Illumio® Core

Version: 21.2.7

Release Notes

05/19/2022

14000-100-21.2.7

illumio

Contents

Welcome

Document Last Revised: May 2022
Document ID: 14000-100-21.2.7

> Illumio Core 21.2.*x* is available for Illumio Core On-premises customers and Illumio Core Cloud customers. Specific resolved and known issues apply to Illumio Core On Premises customers only. Each of those issues is noted in this release notes.

These release notes describe the resolved issues and known issues for the Illumio Core 21.2.*x* releases.

> Container issues have been moved to the another document named "Illumio Containerized VEN Release Notes 21.2."

Product Version

Illumio On-premises Customers

Current PCE Version: 21.2.7 (LTS)
Current VEN Version: 21.2.5 (LTS)

Standard versus LTS Releases

21.2.7-PCE is a Long Term Support (LTS) release.
21.2.5-VEN is a Long Term Support (LTS) release.
For information on Illumio software support for Standard and LTS releases, see Versions and Compatibility on the Illumio Support portal.

Release Types and Numbering

Illumio ASP release numbering uses the following format: "a.b.c-d+e"

- "a.b": Standard or LTS release number, for example, "21.2"

- ".c": Maintenance release number, for example, ".2"
- "-d": Optional descriptor for pre-release versions, for example, "preview2"

What's New in This Release

To learn what's new and changed in 21.2, see What's New in This Release on the Illumio Technical Information portal.

> ⚠ The Illumio Core platform was previously known as the Illumio Adaptive Security Platform (ASP). References to "Adaptive Security Platform" and ASP still appear in these release notes.

Updates for Core 21.2.7-PCE

Resolved Issues in Core 21.2.7-PCE

- **PCE response header names were lower case** (89767)
  HTTP response header names from the PCE could sometimes be sent in lower case. This could affect scripts that were written for earlier PCE versions, which expected mixed-case headers. For example, Content-Length in the response header of a previous PCE version might be content-length in a later version. This issue is resolved. The PCE will continue to provide mixed-case header names for the moment. However, any tooling that parses the HTTP headers should be changed to allow case-insensitive header name matching in order to retain compatibility with future PCE releases. Refer to RFC 7230, section 3.2, "Header Fields," which states that field names should be case insensitive.
- **Labels disappeared when editing one of the labels in a virtual server** (E-89636, E-87402)
  When changing a label of a virtual server, all the other labels were automatically removed. This issue is resolved.
- **The number of workloads reported was inconsistent** (E-89231, E-88766)
  The number of workloads reported on the App Group Map sometimes differed from the number of workloads shown in the detailed popup window when the App Group was clicked. This issue is resolved.
- **Labels were incorrectly marked as unused and could be deleted** (E-89189)
  Labels could be incorrectly marked as not in use by the workload, based on the status of the VEN. As a result, it was possible to delete the label if the VEN had a status other than Active. This issue is resolved.

- **Container workloads could continuously sync policy with the PCE** (E-88967)
  Environments with high rates of container workload changes may cause all VENs to continuously sync policy. This issue is resolved.
- **Database migration failed during upgrade** (E-88273)
  When upgrading Illumio Core on a Supercluster, an error message like the following appeared during the database migration step: " 'id' column is missing. A multimaster table requires an INSERT statement to provide 'id' column explicitly." Data being generated during the migration required an explicitly specified database primary key to verify Supercluster region ownership. The migration involving the `clone_detected` state triggered this restriction. This issue is resolved. The migration involving the `clone_detected` state no longer triggers this restriction.
- **Event forwarding UI rejected FQDNs containing underscores** (E-86061)
  When configuring the PCE to forward syslogs to an external server (**Settings > Event Settings**), addresses that include the underscore character (_) were disallowed and the message **Invalid address** appeared below the **Address** field. This issue is resolved. The Address field now accepts addresses that contain underscores.

Limitations in Core 21.2.7-PCE

- **Can not perform Supercluster rolling upgrade to 21.2.7 from 21.2.0 or 21.2.1** (E-90663)
  Due to a software change in 21.2.2, you can only do a rolling upgrade when the installed and upgrade versions are both either before 21.2.2 or after it. For example, you can do a rolling upgrade from 21.2.3 to 21.2.7, but not from 21.2.0 or 21.2.1 to 21.2.7.

Resolved Issues in Core 21.2.5-VEN

- **VENs flooded DNS server with DNS queries of PCE FQDN** (E-86835)
  VENs were performing multiple DNS queries and flooding their DNS server instead of performing such queries as expected (every 5 minutes). This issue is resolved.
- **Pairing line failed with 21.2.4 VEN on Debian 11.2** (E-87023)
  A workload failed its installation of Illumio packages. The pairing script gave an error when pairing the PCE with 21.2.4 VEN on Debian 11.2. This issue is resolved.
- **Windows 2016 VEN needed a reboot every couple months for policy sync** (E-86183)
  Persistent errors with policy sync on a workload occurred and required regular reboots of the VEN. This issue is resolved.
- **PCE Event forwarding repository configuration failed when an underscore was present in the FQDN** (E-86061)
  When configuring the PCE to forward syslogs to an external server (**Settings** > **Event Settings**), addresses that included the underscore character (_) were disallowed and the

message Invalid address appeared below the Address field. This issue is resolved. The Address field now accepts addresses that contain underscores.
- **Optimized policy application to workloads** (E89231, E-84537)
  The VEN used to take a long time to process policies with a large number of empty IP sets, usually caused by label group usage. This issue has been optimized.

Resolved Issues in Core 21.2.4

PCE Web Console

- **Events page missing information for workload.offline_after_ven_goodbye event** (E-84391)
  When the PCE encountered the workload.offline_after_ven_goodbye event, it didn't display the name, hostname, HREF, and labels for the affected workload in the PCE web console **Events** page. This issue is resolved. The **Events** page now displays this information for affected workloads.

Policy and Workloads

- **AUS rules could fail to allow outbound traffic to virtual services** (E-85508)
  When an AUS rule included a virtual service in the provider field or a label in the provider field applied to the virtual service, the rule could fail to allow outbound traffic to that virtual service when it should be allowed. This issue is resolved. In this release, rules with virtual services in the provider field correctly allow traffic for AUS users.
- **Label-based policy for virtual service could be overly broad** (E-85061, E-84702)
  In rare cases, label-based policy for virtual services could be overly broad. This issue could occur when you specify a label in a rule but the label wasn't applied to any virtual services. This issue is resolved.
- `workload.offline_after_ven_goodbye` **wasn't including affected workloads** (E-84040, E-78148)
  The event message reported only an event but there was no information about which workload(s) went offline after the goodbye message. This issue is resolved partially for consuming events via API and syslog.

Data Visualization

- **PCE Health could report a high failure percentage for the flow rate** (E-82901)
  The **PCE Health Application** tab could report a high failure percentage (possibly as high as 100%) in the **Collector Summary** section. The collector log indicated the failures occurred because the database cache wasn't ready and wasn't processing collector requests. The issue occurred after services restarted on the PCE data node. This issue is resolved. In this release,

restarting services on the data node no longer causes the PCE Health page to report a high failure percentage for the flow rate.

- **High CPU utilized by Redis server on primary data node** (E-85396)
  High CPU was utilized by a Redis server 6200 on the primary data node.
  This is considered to be normal behavior.
- **Qualys vulnerability reports failing to import when using the CLI Tool** (E-85068)
  Qualys vulnerability reports could fail to upload into the PCE when using the CLI (ILO) Tool. This issue occurred when the scan reports in the XML file had overly long names. This issue is resolved. In this release, the CLI Tool successfully uploads Qualys vulnerability reports even when scan reports in the XML file have long names.
- **Explorer queries could return zero results when searching by FQDNs that had wildcard characters** (E-85032)
  This issue occurred because of the way that the PCE supported FQDNs with wildcard characters. It didn't support FQDNs with wildcard characters in IP lists at all. In user-specified FQDNs, the PCE supported wildcards in domain names but only when the wildcards appeared at the beginnings or ends of the domain names; for example, `*.wns.windows.com` was supported but `foo.*.bar` wasn't supported. This issue is resolved for both cases. Explore queries that search by FQDNs that have wildcard characters correctly return results.
- **High latency could impact Illumination map display in PCE web console** (E-84816)
  When a user viewed the Illumination map, the PCE web console always refreshed map data regardless of currentness. This behavior could impact performance. This issue is resolved. In this release, the PCE web console will display cached data in the Illumination map when the map has less than 200 workloads (controlled by the user's workload RBAC permissions).
- **Database backup could fail with an error message that illumio/tmp subdirectory already exists** (E-84731)
  When the `ephemeral_data` directory was universally writable, backing up traffic and reporting databases could fail and return a confusing error message. This issue is resolved. In this release, the PCE checks whether the `ephemeral_data` directory is universally writable before the back up runs and, if it is writable, returns an informative error message.
- **Archived flow data caused high backlog disk utilization** (E-84587)
  Unexpected archiving of flow data caused an increase in the archive folder size. The problem stemmed from a special character in the username which caused routine uploading of reference data to fail, which in turn caused flow data to be archived, resulting in an abnormal increase in the size of the flow data archive file. Affected customers would have seen an indication of this in **PCE Health > Application > Traffic Summary > Backlog Disk Utilization**. This issue is resolved. The PCE now handles invalid characters in a way that no longer causes this problem.
- **Legend wasn't clear in Executive Summary Reports** (E-84343)
  In Executive Summary reports, you view data over a time range. These sections include a legend on the left that displays data for the report time range only. The right side displays the data in stacked bar graphs each time the recurring report is run. When the report was run daily, the legend didn't include a date so it appeared that data was aggregated across all

recurring reports, which isn't correct. This issue is resolved. In this release, the legend includes the date for the data. Additionally, the following fields in the feature have clearer values:
Add Report > Time Range: "Last 24 Hours" changed to "Last Day"
Report PDF > Top Summary > Time Range: "1 day" changed to "Last 1 day"

- **Workload count incorrect in Executive Summary Report** (E-84300)
  In some environments with workloads that have been paired and unpaired, the Total Workloads count was incorrect in the generated Executive Summary Report (**PCE > Reports**). This issue is resolved.
- **Global Explorer queries could fail at least half the time** (E-83921)
  When the Supercluster leader was deployed in a split data center, Global Explorer queries could fail 50% of the time. This issue is resolved.
- **Global Explorer async query sometimes failed when Supercluster member experienced Health issues** (E-83287)
  The PCE Health monitoring feature provides warnings and errors when Supercluster members experience issues. Under these circumstances, Global Explorer asynchronous queries sometimes failed for all members instead of returning data for the healthy members. This occurred only in situations where the PCE consul service was unavailable in a Supercluster region and didn't occur for other PCE Health warnings or errors in a region. This issue is resolved.
- **Input validation error using Policy Generator** (E-82828)
  When using Policy Generator, if the ruleset included a rule containing a label_group and Vulnerabilities were enabled, the message "Unexpected input validation error" appeared. This issue is resolved. Policy Generator now works as expected under these circumstances.

PCE Platform

- **Couldn't log into the PCE** (E-84777)
  If the web server was under heavy load, occasional failures could occur when attempting to log in to the PCE. This issue is resolved.
- **Potentially blocked syslog traffic was not present in log** (E-84710, E-84789)
  With the PCE set up to forward potentially blocked traffic to the syslog server, other logs appeared, but not potentially blocked traffic. The cause was an error in the syslog configuration code. This issue is resolved. Potentially blocked traffic is now logged.
- **(Supercluster) Migration failed and slony services did not start on upgrade** (E-84281)
  In some environments and after certain previous upgrades, Supercluster upgrade to 21.2.x or later PCE versions failed during migration on member PCEs with an error like "An error has occurred, this and all later migrations canceled". Or, if migration succeeded, slony services would not start, with an error like "[agent_slony_service] Configuration appears to have failed." Also, on member PCEs, one or more tables might have missing replication triggers, causing replication issues. This issue is resolved. These upgrade issues no longer occur. This

issue was described in more detail in Supercluster Upgrade Failure When Upgrading to 21.2.x or Later (login required).

- **LDAP user unable to log into PCE when directory search returned more than one result** (E-83974)
  User authentication could fail for user DNs that had LDAP entries below them. This configuration is common for user devices, such as `ExchangeActiveSyncDevices`. This issue is resolved. In this release, the PCE only queries the LDAP directory for username attributes that are an exact match.
- **Error occurred when editing labels or unpairing workloads** (E-83924)
  When you added a scoped role to a user with an unrestricted role, then tried to edit the labels on a paired workload or manually unpair a workload, a "500 Internal Server Error" occurred. This issue is resolved.
- **Service discovery log contained debug messages in production** (E-83455)
  In the `service_discovery` log, DEBUG level messages sometimes appeared. These messages could be identified by containing the text "level=debug." This issue is resolved. Only messages of type INFO are now logged, as expected.
- **User RBAC permissions not properly enforced for /system_health API endpoint** (E-82750)
  Local PCE users with no role assigned were able to use the API to obtain potentially sensitive information. This issue is resolved. A user who has no role assigned and is sending requests via API now receives the forbidden access error 403.
- **Virtual server events API could return missing or incorrect data** (E-81611)
  When using the Events API to update a virtual service, the API did not expose label deletion information in the resource changes section. This issue is resolved. In this scenario, the Events API now exposes label deletion information.
- **21.2 async API call response time doubled** (E-80282)
  This issue is resolved so that the Exit Strategy is now memory-usage based, rather than job-count based, which also helps customers with large databases.

VEN

- **On CentOS 8, VEN couldn't load the FTP and TFTP modules** (E-85127)
  On CentOS 8, the VEN couldn't load the `nf_conntrack_ftp` and `nf_conntrack_tftp` modules, which blocked the workload from uploading and managing files. Due to this issue, customers couldn't upgrade the VEN on CentOS 8 workloads. This issue is resolved. In this release, the VEN loads those modules and the issue no longer potentially impacts customers from upgrading the VEN on this platform.
- **UDP traffic flows in Illumination could be confusing** (E-84615)
  How the PCE displayed UDP traffic flows in Illumination could be confusing because of the way the VEN evaluated flows for UDP (which is connectionless). For example, Illumination could display false positive flows for the syslog service. Syslog listens on local UDP ports while acting as a client (sending only outbound packets from those ports). This issue is

resolved. In this release, Illumio adjusted VEN heuristics for determining UDP flow directions. The VEN now accounts for local and remote UDP port numbers. If local UDP port numbers are ephemeral (>= 1024) and remote UDP port numbers are privileged (< 1024), the VEN doesn't treat these UDP flows as inbound even when a service is listening on the local port.

- **VEN installed on mail server could cause higher failure percentage for PCE and 500 errors in log** (E-83722, E-83439)
  When installing the VEN on a mail server, the PCE could report a higher failure percentage and the PCE collector logs included HTTP 500 errors. This issue occurred because each FQDN on a mail server can map to multiple aliases.The VEN's ability to report all aliases mapped to each FQDN greatly increased the size of the VEN flow log file, which in turn negatively impacted the PCE collector. This issue is resolved. This information was not being used by the PCE. Therefore, the VEN no longer reports all aliases mapped to each FQDN in this release.

Resolved Issues in Core 21.2.3

PCE Web Console

- **Initial VEN Version reverted to the Current Default when editing a profile** (E-82523)
  When editing a pairing profile (**Workloads and VENS > Pairing Profiles**), the VEN version specified in the **Initial VEN Version** field reverted to the **Current Default** VEN version automatically. This meant that, unless the user re-entered the previously-specified VEN version, the current default version of the VEN was installed on the workload instead, which was unexpected. This issue is fixed; the Initial VEN Version field retains it's configured version unless it's changed by the user.
- **Problem forwarding syslogs to an external server** (E-82503)
  When configuring the PCE to forward syslogs to an external server (**Settings > Event Settings**), addresses that include letters followed by any number were disallowed and the message " Invalid address" appeared below the Address field. This issue is fixed. The Address field now accepts addresses with numbers that follow letters.
- **Options missing when filtering Virtual Services** (E-82441, E-82227)
  When trying to filter a list of Virtual Services (**Policy Objects > Virtual Services**) by 'Name', 'Protocol', 'Port', or 'IP Address' categories, filter options didn't appear. This prevented fine-grained searches. This issue is fixed; filter options now appear as expected when filtering Virtual Services.
- **Could not search for segmentation rules by all services** (E-82342, E-82223)
  When searching for segmentation rules, you could not search by all services as the providing service in the PCE web console. From the PCE web console main menu, choose **Rulesets and Rules** > **Segmentation Rule Search** > **Segmentation Rules** tab. The filter drop-down list did not contain an option for “All Services.”

NOTE: You could still specify all services when searching for segmentation rules by using `POST /sec_policy/:pversion/rule_search` in the Illumio REST API.
This issue is resolved. In this release, the filter drop-down list in the PCE web console contains an option to search for segmentation rules by "All Services."

- **Navigation error when filtering with 'Policy Last received' in workloads list page** (E-82047)
  In the Workloads list page, when filtering with Policy Last Received, the error "Navigation has been canceled due to an error" was displayed. This issue is resolved.
- **Could not delete attributes from workload** (E-81922)
  When editing a workload in the Edit Workload page, if you deleted attributes in the Host Attributes section, the deletion did not take effect. This issue is resolved.
- **Enforcement Boundaries page wasn't available to SuperCluster members** (E-81891)
  In the web console for PCE SuperCluster members, the Enforcement Boundaries page (**Rules and Rulesets > Enforcement Boundaries**) was not available. This issue is fixed. SuperCluster members can now view the Enforcement Boundaries page.

Policy and Workloads

- **Deleting a rule incorrectly updated provision status** (E-82089)
  Deleting a rule updated the provision status for all rules in the ruleset to "Modification Pending" when they hadn't changed. The status for the deleted rule was correctly updated to "Deletion Pending." This issue is resolved. Deleting a rule no longer impacts the provision status of other rules in the ruleset.

PCE Platform Resolved Issues

- **Internal `syslog-ng` configuration incorrectly filtered forwarding rules** (E-81996, E-77709)

  ⚠ This issue applies to Illumio Core On-Premises customers only.

  Forwarding rules could be incorrectly filtered, which resulted in events incorrectly appearing in `collector.log` or failing to appear. This issue occurred under the following conditions:
  (1) When configuring a forwarding destination for traffic flow events, if the user selected allowed events, all traffic events for that org were forwarded to the same destination.
  (2) In other configurations, flow events could fall through to the on-disk `collector.log`, instead of being discarded.
  (3) For multi-org configurations, any orgs without a configuration could result in logs falling through to the `collector.log`. System events could also fall through to the `collector.log`. Health events were not affected.
  This issue is resolved. Under these conditions, forwarding rules are correctly filtered.

- **Removing node from cluster no longer results in undefined method error** (E-81801)
  The command `illumio-pce-ctl cluster-leave ip|node-name` removes a failed node from the cluster. Because of a temporary connectivity issue at the consul level, this command sometimes failed with an error like the following:
  `undefined method `code' for nil:NilClass (NoMethodError)`
  This issue is resolved.
- **Time Drift warning for PCE nodes was misleading** (E-81610)
  The Time Drift health warning is displayed in the PCE Health page when time drift is detected between two PCE nodes. Time drift is the difference between the time when PCE cluster health was generated and the time when node health was generated. If NTP was not set up correctly, the PCE might use stale information to generate the Time Drift warning, so the Time Drift warning message could be misleading. This issue is resolved. The Time Drift warning message is now accurate.
- **Auditable events were missing Label changes in a label group** (E-81608)
  If you added or deleted labels in a label group, the generated auditable event didn't show the label changes you made in the label group. This issue is resolved. Label addition and deletion in a label group now shows up properly in auditable events.
- **Details for removed node no longer visible in PCE Health** (E-81353)
  The command `illumio-pce-ctl cluster-leave` removes a node from the PCE, but it did not remove details about the removed node from the PCE internal registry. As a result, the PCE Health page showed nodes that were no longer participating in PCE operations. This issue is resolved. The removed nodes do not appear on the PCE Health page.

REST API

- **Events API returns improper information** (E-81615)
  The Events API did not correctly provide all resource changes in the resource changes section of the event for ruleset changes. This issue is resolved.
- **Virtual Services events incorrectly reported** (E-81609)
  The Events API did not expose address pool changes or label deletion information when performing virtual service updates. This issue is resolved.
- **Events API returning insufficient information** (E-81867)
  The Events API did not expose changes to the service process `name` or process `path` for Windows-based service updates. This issue is resolved.
- **Events API firewall_settings returns wrong values** (E-81959)
  The Events API was exposing only creation and not the deletion information for policy scope sub-properties on `firewall_settings` resource changes. This issue is resolved.

VEN

- **Windows VEN stopped PCE REST API requests and responses** (E-82436)
  When the REST API for Windows proxy discovery returned an undocumented error, the VEN ended the API call. This issue is resolved. In this release, when Windows proxy discovery returns an error, the VEN connects directly to the PCE instead of connecting through the proxy.
- **Linux VEN reported tampering events** (E-81589)
  When the VEN was running on a CentOS 6 host and that workload was configured to use firewall coexistence, the VEN could incorrectly report tampering events every 10 minutes. This issue is resolved. The VEN no longer reports tampering events when running on CentOS 6 with firewall coexistence.
- **PCE Windows pairing script could unexpectedly uninstall an installed VEN** (E-81163)
  The PCE pairing scripts do not support upgrading installed VENs. However, when accidently run on an installed VEN, the Windows pairing script can unexpectedly uninstall the VEN on the workload. When a VEN is already installed on a workload, attempting to pair a new VEN for that workload should fail and leave the currently installed VEN intact. Instead, the PCE does not detect that the VEN is already installed. This issue is resolved. In this release, running the Windows pairing script on an installed VEN fails and leaves the VEN installed.
- **VENs on RHEL 8.3 and 8.4 workloads unable to apply policy to affected workloads** (E-81276)
  Due to an nftables issue in RHEL 8.3 and 8.4, the VENs on these workloads failed to load ipsets and apply policy to the affected workloads. Consequently, the workloads remained in a policy sync mode error state. Additionally, the VENs logged errors in the Workload Support report every 5 minutes after they heartbeat with the PCE. This issue is resolved. In this release, the VEN is able to workaround the underlying nftables issue so that RHEL 8.3 and 8.4 workloads can load ipsets and apply policy to the workloads without the workloads getting stuck in an error state.
- **Moving Windows VEN to Enforced mode could cause host to crash** (E-81136, E-81699)
  The host could crash when moving the VEN to Enforced mode. This issue occurred when the VEN was installed on Windows 7 or Windows Server 2008 R2 hosts that were also running McAfee or Symantec Endpoint Protection software. This issue occurred because of a defect in the Windows Filter Platform (WFP). Newer Windows operating systems were unaffected. This issue is resolved. Moving a Windows VEN to Enforced when running on a host described above no longer causes the host to crash.
- **Error thrown after initial VEN installation on Solaris** (E-79785)
  After installing a VEN on Solaris for the first time, the following errors occurred during activation:
  ```
  ld.so.1: curl: fatal: libcurl.so.4: open failed: No such file or directory
  ld.so.1: AgentSend: fatal: libjansson.so.4: open failed: No such file or directory
  ```
  These errors were caused by applying a non-default setting of `LD_LIBRARY_PATH_64` in the root

shell environment. This issue is resolved. Installing the VEN on Solaris no longer triggers these errors during VEN activation.

Security Information

- **Postgres password included in command line** (E-82459)
  In certain scenarios, such as a PCE upgrade, the Postgres password was passed as an argument on the command-line, and could be viewed during a brief window of time by other users logged-in locally to the host. This issue is resolved.
- **Security headers for nginx** (E-82298)
  In this release, Illumio has enabled additional security headers for the nginx endpoint. Under normal circumstances, nginx is inaccessible outside the PCE cluster.

Resolved Issue in 21.2.2+UI2-PCE

⚠ This release upgrades the PCE web console UI alone, which is possible because the UI version is compatible with the installed PCE version. The resolved issue in this release affects the PCE web console UI only. For information about upgrading the PCE UI, see PCE UI-Only Upgrade in the *PCE Installation and Upgrade Guide*.

- **Unable to search for segmentation rules by all services** (E-82342, E-82223)
  When searching for segmentation rules, you could not search by all services as the providing service in the PCE web console. From the PCE web console main menu, choose **Rulesets and Rules** > **Segmentation Rule Search** > **Segmentation Rules** tab. The filter drop-down list did not contain an option for "All Services."
  NOTE You could still specify all services when searching for segmentation rules by using `POST /sec_policy/:pversion/rule_search` in the Illumio REST API.
  This issue is resolved. In this release, the filter drop-down list in the PCE web console contains an option to search for segmentation rules by "All Services."

Resolved Issues in Core 21.2.2

PCE Web Console

- **Incorrect policy delivered to VEN due to race condition** (E-80317)
  An extremely rare race condition could cause the PCE to deliver partial policy to the VEN.

This condition occurred when two independent processes—one that reads from a cache and one that invalidates the cache—interleaved at exactly the right time. This issue is resolved.

- **Location of All Services option was inconsistent in Enforcement Boundaries page** (E-79953)
  In the Enforcement Boundaries editing page, the All Services option could only be selected by searching in the Services category. This was inconsistent with other rule writing pages, where All Services exists as a separate category, and could therefore be selected directly without searching. This issue is resolved. The All Services option is now in its own separate category, not in the Services category.

Policy and Workloads

- **PolicyPerspectiveDraftCache Can Be Stale** (E-81152)
  In very rare cases, draft policy decisions in Illumination and Explorer, rule search, and policy check would return incorrect results based on an older version of the policy. This has not been observed in on-prem deployments. It is fixed for all PCE deployments.
- **Unable to add unmanaged workload on a rule if it is not within the scope of labels previously added** (E-80031)
  Scoped workloads were not shown in the Workloads list that is used to add a workload to a rule, unless the workload's scope was within the rule's scope. This issue is resolved. Workloads are no longer filtered out of the Workloads list based on their scope.
- **Decreasing PCE runlevel causes node stuck in EXCEED** (E-79930)
  When the runlevel was decreased from 5 to a lower level (2 or 1), the PCE software might fail to stop all the processes of services not allowed to run at the lower runlevel. Checking the PCE status (`illumio-pce-ctl status -s -v`) would show the message `Runtime system EXCEED`. This issue is resolved.
- **VEN upgrade timeout condition persisted when VEN upgraded outside PCE** (E-79692)
  When a VEN upgrade is initiated from the PCE UI or API, if the VEN does not successfully upgrade within 1 hour, the event notification message `agent.upgrade_time_out` is issued, and the VEN page in the PCE UI shows "Warning: VEN Upgrade timed out." In previous releases, if a VEN upgrade timed out and the VEN was later upgraded independently (such as with RPM or MSI), the timeout condition was not cleared. This issue is resolved. No matter what technique is used for the successful VEN upgrade, the timeout condition is cleared, and the "VEN Upgrade timed out" message is removed from the VEN page.
- **After adding a rule, App Group Map is not filtering out the correct traffic** (E-79587)
  In the App Group Map, when two flows between the central app group and two connected app group roles used the same ports, and a rule was written to allow one of the flows, both flows were considered allowed for the collapsed app group. This could be seen by filtering allowed flows out of the App Group Map. The connected app group no longer appeared in the list of connected groups, even though there was still a blocked flow left. This issue is resolved. The rules for one flow no longer affect the display of other flows using the same ports.

- **Internal Server error when bulk creating Unmanaged Workloads in public cloud datacenters** (E-77964)
  A 500 error on workload bulk create could appear when the workload triggered the PCE's public cloud detection algorithm. This only happened when the workload had a `data_center` property that matched a public cloud data center that the PCE knew about. In addition, there had to be a default gateway address on one of the workload interfaces, and the workload must have had a public IP. This issue is resolved.

Data Visualization

- **Custom iptables UI issue** (E-80817)
  The UI for the custom IP tables rules column and the notes column was improperly sized and obstructed the custom IP tables rules.
  This issue is resolved.
- **Reloading Illumination could take a long time** (E-80735)
  Reloading the Location view of the Illumination map could take a long time when the PCE had to rebuild the cache for the graph. This issue could occur when different workloads within the queried graph communicated with the same peer workloads and the PCE processed the peer workload subgraphs multiple times. This issue is resolved. In this release, peer workloads are added to the graph after removing duplication.
- **Virtual Server rules information inconsistent for read-only users** (E-80692)
  For read-only users, “Active version of rules” that is shown is not the current version of active rules on the Virtual Server. Read-only users were unable to identify which active rules are applicable to the Virtual Server before the changes are provisioned. They were also unable to switch between draft and active version of Virtual Server. This issue is resolved.
- **Initial search results missing after navigating back to Explorer** (E-79823)
  When searching in Explorer, navigating away, and then returning to Explorer, the results of the most recent search were not displayed. This issue is resolved. When you click **Results**, the results of previous searches (not older than 24 hours) are now displayed correctly.

VEN Resolved Issues

All VEN Platforms

- **Firewall tampering sometimes detected in error** (E-81509)
  In some cases, VENs falsely detected host firewall tampering. This in turn caused the VEN's firewall tampering protection to fetch the current security policy stored on the PCE and return the host firewall to its pre-tampered security policy state. The tampering attempt, though false, was reported to the PCE as an `agent.tampering` event. This issue is resolved.

- **VEN didn't resume TLS session with PCE** (E-81019)
  In Illumio Core 20.2.0 and later releases, the VEN could encounter an issue that caused it to not resume its TLS session with the PCE. This issue adversely impacted PCE performance by increasing CPU utilization. This issue is resolved. In this release, the VEN is no longer impacted and correctly resumes TLS sessions with the PCE.

Linux VEN

- **Linux VEN with custom iptables rules reported tampering alert after VEN upgrade** (E-80836)
  This issue occurred after upgrading the VEN from a release prior to 20.2.0 to 21.1.0 or a later release. This bug only applies to customers with custom iptables rules. This issue is resolved.

Windows VEN

- **High Memory Consumption by Windows VEN Platform Handler** (E-81379)
  On Windows workloads, the VEN Platform Handler process was consuming an unusually high amount of memory. This issue is resolved.
- **Explorer wasn't displaying FQDN information when the workload's DNS server list changed** (E-81131)
  When a workload's DNS server list changed while the VEN was running, Explorer could stop providing the FQDNs associated with traffic flows. This issue occurred when FQDN policy wasn't created for the workload.
  This issue is resolved. In this release, changes to a workload's DNS server list no longer cause Explorer to stop providing the FQDNs for flows even when FQDN policy wasn't applied for the workload.

AIX/Solaris VEN

- **Adding FQDN-based rule for AIX/Solaris workload generated tampering events** (E-82001)
  When adding an FQDN-based rule to an AIX/Solaris workload, the PCE generated an erroneous egress rule for the workload, which triggered tampering events every 10 minutes. (FQDN-based rules aren't supported for AIX/Solaris workloads because they use ipfilter.) This issue is resolved. Adding an unsupported FQDN-based rule for an AIX/Solaris workload no longer generates tampering events for the workload.

Security Information

- **Security fix in the PCE** (E-66806)
  In Core Core 21.2.2-PCE, Illumio patched GNOME glib to address *CVE-2019-12450*. For

information see https://access.redhat.com/security/cve/cve-2019-12450 in the Red Hat Customer Portal.

> ⚠ The glib version in the PCE open-source packages did not change due to this patch. The PCE still uses glib version 2.54.3 (licensed by LGPLv2.1). See the Illumio Core Open Source Licensing Disclosure 21.2.2 in the Illumio Documentation Portal for more information.

For additional information about security issues, security advisories, and other security guidance pertaining to this release, see Illumio's Knowledge Base in Illumio's Support portal.

Resolved Issues in Core 21.2.1+H3-PCE

> ⚠ This release is available for Illumio On-Premises customers only.

- **PCE Support for RHEL 8** (E-81135)
  In 21.2.1, Illumio added support to run the PCE on RHEL 8. See Changes in This Release - RHEL 8 Support in the *What's New Guide*.
  In Core 21.2.1+H2-PCE, Illumio introduced a fix that inadvertently prevented PCE services from starting correctly on RHEL 8. This issue is resolved in Core 21.2.1+H3-PCE.
- **Lightning bolts to VENs failed** (E-81209)
  In some cases, lightning bolts to VENs could fail and the PCE couldn't propagate policy until the next VEN heartbeat. This issue is resolved in Core 21.2.1+H3-PCE.

Resolved Issues in Core 21.2.1+H3-VEN

> ⚠ This release is available for Illumio Cloud customers and Illumio On-Premises customers.

- **(Windows) Explorer wasn't displaying FQDN information when the workload's DNS server list changed** (E-81131)
  When a workload's DNS server list changed while the VEN was running, Explorer could stop providing the FQDNs associated with traffic flows. This issue occurred when FQDN policy wasn't applied to the workload. This issue is resolved. In this release, changes to a workload's DNS server list no longer cause Explorer to stop providing the FQDNs for flows even when FQDN policy hasn't been applied to the workload.

- **VEN deleted custom iptables rules from workload policy** (E-81055)
  This issue occurred when the VEN detected a change in the environment, such as adding a new member to an IPList in the PCE (often referred to as an “actor-only” change). After the PCE synced policy with the VEN, the VEN deleted custom iptables rules from the workload policy. As soon as the VEN performed a tampering check (usually within 10 minutes), it reapplied the custom iptables rules to the workload policy. This issue is resolved. In this release, the VEN no longer deletes custom iptables rules when it detects a change in the managed environment, such as new IPLists members.
- **VEN didn't resume TLS session with PCE** (E-81019)
  In Illumio Core 20.2.0 and later releases, the VEN could encounter an issue that caused it to not resume its TLS session with the PCE. This issue adversely impacted PCE performance by increasing CPU utilization. This issue is resolved. In this release, the VEN is no longer impacted and correctly resumes TLS sessions with the PCE.
- **(Windows) Policy sync could fail for IPv6 addresses that ended with “::”** (E-80565)
  When a Windows VEN encountered an IPv6 address that ended with "::" in the DNS server list, policy sync for that workload could fail; for example:
  2001:4888:66:ff00:645:d::
  This issue is resolved. In this release, IPv6 addresses in the DNS server list that end with “::” no longer cause policy sync with the PCE to fail on the workload.
- **(Linux) VEN dropped traffic** (E-79540)
  For workloads running nftables (CentOS 8.2 and RHEL 8.2), the native host firewall was dropping packets for ingress and egress traffic to and from the workload. This issue is resolved. In this release, the host firewall no longer drops packets when the VEN is running on CentOS 8.2 or RHEL 8.2.

Resolved Issue in Core 21.2.1+H2-PCE

⚠ This release is available for Illumio Cloud customers and Illumio On-Premises customers.

- **Reloading Illumination could take a long time** (E-80735, E-80590)
  Reloading the Location view of the Illumination map could take a long time when the PCE had to rebuild the cache for the graph. This issue could occur when different workloads within the queried graph communicated with the same peer workloads and the PCE processed the peer workload subgraphs multiple times. This issue is resolved. In this release, peer workloads are added to the graph after removing duplication.
- **Change to HAProxy version** (E-80812)
  Portions of the Illumio Core software are comprised of Open-Source Software and Third-Party

Software. In this release, the haproxy package version downgraded from v2.2.8 (Core 21.2.1-PCE) to v1.8.20 (Core 21.2.1+H2-PCE).

Resolved Issue in Core 21.2.1+H2-VEN

⚠ This release is available for Illumio Cloud customers and Illumio On-Premises customers.

- **Timeout for firewall requests increased to reduce PCE system load** (E-80649)
  In the previous release, the timeout value the VEN used to wait for PCE responses was the same as the PCE's maximum queuing time. When the PCE experienced heavy system load, the VEN could timeout before the PCE retrieved the VEN request from its queue. The PCE still computed workload policy but consistently discarded it. This issue kept the system load on the PCE high. In this release, Illumio increased the VEN "wait-for-response" timeout value to reduce PCE system load.

Resolved Issue in Core 21.2.1+H1-PCE

⚠ This release is available for Illumio Cloud customers only.

- **Incorrect policy delivered to VEN due to race condition** (E-80665, E-80317)
  An extremely rare race condition could cause the PCE to deliver partial policy to the VEN. This condition occurred when two independent processes—one that reads from a cache and one that invalidates the cache—interleaved at exactly the right time. This issue is resolved.

Resolved Issues in 21.2.1

PCE Web Console Resolved Issues

- **Incorrect or incomplete policy could occur due to a race condition** (E-80317)
  In rare cases, a race condition caused the PCE to deliver incomplete policy to the VENs. VENs in the enforced policy state could drop traffic until a policy change occurred. This condition was (but not exclusively) triggered by stopping the PCE software non-gracefully or by performing a hard reboot of the PCE data nodes. This issue is resolved.
- **Blank page displayed in Virtual Services tab** (E-80248)
  In the Workload details page for a workload that was bound to a virtual service, when clicking

the Virtual Services tab, a blank page was displayed. The cause of this issue was an error in a function call. This issue is resolved, and the Virtual Services page is now displayed.

- **Blank page displayed after clicking Bind under Virtual Service > Workloads** (E-80149)
  When trying to bind workloads to a virtual service using the **Virtual Service** > **Workloads** page, after clicking **Bind**, a blank page was displayed. The error occurred when a service was created with Window Services without protocol and ports, which caused a JavaScript error. This issue is resolved, and the Bind page is now displayed.
- **Blocked traffic page doesn't display results** (E-79486)
  In the browser's network console, the data download is visible but that download never populates the page.
  This issue is resolved and the blocked traffic page now working well.
- **Blank page for enforcement boundary after deleting its IP list** (E-79476)
  After deleting an IP List that is referenced by an enforcement boundary, a blank page is displayed in the enforcement boundary's page. This issue is fixed by not allowing an IP List to be deleted if it is referenced by an enforcement boundary.
- **Unable to remove a CSV or JSON report** (E-77774)
  You could view and download CSV and JSON reports for workloads and VENs from Export Reports, but you could not delete the reports. Clicking the **Remove** button, resulted in an "Invalid UUID format" error. This issue is resolved. In this release, you can remove Export Reports.

Policy and Workloads Resolved Issues

- **Policy review unable to determine if service was deleted** (E-78946)
  When the number of services exceeded 10, the policy review was unable to determine whether the service was deleted. This issue is resolved.
- **Policy Generator used the wrong label for the extra-scope rule** (E-78595)
  Policy Generator was not using the right label when generating the extra-scope rule. This issue is resolved.
- **In multi-port rules, deleting a port didn't reflect the change** (E-77405)
  In multi-port rules, deleting a port did not reflect the change when the rule had more than 10 ports or services. This issue is resolved.
- **Intermittent PCE performance issues occurred** (E-76881)
  A long IP list in the Exclude field was greatly affecting the query performance. This issue is resolved.

Data Visualization Resolved Issues

- **Unmanaged workload didn't show labels in Explorer search** (E-79098)
  When querying for an unmanaged workload, the workload was found, but its labels did not

appear. This issue is resolved. The PCE now performs a periodic resync of all unmanaged workload data.

- **Explorer kept old scope active after user label scope change occurred** (E-77717)
  When you changed a User scope, there was a delay of several minutes before the old scope data disappeared and the new scope could be queried. This issue occurred only when the session was obtained from an asynchronous query API. For other APIs, the user session is obtained directly, and this issue did not happen. This issue is resolved. The delay in refreshing scope data no longer occurs.
- **Container workloads weren't searchable in Explorer view** (E-72547)
  Using Explorer, users have to be able to search for Consumer or Provider container workloads. However, these workloads were not searchable.
  This issue is resolved.

PCE Platform Resolved Issues

- **Connectivity issue occurred after switching server IP addresses** (E-79229)
  In rare circumstances, concurrent changes to workloads, such as changes to labels or IP addresses, and VEN policy requests would result in partial or incorrect policy. This issue is resolved.
- **Ephemeral directory was sometimes temporarily deleted during PCE start, stop, restart** (E-79062)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  When using `illumio-pce-ctl` commands, the ephemeral directory would sometimes be temporarily deleted, which would lead to the following error being displayed: `The property 'ephemeral_data_root' value='/var/lib/illumio-pce/tmp' directory doesn't exist`. The directory would later be recreated, so there was no functional impact. This issue has now been resolved, and the directory is no longer deleted.
- **Self-signed certificate validation error occurred on RHEL 8** (E-78985)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  On RHEL 8, a self-signed certificate could not be validated when installing the PCE. When running the `illumio-pce-env check` command, an error like the following was displayed: `Certificate validation issue with web_service_certificate`. The cause was differences between versions of OpenSSL. This issue is resolved. Certificate validation is now successful.

- **Container workloads were not reported to PCE in IKS** (E-78971)
  Container workloads running in IKS were not reported to the PCE. This was caused by the usage of loopback interfaces in IKS clusters. This issue has been resolved.
- **Cached header fields could display inaccurate information in PDF reports** (E-78744)
  When an identical report was requested by two users within a span of one hour, some fields in the report (in PDF format) were inaccurate. The same was true for two recurrence reports that were run within one hour of each other. Because reports are stored in cache for one hour, two identical requests could have displayed the incorrect cached data for the "title" or "generated by" fields in the PDF document. Reporting is a "Preview" feature in Release 21.2.1. This issue is resolved.
- `node-revert-config` **failing to restart the services** (E-78609)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  During the restoration to a full cluster from a split-brain situation, `illumio-pce-ctl node-revert-config` might have failed to restart the services causing the cluster to get stuck in status PARTIAL. This issue is resolved.
- **PCE Health timestamp was incorrect** (E-78207)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  In Core Release 21.2.0, the PCE timestamp that appears on the PCE Health user interface displayed the Universal Time Coordinated (UTC) instead of the local time. The time reported was not synchronized with the actual time zone. This issue is resolved by applying the timezone offset beside the timestamp, which results in the expected local time.
- **Support for consumer process/service/username was missing** (E-78198)
  This issue is resolved. There is no need anymore to separate consumer and provider side process/service/user names in the exported CSV file.
- **Cluster name for SAML configuration displays the cluster on which the SAML configuration was created** (E-76489)

  > ⚠ This issue applies to Illumio Core Cloud customers only.

  By default, customers get Single Sign-On Access to different clusters in Illumio Cloud. When logged in to any one cluster, the cluster name for SAML configuration displayed the cluster on which the SAML configuration was created. The cluster name displayed was incorrect if the user was logged into a different cluster. This issue is resolved.
- **PCE public cloud detection was not working** (E-76238)
  CE NAT detection was not working for certain AWS EC2 regions, and workloads in specific EC2 regions would not be associated with their public/elastic IP addresses. As a result, the

workloads' NAT addresses were not programmed in the peer workloads' firewalls, which could lead to dropped traffic if it came from the NAT address.
This issue is resolved for newly paired VENs.

- **Audit Events 2.0 data isolation was fragile** (E-59448)
  All events were logged with the user syslog facility, and auditable events were not well separated into easily findable categories. This issue is resolved. When remote syslog forwarding is turned on, events will now be logged using the local5, local6, and local7 syslog facilities for audit, traffic, and health events respectively.

Supercluster Resolved Issues

⚠ These issues for Supercluster apply to Illumio Core On-Premises customers only.

- **User still logged in after logout on Supercluster member** (E-79936)
  On a Supercluster member PCE, the user session could persist after the user logged out. The login session did not expire. This issue is resolved. The more accurate logout mechanism from the leader PCE is now used on the members as well.
- **Inconsistent numbers of VENs and workloads reported on PCEs in Supercluster** (E-79205)
  In a Supercluster, the VEN status and count could be inconsistent across PCEs. This issue occurred as a result of the following sequence of events: a VEN was unpaired from the UI or northbound API, the host was decommissioned so the unpair was not acknowledged by the VEN, and there was a Supercluster backup/restore. This issue is resolved. Inactive VENs are now correctly removed from the total.
- **Replication check failed on Supercluster** (E-78722)
  When a replication service restart was requested from a remote region, the request could be ignored by the target region if a restart was already in process. This race condition could result in ignoring the replication configuration change. Replication could be performed based on an older configuration. This could result in replication failure. This issue is resolved. Replication no longer gets stuck in an older configuration.
- **Adding addresses to cluster_public_ips failed to work on member** (E-78618)
  In a Supercluster, when a PCE's public IP addresses are changed (`public_ips` in the PCE Runtime Environment File), the PCE must be restarted. After a restart, once all services are running on this PCE, the other PCEs should be restarted. Without ordering the restart, there's a chance that VENs paired to other PCEs in the Supercluster might not get the IP address change update.
- **PCE did not prune uninstalling agents after a Supercluster restore** (E-78498)
  In a Supercluster, the VEN status and count could be inconsistent across PCEs. This issue occurred as a result of the following sequence of events: a VEN was unpaired from the UI or northbound API, the host was decommissioned so the unpair was not acknowledged by the VEN, and there was a Supercluster backup/restore. This issue is resolved. Uninstalled VENs

are now removed from the PCE after the appropriate delays, even if a Supercluster backup/restore is performed.

- **Running pg_app_lock and supercluster-join commands could cause a broken state** (E-78380)
  Supercluster commands sometimes resulted in a locked state due to the IP restrictions and PG app lock flow. This issue is resolved.
- **Attempt to create API key on Supercluster member returned incorrect error code** (E-75627)
  When creating a new API key with a POST call to the `api_keys` endpoint on a PCE that was a member of a Supercluster, the API returned an error. This is the expected behavior because creating an API key on a Supercluster member is not allowed. However, the API returned a 500 error, which was the incorrect code; it should be 403. This issue is resolved. The API call now returns the correct 403 error code.

VEN Resolved Issues

- **VEN could fail to block outbound UDP traffic when FQDN policy was used** (E-80134)
  This issue occurred under the following conditions:
  - The FQDN-based rule included a non-TCP protocol, port, or port range
  - An app sent traffic to an IP address that didn't use the FQDN A/AAAA record
  - The outbound traffic had the same port or was in the same port range as the FQDN policy

  This issue is resolved in this release.
- **Korn shell (ksh) limitation on array size** (E-79381)
  The platform log could include an error similar to the following one:
  `ERROR:: unknown line in ilo_ipset output: /opt/illumio_ven/bin/ilo_ipsets: arr: 0403-046 The specified subscript cannot be greater than 4095`
  The issue occurred because the version of `ksh` being used did not support arrays larger than 4095 elements. This issue is resolved. The array size limitation is no longer encountered.
- **venAgentMonitor incorrectly reported venVtapServer was not running** (E-79244)
  When using the VxFS filesystem, the VEN agent monitor might indicate that a VEN process was not running, even though the VEN process was running. This issue is resolved.
- **Erroneous event reported on Solaris or Linux systems** (E-79206)
  When IPv6 addresses were not configured on Solaris systems or when IPv6 transport was disabled on Linux systems, they could result in the VEN erroneously reporting `fw_tampering_revert_failure` events. This was due to transient connectivity problems that prevented the VEN from reaching the PCE. This issue is resolved.
- **Traffic allowed by FQDN rules was blocked approximately every 24 hours** (E-79156, E-78469)
  The Windows implementation of the FQDN feature did not re-calculate the effective DNS record TTL correctly, which could lead to sporadic blocking of traffic that should have been allowed by FQDN policies. This issue is resolved.

- **Netlink socket buffer overflow prevented vTAP from entering sampling mode** (E-78792)
  When a workload experienced a high rate of connections/traffic flows, the Illumio vTAP process `venVtapServer` running on the workload couldn't enter sampling mode and consumed a high percentage of CPU utilization (30-40%). This issue is resolved. Note that high rates of connections/traffic flows can still cause the Netlink socket buffer on the workload to overflow; however, the situation won't prevent the vTAP process from entering sampling mode.
- **VEN could fail to pair with the PCE when a proxy server was present** (E-78610)
  In Core 20.2.0-VEN and later releases, the Windows VEN automatically detects the presence of a web proxy server in a network environment. When the VEN detects a web proxy server, it communicates with the PCE using only that web proxy server. However, when the web proxy server was misconfigured, the VEN wasn't able to connect to the PCE. This issue is resolved. In this release, the VEN first connects with PCE directly even when it detects a web proxy server. If that attempt to connect with the PCE fails, then VEN uses the web proxy server for communication.
- **VEN issues as a result of recent Solaris patches now resolved** (E-77942, E-77712)
  Recent Solaris patches for Solaris 10 SPARC 148379-16, Solaris 10 Intel 148380-16, and Solaris 11 LSU 11.3.36.23.0, provided a fix for an IP Filter kernel memory leak. These patches introduced an unexpected behavior in IP Filter `/usr/sbin/ippool`. It resulted in the VEN inaccurately flagging potentially blocked traffic in test mode, inadvertently blocking traffic in enforced mode, and causing the VEN to go offline. These issues are resolved.
- **VEN NFTable machine auth egress rule issues** (E-77937)
  On a Linux device, a VEN with NFTable support failed to generate machine authentication egress rules. This issue is resolved.
- **(AIX and Solaris) File group ownership issues are resolved** (E-77763)
  On AIX and Solaris systems, incorrect group ownership of files posed a problem. The following three files were inaccurately assigned to the `ilo-ven` group:
  - `/etc/ipf/ipf.conf`
  - `/etc/ipf/ippool.conf`
  - `/etc/objrepos/usilc.vc`

  This issue is resolved. The `/etc/ipf/ipf.conf` and `/etc/ipf/ippool.conf` files are now correctly assigned to the `sys` group on Solaris and the `system` group on AIX. The `/etc/objrepos/usilc.vc` file is no longer generated.
- **Windows workloads reported Teredo tunnel interfaces** (E-75043)
  The behavior to report Teredo tunnel interfaces changed in the Core 21.2.0 release; however, Windows workloads continued to report them. This issue is resolved in Core 21.2.1.
- **(AIX) Workloads dropped traffic from NFS servers** (E-73353)
  AIX workloads dropped traffic from NFS servers added to the PCE as unmanaged workloads. The AIX workload dropped this traffic even when a rule existed in the PCE allowing the traffic. This issue occurred due to TCP port number reuse. This issue is resolved in the following way. In 21.2.1, the VEN IPFilter state table supports a new option to handle this situation:

VEN File Setting: `IPFILTER_TCPCLOSED=<value>`
ipfilter Setting: `fr_tcpclosed=<value>`
The values for the VEN File Settings options are defined in 500ms units. By default, the value for v`fr_tcpclosed` is 120, which is 60 seconds. To address this issue with NFS traffic, add the `IPFILTER_TCPCLOSED` option to the `/etc/default/illumio-agent` file and specify a new value. Create the file on the workload if it doesn't exist. Illumio customers have found that setting the value for the `IPFILTER_TCPCLOSED` option to 2 (2 equals 1 second) resolved the issue.

Updates for 21.2.0+H2-VEN

Starting with the Illumio Core 21.2.1 release, the Windows VEN installer will switch from the MSI to EXE package format. Customers upgrading their VENs by using the PCE-based VEN deployment (the VEN Library) must take an extra step for the transition.

Specifically, Illumio Core customers running older MSI-based Windows VENs must upgrade to 19.3.6+H1-VEN or 21.2.0+H2-VEN before upgrading their VENs to 21.2.1 or a later version. The 21.2.0+H2-VEN release contains the necessary VEN changes to handle the transition in the VEN packaging from MSI to EXE format.

Changed Behavior in 21.2.0+H3-PCE

- **Support for weak ciphers enabled by default** (E-79662)
  This release changes the default value of the PCE runtime parameter `insecure_tls_weak_ciphers_enabled` from false to true. The behavior change only affects customers who have already upgraded their Core PCE to 21.2.0, 21.2.0+H1, or 21.2.0+H2. Stronger ciphers are recommended; however, the use of weak TLS cipher block chaining (CBC) is now supported by default. You can change the default setting to disable the weaker CBC ciphers on the PCE. See Enhanced Security for PCE TLS Configuration in the *What's New In This Release Guide* for more information.

Resolved Issues in 21.2.0

PCE Web Console

- **Blocked Traffic page didn't display results** (E-79486)
  The Blocked Traffic page in the PCE web console was always empty and didn't display any blocked traffic even when the PCE was blocking traffic to managed workloads. To work

around this issue, customers used Explorer in the PCE web console to view blocked traffic to their workloads. When you upgrade to the 21.2.0+H2-PCE release, this issue is resolved.

- **PCE web console didn't provide error information** (E-77781)
  When you provisioned policy to workloads, the PCE web console UI didn't provide information when an error occurred. A dialog box appeared when an error occurred but it did not provide any information about the error. This issue is resolved. When you encounter an error while provisioning policy, the PCE web console UI displays a dialog box with details about the error so that you can address the issue.
- **Multiple label groups could not be configured at the same time** (E-77018)
  Previously, only a single label group could be configured, not multiple label groups. This issue is resolved. Now, you can configure multiple label groups at the same time.
- **User interface did not display the list of virtual servers if greater than 500** (E-76894)
  The system has a limit of 500 virtual servers returned to the user interface. If more than 500 virtual servers were present in the system, the list of virtual server entries might not have included the entries that were expected. In addition, if filters were used, expected virtual servers might not have appeared on the list or merely appeared as a blank list because the returned virtual servers did not meet the filtered criteria. This issue is resolved.
- **Name field description for unmanaged workloads needs to be changed** (E-76695)
  The description help text next to the Name field for an unmanaged workload should have said, “Type a name for the new Unmanaged Workload” and not “Type a name for the new Pairing Profile.” This issue is resolved.
- **Privileges displayed for Global and Scoped Roles are incorrect** (E-76313)
  Inaccuracies regarding privilege levels and provisioning capabilities appeared in the user interface for global and scoped roles. These inaccuracies have been resolved.
- **PCE user interface did not allow you to view or change the configuration of switches** (E-75988)
  After a switch was set up from the Infrastructure menu, the user interface did give you to option to access the individual switch to view or change parameters. The browser only displayed a blank screen. This issue is resolved.
- **Online Help didn't display information in the Help popup** (E-75943)
  The Help popup didn't display information sometimes when it launched a separate popup window. For example, when you clicked the question mark icon, and then clicked the upward arrow in the Help popup that appeared, the new Help window that appeared didn't contain any Help information. This issue is resolved. The Help popups that appear in the PCE web console contain the relevant Help information.
- **Remove button counter is not cleared after removing members in a label group** (E-73775)
  After a member in a label group is selected and removed, the counter that displays a number when the member is selected does not clear that number when the member is deleted. This issue is resolved.
- **The “In Use By” field did not display that a provisioned Label Group was used** (E-73300)
  When a Label Group was provisioned and used by objects that were not provisioned, the “In

Use By" field did not accurately reflect that the Label Group was actually being used. The field displayed a "No" instead of a "Yes." This issue is resolved.

Policy and Workloads

- **Newly-created Unmanaged Workloads on a SaaS PCE inherited Public IP Addresses** (E-77070)
  After an upgrade, when unmanaged workloads on a SaaS PCE were created or updated, the workload's public IP was set to the public IP address of the device (or browser) that was used to make API calls. This IP address was not distributed to the peer workloads. This issue is resolved.
- **SLB user interface did not accurately update the "In Use" column** (E-77062)
  If more than 500 virtual servers were present in the system, the "In Use" value in the Virtual Servers column on the Server Load Balancers list page might not have been accurate. This issue is resolved.
- **Occasional issues with rules** (E-76344)
  In rare circumstances, some issues with rules were seen, where the VEN used to enforce incorrect IP addresses in the policy. This might have been caused by workloads (instead of labels) being used extensively in rules. Issues of this nature have been resolved.
- **App Group Map assumed flows allowed between labels in a label group** (E-75775)
  In the App Group map, flows that were not allowed could be shown as allowed. The issue occurred only when a label group was used in the scope of a ruleset. The map showed that flows between labels in the label group were allowed, but they should have been shown as blocked. This issue is resolved. Flows between labels in a label group are now correctly shown as not allowed.
- **Virtual Servers rules tab does not display IP addresses of pods** (E-74635)
  The IP addresses in the rules tab of a Virtual Server used to display only host IP addresses and not the container workload IP addresses. This issue is resolved.
- **Service protocols with no ports were handled incorrectly in CSV reports** (E-71321)
  When a CSV report contained embedded spaces, it implied that the service protocol contained ports even though it did not. This issue is resolved. The trailing spaces have been removed for protocols that do not contain ports.

Data Visualization

- **Services with a broader port range remove connections** (E-77915)
  Services with a broader port range do not remove connections in all cases. Only when the first port of the broader port range Services does not match the first port of the connections included on Policy Generator on the preview rule page, the connections are removed when the user selects the option to include policy services with a broader port range on the preview rule page.

For example:
If a broader port range policy service exists (such as a port range with 20-60 TCP) and the included connections on the policy generator configuration page are 20 TCP, 21 TCP, 22 TCP, then the connections are not removed when a user chooses to apply the Service with this broader port range on the Policy Generator preview rule page.
However, if the ports included in the policy generator configuration page are 22 TCP, 22 23 TCP, 24 TCP, then the connections are removed from the policy generator preview rule page.
NOTE: If multiple broad range services exist and one of them matches the first scenario in the example, the connections will not be removed. If only one service (instead of multiple services) with a broader port range exists and it does not match the first scenario in the example, the connections are removed.

- **Cluster restart can cause flow data loss** (E-77473)
  PCE cluster restart *could* result in flow data loss as the flows which are in-process would get archived. This issue is resolved.
- **Syslog did not receive all flow data** (E-77330)

  ⚠ This issue applies to Illumio Core On-Premises customers only.

  Syslog destinations can be configured to forward a subset of flows. When multiple syslog destinations were configured, the PCE would only consider the last configured destination when sending flow data to syslog. This could result in some classes of flows not being sent to syslog, even if some destinations were configured to allow them. For example, when the first destination was configured for allowed flows, and the last destination was not, no allowed flows would be forwarded. The issue has been resolved. All classes of flows configured in all destinations are forwarded to syslog.
- **UI Issue with the App Group Map** (E-77167)
  Users get incorrect data from the UI if the location label has more than 40 characters and selected behavior becomes erratic when using the App Group map.
- **Custom range not parsing the date correctly when not in US (month/day/year) format** (E-77071)
  Users have to change the browser time format to US.
- **Flow data was not available in Explorer due to missing** `fuser` (E-77010)
  The PCE relies on the `fuser` system program when processing flow data. However, in some operating systems, `fuser` is not present by default. As a result, the PCE would skip processing some batches of flows, so they would not be inserted into the traffic database, and the flow data would not be visible in Explorer. The data was still written to redis and syslog. This issue is resolved. A replacement method is provided for `fuser`.
- **Allowed Virtual Services flows shown as no policy** (E-76970)
  There was an underlying bug for 'Quick Response' Rule Coverage: If two flows had the same labels where one went to a virtual service and another went to a workload (and a rule existed

for 'Virtual Services Only'), the virtual service flow would show as “blocked” when it was actually “allowed.” This issue is resolved.

- **Explorer shows wrong Matched records** (E-76758)
  When the “maximum displayed” setting is exceeded, Explorer will show the number of “connections” in the table header instead of “matched” since the explorer table will limit the number of records.
- **Revise configuration parameters for scp1** (E-76640)
  Revise the `citus.max_intermediate_result_size` configuration parameters for scp1.
  When the amount of data set queried from the explorer is large (such as when making an 'Anytime' query), sometimes the database memory configuration of `max_intermediate_result_size` that was set to 1GB is reached and the queries fail.
  The fix was to increase the default value of this configuration to 2GB based on the in-house performance tests.
- **PCE crashed due to OOM** (E-76518)

  ⚠ This issue applies to Illumio Cloud customers only.

  When the number of concurrent queries from Explorer goes over a certain limit, the `citus` worker nodes run out of memory as the memory required to execute those queries is much higher than the available memory. This caused the PCE worker nodes to crash.
  Several configuration changes to Postgres and the node types have been provided so that this issue is not occurring anymore.
- **PCE performance for customers could be slow** (E-76377)
  When backing up the PCE database, Illumio customers could experience slow performance during Explorer queries, especially when the traffic database was reaching disk limits. This issue is resolved. Customers will no longer potentially experience slow performance with Explorer queries during their database maintenance for the PCE.
- **The policy generator doesn't map policy services correctly** (E-75845)
  When the policy service existed with a port range, the policy service was showing both on the connection and on the ports included in the policy service. These ports were also listed under the policy service on the Policy Generator Preview Rule Page.
  However, these ports should not have been listed separately under the policy service as it was a duplication. Only the policy service should have been listed as it included the ports listed separately for the connection.
  This duplication was removed with the fix. What you can view now on the preview rule page is only the policy service that has the port range shown on the policy generator for all connections on ports within the policy service port range.
- **Some larger groups do not work well in Draft View** (E-75786)
  Larger groups with extensive connectedness with vulnerabilities do not work well in the Draft View.
  Optimization was performed with data upload on the Illumination App Group Maps with

extensive connectedness. With data upload enhancements, this issue was not observed. Data upload has happened within the stipulated time frame for big groups.

- **Backlog disk utilization rises** (E-75600)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  (Partial fix) This issue has been updated with a new workaround. In 19.3.6+H1, additional logging functionality has been added to help when this issue occurs. For updated workaround instructions, see Data Visualization Known Issues in these release notes.

PCE Platform

- **PCE nodes ended up in PARTIAL state** (E-76711)

  > ⚠ This issue applies to Illumio Core On-Premises customer only.

  When performing PCE operations on nodes and the operation required restarting PCE software, some nodes could get stuck in the PARTIAL state because they failed to get information from the PCE consul. For example, restoring a PCE in a Supercluster and assigning the leader node caused other nodes in the cluster to get stuck in the PARTIAL state. This issue is resolved. Performing PCE operations that require restarting the PCE no longer cause nodes to get stuck in PARTIAL and now show the RUNNING status.
- **log: exception undefined method `private_dirty_rss'** (E-75972)
  In version 21.1, an occasional `private_dirty_rss` error occurred and was seen in logs. The error did not affect the functionality of the PCE. This issue occurred because the passenger was upgraded from 5.0.x to 6.0.7. In this version, the passenger changed the internal naming of processes that the PCE was using to distinguish application processes from others. This issue is resolved.
- **PCE system-generated events incorrectly contained internal PCE IP addresses** (E-75387)
  Within the events summary, there are certain events that are generated internally by the PCE, labeled as system tasks. These events included a source IP address which was displayed as one of the PCE node IP addresses. This issue is resolved. The string 'FILTERED' is displayed instead of the IP address.
- **Label groups were not allowed for a scoped user when adding/updating rule set, but choice appeared in UI** (E-63960)
  In the PCE Web Console's Add Ruleset dialog, when a user with a scoped role chose a label group in one of the Scope fields, the message "You cannot modify Rulesets with broader Scope(s) than your permitted Scope(s)" was displayed. The error was caused by the UI improperly presenting a scoped user with the choice to select a label group. The choice

should not have appeared in the drop-down list. This issue is resolved. Label groups are now supported for users with the appropriate RBAC permissions when creating rules and rulesets.

- **PCE sometimes failed to start** (E-73518, E-60012)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  The PCE services would fail to start with one or more nodes stuck in a PARTIAL state. When this error occurred, running the command `illumio-pce-ctl status -v -s` on a node in the PARTIAL state showed the status of `consul-agent` or `service-discovery` and other services as NOT RUNNING. This could be caused by the service startup scripts failing to completely start the Consul agent or to detect that it had been started successfully before the timeout. This issue is resolved.

Supercluster

> ⚠ These issues for Supercluster apply to Illumio Core On-Premises customers only.

- **PCE `supercluster-data-restore` was not working without `--no-include-nen`** (E-77011)
  When running the command `supercluster-dump` from a leader with NEN installed, on `supercluster-data-restore`, NEN data could cause a failure. This issue was caused by `supercluster-data-restore` incorrectly assuming NEN was a webservice and also restoring data on the members as well. This issue is resolved. The `--no-include-nen` option is no longer needed, and NEN data is now handled correctly without it.=
- **container_workloads tables indexes are not consistent across PCEs in supercluster** (E-68414)
  Some tables in a supercluster could end up with additional indices. These tables were used for replication, but not for querying data. The presence of extra indices did not have any significant effect on the PCE, other than the time and space to build and update these indices. This issue is resolved. The unnecessary indices have been removed.
- **Slony failure on Supercluster-drop** (E-56439)
  When running the `supercluster-drop` command, the failover operation could fail due to a deadlock issue. This issue is resolved.

REST API

- **Incorrect security principal GET schema** (E-75525)
  When executing a GET call, errors like the following were seen: `"The property '#/' contains additional properties [\"href\", \"deleted\", \"used_by_ruleset\", \"description\"] outside of the schema when none are allowed in schema`

`security_principals.schema.json#`." This issue is resolved. The schema no longer correlates these incorrect properties.

- **GET on unique event UUID did not always return the same event** (E-73129)
  A GET request for an event with a unique UUID could randomly return any one of several events that shared the same UUID. This was caused by using the request ID as the UUID for the event: multiple events with the same UUID could be created. For example, if a call to agent creates an event and also makes an interservice call that creates an event, both events would have the same UUID, but appear in different databases. If the event was queried by UUID, the events from both databases were found, but only one was kept. This issue is resolved. The PCE creates a new (unique) UUID for events, instead of using the request ID.

VEN

All Platforms

- **NFQueue did not work as expected** (E-77466)
  When in debug mode, NFQueue was redirected to NFlog due to a software issue. However, this did not interrupt operations. It merely generated incorrect log messages.
- **VEN Platform Handler process crashes after every 15 minutes** (E-77384)
  When either VPN or SecureConnect was enabled, the VEN Platform Handler crashed on workloads in Windows. This created a dump file. When this occurred, the VENs initially displayed policy sync errors and then proceeded to sync thereafter. This was a repetitive pattern. This issue is resolved.
- **VENs running on Windows hosts experienced high memory usage** (E-76748)
  On managed Windows workloads, a Windows firewall process consumed excessive kernel memory over time. This issue occurred when the environment managed by the PCE experienced high policy churn. Unchecked, the process could cause the Windows system to crash. This issue is resolved. On managed Windows workloads, the firewall process that was causing this issue no longer consumes excessive memory even in a high policy churn environment.
- **A tampering event was generated after upgrade to VEN 20.2-21.1** (E-76548)
  After an upgrade from VEN Release 19.3.2 to Release 20.2 or Release 21.1, a tampering event was generated. This issue is resolved.
- **High input/output operations (IOPs) per second have been resolved** (E-76245)
  On Linux, Windows, Solaris, AIX, high IOPs on the VEN failed to manage the size of `venstat.db`. While this file could have grown large over a period of time, with policy churning, it could have grown large at a faster pace. This issue is resolved.
- **Issues with VEN firewall policy updates have been resolved** (E-76057)
  The VEN did not clean up firewall anchors completely after policy updates. This issue is resolved.

- **VEN reactivation was slow** (E-74980)
  When a VEN was deactivated and then re-activated, the `PlatformHandler` service did not restart for several minutes, and meanwhile, the VEN was stuck in Active Syncing mode. This issue was caused by a flag that was not cleared, leading the `PlatformHandler` to exit early instead of waiting. This issue is resolved. The flag is now properly cleared, and VENs reactivate more quickly.
- **Repeated and incorrect interface change notifications** (E-72458)
  When IPv6 interfaces were changed, the VEN reported IPv4 interface information to the PCE, even though there were no changes to those IPv4 interfaces. This issue is resolved. Now updates are sent only when changes are actually made to the IPv4 interfaces.
- **The `illumio-ven-ctl.ps1` check-env output was inaccurate** (E-70925)
  When the workload was paired, the check-env showed the inaccurate PCE port and PCE FQDN. This issue is resolved.

Linux

- **Support report failed to include system information for Ubuntu systems** (E-78208)
  Running a report to generate an Illumio VEN Support Report for Ubuntu systems did not collect the system information. This issue is resolved.
- **Removing VEN with `rpm` command did not remove the VEN firewall policy** (E-76403)
  For VENs distributed as an RPM package, when the VEN was uninstalled using `rpm -e`, the Illumio firewall was not removed. The issue occurred only with the use of `rpm -e`, not `illumio-ven-ctl unpair`. This issue has been resolved, and the firewall is now removed.

Windows

- **VEN install failed when INSTALLFOLDER or DATAFOLDER specified** (E-82009)
  VEN upgrade could fail if INSTALLFOLDER or DATAFOLDER was specified. The issue was caused by a mismatch between the folder values in the Windows registry and the folders specified when invoking the VEN installer. This issue is resolved. The INSTALLFOLDER and DATAFOLDER values in the Windows registry are always used.
- **VEN failed to connect to PCE eventservice service with s elf-signed certificates** (E-78076)
  The Windows VEN failed to connect to the PCE `eventservice` service with self-signed certificates. This issue is resolved.
- **PowerShell failure error messages appeared when you tried to pair the Windows 7 and Windows Server 2008 R2 VEN** (E-75974)
  On Windows 7 and Windows Server 2008 R2 VENs, though the VEN pairing process was successful, you could have seen some PowerShell failure errors even when the pairing process was successful. This issue is resolved.

Solaris and AIX

- **VEN installation did not restore the previous contents of IPFilter** (E-77508)
  On Solaris running 19.3.5, the VEN did not save the current firewall as part of the pairing operation. This caused issues when the VEN was unpaired from the "saved" firewall. The VEN now saves and restores the firewall of IPFilter correctly on Solaris. This issue has been resolved
- **AIX/Solaris VENs used to report tampering events** (E-74955)
  In build state, when policies with certain IP lists were applied to AIX and Solaris VENs (version 19.3.3-6328), the VENs reported tampering events every 10 minutes.
- **Packet Filter issues were seen on Solaris 11.4 during policy changes** (E-69769)
  On Solaris 11.4, the VEN firewall process would configure the PF tables (accidentally flushing the firewall rules) and then would configure the PF firewall rules. During this process, there was a minuscule window (typically a fraction of a second) when no firewall policy was in effect. This issue is resolved.

Known Issues in 21.2.7-PCE

PCE Web Console

- **Rule search export does not delimit labeled scopes** (E-78378)
  When a rule search query completes and the results are exported to CSV, downloaded, and imported into Excel format, the multiple labels are not delimited in the Scopes column. Instead of the labels being separated by spaces, they show up in a single column with no spaces between labels. It displays "web_appproductionUS" instead of displaying "web_app production US."
- **PCE user interface displays the Program Name and Service Name on the same ports** (E-77450)
  Typically as soon as the VEN is paired, on certain connections, the PCE user interface displays both the Program Name and Service Name as using the same ports. For example, both the service name, `svchost.exe`, and the program name, TermService, both could seem to be using port 3389.
- **Specifying multiple labels within each label type is not supported** (E-73039, 72388)
  You can filter one label per Role, Application, Environment, or Location label type. While you have the ability to indicate multiple labels in your search filter within each type, you will not receive any results.
- **Incorrect count in selector static categories** (E-68895)
  When a user enters a value in a selector in the PCE web console, the options matching the input are displayed along with the matched and total count. In the case of Static categories,

the matched count is correct but the total count displayed is incorrect.
Workaround: While a workaround is not available, the issue occurs only when the user filters a static category. The matched count is correct but the total count is incorrect and will be fixed in a future release.

- **No error message is displayed after typing in an invalid port** (E-68255)
  When you enter an invalid port number while editing a service, the PCE still displays options to select from. When you move to another field without making a selection, the entered letters/digits are not cleared to reflect that the entered value was not selected. It can appear that the value you entered was accepted even though invalid.
  Workaround: Press ENTER after entering text. When the combination was valid, it will be selected. Otherwise, it will be cleared.
- **Filtering by an Invalid Protocol in the Services List page displays all services** (E-68251)
  When you type an invalid protocol and press ENTER, the protocol appears as a filter item but the list page is not refreshed. The PCE web console validates the entered protocol and refreshes the page only when the protocol is valid.
  Workaround: There is no workaround but this is only a cosmetic issue.
- **Filtering by an invalid port in the Services List page displays an error** (E-68249)
  When you filter the Services list using an invalid port, you receive the 406 error: “Port value out of range.” The port filter category is a free search and your input is passed to the PCE without validation.
  Workaround: Clear the entered port number and filter the list with a value in the valid port range.
- **The wildcard in the workloads filter not working** (E-65232)
  In the Workloads page of the PCE web console, the filter field should accept the asterisk (*) wildcard in filter expressions to filter the workload list; see Use a Wildcard to Filter Workloads. However, while the PCE web console accepts the asterisk as a valid character, the filter will always return zero results, even when there are workloads that should match the filter expression.
- **Filter doesn't handle the percentage symbol** (E-64904)
  When users select a filter option from the drop-down list, the selected value is added to the URL. When the selected value contains the percentage symbol (%), the PCE web console displays an error and a blank page appears.
  There is no workaround; however, this is a rare situation because the % symbol is not used often in values.
- **Pressing Enter doesn't select the default option in the dialog box** (E-53831)
  When the PCE web console displays a dialog box, pressing **Enter** might select an action other than the default.
  Workaround: Use your mouse to click the required button in the dialog.

Policy and Workloads

- **Labels added unnecessarily in rules** (E-81286)
  For extra-scope rules, Illumination unnecessarily adds labels that are already in the scope of the ruleset into the rules.
- **Vacuum backlog warning at almost 50%** (E-80929)
  On systems with very light database activity, the vacuum backlog metric of the policy database can show a high percentage (>= 40%) and the metric may be in a warning state. This should not be worrisome unless the warning state persists for more than 12 hours.
- **Virtual Server Mode does not map directly to the management state in the Web Console** (E-78370)
  Any virtual server discovered on an SLB is considered to be in the "Managed" state when it has a corresponding entry in the virtual server list page. A managed virtual server could be either Not Enforced or Enforced. The virtual_servers object in the API returns a "Managed: Not Enforced" virtual server as "unmanaged."
- **All|All|All does not work for static policies** (E-76447)
  From Release 17.3 and above, when configuring static policies, All|All|All does not work. Instead of all workloads having static policies, no workloads have static policies.
- **Incorrect error message displayed when ruleset renamed to a name that's in use** (E-74498)
  On creating and provisioning rule set, for example, rule set A, renaming it to B, then creating ruleset A and reverting modifications to ruleset B, the UI displays an incorrect "500" error instead of an error message informing that the ruleset name is already in use.
- **Policy restore impacts the virtual services of a container cluster** (E-73979)
  The existing issues are as follows:
  - When policy is restored to a version before the creation of a container cluster's virtual services, the container cluster's virtual services are marked for deletion in the draft change.
  - When a container cluster is deleted, restoring its virtual services is possible through policy restore.
- **Rule search incorrectly calculates label-groups in Scopes** (E-72318)
  When a rule has label groups in the scope, multiple scopes are created and traffic is not allowed between scopes unless specified with extra-scope rules. For example, Workload 1 and Workload 2 cannot talk to each other based on the policy because they are in different scopes. However, rule search for Workload 1 to Workload 2 allows access by this rule.
- **Inconsistencies in rule coverage for the Windows process-based rules** (E-71700)
  The draft view of Illumination and Explorer might show an incorrect draft policy decision for traffic covered by a rule using a service with a Windows process or service name. This generally happens when there is a port/protocol specified in the rule in addition to the process/service name, or when a non-TCP/UDP protocol is used in the rule. In these cases,

the reported view will provide the correct policy decision as reported by the VEN based on the active policy.

- **"Upgrade" option is enabled for a Read-Only User in the VENs list** (E-70341)
  After logging in as a Read-Only user, on navigating to the VENs list page, the "Upgrade" option is enabled instead of being disabled.
- **The timestamp "updated_at" not changed when a workload label is edited** (E-68720)
  When workload labels are updated through the API or the PCE web console, the timestamp "updated_at" in the workload API response will not be updated. This field is not visible in the PCE web console.
  This issue does not have a workaround; however, it affects only the timestamp and no other PCE functionality.
- **Incorrect Group Label count is displayed while editing a group for a workload** (E-68691)
  Workaround: This issue can be resolved by the backend providing a subset of results with the total filtered count.
- **Rule search with virtual service and labels returns an incorrect rule** (E-65081)
  When a rule is written with a virtual service whose labels conflict with the ruleset scope, and a rule search is done for the virtual service, the rule search could return the rule even though the rule does not apply due to the scope conflict.
  Workaround: Use the rule search to ensure that the rule applies to the virtual services and the scope labels separately.
- **Incorrect user name in Support Reports page after generating a report from VEN** (E-62935)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  After generating a support report from VEN using the `illumio-pce-ctl` command, the Support Reports page on the PCE displays either an incorrect user name or "Unknown" for the generated support report.
- **Clicking deleted ruleset in Policy Versions shows "Resource Not Found"** (E-62929)
  In the PCE web console **Policy Versions** page, when you click the name of a deleted ruleset, the message "Resource Not Found" is displayed. This is because the deleted ruleset does not exist in that version. The message is correct but not as informative as it could be.
- **Cannot create a rule with a label type defined in the Scope** (E-59100)
  In the PCE web console, you cannot create a rule with a label type that has also been used in the scope.
  Workaround: You can create such a rule using the API.
- **Unable to select multiple protocols in Rule Search** (E-57782)
  When you try to select multiple protocols in Rule Search, you cannot select a second protocol after selecting a protocol once. For example, you select TCP and then want to select UDP, the PCE web console does not display the protocol option again.
  Workaround: Use the REST API to select multiple protocols and obtain the correct search results. The above issue happens only in the PCE web console.

Data Visualization

- **Explorer Results page displays a message that query results exceed limit** (E-82743)
  When querying in Explorer, the result pages could show an indication that the number of returned results exceeds the configured maximum number in the PCE. This issue occurs because the PCE incorrectly validates the count based on total matches in the traffic database and not the actual results the user can view due to RBAC permissions or the actual number of results after filtering query exclusions.
  Workaround: None. However, this issue is cosmetic and you can ignore the message. Explorer will return query results less than the configured maximum number in the PCE.
- **Explorer: No notification when data from other regions' workloads is not displayed** (E-77680)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  Superclusters users who log into the member PCE and load Explorer data only see traffic reported by VENs that are paired to that member. The query selector shows the workloads from other regions but no data is returned when querying for those workloads. The system doesn't warn users on the Explorer page that they are seeing a partial data set.
  There is no workaround: Users can only log into the leader PCE to get the full Explorer data set.
- **Policy Generator: Consumer/Provider order is not showing properly** (E-76766)
  When the Provider & Consumer order is configured in Policy Settings to “Display Consumer Column First,” the order will not change in one of the Policy Generator columns.
- **App group name showing in error** (E-76638)
  App group name should not be showing in the consumer or provider filter for the workload manager role.
  The return from database flows the Explorer display is showing as “0” flows.
  This is specific to users with workload manager roles. The app groups should not show in the Consumer or Provider filter.
- **“Visibility Only” Workload Filter does work properly** (E-74231)
  Applying the "Visibility Only" workload filter does not reduce the Connected App Groups count reliably and can be changed again after a refresh.
  Workaround: Not available
- **Vulnerability - V-E score is not showing correctly** (E-73277)
  V-E score is not correct when compared with V-E score column and Total V-E score. For example, when adding V-E score column showing as 69.8 the Total is showing as 71 instead of 70.
  Workaround: Not available

- **VES and E/W exposures wrong for the internet and other workloads** (E-73023)
  If a rule provides a service on a vulnerable port/protocol to the internet and to some set of workloads, the workloads in the port exposure are not counted. This leads to a VES of 0 instead of larger than 0. The exposure calculation is correct if the internet is not provided as a consumer.
  Workaround: Not available
- **Add Rule panel not displaying for selected traffic with right-click actions** (E-68548)
  On right-clicking on selected traffic and clicking Add Rule, the Add Rule panel should display for selected traffic. Instead of the current selection, it displays the previous Add Rule panel for other selected traffic.

PCE Platform

- **After stopping data1 node, multiple nodes stuck in PARTIAL** (E-78519)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  When the primary instance of the database service, Citus coordinator service, or reporting database service goes down, failover can fail. This issue is caused by a failure to access the cluster KV store. The replica instance of the service also stops working, leaving the cluster in a PARTIAL state.
  Workaround: Try restarting the services on the node that was hosting the replica instance. If this does not fix the issue, contact Illumio support.
- **UI shows that the Listen Only mode as enabled even though it is disabled** (E-78451)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  (Supercluster) On one region of a supercluster, the PCE Web Console shows the Listen Only mode as enabled, even though it is actually disabled. This issue can occur when Listen Only mode is disabled for multiple PCEs at the same time.
  Workaround: The correct Listen Only status can be seen by using the command `illumio-pce-ctl listen-only-mode status`.
- **The `agent.activate events` are not always classified correctly** (E-74682)
  Events generated when an agent is activated (`agent.activate` events) are categorized inconsistently. Success events are classified as auditable, and failure events are categorized as `system_events`.
- **PCE uptime value can be wrong in the PCE Health page** (E-45143)

> ⚠ This issue applies to Illumio Core On-Premises customers only.

Temporary, expected PCE service restarts can reset the PCE uptime values displayed in the PCE web console PCE Health page so that it is not consistent with the uptime values displayed by `illumio-pce-ctl start`.

NEN

- **PCE Listen Only mode does not yet apply to NENs** (E-80376)
  Listen Only mode allows you to temporarily stop the PCE from sending policy updates to your VENs. Policy updates resume only after you disable Listen Only mode. This behavior is not yet available for NEN/F5 policy updates, which means that there's a chance that an F5 SLB could receive a stale policy when the PCE is in Listen Only mode.

Containers

- **IKS VPN Pod traffic not showing in Illumination/Explorer** (E-71163, E-54201)
  You may not see long lived flows that were established before the firewall is programmed for container workloads (this does not apply to host workloads). There is no workaround because it's a feature that has not yet been implemented for container workloads and not an issue.

Known Issues in 21.2.5-VEN

All Platforms

- **platform.log shows "No such file or directory" and "Could not set connection policy to loose error" errors** (E-71943)
  Error messages similar to these show up in platform.log:
  ```
  2020-09-29T10:41:36.126-07:00 INFO:: TCP loose connection grace period set to zero. Disabling strict tcp connections.
  2020-09-29T10:41:36.186-07:00 ERROR:: Could not set connection policy to loose error
  ```
  Cause: VEN transitions between managed and unmanaged (Idle) state before Conntrack check timer expires. No workaround is required. The VEN will recover itself once it is in a managed state (out of Idle) and the Conntrack loose timer expires.
- **VEN generates event with severity `Err` instead of `Info` when the unsuspend command is run twice** (E-69196)
  Unsuspend a VEN by using the PCE web console or REST API so that the VEN is active. Then,

unsuspend the VEN using the command `/opt/illumio-ven/illumio-vent-ctl unsuspend`. The VEN generates an event with severity Err when it should be severity Info.

- **Upgrading VEN on workload can cause API to generate 406 error** (E-40132)
  This API error occurs when the API version is incompatible with the VEN. Every 24 hours the VEN retrieves a new master configuration file, which will correct the API version incompatibility.
  Workaround: In most cases, this issue corrects itself within a few minutes. When it does not, wait for the VEN to retrieve a new master configuration file or restart the VEN to force it to update the file.

Solaris

- **Repeated logs observed in `vtap.log` after restarting VEN on Solaris** (E-63072)
  The message `INFO: Waiting for first reconcile file` is logged repeatedly after restarting a VEN. The contents of the Conntrack table are not removed at the restart, so long-lived connections established while the VEN was stopped stay active until the next policy change, instead of being marked as "potentially blocked" or removed from the Conntrack table.

Windows

- **Windows Services with invalid process paths trigger Policy Sync errors for affected VENs** (E-77105)
  Creating a Windows service with an invalid process path can trigger a Policy sync error on affected Edge endpoints and Core VENs. For example, the path `*\spoolsv.exe` is invalid because Illumio doesn't support wildcards in paths. To avoid this issue when specifying a process path, make sure to provide the full path beginning with the drive letter.

Legal Notices