

VMware BC/DR



# **Table of contents**

Protecting and Recovering Mission-Critical Applications in a VMware Hybrid Cloud with Site Recovery Manager 3
Overview
Terminologies and Applications used in this Guide
"Cold" Recovery Site Topology
Windows Active Directory Domain Controllers 4
Microsoft SQL Server
Windows Client Machine
"High Availability" vs "Disaster Recovery" 5
Assumptions
Requirements
Setting up BCDR Environment and Workflow in VMware vSphere Site Recovery Manager
Factors Influencing our Design and Configuration Choices
Putting it all Together
RPO/RTO, Run Book, Protection Group and Recovery Plan Defined
Virtualized Domain Controller Safety Feature
Changing Recovered VM's IP Settings in SRM
SRM and Test Disaster Recovery
Safe Active Directory Domain Controllers Recovery with VMware Site Recovery Manager in Action
Recovering Microsoft SQL Server (AG) with VMware Site Recovery Manager
Cleaning up after Test Recovery
Performing a Real Disaster Recovery
Re-protecting Business Critical Applications with SRM after a Disaster Event
Considerations for in-Guest Scripts in SRM after a Disaster Recovery Operation
Conclusions
References
Sample Scripts
Run-Post-Script.ps1 (This is for simply rebooting the first DC recovered by SRM)
Change-Cluster-AG-VIP.ps1 (For reconfiguring recovered MS SQL Server cluster properties)
Change-Cluster-AG-VIP-Reversed.ps1 (For when the recovered MS SQL Server VM is re-protected)
About the Author



# 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 <u>Disaster Recovery</u> 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 (<u>Note:</u> 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 vSp	here Replication or Site Recovery Manager are displ	ayed below. If you want to see more details,	use the Open button. The Site Recover
	🗗 tsa-	Jb.local	
> vSphere Replication	Ø OK		
> Site Recovery Manager	🖉 ОК		
	OPEN Site Recover	· C	

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

	C vcenter.sd	warevmc.com			
> vSphere Replication	📀 ок				
> Site Recovery Manager	<b>О</b> К				
OPEN Site Recovery 🖸					

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".

vmw Site Recovery Menu V	
NEW SITE PAR	
Replications within the same vCenter Server	
⊕ within <u> </u>	
VIEW DETAILS	

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	Site details First site	×
1 Site details	Select a local vCenter Servers you want to pair.	
2 vCenter Server and services 3 Ready to complete	Center Server     .com	Ŧ
	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	
	CANCEL	NE

**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	vCenter Server and services	×
1 Site details	vCenter Server	Υ
2 vCenter Server and services	O 🙋 '." ' 'ocal	
3 Ready to complete		
	The following services have been identified on the vCenter Servers. Select the ones you want to pair:	w.com y .'.', ''docal y
	(1) Site Recovery Manag	T SLab
		CANCEL BACK NEXT

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.



N	ew Site Pair	Ready to complete Review your selected settings.					
	1 Site details	First site	First site				
	2 vCenter Server and services	Second site	di.,;;b.local				
	3 Ready to complete	vSphere Replication	Yes				
		Site Recovery Manager	Yes				
				CANCEL	BACK		

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

vmw Site Recovery	C	¢	?	2 ×	٢	VITIW Site Recovery	С	¢	?
NEW SITE PAIR					?	NEW SITE PAIR			
	' '.loca	al III						~~	
Site Recovery Manager  Protection Groups 0  Recovery Plans 0  vsphere Replication  Outgoing 0  Chincoming 0  VEW DETAILS ACTIONS ~						Site Recovery Manager  Protection Groups 0  Recovery Plans 0  VSphere Replication  Coutgoing 0  Chi Incoming 0  VIEW DETAILS  Actions >			
Replications within the same vCenter Server						Replications within the same vCenter Server			
€ within						E within deg ave versional local 0			
VIEW DETAILS						VIEW DETAILS			

# • Click "View Details"

vmw Site Recovery Menu ~	
NEW SITE PAIR	
	Replications within the same vCenter Server
Site Recovery Manager       Protection Groups 0         Recovery Plans 0	ⓓ within vc 1-2017-0-007 (20-07-00
vSphere Replication               Outgoing 0	
VIEW DETAILS ACTIONS ~	VIEW DETAILS

• 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 o	credentials		
vCenter Server	ts	ocal	
User name	administrator@vSphere.loca	il	
Password	•••••	Q	>
		CANCEL	LOG IN

#### 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):
  - $\circ\,$  The default storage option for VMware Clouds is vSAN
  - $\circ\,$  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	srm com RENAME		TSALab-VMC RENA	ME
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\A	dministrator
Remote SRM connection	✓ Connected		✓ Connected	
vCabero Deplication				
vsphere Replication				
Replicated VMs from vcenter.	arevmc.com:5	Replicated VMs from TSALab-VMC:0		
Name	vcentei	.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 an	evmc.com	TSA-	local
Remote VR connection VC 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.



vmw Site Recovery			
Site Pair Replications	Protection Groups 📃 Recovery Plans		
Summary	Replication Servers		
Issues		.com (the second s	]
∨ Configure	REGISTER		
Replication Servers	Replication Server	1 T Domain Name / IP	▼ Status
✓ Array Based Replication	○ □ VRS01	vrs01	Connected
Storage Replication Adapters	○ □	vrs02	Connected
Array Pairs	O 🗍	vrs03:	, 🔌 Connected
Network Mappings			
Folder Mappings			
Resource Mappings			

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

vmw Site Recovery vc.		
Site Pair Replications	Protection Groups 🔲 Recovery Plans	
Summary	Network Mappings	
lssues	vc.e.	
∨ Configure	NEW	
Replication Servers		↑ T Recovery Netwo
$\checkmark$ Array Based Replication		
Storage Replication Adapters		
Array Pairs		
Network Mappings		
Folder Mappings		
Resource Mappings		
Storage Policy Mappings		

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

#### Click "Next".

New Network Mappings	Creation mode	×
1 Creation mode	Select the way you want to create mappings.	
2 Recovery networks	The system automatically prepares mappings for networks with matching names under the selected network containers.	
3 Reverse mappings	Prepare mappings manually Manually select which exact networks to map.	
4 Test networks		
5 Ready to complete		
	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	Recovery networks	×
1 Creation mode	Configure recovery network mappings for one or m or prepared.	ore networks. The mappings for objects marked with * are already created
2 Recovery networks	Q Search	Q Search
3 Reverse mappings	> () [] TSA-70b-DC01	> C B SDDC-Datacenter
4 Test networks		
5 Ready to complete		
	(	↓ ADD MAPPINGS
	tsu-vous ab.local	Vcel.comoutc-34-220-10Vmwarevmc.com
	: 🛛 🖀 TSA-70b-DC01 > TSA-70b-vDS01 > TSA-	70b-PG 🖓 SDDC-Datacenter > vmc-hostswitch > sddc-cgw-networ
	٢	>
		1 mapping(s)
		CANCEL BACK NEXT

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

New Network Mappings	Reverse mappings	$\times$
1	Select configured mappings for which to automatically create reverse mappings. This might overwrite existing mappings.	
1 Creation mode	vcenter.sddc-34-223-133-154.vmwarevmc.com	
2 Recovery networks	☑ Am SDDC-Datacenter > vmc-hostswitch > sddc-cgw-networ Am SDDC-Datacenter > vmc-hostswitch > sddc-cgw-networ	
3 Reverse mappings		
4 Test networks		
5 Ready to complete		
	✓ 1 1 mapping(s)	
	CANCEL BACK NEXT	

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	Test networks are used instead of the recovery networks while running tests, isolated networks are automatically created and
1 Creation mode	used during tests for all networks.
2 Recovery networks	(i) 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.
3 Reverse mappings	Recovery Network 🔨 🕆 Test Network
4 Test networks	Image: SDDC-Datacenter > sddc-cgw-network-1       Image: S
5 Ready to complete	
	1 network(s)
	CANCEL BACK NEMT

Click "Finish" to proceed.

New Network Mappings	Ready to complete	g the wizard		×
1 Creation mode	tsa-	vcentei	Reverse Mapping	Test Network
2 Recovery networks	▲ TSA-70b-DC01 > TSA-70	SDDC-Datacenter > vmc	Yes	Test DR Segment
3 Reverse mappings				
4 Test networks				
5 Ready to complete				
				CANCEL BACK FINIS

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	t.c.com tsTIT_TIT_TIT_TIT_Coal
NEW EDIT DELETE CR	EATE REVERSE MAPPING
vcenter.sddc-34-223-133-154.vmw	Edit Tost Natwork Mapping
🕑 🛛 🖓 BCDR Segment	
sddc-cgw-network-1	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.	
<ul> <li>Isolated network (auto created)</li> <li>Select a specific network</li> </ul>	
Q Search         ✓ ② tsa-vcsa703-SiteA.tsalab.local         ✓ ③ TSA-70b-DC01         > 圖 TSA-70b-vDS01         ○ ④ Avi Internal         ○ ⑨ VM Network	
CANCEL	

"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		
ts <b>erver</b> blocal	vccmwarevmc.com	
Create New Folder Mapping Cal	↑ ▼ Vccwarevmc.com	Ŧ

2. Click "Next".

New Folder Mappings	Creation mode Select the way you want to create mappings.		×
1 Creation mode	• Automatically prepare mappings for folders with matching names		
2 Recovery folders	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 Reverse mappings	Mandairy serect which exact forders to map.	CANCEL	NEXT

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

New Folder Mappings	Recovery folders Configure recovery folder mappings for one or more prepared.	imes e folders. The mappings for objects marked with * are already created or
2 Recovery folders	Q Search	Q Search
3 Reverse mappings	> () III TSA-70b-DC01	<ul> <li>&gt; ○ ■ SDDC-Datacenter</li> </ul>
4 Ready to complete		↓ ADD MAPPINGS
	tstsalab.local	Y     Vcr
	:   TSA-70b-DC01 > FIOIN-VMC	SDDC-Datacenter > SRM-BCDR > From-TSALab
		2 mapping(s)
		CANCEL BACK

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



# 6. Click "Finish".

New Folder Mappings	Ready to complete Review your settings before finishing the wizard			$\times$
1 Creation mode	tsaalab.local	vcernwarevmc.com	Reverse Mapping	
2 Recovery folders	TSA-70b-DC01 > From-VMC	SDDC-Datacenter > SRM-BCDR > To-TSAL	Yes	
3 Reverse mappings	TSA-70b-DC01 > To-VMC	SDDC-Datacenter > SRM-BCDR > From-TS	Yes	
4 Ready to complete				
		CANCEL	BACK	•



- 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.

Resou	rce Mappings			
tsa-	Too oii te <mark>i</mark> salab.local	vcent		
NEW				
Creat	te New Resource Mapping	↑ ▼ V	arevmc.com	Reverse Mapping

- 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	Recovery resources	×
1 Recovery resources	Configure recovery resource mappings for one or more reso created or prepared.	urces. The mappings for objects marked with * are already
2 Reverse mappings	Q Search ✓ 健 tsa	Q Search ✓ @ vcc
3 Ready to complete	> 🔝 TSA-70b-DC01	SDDC-Datacenter
	↓ ADD	MAPPINGS
	tsa	vcc mwarevmc.com T
		1 mapping(s)
		CANCEL

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

New Resource Mappings	Reverse mappings	×	(
1 Recovery resources	Select configured mappings for which to automatically crea	te reverse mappings. This might overwrite existing mappings.	
2 Reverse mappings	SDDC-Datacenter > Cluster-1	TSA-70b-DC01 > TSA-70b-Clus01	
3 Ready to complete			
	1	1 mapping(s)	
		CANCEL BACK	

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



New Resource Mappings	Ready to complete Review your settings before finishing the wiza	ard	×
1 Recovery resources	tsa,,,,,,local	v arevmc.com	Reverse Mapping
2 Reverse mappings	TSA-70b-DC01 > TSA-70b-Clus01	SDDC-Datacenter > Cluster-1	Yes
3 Ready to complete			
		CANCEL	BACK FINISH

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				
tsa-				
NEW REMOVE				
Name	↑ T Host/Cluster			
✓ SworkloadDatastore	Cluster-1			

Here is our Placeholder Datastore at the Protected Site:

by Broadcom

Placeholder Datastores				
tsa-charles local vc i i i i i mwarevmc.com				
NEW REMOVE				
☑ Name	↑ T Host/Cluster			
SA_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".				
🛄 Site Pair	Replications Pro	tection Groups 📃 Rec	covery Plans		
Outgoing		🗗 tsa=		vcente	™mwarevmc.com
Incoming		NEW_ Virtual Machine	↑ Υ Status	Target	Replication 5
	re° © VMwar	e LLC.			Document   <b>21</b>

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	Target site ×
1 Target site 2 Virtual machines	Site name 🔁 vcent: arevmc.com
3 Target datastore	Select the vSphere Replication server that will handle the replication.  Auto-assign vSphere Replication Server  Manually select vSphere Replication Server
4 Replication settings	Name         ▼         Replications         ▼           ○         □
6 Ready to complete	
	1 replication server(s)
	CANCEL

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	Virtual machines Select the virtual machines that you want to	protect. Already replicated VMs are not sh	. www.in.this.list.
1 Target site	All Selected (5)		
2 Virtual machines	Name	↑ ⊤ Status	Ŧ
<ul><li>3 Target datastore</li><li>4 Replication settings</li><li>5 Protection group</li></ul>	:       日       BCDR-2K22-CL01         :       日       BCDR-2K22-DC01         :       日       BCDR-2K22-DC02         :       日       BCDR-2K22-SQL01         :       日       BCDR-2K22-SQL02	<ul> <li>✓ OK</li> <li>✓ OK</li> <li>✓ OK</li> <li>✓ OK</li> <li>✓ OK</li> </ul>	
			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	Target datastore Select a datastore for the replicated f	files.		Configure da	atastore per virtual machine	×
1 Target site	The selected virtual machines are using 68.62 GB. (1)					
2 Virtual machines	Disk format: Same as source VM storage policy: Datastore Defa	v	~			
3 Target datastore	Name	Λ τ	Capacity	Free	Туре	Ŧ
4. Peolication settings	O   🗐 ma-ds-52c89299-d3ee68	314-26f0-2	500 TB	500 TB	VMFS	
4 Replication settings	💿 🗐 WorkloadDatastore		137.52 TB	120.33 TB	vsan	
5 Protection group					2 datastore(	(s)
	Select seeds					
	Auto-include new disks in replicat	ion 🛈				
				CANC	EL BACK NEX	Ţ

## 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	Replication settings       ×         Configure the replication settings for the virtual machines.
1 Target site 2 Virtual machines	Recovery point objective (RPO) (1) 5 minutes 5 minutes
3 Target datastore	Enable point in time instances ()
4 Replication settings	Days 5
5 Protection group	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
6 Ready to complete	the number of instances that you want to keep.  Enable guest OS quiescing ()
	Enable network compression for VR data
	Enable encryption for VR data (i)
	CANCEL BACK NEXT

• Review the choices, then click "Finish".



Reconfigure Replication - 5 VMs	Ready to complete Review your selected settings.	×
1 Target site	Target site	vcente mwarevmc.com
2 Replication settings	Auto-replicate new disks	Enabled
3 Ready to complete	Quiescing	Disabled
	Network compression	Disabled
	Encryption	Disabled
	Recovery point objective	5 minutes
	Points in time recovery	Disabled
		CANCEL BACK FINISH

We are done with setting up the replication.

Site Pair Replications	Protection Groups	Recovery Plans	ns
Outgoing 👌			B tsa-: salab.local →      B vcenter     Vrwwarevmc.com     .vmwarevmc.com
Incoming			NEW
			Virtual Machine 🕆 T Status T RPO T Target T Replication Server
			→ BCDR-2K22-CL01 ✓ OK 5 minutes D vcent 4.vmwarevmc.com vr
			→ BCDR-2K22-DC01 ✓ OK 5 minutes In vcenter /mwarevmc.com
			→ BBCDR-2K22-DC02 ✓ OK 5 minutes 🔄 vcente
			→ BBCDR-2K22-SOL01 ✓ OK 5 minutes 🔄 vcenter
			→ BCDR-2K22-SQL02 ✓ OK 5 minutes 🗎 vcenter

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".

II Site	e Pair	Replications	Protection Groups	Recovery Plans	
Q Sea	irch				Protection Groups
Protection	on Group	s			NEW New Protection Group 1 T Protection Status



- 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	Name and direction	on	×
	All fields are required unless marke	:d (optional)	
1 Name and direction	Name		
2 Туре	Name:	68 characters remaining	
3 Datastore groups	Description: (Optional)		
4 Recovery plan			1.
5 Ready to complete	Direction:	4096 characters remaining STSALab-VMC → srm	
	Location:	Q Search Protection Groups	

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

New Protection Group	Туре	×
1 Name and direction	Select the type of protection group you want to create:  Datastore groups (array-based replication)  Protect all virtual machines which are on specific datastores.	
2 Туре	<ul> <li>Individual VMs (vSphere Replication)</li> </ul>	
3 Virtual machines	Protect spech-c virtual machines, regardless of the datastores.	
4 Recovery plan	Protect virtual machines which are on replicated vVol storage.	
5 Ready to complete	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	Virtual machines	protection group	×
1 Name and direction	All Selected (2)		
2 Туре	Virtual machine           □         Image: BCDR-2K22-CL01	↑ Ţ Status OK	T Protection Status T
3 Virtual machines	☑ ☐ BCDR-2K22-DC01	ОК	Add to this protection group
4 Recovery plan	☑         Image: BCDR-2K22-DC02           □         Image: BCDR-2K22-SQL01	<b>ок</b> ОК	Add to this protection group
5 Ready to complete	BCDR-2K22-SQL02	OK	
	2		5 VM(s)
			CANCEL BACK

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"

Recovery plan		
You can optionally add t	his protection group to a recovery plan.	
Add to existing record	wery plan	
<ul> <li>Add to new recover</li> </ul>	y plan	
<ul> <li>Do not add to recov</li> </ul>	ery plan now	
Recovery plan name:	BCDR-DC-RP01	
	68 characters remaining	
		CANCEL BACK NEXT
	Recovery plan  'tou can optionally add to  Add to existing recover  Add to new recover  Do not add to recov  Recovery plan name:	Processery plan         Interview         Interview

• Review the result, then click "Finish".



New Protection Group	Ready to complete Review your selected settings.	te s.	×
1 Name and direction	Name	BCDR-DC-PG01	
2 Туре	Description		
3 Virtual machines	Protected site	TSALab-VMC	
	Recovery site	srm.sddc varevmc.com	
4 Recovery plan	Location	Protection Groups	
5 Ready to complete	Protection group type	Individual VMs (vSphere Replication)	
	Total virtual machines	2	
	Recovery plan	BCDR-DC-RP01 (new)	
		CANCEL BACK FI	иізн

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	
NEW EDIT MOVE DELETE TEST CLEANUP RUN	
Name Edit Recovery Plan	Status
BCDR-Client-RP01	$\rightarrow$ Ready
	•
Recovery Plans	
Name Edit Recovery Plan	Status
BCDR-Client-RP01	$\rightarrow$ Ready
	•

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

Edit Recovery Plan - BCDR-Client-RP01	Test Networks Select the networks to use while running tests of this plan.					
1 Name and direction	() If "Use site-level mapping" is selected and no such mapping exists, an isolated test network will be created.					
	Recovery Network 🔨 🕆 Test Network					
2 Protection Groups	CHANGE					
3 Test Networks	CHANGE ♀ SDDC-Datacenter > cross-vpc-ls ♀ Use site-level mapping CHANGE					
4 Ready to complete	CHANGE SDDC-Datacenter > direct-connect-Is ♀ Use site-level mapping CHANGE					
	A SDDC-Datacenter > hcx-t ○ 111 0000 1. Q Use site-level mapping CHANGE					
	1 - 20 of 32 network(s)  < < 1 / 2 → >					
	CANCEL BACK NEXT					



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

III Site Pair 🕞 Replications 🖤 Protection Groups 🔲 Recovery Plans					
Q search	Protection Groups				
© BCDR-Client-PG01	Name 1 T Pro	tection Status T Recovery Statu: T	Protection Type y Protected Site	T Recovery Site	
DECDR-DC-PG01	◯   ♥ BCDR-Client-PG01 ✓	OK Ready	Individual VMs TSALab-VMC	srm.sddc	arevmc.com
	◯   ♥ BCDR-DC-PG01 ✓	OK Ready	Individual VMs TSALab-VMC	srm.sddc	. 4.vmwarevmc.com
	O BCDR-MSSQL-PG01 ✓	OK Ready	Individual VMs TSALab-VMC	srm.sddr	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**

III Site Pair 🕞 Replications 🖤 Protection Groups 📃 Recovery Plan	
Q Search	Recovery Plans
Recovery Plans	NEW 🚯
BCDR-Client-RP01	Name         ↑         ▼         Status         ▼         Protected Site         ▼         Recovery Site
BCDR-DC-RP01	□         □         BCDR-Client-RP01         → Ready         TSALab-VMC         srm.sddc         vmwarevmc.com
	□         E         BCDR-DC-RP01         → Ready         TSALab-VMC         srm.sddc-        vmwarevmc.com
	□         E         BCDR-MSSQL-RP01         → Ready         TSALab-VMC         srm.sddc         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.

Site Pair Replications	Protection Groups	Recovery Plans						
Q Search	Recovery	Plans						
Recovery Plans	NEW							
BCDR-Client-RP01	Name		↑ т	Status	Τ	Protected Site	Τ	Recovery Site
BCDR-DC-RP01		R-Client-RP01		→ Ready		TSALab-VMC		srm.sddc-34-223-133-154.vmwarevmc.com
		R-DC-RP01		$\rightarrow$ Ready		TSALab-VMC		srm.sddc-34-223-133-154.vmwarevmc.com
E BODK-MSSGE-RPUI	O   E BCD	R-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.

Site Pair Replications Pro	tection Groups	Recovery Plan	s		
Q Search	BCDR-I	DC-RP01	DIT MOVE DELETE	TEST CLEANUP	RUN REPROTECT CANCEL
Recovery Plans	Summary	Recovery Steps	Issues History Pe	ermissions Prote	ction Groups Virtual Machines
BCDR-Client-RP01					
BCDR-DC-RP01					
	Vi	rtual Machine	1 τ		
BCDR-MSSQL-RP01		BCDR-2K22-DC01			
		BCDR-2K22-DC02			

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



Site Pair Replications Pro	otection Groups Recovery Plans			
Q Search	BCDR-DC-RP01 edit move delete test cleanup run reprotect cancel			
Recovery Plans	Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines			
BCDR-Client-RP01				
BCDR-DC-RP01				
	Virtua Change the VM Recovery Settings			
BCDR-MSSQL-RPOT				
	□ 》 目 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

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

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" VM Recovery Properties BCDR-2K22-DC02

×

	1 (Highest) 🗸				
riority Group	All virtual machines w machines within a prio parallel, unless ordere	rithin a priority group will be started before p prity group may be specified by adding VM o ed by VM dependencies.	roceeding to the nex lependencies. The vi	t priority group. The start rtual machines within a pr	tup order of virtual iority group will start
M Dependencies					
View all					
elect the VMs which will be started	before this VM:			SELECT ALL	CLEAR SELECTIO
elect the VMs which will be started	before this VM:	Priority Group	Ŧ	SELECT ALL Protection Group	CLEAR SELECTIO
elect the VMs which will be started Virtual Machine BCDR-2K22-DC01	d before this VM: T V Status OK	Priority Group 1 (Highest)	Ŧ	SELECT ALL Protection Group BCDR-DC-PG01	CLEAR SELECTIO

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.

Recovery Properties IP Customiz	ation		
vMotion	Disabled (The protection group of the V	M does not support vMotion)	
> Pre Power On Steps	None		
✓ Post Power On Steps			
These steps run after the VM is powe	red on.		
+ NEW 🖉 EDIT 🛛 X DELE	re ↑ move up ↓ move down		
New	Type	Timeout	
TNEW			

- 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".



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.

covery roperties in customiz						
vMotion	Disabled (The protection group of the VM does not support vMotion)					
> Pre Power On Steps	None	None				
✓ Post Power On Steps						
These steps run after the VM is powe	ered on.					
+ NEW 🛛 🖉 EDIT 🛛 × DELET	TE ↑ MOVE UP ↓ MOVE DOWN					
+ NEW 🖉 EDIT X DELE	TE ↑ MOVE UP ↓ MOVE DOWN	Timeout				
+ NEW 2 EDIT X DELE	TE ↑ MOVE UP ↓ MOVE DOWN Type Run on Recovered VM	Timeout 5 min 0 sec				
+ NEW 2 EDIT X DELET Name Reboot-FSMO-Holder	TE ↑ MOVE UP ↓ MOVE DOWN Type Run on Recovered VM	Timeout 5 min 0 sec				
+ NEW    C EDIT × DELE Name Reboot-FSMO-Holder	TE ↑ MOVE UP ↓ MOVE DOWN Type Run on Recovered VM	Timeout 5 min 0 sec				

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

📕 🚽 🚽 install-files			_		×		
File Home Share View					~ ?-		
← → × ↑ 📙 « Local Disk (C:) > install-files v	ē	♀ Search install-files					
🕹 Downloads 🖈 ^ Name ^		Date modified	Туре	Size			
🔮 Documents 🖈 🛛 🙀 Run-Post-Script		5/17/2022 5:13 PM	Windows PowerS		1 KB		
📰 Pictures 🖈 🚽							
install-files							
🛃 Windows PowerShell ISE						—	
File Edit View Tools Debug Add-ons Help							
1 🖻 🔒 🦨 🔓 🗎 🔉 🔊 (*) 🕨 🗈		🐅 🗾 🖃 🖽	- D				
Run-Post-Script.ps1 🗙							
A Maite Output "Debetting MM to semilate account		" \$(Get-Date) > c:\i	nstall_files\reco	verv t	vt.		

#### 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 properti	s will apply to this VM in all recovery plans.	
Recovery Properties	IP Customization	
Select IP customization m	de 3	
Auto Use IP customization rule	if applicable MapperAutomatically' is set to True - Site Recovery Manager evaluates the IP subnet mapping rules during recovery to	
Manual IP customization No IP customization recovery.	ApperAutomatically' is set to False - Site Recovery Manager does not evaluate the IP subnet mapping rules during	

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.

Rec	overy Properties	IP Customization				
Seleo	t IP customization mo	de (i)				
Ma	nual IP customization	~				
_, Ĩm	IP settings - NIC 1	1				
	Protected Site:	CONFIGURE	2			
	Recovery Site:		evmc.com	CONFIGURE		
	Property			Protected Site	Recovery Site	

- 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 IPv6 DNS	WINS
IPv4 Address for Protec	ted Site
Use DHCP to obtain an IP Use the following IPv4 ad	address: 1 dress:
IPv4 Address:	10.128.138.231
Subnet Mask:	255.255.252.0
Default Gateway:	10.128.139.253
Alternate Gateway:	
RETRIEVE Retrieve the of manually.	surrent IP settings from the protected VM (requires VMware Tools and ESX 4.1 or higher). Some settings may need to be entered

• Let's repeat the process for the DNS information (we will skip IPV6 and WINS sections for

CANCEL

 $\times$ 

this exercise).

• Click "OK" to complete the configuration.

Configure Protected Site IP Settings - NIC 1

IPv4	IPv6	DNS	WINS			
DNS S	erver					
O Use	DHCP to o	obtain D ing DNS	NS address automatically			
Preferr	ed DNS Se	erver:	127.0.0.1			
Alterna	te DNS Se	rver:	10.128.138.232			

#### **DNS Suffixes**

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

	ADD
bcdr.local	REMOVE
	MOVE UP
	MOVE DOWN
2	
RETRIEVE 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

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.

	3
CANCEL	ок

- 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.

Recovery Properties IP Customization							
elect IP customization mode (							
Manual IP customization							
✓ IP settings - NIC 1							
Protected Site: CONFIGURE							
Recovery Site:	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	1C1					
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					
		CANCEL					

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

Site Pair Replications Protection Groups	
Q Search	BCDR-DC-RP01 EDIT MOVE DELETE TEST CLEANUP RUN REPROTECT CANCEL
Recovery Plans	Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines
BCDR-DC-RP01	CONFIGURE RECOVERY PRIORITY GROUP V STARTUP ACTION V
BCDR-MSSQL-RP01	Change the VM Recovery Settings         ↑ ▼           ≫         ⊕ 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	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 i parallel, unless ordered by VM dependencies.					
/M Dependencies						
View VM dependencies ~	poforo this \/M					
View VM dependencies V he following VMs will be started Virtual Machine	before this VM:	Status	Priority Group	Ţ	Protection Group	

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) – V All virtual machines within a priority group will be started before proceeding to the next priority group. The startup order of virtue exercisional view of the startup order of virtue exercision of the started before proceeding to the next priority group. The startup order of virtue exercision of virtue exe	Jal
Pre Power On Steps	None	
Post Power On Steps		
These steps run after the VM is po	ered on.	
These steps run after the VM is po + NEW ØEDIT × DEI Name	ered on. ETE ↑ MOVE UP ↓ MOVE DOWN Type Timeout	
These steps run after the VM is po + NEW Name Reconfigure-Cluster-AG-	ered on. TE ↑ MOVE UP ↓ MOVE DOWN Type Timeout IPs Run on Recovered VM 5 min 0 sec	
These steps run after the VM is po + NEW PEDIT × DE Name Reconfigure-Cluster-AG-	ered on. TE ↑ MOVE UP ↓ MOVE DOWN Type Timeout IPs Run on Recovered VM 5 min 0 sec	



 $\times$ 

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

Туре:	<ul> <li>Command on SRM Server</li> <li>Prompt (requires a user to acknowledge the prompt before the plan continues)</li> <li>Command on Recovered VM</li> </ul>	
Name:	Reconfigure-Cluster-AG-V 53 characters remaining	
Content:	powershell.exe E:\Install-Files\Change-Cluster-AG-VIP.ps1 4039 characters remaining	111.
Timeout:	5 🗘 minutes 0 🗘 seconds	

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

ſ	Change	e-Cluster-AG-VIP.ps1 🗙
	1	Import-Module FailoverClusters
	2	
	3	# Let's Force-Start our Cluster first
	4	# Immediately post-recovery, the whole Cluster is down
	5	Start-ClusterNode -FQ
	6	# Let's set the new values for the IP Address (and Subnetmask) of the Cluster resource
	7	\$GetClusRes = Get-ClusterResource "BCDR-Clus"
	8	<pre>\$NewClusIP = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter \$GetClusRes,Address,10.72.255.236</pre>
	9	<pre>SNewClusSub = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter \$GetClusRes,SubnetMask,255.255.255.0</pre>
	10	<pre>\$NewClusVal = \$NewClusIP, \$NewClusSub</pre>
	11	# Latin and the any values for the TD Address (and Schestmark) of the AC assumes
	12	# Let s set the new values for the IP Address (and Subhetmask) of the AG resource
	13	Sucreation - New Object Microsoft Epilower(Luctors PowerShall ClusterParameter (CatACPas Address 10, 72, 255, 227
	14	SNewAgir - New-Object Microsoft EsiloverClusters DowerChall Clusterer additer Statkacker Should 55,1072-053-05
	16	(Nau/G/J) = (Nau/G/J) (Nau/G/J) (Nau/G/J)
	17	ancendyal - ancendir, ancendiu
	18	# Let's ensure that all the resources are offline
	19	Stop-ClusterResource "BCDR-Clus"
	20	Stop-ClusterResource "Cluster Name"
	21	Stop-ClusterResource "SQL-2K22-AG-IP" # This is usually already down
	22	Stop-ClusterResource "SQL-2K22-AG" # This is usually already down
	23	
	24	# Now, commit the change
	25	<pre>\$NewClusVal   Set-ClusterParameter</pre>
	26	<pre>\$NewAGVa1   Set-ClusterParameter</pre>
	27	
	28	# Now, we start everything back up
	29	Start-ClusterResource "BCDR-Clus"
	30	Start-ClusterResource "Cluster Name"
	31	Start-ClusterResource "SQL-2K22-AG-IP"
	32	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".

 $\times$ 

CANCEL

SAVE

• 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.

Site Pair 4 Replications V Protections	ction Groups E Recovery Plans
Q Search Recovery Plans	BCDR-DC-RP01 EDIT MOVE DELETE TEST CLEANUP RUN REPROTECT CANCEL
BCDR-Client-RP01	
BCDR-DC-RP01	Recovery Plan: BCDR-DC-RP01
BCDR-MSSQL-RP01	Recovery Site: mc.com Description:
	> Plan Status
	Plan Status: $\rightarrow$ Ready
	This plan is ready for test or recovery

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

Test - BCDR-DC-RP01	Confirmation options >	<
<ol> <li>Confirmation options</li> <li>Ready to complete</li> </ol>	Test confirmation         Image: Second state:         Protected site:         Connected:         Server connection:         Connected:         Mumber of VMs:         2    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. Image: Protected state: Image: Protected state: Protected state: Description: Connected: Description: <	1

• Click "Finish" to begin the Test Recovery process.

Test - BCDR-DC-RP01	Ready to complete Review your selected settings.	×
1 Confirmation options	Name	BCDR-DC-RP01
2 Ready to complete	Protected site	МС
	Recovery site	mc.com
	Server connection	Connected
	Number of VMs	2
	Storage synchronization	Replicate recent changes to recovery site
		CANCEL BACK FINISH

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 R	UN 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 pl	an history to view any errors or warnings. W
Recovery Step	Status	Step Started
Sinchronize 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
5.2.6. Command: Reboot-FSMO-Holder	V Success	Thursday, June 16, 2022 5:44:55 PM
2 7. Power on priority 2 VMs		
3 8. Power on priority 3 VMs		

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



E From-TSAL Summary Monitor	ab : ACTIONS	rmissions VMs Updates					
Virtual Machines	VM Templates v	Apps VM Folders					
Name	$\uparrow$	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
BCDR-2	K22-CL01	Powered Off	V Normal	13.92 GB	236 MB	0 Hz	0 B
🗌 🗏 📅 BCDR-2	K22-DC01	Powered On	🗸 Normal	373.06 GB	32.52 GB	24 MHz	2.56 GB
🗌 🗏 📅 BCDR-2	K22-DC02	Powered On	🗸 Normal	373.01 GB	32.62 GB	24 MHz	2.53 GB
BCDR-2	K22-SQL01	Powered Off	🗸 Normal	21.92 GB	228 MB	0 Hz	0 B
BCDR-2	K22-SQL02	Powered Off	V Normal	21.92 GB	228 MB	0 Hz	O B
BCDR-2K22-DC01 Summary Monitor Confi	D 🗖 🛃 🖓 🐼 gure Permissions Dat	ACTIONS astores Networks Snapshots	計 BCDR- Summary	2K22-DC02   D C Monitor Configure Pe	n 🚅 <table-row> 🐼   ermissions Datas</table-row>	ACTIONS tores Networks	Snapshot
A Dowered On LAUNCH WEB CONSOLE LAUNCH REMOTE CONSOLE	Guest OS: Microsoft W Compatibility: ESX1 7:0 U2 VMware Tools: Running, ve MORE INFO DNS Name: bcc IP Addresses: 10.1 Host: 10.1 Managed By: VMware VC DETAILS	Indows Server 2022 (64-bit) and later (VM version 19) rsion:11365 (Current) r.local enter Site Recovery Manager Extension	D Powered O LAUNCH WEB ( LAUNCH REMO	Guest OS Compatib VMware 1 DNS Nam IP Addres Managed Adort: Managed	Microsoft Wine illiy: ESXi 7.0 U2 an fools: Running, versie MORE INFO e: bcc ses: 10.1 10.0 By: VMware vCent DETAILS	Jows Server 2022 (64 d later (VM version 19 nr.11355 (Current) Ir.local er Site Recovery Mar	I-bit) Э) Hager Extension
'he same Domain C	Controller VMs are	still running uninterrupted a	t the <b>Protect</b>	ed Site.			

🖻 To-VMC	ACTIONS							
Summary Monit	tor Configure	Permissions	VMs Up	dates				
Virtual Machines	VM Templates	vApps VI	M Folders					
Name		↑ State		Status	Provisioned Space	Used Space	Host CPU	Host Mem
	R-2K22-CL01	Powere	d On	🗸 Normal	90 GB	16.91 GB	24 MHz	3.76 GB
	R-2K22-DC01	Powere	d On	🗸 Normal	90 GB	12.6 GB	95 MHz	6 GB
🗌 🛛 🖞 🐻 🔂	2-2K22-DC02	Powere	d On	🗸 Normal	90 GB	13.52 GB	24 MHz	4.29 GB
	2-2K22-SQL01	Powere	d On	V Normal	240.01 GB	20.9 GB	407 MHz	9.32 GB
	R-2K22-SQL02	Powere	d On	🗸 Normal	240.01 GB	20.35 GB	96 MHz	7.28 GB
BCDR-2K22-DC01 Summary Monitor Config > Powered On LAUNCH WEB CONSOLE LAUNCH REMOTE CONSOLE ①	Guest OS: Compatibility: VMware Tools: DNS Name: DNS Name: None INFO DNS NAME: NA	es Networks rs Server 2022 (64-bit) ater (VM version 19) 1365 (Current) Jocal	Snapshots Updates	5	BCDR-2K22-DC02  ummary Monitor Configur  Conf	Permissions Datastore     Permissions Datastore     Wernorott Window     monabibility: ESXi 7.0 U2 and la     More INFO     NS Name: bcd     Addresses: 10.1     ost: 10.1     G    G	ACTIONS es Networks Snaj rs Server 2022 (64-bit) ter (VM version 19) 1365 (Current) 1Jocal	oshots Updates

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





#### 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.

		-									
📌 BCDR-2K22-DC01 - VMware Remote Console						📌 BCDR-2K22-DC02 - VMware Ren	note Console				
VMRC 🕶 📙 👻 🔂				» 🔒	8 🕏 0 0 A # 0 0	VMRC 🕶 📙 🖛 🛱 📋				*	- 6
Event Viewer					- ø ×	- C X iii Event Viewer					
											_
Event Viewer (Local)	Directory Service	Number of events: 598			Actions	Event Viewer (Local)	Directory Service	Number of events: 539			
> 🙀 Custom views	🐨 Filtered: Log: D	irectory Service; Levels: Critical, Error, Wa	arning; Source: . Number of events:	97	Directory Service	> Windows Logs	Piltered: Log: D	rectory Service; Levels: Critical, Error, Wa	rning; Source: . Number of events: 63		
<ul> <li>Chapfications and Services Lo Active Directory Web Ser OFS Replication OFS Replication OFS Replication Instructory Service Instructory Service Mediana Explorer Key Management Service Minagement Service Minag</li></ul>	Level Warning Warning Warning Warning Warning Warning Warning Warning Warning Warning Warning Warning Warning Warning Warning Warning Warning Warning	Date and Time 6/16/2022 54:43 PM 6/16/2022 54:43 PM 6/16/2022 54:47 PM 6/16/2022 54:47 PM 6/16/2022 54:47 PM 6/16/2022 54:47 PM 6/16/2022 54:40 PM 6/16/2022 54:38 PM 6/16/2022 54:38 PM	Source ActiveDirectory_D ActiveDirectory_D ActiveDirectory_D ActiveDirectory_D ActiveDirectory_D ActiveDirectory_D ActiveDirectory_D ActiveDirectory_D	Event ID         Task Category         Papication           2092         Replication         100           2007         DS RPC Client         2002           2001         DS RPC Client         2004           2002         Replication         2004           2003         LDAP Interface         2005           2004         Security         2007           2005         Replication         2007           2007         DS RPC Client         2007           2007         DS RPC Client         2004           2004         DAP Interface         2004	Clear Log  Clear Log  Clear Log  Clear Log  Clear Filter  Properties  Find  F	Constructions and Services Lo Cancel Directory Web Ser Cancel Directory Web Ser DFS Replication DFS Server Cancel Directory Service The Hardware Events Cancel Directory Cancel Directory OpenSSH Windows PowerShell Subscriptions	Level Warning Warning Warning Warning Warning Warning Warning Warning Warning Warning Warning Warning	Date and Time 6/16/2022 54522 PM 6/16/2022 54522 PM 6/16/2022 54522 PM 6/16/2022 54511 PM 6/16/2022 54524 PM 6/16/2022 54224 PM 6/16/2022 54228 PM 6/16/2022 54228 PM	Source ActiveDirectory, Do ActiveDirectory, Do ActiveDirectory, Do ActiveDirectory, Do ActiveDirectory, Do ActiveDirectory, Do ActiveDirectory, Do ActiveDirectory, Do ActiveDirectory, Do	Event ID Task Category 3041 LDAP Interface 2086 LDAP Interface 3055 Security 3055 Security 2087 DS RPC Client 3041 LDAP Interface 2170 Internal Configuration 3054 Security 3055 Security	
	A Warning	6/16/2022 5:42:38 PM	ActiveDirectory_D	2886 LDAP Interface	Attach a lask to this Log		Event 2170 ActiveDia	erton: DomainSensice	A storellowsteer. De		×
	A Warning	6/16/2022 5:42:28 PM	ActiveDirectory_D	2054 Security	Save Filter to Custom view		Event 2110, Activeou	ectory_bomaniservice			-
	Event 2170, ActiveDi General Details	rectory_DomainService		×	Refresh     Help		A Generation ID o	hange has been detected.			
	A Generation ID Generation ID ca 134005613917640 Generation ID cc 974655796768407 The Generation operation or afte domain controllar method to reston backup made wi	change has been detected. ched in DS (old value): 30776 30776 57634 D change occurs after the application of r a live migration operation. Active Direc • Virtualized domain controllers should re or rollback the content of an Active Direc th an Active Directory Domain Services a	a virtual machine snapshot, after a vortup Domain Services will create a not be restored using virtual mach ectory Domain Services database i were backup application.	virtual machine import new invocation ID to recover the ins aspathots. The supported to restore a system state	Event 2170, ActiveDirectory_Do		Generation ID Ca 7592823038537 Generation ID cu 159503127675378 The Generation II after a live migra Virtualized doma the content of ar Domain Services	arter in 2010 viewel; 2273 2273 2015 2 change occurs after the application of iso operation. Active Directopy Domain is controllers should not be restored usin Active Directopy Domain Services databi aware backup application.	i virtual machine snapshot, after a virtu ienvices will create a new invocation ID g virtual machine snapshots. The supp use is to restore a system state backup	al machine import operation or to recover the domain controller sorted method to restore or rollback made with an Active Directory	

• 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 - VMware Rem	iote Console				- • ×	H BCDR-2K22-DC02 - VMware Ren	note Console				
VMRC 🕶 📘 👻 📮 📋				» 📮	8 🖪 () () () () () () () () () () () () ()	VMRC ▼ 📔 ▼ 🖧 📋				» 📮	
Event Viewer					– ø ×	8 Event Viewer					
File Action View Help						File Action View Help					
🗢 🔿 🙍 🖬 📓 🖬						(+ +) 2 📅 🛛 🖬					
8 Event Viewer (Local)	Directory Service	Number of events: 598			Actions	B Event Viewer (Local)	Directory Service	Number of events: 539			
S Gustom Views     Windows Logs	Piltered: Log:	Directory Service; Levels: Critical, Error, W	/arning; Source: . Number of events	: 97	Directory Service	> Custom Views	Filtered: Log: D	irectory Service; Levels: Critical, Error, War	ming; Source: . Number of events: 63		
<ul> <li>Applications and Services Lo</li> </ul>	Level	Date and Time	Source	Event ID Task Category ^	👩 Open Saved Log	<ul> <li>Applications and Services Lo</li> </ul>	Level	Date and Time	Source	Event ID Task Category ^	
Active Directory Web Ser	Warning	6/16/2022 5:45:17 PM	ActiveDirectory_D	2092 Replication	Y Create Custom View	Active Directory Web Ser	(1) Warning	6/16/2022 5:45:22 PM	ActiveDirectory_Do	3041 LDAP Interface	
DFS Replication	Error	6/16/2022 5:44:53 PM	ActiveDirectory_D	2087 DS RPC Client	Import Custom View	DFS Replication	A Warning	6/16/2022 5:45:22 PM	ActiveDirectory_Do	2886 LDAP Interface	
DNS Service	A Warning	6/16/2022 5:44:47 PM	ActiveDirectory_D	2092 Replication	Clear Log	DIrectory service	A Warning	6/16/2022 5:45:11 PM	ActiveDirectory_Do	3054 Security	
Hardware Events	🔔 Warning	6/16/2022 5:44:17 PM	ActiveDirectory_D	3041 LDAP Interface	Tiber Connection	Hardware Events	A Warning	6/16/2022 5:45:11 PM	ActiveDirectory_Do	3051 Security	
Internet Explorer	A Warning	6/16/2022 5:44:17 PM	ActiveDirectory_D	2886 LDAP Interface	Y Pitter Current Ebg	Internet Explorer	Error	6/16/2022 5:42:43 PM	ActiveDirectory_Do	2087 DS RPC Client	
Key Management Service	A Warning	6/16/2022 5:44:07 PM	ActiveDirectory_D	3054 Security	Clear Filter	Key Management Service	A Warning	6/16/2022 5:42:39 PM	ActiveDirectory_Do	3041 LDAP Interface	
> 📫 Microsoft	A Warning	6/16/2022 5:44:07 PM	ActiveDirectory_D	3051 Security	Properties	> 📫 Microsoft	A Warning	6/16/2022 5:42:39 PM	ActiveDirectory_Do	2886 LDAP Interface	
> 🛄 OpenSSH	A Warning	6/16/2022 5:43:08 PM	ActiveDirectory_D	2092 Replication	🙀 Find	> 🎽 OpenSSH	A Warning	6/16/2022 5:42:28 PM	ActiveDirectory_Do	2170 Internal Configurati	
Windows PowerShell	Error	6/16/2022 5:42:43 PM	ActiveDirectory_D	2087 DS RPC Client	Save Filtered Log File As	Windows PowerShell	A Warning	6/16/2022 5:42:28 PM	ActiveDirectory_Do	3054 Security	
Subscriptions	A Warning	6/16/2022 5:42:38 PM	ActiveDirectory_D	3041 LDAP Interface		Subscriptions	A Warning	6/16/2022 5:42:28 PM	ActiveDirectory_Do	3051 Security	
	Warning	6/16/2022 5:42:38 PM	ActiveDirectory_D	2886 LDAP Interface	Attach a lask lo this Log			2/12/10/12/12/10/1644	A di abiadana Ba	3000 10401-0-2-0	
	A Warning	6/16/2022 5:42:28 PM	ActiveDirectory_D	21/0 Internal Configur	Save Filter to Custom View		Event 2087, ActiveDi	rectory_DomainService		*	
	Contraction	BIRAND SALAR DA	Actual bractony D	dist. Sacurity	View 🕨		General Details				
	Event 2007, ActiveD	irectory_Domainservice		^	G Refresh						
	General Details				👔 Help 🕨		Active Directory address. This err	Domain Services could not resolve the foll or prevents additions, deletions and chang	lowing DNS host name of the source of the source of the so	Iomain controller to an IP s from replicating between one	
	Active Directory	Domain Services could not resolve the f	following DNS host name of the sou	rce domain controller to an IP \land	Event 2087, ActiveDirectory_Do		or more domain	controllers in the forest. Security groups,	group policy, users and computers an resolved, potentially affecting logon a	d their passwords will be uthentication and access to	
	address. This en	ror prevents additions, deletions and char	nges in Active Directory Domain Se	rvices from replicating	Event Properties		network resourc	es.			
	between one or nasswords will b	more domain controllers in the forest. So the inconsistent between domain controll	ecurity groups, group policy, users lers until this error is resolved inster	and computers and their dially affecting logon	Attach Tack To This Fuget						
	authentication a	and access to network resources.			Autoch lask to his evenu.		body-2k22-de01	controller:			
					Lopy		Failing DNS host	name:			
	bcdr-2k22-dc0	2			Save Selected Events		efd52b36-5d57-	4e53-9fcc-373c20c22e5emsdcs.bcdr.loca	sl		
	Failing DNS hos	t name:			G Refresh		NOTE: By defaul	only up to 10 DNS failures are shown for	any given 12 hour period, even if mor	e than 10 failures occur. To lon	
	e14aa984-ccfb-	-44f0-b5e1-88fbe266c5d5msdcs.bcdr.lo	cal		12 Help		Vol. Explored and a long of the Vol. We have a set anome in the structure for the Vol. For the Vol. Here is note that not another occur. To nog all individual failure events, set the following deprecision segurity when to 1: Registry Ref. High Mosteren (Control Set Service ex NITDSD) baconstrict/22 DI SEPC Claret				
	NOTE: By defau To log all indivis	lt, only up to 10 DNS failures are shown f dual failure events, set the following diag	for any given 12 hour period, even it prostics registry value to 1:	more than 10 failures occur.							

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

H BCDR-2K22-DC01 - VMware Rem	note Console					
VMRC 🕶 📘 👻 📮					$\gg$	6
🛃 Event Viewer						
File Action View Help						
🔶 🔿 🔁 📰 🛛 🖬						
Event Viewer (Local)	Directory Service N	umber of events: 598				
> Gustom Views	Level	Date and Time	Source	Event ID	Task Category	~
> Windows Logs		6/16/2022 5:45:52 PM	ActiveDirecton/ D	1587	Replication	
Applications and Services Lo Active Directory Web Services	A Warning	6/16/2022 5:45:47 PM	ActiveDirectory D	2002	Replication	
DES Replication	A Warning	6/16/2022 5:45:47 PM	ActiveDirectory D	2092	Replication	
Directory Service		6/16/2022 5:45:23 PM	ActiveDirectory D	1304	Service Control	
DNS Server	Warning	6/16/2022 5:45:17 PM	ActiveDirectory D	2092	Replication	
Hardware Events	Error	6/16/2022 5:44:53 PM	ActiveDirectory D	2087	DS RPC Client	
Internet Explorer	Warning	6/16/2022 5:44:47 PM	ActiveDirectory D	2092	Replication	
📔 Key Management Service		6/16/2022 5:44:17 PM	ActiveDirectory D	1000	Service Control	
> 🧮 Microsoft	Warning	6/16/2022 5:44:17 PM	ActiveDirectory D	3041	LDAP Interface	
> 🛄 OpenSSH	Warning	6/16/2022 5:44:17 PM	ActiveDirectory D	2886	LDAP Interface	
Windows PowerShell	(i) Information	6/16/2022 5:44:07 PM	ActiveDirectory D	2405	Internal Configur	
📑 Subscriptions	(i) Information	6/16/2022 5:44:07 PM	ActiveDirectory D	2405	Internal Configur	
	(i) Information	6/16/2022 5:44:07 PM	ActiveDirectory D	2120	Internal Configur	
	Information	6/16/2022 5-44-07 DM	ActiveDirectory D	2172	Internal Configur	$\checkmark$
	Event 2092, ActiveDired	tory_DomainService				×
	General Dataila					
	Details					1
					^	
	This server is the ov	vner of the following FSMO role, but	does not consider it valid. For the p	artition which co	ntains the	
	errors are preventin	ig validation of this role.	y of its partners since this server ha	is been restarted.	Replication	
	Operations which r	equire contacting a FSMO operation	master will fail until this condition i	is corrected.		
	FSMO Role: CN=RI	D Manager\$,CN=System,DC=bcdr,D0	C=local			
	User Action:					
	1. Initial synchroniz	ation is the first early replications dor	ne by a system as it is starting. A fai	lure to initially sy	nchronize	
	may explain why a	FSMO role cannot be validated. This	process is explained in KB article 30	5476.	common d	
	repadmin /showren	of to display the replication partners, and r	prication is failing for all of these p prect the error in question. For exar	mple there maybe	e problems	
	with IP connectivity	, DNS name resolution, or security a	uthentication that are preventing su	uccessful replicati	on.	
	3. In the rare event	that all replication partners are expec	ted to be offline (for example, beca	use of maintenar	nce or disaster	
	recovery), you can	torce the role to be validated. This ca	n be done by using NTDSUTIL.EXE t articles 255504 and 324801 on http:	o seize the role to	off com	
	server. This may be	done daily the steps provided in Kb	and de 200004 and 024001 011 <u>intep.</u>	rapportanteros	V V	

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

	ite console					
/MRC ▼ 📕 ▼ 🖧 📋					≫ [	
Event Viewer						
- ile Action View Help						
• 🔶 🙍 📰 🚺						
Event Viewer (Local)	Directory Service N	umber of events: 598				
🛛 🛱 Custom Views	Land	Data and Taxa	Courses	Et.ID	Tel Colores	
🛛 🛍 Windows Logs	Level	Date and Time	Source	Event ID	lask Category	
Applications and Services Lo	(i) Information	6/16/2022 5:45:52 PM	ActiveDirectory_D	1587	Replication	
😭 Active Directory Web Ser	🔔 Warning	6/16/2022 5:45:47 PM	ActiveDirectory_D	2092	Replication	
DFS Replication	<u> Warning</u>	6/16/2022 5:45:47 PM	ActiveDirectory_D	2092	Replication	_
📔 Directory Service	Information	6/16/2022 5:45:23 PM	ActiveDirectory_D	1394	Service Control	
🛃 DNS Server	🛕 Warning	6/16/2022 5:45:17 PM	ActiveDirectory_D	2092	Replication	
😝 Hardware Events	🕕 Error	6/16/2022 5:44:53 PM	ActiveDirectory_D	2087	DS RPC Client	
👔 Internet Explorer	🛕 Warning	6/16/2022 5:44:47 PM	ActiveDirectory_D	2092	Replication	
📔 Key Management Service	(i) Information	6/16/2022 5:44:17 PM	ActiveDirectory_D	1000	Service Control	
> 🧮 Microsoft	A Warning	6/16/2022 5:44:17 PM	ActiveDirectory_D	3041	LDAP Interface	
> 🦰 OpenSSH	Warning	6/16/2022 5:44:17 PM	ActiveDirectory D	2886	LDAP Interface	
Windows PowerShell	(i) Information	6/16/2022 5:44:07 PM	ActiveDirectory D	2405	Internal Configur	
Subscriptions	(i) Information	6/16/2022 5:44:07 PM	ActiveDirectory D	2405	Internal Configur	
	(i) Information	6/16/2022 5:44:07 PM	ActiveDirectory D	2120	Internal Configur	
		6/16/2022 5-44-07 PM	ActiveDirectory D	2172	Internal Configur	×
Γ	Event 1394, ActiveDired	tory_DomainService				×
	General Details					
	Details					
	All problems preve	nting updates to the Active Directory	Domain Services database have bee	en cleared. New	updates to the	
	Active Directory Do	main Services database are succeedi	ng. The Net Logon service has resta	nea.		

• 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.

BCDR-2K22-DC01 - VMware Rer	note Console				- O >	< 🔰 📌 в	CDR-2K22-DC02 - VMware Rem	iote Console				
VMRC 🕶 📘 👻 🛱 🔲				» 📮	0 5 0 0 0 × 0	VMR	••    • 尋 []				>	• 📮 🕤
Event Viewer					- a ×	< 👔 Evi	ent Viewer					
File Action View Help						File	Action View Help					
(+ +) 2 🕅 🛛 🕅							) 🗶 📰 📓 📷					
Event Viewer (Local)	Directory Service	Number of events: 598			Actions	Ev	ent Viewer (Local)	Directory Service N	umber of events: 539			
> Custom Views	Level	Date and Time	Source	Event ID Task Category	Directory Service	• 25	Custom Views	Level	Date and Time	Source	Event ID Task Category	~ 6
Applications and Services Lo	A Warning	6/16/2022 5:46:16 PM	ActiveDirectory D	3054 Security	open Saved Log	- C 2	Applications and Services Lo	(i) Information	6/16/2022 6:00:22 PM	ActiveDirectory Do	3027 Garbage Collection	
Active Directory Web Ser	Warning	6/16/2022 5:46:16 PM	ActiveDirectory_D	3051 Security	Create Custom View		Active Directory Web Ser	<li>Information</li>	6/16/2022 6:00:22 PM	ActiveDirectory_Do	3033 Garbage Collection	
DFS Replication	<li>Information</li>	6/16/2022 5:46:01 PM	ActiveDirectory_D	1004 Service Control	Immed Custom View		DFS Replication	<li>Information</li>	6/16/2022 6:00:22 PM	NTDS ISAM	701 Online Defragment	.
Pirectory Service	🕕 Error	6/16/2022 5:46:01 PM	ActiveDirectory_D	1126 Global Catalog	import custom view		Directory Service	<li>Information</li>	6/16/2022 6:00:22 PM	NTDS ISAM	700 Online Defragment	.   -
DNS Server	<ol> <li>Information</li> </ol>	6/16/2022 5:45:58 PM	ActiveDirectory_D	2179 Internal Configur	Clear Log		DNS Server	<li>Information</li>	6/16/2022 6:00:22 PM	NTDS ISAM	330 General	
Hardware Events	<ol> <li>Information</li> </ol>	6/16/2022 5:45:58 PM	ActiveDirectory_D	2041 Internal Processing	Filter Current Log		Hardware Events	<ol> <li>Information</li> </ol>	6/16/2022 6:00:22 PM	NTDS ISAM	326 General	
Internet Explorer	Error	6/16/2022 5:45:56 PM	ActiveDirectory_D	1126 Global Catalog	Properties		Internet Explorer	<ol> <li>Information</li> </ol>	6/16/2022 6:00:22 PM	NTDS ISAM	330 General	6
Key Management Service	Information	6/16/2022 5:45:52 PM	ActiveDirectory_D	1999 Replication	00 Find.		Misseeft	(i) Information	6/16/2022 6:00:22 PM	NTDS ISAM	105 General	6
> OpenSSH	(1) Information	6/16/2022 5:45:52 PM	ActiveDirectory_D	1587 Replication			OpenSSH	(1) Information	6/16/2022 6:00:22 PM	NTDS ISAM	102 General	- 1 ř
Windows PowerShell	(1) Information	6/16/2022 5:45:52 PM	ActiveDirectory_D	1999 Replication	He save All Events As	- í	Windows PowerShell	Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do	1999 Replication	<b>4</b>    b
Subscriptions	(1) Information	6/16/2022 5:45:52 PM	ActiveDirectory_D	1587 Replication	Attach a Task To this Log	1	Subscriptions	(1) Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do	1587 Replication	
	(1) Information	6/16/2022 5:45:52 PM	ActiveDirectory_D	1999 Replication	View	•	· ·	(1) Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do	1999 Replication	
	Information	6/16/2022 5:45:52 PM	ActiveDirectory_D	1587 Replication	Refresh			Event 1999, ActiveDirec	tory_DomainService			×
	C		Active sectory 11	I VAN KANICSTON				General Dutails				
	Event 1999, ActiveDire	ectory_Domainservice		^	- B riep	-		Details				- L'
	General Details				Event 1999, ActiveDirectory_Do	-		The source director	service has optimized the update sequ	uence number (USN) presented by the	destination directory service.	E
					Event Properties			The source and des	ination directory services have a comm	non replication partner. The destinatio	n directory service is up to date	6
	The source directo	ory service has optimized the update se	quence number (USN) presented by	the destination directory	D Attach Task To This Event			with the common r	eplication partner, and the source direc	tory service was installed using a back	up of this partner.	
	service is up to da	e and destination directory services has te with the common replication partne	r, and the source directory service w	vas installed using a backup	Bo Conv			Destination director	y service ID:			i i
	of this partner.				Come Selected Events			efd52b36-5d57-4e5	3-9fcc-373c20c22e5e (bcdr-2k22-dc01.t	bcdr.local)		
1	Destination direct	on service ID-			Ha save selected events			904851d2-2cda-483	f-8ac4-8e4bbe2cbd0d			b
	e14aa984-ccfb-44	f0-b5e1-88fbe266c5d5 (bcdr-2k22-dc0)	2.bcdr.local)		G Refresh			Common property	USN:			3
	Common director	y service ID:			📝 Help	•		94416				
1	bbcc4ba6-e98d-4	53a-900c-dabs2/409226						Ar Service the sheares t	a datamate costar of the doctoration di	reston conice has been configured u	ith the following settings	



BCDR-2K22-DC01 - VMware Rem	iote Console				- 0	×	📌 BCDR-2K22-DC02 - VMware Ren	note Console			
VMRC 🕶 📕 👻 🛱 🔲				≫ 📮	8 😼 (C. A. A. O		VMRC 🕶 📕 👻 🛱 🔲				» 🗔
8 Event Viewer					- 0	×	Event Viewer				
File Action View Help							File Action View Help				
🗢 🏟 🖄 📰 📓 📰							🗢 🧼 🙇 📰 📓 📰				
🛃 Event Viewer (Local)	Directory Service N	umber of events: 598			Actions		🛃 Event Viewer (Local)	Directory Service N	umber of events: 539		
> Custom Views	Level	Date and Time	Source	Event ID Task Category	Directory Service		> Custom Views	Level	Date and Time	Source	Event ID Task Category
<ul> <li>Applications and Services Lo</li> </ul>	(i) Information	6/16/2022 5:45:52 PM	ActiveDirectory_D	1587 Replication	open Saved Log		Applications and Services Lo	(i) Information	6/16/2022 6:00:22 PM	ActiveDirectory_Do	3033 Garbage Collection
Active Directory Web Ser	<li>Information</li>	6/16/2022 5:45:52 PM	ActiveDirectory_D	1999 Replication	Create Custom View		Active Directory Web Ser	<li>Information</li>	6/16/2022 6:00:22 PM	NTDS ISAM	701 Online Defragment
DFS Replication	<li>Information</li>	6/16/2022 5:45:52 PM	ActiveDirectory_D	1587 Replication	i Import Curtom View		DFS Replication	(i) Information	6/16/2022 6:00:22 PM	NTDS ISAM	700 Online Defragment
Directory Service	<li>Information</li>	6/16/2022 5:45:52 PM	ActiveDirectory_D	2041 Internal Processing	and the second s		Directory Service	<li>Information</li>	6/16/2022 6:00:22 PM	NTDS ISAM	330 General
DNS Server	<ol> <li>Information</li> </ol>	6/16/2022 5:45:52 PM	ActiveDirectory_D	1999 Replication	Clear Log		DNS Server	Information	6/16/2022 6:00:22 PM	NTDS ISAM	326 General
Hardware Events	(1) Information	6/16/2022 5:45:52 PM	ActiveDirectory_D	2041 Internal Processing	Filter Current Log		Hardware Events	(1) Information	6/16/2022 6:00:22 PM	NTDS ISAM	330 General
Key Management Service	Information	6/16/2022 5:45:52 PM	ActiveDirectory_D	1587 Replication	Properties		Key Management Service	() Information	6/16/2022 6:00:22 PM	NTDS ISAM	105 General
> Microsoft	Warning	6/16/2022 5:45:47 PM	ActiveDirectory_D	2092 Replication	👭 Find		> Microsoft	Information	6/16/2022 6:00:22 PM	N IDS ISAM	102 General
> 🔛 OpenSSH	warning     Information	6/16/2022 5/45/47 PM	ActiveDirectory_D	12042 Replication	Save All Events As		> 🔛 OpenSSH	Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do	1597 Replication
Windows PowerShell	Warping	6/16/2022 5:45:17 PM	ActiveDirectory_D	2002 Replication	Attack a Task Ta this I an		Windows PowerShell	Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do	1967 Replication
Subscriptions	Error	6/16/2022 5:44:53 PM	ActiveDirectory_D	2087 DS RPC Client	Attach a lask to this bog		💮 Subscriptions	Information	6/16/2022 5:46:56 PM	ActiveDirectory Do	1587 Replication
	A Warning	6/16/2022 5:44:47 PM	ActiveDirectory D	2092 Replication	View	•		5			
	Information	6/16/2022 5-44-17 DM	ActiveDirectory D	1000 Sensice Control	Refresh			Event 1999, ActiveDirec	tory_Domainservice		*
	Event 1587, ActiveDirec	tory_DomainService		×	Help	۲		General Details			
	General Details				Event 1587, ActiveDirectory_Do.			The source director	y service has optimized the update sequ	uence number (USN) presented by the	destination directory service.
					Event Properties			The source and des	tination directory services have a comm	non replication partner. The destination	n directory service is up to date
	This directory service	e has been restored or has been confi	gured to host an application directo	ry partition. As a result, its A	Attach Task To This Event			with the common	replication partner, and the source direc	tory service was installed using a back	up of this partner.
	sequence number h	has been adjusted.	replication changes using our ordi	sentity. The starting	Copy			Destination directo	ry service ID:		
	The destination dir	ectory service corresponding to the fo	llowing object GUID has requested	changes starting at a USN	Save Selected Events			efd52b36-5d57-4e5	i3-9fcc-373c20c22e5e (bcdr-2k22-dc01.)	bcdr.local)	
	that precedes the U	Siv at which the local directory service	was restored from backup media.		Refrech			904851d2-2cda-483	8f-8ac4-8e4bbe2cbd0d		
	Object GUID: e14aa984-ccfb-44f0		hedr local)		1 Martan			Common property 94416	USN:		
	USN at the time of	restore:	(bcdr.iocal)		I Help	'					
	81928							As a result, the up-	to-dateness vector of the destination di	rectory service has been configured wi	th the following settings.
	As a result, the up-t	o-dateness vector of the destination of	lirectory service has been configure	d with the following settings.				Previous object US	N:		
	Denvirus databases (	uin.						94329 Previous property I	ISN:		
	b6cc4ba6-e98d-4e3	a-9b5c-dab327459226						94329			
	Previous object USI	4:						Database GUID: bd1e6191-492- 4-1	6.0b1a.b7c1222d1112		
	Previous property L	ISN:						Object USN:	10-9018-070122201112		
	80088			~				94416			<u>_</u>
I I I							I 1	IProperty USN:			*

• 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

VMRC 🕶 📔 👻 🛱 📋					$\gg$	<b>-</b> (
🛃 Event Viewer						
File Action View Help						
🔶 🧼 🖄 📰 🔢 🖬						
🛃 Event Viewer (Local)	Directory Service Nu	umber of events: 598				
> 📑 Custom Views	Level	Date and Time	Source	Event ID	Task Category	~
Applications and Services Lo	(i) Information	6/16/2022 5:46:16 PM	ActiveDirectory D	2406	Internal Configur	
Active Directory Web Ser	(i) Information	6/16/2022 5:46:16 PM	ActiveDirectory D	2406	Internal Configur	
DFS Replication	(i) Information	6/16/2022 5:46:16 PM	ActiveDirectory D	2121	Internal Configur	
Directory Service	A Warning	6/16/2022 5:46:16 PM	ActiveDirectory D	3054	Security	
DNS Server	Warning	6/16/2022 5:46:16 PM	ActiveDirectory_D	3051	Security	
😭 Hardware Events	(i) Information	6/16/2022 5:46:01 PM	ActiveDirectory_D	1004	Service Control	
😭 Internet Explorer	Error	6/16/2022 5:46:01 PM	ActiveDirectory_D	1126	Global Catalog	
📔 Key Management Service	Information	6/16/2022 5:45:58 PM	ActiveDirectory_D	2179	Internal Configur	
> 🔛 Microsoft	(i) Information	6/16/2022 5:45:58 PM	ActiveDirectory_D	2041	Internal Processing	-
> OpenSSH	Error	6/16/2022 5:45:56 PM	ActiveDirectory_D	1126	Global Catalog	
Windows PowerShell	(i) Information	6/16/2022 5:45:52 PM	ActiveDirectory_D	1999	Replication	
Subscriptions	<ol> <li>Information</li> </ol>	6/16/2022 5:45:52 PM	ActiveDirectory_D	1587	Replication	
	(i) Information	6/16/2022 5:45:52 PM	ActiveDirectory_D	1999	Replication	
	Information	6/16/2022 5:45:52 DM	ActiveDirectony D	1587	Replication	×
	Event 2179, ActiveDirec	tory_DomainService				×
	General Details					
	The msDS-Generation	onid attribute of the Domain Contro	lier's computer object has been set	to the following	parameter:	
	GenerationID attrib	ute:				
	97465579676840764	24				

• 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.



DCDD 2K22 DC01 VMA

BCDR-2K22-DC01 - VMware Rem	note Console				- 🗆 X	📌 BCDR-2K22-DC02 - VMware Ren	note Console			
VMRC - 📙 - 🖧 🔲				≫ 📮	S 📴 (C (B A A O O	VMRC 🕶 📘 👻 🛱 🔲				≫ 📮
Event Viewer					– 0 ×	Event Viewer				
File Action View Help						File Action View Help				
🗢 🔿 🙍 🖬 📓 📷						🗢 🤿 🙇 🚾 📓 🖬				
Event Viewer (Local)	Directory Service	Number of events: 598			Actions	Event Viewer (Local)	Directory Service	lumber of events: 539		
Generation Views     Windows Logs	Level	Date and Time	Source	Event ID Task Category ^	Directory Service	> G Custom Views	Level	Date and Time	Source	Event ID Task Category ^
Applications and Services Lo	<li>Information</li>	6/16/2022 6:01:26 PM	NTDS ISAM	326 General	👩 Open Saved Log	Applications and Services Lo	<li>Information</li>	6/16/2022 5:46:56 PM	ActiveDirectory_Do	1587 Replication
Active Directory Web Ser	<ol> <li>Information</li> </ol>	6/16/2022 6:01:26 PM	NTDS ISAM	330 General	Treate Custom View	Active Directory Web Ser	<li>Information</li>	6/16/2022 5:46:56 PM	ActiveDirectory_Do	1999 Replication
DFS Replication	(i) Information	6/16/2022 6:01:26 PM	NTDS ISAM	105 General	Import Custom View	DFS Replication	<ol> <li>Information</li> </ol>	6/16/2022 5:46:56 PM	ActiveDirectory_Do	1587 Replication
Directory Service	(1) Information	6/16/2022 6:01:26 PM	NTDS ISAM	102 General	Insport custom fremm	Directory Service	Information	6/16/2022 5:46:56 PM	ActiveDirectory_Do	1999 Replication
DNS Server	Information	6/16/2022 5:46:56 PM	ActiveDirectory_D	1394 Service Control	Clear Log	DNS Server	<ol> <li>Information</li> </ol>	6/16/2022 5:46:56 PM	ActiveDirectory_Do	1587 Replication
Hardware Events	🛕 Warning	6/16/2022 5:46:56 PM	ActiveDirectory_D	2092 Replication	Filter Current Log	Hardware Events	Information		ActiveDirectory_Do	1394 Service Control
😭 Internet Explorer	(i) Information	6/16/2022 5:46:26 PM	ActiveDirectory_D	1000 Service Control	Properties	Internet Explorer	<ol> <li>Information</li> </ol>	6/16/2022 5:45:22 PM	ActiveDirectory_Do	1000 Service Control
Key Management Service	🛕 Warning	6/16/2022 5:46:26 PM	ActiveDirectory_D	3041 LDAP Interface	00.004	Key Management Service	🔥 Warning	6/16/2022 5:45:22 PM	ActiveDirectory_Do	3041 LDAP Interface
> Microsoft	🔔 Warning	6/16/2022 5:46:26 PM	ActiveDirectory_D	2886 LDAP Interface	lege rind	> Microsoft	A Warning	6/16/2022 5:45:22 PM	ActiveDirectory_Do	2886 LDAP Interface
> OpenSSH	(i) Information	6/16/2022 5:46:16 PM	ActiveDirectory_D	2405 Internal Configur	Save All Events As	> OpenSSH	<ol> <li>Information</li> </ol>	6/16/2022 5:45:12 PM	ActiveDirectory_Do	2405 Internal Configurati
Windows PowerShell	(i) Information	6/16/2022 5:46:16 PM	ActiveDirectory_D	2405 Internal Configur	Attach a Task To this Log	Windows PowerShell	Information	6/16/2022 5:45:12 PM	ActiveDirectory_Do	2405 Internal Configurati
5ubscriptions	(1) Information	6/16/2022 5:46:16 PM	ActiveDirectory_D	2120 Internal Configur	View	Subscriptions	(i) Information	6/16/2022 5:45:12 PM	ActiveDirectory_Do	2120 Internal Configurati Y
	<ol> <li>Information</li> </ol>	6/16/2022 5:46:16 PM	ActiveDirectory_D	2172 Internal Configur			Event 1204 ActiveDire	stony DomaioSensise		v
	Information	6/16/2022 5-46-16 DM	ActiveDirectory D	2168 Internal Configur	G Refresh		Event 1354, ActiveDire	ctory_bomainservice		^
	Event 1394, ActiveDire	ectory_DomainService		×	🛛 Help 🕨 🕨		General Details			
	General Details				Event 1394, ActiveDirectory_Do 🔺		All problems prev	nting updates to the Active Directory D	omain Services database have been cl	eared. New updates to the Active
	The second				Event Properties		Directory Domain	Services database are succeeding. The N	let Logon service has restarted.	
	All problems prev Active Directory D	enting updates to the Active Directory Iomain Services database are succeedir	Domain Services database have be ng. The Net Logon service has resta	in cleared. New updates to the ted.	Attach Task To This Event					
					Ba Copy 🔸	I				

#### 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 EDIT MOVE DELETE	TEST CLEANUP RUN REPROTECT CANCEL				Learn
Communication Communications	Destanting General Mathematican				
summary Recovery steps issues History Permissions	s Protection Groups Vintual Machines				
EXPORT STEPS   TEST CLEANUP RUN REPROTECT CAN	NCEL				
Plan status	Test in progress.				
	A construction of the state				
	96%				
Description:	A test of this plan is currently in progress.				
				View Tax	
(					
Necovery scep		status	step started	Step Compreses	
: > Call. Synchronize scorage		♥ success	Trunsday, June 16, 2022 9:42:57 PM	Thorsday, June 16, 2022 0.4257 PM	
2. Nestore recovery site hosts from standby		✓ success	Thursday, June 10, 2022 3042:57 PM	Thursday, June 10, 2022 9/12/37 PM	
3. Suspend non-critical VMs at recovery site					
: V@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-MSSGL-PS01		✓ Success	Thursday, June 16, 2022 9:42:57 PM	Thursday, June 16, 2022 9:42:57 PM	
4.2. BCDR-2K22-SOL01		✓ 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-SOL02		✓ 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	
v@ 5. Configure test networks		✓ Success	Thursday, June 16, 2022 9:43:05 PM	Thursday, June 16, 2022 9:43:06 PM	
5.1. BCDP-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		III Running	Thursday, June 16, 2022 9:42:05 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 9:42:58 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-VPs		✓ Success	Thursday, June 16, 2022 9:44:58 PM	Thursday, June 16, 2022 9.45:20 PM	
v 6.2. BCDR-2K22-SQL02		IP Running	Thursday, June 16, 2022 9:43:05 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		III Running	Thursday, June 16, 2022 9:45:24 PM		

Recovery done

BCDR-MSSQL-RP01 edit move delete test cleanup run reprotect cancel								
iummary 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 pla	n history to view any errors or warnings. \					
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					
5. Power on priority 1 VMs		✓ Success	Thursday, June 16, 2022 9:43:06 PM					
: 57 Dower on priority 2 VMe								



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

📲 Failover Cluster Manager							
File Action View Help							
							-
Billover Cluster Manager	B-1 (4)						
V BCDR-Clus.bcdr.local	Roles (1)					-	
Roles	Search						
Nodes	Name	Status	Туре	Owner Node	Priority	Information	
> Contrage	SQL-2K22-AG	(1) Running	Other	bcdr-2k22-sql01	Medium		
Cluster Events							
	<						
	V SQL-2K22-AG					ſ	P
	Name			Status	Information		
	Other Resources						
	SQL-2K22-AG			🕥 Online			
	Server Name						
	🖃 📑 Name: BCDR-List			🕥 Online			
	📑 IP Address: 10.	:37		🕥 Online			
Bailover Cluster Manager							
File Action View Help							
Hailover Cluster Manager	Nodes (2)						
BCDR-Clus.bcdr.local     Boles	Search						P
Nodes	Name			Status As	signed Vote	Current Vote	_
> <u>[</u> Storage	bcdr-2k22-sql01			🕥 Up 1		1	
Networks	bcdr-2k22-sql02			🕥 Up 1		1	
Eluster Events							
	<						
	v bcdr-2k22-sql	01					
	Name	Status	Туре	Priority	Information		
	🕞 SQL-2K22-AG	Running	Other	Medium			
1	101						

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



🛃 Microsoft SQL S	erver Management Studio		
File Edit View	Tools Window Help		
G - O 🏠 - 1	🗄 👻 🏭 🔐 📳 New Qu	ery 🗈 🛱 🕅 🕅 XNLA 🗛 🕹 🕹 🗂	ツ - ペ -   🔗   🏓
8 <b># \%</b>	- 🕨 Exec	ute 🔳 🗸 👯 🗐 🗐 🔡 👫 👘	a 🖩 🗅 🗏 🦉 🚝 🔁 👘
Object Explorer		<b>▼</b> ₽ ×	
Connect 🕶 🍟 📲	I ▼ C -*-		
	Connect to Server		X
		SQL Server	
	Server type:	Database Engine	~
	Server name:	BCDR-List	~
	Authentication:	Windows Authentication	~
	User name:	BCDR\deji	$\sim$
	Password:		
		Remember password	
	Ca	onnect Cancel Help	Options >>

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.

SQLQuery1.sql - BCDR-List.AdventureWorks2017 (BCDR\de	ji (64)) - Microsoft SQL	L Server Manag	ement Studio								YMRC -   - ⊕ [□]								* 🖂 🖂 🖄 🗉	
Elle Edit View Query Project Jools Window !	Help																			0 -
0 - 0 🔁 - 뉩 - 🖆 🔐 🚰 🐊 New Query 🐊 🖉	0 2 2 2 2 2 2 2	自 ワー	9 - 18	- 🏓			· 🗊 🔑 :	i 🖸 - 🚬			SQLQuery1.sql - BCDR-List.AdventureWorks2017 (BCDR\c	leji (55)) - Microsoft SQ	L Server Manager	nent Studio					aick Launch (Ctrl+Q)	2 - 6 ×
₩ 💘 AdventureWorks2017 - 🕨 Execute = 🖌	22 4 4 2 2 2 2	8 e 10 m	0 3 3	48 84	*ð -						File Edit View Query Project Tools Window	Help								
											🔆 O - O 📅 - 🔄 - 🛀 🔐 🖉 🎵 New Query 🔊 ,	<i></i>	P 6 9 - 9	- 🖾 -	<b>2</b>		- 17	- 🗆 🗳 🖓 🖥		
Object Explorer + # ×	SQLQuery1.sql - BC	.17 (BCDR\deji	(64)) + ×		from 11		,				AdventureWorks2017 • D Execute = -	/ 88 🗗 🖬 89 8	8 P 8 B	0 1 2 4	· · ·					
Connect * 🕈 🍟 = 🝸 😋 🚸	HISELECT TOP	(1000) [Bus	inessEntity	COMMAND TD1	Tros St	970	/												(	
😑 📾 BCDR-List (SQL Server 16.0.500.2 - BCDR\deji)	, [Per	rsonType]	1	1							Object Explorer • 4 ×	SULUUBYI.SQI - BC.		5)) = ×	and free					
😑 🗰 Databases	, [Nem	meStyle]									Connect - 🕴 🍟 🗏 🝸 🖸 🤸	FISELECT TOP	(1000) [Busi	ressEntityID		3315	1			T
im System Databases	,[11]	tiej ortNama]									😑 🐻 BCDR-List (SQL Server 16.0.500.2 - BCDR\deji)	, [Pe	rsonType]							
Database snapshots	[Nid	dleName]									😑 📕 Databases	, [Na	meStyle]							
Adventitievonscorr (synchronized)	,[Las	stName]					Induction	501.01			🗉 🧰 System Databases	,[T1	tiej orthismol							
E Server Objects	, [Suf	ffix]					rouuction	GGLUI			Database Snapshots	101	ddleName]			_ I -				
🕫 📁 Replication	, [ CR8	silpromotion	j actTofol								Adventalewonszon/ (synchronized)	,[ta	stName]				est Rec	covered S		
🛞 🗰 PolyBase	(Der	nographics]	accunoj								Tabler	, [Su	ffix]							
😑 🗯 Always On High Availability	(ree	(biuge									T Views	, En	ailPromotion]							
🖂 💼 Availability Groups	. FMod	difiedDate1									External Resources	. De	mographics]	cerino)						
R# SQL-2K22-AG (Primary)	200 M -										🗉 📕 Synonyms	, [ro	wguid]							
Availability Replicas	IIII Hesuits Es Me	resages									Programmability	, [No	difiedDate]							
Fig. body 2k22-sql() (Primary)	BusinessEntity	D PersonType	e NameStyle	Title I	istName	MiddeName	LastName	Suffix EmailPromo	ion AdditionalContactin	to Demographics	🛞 📫 Service Broker	100 %	Cantination by 5	HTTI IDeeroo	Decroal					
a dvailability Databases		EM	0	NULL	Ken	4	Sanchez	NULL 0	NULL	chdviduatsurvey strate Titlp /	🗉 📫 Storage	III Beauta (c) M	******							
AdventureWorks2017	2 2	EM	0	NULL	Debede	NULL	Taskada	NULL O	NULL	chidwidus Survey shirts - http://	Security	BusinessEnth	ID PersonType	NameSule T	ie FintNao	e MiddeName	LastName	Siffy EnalProp	ion AdditionalContactinfo	Demographics A
Availability Group Listeners	4 4	EM	0	NULL	Rub	NULL	Waten	NULL 0	NULL	characterization and a finite of	B Secondy	1 1	EM	0 1	ULL Ken	J	Sinchez	NULL 0	NULL	chdydai Survey snins
BCDR-List	5 5	EM	0	Ma	Gal	A	Fickan	NULL 0	NULL	(holividualSurvey veloas/http://	H Replication	2 2	EM	0 7	ULL Tem	Lee	Duffy	NULL 1	NULL	<hd>chdvidualSurvey xmins</hd>
🗉 📁 Management	6 6	EM	0	Mr	lossef	H	Goldbern	NULL 0	NULL	chdydus@urvey.xnins="http://	🛞 🗰 PolyBase	3 3	EM	0 7	ULL Roberto	NULL	Tanburelo	NULL 0	NULL	cindividualSurvey amina
Integration Services Catalogs	7 7	EM	0	NULL	Dvlan	A	Mier	NULL 2	NULL	<a>cindividualSurvey xmins="http://</a>	😑 📕 Always On High Availability	4 4	EM	0 1	ULL Rob	NULL	Waters	NULL 0	NULL	sindvidualSurvey amina
B SQL Server Agent	8 8	EM	0	NULL	Dane	L	Margheim	NULL 0	NULL	cindividualSurvey smina="http://	😑 📁 Availability Groups	5 5	EM	0 9	s. Gal	A	Erickson	NULL 0	NULL	cindividualSurvey xmins
I Atvent Prohier	9 9	EM	0	NULL	Gigi	N	Mathew	NULL 0	NULL	cindividualSurvey xmina="http://	SQL-2K22-AG (Primary)	6 6	EM	0 1	r. Jossef	н	Goldberg	NULL 0	NULL	cindividualSurvey xmins
	10 10	EM	0	NULL	Michael	NULL	Raheem	NULL 2	NULL	<a>cindividualSurvey.xnins+"http://</a>	Availability Replicas	7 7	EM	0 1	ULL Dylan	A	Miler	NULL 2	NULL	sindvidualSurvey amina
	11 11	EM	0	NULL	Ovidiu	V	Cracium	NULL 0	NULL	cindividualSurvey.xnina=Thtp://	Bcdr-2k22-sql01 (Primary)	8 8	EM	0 1	ULL Dane	L	Margheim	NULL 0	NULL	<hr/> cindividualSurvey xmins
	12 12	EM	0	NULL	Thierry	8	D'Hers	NULL 2	NULL	<a <="" href="http://cindualSurvey.xnlna=" http:="" td=""><td>Availability Databases</td><td>9 9</td><td>EM</td><td>• •</td><td>ULL Gg</td><td>N</td><td>Mathew</td><td>NULL 0</td><td>NULL</td><td><u>cindvidualSurvey xmins</u></td></a>	Availability Databases	9 9	EM	• •	ULL Gg	N	Mathew	NULL 0	NULL	<u>cindvidualSurvey xmins</u>
	13 13	EM	0	Ms.	Janice	м	Galvin	NULL 2	NULL	<a>cindividualSurvey.xmins="http://</a>	AdventureWorks2017	10 10	EM	•	ULL Michael	NULL	Raheem	NULL 2	NULL	cindwidualSurvey xmina
	14 14	EM	0	NULL	Michael	1	Sullivan	NULL 2	NULL	<a>chdvidualSurvey.xnina="http://</a>	Availability Group Listeners	11 11	EN	0	ULL Ovidu	V	Crecium	NULL	NULL	chdvdua/Survey smins
	15 15	EM	0	NULL	Sharon	8	Salavaria	NULL 2	NULL	<hd>vidualSurvey.xmina="http://</hd>	BCDR-List	12 12	EN		ULL Intery	8	Uners	NULL 2	NULL	chavaus survey strins
	16 16	EM	0	NULL	David	M	Bradley	NULL 1	NULL	<a>  <a>  <a>  <a>  <a>  <a>    <a>    <a>    <br< td=""><td>🛞 💼 Management</td><td>13 13</td><td>EM</td><td></td><td>s. Jance</td><td>N</td><td>Salver</td><td>NULL 2</td><td>MULL</td><td>Charles and Service and the</td></br<></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></br></a></br></a></br></a></br></a></a></a></a></a></a></a></a></a></a></a></a></a>	🛞 💼 Management	13 13	EM		s. Jance	N	Salver	NULL 2	MULL	Charles and Service and the
	17 17	EM	0	NULL	Kevin		Brown	NULL 2	NULL	chdviduatsurvey strate Titlp 2.	Integration Services Catalogs	15 15	EM		III Shann	8	Salavata	NULL 2	NULL	Checked of Survey strike
	10 10	EM	0	NULL	John Maai		Wood .	NULL 2	NULL	chidwidue Survey share - http://	Command Premet	- 0	×		UII David	M	Badey	NULL 1	NULL	chdvid alSuney mini
	20 20	EM	0	NULL	Wanida	M	Barahood	NULL 2	NULL	clock of the second sec	Commind Prompt	5	~	0 1	ULL Kevin	F	Brown	NULL 2	NULL	cindwidual Survey amina
	20 20	-	0	NULL	Terry	1	Eminhiner	NULL 2	NULL	(Individual Survey values "http://			^	0 7	ULL John	L	Wood	NULL 2	NULL	<hd>chdvidualSurvey xmlns</hd>
Command Prompt	- 0	×	0	NULL	Same	F	Harmado postava	NULL 0	NULL	cheductualSurgers verlage "http://	Ethernet adapter Ethernet0:			0 7	ULL May	A	Denosey	NULL 1	NULL	<hd>kindwidualSurvey xmlms</hd>
		<b>^</b>	0	NULL	Mary	E	Gibson	NULL 0	NULL	<a>cindividualSurvey xmins="http://</a>				0 1	ULL Wanida	M	Benahoof	NULL 2	NULL	sindvidualSurvey amina
			0	Ma.		A	Williams	NULL 0	NULL	chdividualSurvey mina="http://	Connection-specific DNS Suffix . :			0 1	ULL Terry	J	Eninhizer	NULL 2	NULL	cindividual Survey amins
Ethernet adapter Ethernet0:			0	NULL	lames	R	Hamilton	NULL 0	NULL	<individualsurvey <="" http:="" td="" xmina="http://&lt;/td&gt;&lt;td&gt;IPv4 Address&lt;/td&gt;&lt;td&gt;-233&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;0 1&lt;/td&gt;&lt;td&gt;ULL Sarlya&lt;/td&gt;&lt;td&gt;E&lt;/td&gt;&lt;td&gt;Hampad&lt;/td&gt;&lt;td&gt;NULL 0&lt;/td&gt;&lt;td&gt;NULL&lt;/td&gt;&lt;td&gt;cindividualSurvey xmins&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Connection enorifie DNE Suffix&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;0&lt;/td&gt;&lt;td&gt;NULL&lt;/td&gt;&lt;td&gt;Peter&lt;/td&gt;&lt;td&gt;J&lt;/td&gt;&lt;td&gt;Krebs&lt;/td&gt;&lt;td&gt;NULL 0&lt;/td&gt;&lt;td&gt;NULL&lt;/td&gt;&lt;td&gt;cindividualSurvey xmins="><td>IPv4 Address</td><td></td><td></td><td>0 1</td><td>ULL May</td><td>E</td><td>Gibson</td><td>NULL 0</td><td>NULL</td><td>cindvidualSurvey smins</td></individualsurvey>	IPv4 Address			0 1	ULL May	E	Gibson	NULL 0	NULL	cindvidualSurvey smins
IPv4 Address			0	NULL	Jo	A	Brown	NULL 0	NULL	cindividualSurvey.xnina+Tritp://	Subnet Mask			0 9	s. Jil	A	Witens	NULL 0	NULL	<hr/> cindividualSurvey amins
Subnet Mask			0	NULL	Guy	R	Gibet	NULL 0	NULL	<a>cindividualSurvey.xmlna="http://</a>	IPv4 Address	.237		0 1	ULL James	R	Hamiton	NULL 0	NULL	cindividualSurvey xmins
IPv4 Address			0	NULL	Mark.	к	NoAthur	NULL 1	NULL	cindividualSurvey.onlns+"http://	Default Gateway 10	1								
Subnet Hask	2.0		0	NULL	Bitta	L	Simon	NULL 0	NULL	<a>chdvidualSurvey.mina="http://</a>	beroote cotenay P					B	08-16+716.07	TR1 SL BCORIdai	SSI AdventureWorks201	7 000000 1000 mm
Subnet Mask	2.0		0	NULL	Margie	W	Shoop	NULL 2	NULL	<hr/> kindividualSurvey.xmlna="http://			× [	_	_	0	1011 0131 (1000 0	acovindi	ing interconstervortscor	1,000 104/5
Default Gateway 10.1			0	NULL	Rebecca	A	Lasdo	NULL 1	NULL	<hr/> <hr/> individualSurvey.xnlns="http://	Ready									

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 - U
👝 Server Manager
  Administrator: Command Prompt
 C:\>ping bcdr-2k22-dc01.bcdr.local
 Pinging bcdr-2k22-dc01.bcdr.local [10.
                                                  31] with 32 bytes of data:
                 31: bytes=32 time<1ms TTL=128
31: bytes=32 time<1ms TTL=128
31: bytes=32 time<1ms TTL=128
31: bytes=32 time<1ms TTL=128
 Reply from 10.
  Reply from 10.
 Reply from 10.
 Reply from 10._____31: bytes=32 time<1ms TTL=128
 Ping statistics for 10.
                                  31:
     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
     Minimum = Oms, Maximum = Oms, Average = Oms
 C:\>ping bcdr-2k22-dc02.bcdr.local
 Pinging bcdr-2k22-dc02.bcdr.local [10
                                                 !32] with 32 bytes of data:
 Reply from 10
                        !32: bytes=32 time<1ms TTL=128</pre>
 Reply from 10
                        !32: bytes=32 time<1ms TTL=128
 Reply from 10
                        !32: bytes=32 time<1ms TTL=128</pre>
 Reply from 10./2.200.232: bytes=32 time<1ms TTL=128
 Ping statistics for 10.
                                  32:
      Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
     Minimum = Oms, Maximum = Oms, Average = Oms
 C:\>ping bcdr-2k22-sql02.bcdr.local
                                                   34] with 32 bytes of data:
 Pinging bcdr-2k22-sql02.bcdr.local [10.
 Reply from 10.70 or 334: bytes=32 time=1ms TTL=128
 Reply from 10.
                        34: bytes=32 time<1ms TTL=128
 Reply from 10.
                        34: bytes=32 time<1ms TTL=128
 Reply from 10.
                        34: bytes=32 time<1ms TTL=128
 Ping statistics for 10
                                  234:
     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
     Minimum = Oms, Maximum = 1ms, Average = Oms
 C:\>ping bcdr-2k22-sql01.bcdr.local
 Pinging bcdr-2k22-sql01.bcdr.local [10.72
                                                      ] with 32 bytes of data:
 Reply from 10.7
                          3: bytes=32 time<1ms TTL=128
 Reply from 10.7
                          3: bytes=32 time<1ms TTL=128
 Reply from 10.7
                          3: bytes=32 time<1ms TTL=128
 Reply from 10.7....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.



Site Pair Replications Pro	Detection Groups Recovery Plans								
Q Search	Recovery Plans								
Recovery Plans	NEW								
BCDR-Client-RP01	Name	1 τ	Status	т	Protected	Site	т	Recovery Site	
BCDR-DC-RP01	O BCDR-Client-RP01		Test complete		T:	1C		srm	vmc.com
	O BCDR-DC-RP01		Test complete		T:	1C		srr	evmc.com
EQ DUDK-MODUL-KHUI	O BCDR-MSSQL-RP01		Test complete		т	1C		srm.s	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.

•	То	do	this,	select	the	Recovery	Plan	and	click	"Cleanup".
---	----	----	-------	--------	-----	----------	------	-----	-------	------------

📰 Site Pair 🕂 Replications 🔍 Pro	ction Groups Recovery Plans
Q Search	BCDR-Client-RP01 edit move delete test cleanup run reprotect cance
Recovery Plans	Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines
BCDR-Client-RP01	
BCDR-DC-RP01	Recovery Plan: BCDR-Client-RP01
BCDR-MSSQL-RP01	Protected Site:     Tf     Tr          Tr          Tr
	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.



• Click "Finish" to commit the changes.



Cleanup - BCDR-Client- RP01	Ready to complete Review your selected settings.	×
1 Confirmation options	Name	BCDR-Client-RP01
	Protected site	TSALab-VMC
2 Ready to complete	Recovery site	srm.sddc-34-223-133-154.vmwarevmc.com
	Server connection	Connected
	Number of VMs	1
	Force cleanup	Do not ignore cleanup warnings
		CANCEL BACK FINIGH

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

III Site Pair Replications Protection Groups	
Q Search	BCDR-Client-RP01 edit move delete test cleanup run reprotect cancel
Recovery Plans	Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines
BCDR-Client-RP01	
BCDR-DC-RP01	Recovery Plan: BCDR-Client-RP01
BCDR-MSSQL-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.

Powered Off

➡ From- summary	TSALab : ACTION Monitor Configure	vs Permissio	ns VMs	Updates					
Virtual Mac	ines VM Templates	vApps	VM Folders	]					
Nam	2	↑ Stat	e		Status	Provisioned Space	Used Space	Host CPU	Host Mem
	BCDR-2K22-CL01	Pov	vered Off		🗸 Normal	13.92 GB	236 MB	0 Hz	0 B
🗌 🛛 👘 🎝	BCDR-2K22-DC01	Pov	vered Off		V Normal	13.92 GB	236 MB	0 Hz	0 B
🗌 🗌 🕴 🎝	BCDR-2K22-DC02	Pov	vered Off		🗸 Normal	13.92 GB	236 MB	0 Hz	0 B
🗌   🛛 🎝	BCDR-2K22-SQL01	Pov	vered Off		🗸 Normal	21.92 GB	228 MB	0 Hz	0 B

Normal

21.92 GB

#### Performing a Real Disaster Recovery

🔲 🗏 📅 BCDR-2K22-SQL02

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.



0 Hz

232 MB

0 B

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**".

III Site Pair C Replications Protection Groups	
Q Search	BCDR-DC-RP01 edit move delete test cleanut run eprotect cancel
Recovery Plans	Summary Recovery Steps Issues History Permissions Protection Run Recovery Planual Machines
BCDR-Client-RP01	Recovery Plan: BCDR-DC-RP01
BCDR-MSSQL-RP01	Protected Site: TS Recovery Site: srn c.com Description:
	> Plan Status
	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".





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	Confirmation options  Confirm that you understand that this process will permanently alter the virtual machines and infrastructure of batter the proceeding of an analysis of the process	×
1 Confirmation options	both the protected and recovery datacenters.	
2 Ready to complete	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:	
	I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.	
	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.     CANCEL	EXT

• Click "Finish" to begin the disaster recovery.



Recovery - BCDR-DC- RP01	Ready to complete Review your selected settings.		×
1 Confirmation options	Name	BCDR-DC-RP01	
	Protected site	T: //C	
2 Ready to complete	Recovery site	srm com	
	Server connection	Connected	
	Number of VMs	2	
	Recovery type	Disaster recovery	
	Forced recovery	Do not force recovery	
		CANCEL BACK FIN	ISH

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 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:	
91%	
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
⇒	
Summary Monitor Configure Permissions VMs Updates	✓ Success
5.1. Protection Group BCDR-DC-PG01	✓ Success
6. Shut down VMs at protected site	<ul> <li>Success</li> </ul>
6.1. Shut down the priority 5 VMs	lost Mem
6.2. Shut down the priority 4 VMs	.13 GB
:         6.3. Shut down the priority 3 VMs         Image: Character and the priority 3 VMs         Powered off <ul></ul>	/B )B
6.4. Shut down the priority 2 VMs	.74 GB
Control Contro	∠25 GB ✓ 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	
2 🕅 10. Prepare protected site VMs for migration	✓ Success
V S 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
VI 14. Power on priority 1 VMs	III Running
> 14.1. BCDR-2K22-DC02	III Running
> 14.2. BCDR-2K22-DC01	III Running

Our Recovery was completed successfully



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:	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.

🖻 From-	TSAL	аb : Астіон	s		
Summary	Monito	r Configure	Permissio	ns VMs	Updates
Virtual Mac	hines	VM Templates	vApps	VM Folders	

Name	↑ State	Status	Provisioned Space	Used
□ 🗄 🗊 BCDR-2K22-CL01	Powered Off	V 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.

۵F	rom-TSALab							b T	D-VMC						
Summ	ary Monitor Configure	Permissions VMs Updates						Summ	ry Monitor Configure	Permissions VMs	Updates				
Virtu	al Machines VM Templates	vApps VM Folders	F	ecovery s	Site			Virtu	al Machines VM Templates	vApps VM Folde	rs P	rotected	Site		
	Name	↑ State	Status	Provisioned Space	Used Space	Host CPU	Host Mem		Name	↑ State	Status	Provisioned Space	Used Space	Host CPU	Host Mer
	BCDR-2K22-CL01	Powered On	V Normal	192.97 GB	35.27 GB	149 MHz	1.61 GB		BCDR-2K22-CL01	Powered Off	V Normal	102.22 GB	16.91 GB	0 Hz	0 B
	BCDR-2K22-DC01	Powered On	<ul> <li>Normal</li> </ul>	193.08 GB	28.58 GB	24 MHz	1.94 GB		BCDR-2K22-DC01	Powered Off	V Normal	102.22 GB	13.26 GB	0 Hz	0 B
	BCDR-2K22-DC02	Powered On	V Normal	193.04 GB	28.76 GB	24 MHz	1.92 GB		BCDR-2K22-DC02	Powered Off	<ul> <li>Normal</li> </ul>	102.22 GB	13.52 GB	0 Hz	0 B
	BCDR-2K22-SQL01	Powered On	V Normal	501.02 GB	44.87 GB	O Hz	2.22 GB		BCDR-2K22-SQL01	Powered Off	V Normal	260.23 GB	20.9 GB	0 Hz	0 B
	BCDR-2K22-SQL02	Powered On	V Normal	500.98 GB	42.38 GB	0 Hz	2.07 GB		BCDR-2K22-SQL02	Powered Off	V 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?

Site Pair 🔄 Replications 🔍 Protection Groups 📃 Recover	ry Plans 🚳			
Q Search	Recovery Plans			
Recovery Plans	NEW			
BCDR-Client-RP01	Name	↑ ⊤ Status	T Protected Site	T Recovery Site
BCDR-DC-RP01	BCDR-Client-RP01 Reprotect needed	Recovery complete	TOTOLO TOTO	n
BCDP-MSSQL-PP01	BCDR-DC-RP01 Reprotect needed	Recovery complete	IC	sm
Lo poprimodal in or	C BCDR-MSSQL-RP01 Reprotect needed	Recovery complete	Tu	sım
Recovery Plans       BCDR-Client-RP01       BCDR-DC-RP01       BCDR-MSSQL-RP01	NEW Name Big BCDR-Client-RP01 Reprotect needed Big BCDR-Dc-RP01 Reprotect needed Big BCDR-Dc-RP01 Reprotect needed Big BCDR-MSSQL-RP01 Reprotect needed Big BCDR-Big BC	<ul> <li>↑ ▼ Status</li> <li>⑦ Recovery complete</li> <li>③ Recovery complete</li> <li>③ Recovery complete</li> </ul>	Protected Site     Torress Find     Torress Find     Torress Find	γ Recovery Site

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".

III Site Pair C Replications Protection Groups Recovery Plan		
Q. Search Recovery Plans		
BCDR-Client-RP01		
BCDR-DC-RP01	Recovery Plan: BCDR-DC-RP01	
🔓 BCDP-MSSOL-APO1	Recovery Site: sm ***********************************	
	Your workloads are not protected. Run reprotect.	
	> Plan Status	
	Plan Status: ORecovery 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 faitback 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.

Reprotect - BCDR-DC- RP01	Confirmation options ×
	Reprotect confirmation
1 Confirmation options	Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.
2 Ready to complete	New protected site:       srm.clicle of coortoo to to non-non-non-non-non-non-non-non-non-no
	CANCEL

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**".



🗈 To-	VMC	ACTIONS						
Summary	Monito	or Configure	Permissio	ons VMs	Updates			
Virtual	Machines	VM Templates	vApps	VM Folders	]			
	Name		↑ Stat	e	Statu	s	Provisioned Space	Used Space
	📅 BCDR-:	2K22-CL01	Pov	vered Off	$\sim$	Normal	13.69 GB	1.02 KB
	📅 BCDR-:	2K22-DC01	Pov	vered Off	$\sim$	Normal	13.69 GB	1.02 KB
	📅 BCDR-:	2K22-DC02	Pov	vered Off	$\sim$	Normal	13.69 GB	1.02 KB
	📅 BCDR-:	2K22-SQL01	Pov	vered Off	$\checkmark$	Normal	21.7 GB	1.02 KB
	📅 BCDR-:	2K22-SQL02	Pov	vered Off	$\checkmark$	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".

Site Pair Replications Protection Groups Recovery Plan	S
Q Search	BCDR-MSSQL-RP01 edit move delete test cleanup run reprotect cancel
Recovery Plans	Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines
BCDR-Client-RP01	
BCDR-DC-RP01	CONFIGURE RECOVERY PRIORITY GROUP V STARTUP ACTION V
BCDR-MSSQL-RP01	Virtual Mc Change the VM Recovery Settings
	□ 》 目 BCDR-2K22-SQL02

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



overy Properties IP Customization			
	1 (Highest) 🗸		
Priority Group	All virtual machines within a priority group will be started machines within a priority group may be specified by add parallel, unless ordered by VM dependencies.	before proceeding to the next priority group. The star ding VM dependencies. The virtual machines within a p	rtup order of virtual riority group will star
Pre Power On Steps	None		
Post Power On Steps			
These steps run after the VM is powered on.			
+ NEW 🛛 🖉 EDIT × DELETE 🔿	MOVE UP 🚽 MOVE DOWN		
Name	Туре	Timeout	
• Reconfigure-Cluster-AG-VIPs	Run on Recovered VM	5 min 0 sec	

- 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 Pow	er On Step	×
Туре:	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:	Bowershell exe E-\Install-Files\Change-Cluster-AG-VIP-Reversed[ps1	Å
Timeout:	5 0 minutes 0 0 Cancel	SAVE

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 Pre Power On Steps Post Power On Steps These steps run after the VM is powered on.	All virtual machines within a priority group will be started machines within a priority group may be specified by add parallel, unless ordered by VM dependencies. None	before proceeding to the next priority group. The startup order of virtual ding VM dependencies. The virtual machines within a priority group will start in
Pre Power On Steps Post Power On Steps These steps run after the VM is powered on.	None	
Post Power On Steps These steps run after the VM is powered on.		
These steps run after the VM is powered on.		
+ NEW 🖉 EDIT X DELETE 个 MOVE	UP 🗸 MOVE DOWN	
Name	Туре	Timeout
Reconfigure-Cluster-AG-VIPs	Run on Recovered VM	5 min 0 sec

CANCEL

X

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 X
          Import-Module FailoverClusters
    2
           # Let's Force-Start our Cluster first
    3
           # Immediately post-recovery, the whole Cluster is down
    4
           Start-ClusterNode -FQ
    5
           #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
    6
    8
           $NewClusSub = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter $GetClusRes,SubnetMask,255.255.252.0
$NewClusVal = $NewClusIP,$NewClusSub
    9
  10
  11
12
          # 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
  13
  14
  15
  16
           $NewAGVal = $NewAGIP,$NewAGSub
  17
           # Let's ensure that all the resources are offline
  18
          Stop-ClusterResource "SCDR-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
  19
  20
  21
  22
  23
           # Now, commit the change
$NewClusVal | Set-ClusterParameter
$NewAGVal | Set-ClusterParameter
  24
  25
  26
  27
28
           # Now, we start everything back up
           * 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"
  29
  30
  31
  32
```



# 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 -F0
# 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 \$NewAGSub = New-Object Microsoft.FailoverClusters.PowerShell.ClusterParameter \$GetAGRes,SubnetMask,255.255.252.0

# 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



