Cisco Tetration Release Notes Release 3.4.1.34

This document describes the features, bug fixes and any behavior changes for the Cisco Tetration software patch release 3.4.1.34. This patch is associated with the Tetration software major release 3.4.1.1. 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_4_1_1.html.

These 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

The following table shows the online change history for this document.

Table 1 Online History Change

Date	Description
June 8, 2021	Release 3.4.1.34 became available.

Contents

This document includes the following sections:

New and Changed Information

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

New Software Features

- There are no new software features in this patch release.

Enhancements

- External Orchestrators Integration for Kubernetes will no longer ingest annotations from Kubernetes objects.

Changes in Behavior

- The run_signed explore endpoint no longer requires a snapshot restart to allow signed scripts to be run multiple times in a row.
- The DiskUsageCritical and DiskUsageWarning service statuses now properly take reserved disk space into account and monitor the following partitions on all cluster nodes:
  - local
  - tmp
  - root
  - var-log

Caveats

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

Open Caveats

There are no known open caveats in this patch release.

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 4 Resolved Caveats

Bug ID	Description
CSCvx15078	Conversations in ADM/Segmentation may display `Filter Unknown`
CSCvw64156	Tetration connector appliance NTP settings may result in inability to sync ntp.
CSCvw63840	Include "./storcli64 /c0 /eall /sall show all J" output in snapshot

CSCvx65882	HW Agent (ACI mode) restarts every 24 hours
CSCvx65896	HW Agent (ACI mode) unintentionally restarts
CSCvu90994	Hardware agents (leaf switches) are not getting auto-upgraded post patch upgrade
CSCvk70127	Fwdinst is not created on spine after enabling Analytics on ifav2-spine2
CSCvk76423	log flood on ta_agent.log for Sugarbowl tor after reload
CSCvw82285	Last Check-in time is kept updating even after Hardware Agent is down
CSCvw78266	Tetration `ta_agent` may crash without VRF or `analytics cluster` configuration
CSCvy04426	[ISE] When session topic is not available add retries

Known Behaviors

No known behaviors in this patch

Compatibility Information

The software agents in the 3.4.1.34 release support the following operating systems (virtual machines and bare-metal servers) for micro segmentation (deep visibility and enforcement):

- Linux:
  - CentOS-6.x: 6.1 to 6.10
  - CentOS-7.x: 7.0 to 7.8
  - CentOS-8.x: 8.0 to 8.2
  - Red Hat Enterprise Linux-6.x: 6.1 to 6.10
  - Red Hat Enterprise Linux-7.x: 7.0 to 7.9
  - Red Hat Enterprise Linux-8.x: 8.0 to 8.3
  - Oracle Linux Server-6.x: 6.1 to 6.10
  - Oracle Linux Server-7.x: 7.0 to 7.8
  - Oracle Linux Server-8.x: 8.0 to 8.2
  - SUSE Linux-11.x: 11.2, 11.3, and 11.4
  - SUSE Linux-12.x: 12.0, 12.1, 12.2, 12.3, 12.4 and 12.5
  - SUSE Linux-15.x: 15.0, 15.1 and 15.2
  - Ubuntu-14.04
  - Ubuntu-16.04
  - Ubuntu-18.04
  - Ubuntu-20.04
- Windows Server (64-bit):
  - Windows Server 2008R2 Datacenter
  - Windows Server 2008R2 Enterprise

  - Windows Server 2008R2 Essentials
  - Windows Server 2008R2 Standard
  - Windows Server 2012 Datacenter
  - Windows Server 2012 Enterprise
  - Windows Server 2012 Essentials
  - Windows Server 2012 Standard
  - Windows Server 2012R2 Datacenter
  - Windows Server 2012R2 Enterprise
  - Windows Server 2012R2 Essentials
  - Windows Server 2012R2 Standard
  - Windows Server 2016 Standard
  - Windows Server 2016 Essentials
  - Windows Server 2016 Datacenter
  - Windows Server 2019 Standard
  - Windows Server 2019 Essentials
  - Windows Server 2019 Datacenter
- Windows VDI desktop Client:
  - Microsoft Windows 8
  - Microsoft Windows 8 Pro
  - Microsoft Windows 8 Enterprise
  - Microsoft Windows 8.1
  - Microsoft Windows 8.1 Pro
  - Microsoft Windows 8.1 Enterprise
  - Microsoft Windows 10
  - Microsoft Windows 10 Pro
  - Microsoft Windows 10 Enterprise
  - Microsoft Windows 10 Enterprise 2016 LTSB
- IBM AIX operating system (Beta):
  - AIX version 7.1
  - AIX version 7.2
- Container host OS version for policy enforcement:
  - Red Hat Enterprise Linux Release 7.1, 7.2, 7.3, 7.4, 7.7
  - CentOS Release 7.1, 7.2, 7.3, 7.4, 7.7
  - Ubuntu-16.04

The 3.4.1.34 release supports the following operating systems for visibility use cases only:

- Linux:
  - CentOS-5.x: 5.7 to 5.11
  - Red Hat Enterprise Linux-5.x: 5.7 to 5.11

The 3.4.1.34 release supports the following operating systems for the universal visibility agent:

- Red Hat Enterprise Linux 4.0 (32-bit and 64-bit)
- CentOS 4.0 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.0 (32-bit)
- CentOS 5.0 (32-bit)
- Windows Server (32-bit and 64-bit)
- Solaris 11 on x86 (64-bit)
- AIX 5.3 (PPC)

The 3.4.1.34 release supports the following Cisco Nexus 9000 series switches in NX-OS and Cisco Application Centric Infrastructure (ACI) mode:

Table 5 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

Usage Guidelines

This section lists usage guidelines for the Cisco Tetration Analytics 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 Analytics 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-V (virtual):

Table 6 Scalability Limits for Cisco Tetration (39-RU)

Configurable Option	Scale

Number of workloads	Up to 25,000 (VM or bare-metal)
Flow features per second	Up to 2 Million
Number of hardware agent enabled Cisco Nexus 9000 series switches	Up to 100

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

Table 7 Scalability Limits for Cisco Tetration-M (8-RU)

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

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

Table 8 Scalability Limits for Cisco Tetration Virtual (VMWare ESXi)

Configurable Option	Scale
Number of workloads	Up to 1,000 (VM or bare-metal)
Flow features per second	Up to 70,000
Number of hardware agent enabled Cisco Nexus 9000 series switches	Not supported

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

Related Documentation

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

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

General Documentation: https://www.cisco.com/c/en/us/support/security/tetration/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). Document Link: https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/hw/installation_guide/Cisco-Tetration-M5-Cluster-

	Hardware-Deployment-Guide.html
Cisco Tetration Virtual Deployment Guide	Describes the deployment of Tetration virtual appliance. Document Link: 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	Document Link: https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/install/b_Tetration_Analytics_Upgrade_Guide.html
Latest Threat Data Sources	https://updates.tetrationcloud.com/