IT Analytics Release Notes

Release: 11.8

VERITAS
now part of Cohesity

IT Analytics Release Notes

Last updated: 2026-06-04

Legal Notice

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1 Introduction 6

About IT Analytics 11.8 6

Chapter 2 Patch Releases 7

Patch releases: IT Analytics 7
- 11.8.2606 Patch Release Notes 7
- 11.8.2605 Patch Release Notes 8

Chapter 3 What's New 10

SMTP Authentication moved to Advanced Configuration 10
Dell PowerStore Policy gets Performance Probe 11
New Views for DataProtect Policy 11
IT Analytics Supports Notifications Using Webhook 11
Backup Policy Details Report Enhanced to Show Scheduled Dates 11
Data Collection Detail Report Enhanced 11
Third-party Library Upgrades 12
Enhanced the Disk Pool Volume Down Alert 12
Enhancements Added in Patch Releases of Earlier Versions 12

Chapter 4 Supported Systems 15

Portal Supported Operating Systems 15
Data Collector Supported Operating Systems 15
Supported Browsers and Display Resolution 16
- Linux Portal Server: Exported and Emailed Reports 17

Third-party and Open Source Products Used 17

Chapter 5 Installations and Upgrades 19

Portal Installation Memory Requirements 19
Performance Profiles and Transmitted Data 20
Reinstate Revoked Public Privileges of Oracle Users 20

Chapter 6 Fixed Issues 22

Overview 22
Fixed Issues 22

Chapter 7 Known Issues, Optimizations, and End-of-Life (EOL) 29

Known Issues 29
Optimization: Customize Linux File Handle Setting for Large Collections 31
BareTail.exe not Shipped with IT Analytics 31
Auto Upload of Logs to Support Discontinued 31
Support Dropped for New Backup Exec Policy Configuration 32

Chapter 1

Introduction

This chapter includes the following topics:

- About IT Analytics 11.8

About IT Analytics 11.8

IT Analytics provides unified visibility of utilization of your storage, virtualization, cloud, file, and fabric resources across on-premise and cloud environments. It reports current and historical data to evaluate performance issues, optimize resource usage, reduce costs, and help IT teams clearly understand and manage their resources.

The IT Analytics 11.8 Release Notes is a cumulative document covering the original 11.8 base release and all subsequent patch releases.

Note: For additional details refer to previous release note versions.

This release incorporates important fixes to issues that existed with the **IT Analytics** software. Many of these fixes pertain to the customer-specific issues that have been documented in the form of technical support cases. In addition to new features, this release offers enhancements and improvements from previous releases.

Chapter 2

Patch Releases

This chapter includes the following topics:

- Patch releases: IT Analytics

Patch releases: IT Analytics

The IT Analytics patch release are cumulative and contains all the previous patch fixes.

If you have already applied a custom patch after upgrading to 11.8.xx, contact Cohesity support before applying one the following patches as patch releases may reverse the updates provided in the custom patch.

11.8.2606 Patch Release Notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

IT Analytics reports

Table 2-1 Enhancements

Issue Number	Description
SC-76064	Updated advanced scope selector option for Backup Reports to ensure all DataProtect jobs are in scope by default

Data Collector policy

Table 2-2 Enhancements

Issue Number	Description
SC-74019	Commvault policy now has a dedicated API Access Token field for collecting additional failure details for Job details. Any access token previously configured via advanced parameters is automatically migrated to the policy during upgrade.

11.8.2605 Patch Release Notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Data Collector Policy

Table 2-3 Enhancements

Issue Number	Description
SC-64470	Cisco Switch Data Collector Policy is enhanced to support REST API collection method. Three new Advanced Parameters have been introduced for the REST API based collection: ■ CISCO_REST_CONNECTION_TIMEOUT ■ CISCO_REST_READ_TIMEOUT ■ CISCO_SWITCH_DISCOVERY_VIA_CREDENTIALS_OVERRIDE See *Cisco switch Data Collection policy* and *Fabric Manager Advance Parameters* sections the the portal help for more information.

IT Analytics Portal

Table 2-4 Enhancements

Issue Number	Description
SC-73314	Tomcat startup process is improved by 30 % (in terms of application loading timing).
SC-75457	Enhanced the Licensing module to fix CVE-2025-7962 vulnerability.

Table 2-4 Enhancements *(continued)*

Issue Number	Description
SC-75589	IT Analytics supports data collection and reporting on Cohesity DataProtect 7.4.
SC-75319	Developed API endpoints for DataProtect Data Collector policy operations.
SC-70768	Introduced API version V3 that are standards-compliant, consistent, and future-ready API experience. V3 APIs are redesigned to fully align with the JSON:API specification, delivering predictable structures, improved interoperability, and enhanced analytics capabilities. Key advantages in V3 include: ■ JSON:API compliance with standardized request/response formats, resource modeling, metadata, and error handling ■ Improved API consistency through uniform naming conventions and predictable pagination, filtering, sorting, and field selection ■ Functional enhancements such as enriched response attributes, stronger query capabilities, and better alignment with current and future product requirements ■ Structured error responses with consistent codes and messages for easier debugging and client integration Backward Compatibility: Existing V1 and V2 APIs remain fully supported and unaffected. New integrations and feature enhancements should adopt V3 APIs moving forward. Any future deprecation plans for earlier versions will be communicated separately.

Chapter 3

What's New

This chapter includes the following topics:

- SMTP Authentication moved to Advanced Configuration
- Dell PowerStore Policy gets Performance Probe
- New Views for DataProtect Policy
- IT Analytics Supports Notifications Using Webhook
- Backup Policy Details Report Enhanced to Show Scheduled Dates
- Data Collection Detail Report Enhanced
- Third-party Library Upgrades
- Enhanced the Disk Pool Volume Down Alert
- Enhancements Added in Patch Releases of Earlier Versions

SMTP Authentication moved to Advanced Configuration

SMTP authentication has been moved out of the **System Configuration** section and placed under the **Advanced** section on the portal UI.

You can perform this configuration from **Admin** > **Advanced** > **Email Configuration** on the IT Analytics Portal UI. See *SMTP Authentication* section of *IT Analytics Administrator Guide* for more information.

Dell PowerStore Policy gets Performance Probe

Performance probe is introduced for the Dell PowerStore Data Collector policy. The probe enables API-driven collection of performance metrics at various levels such as volumes and ports. The collection is triggered based on the configured schedule.

New Views for DataProtect Policy

Two new DataProtect-specific views apt_v_chdp_storagedomaindetails and apt_v_chdp_protectiongroup are introduced in Cohesity DataProtect Data Collector policy to help create reports without adding additional filter for DataProtect product.

IT Analytics Supports Notifications Using Webhook

IT Analytics supports event-driven notifications of system-generated alerts using Webhook. You can add Webhook configuration from **Admin** > **Advanced**, provided you have the required permissions, Webhook URL, and API key. Once configured, you can add it as a notification option to your alert policy.

In addition, you can also define the number of days for which the webhook events data must be retained in the database from **Admin** > **Advanced** > **System Configuration** > **Data Retention** section on the portal.

See *Webhook Configuration* in *IT Analytics Administrator Guide* for more information.

Backup Policy Details Report Enhanced to Show Scheduled Dates

The Calender Schedule section of Backup Policy Details report is enhanced to display scheduled dates of the policy in addition to the specific dates. The enhancement is applicable only to **Include Dates** list.

Data Collection Detail Report Enhanced

Data Collection Detail report is enhanced to display error-specific resolution. This change will provide specific directions to end users, support teams, and CFT teams to timely and efficiently troubleshoot the causes for failed probes. This improvement is implemented for the following probes:

- Job Details Probe

- SLP Job Details Probe
- Backup Policies Probe

Third-party Library Upgrades

The following third-party library upgrades were performed in this release:

- Jetty upgraded from 12.0.16 to 12.0.21 (to fix CVE-2025-1948, CVE-2024-6763, and CVE-2025-5115)
- Netty codec and codec compression upgraded to 4.1.129 (to fix CVE-2025-67735).
- Apache Commons Collections in Kafka from 4.2.0 to 4.5 (to fix CVE-2022-2414).

Enhanced the Disk Pool Volume Down Alert

Enhanced the Disk Pool Volume Down alert to include Disk Pool name to facilitate easier detection of which disk volume is down.

Enhancements Added in Patch Releases of Earlier Versions

The following enhancements were added in the patch releases.

Portal

Table 3-1 Enhancements

Issue number	Description
SC-75460	IT Analytics supports data collection and reporting for NetBackup 11.1.0.2. For detailed list of supported versions, see *Supported systems and access requirements* section in the *IT Analytics Certified Configuration Guide*.
SC-56884 SC-72826	Capability of Job Details probe is enhanced to collect additional deduplication statistics. This enhancement provides visibility into multi-threaded streaming usage, Variable Length Deduplication (VLD) settings, and Storage Object (SO) metrics, which enables detailed analysis of backup efficiency and storage consumption patterns.
SC-74454	Cohesity DataProtect policy configuration entitlement is discontinued from Foundation license. Subscribe to Premium license for Cohesity DataProtect entitlement. Pre-configured DataProtect policy function is not impacted by this change.

Table 3-1 Enhancements *(continued)*

Issue number	Description
SC-73899	Introduced new database indexes to enhance query performance during the persistence of audit information.
SC-74260	Introduced index APT_COLL_PROBE_STATE_DK7 to improve query efficiency when persisting collector probe state.
SC-72800	IT Analytics is enhanced to support Spring Boot and its dependencies to version 3.4.9.
SC-72785	IT Analytics is enhanced to support Apache HTTP server version to 2.4.65.
SC-72814 SC-73250	IT Analytics now supports Apache Tomcat version to 10.1.44.
SC-72784	IT Analytics is enhanced to support Angus Mail SMTP provider from version 2.0.3 to 2.0.4 or later.

Reports

Table 3-2 Enhancements

Issue number	Description
SC-73818	DataProtect Active Snapshots By Object Details (drilldown): Detailed view of active Cohesity snapshots by object, including status, timing, and data reduction metrics. You can drilldown to this report from DataProtect Active Snapshots By Object report.

Data Collector Policy

Table 3-3 Enhancements

Issue number	Description
SC-73600	Two new DataProtect-specific views apt_v_chdp_storagedomaindetails and apt_v_chdp_protectiongroup are introduced in Cohesity DataProtect Data Collector policy to help create reports without adding additional filter for DataProtect product.

Alerts

Table 3-4 Enhancements

Issue number	Description
SC-73600	Two new DataProtect-specific views apt_v_chdp_storagedomaindetails and apt_v_chdp_protectiongroup are introduced in Cohesity DataProtect Data Collector policy to help create reports without adding additional filter for DataProtect product.

Table 3-4 Enhancements *(continued)*

Issue number	Description
SC-73747	Enhanced NetBackup Appliance Hardware Failure alert to include more details on the Appliance in the alert message.

Chapter 4

Supported Systems

This chapter includes the following topics:

- Portal Supported Operating Systems
- Data Collector Supported Operating Systems
- Supported Browsers and Display Resolution
- Third-party and Open Source Products Used

Portal Supported Operating Systems

The Portal supports the following 64-bit platforms:

Table 4-1

Operating Systems	Version
Red Hat Enterprise Linux	7, 8.6 (update 10), and 9
SUSE Linux Enterprise Server	■ SLES 12 SP3, SP4, SP5 ■ SLES15 SP4
Windows	2016, 2019, and 2022
OEL	7, 8, and 9

Data Collector Supported Operating Systems

Install the Data Collector on a virtual machine (VM). The following 64-bit platforms are supported:

Table 4-2 Data Collector supported operating systems

Operating System	Version
Red Hat Enterprise Linux	7, 8.6 (update 10), and 9
SUSE Linux Enterprise	■ SLES 12 SP3, SP4, SP5 ■ SLES15 SP4
OEL	7, 8, and 9
Windows Server	2016, 2019, and 2022

Supported Browsers and Display Resolution

The Portal was certified on the following browsers. Please note that if you are using other versions of these browsers your user experience may vary:

Table 4-3 Supported Browsers

Browser	Apple Macintosh	Microsoft Windows	Linux
Microsoft Edge Version 144.0.3719.104 (Official build) (64-bit)	✓	✓	
	✓	✓	✓
Google Chrome Version 144.0.7559.110 (Official build) (64-bit)	✓	✓	
Apple Safari 18.3 (20620.2.4.11.5)	✓		

Browser performance

Several factors can impact web browser performance and behavior, such as:

- Client memory size and free memory
- Number of objects to be displayed in the Inventory
- Volume of data to be displayed

The Portal is designed to handle data in large-scale environments, however, your browser vendor/version may not be able to render all the objects. If your browser

cannot accommodate the volume, you can reduce the total number of items displayed in the Inventory, or try a different browser.

For larger data sets, use a Google Chrome browser for an optimal experience. Based on browser performance testing using very large data sets, Firefox and IE are supported, but the performance may be degraded.

Compatibility mode

For supported browsers, some windows may not display properly if you are running in compatibility mode rather than the preferred standard mode. Steps to change from compatibility mode to standard mode can be found by searching the Help in your vendor-specific browser window.

Linux Portal Server: Exported and Emailed Reports

On a Linux Portal server, to ensure proper rendering of reports that are emailed or exported as HTML images or PDF files, a graphics manager such as X Virtual Frame Buffer (Xvfb) is required. Contact your IT organization to configure this capability, if you plan to export/email reports as HTML images or as PDF files.

Third-party and Open Source Products Used

When you install the portal and reporting database, you install a compilation of software, which includes open source and third-party software.

For a list of open source components and licenses, see the license.txt file on the portal server.

Table 4-4 Open Source Products Used

Software Product	Linux	Windows
Apache HTTP Web Server	2.4.66	2.4.66
Apache Tomcat Java Servlet Engine	10.1.53	10.1.53
Java	Amazon Corretto 17.0.19.10.1	Amazon Corretto 17.0.19.10.1
Kafka	4.1.2.1	4.1.2.1
Oracle 19c	19c: 19.3.0.0.0	19c: 19.3.0.0.0

Note: If your environment has IT Analytics portal server and Data Collector installed on separate Linux servers and use Cohesity-provided Oracle, ensure the Oracle client RPM is installed or upgraded to 21.21.0.0.0-1.el8.x86_64.

If other versions of the above components are already running on the designated IT Analytics system, or other components are utilizing resources (such as specific ports) typically used by IT Analytics, the product usually can be reconfigured to work around these conflicts; however, this cannot be guaranteed.

*Refer to Support for updated binaries as they become available.

Chapter 5

Installations and Upgrades

This chapter includes the following topics:

- Portal Installation Memory Requirements
- Performance Profiles and Transmitted Data
- Reinstate Revoked Public Privileges of Oracle Users

Portal Installation Memory Requirements

For new Portal installations, the minimum server memory requirement is 32 GB. Oracle database requires a minimum of 24 GB of memory. Portal installations will fail if sufficient memory resources are not available on the Portal server.

The Portal Installation software checks the following resources:

- Total physical memory (physical + virtual) must be greater than 24 GB, otherwise Oracle will fail to start. Add more physical memory to the Portal server. [Windows and Linux OS]
- Windows Virtual Memory must be 24 GB or greater, otherwise Oracle will fail to start. Increase the size of the virual memory if required (**Windows** > **System** > **Advanced System Settings** > **Advanced** tab > **Settings** > **Advanced** tab > click **Change**) [Windows Only]
- Total temporary file system (tmpfs) memory must be 24 GB or greater, otherwise Oracle will fail to start. Increase the size of tmpfs, typically in /etc/fstab. [Linux OS only]
- Shared memory (kernel.shmmax parameter) must be 12 GB or greater, otherwise Oracle will fail to start. Increase the value of the shmmax parameter, typically in /etc/sysctl.conf. After increasing the value for the shmmax parameter, execute: **sysctl -p** [Linux OS only]
- Swap space of minimum 16 GB must be created. [Linux OS only]

For portal installation and upgrade steps, see the following sections of the respective *IT Analytics Installation and Upgrade Guide*:

- Windows: *Install IT Analytics Portal on a Windows server* and *Upgrade IT Analytics Portal on Windows*.
- Linux:*Install IT Analytics Portal on a Linux server* and *Upgrade IT Analytics Portal on Linux*.

Performance Profiles and Transmitted Data

Performance profiles are securely transmitted (over https) as anonymous and aggregated with other customers' profile data in Profile Central--the community pool is hosted, which is then imported into a customer's profile for reporting purposes. This import/export task occurs in a single, daily scheduled Portal process. Using the aggregated community profiles, companies can better gauge if the metrics collected in their environments are within a normal performance range. Profile data cannot be associated with any contributor. No company or environment-specific details, such as storage array or server names, are transmitted. No personally identifiable information is collected, used, or disclosed.

Note: To enable participation in Community Performance Profiling Cloud Policies, an authorized representative of your company must opt-in. Profile data cannot be associated with any contributor. No company or environment-specific details, such as storage array or server names, are transmitted. No personally identifiable information is collected, used, or disclosed. Note that you can opt-out at any time.

Reinstate Revoked Public Privileges of Oracle Users

This script reinstates the public privileges of Oracle users that were revoked when the IT Analytics Portal was either installed or upgraded.

To reinstate the public privileges:

1. Run the script from `$ORACLE_HOME/ora_scripts` folder.
2. Switch to aptare user.

   ```
   su -aptare
   ```

3. Reinstate the privileges as directed below.

   ```
   cd /opt/aptare/database/ora_scripts
   ```

   or

   ```
   $ORACLE_HOME/ora_scripts
   ```

   ```
   sqlplus / as sysdba
    alter session set container=scdb

    @  grant_public_role_grants.sql

   Granting PUBLIC role grants
   Disconnected from Oracle Database 19c Standard Edition 2 Release
    19.0.0.0.0 - Production
   Version 19.26.0.0.0
   ```

Chapter 6

Fixed Issues

This chapter includes the following topics:

- Overview
- Fixed Issues

Overview

The 11.8 release includes all patch release fixes of version 11.7.

Fixed Issues

The following issues were fixed or resolved in this release.

Table 6-1 Fixed issues in 11.8 release

Issue number	Description
SC-71970	Updated the collection window start time to fix the issue that caused reports to miss details of jobs created at the hour boundary.
SC-73821	Fixed the DTD reports "time period" issue that showed the report scope date and time range details based on the time zone of the server with the latest collected client job instead of picking the actual time zone of selected backup server from scope selection. The report now populates correct date and time ranges in matching with the "time period" range scope inputs by considering individual time zones of the respective backup servers when selected as single backup server from report scope.
SC-74927	Fixed the Azure billing probe issue, where the API was failing.
SC-75180	Apache HTTP server 2.4.66 is built with OpenSSL 3.0.19 which makes CVE-2025-15467 non-exploitable.

Table 6-1 Fixed issues in 11.8 release *(continued)*

Issue number	Description
SC-73640	Upgraded Logback to version 1.5.25, which makes CVE-2025-11226 and CVE-2026-1225 non-exploitable.
SC-74923	Fixed the issue that displayed miscalculated file share data for Azure Storage account probe.
SC-73674	Upgraded Spring Framework to 6.2.15, which makes CVE-2025-41254 non-exploitable.
SC-75152	Resolved database error APT-DB-107192 (library is invalid) reported by HPDP Session probe data collection that is caused by incorrect parsing of library names containing multiple colons.
SC-73842	Fixed the issue with Veeam Backup and Replication policy that prevented identification of the restored device due to incorrect reporting in client name.
SC-73884	Fixed the issue causing error while upgrading IT Analytics from 11.6 and 11.7. The error caused by PowerStore connector deployment failure is addressed through correction in constraint definitions in the schema file of its table.
SC-74466	Resolved an issue where exporting large reports in Excel either failed or resulted in incomplete output. The export process is improvised to ensure successful export of reports with large volumes of data in Excel format.
SC-67924	Upgraded LZ4 to version 1.10.2, which makes CVE-2025-66566 and CVE-2025-12183 non-exploitable.
SC-75254	Fixed the issue where the Apache service failed to start due to hard-coded User and Group values (apache) in `httpd-aptare.conf`. The configuration now uses the actual Apache runtime user and group to ensure successful service startup.
SC-75504	Fixed the issue where the aptare_agent service was not enabled at boot on SUSE 15 due to improper registration of the `SysV init` script. The fix registers the `init` script using `insserv`, reloads `systemd`, and enables the service to ensure it starts automatically at system boot.
SC-74528	Fixed the issue causing some portal installations with the VENDORJOBID column missing in two Cohesity DataProtect tables and views.
SC-75675	Fixed an Apache upgrade issue where SSL certificates were not copied when IT Analytics was installed in a mixed- or uppercase path on Linux. The fix preserves case sensitivity in certificate path handling, ensuring certificates are correctly copied and Apache starts successfully after upgrade.
SC-75978	Updated Job Summary report to return unique rows to prevent duplicate rows from being displayed.
SC-75505	Resolved missing environment values in the DataProtect Active Snapshots By Object report that caused incorrect or broken drilldowns.The query was corrected to join on policy_id and vendor identifiers instead of names, ensuring consistent data population and accurate drilldown results.

Table 6-1 Fixed issues in 11.8 release *(continued)*

Issue number	Description
SC-73464	Resolved issue with NetBackup Audit Report and drilldown report NetBackup Audit Report Details to ensure Changed Attributes count is matching in both reports
SC-75489	Fixed an issue where backup forecasting and capacity planning reports displayed inconsistent Total values on mouse-over when using TBytes: the value passed to ByteSizeFormatter is now converted using the correct database input unit, ensuring numeric values and unit labels remain consistent across chart bars and hover details.
SC-75805	Resolved the issue where the file-level compression probe was failing with a NullPointerException, caused by null values in optional fields (such as LocalComp) during KB conversion.
SC-74528	Fixed an issue where the VendorJobId column was missing from the SDK_CHDP_ARCHIVALDATA and SDK_CHDP_REPLICATIONDATA tables in certain upgraded environments. The upgrade process now adds the missing column and required indexes via upgrade_database.sql when upgrading from older IT Analytics versions, ensuring schema consistency across releases.
SC-75673	Fixed an issue in the NetBackup Backup Policy probe where Oracle database instances were missing when a single policy included instances from multiple clients. The client-matching logic was corrected to avoid false matches on empty IP addresses, ensuring all Oracle instances across different client hostnames are correctly recorded and persisted.
SC-75993	Fixed a data persistence failure caused by the TIMEZONE column in SDK_DEPS_SNAPSHOT_RULE_INSTANCE being too small to store larger timezone values. The column size has been increased to prevent persistence errors and ensure successful snapshot rule data storage.
SC-75246	Fixed an issue where Performance APIs collected data at very fine granularity (5-second and 20-second intervals), generating excessively large datasets that caused report and chart failures. The data collection granularity has been updated to 5-minute intervals, improving report performance, system stability, and user experience.
SC-75247	Fixed an issue where the data reduction ratio was persisted as an integer, resulting in inaccurate values in dashboards and reports. The collector now stores the data reduction ratio using a decimal data type, ensuring accurate reporting and trend analysis.
SC-74564	Fixed an intermittent DataReceiver persistence failure in Kerberos-authenticated environments where UCP connection pools were recreated based on credential field updated in data-receiver property file. This led to invalid pool lifecycle state (UCP-45060) and “Failed to get a connection” (UCP-29) errors. Recreation of connection pool on credential change is now limited to non-Kerberos mode.
SC-75290	Fixed an issue on Windows where reinstallTomcatService.bat utility stopped execution prematurely and failed to reinstall the Agent Tomcat service. The script now uses CALL when invoking other batch files, ensuring control returns correctly and both Portal and Agent Tomcat services are fully reinstalled.

Table 6-1 Fixed issues in 11.8 release *(continued)*

Issue number	Description
SC-74684	Reduced database TEMP usage during data collection by changing how large text (CLOB) fields are saved. The receiver no longer creates temporary LOBs for each value; it binds CLOB data directly (Oracle: string-based CLOB bind with support for pooled statements; other databases: character stream bind), which helps avoid ORA-01652 / TEMP exhaustion under heavy PPDM-style loads.
SC-76065	Fixed incorrect policy names for Cohesity DataProtect (product 200900) where numeric identifiers were shown instead of policy/protection group names in related reports. Updated the decode logic to correctly replace identifiers with the proper policy name when valid name data is received, ensuring reports now display the expected policy names.
SC-75950	Fixed incorrect Swagger/OpenAPI media type profiles that referenced the external domain ita.com. Updated all API YAML spec files to use the correct cohesity.com domain in the JSON:API Content-Type profile, ensuring accurate and non-misleading API documentation and responses.
SC-75968	Fixed NetWorker onboarding failures in large environments caused by excessive REST API payloads from the /global/volumes endpoint. Updated the collector to use field filtering (fl= parameter) to fetch only required volume fields, significantly reducing response size and preventing probe termination during SaveBackup and SaveStorageResource phases.
SC-75993	Fixed data persistence failures caused by oversized TIMEZONE values in the SDK table. Increased the column size to accommodate larger timezone data, preventing insert errors and ensuring successful persistence during connector operations.
SC-75942	Updated database view aps_v_hnas_virtual_volume to prevent divide by zero error.
SC-75563	All Jetty jar versions have been upgraded to 12.1.7, including the version bundled with Data Collector and the Jetty libraries coming from Kafka dependencies. This addresses CVE-2025-5115, CVE-2026-1605, and CVE-2025-11143 vulnerabilities.
SC-76100	Realtime log collection failures after upgrade have been fixed by addressing incorrect ownership/permissions on the realtime logs directory. The issue caused “Exception while writing realtime logs” errors due to permission denied when Tomcat attempted to create log files, impacting realtime logs on the policy screen.
SC-77701	Resolved the problem that generated unexpected dump files during an automated uninstall by stabilizing the shutdown and exit flow.
SC-77747	An issue where hosts in the “All Backup Servers” scope selector were not displayed in alphabetical order when Authorization Attributes (Authz) were enabled has been fixed. The UI now preserves the original sorted order by using an order preserving map during Authz-based filtering, ensuring consistent alphabetical sorting regardless of Authz configuration.

Table 6-1 Fixed issues in 11.8 release *(continued)*

Issue number	Description
SC-76110	An issue where the EMC Avamar Activity Details probe missed the most recent hour of backup data due to incorrect timezone and DST handling has been fixed. The probe now correctly converts timestamps using DST aware timezone offsets, ensuring recent Avamar activity data is fully collected across timezone differences.
SC-77758	Fixed an issue in NetBackup Data Collector where CLOB-heavy asset persistence (APT_NBU_ASSET.ASSET_DETAIL) caused excessive TEMP usage due to temporary LOB allocation. The Data Collector persistence logic was updated to free the temporary CLOB space and reducing temporary LOB pressure under load without impacting asset ingest or consumers.
SC-76120	Upgraded the Spring Framework to 6.2.15, which makes the following vulnerabilities non-exploitable: ■ CVE-2026-22737 ■ BDSA-2026-7607 ■ BDSA-2026-7608.
SC-76369	Upgraded Spring Boot and their dependences to 3.5.13, which makes the following vulnerabilities non-exploitable: ■ CVE-2026-22731 ■ CVE-2026-22733 ■ CVE-2026-40972 ■ CVE-2026-40973 ■ CVE-2026-40974 ■ CVE-2026-40975 ■ CVE-2026-4097
SC-76370	Upgraded the Spring Security which makes the following vulnerabilities non-exploitable: ■ CVE-2026-22732 ■ CVE-2026-22748 ■ CVE-2026-22751 ■ CVE-2026-22746
SC-75001	Upgraded Log4j to 2.25.4, which makes the following non-exploitable: ■ CVE-2025-68161 ■ CVE-2026-34480 ■ CVE-2026-34477 ■ CVE-2026-34481 ■ CVE-2026-34479

Table 6-1 Fixed issues in 11.8 release *(continued)*

Issue number	Description
SC-75804	Fixed a parsing failure in the MessageLogsProbe for Alta View customers caused by a StringIndexOutOfBoundsException in the NetBackup parser when handling malformed or skipped filenames. The fix hardens the parsing logic to safely handle invalid bounds, ensuring data collection completes successfully without probe failure.
SC-75856	Fixed excessive stack trace logging during NetBackup jobs API requests when using older API versions, where certain job attribute serialization caused noisy logs despite successful (HTTP 200) responses. The resolution recommends updating the API client to use a newer jobs API version (v9.0 or higher, ideally v14.0 via the Accept header), which includes fixes to policy and schedule attributes and prevents the unnecessary stack traces.
SC-73165	Fixed an HTTP 500 error in the Cohesity DataProtect ProtectionDetails probe caused by a MissingPropertyException due to improper variable scoping of the REST API command. The fix ensures the command variable is correctly scoped across the logic block and adds warning logs to surface hook/API failures instead of silently ignoring them.
SC-76121	Upgraded vulnerable plexus-utils coming from Kafka to 3.6.1.
SC-76134	Fixed an issue where Mission Control Backup graphical data was not displayed in the API response.
SC-76224	Resolved the problem that prevented a scheduled task from running by updating its timing configuration to use valid future run times.
SC-77902	Fixed the issue related to NetBackup FETB data persistence, where MS-Windows policies were incorrectly mapped as MS-Windows-NT, causing ITA to report incorrect information.
SC-71497	An issue where Oracle purge jobs failed to delete Veritas Flex Appliance hosts—leaving orphaned SDK_VTFA_* records and impacting DXC reports—has been fixed. The fix introduces a new database procedure to explicitly remove SDK_VTFA-related entries by HostID before deleting the host from base tables, ensuring successful purging without constraint violations or database errors.
SC-76073	An issue where the Collection Status page appeared blank or showed incorrect data for multi-device policies has been fixed. The filtering logic has been corrected to use the unique collector identifier instead of a comma-separated policy name, ensuring probe statuses display correctly and only for devices associated with the selected policy.
SC-76128	An issue where the EMC Avamar Configuration Changes Probe failed with an Oracle unique constraint violation due to improper handling of NULL default values has been fixed. The probe logic now correctly updates existing dataset records with NULL defaults, preventing duplicate key errors and ensuring apt_avm_dataset_detail reflects the latest data without database errors.

Table 6-1 Fixed issues in 11.8 release *(continued)*

Issue number	Description
SC-78034	Fixed a startup-blocking ORA-00932 (“inconsistent datatypes”) error introduced after upgrading to Oracle 19.31, which prevented Tomcat-* services from starting due to failures in common_package.getNbrOfClients(). The fix updates affected stored procedures to ensure consistent datatype handling across CAST/SUBSTR expressions used in SET/CAST/COLLECT operations (including ORDER BY clauses), maintaining type safety for nested-table aggregation under stricter datatype enforcement of Oracle 19.31.
SC-71991	The end-to-end file upload library used for data collection is changed to ensure compliance and consistency with licenses and checks, which makes the CVE-2025-48976 vulnerability non-exploitable.

Chapter 7

Known Issues, Optimizations, and End-of-Life (EOL)

This chapter includes the following topics:

- Known Issues
- Optimization: Customize Linux File Handle Setting for Large Collections
- BareTail.exe not Shipped with IT Analytics
- Auto Upload of Logs to Support Discontinued
- Support Dropped for New Backup Exec Policy Configuration

Known Issues

The following known issues are present in this release.

Table 7-1 IT Analytics 11.8 Known Issues

Issue Number	Description
SC-43138	The Performance Statistics probe of the Cohesity Flex Appliance policy is unable to collect the node disk statistics details, as node_disk_% metrics are temporarily restricted in Flex Appliance /metric/federate API response

Table 7-1 IT Analytics 11.8 Known Issues *(continued)*

Issue Number	Description
SC-31736	File Analytics can be enabled either from the Host File Analytics policy or through NetBackup File Analytics policy. If you enable both for the same host, then the data appearing in the reports will not be accurate. Hence, ensure you configure File Analytics for a given host only in one policy, preferably through the NetBackup File Analytics policy.
SC-40668	IT Analytics Portal with Foundation licenses displays host groups that are unrelated with Cohesity NetBackup under HostGroups Menu in **Admin** tab. You can ignore the Non-NetBackup hosts groups.
SC-41008	When a license is expired, consumed count on the license report may not show correct value.
SC-31099	In case of Hyper-V Intelligent policy, the client name returned by Cohesity Backup Manager is always VM UUID, regardless of the Primary VM Identifier of the Hyper-V Virtual Machine, which causes failure in collection of file metadata. This behavior also leads to IT Analytics reporting some or all such clients as unprotected.
SC-32319	File Analytics Collection Status report displays the same **File Count** value for both **Current Collection** and **Previous Collection**.

SC-74069	If you deleted a report schedule configured on v11.5 or v11.6 and later tried to upgrade to v11.7, the upgrade fail. To address the upgrade failure you can run the following SQL commands on the Portal database and subsequently, perform the upgrade.
	1 Create a backup of the old Quartz table.
	`SQL> CREATE TABLE BKP2511_APT_QZ_CRON_TRIGGERS AS SELECT * FROM APT_QZ_CRON_TRIGGERS;`
	2 Truncate the table. This ensures the upgrade completes seamlessly.
	`SQL> TRUNCATE TABLE APT_QZ_CRON_TRIGGERS;`

SC-75263	The Exclude Dates field of Backup Policy Details report for a NetBackup policy does not display details of exclude dates configured in the policy.

Optimization: Customize Linux File Handle Setting for Large Collections

Certain environments may require optimizations to improve performance or to accommodate a large number of data collection policies.

In Linux, a portion of memory is designated for file handles, which is the mechanism used to determine the number of files that can be open at one time. The default value is 1024. For large collection policy environments, this number may need to be increased to 8192 so that the collector does not exceed the open file handle limit. A large environment is characterized as any collector that is collecting from 20 or more subsystems, such as 20+ TSM instances or 20+ unique arrays.

To change the number of file handles, take the following steps.

1. On the Linux Data Collector server, edit **/etc/security/limits.conf** and at the end of the file, add these lines.

   ```
   root soft nofile 8192
   root hard nofile 8192
   ```

2. Log out and log back in as **root** to execute the following commands to validate all values have been set to 8192.

   ```
   ulimit -n
   ulimit -Hn
   ulimit -Sn
   ```

3. Restart the Data Collector.

BareTail.exe not Shipped with IT Analytics

BareTail.exe utility, real-time log file monitoring tool on Windows systems, will not be shipped with IT Analytics Portal installer from 11.8 release.

Auto Upload of Logs to Support Discontinued

The facility to send portal and Data Collector logs within available from **Admin** > **Advanced** > **Support Tools** had a provision to get email notification and upload logs to a Veritas server. This provision of email notification and storing support logs is no longer available. The facility to download portal and Data Collector logs has been retained.

Support Dropped for New Backup Exec Policy Configuration

IT Analytics will no longer support the new configuration Veritas Backup Exec Data Collector policy. Existing Backup Exec policy configurations will continue to function normally. Support for existing configuration of the policy will be dropped from the next major release.