COHESITY

SiteContinuity User Guide

May 15, 2025

Published on May 15, 2025

Contents

Cohesity Data Cloud

Cohesity Data Cloud is a unified cloud data management platform for securing, managing, and extracting value from your data, available as self-managed software and SaaS. The following are the key features of Cohesity Data Cloud:

- **Scale and simplicity**—Manage your entire data estate easily across data centers, edge sites, and public cloud environments.
- **Zero Trust Security**—Keep your data safe with in-flight and at-rest encryption, immutability, Write Once Read Many (WORM), Role-based Access Control (RBAC), and Multi-factor Authentication (MFA).
- **AI/ML Powered**—Streamline operations and defend against ransomware with Machine Learning (ML) and Artificial Intelligence (AI)-powered recommendations.
- **3rd Party Extensibility**—Connect Cohesity Data Cloud to your other IT investments to improve visibility and streamline operations.

Pillars

Cohesity Data Cloud includes five pillars. Each pillar encompasses a set of features and functionalities tailored to a specific aspect of data management. Each pillar contains one or more specialized apps. These apps are tailored to provide you with a focused and streamlined experience for achieving your goals within that particular area. Following are the five pillars:

- Protection
- Security
- Mobility
- Access
- Insights

Protection

The **Protection** pillar offers the most comprehensive backup and recovery solution to protect cloud-native, SaaS, and on-premises data at scale. You can simplify and accelerate the backup and recovery of enterprise workloads across on-premises and cloud with a secured unified platform for data resilience.

The **Protection** pillar includes the following apps:

- **DataProtect**—Offers a unified view and global management of all your Cohesity clusters, whether on-premises, in the cloud, or as Virtual Editions, regardless of the cluster size. You can easily connect your clusters to Helios and access them from anywhere using an internet connection and your Cohesity Support Portal credentials. It simplifies cluster management and enables efficient monitoring and control across your entire infrastructure.

  > **Important:** The previous **Cluster Manager** app has been integrated into the **Protection** pillar and it is now known as **DataProtect**.

- **DataProtect as a Service**—With Cohesity DataProtect delivered as a service, you can embrace a more predictable OpEx cost model, streamline backup operations across the hybrid cloud, and harness the power of your data for greater possibilities. By signing up, connecting, and initiating data protection, you can get started within minutes, ensuring your valuable data is safe and secure. Experience the convenience and efficiency of our seamless cloud-based solution for all your backup needs.

  > **Important:** The previous **DataProtect** app has been integrated into the **Protection** pillar and it is now known as **DataProtect as a Service**.

Security

The **Security** pillar empowers you to mitigate the risks posed by ransomware and other threats through an intelligent data security and management platform, purpose-built to safeguard your data and ensure its utmost security. You can boost cyber resiliency with ransomware recovery capabilities. These solutions help enterprises identify, protect, and recover data and processes from sophisticated cybersecurity threats.

The **Security** pillar includes the following apps:

- **Security Center**—Provides a comprehensive suite of security features, including DataHawk Threat Protection, Data Classification, Cyber Vaulting, and Platform Security, all conveniently accessible from a single unified platform.
- **FortKnox**—An award-winning cyber-vaulting solution that offers a SaaS-based data isolation and recovery platform that securely stores an immutable copy of data in a Cohesity-managed cloud vault.

Mobility

The automated disaster recovery solution in the **Mobility** pillar empowers you to achieve near-zero application downtime and zero data loss through unified backup and automated disaster recovery capabilities. You can eliminate secondary data centers and reduce the complexity of your on-premises operations.

SiteContinuity simplifies business continuity and disaster recovery with automated failover and failback orchestration for your mission-critical workloads.

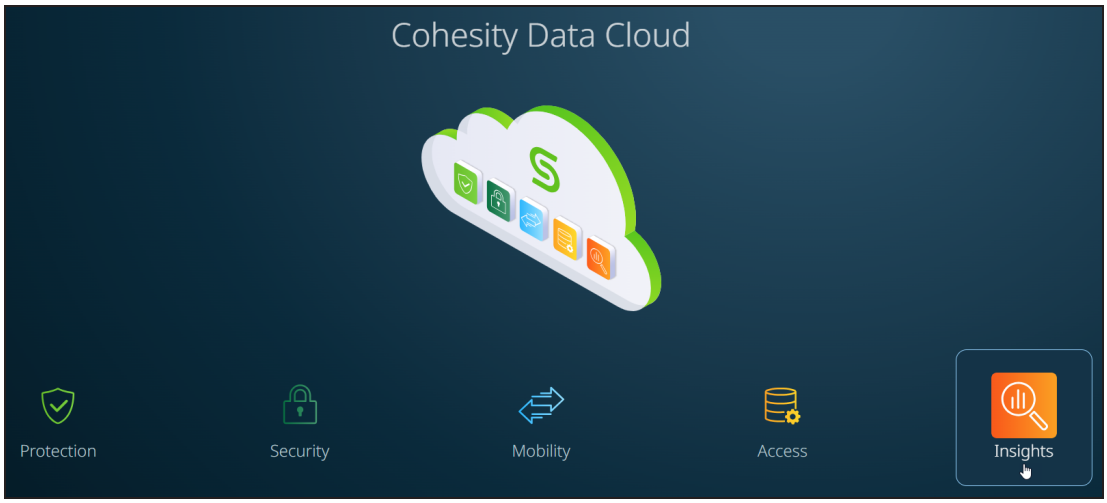
Access

SmartFiles, the unified file and object services solution in the **Access** pillar, enables you to manage, secure, and do more with your data with software-defined file and object services for the hybrid cloud.

SmartFiles enables seamless data access for your users and applications with simultaneous multiprotocol support for NFS, SMB, and S3. You can also manage your data efficiently from a single console, giving you global control over data on-premises, at the edge, and in the cloud.

Insights

The **Insights** pillar empowers you to engage with and uncover valuable insights from your data:



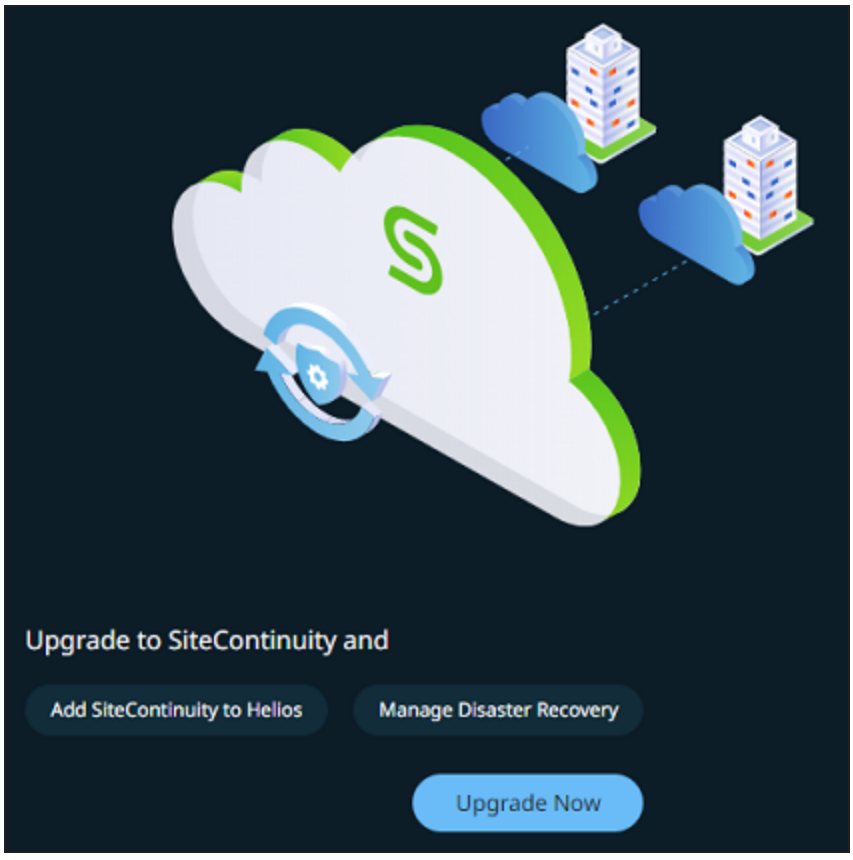
The **Insights** pillar includes the following apps:

- **Data Insights**—Harness the potential of your most important enterprise data and gain deep meaningful insights and learnings into your organization and data with Cohesity's AI-powered conversational search solution.
- **Platform Insights**—Optimize, plan, and scale your data management by providing insights into your cluster's storage and load utilization, along with other essential performance metrics.

Set Default Landing Page

When you log in to Cohesity Data Cloud, all five pillars and apps are displayed by default. You have the ability to view all the pillars and apps, regardless of whether you have subscribed to them or not. If you have not subscribed to the app, an **Upgrade Now** option is displayed.

Click **Upgrade Now** to easily upgrade your subscription and gain access to the additional features and capabilities offered by the app:

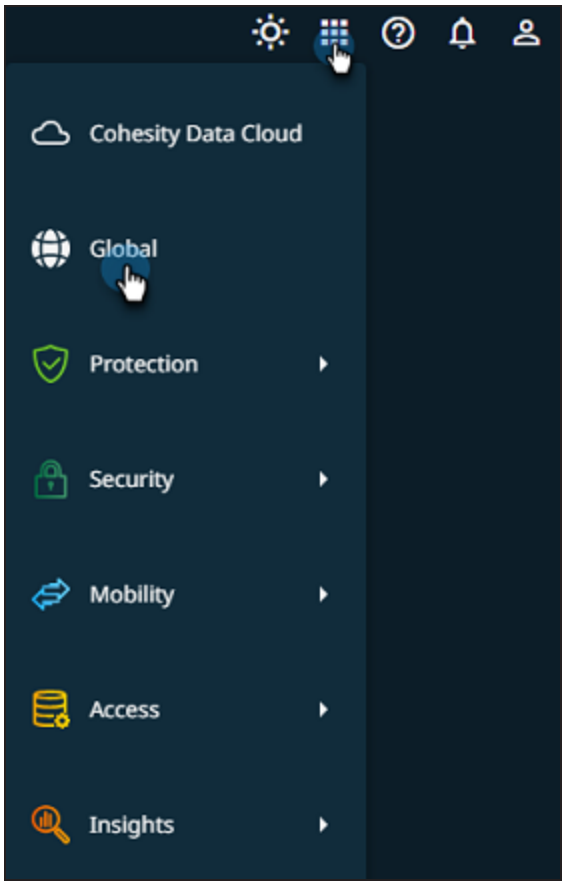


To set a specific page as the default landing page when accessing Cohesity Data Cloud, follow these steps:

1. Log in to Cohesity Data Cloud.
2. Click any pillar and select an app.

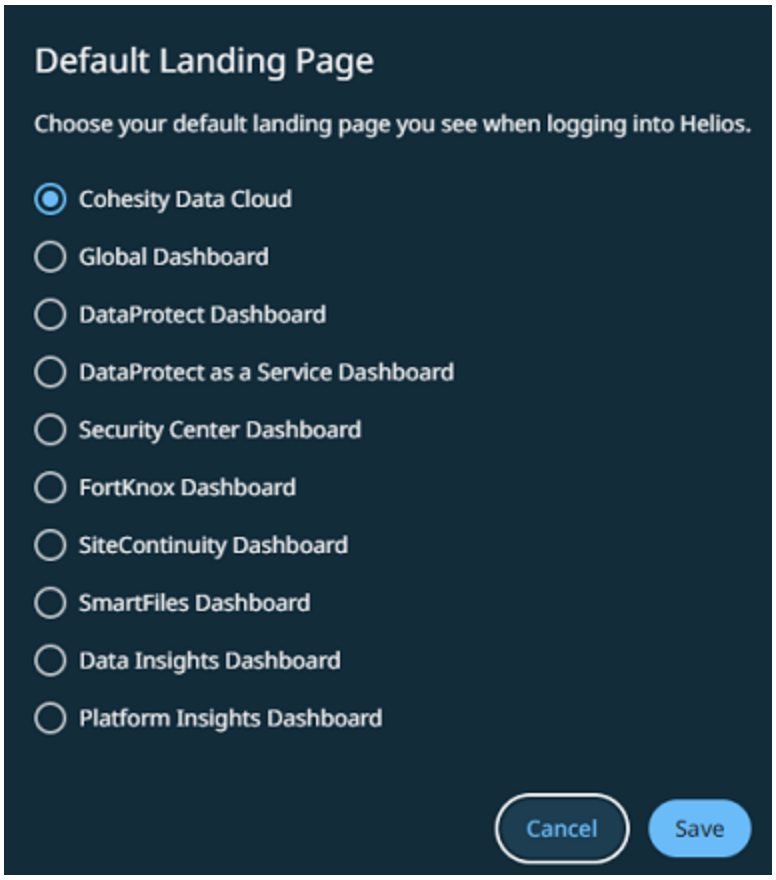
For example, you can click the **Protection** pillar and select **DataProtect**.

3. Click the app-selector menu and select **Global**:



4. On the **Global > Dashboard** page, click the vertical ellipsis icon and click **Default Landing Page**:

5. On the **Default Landing Page** dialog, choose your default landing page and click **Save**:



To view the changes to the default landing page in Cohesity Data Cloud, follow these steps:

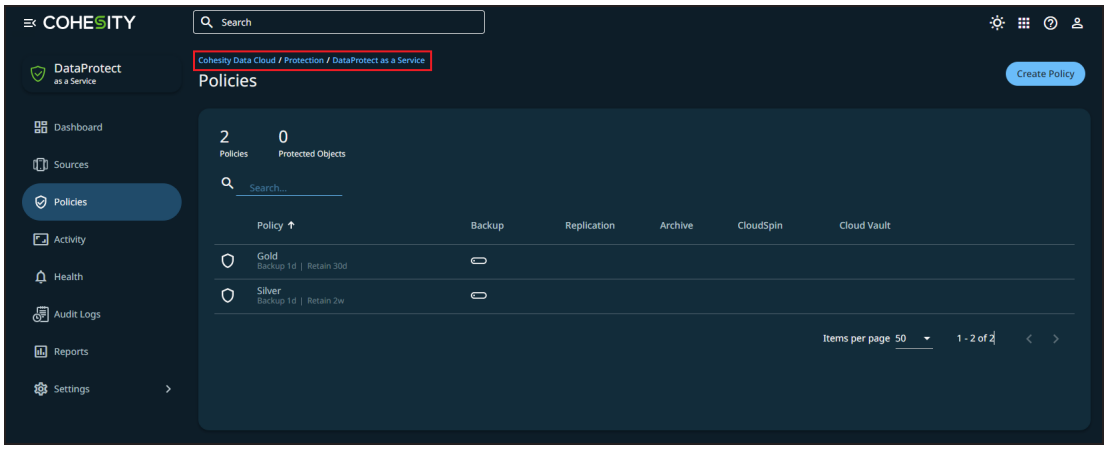
1. Log out of Cohesity Data Cloud.
2. After logging out, navigate back to the **Cohesity Data Cloud** login page.
3. Enter your credentials and log back in to Cohesity Data Cloud.

   After logging back in, you can notice that the default landing page has been updated as per your preference.

Breadcrumbs

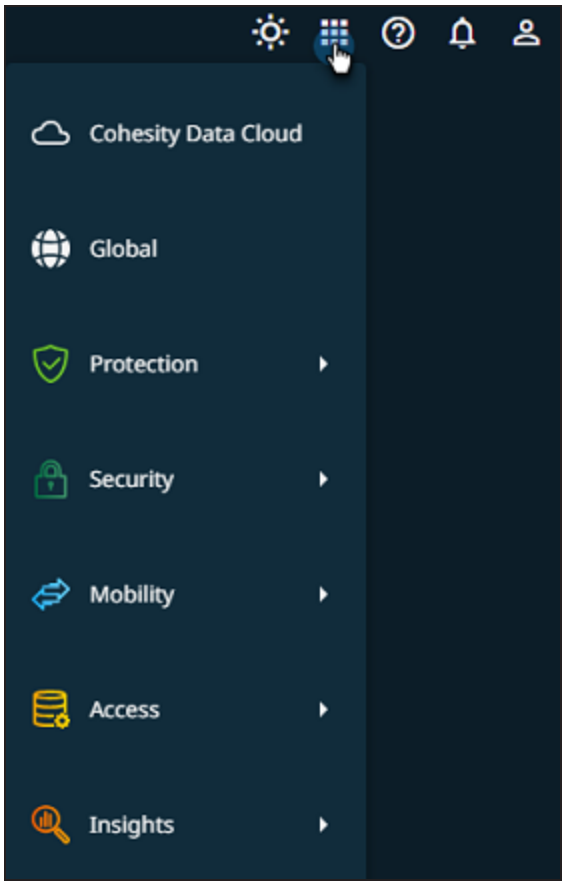
Cohesity Data Cloud introduces support for breadcrumbs, a user-friendly and efficient navigation aid. Breadcrumbs enable you to easily track your path and quickly navigate between pages within Cohesity Data Cloud. By understanding how to use breadcrumbs effectively, you can streamline your workflow and enhance your overall experience.

Breadcrumbs appear below the search bar and show the sequence of steps taken to arrive at the current location. Breadcrumbs consist of clickable links, allowing you to easily navigate back to previously visited pages:



Switch Between Apps

You can use the app-selector menu to navigate between different apps:



Do one of the following:

- Click **Cohesity Data Cloud** to navigate to the Cohesity Data Cloud landing page. On this page, the easy navigation options allow you to explore the five pillars provided by

Cohesity.

- Click **Global** to navigate to the Global dashboard. The Global dashboard provides a comprehensive view with dashboards displaying key metrics and data from the clusters you manage and applications you have subscribed to across the five pillars in Cohesity Data Cloud.
- Hover over **Protection** and select one of the following apps:
  - **DataProtect**—Offers you a unified view and global management of all your Cohesity clusters, whether on-premises, in the cloud, or as Virtual Editions, regardless of the cluster size.
  - **DataProtect as a Service**—Embrace a more predictable OpEx cost model, streamline backup operations across the hybrid cloud, and harness the power of your data for greater possibilities.
- Hover over **Security** and select the following apps:
  - **Security Center**—Provides a comprehensive suite of security features, including DataHawk Threat Protection, Data Classification, Cyber Vaulting, and Platform Security, all conveniently accessible from a single unified platform.
  - **FortKnox**—A SaaS-based data isolation and recovery platform that securely stores an immutable copy of data in a Cohesity-managed cloud vault.
- Hover over **Mobility** and click **SiteContinuity**. The automated disaster recovery solution empowers you to achieve near-zero application downtime and zero data loss through unified backup and automated disaster recovery capabilities.
- Hover over **Access** and click **SmartFiles**. The unified file and object services solution enables you to manage, secure, and do more with your data with software-defined file and object services.
- Hover over **Insights** and select **Platform Insights**. Platform Insights offers a predictive and planning model that can make projections on cluster utilization and storage consumption and a set of 17 built-in reports.

Set User Preferences

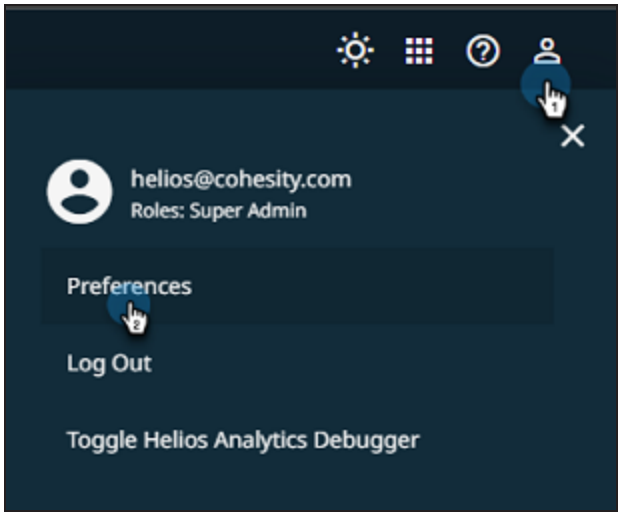
The **User Preferences** page in Cohesity Data Cloud allows you to customize various settings and options to tailor your experience according to your personal preferences. You can modify settings related to your account, user interface, and interactions with the Cohesity platform.

To set user preferences:

1. Log in to Cohesity Data Cloud.
2. Click any pillar and select an app.

   For example, you can click the **Protection** pillar and select **DataProtect**.

3. Click the user icon in the upper-right corner and click **Preferences**:



   The **User Preferences** dialog is displayed.

4. You can customize the following:
   - **Language**—Select the language. Cohesity Data Cloud supports the following languages:
     - English
     - Japanese
   - **Theme**—Select the theme. The theme you choose remains consistent across all Cohesity Data Cloud applications. Cohesity Data Cloud supports the following themes:
     - Dark
     - Light
   - **Default Landing Page**—Select the default landing page that appears upon logging into Helios:
     - Cohesity Data Cloud
     - Global Dashboard
     - DataProtect Dashboard
     - DataProtect as a Service Dashboard
     - Security Center Dashboard
     - FortKnox Dashboard
     - SiteContinuity Dashboard
     - SmartFiles Dashboard

    - Data Insights Dashboard
    - Platform Insights Dashboard
- **Unsubscribed Services**—Opt to display or hide navigation items and content for any services that you have not subscribed to:
    - **Show**—Displays all the five pillars and all available services.
    - **Hide**—Displays only the pillar(s) and service(s) that you have subscribed to.
- **Byte Scaling**—Adjust the scale or size of data in terms of bytes. Cohesity Data Cloud offers the following byte scaling options:
    - Base 1024 (1 KiB = 1024 bytes)
    - Base 1000 (1 KB = 1000 bytes)
- **Time Format**—Select how time should be represented in Cohesity Data Cloud:
    - 12-hour clock
    - 24-hour clock
    - Time Zone—Displays the time zone.
- **Persist Snack Bars**—Choose whether to keep messages, alerts, or notifications visible until you interact with them or let them disappear automatically.
    - **Persist Snackbar Messages**—Messages, alerts, or notifications stay visible until you acknowledge the message or dismiss it manually.
    - **Disappearing Snackbar Messages**—Messages, alerts, or notifications disappear automatically after a few seconds.

5. Click **Save**.

Global Dashboard

If you manage your Cohesity clusters through Cohesity Platform and if you have subscribed to any service, the **Global** dashboard provides a consolidated view of your cluster(s) and service(s).

On the **Cohesity Data Cloud** landing page, click the **Cohesity Data Cloud** icon to navigate to the **Global** dashboard.

The **Global** dashboard provides a comprehensive overview of various aspects, including the health of managed clusters, protection status of objects, posture advisor score, discovered threats, and consumption metrics. The dashboard includes the following cards:

- Health
- Protection Status

- Posture Advisor Score
- Threats Discovered
- Consumption

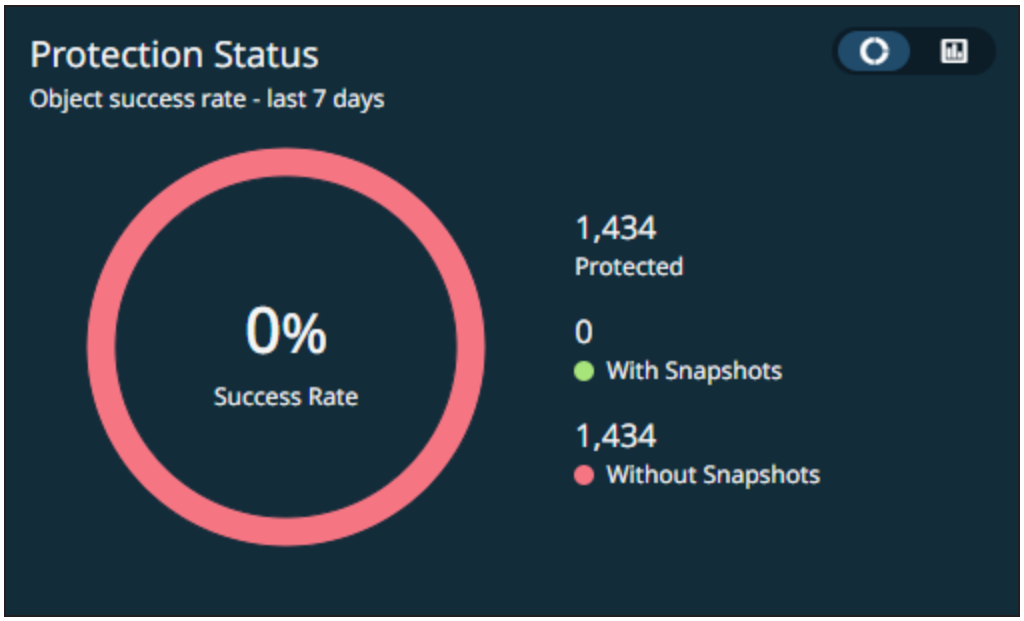
Health

The **Health** card summarizes the health of clusters managed in Cohesity Platform. It displays the following details:

- The number of healthy and unhealthy clusters
- Summary of alerts generated by the Cohesity cluster(s)
- Geographical locations of the Cohesity cluster(s)

Protection Status

The **Protection Status** card provides a summary of all protected objects that had a backup run. You can view a summary of the following:

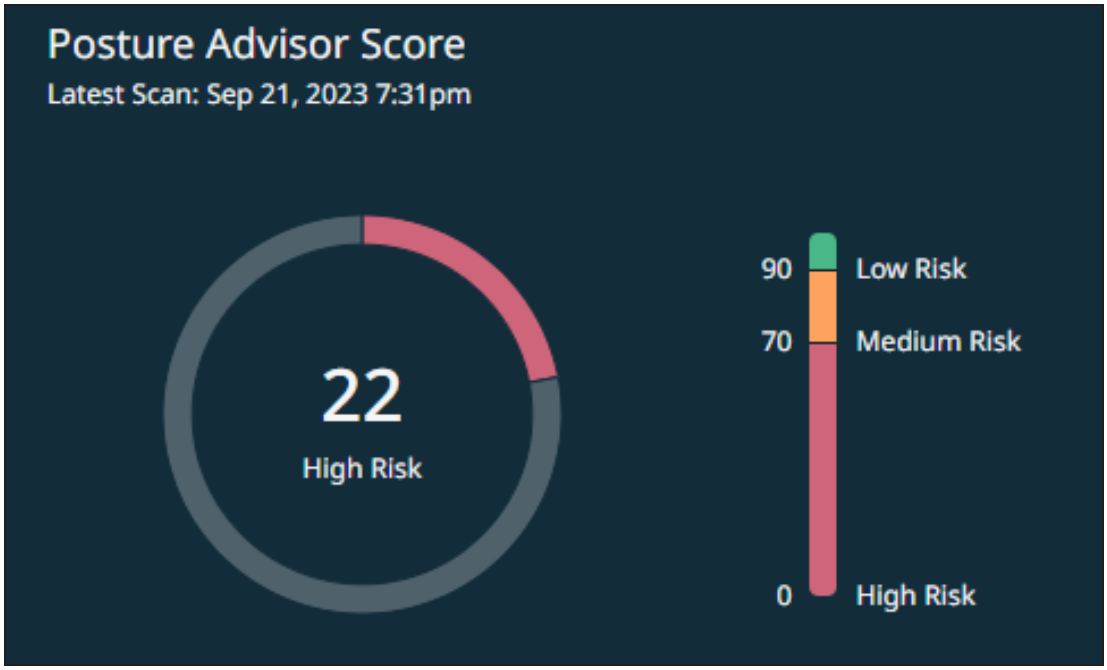


- Backup success rate
- Objects with and without snapshots
- Protected objects by type

Click on the card to navigate to the Protected Objects report page, where you can access detailed and granular information about the protected objects.

Posture Advisor Score

The **Posture Advisor Score** card allows you to get a global view of the security posture across all clusters managed in Cohesity Platform:



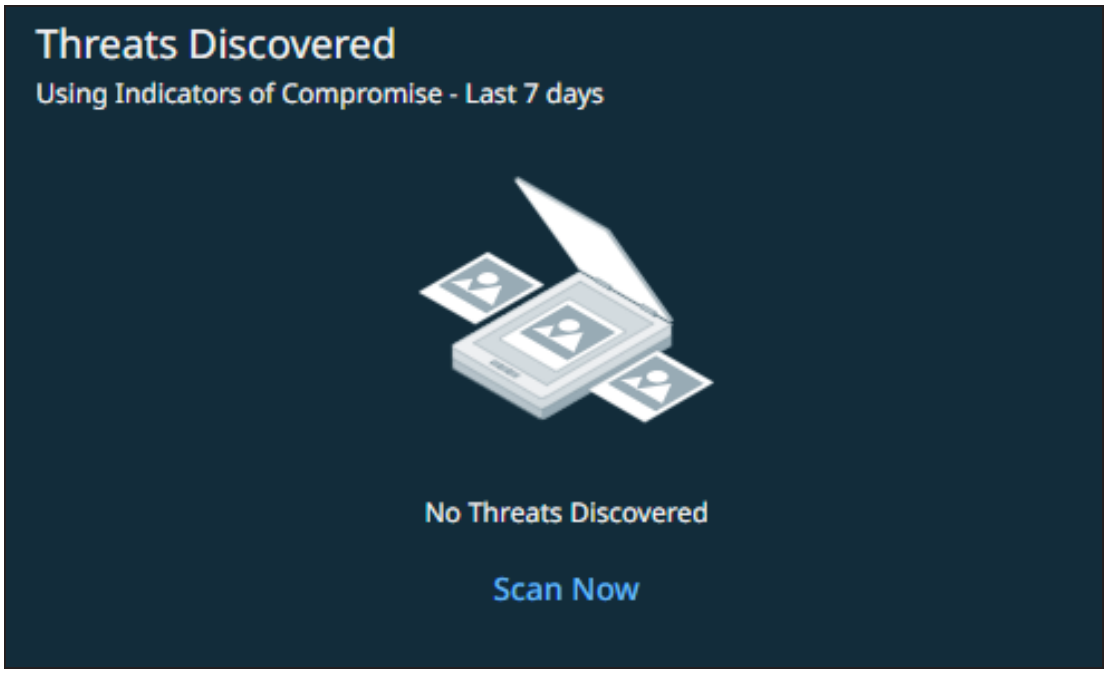
The card categorizes the score into the following categories:

- Less than 70—High risk
- 70 to 90—Medium risk
- Greater than 90—Low risk

For more information, see Posture Advisor.

Threats Discovered

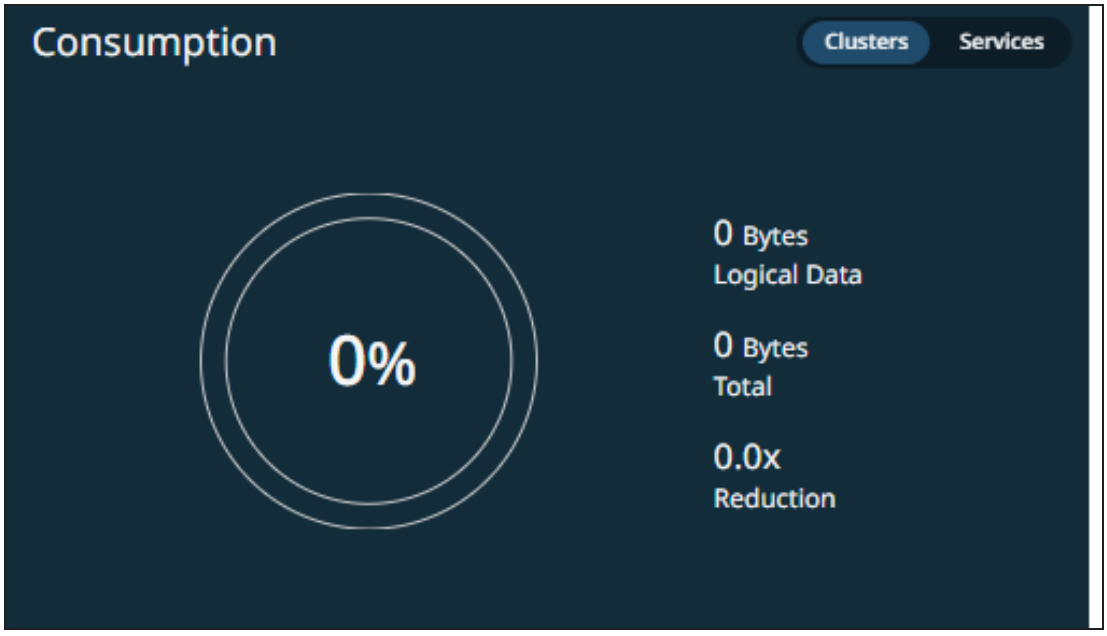
The **Threats Discovered** card summarizes the threats found during scans for malware and cyber threats using Indicators of Compromise (IOCs). You can click **Scan Now** and perform a threat scan:



For more information, see Threat Detection.

Consumption

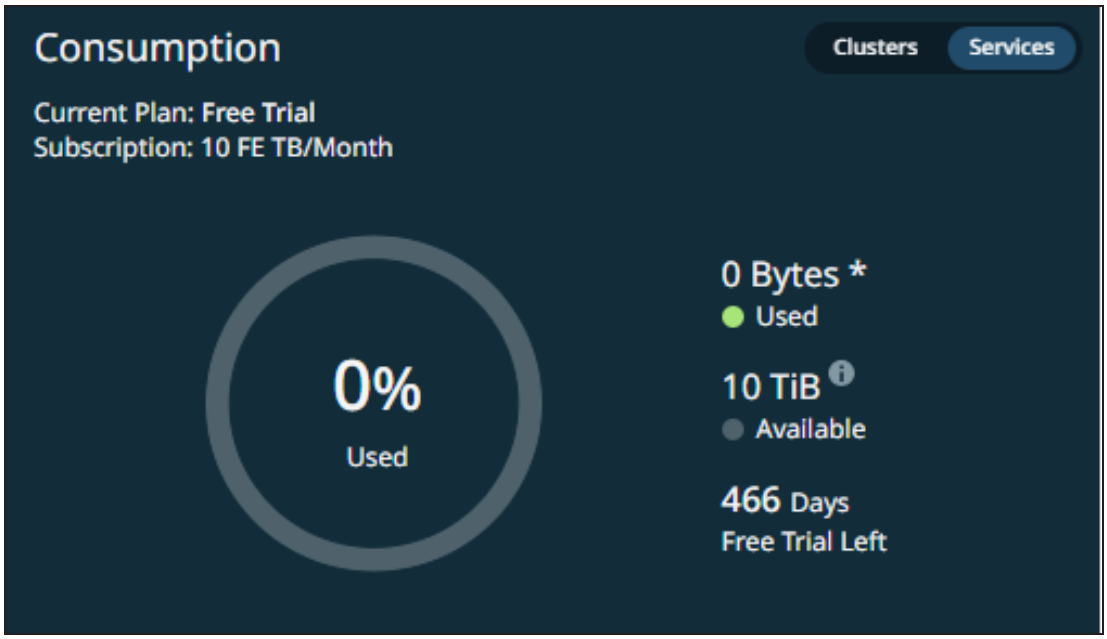
The **Consumption** card provides the storage statistics across all clusters managed in Cohesity Platform. You can view the following details related to clusters:



- Logical data consumed
- Total capacity available

- Storage reduction

On the **Consumption** card, click **Services** to view:



- Current plan—Free trial or a paid plan.
- Details about your subscription plan.
- Storage consumed by the protected objects in DataProtect as a Service. Click **Used** to access the Service Consumption report, which provides detailed consumption statistics.
- The amount of storage included in your subscription.
- The remaining duration of your subscription.

Cohesity SiteContinuity

Modern businesses, despite their technological advancements, remain vulnerable to natural disasters such as floods and hurricanes, along with unnatural threats like cyberattacks and power outages. These events can severely disrupt critical systems. Given the increasing frequency of such incidents, ensuring effective Disaster Recovery (DR) is paramount. Rapid recovery of systems and applications to a stable state is essential for sustaining business operations and continuity.

Cohesity SiteContinuity offers a robust solution, integrating data security, protection, and DR for applications and virtual infrastructure. Leveraging our trusted data protection service, SiteContinuity provides tailored capabilities that are designed to meet the unique needs of businesses today.

Improved DR Orchestration

SiteContinuity provides a unified tool to manage disaster recovery for your entire range of applications. This includes both mission-critical applications and less critical operational systems, ensuring comprehensive coverage.

Intuitive User Interface

SiteContinuity operates on a single, web-scale platform seamlessly supporting operations from on-premises to on-premises. SiteContinuity features an intuitive user interface that utilizes your existing backups, eliminating the need for external applications for orchestration.

Self-Contained DR Plans

SiteContinuity empowers business continuity teams by allowing them to create reusable blueprints of applications for use in DR plans. These plans can be regularly tested without causing disruptions. In the event of a disaster, an automated DR plan can be activated instantly with a single click. This provides seamless end-to-end automation and orchestration for applications at the DR site, enabling rapid recovery within minutes.

With SiteContinuity, businesses can have confidence in their ability to protect their data and quickly recover in the event of a disaster.

VMware VMs

Cohesity SiteContinuity simplifies and streamlines the orchestration of disaster recovery, automating critical manual steps involved in the process.

SiteContinuity allows you to create a comprehensive DR plan with an acceptable Recovery Point Objective (RPO) for automated disaster recovery of VMware virtual machines (VMs). In this process, SiteContinuity utilizes data backed up on your primary Cohesity cluster. This data, originating from your source VMware vCenter on the primary Cohesity cluster, is replicated to a secondary (DR) Cohesity cluster. This DR cluster can be failed over to a target VMware vCenter. After a successful failover, you have the option to fail back your VMware VMs to the original vCenter or a new one. In addition to restoring the VMware VMs on the DR site, SiteContinuity also ensures the protection of these VMs. This comprehensive solution caters to the specific needs of modern businesses.

Key Features

- **Ransomware Sandbox**: Create a sandbox environment within the DR cluster. This environment serves as a safe space to investigate ransomware anomalies, conduct diagnostics, and test potential remediation strategies.
- **Simplified Setup**: Set up disaster recovery through a simple three-step process:
    1. **Define DR Requirements**: Specify your DR requirements such as source and target sites, along with your desired RPO.
    2. **Orchestrate Your Applications**: Specify the orchestration for your applications, covering VMs, their order, scripts, and any required time delays.
    3. **Configure Resource Profiles**: Create one or more resource profiles to be utilized during DR operations.
- **Automated DR Solution**: Ensures business continuity with a 15-minute RPO and near-instant Recovery Time Objective (RTO).
- **Restore Applications**: Restore applications to a specific point in time as needed.
- **Test DR Plans**: Test DR plans to identify gaps and adjust the plan for expected functionality.
- **Audit and Activity Logs**: Get comprehensive logs that record every action and change to your DR environments.

Supported Workloads

SiteContinuity is currently supported only for on-premises to on-premises (site-to-site) disaster recovery of VMware VMs.

Key Concepts

Read through the following concepts for a better understanding of some of the key concepts in SiteContinuity. It will help you navigate the planning and preparation for the DR operations in your DR plan.

Sites

To facilitate DR operations in SiteContinuity, you need to designate Cohesity clusters as sites and map them to specific locations. As SiteContinuity is an as-a-Service solution offered via Helios, connect the clusters to Helios before designating the clusters as sites.

If the primary IT infrastructure becomes unavailable, the applications are replicated from the primary site to a secondary or DR site to resume operations with minimal disruption. For this reason, designate separate Cohesity clusters for the primary sites and DR sites. Map clusters that protect your applications as Primary sites. Map clusters to which you want to replicate the applications as DR sites.

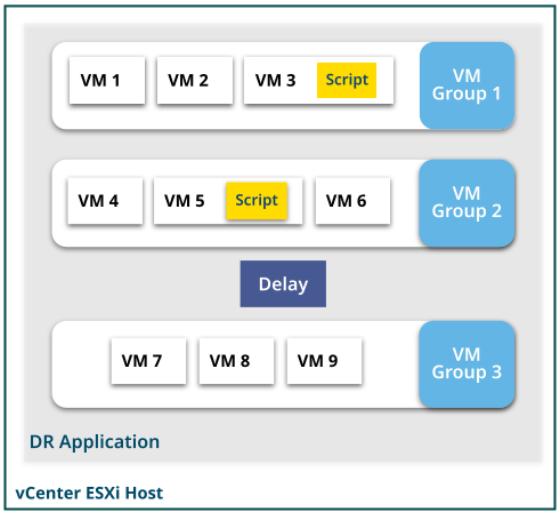
For details on how to map a Cohesity cluster to a site, see Add Sites.

DR Plan

To facilitate DR orchestration, you must create a DR plan. A DR plan is a business plan that defines which DR Applications can be effectively brought up and where (DR site). SiteContinuity offers a simple, easy-to-use interface to create DR plans that consists of DR Applications, primary and DR sites, and Resource Profiles. For details on how to create a DR plan, see Create a DR Plan.

DR Application

A DR Application allows you to specify the orchestration order of VMs with the ability to insert executable scripts and time delays. Orchestration order is the sequence by which the VMs are brought online and to an operational state on a site. You can group the VMs in the DR application into multiple VM Groups.



SiteContinuity executes the components of the DR Application in the order in which they are defined in the DR plan. The VMs within a VM Group (along with scripts applied on the VMs) are executed concurrently. For example, in the above image, VM Group 1 is executed first, followed by VM Group 2. After the delay, VM Group 3 is executed. When VM Group 1 is executed, VM 1, VM 2, and VM 3, along with its script, are executed concurrently.

A DR Application is mapped with a single vCenter registered on the primary site. For details on how to create a DR Application, see Create DR Application.

VM Group

A VM Group is a logical grouping of VMs that represents a specific tier in your application. For example, if you have a multi-tier application that consists of several VMs (some running databases, some applications, and others web services), you can create a VM Group for each tier (such as Database tier, Application tier, and Web tier).

Custom Scripts

Custom scripts are user-defined scripts that can run on VMs. Use these scripts to run configuration changes on the failed over or failed back VMs. For security purposes, SiteContinuity requires that you provide the credentials of the VMs to apply a custom script. An uploaded script is saved only after the authentication of the provided credentials are verified. For VMs running on Windows OS, Cohesity supports batch scripts, and for VMs running on Linux OS, Cohesity supports bash scripts.

Time Delay

You can add time delays to your DR plan. SiteContinuity pauses the DR execution for the defined interval before resuming the operation. For example, if the delay is defined as 10 seconds in the above image, SiteContinuity would wait for 10 seconds after executing VM Group 2. After the delay, VM Group 3 is executed.

Resource Profile

Resource Profile is a combination of a Default Resource Set and one or more Custom Resource Set. A DR plan can have multiple Resource Profiles.

The Resource Profile needs to be redefined every time you perform a Test or Actual Failover or Failback because the vCenter settings specific to each VM used in the previous operation are no longer applicable when working with a new set of VMs in the sites.

Default Resource Set

When creating a Disaster Recovery (DR) plan, you define a Default Resource Set, which consists of a collection of Data Center settings. SiteContinuity applies these Data Center settings to all VMs defined in the DR plan after a Failover event. Similarly, you need to define a Default Resource Set when failing back VMs to the primary site. The Data Center settings in the Default Resource Set are:

- **Data Center.** An aggregation of selected objects in the vCenter inventory that is needed for the virtual infrastructure, such as the VMs, clusters, networks, and data stores, to work. An organization can have multiple Data Centers.
- **Cluster.** A collection of ESX/ESXi hosts and associated VMs intended to work together as a unit.

- **Resource Pool.** A resource pool is the collection of VMs. Resource pools can be grouped into hierarchies for partitioning available CPU and memory.
- **Data Store.** A virtual storage entity created by VMware ESX/ESXi hosts as a repository for the log files, scripts, configuration files, and virtual disks of the VMs.
- **Network.** In a Data Center, the network enables the communication between VMs, virtual servers, and data center locations.
- **DNS Server.** Dynamic Host Configuration Protocol (DHCP) or Static Domain Name System (DNS) servers to translate domain names into IP addresses.

Custom Resource Set

Custom Resource Sets override the Default Resource Set for specific VMs. By creating Custom Resource Sets, you can apply unique settings to one or more VMs. You can create as many Custom Resource Sets as needed.

RPO

Recovery Point Objective (RPO) indicates the data loss a business can tolerate. When disaster strikes, RPO defines how far you can roll back to the last usable snapshot. With SiteContinuity, you can achieve a Recovery Point Objective (RPO) of 15 minutes. This means that in the event of a disaster, you can recover your applications to a state as near as 15 minutes before the occurrence of the disaster, resulting in reduced downtime and data loss.

RTO

Recovery Time Objective (RTO) refers to the downtime a business can tolerate in a disaster.

Continuous Data Protection

Cohesity's CDP provides 15-min RPOs for applications in VMware environments. If you want to recover your VMware VMs from any point in time, then you must enable CDP. For more information, see Cohesity CDP for VMware.

What's New

Cohesity SiteContinuity keeps evolving. We regularly add new features and support for additional workloads that you can recover after a disaster using the service.

Keep up with the latest developments here!

May 2025

Alta Copilot: Cohesity introduces support for Alta Copilot, an AI-powered interactive assistant designed to offer self-service product support. You can use natural language to request help or guidance on managing your data. Alta Copilot is available to all users across all apps in Cohesity Data Cloud.

January 2024

The following features are included in this release:

- **Reports**: You can now use the reporting capabilities in SiteContinuity to assess the Disaster Recovery (DR) Plan's efficacy, identify areas for improvement, and ensure preparedness for future incidents. The DR Plan report consists of all operations initiated on a DR plan within the specified time range and provides the final status of these operations. The Activity Detail report provides a holistic overview that consolidates DR plan details, Resource Profile specifics, VM-level insights, and a chronological depiction of the steps in the activity. For more information, see:
  - Disaster Recovery Plan Report
  - Activity Detail Report
- **Subscription Banners**: Cohesity Helios now displays banners on the UI, providing details on your Cohesity SiteContinuity subscription status, allowing you to take necessary actions. For more information, see Subscription Status.
- **Pillars**: Cohesity Data Cloud now includes five pillars. Each pillar encompasses a set of features and functionalities tailored to a specific aspect of data management. Each pillar contains one or more specialized apps. These apps are tailored to provide you with a focused and streamlined experience for achieving your goals within that particular area. Following are the five pillars:
  - Protection
  - Security
  - Mobility
  - Access
  - Insights

If you are an existing user, refer to the table below to identify the pillar to which the app belongs now and its updated name:

> **Note:** The table excludes **Access** and **Insights** pillars since these pillars do not contain pre-existing apps.

Existing App Name	Pillar	Updated App Name	Description	Navigation
Cluster Manager	Protection	DataProtect	The previous **Cluster Manager** app has been integrated into the **Protection** pillar and it is now known as **DataProtect**. DataProtect allows you to efficiently manage your Cohesity clusters.	1. Log in to Cohesity Data Cloud. 2. Click the **Protection** pillar. 3. Click **DataProtect**.
DataProtect	Protection	DataProtect as a Service	The previous **DataProtect** app has been integrated into the **Protection** pillar and it is now known as **DataProtect as a Service**. You can utilize DataProtect as a Service, an enterprise-grade Backup as a Service (BaaS) solution, to safeguard your critical SaaS, cloud-native, and on-premises data sources.	1. Log in to Cohesity Data Cloud. 2. Click the **Protection** pillar. 3. Click **DataProtect as a Service**.

Existing App Name	Pillar	Updated App Name	Description	Navigation
DataHawk	Security	Security Center	The previous **DataHawk** and **Security Center** apps have been unified and integrated into the **Security** pillar, now collectively known as **Security Center**. Security Center provides you with the capability to monitor the security posture of your Cohesity clusters, perform threat scans, and classify your critical data.	1. Log in to Cohesity Data Cloud. 2. Click the **Security** pillar. 3. Click **Security Center**.
Security Center	Security	Security Center The app name remains unchanged.		
FortKnox	Security	FortKnox The app name remains unchanged.	The **FortKnox** app has been integrated into the **Security** pillar. Enhance your cyber resiliency with FortKnox, a robust SaaS data isolation and recovery solution that ensures the safety of your data by maintaining an immutable copy in a Cohesity-managed cloud vault.	1. Log in to Cohesity Data Cloud. 2. Click the **Security** pillar. 3. Click **FortKnox**.

Existing App Name	Pillar	Updated App Name	Description	Navigation
SiteContinuity	Mobility	SiteContinuity The app name remains unchanged.	The **SiteContinuity** app has been integrated into the **Mobility** pillar. Simplify business continuity and disaster recovery with automated failover and failback orchestration for your mission-critical workloads.	1. Log in to Cohesity Data Cloud. 2. Click the **Mobility** pillar. 3. Click **SiteContinuity**.

- **New Landing Page**: A newly introduced Cohesity Data Cloud landing page now presents a consolidated view of the five pillars. This user-friendly interface enables you to effortlessly navigate into the diverse pillars provided by Cohesity. For more information, see Access SiteContinuity.
- **Application Switcher Changes**: The application switcher has undergone an update to align with the five pillars. Consequently, this modification has brought about changes to the existing navigation. For more information, see Switch Between Apps.
- **Default Landing Page**: When you log in to Cohesity Data Cloud, all five pillars are displayed by default. However, you can set a specific page as the default landing page. For more information, see Set Default Landing Page.
- **User Preferences**: Customize various settings and options to tailor your experience according to your personal preferences. You can modify settings related to your account, user interface, and interactions with the Cohesity platform. For more information, see Set User Preferences.
- **Global Dashboard**: The Global dashboard has been revamped to provide a comprehensive overview of various aspects, including the health of managed clusters, protection status of objects, posture advisor score, discovered threats, and consumption metrics. For more information, see Global Dashboard.
- **Breadcrumbs**: Cohesity Data Cloud introduces support for breadcrumbs, a user-friendly and efficient navigation aid. For more information, see Breadcrumbs.

Alta Copilot

Alta Copilot is an AI-powered interactive assistant designed to offer self-service product support. You can use natural language to request help and guidance on managing your data. Alta Copilot:

- Leverages Retrieval-Augmented Generation (RAG) to enhance response accuracy by retrieving content from Cohesity Product Documentation, Knowledge Base articles, and Technical Guides
- Uses generative AI to deliver contextually relevant answers

Cohesity Data Cloud includes five pillars. Each pillar encompasses a set of features and functionalities tailored to a specific aspect of data management. Each pillar contains one or more specialized apps. Alta Copilot is available across all apps:

Pillar	App
Protection	• DataProtect • DataProtect as a Service
Security	• Security Center • FortKnox
Mobility	SiteContinuity
Access	SmartFiles
Insights	• Data Insights • Platform Insights

The table below lists the documents that Alta Copilot can assist with:

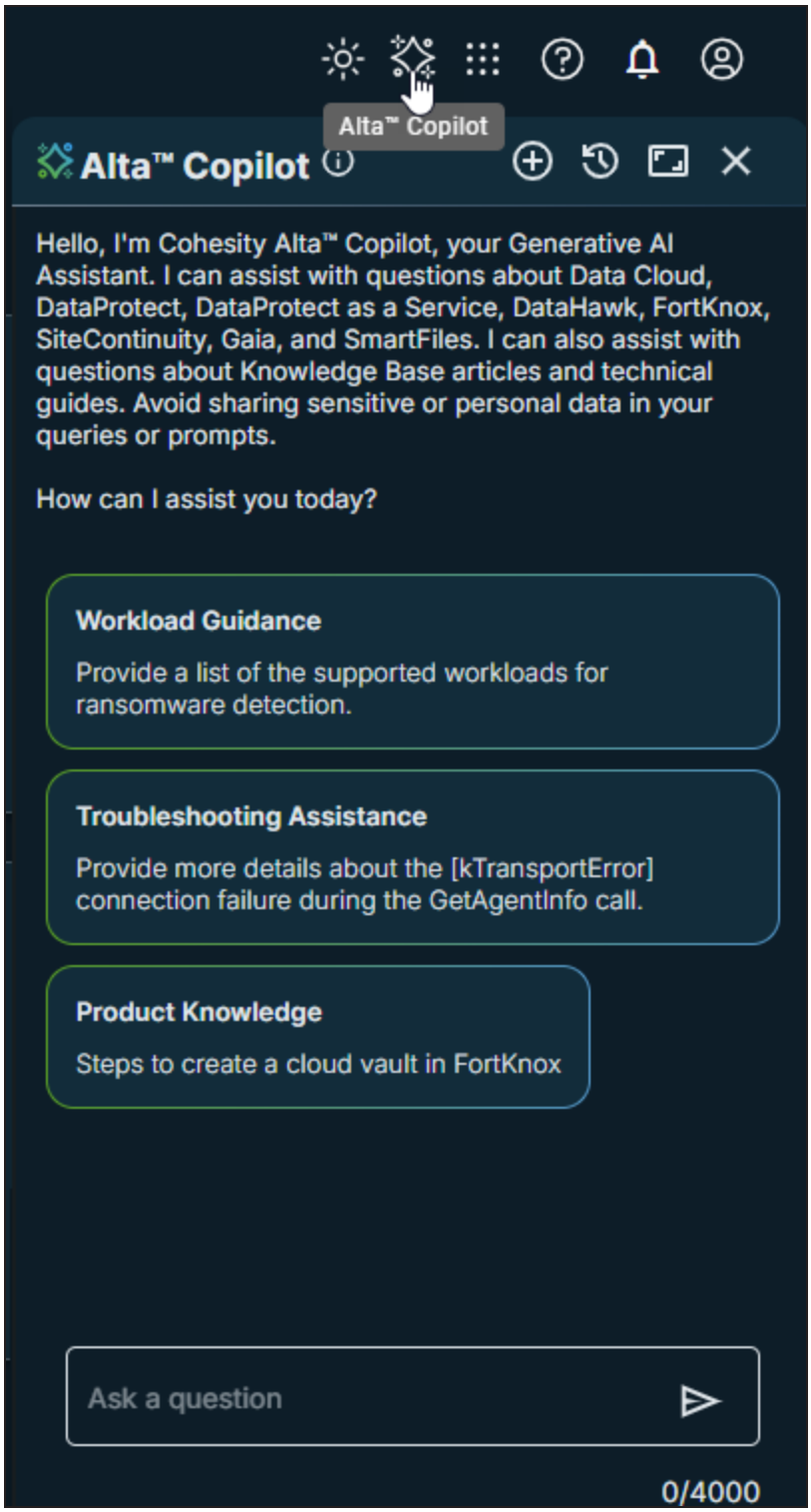
Documentation Category	Documents
Product Documentation	• 6.8.2 • 7.1.2 • 7.2 • 7.2.1 • Helios • DataProtect as a Service • Insights • Security Center • FortKnox • SiteContinuity • SmartFiles • Cluster Setup Guides
Knowledge Base	All knowledge base articles published on the Cohesity Support portal
Technical Guides	All technical guides published on the Cohesity documentation portal

About Alta Copilot User Interface

Alta Copilot integrates seamlessly into Cohesity Data Cloud, offering an intuitive experience that enhances the overall user experience. Accessing Alta Copilot is as simple as clicking an icon in the Cohesity Data Cloud user interface.

To launch Alta Copilot:

1. Log in to Cohesity Data Cloud.
2. Click the Alta Copilot icon:



Alta Copilot opens, and you can either begin typing your question in the chat window or select one of the assistive prompts to help guide your interaction.

The following are the UI options:

Option	Task
	Start a new conversation
	View chat history
	Expand the Alta Copilot user interface
	Collapse the Alta Copilot user interface
	Close the Alta Copilot user interface

Converse With Alta Copilot

Alta Copilot is available to all users of Cohesity Data Cloud. Click the Alta Copilot icon to start a chat.

You can either type your question directly into the chat window or choose from the assistive prompts provided. Alta Copilot processes your query and gives a relevant response.

You can provide feedback by using the thumbs up or thumbs down buttons. Additionally, Alta Copilot includes source references within its responses, allowing you to access relevant resources.

After delivering an answer, Alta Copilot offers assistive prompts to help guide the conversation and keep the conversation focused.

View Chat History

Alta Copilot saves chat interactions. You can review past conversations to keep track of key discussions for future reference or resume a conversation from where it ended. The chat history is organized chronologically and grouped by day(s).

To view the chat history:

1. Log in to Cohesity Data Cloud.
2. Click the Alta Copilot icon:

3. Click  .

   The chat history is displayed.

Rename Chat

You can rename a chat from the **History** section.

To rename a chat:

1. Open the chat history, hover over the chat you want to rename, click on **Actions**, and select **Rename**.
2. In the **Rename chat** dialog, enter the new name for the chat and click **Rename**.

Delete Chat

You can delete a chat from the **History** section.

To delete a chat:

1. Open the chat history, hover over the chat you want to delete, click on **Actions**, and select **Delete**.
2. In the **Delete Chat** dialog, click **Delete** to confirm and remove the chat.

Guidelines for Asking Questions

Cohesity recommends that you adhere to the following guidelines to enhance the effectiveness of questions. As an AI-driven tool, Alta Copilot's ability to provide accurate and relevant answers is directly influenced by the quality of the questions it receives. It is essential to understand the importance of asking the right questions.

- **Be Specific**: The accuracy in delivering accurate answers depends on the specificity of your question. If the question is detailed and specific, Alta Copilot can effectively retrieve relevant documents to provide precise and pertinent information.
- **Provide Context**: Providing context in your question can significantly improve the quality of the answer. The context could be in the form of a product name, product version, alert ID, or error message.
- **Use Keywords**: Including relevant keywords in your question can help the system retrieve the most relevant documents.

- **Use Proper Grammar and Spelling**: Although RAG systems are designed to comprehend and process natural language, their performance is optimized when the question is grammatically correct and free of spelling errors. This ensures that the system accurately understands your question and retrieves the most relevant documents.
- **Ask One Question at a Time**: RAG systems are designed to answer one question at a time. If you have multiple questions, it's best to ask them separately to ensure that each question gets a detailed and accurate answer.
- **Rephrase for Better Results**: If the answer provided is not satisfactory, consider rephrasing your question. Sometimes, asking the same question differently can lead to a more accurate response.

The following are a few examples to help you get started:

- What are the new features introduced in 7.1.2 LTS?
- How do I set up Cohesity SaaS Connectors?
- What are the prerequisites for registering Microsoft 365 sources with DataProtect as a Service?
- How can I get Microsoft 365 Backup Status Overview?
- What is Quorum?
- How can I investigate anomalous objects?
- What are the supported workloads for ransomware detection?
- What are the steps to create a cloud vault in FortKnox?
- How can I configure the vaulting window in FortKnox?
- Can you provide more information about `CE00101034 BootDiskHealth` alert?
- Can you provide more information about `[kTransportError]: Connection failure during the call GetAgentInfo`?

Responsible AI

Cohesity places a strong emphasis on assisting organizations in employing AI responsibly and securely. This approach aligns with the best practices of responsible AI development and deployment. By prioritizing responsibility and security, Cohesity adheres to ethical standards and promotes the responsible use of these powerful technologies.

Alta Copilot prioritizes data security and is committed to adhering to industry standards and best practices for data security, ensuring compliance with relevant regulations and certifications.

Prerequisites

Ensure your infrastructure aligns with the following prerequisites. These requirements are essential for a seamless setup and utilization of SiteContinuity's disaster recovery features:

- Requirements
- Supported VMware Versions
- Firewall Ports
- Considerations
- Set Up Primary and DR Cohesity Clusters
- Connect Clusters to Helios
- Persona-Based Approach

Requirements

To orchestrate DR for SiteContinuity, you require the following infrastructure:

Requirement	Description
System Requirements	
Cluster Requirements	Supported Cohesity software versions are: • **Primary site**: A minimum of a three-node cluster, either physical or virtual edition, running version 7.1 or later is required. • **DR site**: A minimum of a three-node cluster, either physical or virtual edition, running version 7.1 or later is required. • **Virtual Edition**: See the Setup Guide for specifications. > **Note:** SiteContinuity is not supported on single-node clusters (ROBO), regardless of whether they are physical or virtual edition.
VMware Requirements	For the list of VMware vCenter versions SiteContinuity supports, see Supported VMware Versions.
CDP Requirements for VMware vCenter	If you are enabling Continuous Data Protection (CDP) for 15-minute RPO, then the VMware vCenter must meet some additional requirements. For more information, see CDP Requirements for VMware vCenter.

Requirement	Description
Minimum Permissions	
VMware vCenter-Related Permissions	For privileges, you need to protect the VMware VMs on the Cohesity cluster, see VMware vCenter Permissions.
CDP-Related Permissions	For CDP, in addition to the VMware vCenter Permissions, you also require CDP related permissions.
Firewall Ports	Ensure the Firewall Ports are open for communication between the primary Cohesity cluster and the DR Cohesity cluster

Supported VMware Versions

To following table lists the supported VMware vCenter versions for SiteContinuity:

vCenter, vSphere, ESXi Version	Virtual Machine Hardware	7.1.2	7.1.1	7.1
vSphere 8.0 U2	9, 10, 11, 13, 14, 15, 17, 18, 19, 20	✓	✓	✓
vSphere 8.0 U1	9, 10, 11, 13, 14, 15, 17, 18, 19, 20	✓	✓	✓
vSphere 8.0	9, 10, 11, 13, 14, 15, 17, 18, 19, 20	✓	✓	✓
vSphere 7.0 U3	9, 10, 11, 13, 14, 15, 17, 18, 19	✓	✓	✓
vSphere 7.0 U2	9, 10, 11, 13, 14, 15, 17, 18, 19	✓	✓	✓
vSphere 7.0 U1	9, 10, 11, 13, 14, 15, 17, 18	✓	✓	✓
vSphere 7.0	9, 10, 11, 13, 14, 15, 17	✓	✓	✓
vSphere 6.7 U3	9, 10, 11, 13, 14, 15	✓	✓	✓
vSphere 6.7 U2	9, 10, 11, 13, 14, 15	✓	✓	✓
vSphere 6.7	9, 10, 11, 13, 14	✓	✓	✓

vCenter, vSphere, ESXi Version	Virtual Machine Hardware	7.1.2	7.1.1	7.1
vSphere 6.5	9, 10, 11, 13	✓	✓	✓

Firewall Ports

Ensure the following ports are open for communication between the primary Cohesity cluster and the target Cohesity cluster:

Ports	Source	Target	Direction (From Node)	Network Protocol	Usage Notes	Type of Traffic
443	Cohesity cluster	VMware vCenter Disaster Recovery Cluster Remote Access Cluster	Bidirectional	TCP	Required for replication. Required for remote access to the Cluster.	Backup and Recovery Replication
11111	Cohesity cluster	Disaster Recovery Cluster	Bidirectional	TCP	I/O Operations Service	Backup and Recovery Replication Management
11114	Cohesity cluster	Cohesity cluster	Inbound	TCP	Replication Service	
24444	Cohesity cluster	Disaster Recovery Cluster	Inbound	TCP	Continuous Replication Management	Continuous Replication Management

Considerations

Review and understand the following considerations:

- For VMs with multiple NICs, IP address customization can only be applied to one of the NICs at the time of Failover.
- If you are enabling Continuous Data Protection (CDP), remember:

- If the timestamp on the Cohesity cluster and the workload VM are not in sync, then the CDP protection window displayed in the Cohesity cluster will be inaccurate.
- You can select point-in-time (PIT) restore only for individual VMs and not for a Protection Group.

Set Up Primary and DR Cohesity Clusters

In SiteContinuity, a Cohesity cluster is designated as a site and mapped to a specific location to help with subsequent DR operations. For more details, see Sites.

Before setting up disaster recovery in SiteContinuity, identify:

- **Primary Cohesity clusters** that will protect your applications. When setting up disaster recovery in SiteContinuity, you will need to add these clusters as primary sites.
- **Secondary Cohesity clusters** to which you want to replicate the applications in the event of a disaster. These clusters will act as secondary sites, also known as DR sites. When setting up disaster recovery in SiteContinuity, you will need to add these clusters as DR sites.

After identifying the clusters, complete the following configurations in the Cohesity cluster:

Step	Description
Step 1:Meet Requirements	Ensure your primary Cohesity cluster and DR Cohesity cluster meet the requirements for disaster recovery in SiteContinuity.
Step 2:Create Backup Admin	Create a Backup Admin who will only have access to the local Cohesity cluster and not Helios or SiteContinuity. A Backup Admin's privileges are restricted to setting up local Cohesity cluster, creating, modifying, deleting Protection Groups and policies, and deleting runs, among other protection tasks. **Note:** You will subsequently create a DR Admin (in Helios) with the privileges to perform any DR operation in SiteContinuity. For more details, see Persona-Based Approach. To create a Backup Admin: 1. In the local Cohesity cluster, create a custom role with Data Protection privilege. 2. Add a local user and assign the newly created custom role. **Important:** As a Backup Admin, complete steps **3** to **5**.

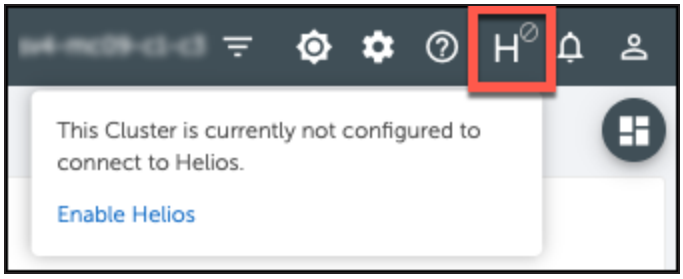
Step	Description
Step 3: Register VMware vCenter server as a source	Register separate VMware vCenter servers as a source with the primary and DR Cohesity cluster. For details on how to register a vCenter server, see Register or Edit a Hypervisor Source.
Step 4:Protect the VMs	In the primary Cohesity cluster, add the critical VMs to a Protection Group and start the protection runs. You need successful backups of the VMs in the primary Cohesity cluster to establish replication between the primary and DR Cohesity clusters. For details on how to set up protection of VMs in Cohesity clusters, see Add or Edit a Protection Group for Virtual Servers.
Step 5:Establish Replication	Set up replication between the primary and DR Cohesity clusters. For details on how to set up replication, see Create a Connection to the Remote Cohesity Cluster. Replication is successfully established when the Protection Group on the primary Cohesity cluster is actively capturing snapshots of VMs and replicating them to the DR or remote Cohesity cluster.

Connect Clusters to Helios

To manage your clusters in Helios, you must connect your clusters to Helios.

To connect a Cohesity cluster to Helios:

1. Sign in to the cluster that you want to connect to Helios.
2. In the Cohesity Dashboard, as a user with Admin privileges, click the Helios icon in the upper right corner and click **Enable Helios**.



   The Helios page is displayed.
3. **Connect to Helios**—Turn on the **Enable** toggle. The Helios portal page is displayed.
4. **Access Permission**—If you want read-only access to the cluster in Helios, turn on the **View Only** toggle. Otherwise, you will have Admin privileges when accessing the cluster in Helios.
5. Enter your Cohesity Support Portal credentials.
6. If this is your first time signing in to Helios, review and accept the End User License Agreement.
7. The cluster attempts to connect to Helios. A message indicates the connection status.

- If the connection is successful, you can optionally click the **Manage this Cluster from Helios** link in the message to verify access to Helios.
- If the connection fails, make sure you have an internet connection and try to connect again.

When the cluster is connected to Helios, a green check mark  is displayed in Helios icon in the top right corner of the Cohesity Dashboard.

Repeat this procedure on each cluster that you want connected to Helios.

> **Note:** Cohesity establishes connections with Helios for:
>
> - **Management and Reporting**: Traffic is enabled when a Cohesity cluster is registered with Helios. Traffic is persistent and bi-directional.
> - **Proactive monitoring**: Traffic is enabled by default and is unidirectional from the Cohesity cluster to Helios. Minimal data is sent every 15 minutes.

For more information about managing clusters, see Manage Cluster Connections.

Persona-Based Approach

SiteContinuity uses a persona-based approach and the roles are segregated according to the responsibilities. By segregating roles, SiteContinuity helps organizations streamline workflows and effectively manage both data protection and disaster recovery processes.

Cohesity recommends that you create custom administrator roles with specific privileges:

Backup Admin	DR Admin
Backup Admin roles are created in the Cohesity clusters when setting up primary and DR Cohesity clusters. For more information, Set Up Primary and DR Cohesity Clusters.	DR Admin roles are created in Helios before setting up disaster recovery workflows in SiteContinuity. For more information, see Custom Roles.
Backup Admins are assigned the Data Protection privilege.	DR Admins are assigned the Manage SiteContinuity privilege.
A Backup Admin's privileges are restricted to setting up local Cohesity clusters, creating, modifying, deleting Protection Groups and policies, and deleting runs, among other data protection tasks.	A DR Admin's privileges are limited to all the DR tasks within SiteContinuity.

Backup Admin	DR Admin
Backup Admins cannot access Helios or SiteContinuity or perform any DR tasks.	DR Admins cannot access the Cohesity clusters or perform any of the data protection tasks that a Backup Admin can.

Get Started

After completing the initial setup, complete the following essential steps to create a comprehensive DR plan for automated disaster recovery of VMware VMs:

- Sign In to Helios
- Access SiteContinuity
- Manage Users and Roles
- Add Sites

Sign In to Helios

Once clusters are connected to Helios, you can sign in to Helios to manage them.

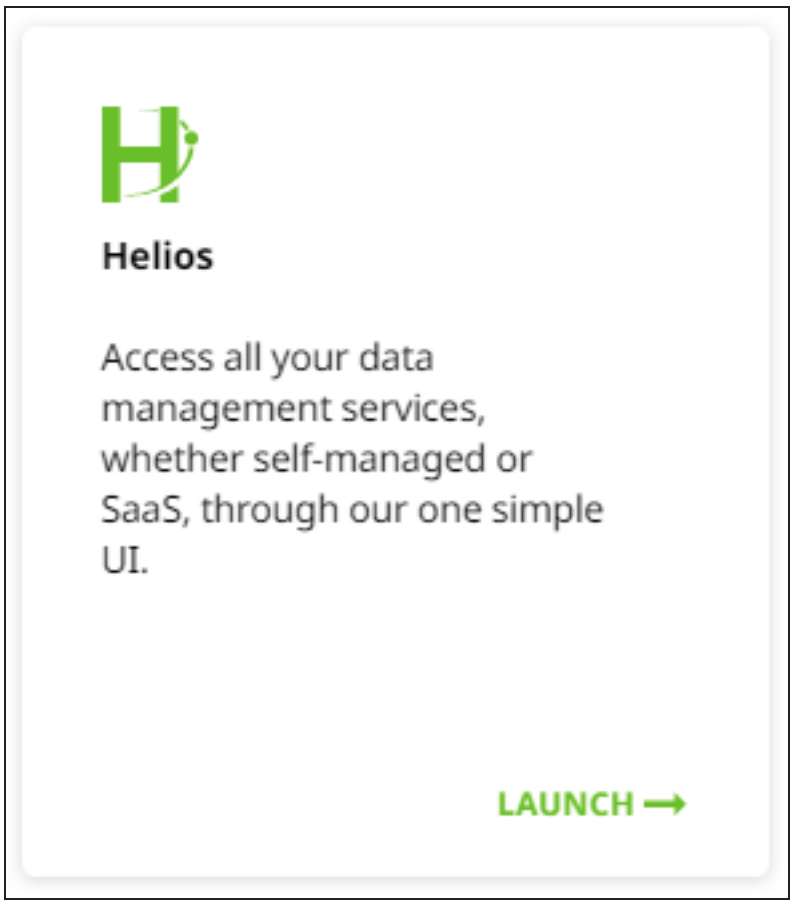
You must sign in to Helios through MyCohesity. MyCohesity is a secure, single sign-on (SSO) portal that provides fast and easy access to all of your Cohesity resources. If you do not have a MyCohesity account, sign up for an account to access all your Cohesity resources from a single dashboard. For more information about MyCohesity, review this page.

To sign in to Helios:

1. Go to the MyCohesity website.
2. Enter your MyCohesity username and password and click **Log in**.

> **Note:** The MyCohesity homepage displays all tiles when you are not logged in. When you log in, you can only see the tiles you are allowed to access. If you do not see a tile, you do not have access to that resource. For more information, see this knowledge base article.

3. On the **Helios** tile, click **Launch**:



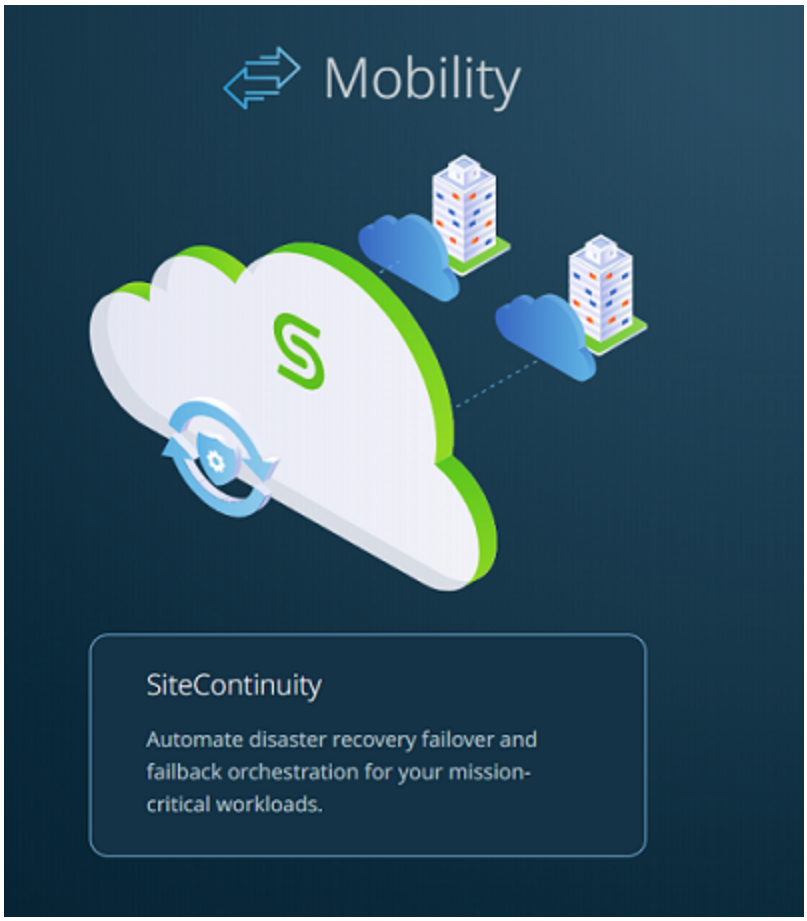
Access SiteContinuity

To access Cohesity SiteContinuity, you'll need the Helios username and the password you set when you activated your Cohesity Data Cloud account. You can check the welcome email or contact your sales representative for the Helios credentials.

To navigate to SiteContinuity:

1. Log in to Helios.
2. On the **Cohesity Data Cloud** landing page, click **Mobility**:

3. On the **Mobility** page, click **SiteContinuity**:



Get to Know the SiteContinuity Interface

The SiteContinuity interface provides the following options:

- The SiteContinuity Dashboard provides stats on the DR plans, DR Activity, Sites, and more.
- On the left of the SiteContinuity interface, the menu lists the pages that enable you to create the DR plan, manage the SiteContinuity resources, and monitor the health of your DR process.
- The following icons are displayed in the upper-right corner of the SiteContinuity interface:
  - User-account icon () which helps you see the user currently logged in to Helios and log out.
  - Dark-mode () icon to enable dark mode.
  - App-selector menu () to navigate between different apps (services) provisioned in your Helios account. For more information, see Switch Between Apps.

Manage Users and Roles

You can create and manage SiteContinuity users and control the permissions assigned to individual users. You can make use of the default roles Helios offers or create custom roles.

SiteContinuity Roles

You can use the default roles that are part of the Helios and create custom roles for SiteContinuity users:

- Default Roles
- Custom Roles

Default Roles

To view the default roles:

1. Click the app-selector menu () and select **Global**.
2. Navigate to **Settings** > **Access Management** and click the **Roles** tab. The names and descriptions of all the default roles are displayed. The default roles relevant to SiteContinuity are:

Roles	Description
Super Admin	Super Admin users have full access to all actions and workflows within a Helios cluster. They can manage other super admins and admins.
Replication	Replication users can set up and replicate data to another cluster.
DR Admin	DR Admin has viewer role privileges and can create and manage DR workflows and associated tasks.
Viewer	Viewer users have read-only access for all workflows within the Cohesity cluster UI.
Self-Service	Self-Service Data Protection users have viewer role privileges. They can manage Clones, Protection Groups, and Policies and create Recover Tasks.
Cohesity	This role allows Cohesity Support to create a Super Admin user for customers. Only Cohesity Support has access to this role, and it is typically used when the customer has lost access to a Super Admin user due to turnover and other events.

Custom Roles

You can create a custom role that defines a specific set of DR privileges. To add a customer role:

1. Click the app-selector menu () and select **Global**.
2. Navigate to **Settings** > **Access Management** and click the **Roles** tab.
3. Click **Add Customer Role**. The **Add Role** page is displayed with some pre-selected **Access Management Privileges**.
4. Under **Role Details**, enter the name and description of the custom role.
5. **SiteContinuity Service** is displayed under **Helios Privileges**. You can provide one of the following privileges to the custom role:
   - **View SiteContinuity**. Selected by default. With this privilege, the user is limited to only accessing and viewing all the resources in SiteContinuity without the ability to make any changes to it.

     > **Note:** To view the Audit Logs in SiteContinuity, an additional Account Management on Helios privilege needs to be selected.

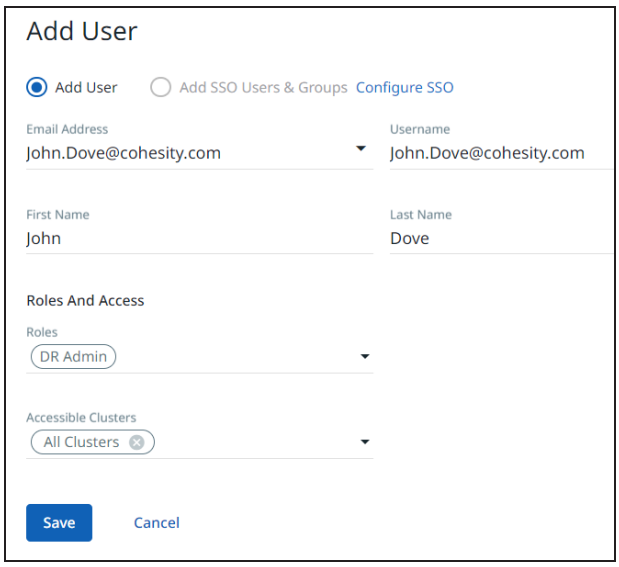
   - **Manage SiteContinuity**. With this privilege, the user can perform all DR activities SiteContinuity. To assign this privilege to the custom role, select **All** or

select **Manage SiteContinuity**.

SiteContinuity Users

To manage user access to your SiteContinuity, Cohesity recommends that you add users. Once you create them, your users can start using SiteContinuity with their logins.

Add Users



To add a user:

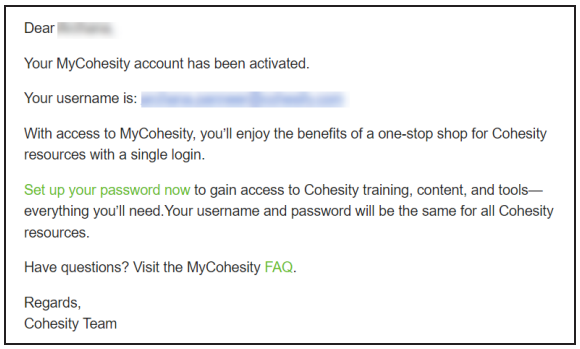
1. Click the app-selector menu ( ) and select **Global**.
2. Navigate to **Settings** > **Access Management** and click the **Users** tab.
3. Click **Add User**.
4. In the dialog, select **Add User** and enter:
    - **Email Address**. The user's email address.
    - **Username**. Same as the Email address. Helios auto-populates this field with the email address entered in the **Email Address** field.
    - **First Name.** The user's first name.
    - **Last Name.** The user's last name.
    - **Roles.** Select a role. For more details, see SiteContinuity Roles.

- **Accessible Clusters**. Displays all the Cohesity clusters registered and actively connected with your Helios account. Select a 7.1 or a later Cohesity cluster that you want the SiteContinuity user to access and manage.

5. Click **Save**.

   The new user is displayed in the **Users** tab on the **Access Management** page.

   The new user receives a welcome email with a link to set up the password. Once the user sets the password, they are redirected to the **MyCohesity** page. From the MyCohesity page, users can sign in to Helios and use SiteContinuity. For details, see Sign In to Helios .


Dear [redacted]

Your MyCohesity account has been activated.

Your username is: [redacted]

With access to MyCohesity, you'll enjoy the benefits of a one-stop shop for Cohesity resources with a single login.

Set up your password now to gain access to Cohesity training, content, and tools—everything you'll need.Your username and password will be the same for all Cohesity resources.

Have questions? Visit the MyCohesity FAQ.

Regards,
Cohesity Team

Manage Users

To manage SiteContinuity users:

1. Click the app-selector menu ( ) and select **Global**.
2. Navigate to **Settings** > **Access Management**.
3. Under the **Users** tab, to change a user's settings, click the Actions menu (⋮) of the user. Tip: You can also manage user details by clicking on the user row to open the **User Details** page.
4. You can select:
   - **Edit.** To update a user's email address, first name, and/or last name.
   - **Delete.** To delete a user from your Helios account.
   - **Reset Password.** To send the user an email with a link to reset their password.

> **Note:** You cannot delete a user who is a Super Admin.

Single Sign-On for SiteContinuity Users

You can now configure Cohesity Data Cloud to use an Identity Provider (IdP), such as Okta, for single sign-on (SSO) access. Cohesity Helios must be added as an application to your IdP, such as Okta. The SSO must then be configured along with the SSO URL and certificate

file in Helios. After the integration, users can sign in to Helios using either the IdP sign-in page or signing in with the SSO link on the Helios login page. The following identity providers are supported:

Identity Provider	Documentation Link
Active Directory Federation Services (AD FS)	Configure SSO with Active Directory Federation Services (AD FS)
Azure	Configure SSO with Azure
Duo Single Sign-on	Integration with Duo for SSO
Ping Identity	Integration with Ping Identity for SSO
Okta Single Sign-on	Configure SSO with Okta

Configure SSO

To enable SSO for SiteContinuity users, you must configure SSO in Helios.

Add SSO Users & Groups

After configuring SSO, you can add SSO users and groups for SiteContinuity.

Add Sites

As the first step to automating disaster recovery using SiteContinuity, add the primary and DR Cohesity clusters as sites. For more information, see Sites.

Before you begin

Register a vCenter server as a source with the Cohesity cluster and connect that cluster to Helios before you add the cluster as a site.

To add a Cohesity cluster as a site:

1. In **SiteContinuity**, navigate to **Infrastructure** > **Sites**.
2. Click **Add Sites**.
3. In the **Add Site** dialog, enter the following:
    - **Site Name**. Enter a name for the new site.
    - **Location**. Enter the location of the new site.
    - **Cluster**. The drop-down list displays all available Cohesity clusters. Select a Cohesity cluster not associated with an existing site from the list.
4. Click **Add**.

The site is created and displayed on the **Sites** page. For details on how to manage the sites on the **Sites** page, see Manage Sites.

Create a DR Application

A DR Application allows you to specify the orchestration order (or the sequence) of the VMs with the ability to insert executable scripts and time delays. For more information, see DR Application.

Before you Begin

To activate DR plans, you need VMs that are being actively backed up by a Protection Group. Before adding the VMs to your DR Application:

- Add the VMs to a Protection Group.
- Initiate protection runs.
- Ensure that the VMs are successfully backed up and replicated to DR cluster.

To create a DR Application:

1. In **SiteContinuity**, navigate to **Infrastructure** > **Applications**.
2. Click **Create DR Application**.
3. Enter a relevant **Application Name**.
4. From the **Site** drop-down, select a primary site.
5. From the **Host** drop-down, select the **VMware vCenter** from which you want to recover VMs.
6. Select **Add VMs** and then **Select VMs**.

   The **VM Selection** dialog displays all the VMs in that vCenter. Click the icon to view the flat list of the VMs. Click the icon to view the hierarchy of the data centers, clusters, ESXi hosts, and folders in that vCenter.
7. To add the VMs, select the checkboxes of the required VMs. You can add more VMs until you have all of the VMs you want in that VM Group.

   Optionally, you can click the search icon and enter the VM name in the **Search** field. As you type, VMs that match your search term appear.

   > **Tip:** Select **Protected by Cohesity** from the **Protection Status** filter to select only the protected VMs.

   > **Note:** You can only add VMs, not part of another DR Application.
8. The **Validate Selected VMs** page displays the VMs you have added, enabling you to evaluate the VM's protection status and RPO. An error icon ( ) highlights the VMs

that are not protected by the Protection Group or have RPOs that do not match the DR plan's RPO. You can do one of the following:

- Click **Back** to navigate to the previous page and unselect the unprotected VMs.
- Click **Done** to continue creating the DR Application. Add unprotected VMs to a Protection Group after the DR Application is created.

9. Click **Done** to create the VM Group.

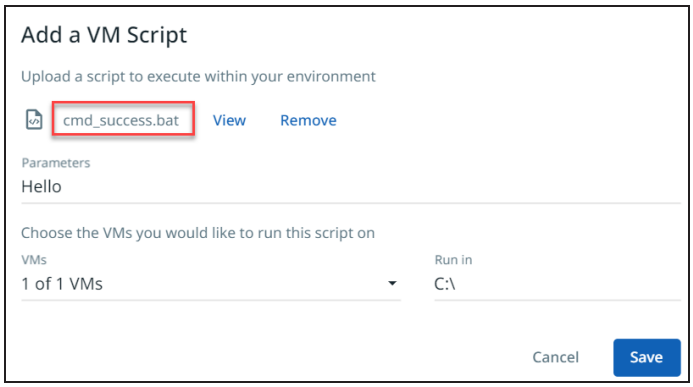
   The new VM Group is displayed on the **Create DR Application** page. To create more VM Groups, repeat steps 6 to 9.

10. (Optional) You can introduce a **Delay** component between any two VM Groups. To add a delay:
    1. Click **Add Delay**.
    2. Enter a number (minimum 1) and select seconds, minutes, or hours from the drop-down.
    3. Drag the **Delay** component and drop it between the VM Groups.
11. (Optional) You can apply scripts to individual VMs.
    - **Add Credentials**. Enter the username and password for the VMs in the VM Group. You can add global credentials that are applicable to all the VMs in the group or add separate credentials for each VM. These credentials are needed to run the scripts on the VMs.
    - **Select a VM script**. This field is enabled only after you add credentials. Click **Upload a Script** to upload a custom script from your local system. You can add arguments to the script by entering the data in the **Parameters** text box. Select the VMs and folder you want the script to run on.

    > **Note:** Cohesity supports Batch scripts for VMs running on Windows OS and Bash scripts for VMs running on Linux OS.

    > **Important:** During the failover of Windows VMs that utilize domain accounts, script execution on the newly failed-over VM may fail if the VM cannot establish connectivity with the Active Directory (AD) domain controller. However, local users will still be able to execute the script. To prevent such issues, ensure that the AD settings on the target VM mirror those of the source VM.

12. Click **Save**:



The new DR Application appears on the **Applications** page. For details on how to manage DR Applications on the **Applications** page, see Manage DR Applications.

Create a DR Plan

A DR plan is a business plan that defines which DR Applications you can effectively bring up and where (DR site) in case of a disaster. For more information, see DR Plan.

The SiteContinuity interface offers a simple three-step workflow to create the DR plan:

- Configure the DR components (source site, target sites, and RPO)
- Configure the DR Application (VM Groups, VMs, scripts, and delays)
- Define the Resource Profile

You can activate the DR plan after you have created the DR Plan. To create a DR Plan:

1. In **SiteContinuity**, navigate to **DR Plans**.
2. On the **Disaster Recovery Plans** page, click **Create Plan**.
3. On the **Create Plans** page, click **Get Started**.
4. On the **Define DR Components** page:
    1. **DR Plan Name**. Enter a unique name for your plan.
    2. **Description**. Enter a brief description of the plan.
    3. Under **Primary Site**, select the source site and host from the **Source Site** and **Source Host** drop-down. If your site is not displayed in the list, click **Add Site**. For details on adding a site, see Add Sites.
    4. Under **DR Site**, select the target site and host from the **Target Site** and **Target Host** drop-down. If your site is not displayed in the list, click **Add Site**. For details on adding a site, see Add Sites.
    5. Configure the RPO in minutes, hours, or days.

        > **Note:** Carefully assess the **Source Site**, **Source Host**, and **Target Site** fields because only the **Target Host** field will be editable once you click **Continue**.

    6. Click **Continue**.
5. On the **Define DR Application** page, you can choose to create a new DR Application or use an existing DR Application. To create a new DR Application, click **Create a New Application** and follow the instructions in the Create a DR Application section.

    If you choose to use an existing DR Application, click **Use an Existing Application** and select a DR Application from the **Applications** drop-down. The primary site to which the DR Application belongs and the associated VM Groups are displayed. You can modify the DR Application by adding VMs, VM Groups, delays, and so on.

6. On the **Define Resource Profile** page, click **Create a Resource Profile**, enter a profile name, and click **Save**.

   It is recommended to create different resource profiles for Test Failover and actual failover with appropriate names for better identification. Example: Test-Failover-Profile and Actual-Failover-Profile. For more information about Resource Profiles, see Resource Profile.

7. Click **Add a Resource Set**.

   The settings you define in the Default Resource Set (in the next two steps) will be applied to all the VMs in your DR Application after the VMs are failed over.

   > **Note:** You need to redefine the Resource Set every time you perform a Test or Actual Failover or Failback because the configurations that are specific to each VM used in the previous operation, such as Static IP or Custom Resource Set, are no longer applicable when working with a new set of VMs in the sites.

8. Select **Infrastructure**. SiteContinuity displays the list of Data Centers available in the vCenter server you defined in the **Target Host** field in 4(d). Select a vCenter from the displayed list. SiteContinuity connects with the selected vCenter server and displays the list of Clusters, Resource Pools, Data Stores, and Networks available in the Data Center in the respective drop-downs. Select from the **Cluster**, **Resource Pool**, **Data Store**, and **Network** fields. For more information on the Default Resource Set, see Default Resource Set.

9. Select **Network**. Add (or update) the IP address settings for the DNS servers of the VMs in the DR Application. The IP address settings The options are:

   - **DHCP**: Select **DHCP** to assign a dynamic DNS server to VMs. Enter the IP address and suffixes for the DNS server.
   - **Static**: Select **Static** to assign a static IP to the VMs. Select **Static**, and then select **Assign IP address** to each VM. SiteContinuity will display the IP Address, Subnet, and Gateway fields for the VMs. Enter the IP address and suffixes of the DNS server for each VM. You can then choose one of the following options:
     - **Use the same subnet and gateway**: If selected, you only need to fill in the **Subnet** and **Gateway** fields of the first VM. The remaining VMs' **Subnet** and **Gateway** fields will be filled automatically when clicked.
     - **Use the same DNS servers and suffixes**: If selected, you only need to fill in the **DNS Server and DNS Suffix** fields for the first VM. The

remaining VMs' **DNS Server** and **DNS Suffix** fields will be filled automatically when clicked.

10. Click **Next**.
11. (Optional) **Custom Resources Set**: Custom Resource sets override the Default Resource Set settings (you defined for all VMs in steps 8 and 9) for specific VMs. You can create as many Custom Resource Sets as needed.
12. Click **Continue**.

    SiteContinuity displays a summary of your DR plan. Click **Back to Disaster Recovery Plans**. Your DR plan appears on the **Disaster Recovery Plans** page.

    For details on how to manage DR Plans on the **Disaster Recovery Plans** page, see Manage DR Plans.

Activate DR Plan

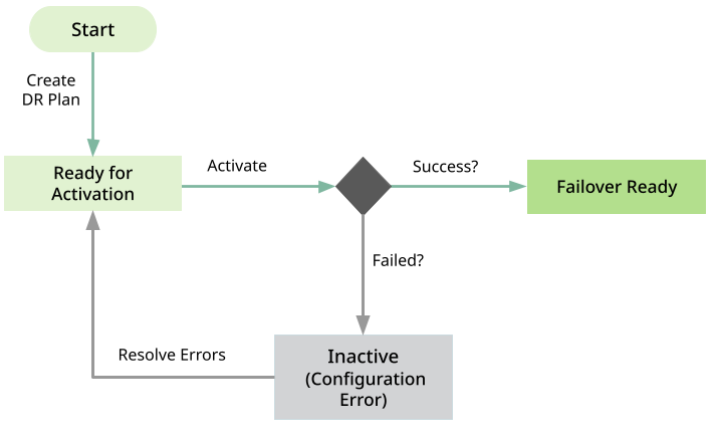
After you create a DR plan, activate the DR plan to test the failover or perform an actual failover.

To activate the DR plan:

1. In **SiteContinuity**, navigate to **DR Plans**.
2. Click the Actions menu (⋮) for the DR plan and select **Activate**.

What's Next > If the activation is successful and your DR plan is in **Failover Ready** state, you can click the Actions menu (⋮) corresponding to the DR plan on the **DR Plans** page and perform the following tasks:

- Test Failover
- Actual Failover

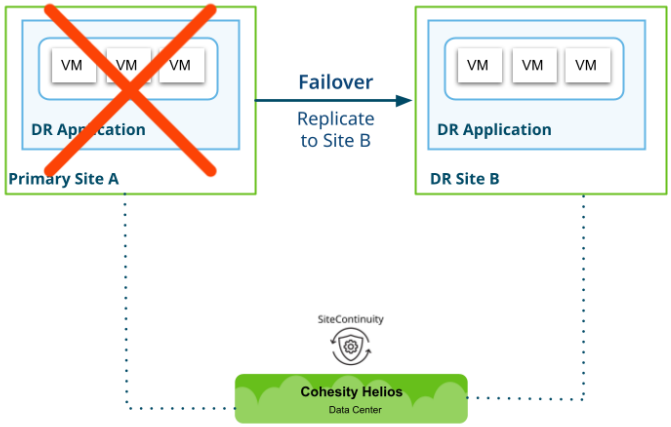


If the activation fails, the DR plan's status transitions to the **Inactive** state. To explore possible causes and resolve the error, see the Troubleshooting section.

Activating the DR plan is a one-time process. Once successfully activated, you can reuse the DR plan to test or perform actual failovers and failbacks any number of times. For all subsequent test failovers or actual failovers, prepare the DR plan before each failover. Similarly, for all subsequent test failbacks or actual failbacks, prepare the DR plan before each failback.

Failover Operations

Failover is the process of bringing up mission-critical and business-critical applications from a primary site to a DR site when the primary system fails due to a disaster. When you initiate a failover, SiteContinuity migrates applications from the primary site to the DR site. You can choose a specific snapshot for VADP backups or point-in-time recovery for Continuous Data Protection backups for the failover. Once migrated, SiteContinuity brings the VM online and to a fully operational state.

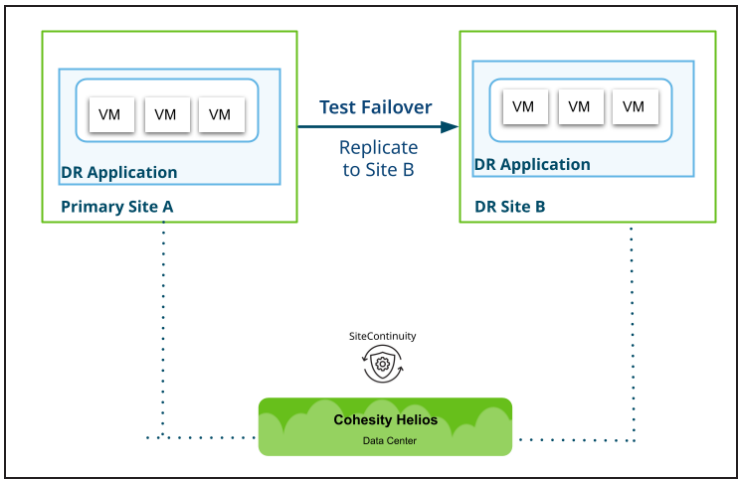


Before you begin

To perform a Test Failover or Failover, you must have an active DR plan that is fully defined, including all DR components, DR applications, and Resource Profiles. For more information, see Create a DR Plan.

Test Failover

As a best practice, regularly test and update your DR plan to ensure that it is effective in the event of an actual disaster. Testing involves checking if the DR plan works as expected and updating the DR plan with any changes that may have occurred since the last failover. During a **Test Failover**, the application is failed over to the DR site without affecting the VMs on the primary site. Once the testing is complete, you can tear down resources created during the Test Failover. Cohesity recommends initiating a Test Failover in an isolated network (with no network reachable route to the source) by configuring the resource profile appropriately.

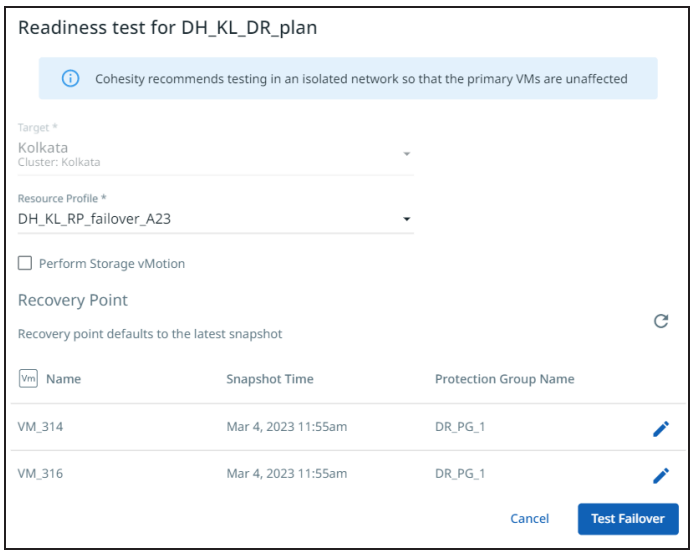


> **Note:** Cohesity recommends initiating a Test Failover in an isolated network (with no network reachable route to the source) so that the primary VMs are unaffected.

Initiate Test Failover

To perform a Test Failover:

1. In **SiteContinuity**, select **DR Plans**.
2. In the **Disaster Recovery Plans** page, choose a DR Plan for testing the failover. A DR Plan must be in the **Failover Ready** state to test the failover.
3. Click the Actions menu (⋮) of the DR plan, and select **Test Failover**. The **Readiness Test** page displays the target DR site and the target Cohesity cluster:



4. From the **Resource Profile** drop-down, select a Resource Profile.

5. (Optional) If you want to test the failover of the VMs and their disks from the source to the target datastore when the VMs are running, select **Perform Storage vMotion**.
6. For recovery, the latest snapshot is used by default. Verify the displayed snapshots or click **Edit** to choose a different snapshot, and click **Apply**.
7. Click **Test Failover**.

On the **Disaster Recovery Plans** page, the **Checks** column displays a beaker icon that indicates the result of the most recent Test Failover or Test Failback. When you click **Test Failover**, the Test Failover starts and shows a progress symbol on the icon (), signifying that the Test Failover is underway.

Validate Test Failover

To validate a test failover:

1. Log in to the DR vCenter.
2. Check if the VM instances come up in the order defined in your DR plan.
3. Confirm that the allocated resources for each VM are correct. Additionally, verify that the network configurations, including IP addresses and connectivity settings, match the intended setup.
4. If an isolated network is used, test the accessibility of the VMs within this network. Ensure that the VMs can communicate with each other as intended.
5. Test the applications hosted on the recovered VMs. Verify that the applications function as expected and can access necessary resources and services.

By following these steps, you can effectively validate the test failover, ensuring that your applications and systems are ready for any actual DR scenario.

Next Steps

If the Test Failover was successful and the beaker icon displays a green tick (), you can click the Actions menu (⋮) corresponding to the DR plan and perform the following tasks:

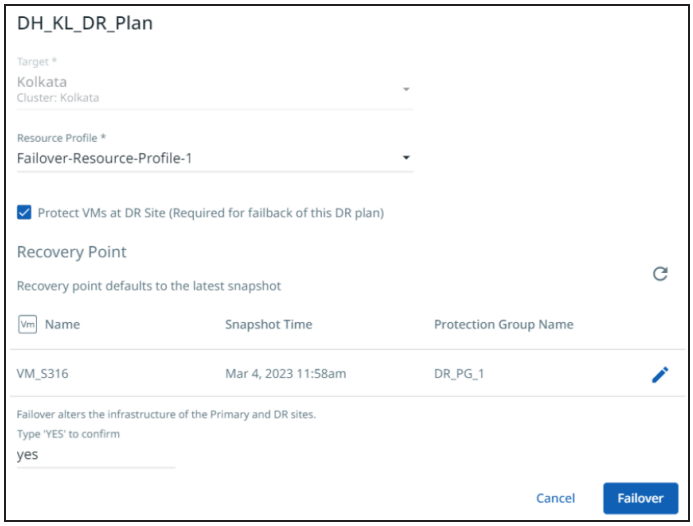
- Repeat Test Failover
- Failover
- Teardown

If the Test Failover fails, the beaker icon shows an error symbol (). Click the icon to see the error message. To explore possible causes and resolve the error, see the Troubleshooting section.

Failover

To perform an actual failover:

1. In **SiteContinuity**, navigate to **DR Plans**.
2. In the **Disaster Recovery Plans** page, choose a DR Plan for failover. A DR Plan must be in the **Failover Ready** state for a failover.
3. Click the Actions menu (⋮) of the DR plan, and select **Failover**. The **Failover** page displays the target DR site and the target Cohesity cluster:



4. From the **Resource Profile** drop-down, select a Resource Profile.
5. If you plan to fail back the DR plan after the failover, select **Protect VMs at DR Site**. If this option is selected, when the failover completes, SiteContinuity enables the protection of the VMs (defined in your DR plan) newly created on the DR site.
6. For recovery, the latest snapshot is used by default. Verify the displayed snapshot or click **Edit** to choose a different snapshot, and click **Apply**.
7. Failovers migrate the DR Application to the DR site. Enter **YES** to confirm and click **Failover**.

Validate Failover

To validate the failover:

1. Log into the DR vCenter:
2. Ensure that the VM instances come up in the order defined in the DR plan.
3. Confirm that the allocated resources and network configurations for each VM are correct.

4. Conduct tests on applications running within the VMs. Ensure they function as expected and validate their connectivity and performance.
5. Navigate to the DR Cohesity cluster and validate that the Protection Group created as part of the failover is active.

By following these steps, you can ensure a comprehensive validation of the failover process, covering both VM-level functionality and data protection integrity in the DR environment.

Next Steps

If the Failover is successful and your DR plan is in **Failover Complete** state, you can click the Actions menu (⋮) corresponding to the DR plan in the DR Plans page and prepare for failback to perform a Test Failback or Failback.

If the Failover is partially successful, the DR plan's status transitions to the **Failover Failed** state but still gives the option to Force Finish to mark the partial success a complete success.

If the Failover fails, the DR plan's status transitions to the **Failover Failed** state. To explore possible causes and resolve the error, see the Troubleshooting section.

Prepare for Failback

After the first successful test failover or actual failover, a DR Plan transitions to the **Failover Complete** state, which means that the VMs have successfully failed over, and are now operational in the DR site. To failback the DR plan in this state, you need to prepare the DR plan for failback.

Prerequisites

- Ensure that the DR plan is active and in the **Failover Complete** state.
- Create Resource Profiles. For more information, see Add the Failback Resource Set to DR Plan.

Add the Failback Resource Set to DR Plan

To add a Resource Set to a DR plan before failback:

1. In **SiteContinuity**, navigate to **DR Plans**.
2. In the **Disaster Recovery Plans** page, select the Actions menu (⋮) of the DR plan you want to failback and select **Edit**.
3. Select the **Resource Group** tab.
4. To add a default Resource Set, click **Add a Resource Set**.

   > **Note:** The settings you define in the Default Resource Set (in the next two steps) will be applied to all the VMs in your DR Application after the VMs are failed over.

5. Select **Infrastructure**. SiteContinuity displays the list of Data Centers available in the vCenter server you defined in the **Target Host** field. Select a vCenter from the displayed list. SiteContinuity connects with the selected vCenter server and displays the list of Clusters, Resource Pools, Data Stores, and Networks available in the Data Center in the respective dropdowns. Select the Cluster, Resource Pool, Data Store, and Network. For more information on the Default Resource Set, see Default Resource Set.
6. Select **Network**. You configure (or update) the IP settings for DNS servers for the VMs in the DR Application. The options are:
   1. **DHCP**: Assigns a dynamic IP address to the DNS server. You can select **DHCP** and then enter the IP address and suffixes for the DNS server.

2. **Static**: Assigns a static IP address to the DNS server that connects to each VM. Select **Static**, and then select **Assign IP address to each VM**. SiteContinuity will display the IP Address, Subnet, and Gateway of the VMs. Enter the IP address and suffixes of the DNS server for each VM. You can then choose one of the following options:
    - **Use the same subnet and gateway**: If selected, you only need to fill in the **Subnet** and **Gateway** fields of the first VM. The remaining VMs' **Subnet** and **Gateway** fields will be filled automatically when clicked.
    - **Use the same DNS servers and suffixes**: If selected, you only need to fill in the **DNS Server** and **DNS Suffix** fields for the first VM. The remaining VMs' **DNS Server** and **DNS Suffix** fields will be filled automatically when clicked.

7. Click **Next**.

   The new default resource set is displayed on the **Define Resource Profile** page and is applied to all the VMs in your DR Application. To create more Resource Profiles, repeat steps 4 to 6.

8. (Optional) **Custom Resources Set**: Custom Resource sets override the Default Resource Set settings (you defined for all VMs in steps 5 and 6) for specific VMs. You can create and apply multiple custom resource sets on individual VMs or a collection of VMs.

9. Click **Save**.

   The Resource Profile is saved in the DR plan.

Initiate Prepare for Failback

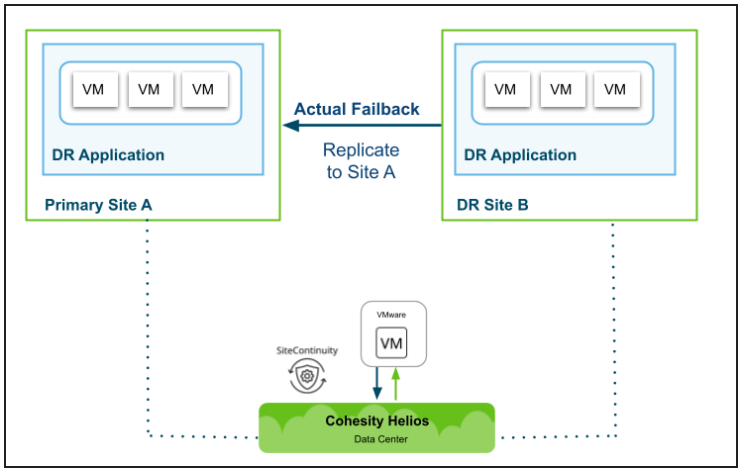
To prepare a DR plan for failback:

1. In **SiteContinuity**, navigate to **DR Plans**.
2. Click the Actions menu (⋮) of the DR plan and select **Prepare for Failback**.

   The DR plan transitions from **Prepare for Failback In Progress** to **Failback Ready** state.

Failback Operations

Failback is performed when the primary site is operational again after a disaster caused the failover. When you initiate a failback, SiteContinuity migrates the applications from the DR site back to the primary site. You can choose a specific snapshot of VADP backups or point-in-time recovery for CDP backups for the failback. Once migrated, SiteContinuity brings the VM online, effectively restoring them to a fully operational state.



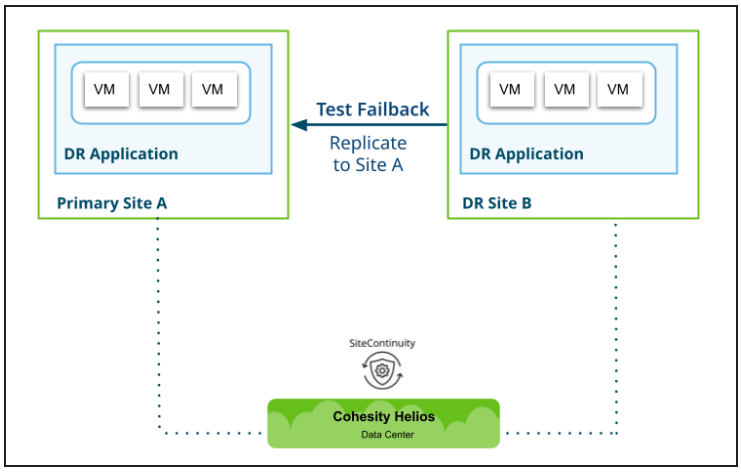
Before you begin

Before you attempt a Test Failback or Failback:

- Establish reverse replication. To establish reverse replication between the DR cluster and the primary cluster, follow the same steps that were taken to establish replication between the primary and DR clusters, except this time, the roles of the primary and DR clusters are reversed and the primary cluster is the remote cluster. For more information, see Establish Replication.
- Create a Resource Profile that will be applied to the VMs once they are failed back to the primary cluster. For more information, see Add the Failback Resource Set to DR Plan.
- To fail back to a new cluster or site not defined in the DR plan, delete DR Plans, create a new DR plan with the required cluster, and create a DR Application.

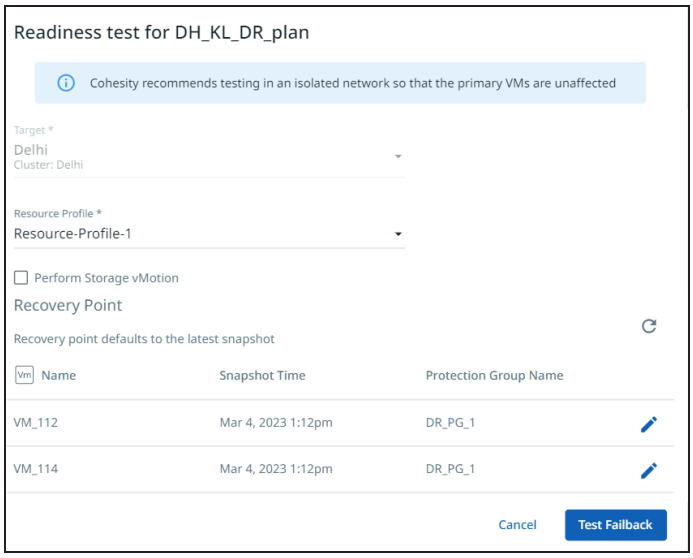
Test Failback

As a best practice, regularly test and update your DR plan to ensure that it is effective in the event of an actual disaster. Testing involves checking if the DR plan works as expected and updating the DR plan with any changes that may have occurred since the last failback. During a Test Failback, the application is failed back to the primary site. Once the testing is complete, you can tear down resources created during the Test Failback.



To test a failback:

1. In **SiteContinuity**, navigate to **DR Plans**.
2. In the **Disaster Recovery Plans** page, choose a DR Plan for testing the failback. A DR Plan must be in the **Failback Ready** state to test a Test Failback.
3. Click the Actions menu (⋮) of the DR plan, and select **Test Failback**. The **Readiness Test** page displays the target DR site and the target Cohesity cluster:



4. From the **Resource Profile** drop-down, select a Resource Profile.
5. (Optional) If you want to fail back the VMs and their disks from the source to the target datastore when the VMs are running, select **Perform Storage vMotion**.
6. For recovery, the latest snapshot is used by default. Verify the displayed snapshots or click **Edit** to choose a different snapshot, and click **Apply**.
7. Click **Test Failback**.

   On the **Disaster Recovery Plans** page, the **Checks** column displays a beaker icon that indicates the result of the most recent Test Failover or Test Failback performed

on the DR plan. When you click **Test Failback**, the **Test Failback** starts and shows a progress symbol on the icon ( ), signifying that the **Test Failback** is underway.

Validate Test Failback

To validate test failback:

1. Log in to the primary vCenter.
2. Ensure that the VM instances come up in the specified order as defined in your DR plan.
3. Verify that the allocated resources and network configurations for each VM are correct.
4. If you have set up an isolated network, test the accessibility of the VMs.
5. Test the functionality of your critical applications to confirm that they are working as expected in the primary environment.

By following these steps, you can ensure that your primary environment is functioning properly and that all VMs and applications are operational.

Next Steps

If the Test Failback was successful and the beaker icon displays a green tick ( ), you can click the Actions menu (⋮) corresponding to the DR plan and perform the following tasks:

- Repeat Test Failback
- Failback
- Teardown

If the Test Failback fails, the beaker icon shows an error symbol ( ). Click the icon to see the error message. To explore possible causes and resolve the error, see the Troubleshooting section.

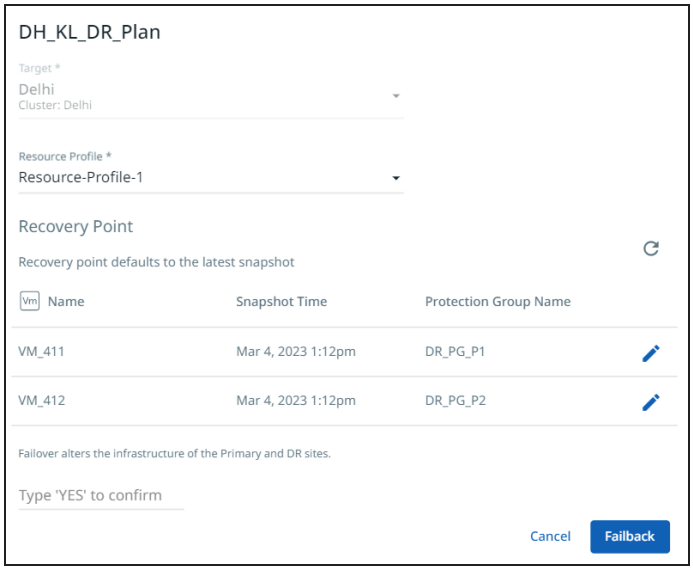
Failback

Failback is the process of returning operations from the DR site back to the primary site.

To perform an actual failback:

1. In **SiteContinuity**, navigate to **DR Plans**.
2. In the **Disaster Recovery Plans** page, choose a DR Plan for failover. A DR Plan must be in the **Failback Ready** state for failback.

3. Click the Actions menu (⋮) of the DR plan, and select **Failback**. The **Failback** page displays the target DR site and the target Cohesity cluster:



4. From the **Resource Profile** drop-down, select a Resource Profile.
5. For recovery, the latest snapshot is always used. Confirm the snapshot, click **Edit**, choose a different one, and click **Apply**.
6. Enter **YES** confirm to confirm and click **Failback**.

Validate Failback

To validate failback:

1. Log in to the DR vCenter.
2. Confirm that the virtual machine instances come up in the specified order as defined in your DR plan.
3. Ensure the allocated resources and network configurations for each VM are correct.
4. Verify the functionality of your critical applications to confirm they are working as expected.
5. Navigate to the primary (DR) Cohesity cluster and validate the Protection Group created as part of the failback process.

Next Steps

If the Failback is successful and your DR plan is in **Failback Complete** state, you can click the Actions menu (⋮) corresponding to the DR plan in the DR Plans page and perform a prepare for failover to then perform a Test Failover or Failover.

If the failover is partially successful, the DR plan's status transitions to the **Failback Failed** state but still gives the option to Force Finish to mark the partial success as a complete success.

If the failover fails, the DR plan's status transitions to the **Failback Failed** state. To explore possible causes and resolve the error, see the Troubleshooting section.

Prepare for Failover

After the first successful test failback or actual failback, a DR Plan transitions to the **Failback Complete** state, meaning that the VMs have successfully failed back and are operational in the primary site. To failover the DR plan in this state, you need to prepare a DR plan for failover.

To prepare a DR plan for failover:

1. In **SiteContinuity**, navigate to **DR Plans**.
2. Click the Actions menu (⋮) of the DR plan and select **Prepare for Failover**.

   The DR plan transitions from **Prepare for Failover In Progress** to **Failover Ready** state.

DR Plan Activities

SiteContinuity supports the following DR plan activities:

- Cancel
- Force Finish
- Teardown

Cancel

To cancel a task that is in progress in a DR Plan:

1. In **SiteContinuity**, navigate to **Activity**.
2. Click on an activity to view the activity's details.
3. Click the Actions menu (⋮) of the task and select **Cancel**.
4. In the confirmation prompt, type **Yes** to confirm.
5. Click **Confirm**.

   The execution status of the DR plan briefly changes to **Canceling** and then to **Canceled**.

Canceling an ongoing operation only stops the operation. Initiate a Teardown to securely remove the resources (such as VMs) and residual data created by a DR operation.

Force Finish

The **Force Finish** option allows you to mark an actual failover or failback process as a successful event if some VMs did not complete the process successfully. Force Finish should only be used if the failed VMs are not critical. Cohesity recommends that you thoroughly assess the impact of the failed VMs on the overall functioning of your virtual infrastructure before marking a partial success as a complete success.

To force finish:

1. In **SiteContinuity**, navigate to **Activity**.
2. Click on an activity to view the activity's details.
3. Click the Actions menu (⋮) of the task and select **Force Finish**.
4. In the confirmation prompt, type **Yes** to confirm.
5. Click **Confirm**.

The partially successful failover or failback is marked as successful and transitions to a **Failover Complete** or **Failback Complete** state, respectively.

If the failed VMs are critical, Teardown the DR plan, resolve the errors, and try again.

Teardown

Tearing down a DR plan after a Test Failover or Test Failback is a recommended practice for clean-up purposes. When you initiate a Teardown, resources such as VMs created during the test are deleted from the site, and any residual data is securely removed. The option to Teardown is displayed for DR tasks in the following states:

- Successful or Failed Test Failover
- Successful or Failed Test Failback
- Failed or Canceled Failover
- Failed or Canceled Failback

To perform a teardown:

1. In **SiteContinuity**, navigate to **Activity**.
2. Click on an activity to view the activity's details.
3. Click the Actions menu (⋮) of the task and select **Teardown**.
4. In the confirmation prompt, type **Yes** to confirm.
5. Click **Teardown**.

The execution status of the DR plan briefly changes to **Tear Down In Progress** and then to **Teardown Complete**. Teardown can only be performed once for a particular DR task.

Tearing down does not change the status of the DR plan.

Validate Teardown

To validate a teardown:

1. Log in to the DR vCenter.
2. Check if the teardown process was successful. Ensure that all the test VM instances have been deleted and removed from the target environment.

Manage Resources

SiteContinuity enables you to effectively administer all the Sites, DR Applications, and DR Plans you have created. The SiteContinuity interface features dedicated pages for each:

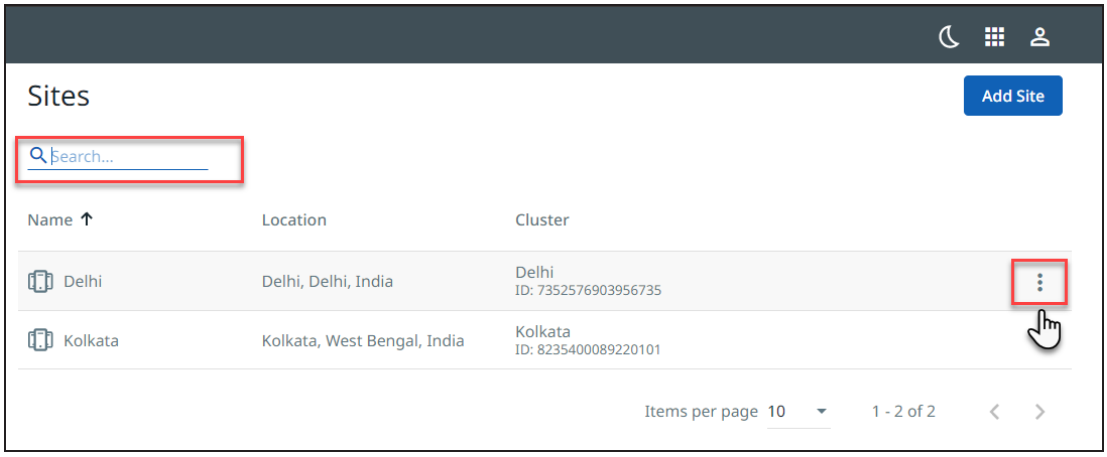
- Manage Sites
- Manage DR Applications
- Manage DR Plans

Manage Sites

The **Sites** page displays all the sites you created in SiteContinuity.

View Sites

To view the **Sites** page, in **SiteContinuity**, navigate to **Infrastructure**> **Sites**.



For each site, the **Sites** page displays:

- **Name**. Name of the site.
- **Location**. The location you entered when you created the site.
- **Cluster**. The name and ID of the cluster the site is mapped to.

Filter Sites

You can click the search icon and enter the site name in the **Search** field. As you type, sites that match your search term appear.

Edit Sites

To edit a site, click the **Actions** menu (⋮) for that site and select **Edit**.

The **Edit Site** page appears with all the components you configured. You can modify the site and save the changes.

Delete Sites

To delete a site:

1. Click the Actions menu (⋮) for that site and select **Delete**.
2. Enter **yes** to confirm the deletion and click **Delete**.

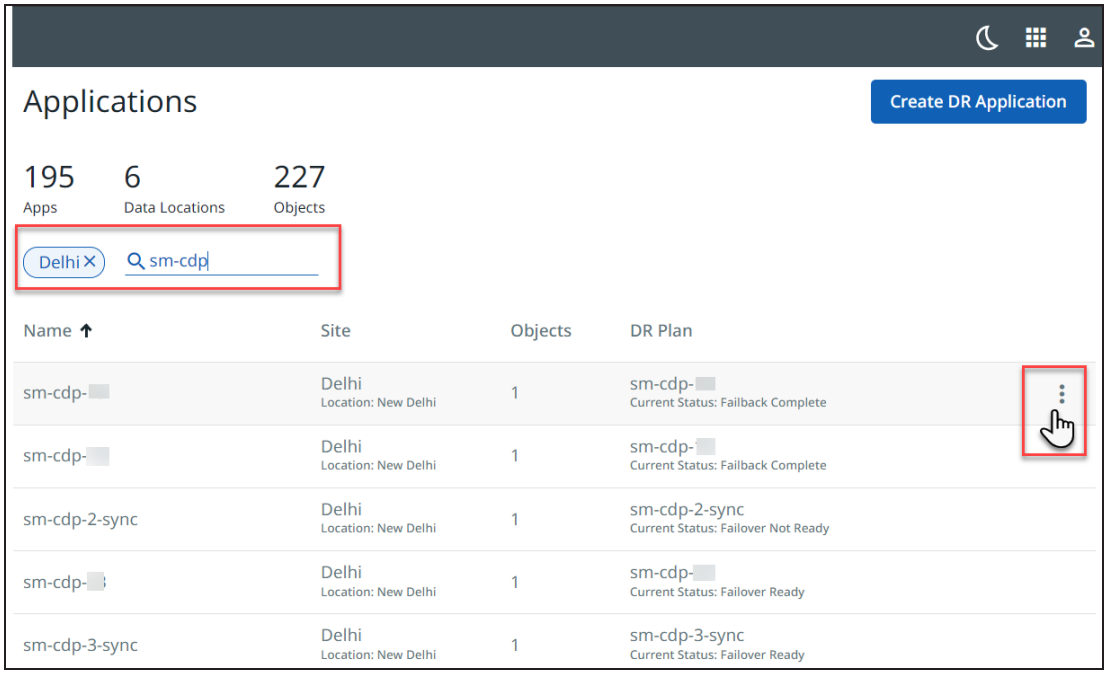
   The site is removed from the **Sites** page.

Manage DR Applications

The **Applications** page displays all the DR Applications you created in SiteContinuity.

View DR Applications

To view the **Applications** page, in **SiteContinuity**, navigate to **Infrastructure**> **Applications**.



For each DR Application, the **Applications** page displays:

- **Name**. Name of the DR Application.
- **Site**. Name of the site (or source of the VMs) the DR Application is currently running on.

- **Objects**. Number of VMs the DR Application contains.
- **DR Plan**. Name and current status of the DR Plan the DR Application is associated with.

Filter DR Applications

The **Applications** page displays the DR Applications you created in SiteContinuity. The **Site** filter helps you display only the DR Applications of the selected site. You can click the search icon and enter the DR Application name in the **Search** field. As you type, DR Applications that match your search term appear.

Edit DR Applications

To delete a DR Application, click the Actions menu (⋮) for that DR Application and select **Edit**. The **Edit DR Application** page of that DR Application appears with all the components you configured. You can modify the DR Application and save the changes.

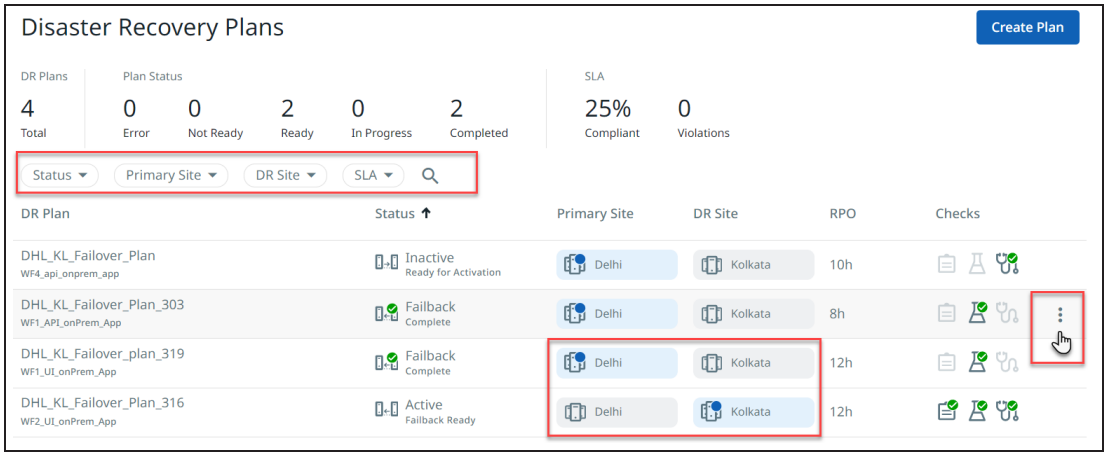
Delete DR Applications

To delete a DR Application, click the Actions menu (⋮) for that DR Application and select **Delete**. In the dialog, enter **YES** to confirm your deletion and click **Delete**.

Manage DR Plans

You can view the DR plans and manage the plans from the **Disaster Recovery Plans** page. In addition to performing tasks such as Activate, Test Failover, Failover, Prepare for Failover, Test Failback, Failback, Prepare for Failback, on DR plans, you can filter, edit, run health checks, cancel, force finish, teardown, and delete DR plans.

Navigate to the **Disaster Recovery Plans** page by selecting **DR Plans** in SiteContinuity.



View the DR Plans List

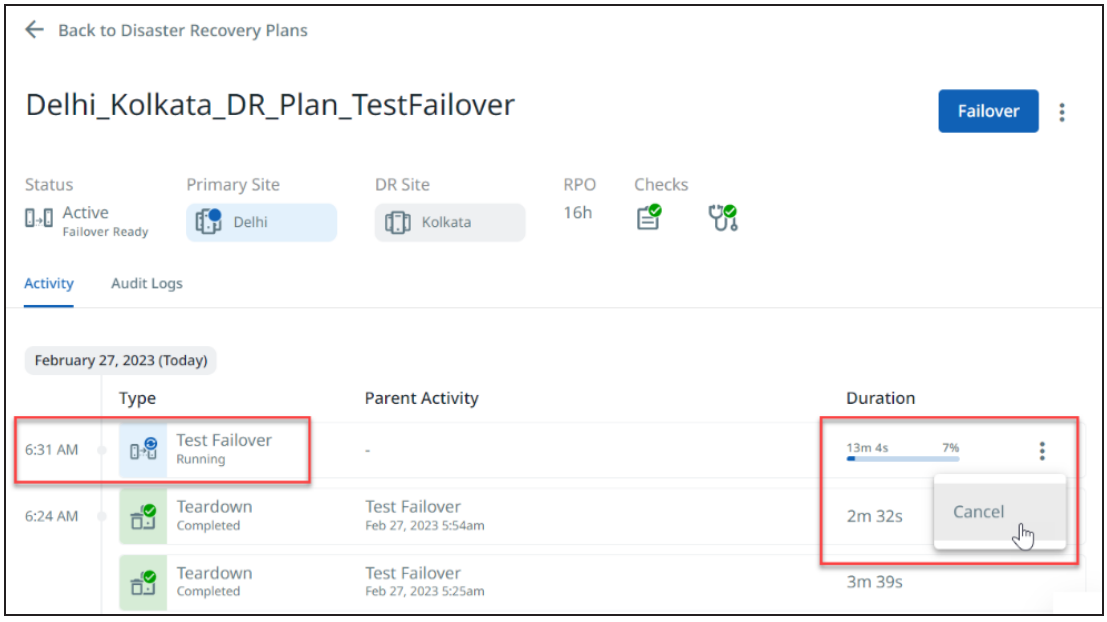
For each DR plan, the page displays:

- **DR Plan**. Name of the DR plan.
- **Status**. The current state of the DR Plan and its status. Example: Active, Failover Ready, Failing over, and Failover Complete. It also indicates configuration errors, if any.
- **Primary Site**. Name of the primary site. The site where the DR Application is currently running is highlighted in blue.
- **DR Site**. Name of the target site. The site where the DR Application is running is highlighted in blue.
- **RPO**. The RPO period configured for the DR plan.
- **Checks**. The three icons display the results of the last health check of the DR plan. For more details on health check, see Run Health Check on a DR Plan.
- **Actions Menu**. Hover over a DR plan row to see that plan's Action menu (⋮) in the right corner.

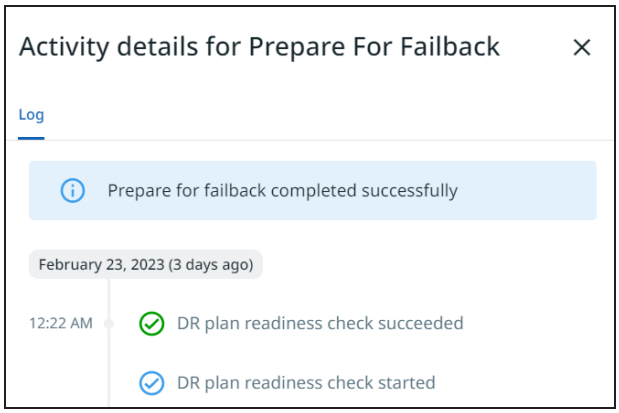
View a DR Plan's Details

You can view all the updates and operations performed on a DR plan since it was created.

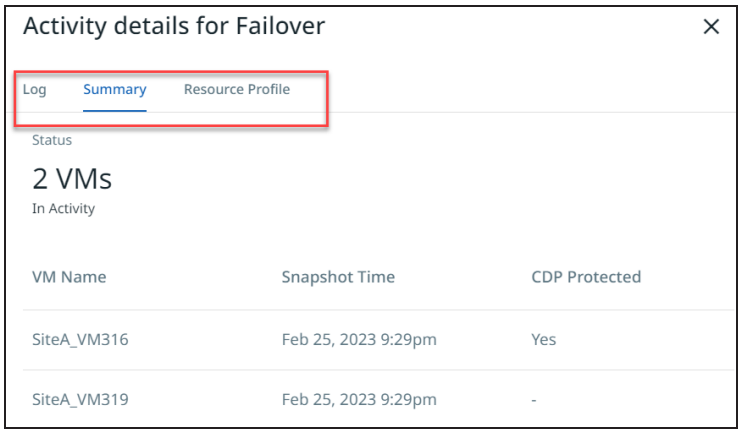
Click the DR plan's name to view a DR plan's **Activity** tab and **Audit Logs** tab. Hover over an activity, and the Action menu (⋮) allows you to cancel, force finish, and teardown that individual activity.



On the **Activity** tab, click on the activity to see the activity log. A blue tick indicates the start of an activity, and a green tick its completion.



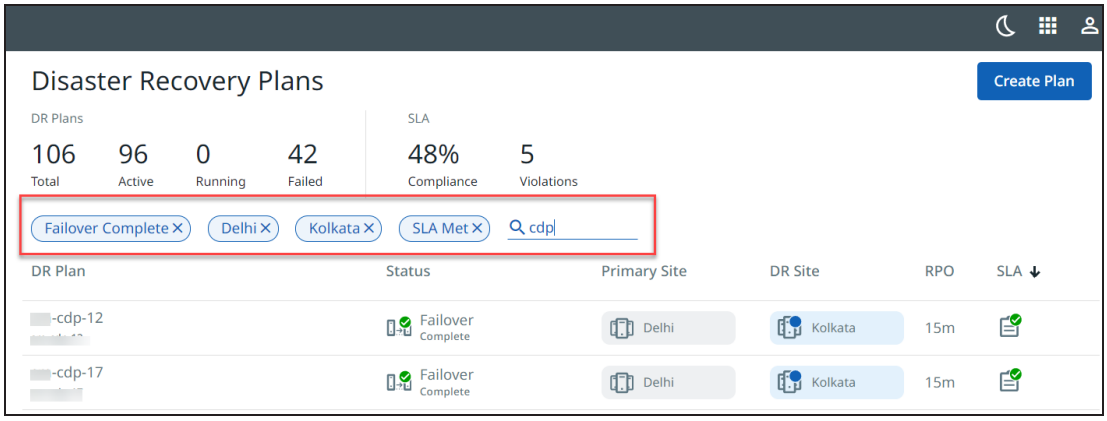
For all activities (other than Activate, Prepare for Failover, and Prepare for Failback), the **Activity Details** page also shows an additional **Summary** tab and a **Resource Profile** tab. The **Summary** tab displays the list of VMs, their last snapshot time, and CDP protection status. The **Resource Profile** tab displays the Resource Profile details.



For more details, see DR Activity and Audit Logs.

Filter DR Plans

The **Disaster Recovery Plans** page displays all the DR plans in SiteContinuity. Filters help you display only the DR plans that match the values you selected.



The filtering options are:

- **Status**. Current status of the plan. Options are Ready for Activation, Failover Not Ready, Failover In Progress, Failover Complete, Failover Failed, and so on.
- **Primary Site**. Filter based on the primary site.
- **DR Site**. Filter based on the target site.
- **SLA**. SLA met, SLA missed.

You can click the search icon and enter the DR Plan name in the Search field. As you type, DR Plans that match your search term appear.

Run Health Check on a DR Plan

After a DR plan is activated, SiteContinuity conducts periodic health checks on a DR plan. These checks involve verifying:

- Replication status between the primary and DR sites specified in the DR plan
- Verifying the connectivity of the primary and DR sites with Helios
- Ensuring that the SLA is being met.

Results of the health check are displayed in the Checks column on the Disaster Recovery Plans page:

- **SLA**: A green tick indicates ( ) SLA is met. A warning symbol ( ) indicates missed SLA.
- **Health Check**: The **Health Check** icon shows the outcome of the last health check.
  - Green tick ( ) indicates the last health check was successful.
  - Error symbol ( ) indicates that the check failed. To explore possible causes and resolve the Health Check error, see the Troubleshooting section.

On-demand Health Check

To instantly start a health check, click the Actions menu (⋮) for that DR plan and select **Health Check**. The health check starts right away and displays a progress symbol ( ), signifying that the health check is underway.

> **Note:** Health checks are available for all DR plans except those in **Ready for Activation**, **Failover Complete**, and **Failback Complete** status.

Edit DR Plans

To edit a DR plan, click the Actions menu (⋮) for that DR plan and select **Edit**.

The **Edit DR Plan** page of that DR plan appears with all the components you configured. You can modify the DR plan and save the changes.

Delete DR Plans

To delete a DR plan:

1. Click the Actions menu (⋮) for that DR plan and select **Delete**.
2. Enter **YES** to confirm the deletion and click **Delete**.

   The DR Plan is removed from the **Disaster Recovery Plans** page.

Monitor DR Activity

SiteContinuity offers the following options to track and manage your DR processes, ensuring complete control and visibility:

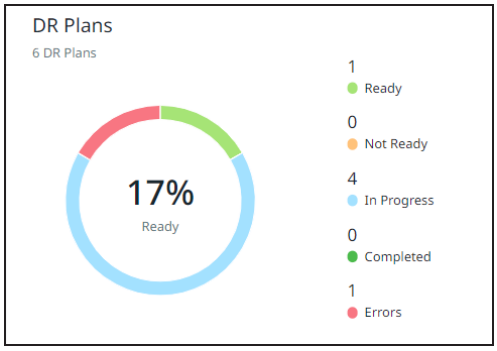
- Dashboard
- DR Activity
- Alerts
- Audit Logs
- Troubleshooting

Dashboard

The panels in the **SiteContinuity Dashboard** provide a summary of the following aspects of your SiteContinuity instance, allowing you to assess the status quickly.

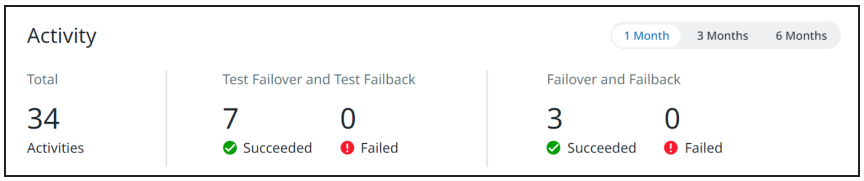
DR Plans Panel

Displays the total number of DR plans you've created in SiteContinuity and the stats on the activation, failovers, and failbacks of the DR plans. The panel displays the number of DR plans that are ready, not ready, and in progress with activation, failover, and failback. The number of DR plans with completed failovers and failbacks is also displayed. The panel also displays the number of DR plans that have not completed the activity due to errors.



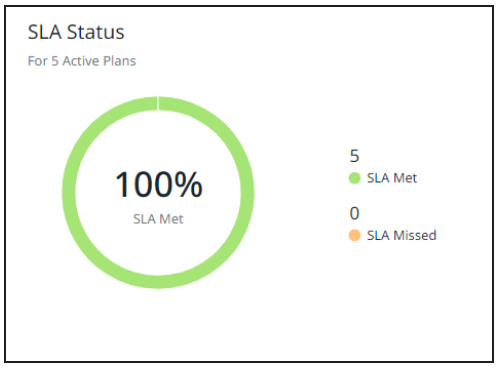
Activity Panel

Displays the number of times the DR Plans were successfully tested and the number of times the tests failed in the last six months. This panel also displays the number of times actual failovers and failbacks succeeded and failed.



SLA Status Panel

Displays the number of active DR Plans that have met and not met the SLAs.

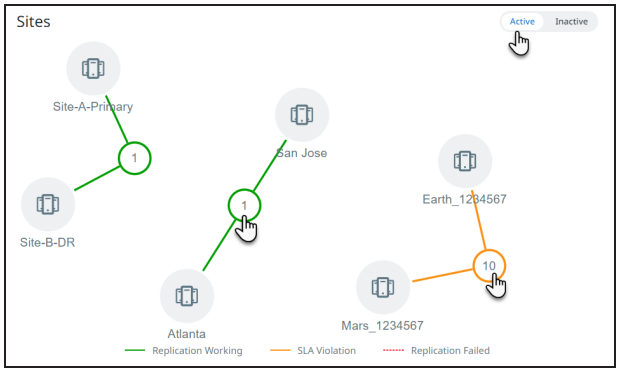


Sites Panel

The **Sites** panel has a tab each for active and inactive sites you have created in SiteContinuity. The **Active** tab displays the mapping between the active sites and the number of DR plans created between each site. The **Inactive** tab displays the inactive sites. The mapping lines' color indicates the DR plans' status:

- **Green**. Indicates that replication is successful between the sites.
- **Yellow**. Indicates that some or all DR plans have missed SLAs.
- **Red**. Indicates that replication has failed between the sites.

Click the number of DR plans to view the list of DR plans. Click the site to see the latest status of the site, the name and ID of the cluster, and the defined geographical location of the site.



DR Activity

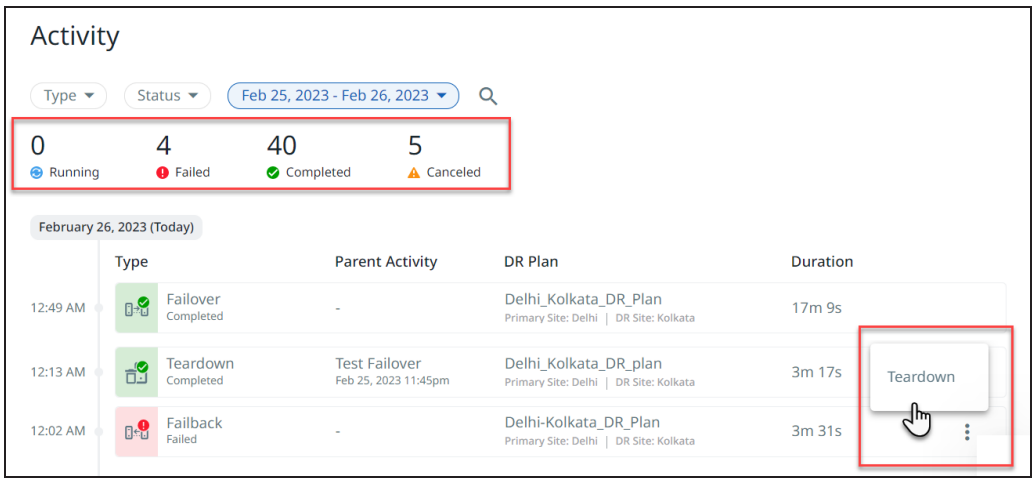
DR Plans are often long-running and span multiple sites, such as two or more Data Centers. On the **Activity** page, SiteContinuity enables you to have accurate and actionable insights into the current activities.

View DR Activity

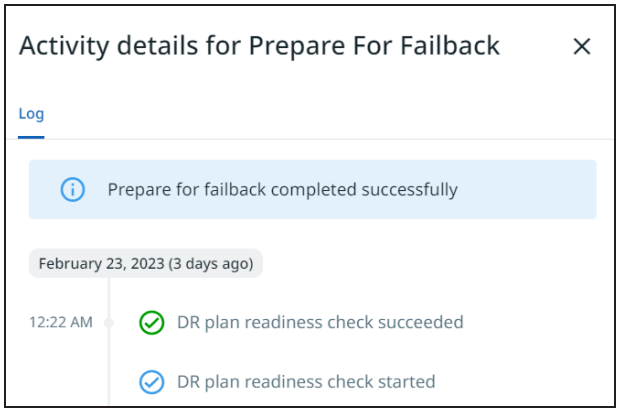
To view the activities of a DR Plan:

1. In **SiteContinuity**, navigate to **Activity**.
2. Click on an activity to view that activity's details.

   SiteContinuity displays all operations performed on a DR plan since it was created. Hover over an activity, and the Action menu (⋮) allows you to cancel, force finish, or tear down that individual activity.

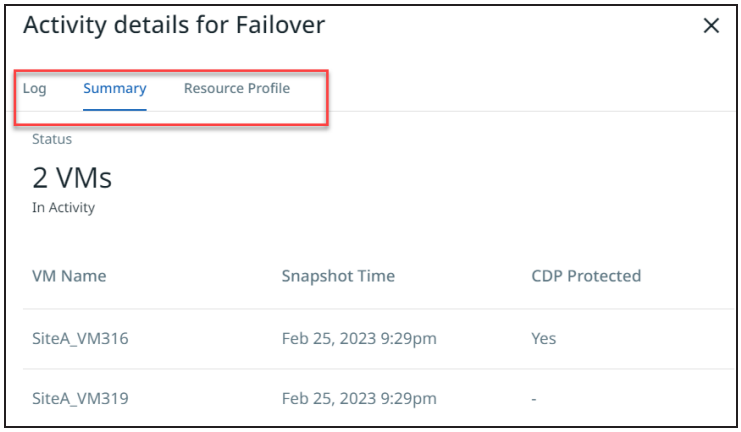


On the **Log** tab, click on the activity to see the activity log. A blue tick indicates the start of an activity, and a green tick its completion.



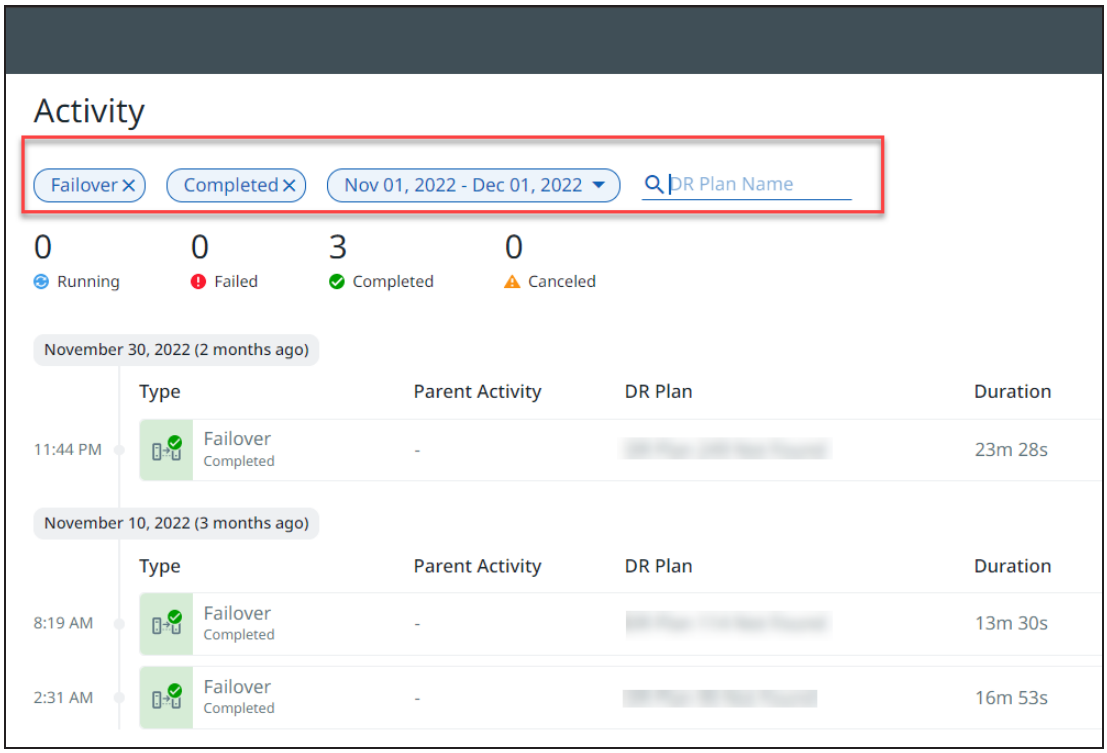
For all activities (other than Activate, Prepare for Failover, and Prepare for Failback), the **Activity Details** page also shows an additional **Summary** tab and a **Resource Profile**

tab. The **Summary** tab displays the list of VMs, their last snapshot time, and CDP protection status. The **Resource Profile** tab displays the Resource Profile details.



Filter DR Activity

Filters on the Activities page help you display only the activities you want.



The filtering options are:

- **Activity Type**. Options are Activate, Cancel, Failback, Failover, Force Finish, Prepare for Failback, Prepare for Failover, Resume, Teardown, Test Failover, and Test Failback.
- **Activity Status**. Options are Canceled, Canceling, Completed, Running, and Failed.

- **Time Range**. Set the period within which the activity was performed.
- **Search**. You can click the search icon and enter the DR plan name in the Search field. As you type, plans that match your search term appear.

Disaster Recovery Plan Report

The Disaster Recovery (DR) Plan report consists of all operations initiated on a DR plan within the specified time range and provides the final status of these operations. The report is crucial for assessing the DR plan's efficacy, identifying areas for improvement, and ensuring preparedness for future incidents.

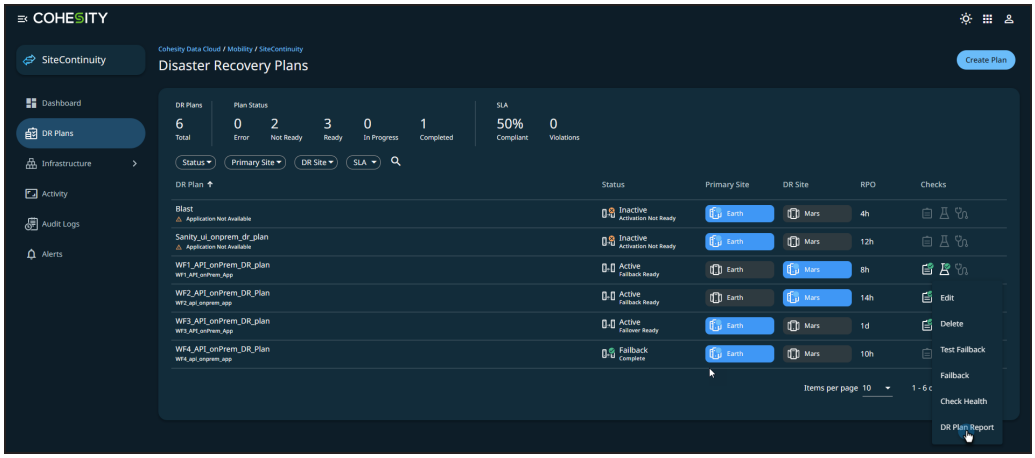
The report contains the following details:

- Details of the primary and DR sites
- Summary of the activities executed
- Application name
- Activity details
- The selected date range of the report

Download the DR Plan Report

To download the DR Plan report:

1. In **SiteContinuity**, navigate to **DR Plans**.
2. On the **Disaster Recovery Plans** page, hover over the DR plan for which you want to view the report, click the vertical ellipsis icon, and select **DR Plan Report**:



3. In the **Disaster Plan Activity Report** dialog, select the format and the date range:

4. Click **Download**.

Activity Detail Report

The Activity Detail Report is a comprehensive report that contains crucial information related to DR planning and execution. The Activity Detail Report provides a holistic overview that consolidates DR plan details, Resource Profile specifics, VM-level insights, and a chronological depiction of the steps in the activity. This comprehensive approach facilitates informed decision-making, post-activity analysis, and continuous improvement in DR strategies.

The following table describes various sections of the report:

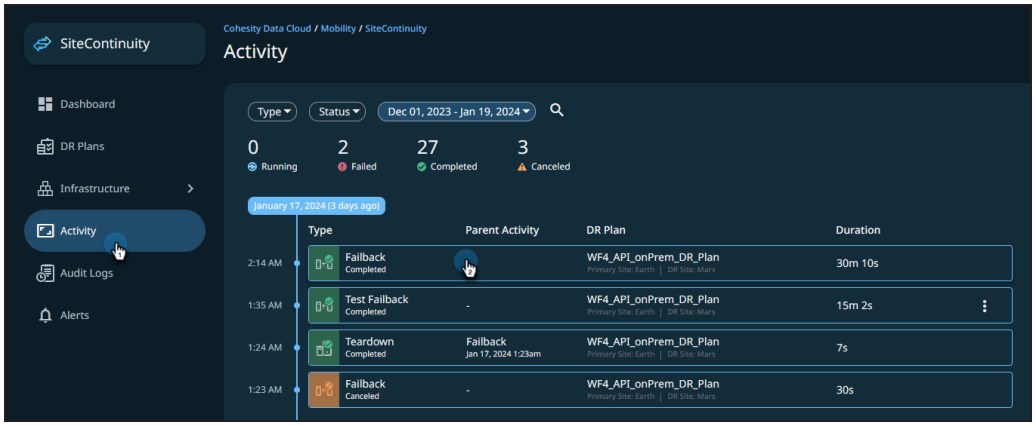
Section	Description
Details	• Name of the DR plan • Status • Reason for failure, if any • Name of the application • Activity ID
Resource Profile Details	• Resource Pool • Name of the datacenter • Name of the cluster • Network management protocol used

Section	Description
VM Level Details	• Name of the virtual machine • Network details • Datastore details • IP address • Subnet gateway • DNS
Activity Steps	• Breakdown of each step and the sequence of operations • Status of the step • Start time of the step

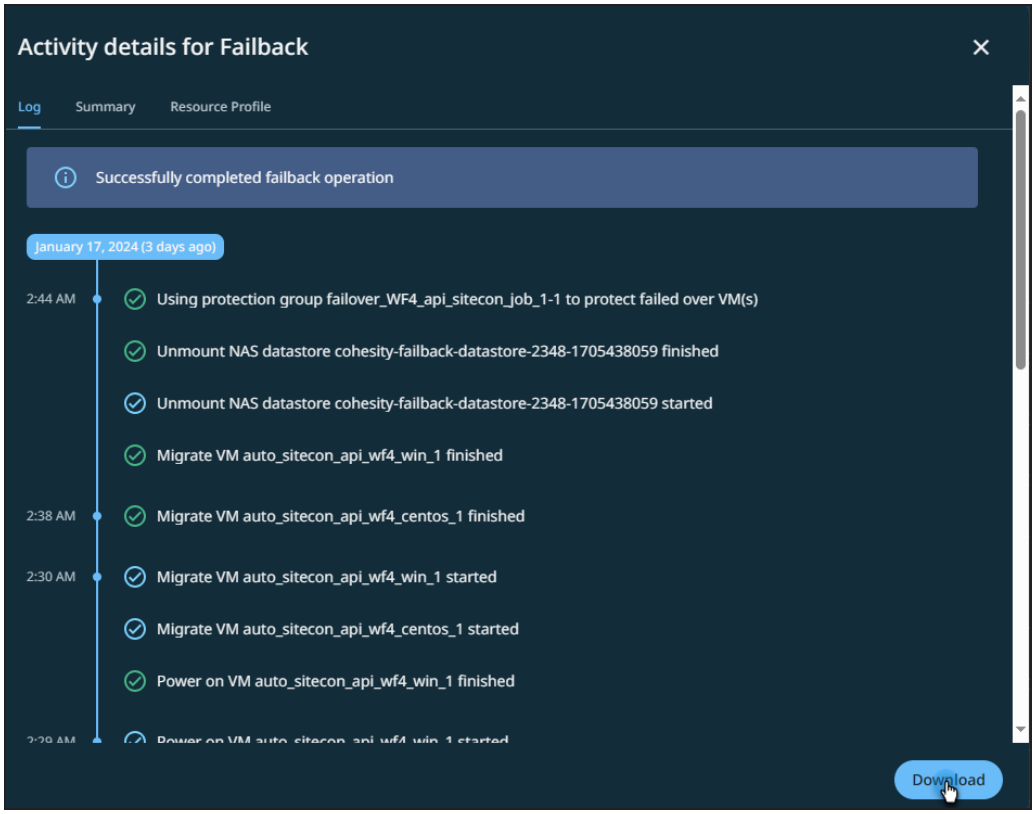
Download the Activity Detail Report

To view and download the activities of a DR plan:

1. In **SiteContinuity**, navigate to **Activity**.
2. Click on an activity to view the details. SiteContinuity displays all operations performed on a DR plan since it was created:



3. Click **Download** and select the format:



Alerts

SiteContinuity creates an alert when specific activities in your DR plan complete successfully or fail. Alerts are generated when Failover, Failback, DR Plan Activation, DR Plan Replication, Tear Down, or Test Failover fails and when Failover and Failback complete successfully.

View Alerts

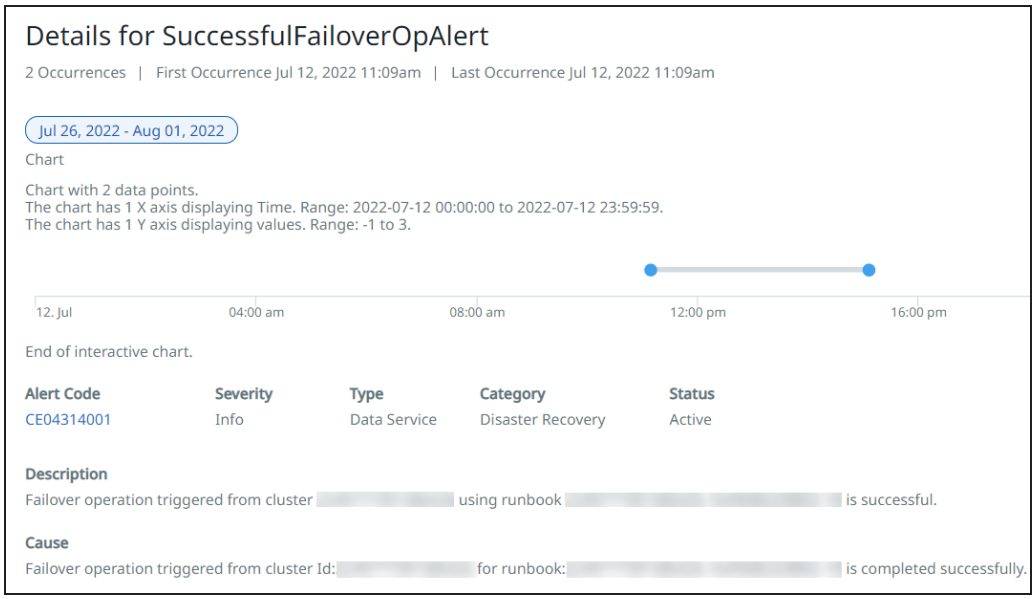
View Alerts List

In SiteContinuity, navigate to the **Alerts** page. The **Alerts** page displays all the alerts.

View an Alert

To view the details of an alert:

1. In **SiteContinuity**, navigate to **Alerts**.
2. From the list of alerts, click on an alert to view that alert's details:



For each alert, the alert details page provides a date range, a chart, and several important fields:

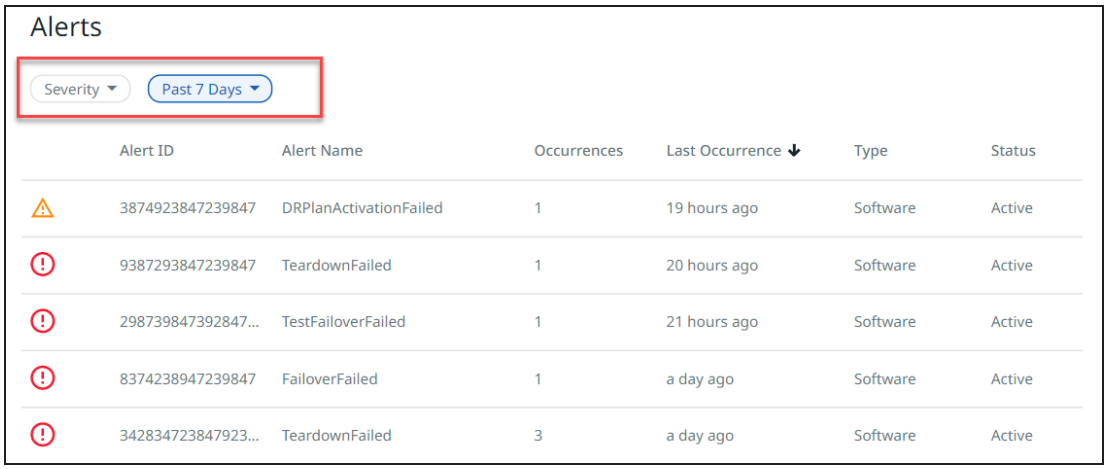
- **Alert Code**. The alert code. Click the alert code for the code description.
- **Severity**. Each alert has a severity rating that indicates the seriousness of the problem:
  - **Critical**. Immediate action is required because it detects a major function not working or a severe problem that might be imminent.
  - **Warning**. Action is required, but the affected functionality is still working.
  - **Informational**. Immediate action is not required, and the alert provides an informational message.
- **Type**. Type is always Software for SiteContinuity alerts.
- **Category**.The alert category is always Disaster Recovery for SiteContinuity alerts.
- **Status**. The status of the alert can be one of the following:
  - **Active**. The issue the alert indicates has yet to be resolved.

    > **Note:** The alert is informational, and no action is required.

  - **Resolved**. The alert has been resolved.
- **Description**. Information about the alert includes the DR plan name
- **Cause**. A brief description of what caused the alert.

Filter Alerts

The **Alerts** page displays all the alerts that SiteContinuity generates. Filters on the **Alerts** tab help you display only the alerts you want.



The filtering options are:

- **Severity**. Critical, Info, or Warning.
- **Time Range**. Set the period within which the alert was generated.

You can click the search icon and enter the **Alert** name in the **Search** field. As you type, DR Applications that match your search term appear.

Audit Logs

The Audit Logs page records all events that occur in SiteContinuity. The following details are recorded:

- Impacted systems
- Timestamp of the event
- User associated with the action

They include system events such as an audit trail of:

- Read or write actions performed by the users on your Cohesity clusters.
- Login and logout actions performed by the Helios users in SiteContinuity.

Configure Audit Log

By default, audit logs are enabled on SiteContinuity. You can configure the following settings based on your requirements:

- Log retention period.
- Capture read logs of specific user roles on the Cohesity clusters.

Set Log Retention Period for Audit Logs

Audit logs are retained in SiteContinuity for 180 days by default, but you can change this to any period between 90 and 365 days.

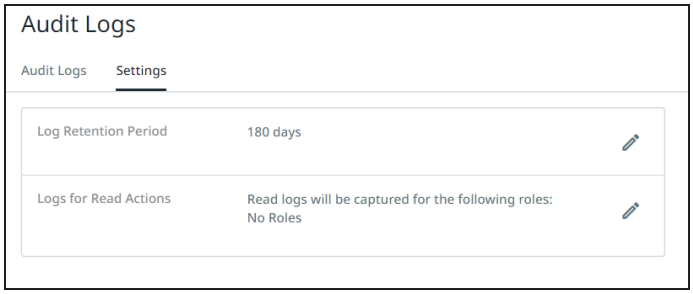
To set a retention period for audit logs:

1. In **SiteContinuity**, navigate to **Audit Logs** and click the **Settings** tab.
2. Under Settings, click the **Edit** icon ( ) for **Log Retention Period**.
3. Enter the desired number and choose a type of retention period (days, weeks, months, or years).

   > **Note:** converts weeks or months into days and displays that number as the **Log Retention Period**. If you enter a value that is less than 90 days or more than 365 days, the change will fail and revert to its existing value when you save it.

4. Select ✓ icon to save.

   A notification with the message **Settings Updated** appears briefly.



Capture Read Actions for Specific User Roles

You can configure SiteContinuity to capture read action logs for specific user roles on your Cohesity clusters.

To specify user roles for read action logs:

1. Navigate to **Audit Logs** and click the **Settings** tab.
2. Under Settings, click the **Edit** icon ( ) for **Logs for Read Actions**.
3. Select a role.

4. Click the **Add** icon (⊕) icon to add more roles.
5. Click the **Save** icon (✓).

A notification with the message **Settings Updated** appears briefly.

The roles you selected for capture are listed under **Logs for Read Actions**.

View Audit Logs

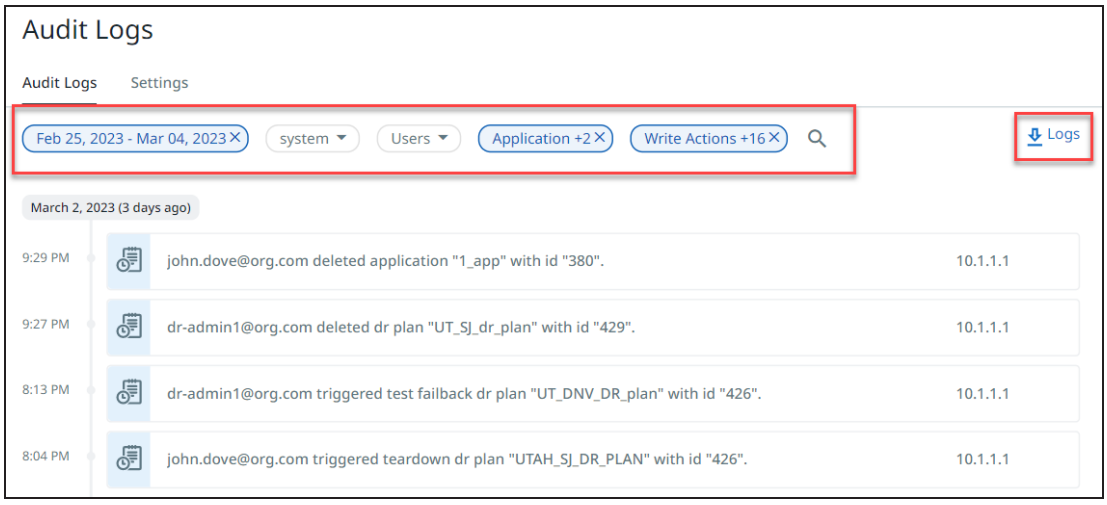
On the **Audit Logs** page in SiteContinuity, click the **Audit Logs** tab to view the audit logs, where you can find the following events as logged by the Cohesity clusters or Helios services:

- Date
- Time
- User and action
- System (cluster IP or Helios service)

> **Note:** By default, only the write actions performed by the users on Cohesity clusters are displayed on the **Audit Logs** page. To see read actions, select **Read Actions** from the **Actions** filter and click **Apply**.

Use Filters to Locate Specific Logs

Use the filters to narrow the listed audit logs and locate the specific logs you're looking for.



The filters are:

- **Date Range.**Filter the audit logs based on the selected time window.
- **System.**Filter the audit logs based on the cluster(s) or Helios service.
- **Users.**View the audit trails of specific users.
- **Category.**Filter the audit logs based on predefined categories. All cluster audit logs are logged under predefined categories for you to find the relevant audit logs and analyze the right logs quickly: Application, DR Plan, Sites.
- **Action.**Filter the audit logs based on the read or write actions performed by the users on the Cohesity clusters that are managed in Helios. See Logged Actions.

Logged Actions

Along with the read actions, the following write actions are logged:

Write Actions	Description
Activate	A user activated an entity, such as a DR plan.
Create	A user created an entity, such as a site.
Delete	A user deleted an entity, such as a DR plan, application, or site.
Failback	A user triggered a failback operation on a DR plan.
Failover	A user triggered a failover operation on a DR plan.
Login	A user logged in to Helios.
Logout	A user logged out of Helios.
Modify	A user modified an entity, such as a DR plan or application.
PrepareFailover	A user triggered a prepare-for-failover operation on a DR plan.
TestFailover	A user triggered a Test Failover operation on a DR plan.
PrepareFailback	A user triggered a prepare-for-failback operation on a DR plan.
TestFailback	A user triggered a Test Failback operation on a DR plan.
Teardown	A user triggered a Teardown operation on a DR plan.
Cancel	A user canceled an ongoing operation on a DR plan.

Write Actions	Description
Resume	A user resumed an operation on a DR plan.
ForceFinish	A user-triggered force finish on a failed failover or failback operation on a DR plan.

Download Audit Logs

You can download the Audit Logs in SiteContinuity for analysis and sharing.

To download audit logs:

1. In **SiteContinuity**, navigate to **Audit Logs**.
2. In the top right, click the **Download** icon next to **Logs**.

   The download of the file in CSV format is initiated.

Troubleshooting

This page provides information on the possible execution status errors you may encounter while executing a DR plan.

> **Note:** The following sections only discuss the possible scenarios with examples to help you understand how to recover a DR plan from a failed state and is not a definitive list.

Configuration Error

Cause

A DR plan transitions to the Inactive (Configuration Error) state if the configuration of a DR plan before activation or changes that have been made to the DR plan or protection settings after the activation is incorrect. Examples of configuration errors are:

- Protection Group or Protection policy is not configured in the cluster or has been removed from the cluster.
- Replication is not enabled in the Protection Policy.
- One or more VMs are not included in the Protection Group.

Solution

The error message can help you identify the root cause of the problem. To see the error message, on the **Disaster Recovery Plans** page, click the name of the DR plan. The error message is displayed along with the other details of the DR plan.

You may try the following to troubleshoot the error:

- Log in to the Cohesity cluster (or access it via Helios) and fix the protection settings of your VMs.
- Modify the DR plan to update the VMs defined in the plan.

System Error

Cause

SiteContinuity transitions the DR plan to an Inactive (System Error) state if a problem caused by external factors is impeding the ongoing operation of that plan. This error usually

also indicates there are no configuration errors in the plan. Examples of system errors are:

- Network connectivity issue between the Cohesity cluster and the vCenter
- vCenter is down
- Cluster services are slow or unresponsive

Solution

The error message can help you identify the root cause of the problem. To see the error message, on the **Disaster Recovery Plans** page, click the name of the DR plan. The error message is displayed along with the other details of the DR plan.

You may try the following to troubleshoot the error:

- Verify network connectivity between the Cohesity cluster and the vCenter.
- Ensure the vCenter server is running.
- Examine the vCenter logs to diagnose the error, and so on.
- Log in to the Cohesity cluster and check the cluster status.

Failover Failed

Cause

If the failover of a DR plan fails, the status is displayed as **Failover Failed**.

Solution

To see the error message and identify the root cause of the problem:

1. In **SiteContinuity**, navigate to **DR Plans**.
2. On the **Disaster Recovery Plans** page, click on the name of that DR plan. The error message is displayed along with the other details of the DR plan.
3. In the **Activity** tab, click on the Failover activity. The **Log** tab displays all the events of the Failover activity in chronological order, including the specific event that encountered the error.

   Examine the error messages and log to check if the errors are due to external factors or configuration errors, and retry after fixing the errors. If the failover fails again, contact Cohesity Support.

Failback Failed

Cause

If the failback of a DR plan fails, the status is displayed as **Failback Failed**.

Solution

To see the error message and identify the root cause of the problem:

1. In **SiteContinuity**, navigate to **DR Plans**.
2. On the **Disaster Recovery Plans** page, click on the name of that DR plan. The error message is displayed along with the other details of the DR plan.
3. In the **Activity** tab, click on the Failback activity. The **Log** tab displays all the events of the Failback activity in chronological order, including the specific event that encountered the error.

   Examine the error messages and log to check if the errors are due to external factors or configuration errors, and retry after fixing the errors. If the failback fails again, contact Cohesity Support.

Test Failover Failed

Cause

If the Test Failover fails, the icon in the **Checks** column of the **Disaster Recovery Plans** page shows an error symbol (). Click the icon to see the error message.

Solution

You have the option to edit the DR plan to fix the issue or delete the DR plan altogether.

Test Failback Failed

Cause

If the Test Failback of a DR plan fails, the icon in the **Checks** column of the **Disaster Recovery Plans** page shows an error symbol (). Click the icon to see the error message.

Solution

You have the option to edit the DR plan to fix the issue or delete the DR plan altogether.

Health Check Failed

Cause

If the Health Check of a DR plan fails, the **Health Check** icon in the **Checks** column of the **Disaster Recovery Plans** page shows an error symbol ( ). Click the icon to see the error message.

Solution

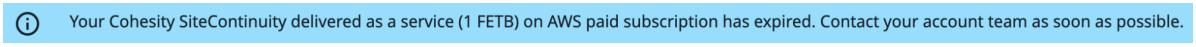
You may try the following to troubleshoot the error:

- Ensure the SLA of the DR plan is met. SLAs might not be met if Replication between the clusters is failing or if protection runs are configured to run shorter cycles when compared to the SLA defined in the DR plan.
- Verify the remote cluster connection on both the primary and DR Cohesity clusters:
  a. Log in to the Cohesity cluster.
  b. Navigate to **Infrastructure** > **Remote Clusters**.
  c. Verify the remote cluster connection and details.
- Verify that the primary and DR sites are connected to Helios:
  a. Log in to the Cohesity cluster.
  b. When the cluster is connected to Helios, a green check mark is displayed in the Helios icon in the top right corner of the **Cohesity Dashboard**.

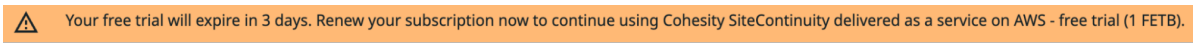
Subscription Status

Cohesity Helios displays banners on the UI, providing details on your Cohesity SiteContinuity delivered as a Service subscription status, allowing you to take necessary actions. The banners are of three types:

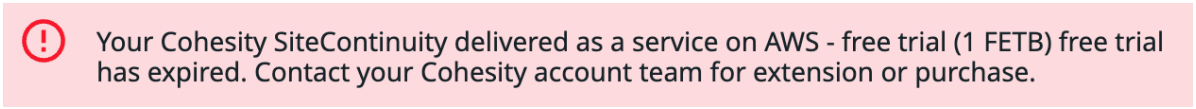
- **Information**
  Sample:

- **Warning**
  Sample:

- **Critical**
  Sample:

Banner Messages

Based on your subscription type and status, Cohesity SiteContinuity UI displays different types of banners. The table below shows the various scenarios and the types of banners displayed in each scenario:

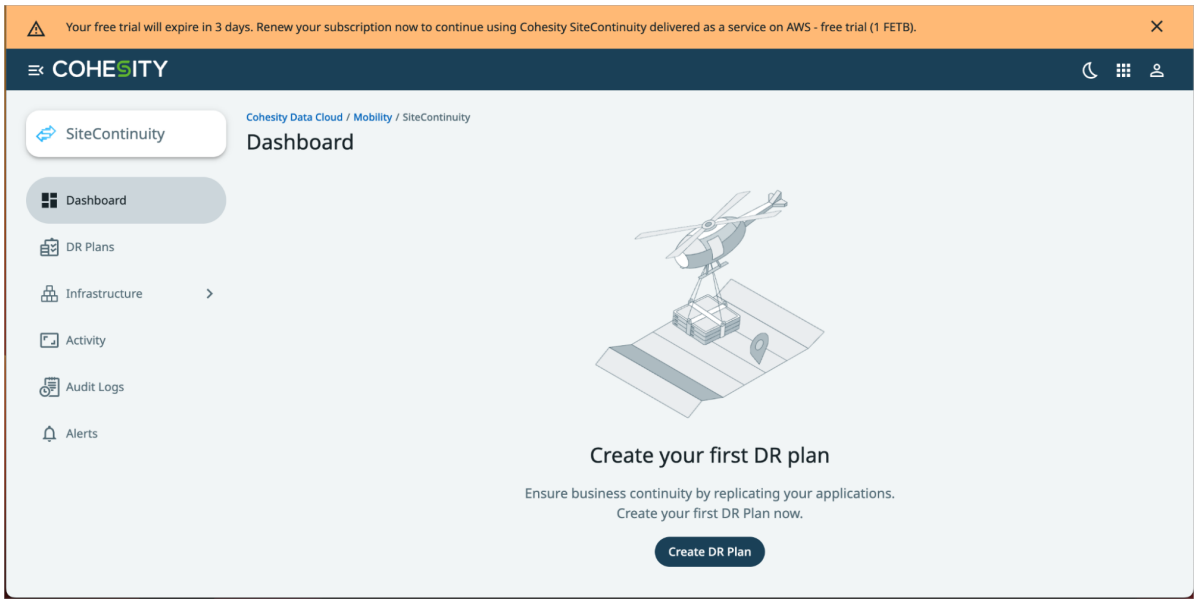
Subscription Type	Subscription Status	Description
Free Trial	Expiration	Before the free trial expires, an information banner is displayed 15 days prior, and a warning banner is displayed 7 days prior to the expiry.
	Post Expiration	A day after the free trial expires, the Cohesity SiteContinuity UI displays the following message: `"Your Cohesity SiteContinuity Delivered as a Service on AWS - Free Trial (1 FETB) free trial has expired. Contact your Cohesity account team for extension or purchase."`
	Grace Period	After the free trial period ends, access to the service will be restricted immediately with no grace period.

Subscription Type	Subscription Status	Description
Paid Subscriptions	Expiration	Cohesity SiteContinuity UI shows a banner 30 days before the subscription expires, a warning at 15 days, and critical after expiry.
	Post Expiration	A day after the paid subscription expiry, the following banner is shown on the Cohesity SiteContinuity UI: `"Your Cohesity SiteContinuity Delivered as a Service (1 BETB); AWS data plane subscription has expired. Contact your Cohesity account team immediately."`
	Grace Period	Once a paid subscription expires, there is a grace period to renew it. During this time, access is unrestricted, but product functionality is limited.

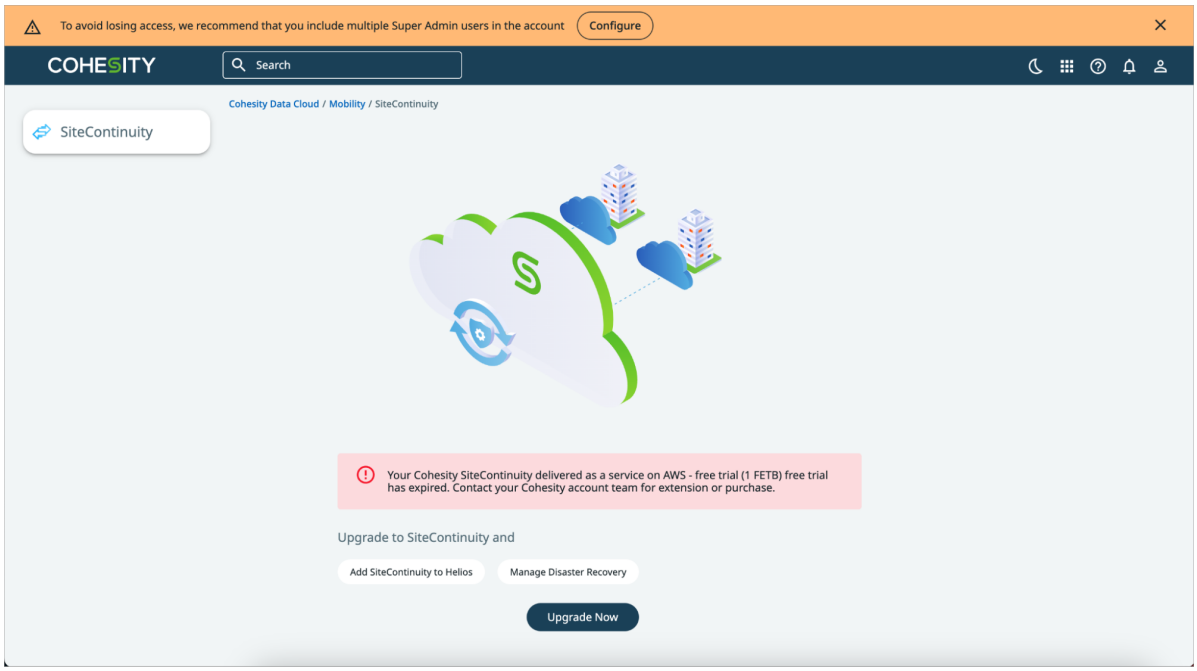
Sample Banner Messages

The following are different banner messages that provide details on the Cohesity DataProtect delivered as a Service subscription status:

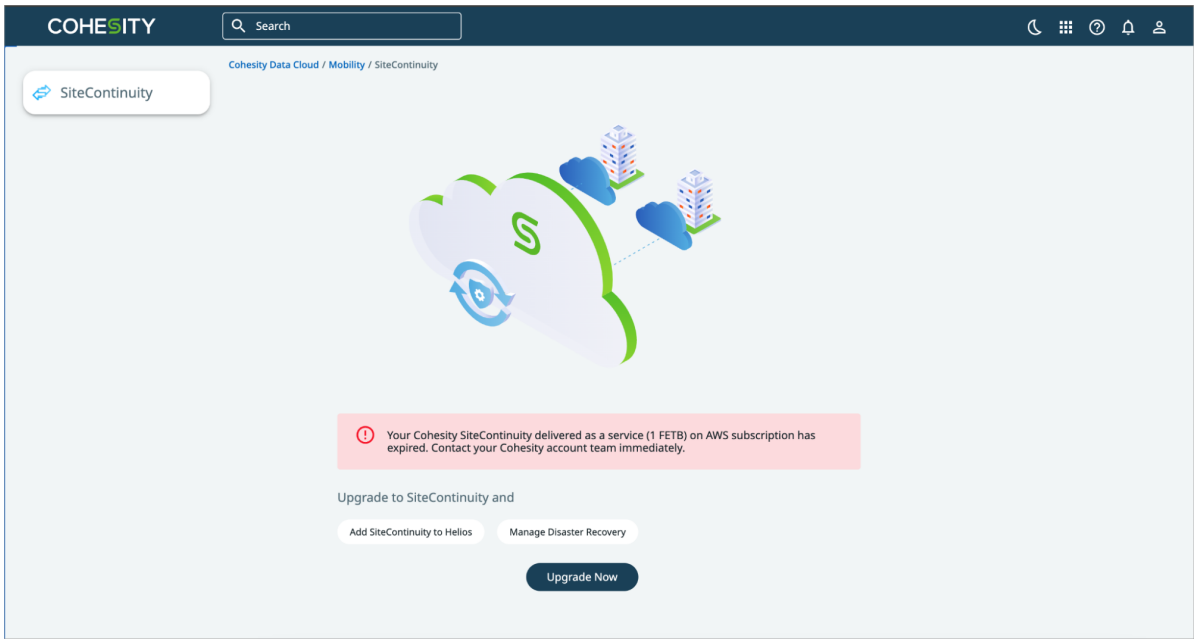
Free trial is about to expire:



Free trial expired:



The paid subscription has expired:



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.

Creating a customer support case for Cohesity Cloud Services (CCS)

When creating a customer support case for Cohesity Cloud Services (CCS), follow the steps listed below:

1. Mention CCS in the subject and select **CCS** as the **Issue Type**.
2. Provide the case information.
3. Edit the **Case Subject** as per you cloud region. For example, for AWS region, **CCS (AWS_Region): <Input Issue Subject Information>**.
4. Update the **Issue Type** field to **CCS**.

Additionally, provide the **Cluster ID** and the **Support Token** information if a SaaS connector is involved.

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

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.