Profiles and choose Create Leaf Switch Profile.
5. Enter the information as appropriate for your leaf switch.
   - Name—Enter the name of the profile that you are creating.
   - Switch Associations—Add the desired leaf switches and choose the leaf switch policy group that you created previously for each switch.

6. Click Submit.

Verifying the Hardware Sensor Agent Firmware Installation

The following procedure verifies the hardware sensor agent firmware installation:

1. Log into the Cisco APIC CLI.
2. Enter the following command:
   ```bash
   apic1# fabric 101 show flow monitor
   101 (Leaf1)
   Feature Prio: Analytics
   ```
   **Feature Prio** should have a value of **Analytics**.

3. Log into the leaf switch’s CLI.
4. Enter the following command:
   ```bash
   Leaf1# ps -ef | grep ta_agent
   root 19200 18286 0 04:42 pts/0 00:00:00 /usr/local/bin/node /bootflash/tetration/ta_agent/ta_agent.js
   admin 33433 32405 0 04:44 pts/2 00:00:00 grep ta_agent
   ```
   You should see the **ta_agent.js** process.

5. Enter the following commands:
   ```bash
   Leaf1# cd /aci/mitfs/sys/analytics/inst-analytics
   Leaf1# cat summary
   # Netflow Instance
   mode : analytics
   adminSt : enabled
   childAction :
   ctrl :
   dn : sys/analytics/inst-analytics
   ipFiltAct : deny
   lcOwn : local
   modTs : 2017-12-01T18:22:16.751+00:00
   monPolDn : uni/fabric/monfab-default
   name :
   nwIssues :
   operErr :
   operSt :
   operStQual :
   ptoperStQual :
   policyDn : uni/fabric/analytics/cluster-pliny/cfgsrv-ACI-HW-Sensor-Pliny
   rn :
   status :
   ```
   You should see various "analytics" values, as shown in the example output. **policyDn** should show the name of the analytics policy that you created.
6. Enter the following commands:

```
Leaf1# cd controller-pliny_ACI-HW-Sensor-Pliny
Leaf1# cat summary
```

# Controller Reachability
Name : pliny_ACI-HW-Sensor-Pliny
InstallOperSt : success
InstallOperStQual : installed
childAction :
descry :
dn : sys/analytics/inst-analytics/controller-pliny_ACI-HW-Sensor-Pliny
dscp : CS4
dstAddr : 10.28.121.132
dstPort : 5640
imageUri : http://10.0.0.1:7777/fwrepo/aci-analyticsagent-dk9.default.bin
imageUri2 : https://10.0.0.1/fwrepo/aci-analyticsagent-dk9.default.bin
imageVer : 2.2.1.31
lcOwn : local
modTs : 2017-12-18T18:22:18.432+00:00
monPolDn : uni/fabric/monfab-default
nameAlias :
rn : controller-pliny_ACI-HW-Sensor-Pliny
srcAddr : 192.168.136.24/24
srcIf : unspecified
status :
uid : 0
vrfName : mgmt:inb

Replace "pliny_ACI-HW-Sensor-Pliny" with the name of the analytics policy that you created.

7. Log into the Cisco Tetration Analytics GUI. We recommend that you use Google Chrome.

8. Click the gears icon > Agent Config.

9. Click on the Hardware Agent Config tab. After the agent registration successfully completes, you should see the switches on this screen.

Creating Tenants and VRF Instances in Cisco Tetration Analytics

By default, all of the data is placed in the Unknown VRF. You must create a VRF instance in Cisco Tetration Analytics to have the data be placed into the VRF instance of your choice.

The following procedure creates a tenant and VRF instance in Cisco Tetration Analytics:

1. Log into the Cisco Tetration Analytics GUI.

2. Click the gears icon > Tenants.

3. Click Add Tenant.

4. Enter an ID and name for the tenant. The ID must be unique in Cisco Tetration Analytics. There is no relationship between the tenant ID and a Cisco Application Policy Infrastructure Controller (APIC) VRF instance ID.

5. Click Add VRF next to the tenant that you just created.

The VRF instance configuration in Cisco Tetration Analytics must match the VRF instance configuration that you created in the Cisco APIC. You can view the VRF instance configuration by using the Cisco APIC GUI or the leaf switch’s CLI. You will use this information in the next steps.

6. Enter a unique ID and a name for the VRF instance. There is no relationship between the VRF ID and a Cisco Application Policy Infrastructure Controller (APIC) VRF instance ID.
7. In the Switch VRFs section, click Add Switch VRF.

8. In the Switch VRFs field that appears, enter the same VRF instance name that you have in your Cisco APIC and click the check button. The name is case insensitive.

To view the configuration using the Cisco APIC GUI, perform the following steps:

a. Log into the Cisco APIC GUI.

b. On the menu bar, choose Fabric > Inventory.

c. In the navigation pane, expand Pod 1 > leaf_name > VRF Contexts. You should see the VRF instance that you created in the navigation pane under VRF Contexts.

To view the configuration using the leaf switch's CLI, perform the following steps:

a. Log into the leaf switch's CLI.

b. Enter the following command:

```
Leaf1# show vrf
```

```
VRF-Name   VRF-ID   State  Reason
black-hole   3   Up    --
BrewingCo:BrewingCoVRF  6   Up    --
mgmt:inb   5   Up    --
SakeCo:VRF1   7   Up    --
overlay-1   4   Up    --
```

9. Click Create.

**Enabling the Precision Time Protocol**

If you use the Network Performance Monitoring and Diagnostics (NPMD) feature with the hardware sensor, you must enable the Precision Time Protocol (PTP). PTP is a time synchronization protocol defined in IEEE 1588 for nodes distributed across a network. With PTP, it is possible to synchronize distributed clocks with an accuracy of less than 1 microsecond via Ethernet networks. PTP’s accuracy comes from the hardware support for PTP in the ACI fabric spines and leafs. It allows the protocol to accurately compensate for message delays and variation across the network. For more information about PTP, see the Cisco ACI Latency and Precision Time Protocol document that you can find at the following URL:


The following procedure enables PTP in the Cisco Application Policy Infrastructure Controller (APIC):

1. Log into the Cisco APIC GUI.

2. On the menu bar, choose System > System Settings.

3. In the navigation pane, choose Precision Time Protocol.

4. In the work pane, click Enabled.

**Troubleshooting**

The following sections provide information about trouble shooting issues with the software agent.

**Troubleshooting the Deep Visibility Agent**

The following procedure trouble shoots issues with the deep visibility agent:
1. Restart the Cisco Tetration Analytics deep visibility agent by running one of the following commands as appropriate to your operating system:
   - `# service tet-sensor restart`
   - `# initctl restart tet-sensor`
   - `# systemctl restart tet-sensor`

2. View the tail end of the Cisco Tetration Analytics enforcer log file to look for error messages:
   ```
   # tail -f /usr/local/tet/log/tet-sensor.log
   ```

Troubleshooting the Enforcement Agent

The following procedure trouble shoots issues with the enforcement agent:

1. Restart the Cisco Tetration Analytics enforcement agent by running one of the following commands as appropriate to your operating system:
   - `# service tet-enforcer restart`
   - `# initctl restart tet-enforcer`
   - `# systemctl restart tet-enforcer`

2. View the tail end of the Cisco Tetration Analytics enforcer log file to look for error messages:
   ```
   # tail -f /usr/local/tet/log/tet-enforcer.log
   ```

Troubleshooting on AIX

Use the following command to trouble shoot issues with the software agent on AIX:

```
# more /usr/local/tet-light/log/lw-sensor.log
```

Virtual Appliances

You can deploy Cisco Tetration Analytics on the following virtual appliances:

- ERSPAN
- NetFlow
- Citrix NetScaler AppFlow Collector
- F5 BIG-IP IPFIX Collector

Cisco Tetration Analytics ERSPAN Virtual Appliance

The following sections provide procedures for and information about deploying the Cisco Tetration Analytics Encapsulated Remote Switch Port Analyzer (ERSPAN) virtual appliance.

Deploying the Cisco Tetration Analytics ERSPAN Virtual Appliance

1. Download the Cisco Tetration Analytics ERSPAN Virtual Machine Appliance OVA file from the Cisco CCO page.
2. Create a Virtual Machine from the OVA file and provision the VM with 8 vCPU cores, 4 gigabytes of RAM, and 3 virtual interfaces in bridged networking mode.
3. Download the `CentOS-7.3 -span` agent image bundle into a directory, which is referred to in this procedure as `<cfg_dir>`. 
4. Add a `<cfg_dir>/ip_config` file containing the IP and gateway address for each interface. The file must contain three rows in the following format:

```
<CIDR>/gateway IP
```

Example: 172.33.9.8/24, 172.33.9.1

All interfaces must belong to the same subnet. Optionally, add a `<cfg_dir>/host_name` file containing the hostname string. The default hostname is "erspan-vm."

The `ip_config` file cannot contain any blank lines, including at the end of the file.

5. Create an ISO file using the following command:

```
mkisofs -r -o <name>.iso <cfg_dir>
```

6. Add the ISO file to the VM as a CDROM/DVD disc image.

7. Boot the VM.

### Configuring the Source ERSPAN Session

The following example steps are for a Cisco Nexus 9000 switch. The configuration steps might differ for other Cisco platforms; refer to the Cisco configuration guide for the Cisco platform that you are configuring.

1. Enter the configuration mode:

   ```
   # config terminal
   ```

2. Configure the ERSPAN source IP address:

   ```
   (config)# monitor erspan origin ip-address 192.168.1.1 global
   ```

3. Create and configure the source ERSPAN session:

   ```
   (config)# monitor session 10 type erspan-source
   (config-erspan-src)# source interface ethernet 1/23 both
   (config-erspan-src)# source vlan 315, 512
   (config-erspan-src)# destination ip 192.168.1.194
   ```

4. Turn on the monitor session:

   ```
   (config-erspan-src)# no shut
   ```

5. Make the configuration persistent:

   ```
   # copy runnin-config startup-config
   ```

The result is that you created a source ERSPAN session with ID 10. The switch will mirror the frames that are ingressing and egressing (both) the interface eth1/23 and VLANs 315 and 512. The outer GRE packet carrying the mirrored frame will have source IP address 192.168.1.1 and destination IP address 192.168.1.194. The source IP address must be the address of a Layer 3 interface on this switch. The destination IP address is one of the IP addresses that is configured on the ERSPAN VM.

### Supported ERSPAN Formats

The Cisco Tetration Analytics SPAN agents can process ERSPAN type I, II, and III packets that are described in the proposed ERSPAN RFC document. Therefore, the agents can process ERSPAN packets that are generated by Cisco devices. Among the non-RFC compliant formats, the agents can process the ERSPAN packets that are generated by a VMware vSphere Distributed Switch (VDS).
Performance Considerations When Configuring the ERSPAN Source

Carefully choose the ERSPAN source's port and VLAN list. Although the SPAN agent has two dedicated vCPUs, the session might generate a considerable amount of packets, which could saturate the processing power of the agent. If an agent is receiving more packets than it can process, the agent will be shown in the Agent Packet Misses graph on the cluster's Deep Visibility Agent page.

More fine-grained tuning on which frames the ERSPAN source will mirror can be achieved with ACL policies, usually by using the `filter` configuration keyword.

If the switch supports it, the ERSPAN source session can be configured to modify the maximum transport unit (MTU) of the ERSPAN packet, usually by using an `mtu` keyword. The default value is usually 1500 bytes. Decreasing the MTU will limit the ERSPAN bandwidth usage in your network infrastructure, but the MTU change will have no effect on the SPAN agent load, given that the agent's workload is on a per-packet basis. When reducing this value, allow room for 160 bytes for the mirrored frame. Refer to the proposed ERSPAN RFC for the ERSPAN header overhead details.

There are three versions of ERSPAN. The smaller the version, the lower the ERSPAN header overhead. Version II and III allow for applying QOS policies to the ERSPAN packets and provide some VLAN information. Version III provides even more settings. Version II is usually the default on Cisco switches. While Cisco Tetration Analytics SPAN agents support all three versions, at the moment they do not make use of any extra information that the ERSPAN version II and III packets carry.

Security Considerations for the Cisco Tetration Analytics ERSPAN Virtual Appliance

The following security considerations apply for the Cisco Tetration Analytics ERSPAN virtual appliance:

- The ERSPAN virtual machine guest operating system is CentOS 7.3, from which OpenSSL server and client packages were removed.
- After the VM is booted and the SPAN agent containers are deployed, no network interfaces, besides the loopback, will be present in the virtual machine. Therefore, the only way to access the appliance is by using its console. booting the VM for the first time takes a few of minutes to complete.
- The VM network interface is now moved inside the Docker containers. The containers run a Centos 7-based Docker image with no TCP/UDP port open.
- The containers are run with the base privileges (no `-privileged` option) plus the NET_ADMIN capability.
- In the unlikely case that a container is compromised, the VM guest OS should be safe from being compromised from inside the container.
- All of the other security considerations that are valid for Cisco Tetration Analytics agents that are running inside a host also apply to the Cisco Tetration Analytics SPAN agents that are running inside the Docker containers.

Troubleshooting Issues with the Cisco Tetration Analytics ERSPAN Virtual Appliance

After the SPAN agents enter the active state on the cluster Monitoring/Agent Overview page, you do not need to perform any action on the ERSPAN virtual machine. You do not need to log into the VM. If SPAN agents do not enter the active state or if the flows are not reported to the cluster, the information in this section will help you to pinpoint deployment problems.

Under normal conditions, on the VM, the following statements will be true:

- The directory `/mnt/sensor-rpm/` contains the `tet-sensor-<...>.span-x86_64.rpm` and the `ip_config` files.
- The `systemctl status tet-span-sensors` command reports an inactive service with the SUCCESS exit status.
- The `systemctl status tet-nic-driver` command reports an active service.
- The `docker network ls` command reports five networks: `host`, `none`, and three `erspan-<iface_name>`.
- The `ip link` command only reports the loopback interface.
- The `docker ps` command reports three running containers.
The **docker logs** `<cid>` command for each container contains the following message:

```
INFO success: tet-sensor entered RUNNING state, process has stayed up for > than 1 seconds (startsecs)
```

The **docker exec** `<cid>` `ifconfig` command reports only one interface, beside the loopback.

The **docker exec** `<cid>` `route -n` command reports the default gateway.

The **docker exec** `<cid>` `iptables -t raw -S PREROUTING` command reports the rule `-A PREROUTING -p gre -j DROP`.

If any of the above statements do not hold true, check the deployment script logs in `/usr/local/tet/log/sensor_container_setup.log` for the reason why the SPAN agent containers deployment failed.

You can troubleshoot any other agent registration or connectivity issue the same way that you do for agents running on a host by using the **docker exec** command:

- The **docker exec** `<cid>` `ps -ef` command reports the two `tet-engine`, `tet-engine check_conf` instances and two
  `/usr/local/tet/tet-sensor -f /usr/local/tet/conf/.sensor_config` instances, one with `root` user and one with `tet-sensor` user,
  along with the process manager `/usr/bin/python /usr/bin/supervisord -c /etc/supervisord.conf -n` instance.

- The **docker exec** `<cid>` `cat /usr/local/tet/tet-sensor.log` command shows the agent's logs.

- The **docker exec** `<cid>` `cat /usr/local/tet/fetch_sensor_id.log` command shows the agent's registration logs.

- The **docker exec** `<cid>` `cat /usr/local/tet/check_conf_update.log` command shows the configuration update polling logs.

If necessary, you can monitor traffic to and from the container with the **tcpdump** command after setting into the container's network namespace:

1. Retrieve the container's network namespace (SanboxKey):
   ```bash
docker inspect <cid> | grep SanboxKey
   ``
2. Set the container's network namespace:
   ```bash
   nsenter --net=/var/run/docker/netns/...
   ```
3. Monitor eth0 traffic:
   ```bash
tcpdump -i eth0 –n
   ```

---

**Cisco Tetration Analytics NetFlow Virtual Appliance**

The following sections provide procedures for and information about deploying the Cisco Tetration Analytics NetFlow virtual appliance.

**Deploying the Cisco Tetration Analytics NetFlow Virtual Appliance**

1. Download the Cisco Tetration Analytics NetFlow Virtual Machine Appliance OVA file from the Cisco CCO page.
2. Create a Virtual Machine from the OVA file and provision the VM with 8 single-threaded cores and 3 interfaces in bridged networking mode.
3. Download the `linux-amd64 -netflow` agent image bundle into a directory, which is referred to in this procedure as `<cfg_dir>`.
4. Add a `<cfg_dir>/ip_config` file containing the IPv4 and gateway address for each interface. The file must contain three rows in the following format:

   `<CIDR>/<gateway IP>`

   Example: `172.33.9.8/24 172.33.9.1`

   All interfaces must belong to the same subnet. Optionally, add a `<cfg_dir>/host_name` file containing the hostname string.

---

24
The ip_config file cannot contain any blank lines, including at the end of the file.

5. Create an ISO file using the following command:

   `mkisofs -r -o <name>.iso <cfg_dir>`

6. Add the ISO file to the VM as CDROM/DVD disc image.

7. Boot the VM.

Configuring NetFlow on the Switch

The following example steps are for a Cisco Nexus 9000 switch. The configuration steps might differ for other Cisco platforms; refer to the Cisco configuration guide for the Cisco platform that you are configuring.

1. Enter the configuration mode:

   ```
   # config terminal
   ```

2. Enable the NetFlow feature:

   ```
   (config)# feature netflow
   ```

3. Configure the flow record. The following commands configure the generation of 5-tuple information of a flow:

   ```
   (config)# flow record ipv4-records
   (config-flow-record)# description IPv4Flow
   (config-flow-record)# match ipv4 source address
   (config-flow-record)# match ipv4 destination address
   (config-flow-record)# match ip protocol
   (config-flow-record)# match transport source-port
   (config-flow-record)# match transport destination-port
   (config-flow-record)# collect transport tcp flags
   (config-flow-record)# collect counter bytes
   (config-flow-record)# collect counter packets
   ```

4. Configure the flow exporter to specify the NetFlow protocol version, template data interval, and NetFlow collector (the NetFlow agent) endpoint details:

   ```
   (config)# flow exporter flow-exporter-one
   (config-flow-exporter)# description NetFlowv9ToNetFlowAgent1
   (config-flow-exporter)# destination 192.168.1.173 use-vrf management
   (config-flow-exporter)# transport udp 4729
   (config-flow-exporter)# source mgmt0
   (config-flow-exporter)# version 9
   (config-flow-exporter-version-9)# template data timeout 20
   ```

5. Create a flow monitor and associate it with a flow record and flow exporter:

   ```
   (config)# flow monitor ipv4-monitor
   (config-flow-monitor)# description IPv4FlowMonitor
   (config-flow-monitor)# record ipv4-records
   (config-flow-monitor)# exporter flow-exporter-one
   ```

6. Apply the flow monitor to an interface. The following commands enable flow monitoring on all input packets on interface 1/1:

   ```
   (config)# interface Ethernet 1/1
   (config-if)# ip flow monitor ipv4-monitor input
   ```
The result is that you configured NetFlow on Nexus 9000 to export NetFlow v9 protocol packets for ingress traffic going through interface 1/1. The flow records will be sent to 192.168.1.173:4729 over the UDP protocol. Each flow record includes 5-tuple information of the traffic and the byte/packet count of the flow.

Security Considerations for the Cisco Tetration Analytics NetFlow Virtual Appliance

The following security considerations apply for the Cisco Tetration Analytics NetFlow virtual appliance:

- The ERSPAN virtual machine guest operating system is CentOS 7.3, from which OpenSSL server and client packages were removed.
- After the VM is booted and the SPAN agent containers are deployed, no network interfaces, besides the loopback, will be present in the virtual machine. Therefore, the only way to access the appliance is by using its console. Booting the VM for the first time takes a few of minutes to complete.
- The VM network interface is now moved inside the Docker containers. The containers run a Centos 7-based Docker image with no TCP/UDP port open.
- The containers are run with the base privileges (no -privileged option) plus the NET_ADMIN capability.
- In the unlikely case that a container is compromised, the VM guest OS should be safe from being compromised from inside the container.
- All of the other security considerations that are valid for Cisco Tetration Analytics agents that are running inside a host also apply to the Cisco Tetration Analytics SPAN agents that are running inside the Docker containers.

Troubleshooting Issues with the Cisco Tetration Analytics NetFlow Virtual Appliance

After the NetFlow agents enter the active state on the cluster Monitoring/Agent Overview page, you do not need to perform any action on the NetFlow virtual machine. You do not need to log into the VM. If NetFlow agents do not enter the active state or if the flows are not reported to the cluster, the information in this section will help you to pinpoint deployment problems.

Under normal conditions, on the VM, the following statements will be true:

- The directory /mnt/sensor-rpm/ contains the tet-sensor-<version>-netflow-linux-amd64-<cluster_name>.rpm and the ip_config files.
- The systemctl status tet-span-sensors command reports an inactive service with the SUCCESS exit status.
- The systemctl status tet-nic-driver command reports an active service.
- The docker network ls command reports five networks: host, none, and three nflow-<iface_name>.
- The ip link command only reports the loopback interface.
- The docker ps command reports three running containers.
- The docker exec <cid> ifconfig command reports only one interface, beside the loopback.
- The docker exec <cid> netstat -rn command reports the default gateway.
- The docker exec <cid> iptables -S INPUT command reports the rule -P INPUT ACCEPT.
- The docker exec <cid> iptables -L INPUT -v command reports the current statistics of the network traffic.

If any of the above statements do not hold true, check the deployment script logs in /usr/local/tet/netflow_containers_setup.log for the reason why the SPAN agent containers deployment failed.
You can troubleshoot any other agent registration or connectivity issue the same way that you do for agents running on a host by using the `docker exec` command:

- The `docker exec <cid> ps -ef` command reports the `tet-netflowsensor-engine` and `/usr/local/tet/tet-netflowsensor -config /usr/local/tet-netflow/conf/tet-netflow.conf` instances, along with the process manager `/usr/bin/supervisord -c /usr/local/tet-netflow/conf/supervisord.conf -n` instance.
- The `docker exec <cid> cat /local/tetration/logs/tet-netflow.log` command shows the agent’s logs.
- The `docker exec <cid> cat /local/tetration/logs/check_conf_update.log` command shows the configuration update polling logs.

**Cisco Tetration Analytics Citrix NetScaler AppFlow Collector Virtual Appliance**

The following sections provide procedures for and information about deploying the Cisco Tetration Analytics Citrix NetScaler AppFlow Collector virtual appliance.

### Deploying the Cisco Tetration Analytics Citrix NetScaler AppFlow Collector Virtual Appliance

2. Create a Virtual Machine from the OVA file and provision the VM with 8 single-threaded cores and 3 interfaces in bridged networking mode.
3. Download the `linux-amd64 -netscaler` agent image bundle into a directory, which is referred to in this procedure as `<cfg_dir>`.
4. Add a `<cfg_dir>/ip_config` file containing the IPv4 and gateway address for each interface. The file must contain three rows in the following format:

   `<CIDR>/<gateway IP>

   Example: 172.33.9.8/24 172.33.9.1

   All interfaces must belong to the same subnet. Optionally, add a `<cfg_dir>/host_name` file containing the hostname string.

   The `ip_config` file cannot contain any blank lines, including at the end of the file.
5. Create an ISO file using the following command:

   `mkisofs -r -o <name>.iso <cfg_dir>`

6. Add the ISO file to the VM as CDROM/DVD disc image.
7. Boot the VM.

### Configuring AppFlow on Citrix NetScaler

The following example steps are for a Citrix NetScaler load balancer.

1. Enable AppFlow on Citrix NetScaler:

   `enable ns feature appflow`

2. Add the AppFlow collector endpoints. The collector receives the AppFlow records from the Citrix NetScaler.

   `add appflow collector c1 -IPAddress 192.168.1.173 -port 4739`

   `add appflow collector c2 –IPAddress 192.168.1.174 -port 4739`

3. Configure an AppFlow action. The action lists the collectors that will get AppFlow records if the associated AppFlow policy matches.

   `add appflow action a1 -collectors c1`
add appflow action a2 -collectors c2

4. Configure an AppFlow policy. The policy is a rule that must match for the AppFlow record to be generated.

add appflow policy p1 CLIENT.TCP.DSTPORT(22) a1
add appflow policy p2 HTTP.REQ.URL.SUFFIX.EQ("jpeg") a2

5. Bind AppFlow policy to a specific LB vserver. Traffic hitting the VIP of this vserver will be evaluated for the AppFlow policy match. On a match, a flow record is generated and sent to all the collectors listed in the associated AppFlow action.

bind lb vserver lb1 -policyname p1 -priority 10

6. An AppFlow policy could also be bound globally to all vservers. This policy applies to all traffic that flows through the NetScaler.

bind appflow global p2 1 NEXT -type REQ_DEFAULT

7. Optionally, set the AppFlow template refresh interval. The default is 60 seconds.

set appflow param -templatereferesh 60

The result is that you configured AppFlow on a Citrix NetScaler load balancer to export IPFIX protocol packets for ingress traffic going through the Citrix NetScaler load balancer. The flow records will be sent to 192.168.1.173:4729 for traffic going through vserver lb1 or to 192.168.1.174:4739 for all traffic going through the Citrix NetScaler load balancer. Each flow record includes 5-tuple information of the traffic and the byte/packet count of the flow.

Security Considerations for the Cisco Tetration Analytics Citrix NetScaler AppFlow Collector Virtual Appliance

The following security considerations apply for the Cisco Tetration Analytics Citrix NetScaler AppFlow Collector virtual appliance:

- The ERSPAN virtual machine guest operating system is CentOS 7.3, from which OpenSSL server and client packages were removed.
- After the VM is booted and the SPAN agent containers are deployed, no network interfaces, besides the loopback, will be present in the virtual machine. Therefore, the only way to access the appliance is by using its console. Booting the VM for the first time takes a few of minutes to complete.
- The VM network interface is now moved inside the Docker containers. The containers run a Centos 7-based Docker image with no TCP/UDP port open.
- The containers are run with the base privileges (no -privileged option) plus the NET_ADMIN capability.
- In the unlikely case that a container is compromised, the VM guest OS should be safe from being compromised from inside the container.
- All of the other security considerations that are valid for Cisco Tetration Analytics agents that are running inside a host also apply to the Cisco Tetration Analytics SPAN agents that are running inside the Docker containers.

Troubleshooting Issues with the Cisco Tetration Analytics Citrix NetScaler AppFlow Collector Virtual Appliance

After the Citrix NetScaler agents enter the active state on the cluster Monitoring/Agent Overview page, you do not need to perform any action on the AppFlow Collector virtual machine. You do not need to log into the VM. If Citrix NetScaler agents do not enter the active state or if the flows are not reported to the cluster, the information in this section will help you to pinpoint deployment problems.

Under normal conditions, on the VM, the following statements will be true:

- The directory /mnt/sensor-rpm/ contains the tet-sensor-<version>-netscaler-linux-amd64.<cluster_name>.rpm and the ip_config files.
- The systemctl status tet-netscaler-sensors command reports an inactive service with the SUCCESS exit status.
The `systemctl status tet-nic-driver` command reports an active service.

The `docker network ls` command reports five networks: `host`, `none`, and three `netscaler-<iface_name>`.

The `ip link` command only reports the loopback interface.

The `docker ps` command reports three running containers.

The `docker logs <cid>` command for each container contains the following message:

```
INFO success: tet-sensor entered RUNNING state, process has stayed up for > than 1 seconds (startsecs)
```

The `docker exec <cid> ifconfig` command reports only one interface, beside the loopback.

The `docker exec <cid> netscaler -rn` command reports the default gateway.

The `docker exec <cid> iptables -S INPUT` command reports the rule `-P INPUT ACCEPT`.

The `docker exec <cid> iptables -L INPUT -v` command reports the current statistics of the network traffic.

If any of the above statements do not hold true, check the deployment script logs in `/usr/local/tet/netscaler_containers_setup.log` for the reason why the Citrix NetScaler agent containers deployment failed.

You can troubleshoot any other agent registration or connectivity issue the same way that you do for agents running on a host by using the `docker exec` command:

- The `docker exec <cid> ps -ef` command reports the `tet-netscalersensor-engine` and `/usr/local/tet/tet-netscalersensor -config /usr/local/tet/netscaler/conf/tet-netscaler.conf` instances, along with the process manager `/usr/bin/supervisord -c /usr/local/tet/netscaler/conf/supervisord.conf -n instance`.

- The `docker exec <cid> cat /local/tetration/logs/tet-netscaler.log` command shows the agent's logs.

- The `docker exec <cid> cat /local/tetration/logs/check_conf_update.log` command shows the configuration update polling logs.

Cisco Tetration Analytics F5 BIG-IP Collector Virtual Appliance

The following sections provide procedures for and information about deploying the Cisco Tetration Analytics F5 BIG-IP Collector virtual appliance.

Deploying the Cisco Tetration Analytics F5 BIG-IP Collector Virtual Appliance

1. Download the Cisco Tetration Analytics F5 BIG-IP Collector Virtual Machine Appliance OVA file from the Cisco CCO page.

2. Create a Virtual Machine from the OVA file and provision the VM with 8 single-threaded cores and 3 interfaces in bridged networking mode.

3. Download the `linux-amd64-f5` agent image bundle into a directory, which is referred to in this procedure as `<cfg_dir>`.

4. Add a `<cfg_dir>/ip_config` file containing the IPv4 and gateway address for each interface. The file must contain three rows in the following format:

   `<CIDR>gateway IP`

   Example: `172.33.9.8/24 172.33.9.1`

   All interfaces must belong to the same subnet. Optionally, add a `<cfg_dir>/host_name` file containing the hostname string.

   The ip_config file cannot contain any blank lines, including at the end of the file.

5. Create an ISO file using the following command:

   `mkisofs -r -o <name>.iso <cfg_dir>`
6. Add the ISO file to the VM as CDROM/DVD disc image.

7. Boot the VM.

Configuring IPFIX on F5 BIG-IP

The following example steps are for a F5 BIG-IP load balancer.

1. Create a pool of IPFIX collectors.

On the F5 BIG-IP appliance, create the pool of IPFIX collectors. These are the IP addresses that are configured on the Cisco Tetration Analytics appliance. F5 BIG-IP IPFIX collector VM. The F5 BIG-IP agents running in Docker containers on the VM listen on port 4739 for IPFIX packets.

2. Create a log-destination.

The log destination configuration on F5 BIG-IP appliance specifies the actual pool of IPFIX collectors that should be used.

3. Create a log-publisher.

A log publisher specifies where F5 BIG-IP sends the IPFIX messages. The publisher is bound with a log-destination.

4. Add a F5 and Cisco Tetration Analytics approved iRule.

Tetration and F5 developed two iRules that will export flow records to Cisco Tetration Analytics F5 BIG-IP agents. These iRules will export complete information about a given transaction: including all the endpoints, byte and packet counts, flow start and end time (in milliseconds). F5 BIG-IP agents will create 4 independent flows and match each flow with its related flow.

5. Add the iRule to the virtual server.

In the iRule settings of a virtual server, add the Cisco Tetration Analytics approved iRule to the virtual server.

The result is that you configured IPFIX on an F5 BIG-IP load balancer to export IPFIX protocol packets for traffic going through the appliance.

The following example shows an F5 BIG-IP configuration:

```bash
root@localhost(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config ltm virtual vip-1 rules ltm virtual vip-1 {
  rules {
    ipfix-rule-1
  }
}
root@localhost(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config ltm pool ipfix-pool-1 ltm pool ipfix-pool-1 {
  members {
    10.28.118.6:ipfix {
      address 10.28.118.6 session monitor-enabled state up
    }
    monitor gateway_icmp
  }
}
root@localhost(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config ltm virtual vip-1 rules ltm virtual vip-1 {
  rules {
    ipfix-rule-1
  }
}
root@localhost(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config sys log-config sys log-config destination ipfix ipfix-collector-1 {
  pool-name ipfix-pool-1
  [ transport-profile udp
  ]
sys log-config publisher ipfix-pub-1 {
  destinations {
```
In the example, flow records will be published to ipfix-pub-1. ipfix-pub-1 is configured with log-destination ipfix-collector-1, which sends the IPFIX messages to IPFIX pool ipfix-pool-1. ipfix-pool-1 has 10.28.118.6 as one of the IPFIX collectors. The virtual server vip-1 is configured with IPFIX iRule ipfix-rule-1, which specifies the IPFIX template and how the template gets filled and sent.

You can download the F5 and Cisco Tetration Analytics-approved iRules from your Cisco Tetration Analytics cluster's documentation page. Before using an iRule, update the log-publisher to point to the log-publisher that you configured in the F5 BIG-IP appliance where the iRule will be added.

F5 has published the following GitHub repository to help users get started with flow-stitching:

https://github.com/f5devcentral/f5-tetration

The iRules for publishing IPFIX records to the Cisco Tetration Analytics F5 sensor for various protocol types are available at the following location:

https://github.com/f5devcentral/f5-tetration/irules

Visit this site for latest iRule definitions. In addition, F5 also developed a script that performs the following tasks:

1. Installs the correct iRule for the virtual servers.
2. Adds a pool of IPFIX collector endpoints where Cisco Tetration Analytics F5 sensors listen for IPFIX records.
3. Configures the log-collector and log-publisher.
4. Binds the correct iRule to the virtual servers.

This tool minimizes manual configuration and user error while enabling the flow-stitching use-case. The script is available at the following location:

https://github.com/f5devcentral/f5-tetration/scripts

Security Considerations for the Cisco Tetration Analytics F5 BIG-IP Collector Virtual Appliance

The following security considerations apply for the Cisco Tetration Analytics F5 BIG-IP Collector virtual appliance:

- The F5 BIG-IP Collector virtual machine guest operating system is CentOS 7.3, from which OpenSSL server and client packages were removed.
- After the VM is booted and the F5 BIG-IP agent containers are deployed, no network interfaces, besides the loopback, will be present in the virtual machine. Therefore, the only way to access the appliance is by using its console. Booting the VM for the first time takes a few of minutes to complete.
- The VM network interface is now moved inside the Docker containers. The containers run a Centos 7-based Docker image with no TCP/UDP port open.
- The containers are run with the base privileges (no -privileged option) plus the NET_ADMIN capability.
- In the unlikely case that a container is compromised, the VM guest OS should be safe from being compromised from inside the container.
- All of the other security considerations that are valid for Cisco Tetration Analytics agents that are running inside a host also apply to the F5 BIG-IP agents that are running inside the Docker containers.

Troubleshooting Issues with the Cisco Tetration Analytics F5 BIG-IP Collector Virtual Appliance

After the F5 BIG-IP agents enter the active state on the cluster Monitoring/Agent Overview page, you do not need to perform any action on the F5 BIG-IP IPFIX Collector virtual machine. You do not need to log into the VM. If F5 BIG-IP agents do not enter the active state or if the flows are not reported to the cluster, the information in this section will help you to pinpoint deployment problems.
Under normal conditions, on the VM, the following statements will be true:

- The directory `/mnt/sensor-rpm/` contains the `tet-sensor-<version>-f5-linux-amd64-<cluster_name>.rpm` and the `ip_config` files.
- The `systemctl status tet-f5-sensors` command reports an inactive service with the SUCCESS exit status.
- The `systemctl status tet-nic-driver` command reports an active service.
- The `docker network ls` command reports five networks: `host`, `none`, and three `f5-<iface_name>`.
- The `ip link` command only reports the loopback interface.
- The `docker ps` command reports three running containers.
- The `docker logs <cid>` command for each container contains the following message:
  ```
  INFO success: tet-sensor entered RUNNING state, process has stayed up for > than 1 seconds (startsecs)
  ```
- The `docker exec <cid> ifconfig` command reports only one interface, beside the loopback.
- The `docker exec <cid> f5 -rn` command reports the default gateway.
- The `docker exec <cid> iptables -S INPUT` command reports the rule `-P INPUT ACCEPT`.
- The `docker exec <cid> iptables -L INPUT -v` command reports the current statistics of the network traffic.

If any of the above statements do not hold true, check the deployment script logs in `/usr/local/tet/f5_containers_setup.log` for the reason why the F5 BIG-IP agent containers deployment failed.

You can troubleshoot any other agent registration or connectivity issue the same way that you do for agents running on a host by using the `docker exec` command:

- The `docker exec <cid> ps -ef` command reports the `tet-f5sensor-engine` and `/usr/local/tet/tet-f5sensor -config /usr/local/tet-f5/conf/tet-f5.conf` instances, along with the process manager `/usr/bin/supervisord -c /usr/local/tet-f5/conf/supervisord.conf -n` instance.
- The `docker exec <cid> cat /local/tetration/logs/tet-f5.log` command shows the agent's logs.
- The `docker exec <cid> cat /local/tetration/logs/check_conf_update.log` command shows the configuration update polling logs.

Reference Information

For more information about the Cisco Tetration Analytics software, go to the following URLs:


Appendix: Microsoft Server DLLs

The DLLs that are installed are as part of Cisco Tetration Analytics are from 3rd party open source software. The DLLs are installed in the `C:\Program Files\Cisco Tetration\` directory by default.

- 7-Zip:
  - 7z.dll
Open Source:
- iconv.dll
- libcrypto.dll
- libssl.dll

Microsoft:
- msvcr120.dll
- msvcp120.dll

OpenSSL:
- ssleay32.dll
- libeay32.dll
- libssl32.dll

Npcap:
- %SYSTEMROOT%\System32\wpcap.dll
- Packet.dll
- npcap.sys
- NPFInstall.exe
- NpcapHelper.exe
- WlanHelper.exe
Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What’s New in Cisco Product Documentation at:

Subscribe to What’s New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.
Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017-2018 Cisco Systems, Inc. All rights reserved.