Using VMware Cloud Disaster Recovery

21 January 2021

VMware Cloud Disaster Recovery
You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/
## Deploying a Recovery SDDC

- Available AWS Regions
- SDDC and Your AWS Account
- SDDC and Cluster Names
- Deploy Recovery SDDC
- SDDC Usage Daily Email Reminder
- SDDC Datastore
- Delete an SDDC
- Add/Remove Hosts
- Add/Delete a Cluster
  - Caveats for Adding Clusters
- Add a Network to an SDDC
  - Request Public IP Addresses
  - Add NAT rules
- Add firewall rule to SDDC network
  - About SDDC Firewall Rules
- Maintaining SDDC Settings
  - SDDC Settings You Should Not Change

## DRaaS Connector and Protected Sites

- Dimensions of Protected Site
- vSphere Protected Site
- Protecting a Site
- Set up a Protected Site
  - Register vCenter
  - Deploy the DRaaS Connector
- Send Support Bundle
- Manage a Protected Site
  - Edit a Protected Site
  - Remove a vCenter from a Protected Site
  - Remove a Connector from a Protected Site
  - Delete a Protected Site
Backup with Protection Groups 61
Backup copy caveats and restrictions 62
Create a Subscription 62
Create a Protection Group 63
Edit a Protection Group 66
Deactivate Protection Group Snapshot Schedule 66
Delete a Protection Group 67
VM Name Pattern 67
Take a manual snapshot 69
Restore a VM 70
Throttle Replication 71

DR Plans 72
DR Plan Configuration 72
Recovery Site Selection 73
Protected Site Selection 73
Protection Group Selection 74
Datastore Mapping 74
vCenter Mapping 76
vCenter Folders Object Inventory Mapping 77
IP Address Mapping 79
Supported IP Address Mapping Combinations 84
OS Compatibility for Static IP Address Mapping 85
Script VM 86
Recovery Steps 87
Script Configuration 91
Alerts 94
Viewing DR Plans 94
Activating DR plans 95

Running a DR Plan 96
Before Running a DR Plan 96
Configure Email Alerts 97
Using VMware Cloud Disaster Recovery

How a Failover Plan Runs 97
Plan States 98
Run a Failover Plan 100
Failover Operation Process 102
  Manual Intervention During Failover 103
  Failover error handling 104
System Behavior During Failover 106
  No Overwrite of Existing VMs 106
  Batching 107
  Skip VMs not Registered with vCenter 108
  VM Tags and Tag Categories 108
  Migration Limits During Failover/Failback 109
Failover Completion 109
  Commit vs Acknowledge 109
  Commit a Failover 110
  Rollback and Acknowledge a Failback 112
  Post-Commit Actions 113
Test Failover 114
  Running a Test Plan 114
  Test Failover Example 115
  Acknowledge Test Plan Cleanup 118
Creating an Isolated Test Environment 119

Failback 123
Failback 124
  Preparing a Failback Plan 124
  Reset the Default Datastore 125
  Running a Failback Plan 126
  Failback Process 130
Run a Failback Plan 132
  Cleaning up Failback Source 133
Continuous Compliance Checks 133
Compliance Check Details  134
Environment Mappings  134
Replication Configuration and Health  135
SDDC Checks  135
Destination Site Resource Availability  136
Split Brain Detection  136
vCenter Checks  136
Protection Group Checks  136
VM Checks  136
Script Execution  137
View a Plan’s Compliance checks  137

Reports  139
Failover and Test Failover Reports  139
Configuration Reports  139
Compliance Reports  140
Automated PDF Report and Email  140

Monitoring  141
Event Filters  141
  Event Category Filter  142
  Event Severity Filter  143
  Event Timestamp Filter  144
Plan-related Events  144
Alarms  144
VMware Cloud Disaster Recovery™

VMware Cloud Disaster Recovery is VMware’s on-demand disaster recovery service that is delivered as an easy-to-use SaaS solution and offers cloud economics to help keep your disaster recovery costs under control.

VMware Cloud Disaster Recovery can be used to protect your vSphere virtual machines by replicating them periodically to the cloud and recovering them as needed to a target VMware Cloud on AWS Software Defined Data Center ("SDDC"). The target SDDC can be created immediately prior to performing a recovery and does not need to be provisioned to support the replications in the steady state.

The Service Offering has the following components:

- **DRaaS Connector** – a virtual appliance installed in the VMware vSphere environment where the virtual machines to be protected are running under normal circumstances.
- **Scale-Out Cloud File System ("SCFS")** – a cloud component that enables the efficient storage of backups of the protected virtual machines in cloud storage and
allows virtual machines to be recovered very quickly without a time-consuming data rehydration process.

- SaaS Orchestrator ("Orchestrator") – a cloud component that presents a user interface (UI) to consume the Service Offering and includes several disaster recovery orchestration capabilities to automate the disaster recovery process.

**Note:** For more information about VMware Cloud, see VMware Cloud Services documentation.

### Capabilities and Benefits

VMware Cloud Disaster Recovery provides the following key capabilities:

- Comprehensive SaaS simplicity across DR automation, on-demand recovery and site preparedness, the SCFS, and failback.
- "Live Mount" snapshots from the cloud
- Cost optimized: Pay-per-use DR site in public cloud, restarting VMs from low cost cloud backup storage
- Disaster & cybercrime recovery based on backups
- Continuous DR compliance checks
- Automated compliance reporting
- End-to-end security

VMware Cloud Disaster Recovery provides a comprehensive, cloud-native DR service for VMware VM workloads. VMware Cloud Disaster Recovery manages all aspects of AWS and VMware Cloud, based on your parameters, with complete runbook automation. For maximum simplicity, the recovery site is VMware Cloud on AWS, so there is a consistent operating environment that seamlessly spans primary and recovery sites. vCenter remains the operating console, VMs still have VMware characteristics without conversion, hosts are still hosts, and DRS and HA continue as usual.

A unique capability of VMware Cloud Disaster Recovery is the ability to “Live mount” snapshots from the cloud. Live Mount means the ability for hosts in VMware Cloud on AWS to boot VMs directly from the copies stored securely in the SCFS, which acts as an NFS Datastore for the recovery SDDC.
To simplify recovery from one of the most common recovery use cases — ransomware — VMware Cloud Disaster Recovery developed the industry’s first method for scalable Live Mount of VMware VMs from our backup store on AWS, so you ‘go back in time’ (sometimes months) to identify uninfected data and find the cleanest recovery point quickly and get your workloads up and running. VMware Cloud Disaster Recovery provides instant VM restart, regardless of the snapshot’s age, or the retention depth of its cloud backup vault.

VMware Cloud Disaster Recovery also undertakes every effort to optimize cloud costs. One key benefit of the cloud is that resources are on demand, including the compute in a DR plan, so you don’t have to pay for it until you need it. For data readiness, backups are stored on AWS with compression and deduplication.

And because VMware Cloud Disaster Recovery is delivered as a service, there is nothing to install and nothing to manage. Monitoring and planned upgrades of all software, including VMware Cloud Disaster Recovery Connectors, are automated and performed by VMware Cloud Disaster Recovery as a part of the service offering.

**Flexible Recovery Topologies**

VMware Cloud Disaster Recovery allows you to configure DR Plans with topologies best suited for the type of DR protection needed for your sites.

VMware Cloud Disaster Recovery provides three contexts in which DR operations are available:

- A **protected site** is vSphere protected by the DRaaS Connector, supporting any storage, on which workloads are covered by DR Plans.

- The **recovery site** takes over workload execution after a disaster occurs. A recovery site is a cloud-created SDDC in VMware Cloud on AWS. VMware Cloud Disaster Recovery uses snapshots that have been replicated to the SCFS to failover to the recovery site, according to the DR plan definition. You can use the Recovery SDDC site to test your DR plans to ensure all mappings and configurations work as intended. For more discussion, see Test Failover.
Note: Site designations are logical, on a per-plan basis. This means, for example, that the same site can act as a protected site for some DR plans, as a backup site for other DR plans, and as a recovery site - all at the same time.

You can configure the DRaaS Connector to ingest data from any storage, then create protection groups (PGs) that regularly replicate snapshots to the SCFS.

You then create DR Plans to orchestrate failover to a VMware on AWS SDDC in the event of a disaster or ransomware attack. You can also use DR plans to failback once you are ready to recover the failed site.
Live Mount

A unique capability of VMware Cloud Disaster Recovery is the ability to “Live Mount” snapshots from the cloud. Live Mount means the ability for hosts in VMware Cloud on AWS to boot VMs directly from the copies stored securely in the SCFS, which acts as an NFS Datastore for the recovery SDDC.

Continuous Compliance Checks

Continuous DR plan compliance checks verify the integrity of a plan to ensure that any changes in the failover operation environment do not invalidate the plan’s directives when the plan is run. Compliance checks also make sure that the specified protection groups continue to be live on the protected site and are being replicated successfully to the target site.

Compliance checks run automatically every 30 minutes for activated plans. A plan can become out of compliance if any of its conditions become violated because of environmental or plan configuration changes.

Failing Compliance checks transition a DR plan into a degraded health state of Warning or Critical. When a plan fails a compliance check, an email will be sent to the recipients configured in your Configure Email Alerts. Health checks are run on a per-plan basis - some plans can have an OK health status, while others can be in degraded states at the same time.

Note that a plan’s Compliance state will not restrict failover or test operations. Even if a plan is non-compliant in some areas, the plan can still be run as a failover or test failover.

Automated Compliance Reporting

Many enterprises have compliance reporting requirements for disaster recovery readiness. With a manual DR plan or with other solutions, creating a DR test or recovery report itself becomes a heavy task.

With VMware Cloud Disaster Recovery, this process is completely automated. As a DR plan is created, tested for compliance, and run, VMware Cloud Disaster Recovery maintains detailed logs of all the actions that were performed, the plans that were
completed, and the compliance checks on those plans. These reports can be downloaded as a PDF or emailed to people on an automated schedule.

**SDDC Deployment**

You can use VMware Cloud Disaster Recovery for Deploying a Recovery SDDC in VMware Cloud AWS to use for recovery and testing of your DR plans. Once you have deployed an SDDC, you can Add/Remove Hosts, Add a Network to an SDDC, request public IP addresses, configure NAT rules, firewall rules, and also delete an SDDC.

To learn more about how SDDC deployments can meet business needs, see SDDC Deployment Types and Use Cases.
Getting Started

Getting started VMware Cloud Disaster Recovery consists of the following tasks:

1. **Request VMware Cloud Disaster Recovery.** The first time user of the VMware Cloud Disaster Recovery service (typically the service organization owner) needs to request deployment of the VMware Cloud Disaster Recovery service. Your sales representative will send you an on-boarding email, which guides you through the process. After requesting the service, VMware support will contact you to assist with your VMware Cloud Disaster Recovery deployment. If you purchased VMware Cloud Disaster Recovery from Amazon Web Services (and not VMware), please work with your sales team to activate VMware Cloud Disaster Recovery service tile. You do not need to perform this task, and can begin with the second task: create an API token.

2. **Create an API Token.** For VMware Cloud Disaster Recovery, you need to configure a VMware Cloud API token to make authorized API connections with the service.

3. **Configure the API Token.** Once a VMware Cloud API token has been created, you need to configure it in the VMware Cloud Disaster Recovery UI.

4. **Invite new users your organization.** Once the VMware Cloud Disaster Recovery service has been deployed, you can start inviting users to your organization from the VMware Cloud Services console. When you invite users to your organization, you can assign specific User Access, which permit the user to perform operations with the service.

Request VMware Cloud Disaster Recovery

To get started with VMware Cloud Disaster Recovery, you need to request the service:

- If you are a new customer to VMware Cloud Services, you can request VMware Cloud Disaster Recovery through your VMware sales representative.
- If you already use VMware Cloud Services, you can request access to the VMware Cloud Disaster Recovery from the VMware Cloud Services console by following the procedures listed below.

After you have requested VMware Cloud Disaster Recovery in your cloud account, you will receive a VMware Cloud Disaster Recovery activation email. This email provides a
Using VMware Cloud Disaster Recovery

link to the VMware Cloud Services console, where you can log in and follow the onscreen instructions to request deployment of the service.

**AWS customers**: If you purchased VMware Cloud Disaster Recovery from Amazon Web Services (and not VMware), please work with your sales team to activate VMware Cloud Disaster Recovery service tile. You do not need to perform the steps in this task.

**Procedure - Request**

1. Log in to [VMware Cloud Services](#) with your VMware account.
2. In the console, under your user name on the menu bar, select the organization you will using with the VMware Cloud Disaster Recovery service.
3. On the Services page, under More Services, search for VMware Cloud DR. *(Note: If the VMware Cloud Disaster Recovery service has already been added then searching for it in “More Services” will give you 0 results.)*
4. In the search results, on the VMware Cloud DR tile click the REQUEST ACCESS link.

![VMware Cloud DR tile](image)

My Services

- [VMware Cloud on AWS](#)

More Services

- [VMware Cloud DR](#)
  Cost-Optimized Disaster Recovery with VMware Cloud on AWS
  REQUEST ACCESS
5. On the Request access to VMware Cloud DR page, click the button to send an email to request-vcdr@vmware.com. Be sure to include your name, company name, and reply-to email address in your email request. If you know your unique VMware Cloud Organization ID, please include it in the email as well to accelerate your request.

Procedure - Activation

1. After you have engaged with your sales representative and purchased sufficient SPP credits to start using VMware Cloud DR, you will receive and activation email, (look for "Welcome to VMware Cloud Disaster Recovery" in the subject line). Click the "ACTIVATE SERVICE" link in email to sign up for the service.

2. Sign in to VMware Cloud Services, and on the Select or Create Organization page, select or create an organization to that you want to provide controlled access to the VMware Cloud Disaster Recovery service. Go to the next page.

3. On the Payment page, select the credit fund you want to use to pay for the VMware Cloud Disaster Recovery service. (If you are also creating a new organization, enter a name for the new organization on this page.) Go to the next page.

4. The final step in signing up for the VMware Cloud Disaster Recovery service is to request deployment of the service. Click the VMware Cloud DR service tile to access the deployment request page. On this page, enter your contact information to request the VMware Cloud Disaster Recovery service: First name, last name, email, and phone number. When you are finished, click Request deployment.

5. After you request the service. VMware support will contact you to gather some basic details to initiate your subscription. Be ready to provide the following:
   - Subscription term (1 or 3 years)
   - AWS region preference
   - Estimated storage capacity and change rate of the workloads you want to protect.

6. VMware support will then guide you through the final on-boarding steps. Once on-boarding is complete, VMware Support will send another email to notify that the service is ready.
7. Once you are fully on-boarded, you can access VMware Cloud Disaster Recovery service by clicking on the tile under My Services in the VMware Cloud Services console.

Create an API Token

You need to create a VMware Cloud API token to make authorized connections with the VMware Cloud Disaster Recovery service. When you provide an API token to VMware Cloud Disaster Recovery, you enable it to interact with VMware Cloud on AWS and perform operations with your SDDC.

An API token authorizes service access per organization. Creating and configuring the API token should be done before your users access the VMware Cloud Disaster Recovery UI.

When you create an API token, you also define its scope of permissions, which you do by assigning specific organization roles and service roles to the token. For VMware Cloud Disaster Recovery, you need to scope the following roles to the API token

- **Organization Role**: Organization Owner
- **Service Roles**:
  - VMware Cloud on AWS Administrator
  - VMware Cloud on AWS NSX Cloud Admin

Once the API token is generated (this task), you can Configure the API Token in the VMware Cloud Disaster Recovery UI.
**Warning:** The maximum lifespan of a VMware Cloud Services API token is 60 months, after which you must regenerate a new token and configure it inside of the VMware Cloud Disaster Recovery UI. If you do not regenerate a new token when the old one expires, and configure the new token in the VMware Cloud UI, the product features will not function. Best practice in this case is to create an API token with the longest Time To Live (TTL) possible, to avoid service interruption.

**Important:** Your user account should have the Organization Owner role and VMware Cloud on AWS service roles (Administrator and NSX Cloud Admin) associated with it in order to create an API token for use with VMware Cloud Disaster Recovery.

**Procedure**

1. Log in to the VMware Cloud Services portal.
2. Select the organization you want to use with VMware Cloud Disaster Recovery.
3. On the VMware Cloud Services toolbar, click your user name and select **My Account → API Tokens**.
4. Click on the Generate new API token link.
5. Enter a name for the token.
6. Specify the lifespan of the token. If you set an expiration on this token, you will need to regenerate it when it expires, and then configure the new token in the VMware Cloud Disaster Recovery UI.
7. Define scopes for the token. For VMware Cloud Disaster Recovery, you must assign the following roles for the API token scope:
   - **Organization Role:** Organization Owner
   - **Service Roles:** VMware Cloud on AWS Administrator and VMware Cloud on AWS NSX Cloud Admin
8. Click **Generate**.

9. Save the token credentials to a safe place so you can retrieve them to use later on.

10. For security reasons, after you generate the token, only the name of the token is displayed on the API Tokens page and not the token credentials. This means that you will no longer be able to reuse the token by copying the credentials from this page.

## Configure the API Token

Once you **Create an API Token**, you need to configure the token in the VMware Cloud Disaster Recovery UI.

**Note:** The maximum lifespan of a VMware Cloud Services API token is 60 months, after which you must regenerate the API token in the VMware Cloud Services Console. Then, you can **Change the API Token** in the VMware Cloud Disaster Recovery UI.
Procedure

1. From the upper right side of the VMware Cloud Disaster Recovery UI, click the small gear icon and choose **Configure API token**.

2. In the Configure API token dialog, under VMware Cloud Token → API token, enter the API token.

3. Click **OK**. If you are changing the API token, then click the **Change token** button.

Change the API Token

Before your current API token expired, you should regenerate a new token and change the token in the VMware Cloud Disaster Recovery UI.

You can regenerate the API token in the VMware Cloud Services Console. Then, you can add the new token in the VMware Cloud Disaster Recovery UI.

Procedure

1. From the upper right side of the VMware Cloud Disaster Recovery UI, click the small gear icon and choose **Configure API token**.

2. In the Configure API token dialog, click the **Change token** button.

3. Enter the new API token in the dialog.

4. Click **OK**. 

User Access

When you sign up for VMware Cloud Services, and request access to the VMware Cloud Disaster Recovery service, you can begin to invite users to the service. As an organization owner, you can assign roles to your organization users, which grant them permissions to perform specific operations in VMware Cloud Disaster Recovery.

When you invite other users to the service, you assign them **organization roles** which specify privileges that an organization member has over organization assets, and **service roles**, which gives users the permission to access and use the VMware Cloud Disaster Recovery service.
For more information about VMware Cloud Service roles, and how to add them to your users, see Identity and Access Management and Edit User Roles.

**Note:** When you modify a VMware Cloud Disaster Recovery user roles in the VMware Cloud console, the changes take approximately 15 minutes to be applied. To apply the changes faster, the user can log out and then log back in to the VMware Cloud console, and then access the VMware Cloud Disaster Recovery service.

### Organization and VMware Cloud on AWS Service Roles

There are two specific operations in VMware Cloud Disaster Recovery that require a user to have the following roles:

- **Creating an API token** requires the following organization and VMware Cloud on AWS service roles:
  - **Organization Role:** Organization Owner
  - **VMware Cloud on AWS Service Roles:**
    - Administrator
    - NSX Cloud Admin

- **Creating a subscription** requires the following organization role:
  - Organization owner

### VMware Cloud Disaster Recovery Service Roles

The following table provides an overview of VMware Cloud Disaster Recovery roles and the features each role permits. Match the user role in each column with the capabilities in each row.

**Note:** VMware Cloud Disaster Recovery roles are additive. For example, if you want a user to create snapshots for backup and also have the ability to configure and run DR plans, you need to assign both DR admin and Backup admin roles to the user account.
Service Roles and Permitted Operations

The below table provides a more detailed description of all operations permitted for each VMware Cloud Disaster Recovery service role.

**Note:** If you apply the Administrator or the Auditor roles to a user account, then you cannot add any other roles to the account.

<table>
<thead>
<tr>
<th>Role</th>
<th>Permitted Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>This user role can perform all operations listed in this table, except for</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>Permitted Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>This user role can perform all operations listed in this table, except for</td>
</tr>
</tbody>
</table>

The below table provides a more detailed description of all operations permitted for each VMware Cloud Disaster Recovery service role.

**Note:** If you apply the Administrator or the Auditor roles to a user account, then you cannot add any other roles to the account.
<table>
<thead>
<tr>
<th>Role</th>
<th>Permitted Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>creating an API token and creating a subscription.</td>
</tr>
<tr>
<td>Auditor</td>
<td>- View the UI read-only: Lists, tasks, reports, dialogs (except user management)</td>
</tr>
<tr>
<td></td>
<td>- Create PDF of a compliance report and download it</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> All other roles include this level of access.</td>
</tr>
<tr>
<td>DR admin</td>
<td><strong>DR Plans</strong></td>
</tr>
<tr>
<td></td>
<td>- Create, edit, delete, duplicate DR plans</td>
</tr>
<tr>
<td></td>
<td><strong>Test recovery</strong></td>
</tr>
<tr>
<td></td>
<td>- Execute a test recovery</td>
</tr>
<tr>
<td></td>
<td>- Stop a test recovery (no cleanup)</td>
</tr>
<tr>
<td></td>
<td>- Cancel test recovery</td>
</tr>
<tr>
<td></td>
<td>- Roll back test recovery</td>
</tr>
<tr>
<td></td>
<td>- Retry failed tasks for a completed test recovery</td>
</tr>
<tr>
<td></td>
<td>- Retry failed tasks in a step and continue</td>
</tr>
<tr>
<td></td>
<td>- Ignore failure and continue without retry</td>
</tr>
<tr>
<td></td>
<td>- Continue tasks after user confirmation</td>
</tr>
<tr>
<td></td>
<td>- View recovery</td>
</tr>
<tr>
<td></td>
<td><strong>Recovery</strong></td>
</tr>
<tr>
<td></td>
<td>- Run recovery</td>
</tr>
<tr>
<td></td>
<td>- Preview recovery</td>
</tr>
<tr>
<td></td>
<td>- Stop an execution task</td>
</tr>
<tr>
<td></td>
<td>- Cancel a recovery</td>
</tr>
<tr>
<td></td>
<td>- Retry failed tasks for a completed recovery operation</td>
</tr>
<tr>
<td></td>
<td>- Retry failed tasks in a step and continue</td>
</tr>
<tr>
<td>Role</td>
<td>Permitted Operations</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Backup admin | - Ignore failures, continue without retry
                  - Continue task post user confirmation
                  - Commit plan after recovery                                |
|              | API token                                                                           |
|              | - Configure API token                                                               |
|              | Protected sites                                                                      |
|              | - Create, update, delete a protected site                                           |
|              | - Add or remove a DRC connector to/from a protected site                           |
|              | - Add or remove a vCenter to/from a protected site                                  |
|              | Protection groups                                                                    |
|              | - Create, edit, delete a protection group                                          |
|              | - Activate/deactivate protection group                                              |
|              | - Snapshots                                                                         |
|              | - Restore, edit, delete a snapshot                                                  |
|              | VMs                                                                                 |
|              | - Restore VM                                                                        |
| Plan tester  | DR Plans                                                                           |
|              | - Create, edit, delete, duplicate a DR plan                                          |
|              | Test recovery                                                                       |
|              | - Run a test recovery                                                                |
|              | - Stop a test recovery                                                               |
|              | - Cancel a test recovery                                                             |
## Role Permitted Operations

<table>
<thead>
<tr>
<th>Role</th>
<th>Permitted Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Rollback a test recovery</td>
</tr>
<tr>
<td></td>
<td>• Retry failed tasks</td>
</tr>
<tr>
<td></td>
<td>• Ignore failed tasks</td>
</tr>
<tr>
<td></td>
<td>Alarms</td>
</tr>
<tr>
<td></td>
<td>• Clear alarms</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SDDC admin</th>
<th>SDDCs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Configure an API token</td>
</tr>
<tr>
<td></td>
<td>• Create and delete an SDDC</td>
</tr>
<tr>
<td></td>
<td>• Add, rename, or delete a network on an SDDC</td>
</tr>
<tr>
<td></td>
<td>• Request a new public IP address</td>
</tr>
<tr>
<td></td>
<td>• Rename or delete a public IP address</td>
</tr>
<tr>
<td></td>
<td>• Add, remove hosts</td>
</tr>
<tr>
<td></td>
<td>• Add, edit, delete NAT rules</td>
</tr>
<tr>
<td></td>
<td>• Add, edit, delete new firewall rules</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>API token</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Configure API token</td>
</tr>
</tbody>
</table>
Dashboard

The VMware Cloud Disaster Recovery Dashboard provides easy access to all service features, including: setup guide, global summary, sites, topology map, and tasks and alarms.

Setup guide

The VMware Cloud Disaster Recovery UI provides a Setup guide on the main dashboard that provides step-by-step guidelines for performing main tasks in the application. For each main product use case, the setup steps window has a list of click-able links that lead directly to the feature in the UI.

Global summary

The global summary displays information about the systems listed in the Sites list, which are protected sites that have been configured for use with VMware Cloud Disaster Recovery, DR plans, and your recovery SDDC (if it has been deployed). The global summary panel shows the following information:
Using VMware Cloud Disaster Recovery

- **System Health.** Overall health of the system. Green indicates if a site is healthy; blue can change to yellow or red, depending on the entity’s health; gray nodes are those which are currently not reporting health and are likely not participating in any DR plans.
- **Cloud backup.** Shows the amount of available cloud backup storage.
- **Protected sites.** Shows the number of VMware Cloud Disaster Recovery protected on-prem vSphere sites.
- **Recovery SDDC.** Shows the deployed SDDC and how long it has been running.
- **DR Plans.** Shows the number of configured DR plans.

**Topology Map**

The topology map shows a dynamic representation of your VMware Cloud Disaster Recovery topology. Included in this view are any protected on-prem vSphere sites and the SDDC that is being used for recovery to VMware Cloud on AWS. The nodes in the topology map also reflect the health of the given entity as monitored by VMware Cloud Disaster Recovery.

An icon’s colors indicate the entity’s health:

- Green indicates if a site is healthy
- Blue can change to yellow or red depending on the entity’s health.
- Grey nodes are those which are currently not reporting health and are likely not participating in any DR plans.

**Topology map icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Recovery SDDC on VMware Cloud on AWS</td>
</tr>
<tr>
<td>Icon</td>
<td>Name</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td>Protected on-premises vSphere site</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
<td>Scale-out Cloud File System (SCFS)</td>
</tr>
</tbody>
</table>

**Arrows and Lines**

The dashed lines with an arrowhead in the topology represent single direction replication between the connected entities.

![Diagram](image3.png)

Protected site  Cloud backup

The bolder, dashed, non-arrowhead edge connecting the SCFS to an SDDC node represents the live mount connection from SCFS to the recovery SDDC. When replication occurs between nodes, the arrowhead edges will turn from dashed to solid, and when highlighted, will display the current data throughput rate for the data replication.
A line with slightly longer blue dashes ending in an arrowhead represent a configured recovery from one protected site to a recovery site (such as an SDDC):

You can highlight a node in the topology map, or highlight an item in one of site lists, by moving your mouse pointer over them, which highlights the protected site in the topology map and its corresponding system list item. In addition, all directly connected nodes and related edges in the topology will be emphasized (and all others de-emphasized) in order to give you a better at-a-glance view of which other systems are connected to the highlighted system.

**SDDC Deployment Types and Use Cases**

VMware Cloud Disaster Recovery provides two main SDDC deployment types that allow you to balance costs vs. RTO:
• On-demand (also known as "just-in-time")
• Pilot Light with cloud bursting

<table>
<thead>
<tr>
<th></th>
<th>Annual SDDC commitment</th>
<th>SDDC startup time</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>On demand</strong></td>
<td>Only when needed</td>
<td>Up to 90 minutes for cluster initiation, plus 15 minutes per host.*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Elastic DRS adds additional hosts as needed.</td>
</tr>
<tr>
<td><strong>Pilot light</strong></td>
<td>Minimum 3 VMware Cloud on AWS hosts at all times</td>
<td>Instant for critical VMs, plus 15 minutes per additional host required for full failover capacity*.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Elastic DRS adds additional hosts as needed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* Times to add additional hosts can vary, and can be less than the figures stated here, which are a conservative average based on testing. These times are subject to change as VMware continues to add more capabilities to VMware Cloud on AWS.</td>
</tr>
</tbody>
</table>

**RTO Components**

For each type of use case, VMware Cloud Disaster Recovery can include one or more dimensions of RTO:

• **Site RTO.** The aggregate time it takes to recover an entire site, composed of the execution times of one or more DR plans executing either concurrently or sequentially. This includes the time required to deploy the VMware Cloud on AWS SDDC and all its hosts.

• **DR Plan RTO.** The time it takes to recover all assets protected by a single DR plan, which may involve sequencing, scripting, or other pacing elements.

• **VM RTO.** The time it takes for ESXi to access an individual VM snapshot for restart.
On-demand

The on-demand (also known as "just in time") deployment of a cloud DR site provides an attractive alternative to continuously maintaining a warm standby cloud DR site. With on-demand deployment, the recurring costs of a cloud DR site are eliminated in their entirety until a failover occurs and cloud resources are provisioned.

The on-demand nature of public clouds enables VMware Cloud Disaster Recovery to drastically reduce the operating costs of disaster recovery by deploying the bulk of the DR infrastructure programmatically following a DR event. During steady-state operation, your VMware Cloud on DR costs remain low and you avoid having numerous active VMware Cloud on AWS hosts. The backups are sent to the SCFS, and after some processing, land in a cost-effective compressed and deduplicated form. In an on-demand type of deployment, a cloud DR site is created only following a disaster. A VMware Cloud on AWS SDDC provides a cloud DR site with a significantly larger server footprint and associated costs, which is deployed only immediately before executing a DR plan.
On-demand Deployment RTO

This deployment type eliminates the costs of running and maintaining an SDDC during normal operations, but increases your RTO.

If you do not want to use Pilot Light or an ahead-of-time deployment, you can use an on-demand deployment, which means you deploy your SDDCs after a disaster is already in progress or has occurred. This deployment type increases failover RTO by an additional 90 minutes for the SDDC deployment plus the length of time needed for SDDC configuration - the time it takes to create vSphere inventory objects such as folders and resource pools, configure the network, and then run the failover DR plan(s). Within the DR plans, VMs may be Live Mounted from SCFS snapshots from any point in time.
With this deployment type, continuous health checks are run every 30 minutes for the source and backup site to ensure that your failover DR plans and configurations are up to date and accurately reflect your environment. Health checks are then run just before a Failover to ensure the plan is in compliance between source and recovery site before the plan is run.

**Pilot Light with Cloud Bursting**

With a Pilot Light deployment, VMware Cloud Disaster Recovery enables a smaller subset of SDDC hosts to be deployed ahead-of-time for recovering critical applications with lower RTO requirements than a purely On Demand approach.

This deployment mode assists organizations to reduce the total cost of cloud infrastructure by keeping a scaled-down version of a fully functional environment always running in warm-standby while ensuring that core applications are readily available when a disaster event is triggered.

Upon use of a Pilot Light deployment, VMware Cloud Disaster Recovery presents an option for administrators to add extra SDDC hosts through Cloud Bursting and failover the remaining applications. Since there is no SDDC initiation time with a Pilot Light, expanding the SDDC by adding hosts happens in minutes providing a lower Site RTO for all applications than the Site RTO of the on-demand deployment at a fraction of the cost of the ahead-of-time deployment. A full SDDC deployment is a more time-consuming operation with a higher Site RTO impact than that of an SDDC expansion. A Pilot Light is a compromise solution with a range of options to balance costs vs. RTO.
A Pilot Light Deployment with Cloud Bursting RTO

This deployment type is useful when you need to mitigate the costs of an SDDC deployment and can accept a slightly longer Site RTO but you still need a low VM RTO/DR Plan RTO for certain workloads.

With such a ‘Pilot Light’ approach, you can deploy a site subset of 3 SDDC hosts ahead of time, with these hosts enabling you to immediately recover critical applications that have lower VM RTO requirements. If more than 3 hosts are required to recover your whole site, you will need to “inflate” the Pilot Light SDDC by adding additional hosts servers. This Pilot Light inflation can be done simultaneously with the Live Mount of mission critical workloads.
With this deployment type, continuous compliance checks are run against both source and target sites every 30 minutes to ensure that your failover DR plans and configurations are up to date and accurately reflect your current environment.

The Site RTO is much shorter than that of an On-Demand SDDC, and is equal to roughly the time it takes to add additional hosts and failover to your already running SDDC. Adding hosts to an already deployed SDDC takes roughly 15 minutes. Additionally, some applications can be pre-deployed on the Pilot Light SDDC during normal operation.

**Additional Use Cases**

These additional use cases further illustrate key VMware Cloud Disaster Recovery capabilities:

**DR for General Purpose Workloads**

For protecting production workloads, you can create snapshots of your VMs and files and replicate them to the SCFS, then create DR plans for failover to the recovery site. In the event of disaster, select the most recent available snapshots for failover.

VMware Cloud Disaster Recovery will automatically check your DR plan for health and compliance every 30 minutes, so you can be confident when a DR event occurs, you can successfully fail over to your SDDC in the public cloud in a short amount of time.

**Single VM Recovery from Snapshots**

Once a snapshot has been taken of VMs on your VMware Cloud Disaster Recovery protected site, you can restore individual VMs from a snapshot. The VM will be restored to the same state it was in when the snapshot was taken, including its vCenter location, configuration, data, etc.

This is useful in cases where an important application is running on a single VM, and when you need to, you can select a recent snapshot of the VM and restore it from the VMware Cloud Disaster Recovery UI.

**Note:** Single VM recovery is supported only for VMs that are included in a VMware Cloud Disaster Recovery protection group.
See Restore a VM for more information.

Ransomware Recovery

Ransomware is becoming more and more prevalent and severe, whereby malicious hackers steal (or encrypt) valuable company data and extort large ransom payments to allow the owner access to their data.

In this use case, you can use VMware Cloud Disaster Recovery to create regular, secure remote backups of critical data through regularly scheduled, application consistent snapshots of VMs and files.

In the event of a ransomware attack, you can easily 'go back in time' to a moment before the attack occurred and recover snapshots or backups from months or years ago. You can use these snapshots to rebuild your VMs and computing environment in a new SDDC deployment to VMware Cloud on AWS.

DR for VDI systems

Virtual Desktop Infrastructure (VDI) systems are used by many organizations to create remote computer environments for end users without needing to buy extra hardware. This can reduce infrastructure costs, but creates a risk concentration in those systems that are running the VDI VMs. These virtual desktops need DR protection just like a physical machine. VMware Cloud Disaster Recovery can provide disaster recovery protection for the VMs that power virtual desktops, as well as the other types of software needed to enable the virtual technologies (e.g., Active Directory, connection servers, etc.).

For example, you might want to spin up VDI desktops for temporary usage, to provide temporary virtual compute resources for a short term project with contract workers. You can use DR plans to recover VDI VMs and other files to create a temporary SDDC for the work. Once the project is finished and the temporary workers no longer need their desktops, you can tear down the SDDC and resume normal operations.

Currently, the following features are not supported for VDI desktops:
- App volumes
- Modifying the golden master image once failed over
Deploying a Recovery SDDC

Using VMware Cloud Disaster Recovery with VMware Cloud on AWS, you can deploy a Recovery SDDC in your cloud environment and configure it as a recovery site.

There are three general types of Recovery SDDC deployments:

- **Single-host SDDC.** A single-host Recovery SDDC can be used for building and testing your DR plans, after which the Recovery SDDC can be deleted to save recurring costs. A single host SDDC does not provide any data protection, does not offer production level SLAs, and will automatically be torn down in 30 days. A single-host deployment should only be used for testing purposes and is not intended for production usage.

- **3-host ‘Pilot Light’ SDDC.** If you are using a Pilot Light deployment, we recommend a minimum of a 3-host Recovery SDDC deployment to reduce recovery time by having a readily usable SDDC.

- **On-demand.** If you are not using a VMware Cloud on AWS Pilot Light, you can use an 'on-demand' deployment, which means you deploy your Recovery SDDCs with one or more hosts after a disaster is already in progress or has occurred. This type of deployment is also sometimes referred to as a 'just-in-time' deployment.

If you deploy a single-host Recovery SDDC (also known as a ‘starter’ SDDC), it will be deleted after 30 days and all data on the Recovery SDDC will be lost. For this reason a single host SDDC should only be used for testing purposes, not in production.

You can scale-up a single host SDDC into a 3 or more ‘multi-host’ SDDC and retain all your data. A multi-host SDDC with 3 or more hosts is not time bound but is subject to recurring costs. A multi-host SDDC also provides data protection and production level SLAs.

**Tip:** For more information about VMware Cloud Disaster Recovery configuration limits, visit the [VMware Configuration Maximums](#) tool.

**Note:** Any vSphere clusters you add to your SDDC from the VMware Cloud Services console will not be usable with VMware Cloud Disaster Recovery. This means you cannot use this cluster (and any VMs associated with it) in snapshots or DR plans.
Available AWS Regions

VMware Cloud Disaster Recovery is available in the following AWS regions:

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>ap-south-1</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>ap-southeast-1</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ap-northeast-1</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>eu-central-1</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>u-west-1</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>eu-west-2</td>
</tr>
<tr>
<td>Europe (Paris)</td>
<td>eu-west-3</td>
</tr>
<tr>
<td>US West (N. California)</td>
<td>us-west-1</td>
</tr>
<tr>
<td>US East (Ohio)</td>
<td>us-east-2</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
</tr>
</tbody>
</table>

SDDC and Your AWS Account

When you deploy your Recovery SDDC, it must be connected to an AWS account belonging to you, called the 'customer AWS account'. This connection allows your SDDC to access AWS services belonging to your AWS customer account. VMware recommends creating a subnet in every AWS Availability Zone in the same region where the SCFS is deployed. VMware Cloud also imposes several other requirements for a network configuration of the customer account as outlined here.
SDDC and Cluster Names

Cluster names are given automatically when you create a new cluster; you cannot provide a custom name for clusters you add to your SDDC.

Clusters added to an SDDC follow this naming pattern: 'Cluster-<x>-<y>'. For example, the first cluster for your first SDDC is named: Cluster-1-1. If you add another cluster to the same SDDC, the new cluster’s name is ‘Cluster-1-2’, and so on.

If you tear down the first SDDC, the cluster names in any DR plans will change and appear with an asterisk (*) for the SDDC name, such as 'Cluster-*-1' and Cluster-*-2. When the second SDDC is deployed, the UI displays the proper cluster names in the DR plans with the incremented SDDC name.

This same behavior applies to cluster names in plan compliance reports. If the SDDC is currently deployed, then the cluster names will appear with the correct name in the report, such as ‘Cluster-1-2’. If the SDDC is deleted at the report is run, then the cluster name will use the asterisk, such as 'Cluster-*-2'.

Deploy Recovery SDDC

You can deploy a Recovery SDDC from the VMware Cloud Disaster Recovery UI.

Important: Once you deploy a Recovery SDDC, follow the guidelines listed here: Maintaining SDDC Settings to ensure a consistent SDDC configuration

Procedure

1. In the VMware Cloud Disaster Recovery UI, click Sites → Recovery SDDC.
2. On the page, click the Deploy SDDC button.
3. In the Deploy Recovery SDDC dialog, enter the following information:
   - SDDC Settings:
     - Name. Enter a name for your Recovery SDDC.
- **Deployment type: Single Host.** If you choose a single-host SDDC, keep in mind that it will expire within 30 days of deployment and all its content will be permanently deleted. A single host SDDC is recommended only for testing and should not be used in production. If you want a permanent Recovery SDDC, choose the multi-host option and select the numbers of hosts to deploy. A single host SDDC can only use the I3 host type. If you want to deploy with I3en hosts, you must deploy a multi-host SDDC.

A single-host SDDC can be upgraded to a multi-host SDDC. However, once you upgrade to a multi-host SDDC, you cannot later downgrade it to a single host.

Scroll down in the dialog to the Host type section, where you can see options for a multi-host deployment:

- **Deployment type: Multi-host.** If you select Multi-host option, you can select I3 or I3en hosts.
  - The I3 host type is the default host type. I3 hosts have 36 cores, 512GiB RAM, and 10.37TiB raw storage capacity per host.
  - The I3en host type is optimized for data-intensive workloads. I3en hosts have 96 logical cores, 768GiB RAM, and approximately 45.84 TiB raw storage capacity per host. Single-host or two-host Recovery SDDCs cannot contain the I3en host type.

- **Number of hosts.** For multi-host deployments, choose 3 or more hosts. Be aware that adding a host increases the available storage capacity and costs.

- **Management subnet.** Enter a subnet for the management network of the Recovery SDDC. This is a private subnet range (RFC 1918) to be used for vCenter Server, NSX Manager, and ESXi hosts.
  - Choose a range that will not conflict with other networks that you will connect to this SDDC.
  - Minimum CIDR sizes: /23 for up to 27 hosts, /20 for up to 251 hosts, /16 for up to 4091 hosts. Reserved CIDRs: 10.0.0.0/15, 172.30.0.0/16. Enter a CIDR block of size either /16 or /20.
- **Compute subnet.** Enter a gateway logical network for the Recovery SDDC. This is a private subnet range for the logical network that the workload VMs will use. Note that only one logical network is created by default. More networks can be created via VMware Cloud Disaster Recovery UI after the SDDC is deployed. For more information, see [Add a Network to an SDDC](#).

- **AWS settings.** Choose the AWS account you want to associate with your SDDC. If you only have one AWS account associated with VMware Cloud Services, then the AWS account will already be selected here. If the availability zone (AZ) where the Recovery SDDC is being deployed has more than one subnet configured, you can select the subnet from the drop-down list, next to the name of the VPC where the SDDC will be deployed.

3. When you are ready to deploy the Recovery SDDC, enter the phrase DEPLOY SDDC in all uppercase letters in the confirmation box, and then click **Deploy**.

### SDDC Usage Daily Email Reminder

Because deploying an SDDC accrues costs, you will receive a daily email reminder to let you know that you have an SDDC deployed, how many hours it has been running, and when it expires (if applicable). The email also indicates how many hosts are associated with this SDDC.

The email reminder will automatically be sent to all email addresses you have configured for alerts in the Configure VMware Cloud Disaster Recovery dialog.

When this email reminder is sent, an event is triggered that sends a daily email to tell you the name of your SDDC and the number of days left before it expires.

### SDDC Datastore

When an SDDC is deployed, the system automatically creates an NFS datastore named 'ds01'.

This NFS datastore is created exclusively for the purpose of exposing VM backups to the SDDC to facilitate disaster recovery and should never be used as general-purpose...
storage. Do not use the vSphere Client, vSphere APIs, or any other means to create and power on VMs directly on this NFS datastore except through the capabilities and workflows available in VMware Cloud DR.

**Delete an SDDC**

When you are ready to stop using your SDDC (and stop accruing further recurring costs), you can delete it.

**Important:** When you delete an SDDC, all running workloads will be terminated, all VMs will be destroyed, and all SDDC data and configurations will be lost.

**Procedure**

1. Click the Sites → SDDC tab.
2. From the small menu next to the Open vCenter button, click **Delete Recovery SDDC**.
3. In the dialog, enter the phrase DELETE SDDC INCLUDING VMS AND SETTINGS in all upper case letters to confirm, and then click **OK** to delete the SDDC.

**Add/Remove Hosts**

You can add hosts to clusters in your SDDC to expand your recovery capacity. A single cluster can support one host type, either I3 or I3en:

- I3. I3 hosts have 36 cores, 512GiB RAM, and 10.37TiB raw storage capacity per host.
- I3en. The I3en host type is optimized for data-intensive workloads. I3en hosts have 96 logical cores, 768GiB RAM, and approximately 45.84 TiB raw storage capacity per host. Single-host or two-host SDDCs cannot contain the I3en host type.

If there is one existing host in the cluster, you can add exactly 2 hosts (no other option available). You cannot revert back from a 3 host cluster down to a 1 host cluster. If there are 3 or more hosts, you can add multiple hosts. For more information on VMware Cloud Disaster Recovery limits, see [https://configmax.vmware.com/home](https://configmax.vmware.com/home).
**Note:** Adding a host will increase both the available storage capacity and costs.

**Note:** If your cluster has 3 or more hosts, and during operation your data grows beyond the capacity of the configured vSAN, VMware’s Elastic DRS will automatically add a host if the SDDC’s free space drops below 25%. Hosts are never removed automatically, but can be removed in the VMware Cloud Disaster Recovery UI all the way down to 3 hosts. Keep in mind also that you cannot remove hosts from 3-host SDDC.

**Procedure — Add a Host**

1. In the VMware Cloud Disaster Recovery UI, click the Sites → Recovery SDDC view.
2. Under the Clusters section, click the **Add hosts** button to the right of the cluster you want to add hosts to. You can only add one host type to a cluster, either I3 or I3en.
   If a cluster only has one host, then the **Delete** button will be deactivated. If there is one existing host, you can add exactly 2 hosts (no other option available). If there are 3 or more hosts, you can add up multiple hosts up to the supported limits.
3. The dialog will show the current number of hosts in the cluster and the estimated capacity. Enter the number of hosts you want to add. The dialog shows the projected storage capacity for the number of hosts to be added.
4. To add the hosts, enter the phrase **ADD HOSTS** in the text field in all upper case letters and then click **OK**.

**Procedure — Remove a Host**

**Note:** If your cluster has only 1 host, then that single host cannot be deleted.

1. In the VMware Cloud Disaster Recovery UI, click the Sites → Recovery SDDC tab.
2. Under the Clusters section, next to the cluster you want to remove hosts from select **Remove hosts** from the drop-down menu.
   If a cluster has three hosts, then this menu item will be grayed out. You cannot remove hosts from a 3 host cluster.
3. In the Remove hosts dialog, enter the number of hosts you want to remove. When you enter a number, the dialog will estimate the amount of removed capacity that will be freed when you remove the hosts.

4. Enter the phrase REMOVE HOSTS in all upper case letters in the text field to confirm.

5. Click OK.

Add/Delete a Cluster

You can add clusters to your Recovery SDDC, with each additional cluster created in the same availability zone as the initially deployed SDDC. Each cluster can support only one host type, either 13 or 13en.

Your SDDC must have a 3 hosts cluster before you can add additional clusters. If you have already deployed a single host cluster, you cannot add a second cluster to your Recovery SDDC until you upgrade to a 3 host cluster.

Caveats for Adding Clusters

There are a few caveats to consider when adding a cluster to your Recovery SDDC:

- Each additional cluster you add increases the costs of your Recovery SDDC.
- You cannot delete the default cluster that was created when your Recovery SDDC was first created (displays as 'cluster1' in the VMware Cloud Disaster Recovery UI).
- You should only add clusters to your SDDC using the VMware Cloud Disaster Recovery UI (not in the VMware Cloud on AWS console). Clusters added to the SDDC using the VMware Cloud on AWS console are not supported. If a cluster is added to your SDDC from the VMware Cloud on AWS console, it will appear in the VMware Cloud Disaster Recovery UI with a status of "Unconnected".
- Before you delete a cluster, make sure you check for any potential breakage to mappings in your DR plans.
Procedure - Add a Cluster

Note: When you first add a cluster to your SDDC, you can only add a 3 or 4 host cluster. Deploying a 3-host cluster takes roughly one hour. You can add either I3 or I3en hosts to a cluster.

1. In the VMware Cloud Disaster Recovery UI, click the Sites → Recovery SDDC tab.
2. Click to expand the Clusters section, and then click Add cluster button.
3. In the Add cluster dialog, select the number of hosts you want to add to this cluster (minimum of 3 hosts).
4. Next, select the host type you want to add to this cluster, either I3 or I3en.
5. In the Confirm section, enter the phrase ADD CLUSTER in all upper case letters.
6. When you are ready to add the cluster, click Add cluster.

Procedure - Delete a Cluster

Note: You cannot delete the first cluster that was created ('cluster1') on your Recovery SDDC.

1. In the VMware Cloud Disaster Recovery UI, click the Sites → Recovery SDDC tab.
2. Click to expand the Clusters section, and then from the small drop-down menu on the right select Delete cluster.
3. In the Delete cluster dialog, under the Confirm section, enter the phrase DELETE CLUSTER in all upper case letters.
4. When you are ready to add the cluster, click Delete cluster.

Add a Network to an SDDC

Since you are not able to create a network in the SDDC vCenter, use VMware Cloud Disaster Recovery to create a routed network segment for your SDDC. For example, if some of your VMs need to connect over logical networks beyond the default network that was created when you first requested the SDDC, you can use VMware Cloud Disaster Recovery to change the default network.
Procedure

1. From the Sites → Recovery SDDC view in the VMware Cloud Disaster Recovery UI, in the drop-down menu next to the Open vCenter button, click the icon and from the menu select Add network:

2. In the Add network dialog, enter the following information:

   - **Network name**: Any name you want to give the network.
   - **Gateway**: The IP address of the Gateway. For example: 192.0.2.1
   - **Bits**: Add an IP prefix for the gateway. For example: 27.
   - **Optional**: DHCP. You can activate DHCP for the new network. In these fields, add the Gateway IP address range.

3. Click **OK**.

4. Once the network is created, you can rename it if you wish by clicking the Rename button.

Request Public IP Addresses

If you want to use public IP addresses for your workloads, you can request them for your SDDC network. Once you have public IP addresses, you can create NAT rules to map them to private IP addresses assigned for your VMs.

**Important**: Public IP addresses increase VMware Cloud Disaster Recovery costs. You can release public IP addresses that are not in use.

Procedure

1. From the Sites → Recovery SDDC view in the VMware Cloud Disaster Recovery UI, under Public IPs click the **Request new IP** button.

2. In the Request public IP dialog, enter an optional label for the public IP address. This is not required, but can be useful for identifying the app or VM that the public IP address is being used for. You can only use letters, numbers, and hyphens when entering the Public IP address label.
3. Click OK.
4. The new public IP address appears under Public IP addresses on the Failover SDDC page. You can rename the IP address label at any time by clicking the Rename button.
5. To delete the public IP address, click Delete.

**Add NAT rules**

You can configure Inbound Network Address Translation (NAT) rules for mapping internet traffic to a public-facing IP address to a private IP address in the SDDC’s compute network.

*Note:* This feature allows you to map public IP addresses to private IP addresses and all services that communicate over whichever port is assigned to the private IP address. If you need to map specific ports or services, contact Support.

**Procedure**

1. From the Sites -> Recovery SDDC view in the VMware Cloud Disaster Recovery UI, under NAT rules click the **Add new rule** button.
2. In the Add new rule dialog, enter the following information:
   - **Rule name.** Enter a name for the NAT rule.
   - **Public IP address.** Enter a public IP address.
   - **Private IP address.** Enter the internal IP address to map the public IP address to.
3. Click **OK**.
4. After the NAT rule is created, click the **Edit** button if you want to rename the rule, or to change the public or internal IP addresses.

**Add firewall rule to SDDC network**

You can add firewall rules to allow or block specific traffic to and from the SDDC network. You can add firewall rules to allow or deny all connections or specific IP
addresses or a range of IP addresses. You can also configure specific services and ports to be allowed or blocked in the rules.

Tip: If there is a firewall rule you are unable to create using the VMware Cloud Disaster Recovery UI, contact Support for assistance.

About SDDC Firewall Rules

Currently, the VMware Cloud DR UI does not display all possible types of SDDC firewall rules that you can create in the VMware Cloud on AWS Console UI. This means it is possible to create some SDDC firewall rules in the VMware Cloud on AWS Console that may not appear in the VMware Cloud DR UI.

By default, when your SDDC is deployed, its network will contain a set of pre-configured firewall rules which begin with the "CloudDR-SystemRule-" prefix. These firewall rules should not be deleted. (Keep in mind that SDDC Firewall rules with this prefix cannot be edited or deleted in the VMware Cloud Disaster Recovery UI, but these rules can be edited and deleted in the VMware Cloud on AWS console UI.

Warning: Make sure you do not delete any SDDC firewall rules which begin with the "CloudDR-SystemRule-" prefix.

Firewall rules with this prefix cannot be edited or deleted in the VMware Cloud Disaster Recovery UI. However, these rules can be edited or deleted in the VMware Cloud on AWS console UI. So, make sure you do not delete any SDDC firewall rules that begin with the "CloudDR-SystemRule-" prefix.

When a user creates a new firewall rule in the VMware Cloud DR UI, those rules will begin with the "CloudDR-UserRule-" prefix. Firewall rules with this prefix can be edited and deleted by VMware Cloud DR users that have the SDDC admin service role granted to them.

Procedure

1. From the Sites → Failover SDDC view in the VMware Cloud Disaster Recovery UI, under Firewall rules, click the **Add new firewall rule** button.
2. In the Add firewall rule dialog, enter a descriptive name for the rule.
3. Under Source, choose Any to specify traffic from any source, or select IP address to enter individual IP addresses or an IP address range.

4. Under Destination, choose Any to specify all traffic to any destination, or select an IP address to enter individual IP addresses or an IP address range.

5. Under Services, choose Any if you want to create a rule for any service on this connection, or select a specific service from the drop-down list and enter the ports on which those services run.

6. Under Action, select either Allow or Drop to permit or deny the specified connection.

7. Click OK when you are finished.

Maintaining SDDC Settings

In order to ensure the health and availability of the overall VMware Cloud Disaster Recovery service offering, the following list SDDC settings should not be changed in the VMware Cloud Disaster Recovery UI.

Changing any of these SDDC settings could interfere with and potentially disrupt the delivery and functioning of the service.

Tip: For more information about VMware Cloud Disaster Recovery configuration limits, visit the VMware Configuration Maximums tool.

SDDC Settings You Should Not Change

Once you have deployed your SDDC, do not change any of the following settings or configurations in the VMware Cloud Disaster Recovery UI:

- **SDDC default firewall rules.** Changing the SDDC firewall could interrupt access from the SDDC to the SCFS or Orchestrator components. By default, when your SDDC is deployed, its network will contain a set of pre-configured firewall rules which begin with the "CloudDR-SystemRule-" prefix. These firewall rules should not be deleted. Keep in mind that SDDC Firewall rules with this prefix cannot be edited or deleted in the VMware Cloud Disaster Recovery UI, but these rules can be edited and deleted in the VMware Cloud on AWS console UI. Make sure you do not delete any of these SDDC firewall rules.
- **Do not rename your SDDC once you have deployed it.** Once you name and deploy your SDDC, do not change its name.

- **Network configuration on the Proxy VM.** Changes to the network configuration on the proxy VM should not be made.
**DRaaS Connector and Protected Sites**

VMware Cloud Disaster Recovery DRaaS connector is a stateless connector software appliance that replicates snapshot deltas from protected sites to the SCFS, driven by policies you set in Protection Groups.

You install the DRaaS connector into an on-premises vSphere environment as a virtual machine, which then connects to VMware Cloud Disaster Recovery with VMware Cloud on AWS. Once the connector is installed in your vSphere environment, your vSphere environment is now considered by VMware Cloud Disaster Recovery as a "protected site."

You can view protected sites under the Sites view in the VMware Cloud Disaster Recovery UI.

Once your protected site is configured, policies are created, and snapshots are replicated to the SCFS, you can recover protected VMs from available snapshot backups into your SDDC in VMware Cloud on AWS. Once the protected site is available again, you can initiate failback using VMware Cloud Disaster Recovery.
Dimensions of Protected Site

A VMware Cloud Disaster Recovery protected site encompasses vCenters, protection groups (PGs) and DR plans. A site include vCenters which contain the VMs you want to protect in a set of plans. A vCenter can only belong to one site, and protection groups (PGs) and DR Plans can only be associated with one vCenter, as illustrated in the image below:

Tip: For more information about VMware Cloud Disaster Recovery configuration limits, visit the VMware Configuration Maximums tool.
vSphere Protected Site

VMware Cloud Disaster Recovery for an on-premises vSphere environment protects VM data backed by any physical storage infrastructure.

In this topology, you can:

- Use VMware Cloud Disaster Recovery to protect your vSphere infrastructure.
- **Create a Protection Group** to identify VMs you want to backup and define snapshot frequency and retention. On that policy basis, VMware Cloud Disaster Recovery will forward changed blocks to the SCFS, which serves as the backup vault used for recovery to VMware Cloud on AWS.
- Create **DR Plans** to orchestrate recovery to your SDDC to VMware Cloud on AWS, and failback when ready.
Protecting a Site

Using VMware Cloud Disaster Recovery, you can protect and provide automated DR for any VMs running on vSphere on-premises environments or in VMware Cloud on AWS.

1. Create a protected site

A protected site in VMware Cloud Disaster Recovery consists of the DRaaS Connector, vCenters, and VMs you want to be protected by cloud backup and DR orchestration. A protected site is comprised of one or more vCenters running in a customer's on-prem environment.
2. **Deploy the DRaaS Connector**

The DRaaS Connector is a stateless VM that connects to your vSphere environment. You download the DRaaS Connector and deploy it as an OVA to in your vCenter. The DRaaS Connector can be redeployed if needed at any time without losing backup data. Software upgrades for it are over-the-air and automatic across time. Each DRaaS Connector provides additional replication bandwidth for the site.

3. **Register vCenter**

Next, using the VMware Cloud Disaster Recovery UI you need to register the protected site's vCenters with DRaaS. Once you provide access to vSphere, you can deploy additional DRaaS Connectors to the site to improve bandwidth to the cloud, if desired.

4. **Create a Protection Group**

To protect your data and fight potential disasters, you can create protection groups (PGs) for your VMs. Protection groups specify the VMs that are to be replicated to the cloud and snapshotted. Schedules can be associated with protection groups so that snapshots are automatically taken periodically.

In the event of a disaster, you can use these replicated snapshots to "go back in time" to a last-known clean snapshot, from before the attack occurred, so you can restore your "clean" VMs and data quickly.

5. **DR Plans**

Now that you have set up your protected site, and created protection groups that will regularly replicate snapshots to SCFS, you can create DR plans that define the orchestration steps for automated recovery.

**Set up a Protected Site**

Protecting your on-premises vSphere environment with VMware Cloud Disaster Recovery requires performing the following tasks:
1. Define a protected site
2. Deploy and configure the DRaaS Connector
3. Register vCenter (requires a vCenter Administrator account credentials)

**Note:** Your user account must have the Administrator or Backup admin role associated with it in order to perform these tasks.

**Procedure**

1. In the VMware Cloud Disaster Recovery UI, click Sites → Protected sites.
2. Click the **Set up protected site** button in the upper right corner.
3. In the dialog, enter a name you have chosen for the protected site.
4. Select a timezone from the drop-down list, and then click the button to the right to set the time zone for the protected site.
5. Click OK.

**Register vCenter**

Once you have deployed the DRaaS Connector and configured it, you need to register the vCenter you want it to protect.

Registering vCenter with the DRaaS Connector requires your vCenter credentials (username and password). These credentials are not stored by VMware Cloud Disaster Recovery.

**Procedure**

1. In the VMware Cloud Disaster Recovery UI, under Sites -> Protected sites, click the on-prem vSphere protected site.
2. On the right side, click the **Register vCenter** button.
3. In the Register vCenter dialog, enter the vCenter server's IP address.
4. Then, enter the vCenter user name and password. (This vCenter user account must possess the vCenter admin-level role.)
5. Click **Register**.
Deploy the DRaaS Connector

After the protected site is created for your on-prem vSphere, you need to download and deploy the DRaaS Connector virtual machine in your vSphere environment.

Deploying the DRaaS Connector requires using both the VMware Cloud Disaster Recovery UI and the vSphere UI.

DRaaS Connector VM Requirements

In order to deploy the DRaaS Connector VM, make sure that the vSphere site where you intend to deploy it has the following available resources for the VM:

- **CPU**: 8 GHz (reserved)
- **RAM**: 12 GiB (reserved)
- **Disk**: 100 GiB vDisk
- **Network connectivity**:
  - Between DRaaS Connector and vCenter and ESXi hosts
  - Between DRaaS Connector and VMware Cloud Disaster Recovery

**Note**: Non-ASCII characters are not permitted for the connector name label.

Ports Required

Your vSphere network configuration needs the following ports open:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Service Description</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1759</td>
<td>TCP</td>
<td>DRaaS Connector</td>
<td>Scale-Out Cloud File System and SaaS Orchestrator</td>
<td>Encrypted tunnel for data transfers and metadata operations</td>
<td>Outbound</td>
</tr>
</tbody>
</table>

VMware, Inc.
<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Service Description</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>DRaaS Connector</td>
<td>vCenter Server</td>
<td>vCenter Web service</td>
<td>Inbound/outbound</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>DRaaS Connector</td>
<td>SaaS Orchestrator</td>
<td>Management service</td>
<td>Inbound/outbound</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>DRaaS Connector</td>
<td>VMware auto-support server</td>
<td>Support service</td>
<td>Outbound</td>
</tr>
<tr>
<td>22</td>
<td>TCP</td>
<td>DRaaS Connector</td>
<td>Scale-Out Cloud File System and SaaS Orchestrator</td>
<td>Software upgrades and remote support access</td>
<td>Inbound</td>
</tr>
<tr>
<td>902</td>
<td>TCP</td>
<td>DRaaS Connector</td>
<td>ESXi Management IP address</td>
<td>Reading/writing vdisks</td>
<td>Inbound</td>
</tr>
</tbody>
</table>

**DRaaS Connector Deployment and SSL Certificate Warning**

When deploying the DRaaS Connector virtual machine .ova in vCenter 6.7 or newer, if you receive a message stating 'SSL certificate cannot be trusted', you have two options:

- Proceed and click **Yes** to accept the certificate.
  
  OR
  
- Install in the necessary certificate authority root certificate in vCenter to enable verification (instructions below).

**Procedure**

1. In a browser, go to [https://www.entrust.com/resources/certificate-solutions/tools/root-certificate-downloads](https://www.entrust.com/resources/certificate-solutions/tools/root-certificate-downloads)
2. Download the Entrust Root Certification Authority (G2) Root Certificate (You can also download the cert directly by going to https://web.entrust.com/root-certificates/entrust_g2_ca.cer.

3. In your vCenter, go to Menu → Administration → Certificate Management

4. Click to add a new Trusted Root Certificate, and use the downloaded 'entrust_g2_ca.cer'.

**Download the DRaaS Connector OVA (VMware Cloud Disaster Recovery UI)**

Your first task is to download the DRaaS Connector OVA. Using the VMware Cloud Disaster Recovery UI, you can obtain a URL you can copy to download the OVA into your environment.

**Procedure**

1. In the VMware Cloud Disaster Recovery UI, under Sites → Protected sites, click the protected site on the left side of the application.

2. On the Protected sites page under Connectors, click the **Download** button.

3. In the Download connector dialog, there is a list of steps that guide you in deploying the connector, as well as the URL to the connector OVA, with an option to download it locally to your system.

4. Click the **Copy** button to copy the connector download URL. You will need this URL when you deploy the OVA in vSphere wizard after you download the connector.

5. Make a note of the Console credentials, which you will need to log in to the VM console: 'admin'/vmware#1'.

6. Also copy (or write down) the Orchestrator Fully Qualified Domain Name (FQDN), which is needed when you configure the connector in the VM console.

7. Click **OK**.
Deploy the DRaaS Connector (vSphere UI)

When you deploy the DRaaS Connector from the vSphere UI, you need to select the host, cluster, or resource pool. The DRaaS Connector will have access to the resources of the selected object.

For example, a VM has access to the memory and CPU resources of the host on which it resides.

Procedure

1. In the vSphere web console, select any inventory object that is a valid parent object of a virtual machine, such as a datacenter, folder, cluster, resource pool, or host, right-click and select Actions → Deploy OVF Template.
2. Click Next.
3. In the Deploy OVF Template dialog, Step 1, Select an OVF template, paste the connector OVA URL into the URL field. The exact URL to download the connector OVA is located in the Download Connector dialog. For example: https://<vmware-cloud-dr-ip-address/cloud-connector.ova.
4. Click Next.
5. Next, select a location for the connector. Choose a folder or site, and then click Next.
6. Select a compute resource for the connector, and then click Next.
7. Review the details for your connector deployment, then click Next to select storage for the connector VM.
8. Select a storage device for the connector and then click Next.
9. Select the network for the connector, and then click Next to review the deployment details.
10. Click Finish. You can now find the Connector VM in your vSphere client.
11. At this point, you should reserve the memory and CPU resources for the VM, as listed DRaaS Connector VM Requirements.
Configure the DRaaS Connector Using the VM Console

Before you configure the DRaaS Connector VM using the CM console, make sure you have all needed information by filling out this (optional) worksheet:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console credentials</td>
<td>admin/vmware#1</td>
</tr>
<tr>
<td><strong>Note:</strong> This password will change at the end of the configuration, and you can obtain the new password in the VMware Cloud Disaster Recovery UI.</td>
<td></td>
</tr>
</tbody>
</table>

If using a static IP address allocation for the Connector:

- IP address: You can enter up to 3, separated by spaces
- Subnet mask
- Gateway
- DNS servers

**Warning:** Google DNS servers (8.8.8.8 and 8.8.4.4) do not work reliably with VMware Cloud Disaster Recovery. We advise that you to use non-Google DNS servers when configuring the Connector VM.

<table>
<thead>
<tr>
<th>VMware Cloud Disaster Recovery FQDN</th>
<th>This temporary passcode is used to configure the DRaaS Connector in the VM console CLI.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td><strong>Tip:</strong> A passcode can be obtained in the Download connector VM dialog from inside the VMware Cloud Disaster Recovery UI. Make sure that you open the dialog from the specific site you want the DRaaS connector to able to connect to.</td>
<td></td>
</tr>
<tr>
<td>Name) to give the connector, as it will appear in the VMware Cloud Disaster Recovery UI</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Use the vSphere web console for this task. Do not use an SSH session to configure the DRaaS Connector VM. You'll need to use the vSphere web console if DHCP is not enabled on your network.

**Note:** The name you give the DRaaS Connector VM should not be similar to the naming conventions you use to name VMs in your vSphere environment. The purpose of this is to avoid giving the DRaaS Connector VM a name that might match the VM name pattern you use when you define protection groups.

Additionally, non-ASCII characters are not supported for the connector name.
Procedure

1. In the vSphere client, select the DRaaS Connector VM, right-click and choose Power → Power on.
2. Under the VM, click Launch web console.
3. When the console session is open, log in to the connector VM console using the following credentials: admin/vmware#1.
4. Next, in the Select the network address IP address allocation, either (a) Static or (b) DHCP.
5. If you chose (a) for static IP address allocation:
   Enter an IP address, Subnet mask, and Gateway.
   Enter the IP address of the DNS server.

   Note: Google DNS servers (8.8.8.8 and 8.8.4.4) do not work reliably with VMware Cloud Disaster Recovery. We advise that you to use non-Google DNS servers when configuring the Connector VM.

6. Next, enter the Orchestrator FQDN (it is located in the browser URL field).
7. Next, enter the DRaaS Connector temporary passcode.
8. Enter a name to identify the connector. Note: Non-ASCII characters are not supported for the connector name.
9. After the DRaaS Connector has been configured, the console window will return you to the command prompt. You can now return to the VMware Cloud Disaster Recovery UI to Register vCenter for this protected site.

Send Support Bundle

For troubleshooting and diagnostic purposes, you can send VMware support information about a given protected site (and the DRaaS Connector), called a 'support bundle'.

When you submit a support bundle, VMware Cloud Disaster Recovery collects support data, creates a support bundle, and sends it to the VMware Support team. Typically, you should submit a support bundle after consulting with VMware support.
Procedure

1. In the VMware Cloud Disaster Recovery UI, click Sites → Protected sites.
2. From the upper right of the window, click the drop-down menu and select Send support bundle.
3. In the dialog, click the Submit support bundle button.

Manage a Protected Site

Once you have created a protected site, you can manage the site by performing the following tasks:

- Edit a protected site
- Remove a vCenter from a protected site
- Remove a DRaaS Connector from a protected site
- Delete a protected site

Edit a Protected Site

To edit or delete an on-prem protected site, follow the steps below.

Procedure

1. To edit or delete a site, click the Sites → Protected sites tab.
2. Click the site you want to edit or delete.
3. From the upper right side of the VMware Cloud Disaster Recovery UI, click Edit site from the drop-down menu, select Edit site (or Delete site, if you are deleting the site).
4. If you are editing the site, in the Edit site dialog, you can change the protected site name label, or change the time zone for the site.
5. If you are deleting the site, click Delete site from the menu.
6. Enter the phrase DELETE SITE in all upper case letters then click OK.
Remove a vCenter from a Protected Site

To remove a vCenter from an protected site, follow the procedure below.

Procedure

1. Click the Sites → Protected sites tab in the VMware Cloud Disaster Recovery UI.
2. From the left side of the application, click the protected site from which you want to add or remove a vCenter.
3. To remove a vCenter, from the vCenters section click the drop-down menu icon next to the vCenter you want to remove and select Remove vCenter.
4. In the remove vCenter confirmation dialog, enter the phrase REMOVE VCENTER in all upper case letters and then click OK.

Remove a Connector from a Protected Site

To remove a connector from a protected site, follow the procedure below.

Procedure

1. Click the Sites → Protected sites tab in the VMware Cloud Disaster Recovery UI.
2. From the left side of the application, click the protected site you want to remove a connector from.
3. Under the Connectors section, to the right of the connector you want to remove, select Remove connector from the drop-down menu.
4. In the Remove connector confirmation dialog, enter the phrase REMOVE CONNECTOR in all upper case letters, and then click OK.

Delete a Protected Site

If you want to complete delete a protected site, make sure you first remove its vCenter, and then remove the DRaaS Connector (in that order). After you have removed the vCenter and deleted the connector, you can delete the protected site.
Procedure

1. To edit or delete a site, click the Sites → Protected sites tab.
2. Click the site you want to edit or delete.
3. From the small drop-down menu on the upper right side of the VMware Cloud Disaster Recovery UI, click Delete site.

4. Enter the phrase DELETE SITE in all upper case letters in the Delete protected site dialog, and then click OK.
Backup with Protection Groups

To protect your data, use the VMware Cloud Disaster Recovery UI to create protection groups that contain one or more VMs in your vSphere environment. Snapshots can be made according to the schedule you define in the protection group configuration wizard.

A protection group consists of the following components:

- Site selection (protected site for on-prem vCenter)
- Members (VMs)
- Policies for snapshots (schedule, retention)
- Replica site (SCFS)

**Note:** Before you create protection groups, make sure you first Create a Subscription for protected capacity.

When you create a protection group, you:

1. Choose the protected site and vCenter instance from which you want to select VMs.
2. Create vCenter queries that define the protection group's dynamic membership. A vCenter query can be defined using vSphere tags, folders, and/or VM name patterns. These vCenter queries are evaluated each time a snapshot is taken and define the contents of the snapshot.
3. Define how frequently you want to take snapshots of the VMs defined in the group using a snapshot schedule. You also define how long you want to retain those snapshots on the SCFS.

**Tip:** Keep in mind when setting a snapshot schedule that research indicates most victims of ransomware don’t discover that they have been compromised until an average of 3-6 months after the initial infection.

Protection groups can then be added to a DR plan, which ensures that in the event of a failure, you can orchestrate recovery to a new site using selected snapshots of your VMs to re-instantiate the source vCenter site.
The members of a single protection group must share the same vCenter. In other words, you cannot create a protection group that contains VMs from two different vCenters.

**Backup copy caveats and restrictions**

- Shared disks are not supported.
- VMware Cloud Disaster Recovery does not create backups of VM templates. If you include a VM template in a protection group, it will not be included in snapshots.
- VMware Cloud Disaster Recovery may exhibit errors with snapshots if the customer environment is running other VM backup software. If a VM is being backed up by VMware Cloud Disaster Recovery by a protection group snapshot, and the same VM is also being backed up by other software that uses vSphere Storage APIs for Data Protection (VADP), the snapshot will still be taken, but that VM will not be included in the snapshot.

**Create a Subscription**

A protected storage capacity subscription is required to use VMware Cloud Disaster Recovery, and can be purchased in 1 or 3 year terms using VMware Subscription Purchasing Program (SPP) credits. Before you create any protection groups, you first need to create a subscription.

Protected storage capacity is the sum of the logical storage size of your protected VMs and the incremental cloud backups you choose to retain. You can create up to 10 subscriptions for a total of 400 TiB of protected capacity. The cost of added protected capacity is calculated automatically according to the current pricing structure.

If you need additional protected storage capacity for VMware Cloud Disaster Recovery, beyond what you initially purchased when you signed up, you can create a subscription and choose the amount of protected capacity you need. You can add anywhere from 5 TiB to 400 TiB, depending on your currently active subscriptions.

**Tip:** If you need more than 400 TiB of protected capacity, contact VMware for assistance.
New subscriptions you create in the same AWS region as the one associated with your initial subscriptions and VMware Cloud Disaster Recovery deployment.

You cannot cancel, convert, or modify a subscription after you have ordered it.

**Note:** Your user account must have the organization owner role in order to create a subscription.

**Note:** You must have purchased SPP credits and associated them with your account before you can buy a subscription.

**Procedure**

1. In the VMware Cloud Disaster Recovery UI, click the Subscriptions tab. The Subscription list shows all currently active subscriptions, including a roll up of the total subscribed capacity and total used capacity.

2. To create a new subscription, click the **Create subscription** button.

3. In the Create subscription dialog, enter the following information:
   - **Capacity to add.** Measured in TiB. Enter a number between 5 and 400. As you add protected capacity, the dialog lists your current total and the new total as you add values.
   - **Term.** Choose either 1 year or 3 years.

4. Under the Confirm section, select the check box to acknowledge your intent to purchase the new subscription.

5. At the bottom of the dialog, enter the phrase **CREATE SUBSCRIPTION** in all upper case letters.

6. When you are ready to purchase the subscription, click **Place order**.

**Create a Protection Group**

When you create a protection group, you define the group membership criteria that determines which VMs will be included in a snapshot. You then set the snapshot schedule, which defines how frequently snapshots are taken of the protection group's VMs.
Protection group membership criteria is defined in a protection group query, of which there are three types:

- **VM Name Pattern.** A VM name pattern is a string of characters that you use to match the names of VMs in your vSphere inventory, either for inclusion or exclusion in the protection group snapshot. Any VMs that match the pattern specified will be added to (or explicitly excluded from) the protection group for snapshots.

- Folders. You can add VM folders that are present in your vSphere inventory to a protection group, so that all VMs in those folders are included in snapshots. Folder selection does not include sub folders, so if you want to include sub-folders, you must choose them specifically. (Note: Folder based snapshots are not supported for VMs that are a part of vApp.)

- vSphere tags. You can use tags to determine protection group membership. Any VMs that match the tags you specify will be included in the protection group snapshot. You can select any tags defined in vSphere on the protected site. For successful failover operations, you must ensure that the selected tags also exist on the target Recovery SDDC vCenter, or the compliance check will display warnings, and failback will not operate successfully.

In a protection group, VMs that match any name patterns are evaluated first, and then are combined with any defined folder and tag queries before a protection group snapshot is taken.

Hence, if you use an exclusion name pattern in your query for a protection group, it is possible that other Folder or tag queries defined in protection group can override the previously excluded name pattern. For example, if one of your queries excludes a VM by name, if that same VM lives inside a folder you have selected in a Folders query, that VM will be included in the snapshot.

If you want to verify the snapshot before a scheduled job, you can Take a manual snapshot.

**Note:** If any VM names use the following special characters, and you wish to create a pattern matching any of these characters, they must be escaped (prefixed with '\') in the specified VM name pattern: '{', '}', '[', ']', '?', '.', ',', '*', as well as double ('') quotation marks.

For example, the VM name pattern "*[0-9]" will match any VM name ending with a
numeric digit (for example: "database7"), while the VM name pattern "^[0-9]" will match any VM name ending with the string "."

**Procedure**

1. In the VMware Cloud Disaster Recovery UI, click the Protection groups tab.
2. From the upper right side of the Protection groups list, click the Create protection group button.
3. In the General page of the Create protection group dialog, enter a name for the protection group.
4. Then, select a protected site and a vCenter instance you want to take snapshots from. Note that the dialog also shows the Cloud backup instance (SCFS) associated with the protected site, and where copies will be replicated to.
5. Next, you can define the dynamic membership of the protection group using VM name patterns, tags and/or VM folders in a vCenter query. All VMs that match the name pattern, are included in the selected folders, or contain the tags selected will be included in the protection group snapshot.
6. Under Group membership, click the VM name pattern, Tags, or Folder buttons.
7. For a VM name pattern query, enter a VM Name Pattern that will be evaluated before each snapshot is taken. You can also enter a name pattern to be excluded in the query in the Excluding field. (If there is already one vCenter query, then use the Add vCenter query drop-down menu and choose VM name pattern.)
8. For a folder query, click the Select folders button. In the vCenter folders dialog, you can search the list of folders in your vCenter and then click one that you want to add to the query. (If there is already one vCenter query, then use the Add vCenter query drop-down menu and choose Folders.) Note that folder selection does not include sub folders, so if you want to include sub-folders, you must choose them specifically. (Note: Folder based snapshots are not supported for VMs that are a part of vApp.)
9. For a tag query, click the Tags button. In the vSphere tags dialog, select the tags you want to use for defining the protection group membership. Any VMs that have the selected tags will be included in the protection group snapshots. Click OK when you are finished.
10. You can optionally click **Preview VMs** to view which VMs currently match your vSphere queries.

11. Click **Next**.

12. To set the snapshot schedule, click **New Schedule**.

13. On the Schedule page, you can create a snapshot schedule to define recurring snapshot operations at a particular time, based on a recurring interval. A protection group can have a maximum of 10 schedules associated with it. The dialog provides schedule fields for a specific time of day based on the following intervals: Every 4, 6, 8, or 12 hours, and Daily, Weekly, or Monthly.

14. When you have finished adding schedules, click **Finish**. The protection group appears in the Protection groups list and can now be added to a DR Plan for testing and execution.

**Edit a Protection Group**

Edit a protection group if you want to change a protection group membership parameters, or you want to change the group's snapshot schedule.

**Procedure**

1. In the VMware Cloud Disaster Recovery UI, click the Protection groups tab.

2. To the right of the protection group you want to edit, from the drop-down menu on the far right, click **Edit**.

3. You can now edit the protection group's VM name pattern, tag, or folder queries.

4. When you click **Next**, you can also edit the snapshot schedule and retention policy for the protection group.

5. When you are done, click **Save**.

**Deactivate Protection Group Snapshot Schedule**

If you want to stop a protection group from replicating its snapshots to the SCFS, you can deactivate its snapshot schedule.
Procedure

1. In the VMware Cloud Disaster Recovery UI, click the Protection Groups tab.
2. Select a protection group.
3. In the protection group details page, in the upper right of the dialog, from the drop-down menu click Disable schedule.

Delete a Protection Group

When a protection group is no longer needed, you can delete it.

Caution: When you delete a protection group, you are also deleting ALL of the snapshots associated with it, forever.

Procedure

1. In the VMware Cloud Disaster Recovery UI, click the Protection Groups tabs.
2. Identify a protection group you want to delete, from the drop-down menu on the far right, click Delete.
3. In the Delete protection group dialog, verify that you want to delete this group (and all the associated snapshots in them) and enter the phrase DELETE GROUP AND SNAPSHOTs in all upper case letter in the confirmation field.
   Note: When you click OK, all snapshots in the group are deleted permanently, forever, and are not retrievable.
4. Click OK to delete the selected protection group and associated snapshots.

VM Name Pattern

When you configure a protection group, you can use VM name patterns (for inclusion and exclusion) to define dynamic group membership. These patterns are used at the time of taking snapshots to determine protection group VM membership.

A VM name pattern is a string of characters. VMware Cloud Disaster Recovery uses glob syntax matching for VM name patterns. For example, the pattern windows[1-5] matches
the set of virtual machines with names in the sequence of windows1..windows5. The search is case-insensitive.

**Important**: In a protection group, VM name patterns are evaluated first, and then are combined with any defined Folders queries before a protection group snapshot is taken. Keep in mind that if you use an *exclusion* name pattern in your vCenter query for a protection group, it is possible that other Folder queries defined in protection group can override the previously excluded name pattern.

**Note**: If any VM names use the following special characters, and you wish to create a pattern matching any of these characters, they must be escaped (i.e., prefixed with '\') in the specified VM name pattern: '{', '}', '[', ']', '?', and '*'.

For example, the VM name pattern "*[0-9]" will match any VM name ending with a numeric digit (e.g., "database7"), while the VM name pattern "*[0-9]" will match any VM name ending with the string "[0-9]".

The following table provides a brief description of the special characters that you can use in a virtual machine name pattern.

<table>
<thead>
<tr>
<th>Virtual Machine Name Patterns – Special Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>*<em>**</em></td>
</tr>
<tr>
<td>For example:</td>
</tr>
<tr>
<td>windows*</td>
</tr>
<tr>
<td>matches all virtual machines with names that start with the string windows.</td>
</tr>
<tr>
<td>*<em>?*</em></td>
</tr>
<tr>
<td>For example, the pattern:</td>
</tr>
<tr>
<td>Linux?</td>
</tr>
<tr>
<td>matches any virtual machine with a name that starts with the string linux followed by any single character.</td>
</tr>
</tbody>
</table>
Virtual Machine Name Patterns – Special Characters

<table>
<thead>
<tr>
<th>Square brackets enclose a set of characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The brackets specify a match of exactly one character out of the set. The character set can include one or more ranges of characters.</td>
</tr>
<tr>
<td>[ ] For example:</td>
</tr>
<tr>
<td>linux[0-9]</td>
</tr>
<tr>
<td>matches anything in the datastore root that begins with the string linux and ends with a single digit.</td>
</tr>
</tbody>
</table>

There are two types of virtual machine name patterns you can set in the protection group configuration:

- Inclusion patterns — VMs to be selected. You must specify at least one inclusion pattern.
- Exclusions patterns — VMs to be excluded from the results of inclusion pattern selection. An exclusion pattern begins with the exclamation character (!).

The order of patterns in a pattern list does not matter. A pattern list uses a comma (, ) as a delimiter.

**Take a manual snapshot**

In addition to having protection groups take snapshots on a recurring schedule, you can also take one-time, manual snapshots of group members.

The manual snapshot will include the current members of the protection group based upon the vSphere queries defined for the group (VM name pattern and/or folders). The snapshot will include all VMs that match any of the query criteria at the time when the snapshot is taken.

**Note:** If another scheduled or manual snapshot is in progress, you will not be able to take a manual snapshot of that protection group until the current snapshot is finished.
Tip: To view a completed snapshot, reload the snapshots list on the protection group page. To verify that a snapshot job has started, you can view the Monitor tab → Events tab → Protection filter to view the snapshot job start event.

Take a manual snapshot:

1. In the VMware Cloud Disaster Recovery UI, click the Protection Groups tab.
2. From the list, select a protection group that you want to take a snapshot of.
3. In the protection group page, from the drop-down menu on the far right, click Take snapshot.
4. In the Take manual snapshot dialog, select a retention time the snapshot, which determines how long the snapshot is retained before it is automatically deleted. For example, you can choose Forever (will never be deleted), for a specific period of time (for example, 12 days), or a specific date on which the snapshot will be deleted.
5. Click Take snapshot.
   Note: If an snapshot job is already in progress, then you will see an error stating that the system failed to take the snapshot. In this case, you will have to wait until the current snapshot job is finished to take the manual snapshot.
6. Refresh the list to see the new snapshot. Click on the snapshot to see its contents.

Restore a VM

Once a protection group has taken snapshots of the VMs on your protected site, you can restore individual VMs from a snapshot. The VM will be restored to the same state it was in when the snapshot was taken, including its vCenter location, configuration, data, etc.

An example of needing to restore a VM is during a failed software upgrade attempt or when something was accidentally deleted or uninstalled from a virtual machine. You can use VMware Cloud Disaster Recovery to restore that VM.

Note: This section shows you how to restore one VM at a time. For multi-VM restore automation, see DR Plans.

A few prerequisites before you can restore a VM:
• There must be at least one snapshot taken of a protection group in order to restore a VM from the group.
• Make sure that the VM you are restoring is powered OFF in vSphere before you restore it.

Procedure

1. In the VMware Cloud Disaster Recovery UI, click the Protection Groups tabs.
2. Select a protection group from the list.
3. Click one of the snapshots associated with the group.
4. In the list of VMs in the snapshot, click the **Restore** button next to the VM you want to restore.
5. In the Restore VM dialog, you see information that describes the VM and the location to which it will be restored on the protected site.
6. Click **OK** to restore the VM.

**Throttle Replication**

If you want to control the speed at which your protected site protection group replicates snapshots to the SCFS, you can set the replication bandwidth throttle settings.

Procedure

1. In the VMware Cloud Disaster Recovery UI, click the Sites → Protected site tab.
2. Select the drop-down menu and click **Throttle replication**.
3. In the Throttle replication dialog, you can select the Throttle to option and then enter a numerical value in the Mbps field to set your desired replication speed.
4. Click **OK**.
**DR Plans**

A DR plan defines the orchestration configuration for disaster recovery and workload mobility.

Plans can be created, named, edited, duplicated, saved for future use, and run. Environment variables map differences between the sites for smooth recovery. VMware Cloud Disaster Recovery uses VMware Cloud on AWS to ensure vSphere configurations and parameters are consistently understood between sites.

Plans can be run either as an actual Running a DR Plan for recovery, or they can be run as a ‘Test recovery, which performs all of the plan’s recovery operations in a test site for validation.

Execution pacing is configurable. When a plan is run, a running instance of the plan is launched and typically continues executing its recovery steps to completion. Or, if configured to do so, a recovery or test plan can continue to specific points in the process and wait for user input, or it can stop and wait for a specified time limit, and then continue until the next stop or to completion. Pre- or post-scripting can be added to a VM’s recovery step.

VMware Cloud Disaster Recovery performs a set of Continuous Compliance Checks for all active plans and resources, and it reports on environmental changes, such as vSphere misconfigurations or network outages. Compliance Checks detect any compromised plan integrity at the time of misconfiguration or equipment failure, giving the user an opportunity to address the detected issues and restore plan integrity prior to a disaster event. This ensures successful recovery. For developing and retaining the skill set of related DR activities, however, you should still perform periodic full DR exercises with the staff involved.

VMware Cloud Disaster Recovery can maintain multiple plans of different types, and multiple plans can be in various stages of execution at any given time, even concurrently.

**DR Plan Configuration**

With DR plans, you need to perform several configurations that direct the plan where to move protected data to from the protected sites when the plan is run.
Specifically, your plan needs to define where protected resources will be moved to on the recovery site: protection groups, VMs, files, vCenter(s), all vCenter folders, compute resources, virtual networks, and IP addresses (individual or ranges). In addition, you will need to configure the Test Site operating environment for failover exercises.

Recovery Site Selection

A DR plan’s meaning is determined by the recovery site defined in the plan; that is, by the target where you want a protected site to recover.

The failover target for a DR plan is an SDDC deployed on VMware Cloud on AWS. Snapshots are replicated to the SCFS in the same AWS region as the recovery SDDC. The backups are made instantly available to a VMware Cloud on AWS SDDC resulting in instant VM power-on, once the SDDC is available and configured.

Backups are replicated to the SCFS in the same region and availability zone as the deployed SDDC.

Protected Site Selection

The Protected Site drop-down menu displays a set of sites known to VMware Cloud Disaster Recovery that are protected by a DR plan. The protected site has live VM workloads organized into protection groups. These protection groups are in the live state and replicate snapshots the SCFS in accordance with a configured replication schedule.

The on-premises recovery site drop-down menu presents a set of options for the recovery site for the chosen DR plan type. The failover process will use this site as a target, and VMware Cloud Disaster Recovery will restart protected workloads on this site.

Advanced options allow you to configure additional backup sites and to select a site for DR plan testing.

In the Site page, you define which protected site you want this to failover using this DR plan. In some cases, you may have multiple protected sites.
Also in the Site page of the Plan wizard, you can choose if you want to run DR test plans directly on the SDDC. This is highly recommended but keep in mind that an SDDC accrues costs while running.

If you are testing a plan, a test failover normally runs on a recovery site. For more about test sites, see Test Failover.

**Protection Group Selection**

By default, the Protection Groups page displays a list of protection groups on the protected site that have scheduled replication to the backup site, identified in the previous Sites step of the plan wizard.

Before a plan can be configured and run, you must have created protection groups with scheduled replication to the SCFS, so that when the failover occurs, the plan can use snapshots of replicated VMs to restore on the target site. When you run the plan, you can choose the snapshot to use for failover.

In the Groups page of the DR Plan wizard, you select the protection groups you want to include for failover. These selections ensure that the plan has sufficient information to recover all VMs and files covered by the selected protection groups. The plan will use snapshots of these protection groups for failover when you run the plan. Protection group selection affects a set of automatic compliance checks run for this plan.

A warning will be displayed if the selected protection groups do not have scheduled replication configured for the backup site.

**Note:** Protection groups that you add to a plan can only originate from the same protected site.

**Datastore Mapping**

When performing a failover to VMware Cloud on AWS, datastore mappings are established automatically. The VMware cloud recovery site has a single datastore making datastore mappings unnecessary.
Note: All VMs that are recovered are located at the root storage folder of the "WorkloadDatastore/" directory after the failover operation.

Datastore mappings for protected sites

To protect your VMs, you can map many source datastores on the protected sites to a single datastore on the recovery site. During failover, if a VM still exists on the source protected site during failback, the failback will use its current datastore and storage folder location.

However, if a VM no longer exists on the protected site, then the failover operation will use that VM’s last known datastore and storage folder for the failover. If for some reason the last known datastore does not exist anymore, you must manually set the default datastore in the failover plan before you can run the failback plan. For example, before you run the failback plan, the Failback datastores mappings must be set:
vCenter Mapping

Mapping vCenters in a DR plan consists of selecting source vCenters that are registered to the protected site. All source vCenters that contain VMs and that are protected by the selected group(s) can be mapped to a target vCenter on VMware Cloud on AWS as the selected recovery site.

Choosing a target vCenter for a Failover SDDC is simple; each SDDC contains a single vCenter instance. For VMware Cloud Disaster Recovery, keep in mind that a protected site can have multiple registered vCenters, but you can only map one vCenter on VMware Cloud on AWS per-DR plan.

Every valid vCenter mapping will create a vCenter mapping for the following three elements:
vCenter folders
Compute resources
Virtual networks

Failover Mapping and Test Mapping Tab Behavior

If the test site is deactivated, the Test mapping tab will not appear.

A mappings table with the current selected mappings will appear for every valid vCenter mapping. If there are existing mappings that are no longer valid, caused by changes in the Sites or vCenters step selections, those mappings will also appear in a table.

Invalid mappings appear in red text. A description of the error can be viewed by moving your mouse pointer over the invalid path and viewing the message in the tooltip.

Mappings can be deleted by clicking the X to the right of each mapping entry. New entries can be added by clicking the Map [vCenter object] button, which will open up a new dialog.

vCenter Folders Object Inventory Mapping

This page of the plan wizard displays a subset of the vCenter object inventory for both the source and target vCenters. Source vCenter object nodes that are detected to contain protected VMs are required to be mapped and are displayed in the UI with blue text. All other mappings are optional.

To add a mapping, select the source vCenter node and the corresponding target vCenter node indicating where the source VMs should be recovered. Then, click Add. Complete this step for each mapping, and then click OK when finished.

Note: If your VMs on the protected vSphere site have tags associated with them, make sure that the same sets of tags and tag categories also exist on the target site of the plan (the Recovery SDDC).

Tip: Avoid having other VMs in target folders because name conflicts can arise when registering VMs with vCenter.
vCenter Folders

Mappable vCenter objects:

- Data center
- Folder

Compute Resources

Mappable vCenter objects:

- Clusters. If the Cluster contains VMs, its icon is highlighted in light blue font to indicate that mapping for this item is required. (This color scheme applies to all mappings.)
- Resource pool
- Standalone host (not in a cluster). Note that a standalone host can only be mapped to another standalone host.

**Note:** Regarding vCenter cluster names, "Cluster-1-<clusterIndex>" represents the name of the initial cluster when the SDDC was first created.

If the SDDC that your clusters belong to is deleted, then any plans with mappings to clusters on that SDDC will display the target cluster names with an asterisk. For example: "Cluster-*-<clusterIndex>".

Additionally, plan compliance reports will indicate an error when clusters are mapped to a deleted SDDC, or if there is a mapping to a deleted cluster.

Virtual Networks

Mappable vCenter objects:

- Virtual network
- Distributed virtual port group
Multi-vCenter Selection

You can only select one vCenter per plan.

IP Address Mapping

IP mappings determine how a VM’s IP address is assigned when a protected source site is failed over to a target site. When a VM is recovered from one site to another, VMware Cloud Disaster Recovery needs to know which IP addresses will be used for the recovered VMs.

IP address mappings can be configured for VMs installed with Linux or Windows guest OS’s. VMs configured for IP address mapping will display with a target IP, target subnet mask, target gateways, and target DNS servers.

**Important:** In order to map IP addresses for Windows VMs, the system drive of the VMs must be mapped to c:\. Additionally, the mapped c:\ drive cannot be dynamic volume; it must be a basic disk.

**Note:** VMware Tools must be installed on the guest OS in order to ensure successful IP address mapping.

**Note:** Only IPv4 is supported for protection plan IP address mapping. This means that any VMs referenced in a DR plan must be using IPv4, or the IP address mapping will not work.

Individual IP Address Mapping

The following figure illustrates IP address mapping page, which has the following fields:

- Optional rule description
- Source and target IP addresses
- Source and target subnet masks
- Source and target gateways
- Source and target DNS servers
Entries for individual IP addresses must be separated either by white spaces or new lines.

Entries for gateways and DNS servers must be separated by white spaces. If multiple IP addresses are specified, they will be matched in the specified order from source to target.

To configure IP address mapping, you must enter:

- The Rule description field text (optional)
- Source and target IP addresses
- Source and target gateways
- Source and target DNS servers
IP Address Range Mapping

Alternatively, you can configure IP address ranges rather than individual IP addresses. Switching to IP ranges can be done by selecting Range from Range/IP addresses, as shown below:

![Edit IP address mapping rule](image)

The IP address mapping page has the following fields: optional rule description, source and target IP range prefixes/bits, source and target subnet masks, source and target gateways, and source and target DNS servers. Entries for gateways and DNS servers must be separated by white spaces.

The Range prefix field provides an IP address within a range of IP addresses to be mapped for both source and target. The available range of IP addresses to be mapped is defined by the Bits field.

The following table describes the available CIDR Prefix values for Bits field:
<table>
<thead>
<tr>
<th>CIDR Prefix</th>
<th>Dotted Decimal Notation</th>
<th># Node addresses</th>
<th># of Traditional Class Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>/13</td>
<td>255.248.0.0</td>
<td>512K</td>
<td>8 B or 2048 C class</td>
</tr>
<tr>
<td>/14</td>
<td>255.252.0.0</td>
<td>256K</td>
<td>4 B or 1024 C class</td>
</tr>
<tr>
<td>/15</td>
<td>255.254.0.0</td>
<td>128K</td>
<td>2 B or 512 class</td>
</tr>
<tr>
<td>/16</td>
<td>255.255.0.0</td>
<td>64K</td>
<td>1 B or 256 class</td>
</tr>
<tr>
<td>/17</td>
<td>255.255.128.0</td>
<td>32K</td>
<td>128 C class</td>
</tr>
<tr>
<td>/18</td>
<td>255.255.192.0</td>
<td>16K</td>
<td>64 C class</td>
</tr>
<tr>
<td>/19</td>
<td>255.255.224.0</td>
<td>8K</td>
<td>32 C class</td>
</tr>
<tr>
<td>/20</td>
<td>255.255.240.0</td>
<td>4K</td>
<td>16 C class</td>
</tr>
<tr>
<td>/21</td>
<td>255.255.248.0</td>
<td>2K</td>
<td>8 C class</td>
</tr>
<tr>
<td>/22</td>
<td>255.255.252.0</td>
<td>1K</td>
<td>4 C class</td>
</tr>
<tr>
<td>/23</td>
<td>255.255.254.0</td>
<td>512</td>
<td>2 C class</td>
</tr>
<tr>
<td>/24</td>
<td>255.255.255.0</td>
<td>256</td>
<td>1 C class</td>
</tr>
<tr>
<td>/25</td>
<td>255.255.255.128</td>
<td>128</td>
<td>( \frac{1}{2} ) C class</td>
</tr>
<tr>
<td>/26</td>
<td>255.255.255.192</td>
<td>64</td>
<td>( \frac{1}{4} ) C class</td>
</tr>
<tr>
<td>/27</td>
<td>255.255.255.224</td>
<td>32</td>
<td>( \frac{1}{8} ) C class</td>
</tr>
</tbody>
</table>

For example:

- Range prefix = 10.116.1.50
- Bits = /24

This means the available range of IP addresses to be mapped would be 10.116.1.0 through 10.116.1.255.

The Bits (CIDR Prefix) specified can be a smaller range within the defined subnet in your environment. For instance you can define the subnet as follows:
- [network: 10.116.0.0/20,
- netmask: 255.255.240.0,
- gateway: 10.116.0.1,
- range: 10.116.0.0 - 10.116.15.255]

In this example, providing a bits value of /24 with Range prefix of 10.116.1.0 allows you to provide a smaller range of IP addresses to be mapped within that subnet. The subnet mask value provided is used when the IP addresses are mapped.

Limitations when mapping IP address ranges:

- You can provide a bits value that is smaller than the subnet mask size (CIDR prefix). For instance, if the subnet is a /20 you can define a CIDR prefix (bits) that provides a smaller IP range (i.e., /21, /22, etc.) for the range mapping.
- You cannot, however, do the reverse. If the subnet is a /20 you cannot enter a CIDR prefix (bits) that provides a greater IP range (i.e., /19, /18, etc.) for the range mapping. If attempted, the UI will display an error.

To configure IP address range mapping, enter:

- Text description (optional)
- Source (protected site) and target (recovery site) ranges expressed in CIDR notation
- Source and target subnet masks
- Source and target gateways
- Source and target DNS servers

To save the IP mapping configuration, click OK.

**Failover Mapping and Test Mapping Behavior**

- If the test site is deactivated, the test tab will not appear
- If the test site is specified, the Failover mappings and Test mappings tabs can be the same depending on check box selection
Supported IP Address Mapping Combinations

The following IP address mappings are supported from source to target systems in a DR plan:

**Note:** VMware Cloud Disaster Recovery does not support IPv6 remapping, and IPv6 addresses cannot be entered in the plan wizard.

<table>
<thead>
<tr>
<th>Mapping</th>
<th>Configuration Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>VMware Cloud Disaster Recovery supports DHCP mappings for both Windows and Linux VMs.</td>
</tr>
<tr>
<td>Static IP addresses - Linux</td>
<td>VMware Cloud Disaster Recovery supports IP address mapping for Linux VMs, with adapters that have exactly one IPv4 and optionally one link local unicast IPv6. Only IPv4 addresses can be mapped. IPv6 configuration(s) will be preserved. Refer to the <a href="#">Linux-specific IP Mapping</a> section for details.</td>
</tr>
<tr>
<td>Static IP addresses - Windows</td>
<td>VMware Cloud Disaster Recovery supports IP address mapping for Windows VMs. Single IPv4 address per network adapter is supported. If present on the interface, IPv6 configuration(s) will be preserved. Refer to the <a href="#">Windows-specific IP Mapping</a> section for details.</td>
</tr>
<tr>
<td>Multiple Gateways</td>
<td>VMware Cloud Disaster Recovery supports mapping of multiple gateways per adapter for supported versions of Windows and Linux VMs.</td>
</tr>
<tr>
<td>Multiple Adapters</td>
<td>DHCP or Static mappings of IPv4 addresses are supported per adapter for Windows and Linux VMs.</td>
</tr>
<tr>
<td>Multiple VM recovery</td>
<td>VMware Cloud Disaster Recovery supports IP address mapping of static and DHCP IPv4 addresses for multiple Linux and Windows VMs. IP address mappings can be specified in the plan wizard as individual IP addresses or IP address ranges.</td>
</tr>
<tr>
<td>Mapping</td>
<td>Configuration Support</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mapping rules do not apply to recovered VMs</td>
<td>If IP address mapping rules added to the plan wizard do not match any recovered VMs, remapping is skipped.</td>
</tr>
</tbody>
</table>

**OS Compatibility for Static IP Address Mapping**

This section describes Linux and Windows OS compatibility for static IP address mapping.

**Linux-specific IP address mapping**

VMware Cloud Disaster Recovery supports IP address mapping for a VM if all NICs have exactly one IPv4, and optionally one link local unicast IPv6.

Also, since IP address mapping for Linux depends on vSphere guest customization, the source VM machine hostname should meet the naming requirements from vSphere Customization Spec. Otherwise, IP address mapping will be skipped.

Supported Linux versions:

- CentOS 7.0-1406
- CentOS 7.3-1611
- CentOS 7.5-1804
- RHEL 6 minimal

**Windows-Specific IP Address Mapping**

VMware Cloud Disaster Recovery supports IP mapping of commonly used Windows versions:

- Windows 10
- Windows 2016
- Windows 2012 R2
Multiple network adapters per VM are supported. Single IPv4 address per network interface is supported. If present on the interface, IPv6 configuration(s) will be preserved.

If the network interface has no statically configured IPv4 addresses, no IP mapping will be performed, even if matching IP address is found on the source.

**Script VM**

The Script VM page of the DR plan wizard provides the ability to add custom scripts that can be run on a dedicated VM during plan execution as a recovery step.

Both Windows (Powershell) and Linux (Python) are supported for the script VM guest OS.

Script VM caveats:

- Only 1 script VM supported per plan. (But you can have multiple script VMs in your VMware Cloud Disaster Recovery environment).
- The script VM must have VMware Tools installed.
- The script VM must be available in the environment before the first step requiring a script call. In other words, the Script VM can be recovered as the first steps of a plan, or already running at the target site.

**Note:** A script VM configured to run on multiple VMs will be run sequentially on each target VM in the batch. Be aware that depending on the number of VMs targeted by the script VM, this can take extra time and slow the recovery completion process.

**Procedure**

1. Choose the Run script VM option.
2. Enter the VM name on which the script will run and the vCenter where the VM is hosted.
3. Once you have configured the script VM settings for the plan, you need to decide when the script will launch when the plan is running plan. For more information on configuring a script for a plan, see the DR Plan Configuration section.
Recovery Steps

A plan’s recovery steps dictate what actions the plan will take during a failover, and the specific order in which those will occur when the plan is running. Recovery steps in a plan consist largely of restoring individual VMs or VMs contained in protection group snapshots, and additionally copying and restoring files and vSphere groups to the target recovery site.

Recovery Step Types

Recovery steps also allow you to specify scripts to be run before and/or after a VM is powered on during a failover. You can also configure how you want the running plan to handle errors it encounters during failover, and also require user input on some steps before the plan continues running.

There are four types of plan recovery steps listed in the following table:

<table>
<thead>
<tr>
<th>Step type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recover protection groups</td>
<td>Allows you to recover any of the protection groups associated with the plan. This step recovers and promotes each protection group, registers all VMs in a protection group snapshot with vCenter, then customizes and powers on the VMs.</td>
</tr>
<tr>
<td>Recover individual VMs</td>
<td>Allows you to recover individual VMs (you can select more than one). This step recovers then promotes each VM, registers each with vCenter, then customizes them and powers them on.</td>
</tr>
<tr>
<td>Recover all remaining VMs, files, and groups</td>
<td>Allows you to recover everything else referenced in plan mappings, in addition to any selected protection groups or individual VMs. This step recovers and promotes all remaining protection group and VMs and other files, registers the VMs</td>
</tr>
</tbody>
</table>
### Recover Protection Groups

When you select this recovery step type, you can choose multiple protection groups to be recovered:

**Step type**
- [ ] Recover protection groups
- [ ] Recover individual VMs
- [ ] Recover all remaining VMs, files, and groups
- [ ] Other actions - wait, run script, and other actions

**Protection groups to recover**
- [x] pg_ds2
- [x] pg_ds3
- [x] pg_ds4
- [x] pg_test_1
Recover Individual VMs

When you select this recovery step type, you can choose one or more individual VMs referenced in your plan. In the DR Plan wizard, click Select individual VMs, as shown here:

The Select individual VMs dialog appears. Select VMs on the left and they will be added to the recovery step on the right side of the dialog:

Note: Any VMs that are recovered over are located at the root of the "WorkloadDatastore/" directory after the failover operation has completed.
Power Action

For each of the three recover actions (protection groups, individual VMs, and all remaining VMs), you need to choose a Power action, which determines whether or not you want the recovered VMs to be powered on when the VMs are recovered.

Power action

- Power on only VMs that were powered-on when snapshotted
- Power on all recovered VMs
- Do not power on VMs

A recovery step for protection groups or VMs require one of these three power actions:

- Power on only VMs that were powered-on when snapshotted
- Power on all recovered VMs
- Do not power on VMs.

Protection groups, Snapshots and VM power state

When a snapshot is taken of a protection group, it captures the power state of VMs in the group - On or Off. If the VM is powered on when a snapshot is taken, after failover the VM will be powered on when it is restored. Conversely, if the VM is powered off at the time the snapshot was taken, the VM will be powered off when it is restored.

It is important to be aware that for VMs that are powered off when the snapshot is taken, it will not be possible to power on the VM until after the storage VMotion of that VM to the SDDC completes.

To be sure, if your VMs must be powered on and ready for use immediately after recovery, you can override that default behavior when you set the recovery power state in your DR plan to be On.
Pre-recover and Post-recover Actions

In addition to choosing a Power action for recovered VMs, you can also choose actions what will occur before and after a VM is powered on:

- **Pre-recover action:**
  - *Run a script in the script VM.* This requires entering the script path and any custom parameters.

- **Post-recover actions:**
  - *Wait for VM IP address.* Wait for the VM’s IP address to be assigned before moving to the next step in the plan.
  - *Wait for VMware Tools.* Wait for VMware Tools to launch before continuing to the next step in the plan.
  - *Run script in the Script VM.* This requires entering the script path and any custom parameters.

**Script Configuration**

If you choose to run a script as a pre-recover or post-recover action, you need to configure script settings. This script VM is independent of the VMs that you recover as part of the plan.

To configure script execution, you need to identify both the script and the script VM.

- You can only specify one virtual machine for script execution. The name of this virtual machine must be unique in its vCenter context.
- You must identify the script by its location on the script VM and by execution requirements. See Recovery steps.

There are two types of script execution:
A pre-recover action script runs before powering on a recovered virtual machine.

A post-recover action script runs after the recovered VM has been powered on. Post-action scripts can be paused for a certain amount of time to allow IP address configuration on recovered virtual machines, and can be paused to allow VMware Tools installation on recovered virtual machines.

**Script Actions**

*Note:* This action runs a script on a VM within the context of plan execution recovery step. The script action takes an absolute path to the script on the script VM as well as a list of parameters that you can specify.

For Powershell scripts, only the absolute path to the 'powershell.exe' can be in the script path, and the Powershell script must be set in the parameters.

For example:
The Timeout field measured in seconds is the amount of time to wait for this action before returning a failure on timeout. In the example above, if the script takes more than 300 seconds, it will fail.

The script execution action returns an exit code for the script, where a non-zero exit code means failure, and an exit code of 0 means success. At the time of recovery execution, you must supply the script VM credentials so that it is possible to run the script in the script VM remotely.

**Failback and Rollback Script Actions**

Script actions have both a forward (failback) and backward (rollback) execution:
If the script was run in the forward direction, a "--failover" flag is added to the parameters list so the script can distinguish between directions.

If the script was run in the reverse direction, a "--rollback" flag is added to the parameter list.

**Alerts**

As a part of DR plan configuration, you can choose to have email notifications sent when specific events related to plan execution occur. You can select which email addresses will be notified and what condition should trigger the email.

For information on how to configure alert email addresses, see [Configure Email Alerts](#).

DR plans support email alerts for the following recovery execution steps as follows:

- Failover execution status changed
- Waiting for user input
- Failover finished
- Waiting for user commit

DR plans also support email alerts for the following compliance check events:

- Every compliance check - after every compliance check run
- Compliance warning - for any compliance check that results in some warning
- Compliance error - for any compliance check that results in some error
- Once per week
- When check results changed - when any individual check result changes

**Viewing DR Plans**

The DR plans tab lists a set of currently defined plans along with plan summary information: the current status, protected and recovery sites, and the last run compliance check results.

Each DR plan protects a single vSphere protected site.
A DR plan maps a protected site to a recovery site (an SDDC on VMware Cloud on AWS) that will take over workload execution following plan completion.

### Activating DR plans

DR plans can be active or inactive (when a plan is 'deactivated'). Newly created plans are active by default. A plan is automatically deactivated upon committing a successful recovery. A previously deactivated DR plan can be explicitly re-activated.

To run either a recovery or test recovery, the plan must be active. Activating the plan also triggers continuous Compliance Checks for the plan. The Active plan state is indicated in the Status column of the plan list. Depending on whether the Test site is configured, an active plan can have either Ready or Ready (not testable) status.

A DR plan’s inactive state is also indicated in the Status column under the Disaster Recovery tab. A plan can be explicitly deactivated by clicking Deactivate plan under the Plan details view, while an inactive can be re-activatde by clicking the Activate plan button.
Running a DR Plan

A DR plan includes a set of recovery steps that capture ordering constraints and action sequencing instructions for DR operations. These are the ordered instructions that will occur when the plan is run.

You can run a DR plan either as a failover or a Test Failover. The running plan creates a ‘workflow instance’ - a runtime representation of the recovery steps in the plan, combined with other information available only when the plan starts running, such as the snapshot selection coupled with the plan’s underlying failover operations.

Plan recovery steps apply to the plan itself and control the failover workflow. For example, a planned failover creates a new workflow of operations based on the recovery steps defined in the plan. An executing plan’s recovery steps are run on the source site (power off VMs, replicate the last snapshot) and destination site (recover VMs in the predefined order).

An unplanned failover creates a different workflow based on the same recovery steps defined in the plan.

When a plan has finished executing and all of the steps in the running plan workflow have completed, you must explicitly Commit a Failover or Rollback and Acknowledge a Failback in order for the plan to transition back to a ready state.

Before Running a DR Plan

Before you run a DR plan as a failover or a test failover, the following tasks must be completed:

- A protected site defined. The DRaaS connector must be deployed and configured on the vSphere protected site. For more information, see Download the DRaaS Connector OVA (VMware Cloud Disaster Recovery UI).
- Protection groups created with snapshot schedules configured. In order to run or test a plan, the plan must have a snapshot schedule configured to replicate to the SCFS that can be used for failover.
- Tags present on the target recovery SDDC. For successful failover operations, you must ensure that any vSphere tags and tag categories associated with your
protected VMs also exist on the target Recovery SDDC vCenter, or the compliance check will display warnings, and failback will not operate successfully.

**Configure Email Alerts**

You can configure a company name for your VMware Cloud Disaster Recovery deployment, and configure emails alert for those users who want to receive notification emails when a failover or test failover has been completed.

Any email addresses you configure here will also receive emails for VMware Cloud Disaster Recovery system alerts. For more information, see Monitoring.

**Procedure**

1. To configure VMware Cloud Disaster Recovery settings, choose Configure email alerts from the small gear menu in the upper right corner of the UI.
2. In the Configure email alerts dialog, enter:
   - A Company name for your organization.
   - Email alert recipients. Enter email addresses for those accounts you want to receive alert emails when a failover or a test failover has completed.
   - Email alert sender. The email address that will appear in the From field of the email.
3. Click OK.
4. Each user that you add will be sent an email verification link that they must click to validate their email address. The verification email link must be clicked and validated before the user will receive alert emails from VMware Cloud Disaster Recovery.

**How a Failover Plan Runs**

A failover plan can be run in the following ways:

- **Failover.** A Failover operation is run following a disaster event when the source site is no longer available. The failover operation is orchestrated on the destination
site based on previously replicated snapshots. When failing over to a VMware Cloud on AWS SDDC, VMs that belong to the protection groups defined in your DR plan are recovered to the vCenter in your Recovery SDDC.

- **Test failover.** A test failover operation is similar to regular failover operation, but is run in the context of its own test execution environment. Another notable difference is that by default, a test failover stops on the first failure, whereas a regular failover continues to run even after encountering failures. All default behaviors can be overridden by custom options prior to starting the failover operation. With a test failover, you have the option to clean up the test plan. For more information, see Test Failover.

## Plan States

Once a plan is defined, it can exist in one of several states:

<table>
<thead>
<tr>
<th>Plan State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready</td>
<td>The plan is ready to be run as a failover or as a test failover operation, or the plan can be deactivated.</td>
</tr>
<tr>
<td>Ready (not testable)</td>
<td>The plan is ready to be run as a failover operation, but no test site or test mappings have been configured. This plan can be run as a failover operation, but it cannot be run as a test failover.</td>
</tr>
<tr>
<td>Incomplete (testable)</td>
<td>The plan is not fully configured for failover, but it is able to be run as a test failover.</td>
</tr>
<tr>
<td>No recovery site</td>
<td>Plan has no recovery site defined.</td>
</tr>
<tr>
<td>Inactive</td>
<td>The plan has been deactivated and cannot be run until it is re-activated. Compliance checks are not run on a plan in this state.</td>
</tr>
<tr>
<td>Plan State</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Failover rolled back</td>
<td>A failover operation was successfully rolled back.</td>
</tr>
<tr>
<td>Rolled back with errors</td>
<td>A test failover was rolled back, but some errors were encountered during rollback.</td>
</tr>
<tr>
<td>Finished with no errors</td>
<td>A failover operation has completed successfully.</td>
</tr>
<tr>
<td>Finished with errors</td>
<td>A failover has completed but with some errors. You should investigate the errors to correct anything that did not go as expected.</td>
</tr>
<tr>
<td>Test finished with no errors</td>
<td>A test failover has completed successfully.</td>
</tr>
<tr>
<td>Test cleaned up</td>
<td>A test failover has been cleaned up successfully.</td>
</tr>
<tr>
<td>Failed over with no errors</td>
<td>A failover operation completed successfully with no errors.</td>
</tr>
<tr>
<td>Test finished with errors</td>
<td>A test failover completed but with errors.</td>
</tr>
<tr>
<td>Test cleaned up with errors</td>
<td>A test failover was cleaned up but with errors.</td>
</tr>
<tr>
<td>Failover stopped</td>
<td>A failover has been stopped. Once a failover is stopped, it cannot be rolled-back or run in forward direction.</td>
</tr>
<tr>
<td>Test stopped</td>
<td>A test failover has been stopped. Once a failover is stopped, it cannot be rolled-back or run in forward direction.</td>
</tr>
<tr>
<td>Failover committed</td>
<td>A failover operation has been committed (cannot be rolled back).</td>
</tr>
</tbody>
</table>

During plan execution, a plan can exist in one of the following states:
### Running Plan State

<table>
<thead>
<tr>
<th>Running Plan State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failing over</td>
<td>A failover operation has been run and is in the process of performing the plan’s recovery steps on the target recovery site.</td>
</tr>
<tr>
<td>Retrying</td>
<td>Plan operation is in the process of restarting.</td>
</tr>
<tr>
<td>Testing</td>
<td>A failover test has been run and is in the process of performing the plan’s recovery steps in a test environment.</td>
</tr>
<tr>
<td>Canceling failover</td>
<td>A failover operation is in the process of being canceled.</td>
</tr>
<tr>
<td>Rolling back failover</td>
<td>A failover operation is in the process of being rolled back.</td>
</tr>
<tr>
<td>Cleaning up test</td>
<td>A test failover is being cleaned up.</td>
</tr>
<tr>
<td>Waiting for user input</td>
<td>A failover operation has been started and is running, but is currently stopped as it waits for user input to proceed.</td>
</tr>
<tr>
<td>Failing over... Error</td>
<td>A failover operation encountered an error.</td>
</tr>
<tr>
<td>Testing ... Error</td>
<td>A test failover encountered an error.</td>
</tr>
<tr>
<td>Terminating</td>
<td>A failover operation is in the process of being stopped.</td>
</tr>
<tr>
<td>Terminating test</td>
<td>A test failover operation is in the process of being stopped.</td>
</tr>
<tr>
<td>Rolling back failover</td>
<td>A failover or failover test is in the process of being rolled back.</td>
</tr>
</tbody>
</table>

### Run a Failover Plan

When you run a plan as a failover, a running instance of the plan recovery steps are launched and the plan continues until completion or until a pause for user input or upon encountering an error if so configured.
Procedure

1. In the VMware Cloud Disaster Recovery UI, click DR Plans.
2. In the list of plans, click on the DR Plan you want to recover. The plan you select must be in the Ready state.
3. Next, click the Failover button.
4. In the Compliance check page of the Failover wizard, you can view the Compliance check for the plan. Click Next.
5. In the Snapshots page, you can verify that the failover plan will use the snapshot you want when it fails over. By default the most recent snapshot will be selected, but if you want to choose a different snapshot, click the Use different snapshot button.
6. In the Select protection group snapshot dialog, select a snapshot you want to use for the failover operation, and then click OK.
7. Click Next. In the Runtime settings page, select one of the following two options:
   - **Ignore all errors.** Select this to run the failover in unattended mode, which allows the failover operation to continue running even when it encounters errors. All the errors will be automatically ignored by default. You can still fix those errors at the end of the failover operation if the failover completes with partial success, by clicking Retry all errors.
   - **Stop on every error.** Select this to run the failover in an attended running mode, where the failover operation stops on every error and waits for you to click Retry or Ignore and continue. This option is useful if you are running this plan as a test failover.
8. Click Next, and in the Preview page, you can view the steps that will be taken when you finally run the plan. These are the steps that were defined in the DR plan’s Recovery steps page. To achieve low RTO, VMs are initially recovered on the staging datastore. This recovery involves no data copy - VMs are powered on using the stored backups directly.
9. Click Next, and in the Confirmation page, to run this failover plan, enter the phrase FAILOVER in all upper case letters in the confirmation field.
10. Click Finish to run the failover operation.
You can monitor the failover process in the VMware Cloud Disaster Recovery UI by clicking the plan to view its details. (You can also monitor the process in the SDDC vCenter). After failover, once the VMs have been powered on, they will be migrated by Storage vMotioned onto the SDDC vSAN datastore.

After a failover operation finishes, you need to Commit the failover in order to make the effects permanent. When you commit a completed failover plan, the plan will transition to the committed state.

You should commit a failover operation with extra precaution. Until the completed failover operation is explicitly committed by an administrator, it can be rolled back (even following a successful completion). But after a commit, there is no rollback.

For more information, see Commit a Failover.

**Failover Operation Process**

When a plan is run as a failover operation, an instance of the plan is launched and begins performing the plan’s failover steps. When it begins running, the plan moves into the failover state. You can observe the running plan’s progress from the plan’s detail page:

![Failover Progress Table](image)

You can also observe the storage VMotion from the Staging datastore to the SDDC datastore following VM recovery:
### Manual Intervention During Failover

When a plan is run and its workflow is running, you can perform the following operations:

- Cancel/Cancel and Rollback
- Wait for user input
- Terminate

### Cancel and Rollback

You can cancel and rollback a running failover operation at any time. A running failover can also be canceled upon completion (but only before you either commit or acknowledge the plan completion). Canceling and rolling back a running failover operation involves reversing the current running direction and rolling back the already completed steps, starting with the last run step until the step sequence is exhausted.

If the failover has already completed, you can choose Rollback. During a rollback, each plan recovery step defines specific actions for both forward and reverse operations. Actions run in reverse direction are meant to cancel out actions that were run in the
forward direction (e.g. power-off vs. power-on, VM delete vs. VM create). A successful rollback implies the elimination of all side effects of a partially or fully completed workflow.

**Wait for User Input**

A failover operation is stopped automatically if a plan’s recovery steps are configured to stop the running plan and wait for user input before proceeding.

**Terminate**

If the running plan is stuck for some reason and cannot make any progress in either forward or reverse direction, the terminate operation will force-stop the failover or test failover. Once a failover is terminated, it cannot be rolled-back or run in forward direction.

Abort is a powerful, permanent operation and should only be used in situations when rollback cannot make any further progress because of errors, or when it is for some reason desirable to retain the side effects of a partially completed operation. The failover runtime environment must be manually cleaned up to avoid conflicts with future failover operations.

**Failover error handling**

During a failover, you might want to handle errors based on the configuration of your plan’s recovery steps.

**Stop on Every Error - Retry or Ignore and Continue**

If your plan is configured to stop when it encounters an error (‘Stop on every error’), the supported error handling actions are:

- **Retry**: Re-attempts the step, after some manual intervention to amend the error. The failed substeps are rolled back and re-ran; it may result in success or a repeated error.
- **Ignore and continue.** Continue the failover after a stop, for example if the error is not critical and the error can be fixed at a later time. This operation skips the failures from the failed substep and continues with the failover operation.

**Retry All Errors**

If your plan is configured to ‘Ignore all errors’ when a failover operation is running, the workflow ends up in a partially completed successful state. To amend those errors, the ‘Retry all errors’ operation inspects the failover from the start and retries all failed substeps. The type of retry is done in the same manner in which it would have been done using the ‘Retry’ operation.

**Retry Events**

When you retry failover steps that initially failed during running plan operation, VMware Cloud Disaster Recovery logs specific events to indicate which recovery steps are being retried.

**Note:** For more information on events, see Monitoring.

<table>
<thead>
<tr>
<th>Retry event message</th>
<th>Severity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Retry recovery of [count] VMs.”</td>
<td>Info</td>
<td>Generated when the recovery of a batch of VMs is retried.</td>
</tr>
<tr>
<td>“Retry recovery of VM [VM name].”</td>
<td>Info</td>
<td>Generated when the recovery of an individual VM is retried.</td>
</tr>
</tbody>
</table>
Ignore Events

When you run a failover or test failover, you have the option to ‘ignore all errors’ when the plan is run. If any errors are encountered when the plan is running, VMware Cloud Disaster Recovery generates the following system events to inform you which recovery steps were ignored.

<table>
<thead>
<tr>
<th>Ignore event message</th>
<th>Severity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Ignore failed recovery of [count] VMs and continue.&quot;</td>
<td>Info</td>
<td>Generated when the recovery of a batch of VMs fails during plan operation and is ignored (but can later be recovered manually).</td>
</tr>
<tr>
<td>&quot;Ignore failed recovery of VM [VM name].&quot;</td>
<td>Info</td>
<td>Generated when the recovery of an individual VM fails and is ignored (but can later be recovered manually).</td>
</tr>
</tbody>
</table>

System Behavior During Failover

You can run a plan as a failover (as opposed to a Test Failover) either intentionally as part of a planned DR exercise, or you can run a failover operation in a situation where you were not planning to failover, but now you must, due to a protected site failure.

No Overwrite of Existing VMs

To avoid undesirable side effects of executing potentially erroneous plans, a running plan never overwrites VMs that already exist on the destination datastore. If another VM is already present on the destination datastore at the exact datastore path matching the path of the recovering VM, VMware Cloud Disaster Recovery will not try to recover that VM.

Such VM recoveries will be flagged as ‘failed’ during failover or test failover and the existing VMs will be preserved. In order to make automatic recovery of these types of VMs possible, the conflicting VMs need to be explicitly deleted from the destination datastore before running a failover operation.
Batching

VMware Cloud Disaster Recovery recovers VMs in fixed size batches, also referred to as ‘substeps’. VM batching is done for these reasons:

- Recover VMs concurrently to improve RTO
- Fine-grained retry on encountering errors
- Control the load on external components

All VMs in a batch are recovered concurrently, improving overall RTO. Recovering individual VMs may involve many different stages, such as retrieving remote snapshots if selected snapshots are not available on the recovery site, customizing IP addresses, reconfiguring VM to reflect failover mappings, powering-on VMs, etc. Parallelizing stage running of a failover plan across a set of all VMs in a batch improves the overall throughput and reduces RTO.

Improving error handling is another reason for failover batching. VMware Cloud Disaster Recovery supports retry of VM recovery on transient errors or following error remediation. When the “stop on all errors” setting is configured in a plan, the running plan will stop following a failed batch running with some VMs encountering errors. Batch running is atomic in that the execution stops after all VMs in a batch have reached a terminal state - either successful recovery or an error. Upon addressing the error condition, the failed batch can be retried. Similarly, VMware Cloud Disaster Recovery can automatically retry the operation of the last batch upon observing transient errors (e.g. transient network connectivity problems).

As part of retry, VMware Cloud Disaster Recovery rolls back the batch operation and then restarts it. Batching reduces the throwaway work for large plans by limiting the rollback to the failing batch only.

As an additional benefit, batching limits concurrency imposed on other external components involved in recovery. For example, batching limits the number of concurrent requests issued to the vCenter server on the recovery site. When failover involves fetching remote snapshots or performing storage vMotion, batching will naturally limit concurrency for these operations resulting in better overall system throughput.
Skip VMs not Registered with vCenter

If a VM is not registered with vCenter on the protected site, it will not be automatically recovered and registered with vCenter on the recovery site.

VM Tags and Tag Categories

The failover process associates vSphere tags with recovered VMs that were associated with the VM on the original protected site. However, the tags and their associated categories must be pre-configured on the recovery SDDC for successful failover and failback.

When you fail over VMs with tags, you need to be aware of two possible environmental situations:

- A) Tags are present on both the protected site's vCenter configuration and on the Recovery SDDC.
- B) Tags are present on the protected site vCenter configuration, but the tags do not exist on the Recovery SDDC.

During a DR Plan compliance check, the system scans every VM in the protection group to make sure all tags associated with all VMs in the PG are available on the Recovery SDDC site.

If the category and the tags present on a VM do not exist on the Recovery SDDC, these will be flagged by the compliance checks as errors.

When you perform a failover in these two scenarios, you may need to perform extra steps before you can commit or failback the DR plan.

In scenario (A), all categories and tags have been created in target SDDC. After failover, each VM will be brought up on the Recovery SDDC and tagged with the same tags it had on the source site. In this situation, no extra action is required before committing or failing back the DR plan.

In Scenario (B), where some tags are missing (and compliance check was failing), failover will proceed, but it will complete with errors.
Hence, before you try to committing the DR plan, or failing back, after the failover completes with errors you will manually have to create the missing tags on the Recovery SDDC, from the VMware Cloud on AWS Console. Then, you can proceed to commit the plan or run a failback operation with the plan.

Migration Limits During Failover/Failback

During failover or failback, VMs in the DR plan are migrated to the 'WorkloadDatastore' in vSphere. When vSphere migration limits are reached, the failover or failback tasks may report 'Resources currently in use by other operations. Waiting'.

For information on vSphere vMotion limits, go to:

Failover Completion

Once DR plan failover is completed and has been explicitly committed, the recovery site becomes the active site. The plan is in the 'Failover committed' state where it is deactivated and no compliance checks are run.

Commit vs Acknowledge

After a failover finishes, you need to commit the plan in order to make the effects permanent. When you commit a completed failover plan, the plan will transition to the Failover committed state.

You should commit a failover with extra caution. Until the failover operation is explicitly committed by an administrator, it can still be rolled back (even following a successful completion). But after a commit there is no rollback.
If you roll back a failover (or clean up a test), or terminate any plan execution, you need to explicitly acknowledge the plan completion in order to transition the plan into Ready state and make it available for future failover operations.

The commit or acknowledgment of the plan officially ends the failover operation. The plan will have no actionable memory of the prior operation invocation outside of historic failover reports. An operation can be committed or acknowledged only after its associated workflow reaches one of the final operation states.

**Commit a Failover**

When a failover has completed with no errors, you can commit the failover permanently. You should commit a successful failover.

When you commit the plan, the effects of the failover become permanent. This cannot be undone, so make sure you are ready to commit to your changes. When you commit the failover or failback, you are asked to confirm the operation and add a note explaining the reason.
Once the failover has been committed you have to explicitly activate the plan to make it ready for future execution.
Rollback and Acknowledge a Failback

If you are not satisfied with the failover, you can perform a rollback operation, which will cause the plan to run its failover steps in the reverse order specified in the plan.

After you perform failover rollback, you need to acknowledge the rollback.
After you acknowledge the rollback, the plan is placed back into the Ready state so it can be re-run:

**Plan details**  Summary  Reports

- **Plan**: dr-plan-1
  - srcDvx → dstDvx
  - remote on-premises recovery

- **Protected groups**: pg-protected2backup

- **Continuous compliance**: 17/17 checks passed 2h ago
  - Show

**Ready**

- Failover  Test plan  Disable plan

**Post-Commit Actions**

Depending on the configuration of your completed plan, after the plan has finished there are some important actions you should take, depending on the context in which the
failover occurred.

If you are preparing for a DR plan failover, on the protected vSphere site, power off all VMs but leave them in place before you run the failover plan.

**Test Failover**

When you need to test a DR plan, you can run a failover plan as a *test failover*. A test failover is run in the context of its own test failover environment specified by the plan’s test mapping rules, so that the results of the test will not permanently affect a target failover destination.

VMware Cloud Disaster Recovery runs continuous compliance checks on a plan to ensure the plan is compliant with the steps and mappings in the plan. But compliance checks alone will not catch all possible errors that might occur during a failover.

<table>
<thead>
<tr>
<th>Test plan - TestFailoverDefaultFailure</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="Snapshots.png" alt="Snapshots" /></td>
</tr>
<tr>
<td>![Execution settings](Execution settings.png)</td>
</tr>
<tr>
<td>Preview</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Running a Test Plan**

You should run a test failover plan on a periodic basis, so you can determine if your plan works as you intended, to make sure that all IP address mappings work correctly on the VM guest OS, all your vCenter folders and settings can be recovered on the target, all scripts run correctly and in the proper order, and so on. Test failovers can also be used with periodic compliance reports to satisfy your company’s DR preparedness auditing policy.
Because test recoveries are intended for debugging problems you might encounter during a real failover, you should evaluate each failure and make sure you understand what caused each one. Once the issue is resolved, you can continue the test failover.

A test failover will stop on the first failure, by default, and all other default behaviors can be overridden by custom options prior to starting the failover operations. For unattended running of the plan, a test failover can be configured to run to completion while ignoring all errors.

Test failover operations give you the option of performing a full storage vMotion from the Staging datastore to the SDDC datastore to fully emulate a real failover, or to keep VMs on the Staging datastore to cut down on the failover time, and to allow you to test and debug your failover faster.

Without a storage vMotion, the SDDC could often be substantially smaller in size since VMs will be kept on the Staging datastore eliminating the vSAN storage capacity constraints. This type of test configuration can be more cost effective.

When you finally click the **Cleanup** button, the test failover rolls back all test side effects on test completion.

**Test Failover Example**

In this example, a failover operation is using a DR plan that will:
• Orchestrate the test failover to an SDDC, for a protection group called Users that regularly replicates snapshots of 4 VMs to the SCFS.

• Return the VMs to the initial power state after failover. When the VMs are recovered, they will be powered on or off based on their power state when the snapshot was taken. I.e., if the VM was powered off when the selected snapshot was taken, then the VM will be powered off after the test failover is complete.

Running the test DR plan consists of these main steps:

• Select snapshots
• Define runtime settings
• Preview plan steps and confirm test operation

Select Snapshots

1. In the VMware Cloud Disaster Recovery UI, select DR plans.
2. In the list of DR plans, click the Users DR plan you want to test. In this example, we are choosing a DR plan called 'User DR', which contains VMs for end user computer systems. Note that the Status indicates Ready, which means the plan is ready to be run as a failover or as a test failover (or the plan can be deactivated).
3. In the Plan details page, to test a plan click the Test plan button.
4. After you click the Test plan button, you see the Snapshot page of the Test plan wizard, which allows you to select a snapshot to use for the test failover. By default, the Test plan wizard will select the most recent snapshot taken of the protection group VMs. If you want to select an older snapshot, click the Use different snapshot button.
5. In the Select protection group snapshot dialog, you can select older snapshots, depending on the DR scenario you want to test.
6. Click OK to choose the selected snapshot. Click Next to continue.

Define Runtime Settings

1. In the Runtime settings page of the wizard, you set two test failover parameters: error handling and test storage migration.
2. Under Error handling, choose one of the following options:

- **Ignore all errors.** If you want to test a failover plan quickly and are interested in the results, you can choose to ignore all errors and run the plan unattended.

- **Stop on every error.** This option will stop the test execution on the first failure, and user intervention is required to resolve each error before continuing. This is a useful option if your plan definition is complex and you want to troubleshoot errors in failover as they occur during plan operation.

3. Under Test storage migration, choose one of the following options:

- **Full storage migration to SDDC.** VMware Cloud Disaster Recovery will perform a full storage vMotion from the staging datastore to the SDDC datastore to fully emulate a real failover. This option can take substantially longer to complete the test failover, depending on the number and size of the VMs being recovered.

- **Leave VMs and files in SCFS.** VMware Cloud Disaster Recovery will keep VMs on the staging datastore in the SCFS to cut down on the plan running time and to allow you to test and debug your failover faster. By selecting this option, the SDDC can often be substantially smaller in size since VMs will be kept on the staging datastore, eliminating the vSAN storage capacity constraints. This test configuration can be more cost effective.

4. Click **Next.**

**During test plan operation**

During a test plan operation, you can watch the progress of the plan on the plan’s details page.

Additionally, you can log in to your SDDC vCenter and see where the 4 VMs were recovered to in vSphere. The VMs are powered on or off based upon the VM power state when the snapshot was taken.
Clean Up Test Plan

If you are satisfied with the results, you can clean up the plan, which will reverse the plans instructions and undo all of the test failover operations and results by unregistering and deleting VM on the test recovery target site.

In this example, the test plan finished with no errors. You can also expand each step of the plan operation to view more information about what actually happened during the failover.

After you review the test plan failover, you can clean up the test plan by clicking the Clean up button.

In the Clean up dialog, review the details, and then enter CLEAN UP. Click the Clean up button to initiate the test plan clean up.

Acknowledge Test Plan Cleanup

You need to explicitly acknowledge that the test was run successfully and you want to tear down the test failover.
Creating an Isolated Test Environment

A test recovery operation should not affect any protected workloads that must continue to operate normally. A test recovery should not have any effect on production workloads that might be executing on the test site. Finally, a test recovery should not interfere with running an actual recovery, should that become necessary while the test recovery is in progress.

To make this possible, tests must run in an isolated runtime environment. An isolated test environment is created by specifying separate test mappings for datastores, folders, compute resources, IP addresses, and so on.

In this example, two different datastore mappings are used for a recovery and a test recovery: production recovery uses the “HQ-Failover” datastore, while test recovery uses the “Datastore1” datastore.

![Screenshot of VMware DR Plan with datastores mapping example]
In the pictures below, the production recovery maps “HQ/VM Network” on the protected site to “DR/VM Network” on the recovery site. However, for testing, “HQ/VM Network” is mapped to “DR/LAB” network on the recovery site.
In a similar manner, vCenters, vCenter folders and Compute Resources can all have different mappings for test operation, in order to avoid conflicts with production workloads.

A plan’s IP address mappings provide an alternative mechanism for network isolation. Mapping all virtual networks on the protected site to isolated virtual networks on the recovery site for testing might be too restrictive when recovery testing is impossible in complete isolation (e.g. recovered VMs might require external network connectivity). In such cases, virtual network mappings can be the same for recovery and test recovery with the two operations using different sets of IP address mapping rules to avoid IP address conflicts.

Similar to other mappings, different IP address mappings for recovery and test recovery are created by deselecting the ‘Same for test and recovery’ option and then establishing two sets of rules.
See **IP Address Mapping** for more details.
Failback

VMware Cloud Disaster Recovery supports failing back from a VMware Cloud on AWS SDDC to a protected vSphere system. Failback from an SDDC brings back only changed data. There is no rehydration — the data remains in its native compressed and deduplicated form.

The failback plan is run by clicking the Failover from VMC button.

A failback from VMware Cloud on AWS runs a number of steps, including the following:

1. VMs are powered off on the SDDC.
2. The last VM snapshot is taken following the power off. The differences between the VM state at the time of recovery and failback are then applied to the snapshot used for recovery to construct a VM backup on the SCFS for subsequent retrieval.
3. These VM backups are then retrieved to an on-premises system using a general forever incremental protocol.
4. VMs are recovered to a protected vSphere site.
5. Upon successful recovery, VMs are automatically deleted from the SDDC.
Note: The last snapshot for each VM is automatically taken and replicated to an on-premises system as a part of execution of VMware Cloud Disaster Recovery failback.

Once a failback DR plan is created from duplicating the plan and reversing its steps, the new failback plan operates the same way as any other plan. You can edit the plan to change the destination site to point to a new VMware Cloud Disaster Recovery protected site. Or, you can change the vCenter mapping if the failback target site has more than one protected site.

You can also use a new protected site and/or vCenter for failback, as long as the proper mappings are configured, but in this case incremental recovery will not be possible. If VMware Cloud Disaster Recovery is able to find a VM with the same instance UUID, then an incremental recovery is performed. If VMware Cloud Disaster Recovery cannot find the same instance UUID for a VM, then a full recovery will be initiated.

Note: You cannot add an individual VM recovery step in failback plans. However, you can Restore a VM individually from a protection group snapshot.

Note: VMware Cloud Disaster Recovery will not failback any newly-created VMs post-recovery in the SDDC that match the PG name pattern or folder criteria defined in a DR plan.

This means that any new VMs that were created after recovery and that match PG name patterns in the DR plan, will not be included when you perform a failback operation to a new or restored protected site.

Failback

DRaaS Connector and Protected Sites activates efficient incremental failback to a protected vSphere site backed by any storage. This type of failback is performed with a failback plan that is created by duplicating a failover plan, which reverses the plan mapping directions.

Preparing a Failback Plan

Once a failback plan is created, it can be edited like any other DR plan. For example, if the original protected site cannot be recovered following a disaster event, a failback
plan can be adjusted to use another on-premises site as its target.

To do this, you need to add a protected site following a normal process and then select this newly added site as a failover target for your failback plan.

**Reset the Default Datastore**

In the following example, the original protected site DRC SITE-1 (NetApp) is no longer available. A failback plan can be edited to select another site DRC SITE-2 (vSAN) as a failover target.

Similarly, if the target vCenter server is no longer available, any other vCenter associated with a failover site can be selected while configuring the failback plan.

A failback DR plan has a special page of the plan wizard for setting the default failback datastore.

Typically, VMs fail back to their original datastores. For example, if at the time of failback the original VM still exists on the failover target, VMware Cloud Disaster Recovery will preserve the datastores and folders of all its VMDKs and the VM itself. However, if the VM no longer exists (or the site is new), VMware Cloud Disaster Recovery will recover this VM to specifically designated default datastore.

So, a newly created failback plan for VMware Cloud Disaster Recovery needs to be edited to select the default datastore, as shown here:
All other failback plan mappings can be edited just like mappings in a regular failover plan.

Running a Failback Plan

A failback plan can be run just like any other DR plan. There are no prerequisites to failback execution. If the target site still contains some VMs covered by the plan, these VMs will be failed back incrementally by transferring only the differences between the state that exists on the target and in SDDC.

VMs that no longer exist on the failback target are fully recovered. VMware Cloud Disaster Recovery uses vCenter VM instance UUID to ascertain VM identity. This instance UUID is preserved for existing VMs.
You can initiate a failback in the VMware Cloud Disaster Recovery UI by clicking **Failover from VMC** button from the Plan details page.

Clicking the **Failover from VMC** button displays the status page of the last performed failback Compliance Checks. Failback compliance checks are very similar to failover compliance checks. However, since an on-premises site plays the role of a failover target, VMware Cloud Disaster Recovery reaches out to the on-premises site to check the health of various components including the on-premises vCenter.

Recovering from an SDDC back to a protected site does not currently allow you to retry steps on error. Once failback is initiated, it runs to completion unless terminated by the user.

Clicking **Next** displays a failback plan operation Preview that provides an outline of steps that will be performed.
In this example, both failover and failback plans have a single defined workflow step. This single step gets translated into ten different steps shown in preview.
The following section provides a detailed description of each of these steps.

Click **Next** and enter the phrase **PLANNED FAILOVER** in all upper case letters to complete the failback initiation.
Click **Finish** to launch the failback execution.

### Failback Process

The failback process consists of two general stages:

- **Undo stage**: VMs on the failback target are restored to the state that matches snapshots used at recovery time.

- **Catchup stage**: VM changes incurred while running in SDDC following failover are applied to the VMs on failover target.

The *Undo stage* of a failback ensures that all VMs protected by a plan are powered off and their state matches the state of the snapshot selected for failover to SDDC. The Undo stage is performed because VMs on the protected site might not be powered off prior to failover (for example, if the site became disconnected). These VMs would
continue to run and accumulate arbitrary changes diverging with the authoritative VM state in SDDC.

**Note:** If VMs are missing or have diverged significantly from their failover snapshots, the Undo Stage can take a substantial amount of time. To avoid prolonged interruptions of service, recovered VMs in the SDDC remain in powered-on state during this stage.

The *Catchup stage* of a failback operation applies incremental changes of all modified VM state in the SDDC to the VM copies on the failback target. The duration of this stage depends on the change rate and the amount of time VMs are running in the SDDC.

During this stage, VMs remain in powered off state on both the failback target and in the SDDC. Because of service downtime during this stage, it might be desirable to schedule it during the maintenance window. For example, you can edit the failback plan and inserting a wait-for-user prompt step prior to running the catchup.

**Failback example**

The following is an example of a failback plan for a plan covering a single Windows VM.

- **Step 1** — Powers off an VM on the failback target to make sure VM changes can be applied safely.
- **Step 2** — Performs the Undo Stage of failback. Because in this case the recovered VM was still present on the target site, this stage was very short. At the end of this step, VM contents match the snapshot used at failover time.
- **Step 3** — Powers off the VM in SDDC in preparation for Catchup.
- **Step 4** — Synthesizes the last snapshot that contains all changes incurred by the VM while executing in SDDC following the failover.
- **Step 5** — These changes are captured in the VM snapshot.
- **Step 6** — Customizes the VM for a failback target site. Specifically, VM IP addresses and other network parameters inside the guest are adjusted for the target site in accordance with the mapping rules.
- **Step 7** — Captures customization changes in a snapshot.
• **Step 8** — Executes Catchup. All VM changes are transferred to the target site and applied to the VM. At the end of this step, VM contents on the target site match those of the snapshot taken in Step 7.

• **Step 9** — Completes VM transformation to match the execution environment of the target site. VM networks are adjusted according to the mapping rules and Ethernet adapters are reconfigured to reflect the desired virtual networks. VM is powered on and a protection schedule is re-activated.

• **Final step** — On successful completion of the failback, VM is deleted from SDDC. This step is skipped if failback does not complete successfully to preserve VMs in SDDC.

Following a successful execution, a failback plan needs to be committed, just like any other plan.

A running failback can be terminated at any point during execution. Manual cleanup is necessary following the terminate operation. If failback is terminated, all VMs remain present in SDDC and could be powered on to resume service.

## Run a Failback Plan

The failback plan can now be activated and run. The plan is run as a recovery operation just like any other plan. Similar to other plans, failback can be tested by clicking the **Failover from VMC** button.

During snapshot selection, select the last snapshot replicated from the failback source site:
Recovery for a failback plan proceeds similarly to any other plan. At the end, it needs to be committed like any other recovery operation.

**Cleaning up Failback Source**

Following a successful failback, the failback source site needs to be cleaned up in preparation for subsequent recovery operations. Specifically, the stale VMs left behind on the datastores of the failback source site need to be deleted to avoid conflicts for future recoveries from the protected site. Similarly, protection groups need to be demoted on the recovery source.

**Continuous Compliance Checks**

Continuous DR plan compliance checks verify the integrity of a plan to ensure that any changes in the failover operation environment do not invalidate the plan’s directives when the plan is run. Compliance checks also make sure that the specified protection
groups continue to be live on the protected site and are being replicated successfully to the target site.

Compliance checks run automatically every 30 minutes for activated plans. A plan can become out of compliance if any of its conditions become violated because of environmental or plan configuration changes.

Failing Compliance checks transition a DR plan into a degraded health state of Warning or Critical. When a plan fails a compliance check, an email will be sent to the recipients configured in your Configure Email Alerts. Health checks are run on a per-plan basis - some plans can have an OK health status, while others can be in degraded states at the same time.

Note that a plan’s Compliance state will not restrict failover or test operations. Even if a plan is non-compliant in some areas, the plan can still be run as a failover or test failover.

**Compliance Check Details**

The following configuration elements are verified during a plan compliance check:

**Environment Mappings**

<table>
<thead>
<tr>
<th>Item</th>
<th>Compliance Check Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter</td>
<td>Checks the presence and availability of all source and destination vCenters referenced in the plan and checks connectivity of the vCenter.</td>
</tr>
<tr>
<td>Datastore</td>
<td>Checks for the existence and health of all source and destination datastores defined in the plan. Datastore capacity is checked on both the source and destination as part of replication health checks. For failback plans, the default failback datastore needs to be set, and compliance checks will indicate an error without it.</td>
</tr>
<tr>
<td>Datacenter folder</td>
<td>Checks for the existence of all source and destination folders listed in the plan.</td>
</tr>
</tbody>
</table>
### Item Compliance Check Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Compliance Check Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network (portgroup)</td>
<td>Checks for the existence of all source and destination port groups defined in the plan.</td>
</tr>
<tr>
<td>IP address</td>
<td>Checks the existence of all source and destination DNS servers and gateways listed in plan.</td>
</tr>
<tr>
<td></td>
<td>If any IP address mappings are defined, the compliance check will report the presence of any VMs without vSphere tools installed as warnings.</td>
</tr>
<tr>
<td>Resource Pool</td>
<td>Checks the existence of all source and destination resource pools listed in the plan. In the case of a Cluster Resource Pool mapped for either source or destination, the compliance check ensures that the Distributed Resource Scheduler (DRS) is activated.</td>
</tr>
</tbody>
</table>

### Replication Configuration and Health

<table>
<thead>
<tr>
<th>Item</th>
<th>Compliance Check Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source &lt;-&gt; Destination</td>
<td>Checks the relationship between source and destination replication to make sure replication is possible.</td>
</tr>
<tr>
<td>Replication Health</td>
<td>Checks to make sure replication is actually occurring successfully.</td>
</tr>
<tr>
<td>Snapshot Parity</td>
<td>Checks to make sure that at least one snapshot exists for every VM referenced in the plan.</td>
</tr>
</tbody>
</table>

### SDDC Checks

<table>
<thead>
<tr>
<th>Item</th>
<th>Compliance Check Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy</td>
<td>Checks that the SDDC proxy is running and reachable from VMware Cloud Disaster Recovery.</td>
</tr>
<tr>
<td>Non-VM Files</td>
<td>Checks that the file structure in the protection groups recovered are valid (i.e., no files allowed at the root of the datastore in the SDDC)</td>
</tr>
<tr>
<td>Item</td>
<td>Compliance Check Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Refresh Token</td>
<td>Checks that the refresh token used for VMware Cloud on AW CLI and operations is valid.                                                                                                                                ---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Datastore</td>
<td>Checks that the datastores ds01 and Workload are in a healthy state by checking existence, maintenance mode status, free space statistics, and mounting and accessibility from hosts.</td>
</tr>
</tbody>
</table>

**Destination Site Resource Availability**

The compliance check makes sure that the destination site is available.

**Split Brain Detection**

The plan compliance check will make sure that the source site is live and that the destination site is replicated. And, if the source site is resurrected after a failover, replication should stop since both sites are live.

**vCenter Checks**

The plan compliance check verifies all vCenter authentication access and version compatibility, to make sure that source and destination vCenters are accessible and version-compatible.

And, the compliance check ensures there are a sufficient number of network ports in the vSwitch.

**Protection Group Checks**

Every plan compliance check verifies the existence of and live status of protection groups referenced by the plan on the source site.

**VM Checks**

For all VMs referenced in the plan, the compliance check verifies:
- The existence of VMs referenced by name in workflow steps on the source - VMs that are recovered outside of their Protection Groups.
- The existence of VMs referenced by name as targets for executing scripts.
- That all VMs referenced by name are unique.

**Script Execution**

Every plan compliance check verifies the user-supplied credentials required to run any custom scripts specified in the plan.

**View a Plan’s Compliance checks**

To view the results of compliance checking, select the DR plans view in the VMware Cloud Disaster Recovery UI and then click on the disaster recovery plan.

In the Compliance pane, click **Show**. In the Continuous compliance dialog, click Create PDF report to generate a PDF version of the compliance report.
Using VMware Cloud Disaster Recovery

Continuous compliance

- All 17 checks passed with no issues!

1h ago

Protected site
- Connection to source site
- Protected groups replication schedule
- Replication health
- Datastores exist on source site
- Networks exist on source site
- Resource pools exist on source site
- Folders exist on source site

Failover site
- Connection to failover site
- vCenter server registered in failover site
- Datastores exist on failover site
- Protection groups can be recovered in failover site
- Networks exist on failover site
- Resource pools exist on failover site
- Folders exist on failover site

Orchestration
- IP address mapping
- Recovery steps
- Script server recovered before script actions

Create PDF report OK
Reports

VMware Cloud Disaster Recovery provides report generation in the PDF format for failover and test failover executions, plan configuration changes, and compliance checks.

Failover and Test Failover Reports

After a failover or test failover plan has completed (and has been committed or acknowledged), you can generate a PDF report of the plan operation by clicking the Reports tab on a plan’s details page. Select the Runtime toggle to display the list of executions for this plan. Select a completed plan execution to see a summary of the plan operation. Click Create PDF report to generate a report for download.

The generated report contains summaries of the plan configuration at the time of recovery, as well as a summary of the recovery. The report also includes details for the recovery mappings, the plan’s recovery steps, and a detailed report on each action that was taken during the recovery operation, as well as any errors that occurred.

Note: Currently, you cannot download VMware Cloud Disaster Recover PDF reports using Microsoft Edge Browser.

Configuration Reports

From the Plan Details → Reports page, click the Configuration tab to display a history of plan configuration changes. Each time a plan is changed and saved, a new version of the plan configuration is created with a time stamp.

Select an item in the list to see a brief summary of the configuration in the area below the list. Click the Create PDF report button to generate a PDF download of the report.

The generated report contains a summary of the plan configuration, as well as failover mapping details and the configured failover steps.
Compliance Reports

You can generate PDF reports for the automatic compliance checks that are regularly run on the system. The manually generated compliance report will cover the details for the last completed compliance check, including any configuration and mapping errors that need to be fixed.

You can generate a compliance report PDF by first clicking the Show button in the Continuous compliance section on a plan’s detail page. And then from the Continuous compliance dialog, click Create PDF report.

VMware Cloud Disaster Recovery will generate a PDF of the report that you can download. The report contents provide information about each compliance check and also shows detailed information for each compliance check that fails, so you can fix the errors before the plan is tested or run.

Automated PDF Report and Email

You can configure some events in a plan that will trigger report alert emails and to specific email addresses configured with VMware Cloud Disaster Recovery. This will send automatic PDF reports to the email addressed configured for all failover and test failover operations, and for compliance check events.
Monitoring

The Monitor tab displays the global collection of events and alarms from all the recovery processes for all plans, as well as other system events.

For those events and alarms that are considered more important and require attention, VMware Cloud Disaster Recovery will send email alerts for those users whose email addresses have been added to the dialog.

- **Events**. An event is an indication of activity on a protected site. Events represent the full set of observations and issues raised by VMware Cloud Disaster Recovery. Events can provide information or they can describe a situation that requires attention or action.

- **Alarms**. An alarm indicates an outstanding issue that requires attention. Alarms are triggered by events. VMware Cloud Disaster Recovery displays these in the Alarms section which will remain visible until you cancel them. A maximum of 100 active alarms are retained at any given time. If the maximum is exceeded, the system will automatically clear the oldest alarm(s).

- **Alerts**. An alert is an email notification that is sent to a specified user. The system sends email alerts for a subset of alarms that are considered critical.

Event Filters

You can filter the Events list in three different ways:

- **Event Category Filter**. Filter by specific event category, such as audit events, user management, protection group operations, and more. OR

- **Event Severity Filter**. Filter by event severity such as Info, Warning, Error, Emergency. AND

- **Event Timestamp Filter**. Filter by a specific duration of time, such as Today, Last 24 hours, Last 7 days, or any specific time frame you choose.

**Note**: The event category and event severity filters are mutually exclusive. This means that when you filter by event category, you cannot also filter by severity. Conversely, if you filter by event severity, you cannot also filter by event category.
You can however, combine the timestamp filter with either category or severity filters.

You can also filter the events list page results further by text strings. This search filters the currently displayed list of events in the UI based on the entered text:

The Events list will show a maximum of 100 events at first viewing. To view more events, you can click the **Load more** button at the bottom of the page.

**Event Category Filter**

Event categories allow you to filter events by the categories listed in the following table.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit</td>
<td>Events related to user authentication, such as when a user logs in and logs out.</td>
</tr>
</tbody>
</table>
### Category Description

**Site**
Events related to sites, such as adding or removing a protected site, downloading a VMware Cloud Disaster Recovery connector VM, registering vCenter.

**SDDC**
Events related to a Recovery SDDC, such as deploying or deleting an SDDC, adding or removing a network, and more.

**Recovery**
Events related to DR plan operations, such as a recovery or failback operation, acknowledging and committing a plan, deleting a plan, and more.

**Organization**
Events related to user management, such as inviting a user, deleting a user, changing a user’s roles, changing an organization name, and more.

**Protection**
Events related to protection groups, such as creating or deleting protection groups, snapshots, and more.

### Event Severity Filter

You can filter by the event severities listed in the following table.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Info</em></td>
<td>Descriptive information about an operation or state of the system, including information that might be useful.</td>
</tr>
<tr>
<td><em>Warning</em></td>
<td>Indicates a situation that requires attention. A warning condition does not affect system operation.</td>
</tr>
<tr>
<td><em>Error</em></td>
<td>Indicates that an operation failed or that there was a hardware error. An error condition does not affect continued system operation.</td>
</tr>
<tr>
<td><em>Emergency</em></td>
<td>Indicates that a fatal event occurred. A fatal event affects continued system operation.</td>
</tr>
</tbody>
</table>
Event Timestamp Filter

You can restrict the events displayed by timestamp, which allows you to set a specific time or time duration to filter events by. This is useful when you want to see recent events, old events, or events that occurred during a specific time period.

You can choose 'quick select' times, or use the Since and Up to calendar selectors to specify a time frame by which to filter the events.

Plan-related Events

When a plan is started and recovery begins, events are populated on the plan details page for the current run of the plan. Each event signifies an action within the substeps in the recovery process, as shown here:

Alarms

An alarm indicates important issue that requires attention. An alarm remains active until you clear the alarm to dismiss it (click the little blue check mark next to the alarm).