Vertiv™ Environet™ Connect

Release Notes

VERSION 1.4, SEPTEMBER 30, 2024

Release Notes Section Outline

1. Updates to This Release (Version 1.4)

September 30, 2024

This version of Vertiv™ Environet™ Connect focuses on added features, performance enhancements, platform updates, bug fixes, and security updates.

Features and Enhancements

- Cloud
  - Feature – Alarms can be cleared manually from dashboard widgets and alarm tabs.
  - Feature – Multi-Factor Authentication via Email or SMS.
  - Improvement – Added Audit Log to Users.
  - Improvement – Vertiv™ Geist™ IMD-5 support.
  - Improvement – Vertiv™ Geist™ IMD-3/IMD-5 Firmware Version 6.0.x+ support.
  - Improvement – Feedback + Suggestions form added.
  - Improvement – Performance improvements in handling of current values.
- Local Agent
  - Feature – Add Events and Alarms tabs to Local Agent.
  - Improvement – Report Agent IP Address(es) to the Cloud.
  - Improvement – Create alarm when local agent is offline.
  - Improvement – Suppress device alarm “noise” when agent offline.
- Newly Supported Devices
  - Vertiv™ Liebert® APS UPS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
  - Vertiv™ Edge™ 230V UPS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
  - Vertiv™ Liebert® XDU1350

Bug Fixes

- Improved asset model selector and device add/edit screen.
- Improved audit logging when adding/editing/deleting objects.
- Improved redirect/authorization when logging in as an expired user.
- Improved logging of bulk firmware updates.
- Change the messaging when trying to log in as an invalid or disabled user.
- Fixed issue where the same device could be added twice on a customer.
- Fixed issues where the sessions were not expiring or were expiring in the background.

- Fixed issues with discovering Vertiv™ Geist™ Watchdog devices via a broadcast scan.
- Fixed issue where filters were not working on the Alarms tab.
- Fixed issue where removing visibility to a group did not remove visibility to its child devices.
- Fixed issue where MAC address is sometimes missing from the discovery scan.
- Fixed issue with the date on the configuration file list
- Fixed issue where certain alarms were not cleared.
- Fixed issue where allocation field was not populated for customers.
- Fixed issue where config. card admin button would sometimes disappear.
- Removed redundant status messages when creating devices, groups, sites.
- Added tooltips to icons in alarms/logs.
- Fixed cosmetic issues with the floorplan and map widgets.
- Fixed cosmetic issue with the numeric widget large COV indicator.
- Fixed cosmetic issue to the dashboard configuration at different resolutions.
- Added in-progress overlay for long running operations.
- Fixed issue where some mandatory fields were not indicated.
- Fixed issue with some agents not receiving configuration updates.
- Fixed issue where local agent version information is not updated.
- Improved refresh rate and logging of agent version changes.
- Fixed issue when deleting groups in bulk.
- Fixed validation of polling rates.
- Fixed issue where the users tab was not appropriately hidden.
- Fixed issue where device fields were intermittently auto cleared.
- Fixed cosmetic issue with the license banner.

2. Version 1.3.1 Update Information

July 2, 2024

Features and Enhancements

- Cloud
  - Feature – Save Dashboard as PDF.
  - Feature – Export Logs (Audit/Event/Alarm) to CSV.
  - Improvement – Added uniqueness check (name/address) when creating partners and customers.
  - Improvement – Upgraded Platform to .NET Core 8.
  - Improvement – Refactored event and alarm logs to improve readability.
- Local Agent
  - Improvement – Updated Agent Installer and Running Agent (Windows/Linux) to .NET Core 8.
  - Improvement – Refactored IPv6 Http client to use .NET 8.0 native libraries.

Bug Fixes

- Improved license enforcement and notifications.
- Improved audit logging, including updates, deletions, provisioning actions, dashboards, and linking behavior.
- Fixed issue with audit logs where org id did not resolve to the name.
- Fixed issue where other events were hidden when the user does not have the audit log permission.

- Fixed issue with downloading one or multiple agent logs.
- Fixed issue where the device name did not change in the logs when expected.
- Fixed issue where clicking the IP address when editing a device caused problems with saving.
- Fixed issue where SNMP credentials were not saved as expected when adding a device from discovery.
- Fixed issue that occurred intermittently when provisioning SNMP v3 credentials.
- Fixed issue where the user was redirected to the home page after clicking recently added devices.
- Added the “Add for Monitoring” option to the ellipsis menu for monitored devices.
- Fixed issue where changes could be lost when adding a device for monitoring.
- Fixed issue where alarms were not cleared when a device was deleted.
- Fixed issue where alarm notifications were not grouped in single notifications.
- Fixed issue where the firmware version did not update after provisioning.
- Fixed issue where the firmware version is not displayed.
- Fixed issue where the firmware update process incorrectly reported an error for successful updates.
- Fixed issue with permissions inheritance.
- Fixed issues with initializing and adjusting visibility permissions.
- Fixed issue where groups did not load for devices.
- Fixed issue with the counts when deleting entities.
- Fixed issue with inconsistencies when accessing users.
- Fixed issue with validation when creating users.
- Fixed issue with validation on agent polling rates.
- Added cosmetic improvements:
  - Improved the sizing, buttons and drop-down locations on mobile views.
  - Improved other buttons, widget headers and view toggles.

Security Updates

REFERENCE NUMBER	DESCRIPTION
CVE-2024-0985	Late privilege drop in REFRESH MATERIALIZED VIEW CONCURRENTLY in PostgreSQL allows an object creator to execute arbitrary SQL functions as the command issuer. The command intends to run SQL functions as the owner of the materialized view, enabling safe refresh of untrusted materialized views. The victim is a superuser or member of one of the attacker's roles. The attack requires luring the victim into running REFRESH MATERIALIZED VIEW CONCURRENTLY on the attacker's materialized view. As part of exploiting this vulnerability, the attacker creates functions that use CREATE RULE to convert the internally-built temporary table to a view. Versions before PostgreSQL 15.6, 14.11, 13.14, and 12.18 are affected. The only known exploit does not work in PostgreSQL 16 and later. For defense in depth, PostgreSQL 16.2 adds the protections that older branches are using to fix their vulnerability.
CVE-2023-32571	Dynamic Linq 1.0.7.10 through 1.2.25 before 1.3.0 allows attackers to execute arbitrary code and commands when untrusted input to methods including Where, Select, OrderBy is parsed.
CVE-2023-36414	Azure Identity SDK Remote Code Execution Vulnerability.
CVE-2023-45853	MiniZip in zlib through 1.3 has an integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_64 via a long filename, comment, or extra field. **NOTE: MiniZip is not a supported part of the zlib product.**

REFERENCE NUMBER	DESCRIPTION
	NOTE: pyminizip through 0.2.6 is also vulnerable because it bundles an affected zlib version and exposes the applicable MiniZip code through its compress API.
CVE-2021-21252	The jQuery Validation Plugin provides drop-in validation for your existing forms. It is published as an npm package "jquery-validation". Prior to version 1.19.3, jquery-validation contains one or more regular expressions that are vulnerable to ReDoS (Regular Expression Denial of Service). This vulnerability issue is fixed in version 1.19.3.
CVE-2021-24112	.NET Core Remote Code Execution Vulnerability.
CVE-2021-26701	.NET Core Remote Code Execution Vulnerability.
CVE-2021-43306	An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the jquery-validation npm package, when an attacker is able to supply arbitrary input to the url2 method.
CWE-384	Session Fixation.
CWE-614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute.
CWE-1004	Sensitive Cookie Without 'HttpOnly' Flag.

3. Version 1.3.0 Information (Initial Release)

April 23, 2024

Version 1.3.0 is the initial release of Vertiv™ Environet™ Connect.