Cisco Tetration Release Notes Release 3.4.1.1

This document describes the features, caveats, and limitations for the Cisco Tetration software, release 3.4.1.1.

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
- 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 agents. There are different types of agents available to support both existing-deployment and new-deployment data center infrastructures. This release supports the following agent types:

- Software agents installed on virtual machine, bare-metal, or container hosts
- ERSPAN agents that can generate Cisco Tetration telemetry from copied packets
- Telemetry ingest from ADCs (Application Delivery Controllers) – F5 and Citrix
- NetFlow agents that can generate Cisco Tetration telemetry based on NetFlow v9 or IPFIX records
- Embedded hardware agents in Cisco Nexus 9000 CloudScale series switches

In addition, support ingesting endpoint device posture, context and telemetry through integrations with:

- Cisco AnyConnect installed on endpoint devices such as laptops, desktops, and smartphones
- Cisco ISE (Identity Services Engine)

Software agents also act as the policy enforcement point for the application segmentation. Using this approach, the Cisco Tetration platform enables consistent micro segmentation across public, private, and on-premises deployments. Agents enforce the 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.

Date	Description
August 10th, 2020	Release 3.4.1.1 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

Software Agents and agent-related features

- Full visibility and policy enforcement support extended for the following operating system versions:
  - Red Hat Enterprise Linux Release 8.2
  - CentOS Release 7.8, 8.0 and 8.1
  - Oracle Linux 7.8, 8.0 and 8.1
- Process forensics, process snapshot, software vulnerability detection capabilities added for
  - Ubuntu 18.04
- AIX deep visibility and enforcement is available in BETA mode for this release:
  - OS versions: 7.1, 7.2 (PPC)
  - In order to use enforcement, ipfilter package version 5.3.0.7 is required to be installed and operating on the workload
  - No other active AIX or third-party firewall should be enabled. Do not use native AIX firewall commands (genfilt, chfilt, rmfilt, mkfilt, expfilt, impfilt)

- A new user role 'Agent Installer' is added for agent life-cycle management only. This role can download agent software from Tetration for installation, monitor agent status and statistics, upgrade an agent to a new release and convert Deep Visibility Agent to Enforcement Agent, but this role cannot delete agents or configure an agent profile.
- Agent conversion from Deep Visibility Agent to Enforcement Agent is added.
  - This feature currently does not work for Linux Agents that were originally installed with a Tetration software version before 3.1.1.53. If the Tetration cluster was deployed with any version before 3.1.1.53, we recommend you do not to use this feature.

Container Enforcement

- Policy enforcement on container orchestration systems has been tested to work with Kubernetes 1.12 to 1.16, and OpenShift 3.11.
- Kube-proxy is now supported when running in both IPtables and IPVS modes. Note that with OpenShift 3.11, kube-proxy with IPVS mode is not supported.
- The requirements for CNI plugins have been updated. Calico 3.13 has been tested to satisfy these requirements, with the appropriate configuration. Details of the configuration requirements can be found in Tetration user guide.
- Policy enforcement enhancements to support Nginx and Haproxy Ingress controllers (feature available in ALPHA mode).

ADM features

- Application dependency mapping now includes an option to generate policies across the entire scope hierarchy (deep policy)
  - Generated policy covers scope-to-scope conversations
  - Eliminates the need for cluster discovery
  - These policies still support policy analysis and policy enforcement

Policy enforcement features

- Policy definitions for micro segmentation now supports additional filters to specify which workloads should receive what policy elements, making policy enforcement much more versatile. This functionality is achieved through “Effective filter” definitions. Use cases where effective filters are recommended are:
  - Enforcing policies for applications that have dynamic VIP (Virtual IP) to support high availability
  - Applications and application components that use link-local addresses

Workload protection features

- This release includes the ability to get vulnerability information from the following Operating System vendors to reduce the false positives associated with the vulnerability detection:
  - Microsoft Windows
  - Redhat
  - Oracle Linux

  Vulnerability information from the OS vendor takes precedence over the general NIST CVE information

Ecosystem Integrations

- Tetration now natively supports integration with ServiceNow CMDB for ingesting CI (Configuration Item) attributes. These CI attributes from ServiceNow can be used to define inventory filters, tag workloads, define policies, and visualize flow traffic.

- Tetration now natively supports integration with Workload AD to bring rich user and workload context. These attributes can be used to define policies, inventory filters and visualize traffic flow.
- The following external Orchestrator integrations are now generally available:
  - Infloblox IP address Management system
  - Domain Name Servers (DNS)

API additions

- A new API endpoint is available to query the workload profile information. The following information can be queried through this endpoint:
  - Long-lived processes
  - Process snapshot
  - Interfaces
  - Packages
  - Vulnerabilities
  - File hashes
- A new API endpoint is available to support agent-management functions. These functions include:
  - Agent status monitoring
  - Agent upgrade
  - Agent software download

Threat

- Lookout Annotation adds the concept of compromised machine state, allowing actions such alerting and policy changes after a workload or endpoint is seen with flows to a known threat.

Alerting

- Alert configuration provides the ability to enable alerts for Federation and external connectors deployed through edge or ingest appliances.

Platform

- A new mode of data backup (DBR) called Continuous Mode is added to back up continuously from the cluster instead of a once-a-day snapshot. This feature aims to reduce the cluster Recovery Point Objective (RPO).
- DBR replaced the current restore workflow to support an additional warm stand-by mode. In the new mode, the stand-by cluster can be pre-deployed, which will continuously pre-fetch backed-up data to keep the cluster ready for failover. This feature aims to reduce the cluster Recovery Time Objective (RTO).
- Federation of multiple Tetration clusters is now supported as a BETA feature. The Federation feature requires a leader to be installed which will act as the central location for all configuration changes. Federation members could be 39-RU, 8-RU, or Tetration-V appliances. These Federation members can be dispersed geographically. Tetration agents and connectors connect to their respective member clusters.
- The Cluster Status page now allows UCS firmware upgrades on any bare-metal node regardless of the node state. The backend will manage allowing or blocking the upgrade depending on various factors. Please see the Usage Guidelines section for more details.
- TA-BNODE-G2, TA-CNODE-G2, TA-SNODE-G2 bare-metal nodes now support Intel I5220 CPUs and 2933 MHz DIMMs.

- TA-UNODE-G2 bare-metal nodes now support Intel I8260 CPUs, 2933 MHz DIMMs and Micron 5300 series SSDs.
- Ability to replace failed disks without requiring entire node recommission. Failed disks and the VMs that have logical volume(s) on those disks can be replaced on their own, without affecting other VMs that are running on the bare-metal nodes containing those failed disks. This also eliminates the need to re-image the bare-metal hosts, further reducing the disk-replacement time.

Enhancements

Agents and agent management

- Agent monitoring page is enhanced to more easily identify agent operational issues. The operational issues are grouped into one of the categories: Critical, Warning and Informational. Users can get the details of the specific agents, including the workload details, that are having issues.
- Agent Installer Download page is enhanced using a more intuitive multiple-steps wizard, and integrating user guide for pre-check, installation and verification. The workflow also provides the user the ability to enter the proxy information, if applicable, as part of the download process. It also provides the information about the dependencies that will be checked when sensor installation occurs.
- Software agent installer now includes an additional option for upgrade (upgrade-by-UUID) that allows an administrator to trigger upgrades for agents whose UUID is listed in a file. The version to which the agent will be upgraded is given by the sensor-version flag.
- Each downloaded installation script will be tracked with an installation ID so that the installed agents can be traced on in the application. However, this feature will only work for agents with 3.4.x versions or newer.
- Agent Upgrade page is enhanced to allow more flexible search and show upgradable versions only.
- Software installer scripts contain the appliance version.
- Teredo interface state change is no longer reported by the sensor. The sensor reports the interface initially, and any subsequent IP address change is not notified. Given the minimal adoption of 6-to-4 tunneling in the data-center domain, the sensor will refrain from issuing such notifications. This change will be specific to the Windows platform, and is for Teredo interfaces only. All other interface changes will be notified.

ADM and policy enforcement

- External Orchestrators with type “F5 BIG-IP” and “Citrix NetScaler” can now be configured to enable/disable enforcement via the new configuration field “Enable Enforcement.” The Tetration application now supports an “Enable Enforcement” switch in external Orchestrator configuration for F5 and Citrix.
  - Note that this field is set to false by default; that is, enforcement is disabled, for all external Orchestrators with these types that were created prior upgrading to release 3.4.1. Please update the respective external Orchestrator if enforcement is desired.
- Policy enhancement such that when a workload has multiple interfaces and an intent matches more than one interface, or all of them:
  - When more than one interface matches the intent, one concrete policy is generated grouping all such interfaces
  - When all interfaces match the intent, one concrete policy is generated grouping all such interfaces
- Enforcement status page now supports filtering/sorting by Status and Policy Count. The matching results also include Status and Policy Count columns.
- TopN Conversations by Consumers/Providers has been added to ADM Conversations table. Users can click the count to view detailed inventory information, along with User Annotations in a pop-up window.

- A Default Exclusion Filters section has been added to the Default ADM Run Config page. Along with this, an option has been added to the Advanced Run Config section for users to choose whether these filters should be included in the ADM run.
- Scope roll-up feature will reduce the number of inter-scope policies published in the Enforcement Kafka Policy Stream.
- Policy enforcement for Kubernetes now writes rules in the PREROUTING chain to enable tighter policies on NodePort services.

Workload protection

- The following new rules to detect MITRE-based techniques and tactics are included in this release:
  - Detect credential dumping type activities
  - Track anomalous execution of clear event log files, delete USN journals, hiding files using attrib.exe, creation of new scheduled tasks, and disable security tools
  - Track if mshta.exe executes a child process, BITS jobs are executed via powershell, and tscon.exe is used to perform lateral movement.
- New rules are added in the Tetration profile to alert on anomalous parent-child relationship for several native Windows processes.
- The Processes tab in workload profile is enhanced to show library information associated with each of the processes, and process hashes are annotated with benign/flagged verdicts.
- In workload file hashes, threat information is added to the details of malicious file hashes.
- In process hash analysis, package version information is considered in the security dashboard score calculation to reduce the false positives.
- Users with the correct privileges can now allow-list ports identified as anomalies through attack surface score. The option to allow-list is available through the security dashboard.

Alerting

- Bosun (Sentinel) has been replaced by Admiral which integrates with service status to process alerts. Alerts generated by Admiral can be viewed under Alerts > Current Alerts with Type = Platform. Additionally, they can be configured via the appropriate Platform Alert Tetration Alert Notifier (TAN) connections to be sent to supported publishers. Admiral alerts are also sent to the email address previously configured for Bosun.
- For platform type alerts, the alert feeds page is enhanced to link service field to service status page, allowing users to force-close an alert, and to allow searching alerts via 'CLOSED' status.

Integrations

- External Orchestrator for Infoblox is enhanced with a new field “progress status” to report the progress of importing Infoblox data as this can be a long running task.
- External Orchestrator for Infoblox now imports A/AAAA records, in addition to the network and host records. Note that only records with extensible attributes attached are considered for the annotation’s generation.

Usability

- The Tetration interface now supports keyboard navigation for all pages except some charts and graphs. Visual focus around the major components was added so the entire navigation and click actions make more sense. The majority of colors in the product are now compliant with accessibility guidelines. Labels and instructions are major components for screen-reader support for visually impaired people.

- The Tetration Users Page now has an option to hide disabled users which is enabled by default.
- Workload profile “Stats” tab is enhanced to display CPU and memory consumption for each of the Tetration agent processes.
- Users with the correct privileges can now edit the “config intent” and “config profile” for a workload through the workload profile page itself.
- Modifications to Interface Config Intents and Agent Remote VRF Configurations via the interface are now included in the Change Log.
- Neighborhood Inbound/Outbound Connections now support map clustering on Bytes Sent/Received with an added IP faceted filter. Visual cues were added directly on the map between the clusters and newly drawn Node/Filter to emphasize the Consumer/Provider mapping to Outbound/Inbound respectively.

Platform

- Site Admin and Customer Support users can now be authenticated with LDAP if external authentication with LDAP is enabled.
- To improve the physical security of the appliance, Tetration software will now disable USB ports (Front, Rear and Internal) through BIOS configuration. This feature is available only for Tetration M5 clusters (TA-CNODE-G2, TA-BNODE-G2, TA-SNODE-G2 and TA-UNODE-G2).
- The Company Cluster Configuration page now allows modification of the CIMC Internal Network and CIMC Internal Network Gateway parameters. Please see the Usage Guidelines for more details on using this enhancement.
- Snapshots page is enhanced to collect CIMC tech-support logs as CIMC snapshots. Collected CIMC snapshots can be downloaded either from the snapshots list page or from the cluster status page.
- Cluster status page is enhanced to detect the failed disks and users will be able to replace the disk(s) without bringing the affected node down. This feature also provides a simpler workflow for replacing faulty disks across multiple nodes.
- Support is added to exclude a faulty server during reboot or upgrade, allowing users to avoid dead-lock scenarios where upgrade/reboot is blocked on RMA of a faulty server, and RMA cannot be started before the upgrade/reboot completes.

Changes in Behavior

These are the changes in behavior for this release:

Platform

- On a Tetration virtual appliance, if the error, `The following unexpected VM state was found: Expected to find VM "orchestrator-1" running 1 instance, but found 0`, is encountered during an upgrade, please be sure that the orchestrator-1 VM is part of the VMware folder in vCenter where the Tetration cluster is installed.
- The Tetration-V installer now performs a check of available system resources to ensure platform requirements are met before permitting deployment to proceed. Please ensure availability of hardware meeting the required specifications before commencing deployment.

Agents

- The following dependencies have been removed for the Windows agent:
  - Curl
  - 7-Zip
  - OpenSSL
  - GPG
- Default AIX software agent (Deep Visibility and Enforcement agent) installation directory has been changed to /opt/cisco/tetration. As part of agent upgrades from 3.3.x.x, agent data/binaries are migrated from /usr/local/tet to /opt/cisco/tetration and /usr/local/tet will be removed after migration.
- Side-channel detection for anomalous cache activity has been discontinued.
- Process and service names of the Windows Tetration software agent have been renamed. Service-name mappings and process-name mappings are:

Service name mappings		
Service name in previous versions	Service display name in this release	Service name in this release
WindowsTetEngine	Cisco Tetration Deep Visibility	TetSensor
WindowsAgentEngine	Cisco Tetration Enforcement	TetEnforcer
Process name mappings		
Process name in previous versions	Process name in this release	
WindowsTetEngine.exe	TetSenEngine.exe	
WindowsAgentEngine.exe	TetEnfEngine.exe	
WindowsTetUpdate.exe	TetUpdate.exe	
WindowsSensor.exe	TetSen.exe	
tet_controller.exe	TetEnfC.exe	
tet_enforcer.exe	TetEnf.exe	

Policy and Enforcement

- Policy analysis page no longer displays MISDROPPED category. The Tetration system no longer infers DROPPED status from observations unless specifically reported by relevant agents. As a result, flows can only receive the DROPPED status when there is a corresponding DENY policy, which subsequently eliminates the MISDROPPED category.
- Only Inter scope policies will be published in the Enforcement Kafka Policy Stream. The source and destination inventory filter IDs will be replaced by the respective scope inventory filter IDs for all Inter scope policies published in the Kafka stream.

Integrations

- Enforcement virtual appliances for “F5 BIG-IP” and “Citrix NetScaler” are not supported any longer, starting with release 3.4.1. Instead Tetration 3.4.1 implements the integration of “F5 BIG-IP” and “Citrix NetScaler” load balancing in the cluster. Any deployed enforcement virtual appliances or enforcement agents for load balancers installed via the provided RPM package must be uninstalled before enabling enforcement for the corresponding external Orchestrators.
- External Orchestrator for AVI (AVI Vantage load balancer) is deprecated starting with Tetration release 3.4.1.
- AVI Connector to pull in flow telemetry is deprecated starting with Tetration release 3.4.1.

Usability

- Neighborhood Geo has been renamed to Inbound/Outbound Connections. In addition, a network connection between the client and Mapbox API server is needed for the map features to render.
- Lookout Annotation will do a complete comparison with the threat feed and delete annotations no longer in the feed. Previous behavior was to only add new threats.

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.

Bug ID	Description
CSCvv09685	The Tetration enforcement (EFE) traffic on port 5660 is not filtered out and will be shown in policy analysis. If there are no corresponding policies to allow this traffic, the flows will show up as ESCAPED in policy analysis and enforcement analysis and may trigger alerts. A workaround is to create manual ALLOW policies to cover this traffic.
CSCvv28548	RHEL/CentOS 5.x sensor incorrectly rejects new 3.4 forensics rules due to incorrect sanitization.
CSCvv23829	Windows Server 2008 R2: version upgrade script sometimes stops at an incomplete state.
CSCvu90994	Tetration deployments with Hardware sensors should not enable ‘Strong SSL Ciphers for Agent Connections’. HW sensors deployments don’t support TLS 1.1 / TLS 1.2 for software upgrade.

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.

Bug ID	Description
CSCvj86618	Site Admin role capabilities should include Customer Support capabilities as well
CSCvu41066	AIX: Lightsensor - taking long time to parse lsof output
CSCvt87488	Agent delete logged in change logs
CSCvs58791	tet_snapshot_manifest.json missing from snapshot
CSCvf27902	RMA: Move to a higher version of firmware for the RAID controller, 1225 VICs, and PSUs
CSCvg78845	CIMC access port mapping (port2cimc) may be incorrect
CSCvo26666	After a node recommission a key file to process CIMC commands is missing from bare metal node
CSCvt89073	Explore cimc_validator missing endpoint overview
CSCvp10580	Unable to change CIMC Internal Network outside of upgrade or reboot
CSCvo96713	Explore add_cimc_vm missing endpoint overview
CSCvo94456	Failure to create snapshot if "comments" field is populated (release 3.1.1.61)
CSCvo62061	Users can visit cluster status page and easily navigate to snapshots page to create cimc tech support logs.
CSCvj86618	Site Admin users have access to Customer Support pages as well.
CSCvo62049	Users can trigger and download cimc tech support collection via snapshot page. Also, it can be downloaded via cluster status page.
CSCvs99019	Workaround for network loss while installing NPCAP driver , during sensor installation , on Windows 2019 only.
CSCvu7645	For Redhat 7.X versions CVE-2016-8666 wrongly tagging for kernel package 3.10.0-1127.10.1.el7

Known Behaviors

- The Admiral Alert Email can be configured via the Company Configuration page. This email address must not be the same as the Tetration Admin email address. While the information pop-up window mentions this restriction, no check is enforced to prevent the user from doing so.
- An existing AIX sensor installed under 3.3 has to be at least of version 3.3.2.28 to be able to upgrade to 3.4.
- A new version of Windows Server 2008 R2 software agent is not available in the release 3.4.1.1, because of CSCvv23829. However, the existing software agents running version 3.3.2.x or before will continue to work with the cluster running 3.4.1.1. This will not affect existing functionality.

- Tetration monitors installed security updates provided by the operating system vendors, and filters out all CVEs fixed by those updates. However, there are some scenarios where CVEs could still be reported for Windows workloads when Tetration cannot obtain the exact patch update ID that fixed a CVE, and match the available patch ID in the feed obtained from Microsoft.

Compatibility Information

The software agents in the 3.4.1.1 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-8x: 8.0, 8.1
  - Redhat Enterprise Linux-6.x: 6.1 to 6.10
  - Redhat Enterprise Linux-7.x: 7.0 to 7.8
  - Redhat Enterprise Linux-8.0 to 8.2
  - Oracle Linux Server-6.x: 6.1 to 6.10
  - Oracle Linux Server-7x: 7.0 to 7.8
  - Oracle Linux Server-8x: 8.0, 8.1
  - 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, 12.5
  - SUSE Linux-15.x: 15.0, 15.1
  - Ubuntu-14.04
  - 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 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 3.4.1.1 release supports the following operating systems for visibility use cases only:

- Linux:
  - CentOS-5.x: 5.7 to 5.11
  - Redhat Enterprise Linux-5.x: 5.7 to 5.11
- Windows Server (64-bit):
  - Windows Server 2008 Datacenter
  - Windows Server 2008 Enterprise
  - Windows Server 2008 Essentials
  - Windows Server 2008 Standard
- Windows VDI desktop Client:
  - Microsoft Windows 7
  - Microsoft Windows 7 Pro
  - Microsoft Windows 7 Enterprise

The 3.4.1.1 release supports the following operating systems for the universal visibility agent:

- Redhat Enterprise Linux 4.0 (32-bit and 64-bit)
- CentOS 4.0 (32-bit and 64-bit)

- Redhat 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 7.1 and 7.2 (PPC)

The 3.4.1.1 release supports the following Cisco Nexus 9000 series switches in NX-OS and Cisco Application Centric Infrastructure (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 Cloud:

Scalability Limits for Cisco Tetration (39-RU)

Configurable Option	Scale
Number of workloads	Up to 25,000 workloads
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.

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

Configurable Option	Scale
Number of workloads	Up to 5,000 workloads
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.

Scalability Limits for Cisco Tetration Virtual (VMWare ESXi)

Configurable Option	Scale
Number of workloads	Up to 1,000 workloads
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 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.

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-M5-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
Latest Threat Data Sources	https://updates.tetrationcloud.com/