Cisco Tetration Release Notes Release 3.5.1.20

This document describes the features, caveats, and limitations for the Cisco Tetration software, release 3.5.1.20.

This document describes the features, bug fixes and any behavior changes for the Cisco Tetration software patch release 3.5.1.20. This patch is associated with the Tetration software major release 3.5.1.17. 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_5_1_17.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

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

Table 1 Online History Change

Date	Description
June 8, 2021	Release 3.5.1.20 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

- No new software features in this patch release

Enhancements

- No new enhancements in this patch release

Changes in Behavior

- No changes in platform behavior

Caveats

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

Open Caveats

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

Table 2 Open Caveats

Bug ID	Description
CSCvx47947	Kubernetes daemonset agent uninstall requires jq utility
CSCvx48421	(Static Enforcement) Pausing enforcement policy update is not supported in the federation setup in the current release.
CSCvx29180	Kubernetes traffic from the host network to cluster ip services escapes Tetration policies.

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
CSCvy09666	Agent having Addresses 10.1.[0-X].0/24 can't connect to collectors post 3.5 upgrade

CSCvx80046	For SNOW connector add additional parameter to rest api call to prevent format issues
CSCvx81976	Tetration Agent Upgrade API is broken
CSCvy04426	[ISE] When session topic is not available add retries
CSCvy10749	Quick analysis and policy analysis show incorrect results for windows agents running in WFP mode
CSCvy23789	Uninstalling the agent is removing the tetration rules on enforced workloads
CSCvy36816	Host based CIMC firmware upgrade may fail on M5 clusters
CSCvy36864	Host based CIMC firmware upgrade may fail during BIOS staging
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 with out VRF or `analytics cluster` configuration

Known Behaviors

- Refer to Cisco Tetration software major release 3.5.1.17 release notes - https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_5_1_17.html.

Compatibility Information

The software agents in the 3.5.1.20 release support the following operating systems (virtual machines and bare-metal servers) for micro segmentation (deep visibility and enforcement):

- Linux:
  - Amazon Linux 2
  - CentOS-6.x: 6.1 to 6.10
  - CentOS-7.x: 7.0 to 7.9
  - CentOS-8.x: 8.0 to 8.3
  - 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 7.9
- Oracle Linux Server-8.x: 8.0 to 8.3
- SUSE Linux-11.x: 11.2 to 11.4
- SUSE Linux-12.x: 12.0 to 12.5
- SUSE Linux-15.x: 15.0 to 15.2
- Ubuntu-14.04
- Ubuntu-16.04
- Ubuntu-18.04
- Ubuntu-20.04

- Linux on IBM Z:
  - Red Hat Enterprise Linux-7.x: 7.3 to 7.9
  - Red Hat Enterprise Linux-8.x: 8.2 to 8.3
  - SUSE Linux-11.x: 11.4
  - SUSE Linux-12.x: 12.4 to 12.5
  - SUSE Linux-15.x: 15.0 to 15.2

- 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 8.1
  - 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:
  - AIX version 7.1
  - AIX version 7.2

- Container host OS version for policy enforcement:
  - Red Hat Enterprise Linux Release 7.1 to 7.7
  - CentOS Release 7.1 to 7.7
  - Ubuntu-16.04

The 3.5.1.20 release supports the following operating systems for deep visibility use cases only:

- Windows VDI desktop Client:
  - Microsoft Windows 7
  - Microsoft Windows 7 Pro
  - Microsoft Windows 7 Enterprise

The 3.5.1.20 release supports the following operating systems for the universal visibility agent:

- Windows Server (32-bit and 64-bit where deep visibility agent is not available)
- AIX 6.1 (PPC)

The 3.5.1.20 release no longer support the following operating systems for any software agent:

- Red Hat Enterprise Linux Release 5.x
- CentOS Release 5.x
- AIX 5.3 (PPC)
- Solaris 11 on x86 (64-bit)
- Microsoft Windows 8

The 3.5.1.20 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

Usage Guidelines

- Refer to Cisco Tetration software major release 3.5.1.17 release notes - https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_5_1_17.html.

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 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 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 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 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 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 Analytics Platform Datasheet: http://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-737256.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/m5_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	Documentation Link: 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/