Cisco Tetration Release Notes Release 3.2.1.31

This document describes the features, compatibility, scalability, usage guidelines, caveats, bug fixes and any behavior changes for the Cisco Tetration software patch release 3.2.1.31. This patch is associated with the Tetration software major release 3.2.1.20. Details of the major release can be found here: https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_2_1_20.html.

Release Notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of this document:

https://www.cisco.com/c/en/us/support/security/tetration/products-release-notes-list.html

Table 1 Change History for this Document

Date	Description
Dec 17, 2021	Release 3.2.1.31 became available.

Contents

This document includes the following sections:

- New and Changed Information
- Caveats
- Compatibility Information
- Usage Guidelines
- Verified Scalability Limits
- Related Documentation

New and Changed Information

This section lists the new and changed features in this release and includes the following topics:

- New Software Features
- Enhancements
- Changes in Behavior

Cisco Tetration Release Notes
Release 3.2.1.31

New Software Features

- This patch release does not include any new software features.

Enhancements

- This patch release does not include any new feature enhancements.

Changes in Behavior

- This patch release does not include any changes in behavior.

Caveats

This section contains lists of open and resolved caveats, as well as known behaviors.

- Open Caveats
- Resolved Caveats
- Known Behaviors

Open Caveats

This patch release does not have any new open caveats.

Resolved Caveats

The following table lists the resolved caveats in this release. Click a bug ID to access Cisco's Bug Search Tool to see additional information about that bug.

Table 3 Resolved Caveats

Bug ID	Description
CSCwa48895	FabricPath is not displayed correctly in scenario with two ACI fabric connected to Tetration Cluster

Known Behaviors

There are no changes to the known behaviors for this patch release. Known behavior details for the major release 3.2.1.20 can be found here: https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_2_1_20.html.

Compatibility Information

There is no new software agent support included in this patch release. For the full list of supported software agents, see the 3.2.1.20 release notes: https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_2_1_20.html.

This release supports the following Cisco Nexus 9000 series switches in NX - OS and Cisco Application Centric Infrastructure (ACI) mode:

Table 4 Supported Cisco Nexus 9000 Series Switches in NX-OS and ACI Mode

Product line	Platform	Minimum Software release
Cisco Nexus 9300 platform switches (NX - OS mode)	Cisco Nexus 93180YC- EX, 93108TC- EX, and 93180LC - EX	Cisco NX- OS Release 9.2.1 and later
	Cisco Nexus 93180YC - FX, 93108TC- FX, and 9348GC- FXP	Cisco NX- OS Release 9.2.1 and later
	Cisco Nexus 9336C - FX2	Cisco NX- OS Release 9.2.1 and later
Cisco Nexus 9300 platform switches (ACI mode)	Cisco Nexus 93180YC - EX, 93108TC- EX, and 93180LC - EX	Cisco ACI Release 3.1(1i) and later
	Cisco Nexus 93180YC - FX, 93108TC- FX**	Cisco ACI Release 3.1(1i) and later
	Cisco Nexus 9348GC - FXP	Cisco ACI Release 3.1(1i) and later
	Cisco Nexus 9336C- FX2	Cisco ACI Release 3.2 and later
	Cisco Nexus 9500 series switches with N9K - X9736C- FX linecards only	Cisco ACI Release 3.1 (1i) and later

**Network performance features using hardware sensors are supported only in Cisco ACI mode with release 3.1 or later.

Usage Guidelines

This section lists usage guidelines for the Cisco Tetration software.

- You must use the Google Chrome browser version 40.0.0 or later to access the web-based user interface.
- After setting up your DNS, browse to the URL of your Cisco Tetration cluster: https://<cluster.domain>

Verified Scalability Limits

The following tables provide the scalability limits for Cisco Tetration (39 - RU), Cisco Tetration - M (8- RU), and Cisco Tetration Cloud:

Table 5 Scalability Limits for Cisco Tetration (39 - RU)

Configurable Option	Scale
Number of workloads	Up to 25,000 (VM or Baremetal)
Flow features per second	Up to 2 Million
Number of hardware sensor enabled Cisco Nexus 9000 series switches	Up to 100

Note: Supported scale will always be based on whichever parameter reaches the limit first

Table 6 Scalability Limits for Cisco Tetration - M (8- RU)

Configurable Option	Scale
Number of workloads	Up to 5,000 (VM or Baremetal)
Flow features per second	Up to 500,000
Number of hardware sensor enabled Cisco Nexus 9000 series switches	Up to 100

Note: Supported scale will always be based on whichever parameter reaches the limit first

Table 7 Scalability Limits for Cisco Tetration Virtual (VMWare ESXi)

Configurable Option	Scale
Number of workloads	Up to 1,000 (VM or Baremetal)
Flow features per second	Up to 70,000

Number of hardware sensor enabled Cisco Nexus 9000 series switches	Not supported

Note: Supported scale will always be based on whichever parameter reaches the limit first.

Related Documentation

The Cisco Tetration Analytics documentation can be accessed from the following websites:

Tetration Analytics Platform Datasheet: https://www.cisco.com/c/en/us/products/security/tetration/datasheet-listing.html.

General Documentation: http://www.cisco.com/c/en/us/support/data-center-analytics/tetration-analytics/tsd-products-support-series-home.html

The documentation includes installation information and release notes.

Table 8 Installation Documentation

Document	Description
Cisco Tetration Analytics Cluster Deployment Guide	Describes the physical configuration, site preparation, and cabling of a single- and dual-rack installation for Cisco Tetration (39-RU) platform and Cisco Tetration-M (8-RU). https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/hw/installation_guide/Cisco-Tetration-Analytics-Cluster-Hardware-Deployment-Guide.html
Cisco Tetration Virtual Deployment Guide	Describes the deployment of Tetration virtual appliance. https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/install/b_Tetration_Analytics_Virtual_Appliance_Deployment_Guide.html
Cisco Tetration Cluster Upgrade Guide	https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/install/b_Tetration_Analytics_Upgrade_Guide.html NOTE: As a best practice, it's always recommended to patch cluster to latest available patch version before performing major version upgrade.
Latest Threat Data Sources	https://updates.tetrationcloud.com/

Cisco Tetration Release Notes
Release 3.2.1.31

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)

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.

© 2019-2021 Cisco Systems, Inc. All rights reserved.