

Lab 08 - DRaaS with VMware Cloud Disaster Recovery (Part 1)

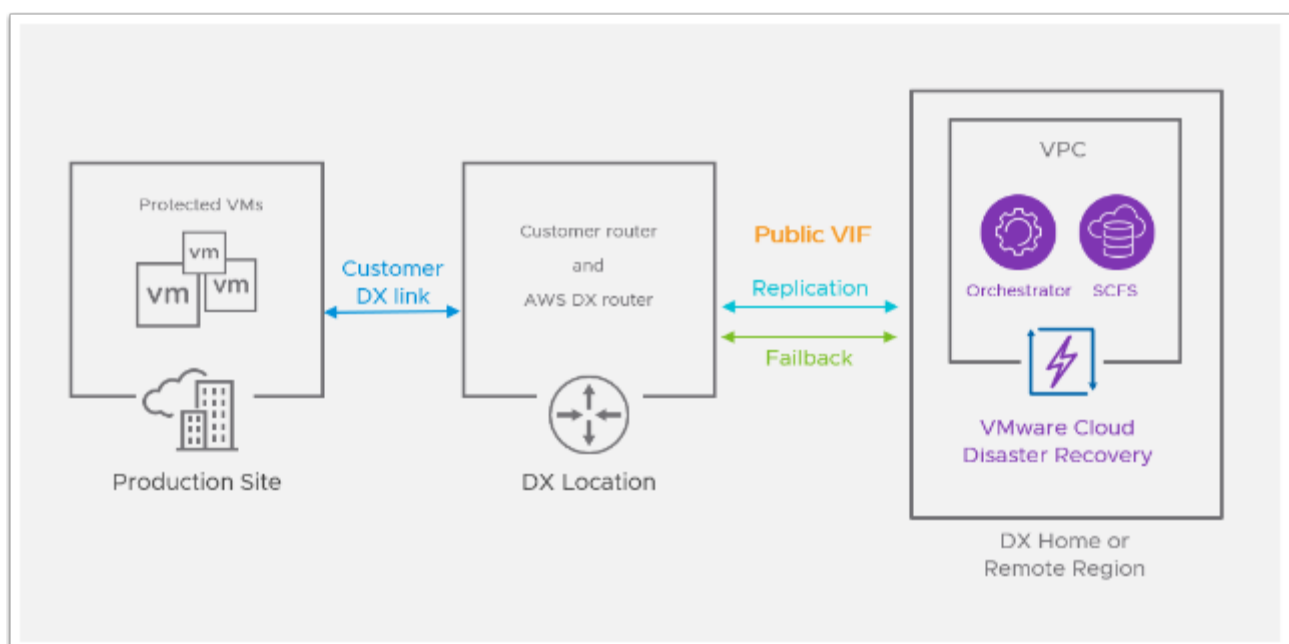
Introduction

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 - 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. It is provided as a recorded interactive simulation to you instead.

To access the i-sim for this task select the link below

[Connect an existing SDDC to VCDR](#)

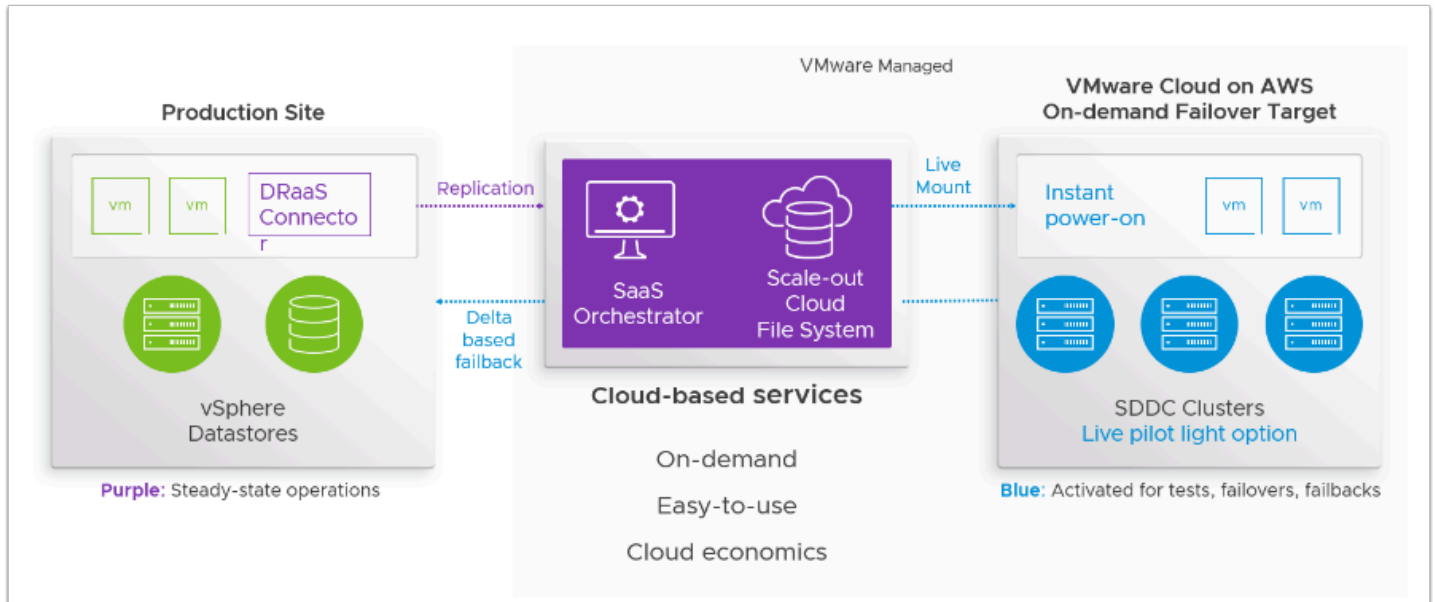
Task 2 - Add and configure a Protected Site

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. It is provided as a recorded interactive simulation to you instead.

To access the i-sim for this task select the link below
[Add and Configure a Protected Site](#)

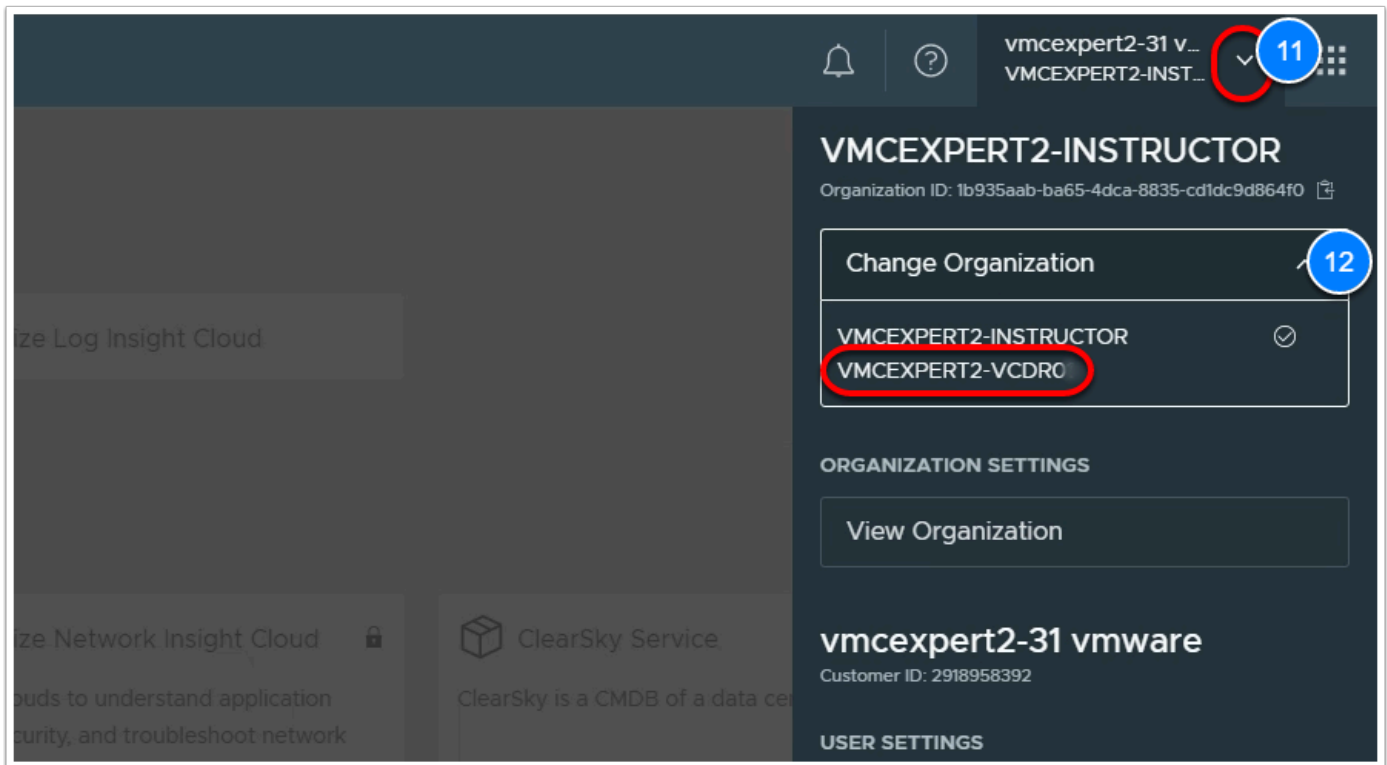
Task 3 - Review the Environment

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 your Laptop/desktop open a new Google Chrome Incognito window
2. Type <https://vdi.27virtual.net> in the browser address bar
3. Click the checkbox "**Check here to skip this screen and always use HTML Access**"
4. Click **VMware Horizon HTML Access**

5. When prompted log in as: **(Get the login details from the Student Assignment Spreadsheet)**
6. Username: **VMCExpert#-XX** (where # is the Environment ID and XX is your student number)
7. Password: **{Password-Provided-by-Instructor}**
8. Select the available Desktop pool
9. From the Horizon VDI Desktop, log into the VMC on AWS Cloud Console.
Go to <https://vmc.vmware.com>
10. Login in as
 - **vmcexpert{1|2|3}-##@27virtual.net** (where ## is your student number)
i.e **vmcexpert1-02@27virtual.net**
 - **{Password-Provided-by-Instructor}**
11. In the upper right-hand corner of the Cloud Console, Click the **Drop-down** next to your account
12. If present, click the **Drop-down** next to Change organization to change/confirm your Org.
Select **Your VCDR Org** (VMCEXP2-VCDR01)



13. On the **Services** Page, click **LAUNCH SERVICE** in the **VMware Cloud DR** Tile, to review the VCDR settings. If you do not see the My Services tiles, select the nine dots in the top right corner and select **VMware Cloud DR**.
14. Click **Manage Region**
15. Click **Cloud File System -> cloud-backup-1** to Review the Cloud File System that will be used for storing the Protected Virtual Machine Images

💡 We will now take a look at the Protected Site(s)

Note: The table below indicates which Protected Site you are assigned to and therefore should use

Protected Site	Student Assignment
Protected DC01	vmcexpertX-01 through vmcexpertX-10
Protected DC02	vmcexpertX-11 through vmcexpertX-20
Protected DC03	vmcexpertX-21 through vmcexpertX-30

16. Click **Protected Sites -> Protected DC##** to review your Protected Datacenter.
You will notice two connector appliances have been deployed to the Protected DC and in a healthy state.
17. You'll also notice that the On-Premises vCenter has been added.
18. Click **Recovery SDDC**, and Select **<The recovery SDDC>** to review its settings
19. 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

vmw VMware Cloud Disaster Recovery

Global console

Dashboard for US West (Oregon)

Dashboard

Cloud file systems

- cloud-backup-1

Protected sites

- Protected DC01
- Protected DC02
- Protected DC03

Recovery SDDCs

Protection groups

Virtual machines

DR plans

Monitor

Settings

Welcome to VMware Cloud Disaster Recovery

VMware Cloud DR is VMware's easy-to-use, on-demand disaster recovery service, delivered as SaaS, with cloud economics.

Quick setup


- 1 Configure the API token
- 2 Deploy the cloud file system
- 3 Set up a protected site
- 4 Create a protection group
- 5 Add the recovery SDDC
- 6 Create the DR plan

Recovery region summary

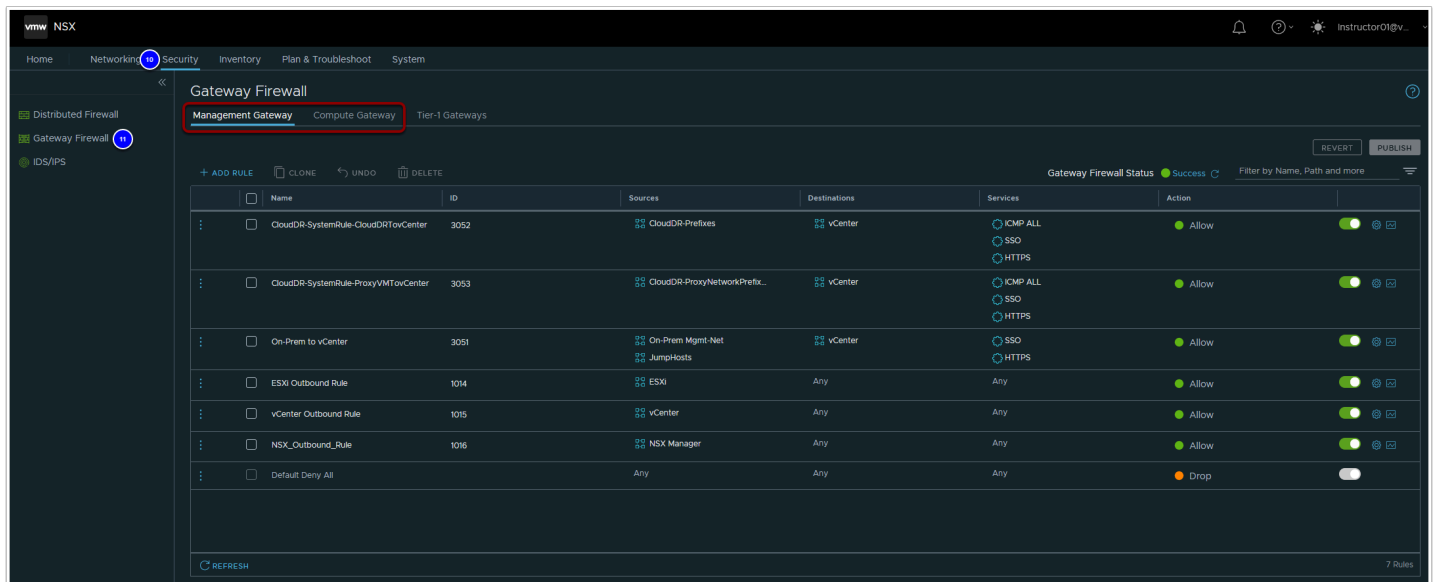
Status	Cloud file systems	Storage	Protected sites
<ul style="list-style-type: none">ProtectionRecoverability	1	~ 0.0 MiB <small>Calculated every 12h</small>	0 <small>VMware Cloud</small> 3 <small>On-premises</small>

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{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. Click the **Drop-down** next to Change organization and select **Your VCDR Org (VMCEPERTX-VCDR01)**
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. In the VMware Cloud on AWS portal click the **OPEN NSX MANAGER** button
9. Click **ACCESS VIA THE INTERNET** to connect to NSX Manager UI
10. Choose **Security** tab
11. Click **Gateway Firewall**. Review both the Compute Gateway and Management Gateway Firewall rules

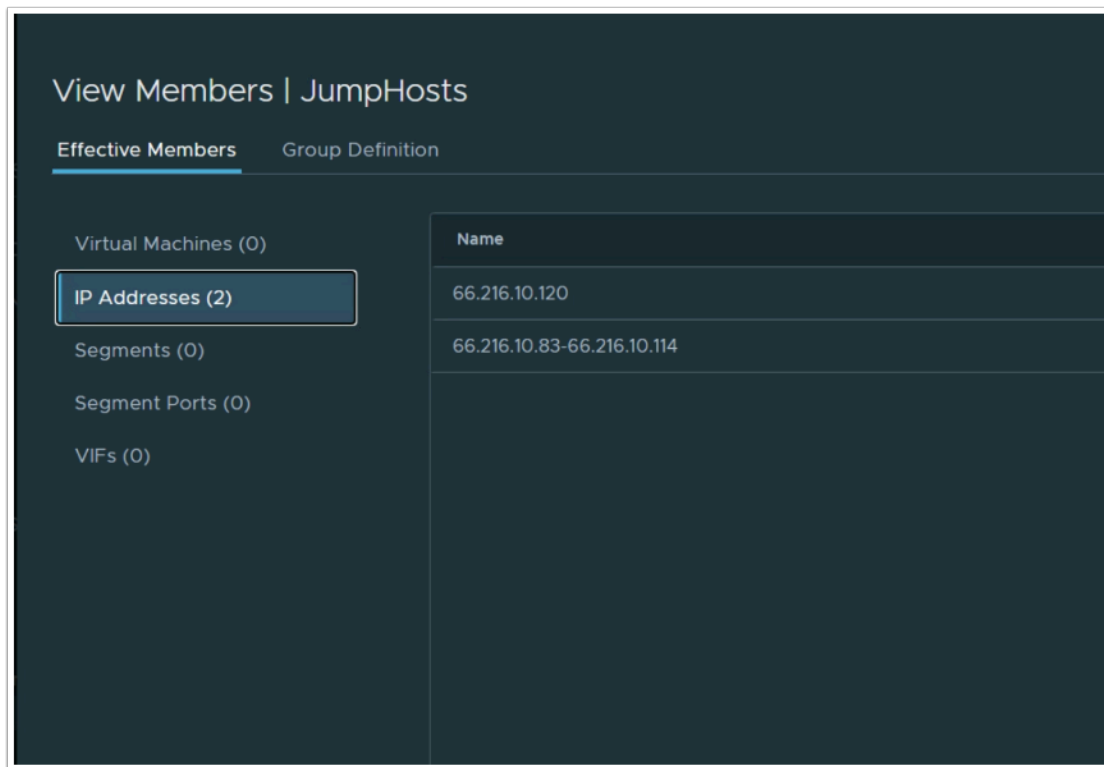
 You'll notice, the Compute Gateway has rules allowing the Cloud Proxy Appliance access to the Scale-Out File System and Vice-Versa

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



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

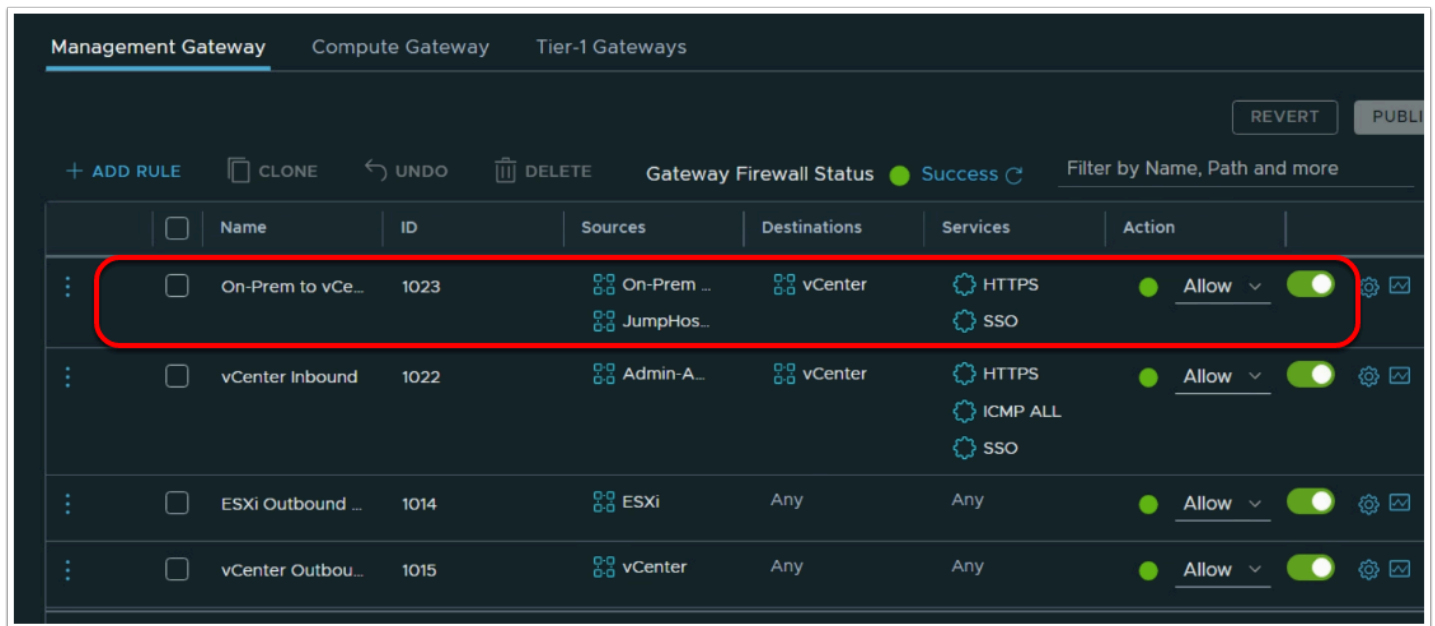
12. Choose **Inventory** tab
13. Select **Groups**
14. Click **Management Groups**
15. Click **View Members** next to **JumpHosts** to confirm that the Public IP of your VDI (On-Premises Environment) is included
16. Click IP Addresses
17. Click **CLOSE**



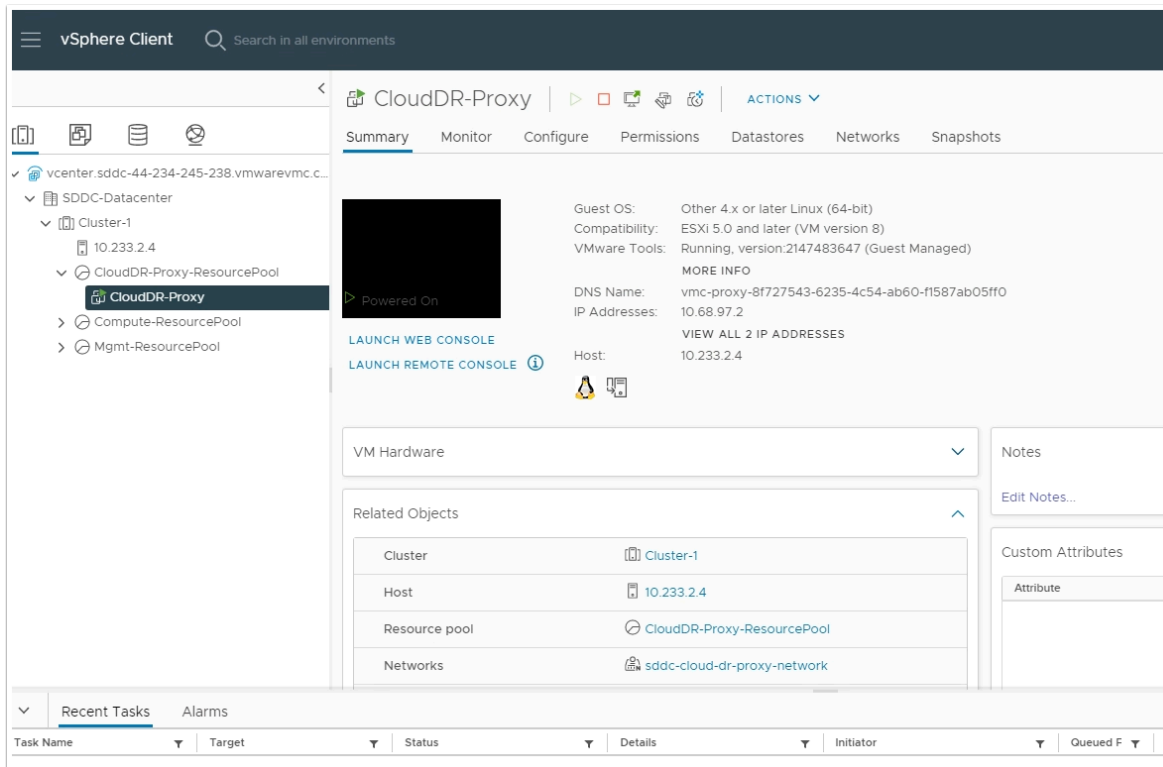
! NOTE: If your public IP (66.216.10.x) is not in the range(s). Please notify your instructor.

Your Public IP should be available in your Lab input workbook or you can go to <http://www.whatismyip.com> from the VDI desktop to discover the Public IP Address

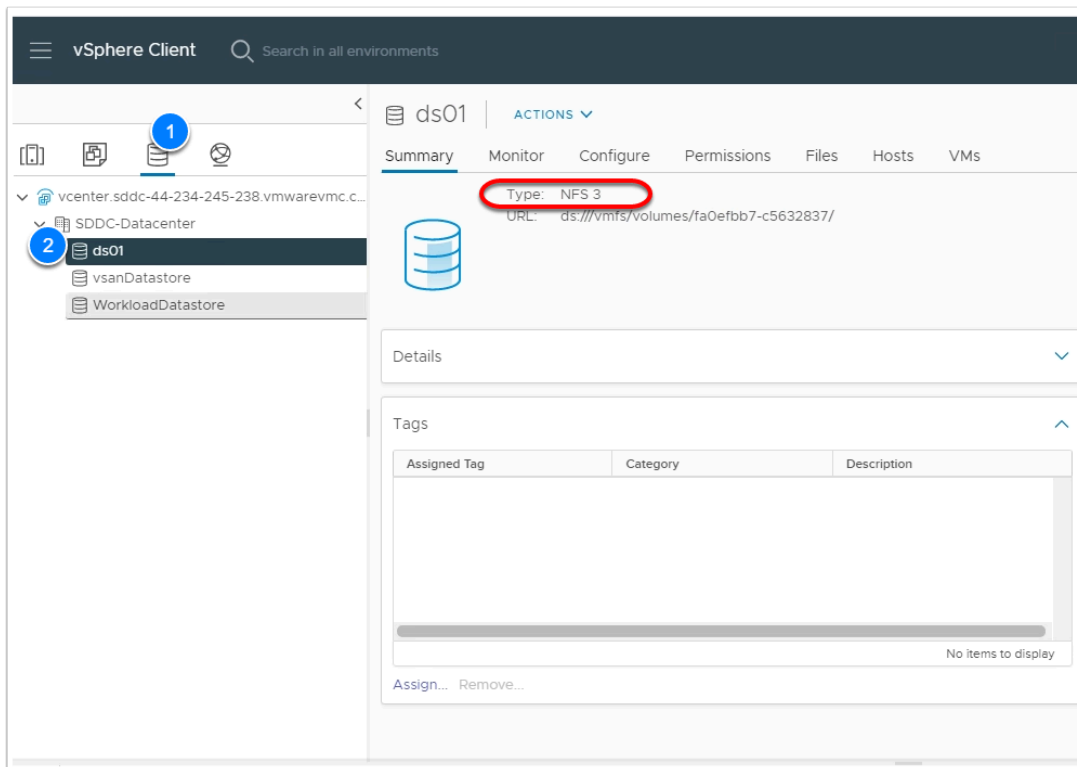
18. Choose **Security** tab
19. Click **Gateway Firewall**
20. Click **Management Gateway**
21. Review the **On-Prem to vCenter Inbound** rule and confirm the following
 - Source:
 - **On-Prem Mgmt-Net** (Mouse over the source field and click the pencil)
 - **JumpHosts**
 - Destination: **vCenter**
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



22. Go back to your **VMC on AWS** SDDC tab in the browser
23. Click the **Settings** Tab
24. Expand the **Default vCenter User** and **vSphere Client (HTML5)** sections
25. Take note of and copy the values for:
 - Username
 - Password
 - vSphere Client URL
26. 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



27. 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
28. Switch to the Datastores View
29. You'll notice an NFS Datastore named **ds01**
VCDR Mounts recovered VMs from this datastore.

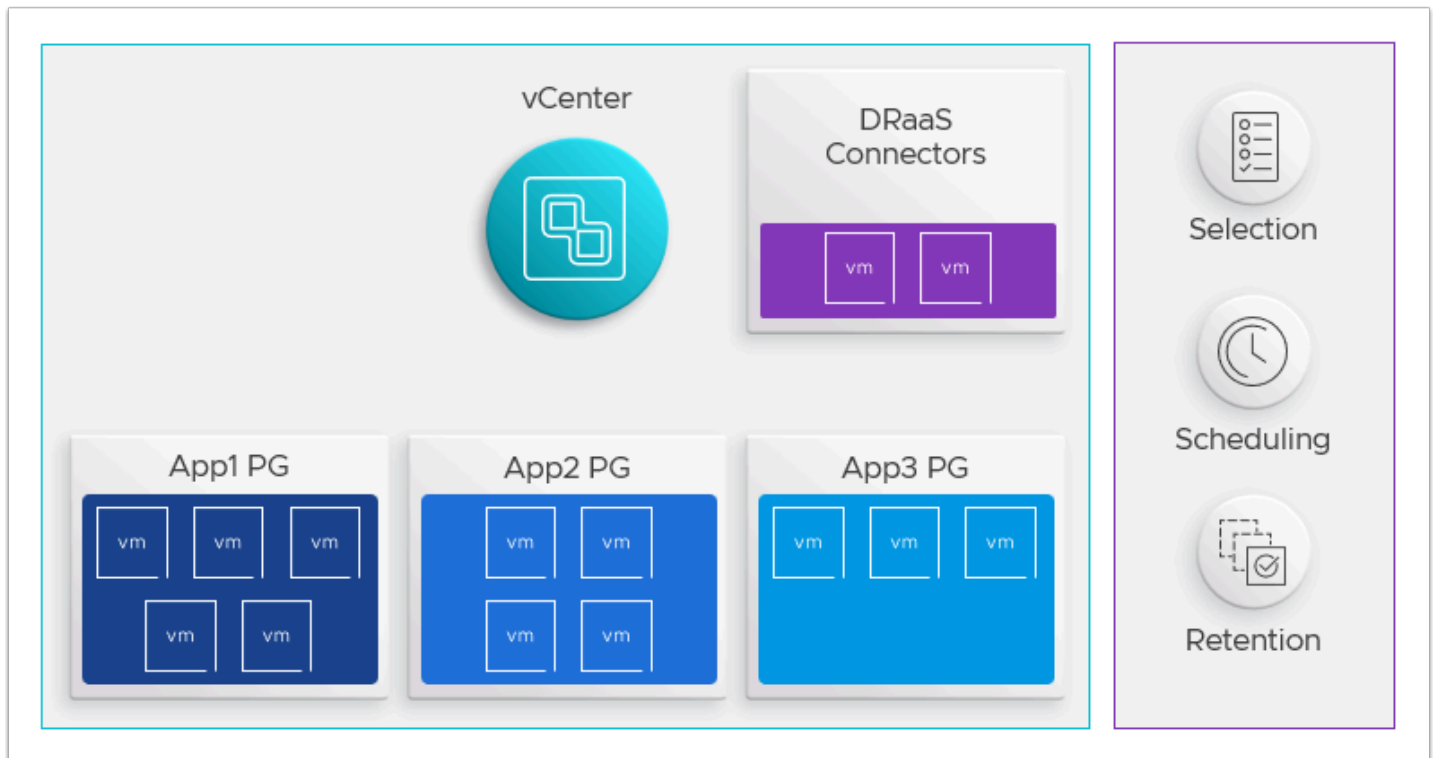


Task 4 - Create a Protection Group

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)



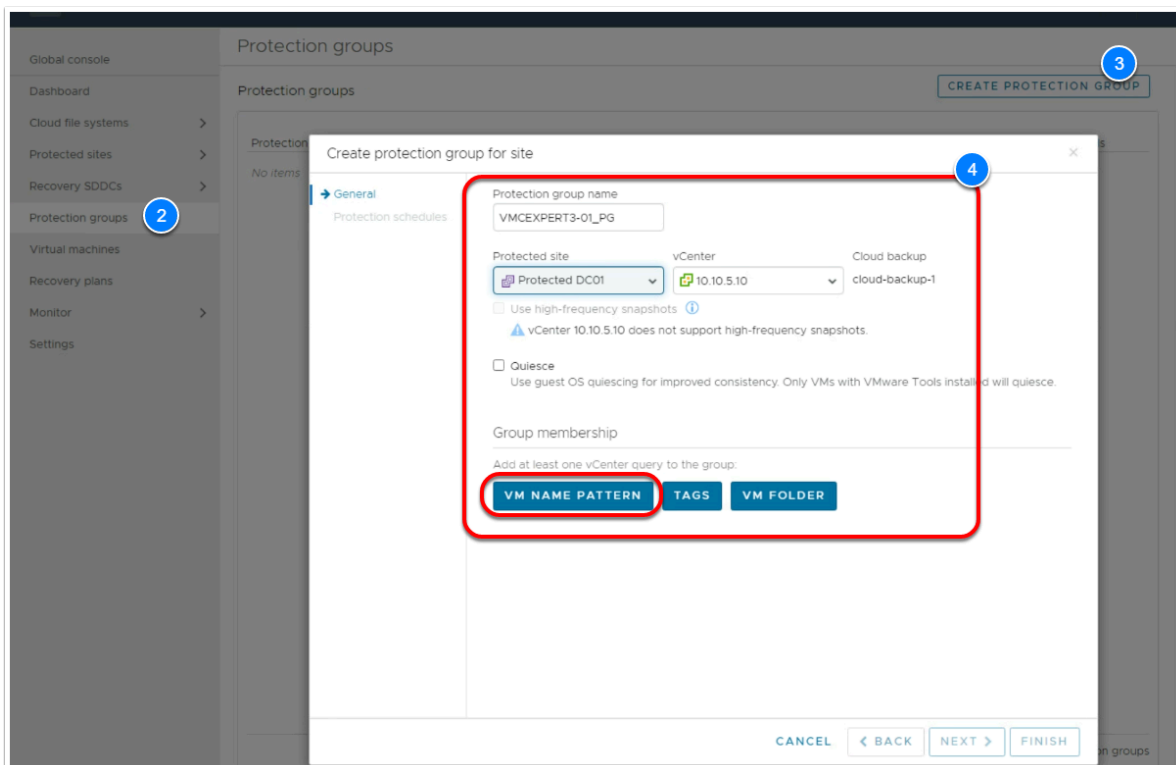
Protection groups can then be added to a DR plan, which ensures that if a failure occurs, you can orchestrate recovery to a new site using selected snapshots of your VMs to re-instantiate the source vCenter site.

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 1-14](#)
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: **<Select-Your-Protected-Site>**
 - 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**

Protected Site	Student Assignment	vCenter
Protected DC01	vmcexpertX-01 through vmcexpertX-10	10.10.5.10
Protected DC02	vmcexpertX-11 through vmcexpertX-20	10.10.5.20
Protected DC03	vmcexpertX-21 through vmcexpertX-30	10.10.5.30



8. Set the following values for the Protection schedule:

- Take Snapshot: **Daily**
- At: **<The next 2 hours from now>** If it's currently 11:25 AM, choose **1:00 PM**.
- Keep snapshots for: **<Leave default>**
- Click **New Schedule** if you'd like to add an additional schedule

9. Click **Finish**

Edit site protection group -

General
Protection schedules

Protection schedules

Schedules are based on the site time zone. Site Protected DC01 is using Berlin, Europe (06:34 pm).

Daily

Take snapshots At Keep snapshots for

Daily 12 AM, 10 PM :00 1 weeks

Daily-2

Take snapshots At Keep snapshots for

Daily 11 AM, 3 PM :00 1 weeks

To improve the chance of recovering your data in case of a ransomware attack, a schedule with a retention of at least 60 days is recommended.

NEW SCHEDULE

These schedules will result in times between snapshots under four hours.

CANCEL < BACK NEXT > 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 2 Days**
13. Click **Take Snapshot**

Protection groups

CREATE PROTECTION GROUP


Protection group	Site	Cloud file system	Status	Schedule	Frequency	Quiesce	Last snapshot	VMs
VMCEXP3-01_...	Protected DC01	cloud-backup-1	Good	Active	Standard	No	Oct-20 08:13 am (1m ago)	1 VM

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

The screenshot displays the VMware Cloud Disaster Recovery console for a protection group named 'VMCEXP3-01_PG'. The interface includes tabs for 'Summary' and 'Events', with 'Summary' currently selected. Action buttons for 'TAKE SNAPSHOT', 'EDIT GROUP', and a dropdown menu are located in the top right. The main content area is divided into three panels: 'Group details', 'Membership', and 'Schedule'. The 'Group details' panel shows 'Snapshots: 1', 'Schedule: Active', 'Status: Good', 'Site: Protected DC01', and 'Type: Standard-frequency'. The 'Membership' panel shows 'VM name pattern: *01'. The 'Schedule' panel lists two schedules: 'Daily: snapshot every day at 9:00 AM. Retain for 1 week' and 'Daily-2: snapshot every day at 12:00 AM. Retain for 1 week'. Below these panels is a 'Snapshots' table with columns for Name, Taken timestamp, Includes, and Expiration. A single snapshot is listed: 'VMCEXP3-01_PG - Manual - 2022-10-20T12:09:16 UTC', taken at 'Oct-20 08:13 am (2m ago)', including '1 VM', and expiring at 'Oct-21 08:13 am (in 1d)'. 'EDIT' and 'DELETE' buttons are positioned above the table.

Name	Taken timestamp	Includes	Expiration
<input type="checkbox"/> VMCEXP3-01_PG - Manual - 2022-10-20T12:09:16 UTC	Oct-20 08:13 am (2m ago)	1 VM	Oct-21 08:13 am (in 1d)

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.

