Cisco Tetration Release Notes, Release 3.1.1.65

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

The Cisco Tetration platform is designed to address number of data center operational and security challenges comprehensively using rich traffic telemetry collected from servers, Cisco Nexus® switches and end point devices (such as laptops, desktops, and smart phones). The platform performs advanced analytics using an algorithmic approach to offer a wholistic 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 allowed-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 the servers
- Enable long-term data retention for deep forensics, analysis, and troubleshooting

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

- Software sensors installed on virtual machine, baremetal, or container hosts
- Embedded hardware sensors in Cisco Nexus 9000 cloudscale series switches
- ERSPAN sensors that can generate Cisco Tetration telemetry from copied packets
- Netflow sensors that can generate Cisco Tetration telemetry based Netflow v9 or IPFIX records
- Cisco AnyConnect proxy to collect telemetry from endpoints, such as laptops, desktops, and smartphones

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

The 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 shows the online change history for this document.

Table 1 Online History Change

Date	Description

Date	Description
June 6, 2019	Release 3.1.1.65 became available.

Contents

This document includes the following sections:

- New and Changed Information
- Caveats
- Compatibility Information
- Usage Guidelines
- 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

This patch release does not include any new software features.

Changes in Behavior

This patch release includes the following changes in behavior:

- The port to access Kafka from outside of the Cisco Tetration cluster has been changed from 9093 to 443. This change applies to all 3.1.1.x releases. Due to this change, you must re-download the Datasinks and Managed Data Taps (MDT) certifications to get the most updated tar.gz file that contains the port change in kafkaBrokerIps.txt file.

Caveats

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

- Open Caveats
- Resolved Caveats
- Known Behaviors

Open Caveats

The following table lists the open caveats in this release. Click the bug ID to access the Bug Search Tool and see additional information about the bug.

Table 2 Open Caveats

Bug ID	Description
CSCvn86706	For the Lookout Annotation, if a new rootscope is added, zeus/bogon tags are not added to that rootscope unless the UAS service is enabled.

Resolved Caveats

The following table lists the resolved caveats in this release. Click the bug ID to access the Bug Search Tool and see additional information about the bug.

Table 3 Resolved Caveats

Bug ID	Description
CSCvn50243	The RedHat 5.11 legacy deep visibility sensor failed send data to Tetration.
CSCvo77499	Dashboards disappear after the creator is disabled.
CSCvo86518	Changes to ADM external dependency and policy optimization should be documented.
CSCvo87526	The Netflow Sensor stops sending flows.
CSCvo98967	The Linux enforcement agent installer fails due to a SafeModeException when Namenode is not in safe mode.
CSCvp06054	An upgrade and reboot fails in pre-upgrade checks in the switch_config.yml script.
CSCvp24340	Inbound rules for the Windows enforcement agent are not allowing inbound multicast or broadcast traffic.
CSCvp26181	The vulnerability scores in the security dashboard show no data.
CSCvp31371	Flow stitching fails on the Citrix NetScaler AppFlow appliance.
CSCvp40579	Policies are regenerated by ADM if an existing policy has the "ANY" keyword.
CSCvp50694	The security dashboard and agent workload profile show the incorrect IE version for Windows 2016 end-points.
CSCvp71462	A default timeframe cannot be chosen for forensic event data.
CSCvp77466	Due to a bug in Linux kernel's ip_set code, the system might crash due to concurrent ipset commands.

Known Behaviors

The following list contains the known behaviors in this release:

- Deployment and Upgrade
  - The configuration fields for syslog (syslog server and syslog port) are deprecated in the Upgrade/Deploy GUI. Changes to these fields can only be made in the TAN GUI.
  - The configuration fields for remote CA (remote CA, remote CA URL, remote CA username, and remote CA password) are not supported on physical and ESX form factors.

- A side effect of the fix for bug CSCvn37738 is that the MSI installation might stop in the middle of the agent upgrade, which leaves the agent in a stalled and unrecoverable state. In such a case, you must reinstall the agent. Check the file "migrate.log" (in the logs folder) to confirm if the migration process runs into an error.

- TAN
  - User App alerts are not supported with the TAN virtual appliance.
  - Large size alerts (>64k) cannot be sent over UDP to the syslog server.
- Data Taps/Kafka
  - On 8 rack unit deployments and ESXi cluster configurations, Cisco Tetration runs only 1 instance of the Kafka broker. Because of this, if there is a decommission or re-commission of the bare metal or VM that is hosting the instance, there will be data loss.
  - Clusters that are upgraded from a pre-3.1.x build will display Alerts MDT (managed Data Tap) ports as 9093 even though the ports have been changed to 443. The downloadable certificates have the correct port (443) information. This text information will be updated in the next release.
- Enforcement
  - When enforcement is enabled and then disabled, agents will flush all of the rules and keep the catchall as ALLOW for both ingress and egress.
  - Agents will store the last known good policy from the backend and will reload the policy upon service restart.
  - During a network policy update, the agent on Linux will reprogram the ipset list in a more atomic fashion by swapping the ipset's content with the new content instead of flushing and reprogramming. This reduces the chances of traffic drops.
  - During a network policy update, the agent on Windows will first set the Windows firewall inbound and outbound default policies to ALLOW, then proceed as before by removing the current rules, programming the new rules, and programming the inbound and outbound default policy as specified by the network policy configuration. This reduces the chances of traffic drops in the case of a DENY catchall policy.
  - Whenever enforcement is stopped in an enforced workspace, do not delete objects in that workspace for approximately 15 minutes after enforcement was stopped. This ensures that pipelines have ample time to refresh the state about that workspace. User inventory filters or scopes referenced by the deleted application will not be deletable for 15 to 20 minutes after the deletion of an application.
- Data leak
  - Data leak detection has 5-minute latency, hence data leak scores have a 5 minute delay compared to the data leak event time.
  - Data leak events are not currently shown in the Forensics Analysis page.
- Process Hash Anomaly
  - Frequency analysis (and thus the output score) is done only at the rootscope level.
  - Analysis is run once per hour.
- AnyConnect
  - Multiple AnyConnect proxies getting data from the same AnyConnect endpoint machine is not encouraged. If you have a use case that needs this mode, contact Cisco.
  - The same endpoint can connect to different proxies at different points in time as long as the endpoint does not flip-flop between different proxies. If a flip-flop occurs, the AnyConnect proxy will limit the scenario so that there should be at least 7 days when such a flip-flop happens. If there is a flip-flop use case in which an endpoint is alternating connections between 2 different proxies, contact Cisco.
- Policy Publish on Kafka

- For client applications, which utilize this feature, we do not recommend that you use the 8 rack unit deployment and ESXi cluster configuration, because this configuration has only one instance of the Kafka broker. If there is a de-/recommission of the bare metal or VM that is hosting the application, the created policy stream will not be recovered correctly and will become inoperational. Instead, use the 39 rack unit cluster configuration for higher availability of the policy stream.

- ADM
  - An ADM run will no longer generate policies for flows that are already covered by manually created policies in the current application.
  - Clusters can no longer be used as a provided service. Existing clusters that are marked as public and referenced by an external application will be converted into inventory filters. Inventory filters become the only way to indicate a service provided by the scope or application.
  - When a cluster is promoted to an inventory filter, the cluster will be removed from the Conversations view. A new ADM run will be needed to generate an updated IP address-to-filter mapping.
  - Exclusion filters will be carried over across ADM runs. If clusters are used as part of an exclusion filter, the flows will only be removed if the application is primary.
  - An SLB upload for the Citrix load balancer configuration does not allow * as a port range. The configuration expects a single port to be specified in the configuration.
- TIM Configuration
  - When F5s are configured in high availability mode:
    - The TIM F5 plugin fetches the configuration from only one F5 out of the configured list of hosts. All features of the F5 where this configuration differs between the primary and standby REST endpoints may experience delays after a switchover until TIM connects to the new primary.
  - Citrix configuration when Netscalers are configured in HA mode:
    - The TIM Citrix plugin fetches the configuration from only one Netscaler out of the configured list of hosts. All features of the Netscaler where this configuration differs between the primary and secondary REST endpoints may experience delays after a switchover until TIM connects to the new primary.
  - When VMware vCenter HA mode is active:
    - The TIM VMware vCenter plugin only fetches the configuration from one VMware vCenter endpoint at a time. The VMware vCenter HA mode and behaviour of the TIM VMware vCenter plugin is untested.

Compatibility Information

This patch requires Cisco Tetration to be running software release 3.1.1.53, 3.1.1.54, 3.1.1.55, 3.1.1.59, or 3.1.1.61. You can upgrade to this patch release directly from any of the release versions mentioned below.

For information about the 3.1.1.53 release, see the following Release Notes:

https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_1_1_53.html

For information about the 3.1.1.54 release, see the following Release Notes:

https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_1_1_54.html

For information about the 3.1.1.55 release, see the following Release Notes:

https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_1_1_55.html

For information about the 3.1.1.59 release, see the following Release Notes:

https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_1_1_59.html

For information about the 3.1.1.61 release, see the following Release Notes:

https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_1_1_61.html

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.
- This release supports the collection of telemetry and analytics from hardware sensors on Cisco Nexus 9300-EX switches. However, you must define the collection rules.
- After setting up your DNS, browse to the URL of your Cisco Tetration cluster: https://<cluster.domain>

Verified Scalability Limits

For the verified scalability limits, see the *Cisco Tetration Release Notes, Release 3.1.1.53* at the following location:

https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_1_1_53.html

Related Documentation

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

Cisco Tetration Platform Datasheet: 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 M4 based 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-Analytics-Cluster-Hardware-Deployment-Guide.html Describes the physical configuration, site preparation, and cabling of a single- and dual-rack installation for M5 based 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-M5-Cluster-Hardware-Deployment-Guide.html
Cisco Tetration Cloud Deployment Guide	Describes the deployment of Cisco Tetration Cloud in Amazon Web Services. Document Link: http://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/nexus9000/hw/Tetration/b_tetration_cloud_setup.pdf
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/