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

Introduction

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

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

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

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

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

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

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

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



TASKS

Task 1 - Activate Site Recovery Add-on

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



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

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

Student19 VMware Cloud on AWS () US West (Oregon)	
Activate Site Recovery for Student19	×
VMware Site Recovery allows you to protect on-premises workloads and recover them on this SDDC.	ize Au
After Site Recovery is activated, you need to install on-premises components on the SDDC you wish to protect. Download the components from http://www.vmware.com/go/download-site-recovery [2]	ted wo
VMware Site Recovery requires you create several firewall rules after activation. Please see the help topic <i>What firewall rules do I need for Site Recovery</i> by pressing the ⑦ icon on the card.	lf-servio rs and n dicies th
opefault extension ID (com.vmware.vcDr)	
Custom extension ID com.vmware.vcDr	

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

- As mentioned in the previous task, the on-premises appliances have already been deployed. In this task we will review and modify the configuration.
- 1. Log into your On-Premises vCenter
- 2. (you may use the **vSphere Client** bookmark in the **VI Management** bookmark folder in Chrome)
- 3. Expand the Shotoku Mgmt&Edge Cluster
- 4. Confirm the existence of the following VMs
 - ・ vr-l-01a
 - srm-l-01a
- 5. Power-on **vr-l-01a**, If it is powered-off
 - NOTE: Do not power-on srm-l-01a until the vSphere Replication appliance configuration has completed successfully

vm vSphere Client Menu V	Q Search in all environments		C @~	Administrator@VSPHERE.L	.ocal 🗸
□ □ □ <u>○</u> <u>○</u>	Summary Monitor Cor	🚰 🤯 🔯 🛛 ACTIONS 🗸 nfigure Permissions Datastores Net	works Snapshots Updates	5	
 Shinobi-On-Prem DC Shotoku Compute01 Shotoku Mgmt&Edge esxi-Ola.vcn.ninja.local en-Ola srm-I-Ola vr-I-Ola 192.168.110.151 	Powered Off	Guest OS: Other 3.x or later Linux (64-1 Compatibility: ESXi 5.5 and later (VM versic VMware Tools: Not running, version:10346 (MORE INFO DNS Name: IP Addresses: Host: esxi-01a.vcn.ninja.local	bit) n 10) Upgrade available)	SWIT	CH TO NEW CPU USAC O HZ MEMORY I O B STORAGE 1,013.6
	VM Hardware CPU Memory	2 CPU(s)	Notes vSphere Replication Appliance Edit Notes		
	Hard disk 1 Hard disk 2 Network adapter 1 CD/DVD drive 1	9 GB 17 GB Shinobi_vDS - Mgmt (disconnected) Disconnected	Custom Attributes Attribute	Value	

- In another browser tab access the vSphere Replication Appliance Bookmark or type <u>https://vr-l-01a.vcn.ninja.local:5480</u> to review settings. You will need to wait for a few minutes for step 4 to complete before the gui works.
 - Use the following login information:
 - Username: admin
 - Password: VMwareNinja1!
- 7. Click the **Configuration Appliance** button
- 8. In the Platform Services Information Page of the Wizard, enter the following values
 - PSC host name: vc-l-01a.vcn.ninja.local
 - PSC port: 443
 - User Name: administrator@vsphere.local
 - Password: VMwareNinja1!
- 9. When prompted Accept the SSL Certificate Click CONNECT
- 10. Click NEXT
- 11. When prompted **Accept** the SSL Certificate Click **CONNECT**
- 12. Enter the following information in the Name and Extension page of the wizard:
 - Site Name: vmcexpert#-xx-Protected-Site (Where # is the Environment ID, and xx is your student number)
 - Administrator email: admin@ninja.local
- 13. Click NEXT
- 14. Click **Finish**
- 15. Note: This process can take up to 5 Mins. Wait for it to complete and confirm that the Tomcat Service is running before proceeding

Configure vSphere Replication	Platform Se	rvices Controller	×
1 Platform Services Controller	Enter the Platforr Replication.	n Services Controller details for the vCenter Server for which you want to configure vSphere	
2 vCenter Server	PSC host name	vc-I-01a.vcn.ninja.local	
3 Name and extension	PSC port	443	
4 Ready to complete	User name	administrator@vsphere.local	
	Password		
	Note: If prompted, y	ou must accept the certificate for the configuration to proceed.	

Configure vSphere	Name and exter	nsion	×
Replication	Enter name and extensio	n for vSphere Replication	
1 Platform Services Controller	Site name	vmcexpert3-01-Protected-Site	
2 vCenter Server		A unique display name for this vSphere Replication site.	
	Administrator email	admin@ninja.local	
3 Name and extension		An email address to use for system notifications.	
4. Ready to complete	Local host	vr-l-01a.vcn.ninja.local \vee	
i notaj to comprete		The address on the local host to be used by vSphere Replication	1.
	Extension ID	com.vmware.vcHms	
	Storage Traffic IP		
		optional	
			CANCEL BACK NEX

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

	RESTART DOWNLOAD SUPPORT BUNDLE STOP
Product	VMware Site Recovery Manager Appliance
Version	8.4.0
Build	17684897
	To start protecting virtual machines you must configure the Site Recovery Manager appliance and connect to a vCenter Server.

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

Configure Site Recovery Manager	Platform S	Services Controller		×
1 Platform Services Controller	Enter the Platf	orm Services Controller details fo Manager.	or the vCenter Server for which you wan	nt to configure
2 vCenter Server	PSC host	vc-l-01a.vcn.ninja.local		
3 Name and extension	name PSC port	443		
4 Ready to complete	User name	administrator@vsphere.local		
	Password	VMwareNinja1!	<u>a</u>	
	Note: If prompted	d, you must accept the certificate for	the configuration to proceed.	
			CAN	ICEL NEXT

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

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

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

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

		_							
view	Gatew	∕ay ⊢	irewall						
vork	Manager	nent Ga	ate Compu	ite Gateway					
gments									
Ν							4 Tota	I Unpublished Changes	REVERT
Т	ADD	RULE	CLONE ←		LETE 4 Unpublished Chan	ges	Success C	Filter by Name, Path	and more
r-1 Gateways									
insit connect			Name	ID	Sources	Destinations	Services	Action	
rity	2		SRM Inbound		🚼 On-Prem	Site Reco	🗘 VMware Site Recovery	🌒 Allow 🗸 🇨) @ 🖂
eway Firew					PR 0 0	PP o i	<u></u>		
ributed Firewall	1		VR Inbound		aa On-Prem	55 vSphere			
ribuled IDS/IPS	1		SRM Outbound		BB Site Reco	Any	Any	🌖 Allow 🗸 🇨) @ 🖂
tory									
ups	1		VR Outbound		vSphere	Any	Any	Allow 🗸 🇨) @ 🖂
vices	:		HCX Outbound	2041	BB HCX	88 On-Prem	Any	Allow V) @ ~
ual Machines	•	0							ар — -
text Profiles			HCX Inbound	2040	Con-Prem	HCX	Appliance Managemen	💧 Allow 🗸 🇨) 🔅 🖂
							⟨} SSH		
X							♦ HTTPS		
Mirroring									
m	C REFR	ESH							1

Task 4 - Pair On-Premises with SDDC

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

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

← → C ▲ Not secure srm-I-01a.vcn.ninja.local/dr/#/home			
📙 VI Management 📀 Web01 📀 Web02 🧐 NSX 3-Tier App -01a 🤄 NSX 3-Tier App - 02a 📀 Planespotter 📀 VMware Cloud SDDC			
vmw Site Recovery Menu V	С	¢	?
NEW SITE PAIR			
Replications within the same vCenter Server			
within vc-l-O1a.vcn.ninja.local 0			
VIEW DETAILS			

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

Peer vCente	er Server		×
1 nter the Platform	Services Controller details for the peer vCenter Server	-	
PSC host name	vcenter.sddc-52-28-33-169.vmwarevmc.com		
PSC port	443		
User name	cloudadmin@vmc.local		
Password	····· @		
2 FIND VCEI Select a vCenter S vCenter Serve 3 Evcenter.s	nter server instances erver you want to pair. er sddc-52-28-33-169.vmwarevmc.com	CANCEL	T BACK
	Peer vCenter	Peer vCenter Server Inter the Platform Services Controller details for the peer vCenter Server PSC host name vcenter.sddc-52-28-33-169.vmwarevmc.com PSC port 443 User name cloudadmin@vmc.local Password @ 2 FIND VCENTER SERVER INSTANCES Select a vCenter Server you want to pair. vCenter Server 3 @ vcenter.sddc-52-28-33-169.vmwarevmc.com	Peer vCenter Server Inter the Platform Services Controller details for the peer vCenter Server. PSC host name vcenter.sddc-52-28-33-169.vmwarevmc.com PSC port 443 User name cloudadmin@vmc.local Password Inter Server Vcenter Server Inter Server

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

vmw Site Recovery Menu V		C	¢	?
NEW SITE PAIR				
vc-l-01a.vcn.ninja.local ↔ vcenter.sddc-52-2	Replications within the same vCenter Server			
Site Recovery Manager Protection Groups 0 Sphere Replication	떠 within vc-l-01a.vcn.ninja.local 0			
면 Outgoing 0 면 Incoming 0				
VIEW DETAILS ACTIONS ~	VIEW DETAILS			

Task 5 - Configure DR for Virtual Machines

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

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

vmw Site Recovery Menu V		C	¢	?
NEW SITE PAIR				
Ø vc-l-01a.vcn.ninja.local ↔ Ø vcenter.sddc-52-2	Replications within the same vCenter Server			
Site Recovery Manager Protection Groups 0 Recovery Plans 0 vSphere Replication Outgoing 0 Incoming 0	④ within vc-l-01a.vcn.ninja.local 0			
VIEW DETAILS ACTIONS ~	VIEW DETAILS			

	Log in Site		×	
	Enter vCenter Ser	ver credentials		
	na.			
	VCenter Server	vcenter.sddc-44-235-221-	106.vmwarevmc.com	
	User name	cloudadmin@vmc.local		
	Password			
			CANCEL LOG IN	
	on			

Site Pair Replications	Protection Groups 🔲 Recovery Plans		
Summary	Summary		RECONNECT BREAK SITE PAIR ?
Issues Configure Replication Servers Array Based Replication Storage Replication Adapt	vCenter Server: vCenter Version: vCenter Host Name: Platform Services Controller:	vc-I-01a.vcn.ninja.local vcenter.sddc-52-28-33-169.vmwarevmc. 7.0.2, 17958471 7.0.2, 18137590 vcenter.sddc-52-28-33-169.vmwarevmc.com vcenter.sddc-52-28-33-169.vmwarevmc.com vc-I-01a.vcn.ninja.local:443 vcenter.sddc-52-28-33-169.vmwarevmc.com	יסה רַז 1443 1443
Array Pairs Network Mappings	Site Recovery Manager Protection Groups:0 Recovery Plans:0		EXPORT/IMPORT SRM CONFIGURATION V
Folder Mappings Resource Mappings Storage Policy Mappings	> Name Remote SRM connection	vmcexpert3-01-Protected-Site RENAME	srm.sddc-52-28-33-169.vmwarevmc RENAME
Placeholder Datastores	vSphere Replication		
Advanced Settings >	Replicated VMs from vmcexpert3-01-Protect	t 0 🔹 Replicated VMs from vcenter.sddc-52-28-33 0	
Permissions	> Name	vmcexpert3-01-Protected-Site	vcenter.sddc-52-28-33-169.vmware
Recovery Plans History vSphere Replication reports	Remote VR connection	✓ Connected	✓ Connected

Task 5.1 - Create a Network Segment in SDDC

ONLY PERFORM THIS TASK IF YOU SKIPPED THE HCX LAB OR YOUR NETWORK EXTENSION OF vm-seg WAS UNSUCCESSFUL!!! If you created a functional network Extension for vm-seg during the HCX lab (Lab 8 - Part 2, Task 2), skip this task and move on to Task 5.1.1 instead.

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

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

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

Student1	VMware Cloud on AWS () US West (Oregon)			OPEN VCENTER ACTIONS *
Summary Networking	& Security Add Ons Maintenance	Troubleshooting Settings	Support	
Overview	Segments			0
Network	Seament List Seament Profiles			
Segm 2				
VPN	ADD SEGMENT			EXPAND ALL Q. Search
NAT				-
Tier-1 Gateways	Segment Name	Туре	Subnets	Status (j)
Transit Connect				
Security	L2E_vm-seg	Routed	▼ * 172.16.101.1/24	*
Gateway Firewall			CIDR e.g. 10.22.12.2/23	
Distributed Firewall			SET DHCP CONFIG	
Inventory				
Groups				
Services	VPN Tunnel ID		Domain Name	Enter Fully Qualified Domain Nan
Virtual Machines	Description	Description	Tags	
Tools			1095	Tag (Rei V Scope (r V T
IPFIX				Max 50 allowed. Click (+) to save.
Port Mirroring	4			
System	SAVE CANCE	Unsaved Changes		
DNS				
DHCP	> SEGMENT PROFILES			
Global Configuration	> DHCP STATIC BINDING	S		
Public IPs				
Direct Connect				CLOSE EDITING
Connected VPC			· · ·	

Task 5.1.1 - Configure Network Mappings

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

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

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

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

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

vmw Site Recovery vc-l-01a.vcn.r	ninja.local - vcenter.sddc-44-235-221-106.vmwarevmc.com V	C	♤	?	Administrat
Site Pair C Replications	Protection Groups 🔲 Recovery Plans				
Summary Issues Configure Replication Servers Array Based Replication Storage Replication Adapters Array Pairs Network Mappings	Network Mappings vc-I-01a.vcn.ninja.local vcenter.sddc-44-235-221-106.vmwarevmc.com NEW 3 vc-I-01a.vcn.ninja.local	verse Mapping	Ŧ	Test Network	
Folder Mappings Folder Mappings Resource Mappings Storage Policy Mappings Placeholder Datastores > Advanced Settings Permissions Recovery Plans History vSphere Penlication reports	I EXPORT ~ No network map	pping selected			
vapilere repication reports					
Recent Tasks Alarms					
Task Name Target	Y Status Y Initiator Y Queued For	▼ Start Time	ψ τ	Completi	on Time ។

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

lew Network Mappings	Recovery networks	a mannings for objects marked with * are already created
1 Creation mode	or prepared.	ie mappings for objects marked with are aready created
2 Recovery networks	A Shinobi_VDS - Ho Access	A Demo-Net Desktop-Net
3 Reverse mappings	□ 🗟 Shinobi_vDS - Storage	A hcx-11852f50-960b-4110-9b6e-6f67e11f
4 Test networks	Shinobi_vDS - vMotion Skinobi_vDS - vMotion Skinobi_vDS - vMotion	2 A L2E_planespotter-seg-65537-e6041af1
5 Ready to complete	🗌 🔐 web-seg	→ L2E_vm-seg-65540-e6041af1
	MA-VMW-Management	○ 🧕 MA-VMW-VMotion
	ADD MAPPI	NGS 3
	vc-I-01a.vcn.ninja.local y vc	center.sddc-44-235-221-106.vmwarevmc.com
	Shinobi-On-Prem DC > Shinobi_vDS > vm-seg	SDDC-Datacenter > L2E_vm-seg-65540-e6041af1
		1 mapping(s)
		CANCEL BACK NEXT

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



Task 5.1.2 - Configure Folder Mappings

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

vmw Site Recovery vc-l-01a.vcn.nir	nja.local - vcenter.sdd	lc-44-235	-221-106.vmwa	irevmc.co	om 🗸				C	¢	?	Administrator@
Site Pair Replications	Protection Groups	E Re	covery Plans									
Summary	Folder Mapp	oings										
Issues	vc-I-01a.vcn.ninj	a.local	vcenter.sdd	c-44-235	-221-10	6.vmwarevn	nc.com					
✓ Configure	2 NEW											
Replication Servers	vc-I-01a.vcn.nir	nja.local			↑ _▼	vcenter.sddc-	44-235-221-	106.vmwarevm	nc.com	Ŧ	Reverse M	apping Exists
✓ Array Based Replication												
Storage Replication Adapters												
Array Pairs												
Network Mappings												
Folder Mappings												
Resource Mappings								$\mathbf{\mathbf{\nabla}}$				
Storage Policy Mappings												
Placeholder Datastores												
> Advanced Settings												
Permissions												
Recovery Plans History												
vSphere Replication reports	FYPOPT											
	LAFORIY											
Recent Tasks Alarms												
Task Name Target	⊤ Status	5	Ŧ	Initiator		Ŧ	Queued F	or T	Start Time	↓ 1	Comp	letion Time T

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



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



Task 5.1.3 - Configure Resource Mappings

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

vmw Site Recovery vc-I-01a.vcn.ninja.loo	cal - vcenter.sddc-44-235-221-106.vmwarevmc.com V
Site Pair Replications Prote	ection Groups 📃 Recovery Plans
Summary	Resource Mappings
Issues	vc-I-01a.vcn.ninja.local vcenter.sddc-44-235-221-106.vmwarevmc.com
✓ Configure	2 _{New}
Replication Servers	vc-I-01a.vcn.ninja.local
✓ Array Based Replication	
Storage Replication Adapters	
Array Pairs	
Network Mappings	
Folder Mappings	
Resource Mappings	Y
Storage Policy Mappings	
Placeholder Datastores	
> Advanced Settings	
Permissions	
Recovery Plans History	
vSphere Replication reports	EXPORT ~

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

New Resource Mappings	Recovery resources \times Configure recovery resource mappings for one or more resources. The mappings for objects marked with * are already
1 Recovery resources	created or prepared.
 Reverse mappings Ready to complete 	Q Search ♥ @ vc-l-01a.vcn.ninja.local ♥ @ shinobi-On-Prem DC ♥ @ 192.168.110.151 ♥ @ Shotoku Compute01 ♥ @ Shotoku Mgmt&Edge Image: Shotoku Mgmt&Edge Image: Vc-l-01a.vcn.ninja.local V @ Search Image: Vc-l-01a.vcn.ninja.local Vc-l-01a.vcn.ninja.local Vc-l-01a.vcn.ninja.local Vc-l-01a.vcn.ninja.local Vc-l-01a.vcn.ninja.local Vc-l-01a.vcn.ninja.local Vc-l-01a.vcn.ninja.local Vc-l-01a.vcn.ninja.local Vc-l-01a.vcn.ninja.local Vc-l-01a.vcn.ninja.local
	0 mapping(s)

Task 5.1.4 - Storage Policy Mapping

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



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

New Storage Policy Mappings	Recovery storage policies Configure recovery storage policy mappings for one or more st	orage policies.
1 Creation mode	Ge Management Storage Policy - Single Node Ge Management Storage Policy - Stretched	Game Management Storage Policy - Single Node Game Management Storage Policy - Stretched
2 Recovery storage policies	Anagement Storage policy - Thin	🔿 🕞 Management Storage policy - Thin
3 Reverse mappings	🚺 🗷 🔓 Shinobi Default Storage Policy	C 🔓 VM Encryption Policy
4. Desetute controlate	VM Encryption Policy	2 G VMC Workload Storage Policy - Cluster-1
4 Ready to complete	SAN Default Storage Policy	🔍 💿 🕞 vSAN Default Storage Policy
	VVol No Requirements Policy	🔿 🕞 VVol No Requirements Policy
		APPINGS
	vc-l-01a.vcn.ninja.local y vce	enter.sddc-44-235-221-106.vmwarevmc.com
	🔓 Shinobi Default Storage Policy	vSAN Default Storage Policy
		1 mapping(s)
		CANCEL BACK NEXT

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

New Storage Policy Mappings	Reverse Select config	mappings ured mappings for which to automatically creat	e reverse map	pings. This might overwrite existing m	appings.
1	1 vcente	er.sddc-44-235-221-106.vmwarevmc.com	↑ Ţ	vc-l-01a.vcn.ninja.local	T.
1 Creation mode		AN Default Storage Policy		🕞 Shinobi Default Storage Policy	
2 Recovery storage policies					
3 Reverse mappings					
4 Ready to complete					
	F 1				America (A)
					2 1 mapping
				CANCEL BACK	NEXT

Task 5.1.5 - Placeholder Datastores

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



3. Select WorkloadDatastore

4. Click ADD

Place	eholder Datastores			Learn more 🗗
vc-l-	01a.vcn.ninja.local vcenter.sddc-52-28-33-169.vmwarevmc.com			
NEW	REMOVE		SELECT ALL	CLEAR SELECTION
	Name	↑ ▼ Host/Cluster		Ŧ
	🗐 ma-ds-52330a3a-a7e498b9-9c7c-eab16b28abf0	10.101.14.24		
	G WorkloadDatastore	Cluster-1		
-				

Task 6 - Setup Replication

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

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

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

vm vSphere Client Menu ∨ Q Sear	rch in all environments	
	🖧 vm-01a 🍄 💷 🦉	B to Actions ∨
V 🗗 vc-l-01a.vcn.ninja.local	Summary Monitor Config	gure Permissions Datastores Networks Snapsh
 Shinobi-On-Prem DC Shotoku Compute01 esxicomp-01a.vcn.ninja.local Planespotter app-01a db-01a On-Prem-to-VMC-IX-I1 On-Prem-to-VMC-NE-I1 On-Prem-to-VMC-WO-I1 	Powered On Launch web console Launch remote console	Guest OS: SUSE Linux Enterprise 11 (64-bit) Compatibility: ESXi 5.0 and later (VM version 8) VMware Tools: Not running, version:10357 (Upgrade available) MORE INFO DNS Name: IP Addresses: esxicomp-01a.vcn.ninja.local
wm-01a	A newer version of VMware T	ools is available for this virtual machine.
i web-02a ✓ [] Shotoku Mgmt&Edge	VM Hardware	^
esxi-01a.vcn.ninja.local	> CPU	1 CPU(s)
🖆 en-01a 🗗 srm-I-01a	> Memory	0.5 GB, 0 GB memory active
🗗 vr-l-01a	> Hard disk 1	2 GB
> 📋 192.168.110.151	> Network adapter 1	vm-sea (connected)

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

Vmw Site Recovery vc-l-01a.	vcn.ninja.local - vcent	ter.sddc-44-235-221-106.	vmwarevmc.com ∨		
Site Pair Replications	Protection Gro	Recovery P	lans		
Outgoing	Ø v	vc-l-01a.vcn.ninja.l	ocal → 🗗 vcenter.sdo	dc-44-235-221-106.vi	mwarevmc.com
Incoming		<i>v</i>			
		Virtual Machine	↑ ⊤ Status	⊤ Target	т
					\bigtriangledown
					ц Ф
		EXPORT ~			
Recent Tasks Alarms					

8. On the Virtual Machines page Select vm-01a

9. Click **Next**

Configure Replication - vm-01a	Virtual machines Select the virtual machines that you want to	o protect. Already replicated VMs are n	ot shown in this list.					
1. Target site	All Selected (1)							
i Target site	Name 1	T VM Folder	T Compute Resource T					
2 Virtual machines	📄 🖶 app-01a	🗖 Workload VMs	📋 Shotoku Compute01					
	🗌 🖶 db-01a	Workload VMs	📋 Shotoku Compute01					
3 Target datastore	🗌 🖶 en-01a	🔄 Shinobi-On-Prem DC	📋 Shotoku Mgmt&Edge					
4. Doplication sottings	🗌 🖶 On-Prem-to-VMC-IX-I1	HCX VMs	📋 Shotoku Compute01					
4 Replication settings	On-Prem-to-VMC-NE-I1	HCX VMs	📋 Shotoku Compute01					
5 Protection group	📄 🖶 On-Prem-to-VMC-WO-I1	HCX VMs	📋 Shotoku Compute01					
	📄 🖶 Planespotter App	🔀 Planespotter	🔡 Planespotter					
6 Ready to complete	📄 📑 Planespotter Redis	器 Planespotter	🔀 Planespotter					
	📄 🖶 Planespotter Web	器 Planespotter	🔀 Planespotter					
	📄 🖶 srm-I-01a	MGMT VMs	📋 Shotoku Mgmt&Edge					
	🗌 🖶 Tiny-Linux	🗂 Workload VMs	📋 Shotoku Compute01					
	1 🔲 🖶 VCLS (3)	CLS	📋 Shotoku Compute01					
	🗹 🗗 vm-01a	Workload VMs	📋 Shotoku Compute01					
	1	·	1 - 13 of 16 VM(s) < < 1 / 2 → >					
			CANCEL BACK NEXT					

10. On the Target Datastore page Select WorkloadDatastore

11. Click Next

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

Configure Replication - vm-01a	Target datastore Select a datastore for the replicated files.	Configure da	X
1 Target site 2 Virtual machines	Virtual machine 'vm-01a' is currently using 467.17 MB. Disk format: Same as source VM storage policy: Datastore Default VM storage policy: Datastore Default VM storage policy: Datastore Default	coningure da	
3 Target datastore	Name A v Canacity	Eree	Type
4 Replication settings	maine r capacity	500 TB	VMFS
5 Protection group 6 Ready to complete	• WorkloadDatastore 10.37 TB	9.19 TB	vsan
	 Select seeds Auto-include new disks in replication ¹ 		2 datastore(s)
		CANCEL	BACK

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

Configure Replication - vm-01a	Protection group × You can add these virtual machines to a protection group.
1 Target site 2 Virtual machines	 Add to existing protection group Add to new protection group Do not add to protection group now
3 Target datastore	
4 Replication settings	
5 Protection group 6 Ready to complete	
	CANCEL BACK NEXT

Task 6.1 - Create a Protection Group

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

vmw Site Recovery vc	:-I-01a.vcn.ninja.local - vcenter.sdd	ic-44-235-221-106.vmwarevmc.co	m ~	С	¢	?	Administra
Site Pair Replicati	ion Protection Groups	Recovery Plans					
Q Search	Protection Groups						
Protection Groups	2 NEW						
	Name	↑ T Protection Status	▼ Recovery Status ▼	Protection	Туре	Ŧ	Protected Site
			\bigtriangledown				
	EXPORT ~						
Recent Tasks Alarms							
Task Name T	Target T	Status T	Initiator T	Queued For	Ŧ	Start Tim	e ↓ _▼

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

New Protection Group	Name and dire	ection ×
1 Name and direction	Name:	VM-PG 1 75 characters remaining
2 Туре	Description:	
3 Datastore groups		
4 Recovery plan		4096 characters remaining
5 Ready to complete	Direction:	 Student20-On-Prem → srm.sddc-44-235-221-106.vmwarevmc srm.sddc-44-235-221-106.vmwarevmc → Student20-On-Prem
	Location:	Q Search
		Protection Groups
		CANCEL 2 NEXT

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



Task 6.2 - Create Recovery Plan

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

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

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

vmw Site Ree	covery	vc-l-01a.v	rcn.ninja.local - vcenter.sd	dc-44-235-221-106.vm	nwarevmc.com ∨			С	¢	?	Administrator@
Site Pair	Replica	ations	Protection Groups	Recovery Plar	ns						
Q Search		Ree	covery Plans								
Recovery Plans		2 NE	w								
			Name			ΎT	Status		т	Protected Site	Ŧ
						~	7				
			EXPORT ~								
Recent Tasks	Alarms										

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

Create Recovery Plan	Name and direction	n ×
1 Name and direction	Name:	VM-RP
2 Protection Groups	Description:	
3 Test Networks		
4 Ready to complete		4096 characters remaining
	Direction:	 Student20-On-Prem → srm.sddc-44-235-221-106.vmwarevmc srm.sddc-44-235-221-106.vmwarevmc → Student20-On-Prem
	Location:	Q Search Recovery Plans
		CANCEL NEXT

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

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

Create Recovery Plan	Protection Groups	\times
1 Name and direction	Protection groups for individual VMs or datastore groups Storage policy protection groups	
2 Protection Groups	All Selected (1)	
3 Test Networks	Name T Description T	
4 Ready to complete	VM-PG	
	2 1 1 group(s)	
	CANCEL BACK NEXT	r -

Task 7 - Run a Disaster Recovery Plan

- Log into your VMC on AWS SDDC vCenter. NOTE: The URL and credentials can be found on the Settings tab of the VMC Console
- Confirm that there a a placeholder VM (ghost vm) for vm-01a (expand cluster 1 > compute RP)

NOTE: This VM cannot be powered-on. To bring the replicated VM(s) online you have to execute an SRM

Planned Migration or Disaster recovery execution

vm vSphere Client Menu N	Q Search in all env	ironments	(<u>?</u> ? ~	cloudadmin@vmc.loc	al V
vcenter stick_44-235-221-106 vmwar	Summary Monitor	Configure Permissions Datastores Networks	Snanshots			
Vcenter.sdoc.44-255-221-106.VmW4r SDDC-Datacenter Cluster-1 10.120.2.4 Compute-ResourcePool Planespotter MySQL Planespotter MySQL @ Vm-Ola webserver01 @ webserver02 @ win10-desktop @ win10-desktop @ wordpress @ Mgmt-ResourcePool	Powered Off LAUNCH WEB CONSOLE LAUNCH REMOTE CONSOLE	Guest OS: SUSE Linux Enterprise 11 (64-bit) Compatibility: ESXI 5.0 and later (VM version 8) VMware Tools: Not running, not installed MORE INFO DNS Name: IP Addresses: Host: 10.120.2.4 Managed By: description ID DETAILS	Shapshots		SWITCH T	O NEW VIEW PU USAGE) HZ HEMORY USAGE) B TORAGE USAGE) B
10.120.14.24	▲ There is no network as	signed to this virtual machine.				Edit Settings
	VM Hardware	~	Notes			^
	Related Objects	^ E	Edit Notes			
	Cluster	Cluster-1	Custom Attributes			^
	Host	10.120.2.4	Attribute	Va	alue	
	Resource pool	Compute-ResourcePool				
cent Tasks Alarms						*

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



8. In the **Confirm Operations** page

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



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

(This is the windows desktop you deployed into the SDDC in lab 2).



Task 8 - Reprotect

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

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

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

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

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





Conclusion



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

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