Adam Sandberg

ITAS 267 – Assignment 1

2023-01-24

Assignment 1 (15%) - DR Strategies with VMware SRM (Site Recovery Manager)

Table of Contents

YouTube Link: https://youtu.be/j1DCZg0in5o

Introduction

In this lab, we will use VMware's Replication & Site Recovery Manager (two separate products) to write and configure a Disaster Recovery (DR) strategy with a 5-minute Recovery Time Objective (RTO) and test and execute the plan using the VMware Site Recovery Manager software. We will deploy and configure a "Protected Site" named PHOENIX (Our student ESXi tower) and a "Recovery Site" named LIVERPOOL (A Virtual ESXi VM on our tower) and document and demonstrate all aspects of the project. The lab will test our understanding of highly available systems design and disaster recovery scenarios and requires the use of best practices learned in class and found online. Our goal is to show the ability to recover critical systems in a given time in case of a disaster.

Part 1 - Install VM Replication and SRM Appliance

Installing a VM replication appliance is a straightforward process that can be completed in a few steps. This appliance allows you to replicate virtual machines to a remote site, ensuring continuity and disaster recovery. Before beginning the installation, make sure you have all the necessary hardware components and have prepared the target environment. Here are the basic steps to follow to install your VM replication appliance:

1. Using the vCenter web appliance, right click on the Datacenter and press “Deploy OVF template.”
2. Select these 3 files shown in the figure below and press next.

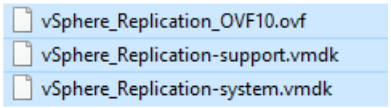

Figure 1 ovf Files

3. Choose the location and the name then press next.
4. Choose your ESXi host as the compute source and press next.
5. Review details and press next. Accept agreement and press next.
6. In configuration choose 2 or 4 vCPUs. Press next.
7. Choose your datastore, choose thin provision and press next.
8. Select your network and press next.

9. In the customize template page, enter a password for root and admin accounts. Then enter the ip address if using static and choose the domain name. Click next.

Ready to complete
Click Finish to start creation.

Provisioning type	Deploy from template
Name	VM Rep App
Template name	vSphere_Replication_OVF10
Download size	779.3 MB
Size on disk	1.7 GB
Folder	Datacenter
Resource	as-liverpool.as
Storage mapping	1
All disks	Datastore: datastore1; Format: Thin provision
Network mapping	1
Network 1	VM Network
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual

Figure 2 Ready to Complete

10. Review the details and press finish.
11. 11 Repeat steps 1 – 10 for the vMware SRM install. The process is the exact same just use the different ISO and a different IP and FQDN.

Note: vCenter servers will need this software so part 4 will be completed for both sites.

Part 2 – Configuring VMware SRM and vRep

Now that the appliances are setup, we need to configure them to work with our sites. To begin part 5 these steps will be used for both sites. But keep in mind proper domain names and IP addresses during the process.

1. Log into the SRM management page. Click summary then click “Configure Appliance”
2. It will ask for your “PSC” enter your appropriate vCenter server domain name.

Enter the Platform Services Controller details for the vCenter Server for which you want to configure Site Recovery Manager.

PSC host name vCenter.AS-Phoenix.as

PSC port 443

User name administrator@asp.local

Password ••••••••••••••••

Note: If prompted, you must accept the certificate for the configuration to proceed.

Figure 3 PSC Setup

Enter the password, press next and accept the certificate.

3. Select the vCenter server you want to configure, press next.
4. Enter your site name, either Phoenix or Liverpool. Then enter and Admin email. Press Next.

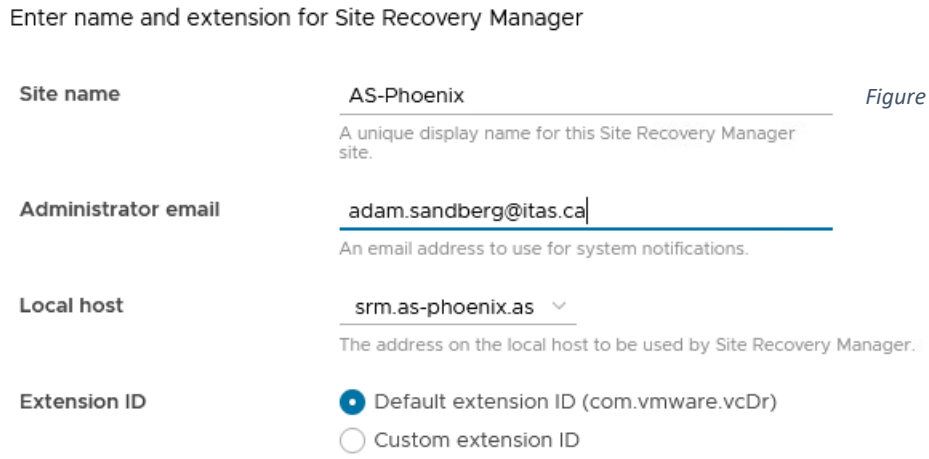

Figure 4 Enter Name for Site

5. Look over the ready to complete page and press finish. The appliance will take a few minutes to configure.

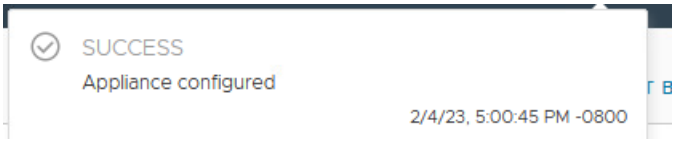

Figure 5 SRM Configured

6. Now that the SRM applications have been registered to there respective vCenter servers. Its time to configure the VRMS appliance. Navigate to the management site and press “Configure Appliance”
7. Same as before, enter the FQDN of your vCenter server and enter the administrator credentials.

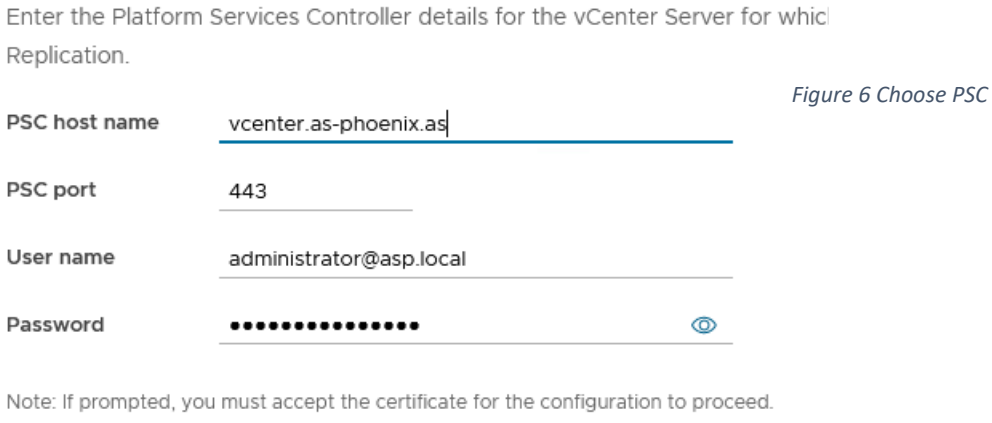

Figure 6 Choose PSC

Press next and accept the cert.

8. Click next on the vCenter server screen.

9. Choose a site name and enter your admin email. Press next.

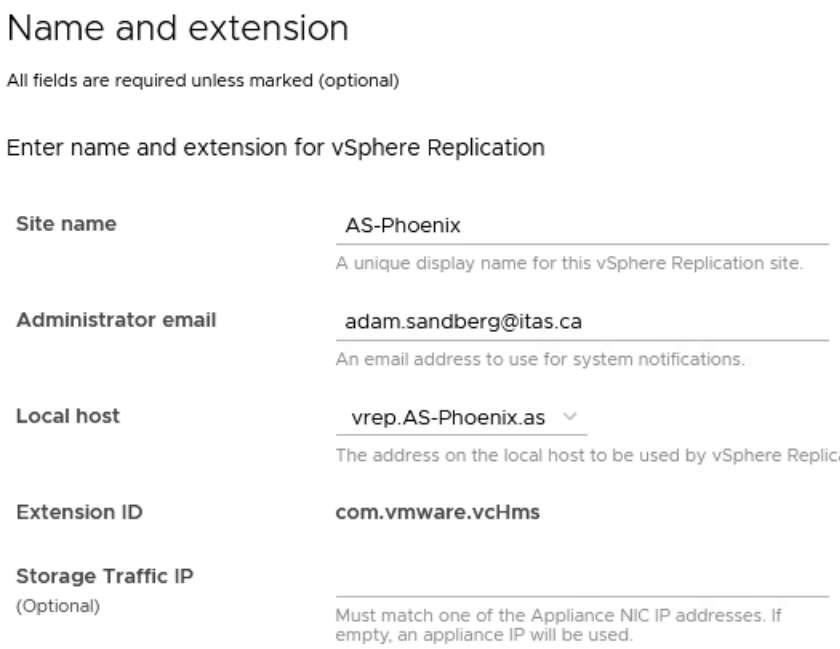

Figure 7 Site Name

10. On the ready to complete page look over the details and press finish.
11. Now that the 4 sites have been registered to our vCenter servers. Its time to make the Protection rules and zones.

Part 3 - Set up a Protection group and Recovery plan

A Protection Group and Recovery Plan will be set up using VMware SRM and VRMs, allowing for the replication and recovery of virtual machines in the event of a disaster.

1. To begin, open the vCenter web page for the Phoenix site. Navigate to the menu then select "Site Recovery".
2. Click "Open Site Recovery" here we will add our protected VM's.

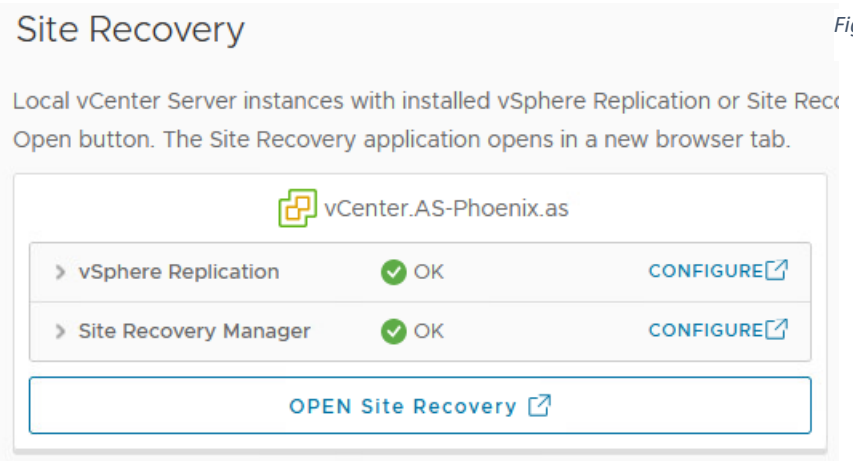

Figure 8 Site Recovery.

3. Click new site pair then enter the FQDN and credentials of the Liverpool site. Click next.

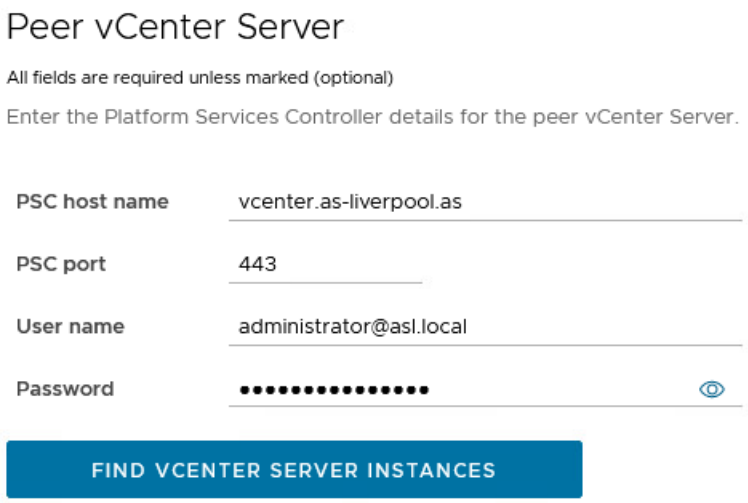

Figure 9 Peer vCenter Server.

4. Choose both available services and press next.

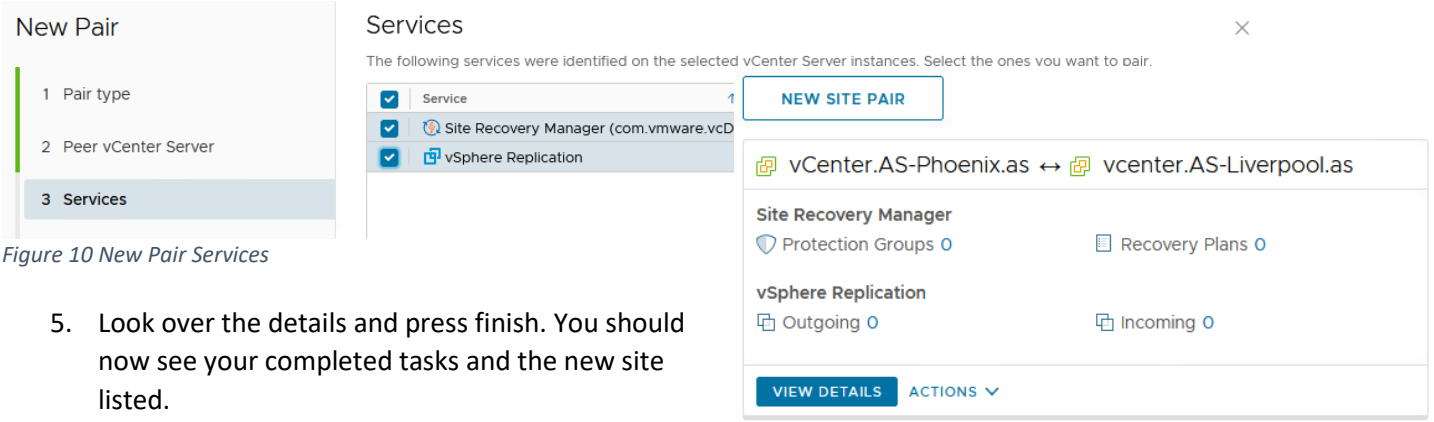

Figure 10 New Pair Services

5. Look over the details and press finish. You should now see your completed tasks and the new site listed.
6. Now that are sites are paired, some resource mapping needs to be done. In the site pair tab. Click Network Mappings and press “New”.
7. Choose the default setting on the first page and press next.

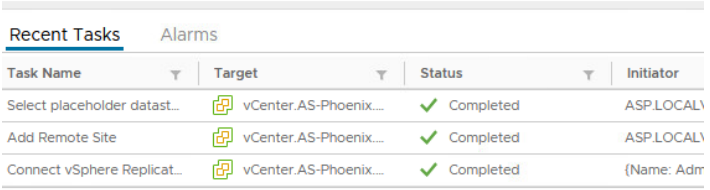

Figure 11 New Site Pair

8. On the recovery networks page. Choose the VM Network from each site and then press “Add Mappings”. Click next.

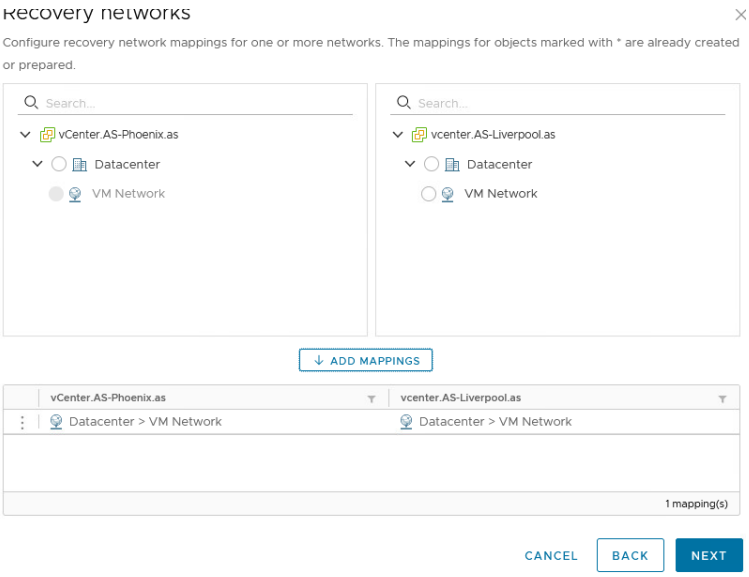

Figure 12 Add Mappings (Network)

9. In the reverse mapping page choose your newly created mapping and press next.

10. On the test network screen press next. Then press Finish.

11. Now click folder mapping – New. This is similar to the network mapping.

12. Choose “Prepare mappings manually” then press next.

13. Select the created mappings in the reverse page and press next, then finish.

14. Now press the “Resource Mapping” icon and press new.

15. In recovery resources choose both ESXi Servers. Press “Add Mappings” then click next.

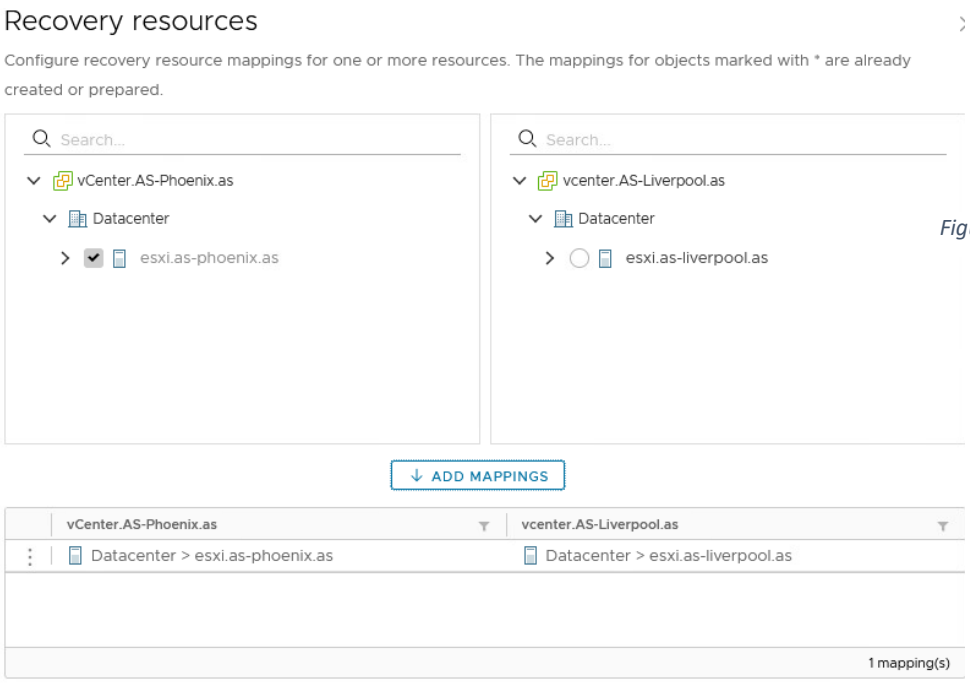

Figure 13 Recovery Resources

16. Choose the mapping in the reverse section and press next, then finish.

Configure VM replication

1. Now that the resources have been mapped. Navigate to the “Replications” tab and press “New”. Note that it is either outgoing or incoming before pressing new. This is the Phoenix to Liverpool replication so my DC/DNS and two file servers will be included in this replication plan.
2. In the target site leave it as default and press next.
3. On the Virtual Machine page, select your VM,s that will be replicated. In this case since its Phoenix to Liverpool, my file servers and DC will be chosen. Press next.

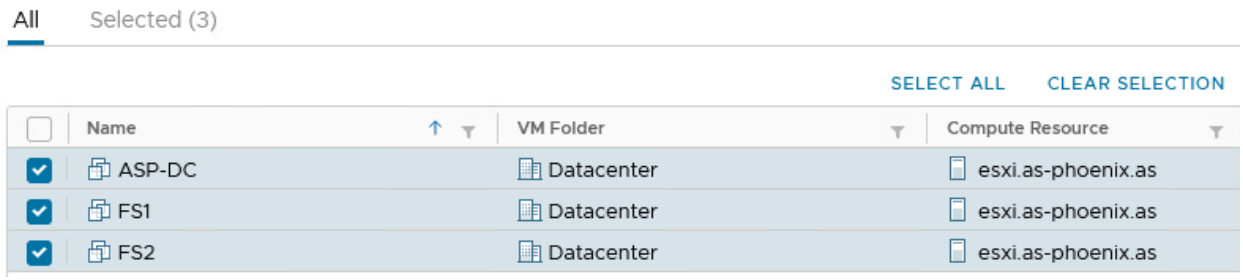

Figure 14 Select VM's

4. In the Datastore page, accept the defaults and ensure your main Datastore is selected. Press next.

5. On the Replication Settings page, click to enable point in time instances. Change it to 2 instances per day for the last 3 days. Click to enable quiescing and network compression for VR data. Click next.

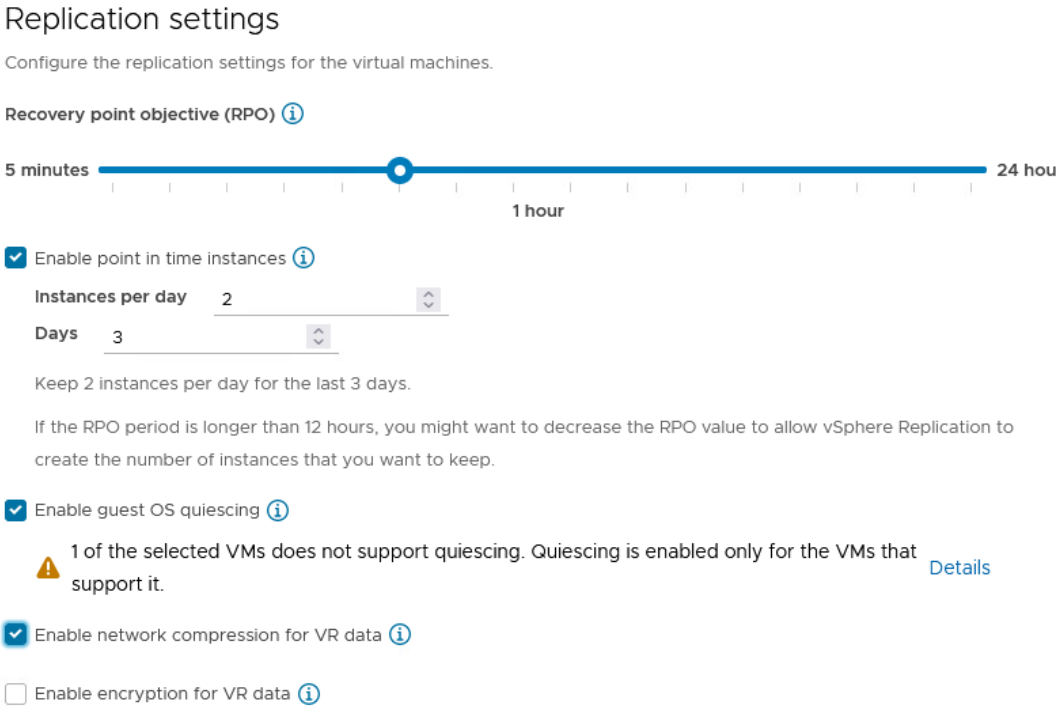

Figure 15 Replication Settings

6. On the protection group choose to not add it one now and press next.
7. Review and click finish.
8. You can click on the replications tab to see the new replications present.

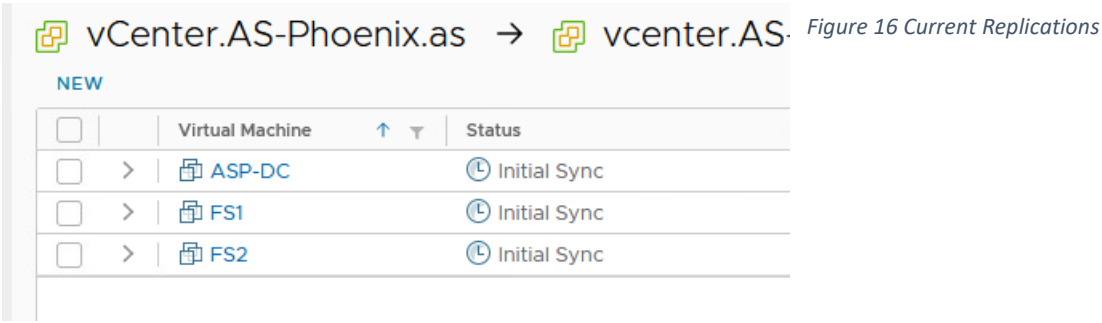

Figure 16 Current Replications

Steps 1 – 8 will need to be done again except it will be for the singular DC from Liverpool to Phoenix.

Protection Group & Recovery Plan

Now that the replication rules have been made, we need to make a Protection Group and a recovery plan.

1. Click the protection group tab. Then select “New”

2. Enter the name and direction of the group. There will be two groups, 1 for each direction. Below is my single DC from the Liverpool site that will go to the Phoenix site. Click next.

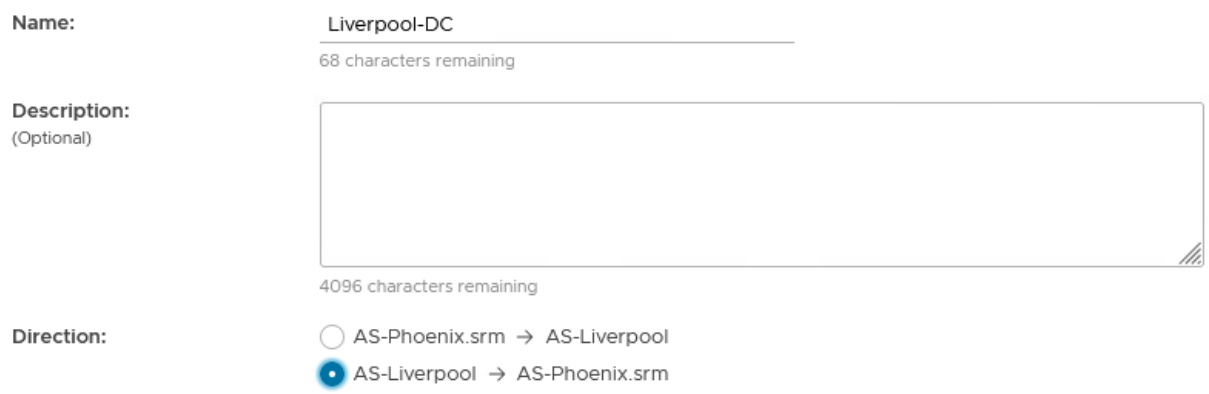

Figure 17 Protection Group Settings

3. On the "Type" page, choose "Individual VMs" and select the required VMs depending on the direction you chose. Click next.
4. On the "Recovery Plan" page choose to create new plan. Name it accordingly and press next.
5. You will complete steps 1-4 for both sites and will have two protection groups, and two recovery plans. See below.

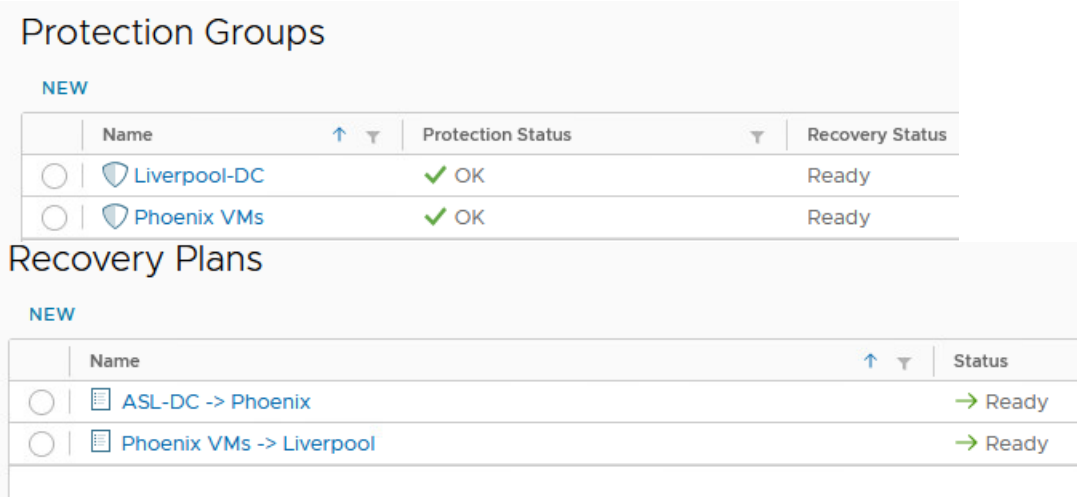

Figure 18 Protection Groups and Recovery Plans

Now we need to configure the Recovery Plan steps.

6. Go to the Recovery Plans tab and choose the Phoenix to Liverpool plan. Since this plan has 3 VMs. Let's set the Domain Controller to have the highest priority and start up first.
7. Go to virtual machine tab, click on the dc and press the priority dropdown menu. Choose 1 (Highest).

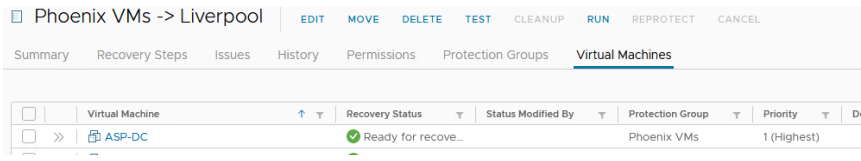

Figure 19 VM Priority.

That concludes the Recovery Plans. Now your recovery environment is complete.

Testing Recovery

In the Recovery Plans tab, you can choose any plan you have and press “Test” this is highly recommended to do before any large-scale implementation.

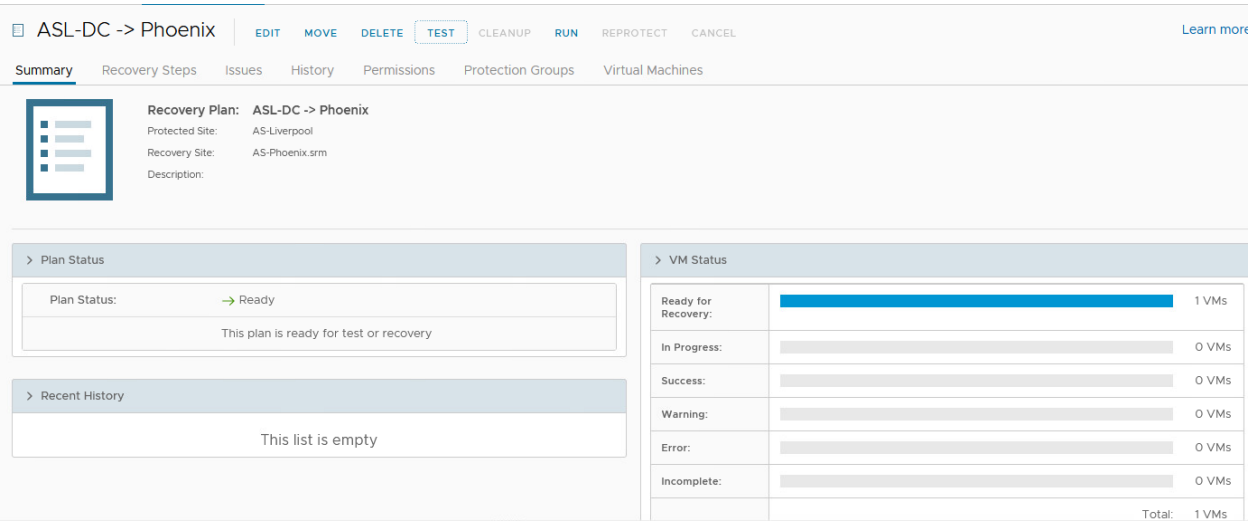

Figure 21 Test Recovery Plan.

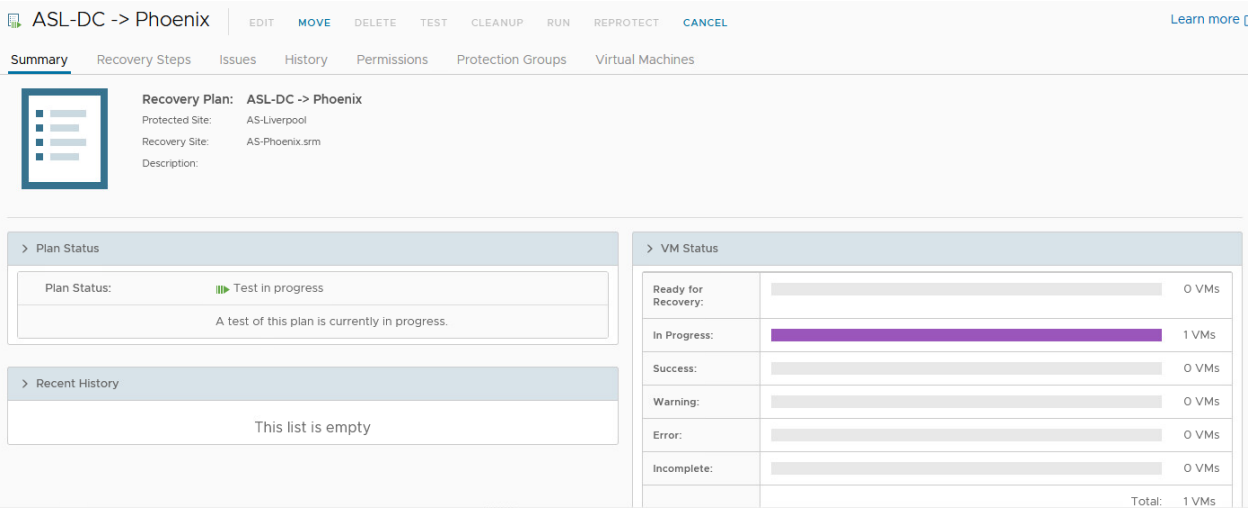

Figure 20 Test in Progress

You can follow along and see if the test is successful.

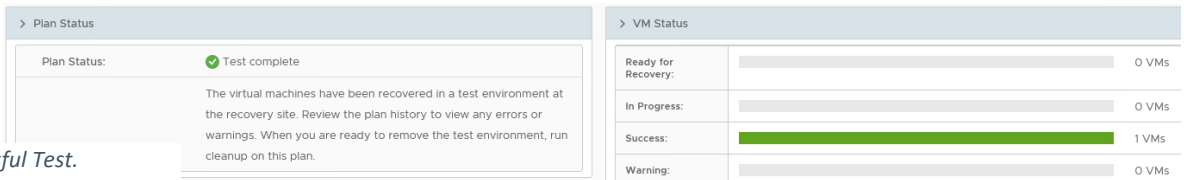

Figure 22 Successful Test.

After the test has been completed, run the cleanup. The cleanup will remove the VM and reset the plan to a ready state.

Conclusion

In conclusion, this lab provided a comprehensive hands-on experience in installing, configuring, and testing disaster recovery solutions using VMware technologies like vCenter Server, vSphere Replication, Site Recovery Manager, and Windows Failover Clustering. It emphasized the importance of backup and recovery strategies in ensuring the availability and accessibility of critical data and services in the event of an unexpected disaster. The lab also demonstrated the power of these technologies in enabling seamless migrations and failovers with minimal disruption to the end-users. The detailed network topology diagrams and IP tables, along with the video demonstration, serve as a clear record of the steps taken and the recoveries in action, emphasizing the need for thorough documentation in any enterprise-level deployment. Finally, this lab highlights the significance of proper planning, resource allocation, and testing in the implementation of successful disaster recovery solutions.

IP Tables

AS-Phoenix Site:

Server Name (FQDN)	IP Address
ESXi.AS-Phoenix.as	192.168.58.10
vCenter.AS-Phoenix.as	192.168.58.11
ASP-DC.AS-Phoenix.as	192.168.58.19, 10.58.0.19
FS1-AS-Phoenix.as	192.168.58.41, 10.58.0.41
FS2-AS-Phoenix.as	192.168.58.42, 10.58.0.42
SRM.AS-Phoenix.as	192.168.58.12
vREP.AS-Phoenix.as	192.168.58.13

AS-Liverpool Site:

Server Name (FQDN)	IP Address
ESXi.AS-Liverpool.as	192.168.58.20
vCenter.AS-Liverpool.as	192.168.58.21
SRM.AS-Liverpool.as	192.168.58.22
vREP.AS-Liverpool.as	192.168.58.23
ASL-DC.AS-Liverpool.as	192.168.58.29, 10.58.0.29

Network Diagram

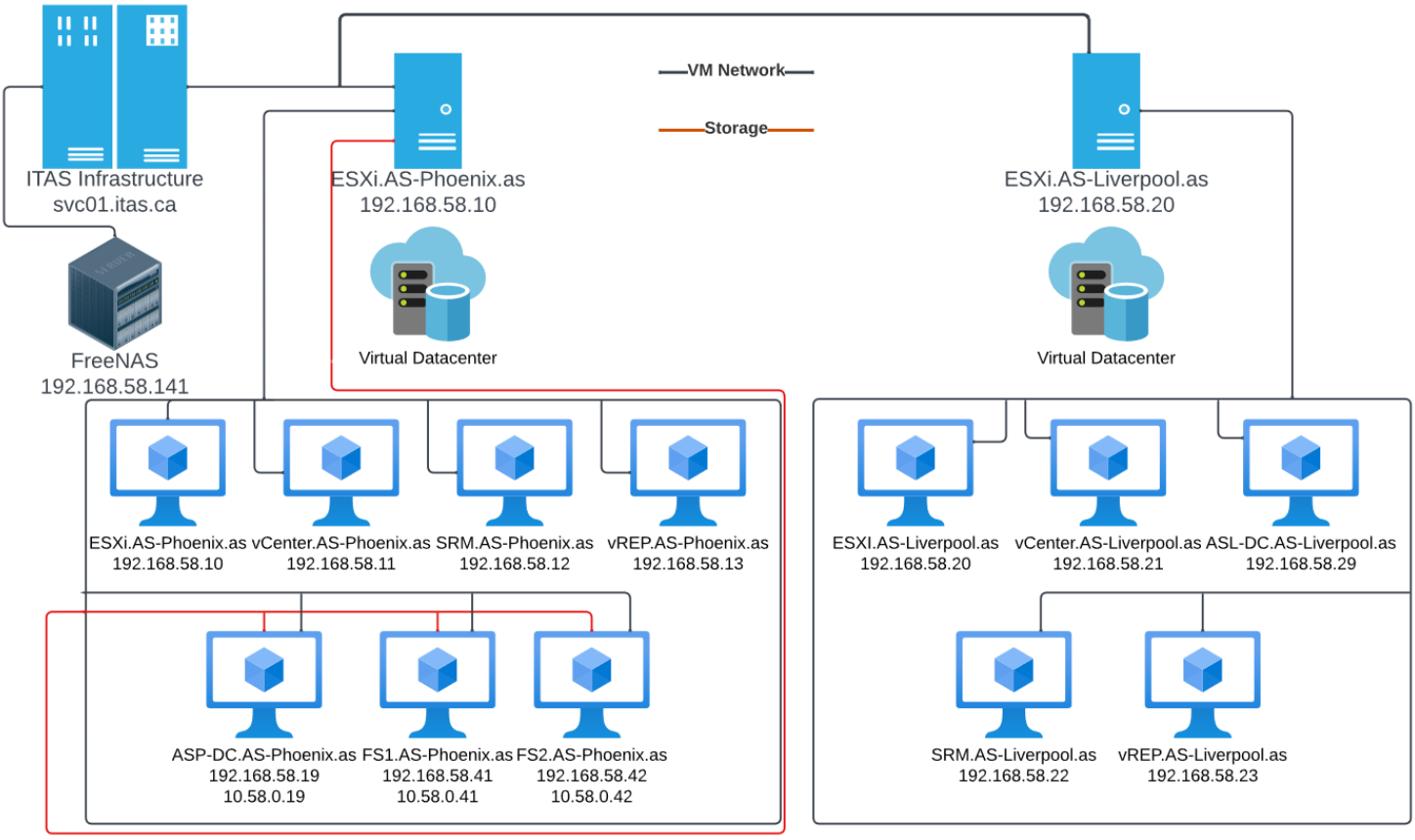

Figure 23 Network Diagram.

References

Altaro, "Site Recovery Manager 8.4 Installation and Configuration," Altaro, www.altaro.com/vmware/site-recovery-manager-8-4/#Site_Recovery_Manager_8_4_Installation_and_Configuration.

VMware Blogs, "SRM Array-based Replication vs vSphere Replication," VMware Blogs, 22 June 2017, blogs.vmware.com/virtualblocks/2017/06/22/srm-array-based-replication-vs-vsphere-replication.

VMware, "vSphere Replication," VMware, www.vmware.com/products/vsphere/replication.html.

VMware, "Getting Started with VMware Site Recovery," VMware, docs.vmware.com/en/VMware-Site-Recovery/services/com.vmware.srmaas.getting_started.doc/GUID-889CD958-1441-4E88-9CB0-FEA53F3F2B1F.html.