COHESITY

Release Notes

Version 7.3

November 13, 2025

© 2025 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, the Helios logo, DataGovern, SiteContinuity, DataHawk, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

No part of this documentation or any related software may be reproduced, stored, transmitted, or otherwise distributed in any form or by any means (electronic or otherwise) for any purpose other than the purchaser's personal use without the prior written consent of Cohesity, Inc. You may not use, modify, perform or display this documentation or any related software for any purpose except as expressly set forth in a separate written agreement executed by Cohesity, Inc., and any other use (including without limitation for the reverse engineering of such software or creating compatible software or derivative works) is prohibited, except to the extent such restrictions are prohibited by applicable law.

Published on November 13, 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 7.3 provides new features and enhancements available for on-premises hardware, Cloud Edition, and Virtual Edition clusters. For more information, see What's New in 7.3?.

For more information on upgrading from previous releases to 7.3, see Upgrading to 7.3.

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

What's New in 7.3?

The following new features and improvements are available in this release. For important information about upgrading from previous releases to 7.3, see Upgrading to 7.3.

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

Cloud Services

Amazon Simple Storage Service (S3) Protection Early Access

Cohesity now supports the backup and recovery of Amazon S3 buckets on Physical and Virtual Edition Cohesity clusters. For more information, see Amazon Simple Storage Service Buckets.

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

Protect Azure Premium SSD v2 and Ultra Disk VMs

Cohesity now supports backup and recovery of Azure VMs that use Premium SSD v2 and Ultra disks using both the Native Snapshot and Snapshot Manager Protection Type methods. For more information, see Azure VMs.

Microsoft 365

Download Teams Posts and Private Chats Controlled Availability

Cohesity now supports backup and download of the following items in Microsoft 365 Teams and Mailbox:

- Posts from all channels in Teams
- Posts from a single channel in Teams
- Chats of a specific user in the Mailbox

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

Protect SubstrateHolds Folder Controlled Availability

You can now protect the SubstrateHolds folder under the Recoverable Items and Archive Recoverable Items root folders in Microsoft 365 Mailboxes. For more information, see Plan and Prepare for Mailbox Protection.

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

Protect 100k Microsoft 365 Objects Per Cluster Controlled Availability

Cohesity now supports the backup and recovery of 100k Microsoft 365 objects per cluster across Microsoft 365 protection.

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

Granular Recovery of Microsoft 365 Groups Controlled Availability

Cohesity now supports granular recovery of Microsoft 365 Groups, enabling faster search and recovery of Groups objects. For more information, see Recover Group Items.

With indexing enabled for Groups objects, you can now use advanced search functionality to quickly and efficiently locate specific Groups items. This enhancement allows you to recover individual Groups components, such as mailbox items or site items—while still offering the option to recover entire Groups.

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

Backup and Recovery of Custom Headers for SharePoint Online Document Libraries and Lists Controlled Availability

Cohesity now supports the backup and recovery of custom headers (columns) in SharePoint Online Document Libraries and Lists. This enhancement ensures that your custom metadata configurations are preserved and recoverable, helping you effectively manage your SharePoint Online content.

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

Protect PHL in SharePoint Online Controlled Availability

Cohesity supports the protection of Preservation Hold Library (PHL) for SharePoint Online sites which store content that is subject to retention policies or litigation holds. For more information, see Recover SharePoint.

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

Granular Recovery for Microsoft 365 Exchange Online Mailbox Items

In addition to full mailbox recovery, Cohesity now supports granular recovery of individual items, including calendar events, contacts, notes, and tasks. For more information, see Recover Mailbox.

Custom Certificates Support for Certificate Based Authentication in Microsoft 365Controlled Availability

Cohesity now supports importing custom certificates during Certificate Based Authentication in Microsoft 365. For more information, see Certificate Based Authentication.

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

Protect PHL in OneDrive Controlled Availability

Cohesity now supports the protection of Preservation Hold Library (PHL) for OneDrive which is used to store the files needed for retention policies or litigation holds compliance reasons. For more information, see Recover OneDrive.

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

Recover Microsoft 365 Exchange Online Data to On-prem Exchange Server Controlled Availability

Cohesity now supports recovering Microsoft 365 Exchange Online Mailboxes data to an on-premises Exchange Server. For more information, see Recover Mailbox.

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

Selective Full Mailbox Recovery Controlled Availability

Cohesity now supports selecting the Mailbox Items for a specific period during full Mailbox recovery. This enhancement speeds up the recovery process by reducing the recovery workload. For more information, see Recover Mailbox.

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

Kubernetes

Quiesce Kubernetes Workloads during Backups

Cohesity now supports quiescing stateful Kubernetes workloads before capturing Persistent Volume Claims (PVCs) volume snapshots during backup in a namespace. After the snapshots are taken, the Kubernetes workloads are automatically unquiesced. This ensures consistent and reliable snapshots for stateful applications running in Kubernetes. For more information, see Quiesce Kubernetes Workloads.

Granular Recovery of Files and Folders in Kubernetes

Cohesity supports Kubernetes clusters for granular recovery of files and folders within Persistent Volume Claims (PVCs). It allows for the selective recovery of files and folders from backed-up data volumes instead of restoring the entire volume in case of data corruption. This capability enables users to recover specific files or related files and folders efficiently. For more information, see Granular Recovery of Files and Folders.

Support for S3 Embedded Credentials for Kubernetes

Cohesity now supports the use of embedded S3 credentials for performing Velero backups. Previously, Kubernetes protection required the same user to both create and manage backups and recoveries. With this update, different users can now initiate backups and recoveries, providing enhanced operational flexibility. For more information, see Plan and Prepare for Protecting Kubernetes clusters.

Virtualization

Preserve Backup Chain of Migrated VMs

Cohesity supports preserving the backup chain of VMs that are migrated from a VMware vCenter protected by a Cohesity instance, to a vCD that is already registered with the same Cohesity cluster. This feature eliminates the need to take a full backup of the migrated VMs when a Protection Group is run on the vCD to which the VMs are migrated. For more information, see Protect Migrated VMs or vCD.

IPv6 Support for Red Hat OpenShift Virtualization

Cohesity now supports backup and recovery of VMs in Red Hat OpenShift Virtualization environments configured in dual-stack mode (IPv4 and IPv6). For IPv6 support, the Cohesity cluster must be configured with a preferred IPv6 address. For more information, see Register and Manage Red Hat OpenShift Cluster.

Support for Label-Based VM Backup Selection for Red Hat OpenShift Virtualization

You can now include or exclude VMs for backup in the Protection Group based on assigned labels. This feature simplifies the selection process by eliminating the need to manually select individual VMs. Labels are recognized at the cluster level and applied across all selected namespaces. For more information, see Backup of Selected VMs.

Support for Disk Inclusion in VMware Backups

Cohesity now supports disk inclusion for VMware VMs and Protection Groups. You can use the **Enable Disk Inclusion/Exclusion** toggle to include specific disks during protection. For more information, see Add or Edit a Protection Group for Virtual Servers.

Support for Elastic Org VDC

Cohesity now supports seamless use of Elastic Org VDCs with multiple resource pools for backup and recovery operations. For more information, see Elastic Org VDC.

Support for Tag-Based VM Selection and Virtual Trusted Platform Module (vTPM) Metadata Backup for AHV

Cohesity now supports tag-based VM selection in AHV Prism Central, allowing Auto Protect or Exclude actions based on tags. For more information, see AHV Prism Central tags. Additionally, Cohesity backs up and recovers Virtual Trusted Platform Module (vTPM) metadata during AHV VM recovery to preserve the original vTPM configuration. For more information, see AHV Virtual Trusted Platform Module (vTPM).

> **Note:** User data within vTPM must be backed up manually.

Support for Enhanced vCD VM Cloning for Test & Dev

Cohesity now provides an enhanced experience for cloning vCD VMs for Test & Dev purposes. For more information, see Clone vCloud Director (vCD) VMs.

Improved Windows Deduplicated Volume Handling for VMware Recovery

Cohesity now enhances VMware recovery workflows by introducing improved error handling for scenarios involving Windows deduplicated volumes. For more information, see Recover Files or Folders.

Recover vCD VM Placement and Sizing Policies on Original Recovery Location

Cohesity now allows restoration of placement and sizing policies when VMs are recovered to their original location. For more information, see Recover VMs from a VCD Source.

Exclude Disk Handling for VM Backups

Cohesity now provides an Exclude Disk Handling option that creates excluded or independent disks as empty disks during recovery. This feature is supported when recovering VMs to the original location, a new location, or when performing Test & Dev cloning. This allows you to preserve the VM's disk configuration while excluding specific disks from backup. For more information, see Recover VMs to the Original Location, Recover VMs to a New Location, and Set Clone Options.

Support for Partial Refresh of the vCD Source

Cohesity now provides the ability to perform a partial refresh of the vCD source. A partial refresh is faster than a full source refresh. This enhancement allows you to selectively discover new VMs, vApps, Organizations, Org VDC, and vApp templates through the APIs into the vCD source, eliminating the need to wait for a full vCD refresh. For more information, see Register and Manage a vCD Source.

Support for Teardown of Failed VM and VMDK Recovery Tasks

Cohesity now supports teardown of failed VM recovery and VMDK recovery tasks, allowing you to clean up residual resources left behind when these tasks are not completed successfully. These resources may include recovered VMs or VMDKs present on Cohesity datastores, the Cohesity datastores themselves, or the recovered view. For more information, see Teardown of Failed VM Recovery Tasks and Teardown of Failed VMDK Recovery Tasks.

NAS

Support for Automatic Denylisting in NAS Sources

Cohesity now automatically deny-lists unreachable IP addresses associated with a NAS source. This prevents their use during backup and recovery operations, ensuring smoother operations. For more information, see Automatic Denylisting in NAS Sources.

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

Cohesity now supports NFSv4.1 Kerberos authentication on NetApp and Generic NAS when registering NAS volumes. For more information, see Plan and Prepare for File-Runner Based NetApp ONTAP Backup and Plan and Prepare for NAS Protection.

Support for NFSv4.1 Kerberos Authentication with Dell EMC Isilon sources

Cohesity now supports NFSv4.1 Kerberos authentication with Dell EMC Isilon sources when registering NAS volumes. For more information, see Plan and Prepare for Isilon Protection.

Databases

Support for SSL-Encrypted Communication in IBM DB2 Data Protection

Cohesity now supports backup and recovery of IBM DB2 environments configured with SSL-encrypted communication between the DB2 client and server, ensuring secure data transfer

during protection workflows.

Support for Amazon RDS Custom for Microsoft SQL Server

Cohesity now supports protecting Amazon RDS Custom for Microsoft SQL Server. This managed database service provided by AWS offers a balance between the automation of Amazon RDS and the flexibility of self-managing a database on Amazon EC2. For more information, see Considerations for Microsoft SQL Server.

Protect Microsoft SQL Server AG as Source

Cohesity has enhanced the Microsoft SQL Server Always on Availability Groups (AGs) registration. AGs are now registered as sources. This enhancement simplifies AG protection by listing databases under AG on the Sources page, rather than under individual physical hosts or replicas.

> **Note:**
> - If AG protection was previously configured, or the cluster is upgraded to this version, this functionality will not be enabled by default. To use this feature, existing AG protections must be removed and reconfigured.
> - This feature is not supported for Volume-based backups.

For more information, see SQL Auto Discovery.

Maintenance Mode in SQL Server

You can now enable maintenance mode for SQL Server instances and databases. Enabling maintenance mode skips any scheduled activities or manually initiated operations, such as protection runs, recoveries, and upgrades. Ongoing backups will be canceled, but ongoing recoveries will continue without any interruptions. For more information, see SQL Maintenance Mode.

Enhancements to PostgreSQL Recovery Configuration

The PostgreSQL recovery workflow now includes a new **Path of SSL Certificate** field. You can use this field to specify a different file path for the Cohesity SSL server certificate when restoring PostgreSQL data, offering more flexibility in secure recovery setups. For more information, see Recover PostgreSQL Database.

This enhancement supports scenarios where the certificate files are stored in a different directory than the default location, ensuring greater flexibility and compatibility with varied deployment environments.

Support for Percona MySQL Data Protection Early Access

Cohesity now supports the backup and recovery of Percona MySQL deployments. For more information, see Percona MySQL on Linux.

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

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

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 recover MySQL EE databases to a specific point in time within the backup window.

Support for Backups and Recovery in Partitioned IBM DB2 Environments

Cohesity now supports backup and recovery operations for IBM DB2 databases in partitioned database environments. This enhancement allows a single database to be distributed across multiple partitions on different physical or logical servers. The feature is supported when using the LOGARCHMETH2 log backup method. For more information, see IBM DB2.

> **Note:** You must specify all the nodes in LOGARCHMETH2 configurations along with the IP Addresses and Hostnames.

Cohesity SAP HANA Connector Support for SAP HANA Backup Encryption

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

Supported encryption methods include:

- SAP HANA Backup Encryption
- System PKI SSFS (for internal communication encryption)
- Data and Log Volume Encryption

Supported secure stores:

- SSFS (Secure Store and File System)
- LSS (Local Secure Store)

> **Note:** No additional configuration is required on the Cohesity cluster. Encryption must be enabled and managed within the SAP HANA system.

Support for Amazon RDS Custom for Oracle

Cohesity now supports protecting Amazon RDS Custom for Oracle databases through two methods — ingest-based protection using the Cohesity Oracle Adapter for RMAN-integrated, application-consistent backups, and snapshot-based protection leveraging native AWS snapshots for fast, storage-level backups and restores. For more information, see RDS Custom Oracle.

Separate Views for Oracle Log and Non-Log Backups

Cohesity now supports separate views for Oracle log and non-log backups. This reduces unnecessary storage consumption in live views and snapshots. Each Oracle backup job uses two Cohesity views—one for log backups and another for non-log backups. The number of mount points for each type is limited to the number of nodes in the cluster, while RMAN channel counts remain unaffected.

Oracle SBT Alerts for Backup and Recovery Failures

Starting with Cohesity cluster version 7.3 and SBT release 20250626_0548b3bd, the cluster generates alerts for failed SBT backup and recovery operations. For more information, see SBT Alerts on Backup and Recovery Failures.

Cassandra Source Refresh Update Controlled Availability

Cohesity now automatically updates the Cassandra version and seed list in the source properties whenever a Cassandra source is refreshed. For more information, see Refersh the Cassandra Source.

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

Physical Servers

Files and folders backup for Linux on z/Architecture

Cohesity now supports backing up files and folders for Linux on z/Architecture. For more information, see Add or Edit a Protection Group for Physical Servers.

Support for Sparse File Backup and Recovery

Cohesity now supports specific handling of sparse files during file-based backups. During file-based backups, information about sparse blocks is captured, avoiding the need to store the blocks themselves. Upon restoration, the sparse file structure is accurately reconstructed, ensuring efficient space utilization and consistency with the original file layout. For more information, see Protect a Physical Server (File-based).

S3-Compatible Storage

Support for S3-Compatible Storage Protection

Cohesity now supports the backup and recovery of S3-compatible storage. For more information, see S3-Compatible Storage.

Replication

Object-based Replication

Cohesity now offers flexibility in custom replication, enabling you to replicate selected objects from a backup run to a target, rather than replicating all runs in a protection group. For more information, see About Replication.

Policies and Protection Groups

Cohesity now allows you to choose more granular weekly, monthly, and yearly options with calendar-based scheduling, which is available for both replication and archival. For more information, see Create or Edit a Standard Policy.

Monitoring

SNMP Configuration

Cohesity has introduced a simplified user experience to enhance the SNMP configuration. For more information, see Configure SNMP.

NoSQL

NoSQL Service Error Code

Cohesity can now manage runtime configuration of connectors powered by NoSQL App using CLI and API and the associated actions using AppInstanceActions API. For more information, see NoSQL and Hadoop Service Error Codes.

DataProtect for Cloud (Legacy CE and NGCE Clusters)

Deploy DataProtect for Cloud in AWS Top Secret

You can now deploy DataProtect for cloud (formerly known as Next-Gen Cloud Edition cluster) in AWS Top Secret environments. AWS Top Secret is a secure, isolated cloud region designed specifically for the U.S. Government to support classified workloads.

Object Lock Support for GCP DataProtect for Cloud External Target

On GCP DataProtect for cloud, you can now enable Object Lock for GCP Cloud Storage buckets when registering them as external targets. For more information, see GCP NGCE Object Lock. A GCP external target with Object Lock enabled can be:

- Associated with the cluster's storage domain to store backed-up data as the primary copy.
- Used for archiving data as a secondary copy.

Deploy DataProtect for Cloud in Azure GovCloud

You can now deploy DataProtect for cloud in Azure GovCloud, a dedicated cloud environment designed to meet the strict security and compliance requirements of U.S. government agencies.

Support for Amazon RDS MySQL Data Protection Early Access

You can now perform the backup and recovery of Amazon RDS for MySQL at database level on AWS DataProtect for cloud. For more information, see Amazon Relational Database Service for MySQL.

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

Support for Amazon Aurora MySQL Data Protection Early Access

You can now perform the backup and recovery of Amazon Aurora MySQL at database level on AWS DataProtect for cloud. For more information, see Amazon Aurora MySQL.

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

Support for Azure MySQL Data Protection

You can now perform the backup and recovery of Azure MySQL data on Azure DataProtect for cloud. For more information, see Azure MySQL.

Support for Google Cloud BigQuery Data Protection Early Access

You can now perform the backup and recovery of Google Cloud BigQuery datasets on GCP DataProtect for cloud. For more information, see Google Cloud BigQuery.

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

Elimination of Manual DNS Configuration

Starting with this release, manual DNS configuration of DataProtect for cloud cluster node IP addresses is no longer required for database protection—even though NGCE does not use Virtual IPs (VIPs).

Support for IMDSv2 in AWS DataProtect for Cloud (Legacy)

Cohesity now supports Instance Metadata Service v2 (IMDSv2) configuration in AWS DataProtect for cloud (Legacy) (formerly known as AWS Cloud Edition) cluster nodes. For

more information, see Cloud Edition AWS Setup Guide.

Amazon Simple Storage Service (S3) Protection

Cohesity now supports the backup and recovery of Amazon S3 buckets on AWS DataProtect for cloud. For more information, see Amazon Simple Storage Service Buckets.

External Target

Azure Cold Tier Support for Archival

Cohesity now supports Azure Cold Tier as an external target for CloudArchive with incremental forever and CloudArchive Direct. For more information, see Register an External Target for Archival.

Configure AWS PrivateLink for S3 Archival

You can now configure AWS PrivateLink for archiving data to AWS S3 when registering AWS S3 as an external target. For more information, see AWS PrivateLink.

Incremental Forever Archival Support for GCP Targets with Object Lock

With Object Lock for enabled, Cohesity now supports archiving data to GCP external targets using the Incremental Forever archival format. For more information, see Archive Object Lock.

Following are the GCP targets supported for Incremental Forever archival with Object Lock enabled:

- Google – Nearline
- Google – Standard
- Google – Coldline

CloudRetrieve Support for S3 Compatible - Tape Based

Cohesity now supports CloudRetrieve of data archived to S3 Compatible-Tape Based. For more information see, CloudRetrieve.

Cluster Management

Support Channel Traffic

Cohesity has now upgraded support channel sites and introduced new endpoints. Unblock the ports for these new endpoints in the firewall to ensure seamless connectivity and effective communication. For more information, see Cohesity Support.

Support Toolbox 3.1

The Support Toolbox Overview, used for diagnosing and resolving cluster issues, can now be accessed through a new web UI in Siren v2. Siren is a web-based tool that provides access to logs and other serviceability information on a Cohesity cluster. For more information, see Support Toolbox Overview.

Cohesity Host OS Transition to Red Hat Enterprise Linux (RHEL 9.6)

Cohesity now supports Red Hat Enterprise Linux 9.6 OS as the Host Operating System, replacing RHEL 9.4.

Security

FortKnox Self-Managed

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

Proxy Support for Azure KMS

You can now configure an HTTP or HTTPS proxy for both new and existing Azure KMS configurations on a Cohesity cluster. This allows Azure KMS operations to run through the web proxy already set up on the cluster. For more information, see External Key Management Service.

Secure Syslog Server Connection

Cohesity now supports secure connections to a syslog server with configurable authentication modes (anon and x509/name). For more information, see Add a Syslog server to the Cohesity cluster.

SmartFiles

Store NetBackup Data on Cohesity SpanFS Using Direct I/O Plugin

Cohesity now supports protecting NetBackup data on Cohesity SpanFS using the Direct I/O plugin which is based on the NetBackup OpenStorage Technology (OST) interface.

Per Protocol Node and Disk Performance Monitoring

You can now monitor the performance of individual nodes and disks on the **Performance** page in the UI. You can also view client connections details at the node level by navigating to the **Nodes** tab under the **Client Connections** page in the UI. For more information, see View Performance by Nodes and View Client Connection Node Details.

Enhanced Create Share and Create Directory Quota Pages

The **Create Share** and **Create Directory Quota** pages in the **Cohesity Views** UI have been enhanced with a user-friendly folder selection workflow. For more information, see Manage Share Aliases and User and Directory Quotas for Views.

Archive Services Category Support for Cohesity Views

A new Archive Services category has been added to the **Predefined Templates** list in Cohesity Views. This category includes a predefined template, General Archive, that is

tailored to track archival workloads and licenses. The General Archive template also replaces the existing PACS Archive and Digital Archive templates. For more information, see About Templates Tab and Create Views Using a Predefined Template.

Support for AWS S3 Access Logs

The AWS S3 access log configuration on the Cohesity cluster now allows you to specify the target buckets where the logs will be stored.

Hardware Platform

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
C6208S	96	8TB HDD / 2x 3.2TB SSD (6.4TB total)	General Purpose Node / Capacity Node	2U1N
C6216S	192	16TB HDD / 2x 6.4TB SSD (12.8TB total)	General Purpose Node / Capacity Node	2U1N
C6224	288	24TB HDD / 2x 6.4TB SSD (12.8TB total)	Capacity Node	2U1N

Cohesity Feature Deprecation

The following features are deprecated from Cohesity 7.3 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 Feature Name	Description	Last Supported Cohesity Version	Alternative Solutions
Winexe Fallback for Recoveries Using the 'Auto Deploy Cohesity Agent' Workflow	This method was used by adapters that support the 'Auto Deploy Cohesity Agent' (Ephemeral Agent) workflow for Windows VMs. It served as a fallback option when the required permissions for the primary deployment method were not available.	7.2.2_u2	Use the 'Auto Deploy Cohesity Agent' option only with accounts that have local administrator privileges on the target Windows VM. If such privileges are not available, use an alternative method such as 'Use Existing Cohesity Agent' or 'Use VMware Tools'.
Physical agent support for Windows 2008 R2	Cohesity 7.3 will be the last release where physical agents for Windows 2008 R2 platform will be supported.	7.3	1. Migrate data to newer versions of the Windows Server platform. 2. Export data using SMB and protect the data using the Generic NAS.

Upgrading to 7.3

Upgrade Paths

You can upgrade your Cohesity cluster from previous releases to 7.3. The following table provides details on supported upgrade paths.

Your Current Release	Upgrade Path to 7.3
• 7.2.2_u2 • 7.2.2_u1 • 7.2.2 • 7.2.1 • 7.2 • 7.1.2_u6 • 7.1.2_u4 • 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	7.3 directly

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 7.3 is supported. 7.3 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 7.3 is supported. 7.3 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 7.3:

- 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 7.3 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 7.3, 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 7.3 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.

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 7.3 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 7.3 version, if you are replicating the Mailbox data to a remote Cohesity cluster, then ensure that you upgrade the remote Cohesity cluster to the 7.3 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.

FortKnox

After upgrading to the 7.3 version, cold vaults created in an AWS Region use Amazon S3-Glacier Deep Archive (GDA) and require a minimum retention period of 180 days. In earlier releases (prior to 7.3), cold vaults were created on Amazon S3-Glacier Flexible Retrieval (FR). Recovery starts up to 12 hours after initiation, due to the data hydration process required for data access from cold vaults.

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:

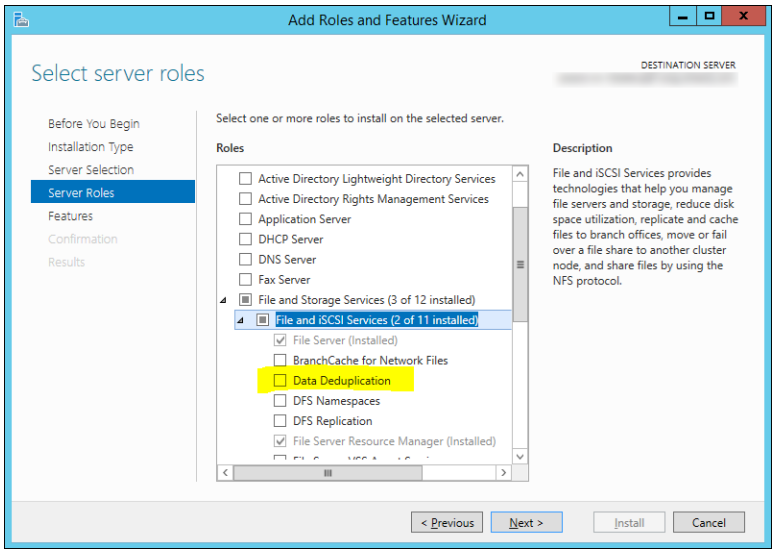
- When recovering a file or instantly mounting a volume from a Windows VM or Physical Server Backup Source that has Windows deduplication installed and enabled for one or more volumes, you must choose a target machine that also has Windows deduplication installed (it does not have to be enabled for any 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 will fail with the error message: "Windows Data Deduplication role is not installed on the target machine. Retry recovery after installing the Windows Data Deduplication role on the target machine."
  - Instant volume mounting will fail with the error message: "Windows Data Deduplication role is not installed on the target machine. Retry recovery after installing the Windows Data Deduplication role on the target machine."

  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`.

Server Type	Volume Type	

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:

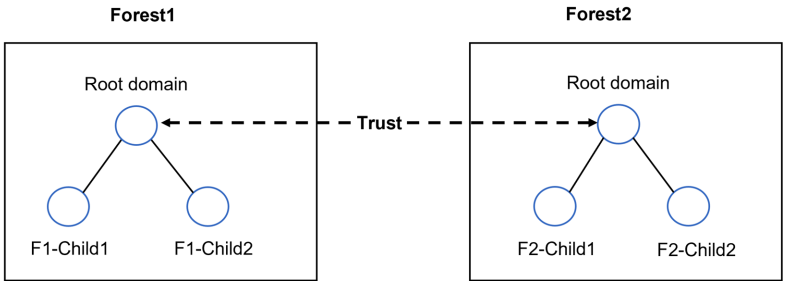
- Backups that are taken on the Full (No CBT) schedule are not currently archived by the Cohesity cluster. Other full backups (first Protection Group run, failed CBT) can be archived because they are not initiated by the Full backup schedule.
- In production environments, Cohesity recommends not replicating 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

Fixed Issues

The **Fixed Issues** page provides a list of issues fixed in the 7.3 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 7.3 release:

Cohesity Version	CVE Name	Details	Threat Severity	CVSS Base Score
7.3	NA	There are no new security fixes in the release.	NA	NA

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

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

Support/Service Assistance

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

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

Cohesity Software Running on Partner Hardware

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

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

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

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

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