Protecting and Recovering Mission-Critical Applications in a VMware Hybrid Cloud with Site Recovery Manager

VMware BC/DR

Table of contents

Protecting and Recovering Mission-Critical Applications in a VMware Hybrid Cloud with Site Recovery Manager

Overview

This Guide provides a comprehensive documentation of the considerations and configuration steps required for using VMware Site Recovery Manager™ (SRM) to protect and recover a reference multi-tiered set of Business-Critical Applications from a source datacenter (on-premises or cloud-based) to a target VMware hybrid cloud-based datacenter, with the least cost (time, financial, and administrative intervention) possible.

This guide is intended to be used by technical architects, administrators or operators as the basis for building similar solutions for their own enterprise infrastructure. Because it assumes that the reader is familiar with the general concepts of business continuity and recovery, this guide does not attempt to define or explain such concepts in any detail. This guide also does not seek to discuss or explain the setup, configuration, operation or administration of Site Recovery Manager, virtualization, VMware Hybrid Cloud or the applications and services hosted on or provided by the protected workloads.

The referenced mission-critical application stack used in this guide (described in the next paragraph) has not been chosen based on any specific technical or technological imposition or requirements of Site Recovery Manager, VMware vSphere® or VMware Hybrid Cloud. VMware's Site Recovery Manager protects a Virtual machine (VM) as an entity, without considerations for the Application hosted in the VM. It is application-agnostic. We have chosen the following set of applications as the use case for this guide solely based on the need to be comprehensive in demonstrating the capabilities of automation and orchestration as well as the simplification of infrastructure recovery tasks possible with Site Recovery Manager.

Terminologies and Applications used in this Guide

"Cold" Recovery Site Topology

Although distributing Servers and Services over multiple Datacenters is a common BCDR strategy, the associated costs of maintaining a dedicated DR site (staffing, cooling, heat, duplicate hardware) have made Cloud-based options more attractive than physical datacenter option for this purpose. An additional benefit of using the cloud-based options is that Enterprises can further reduce the associated costs by minimizing actual utilization of the cloud-located resources until it is necessary to do so - when an actual disaster event has happened, or during a simulation/testing/validation exercise. This type of "use only when needed" utilization is commonly described as having a "Cold Site" for BCDR purposes. In this configuration, no "live" (or "hot) device, server or service is hosted in the target DR site, saving Enterprises lots of money and resources in their BCDR plans. We will demonstrate how SRM achieves this cost-saving objective while at the same time providing the simplified, flexible, automated, and repeatable BCDR solution for enterprises.

Windows Active Directory Domain Controllers

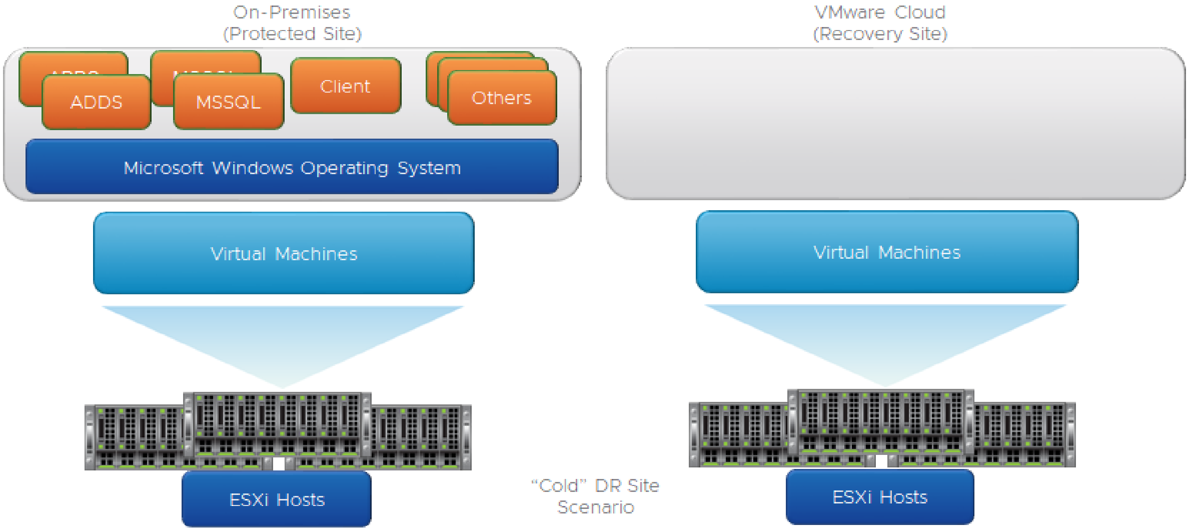
Since Domain Controllers are ubiquitous in most enterprise network infrastructures because a large number of applications depend on the services they provide, most BCDR plans tend to include considerations and provisions for them. In the "Cold DR Site" scenario described in this guide, recovering modern versions of Windows Domain Controllers (anything newer than Windows Server 2008 R2) in the event of a Disaster is a little bit tricky and complicated, chiefly due to the security features Microsoft introduced into virtualized Domain Controllers beginning from Windows Server 2012. This Guide will cover this consideration and show how Site Recovery Manager helps minimize these challenges.

Microsoft SQL Server

Because of its integration with so many front-end applications, services, and solutions, Microsoft SQL Server is arguably one of the most prevalent Business Critical Applications one can find in any Microsoft-based corporate IT infrastructure. This close integration creates both upstream and downstream dependencies which can result in significant cascading negative impacts when Microsoft SQL Server instances experience unexpected or prolonged outages in production. Microsoft SQL Server has native, built-in resilience to maximize its availability, enabling Enterprises to minimize the possibility of service disruption in the event of an outage. Combining Windows Failover Clustering Service (WSFC) with the Microsoft SQL Server Always On feature is a high availability option that helps ensure that, in the event of a failure of a member of the node, the services (databases especially) become available faster than otherwise possible in the absence of these features. Even then, this resilience is more useful and intended for high availability (which protects against component or service failures) rather than for disaster recovery events. We shall now attempt to make a high-level distinction between an "HA" event and a "DR" event, for clarity.

Windows Client Machine

The third tier in our 3-tier workloads scenario is more for illustration than for technical purposes. We could have chosen, say, a Web Server providing front-end services and dependent on the SQL Server services. We have chosen an ordinary Windows client machine, from which we would test connectivity and access to the servers and services we will recover in our failure scenarios. Come to think of it, what is the value of a disaster recovery exercise if it does not include facilitating clients’ and administrative access to the recovered resources?



“High Availability” vs “Disaster Recovery”

Application High Availability is more focused on an application’s ability to continue to operate and provide services even when the application's component(s) or the application itself has failed. This application's ability to survive (and recover from) failures is largely dependent on the resilience built into the application (either natively or through the use of third-party solutions or add-ons). In the scenario documented in this guide, the application-level resilience is provided through the combination of Windows Server Failover Clustering (WSFC) and the Microsoft SQL Server Always On features. These features enable the Services provided by Microsoft SQL Server to continue to be available (after a brief interruption) even after the original Server providing that Service has become unavailable for any reason. When the original Server fails, WSFC brings up its resources on a surviving node, usually without any administrative intervention. This, in a nutshell, is Microsoft SQL Server's "High Availability".

A Disaster Recovery event, in contrast with what we just described above, is a catastrophic failure impacting more than just a component or a Server. Without regard to its severity or duration, a disaster event can be described as a superset of multiple HA events which cannot be easily overcome by the resilience of a specific application, component or service. Because it is hardly ever transient in nature, the effects of a Disaster event are more impactful, disruptive and destructive on an Enterprise. Also, because, in a disaster event, multiple layers of the infrastructure are negatively impacted, recovering from such event is considerably more difficult, expensive, and slower compared to recovering from an HA event. Consequently, preparing and planning for recovering from a disaster event is materially and financially more expensive.

Assumptions

Because this guide is strictly focused on demonstrating how to use SRM to protect virtualized Business Critical Applications to any VMware vSphere-based Hybrid Cloud, a detailed description of the following topics is out of focus:

- Installation, setup, configuration and/or administration of VMware vSphere infrastructure
- Installation, setup, configuration and/or administration of specific VMware vSphere-based Cloud infrastructure
- Installation, setup, configuration and/or administration of VMware Site Recovery Manager
- Installation, setup, configuration and/or administration of Microsoft Active Directory Domain Services or Domain Controllers
- Installation, setup, configuration and/or administration of Microsoft SQL Server, Windows Failover Cluster or Always On

We assume that the infrastructure to perform these tasks has been configured as recommended in the applicable references.

Requirements

The following are expected to have been completed before undertaking the configuration and other tasks demonstrated in this guide:

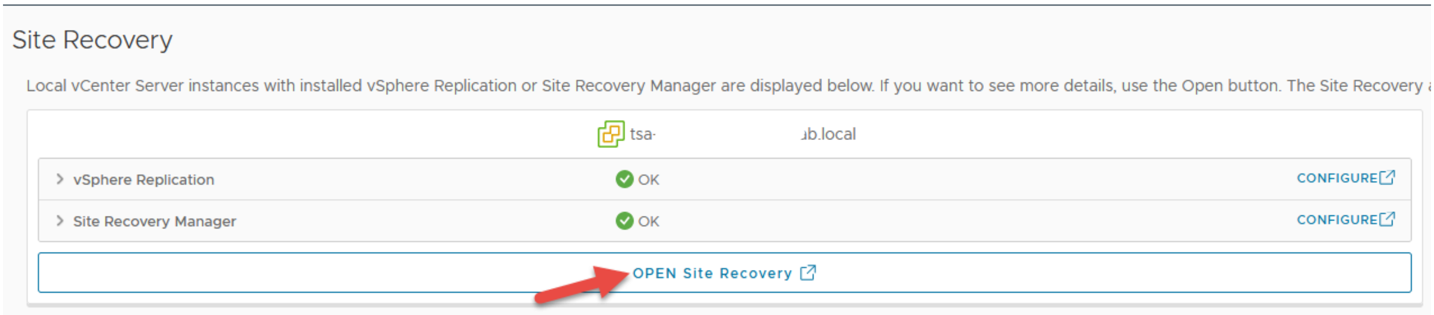
- Network connectivity between (or among) the source infrastructure. We will henceforth refer to this as the "protected site".
- Network connectivity between (or among) the target infrastructure, which could be any of the publicly available brand of the VMware Cloud infrastructure options (VMware Cloud on AWS, Azure VMware Solution, Google Cloud VMware Engine). We will henceforth refer to this as the "Recovery Site".
- The "Network Connectivity" type required for VMware SRM is dictated by the VMware Cloud brand and version - consult the Cloud Provider's reference materials for more information.
- Successful installation of VMware SRM on both the protected and recovery sites.
- Successful installation of VMware vSphere Replication appliances in the same vCenter Server in which the SRM instance is registered on each of the sites.
- Environment configuration information (VM IP addresses, DNS Server IP addresses, Network segment, datastore) is required to complete the protection and recovery plans.
- All the VMs which are to be protected and recovered by VMware Site Recovery Manager have an up-to-date version of the VMware Tools installed (**Note:** *This is a standard recommendation, but it is especially relevant if the VMs will be reconfigured or customized as part of the Recovery process*)

Setting up BCDR Environment and Workflow in VMware vSphere Site Recovery Manager

Now, let's get technical.

The process of configuring VMware SRM to protect and recover workloads begins with the pairing of the **Protected** and **Recovery** Sites. SRM administrative interface is integrated into the VMware vSphere Client interface. The exercises presented in this guide will be conducted entirely through these Web interfaces, with the exception of a few review tasks conducted inside the recovered workloads (Windows Operating System, Active Directory Domain Services (ADDS) and Microsoft SQL Server) to confirm functionalities after recovery.

Here is the SRM interface on the **Protected Site.**



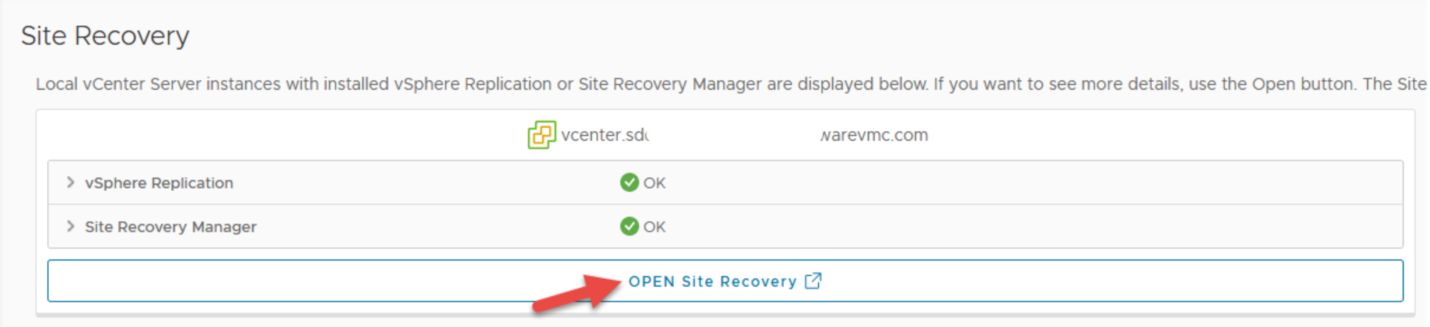
Site Recovery

Local vCenter Server instances with installed vSphere Replication or Site Recovery Manager are displayed below. If you want to see more details, use the Open button. The Site Recovery

tsa- ıb.local

vSphere Replication	✓ OK	CONFIGURE
Site Recovery Manager	✓ OK	CONFIGURE

Here is the SRM interface on the **Recovery Site.**



Site Recovery

Local vCenter Server instances with installed vSphere Replication or Site Recovery Manager are displayed below. If you want to see more details, use the Open button. The Site

vcenter.sdı ıarevmc.com

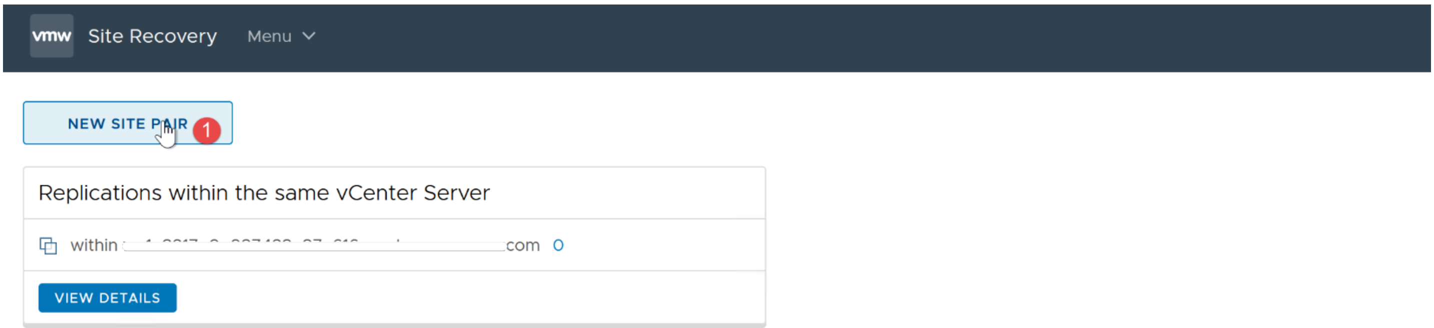
vSphere Replication	✓ OK
Site Recovery Manager	✓ OK

We will be completing most of the tasks in this exercise from the **Protected Site**, so let's get started

- Click on **"OPEN Site Recovery"**

We are now going to connect the vCenter and SRM instances on each site to one another. This is called **"Pairing the Sites".**

- Click on **"New Site Pair".**

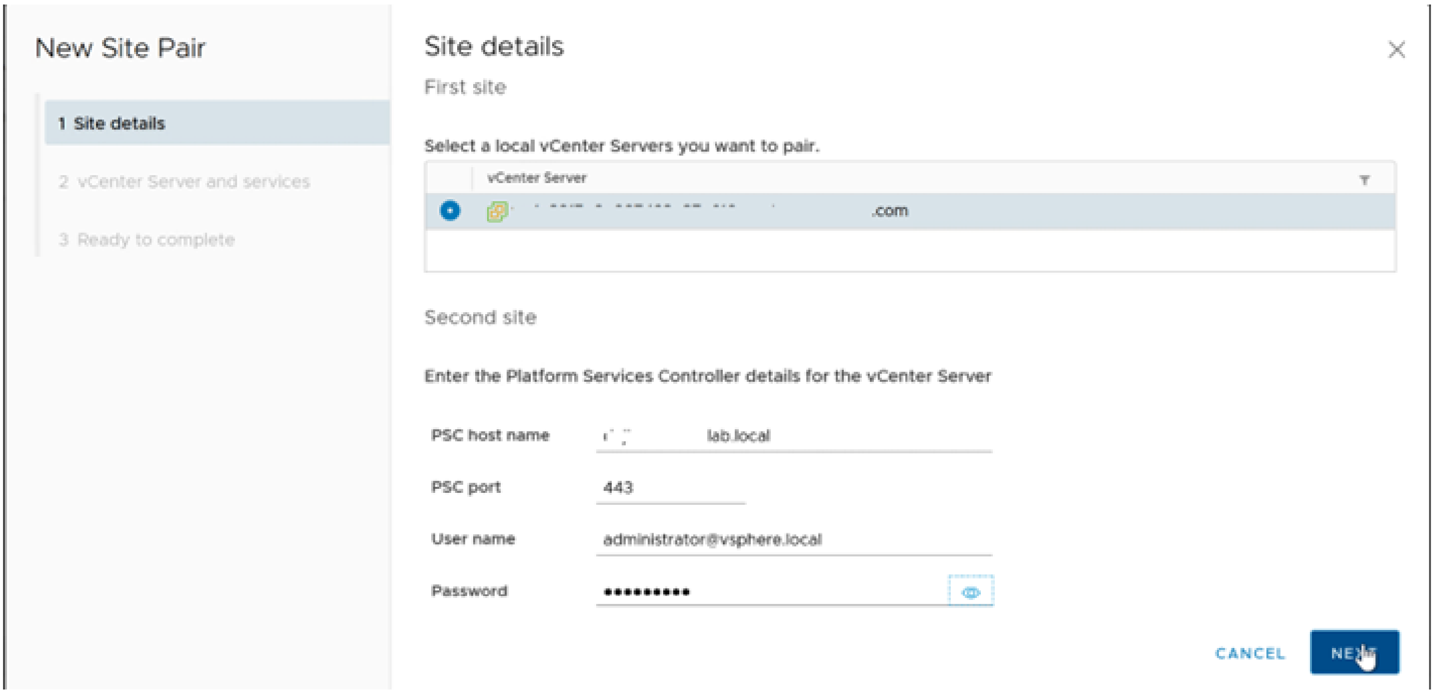


Replications within the same vCenter Server

within com 0

We are prompted for the vCenter Server Credentials.

Because we are doing this from the Recovery Site's vCenter instance (our VMware-based Cloud BCDR environment), the credentials we provide here will be for the Protected Site's vCenter instance.



New Site Pair

1 Site details

2 vCenter Server and services

3 Ready to complete

Site details

First site

Select a local vCenter Servers you want to pair.

	vCenter Server
●	.com

Second site

Enter the Platform Services Controller details for the vCenter Server

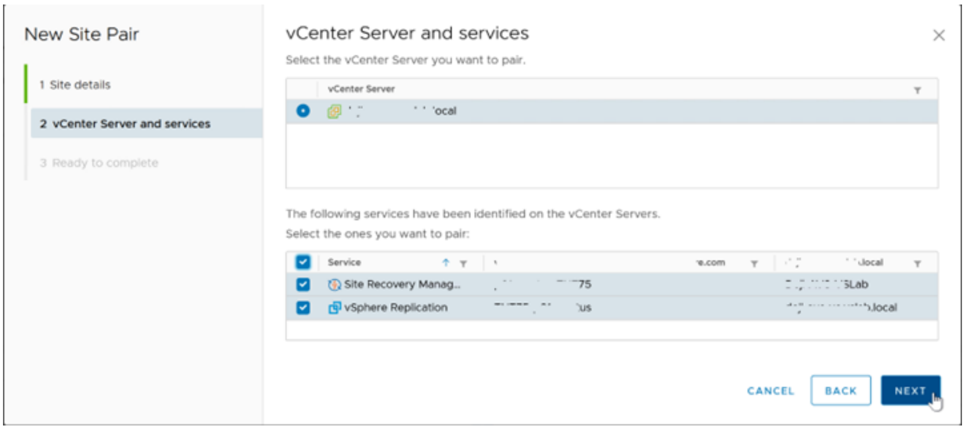
PSC host name: lab.local

PSC port: 443

User name: administrator@vsphere.local

Password: ●●●●●●●●●●

Note: If you are using default self-signed certificates in your environment, you will need to click **"Connect"** to ignore the vCenter's self-signed certificate security warning and proceed.



New Site Pair

1 Site details

2 vCenter Server and services

3 Ready to complete

vCenter Server and services

Select the vCenter Server you want to pair.

	vCenter Server
●	'ocal

The following services have been identified on the vCenter Servers.

Select the ones you want to pair:

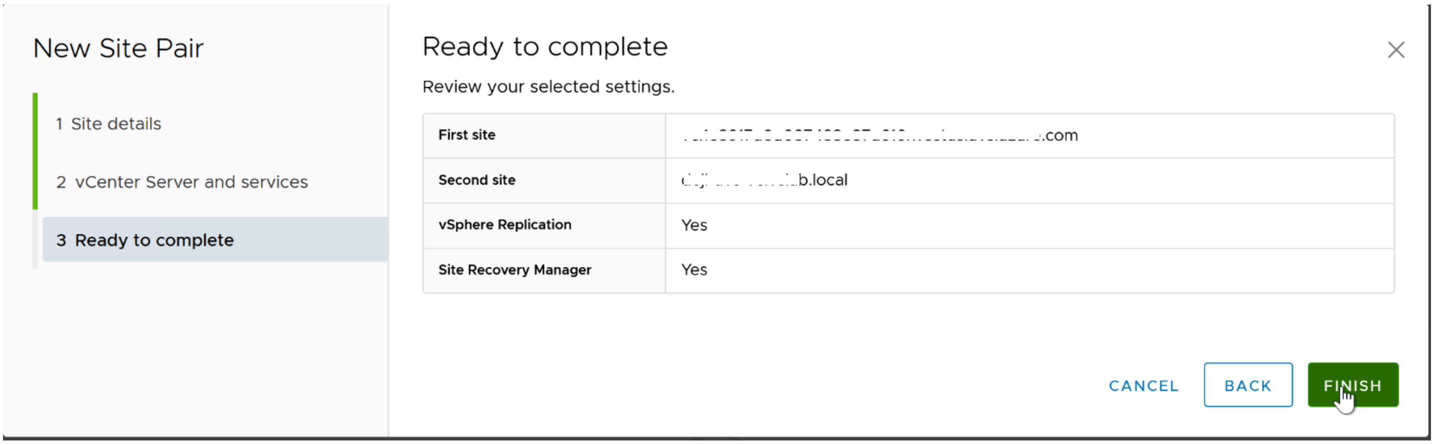
☑	Service	e.com	local
☑	Site Recovery Manag...	75	5Lab
☑	vSphere Replication	us	.local

We are using VMware vSAN for the Storage subsystem in our environments. vSAN is the default Storage option for all VMware vSphere-based Cloud infrastructure. In this configuration, we see that the SRM and the VMware vSphere replication appliance are both registered on our vCenter Server

- Click **"Next"** to continue

Note: If you are using default self-signed certificates in your environment, you will need to click **"Connect"** to ignore the vCenter's self-signed certificate security warnings and proceed.

Click **"Finish"** to complete the **Site Pairing** process.



New Site Pair

1 Site details

2 vCenter Server and services

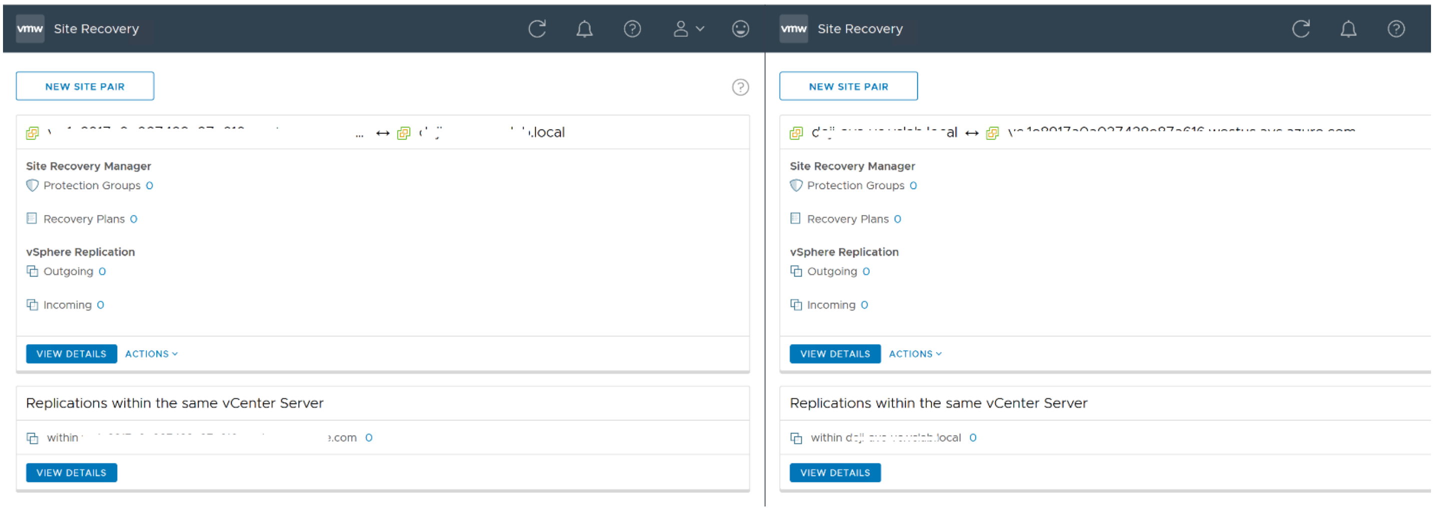
3 Ready to complete

Ready to complete

Review your selected settings.

First site	[illegible].com
Second site	[illegible]b.local
vSphere Replication	Yes
Site Recovery Manager	Yes

Now we are done with the **Site Pairing** exercise.



[illegible] ↔ [illegible].local

Site Recovery Manager
Protection Groups 0
Recovery Plans 0

vSphere Replication
Outgoing 0
Incoming 0

Replications within the same vCenter Server

within [illegible].com 0

[illegible]al ↔ [illegible]

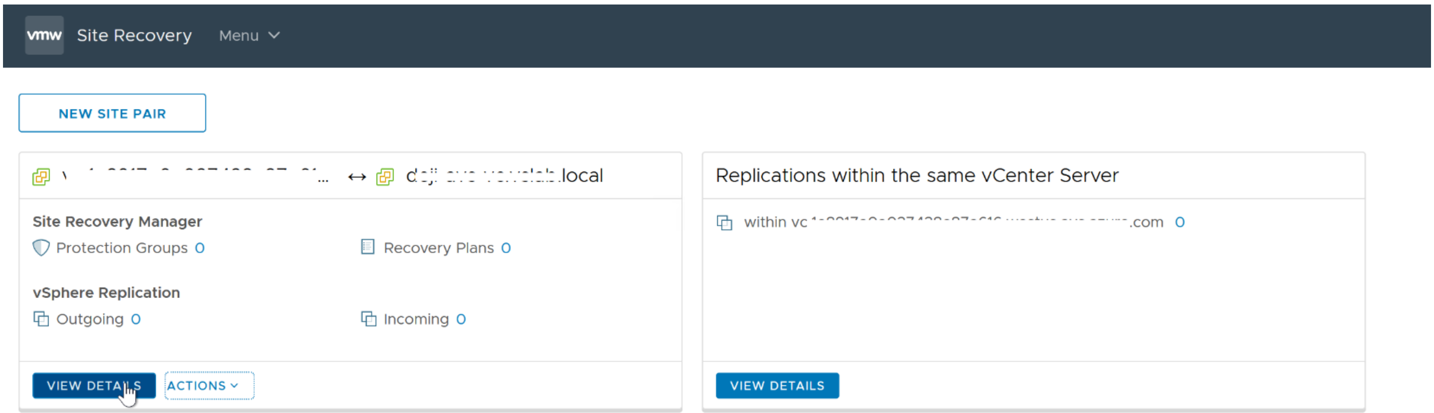
Site Recovery Manager
Protection Groups 0
Recovery Plans 0

vSphere Replication
Outgoing 0
Incoming 0

Replications within the same vCenter Server

within [illegible].local 0

- Click **"View Details"**



[illegible] ↔ [illegible].local

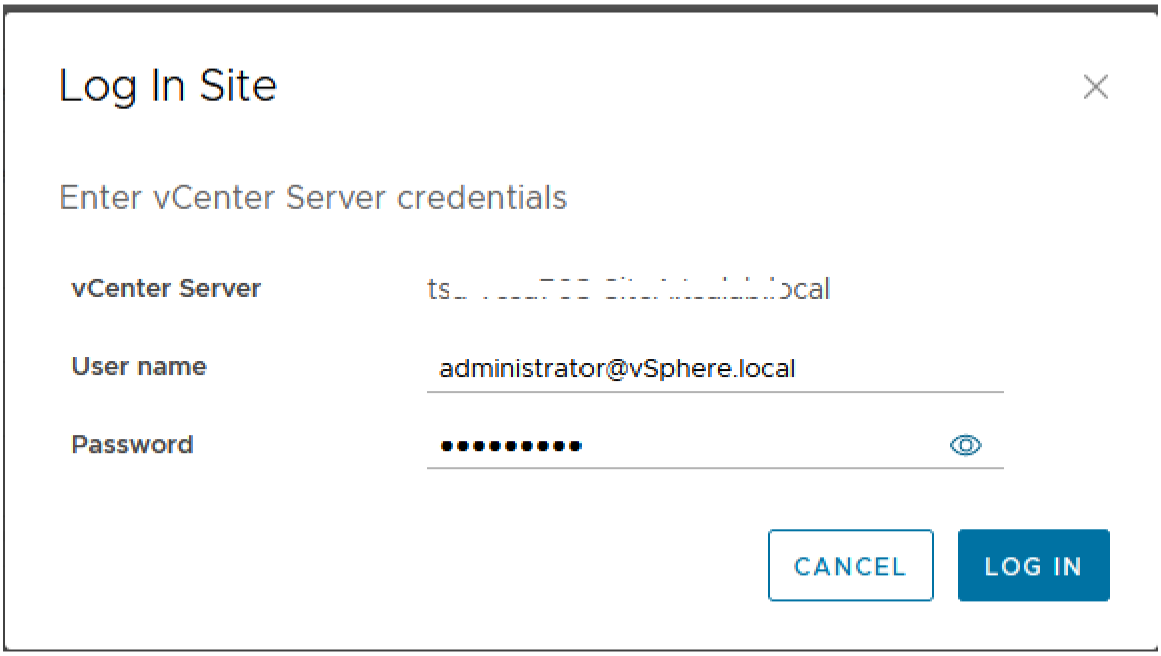
Site Recovery Manager
Protection Groups 0
Recovery Plans 0

vSphere Replication
Outgoing 0
Incoming 0

Replications within the same vCenter Server

within vc[illegible].com 0

- Provide the admin credentials for the **Protected Site's vCenter** Server, then click **"Login"** to complete the initial pairing.



Log In Site

Enter vCenter Server credentials

vCenter Server ts[redacted]ocal

User name administrator@vSphere.local

Password ••••••••••

Factors Influencing our Design and Configuration Choices

Before we begin putting all the pieces in place, let's describe our objectives in more detail.

VMware SRM allows you to configure an orchestrated workflow of all the actions and steps required to recover a VM including the guest operating system, applications, processes, etc. SRM does this by using the features and capabilities of the VMware vSphere infrastructure and the storage subsystem to create a point-in-time copy of the VM at the Source (Protected Site) to the Target (Recovery Site). SRM can utilize either array-based replication or vSphere Replication to replicate VM data from a source site to a target site. For this paper, only vSphere Replication was used.

Because vSphere Replication is host-based replication, it is independent of the underlying storage and it works with a variety of storage types including vSAN, traditional SAN, NAS, and direct-attached storage (DAS). Unlike many array replication solutions, vSphere Replication enables virtual machine replication between heterogeneous storage types. For example, vSAN to DAS, SAN to NAS, and SAN to vSAN. vSphere Replication can, of course, replicate virtual machines between the same types of storage, such as vSAN to vSAN.

When a (real or simulated) failure occurs at the Protected Site, administrators are enabled to initiate the pre-configured recovery steps and actions (recovery plan).

These steps include (among others) the order in which SRM recovers the protected VMs; the network to which the recovered VMs are connected to; whether to customize or change the IP addresses for the recovered VM (or let them obtain such addresses from an available/accessible DHCP Server; in-Guest configuration scripts to run on the recovered VMs, etc.

When an administrator initiates this recovery plan, SRM uses the copy of the VMs data created by vSphere Replication to prepare the VMs for recovery. The VMs are added to inventory, connected to the appropriate resources (networks, folders, resource pools, and storage policies, powered on in the order specified and customized as required. If the workflow includes running scripts inside the VMs as part of the process, the guest operating system is instructed to call and run the scripts (of course, the scripts must exist on the VMs and be accessible during the recovery process).

Here is a high-level description of the protection and recovery workflow we will configure for our exercise.

- The SQL Server instances in our use case run on VMs running the Windows Operating System and are joined to the Active Directory Domain Services (ADDS) infrastructure. For this reason, we need the Domain Controllers to be available and functional before the SQL Server VMs are brought up.
  - Our SQL Server instances are clustered in a 2-node always-on availability group configuration. Clustering SQL Servers requires the use of a Windows Server Failover

  Cluster. We are using a file share witness (a folder located on one of the domain controllers) as the quorum option for this configuration.
  - We specifically use Availability Groups in this Guide and demonstration because (as of the time of this writing):
    - The default storage option for VMware Clouds is vSAN
    - The default replication option for vSAN is vSphere Replication
    - vSphere Replication does not currently have the capabilities to replicate disks used for shared-disk Windows clustering
    - Although the scripts and all other required steps are similar, the factors mentioned above preclude the use of the steps documented in this guide for protecting and recovering Microsoft SQL Servers configured in shared-disk mode – Always On Failover Clustering Instance (FCI).
  - In steady state operation, applications, scripts, and processes access the SQL Server instance and the database through a common name (called "Listener"). The Listener is (simply) a host name that resolves to a specific IP address. This resolution is handled by the DNS Service provided by our Domain Controllers. This IP Listener is a resource that must be available for the services provided by our SQL Servers to be accessible.
  - Usually, the IP address segments in our Protected Site are different from the ones used in our Recovery Site.
  - It is possible to extend our network segments from the Protected Site to the Recovery Site. Because the mechanism for achieving this configuration differs among the various brands of VMware Cloud, it is impractical for us to include this consideration in this guide. For simplicity, our exercise will include the workflow to change the IP addresses of the recovered VMs to match what is available at the Recovery Site.
  - This choice of IP address change means that, we will not only need to change the VM's IP (a trivial task in SRM), but we will have to also change the IP address of the Listener described in the previous paragraph.
  - Because SRM orchestrates and automates the protection and recovery of VMs without any insight into the Applications hosted therein, it is impossible for SRM itself to make Application-level configuration changes as part of its automation process. For this purpose, we will be using the script-triggering feature of SRM to instruct the guest operating system to run a script, which will change the IP address of the Listener and update the record in DNS after the recovery.

- Around 2012, with compute resources getting larger and virtualization maturing and becoming well-accepted in the enterprise, dedicating a Physical Server to running a domain controller became impractical and inefficient from a cost and ROI perspective. Security and stability concerns with virtualized Domain Controllers prompted Microsoft to introduce some measures to make virtualized Domain Controllers safer and more stable. One of the concerns addressed by these measures is the ease with which an insider or attacker with elevated privileges in the virtual infrastructure can make a copy of a virtualized domain controller (either by cloning it or just making a copy of the VMDK). These measures are implemented mainly through what is known as VM-generation ID.

- What does VM-Generation ID do? It makes virtualizing domain controllers a much safer proposition.

- Because, at a high level, a domain controller has a full copy of the Domain's users, passwords and other secrets, the effect of such an attack cannot be easily minimized or mitigated. Among other capabilities, VM-Generation ID helps prevent the type of attack described earlier by:
  - Storing and tracking a unique counter for every copy of a virtualized domain controller - the Hypervisor assigns a counter to the VM (in vSphere, this is the **"VM Gen-IDx"** value you see in a Windows VM's vmx file).
  - When the Domain Controller boots up, it reads this counter from its configuration file and then stores it internally.
  - This counter persists over the lifetime of the VM - unless a specific type of operation (listed here) is performed on that VM. These actions alter the state and identity of the virtual machine, so whenever any of them is performed, the hypervisor changes the counter.
  - The next time the Domain Controller is powered-on, Windows will read its generation ID, compare it to what was previously stored and discover that there is a mismatch.
  - When this happens, Windows immediately takes a number of steps in response to the disparity and triggers the safety measures provided by the VM-Generation ID feature. Please refer to the following link for a more detailed discussion of "Virtualization-based Safeguards”.

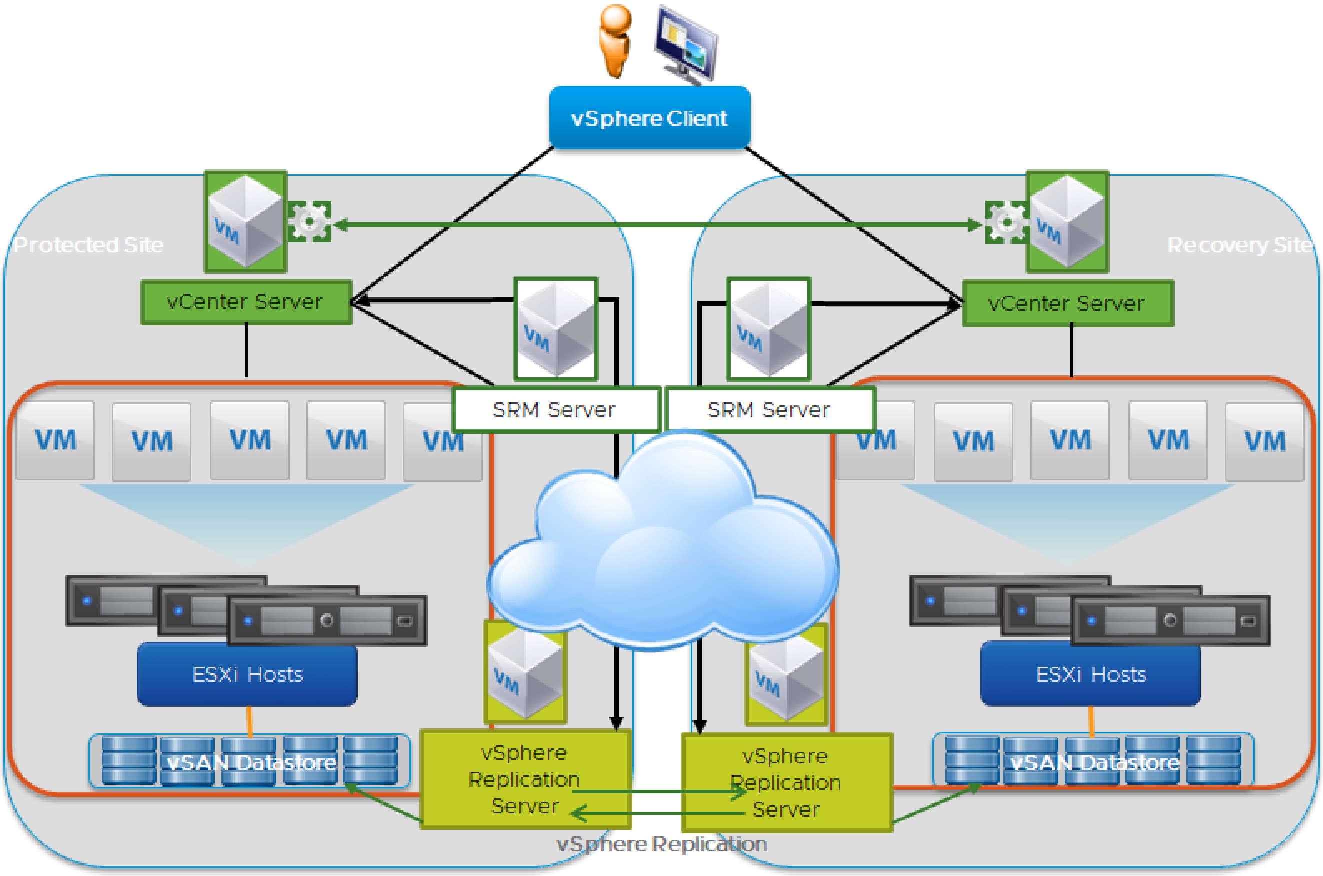
- SRM recovery workflow includes bringing up A REPLICATED COPY of a Protected VM at the Recovery Site when (in a real Disaster event) the real Domain Controller is unavailable) or in a simulated DR exercise (when the VM is recovered to a fenced-off "Test" network). Recovering a domain controller requires us to instantiate a replicated copy of a real Domain Controller. Such a "Copy" operation automatically changes the VM-generation ID of the domain controller, which then automatically triggers the domain controller safety responses from Windows.

- One of the responses is an instruction to the domain controller to (among other things) reset its InvocationID and discard its RID Pool. For all practical purposes, the domain controller is no longer a domain controller at this point, due to the change in its VM-generation ID. Windows then updates the VM-generation ID it had stored previously to match the new one provided by the hypervisor. The VM then obtains a new set of RID Pool from the RID Master, and life is good. Well, we have abbreviated the complete narrative for our purposes, but what is of relevance to us for this Guide is that, in spite of the fact that recovering a domain controller with SRM triggers Windows to invoke the Virtualized Domain Controller Safety feature, doing so is a supported, repeatable, more efficient, reliable, and faster option than anything else available as of the time of this writing.

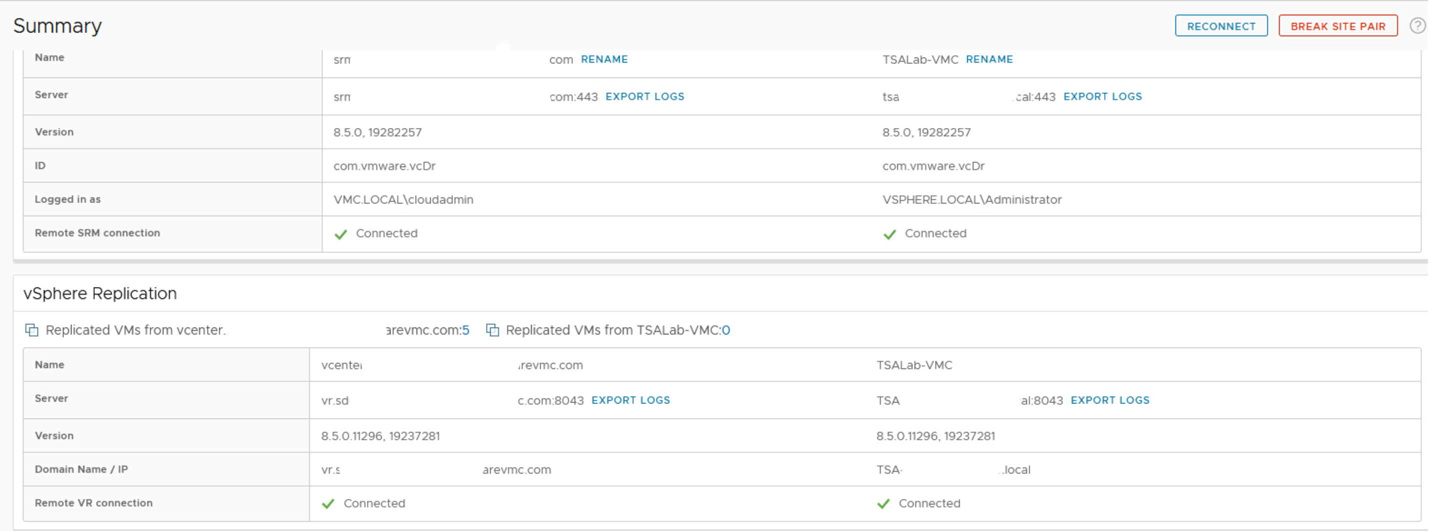
Putting it all Together

Now that we know our desired outcome and the considerations governing our ability to achieve it, we are ready to proceed.

Here is an approximate representation of the logical topology of our SRM Infrastructure



This is what our paired SRM initial configuration looks like.



Summary

RECONNECT BREAK SITE PAIR

Name	srn com RENAME	TSALab-VMC RENAME
Server	srn com:443 EXPORT LOGS	tsa .cal:443 EXPORT LOGS
Version	8.5.0, 19282257	8.5.0, 19282257
ID	com.vmware.vcDr	com.vmware.vcDr
Logged in as	VMC.LOCAL\cloudadmin	VSPHERE.LOCAL\Administrator
Remote SRM connection	✓ Connected	✓ Connected

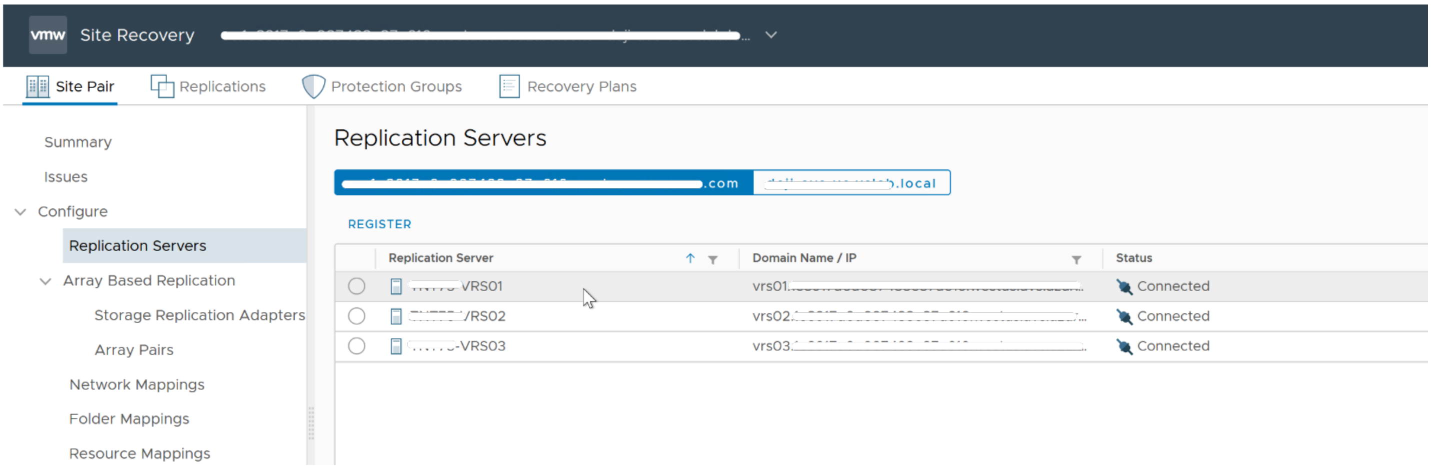
vSphere Replication

Replicated VMs from vcenter. arevmc.com:5 Replicated VMs from TSALab-VMC:0

Name	vcente .revmc.com	TSALab-VMC
Server	vr.sd c.com:8043 EXPORT LOGS	TSA al:8043 EXPORT LOGS
Version	8.5.0.11296, 19237281	8.5.0.11296, 19237281
Domain Name / IP	vr.s arevmc.com	TSA- .local
Remote VR connection	✓ Connected	✓ Connected

vSphere Replication Server will be responsible for replicating our protected VMs from the Protected Site to the Target Site (and vice versa). No special configuration is required for this part at this point.

We will ignore the "Array Based Replication" part because it does not apply to vSAN, which is the default storage option for VMware Cloud.



Site Recovery [redacted]

Site Pair | Replications | Protection Groups | Recovery Plans

- Summary
- Issues
- Configure
  - Replication Servers
  - Array Based Replication
    - Storage Replication Adapters
    - Array Pairs
  - Network Mappings
  - Folder Mappings
  - Resource Mappings

Replication Servers

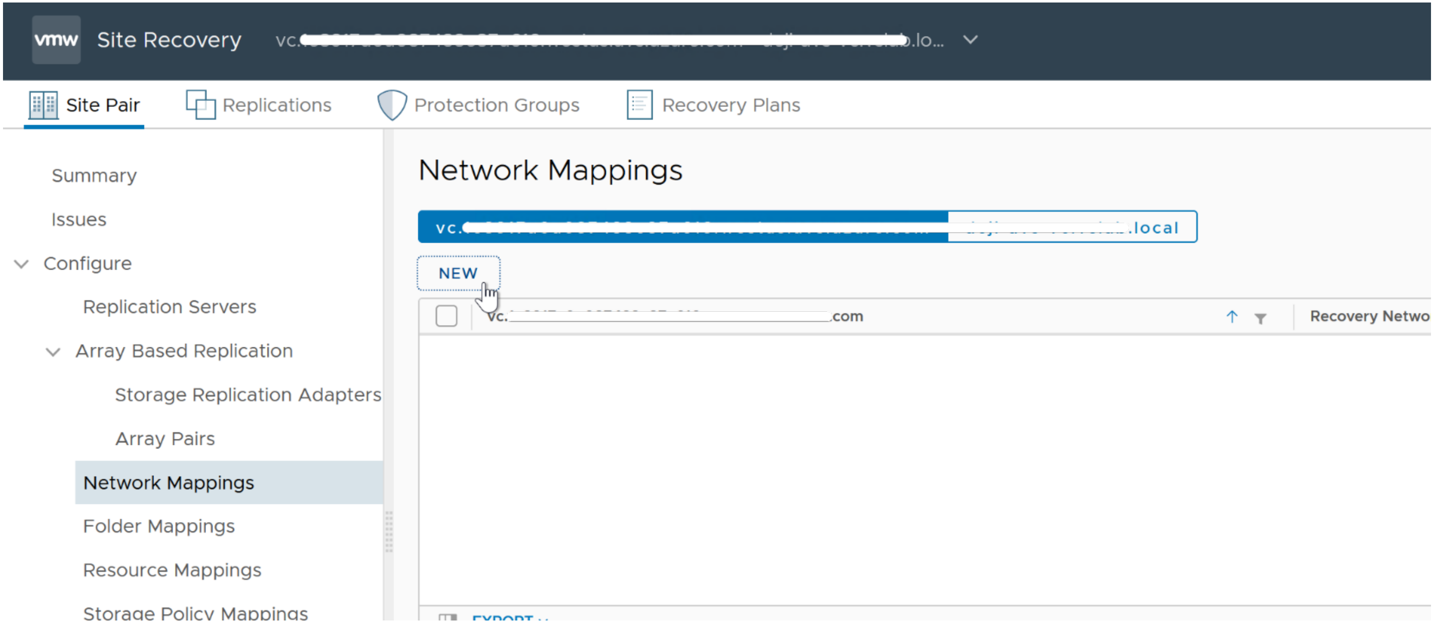
[redacted].com | [redacted].local

REGISTER

	Replication Server	Domain Name / IP	Status
○	[redacted]-VRS01	vrs01.[redacted]	Connected
○	[redacted]/RS02	vrs02.[redacted]	Connected
○	[redacted]-VRS03	vrs03.[redacted]	Connected

Network pairing allows us to map the network segments on one side to a corresponding segment on the other.

- Click **"New"** to begin creating our mapping



Site Recovery vc.[redacted].lo...

Site Pair | Replications | Protection Groups | Recovery Plans

- Summary
- Issues
- Configure
  - Replication Servers
  - Array Based Replication
    - Storage Replication Adapters
    - Array Pairs
  - Network Mappings
  - Folder Mappings
  - Resource Mappings
  - Storage Policy Mappings

Network Mappings

vc.[redacted] | [redacted].local

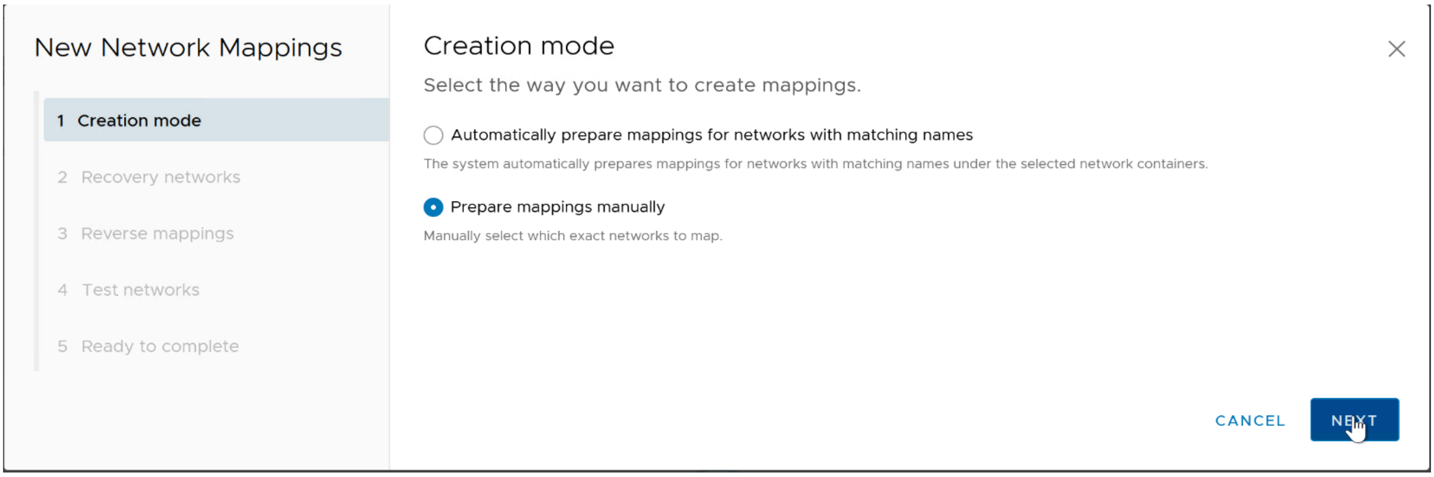
NEW

☐	vc.[redacted].com	Recovery Netwo

EXPORT

Select "Prepare mappings manually" because we would like to be able to select the specific mappings we desire.

Click "Next".



New Network Mappings

1 Creation mode
2 Recovery networks
3 Reverse mappings
4 Test networks
5 Ready to complete

Creation mode

Select the way you want to create mappings.

○ Automatically prepare mappings for networks with matching names

The system automatically prepares mappings for networks with matching names under the selected network containers.

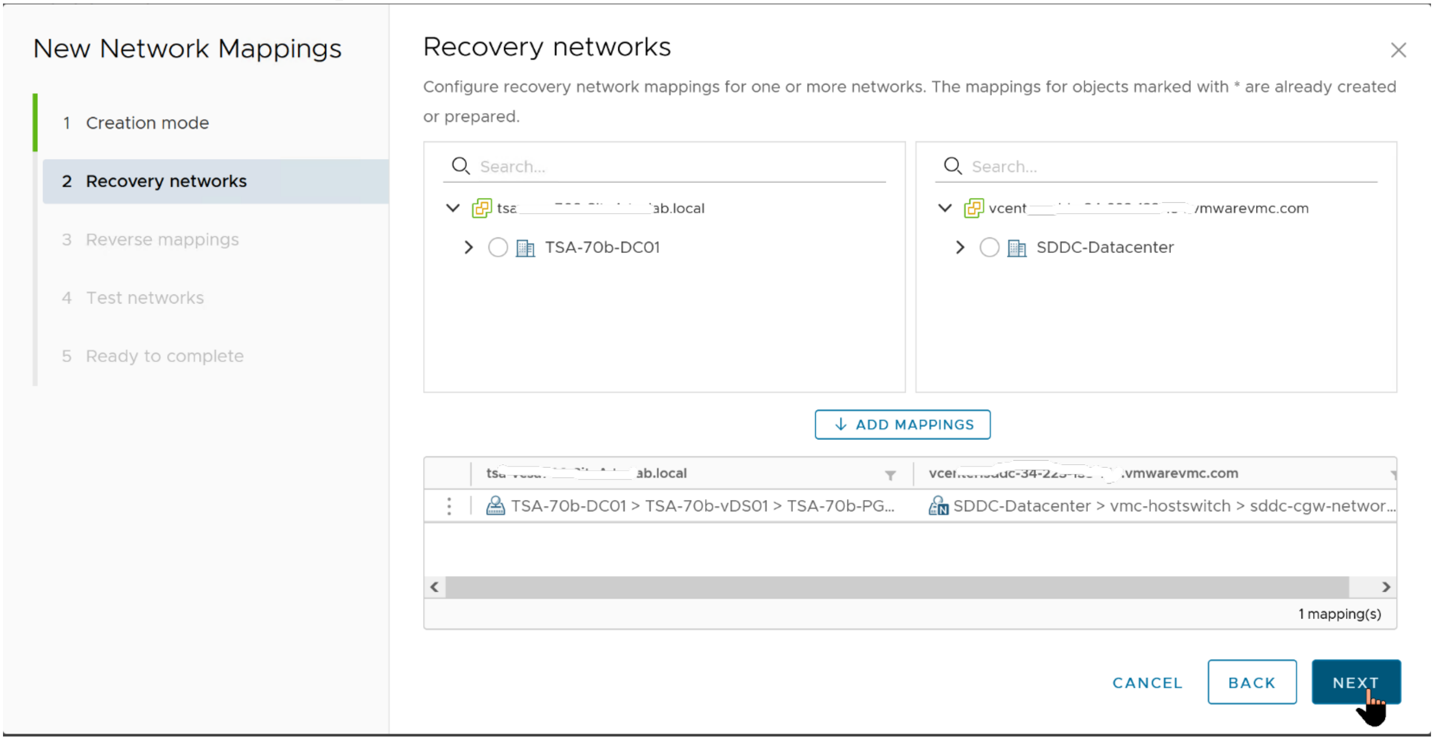
● Prepare mappings manually

Manually select which exact networks to map.

CANCEL | NEXT

We will choose to map at the virtual Distributed Switch (vDS) level, instead of selecting an individual Port group to map. This is just for simplicity.

- Select the radio button near the vDS on each site and click **"Add Mappings".**
- Click **"Next"** to proceed.



New Network Mappings

1 Creation mode
2 Recovery networks
3 Reverse mappings
4 Test networks
5 Ready to complete

Recovery networks

Configure recovery network mappings for one or more networks. The mappings for objects marked with * are already created or prepared.

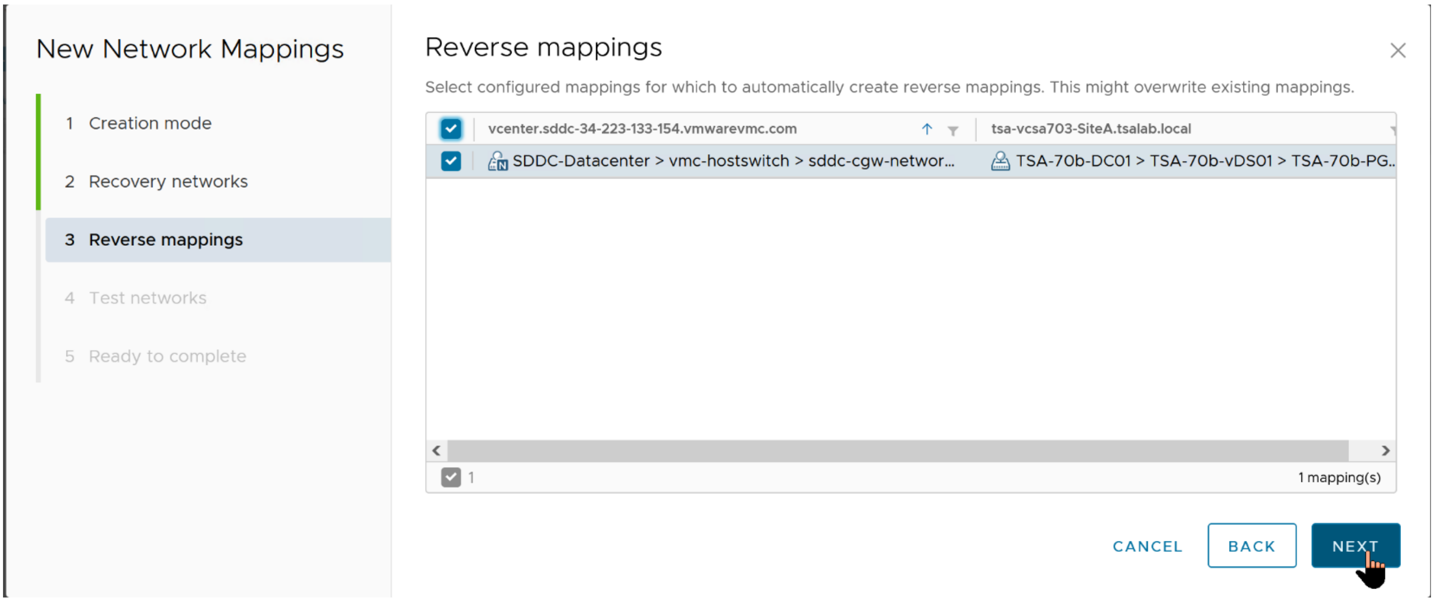
tsa[redacted]ab.local
TSA-70b-DC01

vcent[redacted]vmwarevmc.com
SDDC-Datacenter

tsa[redacted]ab.local	vcen[redacted].vmwarevmc.com
TSA-70b-DC01 > TSA-70b-vDS01 > TSA-70b-PG...	SDDC-Datacenter > vmc-hostswitch > sddc-cgw-networ...

1 mapping(s)

- Click the option to automatically create a reverse mapping, just so we do not have to do it manually.
- Click **"Next".**



New Network Mappings

1 Creation mode
2 Recovery networks
3 Reverse mappings
4 Test networks
5 Ready to complete

Reverse mappings

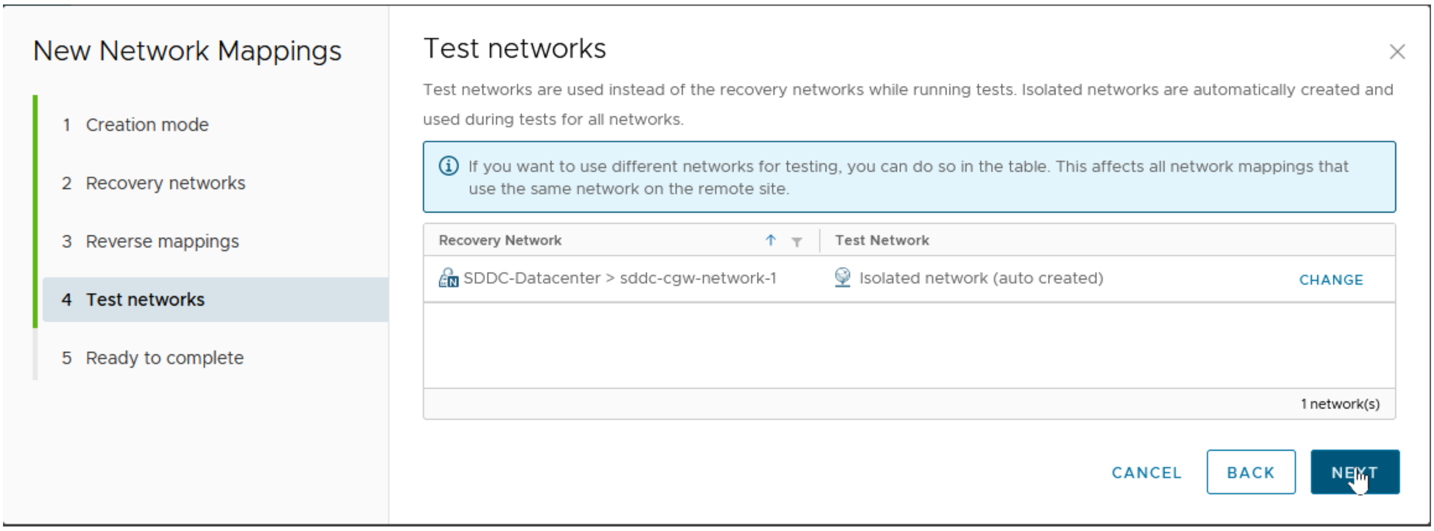
Select configured mappings for which to automatically create reverse mappings. This might overwrite existing mappings.

☑	vcenter.sddc-34-223-133-154.vmwaremvc.com	tsa-vcsa703-SiteA.tsalab.local
☑	SDDC-Datacenter > vmc-hostswitch > sddc-cgw-networ...	TSA-70b-DC01 > TSA-70b-vDS01 > TSA-70b-PG...

☑ 1 1 mapping(s)

One of the most compelling features in SRM, and, consequently, why it is much preferred over competing for BDCR orchestration Solutions (or manual option) is being able to conduct simulated (Test) Disaster Recovery exercises without impacting the production environment. Administrators can demonstrate and prove their infrastructure Disaster Recovery readiness by conducting a recovery of the Protected workloads into the Recovery Site while the Protected workloads continue to provide uninterrupted services at the Protected Site. SRM does this by bringing up a copy of the Protected workload in an isolated network segment at the Recovery Site. SRM creates this isolated network by default, but Administrators can choose to specify their own Recovery Test (aka "Bubble") network. The default isolated network is inaccessible to anything outside of the bubble, but what if an Administrator wants to demonstrate functionalities and accessibility of recovered workloads to their auditors? They can do this by recovering the workloads into a specific network of their choices (assuming they have such controlled network in place).

- For this guide, we will accept the default **"Isolated network (auto created)"** option.
- Click **"Next"** to continue.



New Network Mappings

1 Creation mode
2 Recovery networks
3 Reverse mappings
4 Test networks
5 Ready to complete

Test networks

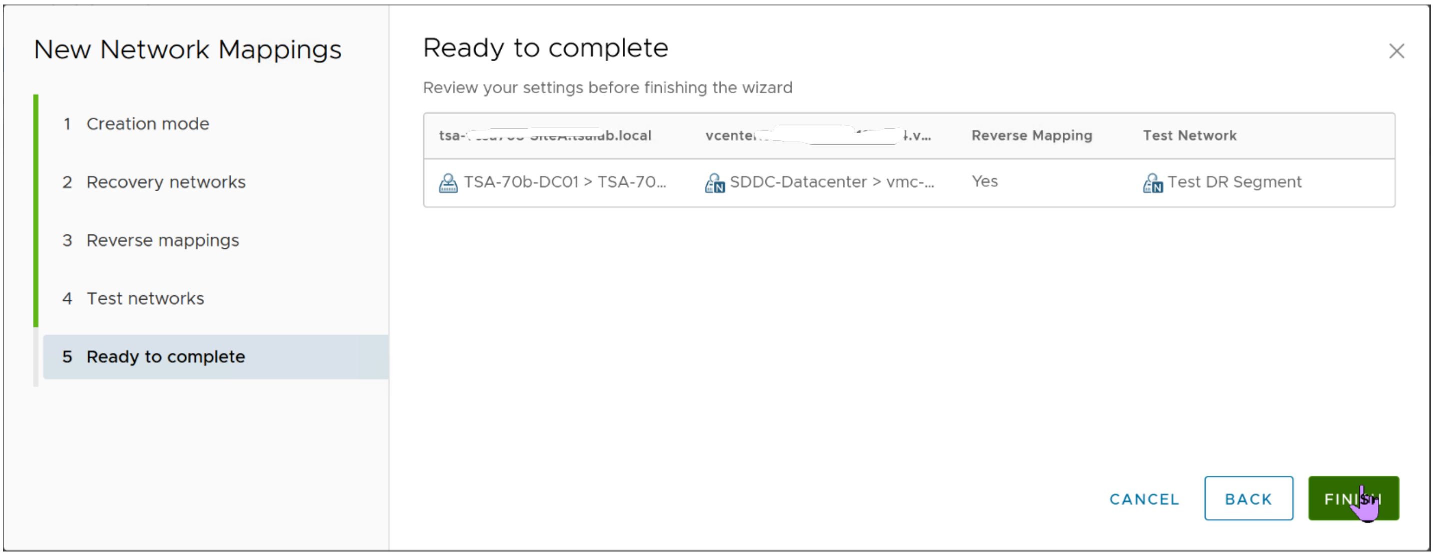
Test networks are used instead of the recovery networks while running tests. Isolated networks are automatically created and used during tests for all networks.

ⓘ If you want to use different networks for testing, you can do so in the table. This affects all network mappings that use the same network on the remote site.

Recovery Network	Test Network	
SDDC-Datacenter > sddc-cgw-network-1	Isolated network (auto created)	CHANGE

1 network(s)

Click **"Finish"** to proceed.



New Network Mappings

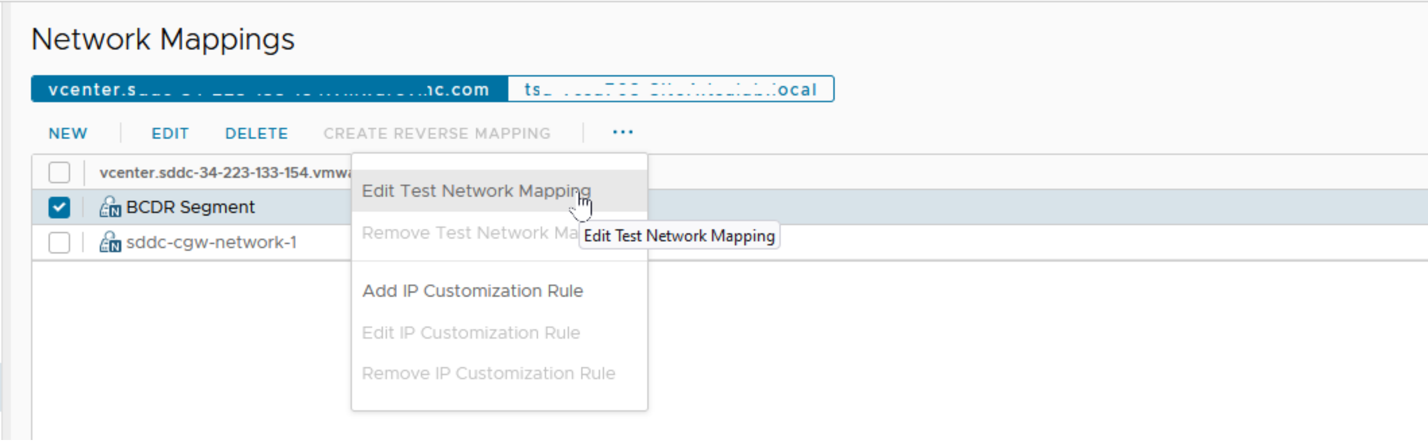
1 Creation mode
2 Recovery networks
3 Reverse mappings
4 Test networks
5 Ready to complete

Ready to complete

Review your settings before finishing the wizard

tsa-[redacted]b.local	vcente[redacted]l.v...	Reverse Mapping	Test Network
TSA-70b-DC01 > TSA-70...	SDDC-Datacenter > vmc-...	Yes	Test DR Segment

If we decide later that we would like to use a dedicated, fenced-off network segment for our **Test Recovery Plans**, we can always go back to **"Network Mappings"**, select the configuration we want to edit (or create a new one), click the "..." on the right-hand side, and click on **"Edit Test Network Mapping"** from the menu.



Network Mappings

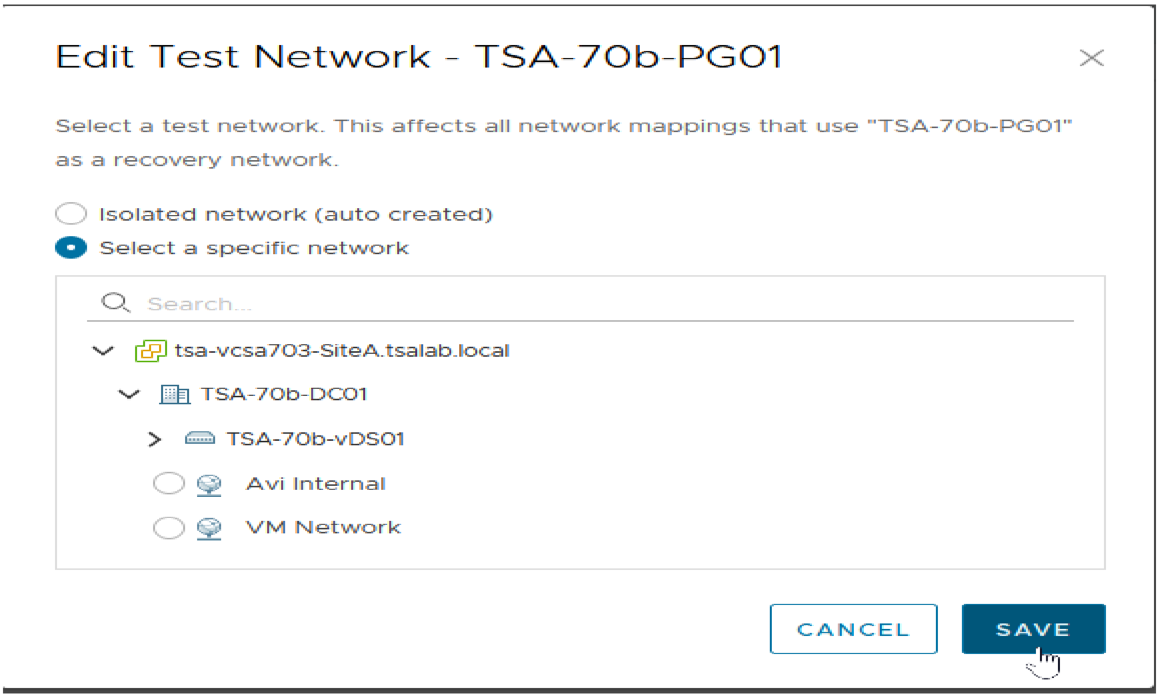
vcenter.s[redacted]c.com | ts[redacted]ocal

NEW
EDIT
DELETE
CREATE REVERSE MAPPING
...

☐ vcenter.sddc-34-223-133-154.vmwa
☑ BCDR Segment
☐ sddc-cgw-network-1

Edit Test Network Mapping
Remove Test Network Ma
Edit Test Network Mapping
Add IP Customization Rule
Edit IP Customization Rule
Remove IP Customization Rule

- Click **"Select a specific network"** and pick the dedicated and isolated recovery network you have prepared for this purpose.
- Click **"Next"** when done.



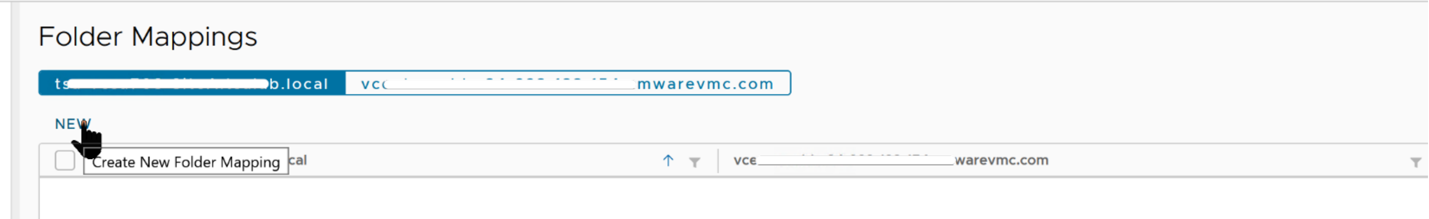
Edit Test Network - TSA-70b-PG01

Select a test network. This affects all network mappings that use "TSA-70b-PG01" as a recovery network.

○ Isolated network (auto created)
● Select a specific network

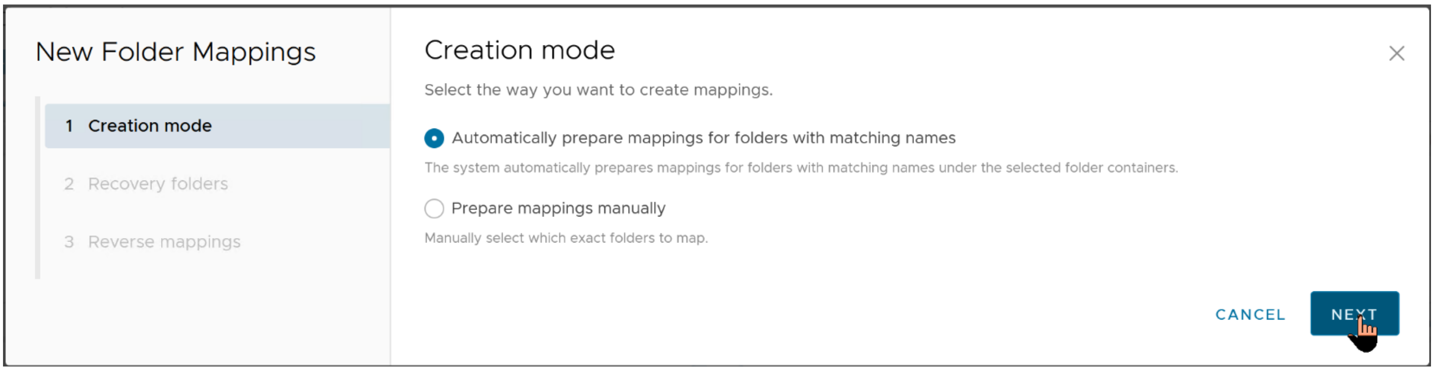
“Folder Mappings” helps us organize our protected and recovered VMs in a logical and intuitive fashion, so let us create one:

1. Click **"New"** to begin.



Folder Mappings

2. Click **"Next".**



New Folder Mappings

Creation mode

Select the way you want to create mappings.

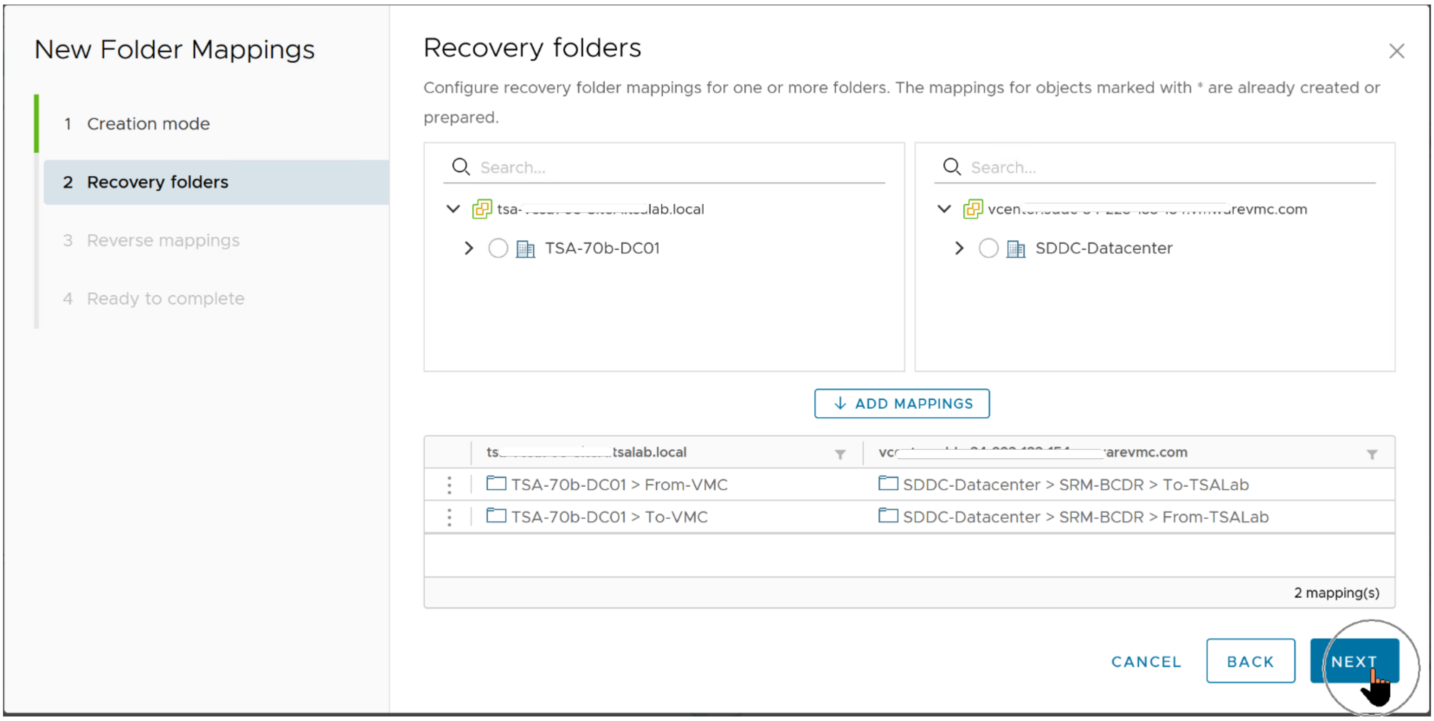
● Automatically prepare mappings for folders with matching names

The system automatically prepares mappings for folders with matching names under the selected folder containers.

○ Prepare mappings manually

Manually select which exact folders to map.

3. Select the **VM Folders** to match up, then click **"Next".**



New Folder Mappings

1 Creation mode
2 Recovery folders
3 Reverse mappings
4 Ready to complete

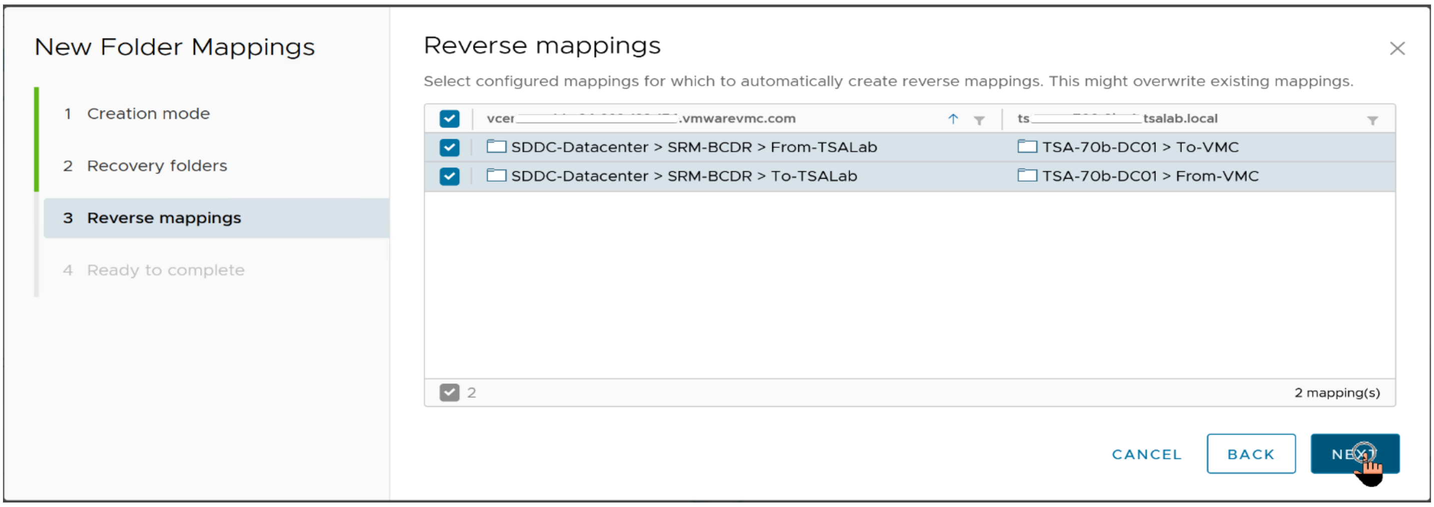
Recovery folders

Configure recovery folder mappings for one or more folders. The mappings for objects marked with * are already created or prepared.

ts[redacted]tsalab.local	vc[redacted]arevmc.com
TSA-70b-DC01 > From-VMC	SDDC-Datacenter > SRM-BCDR > To-TSALab
TSA-70b-DC01 > To-VMC	SDDC-Datacenter > SRM-BCDR > From-TSALab

2 mapping(s)

4. Select the checkboxes to accept the option to automatically create a matching **Folder Map** in the opposite direction.
5. Click **"Next".**



New Folder Mappings

1 Creation mode
2 Recovery folders
3 Reverse mappings
4 Ready to complete

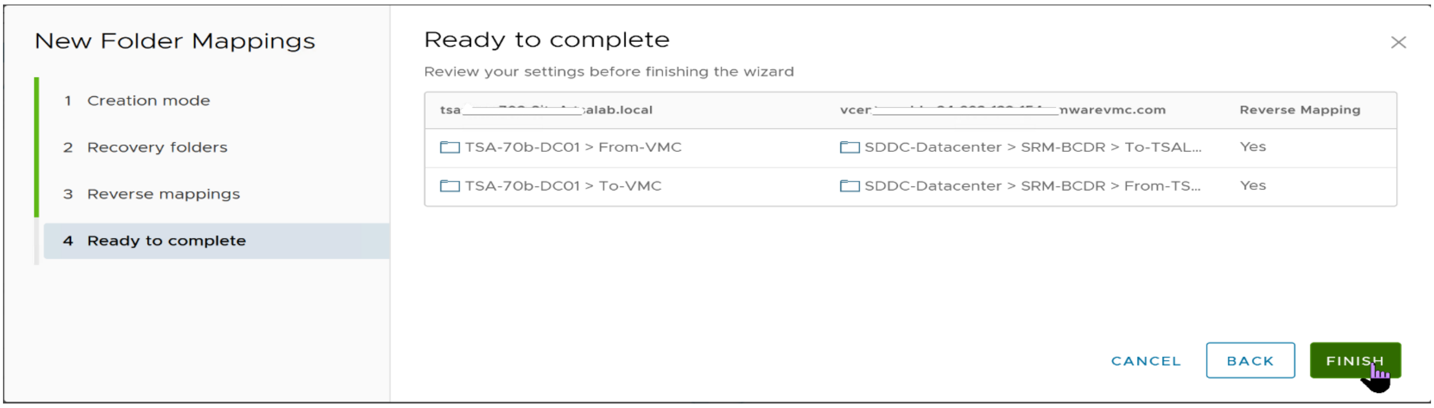
Reverse mappings

Select configured mappings for which to automatically create reverse mappings. This might overwrite existing mappings.

☑	vcer[redacted].vmwarevmc.com	ts[redacted]tsalab.local
☑	SDDC-Datacenter > SRM-BCDR > From-TSALab	TSA-70b-DC01 > To-VMC
☑	SDDC-Datacenter > SRM-BCDR > To-TSALab	TSA-70b-DC01 > From-VMC

☑ 2 2 mapping(s)

6. Click **"Finish".**



New Folder Mappings

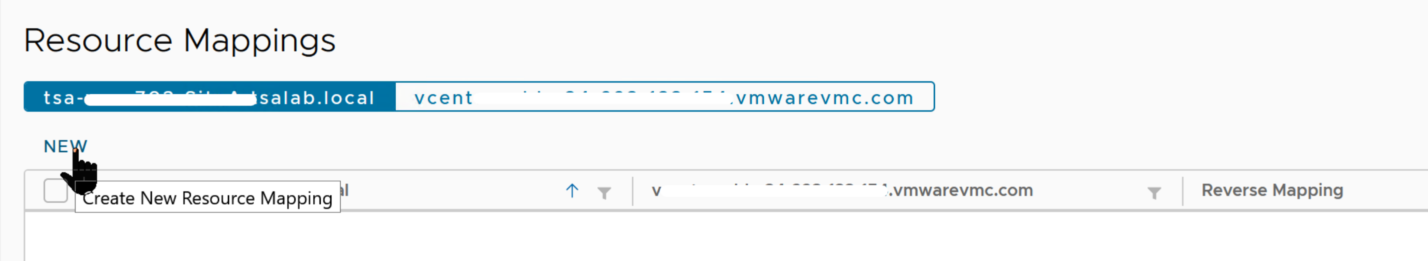
1 Creation mode
2 Recovery folders
3 Reverse mappings
4 Ready to complete

Ready to complete

Review your settings before finishing the wizard

tsa[redacted]alab.local	vcer[redacted]nwarevmc.com	Reverse Mapping
TSA-70b-DC01 > From-VMC	SDDC-Datacenter > SRM-BCDR > To-TSAL...	Yes
TSA-70b-DC01 > To-VMC	SDDC-Datacenter > SRM-BCDR > From-TS...	Yes

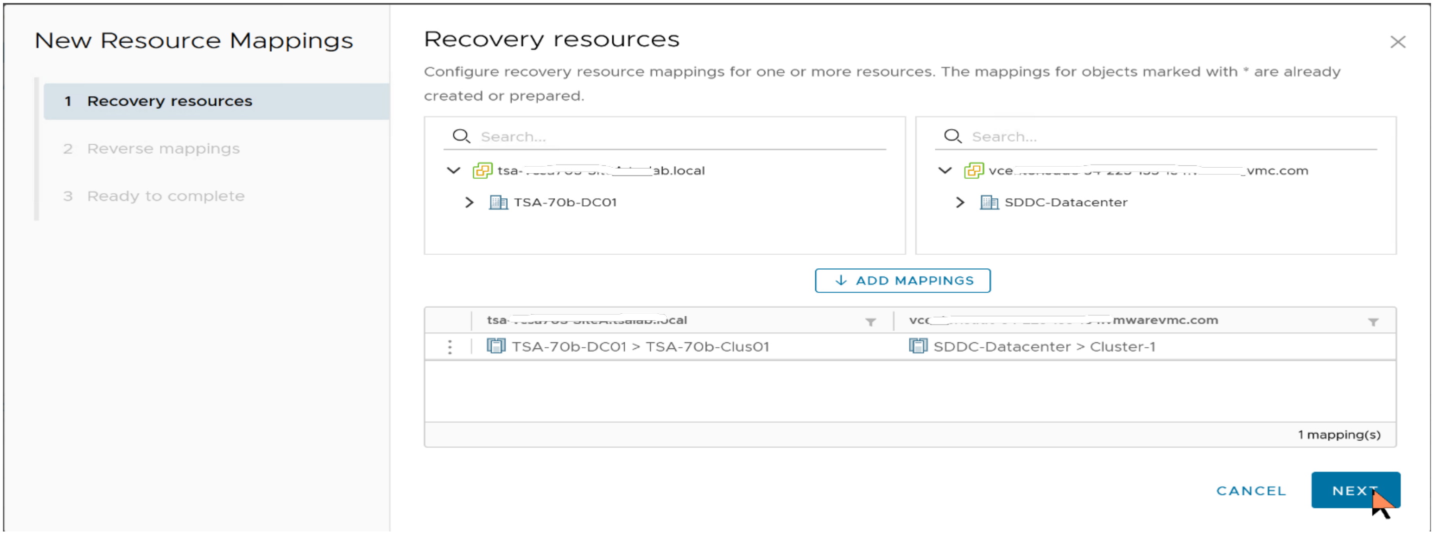
7. For **"Resource Mappings"**, we will (again) just map our resources at the highest level possible (Cluster level, in this case).
8. Click **"New"** to begin.



Resource Mappings

tsa-[redacted]salab.local | vcent[redacted].vmwarevmc.com

9. Select the Cluster containing your protected workloads and map it to the cluster you would like for them to be placed in at the **Recovery Site.**
10. Click **"Add Mappings"**, then click **"Next"**



New Resource Mappings

1 Recovery resources
2 Reverse mappings
3 Ready to complete

Recovery resources

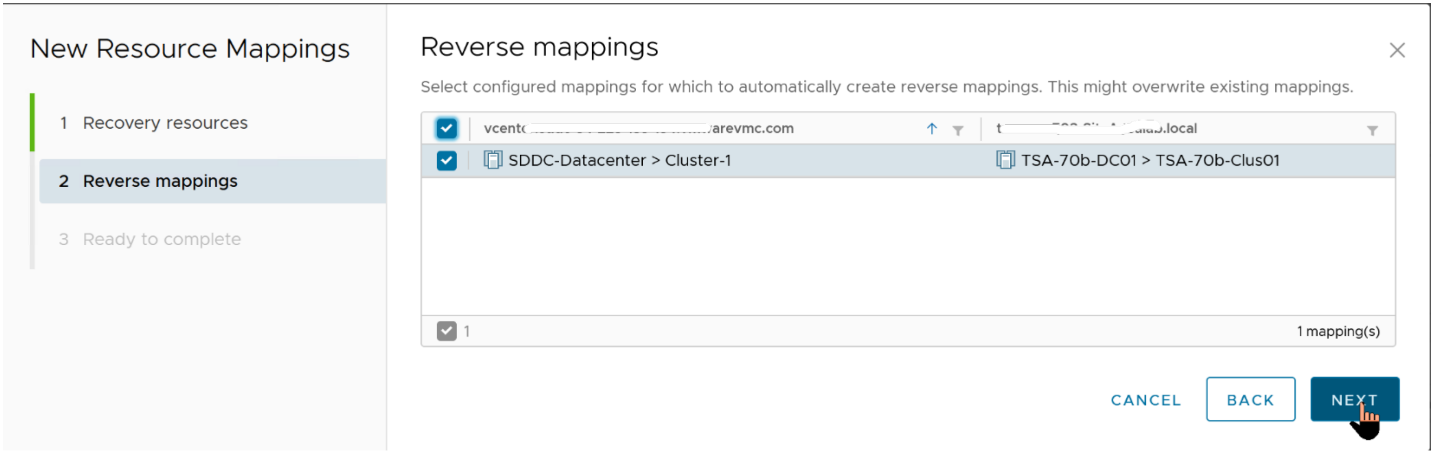
Configure recovery resource mappings for one or more resources. The mappings for objects marked with * are already created or prepared.

tsa-[redacted]ab.local	vce[redacted]vmc.com
TSA-70b-DC01	SDDC-Datacenter

tsa[redacted]cal	vcc[redacted]mwarevmc.com
TSA-70b-DC01 > TSA-70b-Clus01	SDDC-Datacenter > Cluster-1

1 mapping(s)

11. Accept the option to auto-configure a reverse mapping, then click **"Next".**



New Resource Mappings

1 Recovery resources
2 Reverse mappings
3 Ready to complete

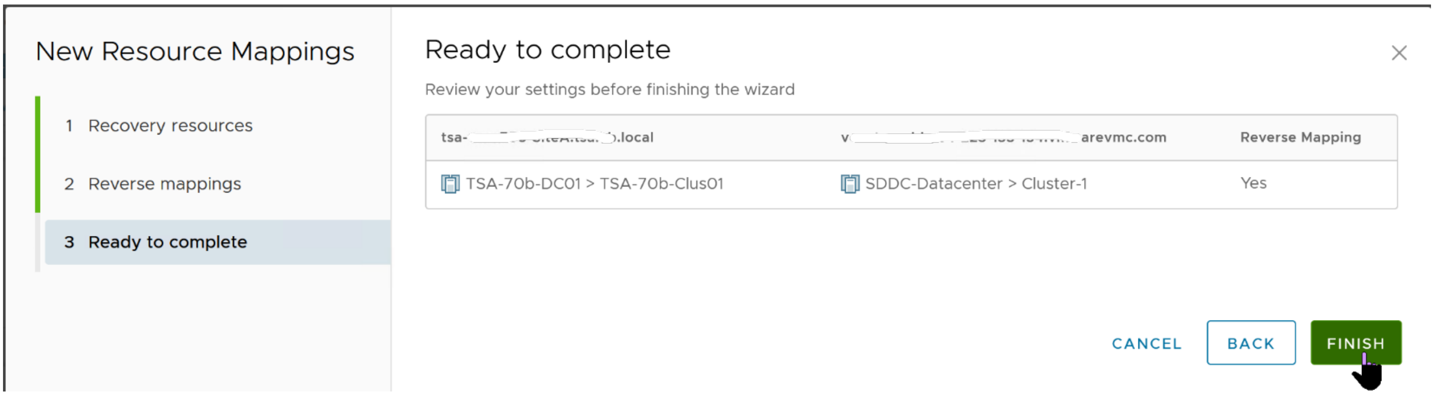
Reverse mappings

Select configured mappings for which to automatically create reverse mappings. This might overwrite existing mappings.

☑	vcent[redacted]arevmc.com	t[redacted].local
☑	SDDC-Datacenter > Cluster-1	TSA-70b-DC01 > TSA-70b-Clus01

☑ 1 | 1 mapping(s)

12. Click **"Finish"** to complete the process.



New Resource Mappings

1 Recovery resources

2 Reverse mappings

3 Ready to complete

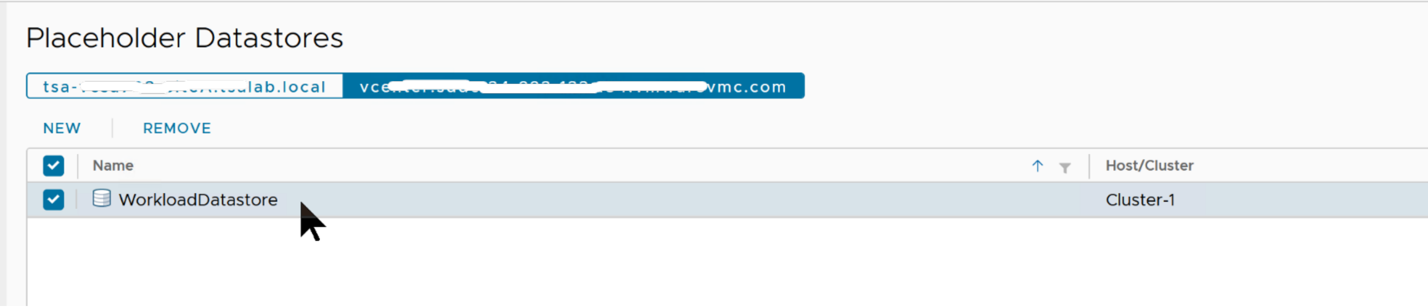
Ready to complete

Review your settings before finishing the wizard

tsa-[redacted].local	v[redacted]arevmc.com	Reverse Mapping
TSA-70b-DC01 > TSA-70b-Clus01	SDDC-Datacenter > Cluster-1	Yes

When SRM uses vSphere Replication to replicate a **Protected VM** to the **Recovery Site**, it also creates a representation of the VM in the vCenter at the Recovery Site. This representation is somewhat similar to the vmx file that describes the running VM at the **Protected Site**. The major difference is that this representation is just a placeholder (aka **"Stub"**), which cannot be powered on. This placeholder file is stored in a designated datastore, which is not the same datastore that has the full replicated copy of the protected VM. The "Placeholder" Datastore needs to exist on both sides, to enable SRM to protect workloads in either direction.

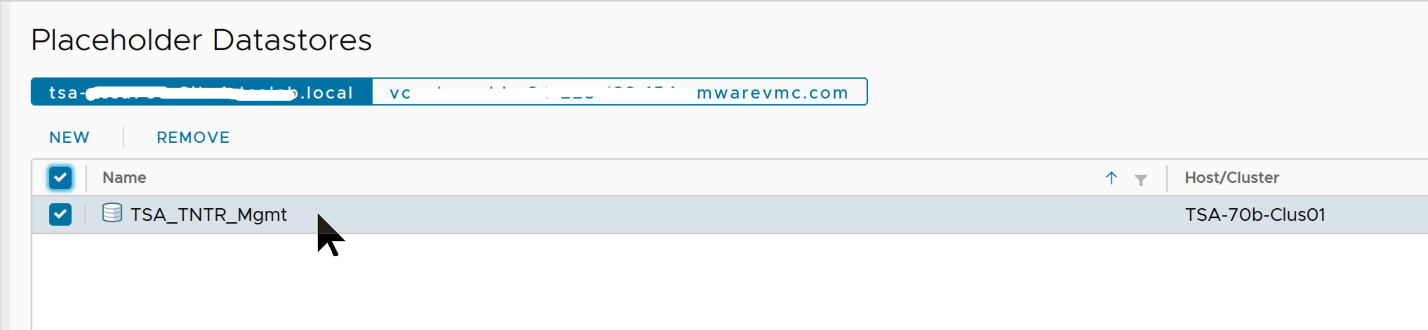
Here is our **Placeholder Datastore** at the **Recovery Site:**



Placeholder Datastores

☑	Name	Host/Cluster
☑	WorkloadDatastore	Cluster-1

Here is our **Placeholder Datastore** at the **Protected Site:**



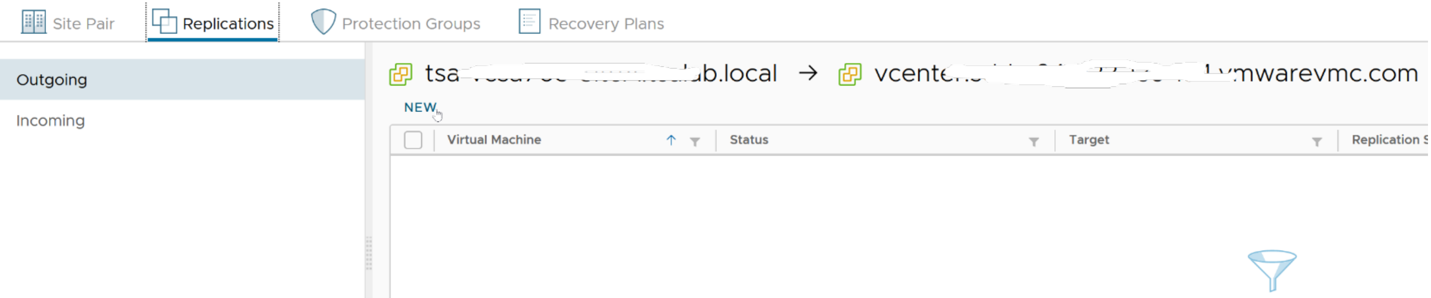
Placeholder Datastores

☑	Name	Host/Cluster
☑	TSA_TNTR_Mgmt	TSA-70b-Clus01

For SRM to protect and recover a VM, a copy of that VM must make its way from the Protected Site to the Recovery Site. Let us set up the replication part of the exercise now.

In this Guide, the Source (Protected) Site is our on-Premises VMware vSphere infrastructure, so let's switch to that and create our "Outgoing" Replication.

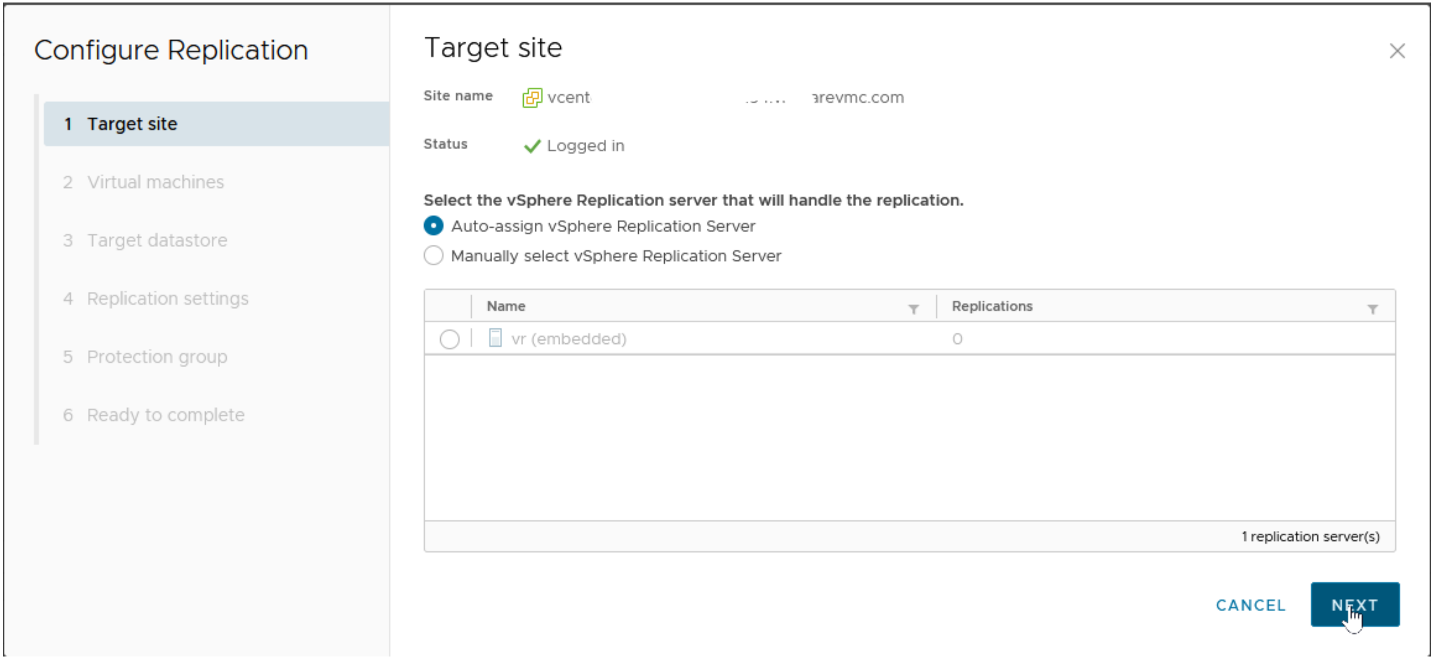
13. Click **"New".**



□	Virtual Machine	Status	Target	Replication S

The Target (Recovery) Site is our VMware Hybrid Cloud infrastructure, which the process auto-identifies (because they are already paired).

- Leave the option to auto-assign **vSphere Replication Server** at default and click **"Next".**



Configure Replication

1 Target site
2 Virtual machines
3 Target datastore
4 Replication settings
5 Protection group
6 Ready to complete

Target site

Site name: vcent[redacted]arevmc.com

Status: ✓ Logged in

Select the vSphere Replication server that will handle the replication.

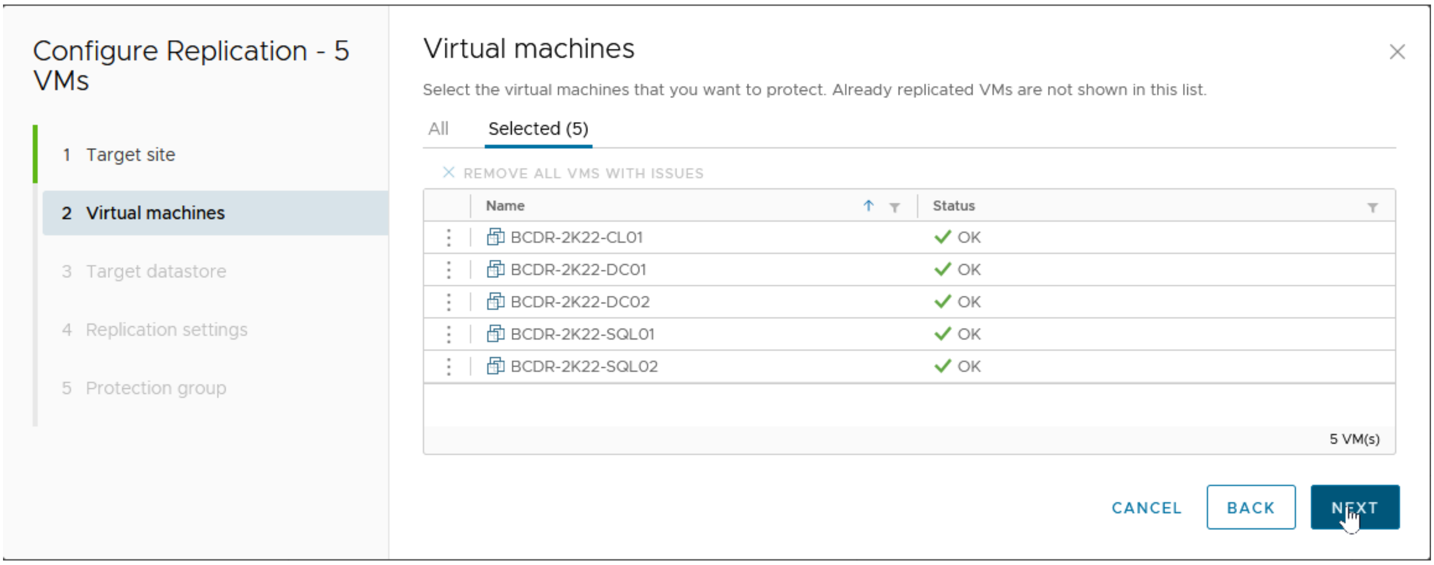
● Auto-assign vSphere Replication Server
○ Manually select vSphere Replication Server

	Name	Replications
○	vr (embedded)	0

1 replication server(s)

Here is where the previous **"Mapping"** exercises we completed in previous steps begin to pay dividends. Because we mapped only a specific **VM Folder**, we can focus our attention on only the specific workloads we would like to replicate as part of our **Disaster Recovery** operation.

- For our purpose, all the VMs in this folder are in-scope, so we will select all of them and click **"Next".**



Configure Replication - 5 VMs

1 Target site
2 Virtual machines
3 Target datastore
4 Replication settings
5 Protection group

Virtual machines

Select the virtual machines that you want to protect. Already replicated VMs are not shown in this list.

All | Selected (5)

✕ REMOVE ALL VMS WITH ISSUES

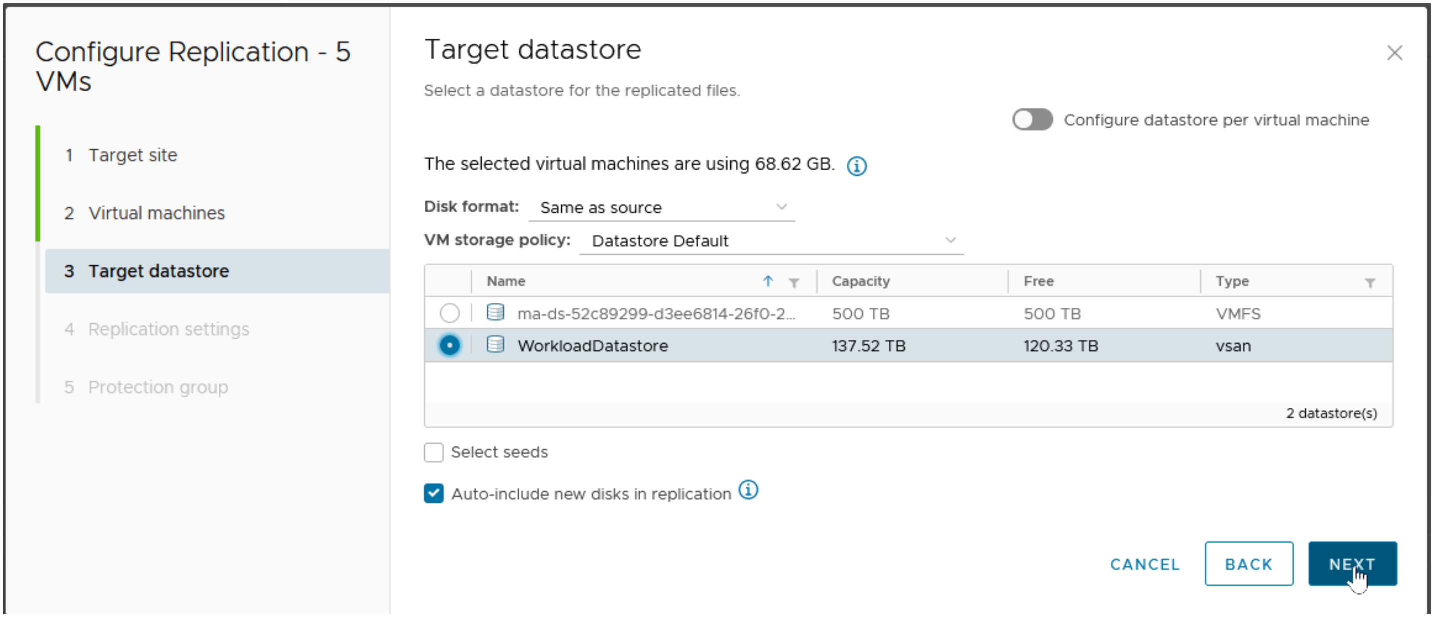
Name	Status
BCDR-2K22-CL01	✓ OK
BCDR-2K22-DC01	✓ OK
BCDR-2K22-DC02	✓ OK
BCDR-2K22-SQL01	✓ OK
BCDR-2K22-SQL02	✓ OK

5 VM(s)

- We select the target datastore.
  - **NOTE:** The option to "Auto-include new disks in replication" is one of the amazing things about vSphere Replication. It anticipates situations where a Protected VM's configuration could change at a later date after we have set up our DR plans. With this option, vSphere Replication automatically incorporates the changes into the

replication tasks

- Select this option, then click **"Next".**



Configure Replication - 5 VMs

1 Target site
2 Virtual machines
3 Target datastore
4 Replication settings
5 Protection group

Target datastore

Select a datastore for the replicated files.

Configure datastore per virtual machine

The selected virtual machines are using 68.62 GB.

Disk format: Same as source

VM storage policy: Datastore Default

	Name	Capacity	Free	Type
○	ma-ds-52c89299-d3ee6814-26f0-2...	500 TB	500 TB	VMFS
●	WorkloadDatastore	137.52 TB	120.33 TB	vsan

2 datastore(s)

□ Select seeds

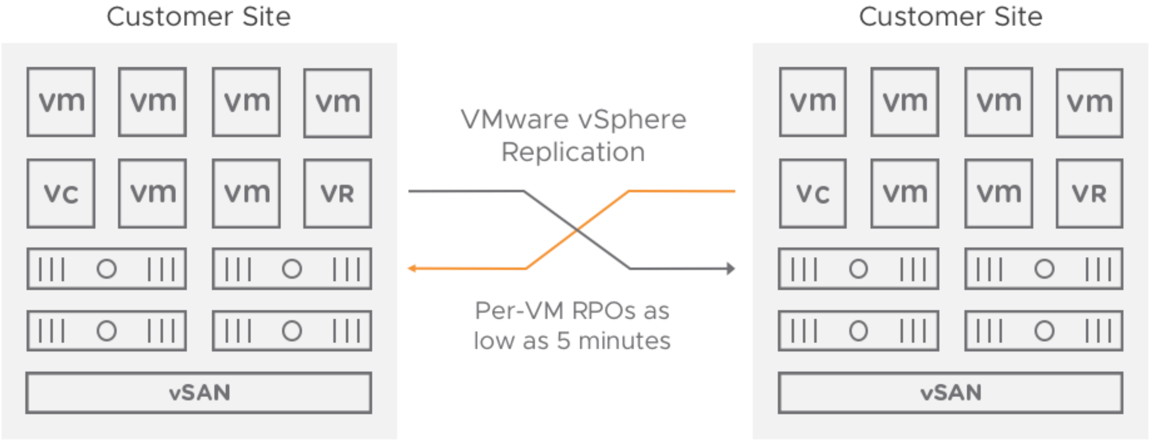
☑ Auto-include new disks in replication

RPO/RTO, Run Book, Protection Group and Recovery Plan Defined

"RPO" and **"RTO"** are probably two of the most over-used acronyms when discussing Disaster Recovery of Mission Critical Applications in the Enterprise. We have consciously avoided mentioning them until now because (as technical topics) they deserve whole book-length attention which we cannot accommodate in this guide. So, simply put:

- **RTO (Recovery Time Objective)** is the term used for measuring how long it would take an enterprise to recover from a disaster event and begin to operate at tolerable capacity. The "Objective" is to make this window as short as technologically and humanly possible.
  - Because an **RTO** is influenced by several external, environmental, and infrastructural factors, we will not be demonstrating this consideration in this guide.
- **RPO (Recovery Point Objective)** is the term used for measuring the tolerable loss of services or data in a disaster event. It measures the up-to-dateness of the Enterprise's data after such an event. While every administrator, operator and business owner/stakeholder desires an RPO of 0, financial, human and technological constraints make such desire difficult to attain at this time.

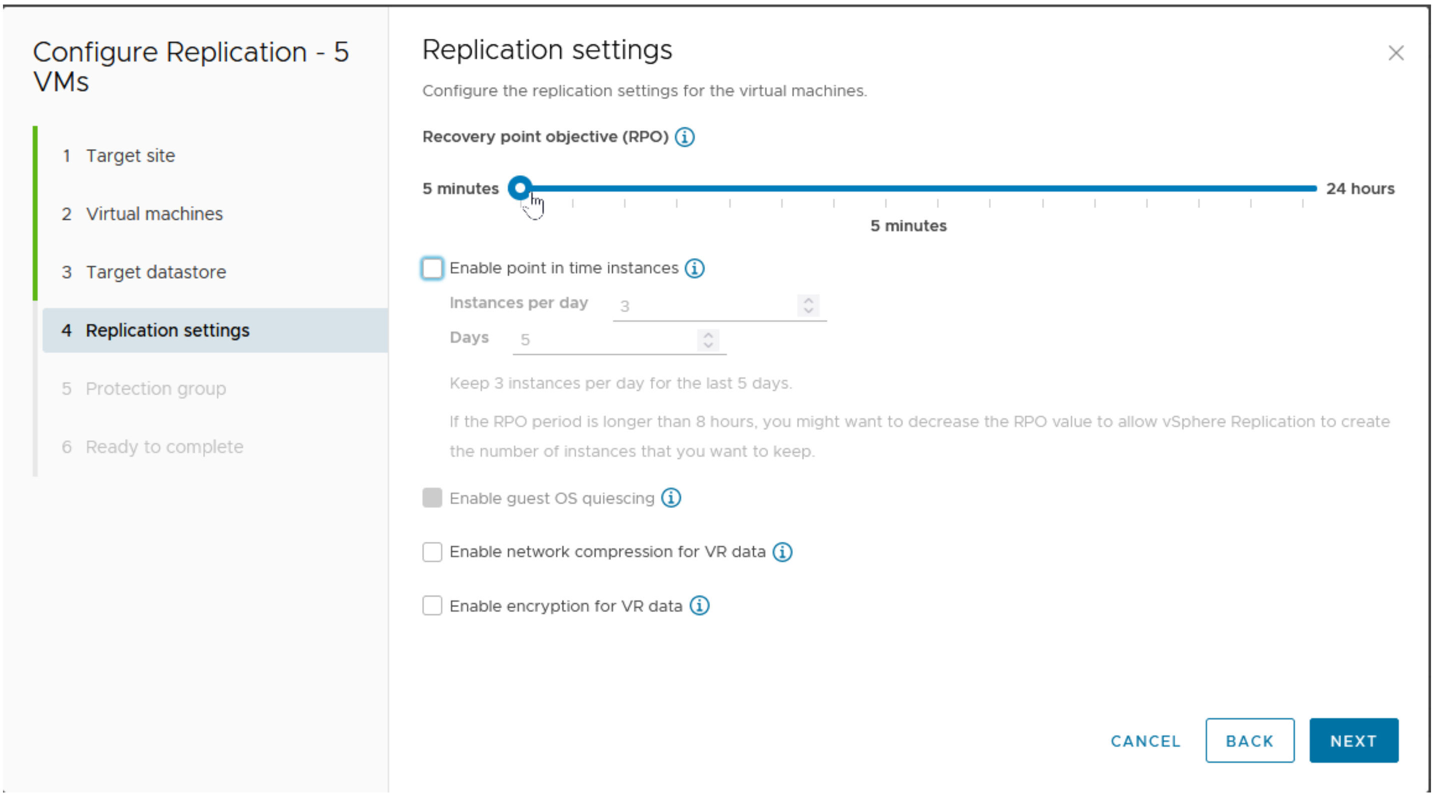
vSphere Replication provides a 5-minute RPO at best. This means that, all things being equal, vSphere Replication attempts to synchronize and replicate every state change in the Protected VM as frequently as every 5 minutes. This means that, at any point in time, the copy of the VM at the Recovery Site is identical to the original Protected VM as of no more than 5 minutes ago. On the extreme end of the spectrum, vSphere Replication can also be configured to maintain a 24-hour RPO.



Site Recovery Manager Technical Overview

We will skip discussion of the other capabilities and features on this screen because they are well documented in the vSphere Replication Admin Guide and they are unimportant for this guide.

- Let's set our RPO to 5 minutes and click **"Next"**.



Configure Replication - 5 VMs

1 Target site
2 Virtual machines
3 Target datastore
4 Replication settings
5 Protection group
6 Ready to complete

Replication settings

Configure the replication settings for the virtual machines.

Recovery point objective (RPO) ⓘ

5 minutes ● 24 hours

5 minutes

□ Enable point in time instances ⓘ

Instances per day 3

Days 5

Keep 3 instances per day for the last 5 days.

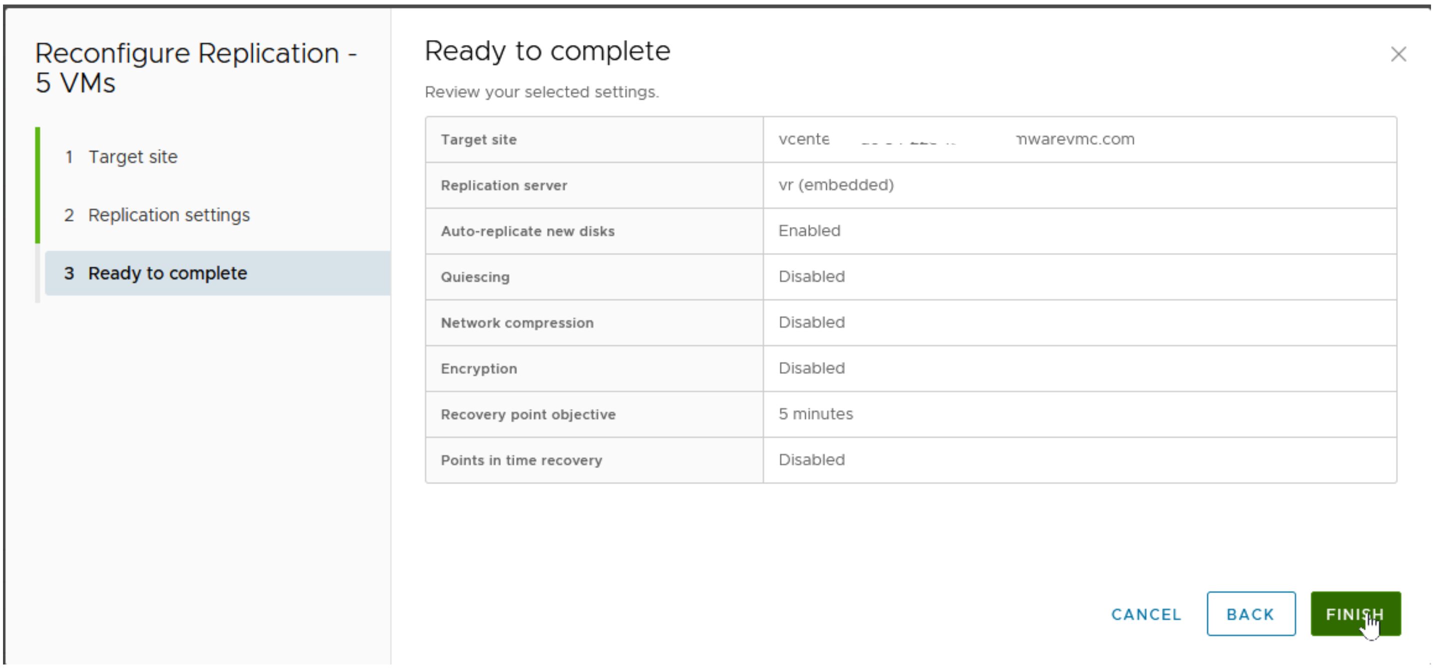
If the RPO period is longer than 8 hours, you might want to decrease the RPO value to allow vSphere Replication to create the number of instances that you want to keep.

□ Enable guest OS quiescing ⓘ

□ Enable network compression for VR data ⓘ

□ Enable encryption for VR data ⓘ

- Review the choices, then click "Finish".

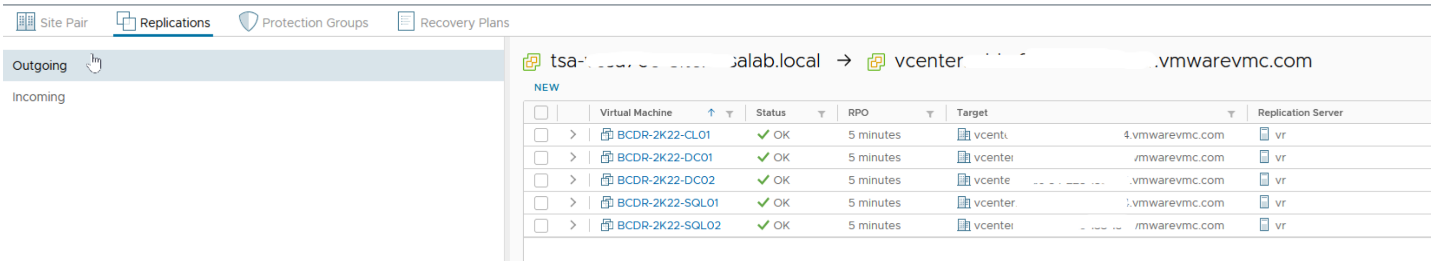


Ready to complete

Review your selected settings.

Target site	vcente [redacted] nwarevmc.com
Replication server	vr (embedded)
Auto-replicate new disks	Enabled
Quiescing	Disabled
Network compression	Disabled
Encryption	Disabled
Recovery point objective	5 minutes
Points in time recovery	Disabled

We are done with setting up the replication.



tsa-[redacted]salab.local → vcenter[redacted].vmwarevmc.com

		Virtual Machine	Status	RPO	Target	Replication Server
☐	>	BCDR-2K22-CL01	✓ OK	5 minutes	vcent[redacted]4.vmwarevmc.com	vr
☐	>	BCDR-2K22-DC01	✓ OK	5 minutes	vcenter[redacted]vmwarevmc.com	vr
☐	>	BCDR-2K22-DC02	✓ OK	5 minutes	vcente[redacted].vmwarevmc.com	vr
☐	>	BCDR-2K22-SQL01	✓ OK	5 minutes	vcenter[redacted].vmwarevmc.com	vr
☐	>	BCDR-2K22-SQL02	✓ OK	5 minutes	vcenter[redacted]vmwarevmc.com	vr

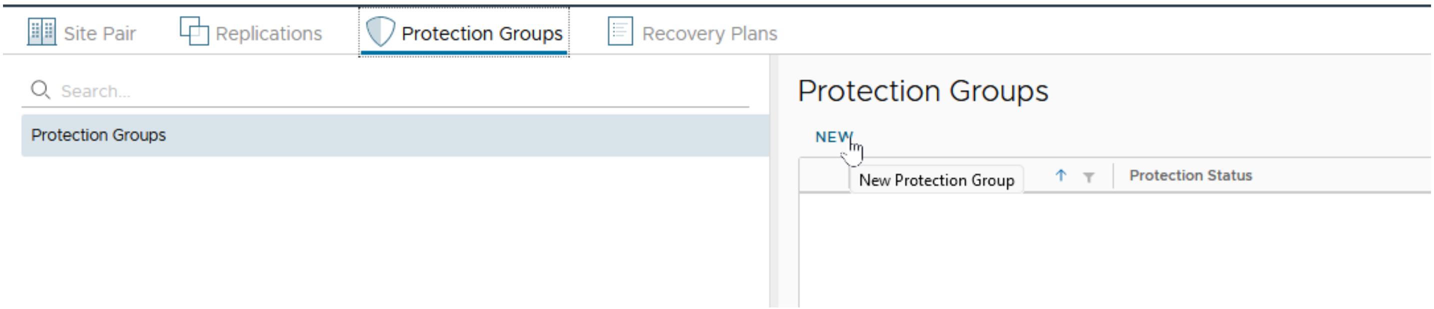
We spent some time discussing upstream and downstream dependencies earlier in this guide. Enterprise-scale Business Critical Applications generally do not exist or operate in a vacuum.

They depend on other services and workloads, and they are similarly dependent upon by others. When designing a BCDR plan, these dependencies influence configuration and workflow choices and options. SRM provides a mechanism for grouping protected workloads together in a way that helps us control their recovery in an orderly fashion to achieve our recovery objectives. A Protection Group in SRM is one such grouping.

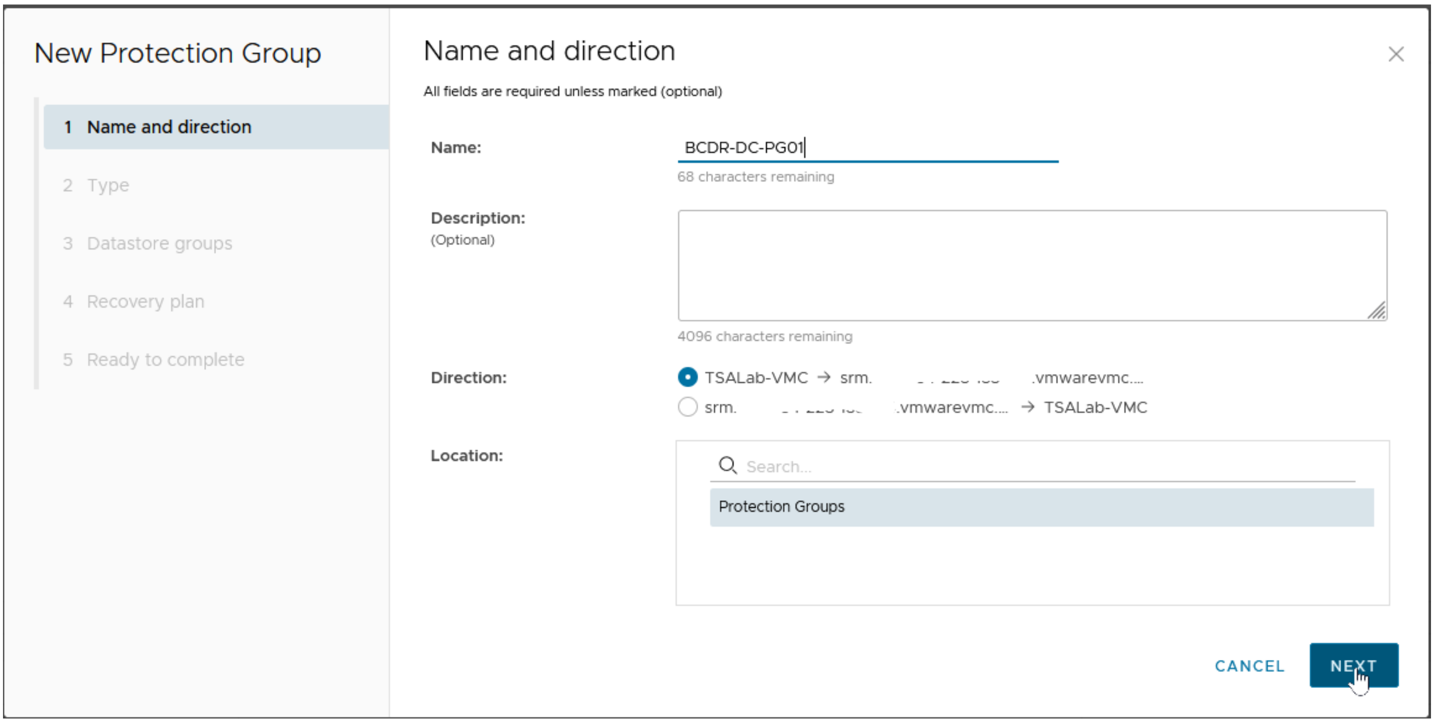
A **Protection Group** contains VMs that we intend to recover together as a unit for any number of reasons. Many factors (the type of storage and the unit of replication are common examples) influence the decision-making processes involved in creating and using Protection Groups.

For our purpose, we will create **Protection Groups** based on the services and characteristics of the VMs we are protecting and recovering. We have three distinct categories *(Domain Controllers, SQL Server and a Windows Client)*, so this is the primary influence on our configuration choice.

Click on the "**Protection Groups**" tab and select "**New**".



- Give the Group a descriptive name.
- Description is optional.
- The Direction is from our **Protected Site** to our **Recovery Site.**
- Click **"Next".**



New Protection Group

1 Name and direction
2 Type
3 Datastore groups
4 Recovery plan
5 Ready to complete

Name and direction

All fields are required unless marked (optional)

Name: BCDR-DC-PG01
68 characters remaining

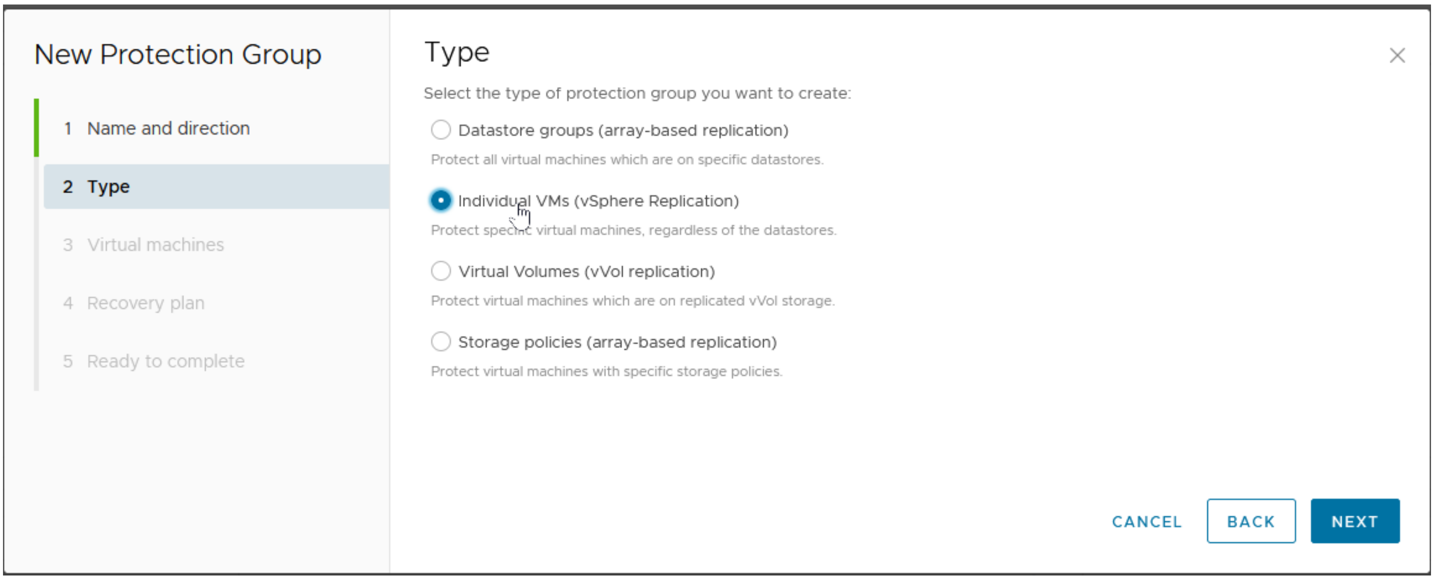
Description:
(Optional)
4096 characters remaining

Direction:
● TSALab-VMC → srm.[redacted].vmwarevmc....
○ srm.[redacted].vmwarevmc.... → TSALab-VMC

Location:
Search...
Protection Groups

CANCEL NEXT

Because we are using vSphere Replication here, we select **"Individual VMs..."** and click **"Next"**



New Protection Group

1 Name and direction
2 Type
3 Virtual machines
4 Recovery plan
5 Ready to complete

Type

Select the type of protection group you want to create:

○ Datastore groups (array-based replication)
Protect all virtual machines which are on specific datastores.

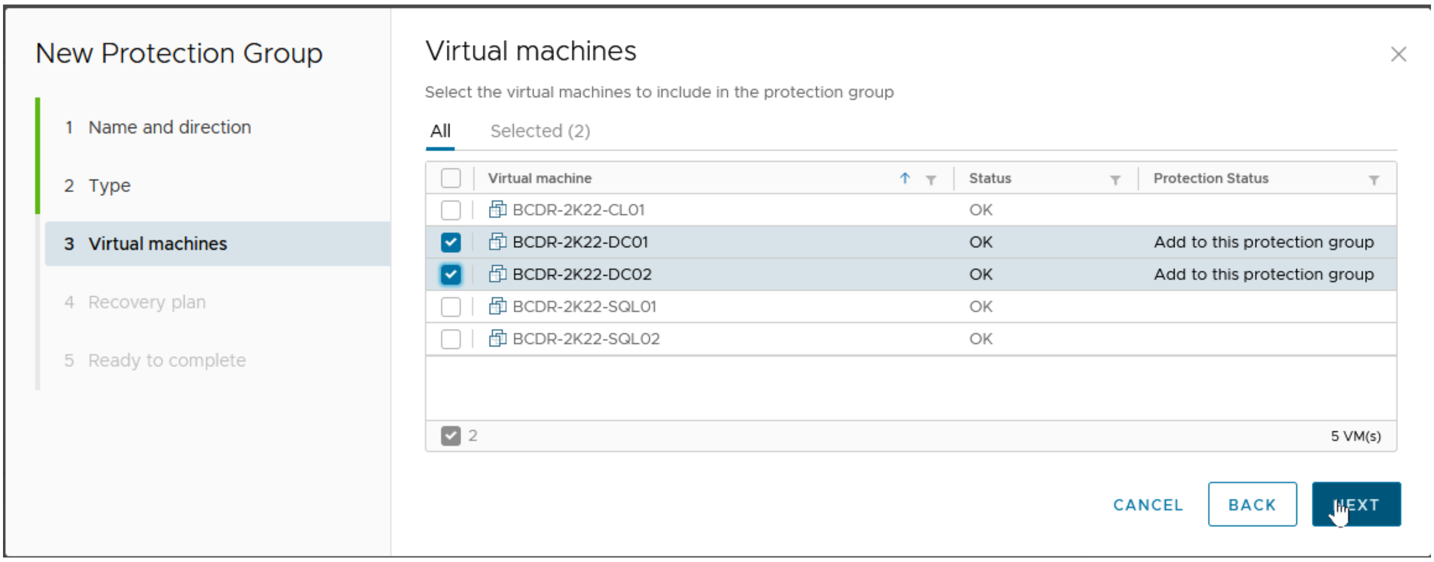
● Individual VMs (vSphere Replication)
Protect specific virtual machines, regardless of the datastores.

○ Virtual Volumes (vVol replication)
Protect virtual machines which are on replicated vVol storage.

○ Storage policies (array-based replication)
Protect virtual machines with specific storage policies.

CANCEL BACK NEXT

- This is for the Domain Controllers, so we will select the applicable VMs and click **"Next".**


New Protection Group

1 Name and direction
2 Type
3 Virtual machines
4 Recovery plan
5 Ready to complete

Virtual machines

Select the virtual machines to include in the protection group

All | Selected (2)

☐	Virtual machine	Status	Protection Status
☐	BCDR-2K22-CL01	OK	
☑	BCDR-2K22-DC01	OK	Add to this protection group
☑	BCDR-2K22-DC02	OK	Add to this protection group
☐	BCDR-2K22-SQL01	OK	
☐	BCDR-2K22-SQL02	OK	

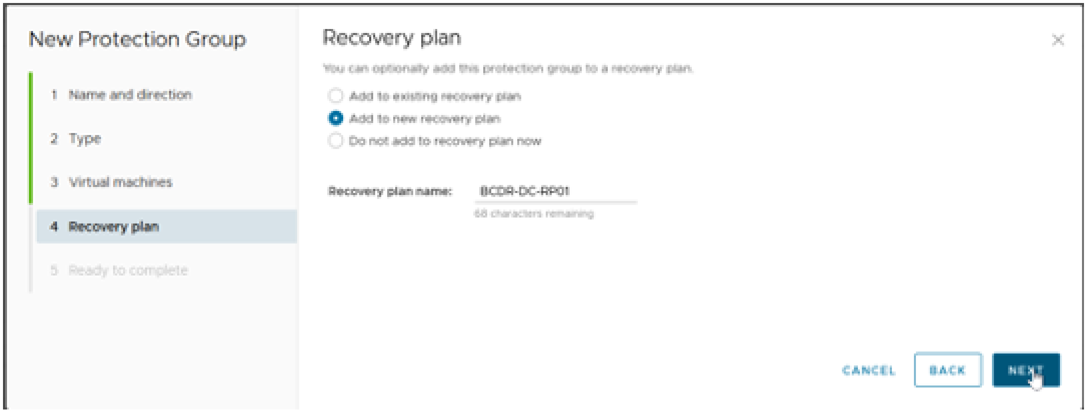
☑ 2 — 5 VM(s)

A **Recovery Plan** is where we define and configure the recovery steps, plans and actions guiding our entire BCDR Plan. You can imagine it as the **"Run Book"** to which an administrator would typically refer to and follow if they were to perform a Disaster Recovery operation manually.

The SRM **Recovery Plan** contains all the logic and flow of getting the copy of the Protected VM up and running in the Recovery Site when a disaster is declared, and the recovery is initiated. Recovery Plans contain at least one Protection Group which, as we have seen, is a grouping of the VMs we are protecting.

A **Protection Group** must be added to at least one Recovery Plan. We do not have a **Recovery Plan** yet, so we will create one here:

- Choose **"Add to a new recovery plan"**
- Give it an intuitive and descriptive name, then click **"Next"**


New Protection Group

1 Name and direction
2 Type
3 Virtual machines
4 Recovery plan
5 Ready to complete

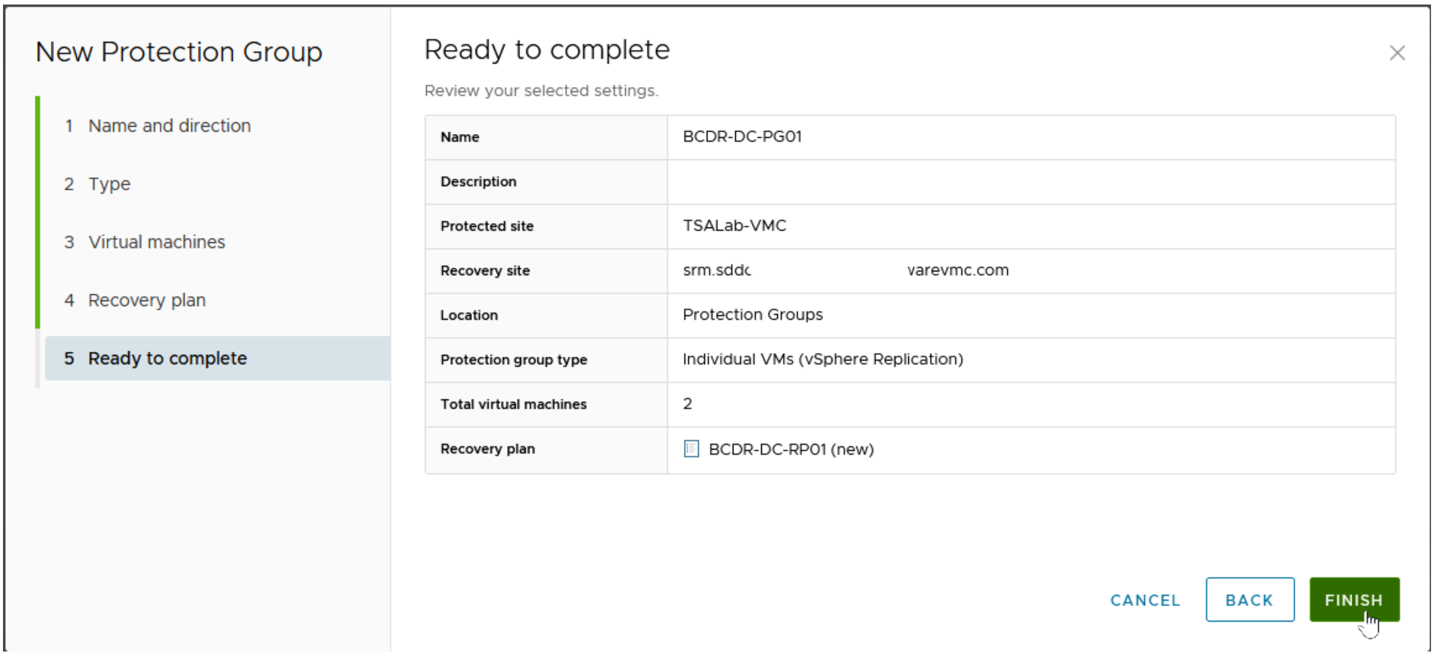
Recovery plan

You can optionally add this protection group to a recovery plan.

○ Add to existing recovery plan
● Add to new recovery plan
○ Do not add to recovery plan now

Recovery plan name: BCDR-DC-RP01
68 characters remaining

- Review the result, then click **"Finish"**.



New Protection Group

1 Name and direction
2 Type
3 Virtual machines
4 Recovery plan
5 Ready to complete

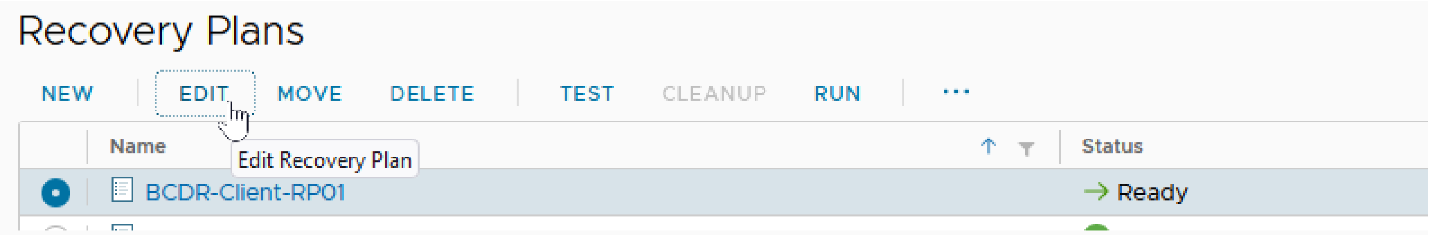
Ready to complete

Review your selected settings.

Name	BCDR-DC-PG01
Description	
Protected site	TSALab-VMC
Recovery site	srm.sddc varevmc.com
Location	Protection Groups
Protection group type	Individual VMs (vSphere Replication)
Total virtual machines	2
Recovery plan	BCDR-DC-RP01 (new)

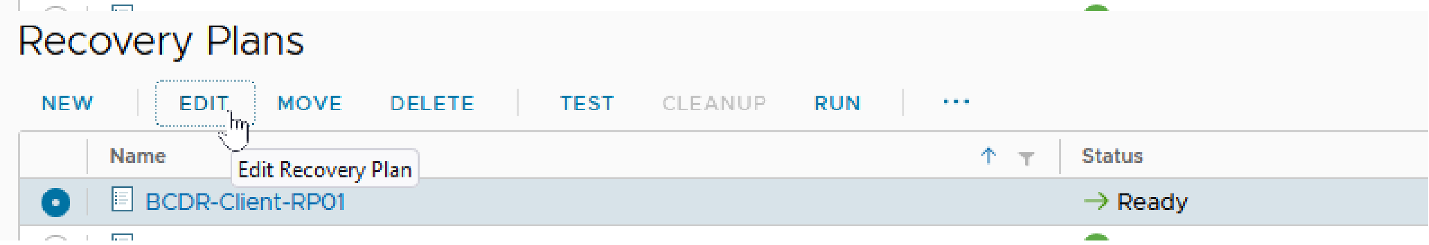
One of the most common tasks you would like to perform on a recovery plan is to configure the specific Test (**"Bubble"**) network you would like to recover VMs into during a "Test Recovery" exercise:

- To do this, select the **Recovery Plan**, then click on **"Edit".**



Recovery Plans

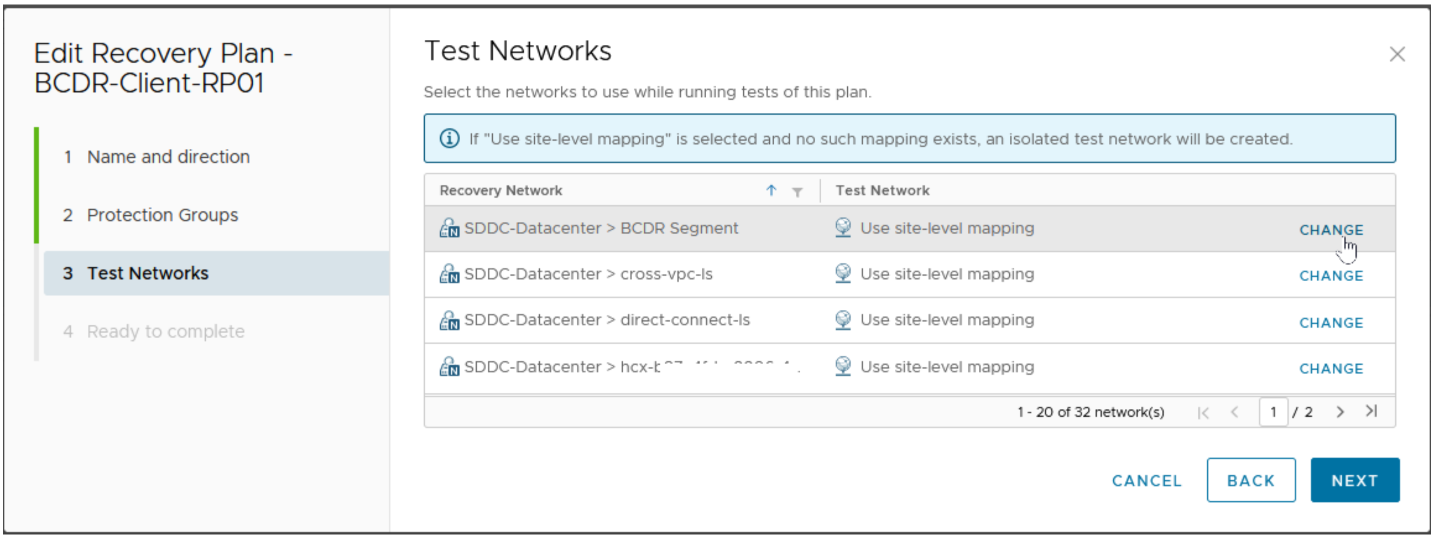
Name	Status
BCDR-Client-RP01	Ready



Recovery Plans

Name	Status
BCDR-Client-RP01	Ready

From this menu, you can select the "Test Network" you prefer for this Recovery Plan.



Edit Recovery Plan - BCDR-Client-RP01

1 Name and direction
2 Protection Groups
3 Test Networks
4 Ready to complete

Test Networks

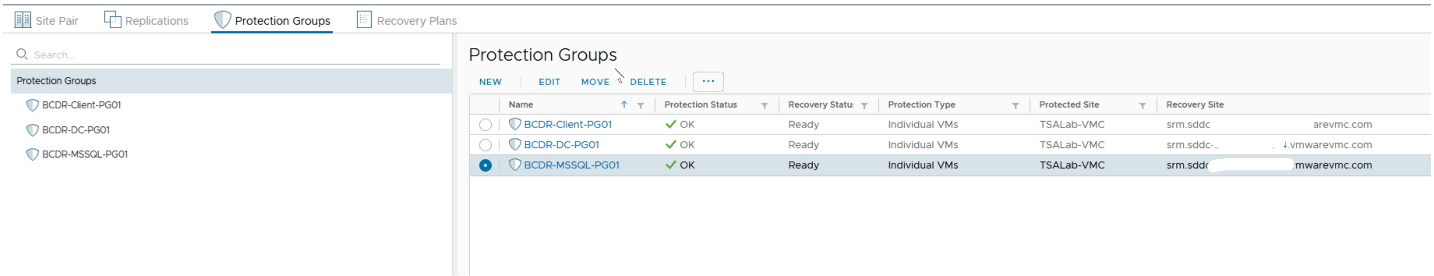
Select the networks to use while running tests of this plan.

ⓘ If "Use site-level mapping" is selected and no such mapping exists, an isolated test network will be created.

Recovery Network	Test Network	
SDDC-Datacenter > BCDR Segment	Use site-level mapping	CHANGE
SDDC-Datacenter > cross-vpc-ls	Use site-level mapping	CHANGE
SDDC-Datacenter > direct-connect-ls	Use site-level mapping	CHANGE
SDDC-Datacenter > hcx-b[illegible]	Use site-level mapping	CHANGE

1 - 20 of 32 network(s) 1 / 2

We will repeat the process to create an additional **recovery plan** for each of the other types of workloads in our use case.

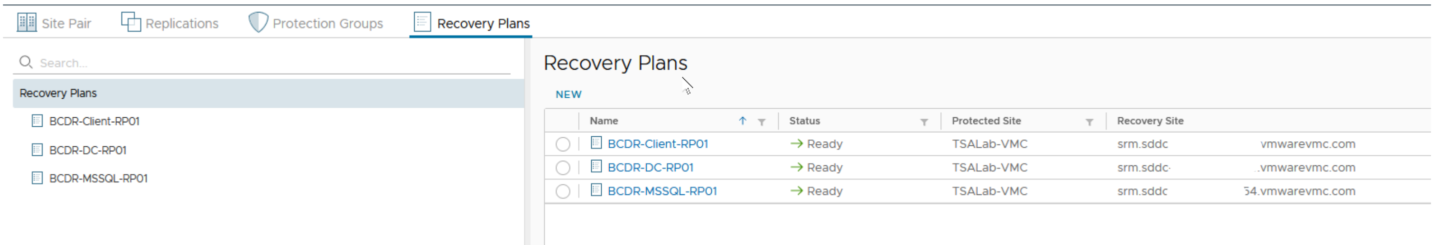


Protection Groups

	Name	Protection Status	Recovery Statu:	Protection Type	Protected Site	Recovery Site
○	BCDR-Client-PG01	✓ OK	Ready	Individual VMs	TSALab-VMC	srm.sddc [redacted] arevmc.com
○	BCDR-DC-PG01	✓ OK	Ready	Individual VMs	TSALab-VMC	srm.sddc- [redacted] ł.vmwarevmc.com
●	BCDR-MSSQL-PG01	✓ OK	Ready	Individual VMs	TSALab-VMC	srm.sddc [redacted] mwarevmc.com

For each of these **Protection Groups**, we create a corresponding **Recovery Plan**. We do this because, based on our need to ensure that one group of protected workloads (the Domain Controllers) becomes completely available before the others are brought online, we want to be able to initiate the recovery of each workload type separately.

Here are our **Recovery Plans**



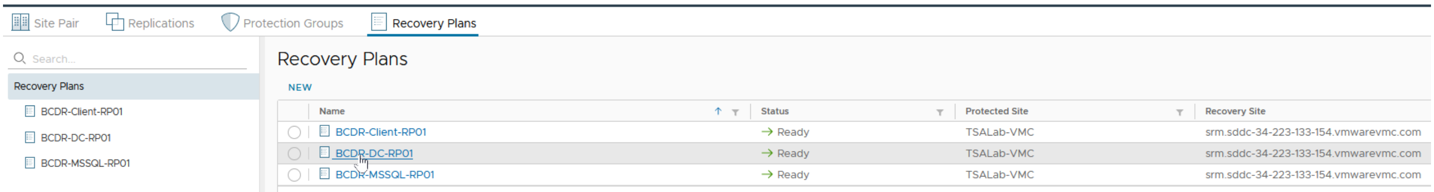
Recovery Plans

	Name	Status	Protected Site	Recovery Site
○	BCDR-Client-RP01	→ Ready	TSALab-VMC	srm.sddc [redacted] vmwarevmc.com
○	BCDR-DC-RP01	→ Ready	TSALab-VMC	srm.sddc- [redacted] .vmwarevmc.com
○	BCDR-MSSQL-RP01	→ Ready	TSALab-VMC	srm.sddc [redacted] 54.vmwarevmc.com

We have previously mentioned that **Recovery Plans** are essentially the **Run Book** for BCDR Projects in SRM. We shall now proceed to define the elements of our Run Book in each of the Recovery Plans.

We are going to configure the **"BCDR-DC-RP01"** Plan, which is the **Recovery Plan** covering our **Run Book** for recovering the **Domain Controllers.**

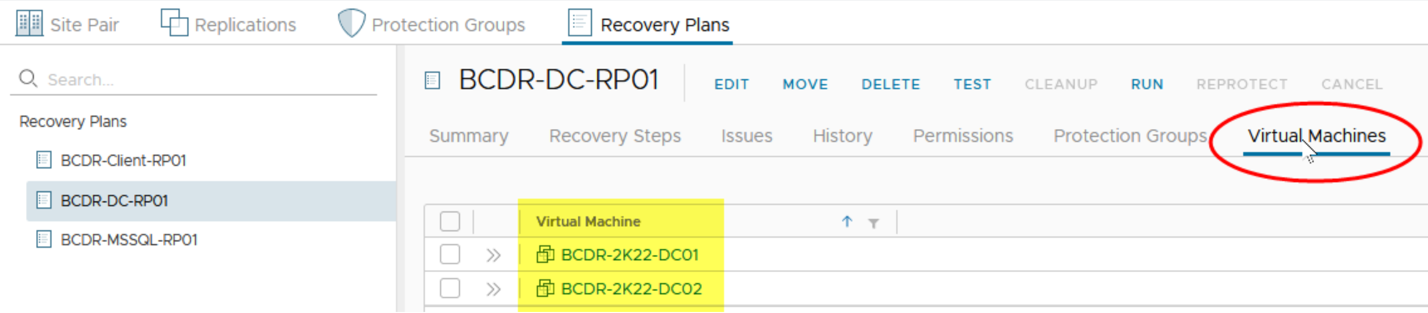
- We click on the name to select it.



Recovery Plans

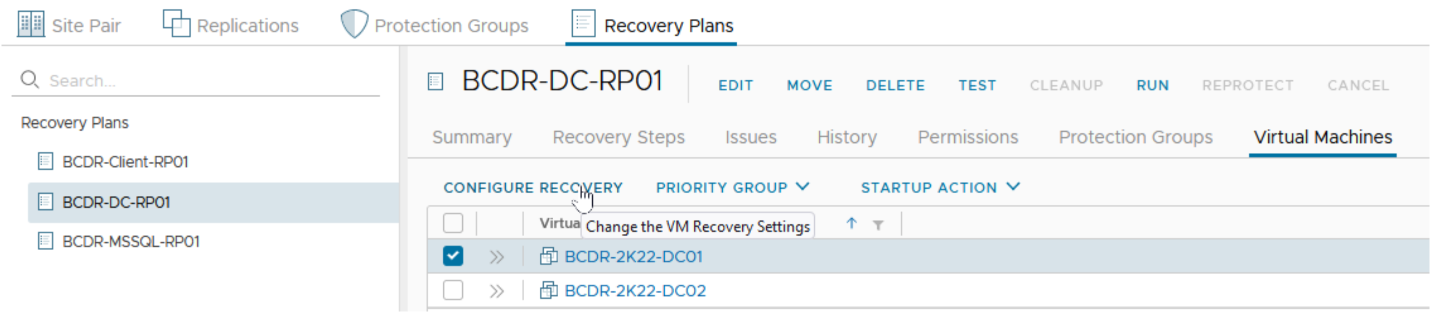
	Name	Status	Protected Site	Recovery Site
○	BCDR-Client-RP01	→ Ready	TSALab-VMC	srm.sddc-34-223-133-154.vmwarevmc.com
○	BCDR-DC-RP01	→ Ready	TSALab-VMC	srm.sddc-34-223-133-154.vmwarevmc.com
○	BCDR-MSSQL-RP01	→ Ready	TSALab-VMC	srm.sddc-34-223-133-154.vmwarevmc.com

- Select the **"Virtual Machines"** tab to display the VMs covered by the Plan.



□		Virtual Machine
□	»	BCDR-2K22-DC01
□	»	BCDR-2K22-DC02

Select the checkbox next to the VM we want to configure, then click "Configure Recovery".



	Virtual Machine
☑	BCDR-2K22-DC01
□	BCDR-2K22-DC02

SRM Recovery Plan gives us many configuration options and flexibility for controlling the desired outcomes for our Disaster Recovery Run Book. As you will see shortly, among other configuration options, here is where we can configure SRM to change the IP address (and other necessary IP configurations) to the recovered VM.

Virtualized Domain Controller Safety Feature

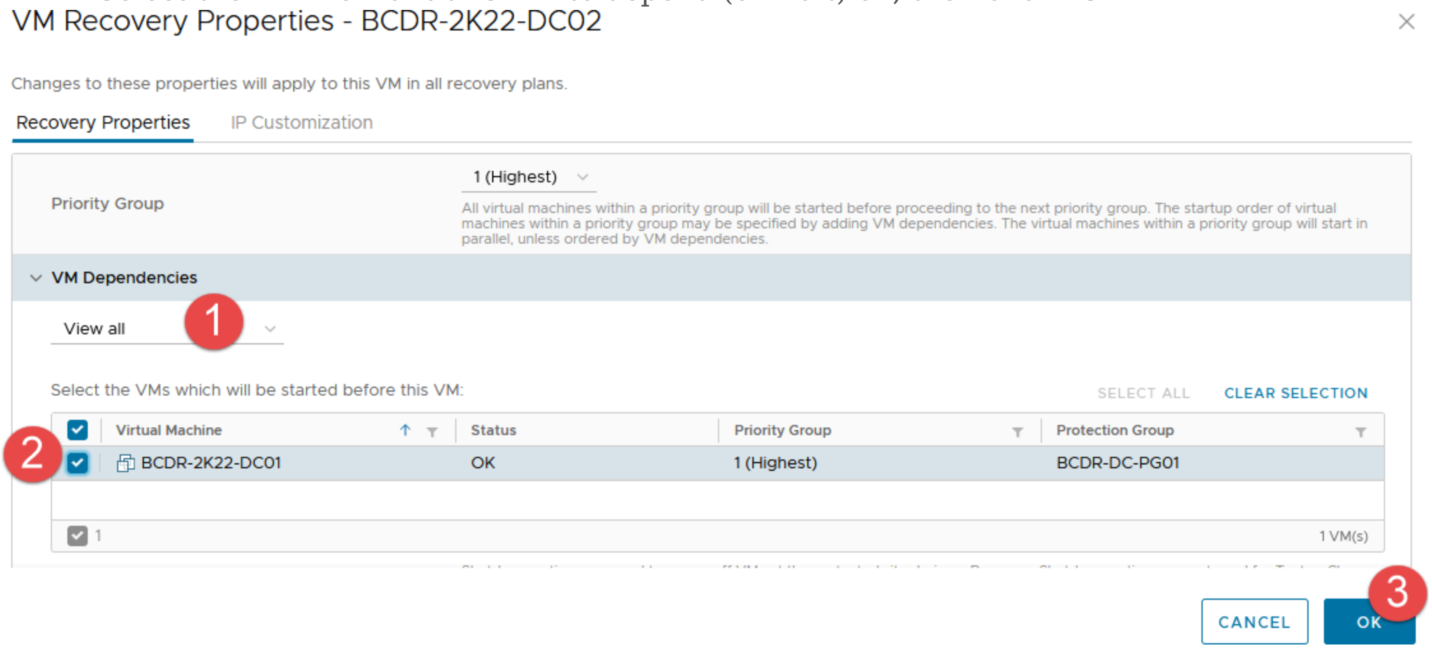
One of the challenges we want to overcome in recovering Domain Controllers is the order in which we want them to come up to account for the **"Virtualized Domain Controller Safety"** feature we discussed earlier. Since restoring a Domain Controller from a backup copy forces the Domain Controller to discard its RID Pool, you are likely wondering "where then does it get a new pool of RIDs if the RID Master is unavailable?"

This is a legitimate question in a Disaster event where we assume that everything in the Protected Site (including the RID Master itself) is unavailable. Luckily for us, the "DC Safety" feature accounts for this scenario by allowing the restored/recovered Domain Controller to regain services after multiple reboots (or by manually forcing the DC's NTDS to start **"*restart-service NTDS -force*"**)), if it can communicate with another Domain Controller).

We will start by ensuring that we are recovering the DC holding the FSMO Roles first and then recover all other DCs only after this one has been fully recovered. The mechanism for doing this in SRM is the **"VM Dependencies"** option.

Here is how we do this for **DC02**, which depends on **DC01** (the **FSMO Roles** holder):

- We select the VM (**DC02**) we want to make dependent and click **"Configure Recovery"**
- Expand **"VM Dependencies"** and select **"View all"**. This will show us all the VMs in the **Recovery Plan**
- Select the VM we want this VM to depend (or wait) on, then click **"OK"**



Changes to these properties will apply to this VM in all recovery plans.

Priority Group: 1 (Highest)

All virtual machines within a priority group will be started before proceeding to the next priority group. The startup order of virtual machines within a priority group may be specified by adding VM dependencies. The virtual machines within a priority group will start in parallel, unless ordered by VM dependencies.

View all

Select the VMs which will be started before this VM:

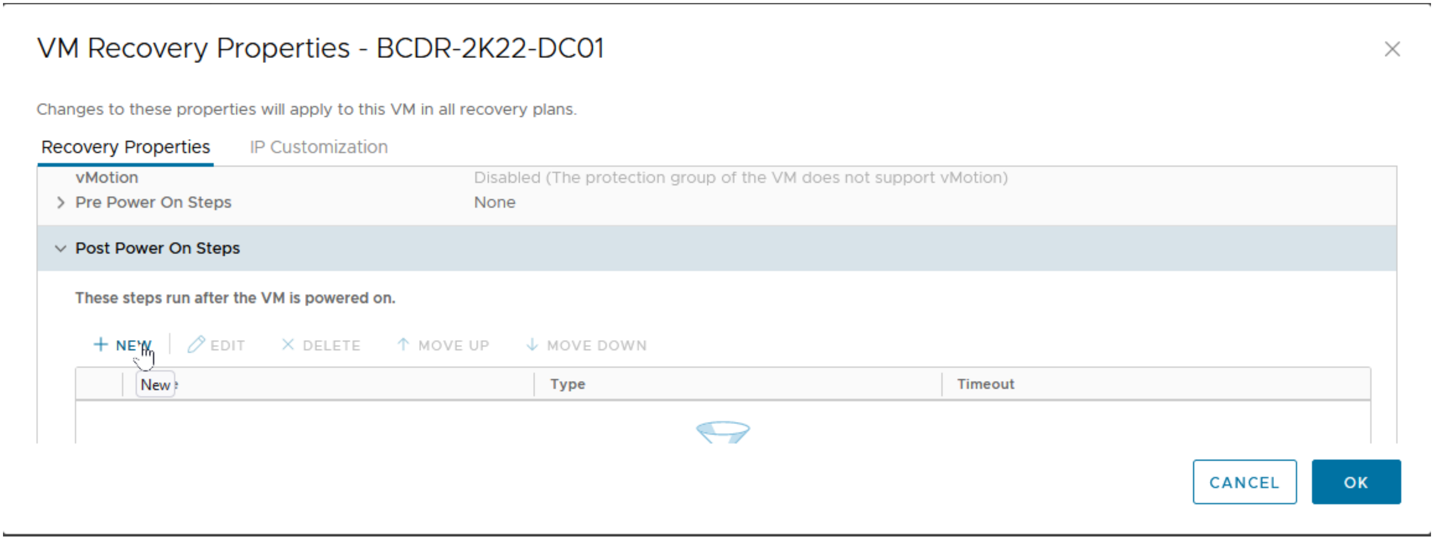
☑	Virtual Machine	Status	Priority Group	Protection Group
☑	BCDR-2K22-DC01	OK	1 (Highest)	BCDR-DC-PG01

☑ 1 — 1 VM(s)

Next, we will add a **"Post Power On Step"** task to **DC01** which calls a Script within Windows to reboot the VM after it has been fully recovered. This is a very simple **"*Shutdown -r -t 0*"** command, nothing fancy. This reboot allows **DC01** to be able to self-heal and start its relevant services, which allows it to be available to heal **DC02** that depends on it.

Here is how we do that.

- We select **DC01** and click **"Configure Recovery".**
- Expand **"Post Power On Steps"**, then click **"New".**



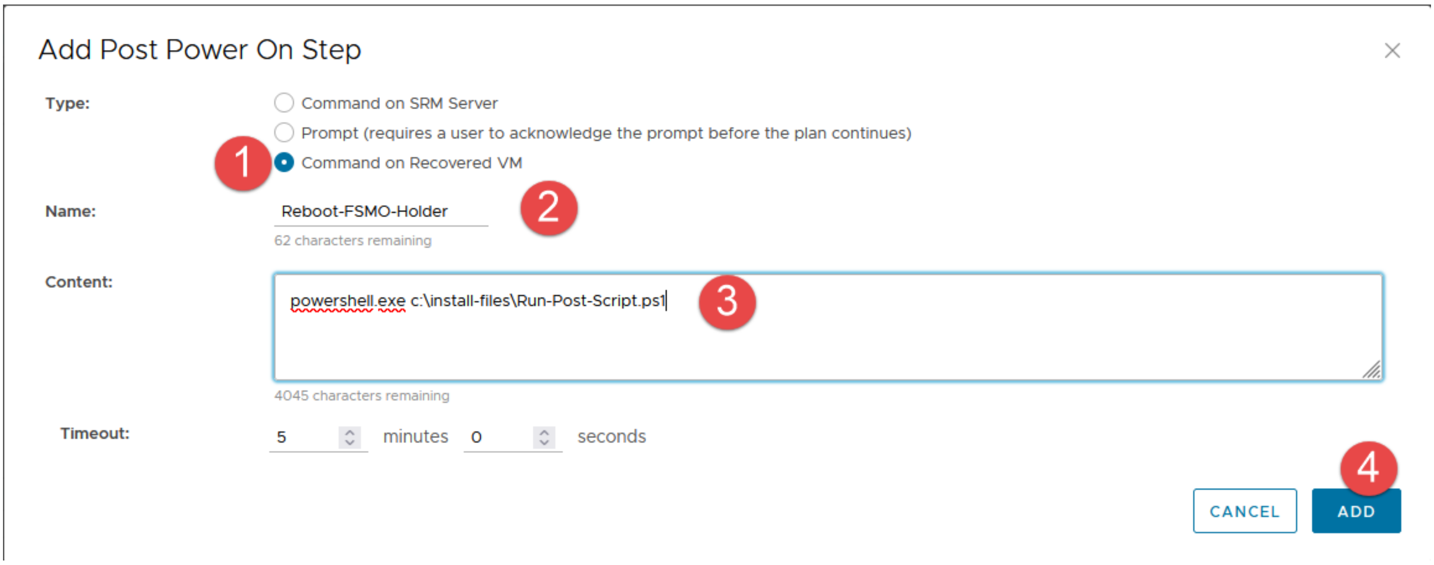
VM Recovery Properties - BCDR-2K22-DC01

Changes to these properties will apply to this VM in all recovery plans.

vMotion	Disabled (The protection group of the VM does not support vMotion)
Pre Power On Steps	None
Post Power On Steps	

These steps run after the VM is powered on.

- Select **"Command on Recovered VM".**
- Give it a descriptive name.
- Type in the Command to run (in our case, we are calling a PowerShell Script named **"*Run-Post-Script.ps1*"**, located in the **"*C:\Install-Files*"** folder.
- Click **"Add".**



Add Post Power On Step

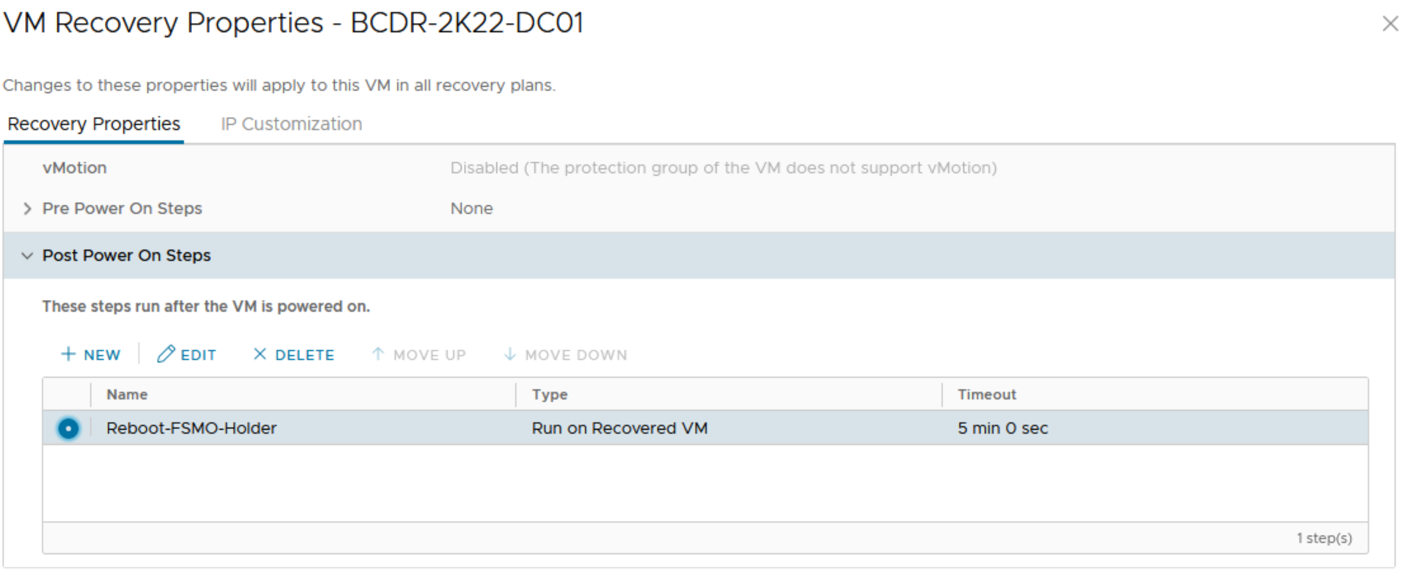
Type:
○ Command on SRM Server
○ Prompt (requires a user to acknowledge the prompt before the plan continues)
● Command on Recovered VM

Name: Reboot-FSMO-Holder
62 characters remaining

Content: powershell.exe c:\install-files\Run-Post-Script.ps1
4045 characters remaining

Timeout: 5 minutes 0 seconds

This brings us back to the **"VM Recovery Properties"** menu.



VM Recovery Properties - BCDR-2K22-DC01

Changes to these properties will apply to this VM in all recovery plans.

vMotion	Disabled (The protection group of the VM does not support vMotion)
Pre Power On Steps	None

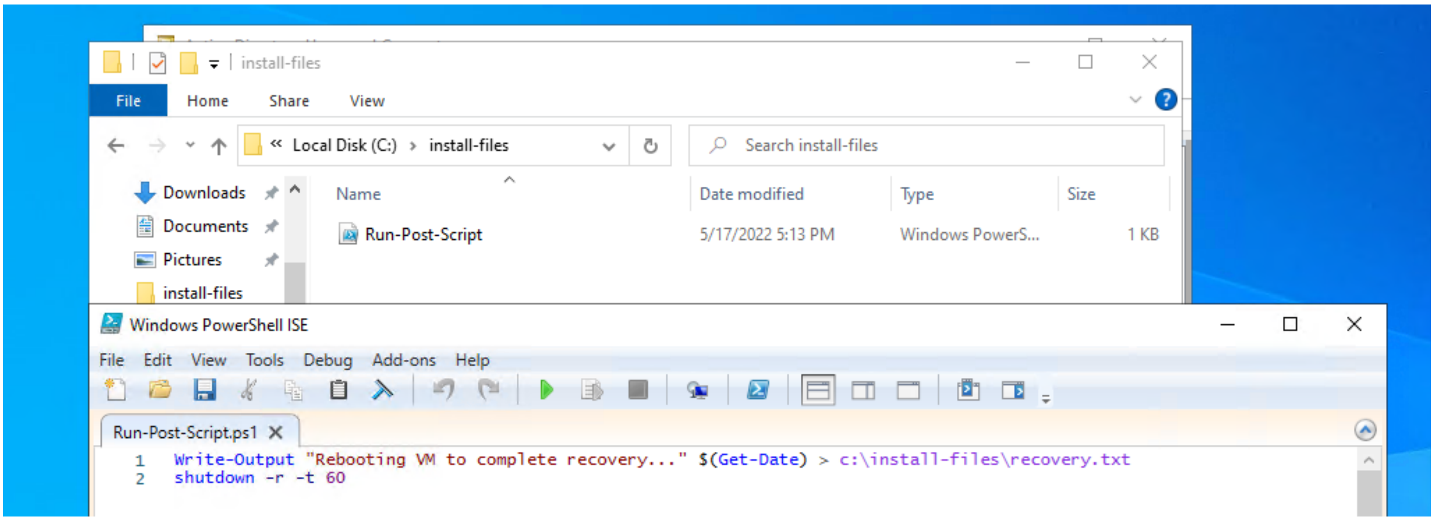
Post Power On Steps

These steps run after the VM is powered on.

	Name	Type	Timeout
●	Reboot-FSMO-Holder	Run on Recovered VM	5 min 0 sec

1 step(s)

Here is the content of our "***Run-Post-Script.ps1***" script.



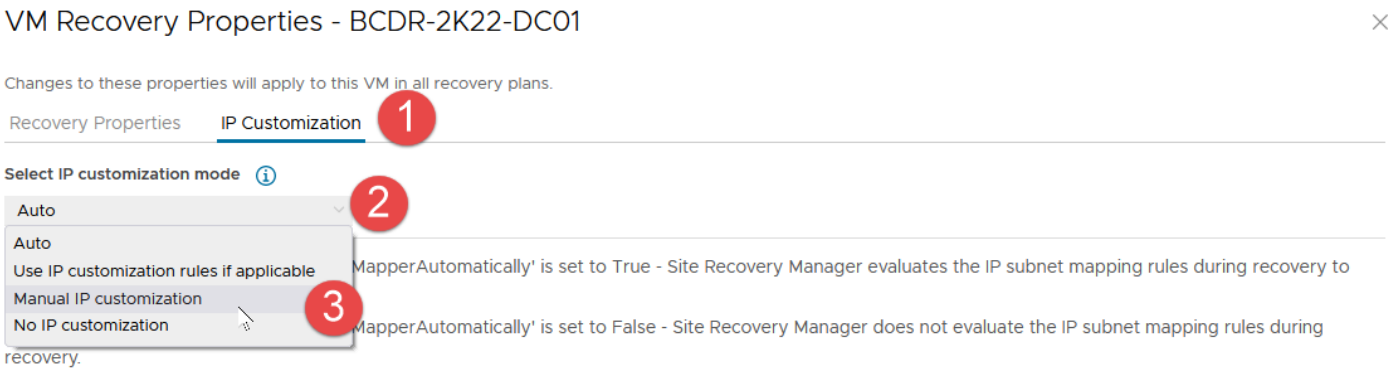
Name	Date modified	Type	Size
Run-Post-Script	5/17/2022 5:13 PM	Windows PowerS...	1 KB

```
Write-Output "Rebooting VM to complete recovery..." $(Get-Date) > c:\install-files\recovery.txt
shutdown -r -t 60
```

Changing Recovered VM’s IP Settings in SRM

Now, we are going to configure the TCP/IP Settings for our **Protected VMs**:

- Let's go back to the **"VM Recovery Properties"** menu, and click on the **"IP Customization"** tab.
- Select the drop-down button in **"Select IP Customization Mode".**
- Select **"Manual IP Customization".**



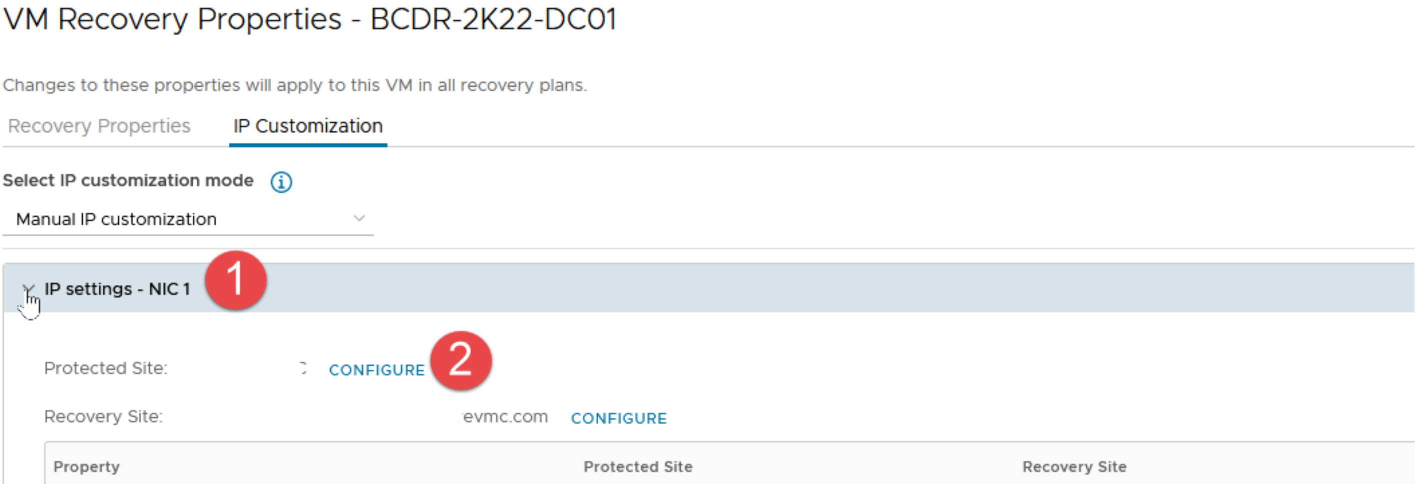
VM Recovery Properties - BCDR-2K22-DC01

Changes to these properties will apply to this VM in all recovery plans.

MapperAutomatically' is set to True - Site Recovery Manager evaluates the IP subnet mapping rules during recovery to

MapperAutomatically' is set to False - Site Recovery Manager does not evaluate the IP subnet mapping rules during recovery.

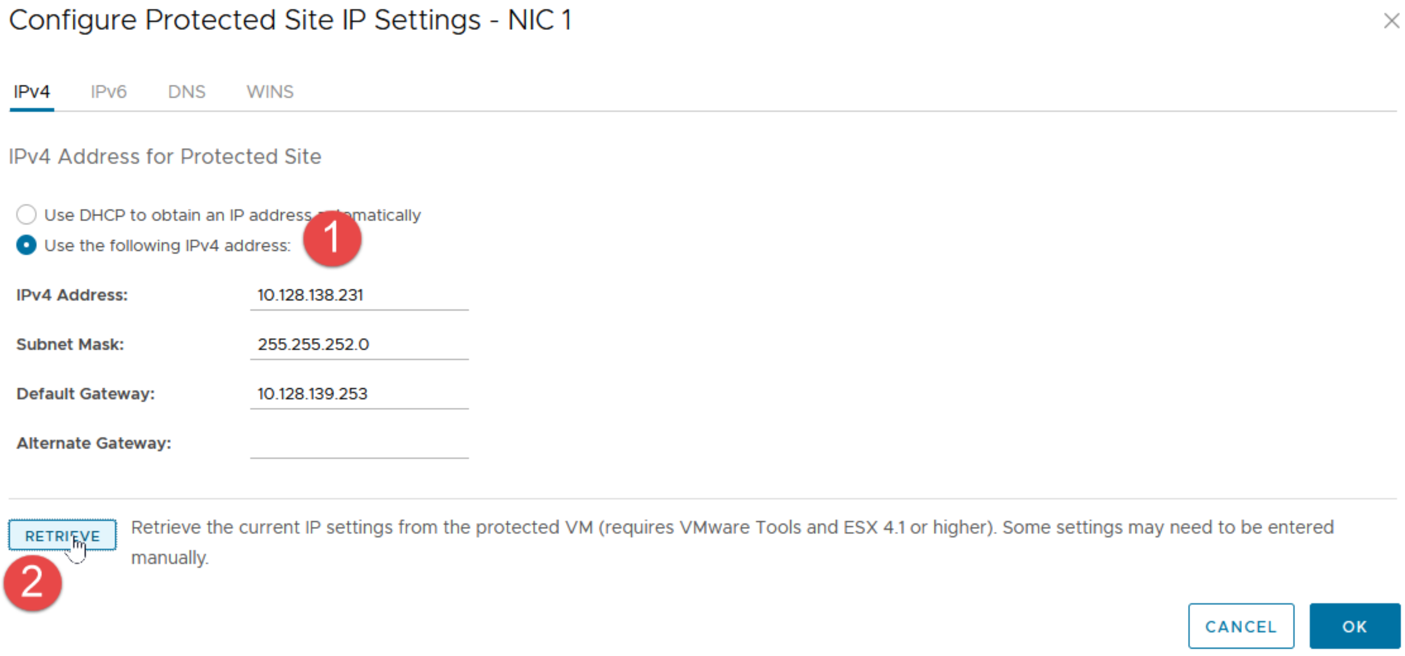
Click on **"IP Settings - NIC 1"**, then on **"Configure"** next to **"Protected Site".**



VM Recovery Properties - BCDR-2K22-DC01

Changes to these properties will apply to this VM in all recovery plans.

- Click on **"Use the following IPv4 address"**, then click **"Retrieve".**
- This auto-populates the fields with the current IP address of the **VM.**



Configure Protected Site IP Settings - NIC 1

IPv4 Address for Protected Site

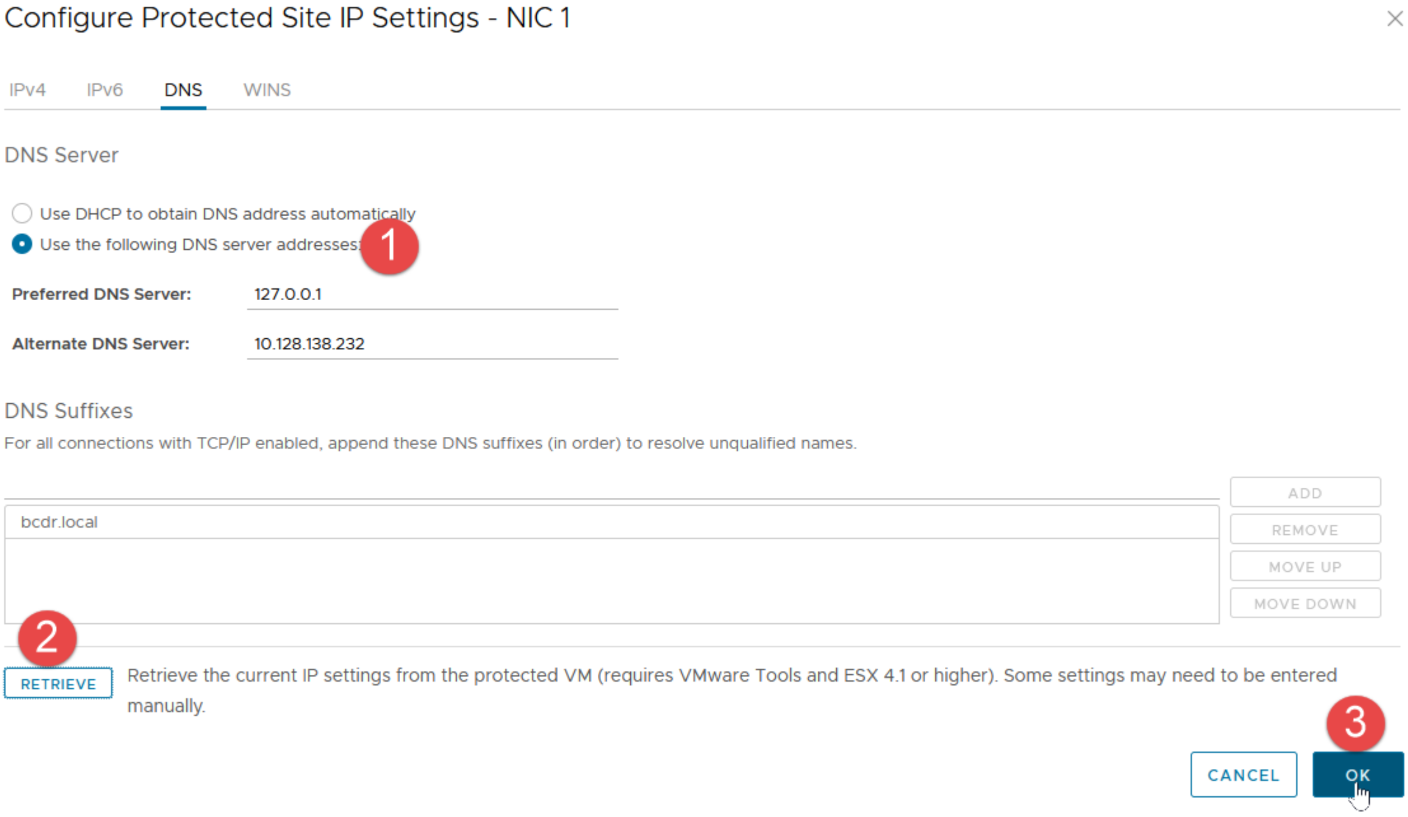
○ Use DHCP to obtain an IP address automatically
● Use the following IPv4 address:

IPv4 Address:	10.128.138.231
Subnet Mask:	255.255.252.0
Default Gateway:	10.128.139.253
Alternate Gateway:	

Retrieve the current IP settings from the protected VM (requires VMware Tools and ESX 4.1 or higher). Some settings may need to be entered manually.

- Let's repeat the process for the **DNS** information (we will skip IPV6 and WINS sections for this exercise).

- Click **"OK"** to complete the configuration.



Configure Protected Site IP Settings - NIC 1

DNS Server

○ Use DHCP to obtain DNS address automatically
● Use the following DNS server addresses:

Preferred DNS Server:	127.0.0.1
Alternate DNS Server:	10.128.138.232

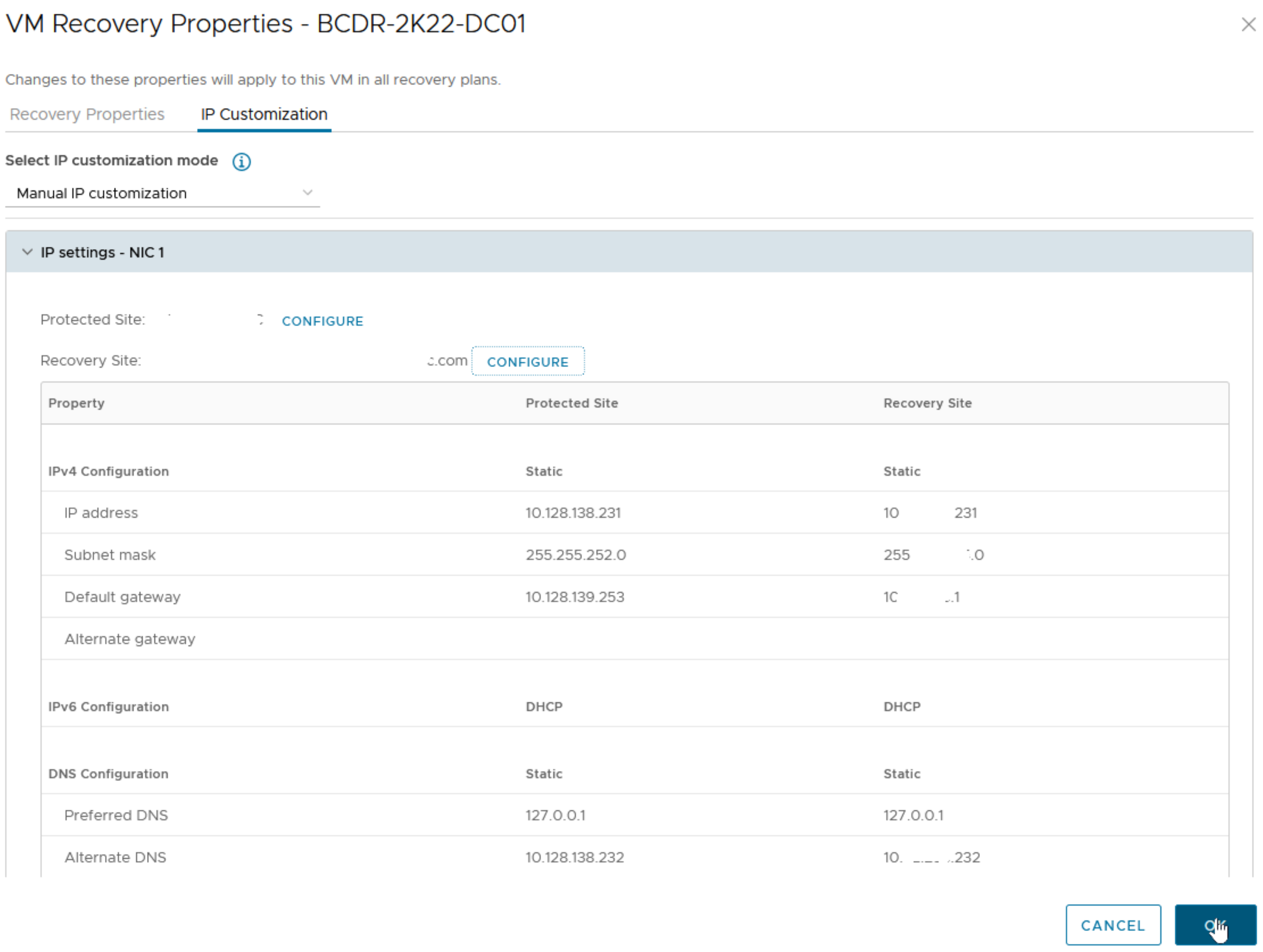
DNS Suffixes

For all connections with TCP/IP enabled, append these DNS suffixes (in order) to resolve unqualified names.

bcdr.local

Retrieve the current IP settings from the protected VM (requires VMware Tools and ESX 4.1 or higher). Some settings may need to be entered manually.

- This brings us back to the **"VM Recovery Properties"** -> **"IP Customization"** screen.
- We will click on **"Configure"** next to **"Recovery Site"** to specify the IP Address information we would like to apply to the VM upon recovery.
- You will notice that the **"Retrieve"** option is not available on this screen because the values do not currently exist on the VM.
- We go through the same steps we did for the **"Protected Site"** values, then click **“OK”** to complete the configuration.



VM Recovery Properties - BCDR-2K22-DC01

Changes to these properties will apply to this VM in all recovery plans.

Select IP customization mode: Manual IP customization

IP settings - NIC 1

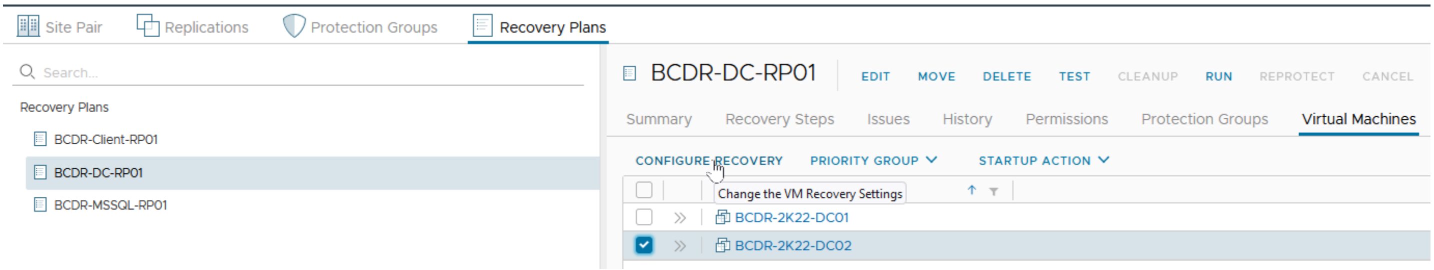
Protected Site: ˙ ˀ CONFIGURE

Recovery Site: ꜀.com CONFIGURE

Property	Protected Site	Recovery Site
IPv4 Configuration	Static	Static
IP address	10.128.138.231	10 231
Subnet mask	255.255.252.0	255 ˙.0
Default gateway	10.128.139.253	1C ..1
Alternate gateway		
IPv6 Configuration	DHCP	DHCP
DNS Configuration	Static	Static
Preferred DNS	127.0.0.1	127.0.0.1
Alternate DNS	10.128.138.232	10. ..232

We will complete this process for all the VMs in all recovery groups unless we:

1. Want them to get their IP Address configuration information from a DHCP Server/IPAM available at the Recovery Site, or
2. Want them to keep the same IP address because we have stretched the Protected Site's network segment(s) to the Recovery Site

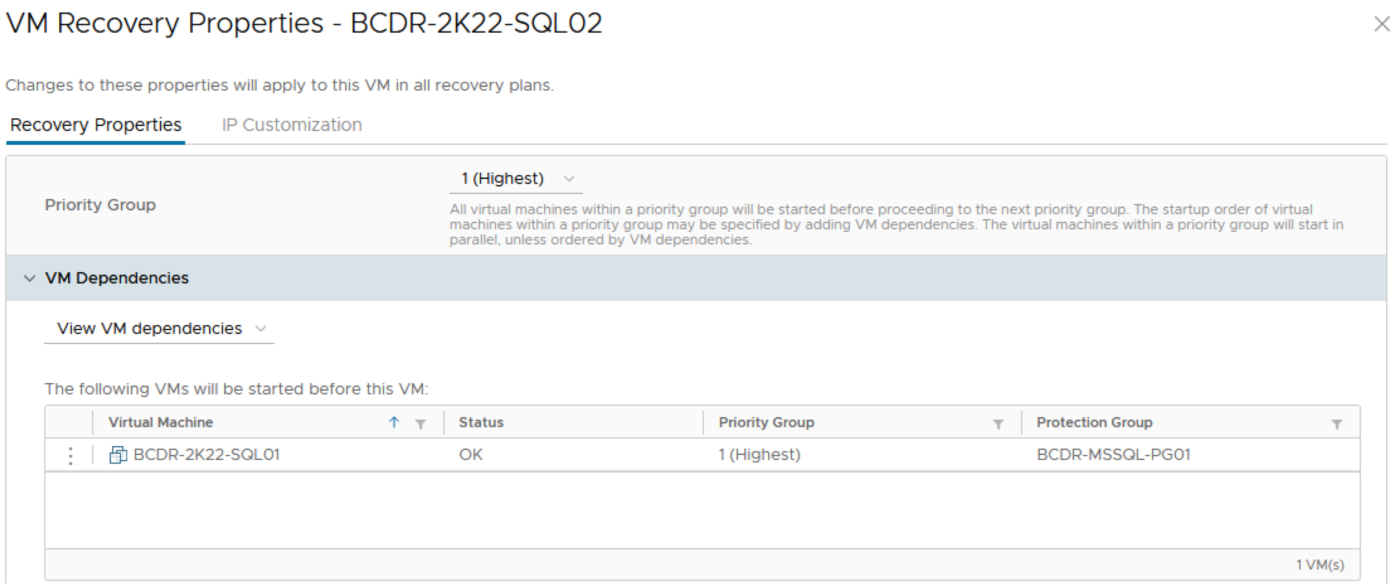


Recovery Plans
- BCDR-Client-RP01
- BCDR-DC-RP01
- BCDR-MSSQL-RP01

BCDR-DC-RP01

- □ BCDR-2K22-DC01
- ☑ BCDR-2K22-DC02

In our use case, we have two SQL Servers in a **Protection Group** and created a **Recovery Group** for them. We have created a dependency between the two of them such that **SQL02** would not be recovered and powered on before **SQL01** has been fully recovered.



VM Recovery Properties - BCDR-2K22-SQL02

Changes to these properties will apply to this VM in all recovery plans.

Priority Group: 1 (Highest)

All virtual machines within a priority group will be started before proceeding to the next priority group. The startup order of virtual machines within a priority group may be specified by adding VM dependencies. The virtual machines within a priority group will start in parallel, unless ordered by VM dependencies.

The following VMs will be started before this VM:

Virtual Machine	Status	Priority Group	Protection Group
BCDR-2K22-SQL01	OK	1 (Highest)	BCDR-MSSQL-PG01

1 VM(s)

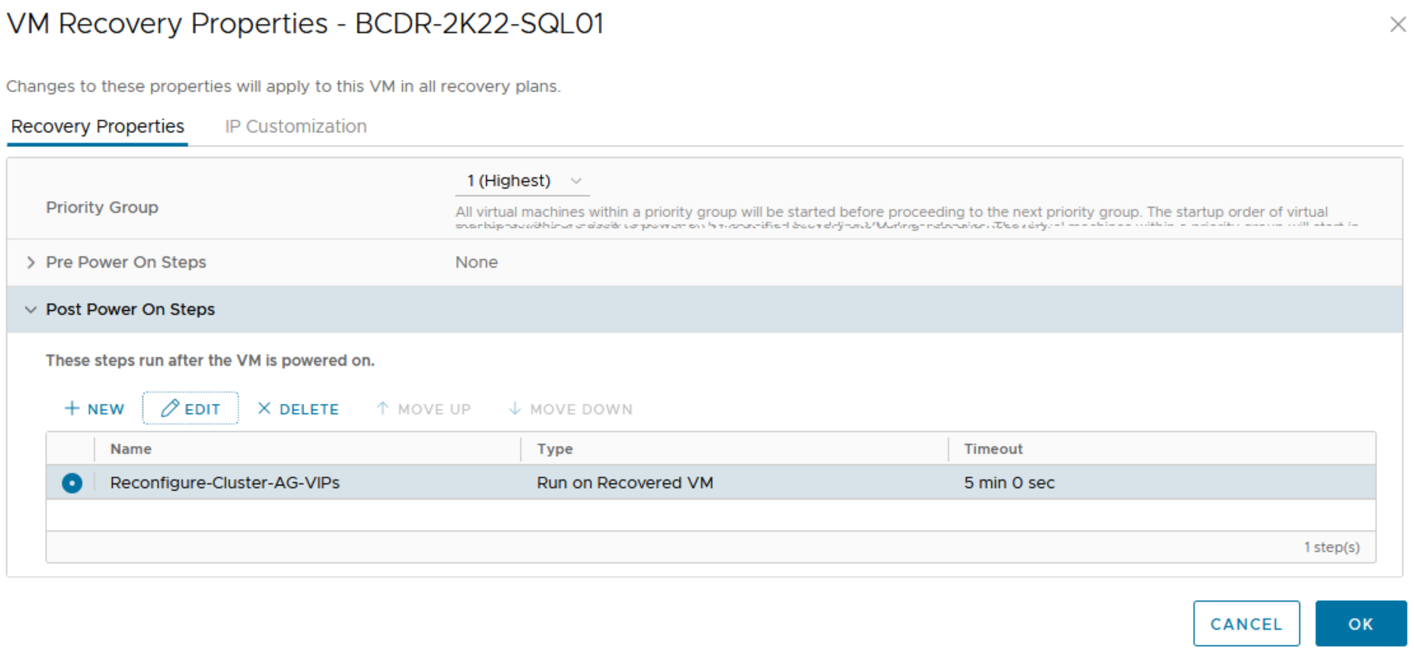
Considering that there are only two of them, and that the **File Share Witness (FSW)** is stored on a **Domain Controller** which we have already recovered before recovering the protected Microsoft SQL Server VMs, and any of the Microsoft SQL Server VMs that come up first will be able to form a majority node quorum by adding its vote to the FSW's vote to bring up the Cluster resources, why then are we creating a dependency?

We are doing it for the **Listener** and **Cluster Virtual IP** configurations. The parameters for these two Windows/SQL Server clustering configuration settings must be correct and available for the Cluster and its resources to become available after recovery.

As you have seen, the recovery process changes the IP address of the recovered VMs and connects them to a different network segment in the **Recovery Site**. Consequently, the **Listener's** and **Cluster VIP's** IP Addresses also need to change. This is something that SRM cannot do natively (because it is Applications-agnostic).

We will use the in-Guest Script initiation capability of SRM to make the changes (just like we did for the Operations Master domain controller). Because we only need to do this once for the Cluster, we have placed the Script inside only one of the SQL Server VMs, and that VM is **SQL01**. We, therefore, want the **SQL01** VM to be recovered first and for the configuration changes to be completed before **SQL02** is recovered.

Here is what that configuration looks like on **SQL01.**



VM Recovery Properties - BCDR-2K22-SQL01

Changes to these properties will apply to this VM in all recovery plans.

Priority Group: 1 (Highest)

All virtual machines within a priority group will be started before proceeding to the next priority group. The startup order of virtual

Pre Power On Steps: None

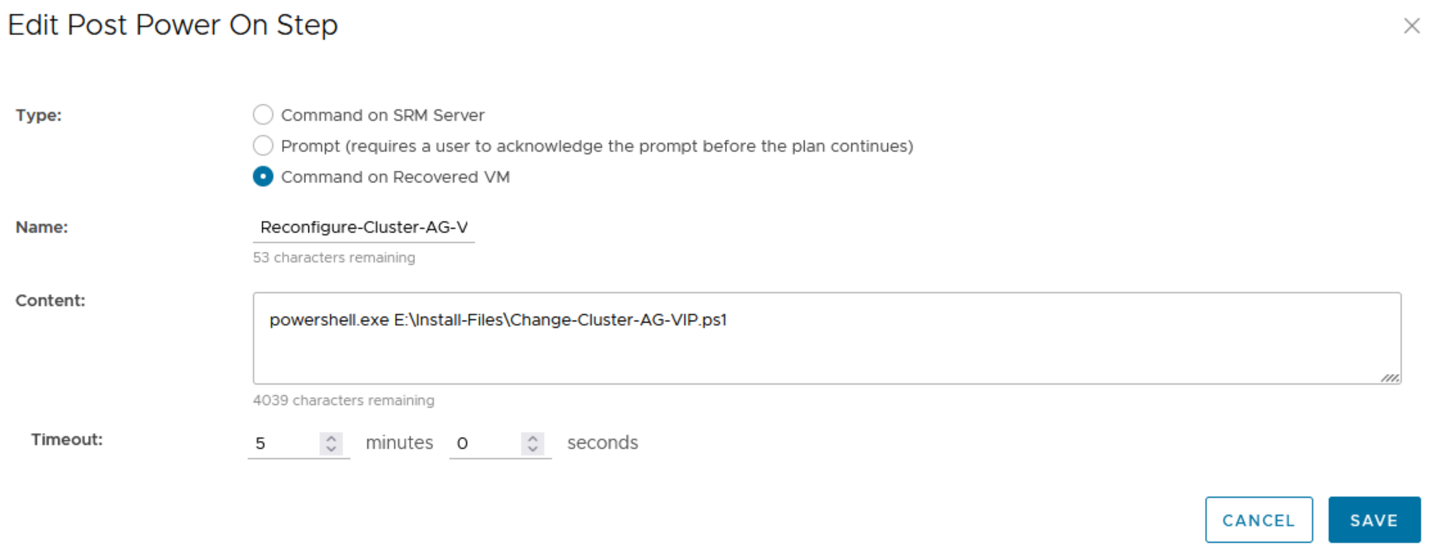
These steps run after the VM is powered on.

	Name	Type	Timeout
●	Reconfigure-Cluster-AG-VIPs	Run on Recovered VM	5 min 0 sec

1 step(s)

Here is the SRM Guest-side Command which calls our in-Guest PowerShell Script (***Change-Cluster-AG-VIP.ps1***), located in the E:\Install-Files folder on the SQL01 VM.

NOTE: Follow your internal Corporate Security practices for storing and running in-Guest Scripts when deciding where to place these sample scripts.



Edit Post Power On Step

Type:
○ Command on SRM Server
○ Prompt (requires a user to acknowledge the prompt before the plan continues)
● Command on Recovered VM

Name: Reconfigure-Cluster-AG-V
53 characters remaining

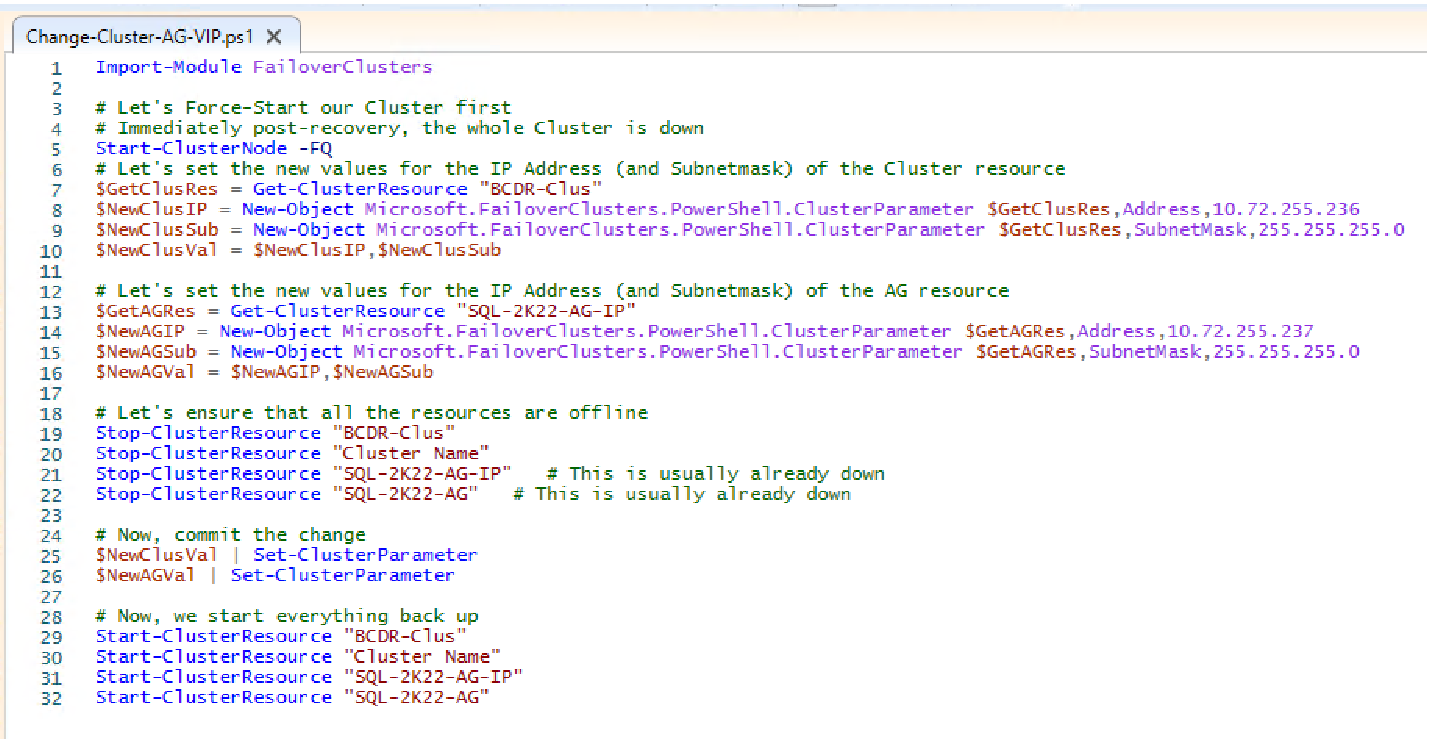
Content:

```
powershell.exe E:\Install-Files\Change-Cluster-AG-VIP.ps1
```

4039 characters remaining

Timeout: 5 minutes 0 seconds

Here is a screenshot of the Script (this Script itself will be included as an appendix to this guide).



Change-Cluster-AG-VIP.ps1

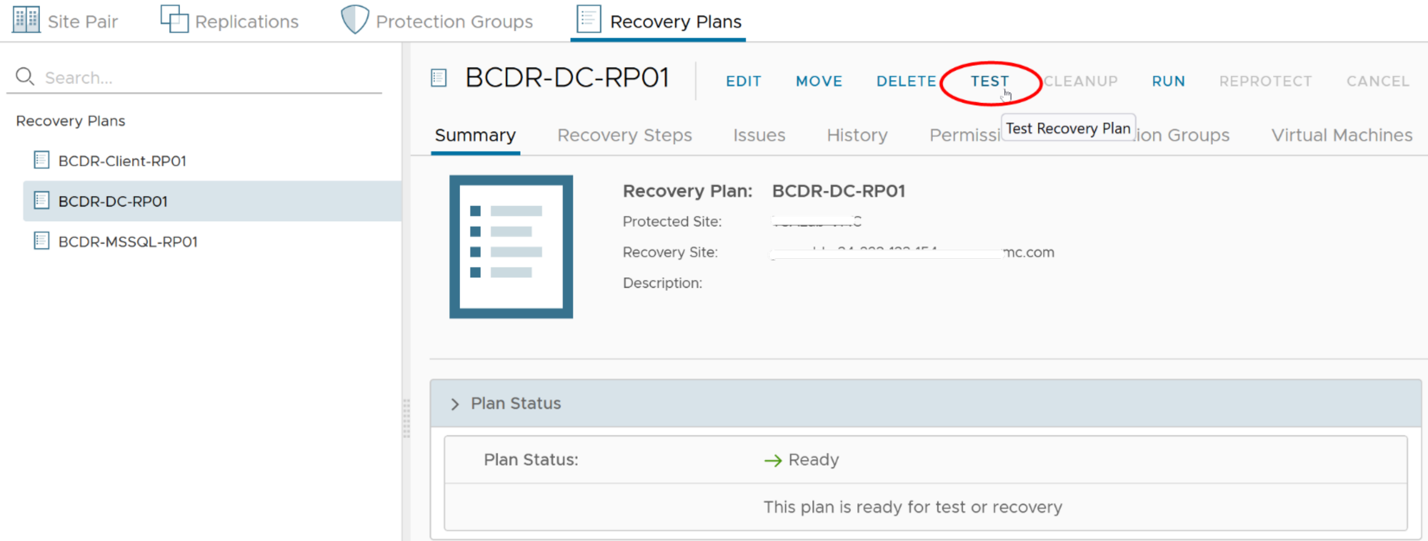
```
Import-Module FailoverClusters

# Let's Force-Start our Cluster first
# Immediately post-recovery, the whole Cluster is down
Start-ClusterNode -FQ
# Let's set the new values for the IP Address (and Subnetmask) of the Cluster resource
$GetClusRes = Get-ClusterResource "BCDR-Clus"
$NewClusIP = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetClusRes,Address,10.72.255.236
$NewClusSub = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetClusRes,SubnetMask,255.255.255.0
$NewClusVal = $NewClusIP,$NewClusSub

# Let's set the new values for the IP Address (and Subnetmask) of the AG resource
$GetAGRes = Get-ClusterResource "SQL-2K22-AG-IP"
$NewAGIP = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetAGRes,Address,10.72.255.237
$NewAGSub = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetAGRes,SubnetMask,255.255.255.0
$NewAGVal = $NewAGIP,$NewAGSub

# Let's ensure that all the resources are offline
Stop-ClusterResource "BCDR-Clus"
Stop-ClusterResource "Cluster Name"
Stop-ClusterResource "SQL-2K22-AG-IP"   # This is usually already down
Stop-ClusterResource "SQL-2K22-AG"   # This is usually already down

# Now, commit the change
$NewClusVal | Set-ClusterParameter
$NewAGVal | Set-ClusterParameter

# Now, we start everything back up
Start-ClusterResource "BCDR-Clus"
Start-ClusterResource "Cluster Name"
Start-ClusterResource "SQL-2K22-AG-IP"
Start-ClusterResource "SQL-2K22-AG"
```

SRM and Test Disaster Recovery

We now have all the configuration pieces, and we are ready to test our DR Plan. Of what use is a **BCDR Plan** if you cannot test it periodically? An actual DR event is not the best time to discover that your DR Plan is missing one or more steps or that the expectations were based on configuration assumptions that have changed so much that they no longer match current steady state realities.

- From the **"Recovery Plans"** tab, click on **"Test".**

- Notice that the **"Plan Status"** shows **"Ready"**. This is an indication that the **Recovery Plan** is in a state where it can be successfully initiated.



Recovery Plans
- BCDR-Client-RP01
- BCDR-DC-RP01
- BCDR-MSSQL-RP01

BCDR-DC-RP01

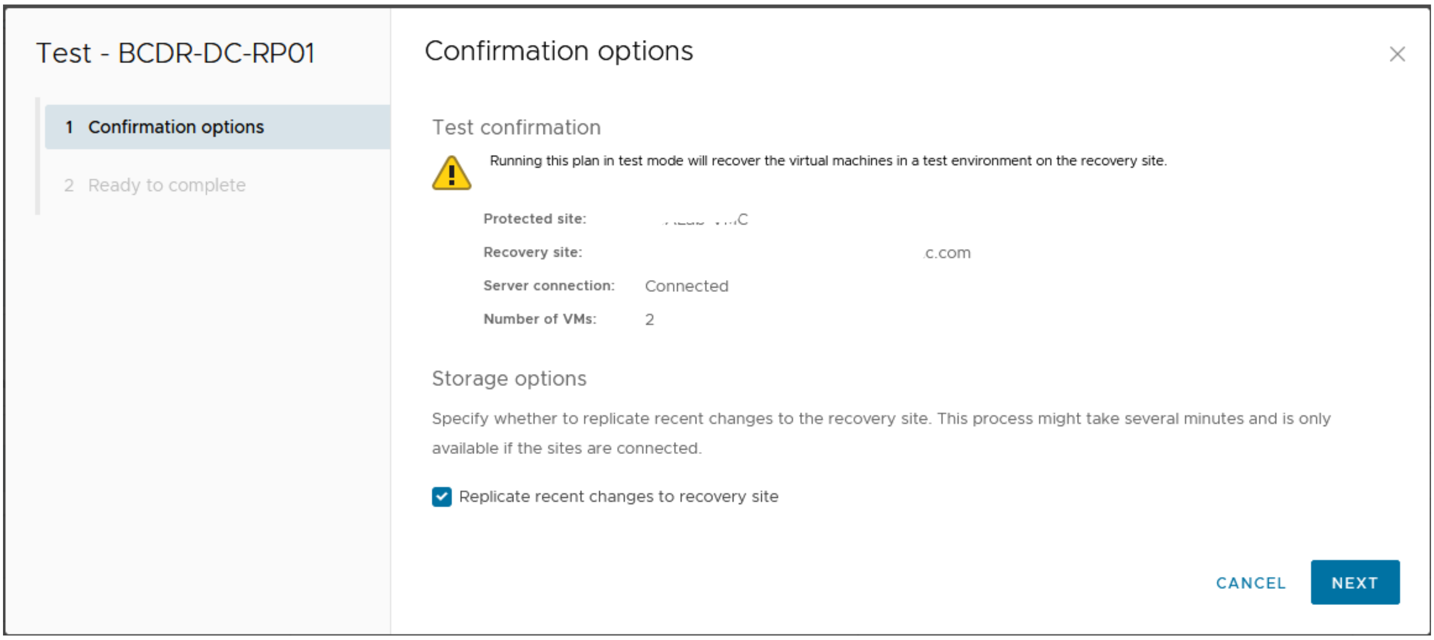
Recovery Plan: BCDR-DC-RP01
Protected Site:
Recovery Site: mc.com
Description:

Plan Status

Plan Status: → Ready

This plan is ready for test or recovery

- Confirm that **"Replicate recent changes to recovery site"** is checked, then click **"Next"**.



Confirmation options

Test confirmation

Running this plan in test mode will recover the virtual machines in a test environment on the recovery site.

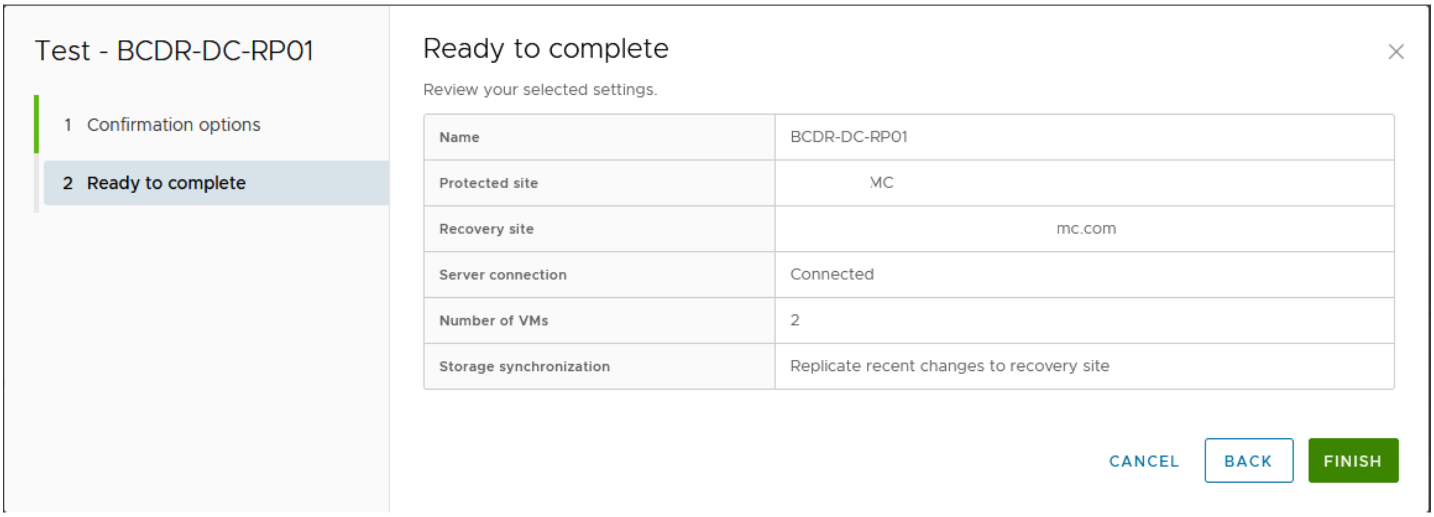
Protected site: C
Recovery site: c.com
Server connection: Connected
Number of VMs: 2

Storage options

Specify whether to replicate recent changes to the recovery site. This process might take several minutes and is only available if the sites are connected.

☑ Replicate recent changes to recovery site

- Click **"Finish"** to begin the **Test Recovery** process.



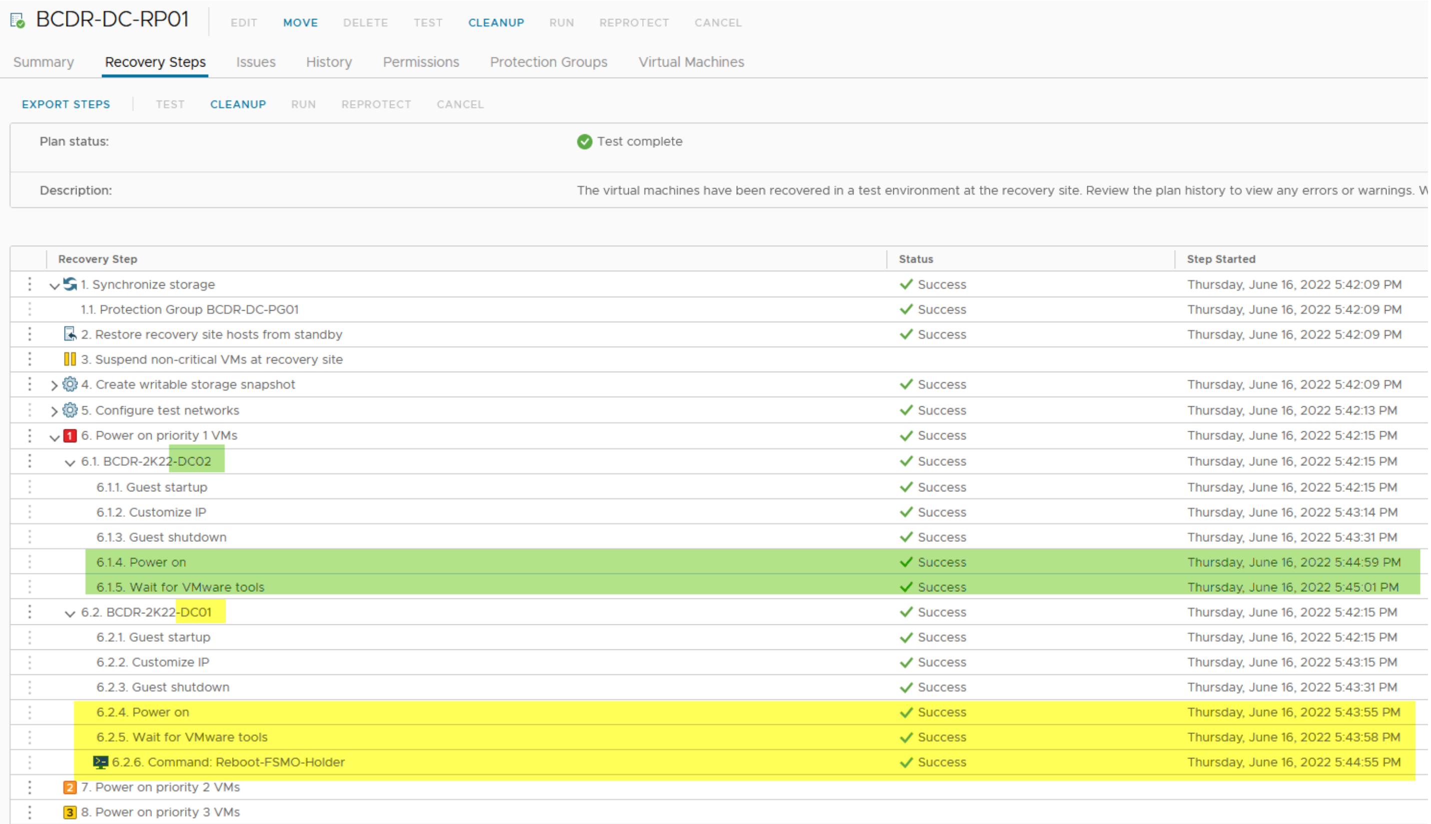
Ready to complete

Review your selected settings.

Name	BCDR-DC-RP01
Protected site	MC
Recovery site	mc.com
Server connection	Connected
Number of VMs	2
Storage synchronization	Replicate recent changes to recovery site

The **"Recovery Steps"** shows detailed information about actions taken during the recovery process.

If we take a close look at what happened when we initiated our DC Recovery Plan, we will notice that **DC02** was powered on only AFTER **DC01** has fully recovered AND the in-Guest Script that we configured had been run. This is the **"Dependency"** we configured in the **Recovery Plan**.



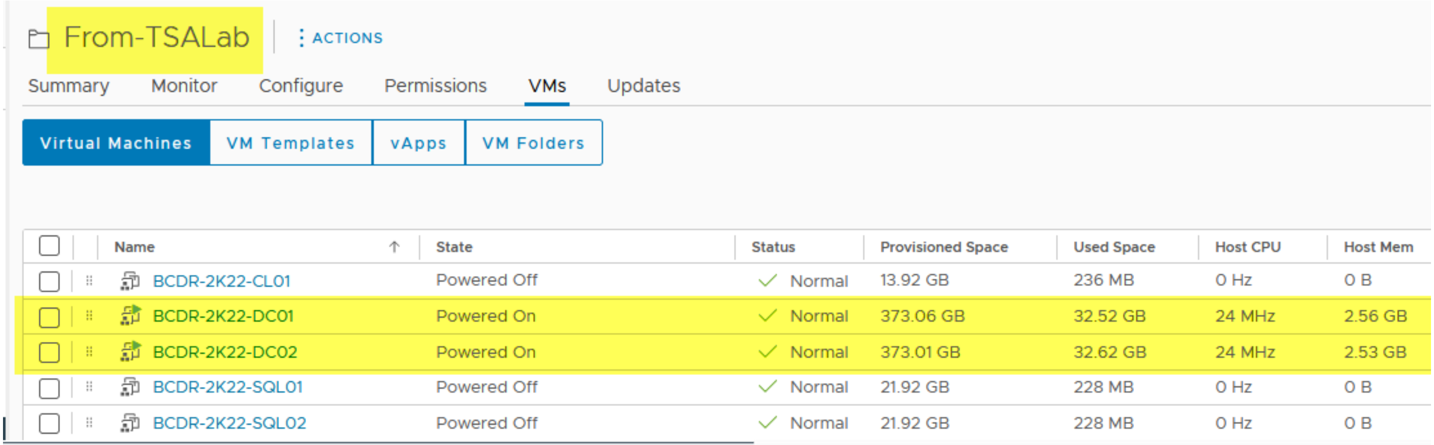
BCDR-DC-RP01
EDIT MOVE DELETE TEST CLEANUP RUN REPROTECT CANCEL
Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines
EXPORT STEPS TEST CLEANUP RUN REPROTECT CANCEL

Plan status: ✓ Test complete

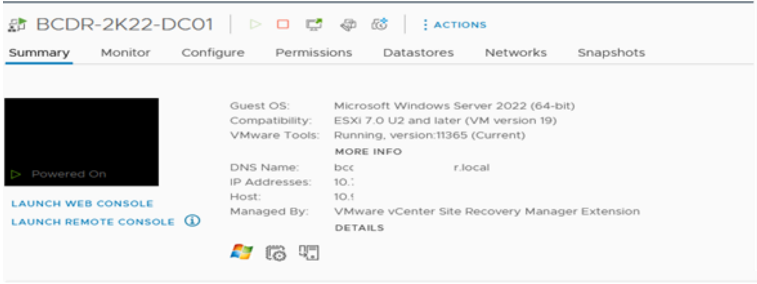
Description: The virtual machines have been recovered in a test environment at the recovery site. Review the plan history to view any errors or warnings. W

Recovery Step	Status	Step Started
1. Synchronize storage	✓ Success	Thursday, June 16, 2022 5:42:09 PM
1.1. Protection Group BCDR-DC-PG01	✓ Success	Thursday, June 16, 2022 5:42:09 PM
2. Restore recovery site hosts from standby	✓ Success	Thursday, June 16, 2022 5:42:09 PM
3. Suspend non-critical VMs at recovery site		
4. Create writable storage snapshot	✓ Success	Thursday, June 16, 2022 5:42:09 PM
5. Configure test networks	✓ Success	Thursday, June 16, 2022 5:42:13 PM
6. Power on priority 1 VMs	✓ Success	Thursday, June 16, 2022 5:42:15 PM
6.1. BCDR-2K22-DC02	✓ Success	Thursday, June 16, 2022 5:42:15 PM
6.1.1. Guest startup	✓ Success	Thursday, June 16, 2022 5:42:15 PM
6.1.2. Customize IP	✓ Success	Thursday, June 16, 2022 5:43:14 PM
6.1.3. Guest shutdown	✓ Success	Thursday, June 16, 2022 5:43:31 PM
6.1.4. Power on	✓ Success	Thursday, June 16, 2022 5:44:59 PM
6.1.5. Wait for VMware tools	✓ Success	Thursday, June 16, 2022 5:45:01 PM
6.2. BCDR-2K22-DC01	✓ Success	Thursday, June 16, 2022 5:42:15 PM
6.2.1. Guest startup	✓ Success	Thursday, June 16, 2022 5:42:15 PM
6.2.2. Customize IP	✓ Success	Thursday, June 16, 2022 5:43:15 PM
6.2.3. Guest shutdown	✓ Success	Thursday, June 16, 2022 5:43:31 PM
6.2.4. Power on	✓ Success	Thursday, June 16, 2022 5:43:55 PM
6.2.5. Wait for VMware tools	✓ Success	Thursday, June 16, 2022 5:43:58 PM
6.2.6. Command: Reboot-FSMO-Holder	✓ Success	Thursday, June 16, 2022 5:44:55 PM
7. Power on priority 2 VMs		
8. Power on priority 3 VMs		

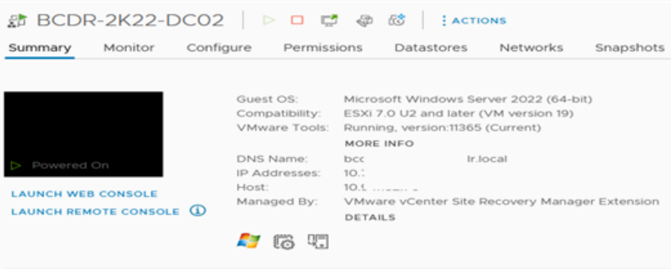
We can see the recovered VMs powered on and run in the **Recovery Site** vCenter.



□	Name ↑	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
□	BCDR-2K22-CL01	Powered Off	✓ Normal	13.92 GB	236 MB	0 Hz	0 B
□	BCDR-2K22-DC01	Powered On	✓ Normal	373.06 GB	32.52 GB	24 MHz	2.56 GB
□	BCDR-2K22-DC02	Powered On	✓ Normal	373.01 GB	32.62 GB	24 MHz	2.53 GB
□	BCDR-2K22-SQL01	Powered Off	✓ Normal	21.92 GB	228 MB	0 Hz	0 B
□	BCDR-2K22-SQL02	Powered Off	✓ Normal	21.92 GB	228 MB	0 Hz	0 B

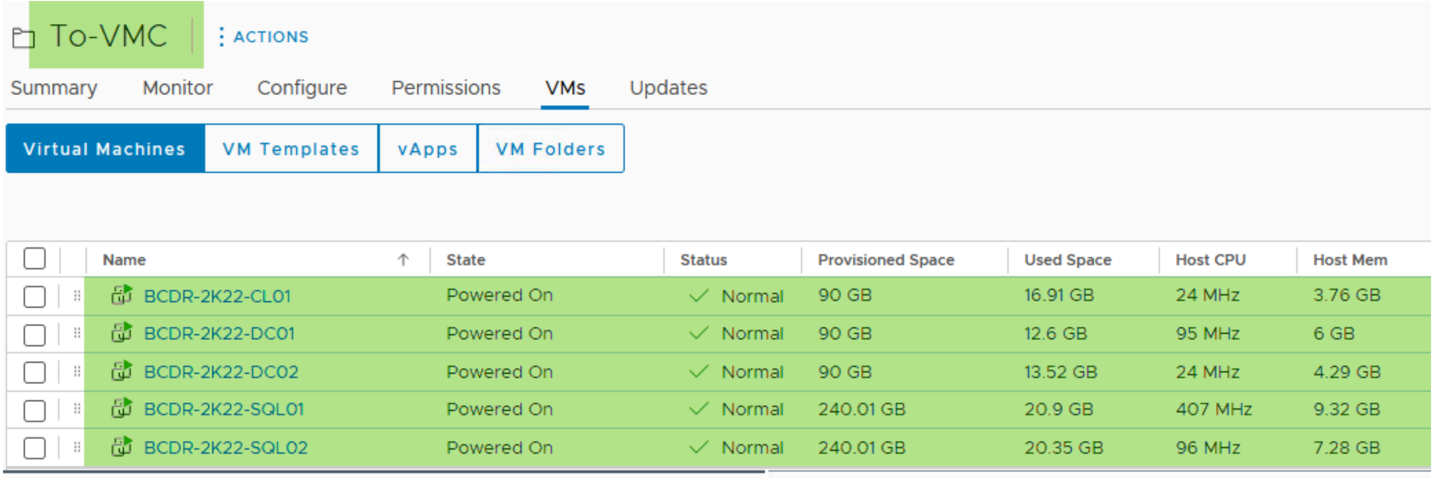


Guest OS: Microsoft Windows Server 2022 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11365 (Current)
DNS Name: bcc r.local
IP Addresses: 10.:
Host: 10.!
Managed By: VMware vCenter Site Recovery Manager Extension

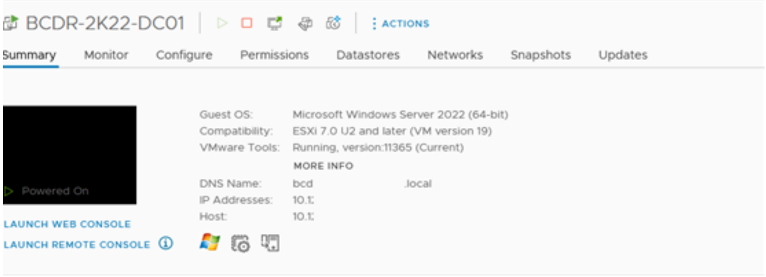


Guest OS: Microsoft Windows Server 2022 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11365 (Current)
DNS Name: bcc lr.local
IP Addresses: 10.:
Host: 10.!
Managed By: VMware vCenter Site Recovery Manager Extension

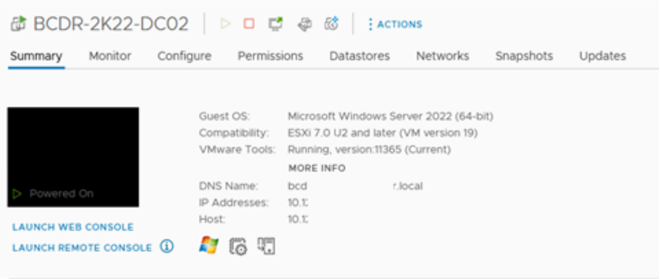
The same Domain Controller VMs are still running uninterrupted at the **Protected Site.**



□	Name ↑	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
□	BCDR-2K22-CL01	Powered On	✓ Normal	90 GB	16.91 GB	24 MHz	3.76 GB
□	BCDR-2K22-DC01	Powered On	✓ Normal	90 GB	12.6 GB	95 MHz	6 GB
□	BCDR-2K22-DC02	Powered On	✓ Normal	90 GB	13.52 GB	24 MHz	4.29 GB
□	BCDR-2K22-SQL01	Powered On	✓ Normal	240.01 GB	20.9 GB	407 MHz	9.32 GB
□	BCDR-2K22-SQL02	Powered On	✓ Normal	240.01 GB	20.35 GB	96 MHz	7.28 GB

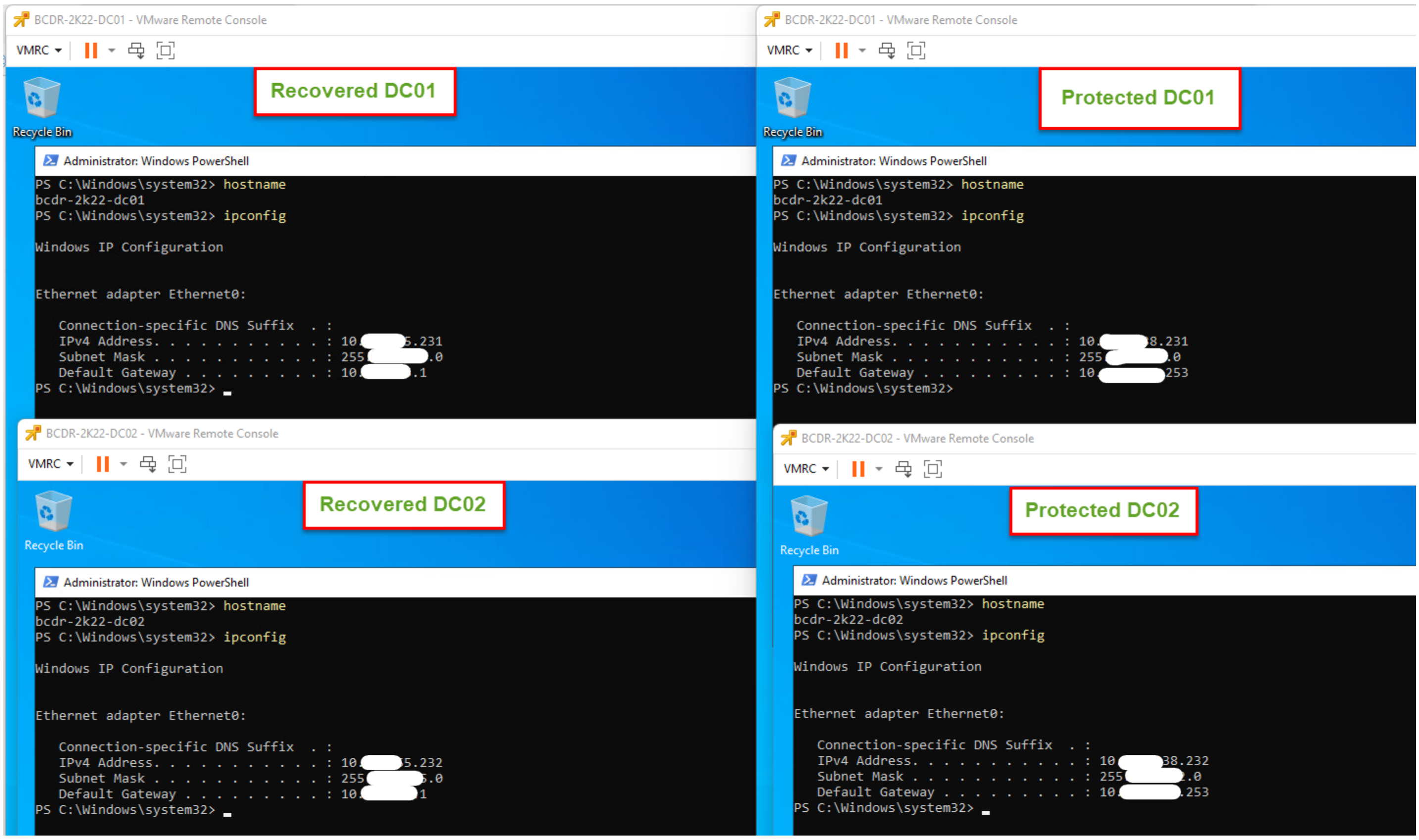


Guest OS: Microsoft Windows Server 2022 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11365 (Current)
DNS Name: bcd .local
IP Addresses: 10.1:
Host: 10.1:



Guest OS: Microsoft Windows Server 2022 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11365 (Current)
DNS Name: bcd r.local
IP Addresses: 10.1:
Host: 10.1:

Let's verify that both protected and recovered VMs are accessible by logging into them.


BCDR-2K22-DC01 - VMware Remote Console
VMRC
Recovered DC01
Protected DC01
BCDR-2K22-DC02 - VMware Remote Console
Recovered DC02
Protected DC02
Recycle Bin
Administrator: Windows PowerShell

Recovered DC01:

```
PS C:\Windows\system32> hostname
bcdr-2k22-dc01
PS C:\Windows\system32> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10[redacted]5.231
   Subnet Mask . . . . . . . . . . . : 255[redacted].0
   Default Gateway . . . . . . . . . : 10[redacted].1
PS C:\Windows\system32> _
```

Protected DC01:

```
PS C:\Windows\system32> hostname
bcdr-2k22-dc01
PS C:\Windows\system32> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10[redacted]8.231
   Subnet Mask . . . . . . . . . . . : 255[redacted].0
   Default Gateway . . . . . . . . . : 10[redacted]253
PS C:\Windows\system32>
```

Recovered DC02:

```
PS C:\Windows\system32> hostname
bcdr-2k22-dc02
PS C:\Windows\system32> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10[redacted]5.232
   Subnet Mask . . . . . . . . . . . : 255[redacted].0
   Default Gateway . . . . . . . . . : 10[redacted]1
PS C:\Windows\system32> _
```

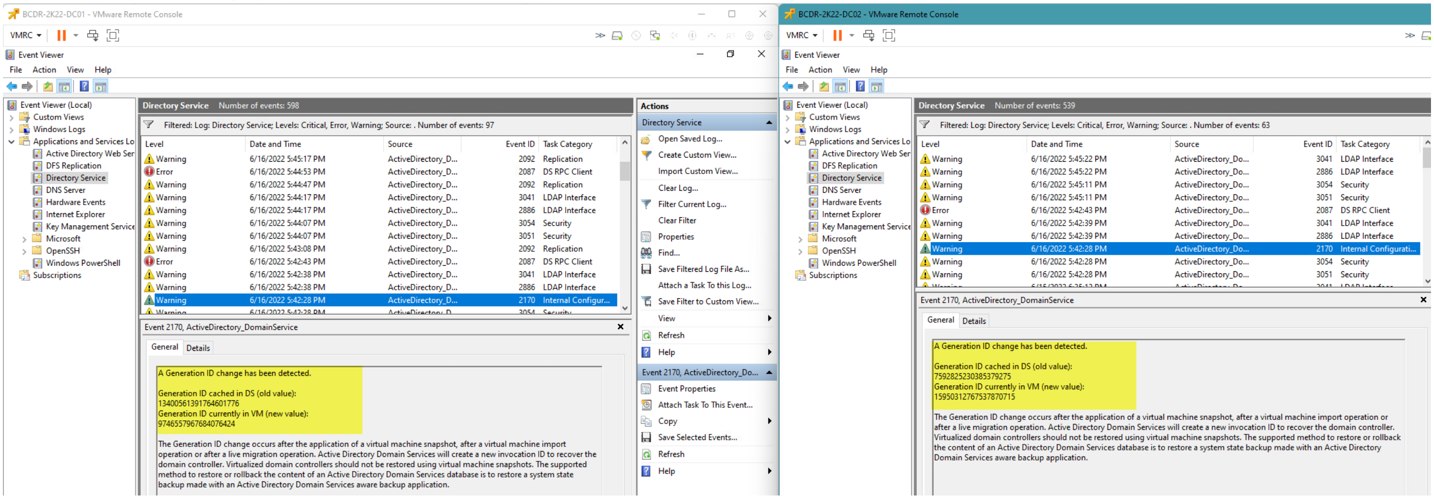
Protected DC02:

```
PS C:\Windows\system32> hostname
bcdr-2k22-dc02
PS C:\Windows\system32> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10[redacted]38.232
   Subnet Mask . . . . . . . . . . . : 255[redacted].0
   Default Gateway . . . . . . . . . : 10[redacted].253
PS C:\Windows\system32> _
```

Safe Active Directory Domain Controllers Recovery with VMware Site Recovery Manager in Action

Let's take a look at what happened to our protected Active Directory infrastructure after a (simulated) Disaster Recovery event was completed using Site Recovery Manager.

- The first time the recovered Domain Controllers boot up, Windows automatically detects the change in their VM-Generation ID.



Directory Service Number of events: 598

Filtered: Log: Directory Service; Levels: Critical, Error, Warning; Source: . Number of events: 97

Level	Date and Time	Source	Event ID	Task Category
Warning	6/16/2022 5:45:17 PM	ActiveDirectory_D...	2092	Replication
Error	6/16/2022 5:44:53 PM	ActiveDirectory_D...	2087	DS RPC Client
Warning	6/16/2022 5:44:47 PM	ActiveDirectory_D...	2092	Replication
Warning	6/16/2022 5:44:17 PM	ActiveDirectory_D...	3041	LDAP Interface
Warning	6/16/2022 5:44:17 PM	ActiveDirectory_D...	2886	LDAP Interface
Warning	6/16/2022 5:44:07 PM	ActiveDirectory_D...	3054	Security
Warning	6/16/2022 5:44:07 PM	ActiveDirectory_D...	3051	Security
Warning	6/16/2022 5:43:08 PM	ActiveDirectory_D...	2092	Replication
Error	6/16/2022 5:42:43 PM	ActiveDirectory_D...	2087	DS RPC Client
Warning	6/16/2022 5:42:38 PM	ActiveDirectory_D...	3041	LDAP Interface
Warning	6/16/2022 5:42:38 PM	ActiveDirectory_D...	2886	LDAP Interface
Warning	6/16/2022 5:42:28 PM	ActiveDirectory_D...	2170	Internal Configur...

Event 2170, ActiveDirectory_DomainService

A Generation ID change has been detected.

Generation ID cached in DS (old value):
13400561391764601776
Generation ID currently in VM (new value):
9746557967684076424

The Generation ID change occurs after the application of a virtual machine snapshot, after a virtual machine import operation or after a live migration operation. Active Directory Domain Services will create a new invocation ID to recover the domain controller. Virtualized domain controllers should not be restored using virtual machine snapshots. The supported method to restore or rollback the content of an Active Directory Domain Services database is to restore a system state backup made with an Active Directory Domain Services aware backup application.

Directory Service Number of events: 539

Filtered: Log: Directory Service; Levels: Critical, Error, Warning; Source: . Number of events: 63

Level	Date and Time	Source	Event ID	Task Category
Warning	6/16/2022 5:45:22 PM	ActiveDirectory_Do...	3041	LDAP Interface
Warning	6/16/2022 5:45:22 PM	ActiveDirectory_Do...	2886	LDAP Interface
Warning	6/16/2022 5:45:11 PM	ActiveDirectory_Do...	3054	Security
Warning	6/16/2022 5:45:11 PM	ActiveDirectory_Do...	3051	Security
Error	6/16/2022 5:42:43 PM	ActiveDirectory_Do...	2087	DS RPC Client
Warning	6/16/2022 5:42:39 PM	ActiveDirectory_Do...	3041	LDAP Interface
Warning	6/16/2022 5:42:39 PM	ActiveDirectory_Do...	2886	LDAP Interface
Warning	6/16/2022 5:42:28 PM	ActiveDirectory_Do...	2170	Internal Configurati...
Warning	6/16/2022 5:42:28 PM	ActiveDirectory_Do...	3054	Security
Warning	6/16/2022 5:42:28 PM	ActiveDirectory_Do...	3051	Security

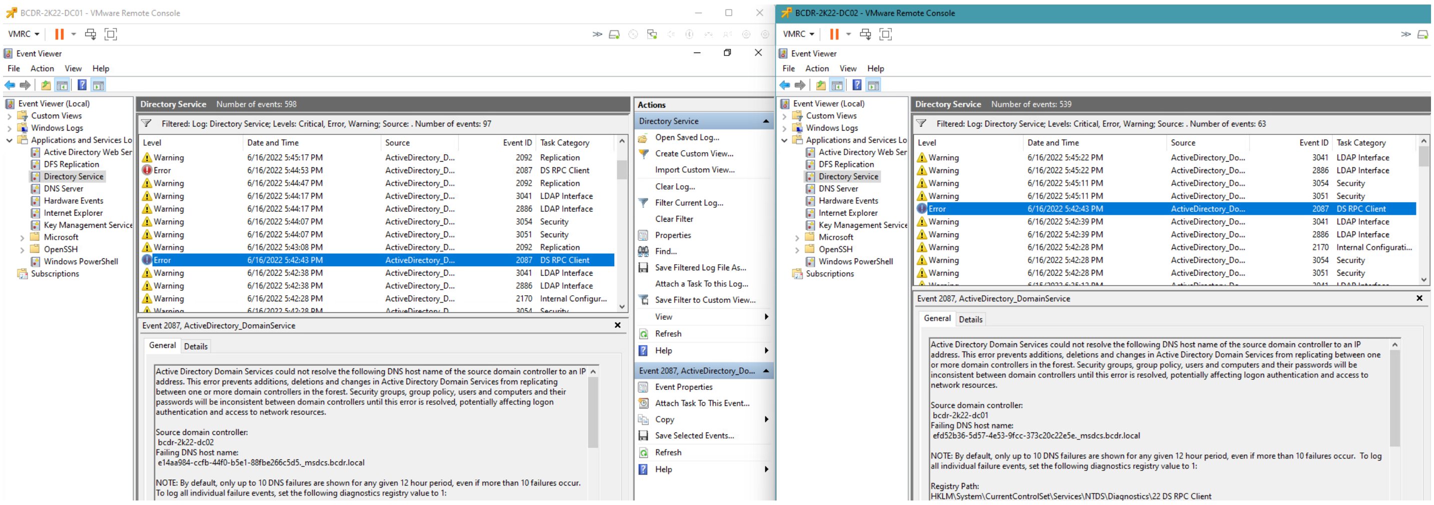
Event 2170, ActiveDirectory_DomainService

A Generation ID change has been detected.

Generation ID cached in DS (old value):
7592825230385379275
Generation ID currently in VM (new value):
15950312767537870715

The Generation ID change occurs after the application of a virtual machine snapshot, after a virtual machine import operation or after a live migration operation. Active Directory Domain Services will create a new invocation ID to recover the domain controller. Virtualized domain controllers should not be restored using virtual machine snapshots. The supported method to restore or rollback the content of an Active Directory Domain Services database is to restore a system state backup made with an Active Directory Domain Services aware backup application.

- Windows' DC Safety feature immediately kicks in and the recovered DC are taken through the remediation process. Among other effects we have discussed in previous sections, the Netlogon, DNS, and other services are unable to start during this remediation process.



BCDR-2K22-DC01:

Directory Service Number of events: 598

Filtered: Log: Directory Service; Levels: Critical, Error, Warning; Source: . Number of events: 97

Level	Date and Time	Source	Event ID	Task Category
Warning	6/16/2022 5:45:17 PM	ActiveDirectory_D...	2092	Replication
Error	6/16/2022 5:44:53 PM	ActiveDirectory_D...	2087	DS RPC Client
Warning	6/16/2022 5:44:47 PM	ActiveDirectory_D...	2092	Replication
Warning	6/16/2022 5:44:17 PM	ActiveDirectory_D...	3041	LDAP Interface
Warning	6/16/2022 5:44:17 PM	ActiveDirectory_D...	2886	LDAP Interface
Warning	6/16/2022 5:44:07 PM	ActiveDirectory_D...	3054	Security
Warning	6/16/2022 5:44:07 PM	ActiveDirectory_D...	3051	Security
Warning	6/16/2022 5:43:08 PM	ActiveDirectory_D...	2092	Replication
Error	6/16/2022 5:42:43 PM	ActiveDirectory_D...	2087	DS RPC Client
Warning	6/16/2022 5:42:38 PM	ActiveDirectory_D...	3041	LDAP Interface
Warning	6/16/2022 5:42:38 PM	ActiveDirectory_D...	2886	LDAP Interface
Warning	6/16/2022 5:42:28 PM	ActiveDirectory_D...	2170	Internal Configur...

Event 2087, ActiveDirectory_DomainService

General | Details

Active Directory Domain Services could not resolve the following DNS host name of the source domain controller to an IP address. This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources.

Source domain controller:
bcdr-2k22-dc02
Failing DNS host name:
e14aa984-ccfb-44f0-b5e1-88fbe266c5d5._msdcs.bcdr.local

NOTE: By default, only up to 10 DNS failures are shown for any given 12 hour period, even if more than 10 failures occur. To log all individual failure events, set the following diagnostics registry value to 1:

BCDR-2K22-DC02:

Directory Service Number of events: 539

Filtered: Log: Directory Service; Levels: Critical, Error, Warning; Source: . Number of events: 63

Level	Date and Time	Source	Event ID	Task Category
Warning	6/16/2022 5:45:22 PM	ActiveDirectory_Do...	3041	LDAP Interface
Warning	6/16/2022 5:45:22 PM	ActiveDirectory_Do...	2886	LDAP Interface
Warning	6/16/2022 5:45:11 PM	ActiveDirectory_Do...	3054	Security
Warning	6/16/2022 5:45:11 PM	ActiveDirectory_Do...	3051	Security
Error	6/16/2022 5:42:43 PM	ActiveDirectory_Do...	2087	DS RPC Client
Warning	6/16/2022 5:42:39 PM	ActiveDirectory_Do...	3041	LDAP Interface
Warning	6/16/2022 5:42:39 PM	ActiveDirectory_Do...	2886	LDAP Interface
Warning	6/16/2022 5:42:28 PM	ActiveDirectory_Do...	2170	Internal Configurati...
Warning	6/16/2022 5:42:28 PM	ActiveDirectory_Do...	3054	Security
Warning	6/16/2022 5:42:28 PM	ActiveDirectory_Do...	3051	Security

Event 2087, ActiveDirectory_DomainService

General | Details

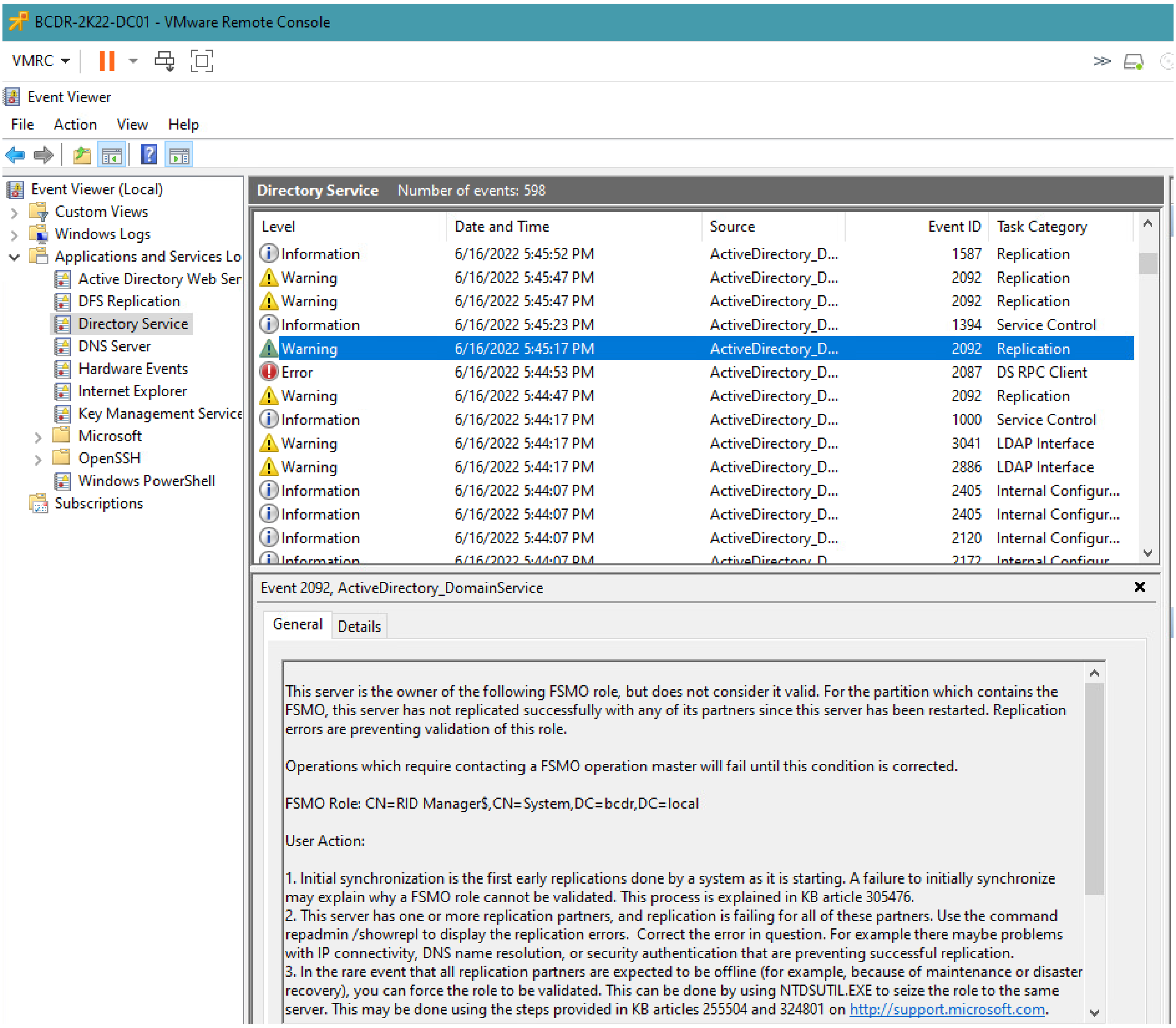
Active Directory Domain Services could not resolve the following DNS host name of the source domain controller to an IP address. This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources.

Source domain controller:
bcdr-2k22-dc01
Failing DNS host name:
efd52b36-5d57-4e53-9fcc-373c20c22e5e._msdcs.bcdr.local

NOTE: By default, only up to 10 DNS failures are shown for any given 12 hour period, even if more than 10 failures occur. To log all individual failure events, set the following diagnostics registry value to 1:

Registry Path:
HKLM\System\CurrentControlSet\Services\NTDS\Diagnostics\22 DS RPC Client

- The FSMO Role holder **(DC01)** does not even consider itself a DC anymore (at least not an authoritative one).



Directory Service Number of events: 598

Level	Date and Time	Source	Event ID	Task Category
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1587	Replication
Warning	6/16/2022 5:45:47 PM	ActiveDirectory_D...	2092	Replication
Warning	6/16/2022 5:45:47 PM	ActiveDirectory_D...	2092	Replication
Information	6/16/2022 5:45:23 PM	ActiveDirectory_D...	1394	Service Control
Warning	6/16/2022 5:45:17 PM	ActiveDirectory_D...	2092	Replication
Error	6/16/2022 5:44:53 PM	ActiveDirectory_D...	2087	DS RPC Client
Warning	6/16/2022 5:44:47 PM	ActiveDirectory_D...	2092	Replication
Information	6/16/2022 5:44:17 PM	ActiveDirectory_D...	1000	Service Control
Warning	6/16/2022 5:44:17 PM	ActiveDirectory_D...	3041	LDAP Interface
Warning	6/16/2022 5:44:17 PM	ActiveDirectory_D...	2886	LDAP Interface
Information	6/16/2022 5:44:07 PM	ActiveDirectory_D...	2405	Internal Configur...
Information	6/16/2022 5:44:07 PM	ActiveDirectory_D...	2405	Internal Configur...
Information	6/16/2022 5:44:07 PM	ActiveDirectory_D...	2120	Internal Configur...

Event 2092, ActiveDirectory_DomainService

General | Details

This server is the owner of the following FSMO role, but does not consider it valid. For the partition which contains the FSMO, this server has not replicated successfully with any of its partners since this server has been restarted. Replication errors are preventing validation of this role.

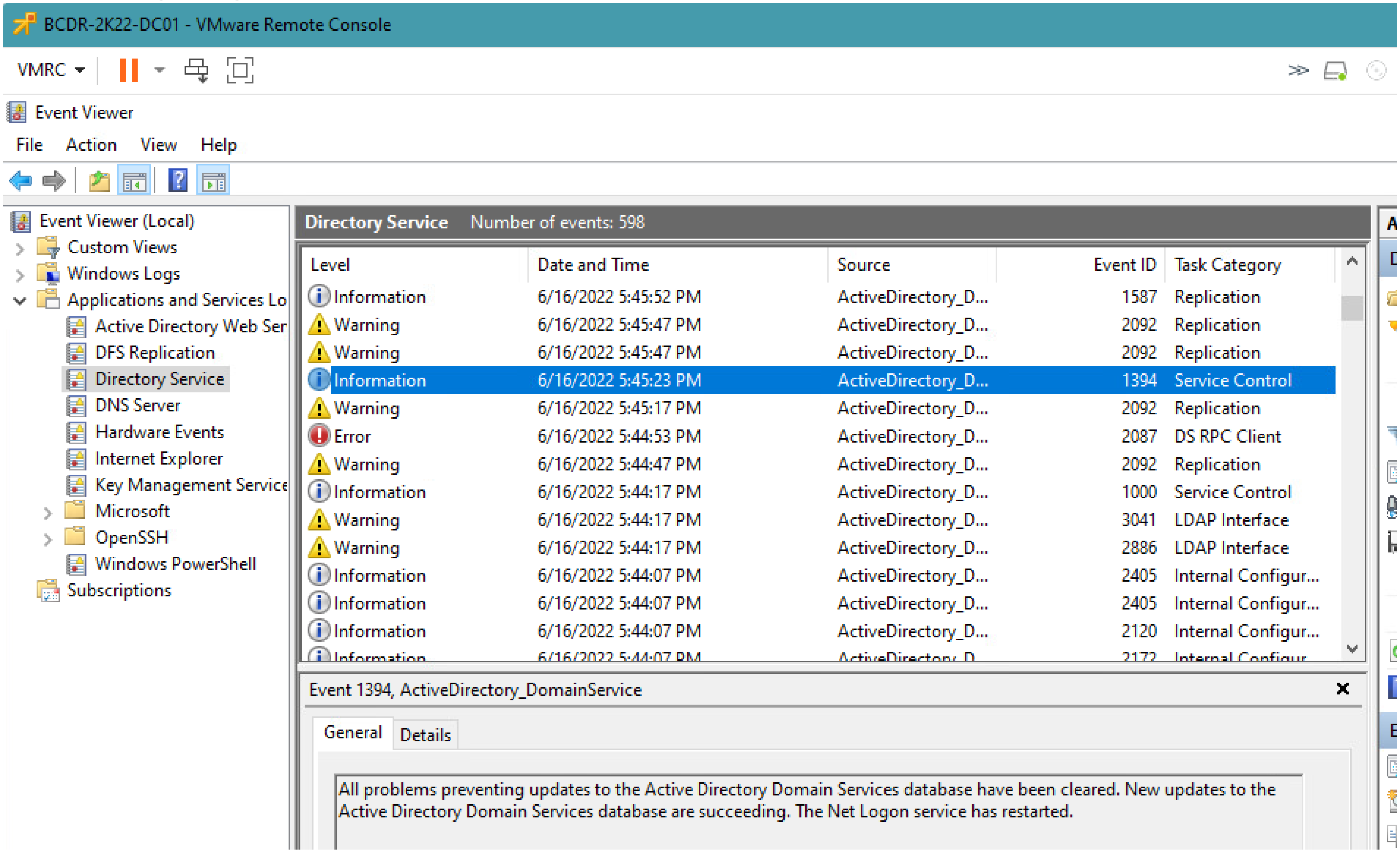
Operations which require contacting a FSMO operation master will fail until this condition is corrected.

FSMO Role: CN=RID Manager$,CN=System,DC=bcdr,DC=local

User Action:

1. Initial synchronization is the first early replications done by a system as it is starting. A failure to initially synchronize may explain why a FSMO role cannot be validated. This process is explained in KB article 305476.
2. This server has one or more replication partners, and replication is failing for all of these partners. Use the command repadmin /showrepl to display the replication errors. Correct the error in question. For example there maybe problems with IP connectivity, DNS name resolution, or security authentication that are preventing successful replication.
3. In the rare event that all replication partners are expected to be offline (for example, because of maintenance or disaster recovery), you can force the role to be validated. This can be done by using NTDSUTIL.EXE to seize the role to the same server. This may be done using the steps provided in KB articles 255504 and 324801 on http://support.microsoft.com.

- After rebooting the FSMO Role Holder **(DC01)** the second time (with our in-guest Script), things begin to look better.



Directory Service   Number of events: 598

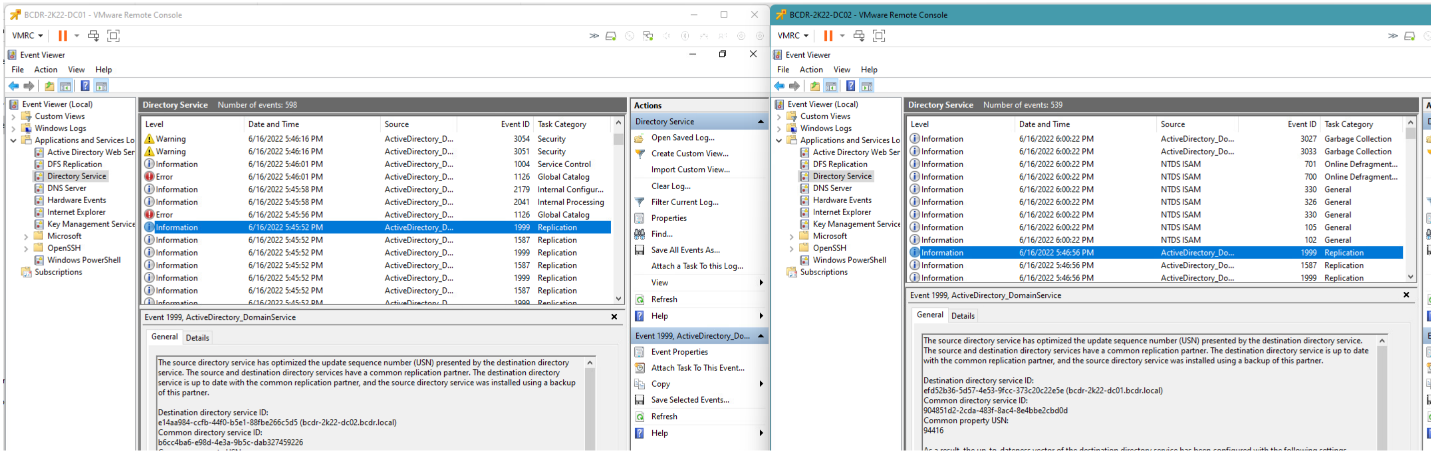
Level	Date and Time	Source	Event ID	Task Category
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1587	Replication
Warning	6/16/2022 5:45:47 PM	ActiveDirectory_D...	2092	Replication
Warning	6/16/2022 5:45:47 PM	ActiveDirectory_D...	2092	Replication
Information	6/16/2022 5:45:23 PM	ActiveDirectory_D...	1394	Service Control
Warning	6/16/2022 5:45:17 PM	ActiveDirectory_D...	2092	Replication
Error	6/16/2022 5:44:53 PM	ActiveDirectory_D...	2087	DS RPC Client
Warning	6/16/2022 5:44:47 PM	ActiveDirectory_D...	2092	Replication
Information	6/16/2022 5:44:17 PM	ActiveDirectory_D...	1000	Service Control
Warning	6/16/2022 5:44:17 PM	ActiveDirectory_D...	3041	LDAP Interface
Warning	6/16/2022 5:44:17 PM	ActiveDirectory_D...	2886	LDAP Interface
Information	6/16/2022 5:44:07 PM	ActiveDirectory_D...	2405	Internal Configur...
Information	6/16/2022 5:44:07 PM	ActiveDirectory_D...	2405	Internal Configur...
Information	6/16/2022 5:44:07 PM	ActiveDirectory_D...	2120	Internal Configur...
Information	6/16/2022 5:44:07 PM	ActiveDirectory_D...	2172	Internal Configur...

Event 1394, ActiveDirectory_DomainService

General | Details

All problems preventing updates to the Active Directory Domain Services database have been cleared. New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted.

- At this point, the DCs have discarded their RID Pool, obtained a new set, have a new Invocational and can begin to use a new batch of USNs.



Directory Service   Number of events: 598

Level	Date and Time	Source	Event ID	Task Category
Warning	6/16/2022 5:46:16 PM	ActiveDirectory_D...	3054	Security
Warning	6/16/2022 5:46:16 PM	ActiveDirectory_D...	3051	Security
Information	6/16/2022 5:46:01 PM	ActiveDirectory_D...	1004	Service Control
Error	6/16/2022 5:46:01 PM	ActiveDirectory_D...	1126	Global Catalog
Information	6/16/2022 5:45:58 PM	ActiveDirectory_D...	2179	Internal Configur...
Information	6/16/2022 5:45:58 PM	ActiveDirectory_D...	2041	Internal Processing
Error	6/16/2022 5:45:56 PM	ActiveDirectory_D...	1126	Global Catalog
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1999	Replication
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1587	Replication
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1999	Replication
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1587	Replication
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1999	Replication
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1587	Replication
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1999	Replication

Event 1999, ActiveDirectory_DomainService

General | Details

The source directory service has optimized the update sequence number (USN) presented by the destination directory service. The source and destination directory services have a common replication partner. The destination directory service is up to date with the common replication partner, and the source directory service was installed using a backup of this partner.

Destination directory service ID:
e14aa984-ccfb-44f0-b5e1-88fbe266c5d5 (bcdr-2k22-dc02.bcdr.local)
Common directory service ID:
b6cc4ba6-e98d-4e3a-9b5c-dab327459226

Directory Service   Number of events: 539

Level	Date and Time	Source	Event ID	Task Category
Information	6/16/2022 6:00:22 PM	ActiveDirectory_Do...	3027	Garbage Collection
Information	6/16/2022 6:00:22 PM	ActiveDirectory_Do...	3033	Garbage Collection
Information	6/16/2022 6:00:22 PM	NTDS ISAM	701	Online Defragment...
Information	6/16/2022 6:00:22 PM	NTDS ISAM	700	Online Defragment...
Information	6/16/2022 6:00:22 PM	NTDS ISAM	330	General
Information	6/16/2022 6:00:22 PM	NTDS ISAM	326	General
Information	6/16/2022 6:00:22 PM	NTDS ISAM	330	General
Information	6/16/2022 6:00:22 PM	NTDS ISAM	105	General
Information	6/16/2022 6:00:22 PM	NTDS ISAM	102	General
Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do...	1999	Replication
Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do...	1587	Replication
Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do...	1999	Replication

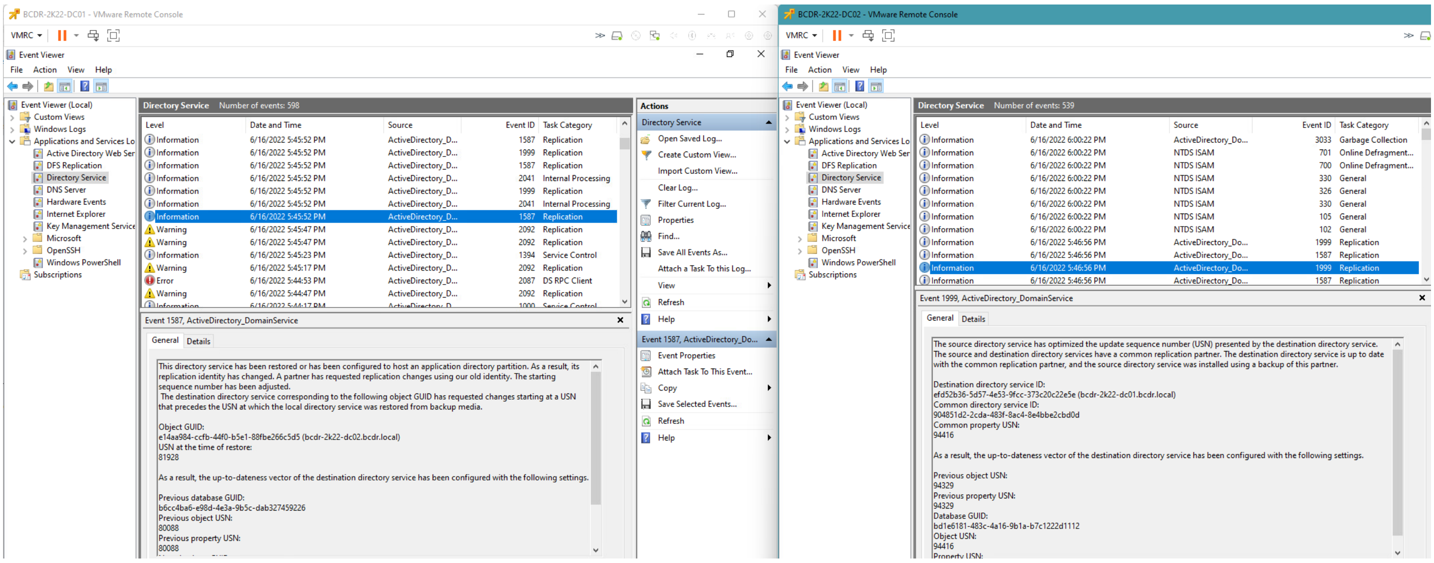
Event 1999, ActiveDirectory_DomainService

General | Details

The source directory service has optimized the update sequence number (USN) presented by the destination directory service. The source and destination directory services have a common replication partner. The destination directory service is up to date with the common replication partner, and the source directory service was installed using a backup of this partner.

Destination directory service ID:
efd52b36-5d57-4e53-9fcc-373c20c22e5e (bcdr-2k22-dc01.bcdr.local)
Common directory service ID:
904851d2-2cda-483f-8ac4-8e4bbe2cbd0d
Common property USN:
94416

As a result, the up-to-dateness vector of the destination directory service has been configured with the following settings.


BCDR-2K22-DC01 - VMware Remote Console
BCDR-2K22-DC02 - VMware Remote Console
Event Viewer
Actions

Directory Service Number of events: 598

Level	Date and Time	Source	Event ID	Task Category
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1587	Replication
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1999	Replication
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1587	Replication
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	2041	Internal Processing
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1999	Replication
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	2041	Internal Processing
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1587	Replication
Warning	6/16/2022 5:45:47 PM	ActiveDirectory_D...	2092	Replication
Warning	6/16/2022 5:45:47 PM	ActiveDirectory_D...	2092	Replication
Information	6/16/2022 5:45:23 PM	ActiveDirectory_D...	1394	Service Control
Warning	6/16/2022 5:45:17 PM	ActiveDirectory_D...	2092	Replication
Error	6/16/2022 5:44:53 PM	ActiveDirectory_D...	2087	DS RPC Client
Warning	6/16/2022 5:44:47 PM	ActiveDirectory_D...	2092	Replication

Event 1587, ActiveDirectory_DomainService

```
This directory service has been restored or has been configured to host an application directory partition. As a result, its
replication identity has changed. A partner has requested replication changes using our old identity. The starting
sequence number has been adjusted.
 The destination directory service corresponding to the following object GUID has requested changes starting at a USN
that precedes the USN at which the local directory service was restored from backup media.

Object GUID:
e14aa984-ccfb-44f0-b5e1-88fbe266c5d5 (bcdr-2k22-dc02.bcdr.local)
USN at the time of restore:
81928

As a result, the up-to-dateness vector of the destination directory service has been configured with the following settings.

Previous database GUID:
b6cc4ba6-e98d-4e3a-9b5c-dab327459226
Previous object USN:
80088
Previous property USN:
80088
```

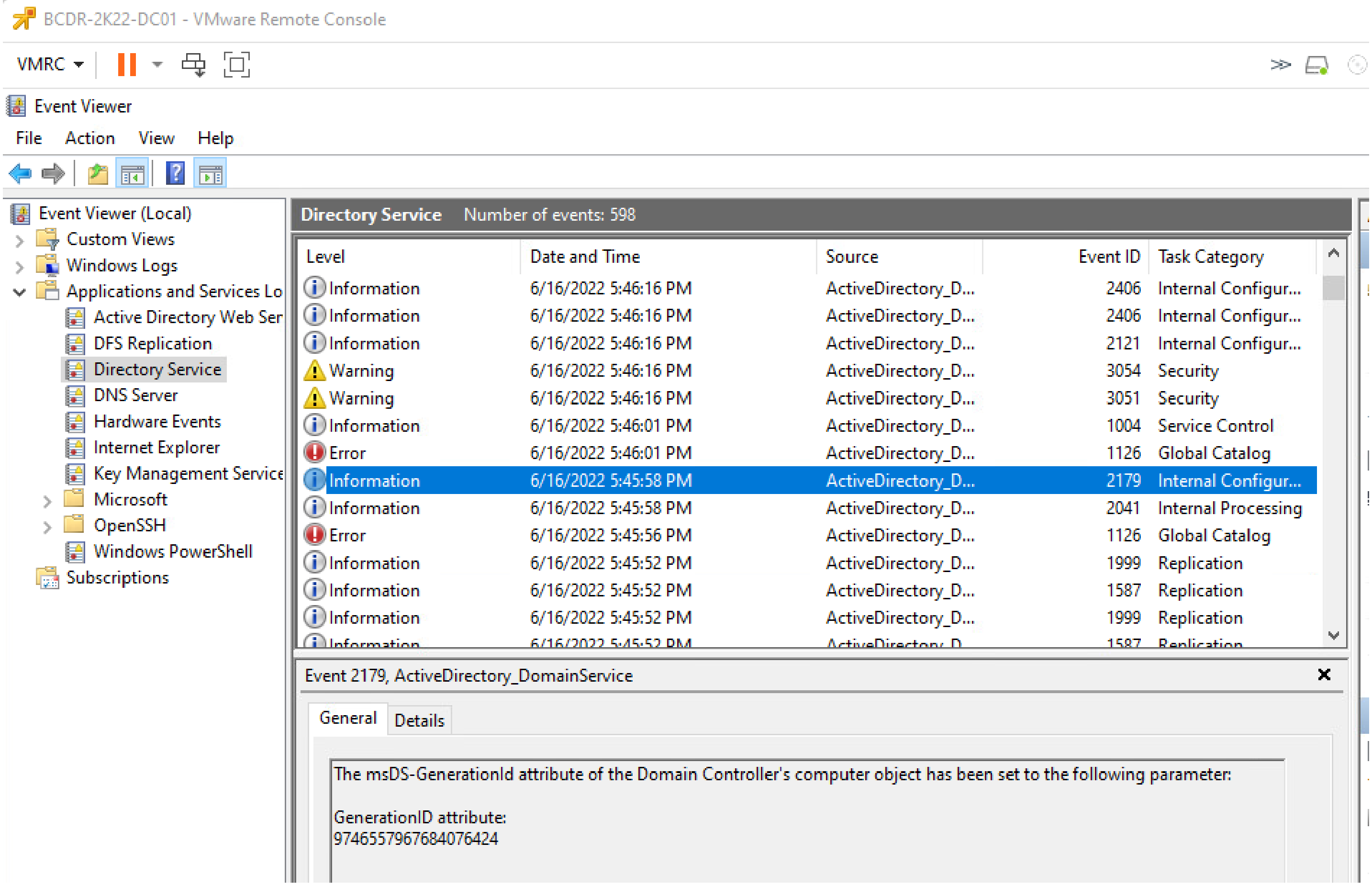
Directory Service Number of events: 539

Level	Date and Time	Source	Event ID	Task Category
Information	6/16/2022 6:00:22 PM	ActiveDirectory_Do...	3033	Garbage Collection
Information	6/16/2022 6:00:22 PM	NTDS ISAM	701	Online Defragment...
Information	6/16/2022 6:00:22 PM	NTDS ISAM	700	Online Defragment...
Information	6/16/2022 6:00:22 PM	NTDS ISAM	330	General
Information	6/16/2022 6:00:22 PM	NTDS ISAM	326	General
Information	6/16/2022 6:00:22 PM	NTDS ISAM	330	General
Information	6/16/2022 6:00:22 PM	NTDS ISAM	105	General
Information	6/16/2022 6:00:22 PM	NTDS ISAM	102	General
Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do...	1999	Replication
Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do...	1587	Replication
Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do...	1999	Replication
Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do...	1587	Replication

Event 1999, ActiveDirectory_DomainService

```
The source directory service has optimized the update sequence number (USN) presented by the destination directory service.
The source and destination directory services have a common replication partner. The destination directory service is up to date
with the common replication partner, and the source directory service was installed using a backup of this partner.

Destination directory service ID:
efd52b36-5d57-4e53-9fcc-373c20c22e5e (bcdr-2k22-dc01.bcdr.local)
Common directory service ID:
904851d2-2cda-483f-8ac4-8e4bbe2cbd0d
Common property USN:
94416

As a result, the up-to-dateness vector of the destination directory service has been configured with the following settings.

Previous object USN:
94329
Previous property USN:
94329
Database GUID:
bd1e6181-483c-4a16-9b1a-b7c1222d1112
Object USN:
94416
```

- Windows has also accepted the new VM-Generation ID generated for the VM by our SRM Recovery exercise. The window will now store this for subsequent comparison next time the VM is rebooted



Directory Service Number of events: 598

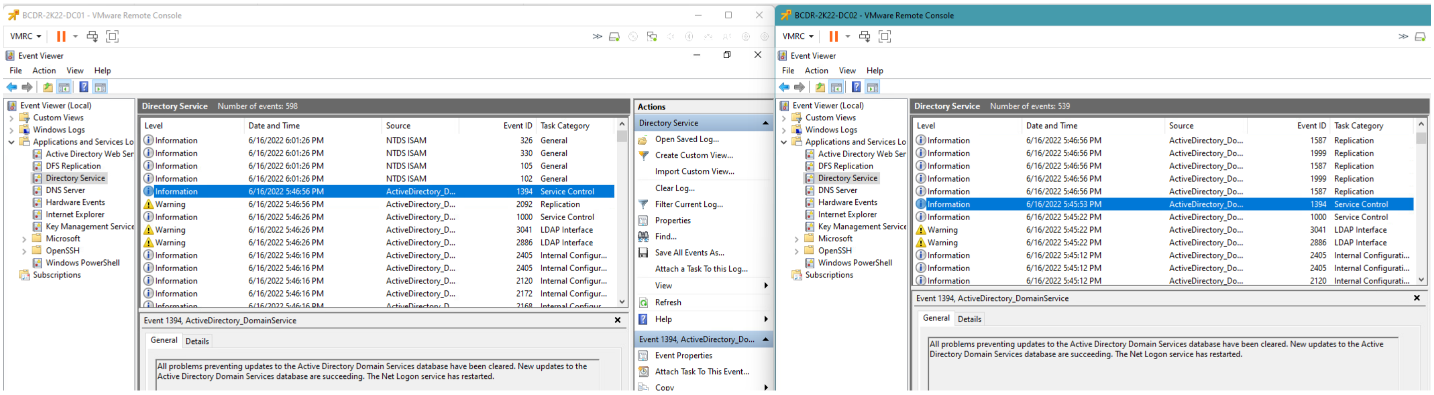
Level	Date and Time	Source	Event ID	Task Category
Information	6/16/2022 5:46:16 PM	ActiveDirectory_D...	2406	Internal Configur...
Information	6/16/2022 5:46:16 PM	ActiveDirectory_D...	2406	Internal Configur...
Information	6/16/2022 5:46:16 PM	ActiveDirectory_D...	2121	Internal Configur...
Warning	6/16/2022 5:46:16 PM	ActiveDirectory_D...	3054	Security
Warning	6/16/2022 5:46:16 PM	ActiveDirectory_D...	3051	Security
Information	6/16/2022 5:46:01 PM	ActiveDirectory_D...	1004	Service Control
Error	6/16/2022 5:46:01 PM	ActiveDirectory_D...	1126	Global Catalog
Information	6/16/2022 5:45:58 PM	ActiveDirectory_D...	2179	Internal Configur...
Information	6/16/2022 5:45:58 PM	ActiveDirectory_D...	2041	Internal Processing
Error	6/16/2022 5:45:56 PM	ActiveDirectory_D...	1126	Global Catalog
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1999	Replication
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1587	Replication
Information	6/16/2022 5:45:52 PM	ActiveDirectory_D...	1999	Replication

Event 2179, ActiveDirectory_DomainService

General | Details

```
The msDS-GenerationId attribute of the Domain Controller's computer object has been set to the following parameter:

GenerationID attribute:
9746557967684076424
```

- DC02 has also been successfully remediated. Because it is not the FSMO Role holder, part of its healing process (for example, obtaining a new RID Pool) had to be supported by the availability of the Role holder.



BCDR-2K22-DC01 - VMware Remote Console

Event Viewer

Directory Service Number of events: 598

Level	Date and Time	Source	Event ID	Task Category
Information	6/16/2022 6:01:26 PM	NTDS ISAM	326	General
Information	6/16/2022 6:01:26 PM	NTDS ISAM	330	General
Information	6/16/2022 6:01:26 PM	NTDS ISAM	105	General
Information	6/16/2022 6:01:26 PM	NTDS ISAM	102	General
Information	6/16/2022 5:46:56 PM	ActiveDirectory_D...	1394	Service Control
Warning	6/16/2022 5:46:56 PM	ActiveDirectory_D...	2092	Replication
Information	6/16/2022 5:46:26 PM	ActiveDirectory_D...	1000	Service Control
Warning	6/16/2022 5:46:26 PM	ActiveDirectory_D...	3041	LDAP Interface
Warning	6/16/2022 5:46:26 PM	ActiveDirectory_D...	2886	LDAP Interface
Information	6/16/2022 5:46:16 PM	ActiveDirectory_D...	2405	Internal Configur...
Information	6/16/2022 5:46:16 PM	ActiveDirectory_D...	2405	Internal Configur...
Information	6/16/2022 5:46:16 PM	ActiveDirectory_D...	2120	Internal Configur...
Information	6/16/2022 5:46:16 PM	ActiveDirectory_D...	2172	Internal Configur...
Information	6/16/2022 5:46:16 PM	ActiveDirectory_D...	2168	Internal Configur...

Event 1394, ActiveDirectory_DomainService

All problems preventing updates to the Active Directory Domain Services database have been cleared. New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted.

BCDR-2K22-DC02 - VMware Remote Console

Event Viewer

Directory Service Number of events: 539

Level	Date and Time	Source	Event ID	Task Category
Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do...	1587	Replication
Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do...	1999	Replication
Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do...	1587	Replication
Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do...	1999	Replication
Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do...	1587	Replication
Information	6/16/2022 5:45:53 PM	ActiveDirectory_Do...	1394	Service Control
Information	6/16/2022 5:45:22 PM	ActiveDirectory_Do...	1000	Service Control
Warning	6/16/2022 5:45:22 PM	ActiveDirectory_Do...	3041	LDAP Interface
Warning	6/16/2022 5:45:22 PM	ActiveDirectory_Do...	2886	LDAP Interface
Information	6/16/2022 5:45:12 PM	ActiveDirectory_Do...	2405	Internal Configurati...
Information	6/16/2022 5:45:12 PM	ActiveDirectory_Do...	2405	Internal Configurati...
Information	6/16/2022 5:45:12 PM	ActiveDirectory_Do...	2120	Internal Configurati...

Event 1394, ActiveDirectory_DomainService

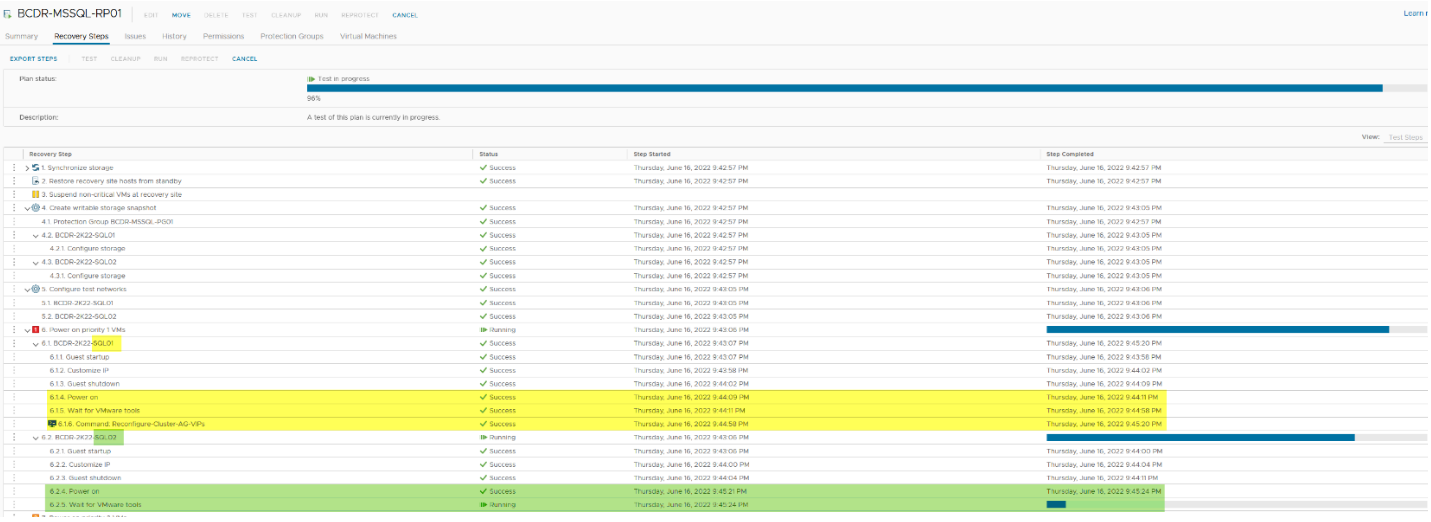
All problems preventing updates to the Active Directory Domain Services database have been cleared. New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted.

Recovering Microsoft SQL Server (AG) with VMware Site Recovery Manager

Now that the Domain Controllers have been recovered at the Recovery Site, we are ready to recover our Microsoft SQL Server Availability Group cluster. Remember that our objective here is to ensure that we do not just recover the individual VMs, we also want to recover the services they provide. This means that, upon recovery, the cluster service and resources (databases, jobs, scripts) also have to be available, accessible and operational.

Let's start our Microsoft SQL Server Recovery Plan, following the same process as we did for the DC Recovery Plan above.

Take note of the startup sequence of the two VMs in our **Recovery Plan**. SRM does not begin to power on **SQL02** until **SQL01** has completed bootup and the **in-Guest Script** has been called - this is **Dependency** at work.



BCDR-MSSQL-RP01

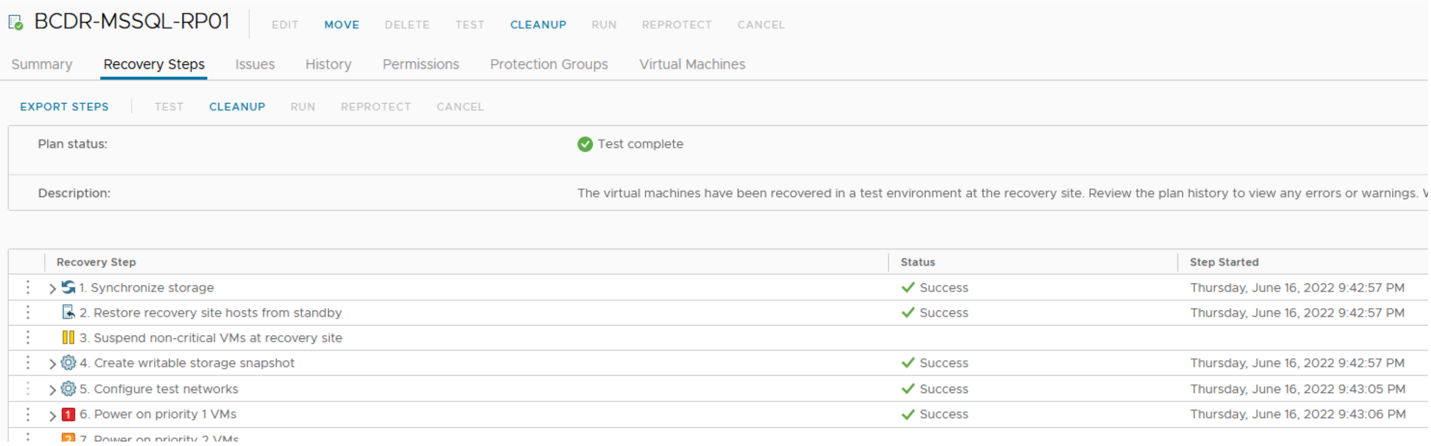
Plan status: Test in progress 96%

Description: A test of this plan is currently in progress.

View: Test Steps

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage	✓ Success	Thursday, June 16, 2022 9:42:57 PM	Thursday, June 16, 2022 9:42:57 PM
2. Restore recovery site hosts from standby	✓ Success	Thursday, June 16, 2022 9:42:57 PM	Thursday, June 16, 2022 9:42:57 PM
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot	✓ Success	Thursday, June 16, 2022 9:42:57 PM	Thursday, June 16, 2022 9:43:05 PM
4.1. Protection Group BCDR-MSSQL-PG01	✓ Success	Thursday, June 16, 2022 9:42:57 PM	Thursday, June 16, 2022 9:42:57 PM
4.2. BCDR-2K22-SQL01	✓ Success	Thursday, June 16, 2022 9:42:57 PM	Thursday, June 16, 2022 9:43:05 PM
4.2.1. Configure storage	✓ Success	Thursday, June 16, 2022 9:42:57 PM	Thursday, June 16, 2022 9:43:05 PM
4.3. BCDR-2K22-SQL02	✓ Success	Thursday, June 16, 2022 9:42:57 PM	Thursday, June 16, 2022 9:43:05 PM
4.3.1. Configure storage	✓ Success	Thursday, June 16, 2022 9:42:57 PM	Thursday, June 16, 2022 9:43:05 PM
5. Configure test networks	✓ Success	Thursday, June 16, 2022 9:43:05 PM	Thursday, June 16, 2022 9:43:06 PM
5.1. BCDR-2K22-SQL01	✓ Success	Thursday, June 16, 2022 9:43:05 PM	Thursday, June 16, 2022 9:43:06 PM
5.2. BCDR-2K22-SQL02	✓ Success	Thursday, June 16, 2022 9:43:05 PM	Thursday, June 16, 2022 9:43:06 PM
6. Power on priority 1 VMs	Running	Thursday, June 16, 2022 9:43:06 PM	
6.1. BCDR-2K22-SQL01	✓ Success	Thursday, June 16, 2022 9:43:07 PM	Thursday, June 16, 2022 9:45:20 PM
6.1.1. Guest startup	✓ Success	Thursday, June 16, 2022 9:43:07 PM	Thursday, June 16, 2022 9:43:58 PM
6.1.2. Customize IP	✓ Success	Thursday, June 16, 2022 9:43:58 PM	Thursday, June 16, 2022 9:44:02 PM
6.1.3. Guest shutdown	✓ Success	Thursday, June 16, 2022 9:44:02 PM	Thursday, June 16, 2022 9:44:09 PM
6.1.4. Power on	✓ Success	Thursday, June 16, 2022 9:44:09 PM	Thursday, June 16, 2022 9:44:11 PM
6.1.5. Wait for VMware tools	✓ Success	Thursday, June 16, 2022 9:44:11 PM	Thursday, June 16, 2022 9:44:58 PM
6.1.6. Command: Reconfigure-Cluster-AG-VIPs	✓ Success	Thursday, June 16, 2022 9:44:58 PM	Thursday, June 16, 2022 9:45:20 PM
6.2. BCDR-2K22-SQL02	Running	Thursday, June 16, 2022 9:43:06 PM	
6.2.1. Guest startup	✓ Success	Thursday, June 16, 2022 9:43:06 PM	Thursday, June 16, 2022 9:44:00 PM
6.2.2. Customize IP	✓ Success	Thursday, June 16, 2022 9:44:00 PM	Thursday, June 16, 2022 9:44:04 PM
6.2.3. Guest shutdown	✓ Success	Thursday, June 16, 2022 9:44:04 PM	Thursday, June 16, 2022 9:44:11 PM
6.2.4. Power on	✓ Success	Thursday, June 16, 2022 9:45:21 PM	Thursday, June 16, 2022 9:45:24 PM
6.2.5. Wait for VMware tools	Running	Thursday, June 16, 2022 9:45:24 PM	

Recovery done



BCDR-MSSQL-RP01

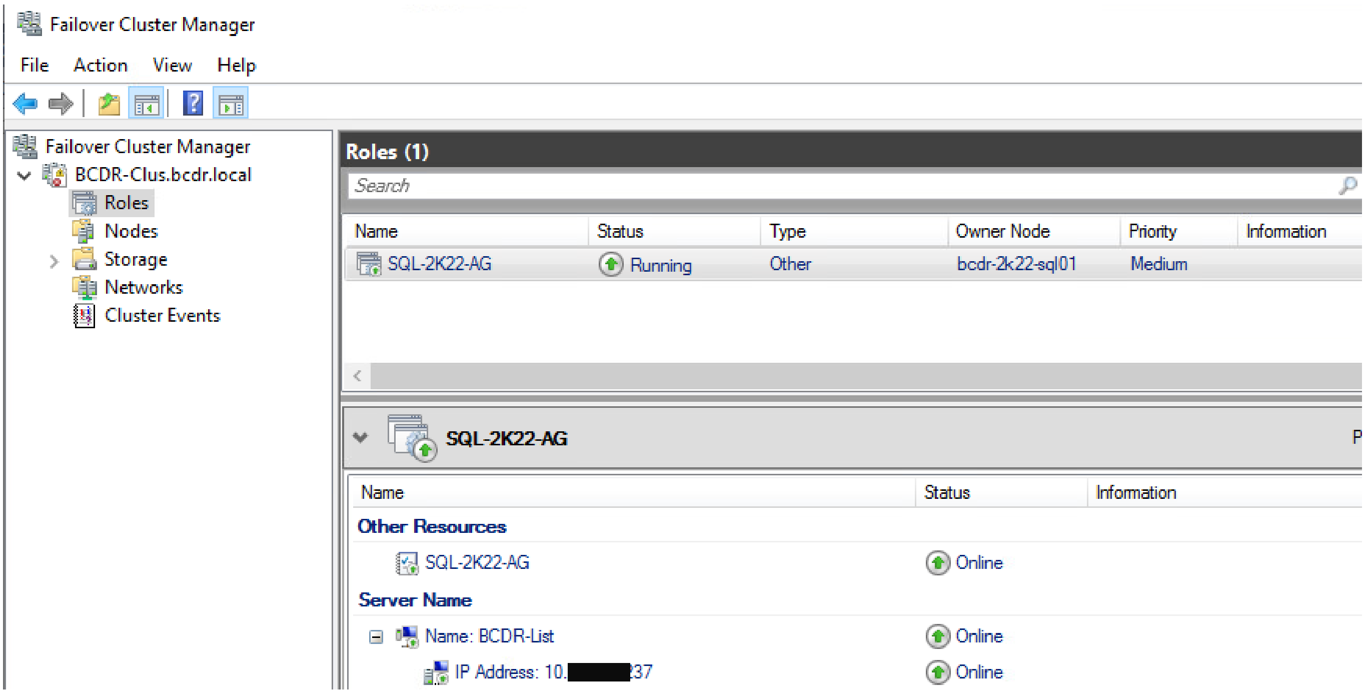
Plan status: ✓ Test complete

Description: The virtual machines have been recovered in a test environment at the recovery site. Review the plan history to view any errors or warnings. V

Recovery Step	Status	Step Started
1. Synchronize storage	✓ Success	Thursday, June 16, 2022 9:42:57 PM
2. Restore recovery site hosts from standby	✓ Success	Thursday, June 16, 2022 9:42:57 PM
3. Suspend non-critical VMs at recovery site		
4. Create writable storage snapshot	✓ Success	Thursday, June 16, 2022 9:42:57 PM
5. Configure test networks	✓ Success	Thursday, June 16, 2022 9:43:05 PM
6. Power on priority 1 VMs	✓ Success	Thursday, June 16, 2022 9:43:06 PM
7. Power on priority 2 VMs		

How is our Microsoft SQL Server Cluster doing? Let's log into Windows and check.

- Windows Server Failover Clustering supporting SQL Server Availability Group is fully functional

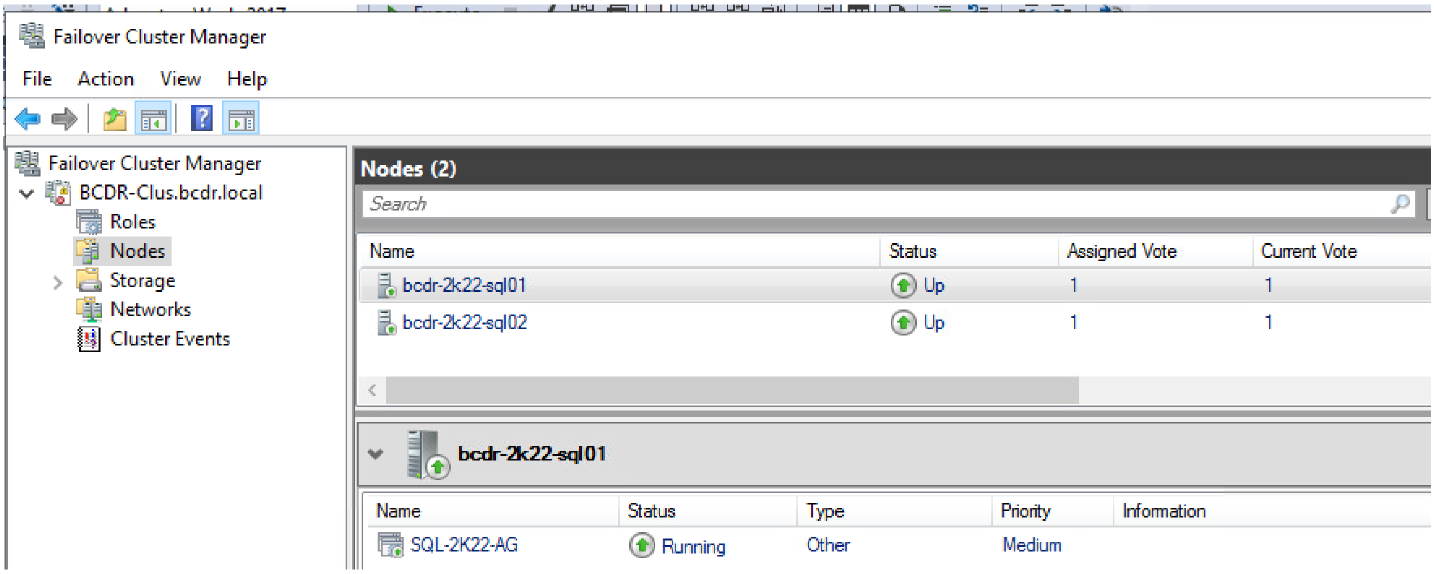


Roles (1)

Name	Status	Type	Owner Node	Priority	Information
SQL-2K22-AG	Running	Other	bcdr-2k22-sql01	Medium	

SQL-2K22-AG

Name	Status	Information
Other Resources		
SQL-2K22-AG	Online	
Server Name		
Name: BCDR-List	Online	
IP Address: 10.[redacted]37	Online	



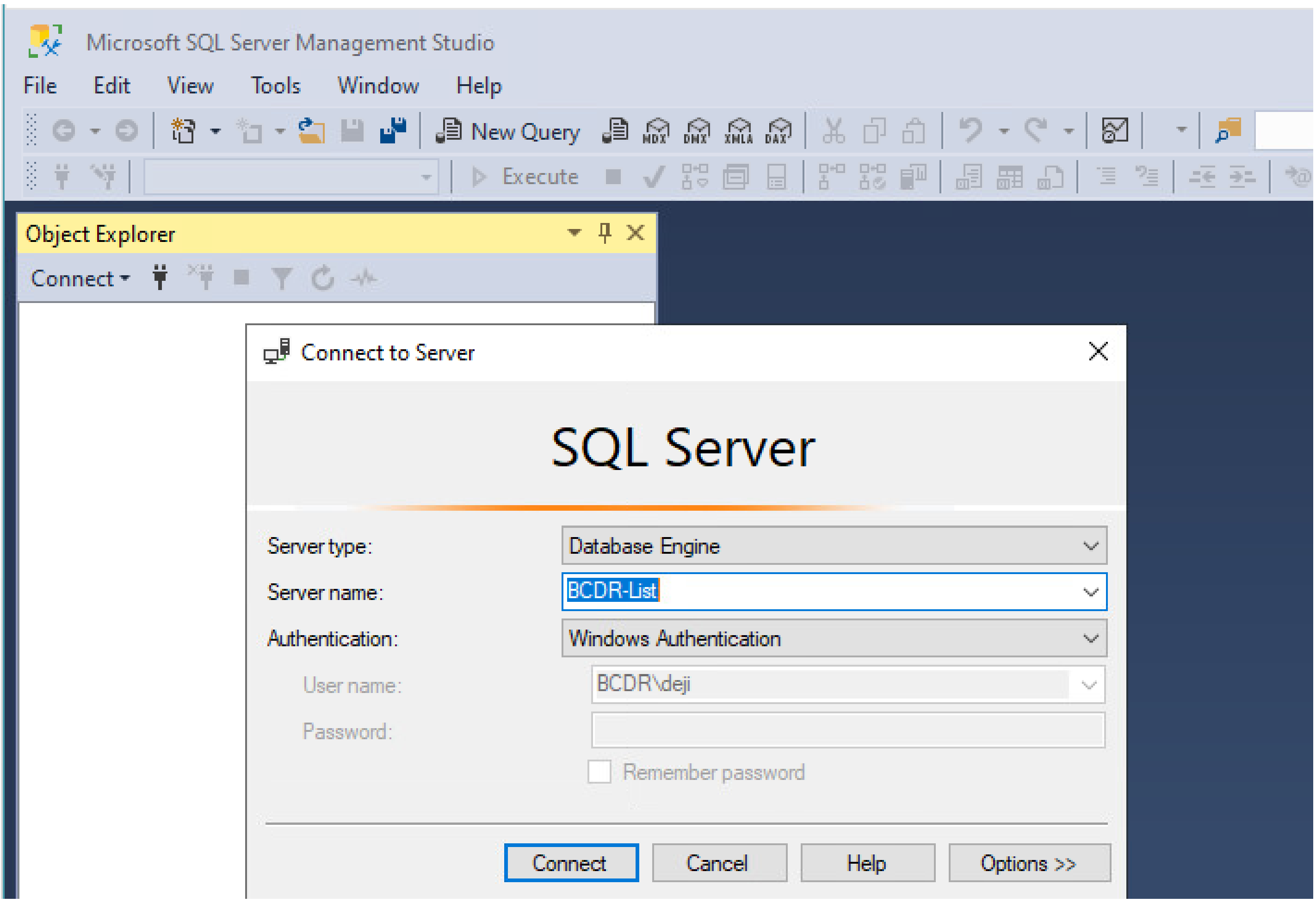
Nodes (2)

Name	Status	Assigned Vote	Current Vote
bcdr-2k22-sql01	Up	1	1
bcdr-2k22-sql02	Up	1	1

bcdr-2k22-sql01

Name	Status	Type	Priority	Information
SQL-2K22-AG	Running	Other	Medium	

- The Microsoft SQL Server **Listener** resource is also up and available.



Server type: Database Engine

Server name: BCDR-List

Authentication: Windows Authentication

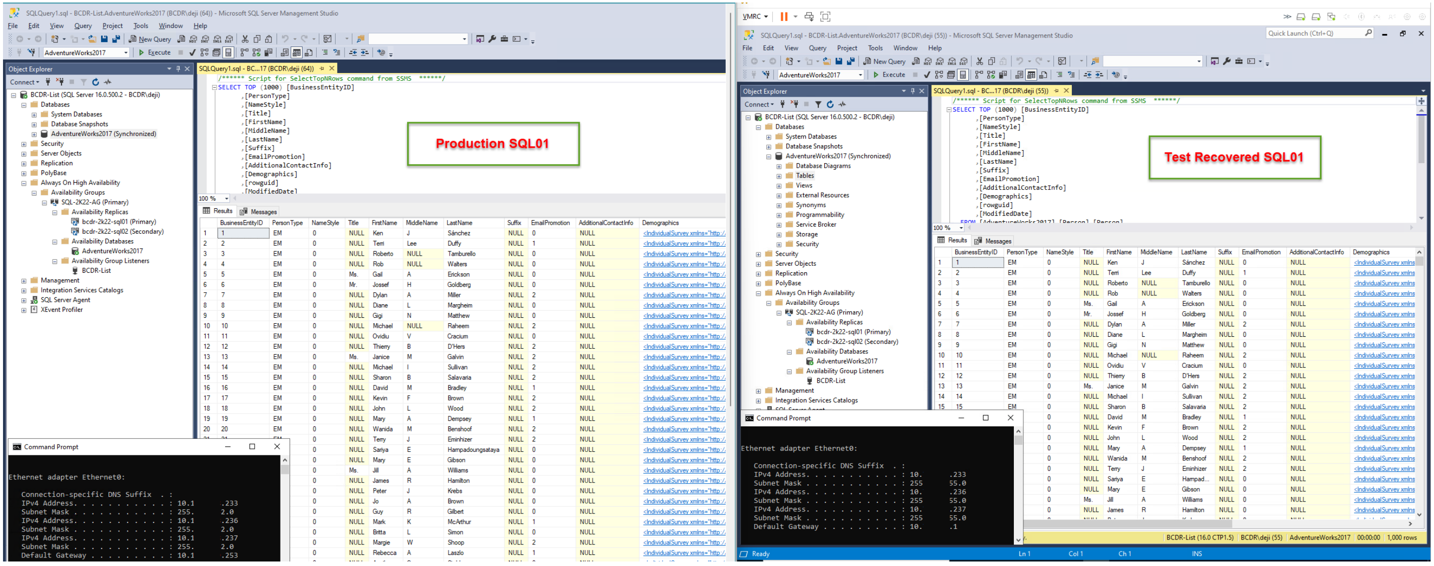
User name: BCDR\deji

Password:

□ Remember password

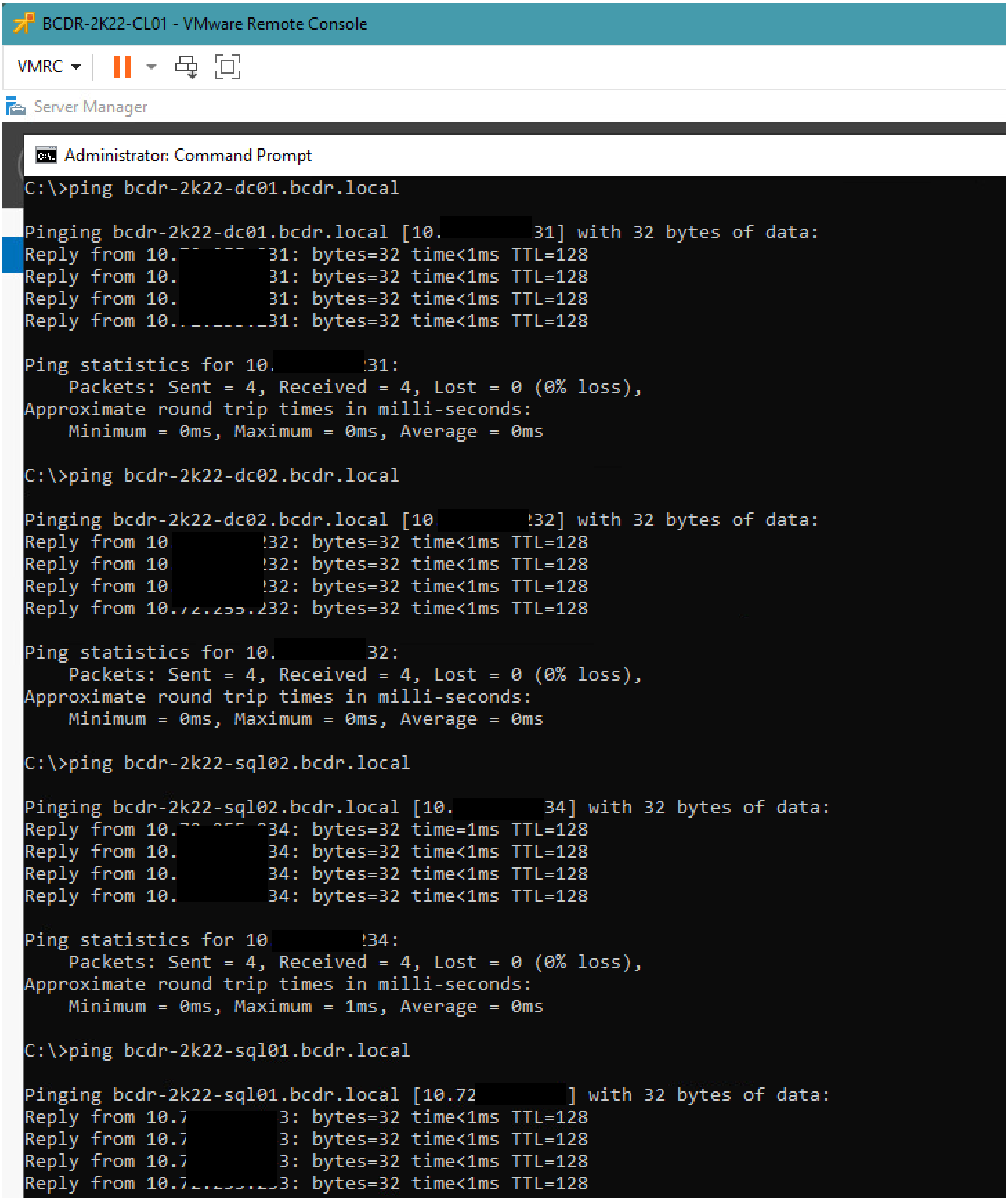
Since this is a **TEST Recovery** exercise, let’s confirm that our **Production Microsoft SQL Server Cluster** is still up and functional at the **Protected Site**.

- Here is the **Production** Microsoft SQL Server instance and its **Test Copy** side-by-side.



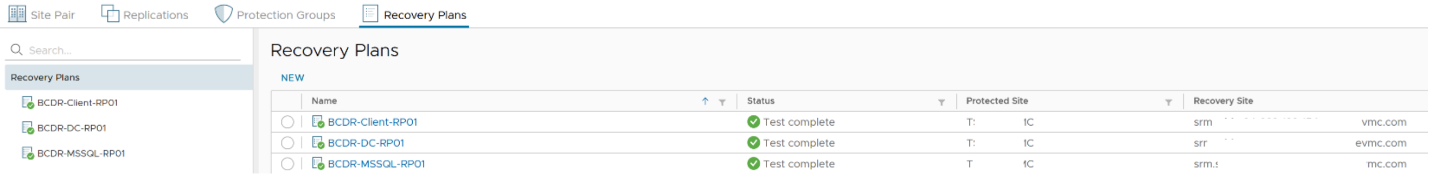
In a TEST Recovery exercise, the recovered workloads are not supposed to be able to communicate with the Production environment. This is because they are recovered into the SRM "Test Network" we specified in the previous steps. All workloads recovered into this **"Test Network"** can communicate with each other, though. This gives the administrators/operators the ability to more robustly test and verify the integrity of the recovery process and ascertain the availability and accessibility of the services they provide.

We are now going to recover our **Client VM** and use it to confirm that our test recovery works as intended.


BCDR-2K22-CL01 - VMware Remote Console
VMRC
Server Manager
Administrator: Command Prompt

```
C:\>ping bcdr-2k22-dc01.bcdr.local

Pinging bcdr-2k22-dc01.bcdr.local [10.[redacted]31] with 32 bytes of data:
Reply from 10.[redacted]31: bytes=32 time<1ms TTL=128
Reply from 10.[redacted]31: bytes=32 time<1ms TTL=128
Reply from 10.[redacted]31: bytes=32 time<1ms TTL=128
Reply from 10.[redacted]31: bytes=32 time<1ms TTL=128

Ping statistics for 10.[redacted]31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping bcdr-2k22-dc02.bcdr.local

Pinging bcdr-2k22-dc02.bcdr.local [10[redacted]32] with 32 bytes of data:
Reply from 10[redacted]32: bytes=32 time<1ms TTL=128
Reply from 10[redacted]32: bytes=32 time<1ms TTL=128
Reply from 10[redacted]32: bytes=32 time<1ms TTL=128
Reply from 10[redacted]32: bytes=32 time<1ms TTL=128

Ping statistics for 10.[redacted]32:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping bcdr-2k22-sql02.bcdr.local

Pinging bcdr-2k22-sql02.bcdr.local [10.[redacted]34] with 32 bytes of data:
Reply from 10.[redacted]34: bytes=32 time=1ms TTL=128
Reply from 10.[redacted]34: bytes=32 time<1ms TTL=128
Reply from 10.[redacted]34: bytes=32 time<1ms TTL=128
Reply from 10.[redacted]34: bytes=32 time<1ms TTL=128

Ping statistics for 10[redacted]34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping bcdr-2k22-sql01.bcdr.local

Pinging bcdr-2k22-sql01.bcdr.local [10.72[redacted]] with 32 bytes of data:
Reply from 10.7[redacted]3: bytes=32 time<1ms TTL=128
Reply from 10.7[redacted]3: bytes=32 time<1ms TTL=128
Reply from 10.7[redacted]3: bytes=32 time<1ms TTL=128
Reply from 10.7[redacted]3: bytes=32 time<1ms TTL=128
```

We have now successfully performed a **Test Recovery** of our **Recovery Plan**. If there were any failures, misconfiguration, or unexpected behaviors, we would be able to correct them by editing the plan and re-testing the changes without any disruption of services in Production.



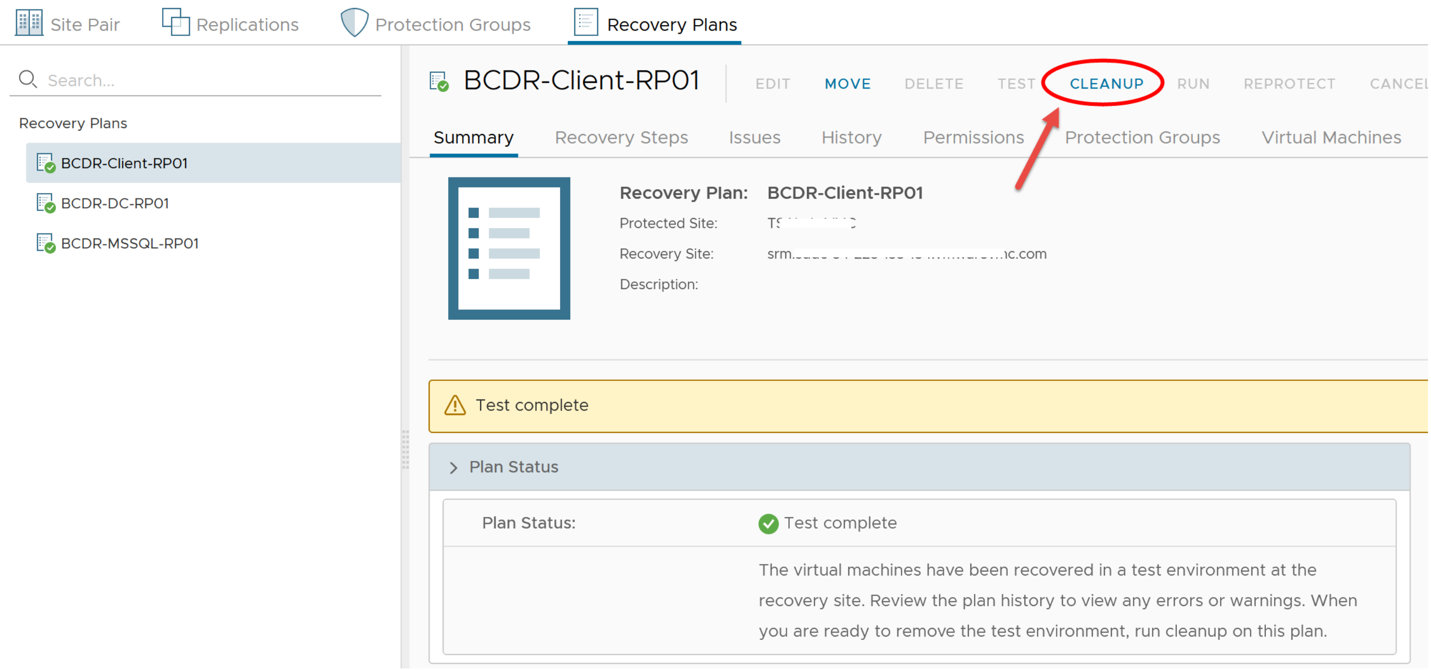
Recovery Plans

	Name	Status	Protected Site	Recovery Site
○	BCDR-Client-RP01	✓ Test complete	T: [redacted] 1C	srm [redacted] vmc.com
○	BCDR-DC-RP01	✓ Test complete	T: [redacted] 1C	srr [redacted] evmc.com
○	BCDR-MSSQL-RP01	✓ Test complete	T [redacted] 1C	srm.: [redacted] mc.com

Cleaning up after Test Recovery

Now that we are done with our **Test Recovery** exercise, we need to clean up the test environment.

- To do this, select the Recovery Plan and click "**Cleanup**".



Recovery Plan: BCDR-Client-RP01

Protected Site: T[redacted]

Recovery Site: srm.[redacted]c.com

Description:

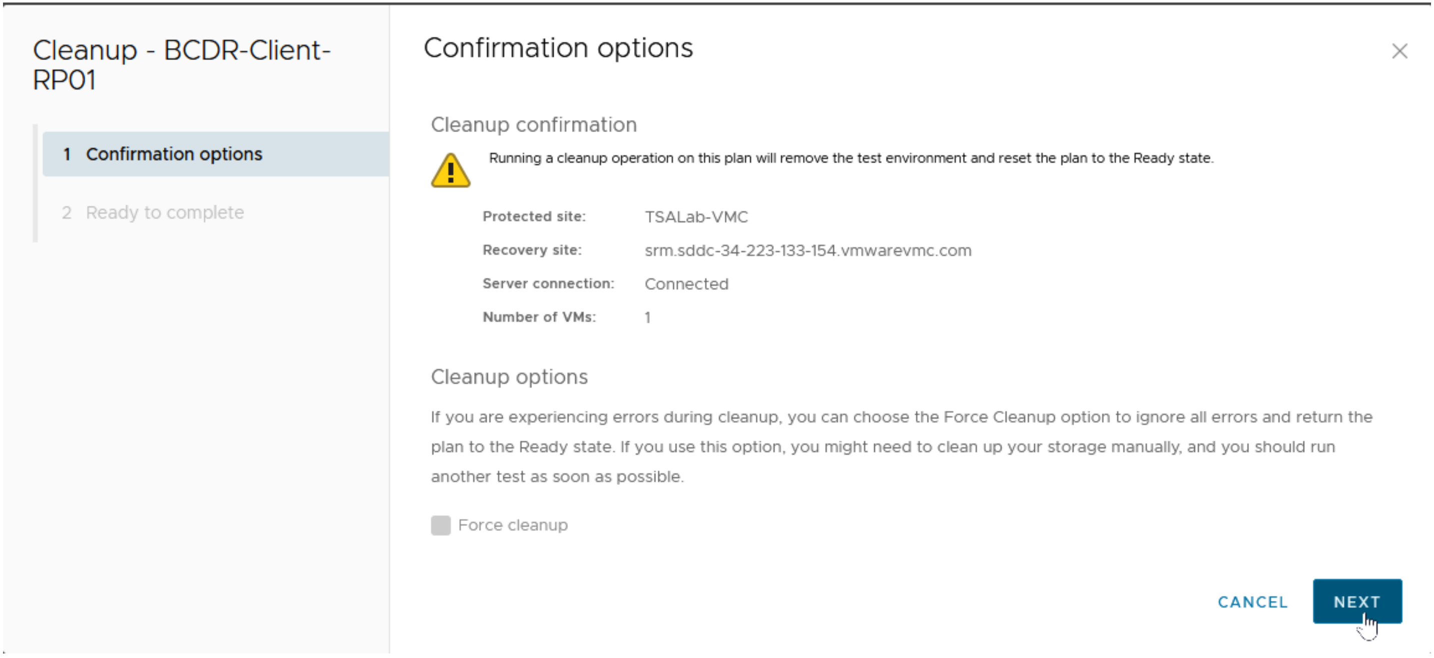
⚠ Test complete

› Plan Status

Plan Status: ✓ Test complete

The virtual machines have been recovered in a test environment at the recovery site. Review the plan history to view any errors or warnings. When you are ready to remove the test environment, run cleanup on this plan.

- Click "**Next**" to confirm that this is exactly what we want to do.



Confirmation options

Cleanup confirmation

⚠ Running a cleanup operation on this plan will remove the test environment and reset the plan to the Ready state.

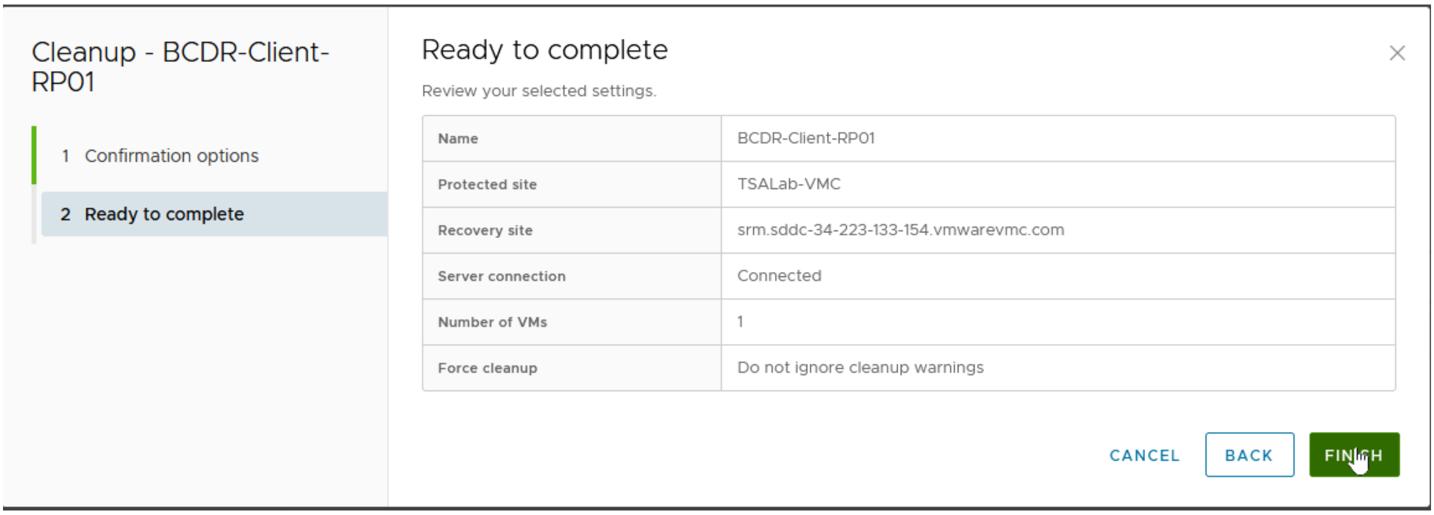
Protected site:	TSALab-VMC
Recovery site:	srm.sddc-34-223-133-154.vmwarevmc.com
Server connection:	Connected
Number of VMs:	1

Cleanup options

If you are experiencing errors during cleanup, you can choose the Force Cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you might need to clean up your storage manually, and you should run another test as soon as possible.

□ Force cleanup

- Click "**Finish**" to commit the changes.



Cleanup - BCDR-Client-RP01

1 Confirmation options

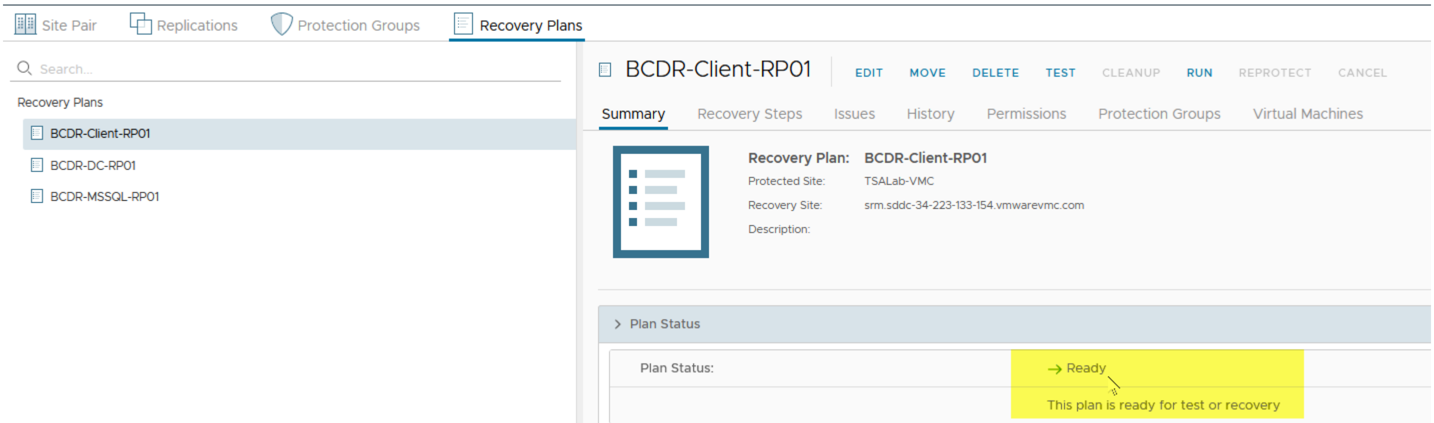
2 Ready to complete

Ready to complete

Review your selected settings.

Name	BCDR-Client-RP01
Protected site	TSALab-VMC
Recovery site	srm.sddc-34-223-133-154.vmwarevmc.com
Server connection	Connected
Number of VMs	1
Force cleanup	Do not ignore cleanup warnings

The Recovery Plans are now returned to a **"Ready"** status, for us to use for another Test or invoke in an actual disaster event.



Recovery Plans

- BCDR-Client-RP01
- BCDR-DC-RP01
- BCDR-MSSQL-RP01

BCDR-Client-RP01

Recovery Plan: BCDR-Client-RP01

Protected Site: TSALab-VMC

Recovery Site: srm.sddc-34-223-133-154.vmwarevmc.com

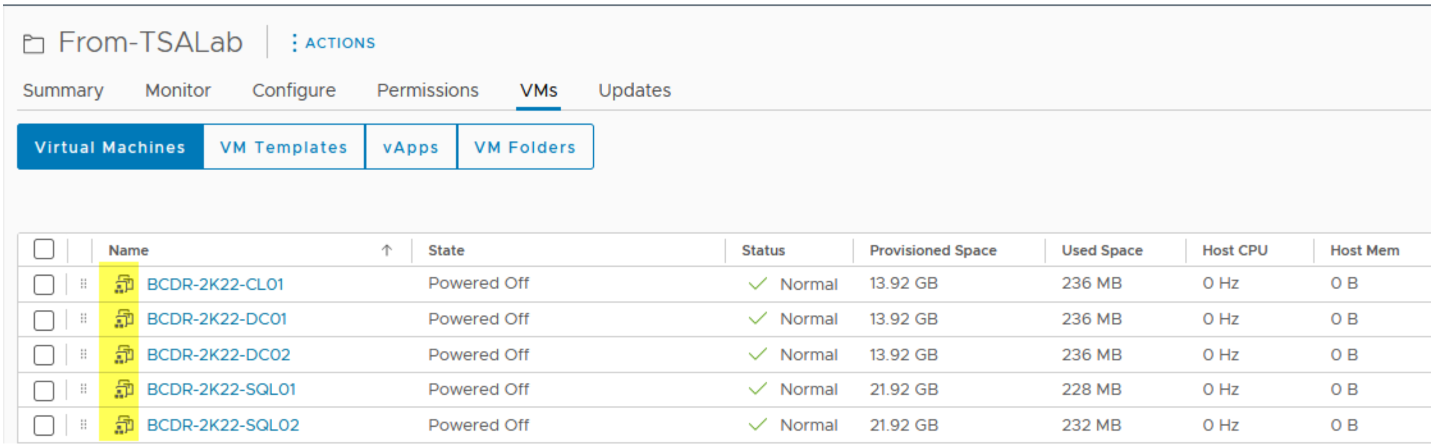
Description:

Plan Status

Plan Status: → Ready

This plan is ready for test or recovery

The Recovered VMs are now restored to their previous "Placeholder" states.



Name ↑	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
BCDR-2K22-CL01	Powered Off	✓ Normal	13.92 GB	236 MB	0 Hz	0 B
BCDR-2K22-DC01	Powered Off	✓ Normal	13.92 GB	236 MB	0 Hz	0 B
BCDR-2K22-DC02	Powered Off	✓ Normal	13.92 GB	236 MB	0 Hz	0 B
BCDR-2K22-SQL01	Powered Off	✓ Normal	21.92 GB	228 MB	0 Hz	0 B
BCDR-2K22-SQL02	Powered Off	✓ Normal	21.92 GB	232 MB	0 Hz	0 B

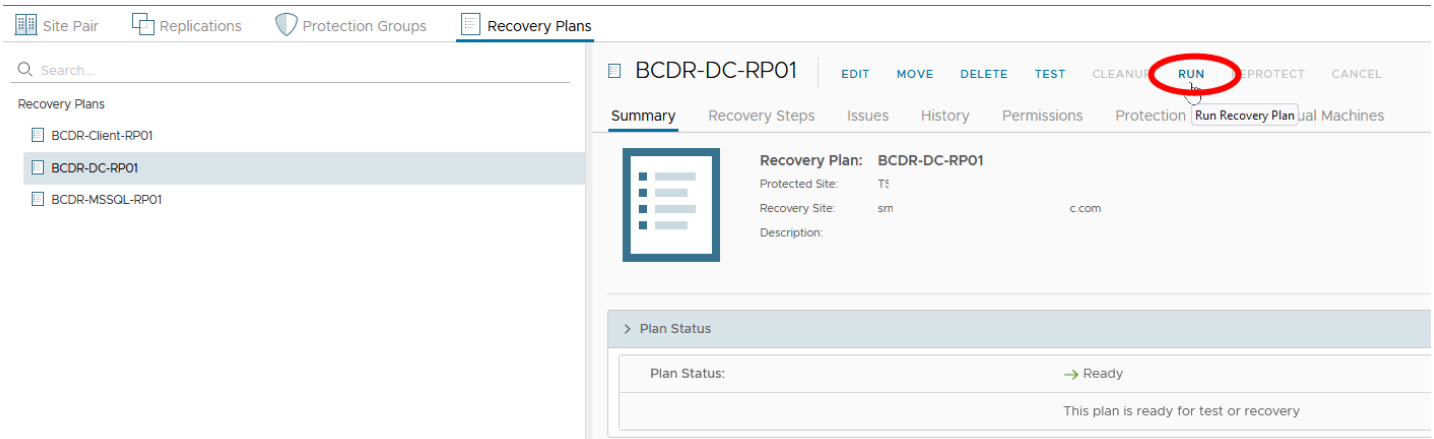
Performing a Real Disaster Recovery

Being able to perform mocked-up or simulated Disaster Recovery exercises is one of the best features of VMware Site Recovery Manager. It gives administrators a piece of mind to know that they are adequately prepared to recover their infrastructure in real disaster events, and it also helps organizations satisfy compliance, regulatory and other legal requirements. A simulated failure and recovery is not usually the desired outcome for investment in a robust BCDR Solution like SRM, though. What the Solution can do for us in a real disaster event is always the end goal. We will now demonstrate SRM's capabilities in a real disaster event.

A Disaster Event can be defined as a catastrophic event that impacts IT services in a given production environment. It implies that all servers and services located in that specific environment are unavailable and need to be re-instantiated or reinstated in another environment for business continuity.

Except for a few considerations and cosmetic differences, the process of performing real disaster recovery exercises is not much different from the process we used in the Test Disaster Recovery that we conducted above. We will highlight those differences in the following section.

- To initiate an actual **Disaster Recovery** exercise, select the **Recovery Plan**, then click **"Run".**



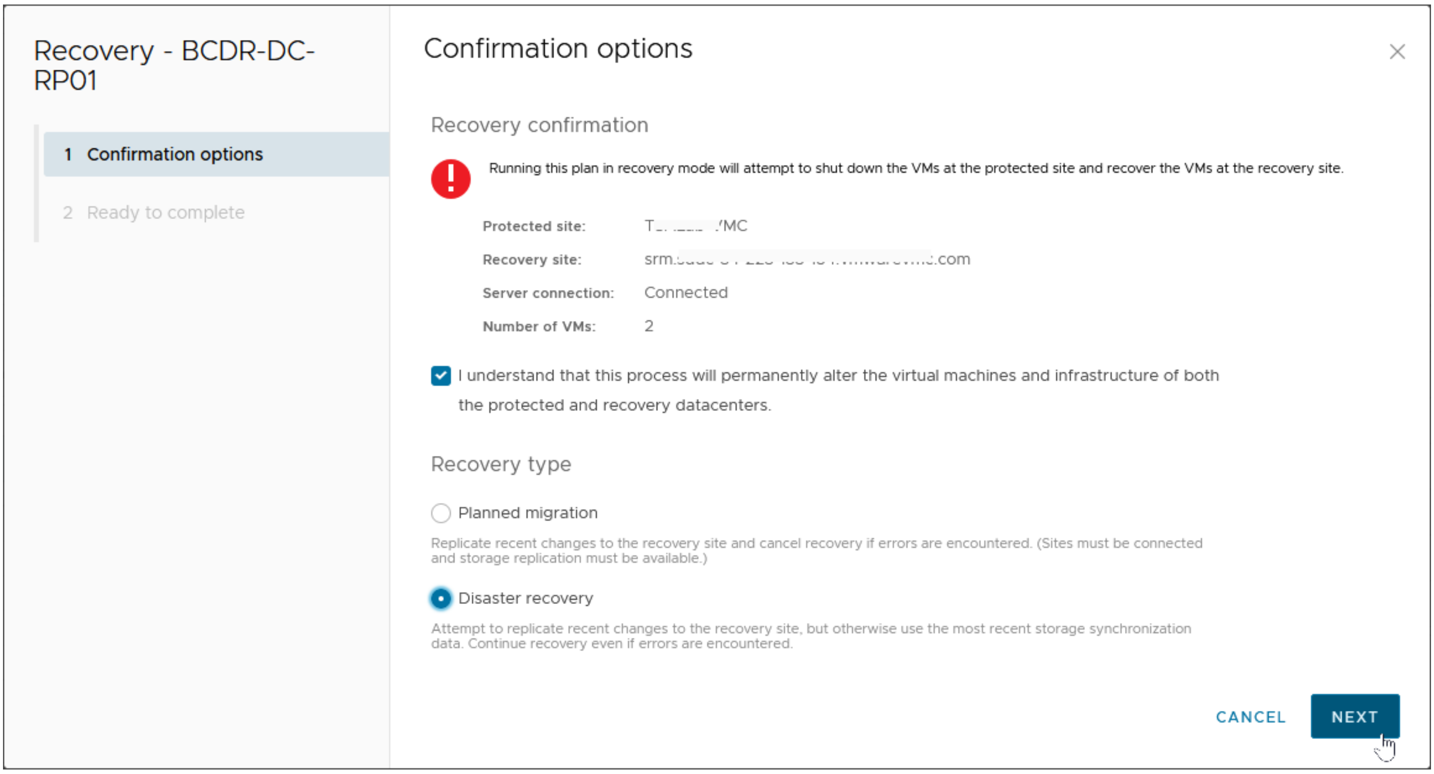
Recovery Plan: BCDR-DC-RP01
Protected Site: TS
Recovery Site: srn c.com
Description:

Plan Status: → Ready
This plan is ready for test or recovery

SRM provides two types of Disaster Recovery operations:

1. **Planned Recovery:** This is good for proactively relocating Business Critical Workloads from one datacenter to another for any business reasons. For example, if a natural disaster event is predicted for the area where the workloads are currently located, organizations can invoke their recovery plans to move them to another Site in a controlled fashion. In this mode, the Recovery operation will (among other things) perform an up-to-date synchronization between the two sites to ensure that changes in-flight are committed to the replicated copies of the workloads at the Recovery Site. The process will also attempt to power off the workloads at the Protected Site to avoid service collision. If these attempts fail, recovery will be aborted.
2. **Disaster Recovery:** This is for situations where the Workloads at the Protected Sites are no longer available. When this option is invoked, SRM makes a best-effort attempt to perform a last-minute replication and a controlled power-off of the workloads at the Protected Site. The Recovery continues even if SRM is unable to successfully perform these steps. It is assumed that when a "Disaster Recovery" is declared, there is an actual disaster event that makes the Protected Site unreachable, and the Services or Servers located there unavailable.

- Click the checkbox to acknowledge that you understand that the action you are about to perform is disruptive.
- Select **"Disaster Recovery".**
- Click **"Next".**



Recovery - BCDR-DC-RP01

1 Confirmation options

2 Ready to complete

Confirmation options

Recovery confirmation

Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

Protected site:	T[redacted]'MC
Recovery site:	srm.[redacted].com
Server connection:	Connected
Number of VMs:	2

☑ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

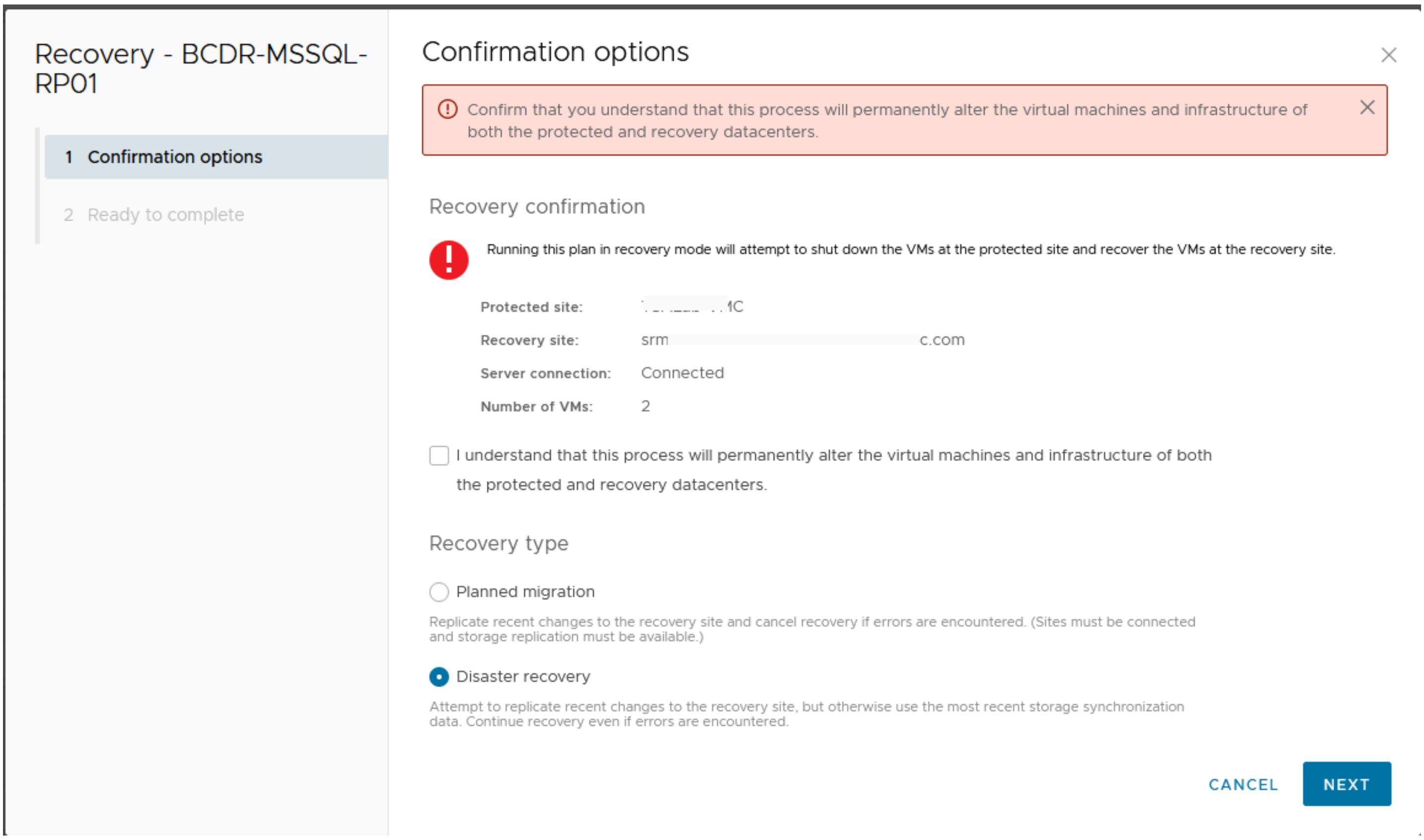
○ Planned migration

Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

● Disaster recovery

Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

SRM does not allow the invocation of a **Real Disaster Recovery** operation without a manual acknowledgement. This is to minimize the possibility of operators/administrators accidentally causing disruption in their environments.



Recovery - BCDR-MSSQL-RP01

1 Confirmation options

2 Ready to complete

Confirmation options

Confirm that you understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery confirmation

Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

Protected site:	[redacted]IC
Recovery site:	srm[redacted]c.com
Server connection:	Connected
Number of VMs:	2

□ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

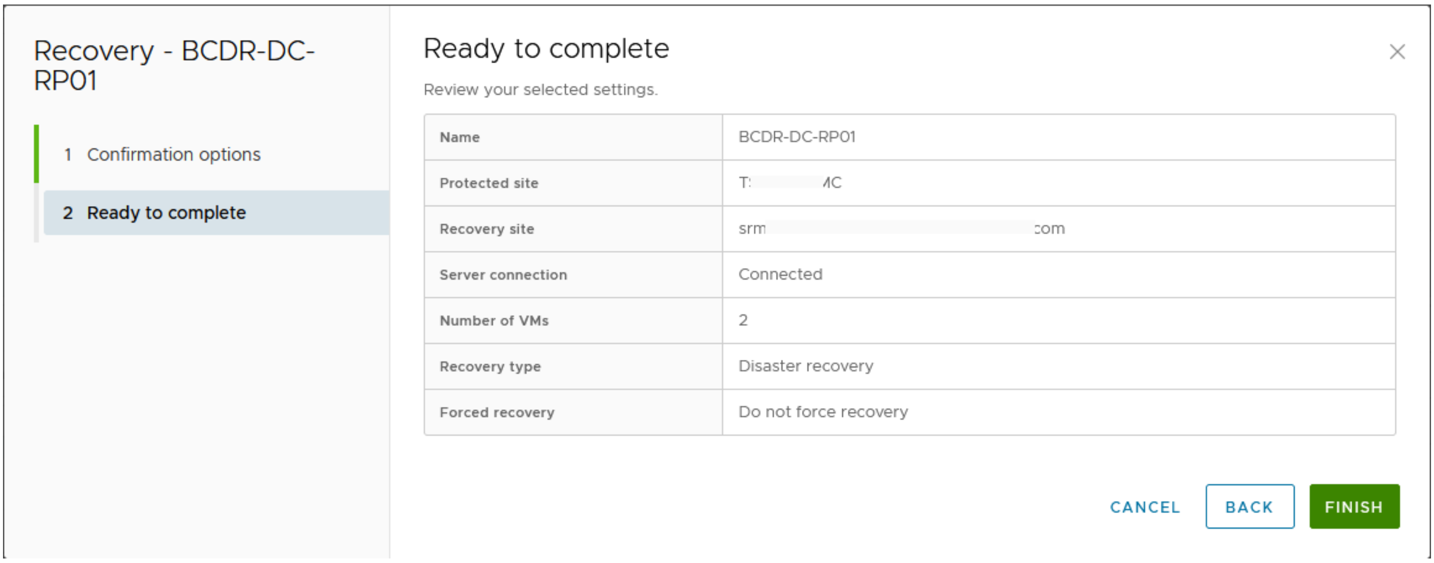
○ Planned migration

Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

● Disaster recovery

Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

- Click **"Finish"** to begin the disaster recovery.



Recovery - BCDR-DC-RP01

1 Confirmation options

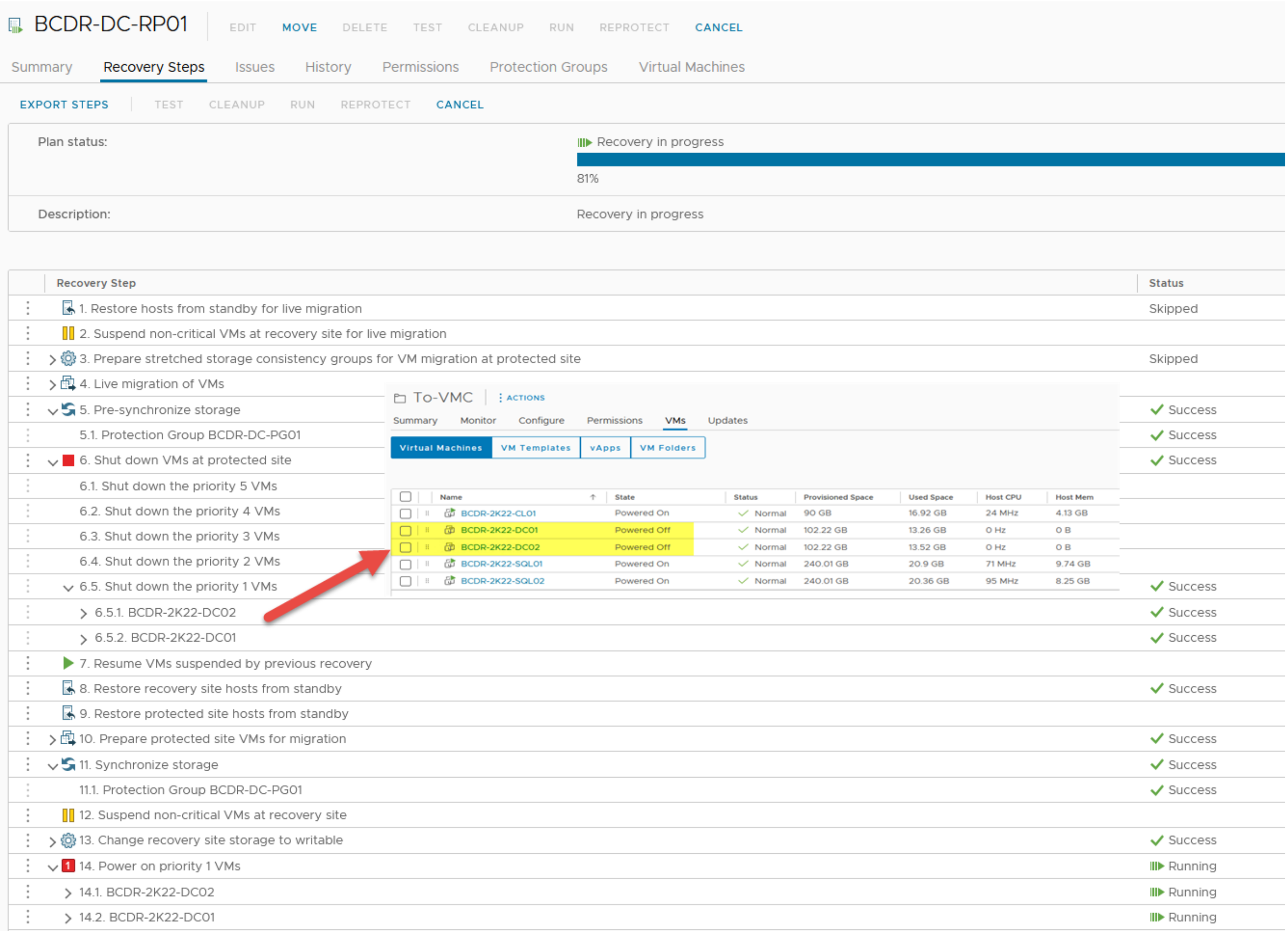
2 Ready to complete

Ready to complete

Review your selected settings.

Name	BCDR-DC-RP01
Protected site	T[redacted]/IC
Recovery site	srm[redacted]com
Server connection	Connected
Number of VMs	2
Recovery type	Disaster recovery
Forced recovery	Do not force recovery

Here, we see SRM powering off the Protected VMs at the Protected Site **before** it starts to recover them at the Recovery Site. The **Power-off** and **Synchronization** attempts succeeded in our case because our Protected Site is not really offline. If it had been, these tasks would not have succeeded, but the Recovery process would have continued regardless.



BCDR-DC-RP01

Plan status: Recovery in progress 81%

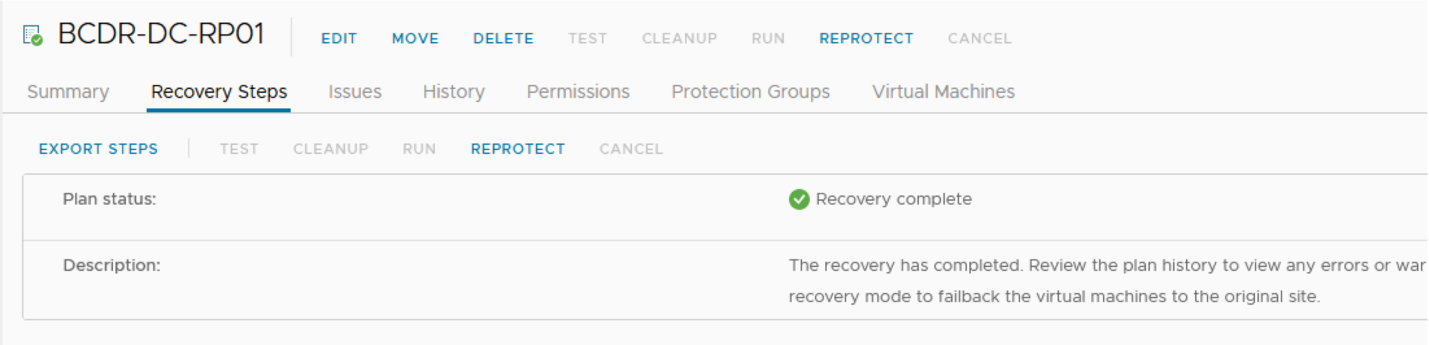
Description: Recovery in progress

Recovery Step	Status
1. Restore hosts from standby for live migration	Skipped
2. Suspend non-critical VMs at recovery site for live migration	
3. Prepare stretched storage consistency groups for VM migration at protected site	Skipped
4. Live migration of VMs	
5. Pre-synchronize storage	✓ Success
5.1. Protection Group BCDR-DC-PG01	✓ Success
6. Shut down VMs at protected site	✓ Success
6.1. Shut down the priority 5 VMs	
6.2. Shut down the priority 4 VMs	
6.3. Shut down the priority 3 VMs	
6.4. Shut down the priority 2 VMs	
6.5. Shut down the priority 1 VMs	✓ Success
6.5.1. BCDR-2K22-DC02	✓ Success
6.5.2. BCDR-2K22-DC01	✓ Success
7. Resume VMs suspended by previous recovery	
8. Restore recovery site hosts from standby	✓ Success
9. Restore protected site hosts from standby	
10. Prepare protected site VMs for migration	✓ Success
11. Synchronize storage	✓ Success
11.1. Protection Group BCDR-DC-PG01	✓ Success
12. Suspend non-critical VMs at recovery site	
13. Change recovery site storage to writable	✓ Success
14. Power on priority 1 VMs	Running
14.1. BCDR-2K22-DC02	Running
14.2. BCDR-2K22-DC01	Running

To-VMC

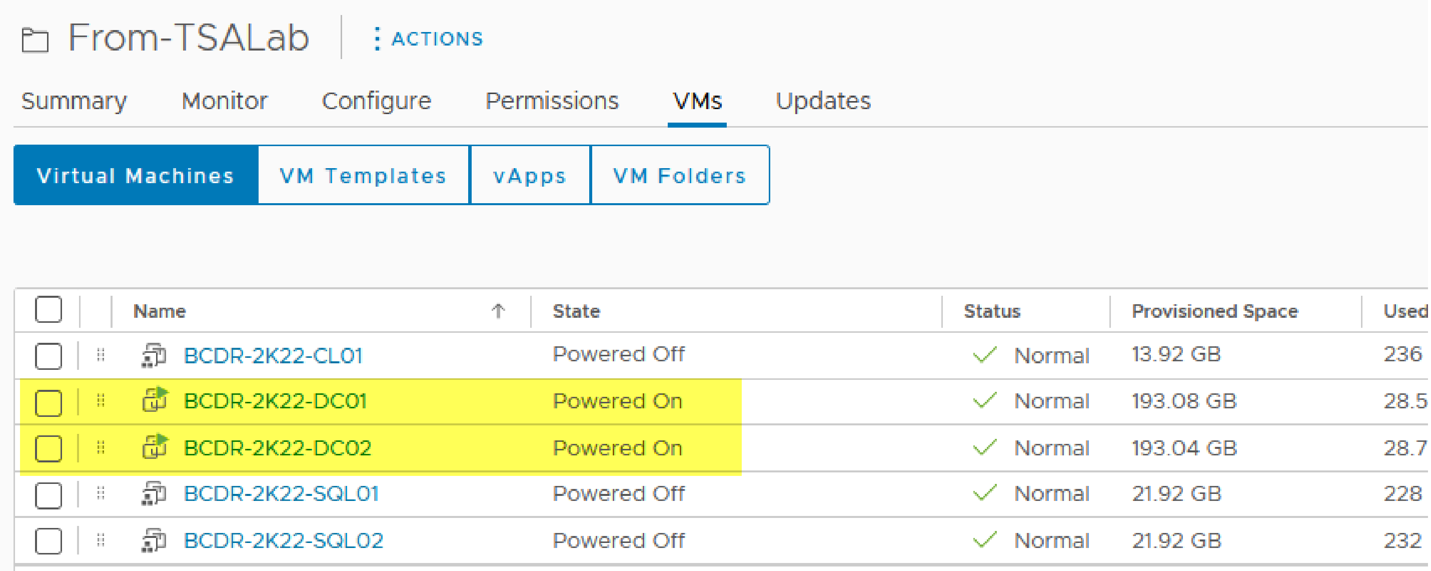
Name	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
BCDR-2K22-CL01	Powered On	✓ Normal	90 GB	16.92 GB	24 MHz	4.13 GB
BCDR-2K22-DC01	Powered Off	✓ Normal	102.22 GB	13.26 GB	0 Hz	0 B
BCDR-2K22-DC02	Powered Off	✓ Normal	102.22 GB	13.52 GB	0 Hz	0 B
BCDR-2K22-SQL01	Powered On	✓ Normal	240.01 GB	20.9 GB	71 MHz	9.74 GB
BCDR-2K22-SQL02	Powered On	✓ Normal	240.01 GB	20.36 GB	95 MHz	8.25 GB

Our Recovery was completed successfully



Plan status:	✓ Recovery complete
Description:	The recovery has completed. Review the plan history to view any errors or war recovery mode to failback the virtual machines to the original site.

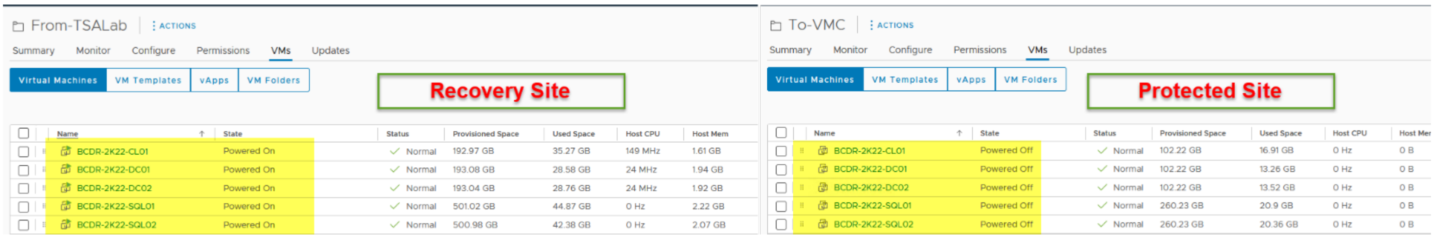
The Domain Controllers in our Recovery Plan are now running and providing services in the Recovery Site. Business Continuity is restored - with just a few mouse clicks.



	Name ↑	State	Status	Provisioned Space	Used
□	BCDR-2K22-CL01	Powered Off	✓ Normal	13.92 GB	236
□	BCDR-2K22-DC01	Powered On	✓ Normal	193.08 GB	28.5
□	BCDR-2K22-DC02	Powered On	✓ Normal	193.04 GB	28.7
□	BCDR-2K22-SQL01	Powered Off	✓ Normal	21.92 GB	228
□	BCDR-2K22-SQL02	Powered Off	✓ Normal	21.92 GB	232

We shall go ahead and invoke the rest of our Recovery Plans.

All the Workloads are now powered on at the Recovery Site and powered off at the Protected Site.

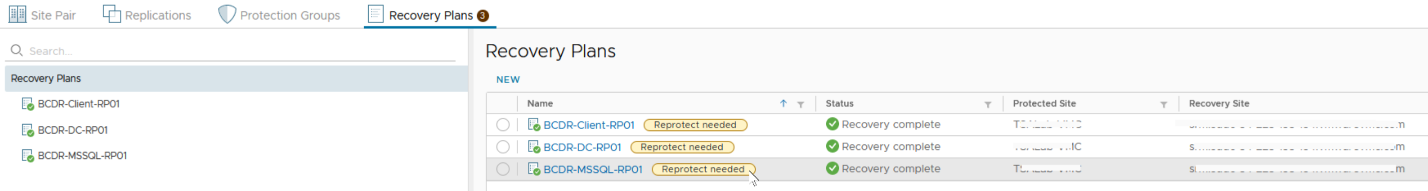


	Name ↑	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
□	BCDR-2K22-CL01	Powered On	✓ Normal	192.97 GB	35.27 GB	149 MHz	1.61 GB
□	BCDR-2K22-DC01	Powered On	✓ Normal	193.08 GB	28.58 GB	24 MHz	1.94 GB
□	BCDR-2K22-DC02	Powered On	✓ Normal	193.04 GB	28.76 GB	24 MHz	1.92 GB
□	BCDR-2K22-SQL01	Powered On	✓ Normal	501.02 GB	44.87 GB	0 Hz	2.22 GB
□	BCDR-2K22-SQL02	Powered On	✓ Normal	500.98 GB	42.38 GB	0 Hz	2.07 GB

	Name ↑	State	Status	Provisioned Space	Used Space	Host CPU	Host Mer
□	BCDR-2K22-CL01	Powered Off	✓ Normal	102.22 GB	16.91 GB	0 Hz	0 B
□	BCDR-2K22-DC01	Powered Off	✓ Normal	102.22 GB	13.26 GB	0 Hz	0 B
□	BCDR-2K22-DC02	Powered Off	✓ Normal	102.22 GB	13.52 GB	0 Hz	0 B
□	BCDR-2K22-SQL01	Powered Off	✓ Normal	260.23 GB	20.9 GB	0 Hz	0 B
□	BCDR-2K22-SQL02	Powered Off	✓ Normal	260.23 GB	20.36 GB	0 Hz	0 B

Re-protecting Business Critical Applications with SRM after a Disaster Event

Wait... what is this "Reprotect Needed" thing?

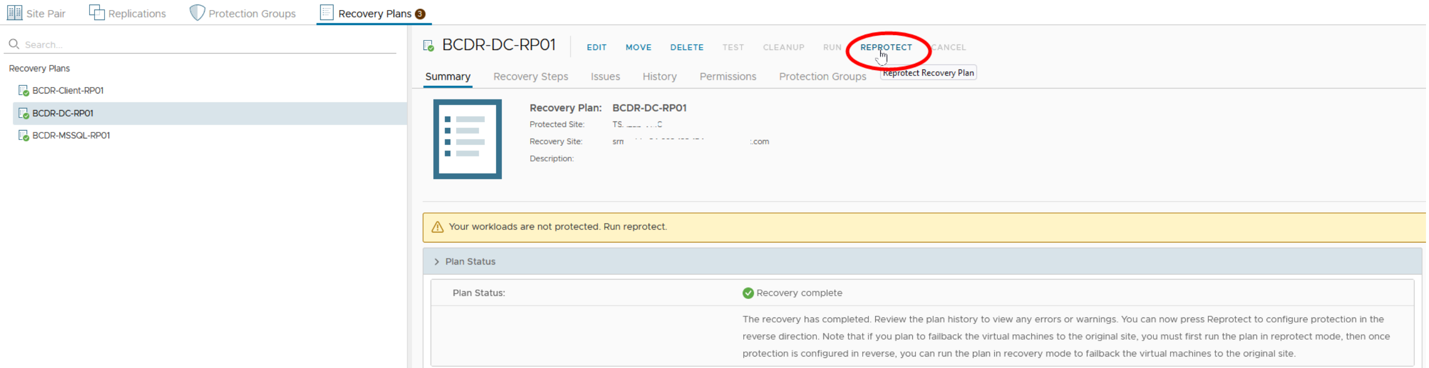


	Name ↑	Status	Protected Site	Recovery Site
○	BCDR-Client-RP01 Reprotect needed	✓ Recovery complete	[redacted]	[redacted]
○	BCDR-DC-RP01 Reprotect needed	✓ Recovery complete	[redacted]	[redacted]
○	BCDR-MSSQL-RP01 Reprotect needed	✓ Recovery complete	[redacted]	[redacted]

Disasters are disruptive, destructive, and sometimes catastrophic. Whatever their degree of severity, though, we all desire to return to normalcy once the disaster is over. For Business Continuity and Disaster Recovery, SRM provides a simplified process for organizations to achieve their return to normalcy by making it easy to quickly configure protection for the Protected workloads after a Disaster Recovery operation.

In the immediate aftermath of a real disaster event, the recovered Workloads do not have any protection (because the original Site is deemed unavailable). Once the disaster is over and the Business is ready to resume operations at that Site, a "Reprotect" operation at the "Recovery Plan" level is the way to do so in SRM.

- Select the Recovery Plan containing the Workloads you want to protect.
- Click on "Reprotect".



Recovery Plan: BCDR-DC-RP01
Protected Site: TS.[redacted]C
Recovery Site: srm[redacted].com
Description:

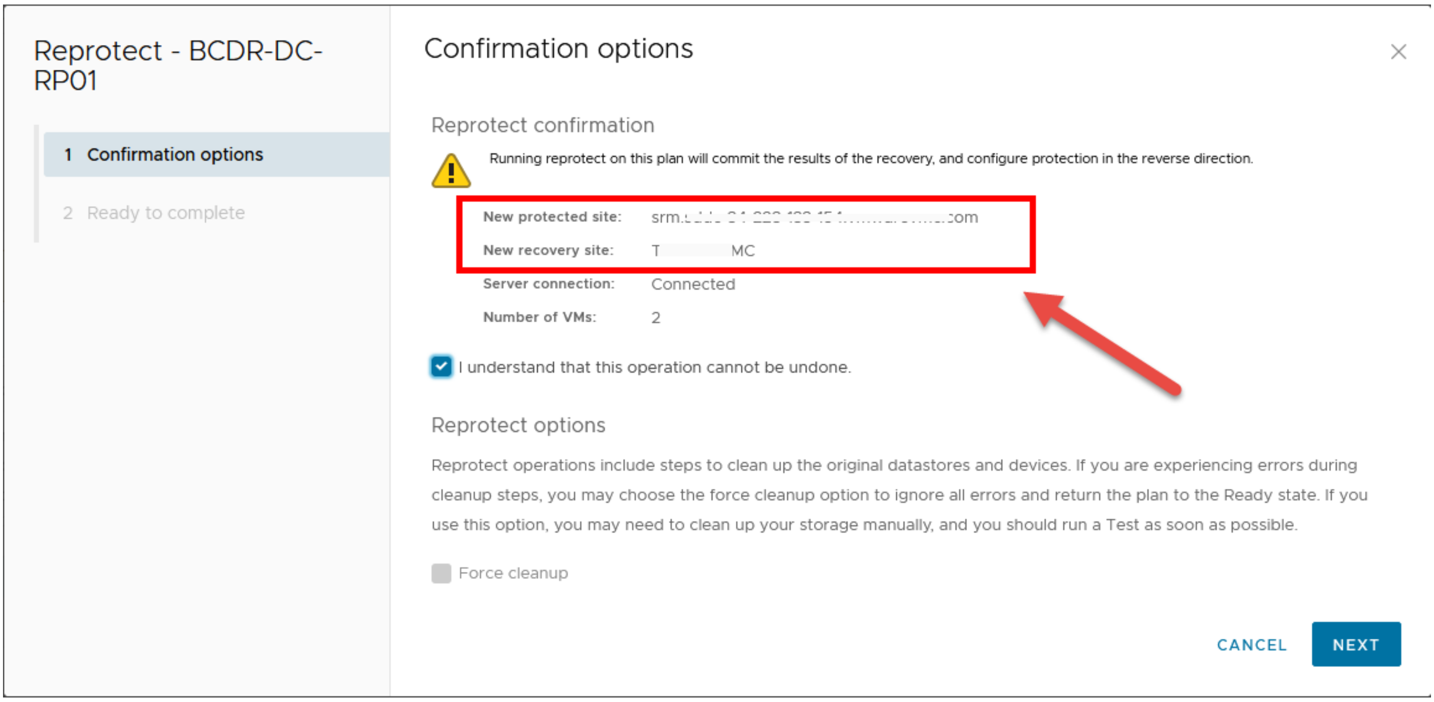
Your workloads are not protected. Run reprotect.

Plan Status: Recovery complete

The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

You will notice that the Source-Target direction has now been automatically reversed. Our original Recovery Site is now our Protected Site (and vice versa) because the Workloads are now running at the original Recovery Site.

- Click the **"I understand that this operation cannot be undone"** checkbox to signal that you understand the effects and implications of the action we are about to perform.
- Click **"Next"** and then **"Finish"** on the next screen.



Confirmation options

Reprotect confirmation

Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.

New protected site: srm.[redacted]com
New recovery site: T[redacted]MC
Server connection: Connected
Number of VMs: 2

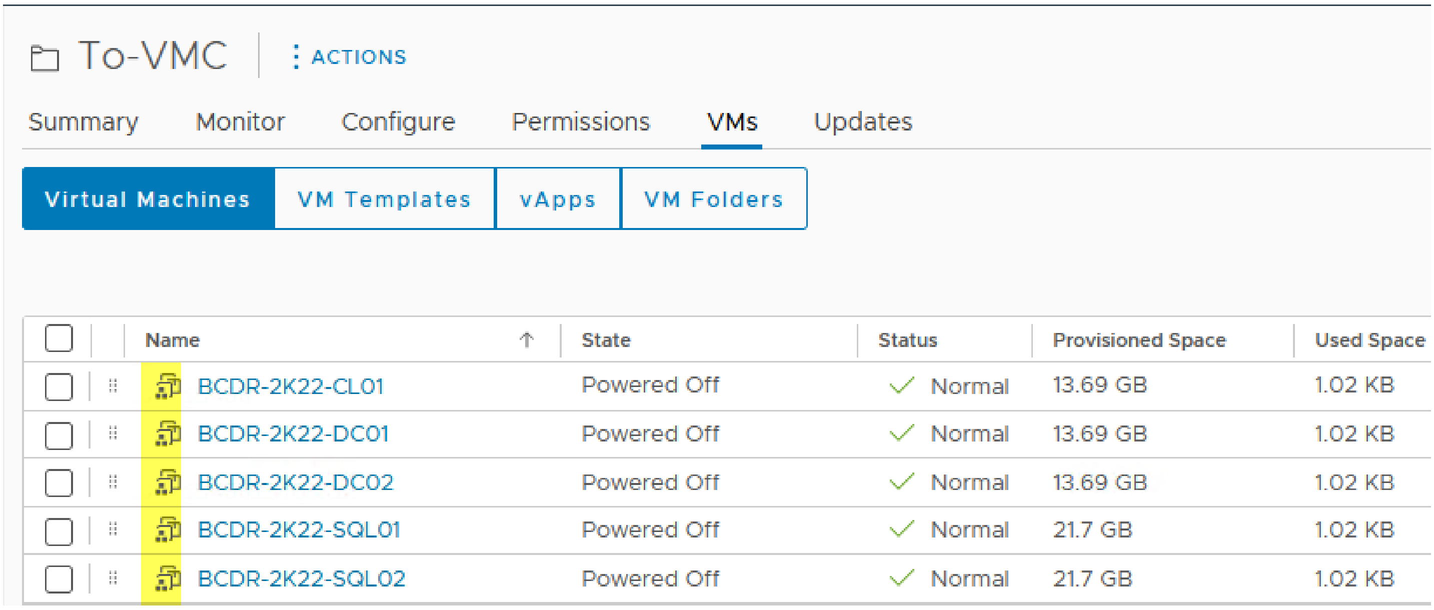
☑ I understand that this operation cannot be undone.

Reprotect options

Reprotect operations include steps to clean up the original datastores and devices. If you are experiencing errors during cleanup steps, you may choose the force cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you may need to clean up your storage manually, and you should run a Test as soon as possible.

□ Force cleanup

One of the things that happen during a **"Reprotect"** operation is that the VMs at the original **"Protected Site"** (which is now the **"Recovery Site"**) will be converted into **"Placeholders"**.



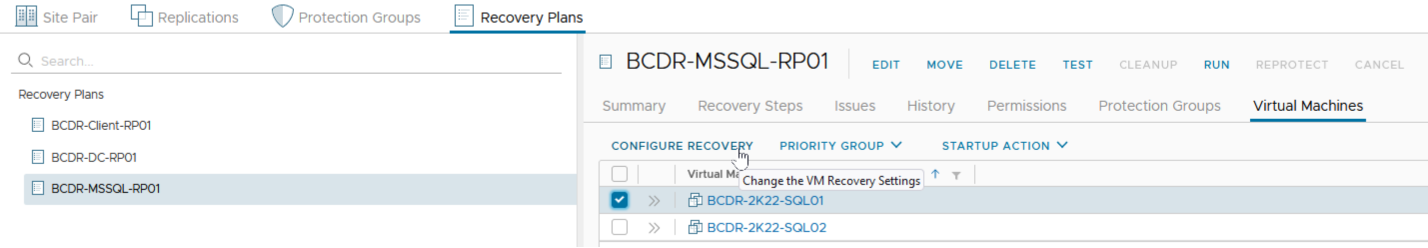
□	Name ↑	State	Status	Provisioned Space	Used Space
□	BCDR-2K22-CL01	Powered Off	✓ Normal	13.69 GB	1.02 KB
□	BCDR-2K22-DC01	Powered Off	✓ Normal	13.69 GB	1.02 KB
□	BCDR-2K22-DC02	Powered Off	✓ Normal	13.69 GB	1.02 KB
□	BCDR-2K22-SQL01	Powered Off	✓ Normal	21.7 GB	1.02 KB
□	BCDR-2K22-SQL02	Powered Off	✓ Normal	21.7 GB	1.02 KB

Considerations for in-Guest Scripts in SRM after a Disaster Recovery Operation

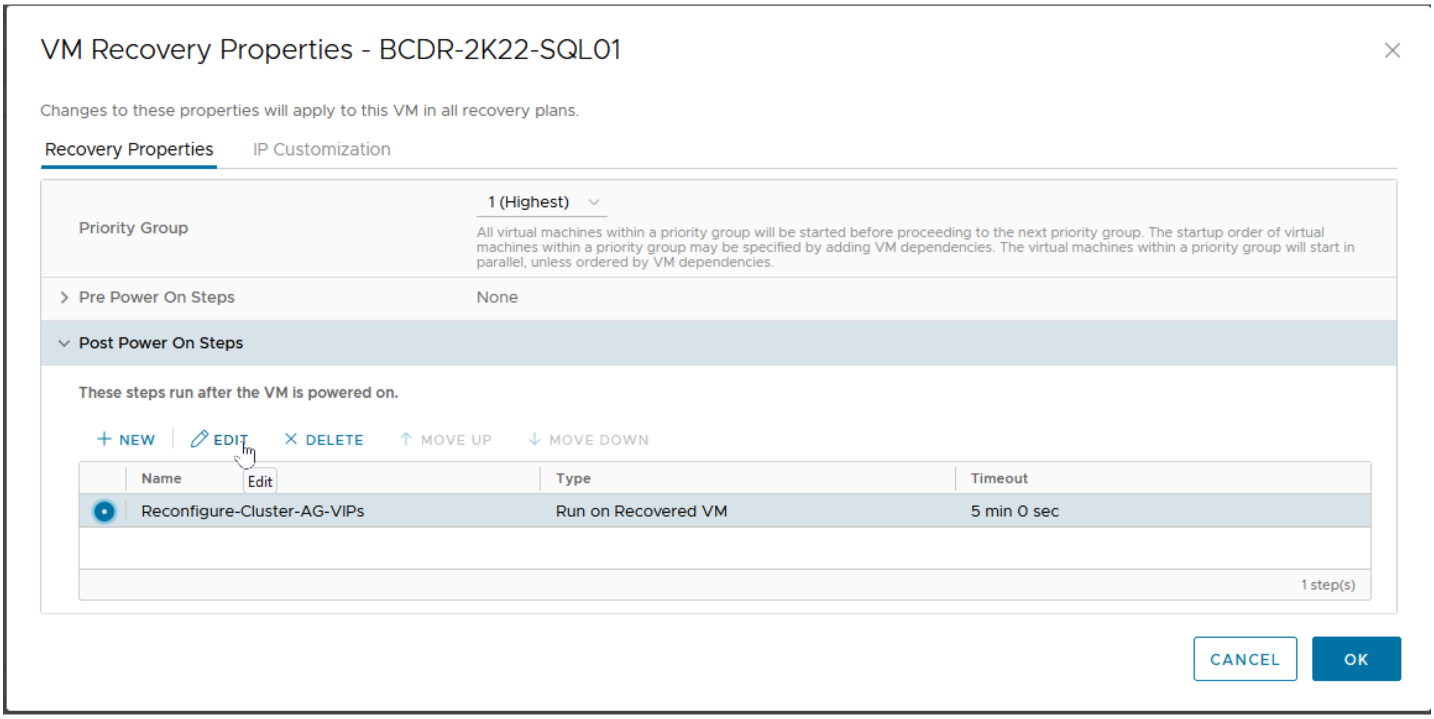
When we configured our original Recovery Plans, we configured a **"Run Command on Recovered VM"** Task in the **"Post Power on Steps"** section for the Domain Controller and Microsoft SQL Server Recovery Plans.

For the DC Recovery Plan, we were just calling a script to reboot the Domain Controller. When we reprotect this Recovery Plan, no modification is necessary for this step. The Microsoft SQL Server Recovery Plan deserves some attention because the Script needs to make site/subnet-specific configuration changes to both Windows Cluster and Microsoft SQL Server Always On. We, therefore, need to modify the original Script so that it will have the correct information if (and when) we need to initiate the DC Recovery Plan in the future. We can do this in one of two ways:

1. Now that the VM is running in the Recovery Site, we can log in and just edit the Script itself.
2. We can edit the Recovery Plan and specify a different Script to be used in the "Post Power on Steps" as we did previously. The next image shows what this looks like:
   - Select the Recovery Plan, click the **"Virtual Machines"** tab, then select the VM whose Recovery Steps we want to modify.
   - Click **"Configure Recovery".**



Select the Step to modify, then click "Edit".



VM Recovery Properties - BCDR-2K22-SQL01

Changes to these properties will apply to this VM in all recovery plans.

Priority Group: 1 (Highest)

All virtual machines within a priority group will be started before proceeding to the next priority group. The startup order of virtual machines within a priority group may be specified by adding VM dependencies. The virtual machines within a priority group will start in parallel, unless ordered by VM dependencies.

Pre Power On Steps: None

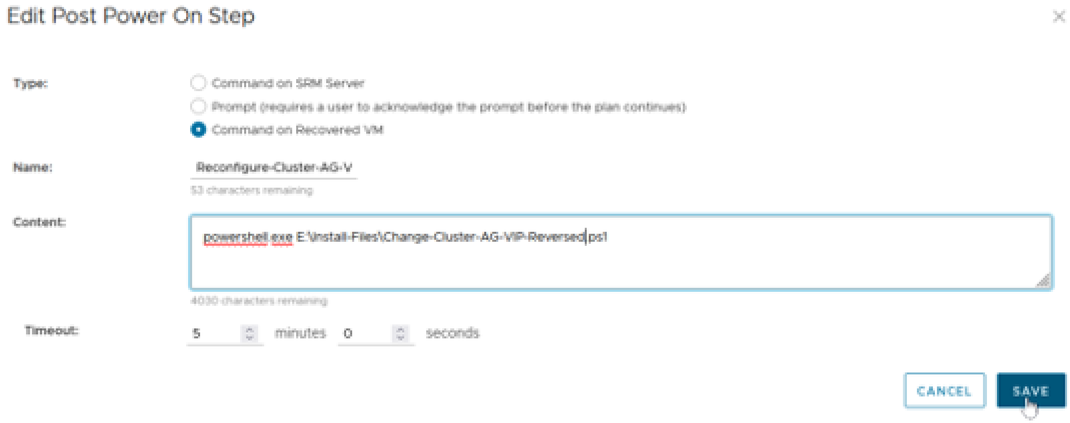
Post Power On Steps

These steps run after the VM is powered on.

	Name	Type	Timeout
●	Reconfigure-Cluster-AG-VIPs	Run on Recovered VM	5 min 0 sec

1 step(s)

- Type in the **Command** to run. In our case, we are calling another Script ***("Change-Cluster-AG-VIP-Reverse.ps1"***) which is also located in the VM.
- Click **"Save".**



Edit Post Power On Step

Type:
○ Command on SRM Server
○ Prompt (requires a user to acknowledge the prompt before the plan continues)
● Command on Recovered VM

Name: Reconfigure-Cluster-AG-V

53 characters remaining

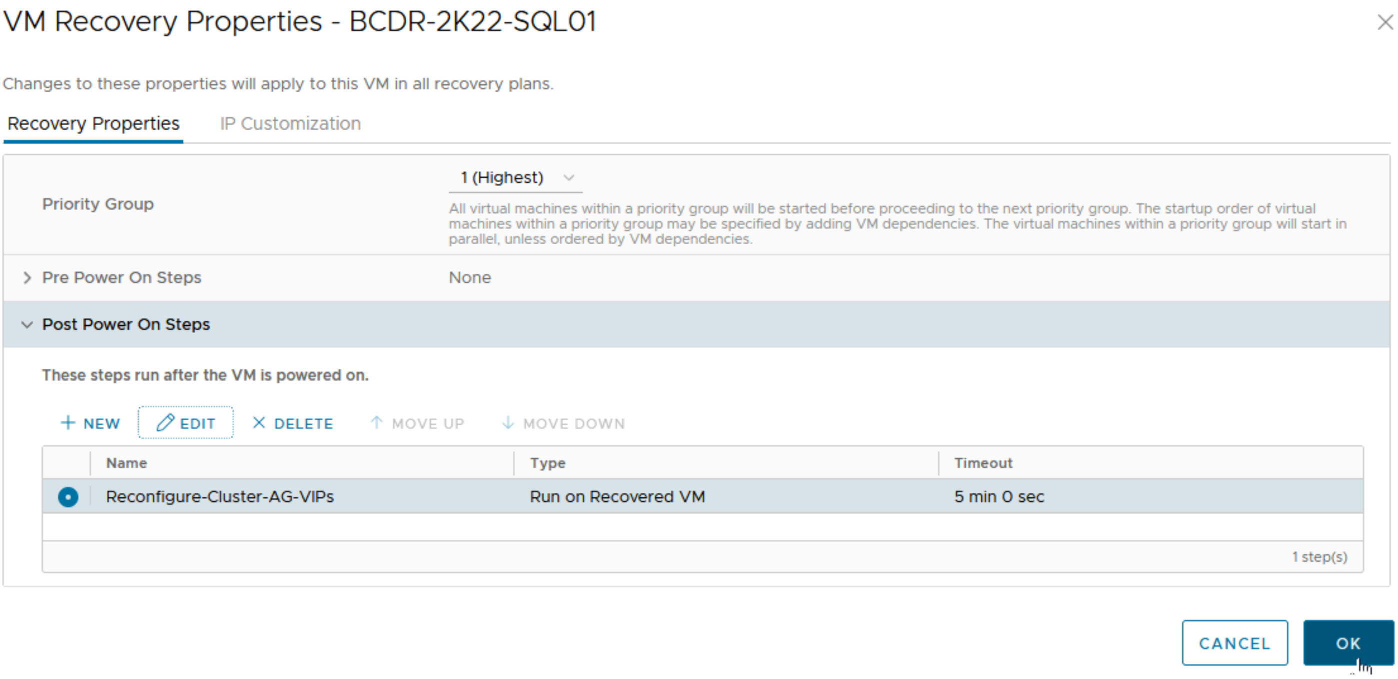
Content:

```
powershell.exe E:\Install-Files\Change-Cluster-AG-VIP-Reversed.ps1
```

4030 characters remaining

Timeout: 5 minutes 0 seconds

Click "OK" to commit the changes.



VM Recovery Properties - BCDR-2K22-SQL01

Changes to these properties will apply to this VM in all recovery plans.

Priority Group: 1 (Highest)

All virtual machines within a priority group will be started before proceeding to the next priority group. The startup order of virtual machines within a priority group may be specified by adding VM dependencies. The virtual machines within a priority group will start in parallel, unless ordered by VM dependencies.

Pre Power On Steps: None

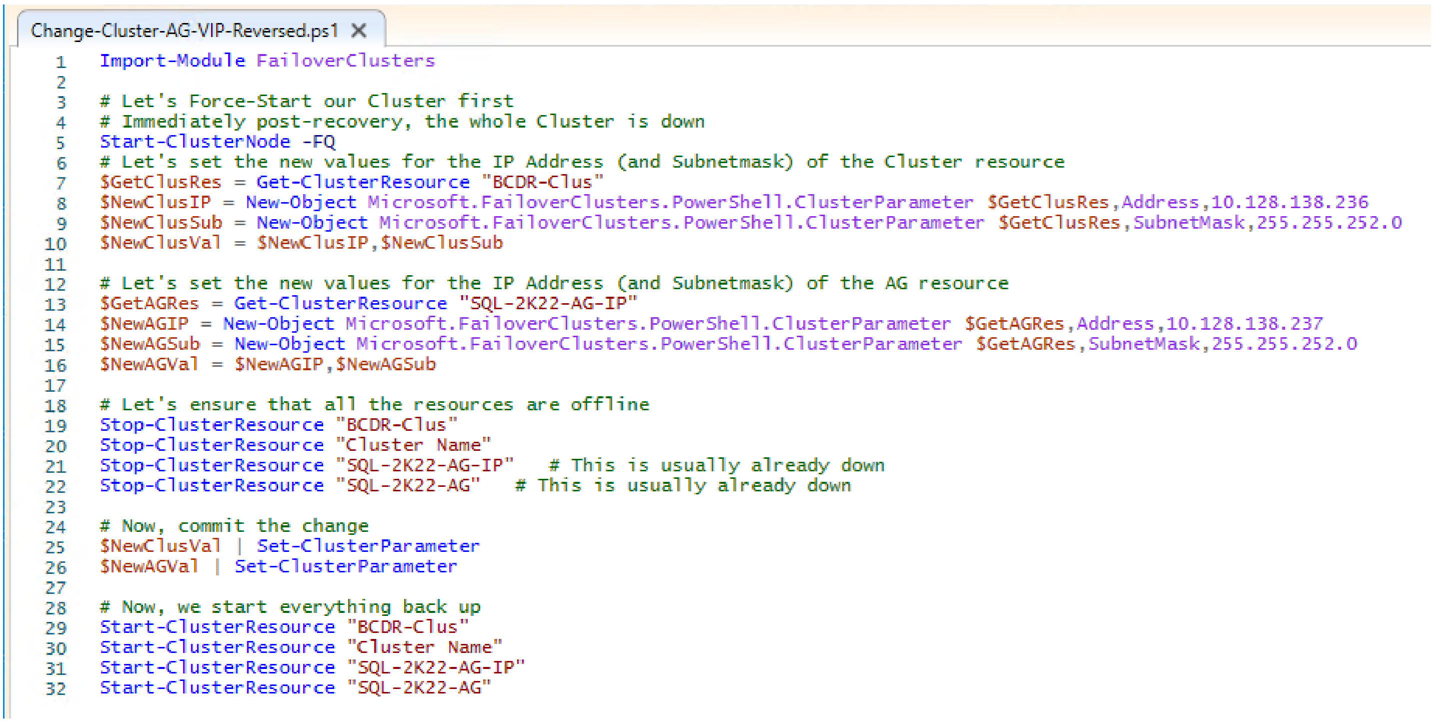
Post Power On Steps

These steps run after the VM is powered on.

	Name	Type	Timeout
●	Reconfigure-Cluster-AG-VIPs	Run on Recovered VM	5 min 0 sec

1 step(s)

For completeness, here is the script we used for this exercise. This will also be posted as an appendix to this Guide.



Change-Cluster-AG-VIP-Reversed.ps1

```
Import-Module FailoverClusters

# Let's Force-Start our Cluster first
# Immediately post-recovery, the whole Cluster is down
Start-ClusterNode -FQ
# Let's set the new values for the IP Address (and Subnetmask) of the Cluster resource
$GetClusRes = Get-ClusterResource "BCDR-Clus"
$NewClusIP = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetClusRes,Address,10.128.138.236
$NewClusSub = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetClusRes,SubnetMask,255.255.252.0
$NewClusVal = $NewClusIP,$NewClusSub

# Let's set the new values for the IP Address (and Subnetmask) of the AG resource
$GetAGRes = Get-ClusterResource "SQL-2K22-AG-IP"
$NewAGIP = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetAGRes,Address,10.128.138.237
$NewAGSub = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetAGRes,SubnetMask,255.255.252.0
$NewAGVal = $NewAGIP,$NewAGSub

# Let's ensure that all the resources are offline
Stop-ClusterResource "BCDR-Clus"
Stop-ClusterResource "Cluster Name"
Stop-ClusterResource "SQL-2K22-AG-IP"   # This is usually already down
Stop-ClusterResource "SQL-2K22-AG"   # This is usually already down

# Now, commit the change
$NewClusVal | Set-ClusterParameter
$NewAGVal | Set-ClusterParameter

# Now, we start everything back up
Start-ClusterResource "BCDR-Clus"
Start-ClusterResource "Cluster Name"
Start-ClusterResource "SQL-2K22-AG-IP"
Start-ClusterResource "SQL-2K22-AG"
```

Conclusions

We have reached the end of our demonstration of how to prepare and configure a set of virtualized Business Critical Applications workloads in a vSphere-based infrastructure to be protected against a disaster event and to be recovered with VMware Site Recovery Manager to survive the event and restore business continuity.

We showcased a multi-tiered Applications stack which requires special considerations. We covered how to use in-Guest scripting to complement the automated workflow and capabilities provided by SRM.

We demonstrated how to use SRM to conduct Test Recovery operations for compliance purposes and to verify the reliability of our BCDR plans on-demand.

We demonstrated how to use SRM to conduct a real disaster recovery operation and reconfigure the recovered workloads to be protected again after we have achieved stability.

We are providing the in-Guest Scripts used in these exercises as appendices to this Guide.

We hope that you have found this comprehensive documentation useful for your own purposes. Please use the Feedback option in this Guide to contact us if you have questions about any part of this Guide. Thank you.

References

- Installation, setup, configuration and/or administration of VMware vSphere infrastructure
- Installation, setup, configuration and/or administration of specific VMware vSphere-based Cloud infrastructure
- Installation, setup, configuration and/or administration of VMware Site Recovery Manager
- Installation, setup, configuration and/or administration of Microsoft Active Directory Domain Services or Domain Controllers
- Installation, setup, configuration and/or administration of Microsoft SQL Server, Windows Failover Cluster or Always On
- VMware vSphere Client

Sample Scripts

The following sample scripts are provided for illustration purposes only. There is no assurance, warranty or guarantee of their suitability for your purposes and usage. VMware does not provide support for these scripts. VMware disclaims any responsibility for any adverse effect that may result from your use of these sample scripts.

Run-Post-Script.ps1 (This is for simply rebooting the first DC recovered by SRM)

```
Write-Output "Rebooting VM to complete recovery..." $(Get-Date) > c:\install-files\recovery.txt
shutdown -r -t 60
```

Change-Cluster-AG-VIP.ps1 (For reconfiguring recovered MS SQL Server cluster properties)

```
Import-Module FailoverClusters
# Let's Force-Start our Cluster first
# Immediately post-recovery, the whole Cluster is down
Start-ClusterNode -FQ
# Let's set the new values for the IP Address (and Subnetmask) of the Cluster resource
$GetClusRes = Get-ClusterResource "BCDR-Clus"
$NewClusIP = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetClusRes,Address,10.72.255.236
$NewClusSub = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetClusRes,SubnetMask,255.255.255.0
$NewClusVal = $NewClusIP,$NewClusSub
# Let's set the new values for the IP Address (and Subnetmask) of the AG resource
$GetAGRes = Get-ClusterResource "SQL-2K22-AG-IP"
$NewAGIP = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetAGRes,Address,10.72.255.237
$NewAGSub = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetAGRes,SubnetMask,255.255.255.0
$NewAGVal = $NewAGIP,$NewAGSub
# Let's ensure that all the resources are offline
Stop-ClusterResource "BCDR-Clus"
Stop-ClusterResource "Cluster Name"
Stop-ClusterResource "SQL-2K22-AG-IP"   # This is usually already down
Stop-ClusterResource "SQL-2K22-AG"   # This is usually already down
# Now, commit the change
$NewClusVal | Set-ClusterParameter
$NewAGVal | Set-ClusterParameter
# Now, we start everything back up
Start-ClusterResource "BCDR-Clus"
Start-ClusterResource "Cluster Name"
Start-ClusterResource "SQL-2K22-AG-IP"
Start-ClusterResource "SQL-2K22-AG"
```

Change-Cluster-AG-VIP-Reversed.ps1 (For when the recovered MS SQL Server VM is re-protected)

```
Import-Module FailoverClusters
# Let's Force-Start our Cluster first
# Immediately post-recovery, the whole Cluster is down
Start-ClusterNode -FQ
# Let's set the new values for the IP Address (and Subnetmask) of the Cluster resource
$GetClusRes = Get-ClusterResource "BCDR-Clus"
```

```
$NewClusIP = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetClusRes,Address,10.128.138.236
$NewClusSub = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetClusRes,SubnetMask,255.255.252.0
$NewClusVal = $NewClusIP,$NewClusSub
# Let's set the new values for the IP Address (and Subnetmask) of the AG resource
$GetAGRes = Get-ClusterResource "SQL-2K22-AG-IP"
$NewAGIP = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetAGRes,Address,10.128.138.237
$NewAGSub = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetAGRes,SubnetMask,255.255.252.0
$NewAGVal = $NewAGIP,$NewAGSub

# Let's ensure that all the resources are offline
Stop-ClusterResource "BCDR-Clus"
Stop-ClusterResource "Cluster Name"
Stop-ClusterResource "SQL-2K22-AG-IP"   # This is usually already down
Stop-ClusterResource "SQL-2K22-AG"   # This is usually already down

# Now, commit the change
$NewClusVal | Set-ClusterParameter
$NewAGVal | Set-ClusterParameter

# Now, we start everything back up
Start-ClusterResource "BCDR-Clus"
Start-ClusterResource "Cluster Name"
Start-ClusterResource "SQL-2K22-AG-IP"
Start-ClusterResource "SQL-2K22-AG"
```

About the Author

Deji Akomolafe, Staff Solutions Architect in Cloud Infrastructure Business Group in VMware, wrote the original content. The following members also contributed to the doc review:

- Oleg Ulyanov, Staff Cloud Solutions Architect in VMware
- Cato Grace, Senior Technical Marketing Architect in VMware
- Christian Rauber, Staff Technical Marketing Manager in VMware
- Mark Xu, Senior Technical Marketing Manager in VMware
- Catherine Xu, Manager in the Workload Technical Marketing team in VMware