*** Optional *** Disaster Recovery with Site Recovery Manager 8.4

Introduction

VMware Site Recover is a business continuity and disaster recovery solution that helps you to plan, test, and run the recovery of virtual machines between a protected vCenter Server on-premises site and a recovery vCenter Server site on VMware Cloud on AWS and the reverse.

VMware Site Recovery uses the host-based replication feature of vSphere Replication and the orchestration of VMware Site Recovery Manager

You can use VMware Site Recovery for orderly evacuation of virtual machines from a protected site to a recovery site. Planned migration prevents data loss when migrating workloads in an orderly fashion. For planned migration to succeed, both sites must be running and fully functioning.

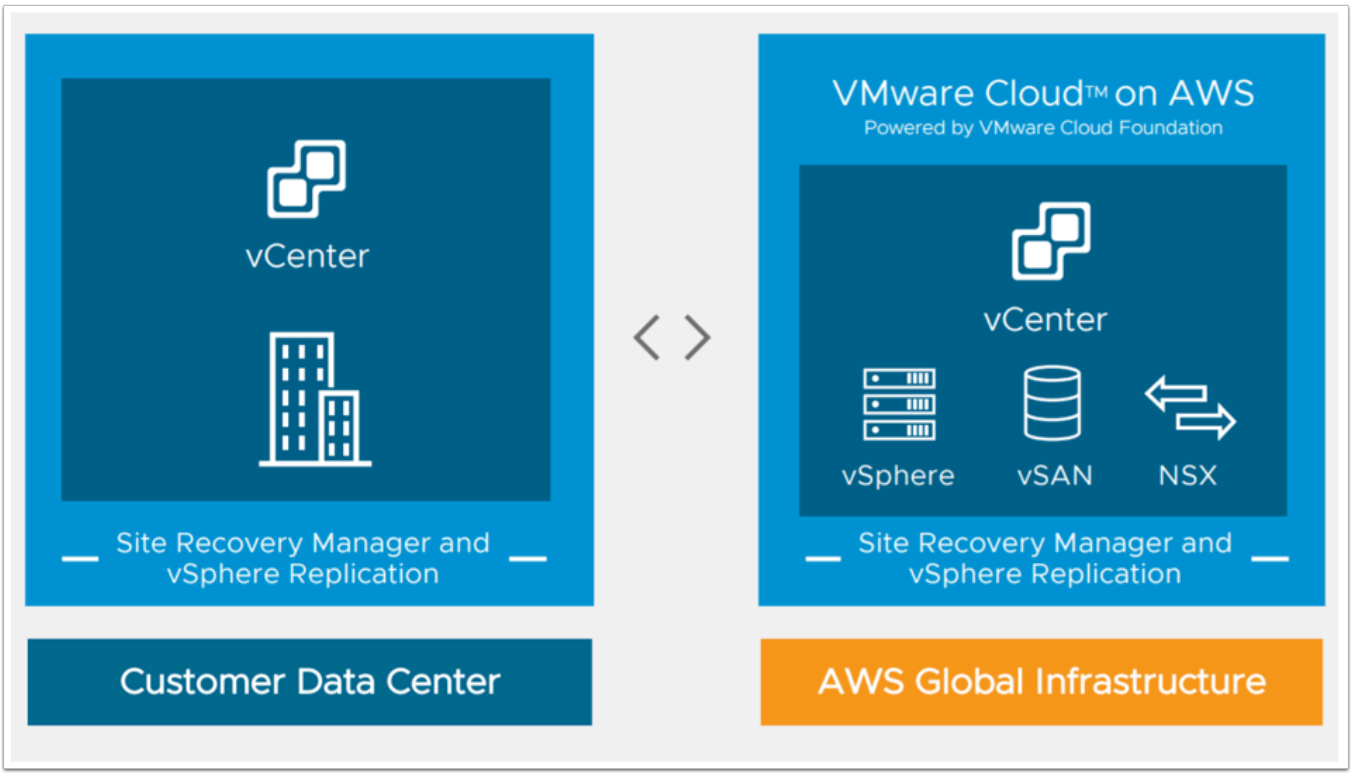
Disaster recovery is similar to planned migration, except that disaster recovery does not require that both sites be up and running, for example if the protected site goes offline unexpectedly. During a disaster recovery operation, failure of operations on the protected site is reported but is otherwise ignored.

In case of site disaster, Site Recovery Manager orchestrates both the recovery process and the replication mechanisms to minimize data loss and system downtime.

- At the protected site, Site Recovery Manager shuts down virtual machines cleanly and synchronizes storage, if the protected site is still running.
- Site Recovery Manager powers on the replicated virtual machines at the recovery site according to a recovery plan.

A recovery plan specifies the order in which virtual machines start up on the recovery site. A recovery plan specifies network parameters, such as IP addresses, and can contain user-specified scripts that Site Recovery Manager can run to perform custom recovery actions on virtual machines.

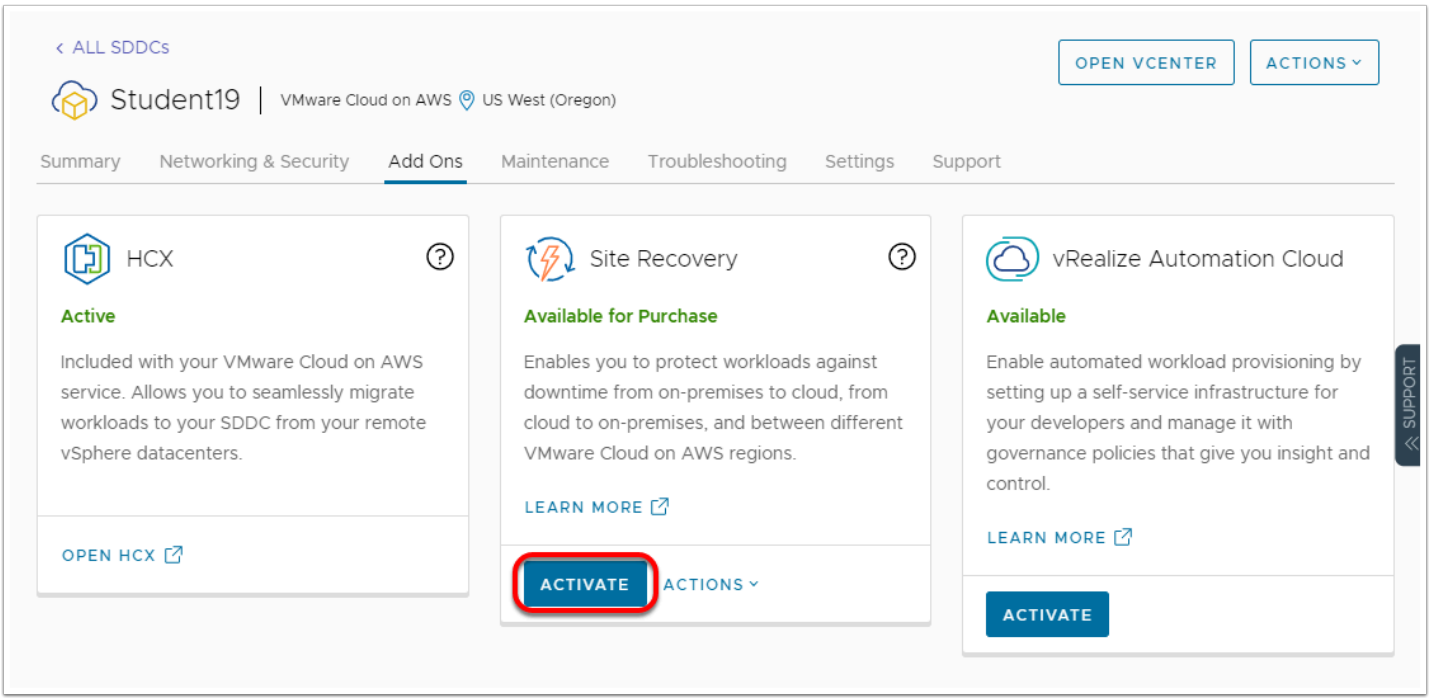
Site Recovery Manager lets you test recovery plans. You conduct tests by using a temporary copy of the replicated data in a way that does not disrupt ongoing operations at either site.



TASKS

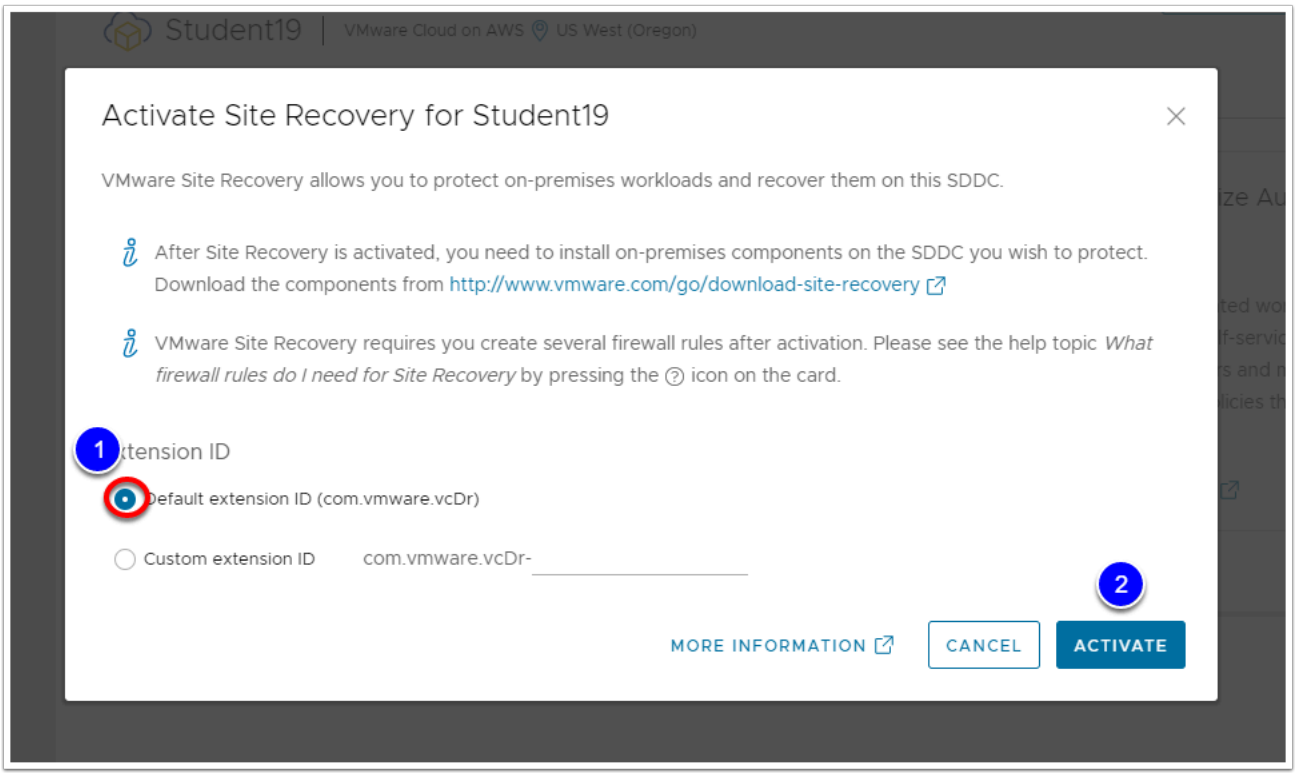
Task 1 - Activate Site Recovery Add-on

1. Log in to the VMware Cloud on AWS Console at https://vmc.vmware.com.
2. Click your **SDDC**, and then click **Add-Ons**.
3. Select Site Recovery and click **Activate**.



4. Leave the **default extension id** selected
5. Read the information on the Activate Site Recovery page and click **Activate**. This takes 10-15 minutes.
6. After the service activates, you will be presented with a link to Download on-premises components
7. The on-premises components have already been downloaded and imported into the on-Premises vCenter

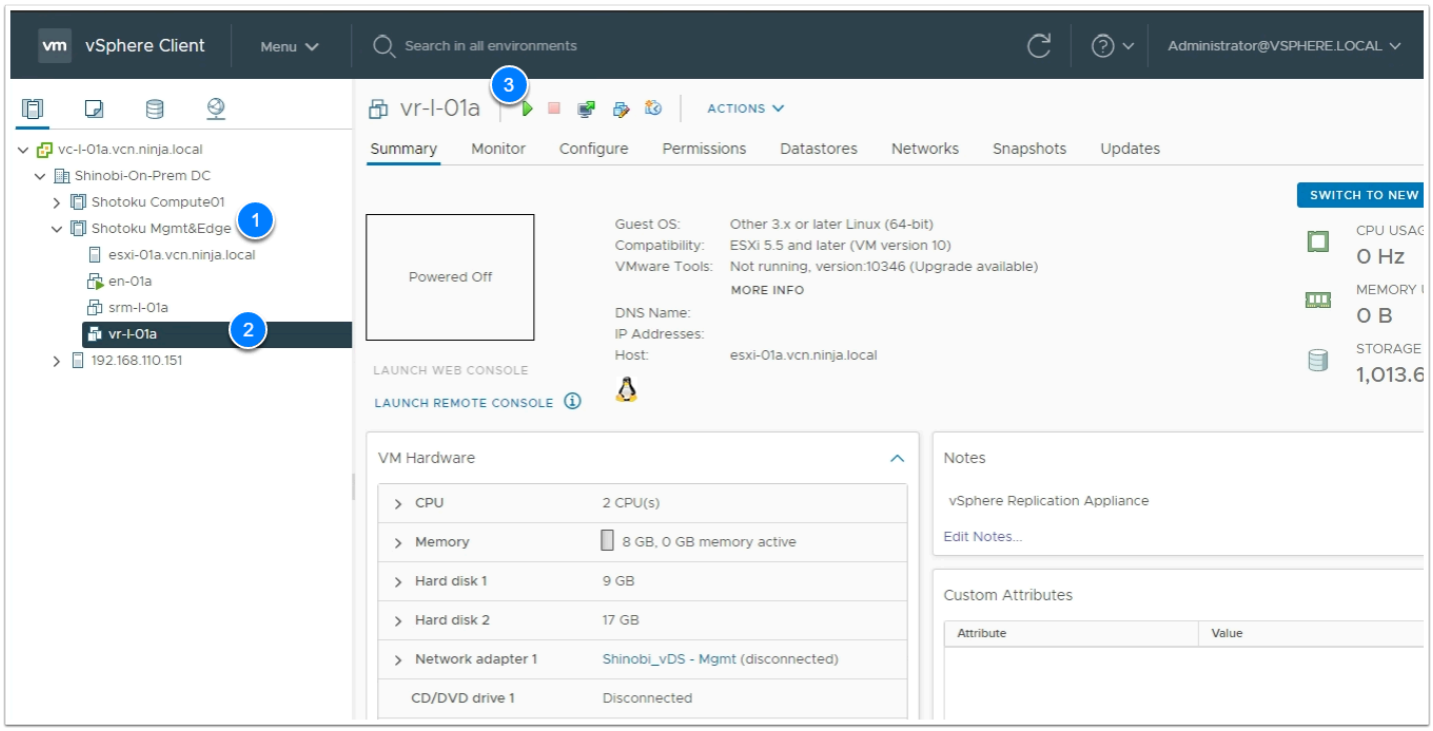
Note:**The VMware Site Recovery license key is part of the subscription to the service, when you pair the Site Recovery Manager on-premises instance with the Site Recovery Manager instance on VMware Cloud on AWS, VMware Site Recovery uses the cloud license**.



Task 2 - Configure the On-Premises vSphere Replication and Site Recovery Manager Appliances

As mentioned in the previous task, the on-premises appliances have already been deployed. In this task we will review and modify the configuration.

1. Log into your On-Premises vCenter
2. (you may use the **vSphere Client** bookmark in the **VI Management** bookmark folder in Chrome)
3. Expand the **Shotoku Mgmt&Edg**e Cluster
4. Confirm the existence of the following VMs
   - **vr-l-01a**
   - **srm-l-01a**
5. Power-on **vr-l-01a**, If it is powered-off
   - **NOTE: Do not power-on srm-l-01a until the vSphere Replication appliance configuration has completed successfully**

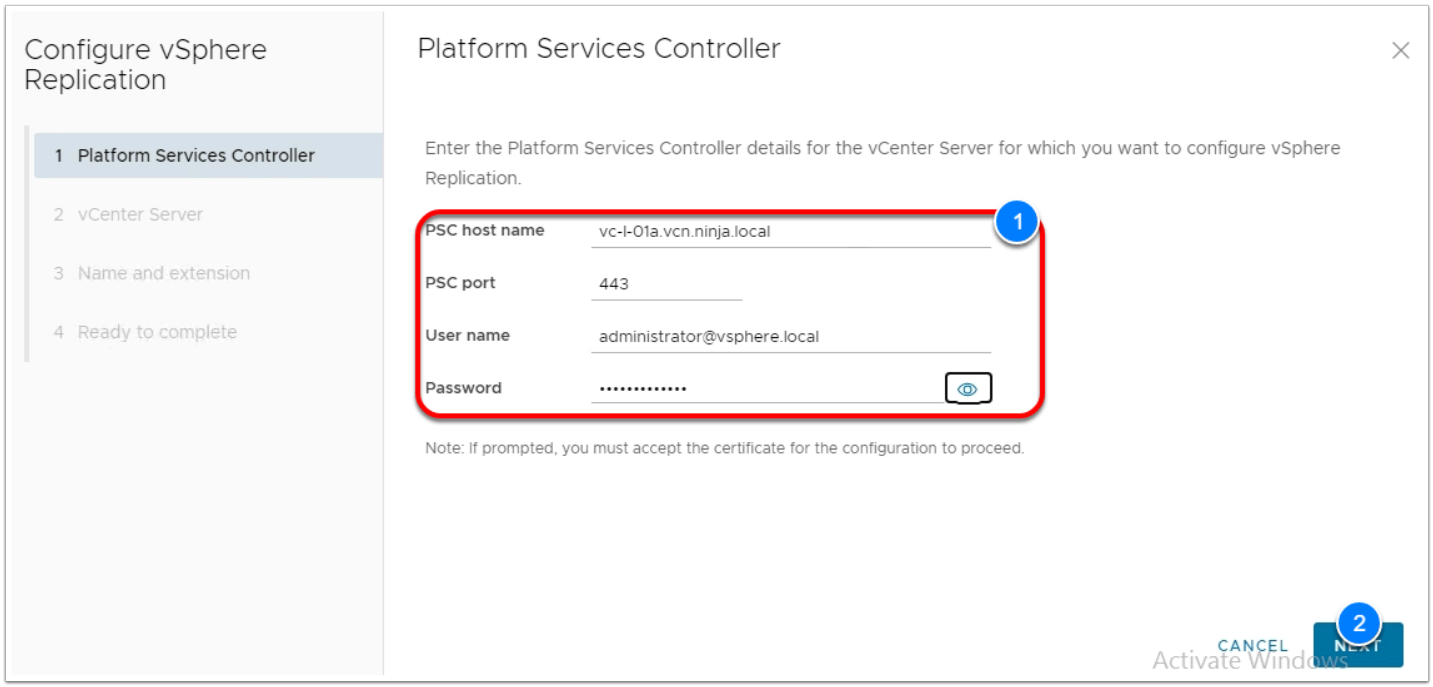


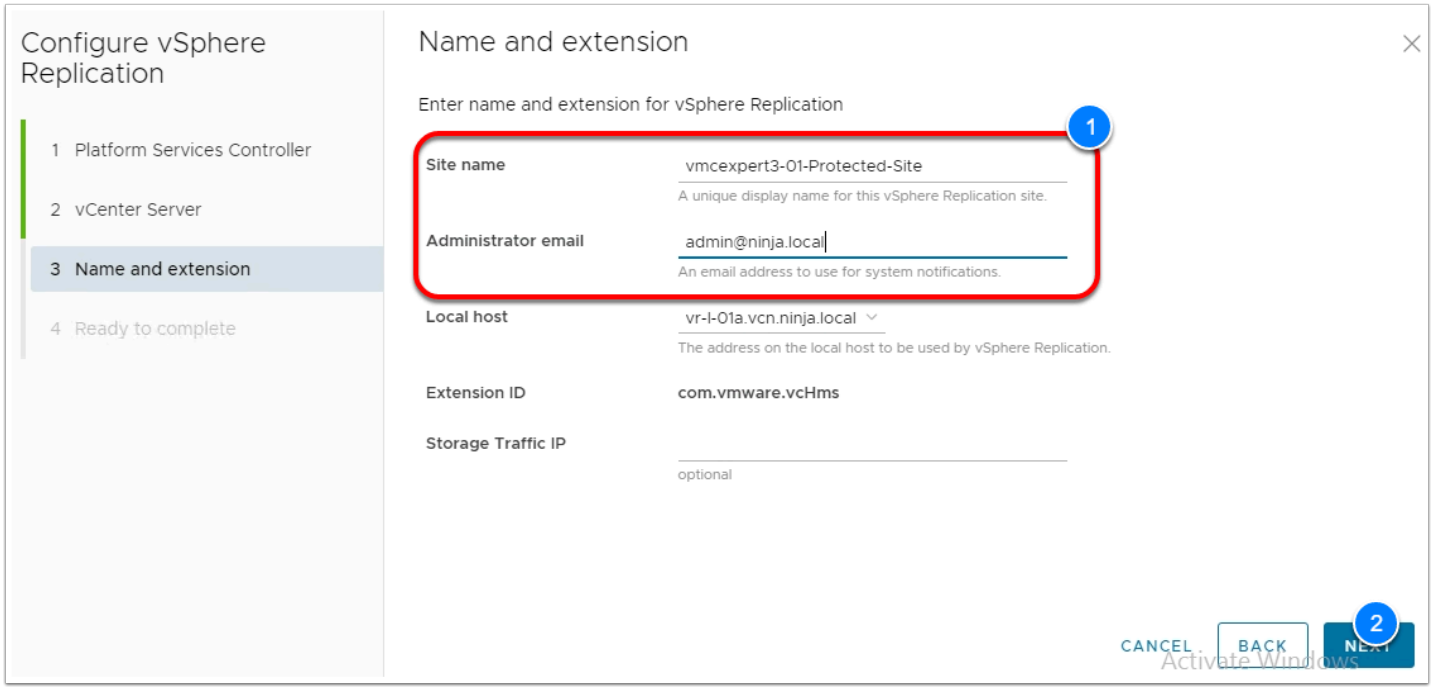
6. In another browser tab access the **vSphere Replication Appliance** Bookmark or type https://vr-l-01a.vcn.ninja.local:5480 to review settings. You will need to wait for a few minutes for step 4 to complete before the gui works.
   - Use the following login information:
     - Username: **admin**
     - Password: **VMwareNinja1!**

7. Click the **Configuration Appliance** button
8. In the Platform Services Information Page of the Wizard, enter the following values
   - PSC host name: **vc-l-01a.vcn.ninja.local**
   - PSC port: **443**
   - User Name: **administrator@vsphere.local**
   - Password: **VMwareNinja1!**

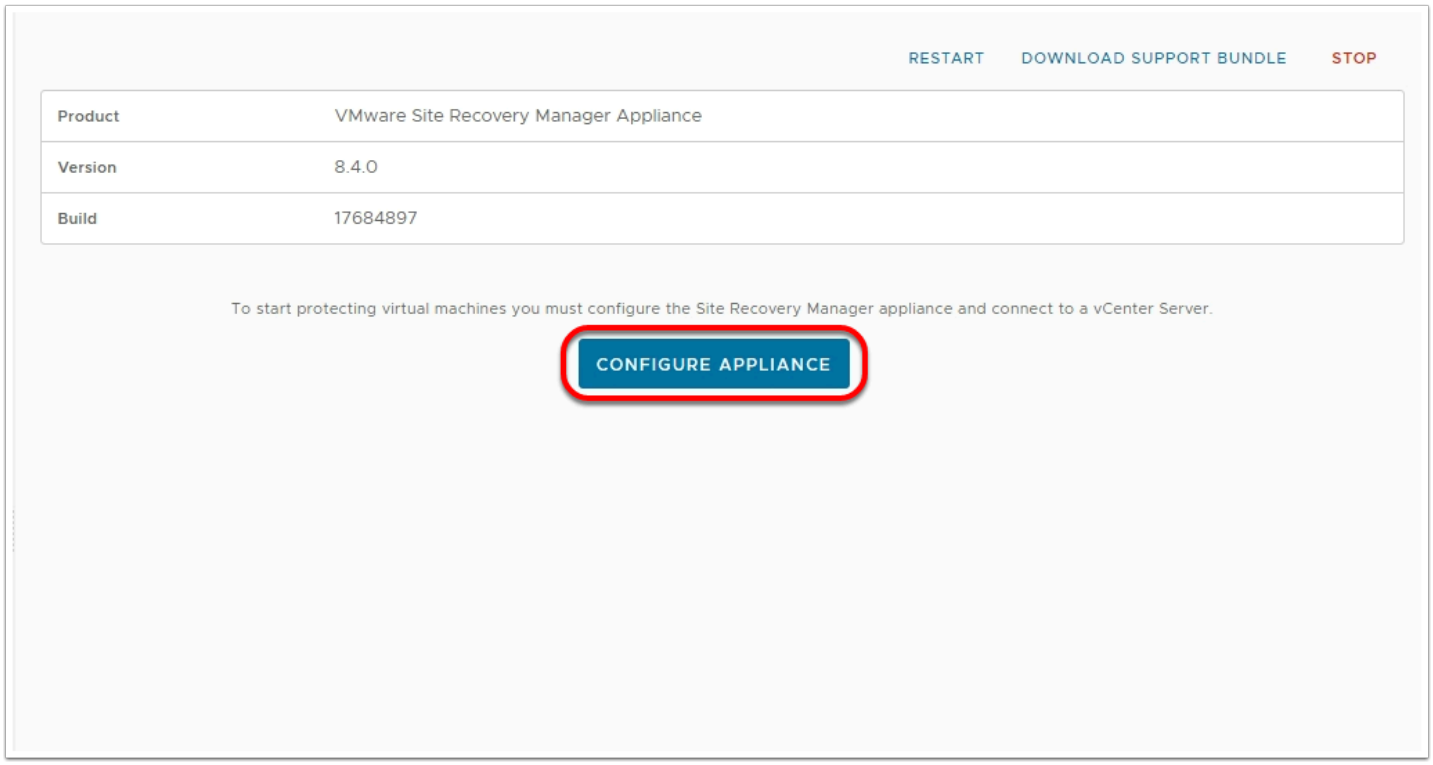
9. When prompted **Accept** the SSL Certificate - Click **CONNECT**
10. Click **NEXT**
11. When prompted **Accept** the SSL Certificate - Click **CONNECT**
12. Enter the following information in the Name and Extension page of the wizard:
    - Site Name: **vmcexpert#-xx-Protected-Site** (Where **#** is the Environment ID, and **xx** is your student number)
    - Administrator email: **admin@ninja.local**

13. Click **NEXT**
14. Click **Finish**
15. **Note**: **This process can take up to 5 Mins. Wait for it to complete and confirm that the Tomcat Service is running before proceeding**

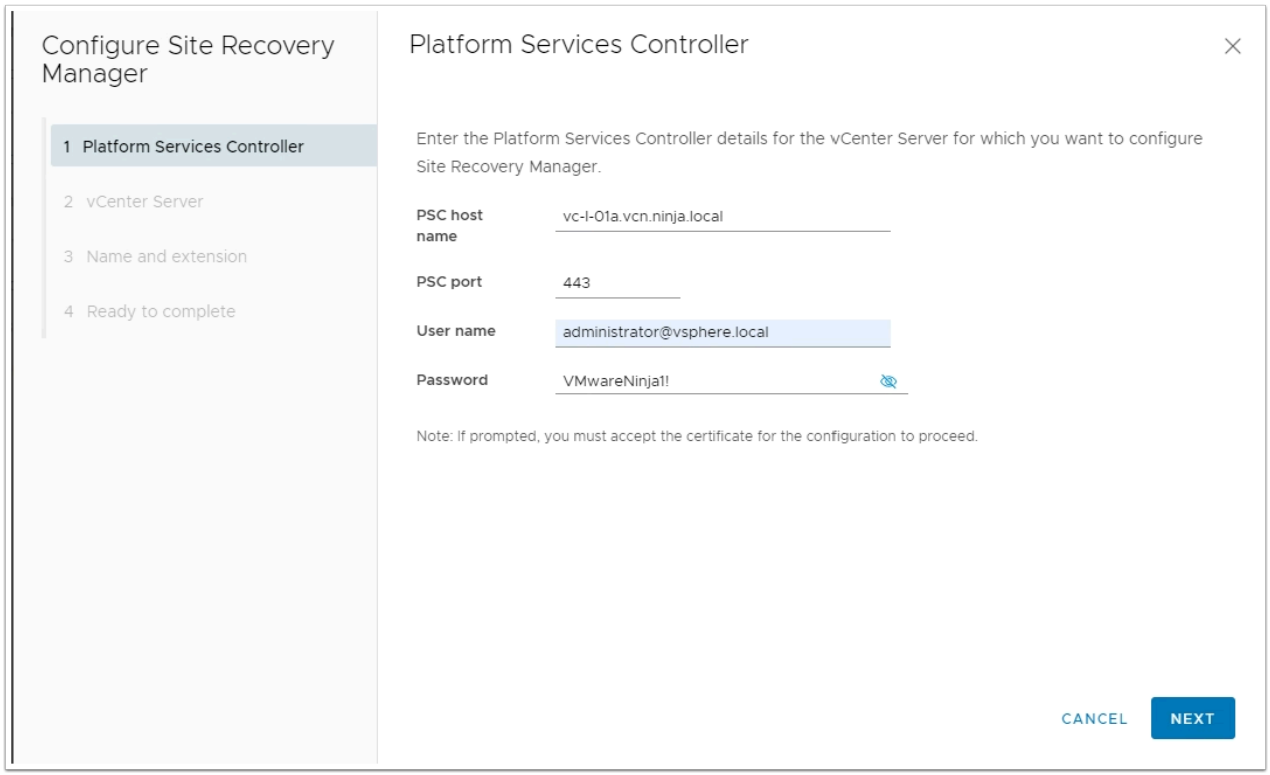


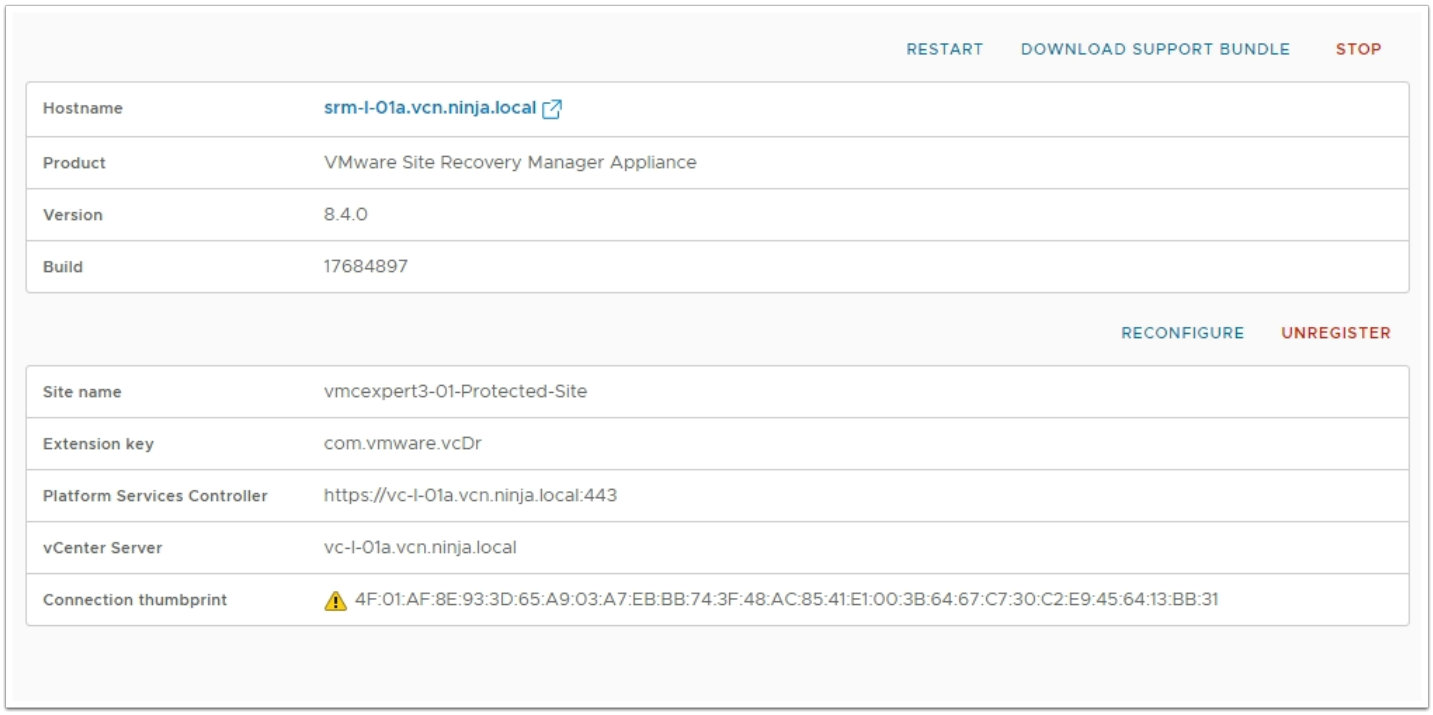


16. In the vSphere Client Select the **srm-l-01a** VM, right-click and select **Power --> Power-on**
17. In another browser tab access the **srm-l-01a** (Site Recovery Manager) vm to review and configure it. Use the following details:
18. URL: https://srm-l-01a.vcn.ninja.local:5480
19. Username: **admin**
20. Password: **VMwareNinja1!**
21. Click the blue **CONFIGURE APPLIANCE** button



19. Enter the Following details:
    - PSC Host Name: **vc-l-01a.vcn.ninja.local**
    - PSC port: **443**
    - User name: **administrator@vsphere.local**
    - Password: **VMwareNinja1!**
20. Click **NEXT**
21. Click **Connect** to accept the SSL Certificate Validation Warning and proceed with the configuration
22. On the **vCenter Server** Page Click **NEXT**
23. Click **Connect** to accept the SSL Certificate Validation Warning and proceed with the configuration
24. On the **Name and Extension** Page Type **vmcexpert#-xx-Protected-Site** in the Site Name field. i.e. vmcexpert3-01-Protected-Site
25. Type **admin@ninja.local** in the Administrator email field
26. Click **NEXT**
27. Click **FINISH**
28. Review the successful completion of the settings

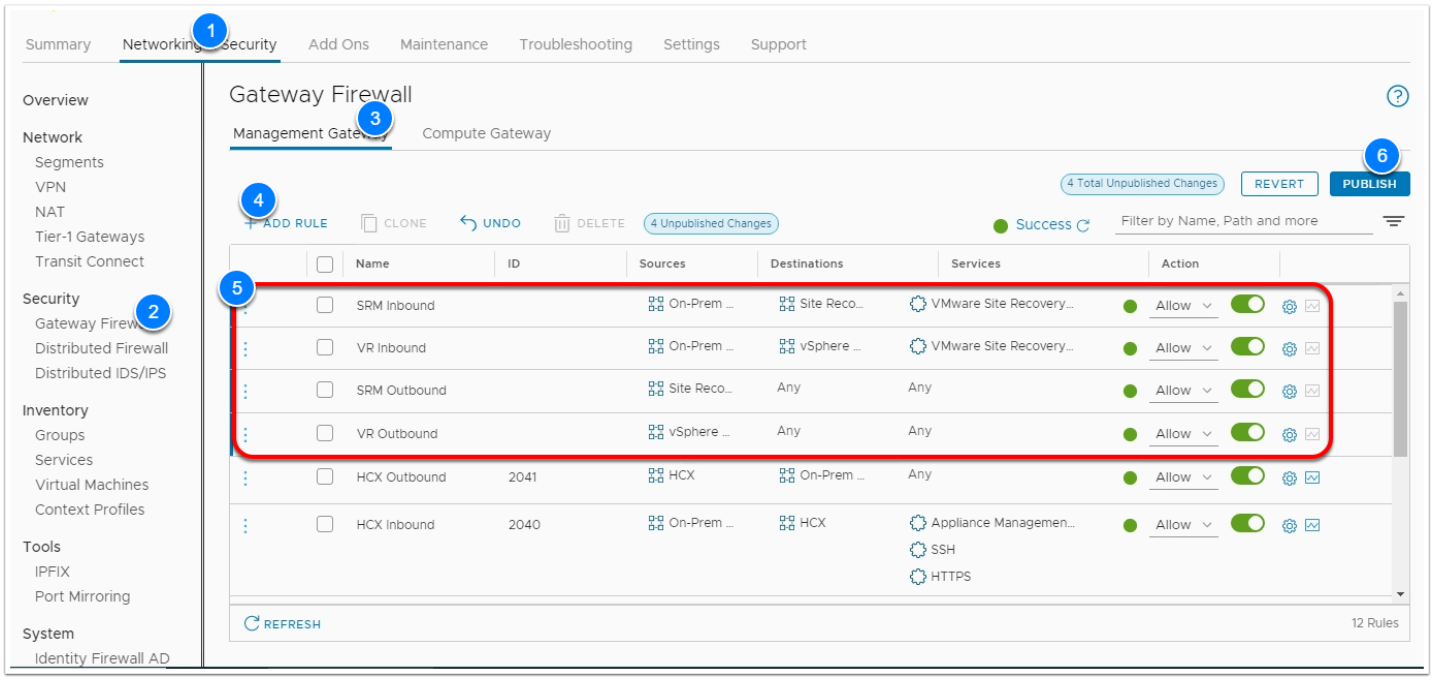

Configure Site Recovery Manager
1 Platform Services Controller
2 vCenter Server
3 Name and extension
4 Ready to complete
Platform Services Controller
Enter the Platform Services Controller details for the vCenter Server for which you want to configure Site Recovery Manager.
PSC host name
vc-l-01a.vcn.ninja.local
PSC port
443
User name
administrator@vsphere.local
Password
VMwareNinja1!
Note: If prompted, you must accept the certificate for the configuration to proceed.
CANCEL
NEXT


RESTART
DOWNLOAD SUPPORT BUNDLE
STOP
Hostname
srm-l-01a.vcn.ninja.local
Product
VMware Site Recovery Manager Appliance
Version
8.4.0
Build
17684897
RECONFIGURE
UNREGISTER
Site name
vmcexpert3-01-Protected-Site
Extension key
com.vmware.vcDr
Platform Services Controller
https://vc-l-01a.vcn.ninja.local:443
vCenter Server
vc-l-01a.vcn.ninja.local
Connection thumbprint
4F:01:AF:8E:93:3D:65:A9:03:A7:EB:BB:74:3F:48:AC:85:41:E1:00:3B:64:67:C7:30:C2:E9:45:64:13:BB:31

Task 3 - Create SDDC Gateway Firewall rules for VMware Site Recovery

We will now create the required firewall rules to allow pairing of the On-Prem and SDDC Site Recovery Managers and allow the vSphere Replication appliances to replicate VM content between the sites.

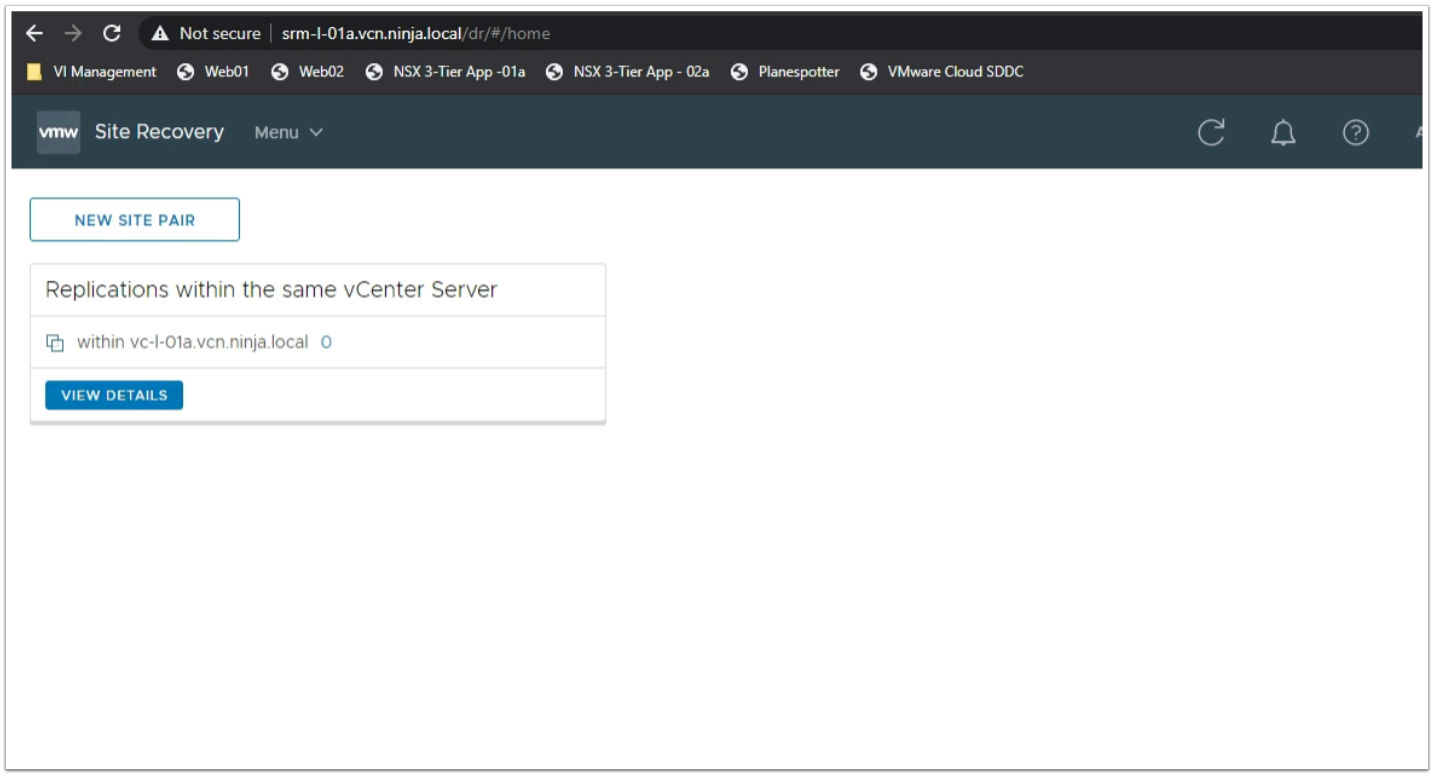
1. In your VMC on AWS Console Click the **Networking & security** tab
2. Click **Gateway Firewall**
3. Click **Management Gateway**
4. Click **Add Rule (4 times)** to add four new rules
5. Configure the Rules as follows:
    1. RULE 1
        - NAME: **SRM Inbound**
        - Sources: (user defined) **On-Prem MGMT NET**
        - Destinations: **Site Recovery Manager**
        - Services:**VMware Site Recovery SRM**
        - Action:**Allow**
    2. RULE 2
        - NAME: **VR Inbound**
        - Sources: (user defined) **On-Prem MGMT NET**
        - Destinations: **vSphere Replication**
        - Services:**VMware Site Recovery vSphere Replication**
        - Action:**Allow**
    3. RULE 3
        - NAME: **SRM Outbound**
        - Sources: **Site Recovery Manager**
        - Destinations: **Any**
        - Services:**Any**
        - Action:**Allow**
    4. RULE 2
        - NAME: **VR Outbound**
        - Sources: **vSphere Replication**
        - Destinations: **Any**
        - Services:**Any**
        - Action:**Allow**
6. Click **Publish**



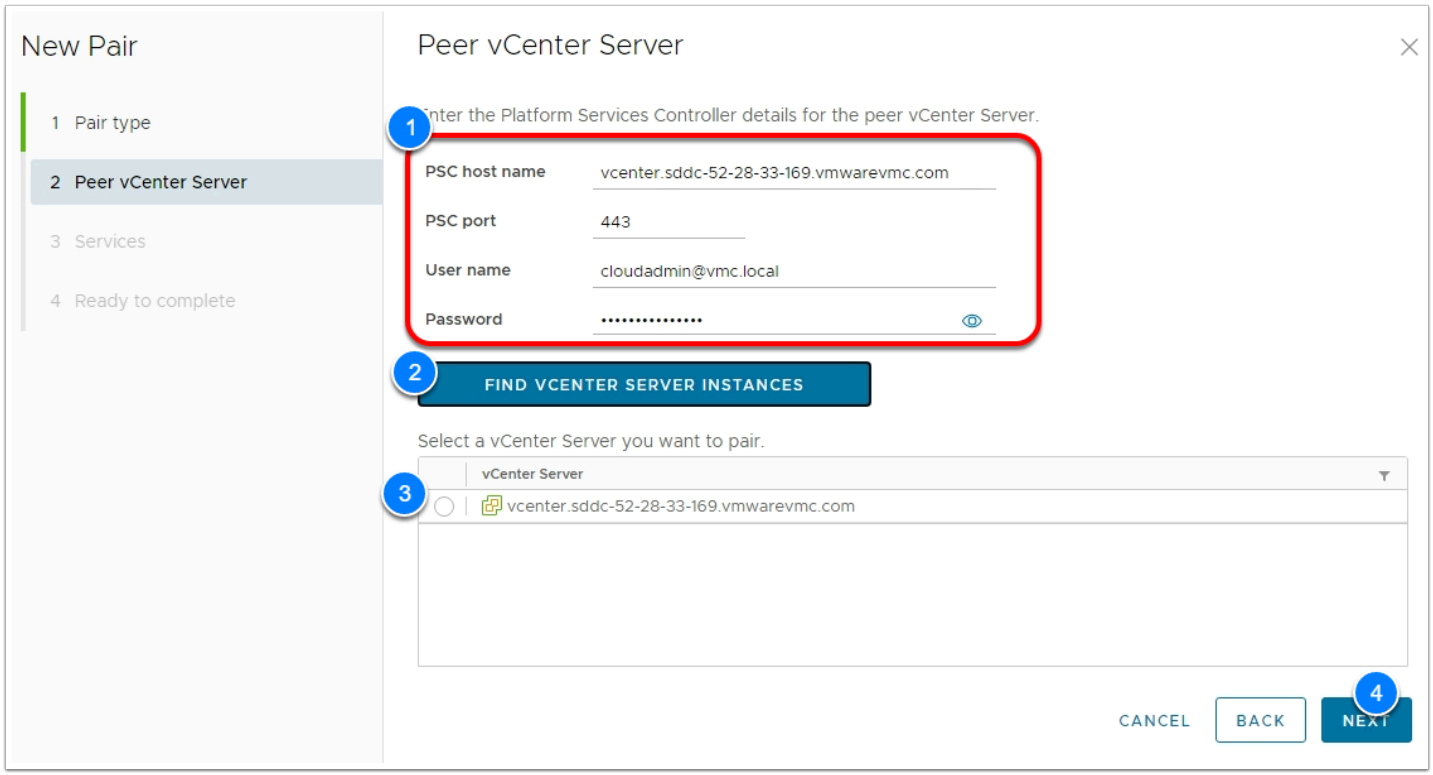
Task 4 - Pair On-Premises with SDDC

We will now Pair the On-Premises SRM instance with the instance deployed in the SDDC. Once SRM has been deployed and configured in both the Protected and recovery site(s). You must first configure pairing between these sites before you can start protecting and ultimately failing over VMs for one site to the other.

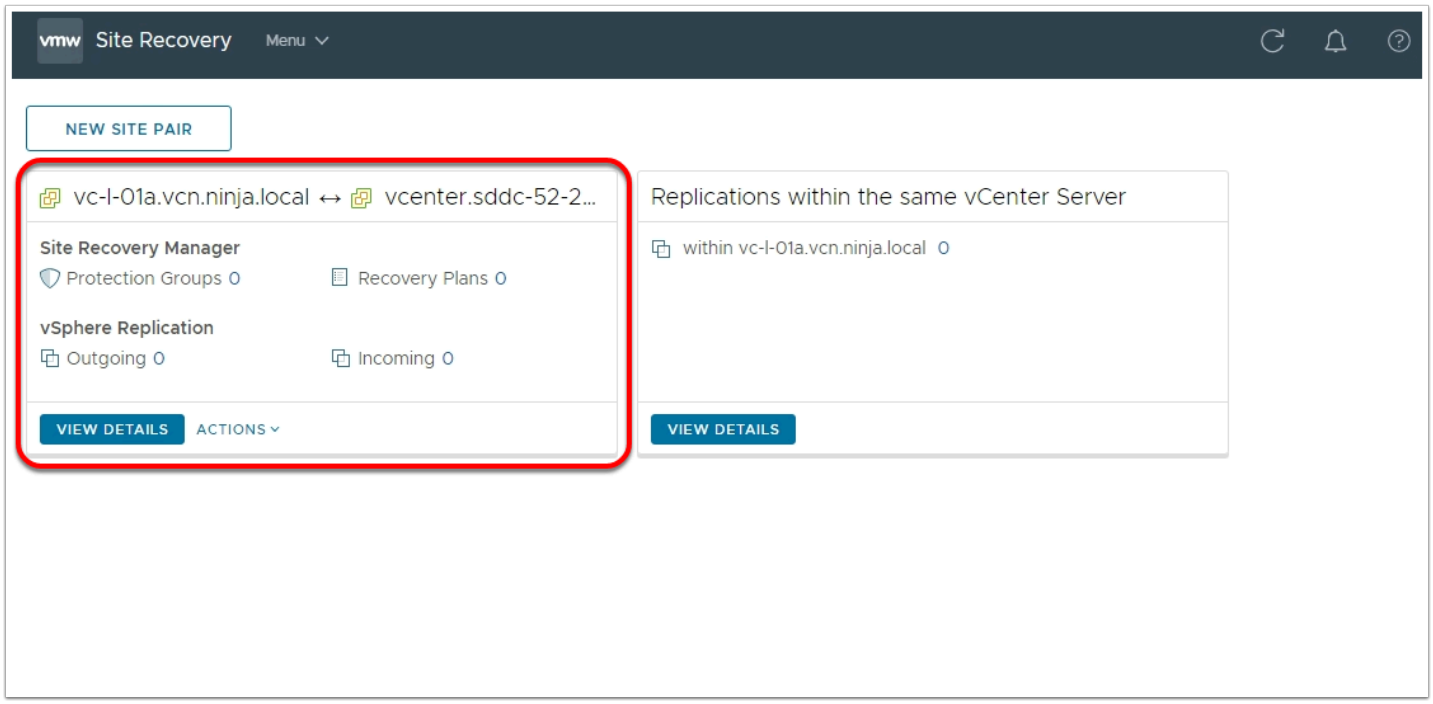
1. In the Google Chrome browser on the desktop access the On-Premises SRM instance. Go to https://srm-l-01a.vcn.ninja.local
2. Click **LAUNCH SITE RECOVERY**
3. If Prompted, log in as
   - **administrator@vsphere.local**
   - **VMwareNinja1!**
4. Click the **NEW SITE PAIR** button
5. Select **Pair with a peer vCenter located in a different SSO domain**
6. Click **NEXT**



5. Pair with the SDDC Environment using the following info:
   - PSC host name: <**Enter the FQDN of your SDDC vCenter**> **NOTE:** this information can be copied from the settings tab
   - of your SDDC in the VMware Cloud Console (vmc.vmware.com)
   - User name: **cloudadmin@vmc.local**
   - Password: <**your cloudadmin password**>
6. Click **Find vCenter Server Instances**
7. Select the **radio button** of the **SDDC vCenter Instance (**vcenter.sddc-xx-xx-xx-xx.vmwarevmc.com**)**
8. Click **NEXT**



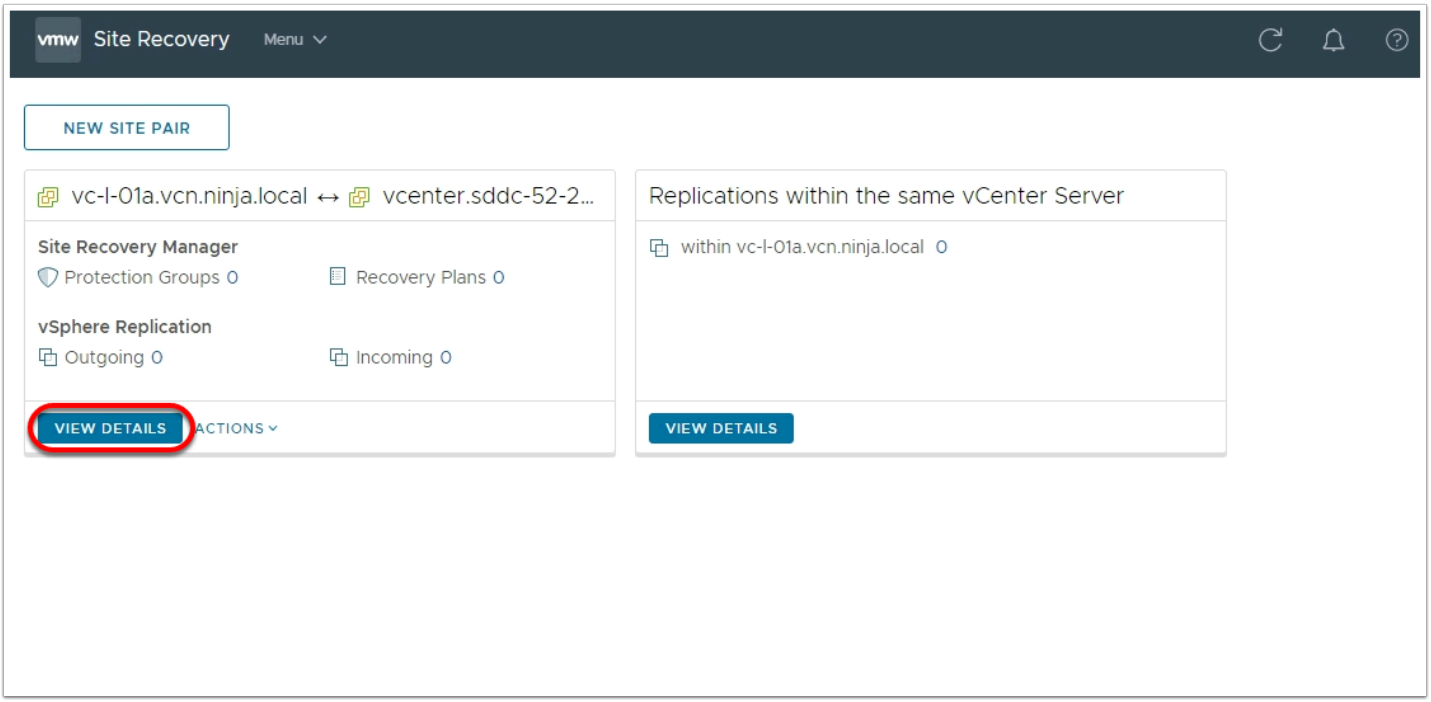
9. Select the **SRM** and **VR** instances configured against your SDDC vCenter
10. Click **NEXT**
11. Click **CONNECT** to Accept the SSL Certificate
12. Click **FINISH**
13. After about 30 to 60 seconds you should see the site pair information populate on the screen

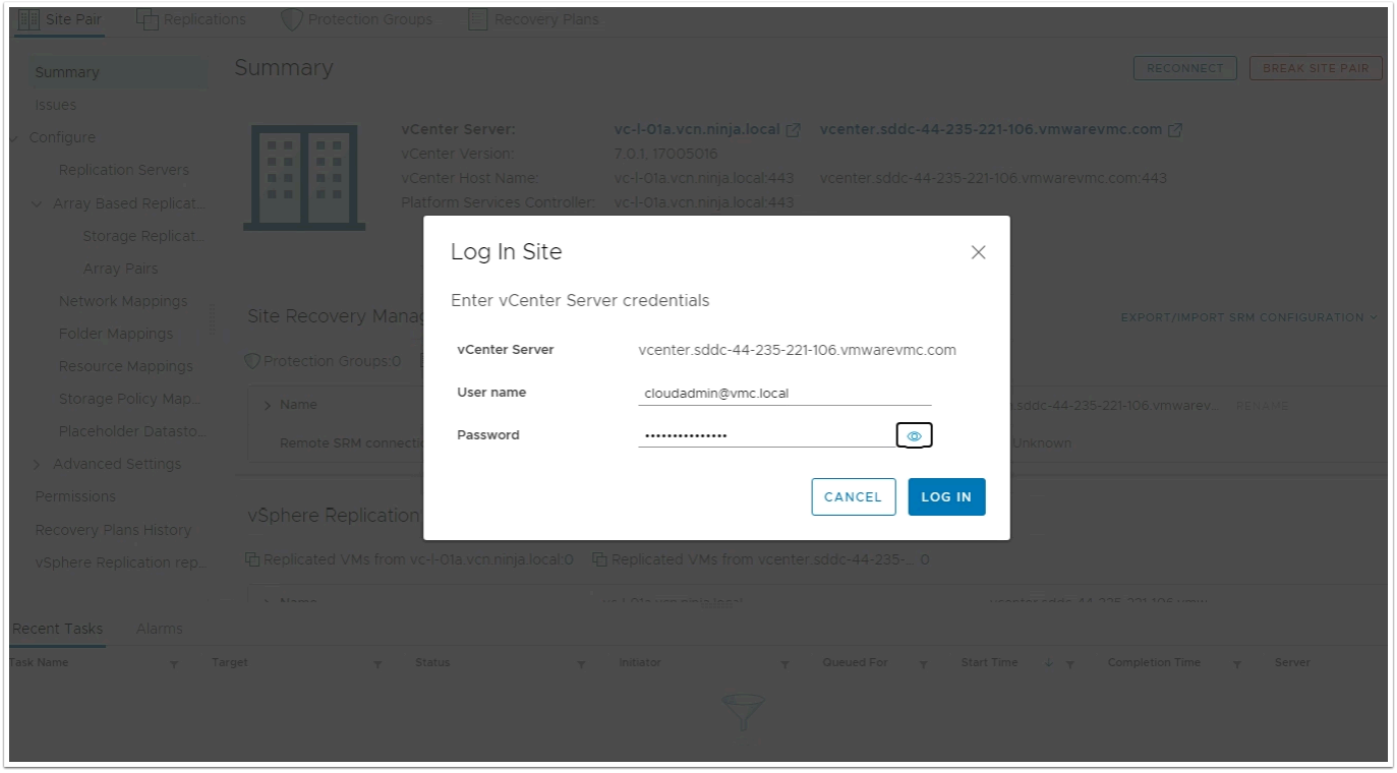


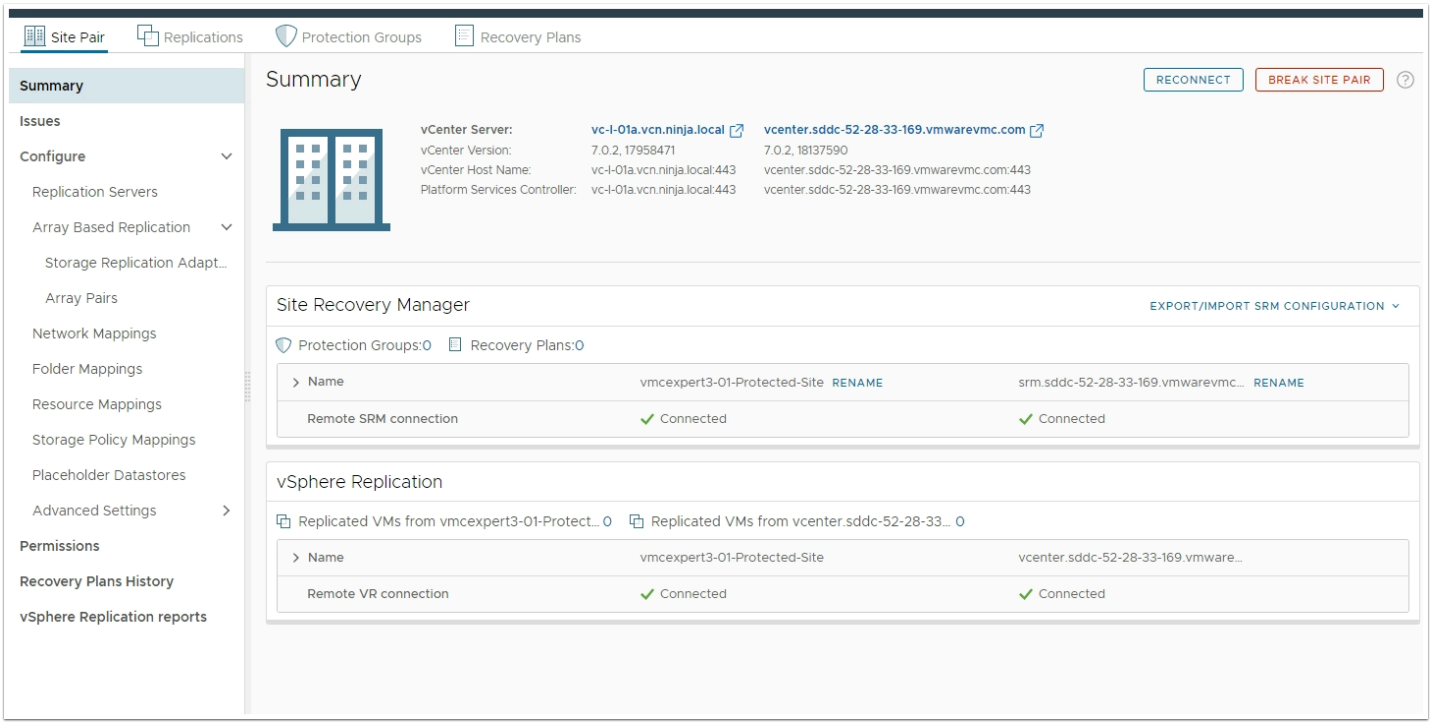
Task 5 - Configure DR for Virtual Machines

Now that we have successfully deployed and configured the SRM infrastructure components, Configured firewall rules to allow communications between the On-Premises appliances and SDDC appliance, and completed the site pairing, we can now begin the process of protecting your Virtual Machines.

1. In The Site Recovery UI Click View Details under your Site Pair
2. When prompted enter your SDDC cloudadmin credentials
   - User name: **cloudadmin@vmc.local**
   - Password: <**your cloud admin password**>







Task 5.1 - Create a Network Segment in SDDC

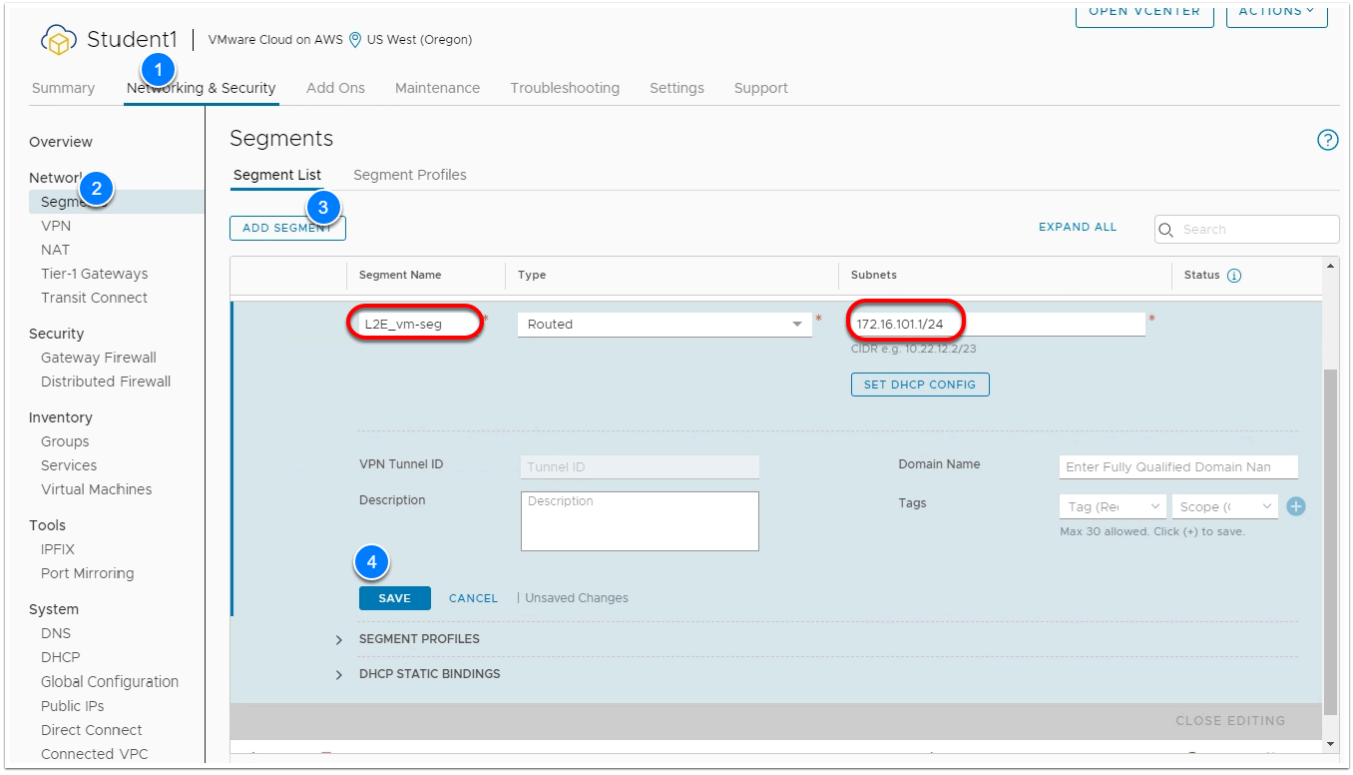
ONLY PERFORM THIS TASK IF YOU SKIPPED THE HCX LAB OR YOUR NETWORK EXTENSION OF vm-seg WAS UNSUCCESSFUL!!!

If you created a functional network Extension for vm-seg during the HCX lab (Lab 8 - Part 2, Task 2), skip this task and move on to Task 5.1.1 instead.

If you successfully complete all HCX lab tasks you should skip this task and proceed with task 5.1.1

HCX is not a requirement for SRM. It does however enhances your Disaster recovery solution by eliminating the need to pre-create networks in the SDDC and potentially re-IP'ing your vms as part of the recovery process.

1. In the VMC SDDC Console Select your SDDC, Click **View Details**
2. Click **Networking & Security**
3. Click **Segments**
4. Click **ADD SEGMENT**
5. Configure the Segment as follows:
   - Name: **L2_vm-seg**
   - Subnets: **172.16.101.1/24**
6. Click **SAVE**



Task 5.1.1 - Configure Network Mappings

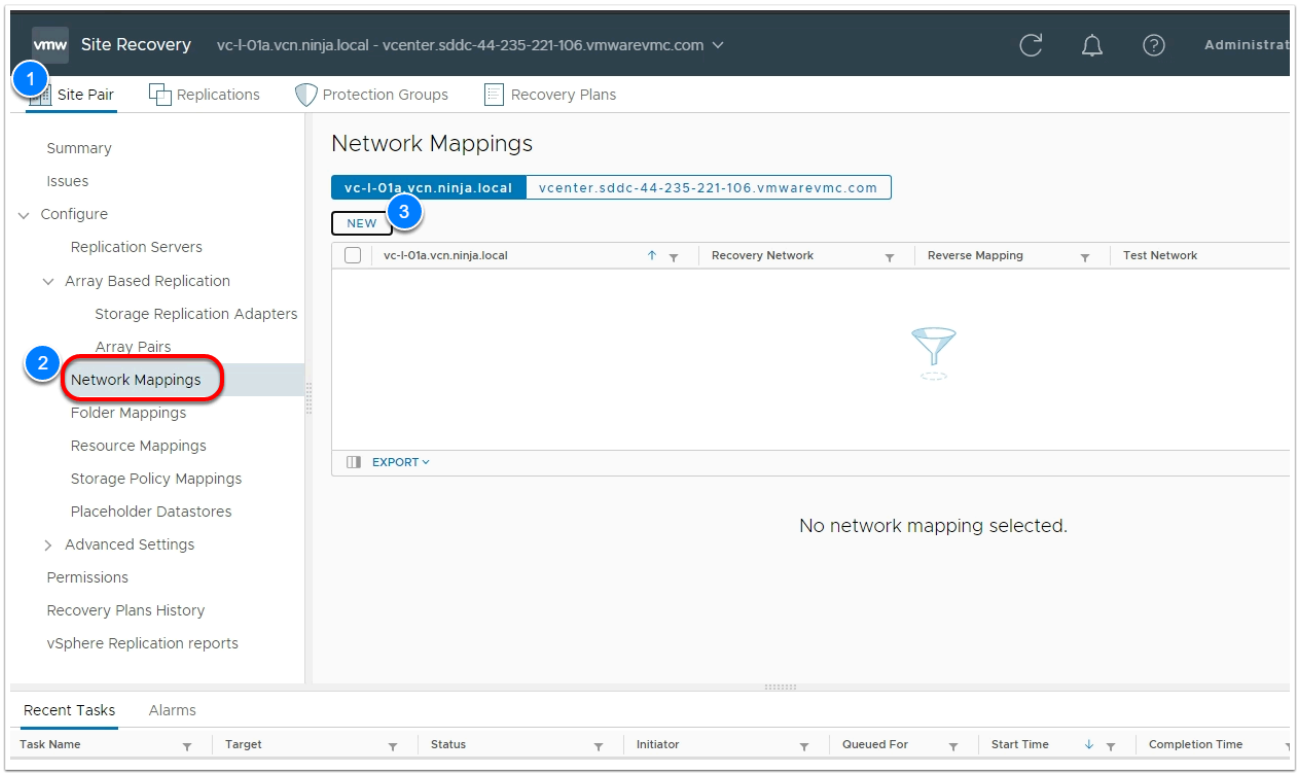
In Site Recovery manager, Mappings allow you to specify how Site Recovery Manager maps virtual machine resources on the protected site to resources on the recovery site.

You can configure site-wide mappings to map objects in the vCenter Server inventory on the protected site to corresponding objects in the vCenter Server inventory on the recovery site.

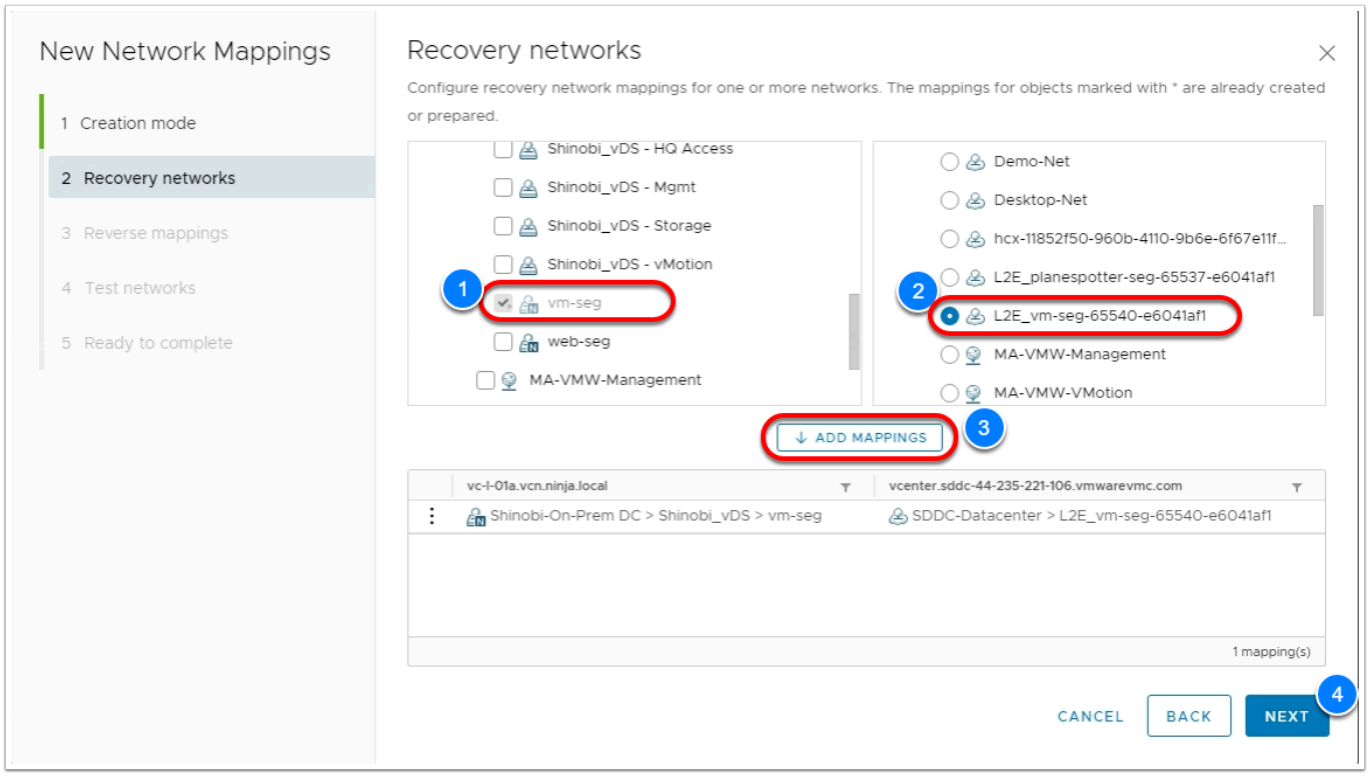
- Networks, including the option to specify a different network to use for recovery plan tests
- Data centers or virtual machine folders
- Compute resources, including resource pools, standalone hosts, vApps, or clusters
- Storage Policy

During a recovery, when virtual machines start on the recovery site, the virtual machines use the resources on the recovery site that you specify in the mappings. To enable bidirectional protection and reprotect, you can configure reverse mappings, to map the objects on the recovery site back to their corresponding objects on the protected site. You can also configure different mappings in the opposite direction, so that recovered virtual machines on a site use different resources to protected virtual machines on that site.

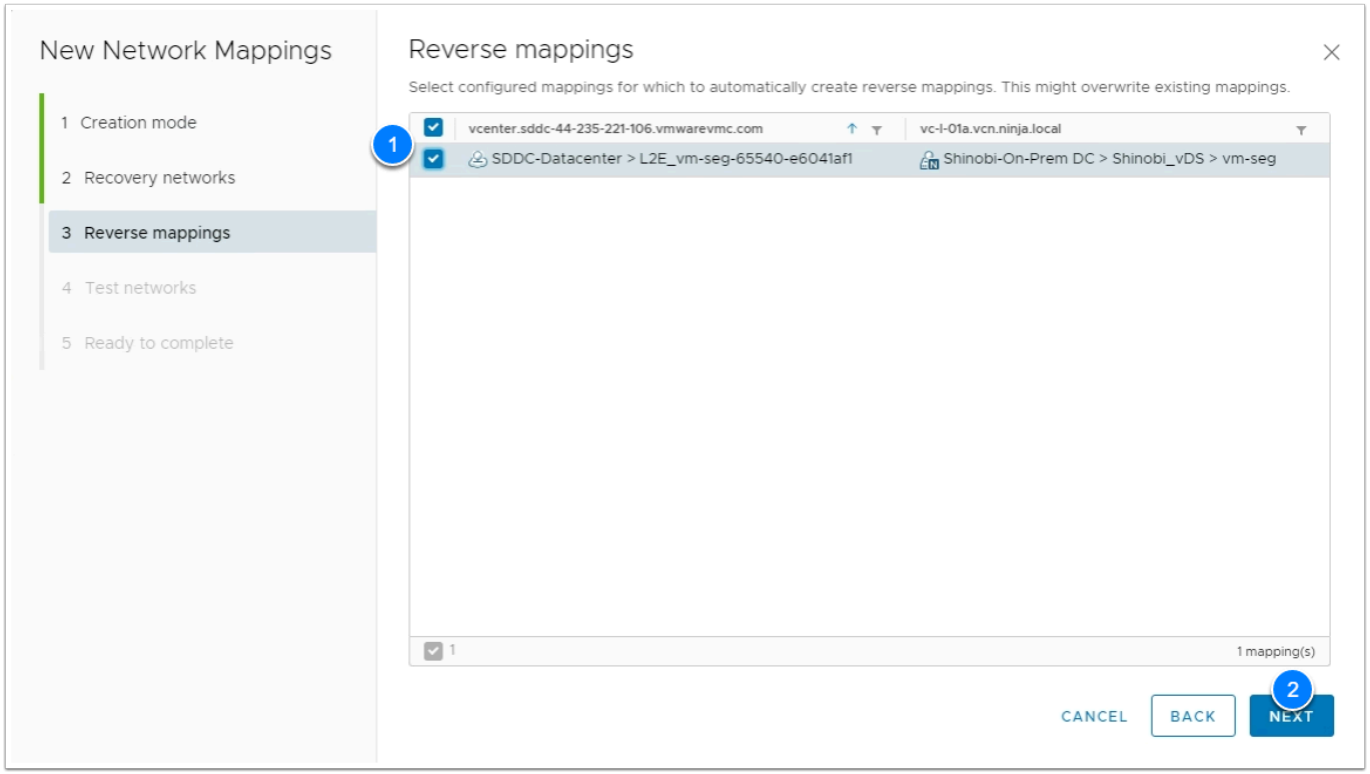
1. Click **View Details** under the new site pair if you have not previously done that
2. In the 2nd menu bar, Ensure that you have clicked **Site Pair**
3. In the left pane under the **Configure** section click **Network mappings**
4. In the right pane click **NEW**



5. In the **Creation Mode** page select **Prepare mappings manually** then **Next**
6. In the **Recovery Networks** page left details pane expand **Shinobi-On-Prem DC** then expand **Shinobi_vDS** then select **vm-seg**
7. In the **Recovery Networks** page right details pane expand **SDDC-Datacenter --> vmc-hostswitch** then select **L2E_vm-seg-###-x#x#** (or **L2E_vm-seg**, if you performed task 5.1)
8. Click the **ADD MAPPINGS** button and the mapping will appear in the bottom details pane
9. Click **NEXT**

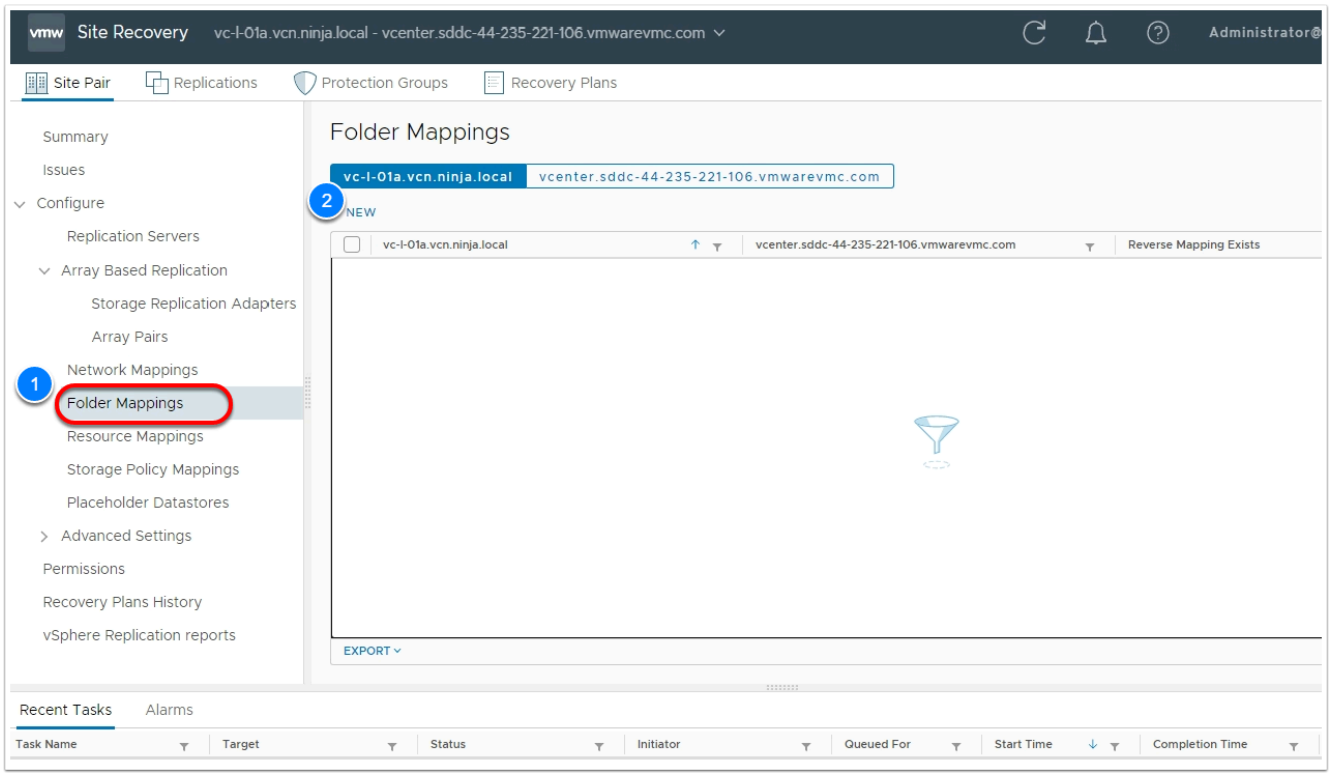


10. On the **Reverse Mappings** page **select** the mapping for any reverse mapping
11. Click **NEXT**
12. On the **Test Networks** page you will notice that SRM auto-created an isolated network for running a failover test click **Next**
13. Click **FINISH**

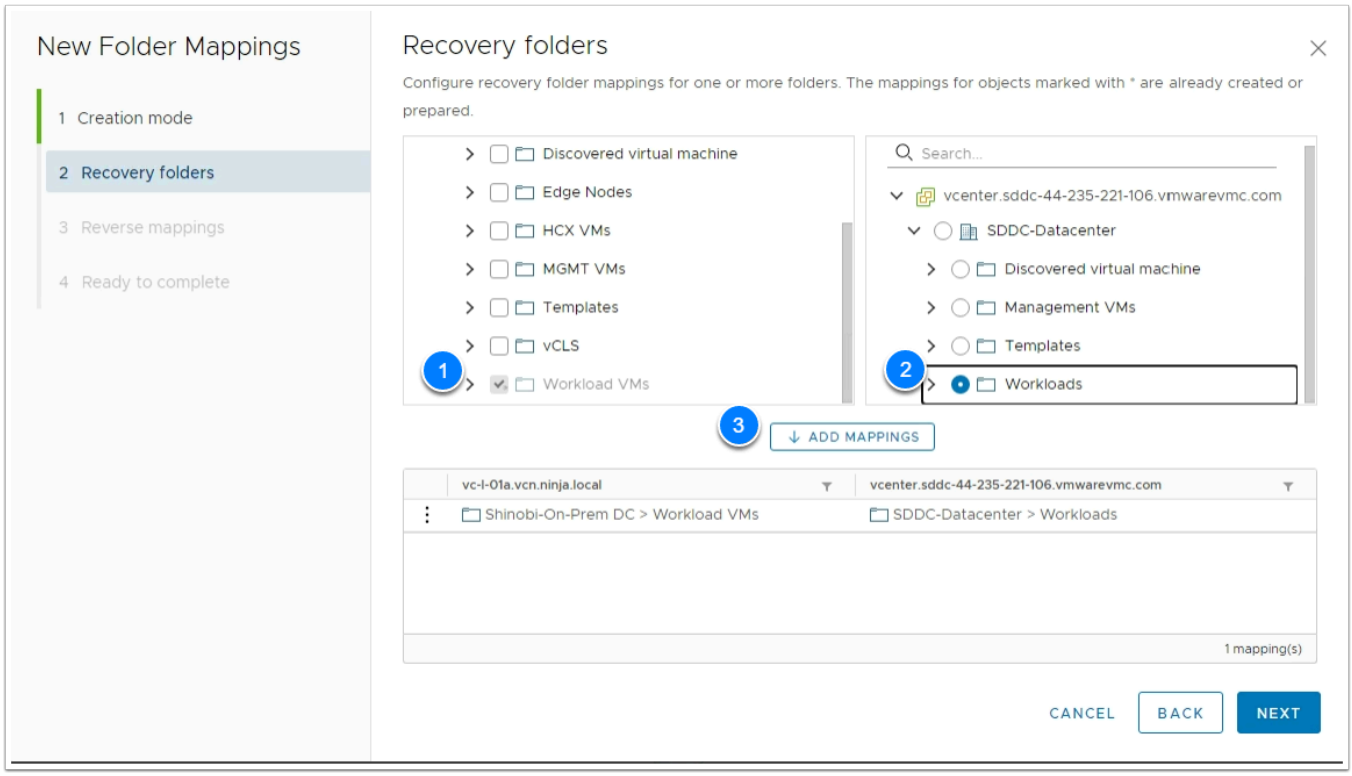


Task 5.1.2 - Configure Folder Mappings

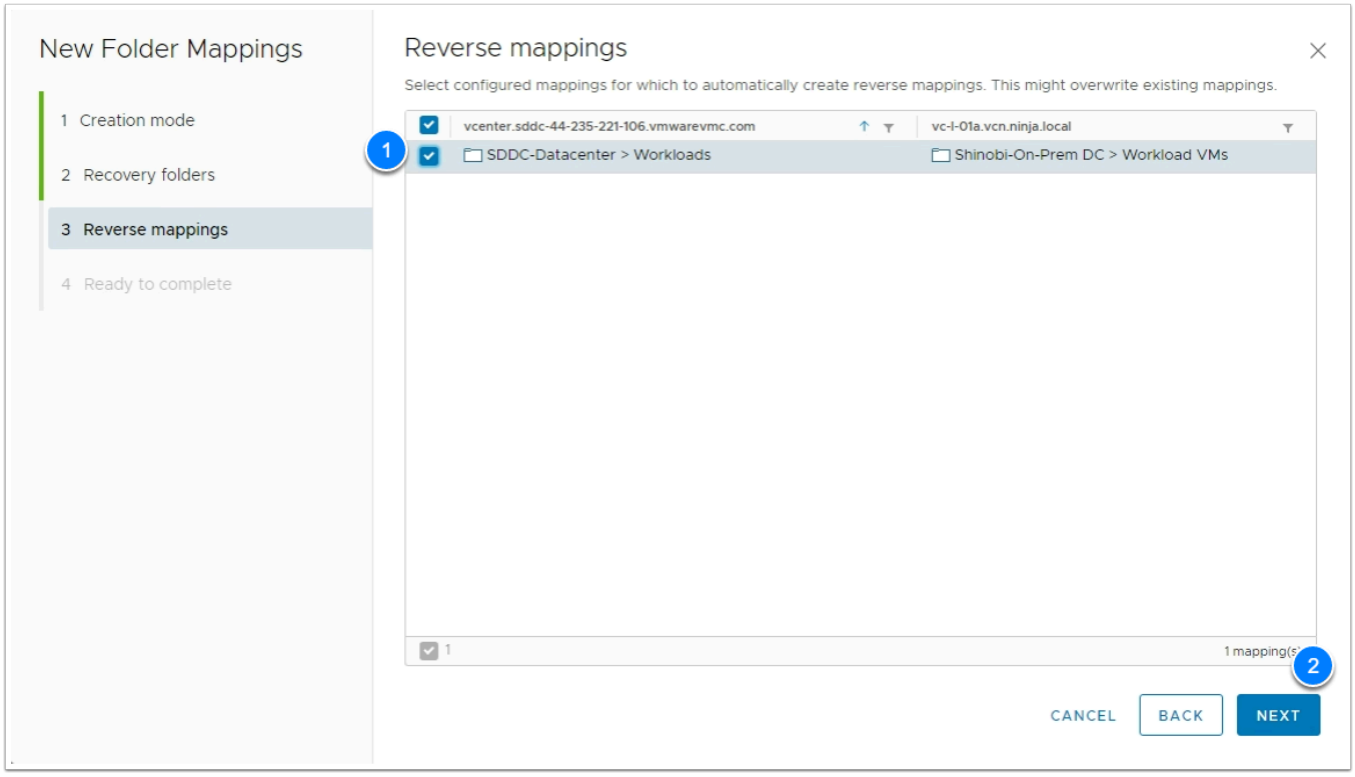
1. In the Left Menu Click **Folder Mappings**
2. In the right pane Click **NEW**
3. In the **Creation Mode** page Select **Prepare mappings manually**



4. In the **Recovery Folders** page in the left details pane expand **Shinobi-On-Prem DC**
5. Select **Workload VMs**
6. In the **Recovery Folders** page in the right details pane expand **SDDC-Datacenter**
7. Select **Workloads**
8. Click **ADD MAPPINGS** then click **NEXT**

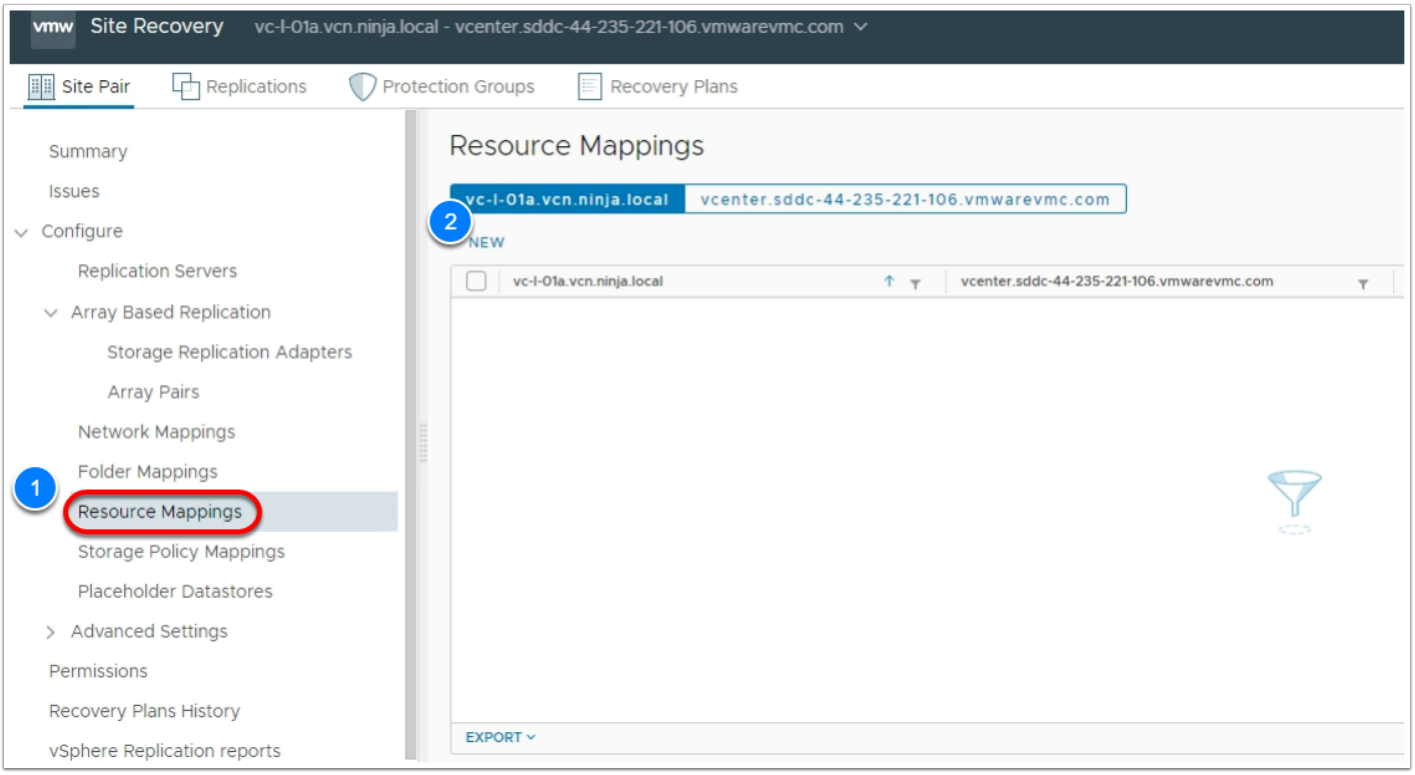


9. In the **Reverse Mappings** page **Select** the mapping for Reverse Folder mapping
10. Click **NEXT**
11. Click **FINISH**

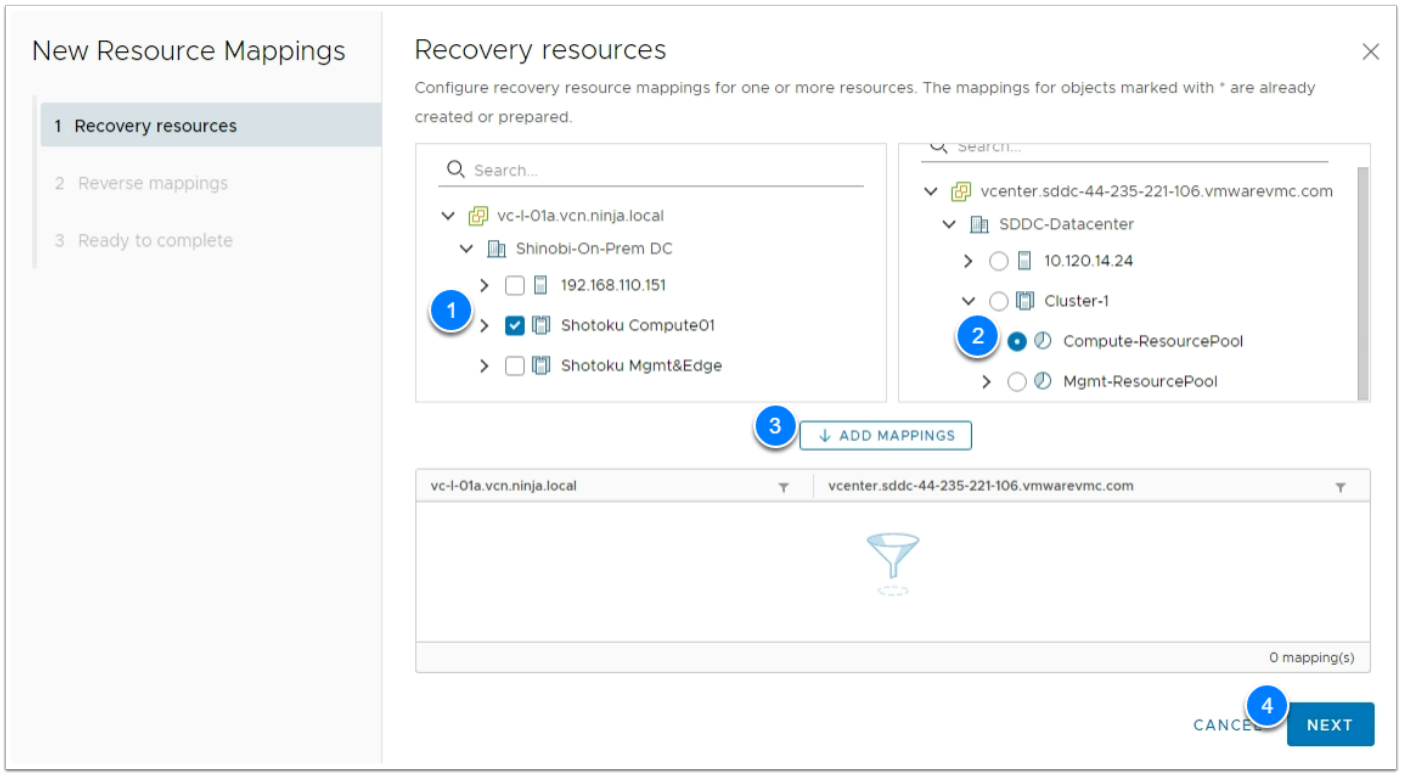


Task 5.1.3 - Configure Resource Mappings

1. In the Left Menu Click **Resource Mappings**
2. In the right pane Click **NEW**

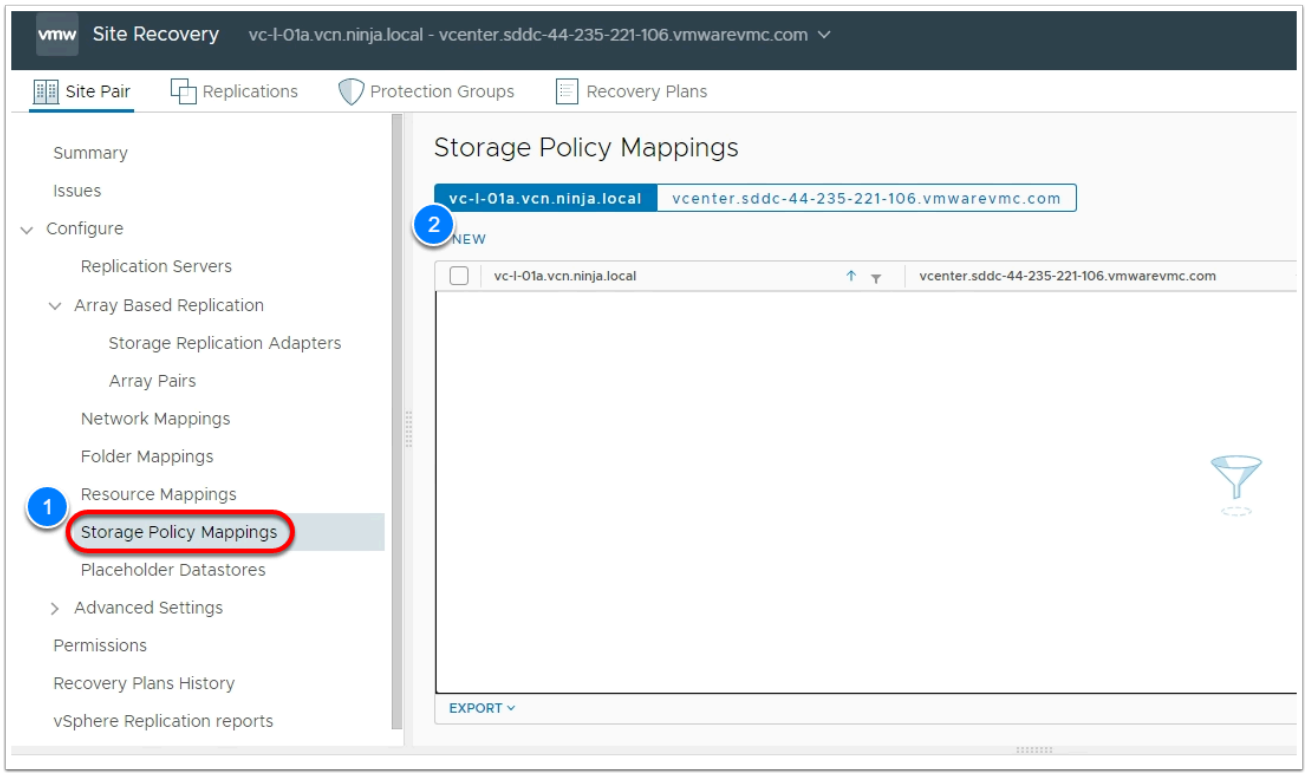


3. In the **Recovery Resources** page in the left details pane expand **Shinobi-On-Prem DC**
4. Select **Shotoku Compute01**
5. In the **Recovery Resources** page in the right details pane expand **SDDC-Datacenter**
6. Expand **Cluster-1**
7. Select **Compute-ResourcePool**
8. Click **ADD MAPPINGS** then click **NEXT**
9. **Select** the mapping for Reverse Folder mapping
10. Click **NEXT**
11. Click **FINISH**

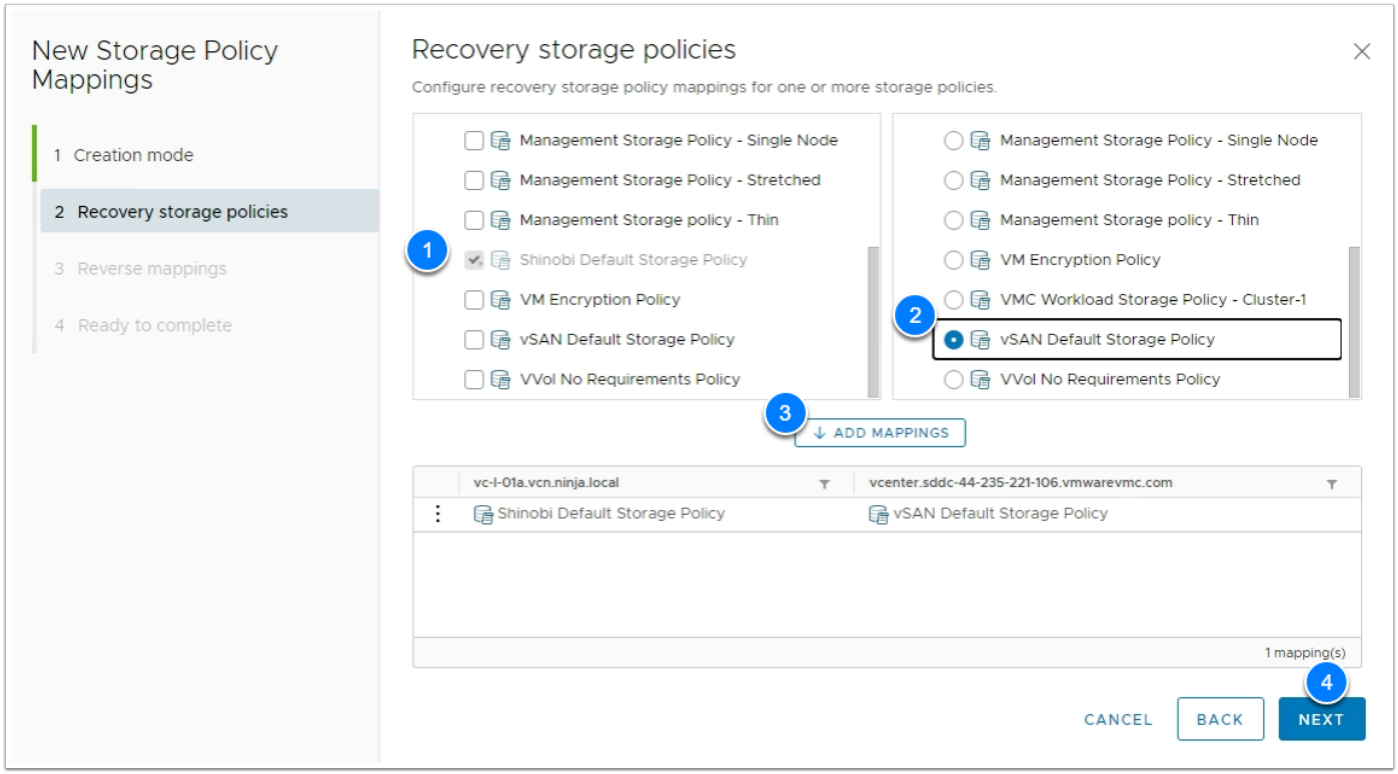


Task 5.1.4 - Storage Policy Mapping

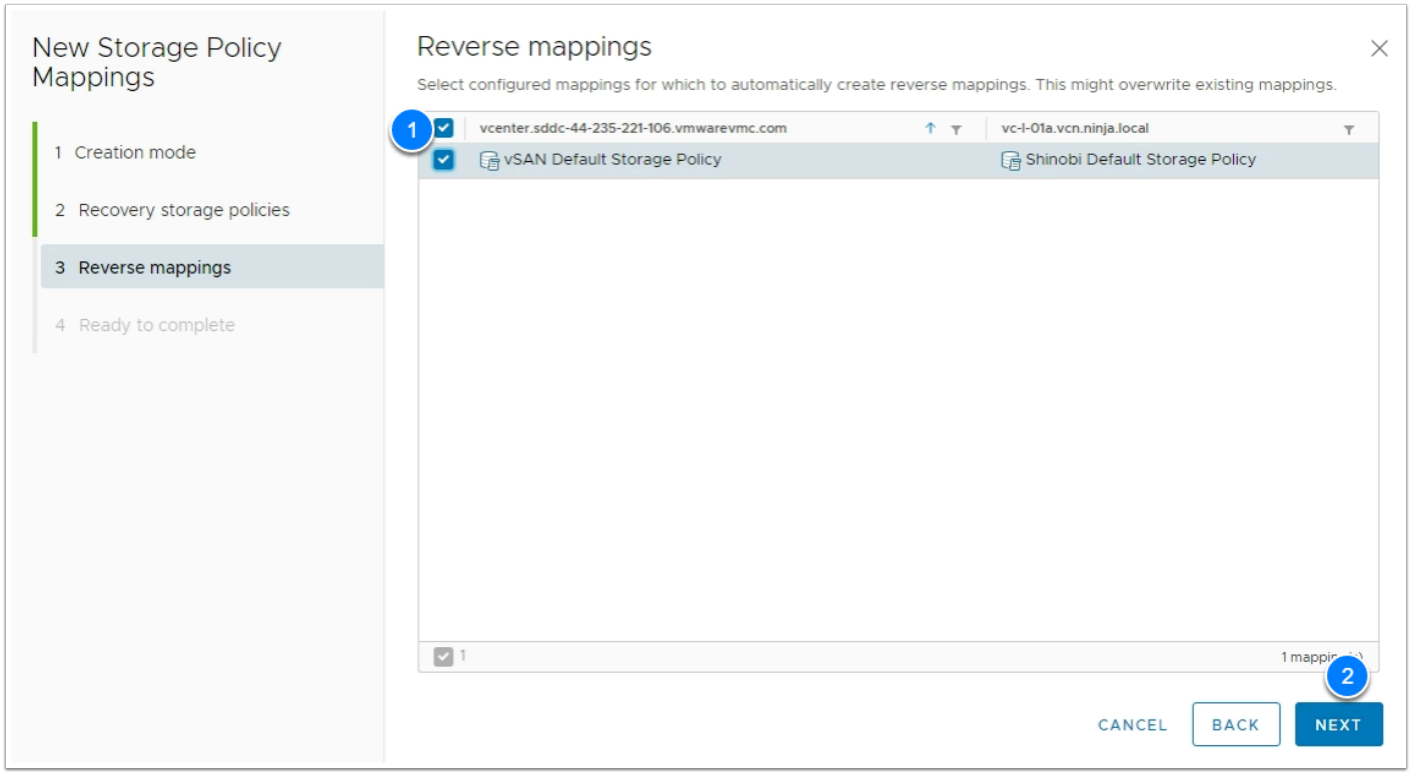
1. In the Left Menu Click **Storage Policy Mappings**
2. In the right pane Click **NEW**
3. In the **Creation Mode** page select **Prepare mappings manually**
4. Click **NEXT**



4. In the **Recovery Storage Policies** page left pane expand the on-premises dc then select **Shinobi Default Storage Policy**
5. In the **Recovery Storage Policies** page right pane expand the VMC SDDC then select **vSAN Default Storage Policy**
6. Click **ADD MAPPINGS** then click **NEXT**

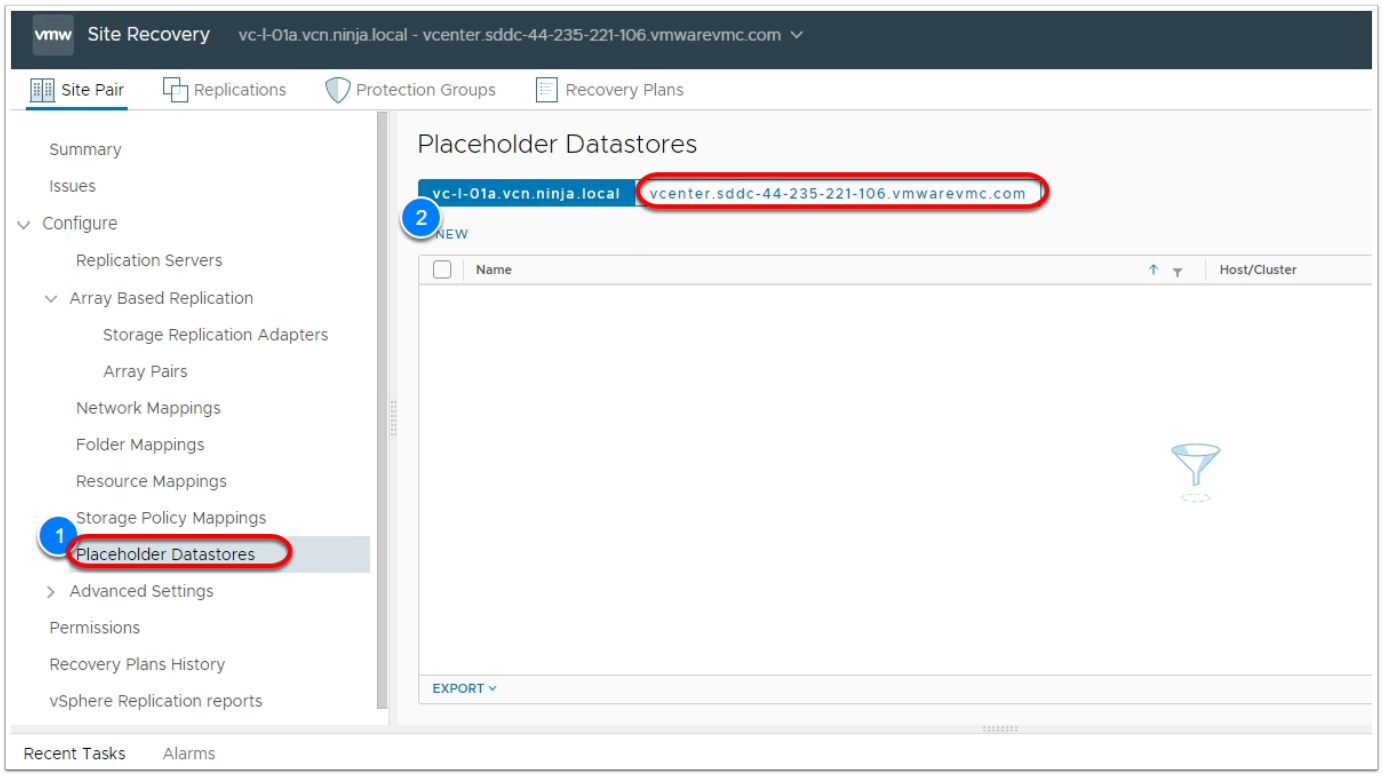


7. **Select** the mapping for Reverse Folder mapping
8. Click **NEXT**
9. Click **FINISH**



Task 5.1.5 - Placeholder Datastores

1. In the Left Menu Click **Placeholder Datastores**
2. Ensure that you are in the tab for the VMC on AWS SDDC vCenter (vcenter.sddc-xx-xx-xx-xx.vmwarevmc.com) at the top under the "Placeholder Datastores" title In the right pane Click **NEW**



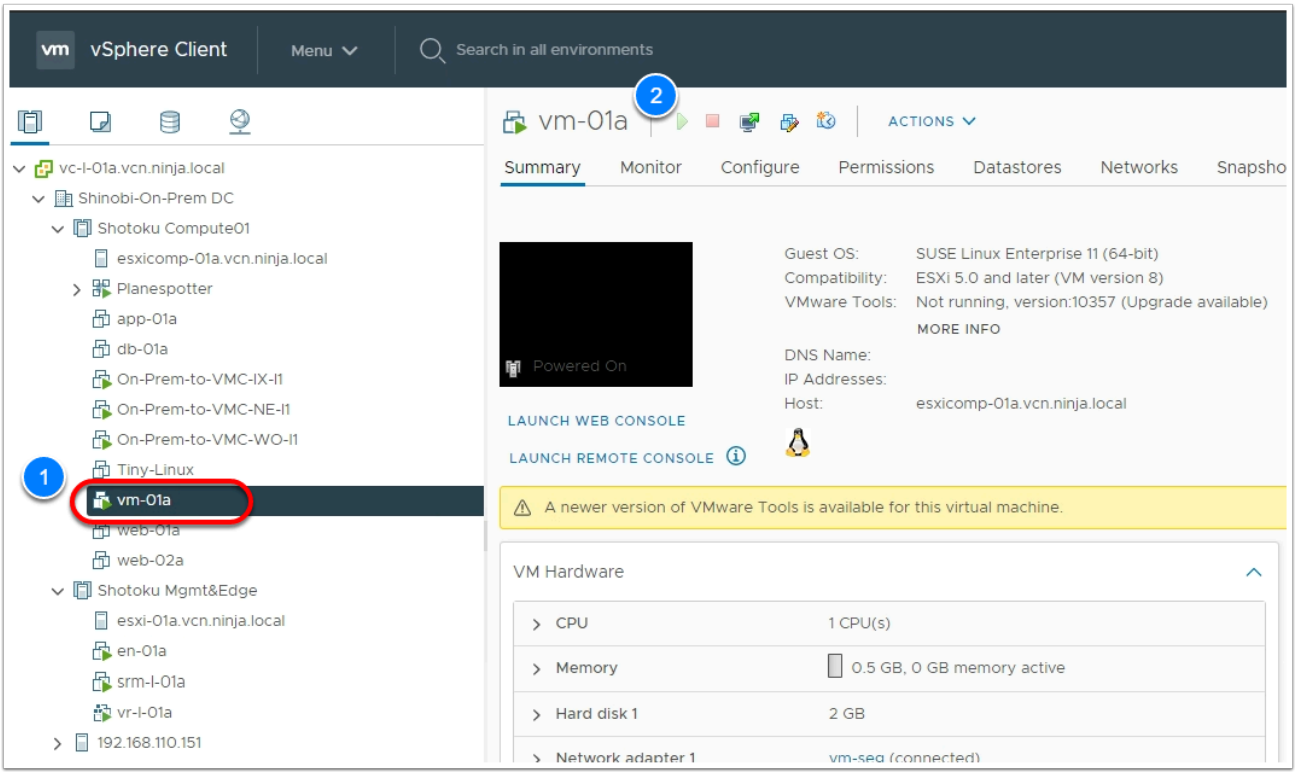
3. Select **WorkloadDatastore**
4. Click **ADD**

Task 6 - Setup Replication

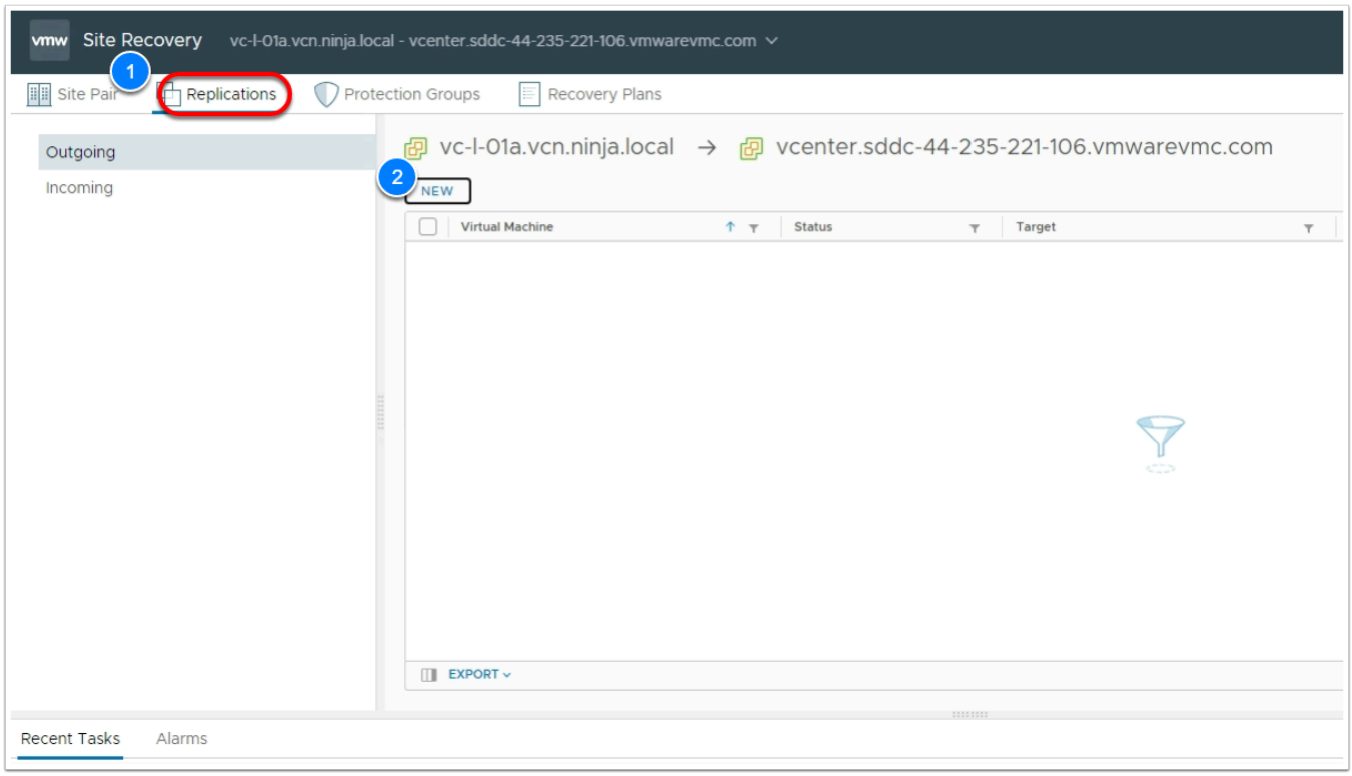
VMware Site recovery Service uses vSphere Replication to copy VMs from the protected site to the recovery site. With vSphere Replication independent replication policies can be

defined per Virtual Machine. In this task we will configure replication for a single Virtual machine

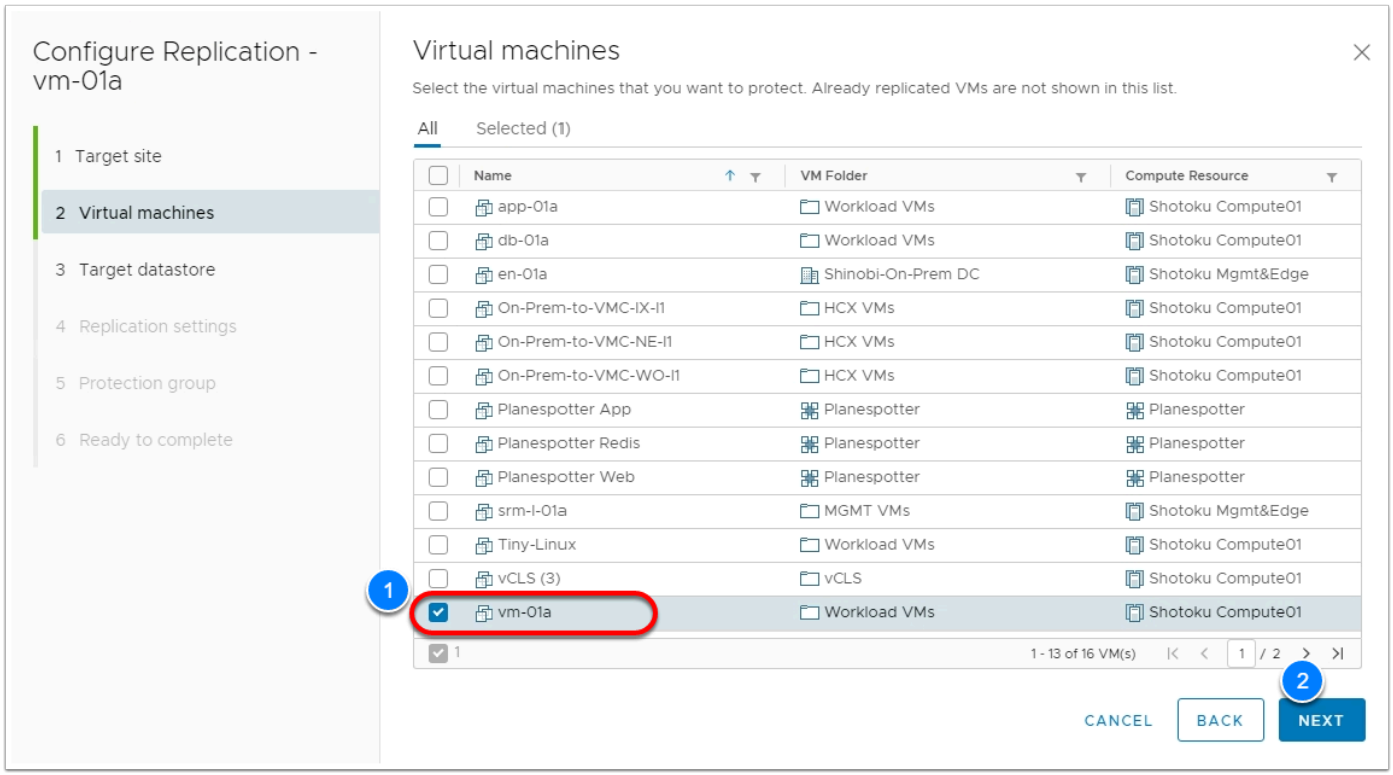
1. In the vSphere Web Client of your On-Premises vCenter Confirm the **vm-01a** is powered-on.
2. If not, select it and **Power-on**
3. **NOTE:** Powered off VMs are not replicated by vSphere Replication



4. In the On-Premises SRM UI Click the **Replications** Tab in the 2nd Menu row (See screenshot below)
5. Select the **Outgoing** menu then click **NEW**
6. On the **Target Site** page Select **Auto-Assign vSphere Replication Server**
7. Click **NEXT**

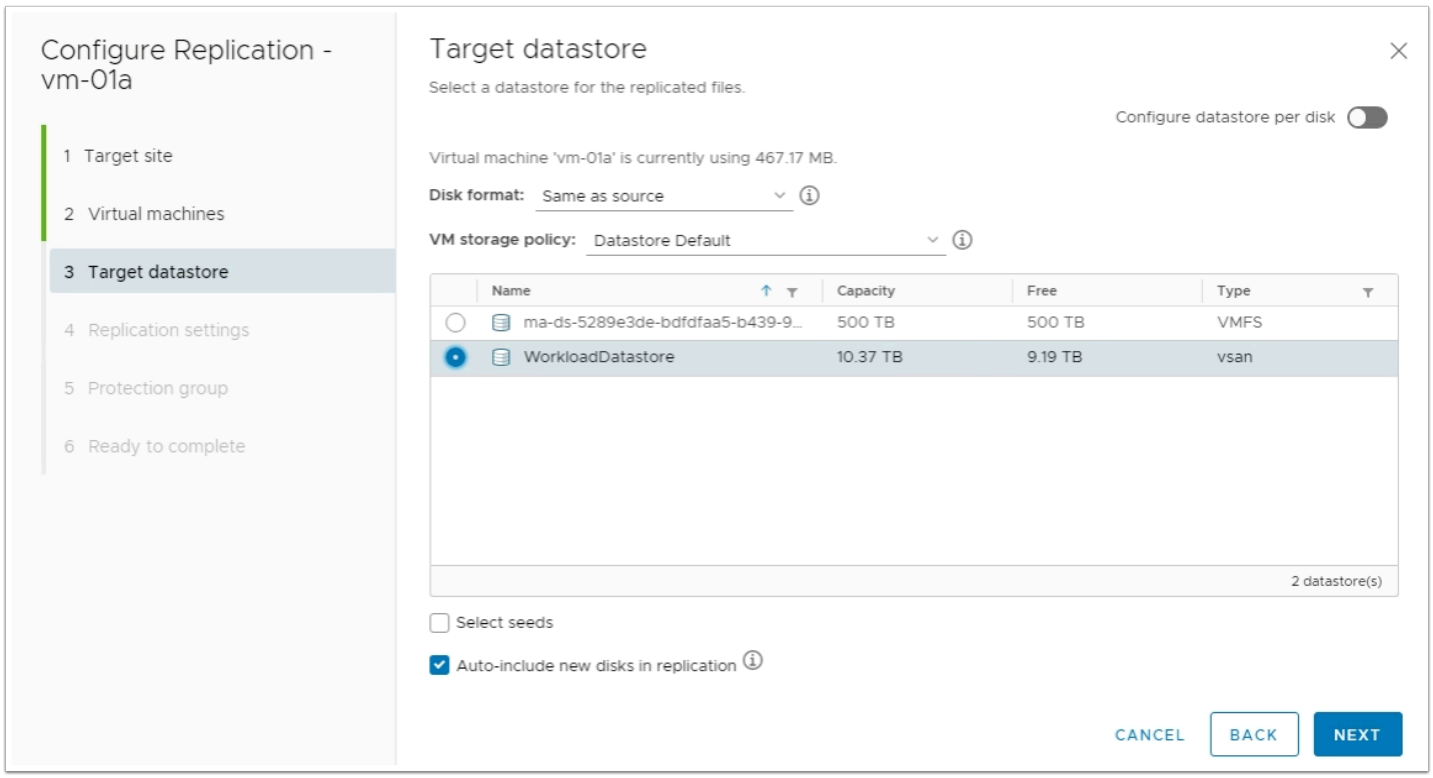


8. On the **Virtual Machines** page Select **vm-01a**
9. Click **Next**

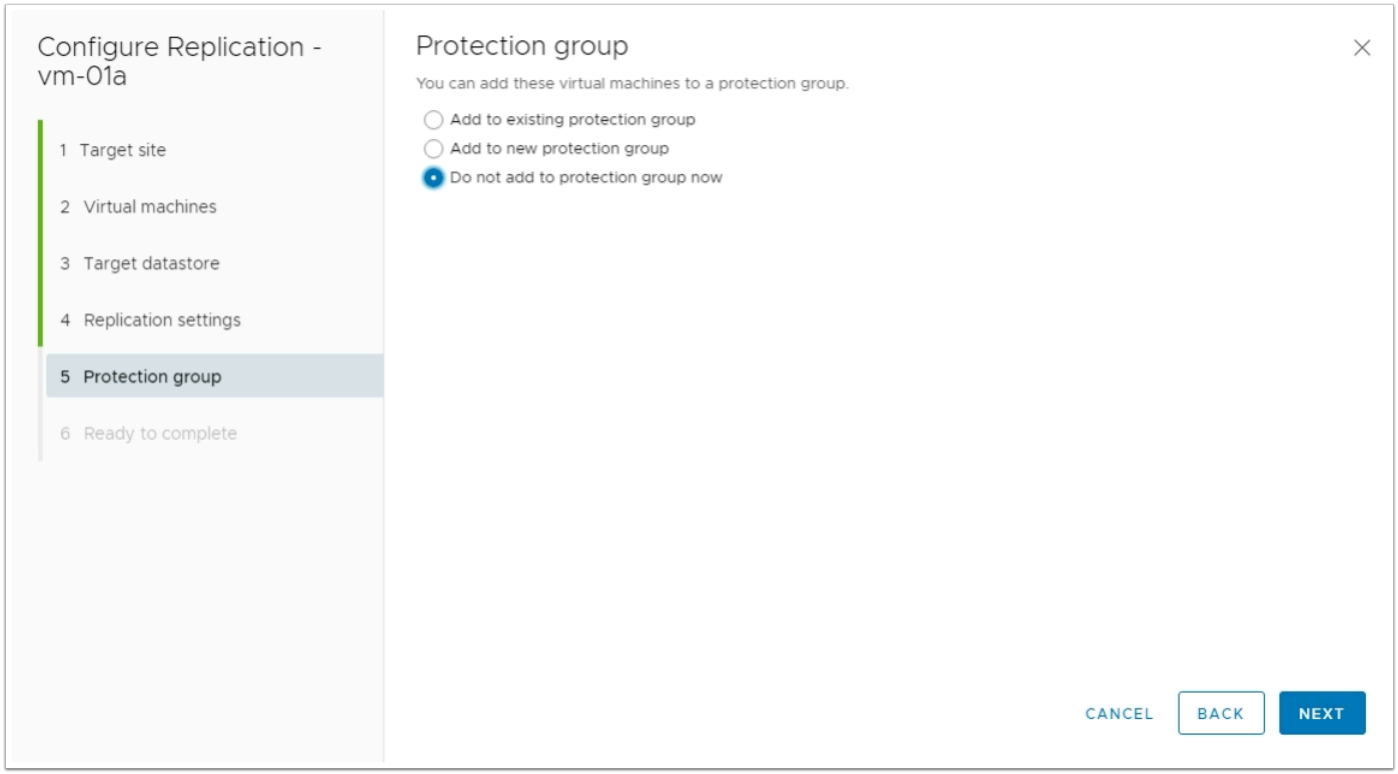


10. On the **Target Datastore** page Select **WorkloadDatastore**

11. Click **Next**
12. On the **Replication Settings** page click **Next** to accept the default RPO of 1 hour

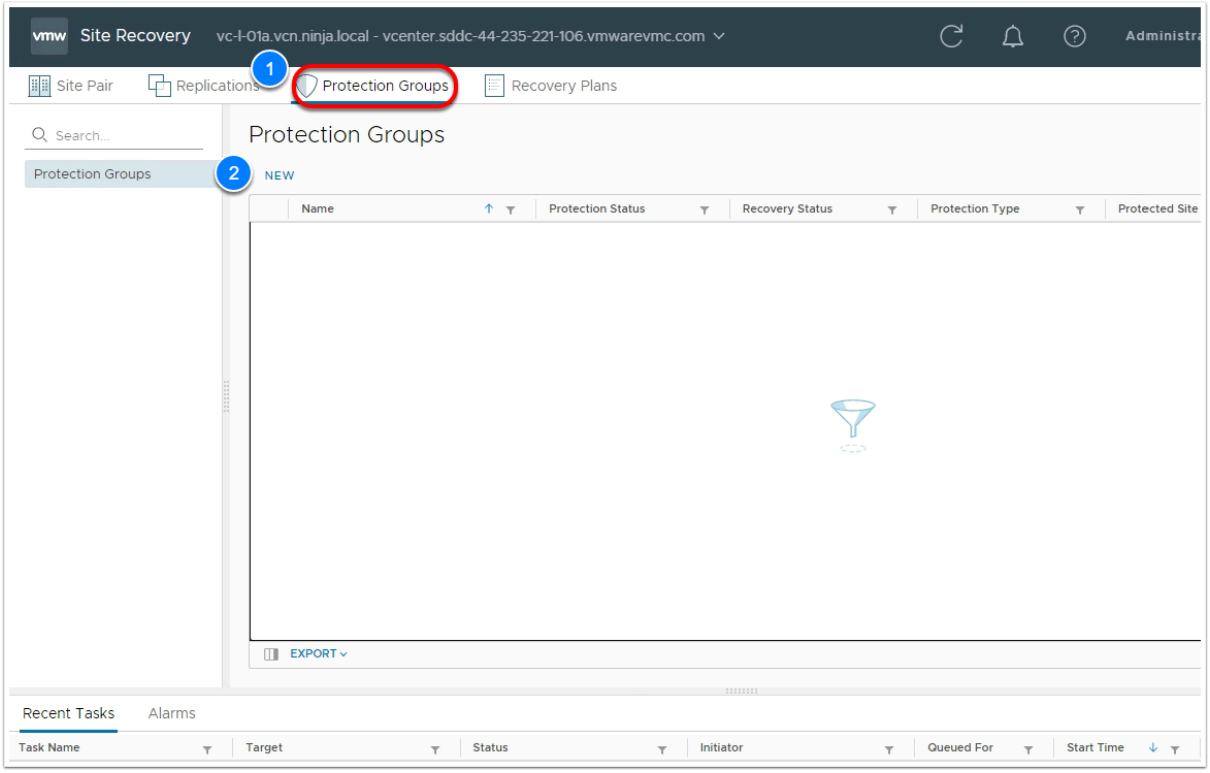


13. On the **Protection Group** page Select **Do not add protection group now**
14. Click **NEXT**
15. Click **FINISH**

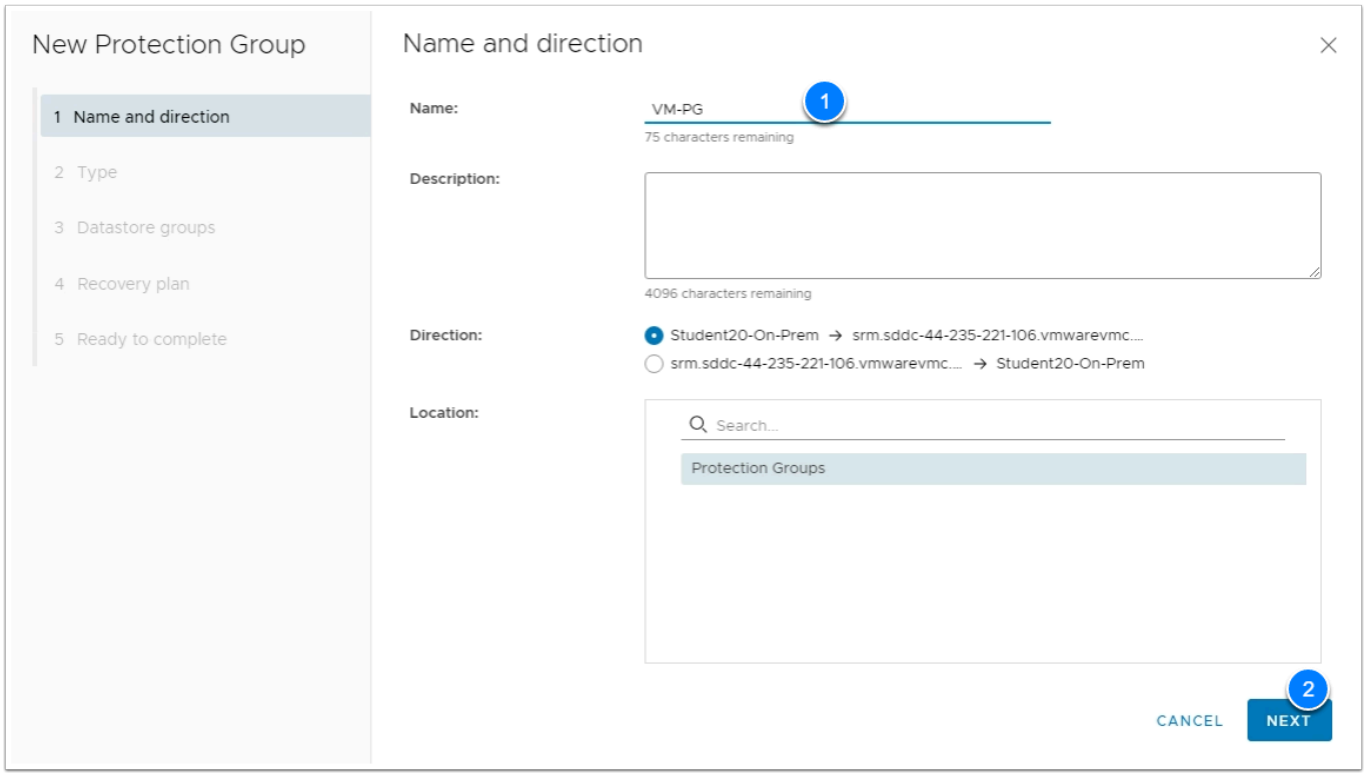


Task 6.1 - Create a Protection Group

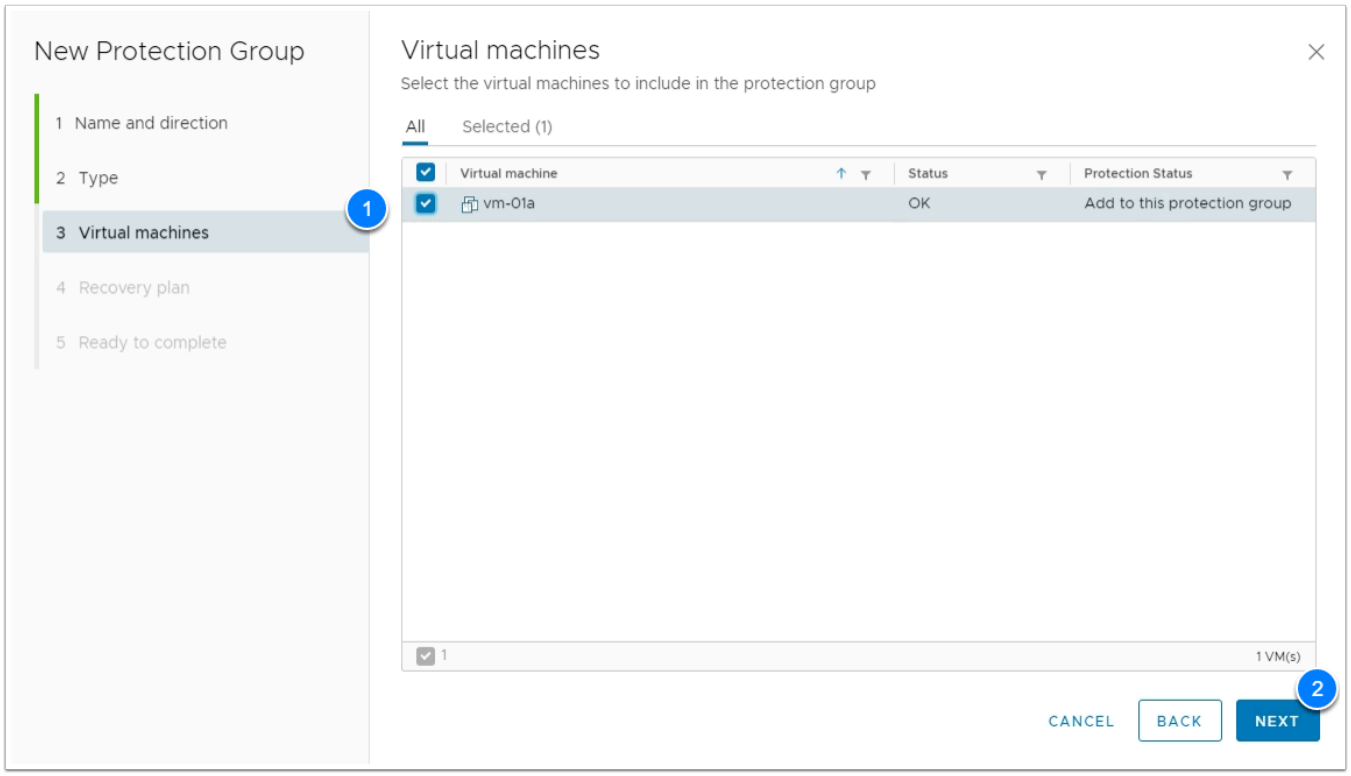
1. In the On-Premises Site Recovery Manager UI Click **Protection Groups** tab in the 2nd menu at the top
2. In the right pane click **NEW**



3. In the **Name and Direction** page enter **VM-PG** as the Name of the Protection Group
4. Click **NEXT**
5. In the **Type** page select **Individual VMs (vSphere Replication)**
6. Click **NEXT**



7. In the **Virtual Machines** page select **vm-01a**
8. Click **NEXT**
9. In the **Recovery Plan** page Select **Do not add to Recovery Plan now**
10. Click **NEXT**
11. Click **FINISH**

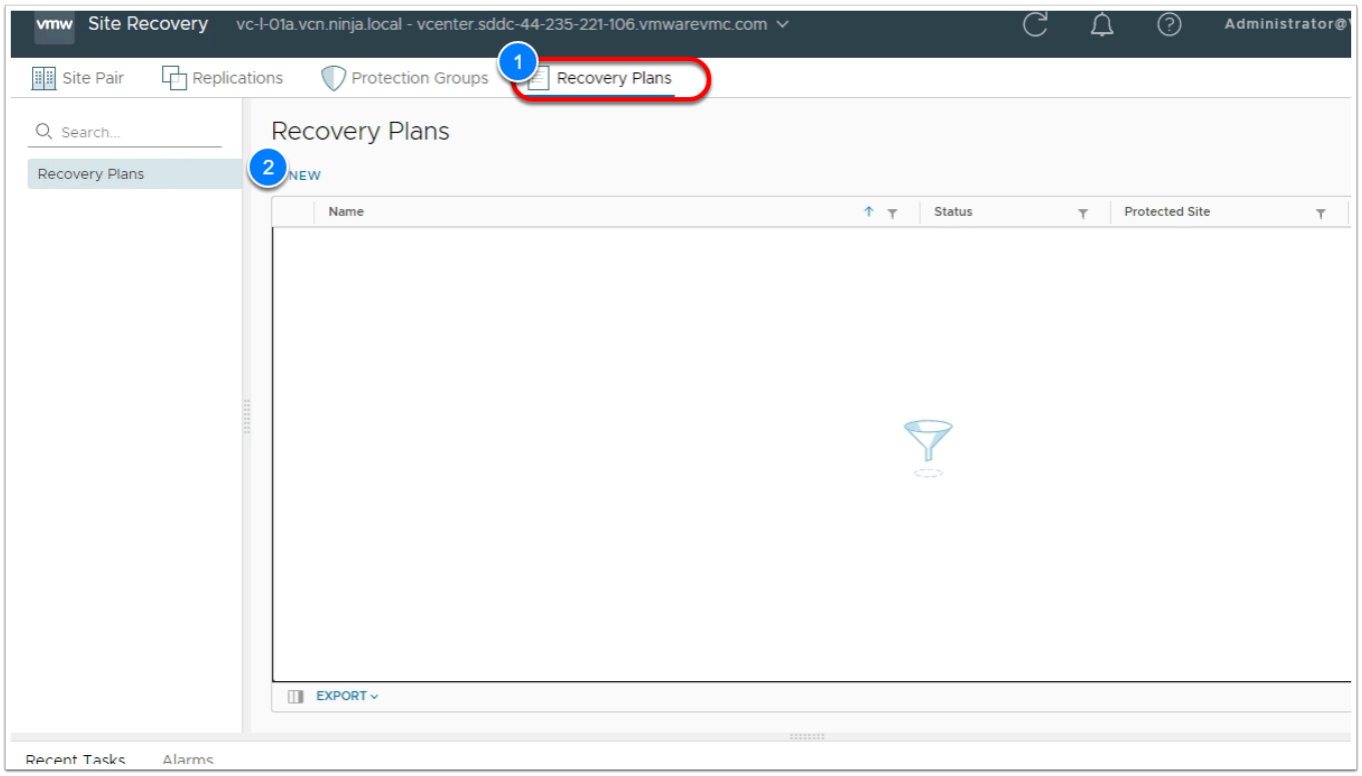


Task 6.2 - Create Recovery Plan

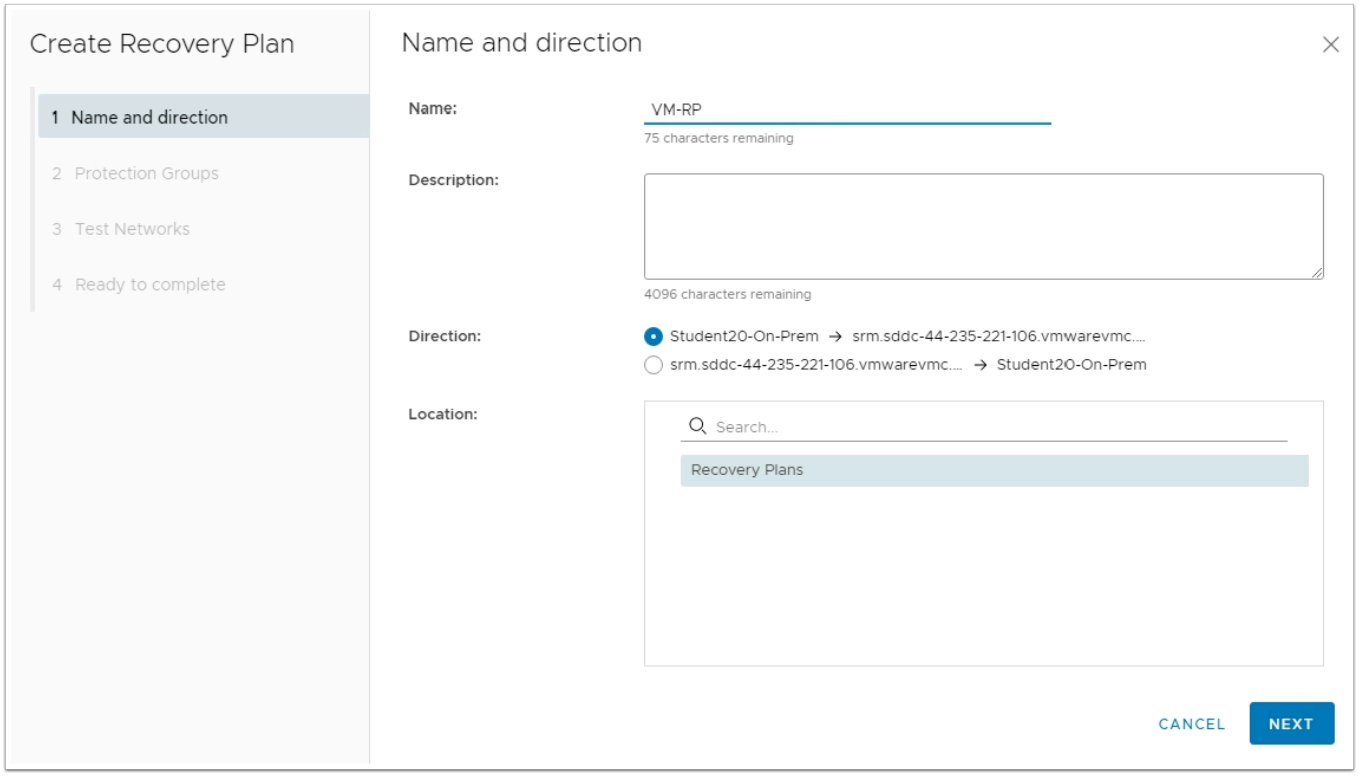
A recovery plan is like an automated run book. It controls every step of the recovery process, including the order in which Site Recovery Manager powers on and powers off virtual machines, the network addresses that recovered virtual machines use, and so on. Recovery plans are flexible and customizable.

A recovery plan can include one or more protection groups. You can include a protection group in more than one recovery plan. For example, you can create one recovery plan to handle a planned migration of services from the protected site to the recovery site for the whole organization, and another set of plans per individual departments. In this example, having these different recovery plans referencing one protection group allows you to decide how to perform recovery.

1. In the On-Premises Site Recovery Manager UI Click **Recovery Plans** tab in the 2nd menu at the top
2. In the right pane click **NEW**

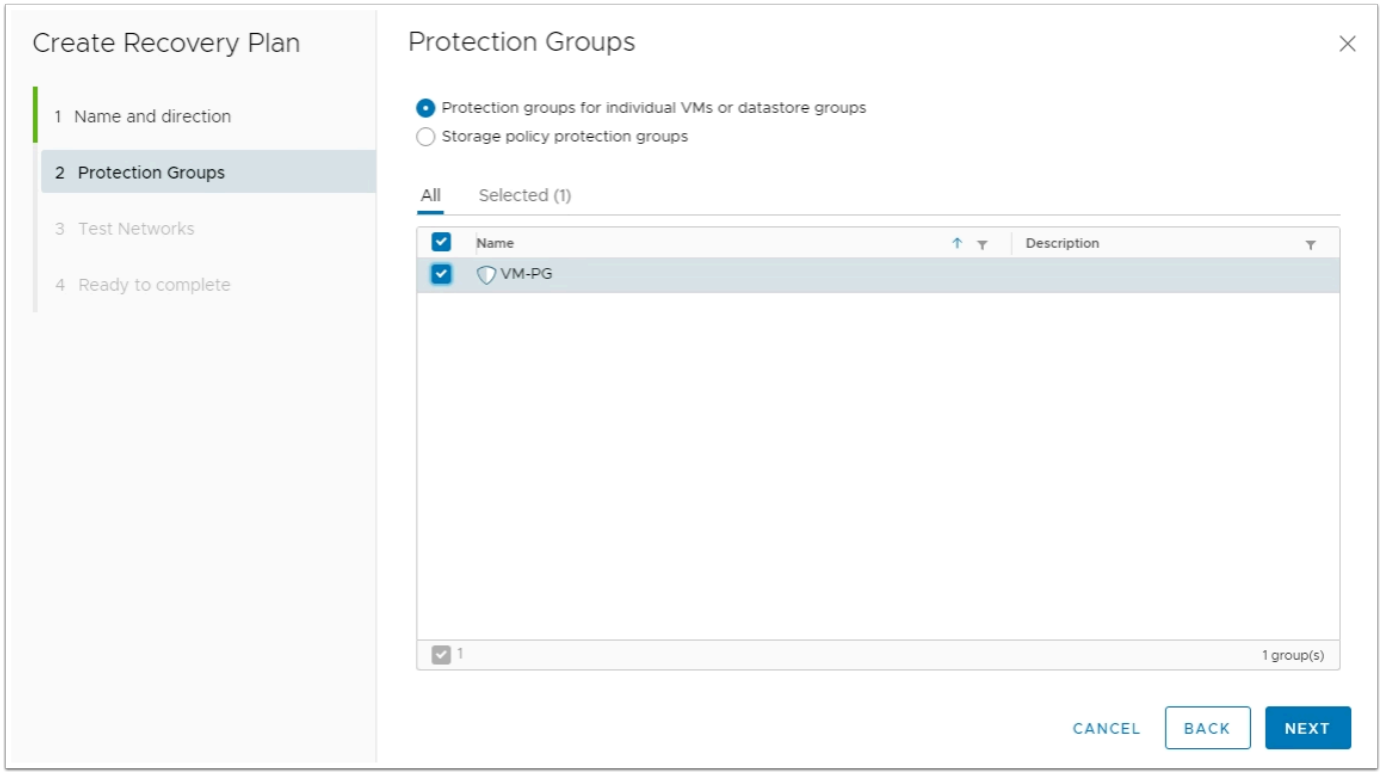


3. In the **Name and Direction** page enter **VM-RP** as the Name of the recovery plan
4. Click **NEXT**



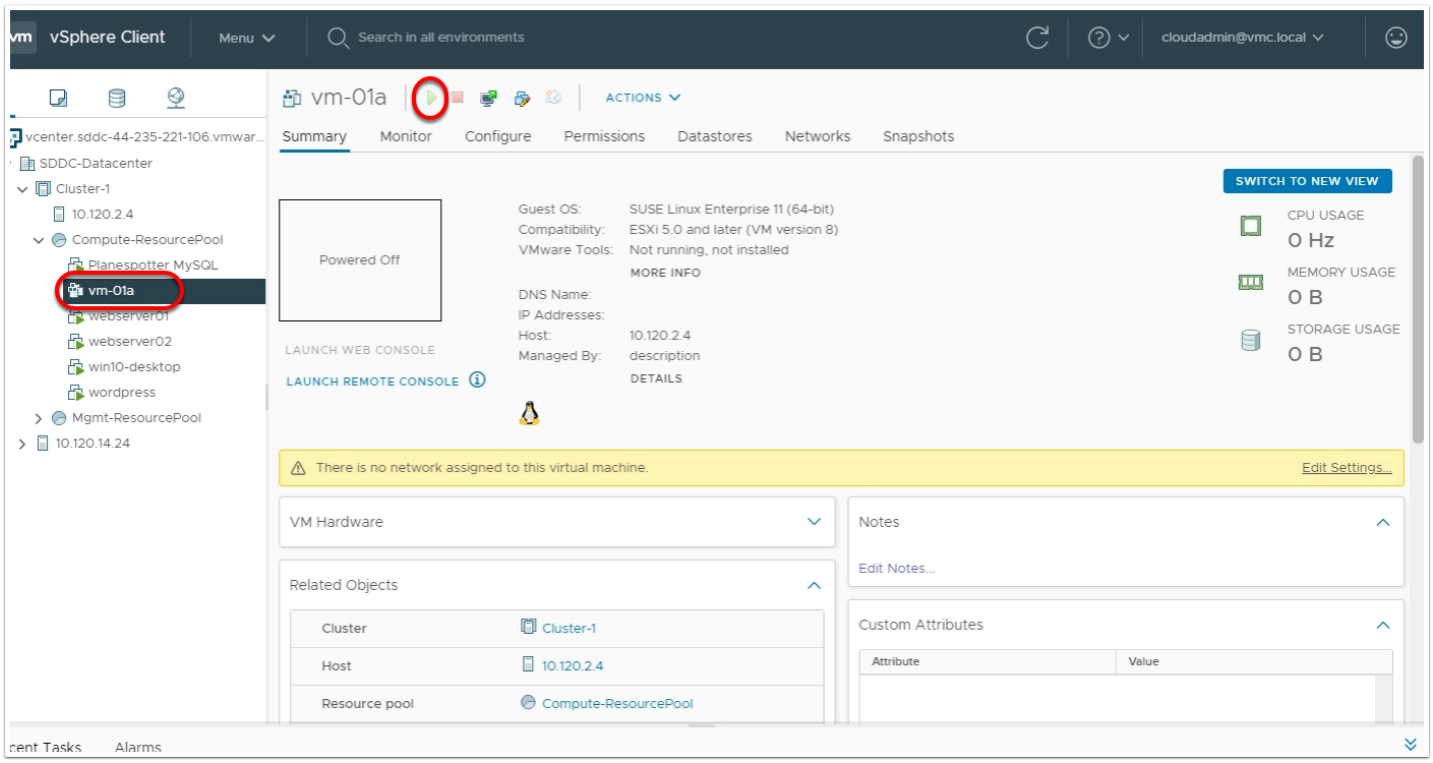
5. In the **Protection Groups** page select the **VM-PG** Protection group

6. Click **NEXT**
7. In the **Test Networks** page click **NEXT** to use the site-level network mapping for test networks
8. Click **FINISH**

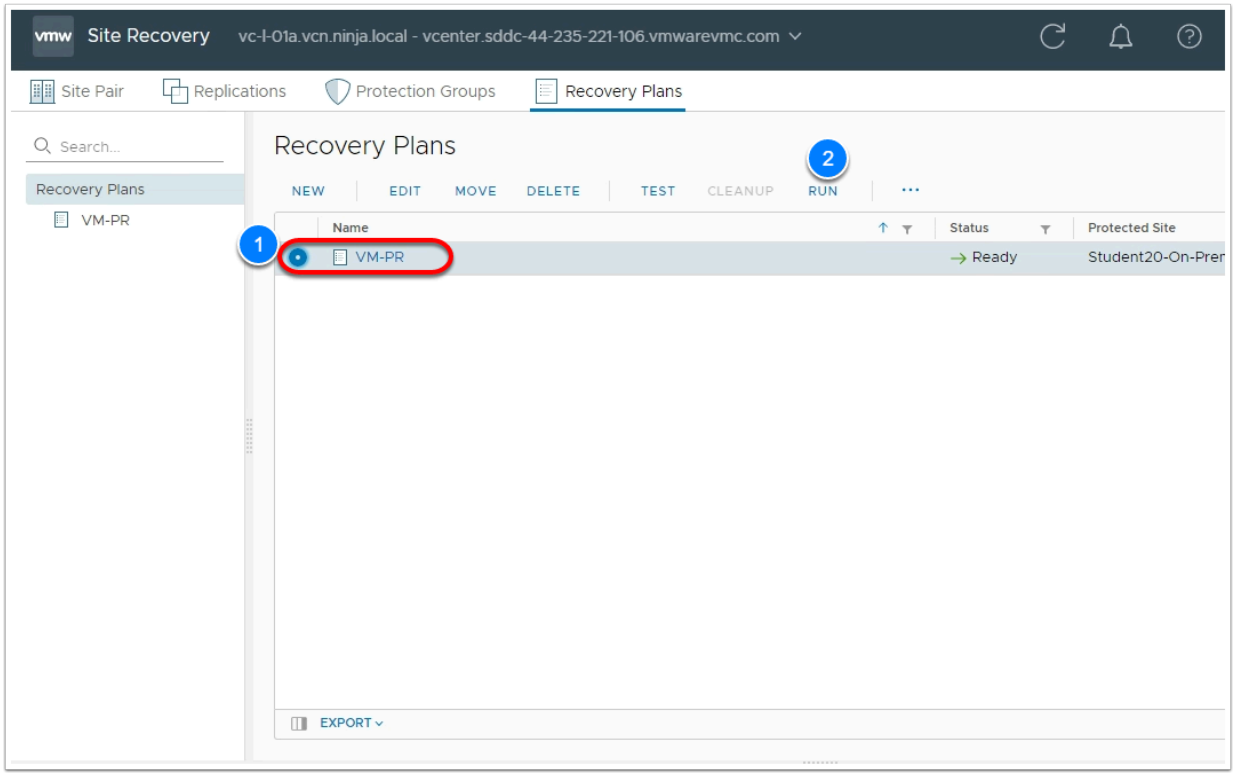


Task 7 - Run a Disaster Recovery Plan

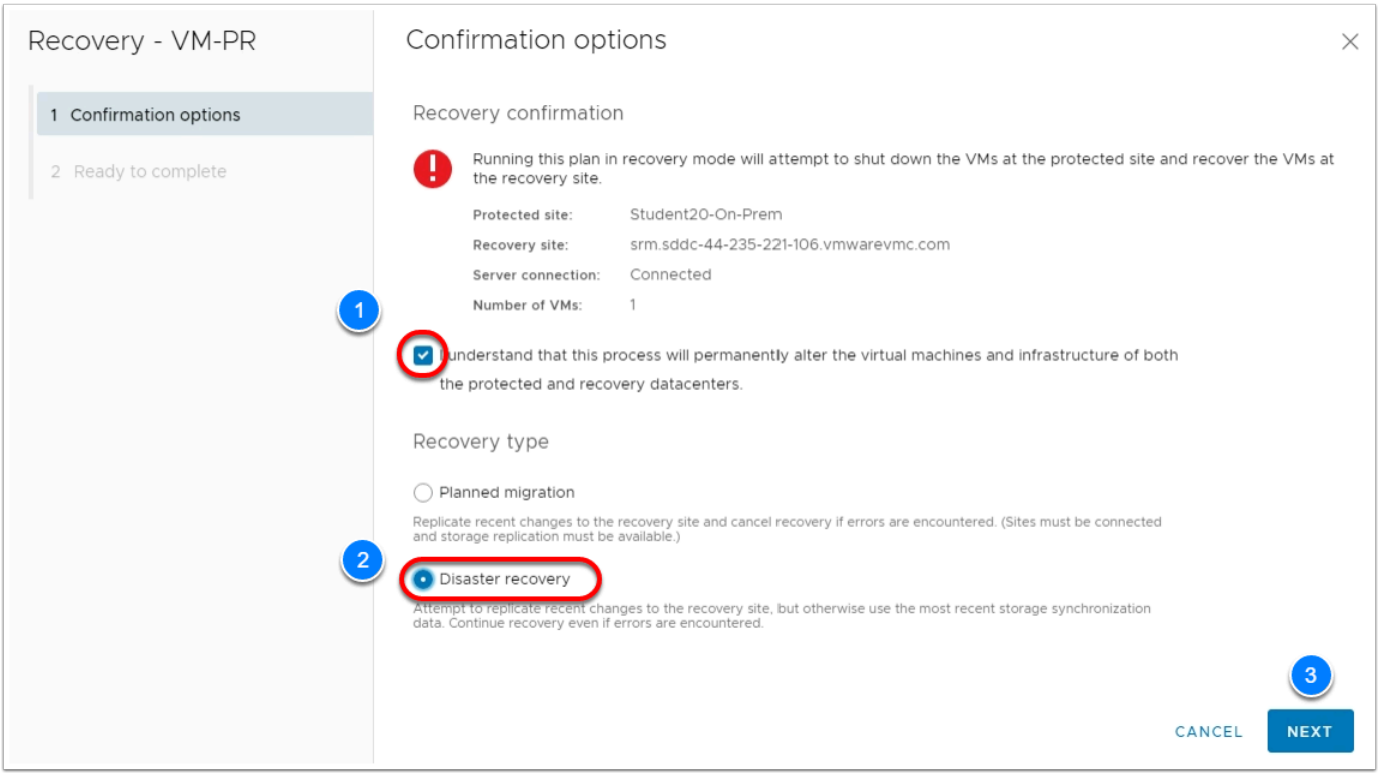
1. Log into your **VMC on AWS SDDC vCenter**.
   NOTE: The URL and credentials can be found on the Settings tab of the VMC Console
2. Confirm that there a a placeholder VM (ghost vm) for **vm-01a** (expand cluster 1 > compute RP)
   NOTE: This VM cannot be powered-on. To bring the replicated VM(s) online you have to execute an SRM
   Planned Migration or Disaster recovery execution



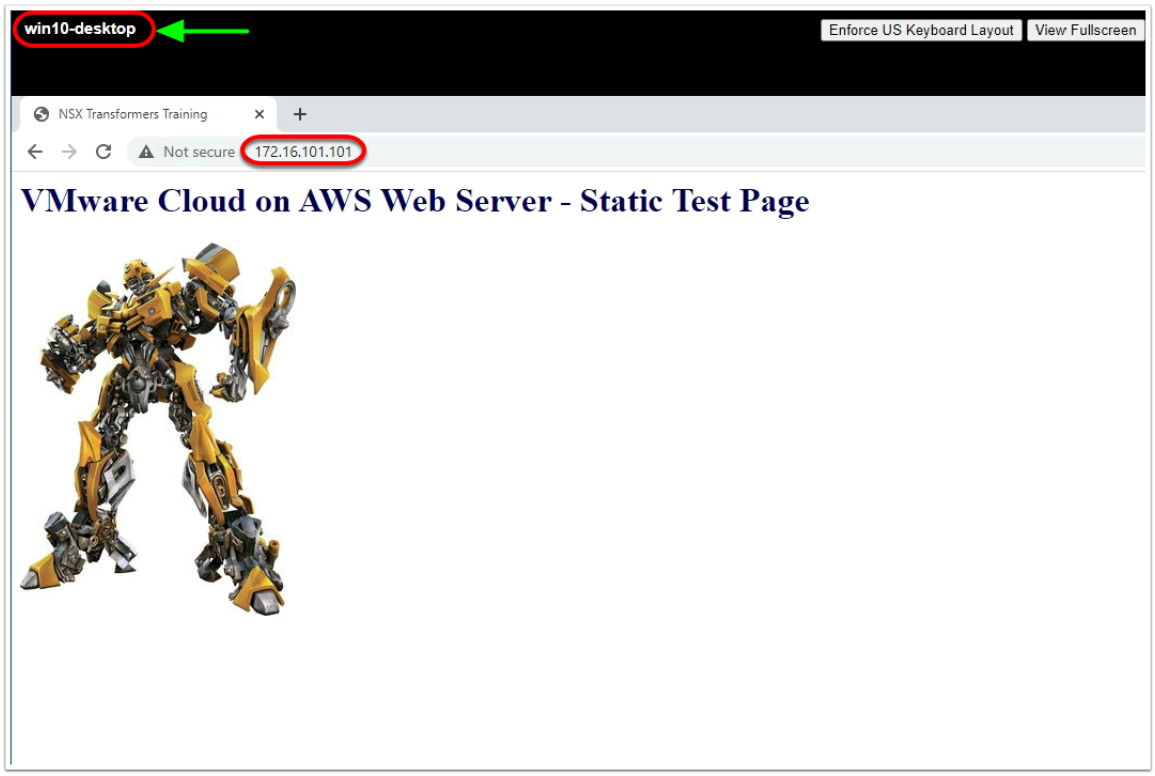
3. In your On-Premises SRM UI, Select the **Replication** Tab in the 2nd menu
4. Confirm that the Status for VM-01a is **OK** before proceeding
5. Click the **Recovery Plans** Tab
6. Select the **VM-RP** Recovery Plan.
7. Click **RUN**



8. In the **Confirm Operations** page
   - Select the "**I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters**"
   - Select the **Disaster Recovery** radio button
9. Click **NEXT**
10. Click **FINISH**
11. Monitor the progress of the Recovery event in the tasks section below



12. Once the recovery is complete, access the **VMC SDDC vCente**r.
13. You'll notice **vm-01a** is powered-on. It also retained its IP address
14. (**OPTIONAL**) You can test connectivity by performing a ping test from vm-01a to the wordpress VM.
    - wordpress IP is 172.16.101.11
15. (**OPTIONAL**) You can also test connectivity by browsing the web page of vm-01a from win10-desktop
    (This is the windows desktop you deployed into the SDDC in lab 2).



Task 8 - Reprotect

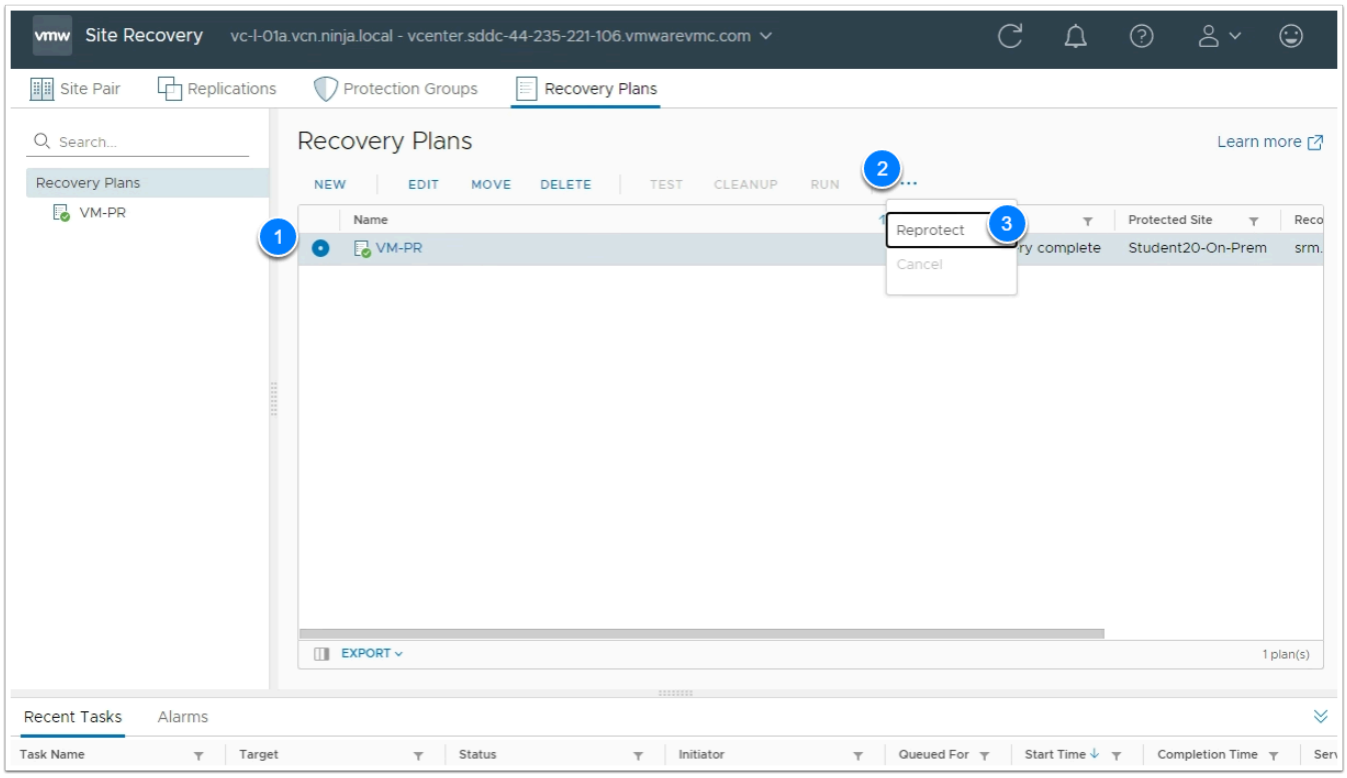
After a recovery, the recovery site becomes the primary site, but the virtual machines are not protected yet. If the original protected site is operational, you can reverse the direction of protection to use the original protected site as a new recovery site to protect the new protected site.

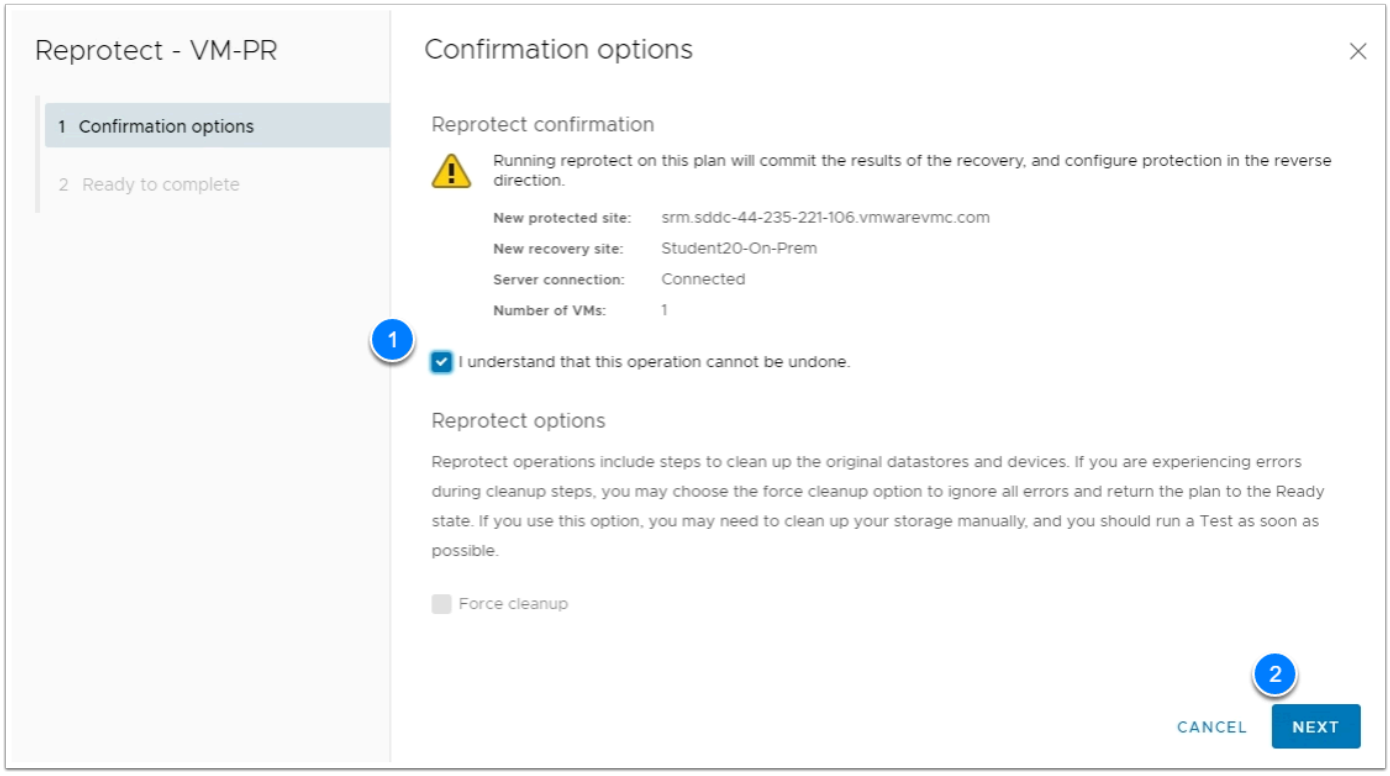
Manually reestablishing protection in the opposite direction by recreating all protection groups and recovery plans is time consuming and prone to errors. Site Recovery Manager provides the reprotect function, which is an automated way to reverse protection.

After Site Recovery Manager performs a recovery, the virtual machines start up on the recovery site. By running reprotect when the protected site comes back online, you reverse the direction of replication to protect the recovered virtual machines on the recovery site back to the original protected site.

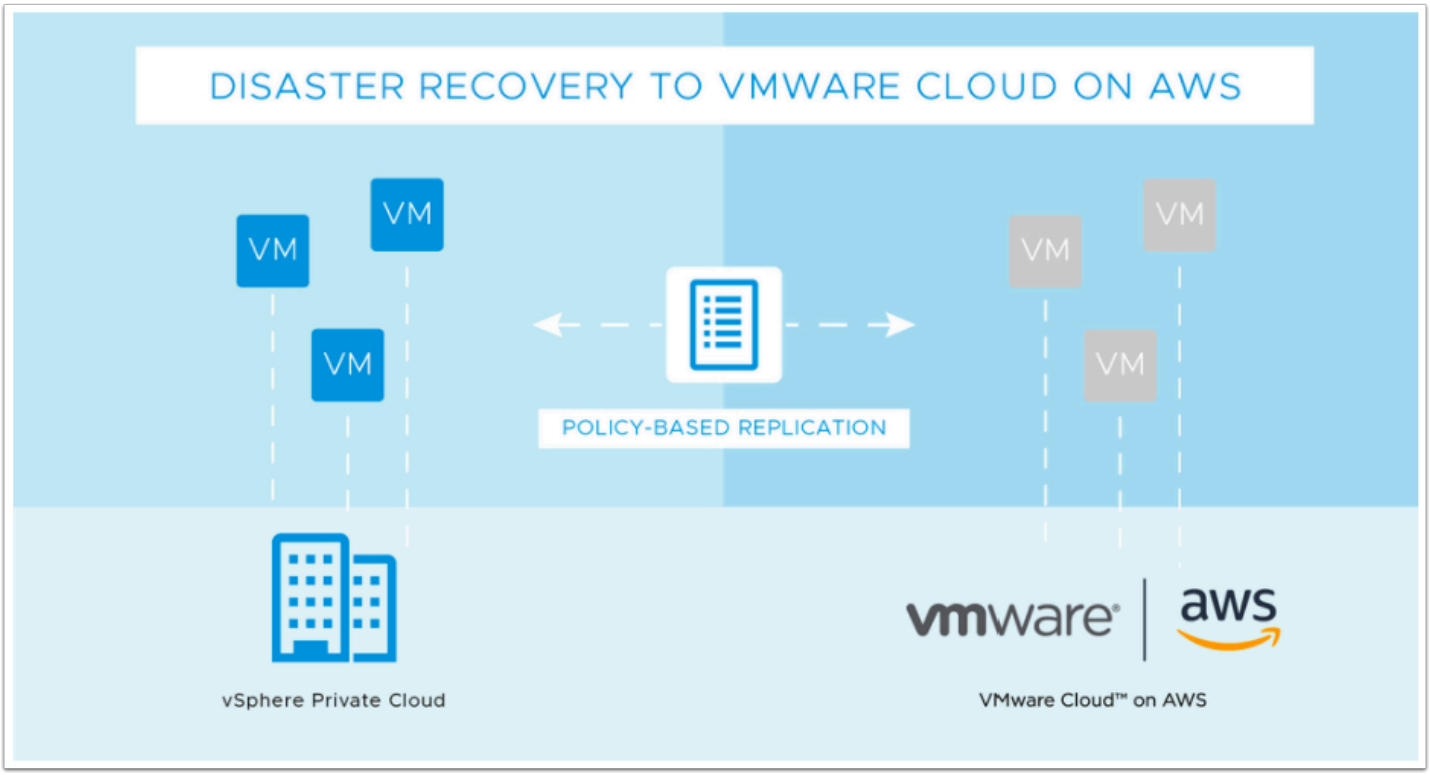
Reprotect uses the protection information that you established before a recovery to reverse the direction of protection. You can initiate the reprotect process only after recovery finishes without any errors. If the recovery finishes with errors, you must fix all errors and rerun the recovery, repeating this process until no errors occur.

1. In the On-Premises SRM UI Click **Recovery Plans** tab in the 2nd Menu then click the **VM-RP** Recovery Plan in the left menu.
2. In the right pane click the **ellipsis** (under the 2nd menu row to the right of run)
3. Click **Reprotect**
4. In the pop up check "**I Understand that this operation cannot be undone**"
5. Click **NEXT**
6. Click **FINISH**





Conclusion



VMware Site Recovery brings VMware enterprise-class Software-Defined Data Center (SDDC) Disaster Recovery as a Service to the AWS Cloud. It enables customers to protect and recover applications without the requirement for a dedicated secondary site. It is delivered, sold, supported, maintained and managed by VMware as an on-demand service. IT teams manage their cloud-based resources with familiar VMware tools without the difficulties of learning new skills or utilizing new tools and processes.

VMware Site Recovery works in conjunction with VMware Site Recovery Manager and VMware vSphere Replication to automate the process of recovering, testing, re-protecting, and failing-back virtual machine workloads. VMware Site Recovery utilizes VMware Site Recovery Manager servers to coordinate the operations of the VMware SDDC. This is so that, as virtual machines at the protected site are shut down, copies of these virtual machines at the recovery site startup. By using the data replicated from the protected site these virtual machines assume responsibility for providing the same services.