Cisco Tetration, Release 3.1.1.53, Release Notes

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

The Cisco Tetration Analytics 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 Analytics platform, consistent telemetry is required from across the data center infrastructure. Rich Cisco Tetration Analytics 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 Analytics 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
October 31, 2018	Release 3.1.1.53 became available.
December 7, 2018	In the New Software Features section, added information about enhancements to the ADM capabilities.

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 FeaturesThe following new software features are available in this release:

- Full visibility and policy enforcement support extended for the following operating system versions:
  - Red Hat Enterprise Linux Release 6.10 and 7.5
  - CentOS Release 6.10 and 7.5
  - Oracle Linux 6.10 and 7.5
  - SUSE Linux 12.3
- Full visibility and policy enforcement capability available as beta functionality for IBM zSystems running the z/Linux operating system. The following distribution and version of z/Linux support is available in this release:
  - SUSE Linux 11.2, 11.3, and 11.4
  - SUSE Linux 12.0, 12.1, 12.2, and 12.3
- Support is added to collect telemetry from endpoint devices, such as laptops, desktops, and smartphones, through the Cisco AnyConnect NVM module. The Cisco AnyConnect support provides the following benefits:
  - This support augments telemetry from endpoints to provide visibility and stronger segmentation policy based on user, user groups, and user location information.
  - Telemetry from Cisco AnyConnect NVM modules is aggregated through a proxy VM. The OVA for this proxy VM is available for download from the Cisco Tetration software download page.
  - For more information on Cisco AnyConnect NVM module, see the following document: https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200600-Install-and-Configure-Cisco-Network-Visi.pdf.
- Other deep visibility and enforcement software sensor related updates in this release for both new sensor installations and sensor upgrades:
  - Starting with this release, administrators do not need to download individual software packages for each OS version. The administrator must select the OS type (Linux or Windows) and visbility only or enforcement. The stub installer will run the precheck to determine the correct OS version and download the necessary installation file from the cluster. The legacy mechanism to download the installation package bundle is still available in this release, but will be deprecated in the future.
  - The Windows sensor installation file is now available in MSI format for easier automation. For a fresh installation, the newer installation script automatically downloads the MSI and installs it onto the host.

For migration from a pre-3.1.1.53 release to the 3.1.1.53 release, you must allow the current sensor to handle the upgrade internally, by way of the UI workflow.
  - The Linux installer script no longer uses nested RPMs nor install the sensor alternate RPMdb.
  - The Linux agent RPM will show "tet-sensor-<version>" in the rpm command output. The sensor binary's version should match the RPM version.
- This release includes the following workload protection features:
  - The security dashboard has been added to show the security posture for an application scope, a tenant (root scope), or the overall data center. This dashboard includes a composite security score and shows various metrics that contribute to the overall score. You can drill down to find out the details for each metric behind the score.
  - Support enabling multicast/broadcast traffic by using a configuration knob from the backend and UI.
  - Enforcement will skip enforcement IPv6 if the IPv6 stack is not enabled (this is done at run-time).
  - Flow disposition for Linux–Whenever the policy contains dropped policies (both concrete rules as well as catch-all drop rules), all dropped flows will be logged using NFLOG so that the deep visibility agent can capture the flows.
  - Forensics capabilities are extended to detect data exfiltration signals based on communication behavior patterns and other criteria. The extended forensics capabilities include the following:
    - Analyzes and baselines the communication between a provider-consumer using temporal analysis (taking into account seasonality).
    - Looks for deviations in communication behavior (default out-of-box rules are available).
    - Correlates new events with other forensic events.
    - Generates an event if conditions are met.
  - New forensic event types in forensic rules:
    - Follow User Logon–Represents process events that report descendant processes (up to 4 levels) that were forked or run after a User Logon event process, such as SSH and RDP. Processes reported under this event type are for auditing purposes and not necessary having any security events.
    - Data Leak–Represents workload events that detect possible data leak incidents by identifying anomalies in the time series of Producer Consumer Ratios. The data leak event type provides the following benefits:
      - Provides default forensic rules to record data leak events and send alerts about data leak events. Users can create their own refined forensic rules based on various attributes of the data leak events to improve the detection results for their systems.
      - Allows users to correlate the PCR anomalies with 3 types of forensics events (login failure, login, and unseen command) happen on the same workloads within 7 days.
      - Provides a seasonality detection method so that users can use a related attribute in the data leak event to reduce false positives caused by periodic cron jobs.
      - Provides data leak scores in the security dashboard based on the severity of the forensic rules for data leaks.
  - New 4 default forensic rules–The new rules help you to construct predefined rules that are meaningful in your environment. The default rules can be applied by enabling the default profile "Tetration Profile" or added into the users' forensic profiles. The rules are displayed in the forensic configuration page. The rules are not editable, and are available only in all root scopes.
  - File Access and Raw Socket creation forensic events on Linux depends on Linux Auditd. Auditd must be enabled on the machines that have a sensor installed. Additionally, the machines must have the settings USE_AUGENRULES="yes" or USE_AUGENRULES="YES" in the /etc/sysconfig/auditd file for Redhat and SUSE machines, and in the /etc/default/auditd file for Ubuntu machines.
  - File Access forensics events monitor a fix set of files. Refer the user guide for more details.
  - Meltdown exploit detection and anomalous cache activity detection can be individually enabled from the agent configuration page. Meltdown exploit detection currently supports CentOS 7, Ubuntu 14.04,

and Ubuntu 16.04 on both bare-metal and virtual machines. Anomalous Cache Activity detection currently supports CentOS 7 and Ubuntu 16.04 running on bare-metal machines.

- Process Hash Anomaly. This feature provides the following functionality:
  - Analyzes and detects process hash anomalies in the system.
  - Detects mismatched process hashes in the same process group across workloads.
  - A process group is defined as the set of processes that have the same combination of executable binary path and OS version.
  - Detects process hashes that appear in a block list that you uploaded (using OpenAPI).
  - Allows you to upload an allowed list to prevent false alarms (using OpenAPI).
  - Allows you to set the NIST RDS hash using Threat Intelligence and use the hash as an allowed list.
  - Supports both SHA-256 and SHA-1.
  - Scores the hashes based on block-list/allowed-list matching and frequency analysis.
- Check processes running on the workloads against an NIST allowed-list database to ensure that the processes are clean.
- Administrators can upload custom processes that must be added to the allowed list.
- Check for consistency of the process hash across the workloads within a specific application scope or root scope. If the hash value is different for the same processes, that will impact the composite security score.
- Policy definitions are extended to support the following LDAP parameters:
  - CN
  - User group
  - Location
  - Description
- You can now manually upload vulnerability and other threat data sources if automatic updates have been disabled. Latest threat data sources can be downloaded from https://updates.tetrationcloud.com. Following data sources can be updated manually:
  - CVE database
  - Geo database
  - Bogon IP address list
  - Team Cymru (Zeus C&C list)

- CMDB Upload
  - OpenAPI now generates a warning for duplicate entries in the CSV file.
  - Subnet-based annotation inheritance is now supported. Any tag values defined for high prefix subnets will be inherited by a lower prefix subnet or IP address the values are if missing.
- The legacy host profile page is now replaced with the workload profile page.
  - A workload profile page is available for any host with a Cisco Tetration software agent installed or AnyConnect NVM enabled endpoint.
  - A workload profile page includes more information than the inventory profile page.
  - Based on the agent type, the information includes long-lived processes, installed packages, process snapshot, enforcement policies, data leaks, file hashes, visit history, and agent related information.
  - The workload information page includes visit history. This page provides information the workload communication destination, including:
    - Geo location–state, country, and subdivision.
    - AS number and AS owner (the organization that owns the AS number).
    - Domain information–This is available only when the Cisco Anyconnect NVM module is sending telemetry to the Cisco Tetration platform.
    - DNS resolvers.
  - The inventory profile page is still available for any IP addresses that are reported through the flow telemetry data. The inventory profile will still be tagged with scopes, user annotations, and other inventory filters.

- This release includes changes to alert configuration workflow as well as expanded options for alerts. Also, it introduces an external virtual appliance for alert processing and publishing.
  - The Alerts Cisco Tetration app has been removed and a new simplified workflow is available for alerts configuration.
  - A centralized user interface page is now available to configure alerts.
  - Alerts can be configured for various categories: compliance, neighborhood graphs, forensics, lookout, fabric, sensors, enforcement, platform, and user apps.
  - In addition to Kafka, alert mechanisms have been expanded to support syslog, email, pager duty, and Amazon kinesis.
  - Each category can publish alerts using one or more mechanisms. The notification mechanism is configured through the alerts UI page.
  - All of the alerts go through an external virtual appliance called the Tetration Alerts Notification (TAN) appliance. The OVA for bringing up TAN can be downloaded from the software download page.
  - TAN establishes a secure connection with the Cisco Tetration cluster to receive alert events and configuration updates as you change the alert settings through the Cisco Tetration GUI.
  - The alert configuration settings for compliance events is now moved under the "Enforcement" tab.
- This release includes the following enhancements to the ADM capabilities:
  - An administrator can set the default ADM run configuration for a root scope. This configuration includes external dependency settings, scope order, and the clustering algorithm and granularity. All application workspaces under the root scope will inherit this default setting. An application owner can change the default for his or her workspaces, if required.
  - When performing subsequent ADM runs, you can use the default configuration from the root scope or use the configuration from a previous run.
  - The ADM-generated policy now includes a new policy confidence attribute. Confidence level is associated with the port, protocol, and client-server direction. This information is available in ADM Conversion tab as well as in the Policy tab.
- The neighborhood graph is extended to support the filtering of neighbors based on protocol and port information. Also, the path shows up to a 3 hop view.
- The Cisco Tetration platform now supports Network Performance Management and Diagnostics (NPMD) features for the following switches in Cisco ACI mode:
  - Cisco Nexus 9336C-FX2 with Cisco ACI release 13.2 or later.
- This release introduces a new dashboard for NPMD features. The dashboard enables operations quickly to identify specific network performance bottlenecks and drill down from there. KPI metrics shown in the dashboard requires Cisco Tetration software sensors to be deployed.
- Per tenant metrics are available in the Fabric page.
- A new performance dashboard helps identify network versus app performance issues based on TCP congestion metrics.
- LDAP has an additional configuration option for choosing "SSL Verify." This gives the customer the ability to upload the LDAP server's SSL certificate.
- LDAP group-to-role mapping–The limit for the number of group to role mappings allowed has increased from 5 to 50.
- The following enhancements to the Cisco Tetration software upgrade process are included in this release:
  - Upgrading from a 2.3.1.x release to the 3.1.1.53 release will display error codes if there are upgrade failures.
  - The upgrade process enforces the RPM upload order before allowing you to upgrade. The RPM order is the same for deployment and upgrading.
  - If the administrator does not receive the upgrade link, the link can be fetched through the Explore UI.
  - Upgrading requires a token that is emailed during the site validation. The same token can be fetched through the Explore UI.
  - The administrator can download all upgrade logs from setup UI.
  - Certain fields in the site info can be changed without the need to trigger an upgrade.

  - You can now resume an upgrade from any failure point. The upgrade will continue from last stable point before the failure.
- The cluster status page provides visibility into the commission, decommission, and reimage workflow when replacing a failed node in a cluster. Failures during this stage are now shown immediately in the GUI.
- The pre-upgrade checks can be run on-demand at any time from the Upgrade page.

Changes in Behavior

The following are changes in behavior for this release:

- The Security dashboard is now the default landing page. The landing page can be changed in the GUI's preferences menu.
- With this release, the syslog tunneling from Site Info is no longer supported. To configure syslog for receiving bosun and other platform-level syslog events, you must configure TAN on the Default Rootscope. See the user guide for more details on what changed.
- The user session expires after 6 hours, at which time you are redirected to the sign in page and asked for your credentials again.
- Five failed login attempts using your email address and password will lock the account. The lock out interval is set to 30 minutes.
- Alerts is now at the first level of the navigation menu in the UI, and not under Data Platform.
- The Alerts app is no longer shown in the App Store. Configuration of alerts to data taps (and then to the new Notifiers) is shown visually from the Alerts > Configuration page. Configuration of alerts to data taps and notifiers must be done by a root scope owner or site admin.
- Cisco Tetration machine data and inventory data will be deprecated from Data Lake and VMware vSphere Distributed Switch (VDS) in the next release. Warnings have been added to the user apps. The equivalent data will be available in the aggregated flows.
- Linux has a new upgrade workflow:
  - The new "Software Download" page now shows the installer download by default.
  - If you are upgrading from a 2.3.1.x release, the process will cleanup so that system rpmdb will show the inner RPM's version and the version should be consistent with the sensor binary.
  - Only the inner rpm will be maintained.
  - The legacy download page is still supported.
  - The installer script is available for deep visibility/enforcement agents only (both Linux and Windows).
  - Bash is now used for Linux.
  - Powershell is now used for Windows (requires Powershell 4.0 or later).
  - The installer uses a new file format: inner RPM for Linux, and MSI for Windows.
  - The upgrade process pre-populates the user.cfg file with ACTIVATION_KEY, if available.
  - The upgrade process runs the pre-check function by default.
- Forensics
  - The "side channel cache attack" forensic event in prior releases is now renamed as "side channel anomalous cache activity."
  - The same rule syntax can now be used for side channel events in both the forensics config page and the forensics analysis page. Side channel forensics events generated from prior releases will be preserved and the event type column will be empty.
  - Data leak events are not shown in the Forensics Analysis page. They can be found from the Security Dashboard, Workload Profile, and Alerts.
- Compliance App
  - The Compliance app is no longer shown in the App Store. Compliance alerts can be configured using the Enforcement tab of an application workspace, or using the new Alert Configuration page. Compli-

ance alerts can only be configured on an enforced application by a user with Enforce capabilities (or higher).
- Compliance alerts on "Live Analysis" applications are no longer available; alerts are only available on "Enforced applications."
- Compliance alerts can now be configured with the "Enable with Flow Details" option. This option only applies to individual alerts, not summary alerts. This option adds a field to the alert details called "constituent_flows," which contains a list of the 5-tuple flows (src, src port, dst, dst port, and protocol) that matched the configured alert.
  - There is a maximum of 100 flows included in the details. Multiple alerts will be generated if there are more than 100 flows.
  - Warning: This option could slow down receiving alerts if there are many flows matching the configured alert.
- The TAN syslog notifier has a maximum UDP message size; compliance alerts with flow details might go over this maximum message size, and if so, they will be dropped.
- Compliance alert details now has the "consumer_scope_names" and "provider_scope_names" fields in addition to "consumer_scope_ids" and "provider_scope_ids."

The following new software features are available in this release:

- Full visibility and policy enforcement support extended for the following operating system versions:
  - Red Hat Enterprise Linux Release 6.10 and 7.5
  - CentOS Release 6.10 and 7.5
  - Oracle Linux 6.10 and 7.5
  - SUSE Linux 12.3
- Full visibility and policy enforcement capability available as beta functionality for IBM zSystems running the z/Linux operating system. The following distribution and version of z/Linux support is available in this release:
  - SUSE Linux 11.2, 11.3, and 11.4
  - SUSE Linux 12.0, 12.1, 12.2, and 12.3
- Support is added to collect telemetry from endpoint devices, such as laptops, desktops, and smartphones, through the Cisco AnyConnect NVM module. The Cisco AnyConnect support provides the following benefits:
  - This support augments telemetry from endpoints to provide visibility and stronger segmentation policy based on user, user groups, and user location information.
  - Telemetry from Cisco AnyConnect NVM modules is aggregated through a proxy VM. The OVA for this proxy VM is available for download from the Cisco Tetration software download page.
  - For more information on Cisco AnyConnect NVM module, see the following document: https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200600-Install-and-Configure-Cisco-Network-Visi.pdf.
- Other deep visibility and enforcement software sensor related updates in this release for both new sensor installations and sensor upgrades:
  - Starting with this release, administrators do not need to download individual software packages for each OS version. The administrator must select the OS type (Linux or Windows) and visbility only or enforcement. The stub installer will run the precheck to determine the correct OS version and download the necessary installation file from the cluster. The legacy mechanism to download the installation package bundle is still available in this release, but will be deprecated in the future.
  - The Windows sensor installation file is now available in MSI format for easier automation. For a fresh installation, the newer installation script automatically downloads the MSI and installs it onto the host. For migration from a pre-3.1.1.53 release to the 3.1.1.53 release, you must allow the current sensor to handle the upgrade internally, by way of the UI workflow.
  - The Linux installer script no longer uses nested RPMs nor install the sensor alternate RPMdb.

- The Linux agent RPM will show "tet-sensor-<version>" in the rpm command output. The sensor binary's version should match the RPM version.

- This release includes the following workload protection features:
  - The security dashboard has been added to show the security posture for an application scope, a tenant (root scope), or the overall data center. This dashboard includes a composite security score and shows various metrics that contribute to the overall score. You can drill down to find out the details for each metric behind the score.
  - Support enabling multicast/broadcast traffic by using a configuration knob from the backend and UI.
  - Enforcement will skip enforcement IPv6 if the IPv6 stack is not enabled (this is done at run-time).
  - Flow disposition for Linux–Whenever the policy contains dropped policies (both concrete rules as well as catch-all drop rules), all dropped flows will be logged using NFLOG so that the deep visibility agent can capture the flows.
  - Forensics capabilities are extended to detect data exfiltration signals based on communication behavior patterns and other criteria. The extended forensics capabilities include the following:
    - Analyzes and baselines the communication between a provider-consumer using temporal analysis (taking into account seasonality).
    - Looks for deviations in communication behavior (default out-of-box rules are available).
    - Correlates new events with other forensic events.
    - Generates an event if conditions are met.
  - New forensic event types in forensic rules:
    - Follow User Logon–Represents process events that report descendant processes (up to 4 levels) that were forked or run after a User Logon event process, such as SSH and RDP. Processes reported under this event type are for auditing purposes and not necessary having any security events.
    - Data Leak–Represents workload events that detect possible data leak incidents by identifying anomalies in the time series of Producer Consumer Ratios. The data leak event type provides the following benefits:
      - Provides default forensic rules to record data leak events and send alerts about data leak events. Users can create their own refined forensic rules based on various attributes of the data leak events to improve the detection results for their systems.
      - Allows users to correlate the PCR anomalies with 3 types of forensics events (login failure, login, and unseen command) happen on the same workloads within 7 days.
      - Provides a seasonality detection method so that users can use a related attribute in the data leak event to reduce false positives caused by periodic cron jobs.
      - Provides data leak scores in the security dashboard based on the severity of the forensic rules for data leaks.
  - New 4 default forensic rules–The new rules help you to construct predefined rules that are meaningful in your environment. The default rules can be applied by enabling the default profile "Tetration Profile" or added into the users' forensic profiles. The rules are displayed in the forensic configuration page. The rules are not editable, and are available only in all root scopes.
  - File Access and Raw Socket creation forensic events on Linux depends on Linux Auditd. Auditd must be enabled on the machines that have a sensor installed. Additionally, the machines must have the settings USE_AUGENRULES="yes" or USE_AUGENRULES="YES" in the /etc/sysconfig/auditd file for Redhat and SUSE machines, and in the /etc/default/auditd file for Ubuntu machines.
  - File Access forensics events monitor a fix set of files. Refer the user guide for more details.
  - Meltdown exploit detection and anomalous cache activity detection can be individually enabled from the agent configuration page. Meltdown exploit detection currently supports CentOS 7, Ubuntu 14.04, and Ubuntu 16.04 on both bare-metal and virtual machines. Anomalous Cache Activity detection currently supports CentOS 7 and Ubuntu 16.04 running on bare-metal machines.
  - Process Hash Anomaly. This feature provides the following functionality:
    - Analyzes and detects process hash anomalies in the system.
    - Detects mismatched process hashes in the same process group across workloads.

        - A process group is defined as the set of processes that have the same combination of executable binary path and OS version.
        - Detects process hashes that appear in a block list that you uploaded (using OpenAPI).
        - Allows you to upload an allowed list to prevent false alarms (using OpenAPI).
        - Allows you to set the NIST RDS hash using Threat Intelligence and use the hash as an allowed list.
        - Supports both SHA-256 and SHA-1.
        - Scores the hashes based on block-list/allowed-list matching and frequency analysis.
    - Check processes running on the workloads against an NIST allowed-list database to ensure that the processes are clean.
    - Administrators can upload custom processes that must be added to the allowed list.
    - Check for consistency of the process hash across the workloads within a specific application scope or root scope. If the hash value is different for the same processes, that will impact the composite security score.
    - Policy definitions are extended to support the following LDAP parameters:
        - CN
        - User group
        - Location
        - Description
    - You can now manually upload vulnerability and other threat data sources if automatic updates have been disabled. Latest threat data sources can be downloaded from https://updates.tetrationcloud.com. Following data sources can be updated manually:
        - CVE database
        - Geo database
        - Bogon IP address list
        - Team Cymru (Zeus C&C list)
- CMDB Upload
    - OpenAPI now generates a warning for duplicate entries in the CSV file.
    - Subnet-based annotation inheritance is now supported. Any tag values defined for high prefix subnets will be inherited by a lower prefix subnet or IP address the values are if missing.
- The legacy host profile page is now replaced with the workload profile page.
    - A workload profile page is available for any host with a Cisco Tetration software agent installed or AnyConnect NVM enabled endpoint.
    - A workload profile page includes more information than the inventory profile page.
    - Based on the agent type, the information includes long-lived processes, installed packages, process snapshot, enforcement policies, data leaks, file hashes, visit history, and agent related information.
    - The workload information page includes visit history. This page provides information the workload communication destination, including:
        - Geo location–state, country, and subdivision.
        - AS number and AS owner (the organization that owns the AS number).
        - Domain information–This is available only when the Cisco Anyconnect NVM module is sending telemetry to the Cisco Tetration platform.
        - DNS resolvers.
    - The inventory profile page is still available for any IP addresses that are reported through the flow telemetry data. The inventory profile will still be tagged with scopes, user annotations, and other inventory filters.
- This release includes changes to alert configuration workflow as well as expanded options for alerts. Also, it introduces an external virtual appliance for alert processing and publishing.
    - The Alerts Cisco Tetration app has been removed and a new simplified workflow is available for alerts configuration.
    - A centralized user interface page is now available to configure alerts.

  - Alerts can be configured for various categories: compliance, neighborhood graphs, forensics, lookout, fabric, sensors, enforcement, platform, and user apps.
  - In addition to Kafka, alert mechanisms have been expanded to support syslog, email, pager duty, and Amazon kinesis.
  - Each category can publish alerts using one or more mechanisms. The notification mechanism is configured through the alerts UI page.
  - All of the alerts go through an external virtual appliance called the Tetration Alerts Notification (TAN) appliance. The OVA for bringing up TAN can be downloaded from the software download page.
  - TAN establishes a secure connection with the Cisco Tetration cluster to receive alert events and configuration updates as you change the alert settings through the Cisco Tetration GUI.
  - The alert configuration settings for compliance events is now moved under the "Enforcement" tab.
- This release includes the following enhancements to the ADM capabilities:
  - An administrator can set the default ADM run configuration for a root scope. This configuration includes external dependency settings, scope order, and the clustering algorithm and granularity. All application workspaces under the root scope will inherit this default setting. An application owner can change the default for his or her workspaces, if required.
  - When performing subsequent ADM runs, you can use the default configuration from the root scope or use the configuration from a previous run.
  - The ADM-generated policy now includes a new policy confidence attribute. Confidence level is associated with the port, protocol, and client-server direction. This information is available in ADM Conversion tab as well as in the Policy tab.
- The neighborhood graph is extended to support the filtering of neighbors based on protocol and port information. Also, the path shows up to a 3 hop view.
- The Cisco Tetration platform now supports Network Performance Management and Diagnostics (NPMD) features for the following switches in Cisco ACI mode:
  - Cisco Nexus 9336C-FX2 with Cisco ACI release 13.2 or later.
- This release introduces a new dashboard for NPMD features. The dashboard enables operations quickly to identify specific network performance bottlenecks and drill down from there. KPI metrics shown in the dashboard requires Cisco Tetration software sensors to be deployed.
- Per tenant metrics are available in the Fabric page.
- A new performance dashboard helps identify network versus app performance issues based on TCP congestion metrics.
- LDAP has an additional configuration option for choosing "SSL Verify." This gives the customer the ability to upload the LDAP server's SSL certificate.
- LDAP group-to-role mapping–The limit for the number of group to role mappings allowed has increased from 5 to 50.
- The following enhancements to the Cisco Tetration software upgrade process are included in this release:
  - Upgrading from a 2.3.1.x release to the 3.1.1.53 release will display error codes if there are upgrade failures.
  - The upgrade process enforces the RPM upload order before allowing you to upgrade. The RPM order is the same for deployment and upgrading.
  - If the administrator does not receive the upgrade link, the link can be fetched through the Explore UI.
  - Upgrading requires a token that is emailed during the site validation. The same token can be fetched through the Explore UI.
  - The administrator can download all upgrade logs from setup UI.
  - Certain fields in the site info can be changed without the need to trigger an upgrade.
  - You can now resume an upgrade from any failure point. The upgrade will continue from last stable point before the failure.
- The cluster status page provides visibility into the commission, decommission, and reimage workflow when replacing a failed node in a cluster. Failures during this stage are now shown immediately in the GUI.
- The pre-upgrade checks can be run on-demand at any time from the Upgrade page.

Changes in Behavior

The following are changes in behavior for this release:

- The Security dashboard is now the default landing page. The landing page can be changed in the GUI's preferences menu.
- With this release, the syslog tunneling from Site Info is no longer supported. To configure syslog for receiving bosun and other platform-level syslog events, you must configure TAN on the Default Rootscope. See the user guide for more details on what changed.
- The user session expires after 6 hours, at which time you are redirected to the sign in page and asked for your credentials again.
- Five failed login attempts using your email address and password will lock the account. The lock out interval is set to 30 minutes.
- Alerts is now at the first level of the navigation menu in the UI, and not under Data Platform.
- The Alerts app is no longer shown in the App Store. Configuration of alerts to data taps (and then to the new Notifiers) is shown visually from the Alerts > Configuration page. Configuration of alerts to data taps and notifiers must be done by a root scope owner or site admin.
- Cisco Tetration machine data and inventory data will be deprecated from Data Lake and VMware vSphere Distributed Switch (VDS) in the next release. Warnings have been added to the user apps. The equivalent data will be available in the aggregated flows.
- Linux has a new upgrade workflow:
  - The new "Software Download" page now shows the installer download by default.
  - If you are upgrading from a 2.3.1.x release, the process will cleanup so that system rpmdb will show the inner RPM's version and the version should be consistent with the sensor binary.
  - Only the inner rpm will be maintained.
  - The legacy download page is still supported.
  - The installer script is available for deep visibility/enforcement agents only (both Linux and Windows).
  - Bash is now used for Linux.
  - Powershell is now used for Windows (requires Powershell 4.0 or later).
  - The installer uses a new file format: inner RPM for Linux, and MSI for Windows.
  - The upgrade process pre-populates the user.cfg file with ACTIVATION_KEY, if available.
  - The upgrade process runs the pre-check function by default.
- Forensics
  - The "side channel cache attack" forensic event in prior releases is now renamed as "side channel anomalous cache activity."
  - The same rule syntax can now be used for side channel events in both the forensics config page and the forensics analysis page. Side channel forensics events generated from prior releases will be preserved and the event type column will be empty.
  - Data leak events are not shown in the Forensics Analysis page. They can be found from the Security Dashboard, Workload Profile, and Alerts.
- Compliance App
  - The Compliance app is no longer shown in the App Store. Compliance alerts can be configured using the Enforcement tab of an application workspace, or using the new Alert Configuration page. Compliance alerts can only be configured on an enforced application by a user with Enforce capabilities (or higher).
  - Compliance alerts on "Live Analysis" applications are no longer available; alerts are only available on "Enforced applications."

- Compliance alerts can now be configured with the "Enable with Flow Details" option. This option only applies to individual alerts, not summary alerts. This option adds a field to the alert details called "constituent_flows," which contains a list of the 5-tuple flows (src, src port, dst, dst port, and protocol) that matched the configured alert.
  - There is a maximum of 100 flows included in the details. Multiple alerts will be generated if there are more than 100 flows.
  - Warning: This option could slow down receiving alerts if there are many flows matching the configured alert.
- The TAN syslog notifier has a maximum UDP message size; compliance alerts with flow details might go over this maximum message size, and if so, they will be dropped.
- Compliance alert details now has the "consumer_scope_names" and "provider_scope_names" fields in addition to "consumer_scope_ids" and "provider_scope_ids."

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
CSCvi59692	The cluster does not indicate the target or source that is highlighted last .
CSCvm68801	A vPC is not configured for the public network on an 8 rack unit deployment.

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
CSCvm57680	keepalived does not failover VIPs on appServer when an interface for Public Network is down.
CSCvm85033	Qualys scan - AutoComplete Attribute Not Disabled for Password in Form Based Authentication

CSCvm84974	Tetration UI Possibly Impacted by CVE-2016-2183 (Birthday attacks against TLS ciphers)
CSCvm84884	Tetration UI Possibly Impacted by CVE-2014-8730 (Poodle Attack - TLS)
CSCvm79202	While trying to restore a deleted user the UI throws a "Object Not Found" message
CSCvm75109	Reboot command removes patch update notation on the version page.
CSCvm72606	Inventory Search button is disabled while trying to search for an inventory first time
CSCvm67112	Tetraiton displays SUNRPC TCP/111 as DNS service in ADM
CSCvm63714	Tetr-V // Graceful cluster power down fails
CSCvm57680	keepalived does not failover VIPs on appServer when an interface for Public Network is down.
CSCvm45307	systemd: dnsmasq.service: main process exited, code=exited, status=1/FAILURE
CSCvm35204	CitrixParser unable to parse configuration lines which represent l4 port as an *
CSCvm35195	CitrixParser in tetration may crash after parsing a SLB config file
CSCvk37602	Ability to disable Neighborhood application on specific tenant
CSCvk34853	Clear text admin passwords written to the orchestrator.log during reimaging.
CSCvk34663	Enhancement: Patch installation succeeds with the upgrade button but doesn't show any logs
CSCvk33093	Application Policy value is incorrect in UI
CSCvk33059	Application workspace delete fails due to orphaned data in Mongo
CSCvk29668	While attempting to switch application versions the request times out with a 502 response
CSCvk24300	SSO with Microsoft Azure errors AADSTS75005: The Request is not a valid Saml2 protocol message.
CSCvk23256	Uploading a annotation file multiple times cause the system to hit the total subnet limit per scope
CSCvk23222	Uploading Annotation file with column name "VRF" throws an error
CSCvj21831	Allow control of scopes where lookout annotations are enabled
CSCvj18549	Inconsistent UI response when uploading annotations csv
CSCvi30385	Upgrades: Script generating vmmgr.log, should identify the DIMM / DIMMs with correctable ECC errors
CSCvi20538	Bosun alert: Correctable ECC errors should be for individual DIMMs not a sum of errors for the node.
CSCvi03468	RPM upload failing due to corrupt RPM without clear error message in Tetration Upgrade UI
CSCvh56702	Tetration Sensor After Delete Shows Duplicate Host Agent

CSCvf70210	Enhancement: Request for group/sub-group creation in agent upgrade panel

Known Behaviors

- 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.
- 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.
- 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, users should 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.
  - A 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

The software sensors in the 3.1.1.53 release supports the following operating systems (virtual machines and bare-metal servers) for legacy deep visibility and deep visibility:

- Linux:
  - CentOS-5.x: 5.1 to 5.11
  - CentOS-6.x: 6.1 to 6.10
  - CentOS-7.x: 7.0, 7.1, 7.2, 7.3, 7.4 and 7.5
  - Redhat Enterprise Linux-5.x: 5.1 to 5.11
  - Redhat Enterprise Linux-6.x: 6.1 to 6.10

  - Redhat Enterprise Linux-7.x: 7.0, 7.1, 7.2, 7.3, 7.4 and 7.5
  - Oracle Linux Server-6.x: 6.0 to 6.10
  - Oracle Linux Server – 7.0, 7.1, 7.2, 7.3, 7.4 and 7.5
  - SUSE Linux-11.x: 11.2, 11.3, and 11.4
  - SUSE Linux-12.x: 12.0, 12.1, 12.2 and 12.3
  - Ubuntu-12.04
  - Unbuntu-14.04 and 14.10
  - Ubuntu-16.04
- 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 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

The 3.1.1.53 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, 7.1, 7.2, 7.3, 7.4 and 7.5
  - Redhat Enterprise Linux-6.x: 6.1 to 6.10

  - Redhat Enterprise Linux-7.x: 7.0, 7.1, 7.2, 7.3, 7.4 and 7.5
  - SUSE Linux-11.x: 11.2, 11.3, and 11.4
  - SUSE Linux-12.x: 12.0, 12.1, 12.2 and 12.3
  - Oracle Linux Server-6.x: 6.0 to 6.10
  - Oracle Linux Server – 7.0, 7.1, 7.2, 7.3, 7.4 and 7.5
  - Ubuntu-14.04 and 14.10
  - Ubuntu-16.04
- 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 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
- 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 Release 16.04

The 3.1.1.53 release supports the following operating systems for the universal visibility sensor :

- 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, 6.1, 7.1, and 7.2

The 3.1.1.53 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 sensors 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 Baremetal)
Flow features per second	Up to 2 Million
Number of hardware sensor 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 sensor 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 Baremetal)
Flow features per second	Up to 70,000
Number of hardware sensor 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:

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/