

Lab 09 - DRaaS with VMware Cloud Disaster Recovery

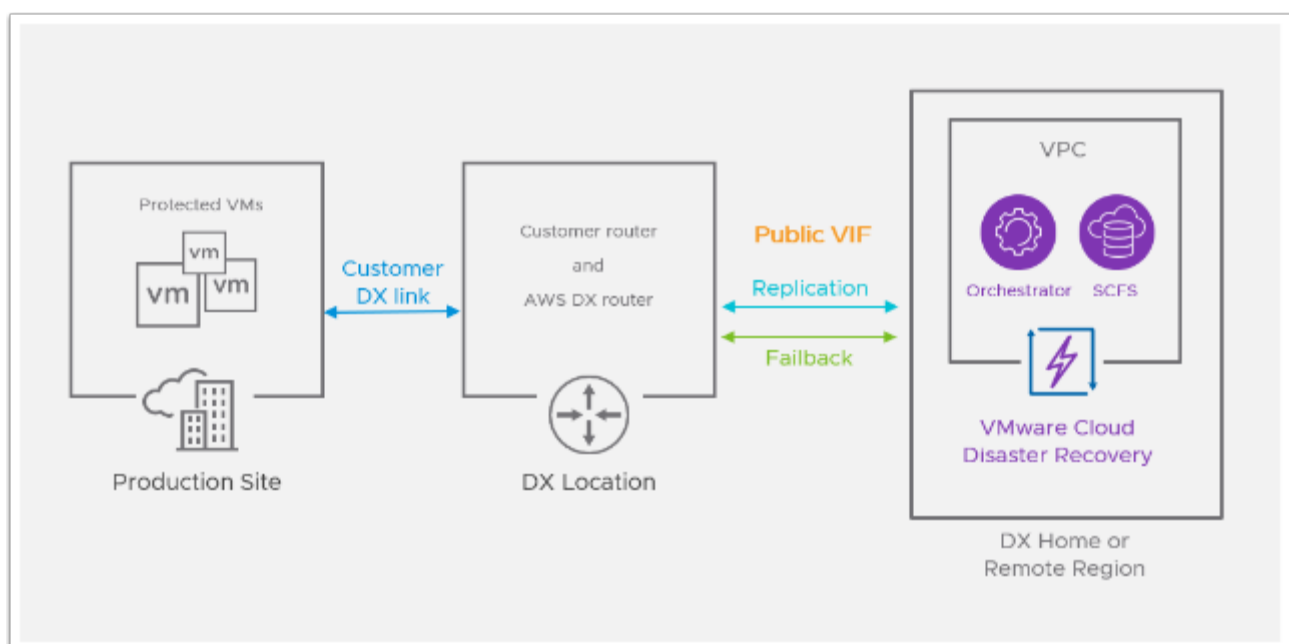
Introduction

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 the 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 - Connect an Existing SDDC to VCDR

VMware Cloud Disaster Recovery leverages the VMware Cloud on AWS Recovery Software Defined Data Center ("SDDC") as a disaster recovery site, which you can use if disaster strikes (or for testing) and you need to fail over your protected vCenter to the cloud. A new SDDC can be created from the VCDR Console for this purpose or you can Import an existing SDDC.

When you add an SDDC a cloud file system is attached to it, and both the SDDC and cloud file system must be in the same AWS availability zone (AZ). If no cloud file systems are available, then you can [deploy a cloud file system](#).



NOTE: Because we are using a shared environment, this step has already been completed for you. You are provided as a recorded video for this step instead.

To access the video for this task select the link below

<https://www.screencast.com/t/a7JqsOiw3>

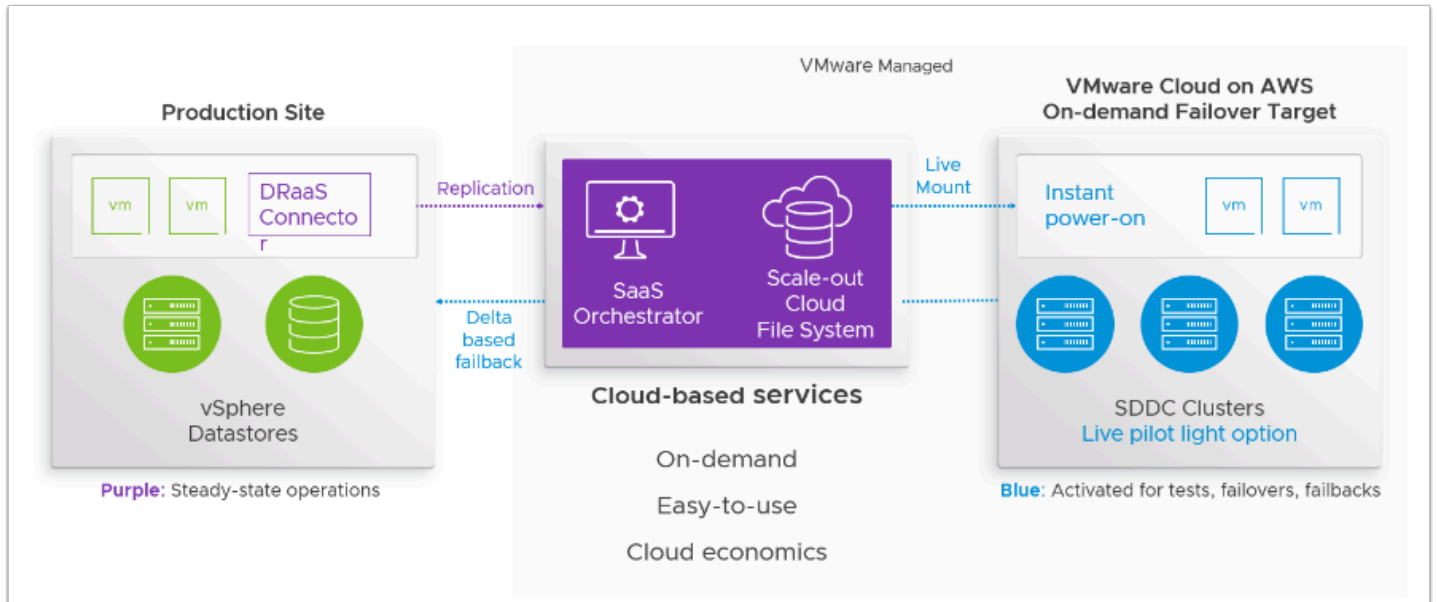
Task 2 - Add and configure a Protected Site

The VMware Cloud Disaster Recovery DRaaS Connector is a stateless software appliance that enables replicating VM snapshot deltas from "protected" vSphere sites (on-premises or VMware Cloud on AWS) to cloud backup sites, and back, driven by policies you set in protection groups.

You install the DRaaS Connector as a virtual machine into an on-premises vSphere environment or on a VMware Cloud on AWS SDDC (one connector per-vCenter), transforming your vSphere into a "protected site". A VMware Cloud Disaster Recovery protected site encompasses vCenters, protection groups, and DR plans.

Once you configure the protected vSphere site, you can create policies in protection groups that replicate snapshots to a cloud file system. You can then use available snapshots from

the cloud file system to recover protected VMs into your Recovery SDDC in VMware Cloud on AWS. Once the protected site is available again, you can initiate failback.



NOTE: Because we are using a shared environment, this step has already been completed for you. You are provided as a recorded video for this step instead.

To access the video for this task select the link below
<https://www.screencast.com/t/ssNcAU0fatmR>

Task 3 - Review the Environment

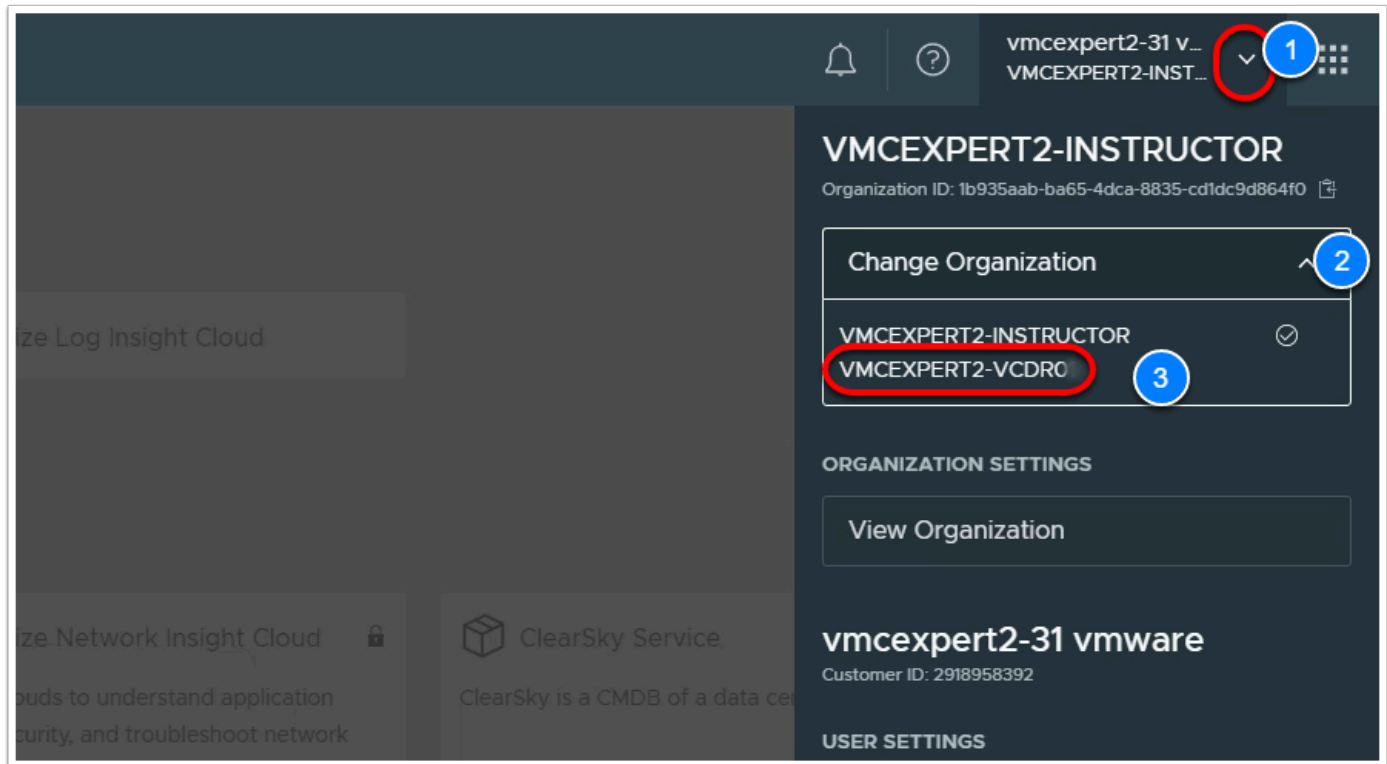
In these sub-tasks we will review the Cloud Services console, the VMC on AWS SDDC environment and the On-Prem.

Task 3.1 - Review VCDR settings

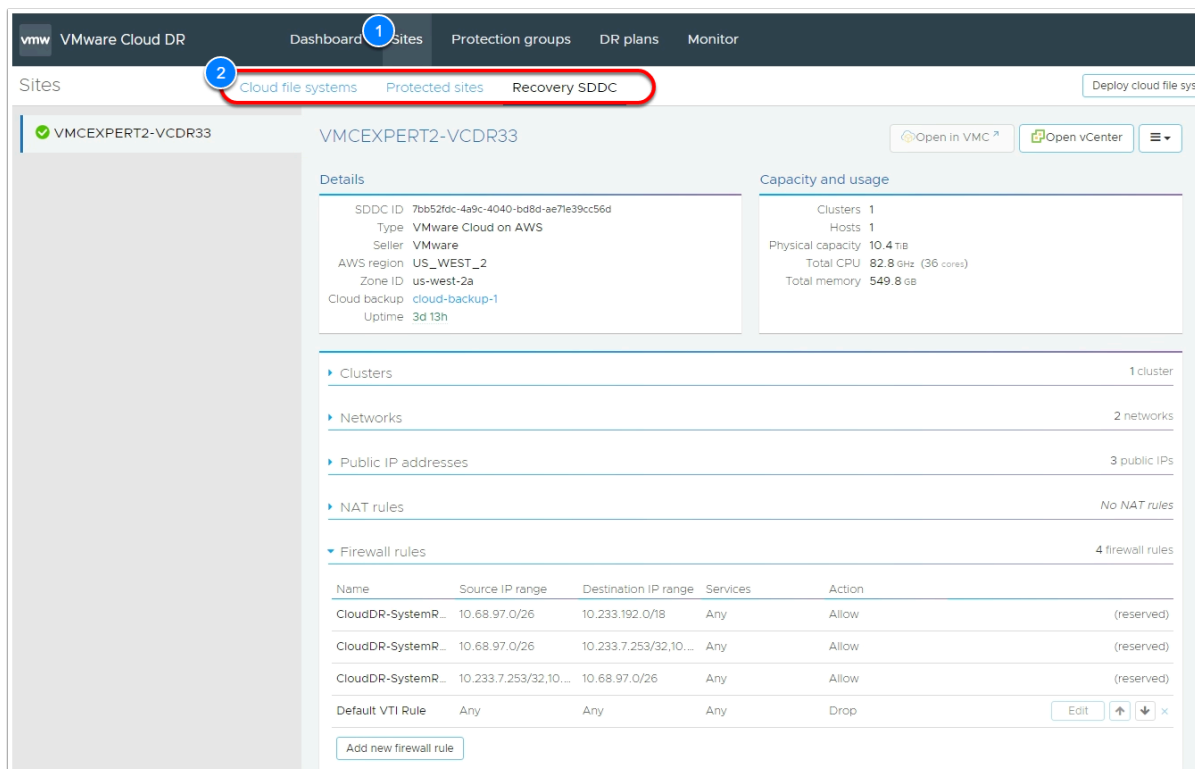
1. From the Horizon VDI Desktop, log into the VMC on AWS Cloud Console.
Go to <https://vmc.vmware.com>
2. Login in as
 - **vmcexpert#-XX@vmware-hol.com**

- **VMware1!**

3. In the upper right-hand corner of the Cloud Console, Click the **Drop-down** next to your account
4. Click the **Drop-down** next to Change organization and select **Your VCDR Org** (VMCEXP2-VCDR##)



4. Under My Services Click the **VMware Cloud DR** Tile, to review the VCDR settings
5. In the Main Menu Click **Sites**
6. Click **Cloud File System** to Review the Cloud File System that will be used for storing the Protected Virtual Machine Images
7. Click **Protected Sites** to review your Protected Datacenter. You will notice two connector appliances have been deployed to the Protected DC and are in a healthy state. You'll also notice that the On-Premises vCenter has been added.
8. Click **Recovery SDDC**, to review the recovery SDDC and its settings
9. Take note of the following items, we will confirm them when we access the SDDC in the next task:
 - SDDC ID
 - Number of Cluster & Hosts
 - Networks
 - Firewall Rules



Task 3.2 - Review Recovery SDDC Settings

1. From the Horizon VDI Desktop, open a new Browser tab.
Click the **VMware Cloud SDDC** Chrome Bookmark
2. If prompted, login in as
 - **vmcexpert#-XX@vmware-hol.com**
 - **VMware1!**
3. In the upper right-hand corner of the Cloud Console, Click the **Drop-down** next to your account
4. Click the **Drop-down** next to Change organization and select **Your VCDR Org** (VMCEXP2-VCDR##)
5. Click **View Details** on the VCDR SDDC Tile
6. On the **Summary** tab confirm the number of **Clusters, Hosts** you captured in the previous task
7. On the **Support** Tab confirm the **SDDC ID** you captured in the previous task
8. Click the **Networking & Security** tab
9. Click **Segments** to confirm the Segments recorded form the previous task
10. Click **Gateway Firewall**. Review both the Compute Gateway and Management Gateway Firewall rules

i You'll notice, the Compute Gateway has rules allowing the Cloud Proxy Appliance access to the Scale-Out File System and Vice-Versa

On the Management Gateway You'll notice the VCDR Cloud resources are granted access to vCenter

Summary **1** Networking & Security Add Ons Maintenance Troubleshooting Settings Support

Overview

Network

Segments

VPN

NAT

Tier-1 Gateways

Transit Connect

Security

Gateway Firewall **2**

Distributed Firewall

Distributed IDS/IPS

Inventory

Groups

Services

Virtual Machines

Context Profiles

Tools

IPFIX

Port Mirroring

System

Identity Firewall AD

DNS

Gateway Firewall

3 Management Gateway Compute Gateway

REVERT PUBLISH

+ ADD RULE CLONE UNDO DELETE Success Filter by Name, Path and more

	<input type="checkbox"/>	Name	ID	Sources	Destinations	Services	Action	
	<input type="checkbox"/>	ESXi Outbound Rule	1013	ESXi	Any	Any	Allow	<input checked="" type="checkbox"/>
	<input type="checkbox"/>	vCenter Outbound Rule	1014	vCenter	Any	Any	Allow	<input checked="" type="checkbox"/>
	<input type="checkbox"/>	CloudDR-SystemRule	1015	CloudDR-Proxy	vCenter	HTTPS SSO ICMP ALL	Allow	<input checked="" type="checkbox"/>
	<input type="checkbox"/>	CloudDR-SystemRule	1016	CloudDR-Proxy	vCenter	HTTPS SSO ICMP ALL	Allow	<input checked="" type="checkbox"/>
	<input type="checkbox"/>	Default Deny All		Any	Any	Any	Drop	<input type="checkbox"/>

REFRESH 5 Rules

i While in the Gateway firewall, let's create appropriate firewall rules to allow access to the recovery SDDC vCenter. We will perform these steps so as to review the vCenter Inventory.

11. Click the **Networking & Security** tab
12. Click **Groups**
13. Click **Management Groups**
14. Click **View Members** next to **On-Prem Mgmt-Net** to confirm that the Public IP of your VDI (On-Premises Environment) is included
15. Click IP Addresses
16. Click **CLOSE**

View Members | On-Prem Mgmt-Net

Effective Members

Group Definition

REFRESH

Virtual Machines (0)

IP Addresses (3)

Segments (0)

Segment Ports (0)

VIFs (0)

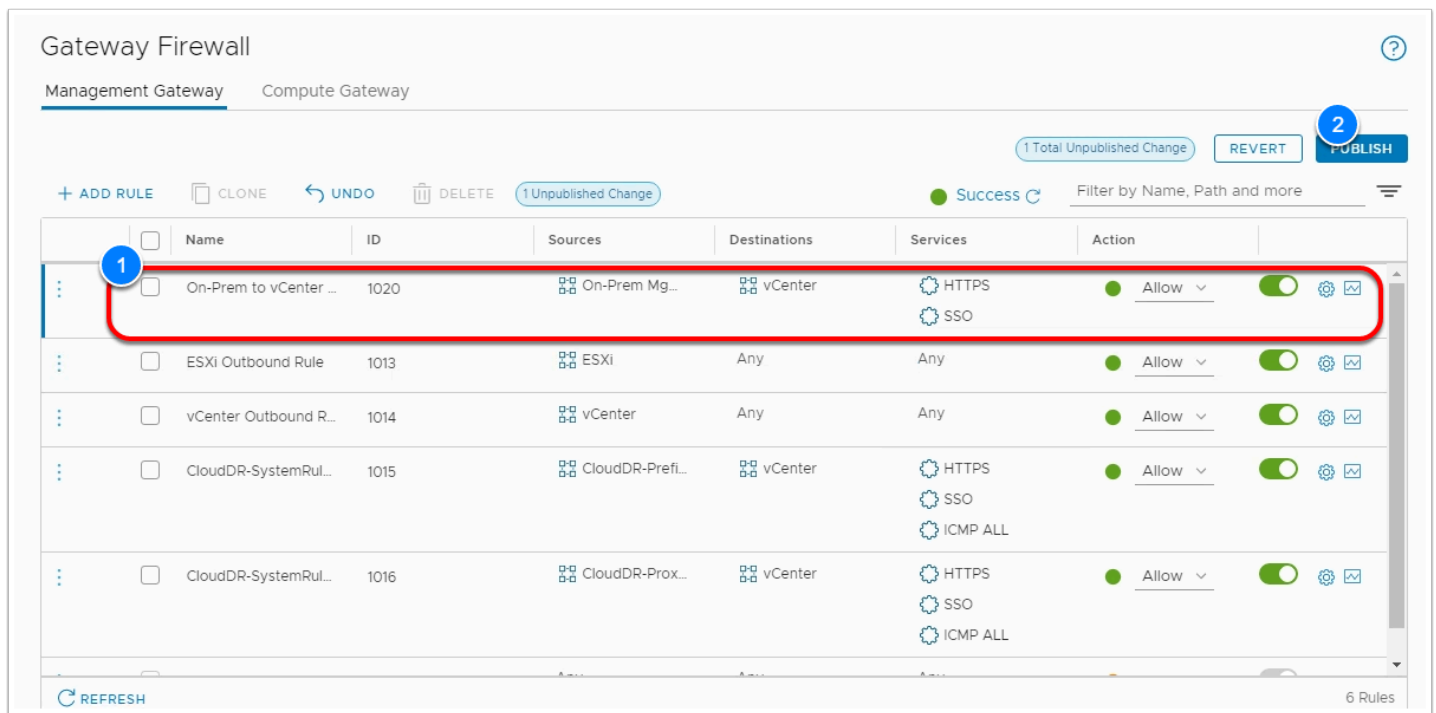
Name
192.168.110.0/24
66.216.10.11-66.216.10.20
66.216.10.41-66.216.10.42

1 - 3 of 3 IP Addresses

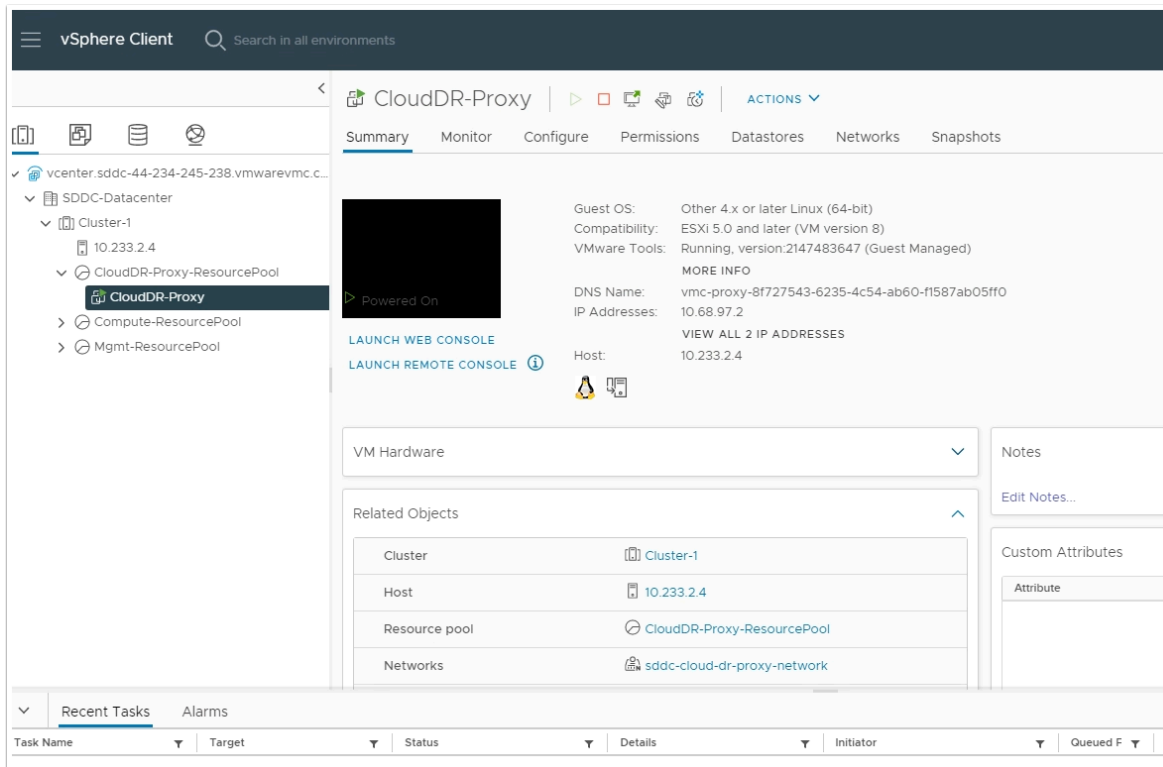
CLOSE

NOTE: If your public IP (66.216.10.x) is not in the range(s). Please notify your instructor.

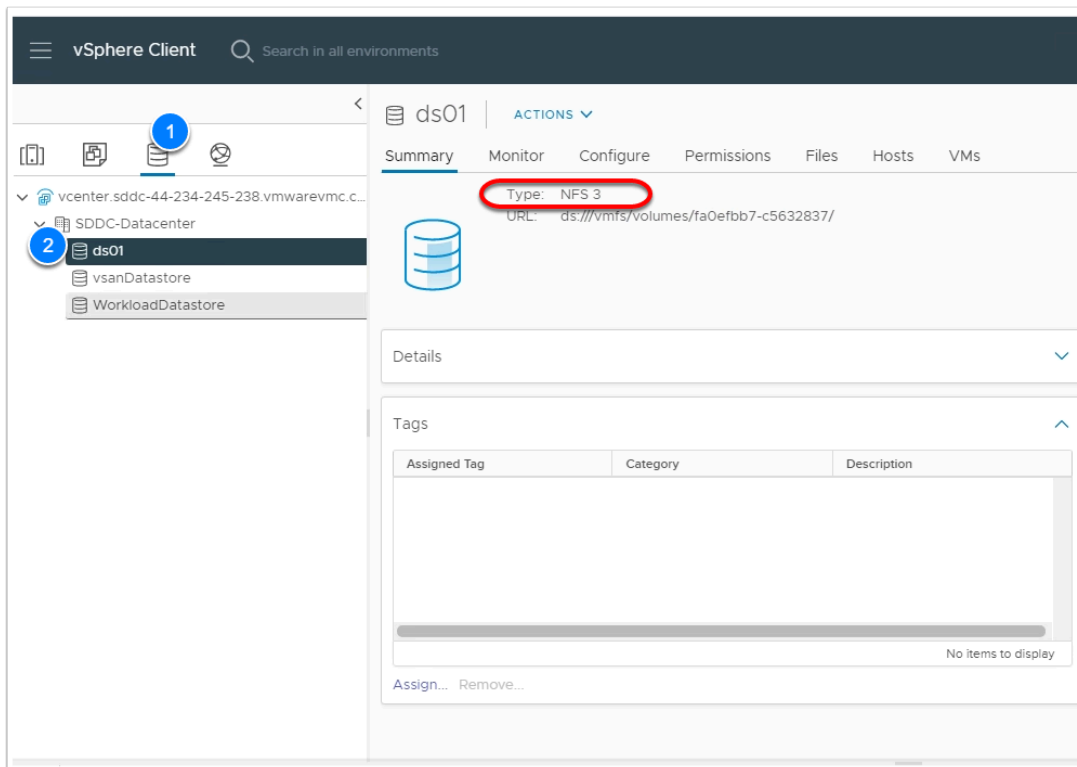
17. Click **Gateway Firewall**
18. Click **Management Gateway**
19. Review the **On-Prem to vCenter Inbound** rule and confirm the following
 - Source: **On-Prem Mgmt-Net** (Mouse over the source field and click the pencil icon)
 - Destination: **vCenter**
 - Services: **HTTPS, SSO**



20. Click the **Settings** Tab
21. Expand the **Default vCenter User** and **vSphere Client (HTML5)** sections
22. Take note of and copy the values for:
 - Username
 - Password
 - vSphere Client URL
23. In a new browser tab from within the VDI Desktop paste in the vCenter URL and login using the information you saved from the previous step



24. Expand the vCenter Inventory and you'll notice a VM Named CloudDR-Proxy. Take note of the IP address of the Cloud Proxy. You'll notice its with the Subnet defined in the Gateway firewall rule for the **CloudDR-ProxyNetworkPrefixes** Group
25. Switch to the Datastores View
26. You'll notice an NFS Datastore names **ds01**
VCDR Mounts recovered VMs from this datastore.

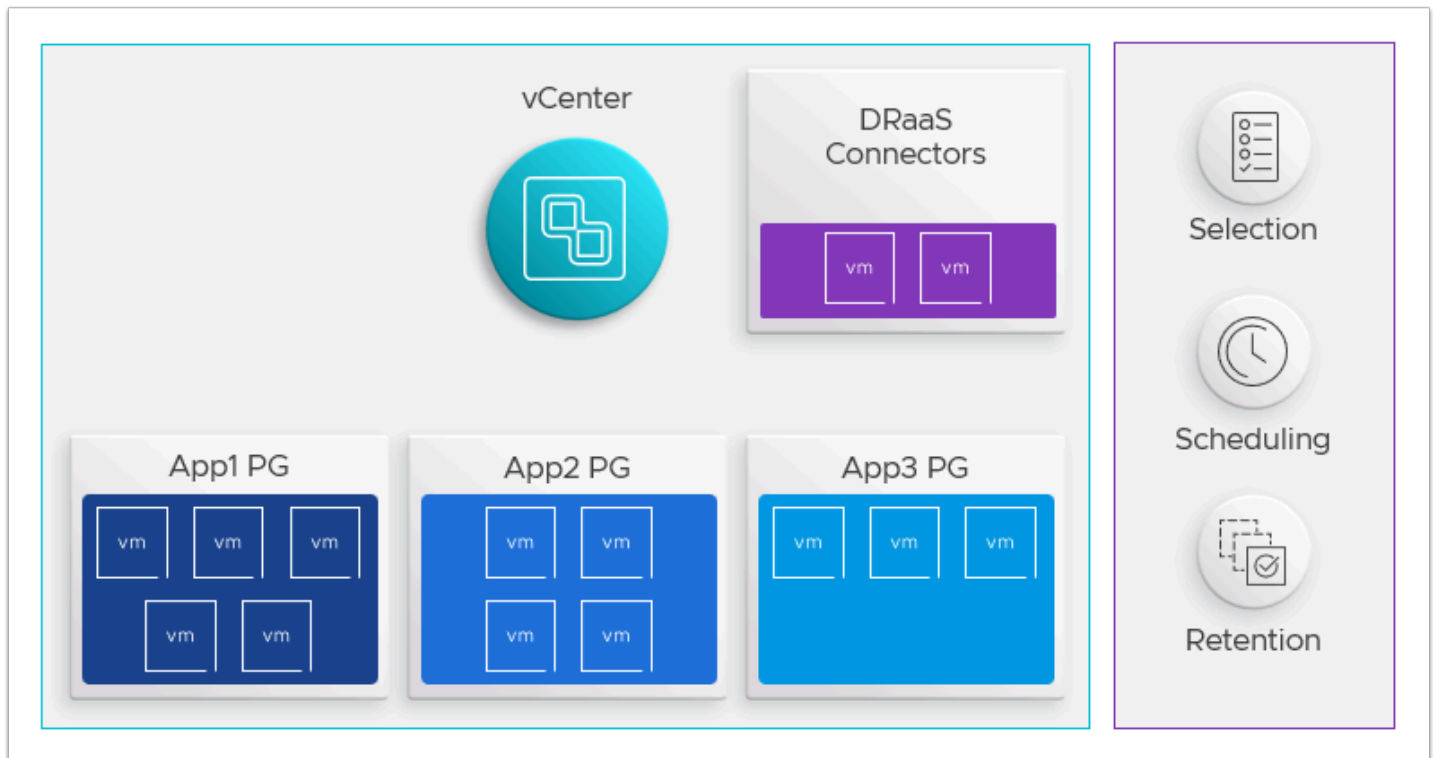


Task 4 - Create a Protection Group

Protection groups allows you to create regularly scheduled snapshots of your VMs which replicate to a VMware Cloud Disaster Recovery cloud file system.

A protection group consists of:

- Site selection (on-premises or SDDC)
- Members (VMs)
- Policies for snapshots (schedule, retention)
- Cloud file system (SCFS)

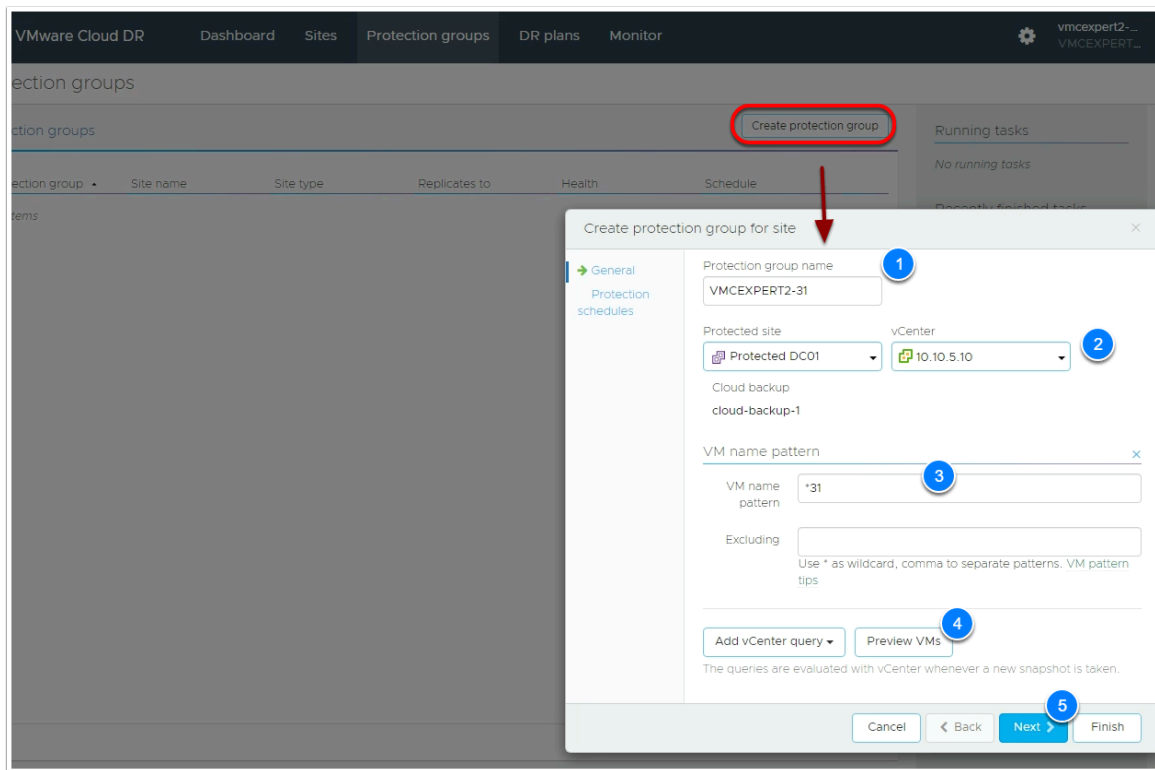


Protection groups can then be added to a DR plan, which ensures that if a failure occurs, you can orchestrate recovery to a new site using selected snapshots of your VMs to re-instantiate the source vCenter site.

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.

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 [Task 3.1, steps 1-4](#)
2. In the VMware Cloud Disaster Recovery UI, click the **Protection groups** tab
3. Click **Create protection group**, in the upper right side
4. Configure the protection group as follows:
 - Name: **VMCEXPERT#-XX_PG** (Where # is your Environment Id and XX is your student number)
 - Protected Site: **<Leave default>**
 - vCenter: **<Leave default>**
 - Group Membership
 - VM name pattern
 - VM name pattern: ***XX** (where XX is your student number. i.e. ***31**)
5. Click **Preview VMs** to identify your Virtual Machine
6. Click **OK**

7. Click **Next**



8. Set the following values for the Protection schedule:

- Take Snapshot: **Daily**
- At: **<The next hour from now>** If it's currently 11:25 AM, choose Noon.
- Keep snapshots for: **<Leave default>**
- Click **New Schedule** if you'd like to add an additional schedule

9. Click **Finish**

💡 Once the protection group appears in the Protection groups list, you can add it to a DR Plan for testing and execution.

Instead of waiting to the schedule we defined we will take a manual snapshot

10. Click the **hamburger menu (3 dashes)** to the right of your protection group
11. Click **Take Snapshot**
12. For retention, select **For 1 Day**
13. Click **Take Snapshot**

Protection group	Site name	Site type	Replicates to	Health	Schedule
VMCEXP2-31	Protected DC01	On-prem site	cloud-backup-1	Unknown	Stopped

14. Monitor the Snapshot in the Running Tasks pane to the right of the UI.
This could take as much as 15 mins depending on the number of concurrent snapshots happening

15. Once the Snapshot process has completed, double-click <**your protection group**> to view the snapshot

VMCEXP2-31

Group details

Snapshots 1
Schedule **Active**
Health OK
Site Protected DC01

Membership

VM name pattern *31

Schedule

Daily: snapshot every day at 12:00 AM and 10:00 PM. Retain for 1 week
Daily-2: snapshot every day at 4:00 AM, 11:00 AM, and 3:00 PM. Retain for 1 week

Snapshots

Delete

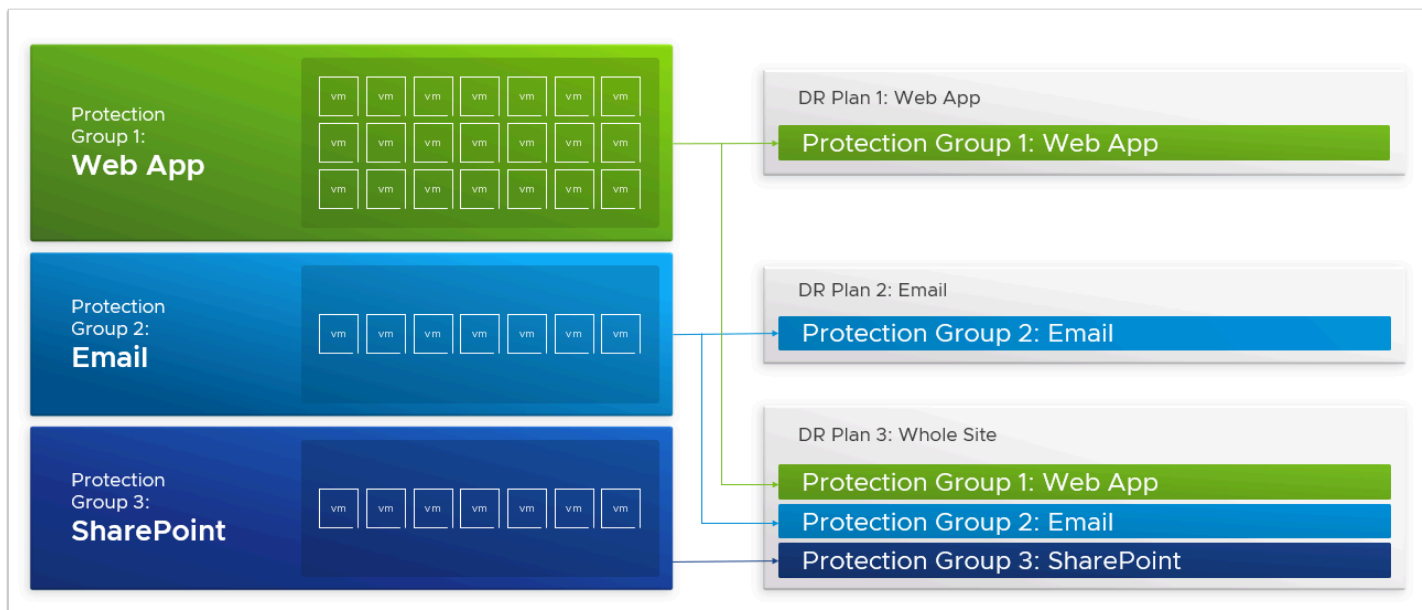
Name	Taken timestamp	Includes	Total size	Expiration
<input type="radio"/> VMCEXP2-31 - Manual - 2021-08-27T17:44:22 UTC	Aug-27-2021 01:46 pm	1 VM	4.1 GiB	Aug-28-2021 01:46 pm

Task 5 - 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.

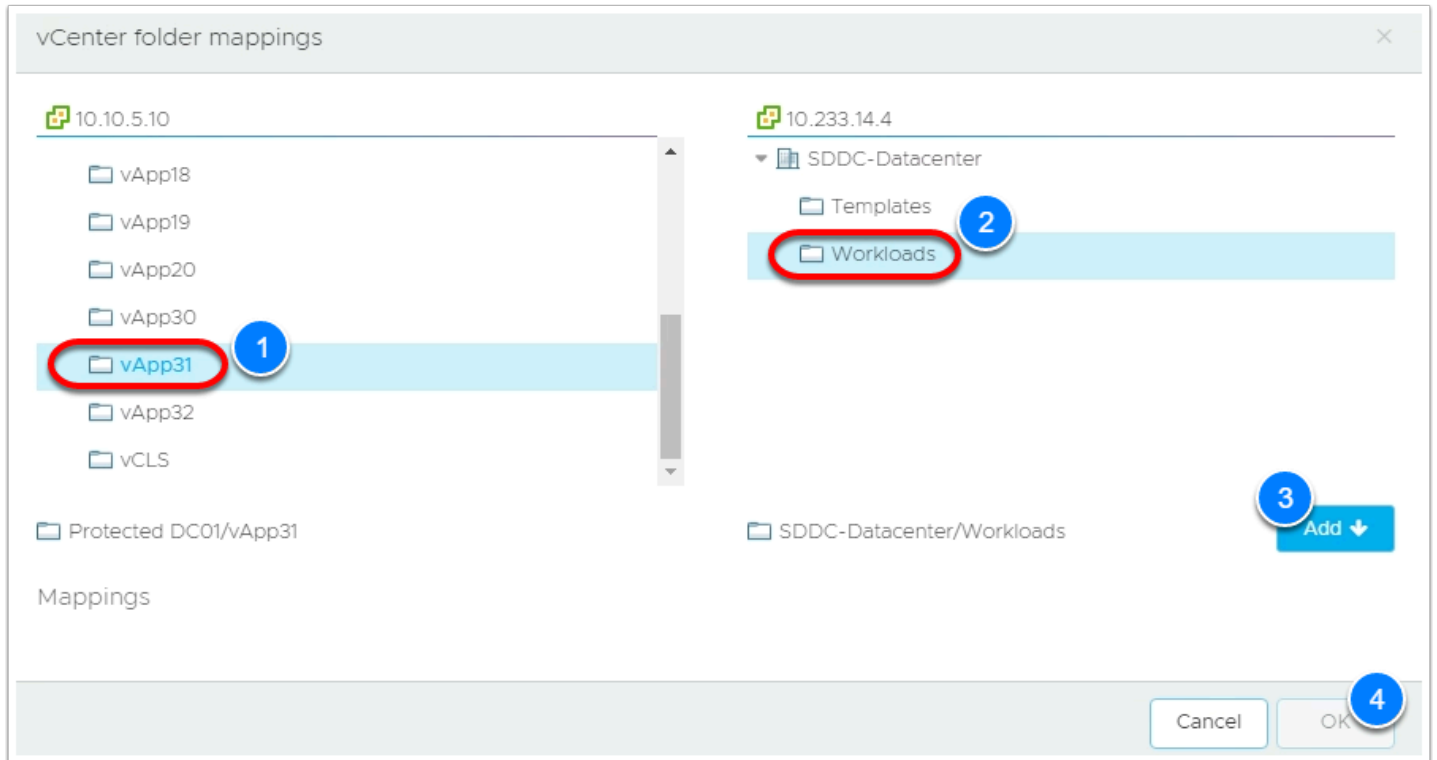


i VMware Cloud Disaster Recovery performs a set of continuous compliance checks for all active plans and resources, and it reports on environmental changes, such as vSphere misconfigurations or network outages. Compliance Checks detect any compromised plan integrity at the time of misconfiguration or equipment failure. Compliance checks give the user an opportunity to address issues and restore the plan's integrity before 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.

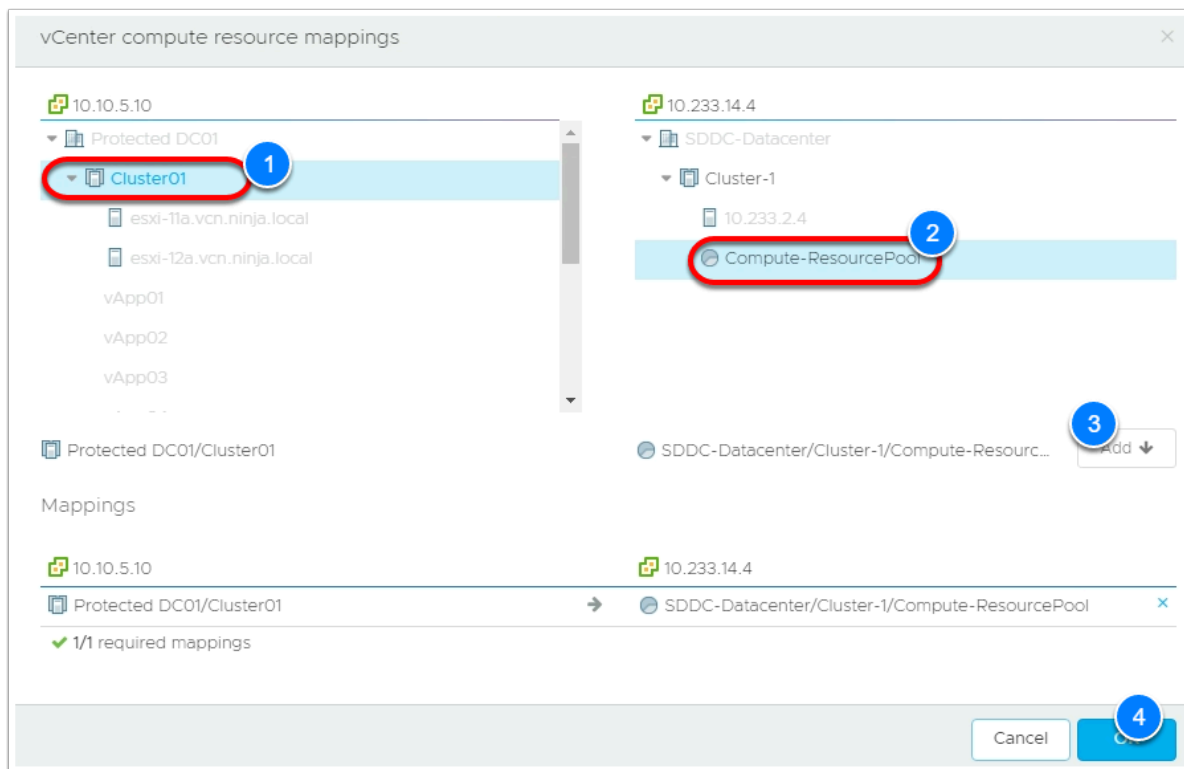
VMware Cloud Disaster Recovery can maintain multiple plans of different types, and multiple plans can be in various stages of execution at any given time, even concurrently.

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 [Task 3.1, steps 1-4](#)
2. In the VMware Cloud Disaster Recovery UI, click the **DR Plans** tab
3. Click **Create plan**
4. In the Create Plan dialog, configure the Plan as follows:
 - Plan Name: **VMCEXPRT#-XX_DR_Plan** (Where # is your Environment Id and XX is your student number)
 - Description: **<Leave default>**
 - Recovery Site: **Existing recovery SDDC**
 - Protected Site: **<Leave default>**
 - vCenter: **<Leave default>**
 - Groups: **<Choose your protection group>** i.e. **VMCEXPRT2-31_PG**
 - vCenter Failover mapping: **<Leave default>**

- vCenter Folder Mapping: **Select Map Folder** 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**

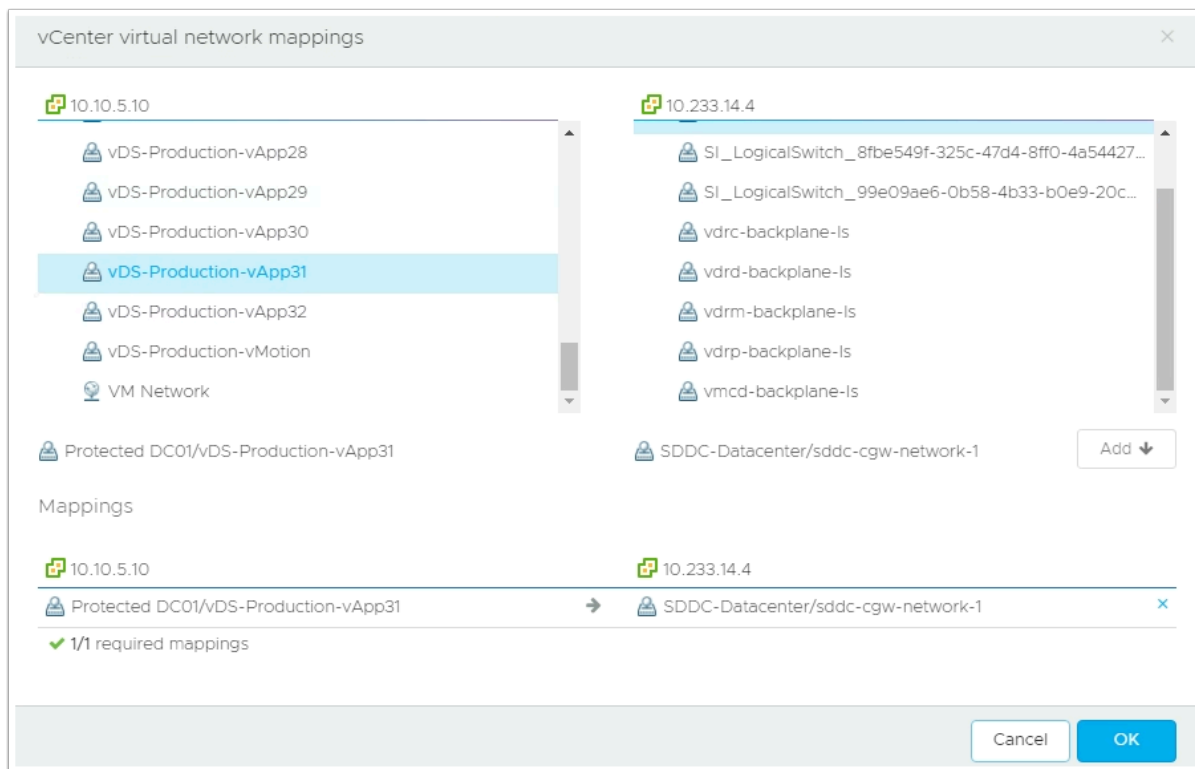


5. Click Next, and continue configuring your Plan
 - Compute Resources Failover mapping Click **Map Compute Resources** button
 - In the Source (On-Premises) vCenter Select **Cluster01**
 - In the SDDC vCenter Select **Compute-ResourcePool**
 - Click **Add**
 - Click **Ok**



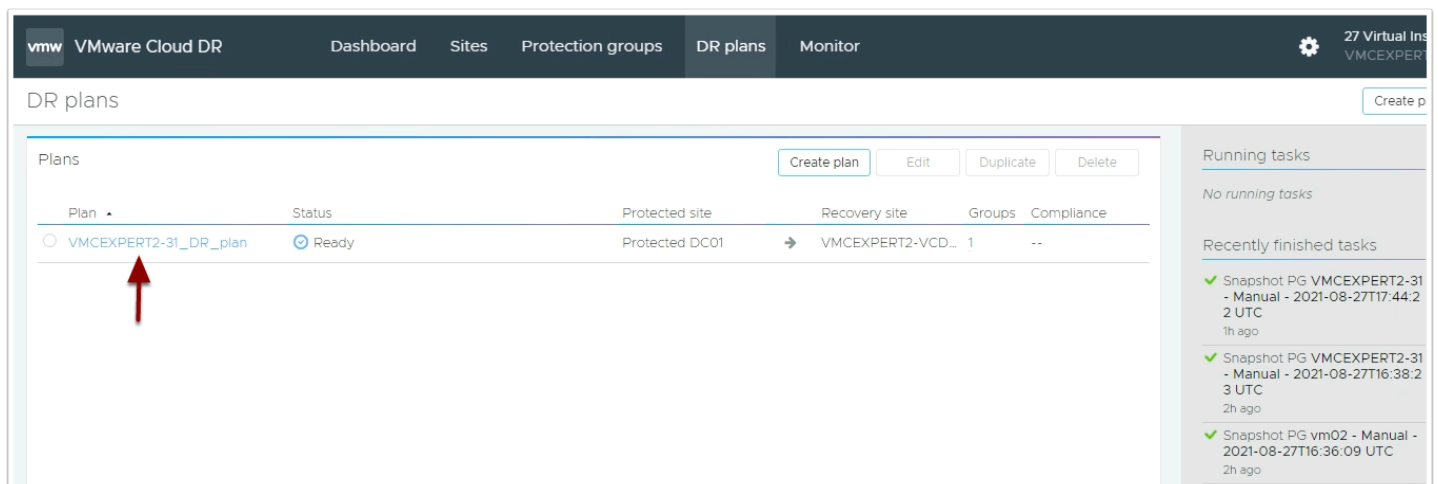
6. Click Next, and continue configuring your Plan

- 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**

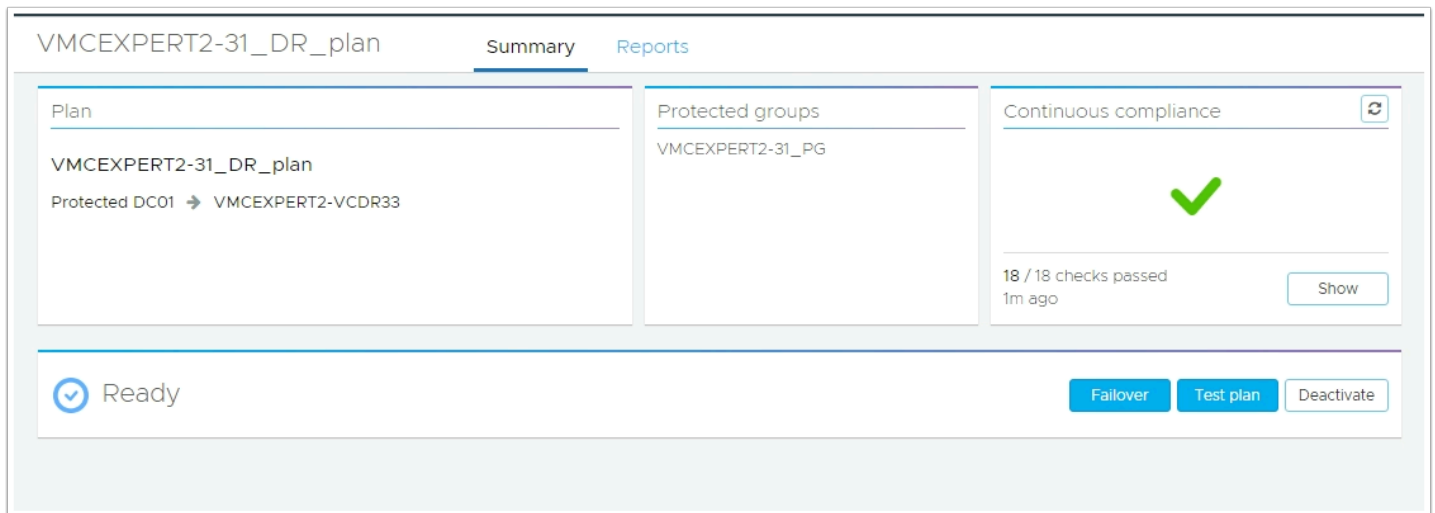


7. Click **Next**, and continue configuring your Plan

- 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**
- On the Alerts Page, click **Finish**



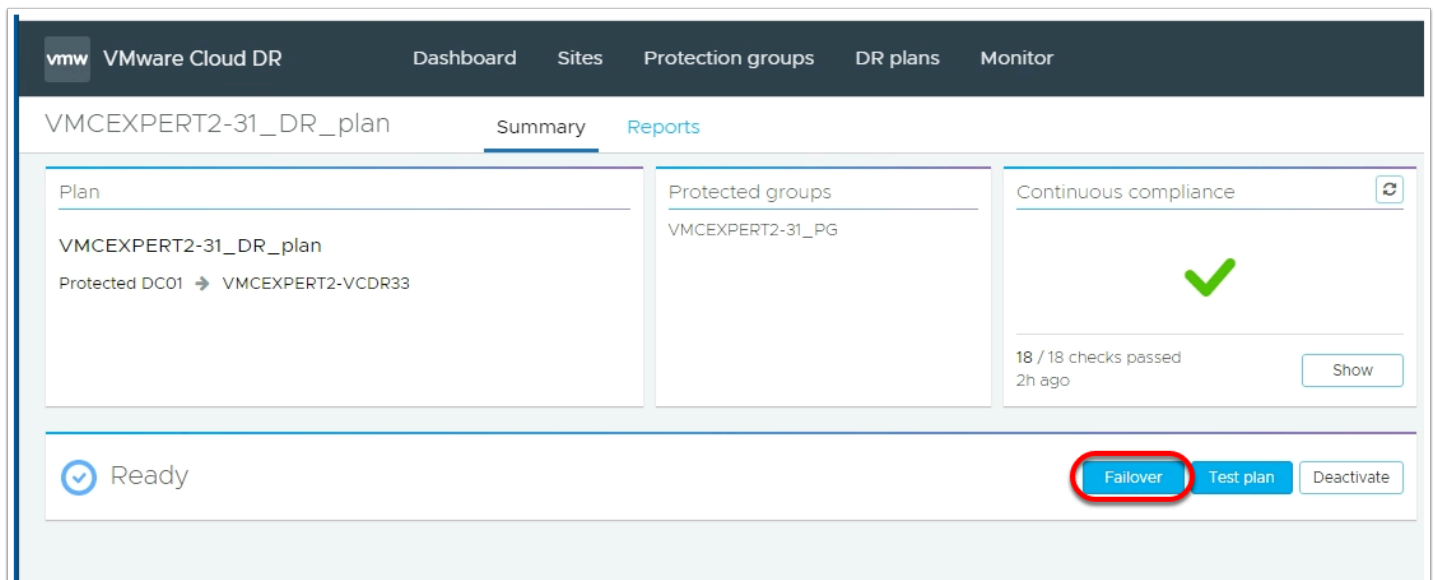
8. Once created, click your DR Plan to review and manage it.



Task 6 - Execute a Failover

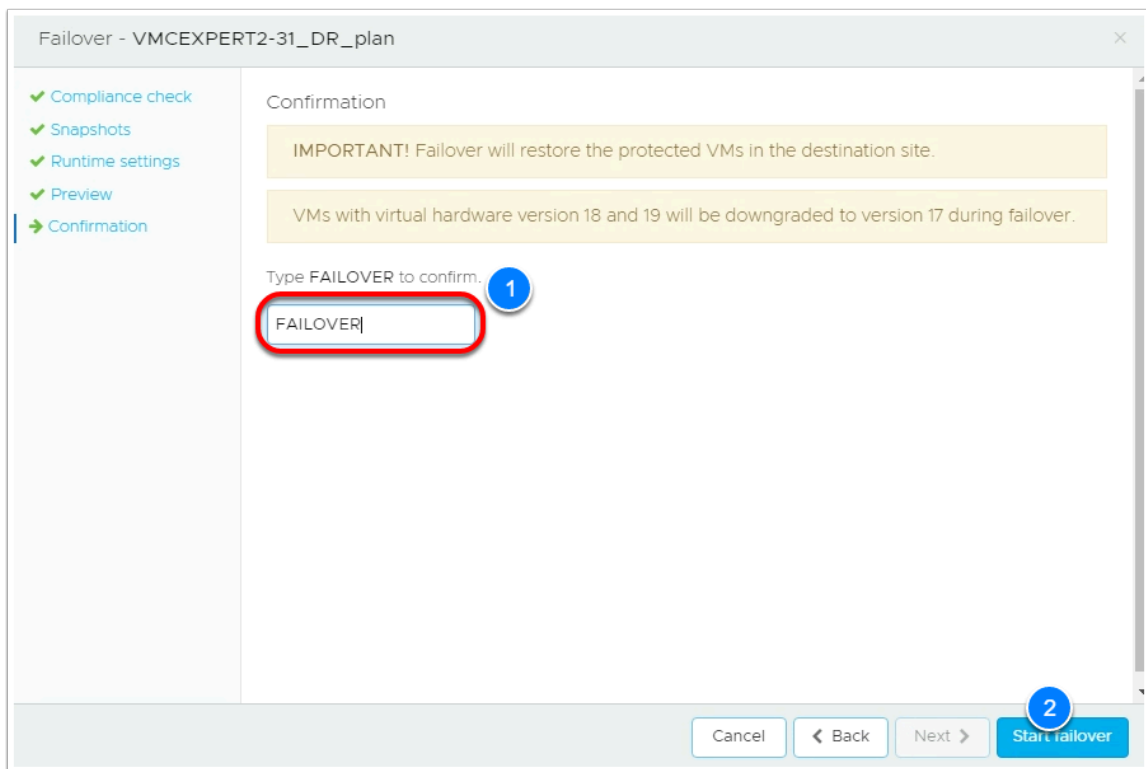
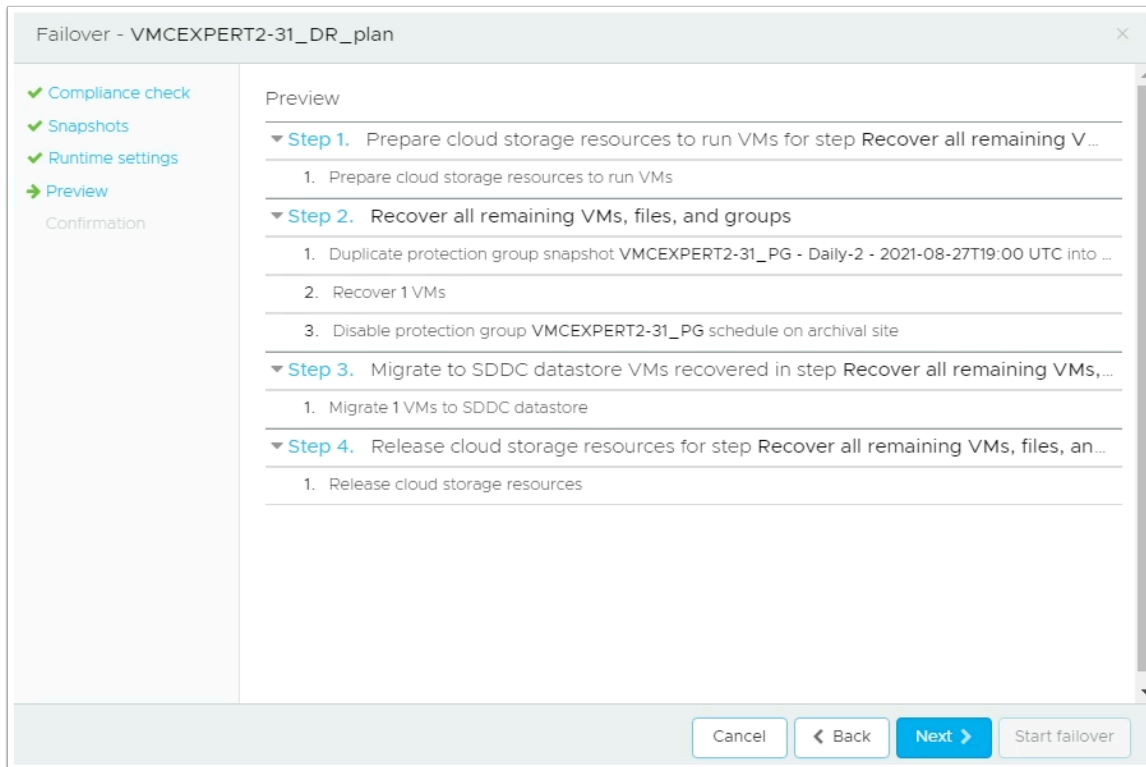
When you run a DR Plan as a failover, a running instance of the plan recovery steps launches and the plan continues to completion, or until a pause for user input, or upon encountering an error (if configured).

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



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 DC01/datastore/NFS SharedDS01**
- Type **COMMIT FAILOVER**
- Click **Commit**

VMCEXP2-31_DR_plan Summary Reports

Plan


VMCEXP2-31_DR_plan

Protected DC01 → VMCEXP2-VCDR33

Protected groups

VMCEXP2-31_PG

Continuous compliance



18 / 18 checks passed
2h ago

Show

✓ Failed over with no errors

Commit Rollback

Success

Step	Timestamp	Duration	Progress
▶ ✓ Step 1. Prepare cloud storage resources to run VMs for step Recover all remaining VMs, files, and gro...	Aug-27 04:47 pm	2m	Finished
▶ ✓ Step 2. Recover all remaining VMs, files, and groups	Aug-27 04:49 pm	< 1m	Finished
▶ ✓ Step 3. Migrate to SDDC datastore VMs recovered in step Recover all remaining VMs, files, and groups	Aug-27 04:50 pm	< 1m	Finished
▶ ✓ Step 4. Release cloud storage resources for step Recover all remaining VMs, files, and groups	Aug-27 04:50 pm	< 1m	Finished

1. Back plan
2. Create a fallback plan

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

Fallback plan name

[fallback] VMCEXP2-31_I

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 fallback site, or if the VM was created in the recovery SDDC, then it will be placed in the datastore specified below.

Default datastore

Protected DC01/datastore/NFS Share...

Confirmation

3. Press COMMIT FAILOVER to confirm.

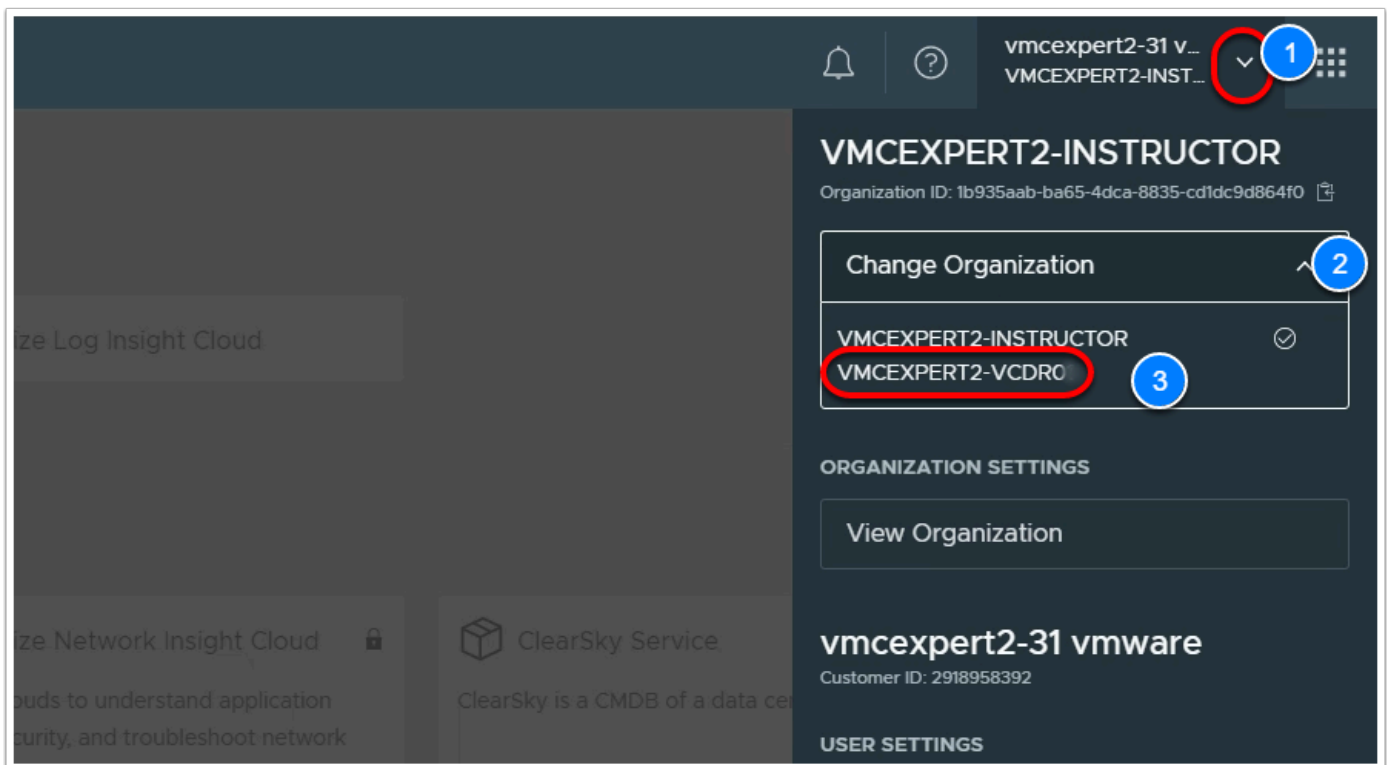
COMMIT FAILOVER

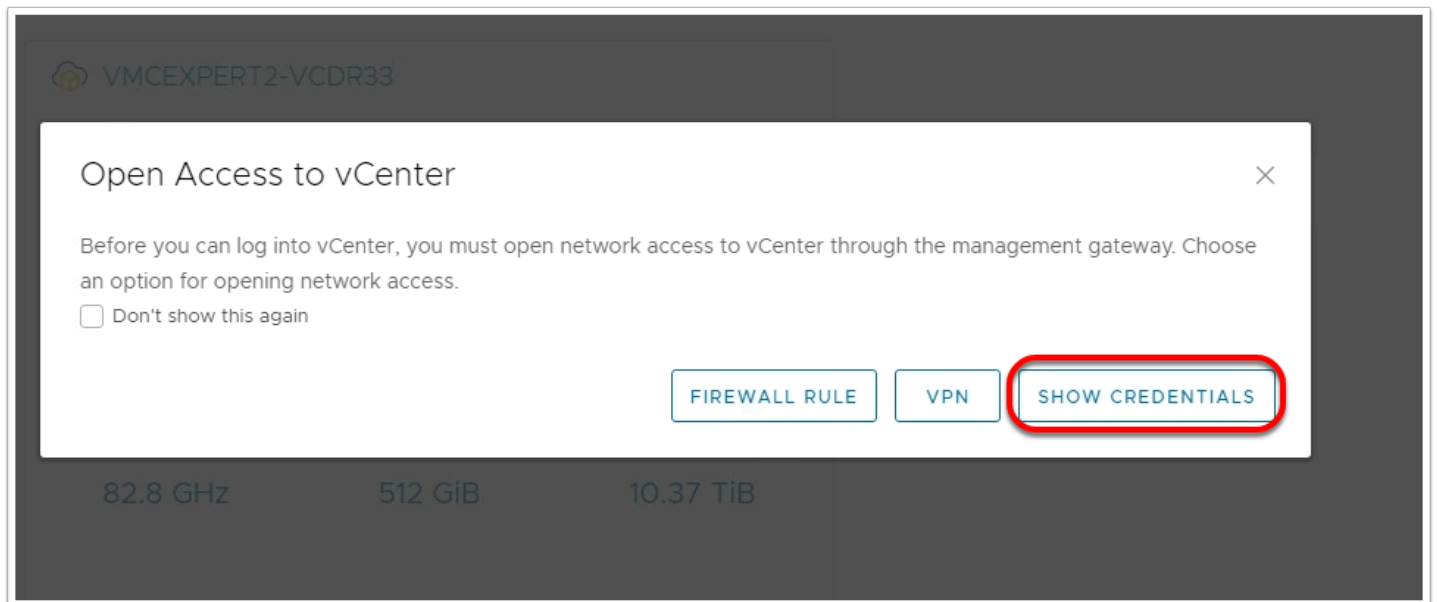
4. Cancel Commit

8. On the Summary page of the DR plan, click the **Create PDF report** button. To generate and download a report of the failover execution. This report can be used for audit and compliance purposes

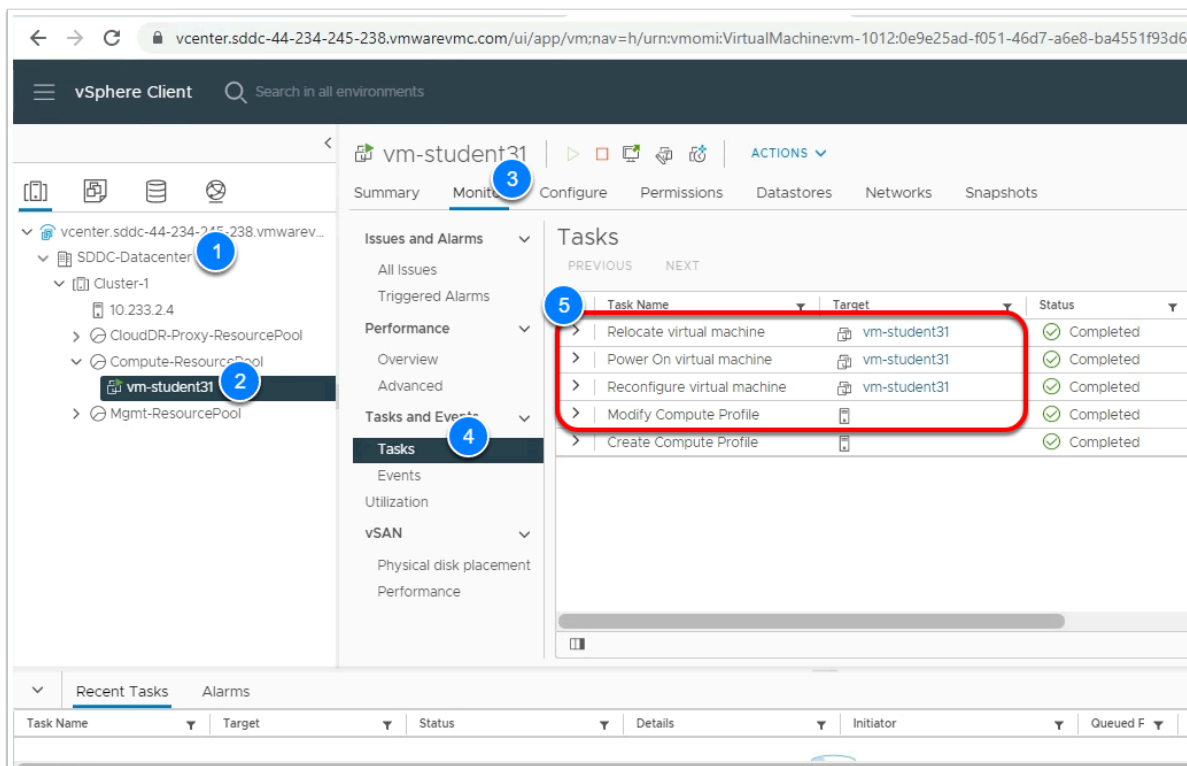
Task 7 - Review the Recovered Virtual Machine

1. In a new Browser tab, click the **VMware Cloud SDDC** Chrome Bookmark
2. If prompted, login in as
 - **vmcexpert#-XX@vmware-hol.com**
 - **VMware1!**
3. In the upper right-hand corner of the Cloud Console, Click the **Drop-down** next to your account
4. Click the **Drop-down** next to Change organization and select **Your VCDR Org** (VMCEXP2-VCDR##)
5. Click **Open vCenter** on the VCDR SDDC Tile
6. Click **Show Credentials**
7. Copy the vCenter Password and Click **Open vCenter**





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



Conclusion

- i** 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.

