IT Analytics Release Notes

Release: 11.7

VERITAS
now part of Cohesity

IT Analytics Release Notes

Last updated: 2026-05-05

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

This chapter includes the following topics:

About IT Analytics 11.7

The IT Analytics 11.7 Release Notes is a cumulative document covering the original 11.7 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

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 11.7.xx, contact Cohesity support before applying one the following patches as patch releases may reverse the updates provided in the custom patch.

11.7.2605 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 2-1 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 2-2 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.
SC-75589	IT Analytics supports data collection and reporting on Cohesity DataProtect 7.4.

11.7.2603 Patch Release Notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Portal

Table 2-3 Enhancements

Issue Number	Description
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.

Table 2-3 Enhancements *(continued)*

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-74626	You can now reconfigure an existing Azure role used for Azure data collection to use RBAC-only authentication with read-only permissions for storage discovery, Azure File Shares, and storage data-plane access. This removes the dependency on storage account keys. See *Reconfigure an Existing Azure Role for Azure Storage Access* section in *IT Analytics Data Collector Installation and Configuration Guide* for more information.

Reports

Table 2-4 Enhancements

Issue Number	Description
SC-73812	Introduced DataProtect - Active Snapshots By Object report. The report summarizes and details active DataProtect snapshots by object, with customizable size units.
SC-74773	Added additional columns in DataProtect Replications report to assist in identifying parent and child jobs and sorting.

11.7.2602 Patch Release Notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Portal

Table 2-5 IT Analytics Portal Enhancements

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-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 2-5 IT Analytics Portal Enhancements *(continued)*

Issue Number	Description
SC-73936	IT Analytics has been enhanced with improvements powered by Helios, focusing on data quality, multi-tenant support, resilience, and security to provide more reliable and scalable reporting. ■ Stronger Helios data foundation: A continuous streaming pipeline now delivers comprehensive and structured Helios data including clusters, jobs, policies, and runs, with new fields fully populated and persisted to support richer analytics without requiring configuration changes. ■ Cleaner and more accurate reports: The system now marks deleted clusters, jobs, and resources appropriately to avoid stale data in reports, improves population of lookup and descriptive fields, and captures retention settings accurately for protection policies, resulting in more precise usage, protection, and compliance views. ■ Improved multi-tenant and secure data handling: Tenant and organization identifiers are integrated throughout the data pipeline to ensure correct data association and lifecycle handling, while intelligent routing respects entitlements to segregate data properly. Additionally, the pipeline is more resilient to errors and manages credentials securely to maintain up-to-date reporting despite system issues.

Reports

Table 2-6 Enhancements

Issue Number	Description
SC-73978	Oracle Patch History displayed within the System Health Check report is updated with Action field to indicate the action taken when Oracle OPatch utility was executed to manage patches. The values it can display are Apply, Rollback, and Remove.

11.7.2601 Patch Release Notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Portal

Table 2-7 Enhancements

Issue Number	Description
SC-71705	The IT Analytics ServiceNow App has been certified by ServiceNow for the following releases: ■ Xanadu ■ Yokohama ■ Zurich
SC-73212	Starting January 2026, versioning scheme for monthly updates of IT Analyticsis being changed to Calendar Versioning (CalVer), i.e., from aa.b.cc to aa.b.YYMM. For example: ■ January 2026 monthly update for 11.7 stream will be versioned as 11.7.2601 ■ February 2026 monthly update for 11.7 stream will be versioned as 11.7.2602

Alerts

Table 2-8 Enhancements

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

11.7.02 Patch Release Notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Portal

Table 2-9 Enhancements

Issue number	Description
SC-67943	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.
SC-73312	Updated drilldown logic for reports which does not impact the report functionality or output.

Table 2-9 Enhancements *(continued)*

Issue number	Description
SC-73394	IT Analytics supports reporting on DataProtect 7.3.
SC-74176	IT Analytics supports reporting on NetBackup 11.1.

Alerts

Table 2-10 Enhancements

Issue number	Description
SC-45181	Changes made to alert rule NetBackup Disk Volume Down to include Disk Pool and Disk Volume names in alert message.

Data Collector Policy

Table 2-11 Enhancements

Issue number	Description
SC-72486	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.
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.
SC-61296	HP 3PAR Data Collector policy is enhanced to persist vLUN Template mappings so that offline hosts retain accurate virtual volume-presentation data.
SC-66492	The data collection of Dell EMC Networker policy is modified to distinctly identify each backup job and store it in the database, in spite of having the same job information (such as same server, client, start date, finish date, parent, object type) to enable differentiation of the backup jobs.
SC-72490	The Data Protection and Data Utilization probes of the Dell PowerStore Data Collector policy have been enhanced to collect the following details: ■ Host data ■ Host mapping data ■ Port data ■ Serial number in a storage array ■ IP address in a storage array ■ OS version in a storage array

Reports

Table 2-12 Enhancements

Issue number	Description
SC-73811	DataProtect Storage Consumption by Cluster Chart: Tracks and summarizes storage consumption trends across DataProtect clusters over time. You can access this report from **Backup Manager** > **Storage Utilization Reports** > **DataProtect Storage Consumption by Cluster Chart**.
SC-73807	DataProtect Storage Consumption by Cluster: Tabular summary of DataProtect cluster storage over time with configurable units, time frame, and rollups. You can access this report from **Backup Manager** > **Storage Utilization Reports** > **DataProtect Storage Consumption by Cluster**
SC-73415	DataProtect Replications: Replication activities across a scoped time frame for quick health checks, troubleshooting, retention validation, and efficiency insights. You can access this report from **Backup Manager** > **Management Reports** > **DataProtect Replications**.
SC-73806	DataProtect Archives: DataProtect archive operations, status, and data transfer for a specified time frame. You can access this report from **Backup Manager** > **Management Reports** > **DataProtect Archives**.
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.

11.7.01 Patch Release Notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Capacity Manager section

Table 2-13 Enhancements and resolved issues

Issue Number	Description
SC-72999	Data Domain Storage policy for DDOS v7.13 and v8.1 has been certified.

Backup Manager data collection section

Table 2-14 Enhancements and resolved issues

Issue number	Description
SC-72999	Data Domain Backup policy for DDOS v7.13 and v8.1 has been certified.

Reports section

Table 2-15 Enhancements and resolved issues

Issue Number	Description
SC-41080	The **Data Collection Performance Detail**, under System Administration reports, is enhanced to support features such as scheduling, filtering, sharing, and alerts. Initially, this report was available as a drill-down report from the Data Collection Performance Summary report.
SC-68270	Resolves an issue in the **Job Summary** report. The report displayed Archived Redo Log Backup in Scheduled/level type column for both Oracle and MS-SQL Server policy type jobs for NetBackup.
SC-71105	Resolves an issue where the custom reports and Backup RTO RPO compliance report are getting truncated when exported in PDF file format.
SC-73220	IT Analytics is enhanced with Job/Event Type and Advanced filtering enabled for the Job Summary by Server and Job Summary by Source reports, allowing more granular options to de-select and select Job/Event Types to be considered in the report output.
SC-72766	The Report Filtering dialog box is enhanced to accept numeric values for is a member of or is not a member of filter.
SC-72776	Resolves an issue where the Azure Daily Usage Forecast by Subscription Details report, being the drilled down report, is displayed in Recent folder for reports. along with parent template (Azure Daily Usage Future Forecast by Org Level). When the drilled down report was selected, the report displayed error message.
SC-73094	Resolves an issue with the reports where user was not able to create a drill-down RTD report from a DTD report.
SC-73350	Resolves an issue with the drill-down report, NetBackup Audit Details, of NetBackup Audit Report. The drill-down report displayed "No data present" even when non-zero hyperlink was selected.
SC-73220	Job / Event Type and Advanced filtering is now enabled for the following two reports, allowing more granular options to de-select and select Job/Event Types to be considered in the report output: ■ Job Summary by Server ■ Job Summary by Source

Portal section

Table 2-16 Enhancements and resolved issue

Issue number	Description
SC-63734	Resolves an issue where the database error logs were incorrectly recorded in `README.txt`. In a split architecture, since the database logs are not available on the PORTAL server, `README.txt` now displays the message: *[INFO] Download database log files from the database server*.
SC-64464	Resolves an issue with AD/LDAP configuration. If a user was configured in the Disable User Attribute name and Disable User Attribute Value, all the users were denied access from Swagger UI to API.
SC-71699	Resolves an issue with SLP Job Details probe where the portal displayed parsing error message.
SC-71625	Linux portal upgrader prompts to perform a cold backup and you must confirm and acknowledge that a it was performed before proceeding with the upgrade.
SC-71930	Resolves an issue with PowerStore collection volume API call failure. The API displayed error message when offset was greater than the content range.
SC-71934	Resolves an issue with EMC Data Domain. The data collector failed collecting local metadata when the Cloud feature was not enabled.
SC-72276	Resolves the stored procedure performance issue.
SC-72519	The following enhancements incorporated for the job tickets created by ServiceNow: Job Finalized alert policy: ■ Two new columns clear_date and clearing_job_id incorporated in apt_job_ticket table. clear_date: Records the timestamp when a job alert was resolved. clearing_job_id: refers to the first successful job that fixed the alert. A 'successful job' means the first time the job ran successfully after one or more failures, for the same client-server pair that triggered the alert. ■ Once the job is successfully executed the system will automatically track the job tickets and mark them as Resolved. ■ Post patch deployment and upon first successful job execution, the system will update, current as well as historic job tickets, for the same server and client combination.
SC-72615	Resolves an issue where the users, with restricted permissions to objects via Authorization attributes, were unable to add Ports under "Show Objects" in Inventory.
SC-72760	The Oracle patch installation process is enhanced. Post successful installation, Cohesity recommends to run the ora_scripts from the $ORACLE_HOME/orascripts folder. The script reinstates the user's access rights which was revoked during the patch installation.
SC-72761	Resolves an issue of broken hyperlinks. After executing a SQL query on APT_PUBLISHED_VIEW, broken hyperlinks were displayed for GitHub documentation.

Table 2-16 Enhancements and resolved issue *(continued)*

Issue number	Description
SC-72784	IT Analytics is enhanced to support Angus Mail SMTP provider from version 2.0.3 to 2.0.4 or later
SC-72785	IT Analytics is enhanced to support Apache HTTP server version to 2.4.65.
SC-72786	IT Analytics is enhanced to support Spring Security from version 6.3.3 to 6.5.5.
SC-72800	IT Analytics is enhanced to support Spring Boot and its dependencies to version 3.4.9.
SC-72807	Resolves an issue where after running the resetPermission.sh utility, logs were not getting generated from the support tool.
SC-72814/SC-73250	IT Analytics now supports Apache Tomcat version to 10.1.44.
SC-72812	IT Analytics now supports Spring Framework from version 6.2.1 to 6.2.11.
SC-72916	IT Analytics now supports Apache HTTP Web server version 2.4.65.
SC-72960	A **Downloads** menu item is added to the user profile menu. It invokes a **Downloads** list that displays all the downloads performed during the browser session of the portal. The list is reset whenever you close or refresh the portal browser.
SC-73068	Resolves an issue after Kafka upgrade. Post upgrade, Kafka failed to start due to reverted access rights of the folders within.
SC-73210	Resolves an issue in the preUpgradeCheck utility where the portal was unable to connect to Oracle due to a mismatch between the connection string using a SID and the `tnsnames.ora` file configured with a SERVICE_NAME.

Chapter 3

What's New

This chapter includes the following topics:

System Administration reports to show error trend

The following system administration reports will show additional insights on error trend:

- Data Collection Message Summary report: New columns will display Error Trend and First Message Date.
- Portal Error Aggregation: New column will display Error Trend.
- Database Error Aggregation report: New column will display Error Trend.

Manage data collection from Flex Appliance using short-lived access token

Flex Appliance v5.0 has a provision to convert a normal account to a service account, which is only capable of creating REST API calls to Flex Appliance and you can restrict its interaction to specific APIs in read-only mode. The provision of short-lived token, which can invalidate itself after a configurable time, is available to the service account.

IT Analytics can use this short-lived token to authenticate and perform data collection from the appliance while the token is live. Service account users can adjust the

maximum token validity from the Flex Appliance Console to accommodate the data collection.

All Job Types Included in Default Scope of Backup Management Reports

The report scope of the following Backup Management reports is modified to include all job types by default:

- Backup Executive Summary
- Consecutive Errors
- Error Log Summary by Server
- Error Log Summary
- Error Log Summary by Policy
- HP DP Session Summary
- Job Duration
- Job Duration By Source
- Job Error Code
- Job Status Summary
- Job Summary
- Job Type Count

The Job Types are visible in the Advanced Options view of the scope selector of the above reports. This enhancement does not impact the scope of the saved reports after upgrade.

See *Backup Manager Scope Selector Settings* section of the *IT Analytics User Guide*.

Chapter 4

Supported Systems

This chapter includes the following topics:

Portal Supported Operating Systems

The Portal supports the following 64-bit platforms:

Table 4-1 Portal Supported Operating Systems

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

Display Resolution: The minimum resolution for the Portal is 1920 x 1200 px.

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 133.0.3065.59 (Official build) (64-bit)	✓	✓	
Mozilla Firefox Version 91.3 and later (91.3 is the extended support version)	✓	✓	✓
Google Chrome Version 133.0.6943.98 (Official Build) (64-bit)	✓	✓	
Apple Safari 18.3	✓		

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 17.0.18.9.1	Amazon Corretto 17.0.18.9.1
Kafka	3.4.0.11	3.4.0.11
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

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

The 11.7 release includes all patch release fixes of version 11.6.

Fixed Issues

The following issues were fixed or resolved in this release.

Table 6-1 Fixed issues in 11.7 release

Issue number	Description
SC-71044	Fixed the error of unique constraint violation "APT-DB-106348 - APS_SWI_TOPOLOGY_C1' while refreshing "aps_swi_topology".
SC-72828	Fixed the Audit API Sort Parameter compatibility issue with the following changes: ■ Updated the audit logs API requet to use sort=auditDateTime for ascending order sorting. ■ Maintain backward compatibility with netBackup 10.4 and earlier versions. ■ Ensured forward compatibility with NetBackup 11.0 and alter versions.
SC-73060	Black Duck vulnerabilities addressed by upgrading Apache Commons Lang to 3.20.0.
SC-73064	Black Duck vulnerabilities addressed by upgrading Netty codec and codec compression to 4.1.128.Final.

Table 6-1 Fixed issues in 11.7 release *(continued)*

Issue number	Description
SC-73372	Fixed the failure of IT Analytics upgrader utility and connector deployer due to absence of alias name. The utility and connector deployer use the full database URL instead to establish the connection. The dependency on the service name alias does not exist anymore.
SC-73395	The Protection Details probe of Cohesity Data Protect Data Collector policy is modified to prevent the data overrun errors caused by its allocated column length.
SC-73538	Restored Alert notifications that were getting blocked when hardware appliance developed issues or was down.
SC-73573	The external loadPortAttributeFile format has been changed. Instead of supplying the switch port element name, the file must include port name (slot number/physical port number) to be able to fetch the unique fc port id and to persist port attributes against supplied Brocade switch data load.. For example, the values in Port column can be 0/60, 0/62, and so on, in slot number/physical port number format.
SC-73637	Black Duck vulnerabilities addressed by upgrading Apache ZooKeeper to 3.9.4.
SC-73639	Black Duck vulnerabilities addressed by upgrading Bouncy Castle to 1.83.
SC-73675	Addressed Apache-specific issues caused when Apache was upgraded to version 2.4.65 in IT Analytics and 11.7. The new build is compiled over OpenSSL 3.0.16 and uses libexpat 2.7.3, resolving the previously reported libexpat vulnerability and the issue with Apache instability.
SC-73758	The backup sessions collected via the Session Probe of the HP Data Protector policy did not include the associated Volume Pool. The probe has been enhanced to enable IT analytics to report both backup details and their corresponding Volume Pool for each session.
SC-73979	Fixed an issue where the dashboard scheduling feature was unavailable.
SC-74274	Corrected issue for the following reports where their icons incorrectly appeared as a bar chart icons. The icon now correctly appear as a line chart icons. ■ Job Throughput by Client ■ NetBackup SLP Backlog ■ DataProtect Storage Consumption by Cluster Chart
SC-74288	Fixed issue with Data Collection Message Summary By Collector or By Host report not rendering data.
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.

Table 6-1 Fixed issues in 11.7 release *(continued)*

Issue number	Description
SC-69799	Resolved the issue that displayed an error message on the UI multiple times even with a single data collection failure of Cohesity NetBackup data collector policy probe.
SC-73384	Resolved the issue that displayed truncated data in the report columns. The issue is fixed and verified all impacted reports including backup RTO and custom RTD reports.
SC-74637	Resolved the issue that continued to display the Compute Resource policy in the policy menu despite being deprecated from IT Analytics.
SC-74255	Resolved the issue that reported data exporter details in the Database Error Summary report along with the data collection of NetBackup Data Collector policy, even after data exporter was deprecated.
SC-74139	Resolved the issue that displayed Flex Appliance access password in clear text when its policy was edited to configure a new Data Collector key.
SC-67924	Upgraded LZ4 to version 1.10.2, which makes CVE-2025-66566 and CVE-2025-12183 non-exploitable.
SC-73679	Resolved ORA-00001 database errors by discarding VMware iSCSI targets with missing or invalid target data (NULL targetName/targetAddress), which prevents unique constraint violations.
SC-74148	Enhanced HIAA Test Connection reliability by adding an HTTPS fallback when HTTP fails with a SocketException.
SC-74852	Resolved the data collection failure in Dell EMC NetWorker, EMC Symetrix, StoreOnce, and PowerFlex Data Collector policies observed after IT Analytics was upgraded to v11.7. Compilation issues in Groovy files of the Data Collectors were resolved to address the issue.
SC-74247	Resolved a race condition in MapDB store access that caused sporadic "Store was closed" errors. This issue previously led to backup policy probe failures when the store was closed while still being accessed.
SC-74927	Fixed the Azure billing probe issue, where the API was failing.
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.

Table 6-1 Fixed issues in 11.7 release *(continued)*

Issue number	Description
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-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-73870	Added FileLevelRestore as new Job Type in IT Analytics for Veeam backup server's restore jobs.
SC-73674	Upgraded Spring Framework to 6.2.15, which makes CVE-2025-41254 non-exploitable.
SC-75180	Apache HTTP server 2.4.66 is built with OpenSSL 3.0.19 which makes CVE-2025-15467 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-74677	Resolved an issue where Data Collector logs and raw data were not available after completing a run or on-demand data collection initiated via the UI, even though the collection process reported successful completion. This fix improves post-collection raw data and Data Collector logs availability for diagnostics.
SC-73617	Report Export on Schedule dialog closes and saves a new schedule when frequency set to minutes or hours.
SC-74465	Resolves an issue with HP 3PAR policy where data collection failed to parse VLUN templates.
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-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.

Table 6-1 Fixed issues in 11.7 release *(continued)*

Issue number	Description
SC-75978	Updated Job Summary report to return unique rows to prevent duplicate rows from being displayed.
SC-75350	Fixed portal upgrade for custom user/group installs by applying upgrade profile logic after aptare_env.sh updates, ensuring the correct users/groups are used during upgrade.
SC-75803	Resolved false alerts for NetBackup Job Policy Attribute Change incorrectly reporting “Cross mount points” changes on NetBackup Catalog backup policies .The policy parser was updated to remove static caching so fresh bppllist data is collected per primary server, eliminating stale data and alert noise.
SC-75505	Resolved the issue that caused incorrect or broken drilldowns due to missing environment values in the DataProtect Active Snapshots By Object report. The report query was corrected to join on policy_id and vendor identifiers instead of names, ensuring consistent data population and accurate drilldown results.
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-75308	Resolved an issue where SDK probes processing Virtual Machine backup items failed to create or match the correct host_id when Host Matching Identifier (HMI) was enabled under another policy. The fix ensures Virtual Machine host resolution now uses the centralized host lookup logic, providing consistent host matching and creation across all backup item types.
SC-75305	Fixed PowerStore collection pagination so arrays with >500 host_volume_mappings are fully captured: the collector now preserves the original command across pages and correctly merges paginated JSON arrays instead of concatenating response strings into invalid JSON, preventing path data beyond the first 500 from being dropped.
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-75805	Fixed an issue where ITA generated false Hung Job alerts for long-running NetBackup jobs due to incorrect job duration calculations. The alert rule now calculates job run duration using the backup server’s timezone, ensuring accurate comparison against alert thresholds and preventing false alarms.

Table 6-1 Fixed issues in 11.7 release *(continued)*

Issue number	Description
SC-73371	Fixed an issue where the Storage Unit Detail Report did not display NetBackup BasicDisk file system details due to an incorrect table reference. The report table reference is changed to ensure correct filesystem and usage information for BasicDisk storage units is populated.
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-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.
SC-75942	Updated database view aps_v_hnas_virtual_volume to prevent divide by zero error.
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.

Table 6-1 Fixed issues in 11.7 release *(continued)*

Issue number	Description
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.

Chapter 7

Known issues, optimizations, and End-of-Life (EOL)

This chapter includes the following topics:

Known Issues

The following known issues are present in this release.

Table 7-1 IT Analytics 11.7 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
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.

Table 7-1 IT Analytics 11.7 Known Issues *(continued)*

Issue Number	Description
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;`

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.

End-of-Life (EOL)

Starting with the next patch release of IT Analytics, support is discontinued for the following features, functionality, OS platforms, and database:

- The JAVA API for XML based RPC (jax.rpc) will be discontinued and support will no longer available.

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.