COHESITY

Release Notes

Version 7.2.2

August 19, 2025

Published on August 19, 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 7.2.2 provides new features and enhancements available for on-premises hardware, Cloud Edition, and Virtual Edition clusters. For more information, see What's New in 7.2.2?.

For more information on upgrading from previous releases to 7.2.2, see Upgrading to 7.2.2.

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

This section provides the following What's New information:

- What's New in 7.2.2_u2?
- What's New in 7.2.2_u1?
- What's New in 7.2.2?

What's New in 7.2.2_u2?

The following new features and improvements are available in this release. For important information about upgrading from previous releases to 7.2.2_u2, see Upgrading to 7.2.2.

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.

Controlled Availability (CA) Feature

A production-quality Cohesity product or feature made available to a limited set of customers. Contact your Cohesity account team to participate.

Data Protection

Kubernetes

Backup and Recovery of Selected VMs for Red Hat OpenShift Virtualization

Cohesity supports granular backup and recovery of selected VMs for Red Hat OpenShift Virtualization present in the Kubernetes namespaces. Instead of backing up or recovering the entire Kubernetes namespace, you can selectively back up and restore specific VMs or groups of VMs within the namespace.

Block Type Volume Mode Support for Red Hat OpenShift Virtualization

Cohesity now supports the backup and recovery of PersistentVolumeClaims (PVCs), with the Volume mode set to Block for Red Hat OpenShift Virtualization.

OpenShift API for Data Protection (OADP) Operator Support for Red Hat OpenShift Virtualization

Cohesity now supports the OpenShift API for Data Protection (OADP) operator, a Red Hat solution that simplifies the registration and maintenance of Velero and Plugin versions.

Manage the use of CSI Driver Snapshots for Backing Up Kubernetes Namespaces

You can now enable or disable the use of CSI drivers to leverage volume snapshots during Kubernetes backups.

Virtualization

Protection of Nutanix AHV Resources Using Prism Central

Cohesity now supports the registration of Prism Central instances to centrally manage Nutanix AHV resources. This simplifies data backup and recovery across multiple Nutanix clusters.

NAS

Support for NFSv4.1 Kerberos Authentication on NetApp and Generic NAS Early Access

Cohesity now supports NFSv4.1 Kerberos authentication on NetApp and Generic NAS when registering NAS volumes.

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

Databases

MongoDB via Ops Manager

The Cohesity MongoDB Integrated Solution integrates with MongoDB Ops Manager to provide full backup, incremental backup, and recovery for MongoDB deployments.

Cohesity SAP HANA Connector Support for SAP HANA Backup Encryption

Cohesity now supports native SAP HANA backup encryption. When encryption is enabled, backup data is encrypted and transferred to the Cohesity cluster for backups created using the Cohesity SAP HANA Connector Agent.

Supported encryption methods include:

- SAP HANA Backup Encryption
- System PKI SSFS
- Data and Log Volume Encryption

> **Note:**
> - Backup, data, and log encryption are currently qualified only with instance SSFS. LSS is not supported in this release.
> - No additional configuration is required on the Cohesity cluster. Encryption must be enabled and managed within the SAP HANA system.

S3-Compatible Storage

Support for S3-Compatible Storage Protection Early Access

Cohesity now supports the backup and recovery of S3-Compatible Storage Protection.

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

External Targets

Incremental Forever Archival Support for S3 Intelligent-Tiering

On Physical, Virtual, and Cloud Edition Clusters:

You can now register Amazon S3 Intelligent-Tiering as an external target with Incremental Forever as the archival format for the following use cases:

- Archiving data as a secondary copy (CloudArchive).
- Directly archiving data as a primary copy (CloudArchive Direct).

On NGCE Clusters:

You can now register Amazon S3 Intelligent-Tiering as an external target with Incremental Forever for the following use cases:

- Associating with the cluster's storage domain to store backed-up data as the primary copy.
- Archiving data as the secondary copy (CloudArchive).

Cloud Edition and Next-Gen Cloud Edition Clusters

Object Lock Support for GCP NGCE External Target Early Access

On GCP NGCE clusters, you can now enable Object Lock for GCP Cloud Storage buckets when registering them as external targets. A GCP external target with Object Lock enabled can be:

- Used as the main backup location by associating with the Storage Domain (primary copy).
- Used for archiving (secondary copy).

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

Enhanced Storage Insights on NGCE Dashboard

The NGCE cluster dashboard has been enhanced to provide more accurate and comprehensive visibility into total storage usage, including both local disk and cloud-based external storage targets.

With this enhancement, you can now:

- View total data stored across local and cloud storage targets.
- Analyze cloud logical data, actual storage consumed, and data reduction ratios.
- Gain accurate insights through the Storage Dashboard and Storage Domain List views.
- Toggle between cloud-only and local-only metrics for focused analysis.

This improvement helps you plan more effectively, optimize storage usage, and monitor NGCE storage footprints holistically.

Support for Amazon Simple Storage Service (S3) Bucket Protection Controlled Availability

You can now perform the backup and recovery of Amazon S3 Bucket on the AWS NGCE cluster.

> **Note:** This is a Controlled Availability feature. Contact your Cohesity account team to enable the feature.

Security

FortKnox Self-Managed Controlled Availability

Cohesity introduces FortKnox Self-Managed, an air-gapped data isolation solution that allows you to vault the backup data to a securely isolated Cohesity cluster within your infrastructure using a pull-based model. It provides WORM (Write Once, Read Many) storage and air-gapped protection to ensure data immutability, security, and compliance.

> **Note:** FortKnox Self-Managed license is required to enable this feature.

> **Note:** This is a Controlled Availability feature. Contact your Cohesity account team to enable the feature.

What's New in 7.2.2_u1?

The following new features and improvements are available in this release. For important information about upgrading from previous releases to 7.2.2_u1, see Upgrading to 7.2.2.

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

Physical Servers

New push model for Cohesity Agent Upgrades

Cohesity agent upgrades will now use gRPC over agent ports, allowing Cohesity clusters to push updates directly instead of relying on agents using the traditional HTTP/HTTPS pull method. This approach makes Cohesity agent upgrades better suited for heavily firewalled or regulated environments that enforce strict egress network traffic controls.

> **Note:** Both cluster and agent must be running version 7.2.2 or later. The new push model applies only to upgrades beyond the 7.2.2 version. Older agents will continue to use the pull method.

NAS

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.

Support for Automatic Denylisting in NAS Sources Early Access

Cohesity now supports implementation of automatic denylisting of IP addresses associated with a NAS source, ensuring smoother backup operations.

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

Support for Extended Attributes using SMB2 Protocol on NetApp ONTAP 9.15.1 Early Access

Cohesity's NAS Data Protection now supports the restore of extended attributes of entities using the SMB2 protocol on NetApp. You can now preserve and restore the file content along with any associated extended attributes, which are metadata that provide additional information about the file.

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

Databases

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.

Support for Log Backups and Point-in-Time Recovery (PITR) for MySQL EE Early Access

Cohesity now supports log backups for MySQL Enterprise Edition (EE) databases, enabling continuous data protection. In addition, Point-in-Time Recovery (PITR) is now supported, allowing you to restore MySQL EE databases to a specific point in time within the backup window.

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

Cloud VM

Recover Azure Unmanaged Disk to Managed Disk

With Azure deprecating support for unmanaged disks, Cohesity now recovers unmanaged disks as managed disks by default.

Virtualization

Support for HPE Alletra MP Storage Array with VMware Backups Early Access

Cohesity now supports using storage array snapshots for VMware backups with the HPE Alletra MP storage array. This integration allows Cohesity to leverage the native snapshot capabilities of the storage array, resulting in more efficient and reliable backups of VMware VMs.

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

Security

Replication

Enhanced Replication Security with TLS Encryption

Replication traffic is now encrypted using Transport Layer Security (TLS) instead of Advanced Encryption Standard (AES), when both the local Cohesity cluster and the remote Cohesity cluster support TLS. TLS-based replication uses ports 23335 and 23336. Ensure these ports are allowed through the firewall if traffic is being blocked. However, if either of the clusters does not support TLS, replication traffic will continue to be encrypted using AES.

> **Note:**
>
> - Ensure to use TLS encryption while pairing clusters only if both the source and target clusters are on 7.2.2_u1 or a higher version.
> - Ensure that the encryption mode is the same on the source and target clusters while pairing.
> - Replication may fail if the source cluster uses AES and the target cluster uses TLS and vice-versa.

Cluster Management

Cluster-Level Encryption Enabled by Default for New Clusters

Cluster-level encryption is now enabled by default when creating a new cluster. Cohesity recommends encrypting data whenever feasible, but administrators can opt out during cluster setup if needed.

Cohesity Host Operating System Update

Cohesity transitions to Red Hat Enterprise Linux 9.4 OS as the Host Operating System starting from version 7.2.2_u1, replacing RHEL 9.2.

What's New in 7.2.2?

The following new features and improvements are available in this release. For important information about upgrading from previous releases to 7.2.2, see Upgrading to 7.2.2.

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 for SAP ASE Databases on Windows

Cohesity now supports the backup and recovery of SAP Sybase ASE databases running on dual-stack (IPv4 and IPv6) mode, single-stack (only IPv6) mode, and single-stack (only IPv4) mode.

IPv6 Support for Cohesity Oracle Databases

Cohesity now supports the backup and recovery of Oracle for Linux and Windows running in dual-stack (IPv4 and IPv6) mode.

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.

Data Guard role-based backup for Oracle Databases

Previously, Cohesity allowed customers to specify a preference only to back up an Oracle Data Guard Database when its Data Guard Role was a Standby. Cohesity has extended this capability now to allow customers to specify a preference to only back up when the Data Guard Role is primary.

Oracle Pluggable Database (PDB) Alternate Restore with Transparent Data Encryption (TDE)

Previously, Cohesity supported data protection of Oracle Container Databases (CDBs) and Oracle Pluggable Databases (PDBs). However, there was a limitation that we did not automate PDB alternate restores when the Oracle CDB database had Transparent Data Encryption (TDE) enabled.

Cohesity now supports alternate restores of Oracle Pluggable Databases (PDBs) when the Oracle CDB database has Transparent Data Encryption (TDE) enabled. This provides the full spectrum of backup and restore operations for CDBs and PDBs.

Enhanced Oracle source registration

Cohesity now supports registering Oracle RAC/AP Clusters through an optional endpoint accessible from the Cohesity cluster. This endpoint can be the IP/FQDN/shortname of any of

the nodes in the Oracle cluster.

Physical Servers

New push model for Cohesity Agent Upgrades

Cohesity agent upgrades will now use gRPC over agent ports, allowing Cohesity clusters to push updates directly instead of relying on agents using the traditional HTTP/HTTPS pull method. This approach makes Cohesity agent upgrades better suited for heavily firewalled or regulated environments that enforce strict egress network traffic controls.

> **Note:** Both cluster and agent must be running version 7.2.2 or later. The new push model applies only to upgrades beyond the 7.2.2 version. Older agents will continue to use the pull method.

SAN

Multi-volume Snapshot Protection Support for Pure Protection Groups

Cohesity now supports the backup and recovery of a Pure Protection Group (multi-volume consistency group).

Cloud VMs

Protect AWS EC2 with UEFI-preferred Boot Mode

Cohesity now supports the backup and recovery of AWS EC2 instances with UEFI-preferred boot mode.

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.

Virtualization

Support for Environment Variables

Cohesity now supports improved snapshot management using Pre/Post script operations through **kStorageArraySnapshot**, which can be used with the COHESITY_BACKUP_TYPE variable in these scripts.

Overwrite Existing VM for Hyper-V

Cohesity now allows you to choose how to handle the original VM when recovering it to the original location for Hyper-V VMs by using the option to overwrite the existing VM.

Kubernetes

Configuring User-defined Priority Class, Labels, and Annotations for Cohesity Deployed Resources Early Access

Cohesity allows you to specify priority class names for pods deployed by it. You also have the option to select labels and annotations that will be applied to the pods and services deployed by Cohesity.

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

Include or Exclude Resource types from the Kubernetes Namespace Early Access

During the backup of Kubernetes Namespace, you now have the flexibility to include or exclude resource types within Kubernetes Namespace using the **Enable Resource Inclusion/Exclusion** option. You can back up only PVCs without capturing entire pods or other Kubernetes resources.

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

Support for Protection of Red Hat OpenShift Virtualization

Cohesity now supports the protection of VMs running on Red Hat OpenShift Virtualization.

Monitoring

Syslog Message Length Improvements

In previous releases, Syslog messages were limited to a maximum length of 1K, resulting in truncation of longer messages. With this enhancement, the truncation limit has been removed, allowing Syslog messages to be transmitted in their entirety without being shortened.

External Targets

Optimize Storage or Network Usage with S3-compatible and NAS External Targets

When registering S3-compatible and NAS external targets with Incremental Forever archival, you can now choose to optimize either the archive storage consumption or network bandwidth utilization.

SmartFiles

Upgrade S3 Views to the Object ID Object Key Pattern

You can now upgrade an S3 View to the Object ID object key pattern. Cohesity recommends using Object ID as the object key pattern to obtain better performance and scalability for

the following operations:

- PutObject
- ListObjects
- ListObjectVersions

Cluster Management

Cohesity Host OS Transition to Red Hat Enterprise Linux (RHEL 9.2)

Starting with this release, Cohesity will transition to Red Hat Enterprise Linux 9.2 OS as the Host Operating System, replacing RHEL 7.9.

Software Update Early Access

Cohesity has revamped the UI to improve the user experience for managing software upgrades and patching within your cluster. You can now track the progress of upgrades and patches in real-time, monitor the status of each node, track completion times, and address any issues that arise during the process. Additionally, the Cohesity patch package format has changed to .img extension instead of .tar.gz.

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

Security

Cluster-Level Encryption Enabled by Default for New Clusters

Cluster-level encryption is now enabled by default when creating a new cluster. Cohesity recommends encrypting data whenever feasible, but administrators can opt out during cluster setup if needed.

CE and Next-Gen Cloud Edition Clusters

Object Lock for AWS NGCE Cluster

The AWS Next-Gen Cloud Edition (NGCE) cluster now supports enabling Object Lock on the AWS object storage (S3 bucket) where protected data will be down-tiered. Object Lock ensures that the down-tiered data remains immutable, preventing any deletion or overwriting.

Object Lock for Azure NGCE Cluster

The Azure Next-Gen Cloud Edition (NGCE) cluster now supports enabling Object Lock on the Azure data storage (Azure Hot Blob Storage) where protected data will be down-tiered. Object Lock ensures that the down-tiered data remains immutable, preventing any deletion or overwriting.

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.

Hardware Platforms

New Hardware Configurations

Cohesity supports the following new configurations on the Cohesity cluster:

Model Number	Capacity Per Node (TB)	Disk/SSD Size (TB)	Category	Form Factor
C5204	12	1.6	General Purpose Node	2U4N
C5208S	24	1.6	General Purpose Node	2U4N
C5212S	36	1.6	General Purpose Node	2U4N
C5218	54	3.2	General Purpose Node	2U4N
CNG3 Compute Node	NA	NA	General Purpose Compute Node	2U4N

Model Number	Capacity Per Node (TB)	Disk/SSD Size (TB)	Category	Form Factor
HPE DL380 Gen11	48	4	General Purpose Node	2U1N
	96	8		
	144	12		

Model Number	Capacity Per Node (TB)	Disk/SSD Size (TB)	Category	Form Factor
Cisco UCS C240 M6 All-Flash	184	7.68	Performance Node	2U1N
	368	15.36		

Model Number	Capacity Per Node (TB)	Disk/SSD Size (TB)	Category	Form Factor
HPE DL345 Gen11	48	4	General Purpose Node	2U1N
	96	8		
	192	16		

Model Number	Capacity Per Node (TB)	Disk/SSD Size (TB)	Category	Form Factor
Cisco UCS C220 M7 All-Flash	76	7.6	Performance Node	1U1N
	153	15.3		

Model Number	Capacity Per Node (TB)	Disk/SSD Size (TB)	Category	Form Factor
Cisco UCS C225 M8 All-Flash	38	3.8	Performance Node	1U1N
	76	7.6		
	153	15.3		

Model Number	Capacity Per Node (TB)	Disk/SSD Size (TB)	Category	Form Factor
Cisco UCS X-Series M7	91	15.3	Performance Node	7U

Model Number	Capacity Per Node (TB)	Disk/SSD Size (TB)	Category	Form Factor
Supermicro ASG-1115S-NE316R All-Flash	122.8	7.68	Performance Node	1U
	245.7	15.36		

Model Number	Capacity Per Node (TB)	Disk/SSD Size (TB)	Category	Form Factor
Lenovo ThinkSystem SR665 v3 All-Flash	153	7.68	Performance Node	2U

Cohesity Feature Deprecation

This topic outlines the features that are deprecated in Cohesity 7.2.2 release or scheduled for deprecation in upcoming Cohesity releases.

Review the following table to determine if you are using any features that are currently deprecated or will be deprecated in the future.

Feature Name	Description	Status	Alternative Solutions
Data Movement	The Lifecycle Management (LCM) feature in Cohesity Protection Policy used to support data down-tiering on external targets. This feature moves data from AWS Standard Storage Tier to AWS Archive Storage Tier after a configured time period.	To be deprecated in the 7.2.2_u2 release.	**For new archives**: Directly archive data to AWS Archive Storage Tier by registering it as the external target. **For existing archives**: New archives will remain in the hot tier. Existing data that has already been down-tiered will stay in the cold tier until it expires.
Remote Access	The ability to register a remote cluster for remote access is no longer supported.	Deprecated in 7.1.2_u3 release	Not Available

Upgrading to 7.2.2

Upgrade Paths

You can upgrade your Cohesity cluster from previous releases to 7.2.2. The following table provides details on supported upgrade paths.

Your Current Release	Upgrade Path to 7.2.2
• 7.2.2_u1 • 7.2.2 • 7.2.1 • 7.2 • 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 with 6.8.2_u1_p3 applied • 6.8.1_u5 • 6.8.1_u4 • 6.8.1_u3 • 6.8.1_u2 • 6.8.1_u1 • 6.8.1	7.2.2_u2 directly

> **Note:** Upgrade from 7.1.2_u4 to 7.2.2x is not supported.

> **Note:**
> For upgrading clusters from 6.8.1_u6 or 6.8.1_u7 to version 7.2.2, follow these upgrade paths:
>
> - 6.8.1_u6 > 6.8.2_u1 > 6.8.2_u1_p3 > 7.2.2
> - 6.8.1_u7 > 6.8.1-p16 > 6.8.2_u1 > 6.8.2_u1_p3 > 7.2.2

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).	7.1.x to 7.2.2 is supported. 7.2.2 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).	6.8.1x to 7.2.2 is supported. 7.2.2 is the current release branch.

Policy	Example
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 7.2.2:

- 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 7.2.2 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.
- Starting 6.8.2 and 7.1.2, the Cohesity indexing service is optimized to automatically identify and delete stale directories at regular intervals, which were created for indexing. After upgrading from a version without 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 7.2.2, 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.
- If you have archived or plan to archive your data with "incremental forever" as the archival format to a bucket with versioning enabled, Cohesity recommends you skip upgrading your Cohesity cluster to 7.2.2 and wait until the upcoming Cohesity release or a subsequent patch for 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.
- Cohesity DataHawk Threat or Data Classification scans may fail after upgrading from 7.1.2_u3 to 7.2.2_u2. Contact Cohesity Support for assistance.

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.
- After upgrading to the latest version, to display SAP HANA log backups in the Cohesity cluster, you need to modify the existing registered source and set the `et-log-backup` source registration parameter to `true`. Only the log backups triggered after enabling `et-log-backup` will be shown on the Cohesity cluster.

> **Note:** After modifying the source configuration (with `-et-log-backup=true`), a full backup is mandatory. The initial full backup must be completed before any log backups appear on the Cohesity user interface.

- If you are upgrading to version 7.2.2 or later, you need to update the existing SAP HANA source configuration to enable auto-discovery and entity hierarchy. Set the `--entity-hierarchy` source registration parameter to "`true`." After updating the source configuration (with `--entity-hierarchy=true`), a full backup is mandatory.
- For **SQL log backups**, if you are upgrading the cluster to version 7.2 and above, ensure that the Cohesity cluster bridge node VIPs on port 11117 are reachable from the SQL source. In case of the multitenant environment, ensure that the Hybrid Extender IPs on port 11117 are reachable from the SQL Source.

> **Note:** The SQL log backup will fail post-upgrade if the above-mentioned port requirement is not satisfied.

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 the Cohesity cluster version 7.2.2, 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 7.2.2 version, if you are replicating the Mailbox data to a remote Cohesity cluster, then ensure that you upgrade the remote Cohesity cluster to the 7.2.2 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, or any other workflow.

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

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 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.

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.)

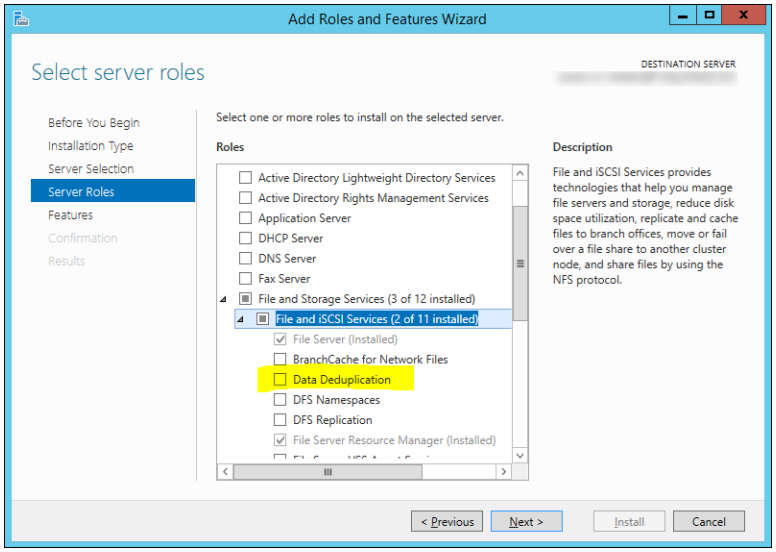
  If the target does not have Windows deduplication installed:

  - 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.

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 is 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.

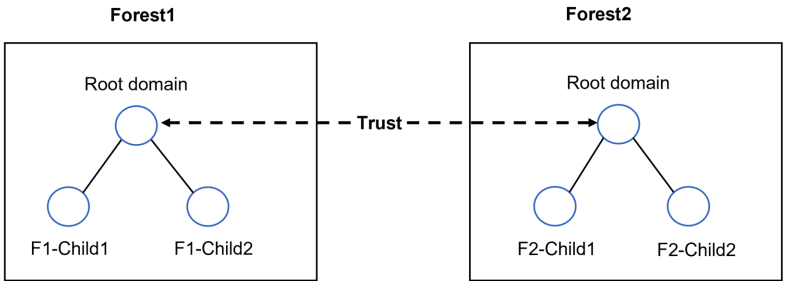
- If you have a Protection Group that is capturing and replicating Snapshots multiple times a day, Cohesity recommends configuring the replication schedule to copy Snapshots daily instead of replicating Snapshots after each protection run. If the replication schedule is too frequent, the replication 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

Security

Review the following consideration:

FortKnox Self-Managed

Enabling FortKnox Self-Managed after upgrading the existing Cohesity clusters to 7.2.2_u2 may lead to vaulting failures. To prevent this issue, apply hotfix 7.2.2_u2_hf1 before enabling FortKnox Self-Managed on upgraded clusters. For new cluster deployments in 7.2.2_u2, FortKnox Self-Managed can be enabled without the hotfix.

Fixed Issues

The **Fixed Issues** page provides a list of issues fixed in the 7.2.2 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 table lists the Common Vulnerabilities and Exposures (CVEs) fixed in the 7.2.2 release:

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
7.2.2_u2	CVE-2025-2784	libsoup (RHSA-2025:8139)	High	7.0
	CVE-2025-4948			7.5
	CVE-2025-32049			
	CVE-2025-32914			
	CVE-2024-52005	git (RHSA-2025:7640)	High	7.5
	CVE-2024-53920	emacs (RHSA-2025:4793)	High	7.8
	CVE-2024-12133	libtasn1 (RHSA-2025:8021)	Medium	5.3
	CVE-2024-12243	gnutls (RHSA-2025:8020)	Medium	5.3
	CVE-2025-0395	glibc (RHSA-2025:4244)	Medium	5.5
	CVE-2025-0938	python3.9 (RHSA-2025:6977)	Medium	6.8

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
7.2.2_u1	CVE-2024-5535	openssl	Medium	5.9
	CVE-2024-55549	libxslt	High	7.8
	CVE-2025-24855			
	CVE-2024-11614	openvswitch3.1	High	7.4
	CVE-2025-27363	freetype	High	8.1
	CVE-2025-21587	java-1.8.0-openjdk	High	7.4
	CVE-2025-30691		Medium	4.8
	CVE-2025-30698			5.6
	CVE-2024-2236	libgcrypt	Medium	5.9

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
7.2.2	CVE-2023-27534	RHEL 9 : curl (RHSA-2023:6679)	High	8.8

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-27533			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-27538			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-27536			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-44487	RHEL 9 : nghttp2 (RHSA-2023:6746)	High	7.5
	CVE-2023-31130	RHEL 9 : c-ares (RHSA-2023:6635)	High	8.6
	CVE-2023-31124			
	CVE-2023-31147			
	CVE-2022-4904			
	CVE-2023-38559	RHEL 9 : ghostscript (RHSA-2023:6544)	Critical	9.8
	CVE-2023-28879			9.8
	CVE-2023-43115		High	8.8
	CVE-2023-2680	RHEL 9 : qemu-kvm (RHSA-2023:6368)	High	8.2
	CVE-2023-39975	RHEL 9 : krb5 (RHSA-2023:6699)	High	8.8
	CVE-2023-36054		High	8.8
	CVE-2007-4559	RHEL 9 : python-pip (RHSA-2023:6694)	Critical	9.8
	CVE-2023-29499	RHEL 9 : glib2 (RHSA-2023:6631)	High	7.5
	CVE-2023-32665			
	CVE-2023-32611			
	CVE-2021-43618	RHEL 9 : gmp (RHSA-2023:6661)	High	7.5
	CVE-2023-34241	RHEL 9 : cups (RHSA-2023:6596)	High	7.1
	CVE-2023-32324			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-38546	RHEL 9 : curl (RHSA-2023:6745)	Critical	9.8

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-38545			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2007-4559	RHEL 9 : python3.9 (RHSA-2023:6659)	Critical	9.8
	CVE-2023-33204	RHEL 9 : sysstat (RHSA-2023:6569)	High	7.8
	CVE-2023-43804	RHEL 9 : python-urllib3 (RHSA-2024:0464)		8.1
	CVE-2023-45803			
	CVE-2022-48624	RHEL 9 : less (RHSA-2024:1692)	Critical	9.8

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2022-3523	RHEL 9 : kernel (RHSA-2023:6583)	High	8.2

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2022-42895			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2022-3565			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-1073			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-1855			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-26545			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-33203			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-1076			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-3358			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-35825			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-1075			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-30456			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-2269			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-1652			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-3772			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-1079			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-3212			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-3773			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-3161			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-4273			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-3141			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2022-3594			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-4194			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-1206			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-1249			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-1989			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-3268			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-4155			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2021-47515			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-5345	RHEL 9 : kernel (RHSA-2023:7749)	High	7.8
	CVE-2023-5088	RHEL 9 : qemu-kvm (RHSA-2024:2135)	High	7
	CVE-2023-6683			
	CVE-2023-3019			
	CVE-2023-42467			
	CVE-2023-3255			
	CVE-2024-25580	RHEL 9 : qt5-qtbase (RHSA-2024:2276)	Critical	9.8
	CVE-2023-51714			
	CVE-2023-37328	RHEL 9 : gstreamer1-plugins-base (RHSA-2024:2302)	High	8.8
	CVE-2022-33065	RHEL 9 : libsndfile (RHSA-2024:2184)	High	7.8
	CVE-2021-41072	RHEL 9 : squashfs-tools (RHSA-2024:2396)	High	8.1
	CVE-2021-40153			
	CVE-2023-43786	RHEL 9 : libX11 (RHSA-2024:2145)	High	7.8
	CVE-2023-43785			
	CVE-2023-43787			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-4692	RHEL 9 : grub2 (RHSA-2024:2456)	High	7.8

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-4693			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2024-1048			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-25193	RHEL 9 : harfbuzz (RHSA-2024:2410)	High	7.5
	CVE-2021-29390	RHEL 9 : libjpeg-turbo (RHSA-2024:2295)	High	7.1

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2024-0841	RHEL 9 : kernel (RHSA-2024:2394)	Critical	9.8

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2024-26593			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-25775			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-52620			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-6622			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2020-26555			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-6176			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-39189			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2022-45934			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-52581			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-52580			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-52610			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-52574			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-46862			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-6531			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-6121			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-6040			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-37453			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-39198			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-39194			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-39193			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-28866			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-24023			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-28464			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-52529			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2024-26609			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-31083			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2022-48947			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-45863			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-42754			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-42756			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2024-26633			

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
	CVE-2023-52476			
	CVE-2023-52597			
	CVE-2023-51780			
	CVE-2023-6915			
	CVE-2023-4133			
	CVE-2023-47038	RHEL 9 : perl (RHSA-2024:2228)	High	7.8
	CVE-2023-40476	RHEL 9 : gstreamer1-plugins-bad-free (RHSA-2024:2287)	High	8.8
	CVE-2023-40475			
	CVE-2023-50186			
	CVE-2023-40474			
	CVE-2023-45233	RHEL 9 : edk2 (RHSA-2024:2264)	High	8.8
	CVE-2023-45232			
	CVE-2022-36764			
	CVE-2023-3446			
	CVE-2022-36763			
	CVE-2024-3651	RHEL 9 : python-idna (RHSA-2024:3846)	High	7.5
	CVE-2022-48622	RHEL 9 : gdk-pixbuf2 (RHSA-2024:3834)	High	7.8
	CVE-2024-0450	RHEL 9 : python3.9 (RHSA-2024:4078)	High	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, 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

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