COHESITY

Release Notes

Version 7.1.2

July 25, 2025

Published on July 25, 2025

Contents

Disclaimer

Features and functionalities herein may become subject to a separate license requirement/fee (even if free during an initial period).

Cohesity provides from time to time - in release notes or in other communications to our customers - written updates about end of support for third-party software versions. Such updates are for informational purposes only, and are not a substitute for information you receive directly from third-party software publishers. Cohesity support practices align to third-party end of support, and as such Cohesity will not in any case support a version of third-party software that is no longer supported by its publisher. For further/up-to-date information, see the Third-Party Software Support Matrix for Cohesity Data Protection.

What's New?

Cohesity Platform 7.1.2 provides new features and enhancements available for on-premises hardware, Cloud Edition, and Virtual Edition clusters. For more information, see What's New in 7.1.2?.

For more information on upgrading from previous releases to 7.1.2, see Upgrading to 7.1.2.

For more information on previous releases, see What's New in Earlier Releases?

> **Important:**
> In the 7.1.2 release train, version 7.1.2_u2 was designated as Long-Term Support (LTS) on October 28, 2024. The latest LTS version, 7.1.2_u4, was released on June 05, 2025. Cohesity recommends that you upgrade to 7.1.2_u4 to benefit from new features, security improvements, and performance enhancements.
>
> To get a full overview of the features and updates introduced between versions, you can refer to the LTS Digest.

This section provides the following What's New information:

What's New in 7.1.2_u4?

The following new features and improvements are available in this release. For important information about upgrading from previous releases to 7.1.2_u4, see Upgrading to 7.1.2.

Early Access (EA) Feature

From time to time, Cohesity may add features and request for feedback on their utility and design. These features are termed as Early Access features. Early access features are limited to a closed group of testers for a limited subset of launches. Participation is by invitation only and may require signing a pre-general-availability agreement, including confidentiality provisions. These features may be unstable, change in backward-incompatible ways, and are not guaranteed to be released. There are no SLAs provided and no technical support obligations. These EA features are by default disabled and hidden and need to be enabled separately. If you wish to use these EA features you need to contact your accounts team, who will internally work within Cohesity to enable the feature on your cluster. Cohesity recommends running these features only on non-production clusters.

Data Protection

Microsoft 365

Protect Recoverable Items in Mailboxes Early Access

Cohesity now supports the backup and recovery of the Recoverable Items folder in the Microsoft 365 Mailboxes. These folders preserve the items that are soft deleted or deleted from the Deleted Items folder.

> **Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

Protect PHL in OneDrive Early Access

Cohesity now supports the backup and recovery of Preservation Hold Library (PHL) in OneDrive which is used to store the files needed for compliance reasons.

> **Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

Protect Lists in SharePoint Online Early Access

Cohesity now supports the backup and recovery of the Lists in Microsoft 365 SharePoint Online. Lists are data collection like links, announcements, contacts, issue trackers, surveys, and so on.

> **Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

Protect Ownerless Teams and Groups Early Access

Cohesity now supports the backup and recovery of Teams and Groups (Public and Private) with no owners, when at least one Exchange Online licensed member is available in the Teams/Groups.

If no owners/members are available in the Teams/Groups, you can contact your Cohesity account team to configure a service account (with an Exchange Online license). This service account will be added as a member of the Teams/Groups before backup/recovery and removed after the backup/recovery is complete.

> **Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

SharePoint Online Sites Protection in Multi-Geo Locations Early Access

You can now discover and protect SharePoint Online sites in the Satellite storage locations of the Microsoft 365 tenant along with the Central storage locations.

> **Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

Recover Deleted Teams Private Channels

You can now recover the deleted private channels to the original Microsoft 365 domain. If you are recovering to an alternate Microsoft 365 domain, you can create a new private channel and recover the data.

Certificate-Based Authentication for Microsoft 365 Applications Early Access

Cohesity supports Certificate-Based Authentication (CBA) when registering Microsoft 365 applications. This feature allows you to authenticate with an X.509 certificate against the Public Key Infrastructure (PKI) and provides phishing resistant authentication.

> **Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

Physical Servers

Allowing file-based backups to fail protection runs on warnings Early Access

Cohesity now supports configuring Physical file-based backup runs to fail if any error is encountered.

> **Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

Databases

Support for Recovering SAP HANA 2.0 Backups Across Hardware Platforms

Cohesity now supports the recovery of SAP HANA 2.0 backups across both Intel x86-64 and Power PC platforms, allowing you to restore your critical SAP HANA data regardless of the underlying hardware architecture.

Support for SSL-Encrypted Communication in SAP HANA Data Protection

Cohesity now supports data protection for SAP HANA deployments that use SSL encryption for communication between the SAP HANA client and server.

Parallel Replication and Archival for Oracle ZDLRA Protection Jobs

Cohesity now supports parallel replication and archival for Oracle ZDLRA protection jobs.

NAS

Add Note when Pausing Protection Groups and Runs

Cohesity now allows you to add notes when pausing current or future runs of Protection Groups.

Recover Files and Folders for SnapDiff Based Backups

Cohesity now allows the recovery of up to eight files or one folder from SnapDiff-based backups.

Replication

Replication from Inactive to Active Protection Job

Cohesity now supports replication from an inactive protection job to an active protection job.

Cloud Edition and NGCE Clusters

New Instance Types Support for AWS CE Cluster

Cohesity now supports m6a.4xlarge and m6i.4xlarge instance types for AWS Cloud Edition cluster nodes.

FortKnox Vaulting Support for AWS and Azure NGCE Clusters

AWS and Azure NGCE clusters can now vault data to a Cohesity FortKnox cloud vault.

Cluster Management

Upgrade Cluster

Cluster Upgrade with Patch Application

Cohesity now supports applying patches along with the upgrade packages. Once the upgrade is completed on the node, the patch application will begin automatically.

What's New in 7.1.2_u3?

The following new features and improvements are available in this release. For important information about upgrading from previous releases to 7.1.2_u3, see Upgrading to 7.1.2.

Early Access (EA) Feature

From time to time, Cohesity may add features and request for feedback on their utility and design. These features are termed as Early Access features. Early access features are limited to a closed group of testers for a limited subset of launches. Participation is by invitation only and may require signing a pre-general-availability agreement, including confidentiality provisions. These features may be unstable, change in backward-incompatible ways, and are not guaranteed to be released. There are no SLAs provided and no technical support obligations. These EA features are by default disabled and hidden and need to be enabled separately. If you wish to use these EA features you need to contact your accounts team, who will internally work within Cohesity to enable the feature on your cluster. Cohesity recommends running these features only on non-production clusters.

Data Protection

Databases

PITR for MongoDB Early Access

MongoDB now supports Point In Time Recovery (PITR) at the protection group level.

> **Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

Kubernetes

Datamover Hostname Verification

In communication with Kubernetes components, hostnames are validated to ensure secure connections and prevent unauthorized access. This validation protects the backup and recovery process by ensuring that only trusted endpoints are utilized.

Physical Servers

Improvements to Physical Server File-based Backup

Cohesity now offers the following improvements for Physical file-based Protection Groups:

- The user interface has been reorganized to simplify the user experience.
- You can download the Inclusion-Exclusion report and the Success logs for file-based Protection Groups on the Cohesity cluster.

Microsoft 365

Granular Recovery of Mailbox Items

Cohesity now supports granular recovery of Exchange Online Mailbox items. With this enhancement, you can now back up and restore specific mailbox items, including:

- Calendar Items
- Tasks
- Contacts
- Notes

Microsoft SQL Server

You can now replay the entire last log backup for a specified point in time without using the STOPAT option for both the Alternate Microsoft SQL Server Instance and the Original Microsoft SQL Server Instance.

Cluster Management

Support Toolbox 3.0 Release

The Support Toolbox 3.0 features a completely redesigned user interface that offers a modern look to improve user experience and performance. This update enables faster interactions, smoother navigation, and enhanced efficiency, simplifying the diagnosis and resolution of cluster issues. As a result, users can achieve greater reliability and streamline troubleshooting workflows.

Monitoring

SNMP OID Improvements Early Access

In previous releases, the SNMP OID for an alert included several properties—such as the alert ID, name, cause, and description—packaged together as a single large string.

Starting with this release, each alert property will have its unique SNMP OID. For example, the diskSpaceLow alert used to have the OID of 1.3.6.1.4.1.47421.0.6, which contained all its properties bundled together.

Now, with the SNMP OID improvement, each property of the diskSpaceLow alert will have its OID:

- 1.3.6.1.4.1.47421.5.1 for the alert ID
- 1.3.6.1.4.1.47421.5.2 for the alert name
- 1.3.6.1.4.1.47421.5.3 for the alert source
- 1.3.6.1.4.1.47421.5.4 for the alert severity
- 1.3.6.1.4.1.47421.5.5 for the alert type
- 1.3.6.1.4.1.47421.5.6 for the alert category
- 1.3.6.1.4.1.47421.5.7 for the alert description
- 1.3.6.1.4.1.47421.5.8 for the alert cause
- 1.3.6.1.4.1.47421.5.9 for the alert help
- 1.3.6.1.4.1.47421.11.2 for the cluster nodeid
- 1.3.6.1.4.1.47421.13.2 for the hardware partition name
- 1.3.6.1.4.1.47421.13.2 for the node IP address

> **Note:**
> - Before enabling the feature, update your SNMP notification configuration with the OID updates.
> - This is an Early Access feature. Contact your Cohesity account team to enable the feature.

New Stream for Syslog Support - Shell Commands Early Access

Cohesity now provides a new Syslog stream, shell_commands_audit, which allows you to send audit logs of shell commands (Host OS only) to your configured Syslog server. This enhancement improves auditing and monitoring capabilities for shell command activities on the Cohesity cluster.

> **Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

Security

DART Tool

Cohesity has now introduced a new Detect and Resolve Tool (DART) to streamline issue detection and resolution on Cohesity platforms. With automated cluster scanning and signature-based detection, DART identifies known issues and offers one-click fixes through a user-friendly interface.

For more information, see DART Knowledge Base article.

What's New in 7.1.2_u2?

The following new feature is available in this release. For important information about upgrading from previous releases to 7.1.2_u2, see Upgrading to 7.1.2.

Cluster Management

Claim Cohesity Clusters Through Tokens

Cohesity now allows you to claim a cluster through a token generated in Helios. Helios validates this token and claims the cluster if it passes all checks. Each account can have up to 32 valid tokens concurrently. Tokens automatically expire after 15 minutes or upon successful claiming. The streamlined process reduces complexity and enhances the user experience. For more information, see Connect Clusters to Helios.

> **Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

Security

Cipher Update

TLS 1.2 ciphers, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA and TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA have been deprecated in this release due to their use of SHA-1. For more information, see cipher.

Cohesity Enhancements

Self-Managed Cohesity Cluster UI Login Update

Starting with the Cohesity 7.1.2_u2 release, the login page for the Cohesity cluster UI will now resemble the Helios UI Login page. This update is part of our ongoing effort to provide a consistent and intuitive experience across all Cohesity products and solutions. By aligning the design of the Self-Managed Cohesity Cluster UI and the Cohesity Helios UI login pages, Cohesity aims to provide a familiar and unified interface across both environments.

How to differentiate the login pages?

Although the login pages for the Self-Managed Cohesity Cluster UI and the Helios UI now share a similar design, here are a few ways to differentiate them:

- **Login Page**: The Cohesity Cluster login page features **Welcome to Cohesity Data Cloud**, indicating that you're accessing the Self-Managed Cohesity Cluster.
- **URL**: The URL provides additional confirmation. The Self-Managed Cohesity Cluster URL displays the IP address or domain of your local cluster, whereas the Helios URL uses the Cohesity Helios web address.
- **Login Credentials**: Use the appropriate credentials for each environment. The Self-Managed Cohesity Cluster UI requires your local cluster credentials, while the Helios UI requires your Cohesity Helios account credentials.

What's New in 7.1.2_u1?

The following new features and improvements are available in this release. For important information about upgrading from previous releases to 7.1.2_u1, see Upgrading to 7.1.2.

Early Access (EA) Feature

From time to time, Cohesity may add features and request for feedback on their utility and design. These features are termed as Early Access features. Early access features are limited to a closed group of testers for a limited subset of launches. Participation is by invitation only and may require signing a pre-general-availability agreement, including confidentiality provisions. These features may be unstable, change in backward-

incompatible ways, and are not guaranteed to be released. There are no SLAs provided and no technical support obligations. These EA features are by default disabled and hidden and need to be enabled separately. If you wish to use these EA features you need to contact your accounts team, who will internally work within Cohesity to enable the feature on your cluster. Cohesity recommends running these features only on non-production clusters.

Data Protection

Cloud Services

WORM Support for Cloud Archive with Periodic Full in Azure Next-Gen Cloud Edition

Azure Next-Gen Cloud Edition (NGCE) now supports Write Once Read Many (WORM) for Cloud Archive with periodic full. The WORM model ensures that the objects written to the WORM-supported targets cannot be tampered (deleted or overwritten). The archives created are immutable for the duration configured.

For the list of external targets with WORM support, see Supported Workflows and External Targets.

SAP HANA

Cohesity SAP HANA Connector Support for SAP HANA Backup Encryption

Cohesity now supports the native SAP HANA backup encryption. When backup encryption is enabled, the backup data is encrypted and transferred to the backup location for backups created using the Cohesity BACKINT plugin for SAP HANA. For more information, see SAP HANA.

Physical Server

Support for Static Port 21213 for Physical Agents Early Access

Cohesity now supports switching to the static port 21213 for physical server sources. See Manage Firewall Ports.

> **Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

Cluster Management

New Utilities in Secure Shell

Cohesity now includes network troubleshooting and quality-of-life utilities in Secure Shell to assist with day-to-day admin activities. These utilities are tcptraceroute, host, dig, mtr, nping, less, and elinks.

> **Note:** The secure shell container image update, which introduced new utilities, was first rolled out in version 6.8.1_u7. With the release of version 7.1.2_u1, the same update has been added to ensure consistent CLI usage across the major releases, further enhancing the user experience.

Multiple Run-now Support

Cohesity now supports triggering multiple runs parallelly for a given job. This function only applies to physical directive file jobs. For more information, see Manage Sources.

Security

Agent Encryption

The encryption algorithm used by Cohesity agents is now reflected within the Pulse log and Agent Summary report.

What's New in 7.1.2?

The following new features and improvements are available in this release. For important information about upgrading from previous releases to 7.1.2, see Upgrading to 7.1.2.

Early Access (EA) Feature

From time to time, Cohesity may add features and request for feedback on their utility and design. These features are termed as Early Access features. Early access features are limited to a closed group of testers for a limited subset of launches. Participation is by invitation only and may require signing a pre-general-availability agreement, including confidentiality provisions. These features may be unstable, change in backward-incompatible ways, and are not guaranteed to be released. There are no SLAs provided and no technical support obligations. These EA features are by default disabled and hidden and need to be enabled separately. If you wish to use these EA features you need to contact your accounts team, who will internally work within Cohesity to enable the feature on your cluster. Cohesity recommends running these features only on non-production clusters.

Data Protection

Databases

IPv6 Support

You can now protect the following databases running in dual-stack (IPv4 and IPv6) mode or single-stack (only IPv6) mode:

- SAP HANA on Linux
- SAP Sybase ASE on Linux
- SAP Sybase IQ on Linux

- SAP MaxDB on Linux
- IBM DB2 on Linux
- PostgreSQL on Linux
- SAP HANA on Linux
- SAP Sybase ASE on Linux
- SAP Sybase IQ on Linux
- SAP MaxDB on Linux
- IBM DB2 on Linux
- PostgreSQL on Linux

Cohesity Oracle SBT Plug-In Restore Visibility for ZDLRA

The Oracle ZDLRA and SBT restore visibility feature allows you to check the reading activities against externally triggered views through the Cohesity SBT plugin. For more information, see Cohesity Oracle SBT Plug-In for ZDLRA.

PITR Backup Run in DR Cohesity Cluster

Cohesity now supports the Point-in-time Recovery (PITR) backup run in the disaster recovery (DR) Cohesity cluster. Enabling the SetPrimary Option in the DR Cohesity cluster will start the backup when failover occurs in the Primary Cohesity cluster. For more information, see PITR Backup run in DR Cohesity. For more information, see Cassandra Point-in-time Recovery (PITR) Backup Run in disaster recovery (DR).

Cleanup Snapshot on Cassandra Primary

Cohesity creates snapshots of the keyspaces that are protected during the Cassandra Data Backup processes. If the backup run is canceled, the snapshots that Cohesity creates on Cassandra Primary will automatically get deleted. For more information, see Backup Cassandra.

Backup and Recover Cassandra System Keyspaces

Cohesity now supports backup and recovery of the following system keyspaces:

- System_auth
- System_schema

For more information, see Backup and Recover Cassandra System Keyspace.

Physical Server

Support for VSS Writers Exclusion on Windows Servers

Cohesity now supports excluding the VSS writers from a selected source for Windows physical block-based backup runs. For more information, see Protect a Physical Server (Block-based). For more information, see Protect a Physical Server (Block-based).

Support for IPv6

You can now protect Windows and Linux physical sources running in dual-stack (IPv4 and IPv6) mode.

Security

Proxy Support for AWS KMS Early Access

You can now configure an HTTPS proxy for new and existing AWS KMS configurations on a Cohesity cluster. For more information, see AWS KMS.

> **Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

SmartFiles

Manage File Aging Policy for NFS and SMB Views Early Access

You can now reduce storage space utilization by managing the file timestamp attributes. You can define criteria for identifying aging files and specify actions to take upon meeting these conditions. By automating the deletion of aged files, storage lifecycle management ensures optimal performance and resource utilization, enabling you to reclaim valuable storage space. For more information, see Storage Lifecycle Management Rules.

> **Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

Cluster Management

Cohesity Host OS Transition to Red Hat Enterprise Linux (RHEL)

Cohesity transitions to Red Hat Enterprise Linux 7.9 OS as the Host Operating System starting from version 6.8.2, replacing CentOS 7.9. This transition is ahead of the end-of-maintenance support for CentOS 7.9, scheduled for June 30, 2024.

Cohesity has Red Hat Enterprise Linux Extended Life Cycle Support (ELS) subscription for RHEL7.9 which can be extended until June 30, 2028.

Cohesity Enhancements

Indexing Service Optimization

The Cohesity indexing service is optimized to automatically identify and delete stale directories at regular intervals, which were created for indexing. After upgrading to a version with this optimization, the cluster indexing service will remove any stale directories identified, which may result in cluster-free space increase.

Cohesity Feature Deprecation

The following features are deprecated from Cohesity release. You can review the following table to check whether you are currently using any features that are deprecated or will be deprecated in the future.

Deprecated Features

Deprecated Feature Name	Description	Last Supported Cohesity Version	Alternative Solutions
Remote Access	The ability to register a remote cluster for remote access is no longer supported.	6.8	NA

Upgrading to 7.1.2

Upgrade Paths

You can upgrade your Cohesity cluster from previous releases to 7.1.2. The following table provides details on supported upgrade paths.

Your Current Release	Upgrade Path to 7.1.2
• 7.1.2_u3 • 7.1.2_u2 • 7.1.2_u1 • 7.1.2 • 7.1.1 • 7.1 • 7.0.1_u1 • 7.0.1 • 7.0_u1 • 7.0 • 6.8.2_u1 • 6.8.2 • 6.8.1_u7 • 6.8.1_u6 • 6.8.1_u5 • 6.8.1_u4 • 6.8.1_u3 • 6.8.1_u2 • 6.8.1_u1 • 6.8.1	7.1.2_u4 directly

> **Note:** Upgrades from version 7.1.2_u4 are only supported to version 7.3 or later. Upgrades to versions such as 7.2.2x are not supported from 7.1.2_u4.

Prerequisites

Prior to upgrading your cluster, Cohesity strongly recommends running the health check for a seamless upgrade experience. For more information, see Support Toolbox Overview.

Release Upgrade Policy

Policy	Example
Cohesity will support upgrades from the latest release of the prior LTS release branch, which includes all LTS designated releases within the branch, to the most recent release of the current LTS branch.	6.6.0d+ (LTS designated releases: 6.6.0d_u3, 6.6.0d_u4, 6.6.0d_u5, 6.6.0d_u6) to 6.8.2 LTS designated release will be supported.
Cohesity will not allow upgrades by default to any release that is older in time irrespective of the release branch. Exceptions are to be managed on a case-by-case basis.	6.5.1f_release-20210825_596bb917 is released after 6.6.0c_release-20210822_0d731348. Therefore, an upgrade from the 6.5.1f version to the 6.6.0c version is not supported. This policy is also applicable to patches. If you have upgraded your Cohesity cluster to a patch released after the LTS release, upgrading to that LTS release is not supported. However, you can upgrade to any LTS version released after the patch. For example, your Cohesity clusters were upgraded to 6.6.0d_u5 in July 2022. Cohesity released 6.8.1_u1 on Nov 2022 and the 6.6.0d-p32 patch on March 2023. If you've applied 6.6.0d-p32, you cannot upgrade to 6.8.1_u1. However, you can upgrade to the upcoming 6.8.1_u2 release.
Cohesity will support the release N-1 upgrade without an intermediate step. (N is defined as the current release branch).	6.8.x to 7.1.2 is supported. 7.1.2 is the current release branch.
Cohesity will support the release N-2 upgrade without an intermediate step. (N is defined as the current release branch).	6.6.0d_u6 to 7.1.2 is supported. 7.1.2 is the current release branch.
When a specific release is declared LTS, Cohesity will support upgrading from the open LTS releases to the new LTS release. This will include the three most recent releases on the LTS branch to the new LTS release.	6.8.1, 6.8.1_u1, 6.8.1_u2, 6.8.1_u3, 6.8.1_u4, 6.8.1_u5, 6.8.1_u6, 6.8.1_u7 to 6.8.2.

Upgrade Considerations

Note the following about upgrading the Cohesity cluster to 7.1.2:

- Cohesity does not support rolling back to older versions.
- To upgrade the Cohesity cluster from a version that is no longer supported, Cohesity recommends you to upgrade to any of the supported versions mentioned in the Upgrade Paths, and then perform an upgrade to the latest release version. For information on Cohesity Products that have reached the end of support, see Cohesity Products End of Support.
- See to review the list of features marked for deprecation for Cohesity 7.1.2 and later releases.
- Before performing the upgrade, ensure that the cluster data space and metadata space utilized is less than 85%. After the cluster upgrade, the Garbage Collection algorithms take 3 to 4 days to trigger. Hence, ensure that the cluster has enough space during this period. Space constraints may lead to backup and replication failures on the Cohesity cluster.
- If you are running remote adapter jobs and the cluster is upgraded, the jobs will be disrupted during the upgrade process. The jobs will be killed and restarted multiple times during the upgrade.
- The Cohesity indexing service is optimized to automatically identify and delete stale directories at regular intervals, which were created for indexing. After upgrading to a version with this optimization, the cluster indexing service will remove any stale directories identified, which may result in cluster-free space increase.
- Cohesity recommends upgrading the Cohesity Agent on Physical Servers and the Cohesity installed Agent on VMs to the latest release version of the Cohesity cluster.
- Cohesity recommends upgrading the Cohesity cluster first, followed by the Cohesity Agent. Upgrading an agent before the cluster is likely to impact the existing functionality and disruptions may be observed due to agent being on a higher version than the cluster. Cohesity also recommends the agents be on the same, latest major version as the Cohesity cluster to get the latest security fixes and benefit from newer features.
- After upgrading to the latest version, if there is an IP subnet conflict, the **Enable Apps Management** toggle in **Marketplace** > **My Apps** is turned off. Navigate to **Settings** > **Summary** > click **Configure** and specify a different IP address in the **Configure Apps management network** field and then turn on the **Enable Apps Management** option.
- If you are on a Cohesity Cloud Edition cluster and using Marketplace Apps, then when you upgrade the Cohesity Cloud Edition cluster to 7.1.2, connectivity among the Marketplace Apps could be impacted* due to Flannel moving to etcd v3 APIs. It is recommended to pause any Marketplace Apps before the upgrade and resume them

once the upgrade is complete.

*__Impact__: Running workloads, Protection Groups, or scans related to the Marketplace App might see network disruption during the upgrade.

- For pure PXG clusters, before upgrading from version 6.6 to 6.8.1 or above, make sure that your cluster usage is below 95%. After the upgrade, there is a known issue where the available data space may decrease. Even clusters that are using only 88% of disk space before the upgrade have experienced out-of-space errors afterward, which can lead to backup failures. To avoid disruptions, Cohesity strongly recommends reducing disk usage well below 95% before starting the upgrade process.

Databases

- The addition of the new Postgres database could cause UI slowness until the ETL process completes. The bootstrap run of the ETL process pulls the entire data set to populate the database. The initial run has a slight performance impact. In the case of upgrades, data population happens in the post-upgrade step. Subsequent upgrades will not be affected.

Administration

- To generate a new SSH key after upgrading the Cluster, contact Cohesity Support.
- Cohesity Support Engineers require a Support Channel token to remotely log into the Cluster using SSH for on-demand assistance. From your Cohesity cluster, you need to copy the Support Channel token and provide it while raising a request for on-demand assistance.
- The Secure Shell restricts access to the host commands or scripts. After you upgrade to 6.7 or later version, the secure shell might have the following impact on your existing Cohesity Data Cloud deployments:
    - Access to the bash shell using SSH will be no longer available to the support user account without authorization from Cohesity.
    - If you run custom scripts using SSH on your Cohesity cluster, the scripts may fail. In this case, Cohesity recommends the following:
        - Verify if there is an alternate method to use Cohesity CLI commands or REST API and update your scripts accordingly.
        - Verify if a corresponding Cohesity CLI command is available in the supported list of CLI commands; if so, use the supported CLI command. If the CLI command is not available in the supported list of commands, contact Cohesity Support to enable the CLI command.
    - The private binary or tools running on the Cohesity nodes might fail. Contact Cohesity Support for options to install private binaries or tools.

    - Sudo access is disabled by default. For support channel access, enable the sudo access. For more information, see Enable or Disable Linux Sudo Access.
- If there is a source that is registered before the upgrade and assigned to an organization, then unassigning its root entity is not allowed. You can unassign the source if it is not assigned to an organization, and it will get assigned after the upgrade.

NoSQL and Hadoop

- To continue using Cohesity NoSQL & Hadoop services on Cohesity cluster version 7.1.2, you must upgrade the NoSQL & Hadoop service to the 7.0.0 version available on Helios.
- If you are running NoSQL and Hadoop app, Cohesity recommends the following before upgrading the Cohesity cluster:
    - Pause the protection runs by navigating to **Data Protection > Protection** . From the Action Menu (⋮) of the required protection run, select **Pause Future Runs**.
    - Pause the NoSQL and Hadoop app by navigating to **Marketplace > My Apps** . From the Action Menu (⋮) of the app instance, select **Pause**.

  After upgrading the Cohesity cluster to the latest version, contact your Cohesity account team to check if the upgraded Cohesity cluster requires a new NoSQL and Hadoop app. If it requires a new version of the app, you must upgrade to the latest version of the NoSQL and Hadoop app. Once the cluster upgrade is complete, resume the app, and then the protection runs.

Microsoft 365

- If you upgrade your Cohesity cluster to 6.8.2 or later versions and currently backing up Microsoft 365, ensure that you add the required Microsoft Graph Permissions related to MS Groups to your custom application to continue using your existing Protection Groups and protect your Microsoft 365 data.
- After upgrading to the 7.1.2 version, if you are replicating the Mailbox data to a remote Cohesity cluster, then ensure that you upgrade the remote Cohesity cluster to the 7.1.2 version.

Single Node Cluster Upgrades

Single node cluster upgrades must be run when the upgrade will have the least impact. During the upgrade of a single node cluster, the node is rebooted and during the reboot, the cluster is unable to process Protection Groups, recover tasks, etc.

Virtual Edition Deployment

The following are the requirements for the Virtual Edition deployment for 6.8 and later versions:

- small (8 TB) configuration supports Virtual Machines with 12 vCPUs, 32 GB of memory, and 64 GB virtual disk to store the operating system.
- large (16 TB) configuration supports Virtual Machines with 24 vCPUs, 64 GB of memory, and 64 GB virtual disk to store the operating system.

For more information, see Virtual Edition for VMware Setup Guide and Virtual Edition for Clustered VMware Setup Guide.

Replication Environments

- If the cluster replication is configured, verify that the network connectivity is functioning properly during the upgrade to ensure the cluster replication relationship is successfully upgraded to use AES-256-GCM for encryption.
- In a replication setup, when you upgrade your Cohesity cluster to Cohesity 6.6 or later and you use the default System Admin password, you will be prompted to change the password. After changing the password, you must update the new password on the replication partner cluster.
- For information about using replication between Cohesity clusters running different versions, see Replication Compatibility.

Cohesity Cluster Patch Upgrades

- Ensure there are no cluster operations or patch updates in progress. A cluster operation is a task on a Cohesity cluster such as add or remove a node, and cluster upgrade.
- When you create a node and connect it to a Cohesity cluster, the service patch updates are done automatically but the Base OS patch is not applied. To apply Base OS patch update on the newly added node, you can refer to the link under the **Instructions** column in the Download portal.

> **Note:** Cohesity recommends that the product patch and the Base OS patch version should be the same.

Patch Upgrades in DoD Mode

In addition to the recommendations mentioned in Cohesity Cluster Patch Upgrades, you should also consider the following points when applying a patch update on a Cohesity cluster that is running on DoD mode.

- If your Cohesity cluster is running on DoD mode, then you should first upgrade to 6.8.1_u2 or later and then apply a cluster patch update. For more information on DoD mode, see Use Cohesity Data Cloud (Self-managed) in DoD Mode.

Supported Sources for Hybrid Extender Based Organizations

From 6.6 onwards, Cohesity Platform in a multi-tenant environment displays only the sources that the Organization (tenant) can register and protect. As a prerequisite, Hybrid

Extender should be enabled for Organizations (tenant).

For a list of supported sources and workflows, see Supported Multitenancy Workflows.

Upgrade Scenarios

- If you upgrade from Cohesity 6.8.2 or later version with the Organizations (multitenancy) feature enabled, you can continue to use the sources that are registered for protection before the upgrade. However, if the Organizations (multitenancy) feature is enabled after the upgrade, you will see only the list of supported sources for tenants. For more details, see Supported Multitenancy Workflows.

Patch Upgrade Instructions

Patches are urgent fixes delivered for maintenance releases. Patches are rolled up cumulatively into the next maintenance release. This topic lists the steps for upgrading the Cohesity Patches and CVE Patch releases.

> **Note:** Product patch upload is not supported via Helios. Login to the cluster for uploading the product patch. Patch apply and viewing the progress via Helios is supported.

Instructions for Applying 7.1.2-p20250722 Patch

Patches are not upgrade images. Upgrade takes the cluster from one release to another release. Whereas applying a patch keeps the cluster on the same release but just replaces some binaries. Please do not use the patch to upgrade a cluster. The following instructions are applicable only for clusters running 7.1.2_u4, 7.1.2_u3, or 7.1.2_u2.

To apply the 7.1.2-p20250722 patch:

1. Download 7.1.2-p20250722 from downloads.cohesity.com under the **Patches** tab.
2. Upload the patch to the cluster.

   You have to log in to the Cohesity cluster as an admin user from Cohesity cluster UI.

   a. Log in to the patch master node, navigate to **Settings** > **Software Update** > **Product Patches** tab.

   b. Click the **Upload Patch File** button at the top right corner to upload the patches.

   c. In the dialog box, select the downloaded patch file. It will take a few minutes to upload the patch to the cluster.
3. **Apply** the patch.

   Once the patch is successfully uploaded, click the **Apply All** button at the top right corner to apply all the service patches.

Note:

- It takes approximately 20 minutes total to apply the patch on the cluster. There is no service disruption during this time.
- Apply hotfixes using the Product Patches tab in the Cohesity cluster UI.

You can now download the Cohesity agent installers for Solaris, HP-UX, and Linux-PPC from the Cohesity UI, in addition to the agent installers available on the Cohesity Package Download page. If both the agent and the Cohesity cluster are at the same release and later versions, then the agents can also be upgraded through the UI. This enhances the existing capability available for Windows, Linux, and AIX agents.

Instructions for Applying 7.1.2-p20250722s1 CVE Patch

Patches are not upgrade images. Upgrade takes the cluster from one release to another release. Whereas applying a patch keeps the cluster on the same release but just replaces some binaries. Please do not use the patch to upgrade a cluster. The following instructions are applicable only for clusters running 7.1.2_u4, 7.1.2_u3, or 7.1.2_u2.

Note: Applying this patch may induce rolling reboots across the nodes of the cluster.

Cohesity CVE patch releases utilize the BaseOS patch within the software bundle to hold the CVE and related security fixes. BaseOS patch may contain critical CVE fixes, kernel updates, driver updates, and optionally bug fixes for other user-mode packages.

This differs from the standard Cohesity patch release which does not include the BaseOS patch.

CVE patch content is cumulative, similar to the regular product patch content. This allows the customer to install the latest patch (CVE or non-CVE) and be brought up to the latest available content.

Follow the steps to install the product patch with security fixes. Review the steps before beginning the installation procedure.

Important:

- Rolling reboots may take more than 15 minutes per node depending on the contents of the patch.
- CVE patch releases cannot be reverted.

Cohesity recommends that you run `hc_cli` tests before applying the BaseOS patch. Use the below command to run the tests as a support user.

> **Note:** Before running the hc_cli commands, you must Enable Host Shell Access. For more information, see Enable Host Shell Access.

```
hc_cli run -c kPreUpgrade
```

To view the test result run

```
hc_cli show --all
```

To apply the security patch, follow the steps listed below:

1. Navigate to **Security Patches** tab.

   You have to login to cluster as an admin user on the cluster UI. After logged in,

   a. Navigate to **Settings** on the left pane. Select **Software Update** and click **Security Patches** tab.

   b. Click **Download Security Patch** button at the top-right corner and in the dialog box, paste the patch file URL from the downloads portal.

   c. If the downloads portal is not accessible from the cluster, host the patch file in a web server that is accessible from the cluster and use the URL of the patch hosted in that server.

2. The downloaded patch gets listed under **Available Patches** section after the download is complete. Click **Apply** button to apply the patch.

> **Note:**
> - Apply the patch from one of the cluster nodes. This will internally apply to all the nodes. Do not apply from multiple nodes simultaneously.
> - It takes approximately 20 minutes total to apply the patch on the cluster. There is no service disruption during this time.
> - A Copy of the console output for the Product patch is stored in `/home/cohesity/data/patches/7.1.2-p20250722s1-00-51497496.out`
> - A copy of the console output for the BaseOS patch is stored in `/home/cohesity/data/patches/baseos-7.1.2_u4_p7-patch-2025Jul23-cdd5517.tgz.out`
> - The BaseOS patch will be automatically applied at the end of a successful Product patch application.
> - Apply hotfixes using the Security Patches tab in the Cohesity cluster UI.

You can now download the Cohesity agent installers for Solaris, HP-UX, and Linux-PPC from the Cohesity UI, in addition to the agent installers available on the Cohesity Package Download page. If both the agent and the Cohesity cluster are at the same release and later versions, then the agents can also be upgraded through the UI. This enhances the existing capability available for Windows, Linux, and AIX agents.

Considerations

Review these considerations before you install the software for the first time or upgrade from a previous version.

Data Protection

Instant Volume Mount

Review the following considerations:

- When recovering a file or instantly mounting a volume from a Windows VM or Physical Server Backup Source that has Windows deduplication installed and enabled for one or more volumes, you must choose a target machine that also has Windows deduplication installed (it does not have to be enabled for any volume). (However, this rule does not apply to Nutanix AHV VMs. If AHV VMs are enabled with Windows deduplication, the only supported recovery option is full VM recovery.)

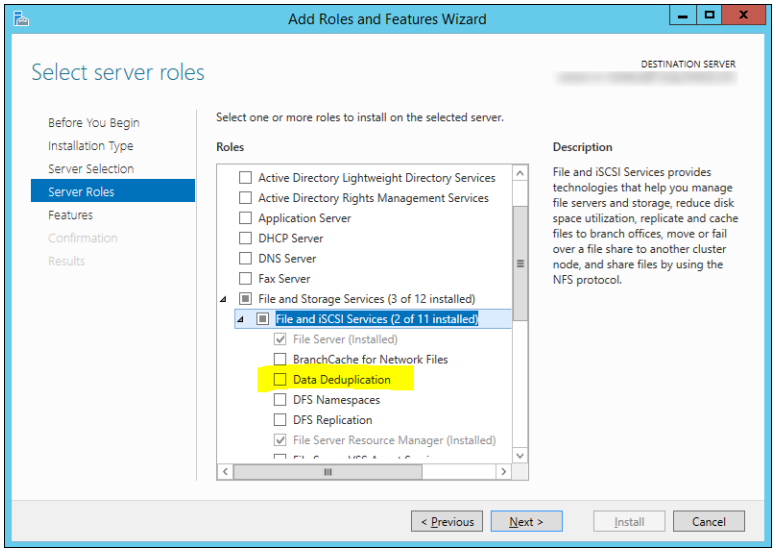
  If the target does not have Windows deduplication installed:

  - File level recovery might fail with robocopy error code 8 (if no file was recovered) or 9 (if some files were recovered and some failed).
  - Instant volume mounting will succeed but you might not be able to browse the volume or access all of its contents.

  To determine if Windows deduplication is installed on the Source or target machine, follow the steps given below:

  1. Open **Server Manager**.
  2. Select **Roles and Features > File and Storage Services > File and iSCSI Services**.
  3. Select the **Data Deduplication** check box, if necessary.

4. Click **Next** until the **Install** button is enabled and then click **Install**.



- Instant Volume Mount (IVM) restore of ReFS volumes backed up using Windows physical block-based jobs cannot be restored to an alternate Windows server running a lower version of ReFS.
- When mounting volumes on a Linux physical Server, the loop devices present on the Server are used for mounting. Therefore, the number of volumes that can be mounted depends on free loop device availability. By default, the number of available loop devices is 8, but this number can be customized. If the number of configured loop devices is the default of 8, up to eight volumes can be mounted. In this example, if an attempt to mount more than 8 volumes occurs, the mounting of all the volumes after the 8th volume fails and errors are reported.
- Tearing down a cloned database or instant volume mount deletes the mounted volumes. Any new or modified data on these volumes will be deleted along with the volumes, so ensure you back up any important data before teardown.
- Review the following considerations when performing instant volume mount to Hyper-V VMs:
    - Only Windows VMs are supported.
    - Dynamic Disks (LDM and LVM) are not supported.
    - The Bring Disks Online option requires the following:
        - VM must be part of Active Directory, the VM and the Hyper-V host must be in the same AD.
        - Users must execute "winrm quickconfig" to enable winrm on the target VM and remote powershell must be enabled from Hyper-V host to VM.
    - Instant volume mount and file level recovery from Gen 1 to Gen 2 type VMs is not supported.

    - If SCVMM is unregistered from the Cohesity cluster, ensure you tear down all instant volume mounts. Not tearing them down can prevent the VM from being backed up when the source is registered with a different Cohesity cluster.
    - Instant volume mounting Hyper-V 2012 R2 VMs without a SCSI controller is not supported. This is because Hyper-V disallows dynamically adding a SCSI controller, which is required to add the virtual disks.
    - On 2012 R2 VMs, if an instant volume mount disk is attached during a Protection Group, that snapshot cannot be application-consistent. If this occurs, the event viewer may contain a VSS-catastrophic error or similar message.
- Instant Volume Mount for NetApp stub file is not supported.
- You cannot instantly mount a volume from a VM to a physical server, and vice-versa.

MongoDB Logical Backup Solution

Review the following consideration:

MongoDB recommends limiting collections to 10,000 per replica set. Customers exceeding this limit may experience degraded backup and recovery performance.

File and Object Services

NFS

Review the following considerations:

- NFS mount names and names of files contained in the mount support ASCII and UTF-8 character codes only.
- When mounting a View, the `-o atime` option for the `mount` command improves the performance marginally. For performance reasons even if you specify the `atime` option, the Cohesity cluster does not record the access time. The `-o noatime` option is always in effect and the Cohesity cluster only records the access time when files are created or modified.
- When data is deleted from a view, it may take up to a day for the disk space to become available again and visible from utilities such as `df`.
- To register an Oracle RAC or a RAC node as physical server, "host" command must be executed on each of the nodes of that RAC.
- Cohesity recommends using a Linux client with kernel version 4.x or higher.
- NFSv4.1 considerations:
    - If you use a single client machine to mount an NFS4.1 view with different node IPs, all mount requests will go to a single node on the Cohesity node and might result in inefficient workload balancing.

    - **Workaround**: If you want to mount a single NFSv4.1 View using different node IPs, Cohesity recommends to use multiple clients for better performance. However, you can use each of these NFS clients to mount Views from different Cohesity clusters.
  - LOCKT operations are not supported.

SMB

Review the following considerations:

- Keeping with the industry standard of change notification for SMB shares, recursive change notifications are not sent due to their effect on process load and network traffic.
- Filenames that contain UTF-16 character codes ranging from U+D800 to U+DFFF are not allowed in Cohesity SMB shares.
- For Linux clients that are members of AD, using "client max protocol = SMB2" in the [global] section of /etc/samba/smb.conf is not supported. Use "client max protocol = SMB3".
- Cohesity SMB shares do not support alternate data streams.
- You can add Cohesity SMB shares as a Microsoft Distributed File System (DFS) target, but note that SmartFiles does not support any additional features or functionalities provided by Microsoft DFS.
- Windows behavior prevents Cohesity SMB shares from being automatically discoverable. Use the `net view` command to probe the cluster explicitly using \\<Cluster-machine-account-name> or \\<Cluster-vip-FQDN> or \\<Cluster-VIP>.

SMB Multichannel

Review the following consideration:

The option to advertise multiple IP addresses on the cluster is not supported.

S3

Review the following considerations:

- You must use one of the following accounts to create an S3 View:
  - A local Cohesity user.
  - An Active Directory user that was explicitly added to the Cohesity cluster and assigned a role. This user does not rely on an AD group for access to the Cohesity cluster.

> **Important:**
> You cannot create an S3 View using one of the following accounts:
>
> - An AD user that has Cohesity cluster access through an Active Directory group only
> - An SSO user
> - A Helios user

- To create a SmartFiles S3 View in a multi-tenant environment, log in to the Cohesity cluster as an Organization user. If you create the S3 View while impersonating an organization, the Service Provider administrator becomes the owner of the S3 View.
- Access Control Lists (ACLs) can be set on a bucket using the AWS CLI.
- You cannot use NFS to mount newly created S3 Views. However, if there are existing S3 Views that were configured to use NFS, you can mount such S3 Views using NFS.
- The maximum number of versions allowed per S3 object is 500,000.
- Cohesity recommends excluding any unsupported header(s) from your requests. By doing so, you can prevent any potential unintended consequences that may arise from using unsupported headers.

Indexing and File Recovery

Review the following considerations:

- The Indexing Helper Service is not supported on a Cohesity cluster that is running on DoD mode. When DoD mode is not enabled, both the proxy and the host machines are available and there is improved resiliency for mounting of volumes. This improved resiliency is lost when the entire dependency is on the host node to perform the volume mounts.
- The Cohesity cluster attempts to index all files and folders to a drive on both Windows and Linux systems. If the Cohesity cluster is unable to find mount point information about files or directories, it indexes and displays these files and directories in the `lvol_N` directory, where `N` is a unique number such as `1`.

  On Windows systems, if the Cohesity cluster finds the mount point information about files and directories, it indexes and displays these files and directories with a drive letter such as `C:`.

  Linux LVM indexing supports the following LVM types only: Linear, Striped, Mirrored, Mirrored + Striped, Thin. On Linux systems, how files and directories are indexed and displayed is dependent on the conditions specified in the following table.

Server Type	Volume Type	

Linux Virtual Machine	Simple Volume	The Cohesity cluster detects mount points for entries in the `/etc/fstab` file with the following formats:
		`UUID=ccd1d599-e68e-4b88-ba9b-6f75b63f1bdc /mnt ext4 auto 0`
		`UUID="ccd1d599-e68e-4b88-ba9b-6f75b63f1bdc" /mnt ext4 auto 0`
		If the Cohesity cluster can detect a mount point, it indexes and displays files and directories in the volume with the mount point that was specified in the `/etc/fstab` file. For these example entries, files and directories are indexed with the `/mnt` mount path, such as `/mnt/example/test.txt`.
		If the Cohesity cluster cannot detect a mount point, the Cohesity cluster indexes the files and directories into a `lvol_N` directory. For example, the `/mnt/example/test.txt` file is indexed as `/lvol_1/example/test.txt`.

Linux Virtual Machine	LVM Volume	The Cohesity cluster detects mount points for entries in the `/etc/fstab` file with the following formats:
		`UUID=ccd1d599-e68e-4b88-ba9b-6f75b63f1bdc /mnt ext4 auto 0`
		`/dev/mapper/VG1-root /mnt ext4 defaults 1 1`
		`/dev/VG1/root /mnt ext4 defaults 1 1`
		If the Cohesity cluster can detect a mount point, it indexes and displays files and directories in the volume with the mount point specified in the `/etc/fstab` file. For these example entries, files and directories are indexed with the `/mnt` mount path, such as `/mnt/example/test.txt`.
		If the Cohesity cluster cannot detect a mount point, the Cohesity cluster indexes the files and directories into a `lvol_N` directory. For example, the `/mnt/example/test.txt` file is indexed as `/lvol_1/example/test.txt`.

Linux Physical	LVM Volume	The Cohesity agent can only return mount data when the volume is mounted on the Linux physical Server. If the volume is mounted, the Cohesity cluster indexes and displays files and directories in the volume with the mount point such as `/mnt/example/test.txt`. If the volume is not mounted, the Cohesity cluster indexes the files and directories into a `lvol_N` directory. For example, the `/mnt/example/test.txt` file is indexed as `/lvol_1/example/test.txt`.

- Cohesity supports recovering files/folders from NTFS (Windows VMs) to Windows VMs, and from Linux VMs to Linux VMs only.
- **Error**: When recovering files or folders, the virtual disks are part of the target VM. These virtual disks are attached as SCSI disks that can be any of the supported adapter types: LSI Logic Parallel, LSI Logic SAS or VMware Paravirtual. During this step, you may encounter the following error: "Disk adapter with required slots - <n> is not available. Try creating a new adapter". Here, <n> is the number of virtual disks that are being attached. This can occur if the VM's disk adapter does not have the required number of slots (one SCSI adapter can support 15 virtual disks).

  Solution:Attempt the operation *after* creating a new SCSI adapter. Additionally, the number of virtual disks where files and folders are being recovered from are limited to 15 at a time. Remove some files (or folders) and retry the recovery.
- For RHEL7, if Open VM Tools is installed instead of VMware Tools, TMPDIR may not point to /tmp. When recovering to location "/tmp/<SOME_DIRECTORY>", files may be recovered to a different location.

  Example: If the recovery location is '/tmp/DIR1', files are recovered to a different location, such as '/tmp/systemd-private-c74aea179e9a43c789a19306d880274f-vmtoolsd.service-9GhOBD/tmp/DIR1'
- When unzipping a zip file that was created by downloading files and folders from an archived Snapshot, if the file or folder name has encoded characters, unzip the zip file using the corresponding encoding. For example if a file name in the zip file has a UTF-8 character, unzip the file using the following command:

  ```
  unzip -O UTF-8 Download-Files_Sep_20_2018_3-17pm_3090.zip
  ```
- For Linux VMs, Cohesity supports file recovery from LVM volumes. One LVM volume can consume more than one loop back device, so Linux VMs may support fewer than 8 volumes when configured with the default number of loop devices.
- When recovering a Linux file, the Cohesity Linux Agent runs the following commands in sudo:
  - mount
  - umount
  - findmnt
  - timeout
  - blkid
  - lsof
  - ls
  - rsync
  - losetup
  - dmsetup

  - lvs
  - vgs
  - lvcreate
  - lvremove
  - lvchange
- For Linux Logical Volume Manager (LVM), if all the disks for a volume group are not found by the Cohesity cluster, the Cohesity cluster will not process that volume group. As a result of that, no volumes of this volume group will be recognized or indexed by the Cohesity cluster.
- Indexing, file recovery and browsing files and folders on VMs are not supported for drives with disk-level encryption (such as BitLocker). On physical Servers, however, these workflows are supported.
- Encrypted VMs are not indexed.
- If a Windows VM includes volumes created from a storage pool (Microsoft Storage spaces), VMDK recovery, IVM, and FLR are not supported.
- Cohesity does not support indexing of Microsoft Storage Spaces.
- File level recovery for VMware ESXi environments does not support RAID-5 volumes on dynamic disks. Simple, striped, spanned and mirrored volumes on dynamic disks are supported.
- A VMware Tools service restart during a Recovery operation may disrupt Recovery. If the VMware Tools service restarts during a Recovery operation, the following error message is returned: The guest operations agent could not be contacted. After multiple retries to contact the guest operations agent, an error message stating that it started the copy but it could not get the status is returned. Go to the recovery location to verify whether the operation succeeded.
- Recovering files to a VM where vMotion is in process is not supported.
- File recovery is not supported for ReFS volumes in these environments: physical, VMware, Hyper-V and AHV.
- Encrypted folders that have been renamed or deleted cannot be recovered.
- Recovering files/folders with names longer than 200 characters may return an error. This is due to Windows behavior when handling files/folders with long names.
- After making system configuration changes to a Windows 8 or Windows 2012 System VM, such as renaming an existing drive letter or adding a new disk, these changes may not immediately take effect due to a Windows registry refresh issue. To force the drive letters to be updated on the VM, reboot the system in the VM. This issue affects how files are indexed by the Cohesity cluster and displayed while browsing the contents of the VM.

- Considerations when recovering to physical servers that run:
  - Windows 2012 or later - None
  - Windows 2008 R2 - Upto 2040 GB. Larger recoveries not supported.

  If the OS does not support your recovery, you must recover to an alternate physical server running Windows 2012 Server or later, or use downloads.
- File-based recovery to Windows VMs does not support hardlinks and alternate data streams.
- Downloading files and folders from tape archive locations is not supported.
- Recovering files and folders from VMs to physical servers and from physical servers to VMs is not supported.
- The downloadable zip file can contain regular files and folders only; symlinks are not supported. When unzipping the downloaded files/folders, use a zip utility that supports the ZIP64 format.
- Recovering files to Linux VMs is not supported in the following cases:
  - When run as a non-root user that does not have sudo access
  - If `ALL=(ALL) NOPASSWD:ALL` is not set for the recover user in the /etc/sudoers file
  - If requiretty is not disabled for the recover user in the /etc/sudoers file

    Recovering to Linux VMs requires requiretty to be disabled for the recover user in the /etc/sudoers file, otherwise recovery will fail. To disable requiretty for a recover userAdd the following line in the /etc/sudoers file, where <USERNAME> is the name of the recover user with sudo access: Defaults:<USERNAME> !requiretty
  - The recovery directory path length is greater than 4096 characters.
  - There is not enough space in /tmp for Cohesity to push linux_agent.

Replication and Archival

Review the following considerations:

- Backups that are taken on the Full (No CBT) schedule are not currently archived by the Cohesity cluster. Other full backups (first Protection Group run, failed CBT) can be archived because they are not initiated by the Full backup schedule.
- In production environments, Cohesity recommends not replicating from one single node Cohesity cluster Virtual Edition to another single node Cohesity cluster Virtual Edition. Cohesity recommends replicating from Cohesity cluster Virtual Editions to Cohesity clusters running directly on hardware.

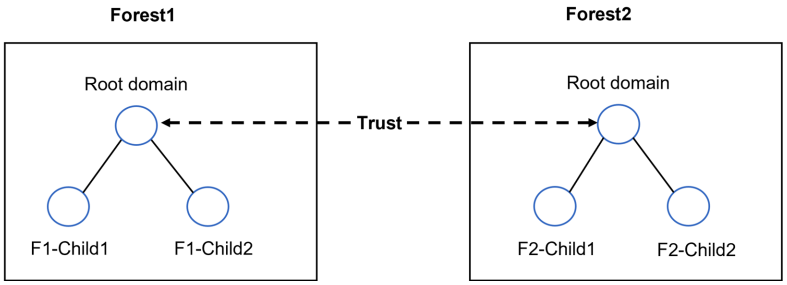
- If you have a Protection Group that is capturing and replicating Snapshots multiple times a day, Cohesity recommends configuring the replication schedule to copy Snapshots daily instead of replicating Snapshots after each protection run. If the replication schedule is too frequent, the replication may lag behind the capturing of Snapshots resulting in a backlog of replication tasks.
- If Snapshots of a VM are replicated to a remote Cluster and the VM is renamed in the vCenter Server, the Cohesity UI on the remote Cluster displays the original VM name in the protection run Details page. However, you can search for new VM name while recovering or cloning and the search results displays the new VM name. Replication is not affected by this issue.

Access Management

Active Directory

Review the following considerations:

- Due to Windows client authentication cache behavior, after you add or remove a Cohesity cluster from an Active Directory domain, clients must log out and log in again to access the Cohesity cluster.
- The Cohesity cluster is added as one or more computer entities with no back-end RPC management API implementation.
- Users from trusted domains with trust type External cannot access Cohesity SMB shares.
- Active Directory lookup to external (non-transitive) trust via LDAP referral setup in AD is not supported.
- Active Directory lookup to a non-Windows-AD trust (Kerberos v5 Realms) is not supported.
- Consider the following trusted domains and forests.



If the cluster is joined to domain F1-Child1, then users from Forest2 or any of its child domains are not authenticated/allowed-access to the cluster. Users from all child domains within Forest1 can authenticate via NTLM.

If the cluster is joined to domain Forest1, then users from all child domains of Forest1 and users from the Forest2 domain only can access the cluster via NTLM. Users from child domains of Forest2 cannot access the cluster via NTLM.

Multitenancy

Review the following considerations:

Organizations (Tenants)

- If a VMware vCloud Director (vCD) source sub-object is assigned to a tenant, the recovery of VMs and vApps to an alternate location will fail in 6.2 release. When an entire vCD is registered within a tenant, then recovery to both original location and alternate location is supported.
- Enabling multitenancy for a cluster cannot not be undone. You cannot revert the cluster to a single tenancy state.
- If a single-tenant cluster is configured with remote access to a multitenant-enabled cluster, the Organizations page will not be available when accessing the multitenant cluster. The workaround is to enable multitenancy on the single tenancy cluster (it is not necessary to add any organizations.)

Hybrid Extender VM

Review the following considerations:

- Hybrid extender supports source registration and backup only for windows and Linux physical sources. AIX, HPUX, Solaris physical sources are not supported with hybrid extender.
- Currently, Cohesity does not support the auto-upgrade of the Hybrid Extender. Therefore, you must upgrade the Hybrid Extender after upgrading the Cohesity cluster from one major release to another major release. For example, if you are upgrading the Cohesity cluster from 6.5.1 to 6.6, use the Hybrid Extender version provided with 6.6.
- When you're upgrading to maintenance releases such as 6.5.1e, you need not upgrade the Hybrid Extender. However, Cohesity recommends that the version of Cohesity cluster and the Hybrid Extender to be same.
- If a tenant deploys multiple Hybrid Extender VMs, SMB and NFS sessions do not failover to the next available Hybrid Extender VM. Cohesity depends on the hypervisor that is hosting the Hybrid Extender VM to ensure high availability. If the hypervisor does not support high availability, I/O requests fail.
- Hybrid Extender does not support the following features:
    - S3
    - SMB Multichannel

- Keystone
- Kerberos client for NFS
- SSO
- NFS authentication

Fixed Issues

The **Fixed Issues** page provides a list of issues fixed in the 7.1.2 release and its associated patch and update releases. Each fixed issue contains an issue ID and a brief description.

On the Fixed Issues page, select one of the following options to view the fixed issues:

- **Filter By Version**—Select a version to filter the fixed issues by a specific version.
- **Search By Issue ID**—Enter an issue ID to search for a specific fixed issue. **Example**: ENG-225665 or 225665.

Security Fixes

Cohesity CVE patch releases utilize the Base OS patch within the software bundle to hold the CVE and related security fixes. BaseOS patch may contain critical CVE fixes, kernel updates, driver updates, and optionally bug fixes for other user-mode packages. Customers can review the fixes and determine if they want to skip a base OS patch and apply just software patches. All patches are cumulative if a patch is skipped and applied using a later patch release.

The following topics list the Common Vulnerabilities and Exposures (CVEs) fixed in the 7.1.2 releases:

- Releases
- Security Patches

Releases

The following table lists the Common Vulnerabilities and Exposures (CVEs) fixed in the 7.1.2 feature and maintenance releases:

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
7.1.2_u4	CVE-2024-24855	RHEL 7: libxslt (RHSA-2025:3612)	High	7.8
	CVE-2025-0624	RHEL 7 : grub2 (RHSA-2025:3396)	High	7.8
	CVE-2025-27363	RHEL 7 : freetype (RHSA-2025:3395)	High	8.1
	CVE-2024-56171	RHEL 7 : libxml2 (RHSA-2025:2673)	High	7.8
	CVE-2025-24928			8.1
	CVE-2024-53197	RHEL 7 : kernel (RHSA-2025:2501)	Medium	5.8
	CVE-2023-52922		High	7.8
	CVE-2024-50302		Medium	6.1
	CVE-2025-0624	RHEL 7 : grub2 (RHSA-2025:2653)	High	7.6
	CVE-2025-1244	RHEL 7 : emacs (RHSA-2025:2130)	High	8.8
	CVE-2024-11187	RHEL 7 : bind (RHSA-2025:1718)	High	7.5
	CVE-2024-6232	RHEL 7: python3 (RHSA-2025:1750)	High	7.5
	CVE-2025-24528	RHEL 7: krb5 (RHSA-2025:1352)	Medium	6.8
	CVE-2020-11023	RHEL 7 : gcc (RHSA-2025:1601)	Medium	6.1

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2024-53104	RHEL7: kernel (RHSA-2025:1281)	High	7.8
	CVE-2024-56326	RHEL7: python-jinja (RHSA-2025:1250)	High	7.8
	CVE-2024-52531	RHEL 7 : libsoup (RHSA-2025:1047)	High	9
	CVE-2024-12085	RHEL 7 : rsync (RHSA-2025:0714)	High	7.5
	CVE-2024-53580	RHEL 7 : iperf3 (RHSA-2025:0402)	High	7.5

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
7.1.2_u3	CVE-2024-37890	Update WS package for address the CVE	High	7.5
	CVE-2024-47537	RHEL 7 : gstreamer1-plugins-base and gstreamer1-plugins-good security update (RHSA-2024:11344)	High	8.4
	CVE-2024-47538			8.8
	CVE-2024-47540			
	CVE-2024-47606			
	CVE-2024-47607		Critical	9.8
	CVE-2024-47613		Medium	6.5
	CVE-2024-47615		Critical	9.8
	CVE-2024-3596	RHEL 7 : krb5 (RHSA-2024:8788)	Critical	9
	CVE-2024-21235	OpenJDK 8 <= 8u422 / 11.0.0 <= 11.0.24 / 17.0.0 <= 17.0.12 / 21.0.0 <= 21.0.4 / 23.0.0 <= 23.0.0 Multiple Vulnerabilities (2024-10-15)	Medium	4.8
	CVE-2024-21210		Low	3.7
	CVE-2024-21217		Low	3.7
	CVE-2024-21208		Low	3.7
	CVE-2024-21235	RHEL 7 : java-1.8.0-openjdk (RHSA-2024:8116)	Medium	4.8
	CVE-2024-21210		Low	3.7
	CVE-2024-21217			
	CVE-2024-21208			
	CVE-2023-48161		High	7.1

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-26604	RHEL 7 : systemd (RHSA-2024:7705)	High	7.1
	CVE-2024-2201	RHEL 7 : kernel (RHSA-2024:6994)	Medium	4.7
	CVE-2024-41071		High	7.8
	CVE-2024-6345	RHEL7 : python-setuptools, python3-setuptools (RHSA-2024:6661, RHSA-2024:6662)	High	8.8
	CVE-2023-31315	RHEL 7 : linux-firmware (RHSA-2024:5978)	High	7.5

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
7.1.2_u2	CVE-2022-1011	RHEL 7 : kernel (RHSA-2024:5259)	High	7.8
	CVE-2024-36971			
	CVE-2024-37370	RHEL 7 : krb5 (RHSA-2024:5076)	High	7.7
	CVE-2024-37371		Medium	6.5
	CVE-2024-21131	RHEL 7 : java-1.8.0-openjdk (RHSA-2024:4560)	Low	3.7
	CVE-2024-21138			
	CVE-2024-21140			4.8
	CVE-2024-21144			3.7
	CVE-2024-21145			4.8
	CVE-2024-21147		High	7.4
	CVE-2024-5564	RHEL 7 : libndp (RHSA-2024:4622)	High	8.1
	CVE-2024-33871	RHEL 7 : ghostscript (RHSA-2024:4549)	High	8.8
	CVE-2022-27635	RHEL 7 : linux-firmware (RHSA-2024:3939)	Medium	6.7
	CVE-2022-46329			
	CVE-2022-40964			
	CVE-2022-36351			6.5
	CVE-2022-38076		High	7.8
	CVE-2024-1737	RHEL 7: Bind (RHSA-2024:5930)	High	7.5
	CVE-2024-1975			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
7.1.2_u1	CVE-2023-4408	RHEL 7 : bind (RHSA-2024:3741)	High	7.5

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-50387			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-50868			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-20592	RHEL 7 : linux-firmware (RHSA-2024:0753)	Medium	5.3
	CVE-2024-32487	RHEL 7: less (RHSA-2024:3669)	High	8.6
	CVE-2024-2961	RHEL 7: glibc (RHSA-2024:3588)	High	8.8
	CVE-2024-33599			7.6
	CVE-2024-33600		Medium	5.3
	CVE-2024-33601		Low	4
	CVE-2024-33602			4
	CVE-2024-31080	RHEL 7: xorg-x11-server (RHSA-2024:1785)	High	7.3
	CVE-2024-31081			
	CVE-2024-31083			7.8
	CVE-2019-14907	RHEL 7 : samba (RHSA-2020:0943)	Medium	6.5
	CVE-2019-10218			
	CVE-2016-2124			5.9
	CVE-2020-25717		High	8.1
	CVE-2021-44142			8.8

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2024-21012	OpenJDK 8 <= 8u402 / 11.0.0 <= 11.0.22 / 17.0.0 <= 17.0.10 / 21.0.0 <= 21.0.2 / 22.0.0 <= 22.0.0 Multiple Vulnerabilities (2024-04-16)	Low	3.7

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2024-21068			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2024-21094			
	CVE-2024-21011			
	CVE-2024-21085			
	CVE-2024-21068	RHEL 7 : java-1.8.0-openjdk (RHSA-2024:1817)	Low	3.7
	CVE-2024-21094			
	CVE-2024-21011			
	CVE-2024-21085			
	CVE-2023-40551	RHEL 7 : shim (RHSA-2024:1959)	Medium	5.1
	CVE-2023-40550			5.5
	CVE-2023-40549			5.5
	CVE-2023-40548		High	7.4
	CVE-2023-40547			8.3
	CVE-2023-40546		Medium	5.5
	CVE-2022-2601	RHEL 7 : grub2 (RHSA-2024:2002)	High	8.6
	CVE-2023-25775		Critical	9.8
	CVE-2020-36558		Medium	5.1
	CVE-2023-2002			6.8
	CVE-2023-4622		High	7
	CVE-2023-4623			7.8

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
7.1.2	CVE-2023-42753	kernel security update (RHSA-2024:0346)	High	7.0
	CVE-2024-20918 CVE-2024-20919 CVE-2024-20921 CVE-2024-20926 CVE-2024-20945 CVE-2024-20952	java-1.8.0-openjdk security and bug fix update (RHSA-2024:0223)	High	7.4
	CVE-2023-6478 CVE-2023-6377	xorg-x11-server security update (RHSA-2024:0009)	High	7.6
	CVE-2023-20569 CVE-2023-20593	linux-firmware security update (RHSA-2023:7513)	Medium	6.5
	CVE-2023-5367	xorg-x11-server security update (RHSA-2023:6802)	High	7.8
	CVE-2022-43552	curl security update (RHSA-2023:7743)	High	5.9
	CVE-2023-40217	python3 security update (RHSA-2023:6823)	High	8.6
	CVE-2023-40217	python security update (RHSA-2023:6885)	High	8.6
	CVE-2023-34058 CVE-2023-34059	open-vm-tools security update (RHSA-2023:7279)	High	7.4

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-3611 CVE-2023-3776 CVE-2023-4128 CVE-2023-4206 CVE-2023-4207 CVE-2023-4208 CVE-2022-40982	kernel security update (RHSA-2023:7424)	High	7.8
	CVE-2023-22067 CVE-2023-22081	java-1.8.0-openjdk security update (RHSA-2023:5761)	Medium	5.3
	CVE-2023-38545 CVE-2023-38546	Libcurl update to 8.4.0 version	Critical	9.8

Security Patches

The following table lists the Common Vulnerabilities and Exposures (CVEs) fixed in the 7.1.2 security patches:

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
7.1.2-p20250722s1	CVE-2024-55549 CVE-2025-24855	RHEL 7: libxslt (RHSA-2025:4098)	High	7.8
	CVE-2025-21587	RHEL 7 : java-1.8.0-openjdk (RHSA-2025:3844)	High	7.4
	CVE-2025-30691			4.8
	CVE-2025-30698			5.6
	CVE-2024-53150	RHEL 7: Kernel (RHSA-2025:3880)	High	7.8
	CVE-2024-55549	RHEL 7: libxslt (RHSA-2025:3612)	High	7.8
	CVE-2025-24855			
	CVE-2025-0624	RHEL 7 : grub2 (RHSA-2025:3396)	High	7.6
	CVE-2025-27363	RHEL 7 : freetype (RHSA-2025:3395)	High	8.1
	CVE-2024-56171	RHEL 7 : libxml2 (RHSA-2025:2673)	High	7.8
	CVE-2025-24928			8.1
	CVE-2024-53197	RHEL 7 : kernel (RHSA-2025:2501)	Medium	5.8
	CVE-2023-52922		High	7.8
	CVE-2024-50302		Medium	6.1
	CVE-2025-0624	RHEL 7 : grub2 (RHSA-2025:2653)	High	7.6
	CVE-2025-1244	RHEL 7 : emacs (RHSA-2025:2130)	High	8.8

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2024-11187	RHEL 7 : bind (RHSA-2025:1718)	High	7.5
	CVE-2024-6232	RHEL 7: python3 (RHSA-2025:1750)	High	7.5
7.1.2-p20250513s1	NA	There are no new security fixes in the **7.1.2-p20250513s1** patch. The **7.1.2-p20250513s1** patch contains all the cumulative fixes until the **7.1.2-p20250306s1** patch.	NA	NA

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
7.1.2-p20250306s1	CVE-2023-50387	RHEL 7 : unbound (RHSA-2024:11003)	High	7.5
	CVE-2023-50868	RHEL 7 : unbound (RHSA-2024:11003)	High	7.5
	CVE-2024-52337	RHEL 7 : tuned (RHSA-2024:10381)	Medium	5.5
	CVE-2024-52530	RHEL 7 : libsoup (RHSA-2024:9654)	High	7.5
	CVE-2025-24528	RHEL 7: krb5 (RHSA-2025:1352)	Medium	6.8
	CVE-2024-53104	RHEL7: kernel (RHSA-2025:1281)	High	7.8
	CVE-2024-56326	RHEL7: python-jinja (RHSA-2025:1250)		
	CVE-2024-52531	RHEL 7 : libsoup (RHSA-2025:1047)		9
	CVE-2024-12085	RHEL 7 : rsync (RHSA-2025:0714)		7.5
	CVE-2024-53580	RHEL 7 : iperf3 (RHSA-2025:0402)		

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
7.1.2-p20240824s1	CVE-2022-27635	RHEL 7 : linux-firmware (RHSA-2024:3939)	Medium	6.7

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2022-46329			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2022-40964			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2022-36351			6.5

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2022-38076		High	7.8

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-4408	RHEL 7 : bind (RHSA-2024:3741)	High	7.5

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-50387			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-50868			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-20592	RHEL 7 : linux-firmware (RHSA-2024:0753)	Medium	5.3
	CVE-2024-32487	RHEL 7: less (RHSA-2024:3669)	High	8.6
	CVE-2024-2961	RHEL 7: glibc (RHSA-2024:3588)	High	8.8
	CVE-2024-33599			7.6
	CVE-2024-33600		Medium	5.3
	CVE-2024-33601		Low	4
	CVE-2024-33602			
	CVE-2024-31080	RHEL 7: xorg-x11-server (RHSA-2024:1785)	High	7.3
	CVE-2024-31081			
	CVE-2024-31083			7.8
	CVE-2019-14907	RHEL 7 : samba (RHSA-2020:0943)	Medium	6.5
	CVE-2019-10218			
	CVE-2016-2124			5.9
	CVE-2020-25717		High	8.1
	CVE-2021-44142			8.8

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2024-21012	OpenJDK 8 <= 8u402 / 11.0.0 <= 11.0.22 / 17.0.0 <= 17.0.10 / 21.0.0 <= 21.0.2 / 22.0.0 <= 22.0.0 Multiple Vulnerabilities (2024-04-16)	Low	3.7

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2024-21068			
	CVE-2024-21094			
	CVE-2024-21011			
	CVE-2024-21085			
	CVE-2024-21068	RHEL 7 : java-1.8.0-openjdk (RHSA-2024:1817)	Low	3.7
	CVE-2024-21094			
	CVE-2024-21011			
	CVE-2024-21085			
	CVE-2023-40551	RHEL 7 : shim (RHSA-2024:1959)	Medium	5.1
	CVE-2023-40550			5.5
	CVE-2023-40549			
	CVE-2023-40548		High	7.4
	CVE-2023-40547			8.3
	CVE-2023-40546		Medium	5.5
	CVE-2022-2601	RHEL 7 : grub2 (RHSA-2024:2002)	High	8.6
	CVE-2023-25775	RHEL 7 : kernel (RHSA-2024:2004)	Critical	9.8
	CVE-2020-36558		Medium	5.1
	CVE-2023-2002			6.8
	CVE-2023-4622		High	7
	CVE-2023-4623			7.8

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 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, 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

Cohesity products may contain or be distributed with third-party software, the use of which may be subject to the following third-party terms and conditions: HPE End User License Agreement – Enterprise Version.

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.

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. Click here to send us your feedback!

Ensure that you provide the following details in your email:

- Document name
- Topic name
- Page number