Cisco Tetration Release Notes

Release 3.3.2.5

This document describes the features, caveats, and limitations for the Cisco Tetration software, release 3.3.2.5.

The Cisco Tetration platform is designed to comprehensively address a number of data center operational and security challenges using rich traffic telemetry collected from servers, layer 4 through 7 service elements, and end-point devices (such as laptops, desktops, and smartphones). The platform performs advanced analytics using an algorithmic approach to offer a holistic workload protection platform. This algorithmic approach includes unsupervised machine-learning techniques and behavioral analysis. The platform provides a ready-to-use solution supporting the following use cases:

- Provide behavior-based application insight to automate Allow-list policy generation
- Provide application segmentation to enable efficient and secure zero-trust implementation
- Provide consistent policy enforcement across on-premises data centers, and private and public clouds
- Identify process behavior deviations, and software vulnerabilities and exposure to reduce attack surface
- Identify application behavior changes and policy compliance deviations in near-real time
- Support comprehensive telemetry processing in a heterogeneous environment to provide actionable insight within minutes
- Comprehensive network performance metrics based on the telemetry collected from both switches and servers
- Enable long-term data retention for deep forensics, analysis, and troubleshooting

To support the analysis and various use cases within the Cisco Tetration Analytics platform, consistent telemetry is required from across the data center infrastructure. Rich Cisco Tetration Analytics telemetry is collected using agents. There are different types of agents available to support both existing and new data center infrastructures. This release supports the following agent types:

- Software agents installed on virtual machine, bare-metal, or container hosts
- Embedded hardware agents in Cisco Nexus 9000 CloudScale series switches
- ERSPAN agents that can generate Cisco Tetration telemetry from copied packets
- NetFlow agents that can generate Cisco Tetration telemetry based on NetFlow v9 or IPFIX records
- Cisco AnyConnect and Cisco ISE integrations to collect telemetry from endpoints, such as laptops, desktops, and smartphones

Software agents also act as the policy enforcement point for the application segmentation. Using this approach, the Cisco Tetration platform enables consistent microsegmentation across public, private, and on-premises deployments. Agents enforce policy using native operating system capabilities, thereby eliminating the need for the agent to be in the data path, and providing a fail-safe option. Additional product documentation is listed in the "Related Documentation" section.

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
October 24, 2019	Release 3.3.2.5 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
- Changes in Behavior

New Software Features

The following new features are included in this patch release:

- Software agent support for visibility and enforcement is now available for Windows 10 Enterprise 2016 LTSB
- Forensics feature for SUSE Linux15 is now available

Changes in Behavior

These are behavior changes for this release:

- The performance monitoring dashboard is now enabled for all platforms
- The fabric monitoring feature requires an activation key; if you were using this feature prior to this release or bought Tetration for its fabric NPMD (network performance monitoring & diagnostic) capability, please contact your Cisco account team to learn how you can unlock this feature for a limited time
- Windows agent now supports hosts with more than 40 IP addresses
- Tetration installer will validate Npcap driver state before installing the agent itself
- AIX agents installed with 3.3.2.2 need to be re-installed after applying 3.3.2.5 patch

- Side Channel attack detection for Anomalous cache activity has been removed
- DBR server is optimized to use less memory during dumping MongoDB
- DBR Copy driver optimizations when a file is part of multiple checkpoints
- After restore upgrade history will show the operation as restore (instead of Deploy)
- Data export connector enables exporting flows and inventory data from Tetration in near real-time through DataExport Managed Data Tap; data export also requires an activation key to use this feature
- The Tetration Secure Connector uses a new connectivity mechanism in this patch; any existing Secure Connector client installed with 3.3.2.2 must be re-installed after the 3.3.2.5 patch is applied

Caveats

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

- Open Caveats
- Resolved Caveats
- 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
CSCvo19895	/local/tetration/log/tet-ldap-loader log requires timestamps in AnyConnect VM
CSCvo42565	Cannot use # in LDAP password on AnyConnect Proxy VM without double quotes around password
CSCvq26107	Enforcement ruleset breaks Linux UDP-Based Traceroute

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
CSCvq91327	An extra unknown node may be shown in cluster status
CSCvr20003	After upgrading to 3.3.2.2, DBR server cannot be started due to missing enum python module
CSCvp10656	For physical clusters, CIMC connectivity within the cluster is now tested periodically and any errors connecting to CIMC are bubbled up to the service status page under the fwmgr service.

CSCvr03130	For physical clusters, switch configuration changes applied during a reboot or upgrade are now properly applied to the switches.
CSCvr55140	Neighborhood geo information is correctly de-duplicated to avoid stalling neighborhood pipeline.
CSCvr32479	Grafana dashboard for tetration-apps is working again.
CSCvr30898	RedHat OS backporting generates false positives in Tetration Vulnerabilities
CSCvr67160	Fixed IFE annotation crash when there are inventories with ipv4 mapped ipv6 addresses

Known Behaviors

- During upgrade when a new RPM is uploaded, adhocKafka is gracefully shutdown. This is done to avoid Kafka index corruption. Kafka comes up after the upgrade. If upgrade is aborted after uploading the RPM, adhocKafka should be restarted using explore command.

Compatibility Information

The software agents in the 3.3.2.5 release support the following operating systems (virtual machines and bare-metal servers) for deep visibility:

- Linux:
  - CentOS-5.x: 5.7 to 5.11
  - CentOS-6.x: 6.1 to 6.10
  - CentOS-7.x: 7.0 to 7.6
  - Redhat Enterprise Linux-5.x: 5.7 to 5.11
  - Redhat Enterprise Linux-6.x: 6.1 to 6.10
  - Redhat Enterprise Linux-7.x: 7.0 to 7.6
  - Redhat Enterprise Linux-8.0
  - Oracle Linux Server-6.x: 6.1 to 6.10
  - Oracle Linux Server-7x: 7.0 to 7.6
  - 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
  - SUSE Linux-15.x: 15.0, 15.1
  - Ubuntu-14.04
  - Ubuntu-16.04
  - Ubuntu-18.04
- Windows Server (64-bit):
  - Windows Server 2008 Datacenter
  - Windows Server 2008 Enterprise
  - Windows Server 2008 Essentials
  - Windows Server 2008 Standard
  - 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 7
  - Microsoft Windows 7 Pro
  - Microsoft Windows 7 Home
  - Microsoft Windows 7 Enterprise
  - Microsoft Windows 8
  - Microsoft Windows 8 Pro
  - Microsoft Windows 8 Home
  - Microsoft Windows 8 Enterprise
  - Microsoft Windows 8.1
  - Microsoft Windows 8.1 Pro
  - Microsoft Windows 8.1 Home
  - Microsoft Windows 8.1 Enterprise
  - Microsoft Windows 10
  - Microsoft Windows 10 Pro
  - Microsoft Windows 10 Home
  - Microsoft Windows 10 Enterprise
  - Microsoft Windows 10 Enterprise 2016 LTSB
- IBM AIX operating system (Alpha):
  - AIX version 6.1
  - AIX version 7.1
  - AIX version 7.2

  Container host OS version for full visibility:

  - Red Hat Enterprise Linux Release 7.1, 7.2, 7.3, 7.4

- CentOS Release 7.1, 7.2, 7.3, 7.4
- Ubuntu-16.04

The 3.3.2.5 release supports the following operating systems for the policy enforcement add-on capability:

- Linux:
  - CentOS-6.x: 6.1 to 6.10
  - CentOS-7.x: 7.0 to 7.6
  - Redhat Enterprise Linux-6.x: 6.1 to 6.10
  - Redhat Enterprise Linux-7.x: 7.0 to 7.6
  - Redhat Enterprise Linux-8.0
  - SUSE Linux-11.x: 11.2, 11.3, and 11.4
  - SUSE Linux-12.x: 12.0, 12.1, 12.2, 12.3 and 12.4
  - SUSE Linux-15.x: 15.0, 15.1
  - Oracle Linux Server-6.x: 6.1 to 6.10
  - Oracle Linux Server-7.x: 7.0 to 7.6
  - Ubuntu-16.04
  - Ubuntu-18.04
- 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 Home

  - Microsoft Windows 8 Enterprise
  - Microsoft Windows 8.1
  - Microsoft Windows 8.1 Pro
  - Microsoft Windows 8.1 Home
  - Microsoft Windows 8.1 Enterprise
  - Microsoft Windows 10
  - Microsoft Windows 10 Pro
  - Microsoft Windows 10 Home
  - Microsoft Windows 10 Enterprise
  - Microsoft Windows 10 Enterprise 2016 LTSB

- IBM AIX operating system (Alpha):
  - AIX version 6.1
  - 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
  - CentOS Release 7.1, 7.2, 7.3, 7.4
  - Ubuntu-16.04

The 3.3.2.5 release supports the following operating systems for the universal visibility agent:

- Linux 32-bit and 64-bit (CentOS 4.x, RHEL 4.x, CentOS 5.x, RHEL 5.x, and so on)
- Windows Server (32-bit and 64-bit)
- Solaris 11 on x86 (64-bit)
- AIX 5.3 (PPC)

The 3.3.2.5 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 agents is supported only in Cisco ACI mode with release 3.1 or 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 Cloud:

Table 5 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 6 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 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 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 Hardware 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	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/

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.