

NetBackup IT Analytics Release Notes

Release: 11.6

NetBackup IT Analytics Release Notes

Last updated: 2026-03-02

Legal Notice

Copyright © 2026 Cohesity, Inc. All rights reserved.

© 2026 Cohesity, Inc. All Rights Reserved. Cohesity, the Cohesity Logo and other Cohesity Marks are trademarks of Cohesity, Inc. in the US and/or internationally. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. COHESITY SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Cohesity Support

21 September 2025

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.

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.

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Cohesity website.

Cohesity Services and Operations Readiness Tools (SORT)

Cohesity Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1	Introduction	6
	About NetBackup IT Analytics 11.6	6
Chapter 2	Patch Releases	7
	Patch releases: NetBackup IT Analytics	7
	11.6.2603 Patch Release Notes	7
	11.6.2602 Patch Release Notes	8
	11.6.2601 Patch Release Notes	8
	11.6.07 patch release notes	9
	11.6.06 patch release notes	10
	11.6.05 patch release notes	13
	11.6.04 patch release notes	15
	11.6.03 patch release notes	17
	11.6.02 patch release notes	18
	11.6.01 patch release notes	21
Chapter 3	What's New	25
	Data Collection Performance Summary Trend report	25
	TLS 1.3 support for Portal	25
	Host and Object matching improvements	26
	Support for Xanadu version of ServiceNow	26
	Data Collector install supported on OEL 9 and Portal supports collection from Netbackup 11.0	26
	Gain insights into data managed by Dell PowerProtect Data Manager-the data protection software platform	26
	Dell PowerStore connector supported	27
Chapter 4	Supported Systems	28
	Portal supported operating systems	28
	Data Collector supported operating systems	28
	Supported browsers and display resolution	29
	Linux portal server: Exported and emailed reports	30
	Third-party and open source products used	30

Chapter 5	Installations and Upgrades	32
	Portal installation memory requirements	32
	Performance profiles and transmitted data	33
	Reinstate Revoked Public Privileges of Oracle Users	33
Chapter 6	Fixed Issues	35
	Overview	35
	Fixed issues	35
Chapter 7	Known issues, optimizations, and End-of-Life (EOL)	38
	Known Issues	38
	Optimization: Customize the Linux file handle setting for large collections	39
	End-of-Life (EOL)	40
	EOL for Data Collector exporters	40
	End of support for EMC NetWorker Data Collection	41
	End of support: WBEM, IBM XIV, and File Analytics	41

Introduction

This chapter includes the following topics:

- [About NetBackup IT Analytics 11.6](#)

About NetBackup IT Analytics 11.6

The NetBackup IT Analytics 11.6 Release Notes is a cumulative document covering the original 11.6 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 **NetBackup 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.

Patch Releases

This chapter includes the following topics:

- [Patch releases: NetBackup IT Analytics](#)

Patch releases: NetBackup IT Analytics

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

If you have already applied a custom patch after upgrading to 11.6.xx, contact Cohesity support before applying one the following patches as patch releases may reverse the updates provided in the custom patch.

11.6.2603 Patch Release Notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Portal

Table 2-1 Enhancements

Issue Number	Description
SC-75460	NetBackup IT Analytics supports data collection and reporting for NetBackup 11.1.0.2. For detailed list of supported versions, see <i>Supported systems and access requirements</i> section in the <i>NetBackup IT Analytics Certified Configuration Guide</i> .

Table 2-1 Enhancements (*continued*)

Issue Number	Description
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 <i>Reconfigure an Existing Azure Role for Azure Storage Access</i> section in <i>NetBackup IT Analytics Data Collector Installation and Configuration Guide</i> for more information.

11.6.2602 Patch Release Notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Portal

Table 2-2 NetBackup IT Analytics Enhancements

Issue Number	Description
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.

Reports

Table 2-3 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.

11.6.2601 Patch Release Notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Portal

Table 2-4 Enhancements

Issue Number	Description
SC-67428	The <code>aptare_env.sh</code> script is modified with a protected block within the script that must remain unchanged, while you can add custom logic using your own variables and mapping them to the product-defined variables. This modification ensures seamless product upgrades, while allowing user-specific customization within the script.
SC-71705	The NetBackup 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 NetBackup IT Analytics is being changed to Calendar Versioning (CalVer), i.e., from <code>aa.b.cc</code> to <code>aa.b.YYMM</code> . For example: ■ January 2026 monthly update for 11.6 stream will be versioned as 11.6.2601 ■ February 2026 monthly update for 11.6 stream will be versioned as 11.6.2602

Alerts

Table 2-5 Enhancements

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

11.6.07 patch release notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Portal

Table 2-6 Enhancements

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

Table 2-6 Enhancements (*continued*)

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

Data Collector Policy

Table 2-7 Enhancements

Issue number	Description
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

11.6.06 patch release notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Reports section

Table 2-8 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-71939	Resolves an issue where Database Aggregation report displayed ORA-00001: unique constraint (PORTAL.APS_PDEV_PK2) violated error message.

Table 2-8 Enhancements and resolved issues (*continued*)

Issue Number	Description
SC-72446	The Backup Master server report scope dialog box has been enhanced to include a new option for selecting previous week date criteria from Monday to Sunday, in addition to the existing Sunday to Saturday range.
SC-72757	Resolves an issue in Database Error Aggregation report. The portal displayed ORA-12899: value too large for column "PORTAL"."APT_DATACOLL_EXEC_TRACKING"."PROCEDURE_NAME" error message.
SC-72775	Resolves an issue with Security Details probe. The Database Error Aggregation, of System Administration Reports, displayed nbu_adaptor_package.saveScanResultList 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-73178	Resolves an issue with data mismatch of licensing capacity between values returned from API and NetBackup FETB Usage Summary 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.

Portal section

Table 2-9 Enhancements and resolved issue

Issue number	Description
SC-60234	NetBackup IT Analytics is enhance to persist CommVault reason codes.
SC-6373	Resolves an issue where the database error logs were incorrectly recorded in <code>README.txt</code> . In a split architecture, since the database logs are not available on the PORTAL server, <code>README.txt</code> now displays the message: <i>[INFO] Download database log files from the database server.</i>
SC-71699	Resolves an issue with SLP Job Details probe where the portal displayed parsing error message.
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-72055	Resolves an issue of incorrect data persisted after executing Storage Inventory probe.
SC-72276	Resolves the stored procedure performance issue.

Table 2-9 Enhancements and resolved issue (*continued*)

Issue number	Description
SC-72519	The following enhancements incorporated for the job tickets created by ServiceNow: Job Finalized alert policy: ■ Two new columns <code>clear_date</code> and <code>clearing_job_id</code> incorporated in <code>apt_job_ticket</code> table. <code>clear_date</code>: Records the timestamp when a job alert was resolved. <code>clearing_job_id</code>: 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-72677	Resolves an error during data collection. The error was logged when executing the Protection Details probe using Cohesity DataProtect policy.
SC-72760	The Oracle patch installation process is enhanced. Post successful installation, Cohesity recommends to run the <code>ora_scripts</code> from the <code>\$ORACLE_HOME/orascripts</code> 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 <code>APT_PUBLISHED_VIEW</code> , broken hyperlinks were displayed for GitHub documentation.
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-72781	Resolves an issue with Data Collector services with the name of the data collector more than 100 characters.
SC-72785	NetBackup IT Analytics is enhanced to support Apache HTTP server version to 2.4.65.
SC-72807	Resolves an issue where after running the <code>resetPermission.sh</code> utility, logs were not getting generated from the support tool.
SC-72814/SC-73250	NetBackup IT Analytics now supports Apache Tomcat version to 9.0.108.
SC-72880	Resolves an issue where the column length prevented persisting data for few tables.
SC-72916	NetBackup IT Analytics now supports Apache HTTP Web server version 2.4.65.
SC-73068	Resolves an issue after Kafka upgrade. Post upgrade, Kafka failed to start due to reverted access rights of the folders within.

Table 2-9 Enhancements and resolved issue (*continued*)

Issue number	Description
SC-73077	Resolves an issue with data purging for EMC Symmetrix where the data was purged based on creation date rather than last discovered date.
SC-73128	Resolves an issue with Groups tab of Alert Rule for ServiceNow: Job Finalized. Portal displayed empty values for product type drop-down.
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.

11.6.05 patch release notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Reports section

Table 2-10 Enhancements and resolved issues

Issue Number	Description
SC-72123	Resolves an issue when exporting the reports from Inventory module.
SC-72271	Resolves an issue with <i>Database Error Aggregation</i> report. The report displayed <i>APT-DB-109880</i> error message related to TSM Backup Event Details Probe.
SC-72454	Resolves an issue with the reports where the report header caption contained HTML tags . The following were the impacted reports. ■ VM Guest to LUN Performance ■ Datastore Performance Summary ■ VM Performance Summary
SC-72766	Resolves an issue where NetBackup IT Analytics encountered error when applying a filter on a numeric field with is a member of or is not member of operator for a comma delimited numeric values.

Portal section

Table 2-11 Enhancements and resolved issue

Issue number	Description
SC-64860	Resolves an issue with upgraded connector and data collectors for Linux. Post connector upgrade, the <code>./downloadlib.sh -skipVerification</code> command failed.
SC-68099	Resolves an issue with Backup policy probe. When the policy was executed (scheduled/on-demand), portal displayed error message - Store was closed.
SC-68318	Resolves an error <i>APT-DB-108000</i> of the Networker Protection details probe.
SC-71397	NetBackup IT Analytics is enhanced with modifying the writable Linux database user's <code>.profile</code> and <code>.bash_profile</code> files. With this enhancements, NetBackup IT Analytics now auto-execute <code>aptare_env</code> which enables seamless SQLPlus access, post login.
SC-71513	Resolves the CVE-2025-1948 and CVE-2024-6763 reported issues.
SC-71545	Resolves the CVE-2024-8176 and CVE-2024-50602 reported issues.
SC-71547	NetBackup IT Analytics is enhanced to support Apache HTTP Server version 2.4.64.
SC-71570	Resolves an issue where the <i>NetBackup Catalog Not Backed Up</i> alert was not clearing after the alert condition or backup occurred.
SC-71608	Resolves an issue that occurred after upgrading to version 11.6.2, where the portal was unable to delete any array. During manual deletion, the portal displayed the error message: <i>Array has child exists</i> .
SC-71623	NetBackup IT Analytics is enhanced with performance improvement while persisting the Data Domain System andmtree compression logs.
SC-71997	Resolves an issue with HP Data Protector policy. Post upgrading the portal to version 11.6.02, the portal was not able to persist the value for Device name and hence the probe failed.
SC-72060	Resolves an issue in the connector deployment logs during synonym creation for Windows portal. Password was displayed in the log file.
SC-72448	Resolves an issue with <i>Alert Notification</i> popup error logged in <code>portal.log</code> file. The error was logged due to de-linking of Alert notification with Syslog configurations.
SC-72494	Resolves an issue where the validator tool failed to validate <code>ITA-SYS-ALERT.mib</code> file.
SC-72524	Resolves a connector deployment / upgrade failure for Microsoft Azure.
SC-72571	Resolves an issue where the preUpgradeCheck and resetPermission utility failed when the Oracle user primary group is other than Oracle group.
SC-72623	NetBackup IT Analytics now supports Flex Appliance policy collection for v6.2.

11.6.04 patch release notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Reports section

Table 2-12 Enhancements and resolved issues

Issue Number	Description
SC-69819	Resolves the export functionality of reports which failed for Storage Optimization Analysis Report and Storage Optimization By Tier report. These reports were having no data to display and hence exporting to CSV, TXT, and EXCEL format failed.
SC-71653	Resolves an issue reported in the DB Error Aggregation report. The report displayed error message - <i>hpd_adaptor_package.saveHPDMedia - library is invalid</i> .
SC-71700	NetBackup IT Analytics is enhanced to stream the ZIP of reports content directly to the HttpServletResponse output stream, eliminating the need for in-memory buffering.
SC-71848	Resolves an issue in updating FETB consumption in OOB NetBackup client and policy reports. The FETB value, policy-wise FETB usage, displayed incorrect values.
SC-71850	Resolves an issue with Backup RTO RPO Compliance report where the column name # Incr After Full and Incr Size After Full was displayed with the HTML tags as # Incr
 After Full and Incr Size
 After Full .
SC-71897	Resolves an issue with Data Collection Performance Summary report which failed post portal upgrade to version 11.6.02.
SC-71947	Resolves an issue when running a new report. This issue was observed when running a drill down report, which is still in process, NetBackup IT Analytics prevented the user to run another report.

Portal section

Table 2-13 Enhancements and resolved issue

Issue number	Description
SC-58600	Resolves the duplicate validations issue of the attribute values in the database. Hence, due to the duplicate attributes, NetBackup IT Analytics displayed error message.
SC-67689	The APS_V_H3P_RCOPY_GROUP SQL view is enhanced to include CREATION_DATE column. This column displays Remote Copy Group creation time for a H3PAR storage Array details, which can be utilized in the specific customs reports.

Table 2-13 Enhancements and resolved issue (*continued*)

Issue number	Description
SC-67897	NetBackup IT Analytics addresses the following CVE reported issues: ■ CVE-2025-24898: The vulnerable signature "ssl::select_next_proto" issue. ■ CVE-2025-3416: The vulnerable functions.
SC-68431	Resolves the Blackduck vulnerability issues due to protobuf. The component has been upgraded to version 1.23.7.
SC-71003	NetBackup IT Analytics addresses the CVE-2025-31672 of OOXML to read files.
SC-71331	Resolves an issue during a new installation of NetBackup IT Analytics. In the process of installation, when the existing database was imported, most of the system parameters where impacted.
SC-71514	NetBackup IT Analytics addresses the CVE-2025-4432 vulnerability.
SC-71523	Resolves an issue with NetBackup Job Finalized Successful alert email. NetBackup IT Analytics failed to email the alert when the alert policies was created with Policy Type , Job Type & in Primary Server in the scope selectors. NetBackup IT Analytics displayed an error message - <i>PTL_NBU_POLICY. POLICY_TYPE_NAME: invalid identifier.</i>
SC-71546	NetBackup IT Analytics addresses the CVE-2025-48734 vulnerability.
SC-71639	Resolves an issue of API not returning the uuid attribute in the response, which is an optional field. However, the data collection failed for Storage unit details probe in Netbackup and the data was not getting persisted.
SC-71650	Resolves an issue when the API response does not return the host group number when a host is not assigned to a host group. Further, the errors are logged in the log file as assigning host to host group is optional which is the expected functionality. To resolve this issue, NetBackup IT Analytics is enhanced to convert this error into a warning message.
SC-71652	Resolves an issue where NetBackup IT Analytics persisted incorrect zone mapped to the host based on WWN.
SC-71820	Resolves an issue with synonym creation when the Oracle user profile do not have the ORACLE_HOME and ORACLE_SID environment variables.
SC-71948	The database performance data logging feature has been enhanced by introducing a new parameter in the <code>systemlogger.xml</code> file. With this update, when troubleshooting the performance issue, NetBackup IT Analytics logs only the database performance-related data in the portal log file, thereby reducing the logging volume and overhead.
SC-71993	The following CVE issues are addressed. ■ CVE-2025-48988 ■ CVE-2025-49124 ■ CVE-2025-49125

Table 2-13 Enhancements and resolved issue (*continued*)

Issue number	Description
SC-72492	NetBackup IT Analytics is enhanced to incorporate alternate commands to collect Directors and Ports related data from the following supported PowerMax version : ■ PowerMax - version 10.2.0.1 ■ Product model - 2500/8500 ■ Policy - EMC Symmetrix Connector.

11.6.03 patch release notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Reports section

Table 2-14 Enhancements and resolved issues

Issue Number	Description
SC-71635	Resolves an issue where NetBackup IT Analytics displayed tag in the Backup RTO RPO Compliance report.

Portal section

Table 2-15 Enhancements and resolved issue

Issue number	Description
SC-67005	Resolves an issue with the REST API where users were able to create hosts outside their home host group.
SC-69784	Resolves the Array Details probe failure for Hitachi Vantara Flash Storage.
SC-71106	NetBackup IT Analytics now supports Tomcat version 9.0.105.
SC-71331	Resolves an issue during a new installation of NetBackup IT Analytics. In the process of installation, when the existing database was imported, most of the system parameters were impacted.
SC-71401	Resolves an issue of data collection job discrepancies between jobs reported by NetBackup primary server as against NetBackup IT Analytics.
SC-71417	Resolves an issue with user audit event where the previous modifications of the user details was not persisted. Hence, whenever a user attribute was modified, modified user audit event was not generated capturing the modifications.

Table 2-15 Enhancements and resolved issue (*continued*)

Issue number	Description
SC-71497	Resolves an issue when NetBackup IT Analytics reported error message after the Flex Appliances was removed from Inventory tab.
SC-71530	Resolves an issue in the Dell PowerProtect Data Manager where the advanced parameters DPDM_LOOKBACK_HOURS, DPDM_ACTIVITY_INCLUDE_CATEGORY, and DPDM_ACTIVITY_EXCLUDE_CATEGORY do not support the default values of empty strings. This limitation caused ITA to throw an error during execution of the Protection Details Probe when these parameters are used without explicitly defined values. DPDM_LOOKBACK_HOURS supports default value of -1, meaning no look back hours.
SC-71563	Resolves an issue where the SQL view apt_v_nbu_dedup_job_details displayed duplicate records.
SC-71626	Resolves the typographical issue in load scripts and view create scripts across columns of SQL views and table of apt_published_view and apt_published_view_column
SC-71664	Resolves the performance issue post NetBackup IT Analytics upgrade to version 11.6.02.

11.6.02 patch release notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Backup Manager data collection section

Table 2-16 Enhancements and resolved issues

Issue number	Description
SC-54797	Resolves documentation issue in <i>Cohesity Data Collector Installation and Configuration Guide for Cohesity NetBackup > Configure a Cohesity NetBackup Data Collector Policy > Add a Cohesity NetBackup Data Collector policy</i> section. The document incorrectly mentioned the schedule for Backup Policies as Weekly and Monthly.

Reports section

Table 2-17 Enhancements and resolved issues

Issue Number	Description
SC-63390	ALTA & NetBackup IT Analytics Resolves an issue in System Administration Report where NetBackup IT Analytics reported Database Error Aggregation error with code - APT-DB-108916.
SC-64274	Resolves an issue with the reports exported as PDF from a Portal server running as a Service on Windows, the report was getting truncated from the right margin.

Table 2-17 Enhancements and resolved issues (*continued*)

Issue Number	Description
SC-67412	Resolves an issue with tool tip in reports. The tool tip of a tabular templet or a DTD template displayed incorrect description of the report type.
SC-67596	Resolves an issue with the backup job reports where the report displayed incorrect data or data gaps due to prolonged processing of job details probe.
SC-67695	Resolves an issue with NetBackup Policies report where the report header mis-aligns when a new inventory tab was added.
SC-68579	Resolves an issue with nbdeployutil utility. The utility was persisting more than one occurrences of policy consumption metrics with different consumption amount at policy level for same client, policy with different images created in different time stamps. This created data discrepancies in FETB reports.
SC-71112	Resolves an issue with NetBackup front end size by workload report where the converting pie chart report to table format NetBackup IT Analytics displayed incorrect report data.

Portal section

Table 2-18 Enhancements and resolved issue

Issue number	Description
SC-62115	Resolves the performance issue of Historic data collection process.
SC-62896	Resolves an issue of backup fragment persistence which was failing when backup job is not active.
SC-62945	NetBackup IT Analytics is enhanced to persist the status of the job from data collection.
SC-65032	NetBackup IT Analytics now supports powerStore connector. See “Dell PowerStore connector supported” on page 27.
SC-66379	The Test Connection feature in data collector policy is enhance to verify the role of the user.
SC-67585	Resolves the probe failure issue due to API login failure. NetBackup IT Analytics is enhanced to successfully execute the probe even after API login failure.
SC-67905	The NetBackup IT Analytics has been enhanced to include the preUpgradeCheck.sh utility for Linux. Users can run this tool prior to upgrading the portal. It verifies that system users, group memberships, and the database user have the necessary permissions.
SC-68154	ALTAView: Resolves an issue with incorrect status code '999999' was displayed in the Exit Code column of Job Summary report.
SC-68173	NetBackup IT Analytics now supports tomcat-servlet-API version 9.0.102

Table 2-18 Enhancements and resolved issue (*continued*)

Issue number	Description
SC-68364	Resolves an issue where the last collection date used in NetBackup Job Details probe was getting deleted during cleanup of obsolete data for probe status information.
SC-68420	ALTA: Resolves an issue with data collector where the collectorConfig.xml was getting generated every minute, impacting the performance.
SC-68423	Resolves an issue with Array Capacity probe of Dell EMC Elastic cloud storage policy where NetBackup IT Analytics displayed error message - LogoutFailureException: Session logout failed.
SC-68450	Resolves an issue where the HP Data Protector data collection policy was not reporting all backed up session objects for same mountpoint and client thus impacting the billing.
SC-68558	Resolves an issue where upgrading the portal to version 11.5.02, the portal failed to display system anomalies.
SC-68597	Optimized the database performance by minimizing parameter value retrievals for a frequently executed process that logs DB time metrics.
SC-69818	Resolves a database error message - ORA-01438: value larger than specified precision allowed.
SC-70771	Resolves an issue encountered when adding a Data Collector with Kerberos enabled.
SC-70779	Resolves an issue where some parameters were left uncategorized, leading to incorrect UI placement.
SC-70847	NetBackup IT Analytics now supports Amazon Corretto version 17.0.15.6.1
SC-70992	Resolves incorrect message displayed while import DTD during versions incompatible.
SC-71002	ALTA: Resolves an issue with the February release where the SLP Job Details Probe was failing with an error An error occurred while collection Catalog Image information.
SC-71081	NetBackup IT Analytics is enhanced to retain the connection between the volume pool and backup details for HP Data Protect backup sessions.
SC-71087	NetBackup IT Analytics is enhanced to incorporate an index to speed up the deletion of stale data from data protect object detail.
SC-71198	Resolves the database issue during the portal upgrade. The change in the column data type is not allowed when having data in it. This scenario occurred during the portal upgrade from the older version to 11.5.05.
SC-71200	Resolves an issue in load password policy where NetBackup IT Analytics logged an error message - no data found.

11.6.01 patch release notes

The patch release includes all the previous patches of versions.

The following changes are included in this release.

Reports section

Table 2-19 Enhancements and resolved issues

Issue Number	Description
SC-62727	Resolves an issue with Job Summary report where the Duration column displayed as Milliseconds instead of hours:minute:seconds format when exported in Excel format. NetBackup IT Analytics is enhanced with new field Export duration column as hh:mm:ss incorporated in My Profile dialog box.
SC-64733	The NetBackup SLP Status by SLP report is updated to show correct values in few fields related to SLP Copies.
SC-67579	Resolves an issue reported in Database Error Aggregation and Database Error Summary reports. The reports displayed application code error message as APT-DB-177065.
SC-67691	Resolves an issue with Running and Queued Job Summary report where incorrect value was displayed for Duration.
SC-67920	Resolves an issue with scheduled emails or report exports where the chart reports, when converted to tables, were still being sent or exported as charts instead of tables.
SC-68219	The Data Domain System Details report is enhanced to include the following columns: ■ Active Metadata Capacity ■ Used Metadata Capacity ■ Usage Archive Metadata Capacity ■ Used Metadata Archive Usage For more information, see <i>NetBackup IT Analytics Report Reference Guide</i> > <i>Backup Storage Utilization reports</i> > <i>Data Domain System Details report</i> section.
SC-68282	Resolves an issue with an SQL view apt_v_nbu_schedule. NetBackup IT Analytics displayed an error message Subscript beyond count when using the view for a report.
SC-68324	The NBU jobs reports in NetBackup IT Analytics is enhanced to include Policy Type column which can also be used during filtering the data.

Portal section

Not applicable in this release.

Table 2-20 Enhancements and resolved issue

Issue number	Description
SC-51735	NetBackup IT Analytics is enhanced to persist additional Microcode details. Added new columns to the relevant database table to support this enhancement. A new SQL view APS_EMG_SYM_STORAGE_ARRAY is available to create reports.
SC-51736	NetBackup IT Analytics is enhanced to persist actual serial number of HPE Nimble sub systems.
SC-53236	NetBackup IT Analytics is enhanced to persist IP address of Hitachi sub systems.
SC-55478	The security details probe is enhanced to persist additional information for NetBackup Malware through the API call.
SC-57657	Resolves an issue where NBU jobs in the NetBackup IT Analytics database were being overwritten when the NBU job database on the primary server was reset, and the same NBU job IDs were created and collected within the last 30 days.
SC-61441	NetBackup IT Analytics is enhanced to support additional time zone which was causing the error message - time zone region not found.
SC-63603	Resolves an issue with Cluster Details Probe which failed if the large amount of data existed in Isilon filers, now known as Dell EMC Isilon.
SC-66323	Resolves an issue with the Oracle, Portal Installers and Portal upgraded where the DB users do not support passwords containing Bash special characters.
SC-66508	NetBackup IT Analytics now supports Dell EMC Power Protect Data Manager(PPDM) connector. For more information, see <i>NetBackup IT Analytics Data collector installation and configuration guide > Data protection > Configuration of Dell EMC PowerProtect Data Manager (PPDM)</i> section.
SC-66559	Resolves an issue where Dell EMC Unity data collection failed to link snapshot to the file system.
SC-66623	NetBackup IT Analytics is enhanced to support bean validation API version 3.1.1.
SC-66665	Resolves an issue with password change from the portal. The portal incorrectly logged the error message for wrong password as invalid user.
SC-66882	NetBackup IT Analytics is enhanced to provide choice to kill the file locking process during the data collector upgrade. For more information, see <i>NetBackup IT Analytics data collector installation and configuration guide for Cohesity NetBackup > Upgrading data collector locally > Resolve file lock issue on Windows host during Data Collector upgrade</i> section.
SC-66960	Resolves an issue with Cohesity data protection details probe where NetBackup IT Analytics displayed an error message while using REST API.
SC-67023	The Oracle patch 19c January 2025 for Windows is now available in the Download center.

Table 2-20 Enhancements and resolved issue (*continued*)

Issue number	Description
SC-67085	Please refer See “ End-of-Life (EOL) ” on page 40.
SC-67100	NetBackup IT Analytics is enhanced with the removal of database parameters related to Internet/Cloud services that have been deprecated.
SC-67567	Following issues are resolved: ■ Resolve the error message in Backup Message logs probe failure: Inserted value too large for column. ■ The skipped backup files are now getting populated.
SC-67595	Resolves an issue with EMC Isilon Performance probe which was failing due to the parsing issue.
SC-67710	Resolves an issue with the Collection Status page search functionality, where NetBackup IT Analytics only searched for the first word in the search.
SC-67725	Resolves an issue with Alerting tab of the Domain Administrator dialog box. When the SNMP Trap payload check box field was selected, the alerting mechanism was default selected as Legacy instead of Enhanced.
SC-67757	Apache Tomcat is upgraded to 9.0.102 to resolve CVE-2025-24813 vulnerability.
SC-67763	The Cohesity NetBackup data collector policy dialog box is enhanced as a part of re-branding to align with Cohesity.
SC-67884	Resolves an issue with EMC Avamar policy. The operational data probes such as Static data and operational data were failing.
SC-67887	Resolves a probe failure issue of Microsoft Azure Virtual Machine.
SC-67891	Resolves an issue with license module. NetBackup IT Analytics displayed an invalid license error message.
SC-67968	Resolves an issue with Backup policy probes. The CLI commands, which were running during the probe execution, failed to log the details due to access denied to the log folder.
SC-68097	Resolves an issue where the duplicate jobs records for host, related to partial jobs with active sessions, were being persisted.
SC-68126	Resolves an error for alert rule ServiceNow: Job Finalized(Category Grouping).
SC-68181	Resolves database issue. NetBackup IT Analytics displayed APT-DB-106004 and APT-DB-106006 database errors.
SC-68223	NetBackup IT Analytics now supports data collector operating system OEL version 9.
SC-68240	Resolves a database error APT-DB-105132 causing the data lose.

Table 2-20 Enhancements and resolved issue (*continued*)

Issue number	Description
SC-68258	Resolves an issue with HPE XP Array details probe where NetBackup IT Analytics was persisting incorrect total logical unit capacity in certain scenario.
SC-68317	Resolves an issue of host decommissioning failure occurred due to incorrect column allocation to persist the values of OS platform and OS version.
SC-68566	Resolves an issue with NBU Job Details Probe where NetBackup IT Analytics displayed incorrect warning status. The warning status occurred in case of multiple primaries in a single collector and any one primary failed thus reflecting the same status to all the primaries.

What's New

This chapter includes the following topics:

- [Data Collection Performance Summary Trend report](#)
- [TLS 1.3 support for Portal](#)
- [Host and Object matching improvements](#)
- [Support for Xanadu version of ServiceNow](#)
- [Data Collector install supported on OEL 9 and Portal supports collection from Netbackup 11.0](#)
- [Gain insights into data managed by Dell PowerProtect Data Manager-the data protection software platform](#)
- [Dell PowerStore connector supported](#)

Data Collection Performance Summary Trend report

This report provides information on how the Data Collection Performance Trend looks over a period of time. Information such as the Data Collector Components, Daily Linear Change and Total Elapsed Time is available from this report. In addition, Performance History and Linear Trend are represented as Sparklines. A good use case for this report can be a Report based Alert with filter set on the column that displays percentage linear change.

TLS 1.3 support for Portal

NetBackup IT Analytics supports TLS 1.3 for Web Portal, Rest APIs, and for communication between Data Collector and Data Receiver (along with TLS 1.2).

Host and Object matching improvements

This improvement is introduced specifically for environments having single IT Analytics domain with multi-client setup (HMI). The improved logic will allow assigning a different host matching identifier (HMI) at the Data Collector policy level. Previously, a Data Collector policy was used to get an HMI, same as the Data Collector level, but now a different HMI can be applied at Policy level. In summary, following changes have been made:

- Supporting HMI for hosts created during NetBackup IT Analytics Data Collector policy creation. This includes policy server to automatically inherit policy's HMI during policy creation.
- Showing HMI in inventory under Host grid report.

Support for Xanadu version of ServiceNow

IT Analytics ServiceNow App has been certified by ServiceNow for Xanadu release.

Data Collector install supported on OEL 9 and Portal supports collection from Netbackup 11.0

NetBackup IT Analytics now supports its Data Collector installation and operations from OEL 9 hosts and its capabilities are enhanced to provide analytics on NetBackup 11.0 data collection.

Gain insights into data managed by Dell PowerProtect Data Manager-the data protection software platform

NetBackup IT Analytics now offers insights on data collected and managed by Dell PowerProtect Data Manager. You can view details based on protection sources such as System Configuration, Licenses, Nodes, Disks, Protection Policies, Protection Rules, and Policies for disaster recovery. You can also perform analytics based on protection details such as Assets, Hosts, and Activities. IT Analytics now includes the Dell PowerProtect Data Manager Data Collector policy to enable data collection for these reporting capabilities. Since the data collected can be viewed only through custom reports, use the dynamic template designer or the SQL template designer to generate reports.

See *Configuration of Dell EMC PowerProtect Data Manager (PPDM)* section in the *NetBackup IT Analytics Data Collector Installation and Configuration Guide* for more information.

Dell PowerStore connector supported

NetBackup IT Analytics now supports Dell PowerStore connector version 4.0.0.0 and 4.1.0.0.

For supported configuration, see *NetBackup IT Analytics Certified Configuration Guide > Capacity manager configuration > Supported systems and access requirements* section.

For installation and prerequisites, see *NetBackup IT Analytics Data Collector Installation and Configuration Guide > Section III. Storage (Capacity) > Pre-installation setup for Dell PowerStore* section.

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 Portal Supported Operating Systems

Operating Systems	Version
Red Hat Enterprise Linux	8 (update 6 onwards) and 9 (update 4, 5)
SUSE Linux Enterprise	SLES 12 SP5 and SLES 15 SP5
Windows	2019 and 2022
OEL	8

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	8 and 9
SUSE Linux Enterprise	SLES 12 SP5 and SLES 15 SP5
OEL	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
- Browser vendor (such as Chrome or Edge) and version

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	9.0.112	9.0.112
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

If other versions of the above components are already running on the designated NetBackup IT Analytics system, or other components are utilizing resources (such

as specific ports) typically used by NetBackup 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.

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 virtual 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 *NetBackup IT Analytics Installation and Upgrade Guide*:

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

Fixed Issues

This chapter includes the following topics:

- [Overview](#)
- [Fixed issues](#)

Overview

The 11.6 release includes all patch release fixes of version 11.5.

[See NetBackup IT Analytics patch releases.](#)

Fixed issues

The following issues were fixed or resolved in this release.

Table 6-1 Fixed issues in 11.6 release

Issue number	Description
SC-62135	Updated the Client Summary Report to prevent Oracle divide by zero (0) error.
SC-62484	Updated the Client Summary Report so that the Total Jobs reflects accurately when Restore Jobs are present for the client.
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.

Table 6-1 Fixed issues in 11.6 release (*continued*)

Issue number	Description
SC-73675	Addressed Apache-specific issues caused when Apache was upgraded to version 2.4.65 in NetBackup IT Analytics 11.6. 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-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
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-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-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-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.
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-71970	Updated the collection window start time to fix the issue that caused reports to miss details of jobs created at the hour boundary.

Table 6-1 Fixed issues in 11.6 release (*continued*)

Issue number	Description
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-74857	Fixed the issue that resulted in error displayed when the end user with very limited privileges opened email/export schedule dialog.
SC-73884	Fixed the issue causing error while upgrading NetBackup 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.

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

This chapter includes the following topics:

- [Known Issues](#)
- [Optimization: Customize the Linux file handle setting for large collections](#)
- [End-of-Life \(EOL\)](#)
- [EOL for Data Collector exporters](#)
- [End of support for EMC NetWorker Data Collection](#)
- [End of support: WBEM, IBM XIV, and File Analytics](#)

Known Issues

The following known issues are present in this release.

Table 7-1 NetBackup IT Analytics 11.6 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 NetBackup IT Analytics 11.6 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	NetBackup 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. - Create a backup of the old Quartz table. <pre>SQL> CREATE TABLE BKP2511_APT_QZ_CRON_TRIGGERS AS SELECT * FROM APT_QZ_CRON_TRIGGERS;</pre> - Truncate the table. This ensures the upgrade completes seamlessly. <pre>SQL> TRUNCATE TABLE APT_QZ_CRON_TRIGGERS;</pre>

Optimization: Customize the 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 NetBackup 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 be available.

EOL for Data Collector exporters

The feature known as the Exporter is being deprecated with the next major release to eliminate the additional testing and certification required. This supplementary collection mechanism utilized the Prometheus exporter framework to probe the host for some pre-specified processes, subsystem internals and metadata but was never adopted by any IT Analytics users.

End of support for EMC NetWorker Data Collection

The support for EMC NetWorker Data Collection functionality will be discontinued. However, the support for Dell EMC NetWorker Backup & Replication will continue.

End of support: WBEM, IBM XIV, and File Analytics

Starting with the next major release after NetBackup IT Analytics 11.6, support is discontinued for the following features, functionality, OS platforms, and database.

WBEM

All Cohesity NetBackup IT Analytics Data Collector policies will discontinue the use of Web-Based Enterprise Management (WBEM) with the next major release after NetBackup IT Analytics 11.6. WBEM is a set of systems-management technologies developed to unify management of distributed computing environments. It is used in some of the NetBackup IT Analytics Data Collection policies. The table below lists NetBackup IT Analytics Data Collector policies that use WBEM code and defines the impact of removing the WBEM on each Data Collector policy.

Table 7-2 Policies using WBEM code

Policy	Impacted version	Impact on collection
Dell Compellent	No	N/A Dell Compellent is not supported since Jan 2, 2023.
HP 3PAR	Earlier than Inform 2.3.1 (March 2014)	None. Cohesity does not support versions earlier than Inform 2.3.1. All versions lower than Inform 2.3.1 will be impacted.
Cisco Switch	All	Complete collection.
HP EVA	No	None.
IBM Enterprise	No	None.
EMC Clariion	No	None.

Table 7-2 Policies using WBEM code (*continued*)

Policy	Impacted version	Impact on collection
EMC Symmetrix	Earlier than symcli 7.1.3 (November 2012)	None. Cohesity does not support versions earlier than symcli 7.1.3. All versions lower than symcli 7.1.3 will be impacted.
Hitachi Storage	No	None.
IBM SVC	All	Complete collection.
IBM XIV	All	Performance collection.
Net App 7	No	None.
Brocade Switch	Earlier than Brocade FOS 7.4 (July 2015)	None. Cohesity does not support versions earlier than Brocade FOS 7.4. All versions lower than Brocade FOS 7.4 will be impacted.

Cisco and IBM SVC

Cohesity plans to rewrite the Data Collector policies for Cisco and IBM SVC to no longer require WBEM support.

IBM XIV

This Data Collector Policy will be deprecated in the next major release after NetBackup IT Analytics 11.6.

File Analytics

This Data Collector Policy and feature will be deprecated in the next major release after NetBackup IT Analytics 11.6. File Analytics is currently available with NetBackup IT Analytics complete suite.