Lab 08 - DRaaS with VMware Cloud Disaster Recovery (Part2)

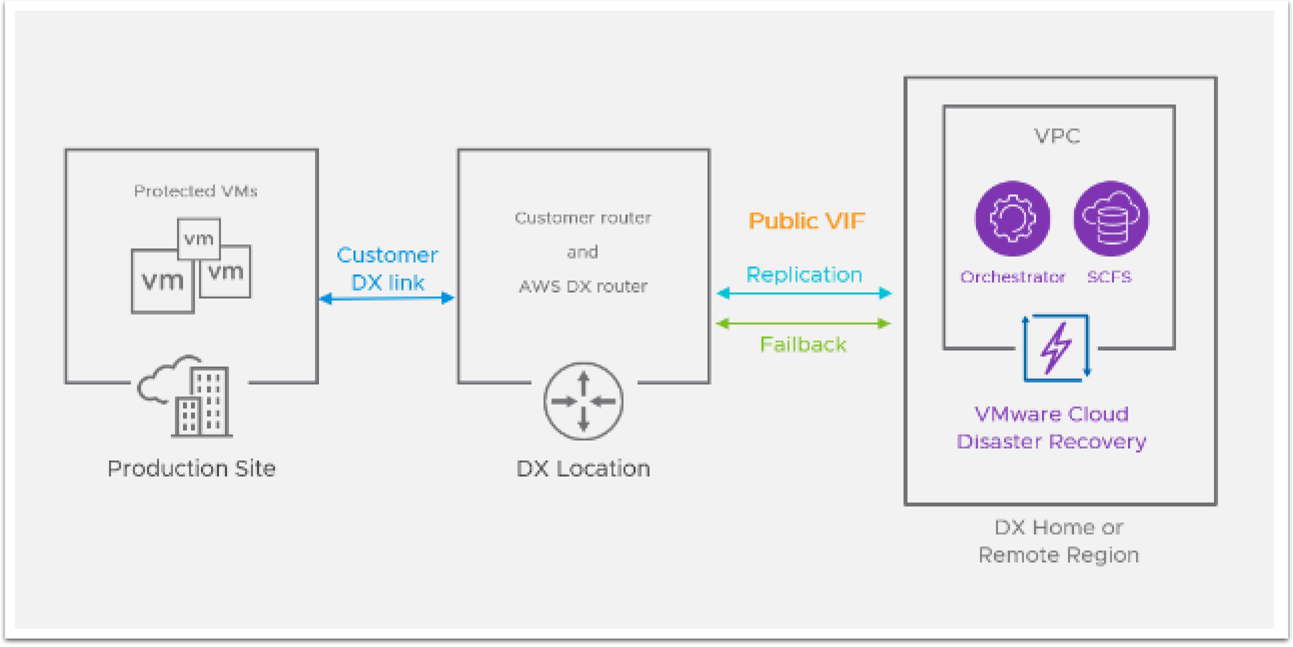
Introduction

VMware Cloud Disaster Recovery is an on-demand disaster recovery service that provides an easy-to-use Software-as-a-Service (SaaS) solution and offers cloud economics to keep your disaster recovery costs under control.

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

Using VMware Cloud Disaster Recovery you can protect your On-premises and/or VMC on AWS SDDCs and recover them into the cloud.

VMware Cloud Disaster Recovery lets you deploy a recovery SDDC in VMware Cloud on AWS (or add an existing SDDC) to use for recovery and testing of your DR plans. You can add hosts, clusters, new networks, request public IP addresses, configure NAT rules, and also delete the recovery SDDC. In the event of a disaster or planned recovery operation, you can recover VMs from your protected site to your recovery SDDC.



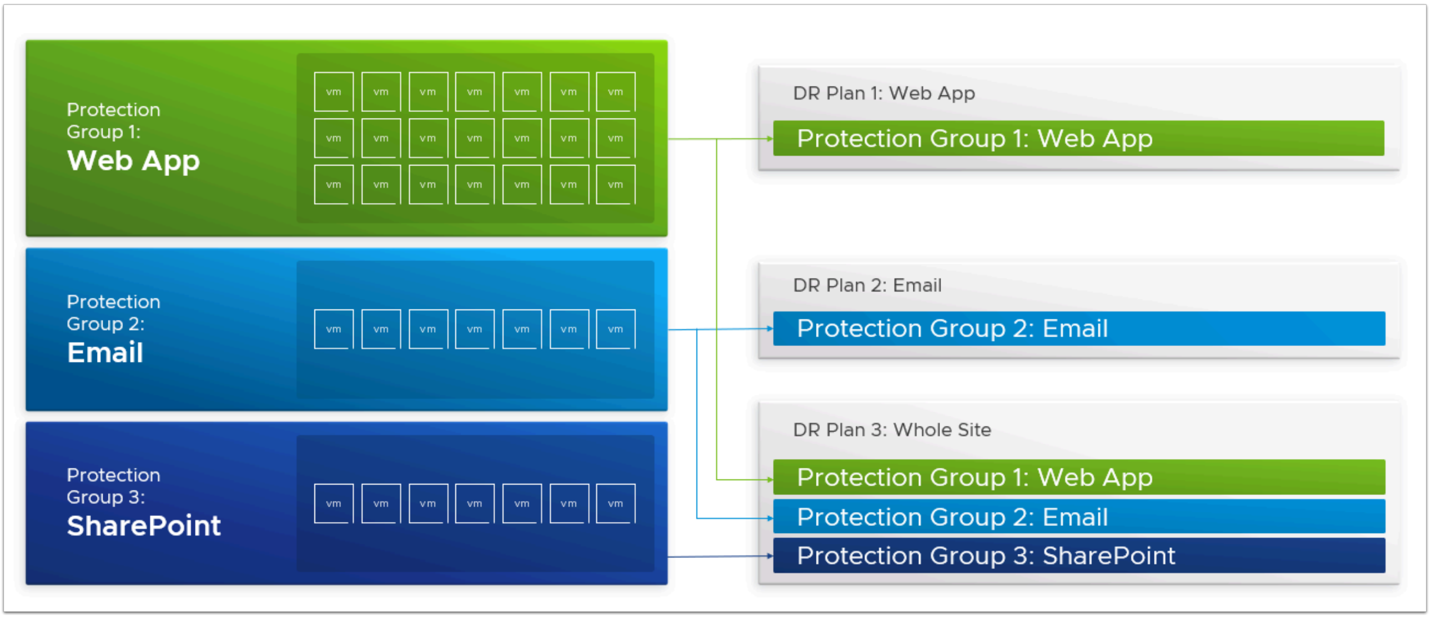
TASKS

Task 1 - Create a DR Plan

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

Plans run either for recovery as an actual DR plan operation, or they run as a test recovery, which performs all of the plan's recovery operations in a test site for validation.

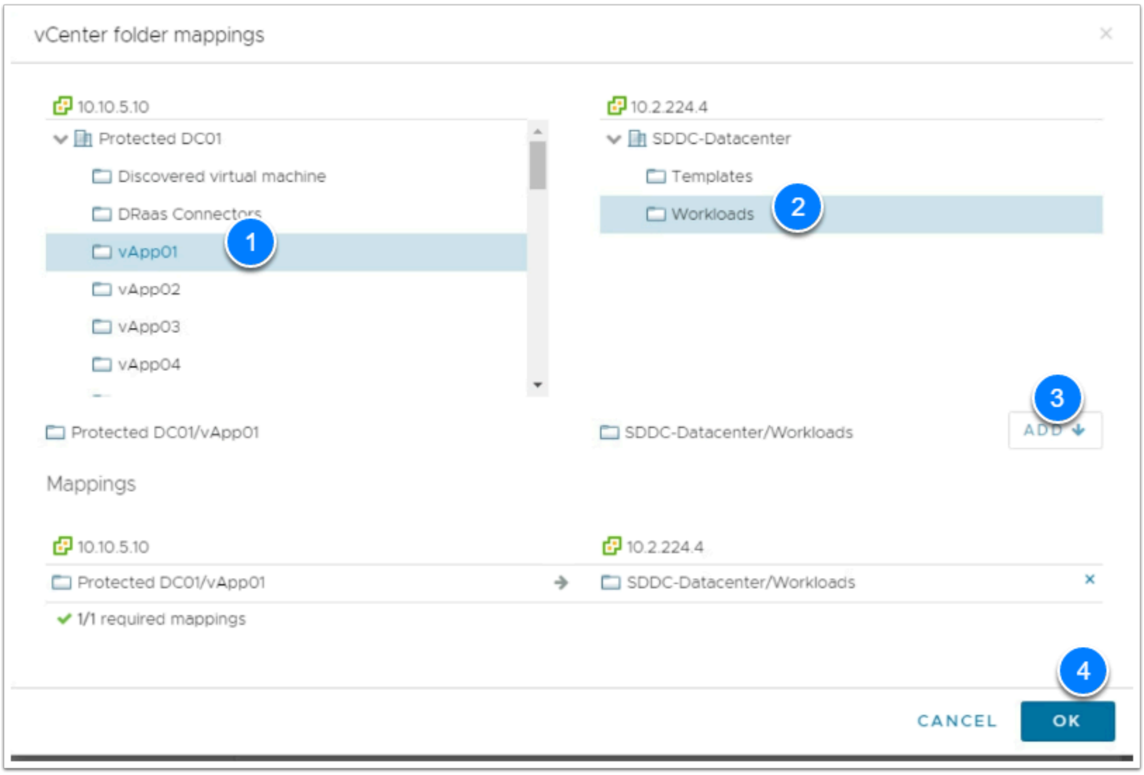
Execution pacing is configurable. When a plan runs, a running instance of the plan launches and typically continues executing its recovery steps to completion. A recovery or test plan can also continue to specific points in the process and wait for user input, or it can stop and wait for a specified time limit, and then continue until the next stop or to completion. You can also add pre or post-scripting to a VM's recovery step.


Protection Group 1: Web App
vm
Protection Group 2: Email
vm
Protection Group 3: SharePoint
vm
DR Plan 1: Web App
Protection Group 1: Web App
DR Plan 2: Email
Protection Group 2: Email
DR Plan 3: Whole Site
Protection Group 1: Web App
Protection Group 2: Email
Protection Group 3: SharePoint

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. Compliance checks give the user the opportunity to address issues and restore the plan's integrity before a disaster occurs. For developing and retaining the skill set of related DR activities, 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.

1. From the VDI desktop access your VMware Cloud DR Browser tab. If you previously closed the tab or if your session timed out please see **Part 1** - Task 3.1, steps 1-14
2. In the VMware Cloud Disaster Recovery UI, click **Recovery Plans**
3. Click **Create plan**
4. In the Create Plan dialog, configure the Plan as follows:
    - Plan Name: **VMCEXPERT#-XX_DR_Plan (**Where **#** is your Environment Id and **XX** is your student number)
    - Description: <**Leave default**>
    - Recovery Site: **Existing recovery SDDC**
    - Protected Site: **<Select you assigned Protected site>** i.e. Protected DC01 (01-10), Protected DC02 (11-20), or Protected DC03 (21-30)
    - vCenter: **<Leave default>**
    - Groups: <**Choose_your_protection_group**> i.e. VMCEXPERT2-31_PG
    - vCenter Failover mapping: **<Leave default>**
    - vCenter Folder Mapping: Select **Map Folders** button
        - In the Source (On-Premises) vCenter Select **vAppXX** (where **XX** is your student number)
        - In the SDDC vCenter Select **Workloads**
        - Click **Add**
        - Click **Ok**



vCenter folder mappings

10.10.5.10
- Protected DC01
  - Discovered virtual machine
  - DRaas Connectors
  - vApp01
  - vApp02
  - vApp03
  - vApp04

10.2.224.4
- SDDC-Datacenter
  - Templates
  - Workloads

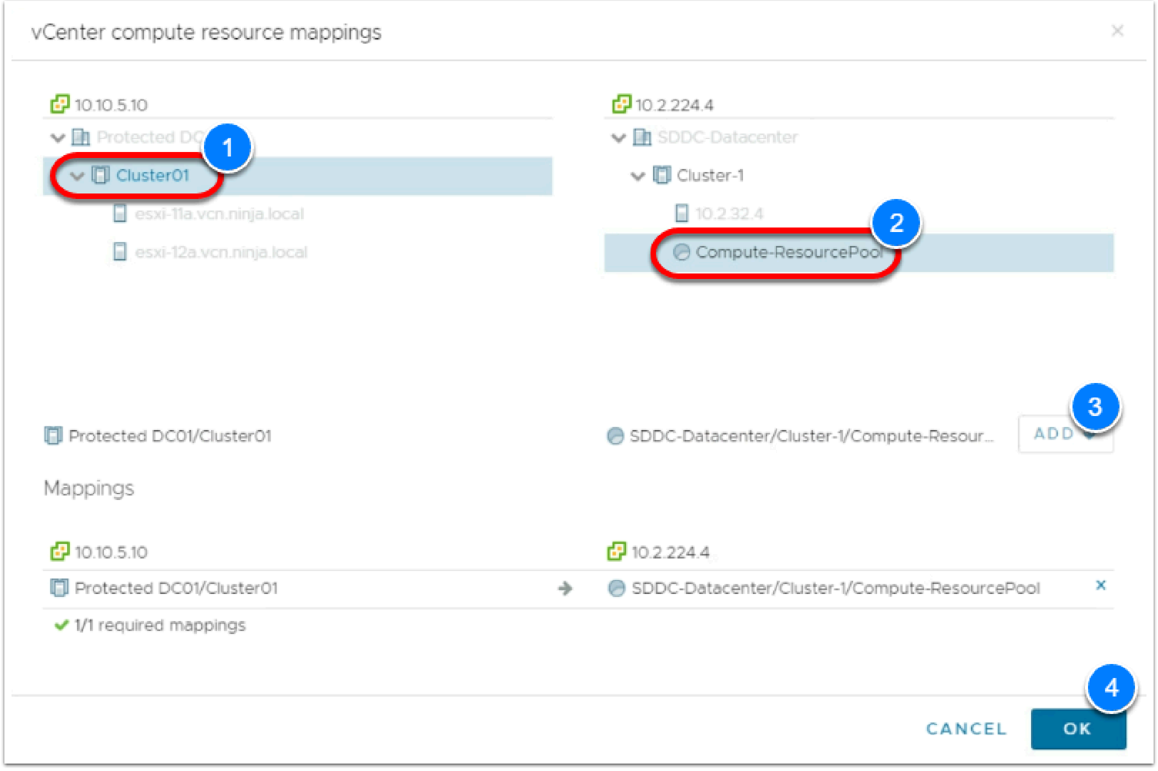
Protected DC01/vApp01 SDDC-Datacenter/Workloads

Mappings

10.10.5.10		10.2.224.4
Protected DC01/vApp01	→	SDDC-Datacenter/Workloads

✓ 1/1 required mappings

5. Click **Next**, and continue configuring your Plan
    - Compute Resources Failover mapping Click **Map Compute Resources** button
        - In the Source (On-Premises) vCenter Select **Cluster01**
        - In the SDDC vCenter Select **Compute-ResourcePool**
        - Click **Add**
        - Click **Ok**



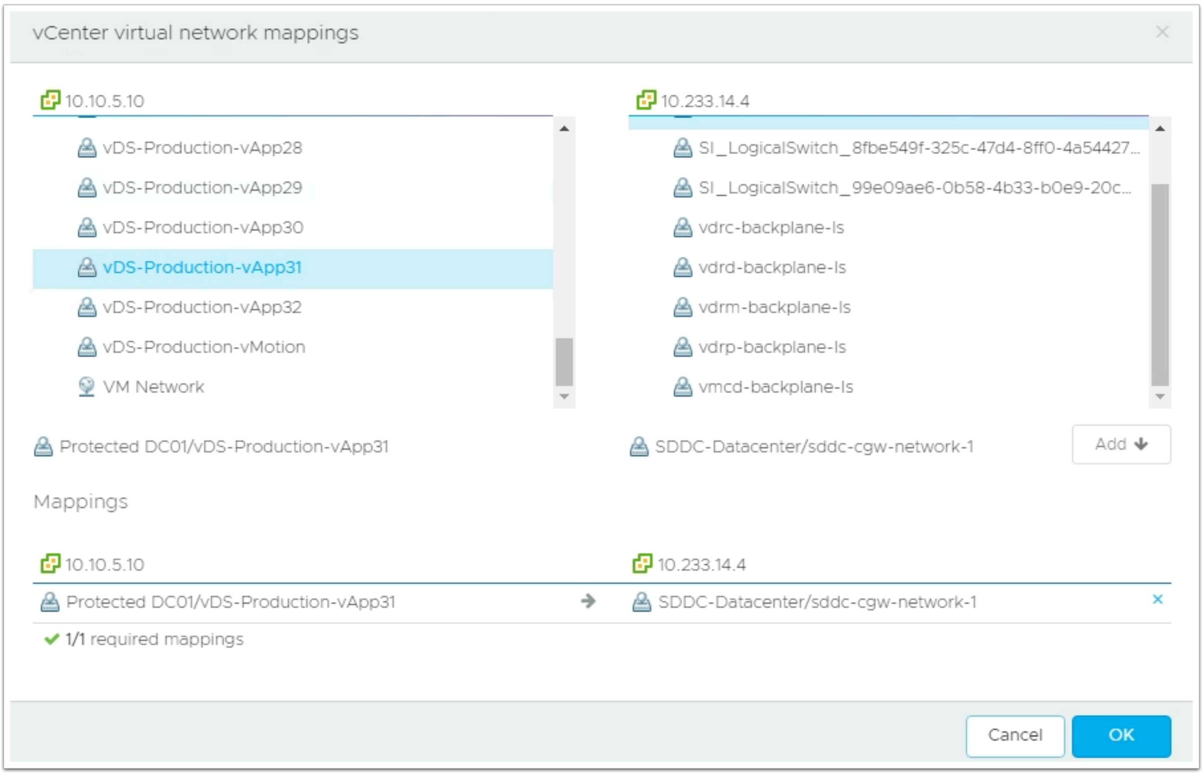
Protected DC01/Cluster01 SDDC-Datacenter/Cluster-1/Compute-Resour...

Mappings

10.10.5.10		10.2.224.4
Protected DC01/Cluster01	→	SDDC-Datacenter/Cluster-1/Compute-ResourcePool

✓ 1/1 required mappings

6. Click **Next**, and continue configuring your Plan
   - Virtual Network Failover mapping Click **Map Virtual Network** button
     - In the Source (On-Premises) vCenter Select <**vDS-Production-vAppXX**> (where **XX** is your student number)
     - In the SDDC vCenter Select **sddc-cgw-network-1**
     - Click **Add**
     - Click **Ok**



vCenter virtual network mappings

10.10.5.10

vDS-Production-vApp28
vDS-Production-vApp29
vDS-Production-vApp30
vDS-Production-vApp31
vDS-Production-vApp32
vDS-Production-vMotion
VM Network

10.233.14.4

SI_LogicalSwitch_8fbe549f-325c-47d4-8ff0-4a54427...
SI_LogicalSwitch_99e09ae6-0b58-4b33-b0e9-20c...
vdrc-backplane-ls
vdrd-backplane-ls
vdrm-backplane-ls
vdrp-backplane-ls
vmcd-backplane-ls

Protected DC01/vDS-Production-vApp31

SDDC-Datacenter/sddc-cgw-network-1

Add

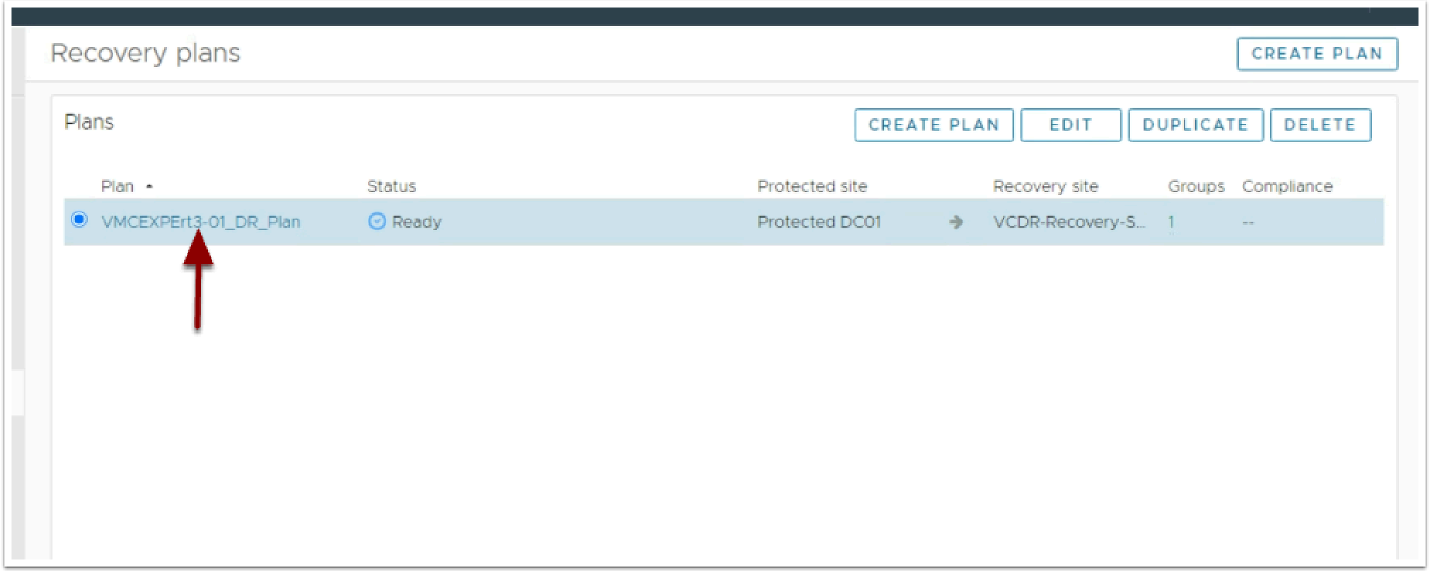
Mappings

10.10.5.10		10.233.14.4
Protected DC01/vDS-Production-vApp31	→	SDDC-Datacenter/sddc-cgw-network-1

✓ 1/1 required mappings

Cancel OK

7. Click **Next**, and continue configuring your Plan
   - On the IP Addresses page Click **Next**.
     We will not provide an IP address rule. The Migrated VMs will use DHCP once recovered
   - Script VM: <**Leave default**>, Click **Next**
   - Recovery Steps: <**Leave default**>, Click **Next**
   - Ransomware: Leave the default and click **Next**
   - On the Alerts Page, click **Finish**



Recovery plans

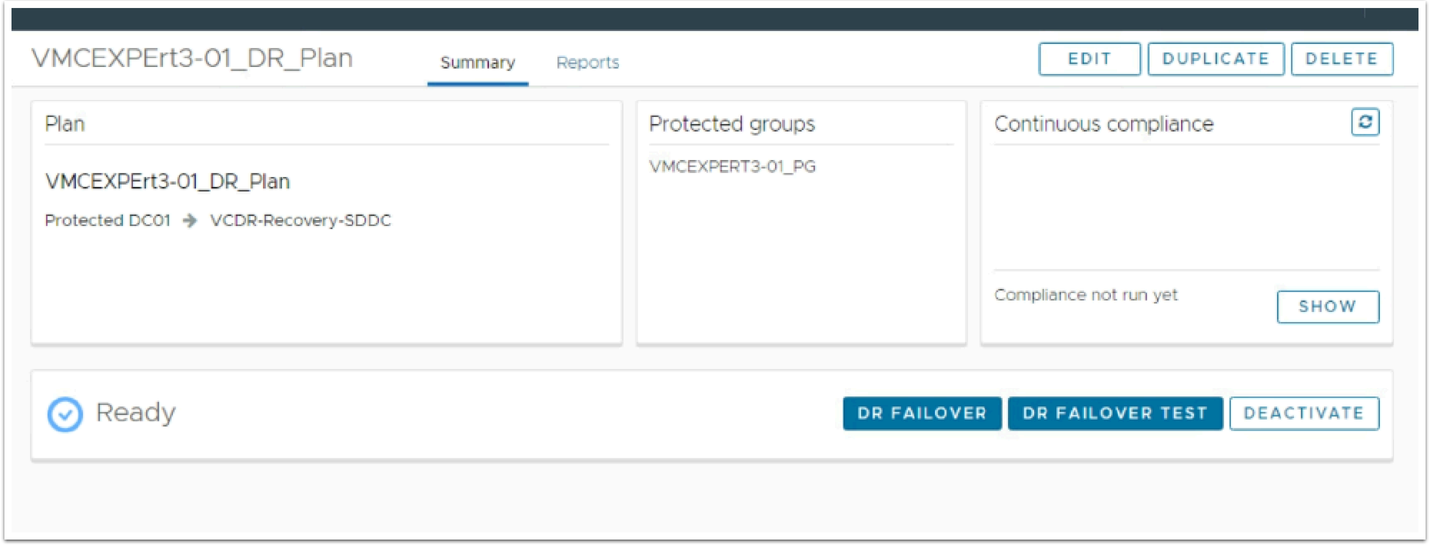
CREATE PLAN

Plans

CREATE PLAN EDIT DUPLICATE DELETE

	Plan	Status	Protected site		Recovery site	Groups	Compliance
●	VMCEXPErt3-01_DR_Plan	Ready	Protected DC01	→	VCDR-Recovery-S...	1	--

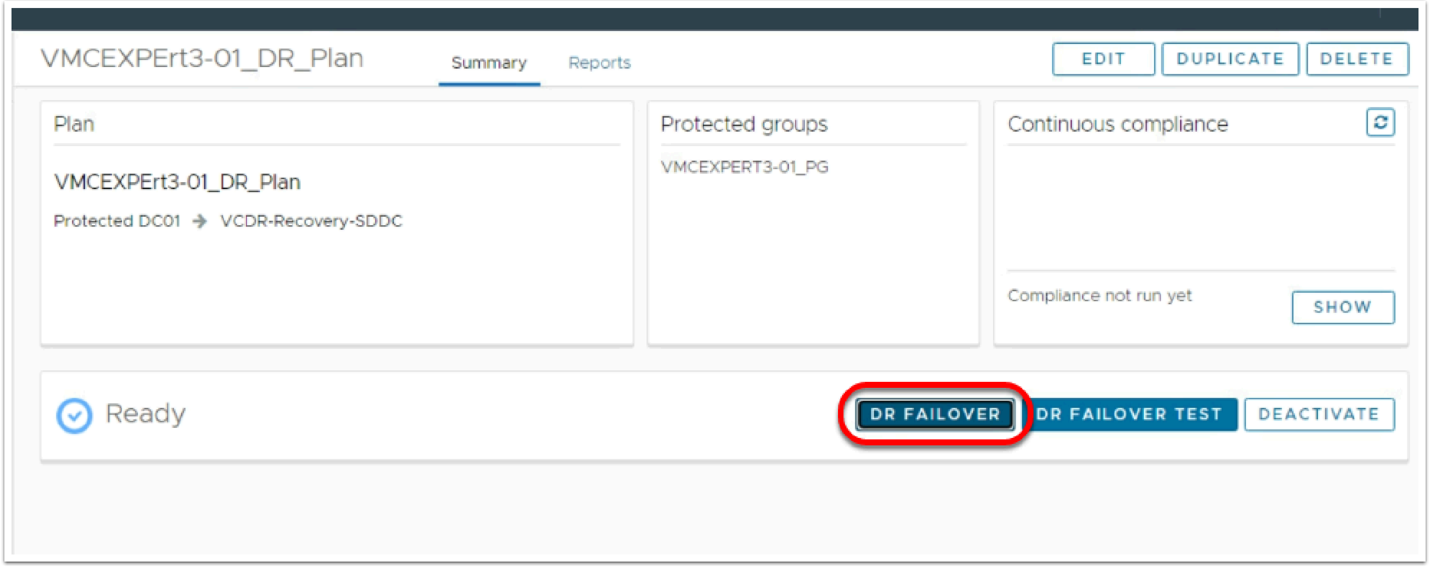
8. Once created, click your DR Plan to review and manage it.



Task 2 - Execute a Failover

When you run a DR Plan as a failover, a running instance of the plan recovery steps launches and the plan continues to completion, or until a pause for user input, or upon encountering an error (if configured).

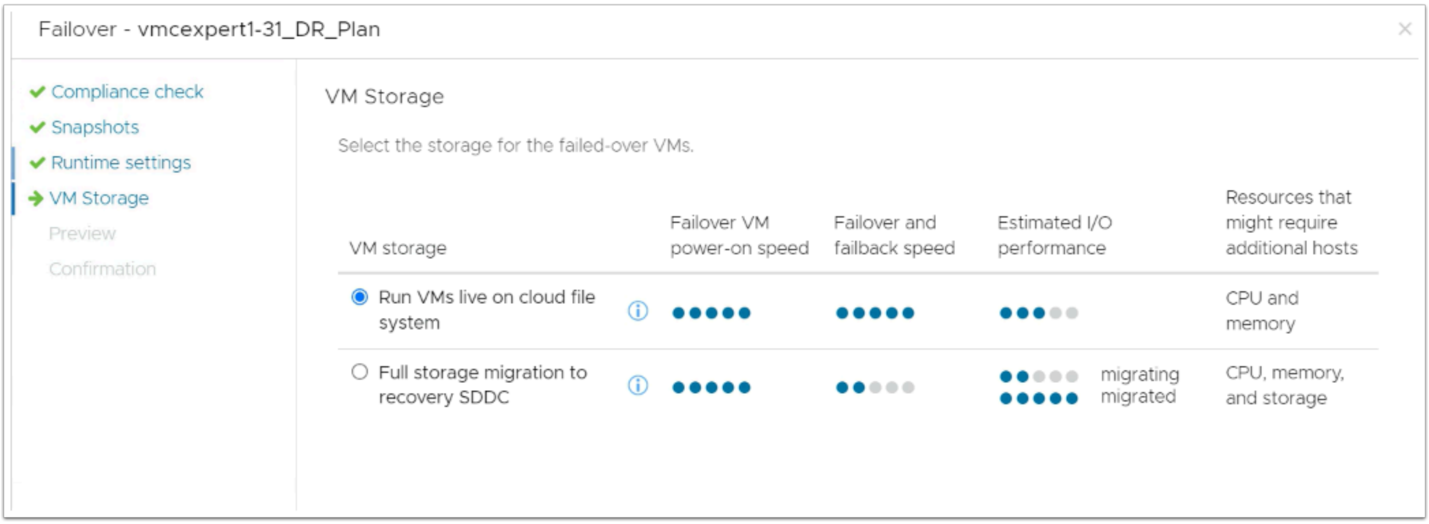
1. From the Summary page of your DR Plan you created in the previous task. Click the **DR Failover** button



2. In the DR Failover wizard click **Next** and select the following options:
   - Snapshot <**Your_Previous_or_latest_Snapshot**>
   - Runtime Settings: <**Leave default**>, click **Next**
   - VM Storage: **Run VMs live on cloud file system**, click **Next**

- Preview: Review the steps to be performed as part of the Failover and click **Next**

3. On the Confirmation Page Type **FAILOVER** in the confirmation textbox
4. Click **Start Failover**

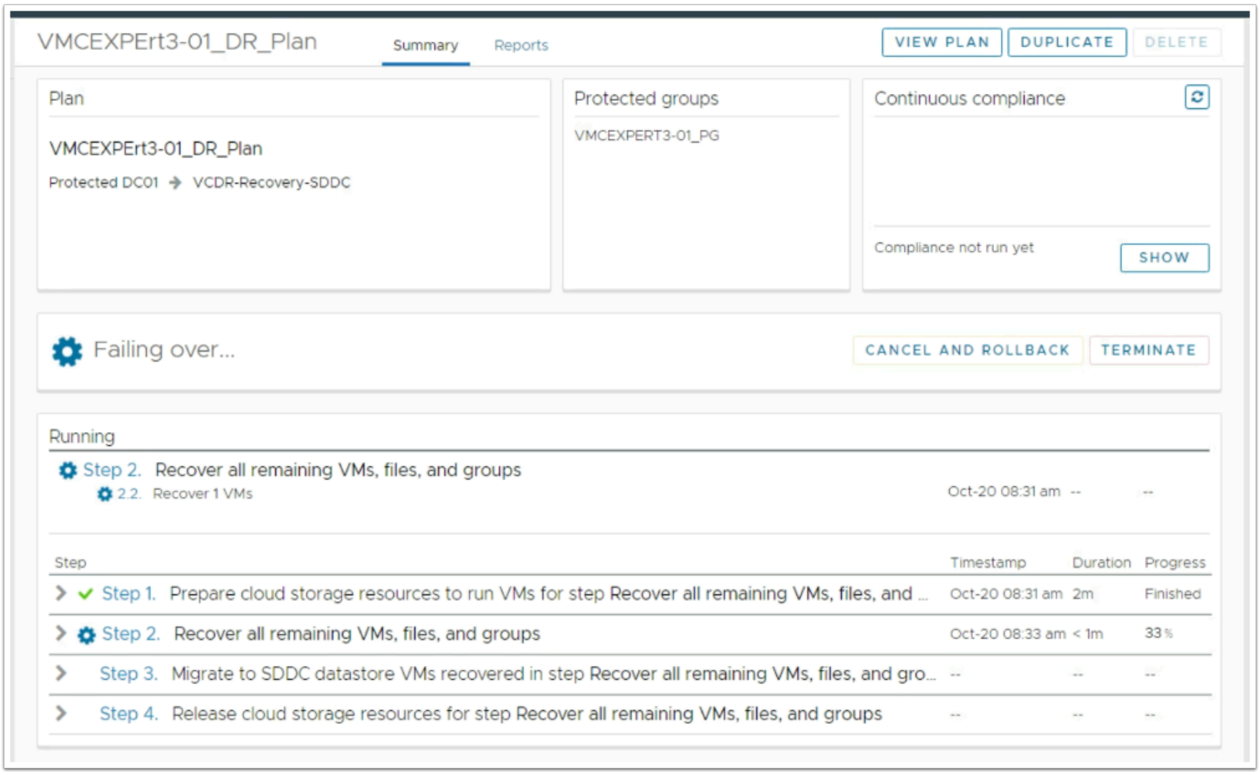


Failover - vmcexpert1-31_DR_Plan

VM Storage

Select the storage for the failed-over VMs.

VM storage		Failover VM power-on speed	Failover and failback speed	Estimated I/O performance		Resources that might require additional hosts
● Run VMs live on cloud file system	ⓘ	●●●●●	●●●●●	●●●○○		CPU and memory
○ Full storage migration to recovery SDDC	ⓘ	●●●●●	●●○○○	●●○○○ ●●●●●	migrating migrated	CPU, memory, and storage



VMCEXPErt3-01_DR_Plan

Plan

VMCEXPErt3-01_DR_Plan

Protected DC01 → VCDR-Recovery-SDDC

Protected groups

VMCEXPERT3-01_PG

Continuous compliance

Compliance not run yet

Failing over...

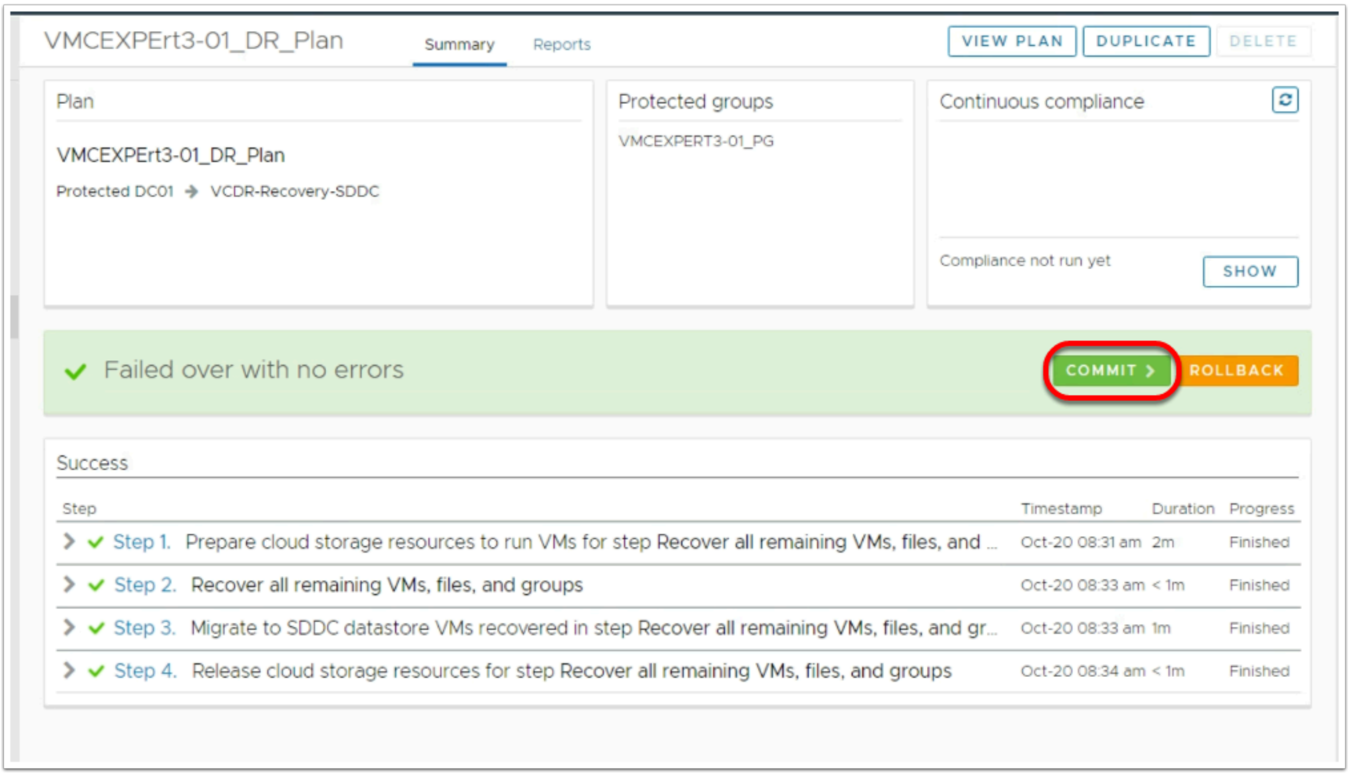
Running

Step 2. Recover all remaining VMs, files, and groups

2.2. Recover 1 VMs Oct-20 08:31 am -- --

Step	Timestamp	Duration	Progress
> ✓ Step 1. Prepare cloud storage resources to run VMs for step Recover all remaining VMs, files, and ...	Oct-20 08:31 am	2m	Finished
> Step 2. Recover all remaining VMs, files, and groups	Oct-20 08:33 am	< 1m	33 %
> Step 3. Migrate to SDDC datastore VMs recovered in step Recover all remaining VMs, files, and gro...	--	--	--
> Step 4. Release cloud storage resources for step Recover all remaining VMs, files, and groups	--	--	--

5. Monitor the Failover process. This can take as much as 10 mins
6. Once the Plan execution has completed without error(s), click **Commit**
7. In the commit dialog:
   - Select the **Checkbox** to **Create a failback plan**
   - Select the On-Premises Datastore **Protected DCXX/datastore/NFS SharedDS01**
   - Type **COMMIT FAILOVER**
   - Click **Commit**


VMCEXPErt3-01_DR_Plan

Plan

VMCEXPErt3-01_DR_Plan

Protected DC01 → VCDR-Recovery-SDDC

Protected groups

VMCEXPERT3-01_PG

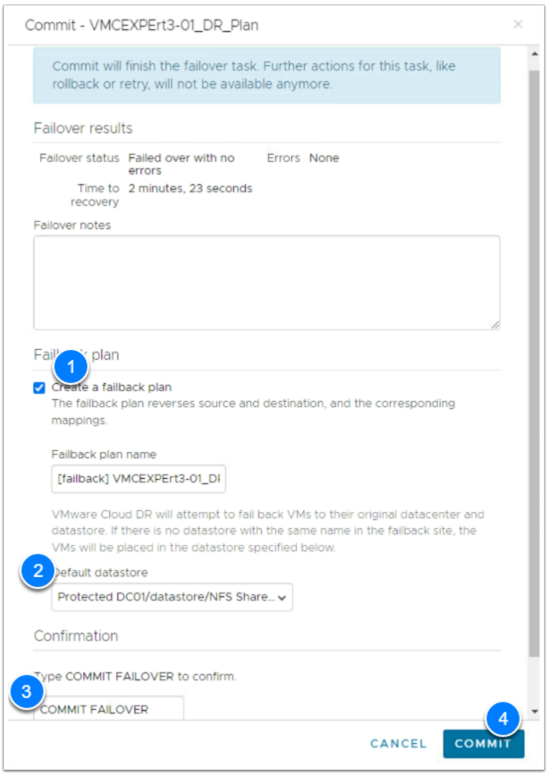
Continuous compliance

Compliance not run yet

✓ Failed over with no errors

Success

Step		Timestamp	Duration	Progress
> ✓ Step 1.	Prepare cloud storage resources to run VMs for step Recover all remaining VMs, files, and ...	Oct-20 08:31 am	2m	Finished
> ✓ Step 2.	Recover all remaining VMs, files, and groups	Oct-20 08:33 am	< 1m	Finished
> ✓ Step 3.	Migrate to SDDC datastore VMs recovered in step Recover all remaining VMs, files, and gr...	Oct-20 08:33 am	1m	Finished
> ✓ Step 4.	Release cloud storage resources for step Recover all remaining VMs, files, and groups	Oct-20 08:34 am	< 1m	Finished


Commit - VMCEXPErt3-01_DR_Plan

Commit will finish the failover task. Further actions for this task, like rollback or retry, will not be available anymore.

Failover results

Failover status: Failed over with no errors

Errors: None

Time to recovery: 2 minutes, 23 seconds

Failover notes

Fail[illegible] plan

1

☑ Create a failback plan

The failback plan reverses source and destination, and the corresponding mappings.

Failback plan name: [failback] VMCEXPErt3-01_DI

VMware Cloud DR will attempt to fail back VMs to their original datacenter and datastore. If there is no datastore with the same name in the failback site, the VMs will be placed in the datastore specified below.

2

Default datastore: Protected DC01/datastore/NFS Share...

Confirmation

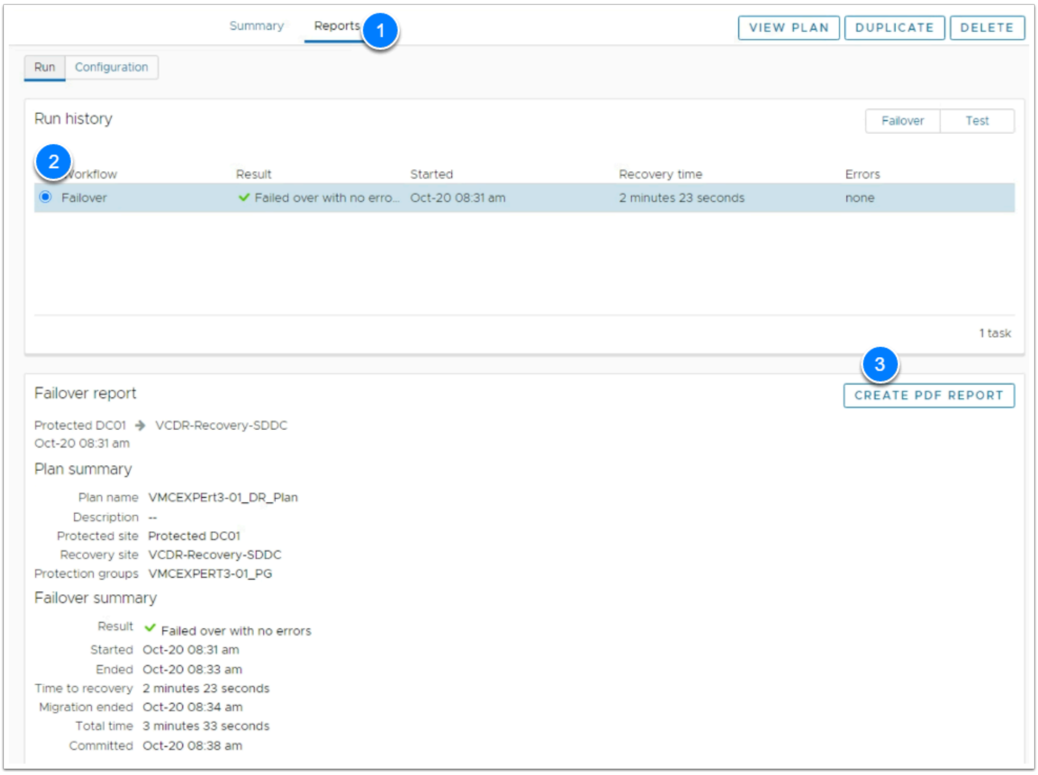
Type COMMIT FAILOVER to confirm.

3

COMMIT FAILOVER

4

8. Click the **Reports** tab at the top.
9. Select the radio button to select your Failover.
10. On the lower right, click **Create PDF Report** to generate and download a report of the failover execution. This report can be used for audit and compliance purposes.



Run history

Workflow	Result	Started	Recovery time	Errors
● Failover	✓ Failed over with no erro...	Oct-20 08:31 am	2 minutes 23 seconds	none

1 task

Failover report

Protected DC01 → VCDR-Recovery-SDDC
Oct-20 08:31 am

Plan summary

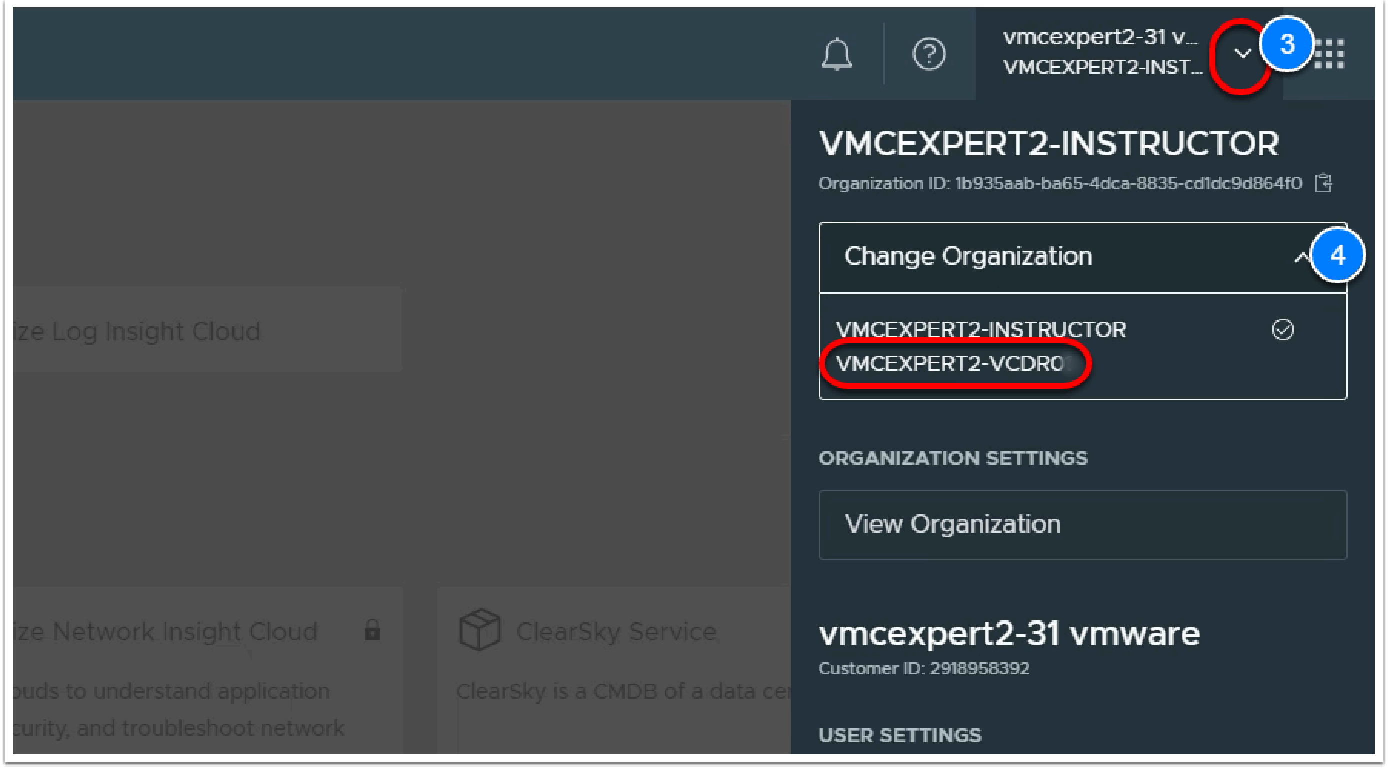
Plan name	VMCEXPErt3-01_DR_Plan
Description	--
Protected site	Protected DC01
Recovery site	VCDR-Recovery-SDDC
Protection groups	VMCEXPERT3-01_PG

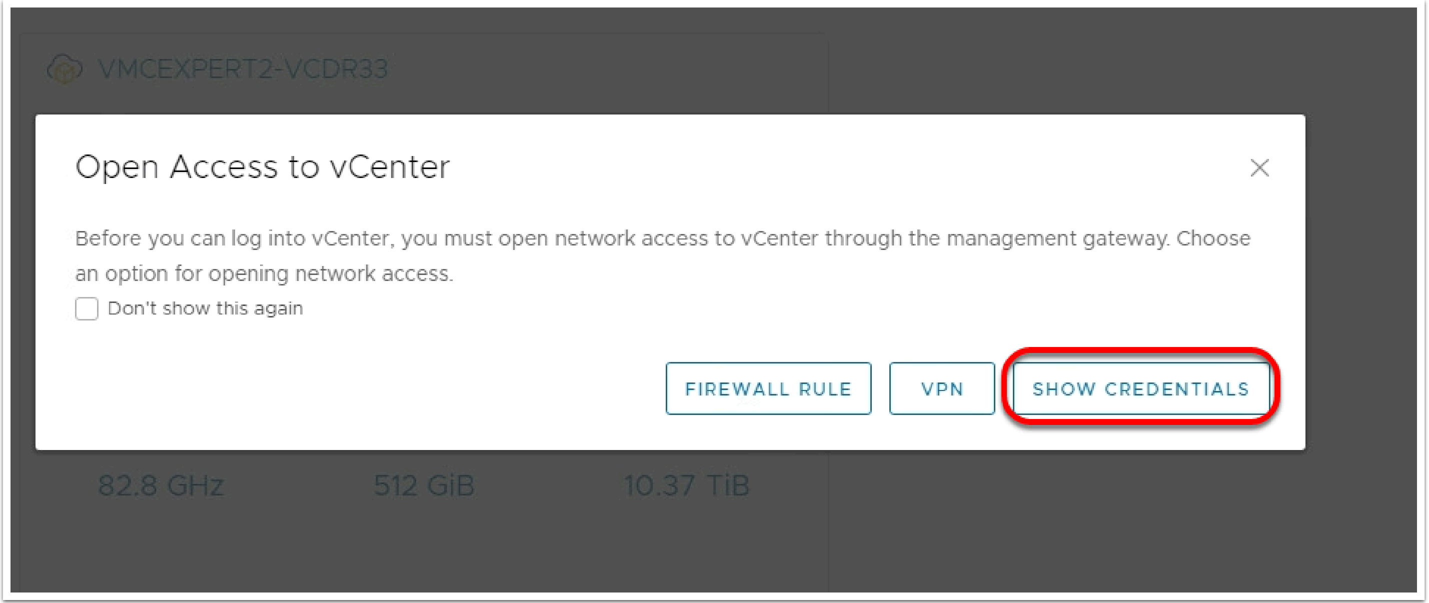
Failover summary

Result	✓ Failed over with no errors
Started	Oct-20 08:31 am
Ended	Oct-20 08:33 am
Time to recovery	2 minutes 23 seconds
Migration ended	Oct-20 08:34 am
Total time	3 minutes 33 seconds
Committed	Oct-20 08:38 am

Task 3 - Review the Recovered Virtual Machine

1. In a new Browser tab, click the **VMware Cloud SDDC** Chrome Bookmark
2. If prompted, login in as
   - **vmcexpert{1|2|3}-##@27virtual.net** (where **##** is your student number) i.e **vmcexpert1-02@27virtual.net**
   - **{Password-Provided-by-Instructor}**
3. In the upper right-hand corner of the Cloud Console, Click the **Drop-down** next to your account
4. If required, click the **Drop-down** next to your username to Change organization and select **Your VCDR Org** (VMCEXPERTX-VCDR01)
5. Click **Open vCenter** on the VCDR SDDC Tile
6. Click **Show Credentials**
7. Copy the vCenter Password and Click **Open vCenter**





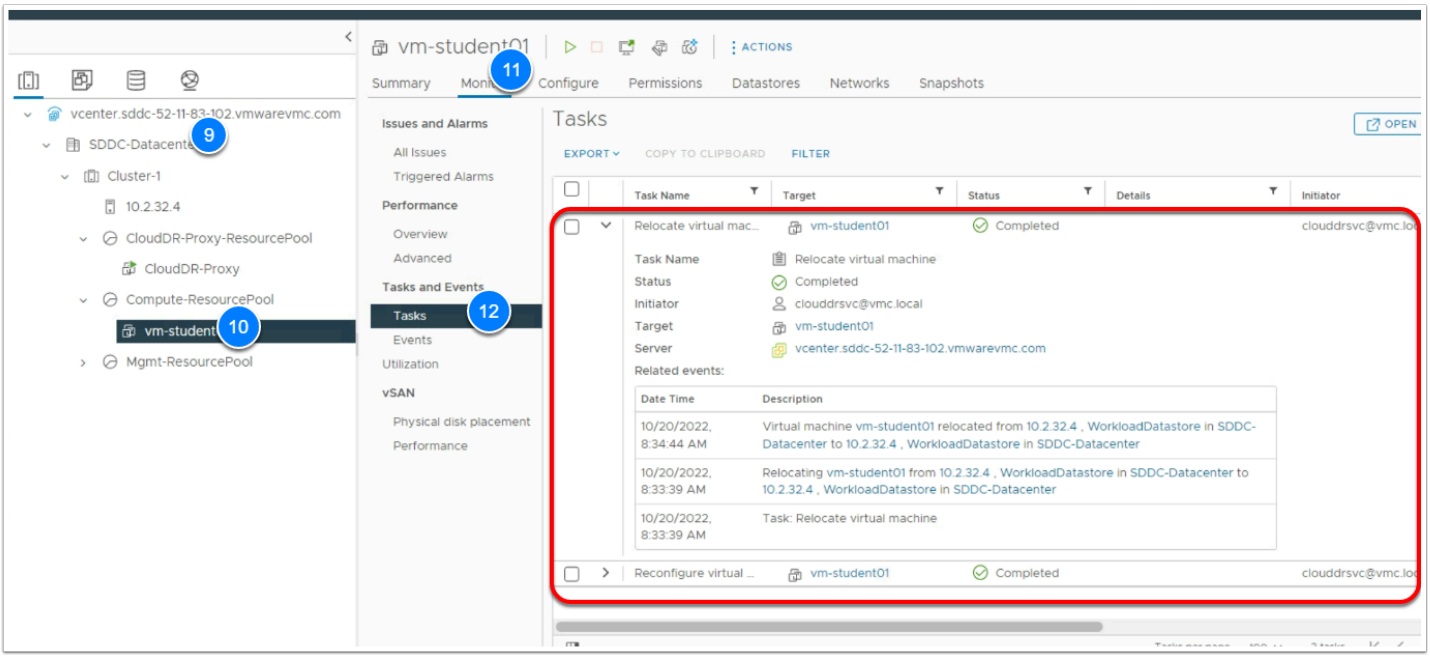
Open Access to vCenter

Before you can log into vCenter, you must open network access to vCenter through the management gateway. Choose an option for opening network access.

□ Don't show this again

FIREWALL RULE | VPN | SHOW CREDENTIALS

8. Log into the VMC on AWS SDDC as:
   - **cloudadmin@vmc.local**
   - **<copied_password_from_step 7>**
9. In the vCenter Inventory expand SDDC-Datacenter --> Cluster-1 --> Compute-ResourcePool to find your recovered vm <**vm-studentxx**> (where **xx** is your student number)
10. Select <**your Virtual Machine**>
11. Select the **Monitor** tab
12. Click **Tasks** to review the vSphere tasks performed when recovering the Virtual Machine



Task Name	Target	Status	Details	Initiator
Relocate virtual mac...	vm-student01	Completed		clouddrsvc@vmc.loc
Reconfigure virtual ...	vm-student01	Completed		clouddrsvc@vmc.loc

Task Name: Relocate virtual machine
Status: Completed
Initiator: clouddrsvc@vmc.local
Target: vm-student01
Server: vcenter.sddc-52-11-83-102.vmwarevmc.com
Related events:

Date Time	Description
10/20/2022, 8:34:44 AM	Virtual machine vm-student01 relocated from 10.2.32.4 , WorkloadDatastore in SDDC-Datacenter to 10.2.32.4 , WorkloadDatastore in SDDC-Datacenter
10/20/2022, 8:33:39 AM	Relocating vm-student01 from 10.2.32.4 , WorkloadDatastore in SDDC-Datacenter to 10.2.32.4 , WorkloadDatastore in SDDC-Datacenter
10/20/2022, 8:33:39 AM	Task: Relocate virtual machine

Conclusion

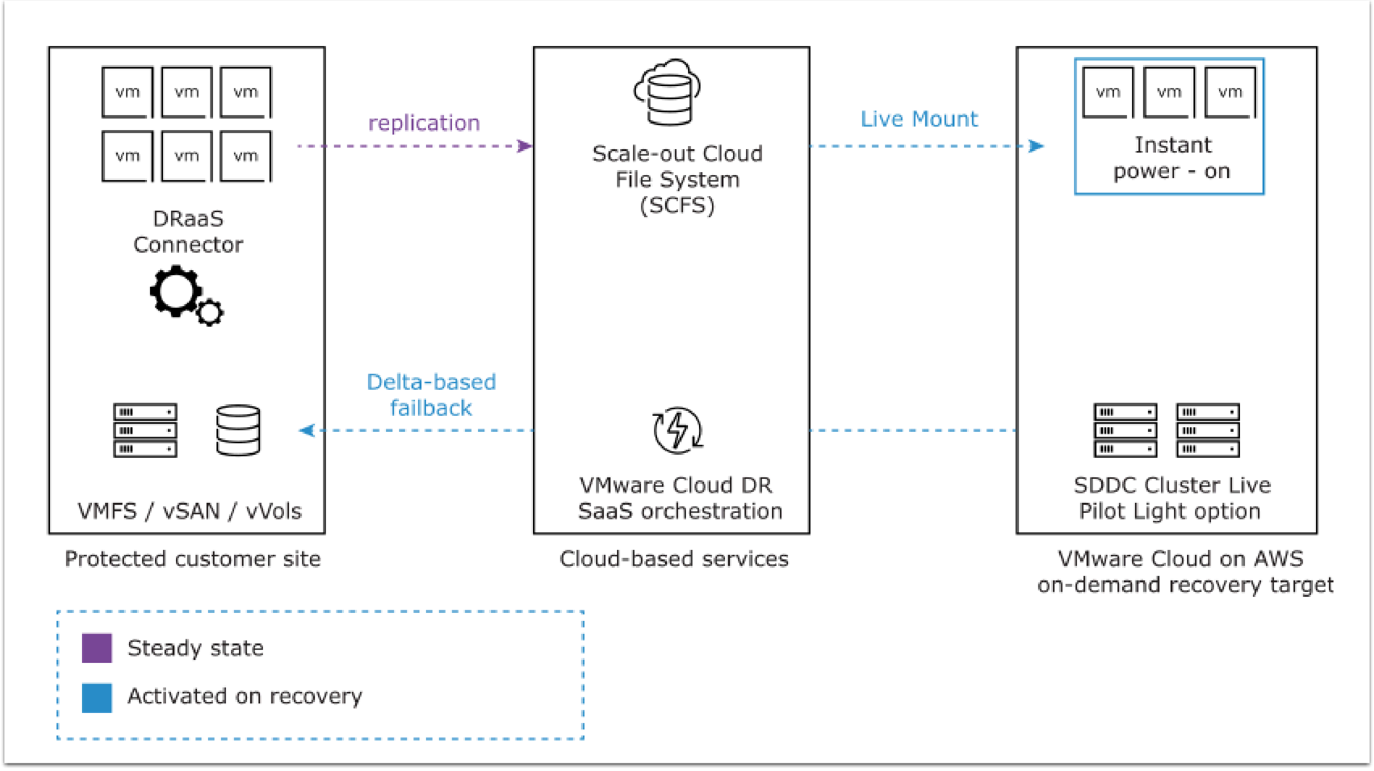
VMware Cloud Disaster Recovery is VMware's on-demand disaster recovery service that is delivered as an easy-to-use SaaS solution and offers cloud economics to help keep your disaster recovery costs under control.

In the latest August Release the following features and capabilities were added:

- **Bring your existing recovery SDDC:** Maximize your investment in VMware Cloud on AWS by using an existing SDDC created from the VMware Cloud console, for recovery with VMware Cloud Disaster Recovery. Clusters and hosts added to VMware Cloud DR from VMware Cloud console are automatically recognized by VMware Cloud Disaster Recovery.
- **User actions added to events list**: View a log of user actions such as log in, log out, configuration changes, and DR Plan executions in the Monitor view of the VMware Cloud Disaster Recovery UI. The user ID and the source IP address are shown for each item in the Events list, enhancing your ability to audit user actions.
- **Protect workloads running in VMware Cloud Foundation**: Expand your DR strategy to include protection of your virtual machines running in VMware Cloud Foundation (VCF) 4.2 and newer versions.
- **DR protection for up to 2500 VMs per AWS region per VMware Cloud organization**: Protect larger environments by replicating up to 2500 virtual machines to a single AWS region in a VMware Cloud organization. You might need to split 2500

VMs across multiple VMware Cloud Disaster Recovery cloud file systems for larger protected capacity scale. See VMware Configuration Maximum tool for operational scale limits of VMware Cloud Disaster Recovery.

- **Replication throughput in UI**: See the network throughput of the replication data traffic between the source site and the target VMware Cloud Disaster Recovery cloud file system. The throughput can be viewed in the Dashboard Topology map and on the Protected Sites page in the VMware Cloud Disaster Recovery UI.
- **AWS Europe (Milan) region:** You can now protect and recover your vSphere virtual machines in the AWS Europe (Milan) region.


vm
DRaaS Connector
VMFS / vSAN / vVols
Protected customer site
replication
Delta-based failback
Scale-out Cloud File System (SCFS)
VMware Cloud DR SaaS orchestration
Cloud-based services
Live Mount
Instant power - on
SDDC Cluster Live Pilot Light option
VMware Cloud on AWS on-demand recovery target
Steady state
Activated on recovery