St. Cloud State University
theRepository at St. Cloud State

Culminating Projects in Information Assurance | Department of Information Systems

3-2016

Building and Protecting vSphere Data Centers Using Site Recovery Manager (SRM)

Ram Santosh Kodeboyina
St. Cloud State University, kora1401@stcloudstate.edu

Building and Protecting vSphere Data Centers

Using Site Recovery Manager (SRM)

by

Ram Santosh Kodeboyina

A Starred Paper

Submitted to the Graduate Faculty

of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science in Information Assurance

March, 2016

Starred Paper Committee:
Dr. Dennis Guster, Chairperson
Dr. Susantha Herath
Dr. Sneh Kalia

Abstract

With the evolution of cloud computing technology, companies like Amazon, Microsoft, Google, Softlayer, and Rackspace have started providing Infrastructure as a Service, Software as a Service, and Platform as a Service offering to their customers. For these companies, providing a high degree of availability is as important as providing an overall great hosting service. Disaster is always being unpredictable, the destruction caused by it is always worse than expected. Sometimes it ends up with the loose of information, data and records. Disaster can also make services inaccessible for very long time if disaster recovery was not planned properly. This paper focuses on protecting a vSphere virtual datacenter using Site Recovery Manager (SRM). A study says 23% of companies close within one year after the disaster struck. This paper also discusses on how SRM can be a cost effective disaster recovery solution compared to all the recovery solutions available. It will also cover Recovery Point Objective and Recovery Time Objective. The SRM works on two different replication methodologies that is vSphere replication and Array based replications. These technologies used by Site Recovery Manager to protect Tier-1, 2, and 3 applications. The recent study explains that Traditional DR solutions often fail to meet business requirements because they are too expensive, complex and unreliable. Organizations using Site Recovery Manager ensure highly predictable RTOs at a much lower cost and level of complexity. Lower cost for DR. Site Recovery Manager can reduce the operating overhead by 50% by replacing complex manual run books with simple, automated recovery plans that can be tested without disruption. For organizations with an RPO of 15 minutes or higher, vSphere Replication can eliminate up to $10,000 per TB of protected data with storage-based technologies. The combined solution can save over USD $1,100 per protected

virtual machine per year. These calculations were validated by a third-party global research firm. Integration with Virtual SAN reduces the DR footprint through hyper-converged, software-defined storage that runs on any standard x86 platform. Virtual SAN can decrease the total cost of ownership for recovery storage by 50 percent (VMware, n.d.a).

Acknowledgement

The successful completion of this paper could not have been possible without the guidance of my beloved professors, Dr. Dennis Guster and Dr. Susantha Herath. I also would like to thank Professor Sneh Kalia for being part of the committee and finding the time to read my thesis.

I also would like to thank my mother K. Ganga Bhavani, father K V S S V Prasad and friends who were with me supporting me the entire way with whatever was needed.

Table of Contents

Page

List of Tables

Table Page

List of Figures

Figure Page

Chapter I

INTRODUCTION

Introduction

Protecting a datacenter and the important applications and services it houses is a critical task for every organization. A *disaster* is any event that halts business activity on a large scale. A disaster, in terms of IT, can be defined as a complete loss of datacenter services for an extended period of time. Individual component failures, host failures, and service interruptions are not considered disasters by this definition.

VMware offers multiple products which allow organizations to reduce downtime caused by disasters and smaller-scale component failures alike. One such product is Site Recovery Manager, which can allow a company to protect its datacenters against natural disasters as well as providing service continuity during planned maintenance of the primary datacenter. Site Recovery Manager offers two ways of protecting a datacenter. One way is vSphere Replication, which works at a host or server virtual machines level and the second at a storage array level.

The first method is better fit for Tier 2 and Tier 3 applications which has some limitations and the second one can be used for protecting Tier 1 which are business critical applications. This paper focuses on building a vSphere datacenter and protecting it from a disaster using Site Recovery Manager. The Key Features and Capabilities of SRM are—it is VM-centric, policy-based storage, and replication. Replicate in flexible topologies, e.g., from external SAN/NAS to Virtual SAN—no need for matching storage at source and target. Provision and manage replication at the VM level—no more replicating LUNs. Define storage policies to be applied at the destination Virtual SAN Datastore while Configuring (VMware, n.d.a).

Top executives say 10 hours to recovery; IT managers say up to 30 hours. Ninty-three percent of business that lost their data center for 10 days went bankrupt within one year. Source and 43% of companies experiencing disasters never re-open, and 29% close within two years. From the above statements we can understand how critical a disaster recovery plan for a datacenter is (Galante, 2009).

Problem Statement

Are we prepared for everything, every time? Well this question continuously repeats in every organization. Every organization has their own Sensitive Data, Customer Data, etc., in Terabytes and Petabytes. Because of the fast growing technology and advancements, many organizations want to make sure their business continuity and data security are at very high level. This paper solely focuses on how a robust disaster recovery solution can be built using vSphere or Array based replication and Site Recovery Manager. That will make sure the above required continuity and security is higher in availability.

Definition of Terms

DB	Database
DR	Disaster Recovery
DRS	Distributed Recourse Scheduler
FT	Fault Tolerance
HA	High Availability
IT	Information Technology
MSCS	Microsoft Cluster Service
RDM	Raw Device Mapping

RPO	Recovery Point Objective
RTO	Recovery Time Objective
SMP	Symmetric Multi Processing
SRM	Site Recovery Manager
SSO	Single Sign On
UP	Uni-processing
vCenter	Virtural Center Server
VM	Virtural machine
VR	Virtual Replication

Chapter II

BACKGROUND AND LITERATURE REVIEW

Virtualization

Virtualization is a revolutionary technology that transforms hardware into software and allows building and running multiple operating systems as virtual machines on a single server platform (Raido, n.d.).

Virtualization Benefits

Virtualization benefits include increased performance and increased resource utilization, easier backup and recovery options, greater flexibility and scalability, lower Total Cost of Ownership (TCO) and reduced capital and operational costs.

vSphere

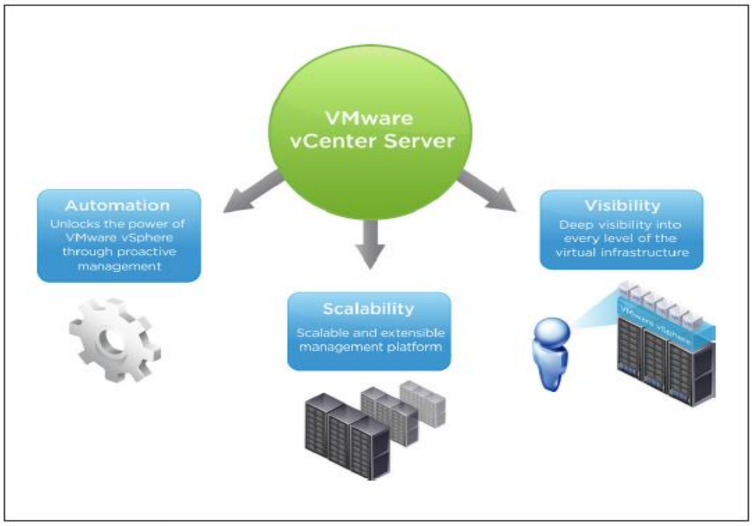
VMware vSphere is a server virtualization product from VMware that allows companies to reduce their capital and operational expenditures. VMware vSphere includes the following technologies; (a) ESXi, (b) vCenter Server, (c) Virtual Networking, (d) High Availability, and (e) Update Manager (WMware, n.d.h).

ESXi

VMware ESXi is a software component which acts as an operating system and enterprise-class hypervisor. ESXi can manage resources from the underlying server hardware and provide them to the virtual machines running on top of it. It facilitates access to the underlying server hardware while ensuring that each VM remains separate from and inaccessible to the others running on the same system (VMware, n.d.d)

vCenter Server

VMware vCenter Server provides centralized administration to vSphere environments. It provides centralized administration of all hosted VMs, as well as additional security and availability features (Gordin, 2015; VMware, n.d.c).


VMware
vCenter Server
Automation
Unlocks the power of VMware vSphere through proactive management
Visibility
Deep visibility into every level of the virtual infrastructure
Scalability
Scalable and extensible management platform

vCenter Server delivers centralized management and proactive management for vSphere virtual infrastructure.

Figure 1. VMware vCenter Server (VMware, n.d.c)

Virtual Networking

A Virtual Distributed Switch (vDS) is created at the datacenter level and acts as a single point of connectivity to all the VMs and other vSphere services present on ESXi hosts (VMware, n.d.f, n.d.j).

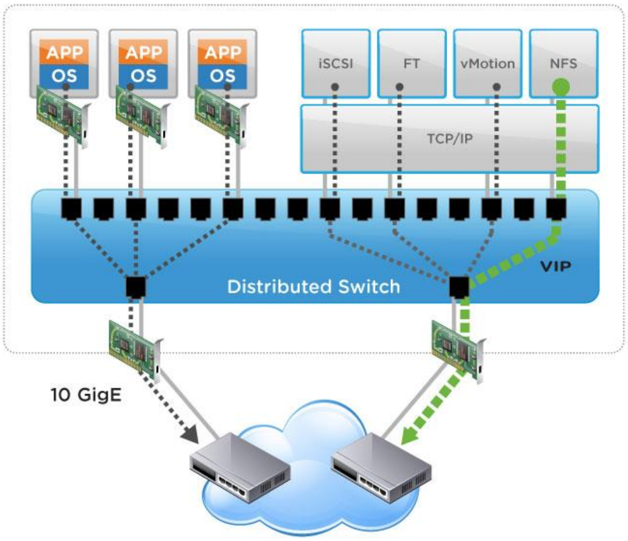


Figure 2. Distributed Switch (VMware n.d.e)

High Availability

High Availability (HA) is a vSphere feature which migrates virtual machines from a failed server to healthy server in the same cluster. It provides services continuity and minimizes downtime for virtualized applications.

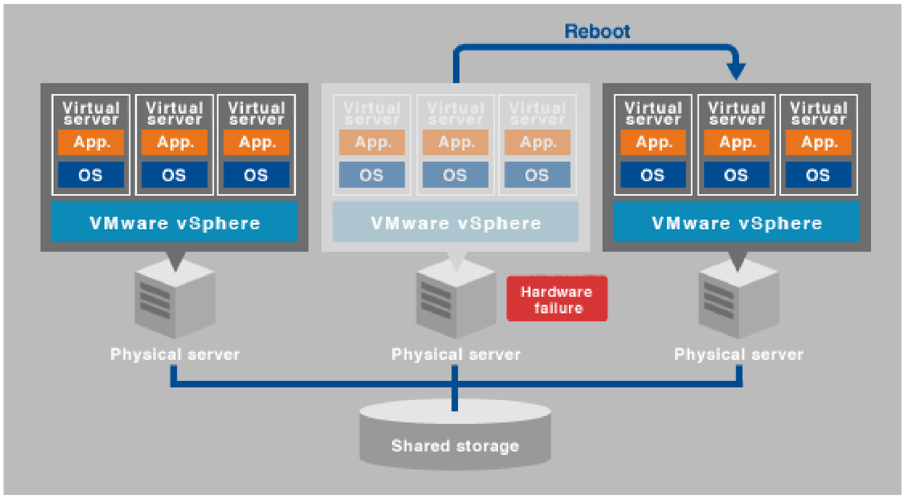


Figure 3: Shared Storage (Listwon, n.d.)

Update Manager

VMware Update Manager is a tool that interacts with vCenter Server, comes as a plugin to vSphere Client, and can be used to patch ESXi servers, virtual machine hardware, and vApps.

Site Recovery Manager

Site Recovery Manager is a disaster recovery product from VMware which can be used to create a disaster recovery site for VMware server infrastructures.

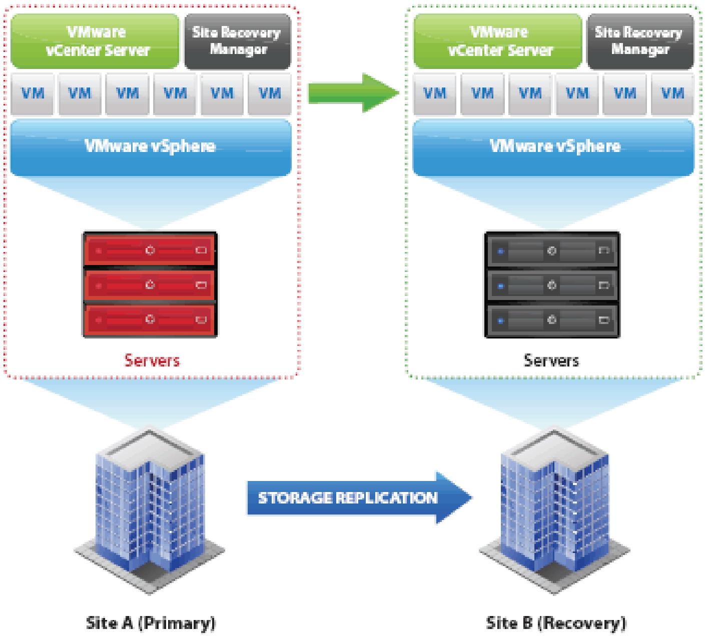


Figure 4. Replication on high level. (Mariusz, 2014)

Recovery Point Objective

Recovery Point Objective (RPO) describes the amount of data loss that is deemed acceptable to an organization. The RPO is the point in time to which you must recover data as defined by your organization. This is generally a definition of what an organization determines is an “acceptable loss” in a disaster situation. The RPO allows an organization to define a window of time before a disaster during which data may be lost. The value of the data in this window can then be weighed against the cost of the additional disaster prevention or loss-prevention measures that would be necessary to reduce or close the window (VMware White Paper, 2009).

Recovery Time Objective

The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. It includes the time for trying to fix the problem without a recovery, the recovery itself, and communication to the end users. In accepted business continuity planning methodology, the RTO is established during the Business Impact Analysis (BIA) by the owner of a process. The RTO attaches to the business process and not the resources required to support the process (VMware White Paper, 2009).

Site Recovery Manager 5.0

VMware vCenter Site Recovery Manager is a business continuity and disaster recovery solution that helps organizations plan, test, and execute a scheduled migration or emergency failover of vCenter inventory between sites. SRM relies on data replication mechanisms, such as array-based or vSphere replication to replicate virtual machines from the protected site to the recovery site. In the event of a failover, SRM coordinates the recovery process with the underlying replication mechanism so that the virtual machines at the protected site can be shut down cleanly (in the event that the virtual machines at the protected site are still available) and the replicated virtual machines can be powered up. Recovery of protected inventory to the recovery site is guided by a recovery plan that specifies the order in which virtual machines are started up (VMware, n.d.g).

Chapter III

METHODOLOGY

Introduction

vSphere Replication duplicates a VMware vSphere infrastructure to an alternate area, inside or in the middle of bunches, and makes that duplicate accessible for reclamation through the VMware vSphere Web Client or through the coordination of a full fiasco recuperation item, for example, VMware vCenter Site Recovery Manager. vSphere Replication secures the virtual machines it protects on a progressive premise. It reproduces to the duplicates just the progressions that are made to the virtual machine. This guarantees that the virtual machine stays secured and is accessible for recuperation from the vSphere Web Client without requiring utilization of an outside apparatus. vSphere Replication is included in all qualified vSphere licenses, extending from VMware vSphere Essentials Plus Kit to VMware vSphere Enterprise Plus Edition. Similarly, as with reinforcements through VMware vSphere Data Protection, securing a virtual machine is a basic capacity of a hypervisor within the datacenter (VMware, n.d.k).

vSphere Replication is managed entirely through components available in the vSphere Web Client. This web-based interface allows centralized administration of all parts of a virtual datacenter, including provisioning, security, and replication tasks. Some replication solutions create unnecessary duplicates of a virtual machine at a remote site without any thought for the consistency of the application data inside the virtual machine. vSphere Replication can help ensure that application and virtual machine data are efficiently and reliably replicated between sites.

How It Works

A solid disaster recovery strategy starts with an array based replication which is the ability to copy the data automatically to a remote site. The result of this is that many storage arrays will have a replication option. This replication option requires one to buy more storage hardware and, hence, most of the vendors provide replication free of cost when you purchase more hardware from them. Copying the data from one location to another is called replication. These copies can be performed at sub-file (block or byte) level wherein the smallest blocks of the data are copied from one site to another and most of the today's replication products have this ability which allows for an optimal usage of bandwidth. A better solution for the question 'How to seed and keep a remote DR site up to date?' would be to make the storage system responsible for the movement of data to a DR site. The array based replication also has some negative effects that need to be considered by storage managers before investing in it. But a point to be noted is that the capacity to clear those comes free with the storage array (Crump, 2011).

Array-based Replication works by replicating storage layer and supports vSphere 3.5 to 6.0, with Recovery Point Objective (RPO) 0 up to max supported by vendor like EMC, NetApp, Dell etc. This scales up to 5,000 VMs protected/2,000 simultaneously recoverable per vCenter/SRM pair and supports write order fidelity within and across multiple VMs in the same consistency group.

The replication takes place at the LUN/VMFS or NFS volume level and can be directly configured on storage array. The major requirement in array base replication is that storage replication solution at both sites (e.g., EMC RecoverPoint, NetApp vFiler, etc.) should be similar. Array based replication supports only FC, iSCSI, or NFS storage and the cost depends on replication and snapshot licensing. Deployment is fairly involved and must include storage administration and networking. Application consistency may be supported with the addition of agents to the VM, depending on the kind of array.

It can replicate UP FT protected VMs (once recovered VM is no longer FT enabled), but this does not support SMP FT VMs. The most innovative feature of array based replication is it replicates powered off VMs, Templates, Linked Clones (as long as all nodes in the snapshot tree are replicated as well), and ISOs. This methodology supports physical and virtual mode of RDMs, MSCS cluster, and vApps can be replicated and replication process is not obstructed by the host failure (Khalsa, 2015).

vSphere Replication

Host-based replication is independent of the underlying storage and it works with a variety of storage types including VMware Virtual SANs, traditional SAN and NAS storage, and direct-attached storage (DAS). Unlike many array replication solutions, vSphere replication enables virtual machine replication between heterogeneous storage types. For example, Virtual SAN to DAS, SAN to NAS, and SAN to Virtual SAN. vSphere replication can, of course, replicate virtual machines between storage targets of the same type, such as Virtual SAN to Virtual SAN (VMware, n.d.m).

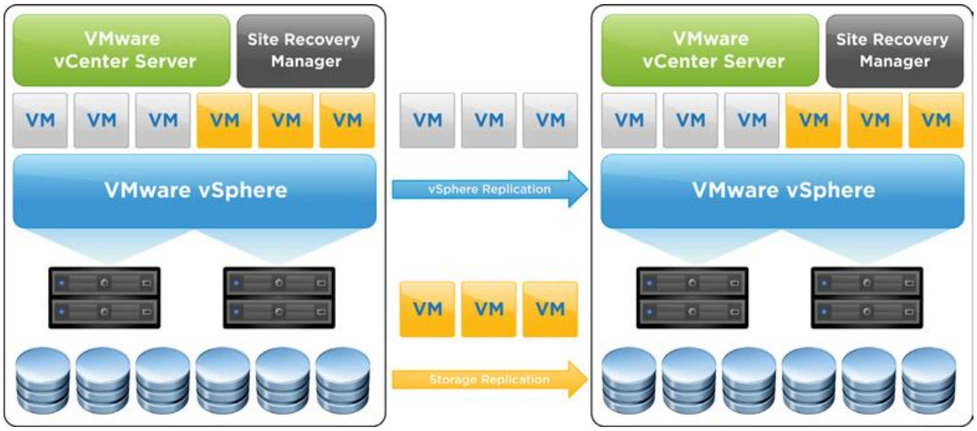


Figure 5. vSphere Replication Mechanism (VMware, n.d.l)

Array Based Replication

Array-based replication is a technology that works at a storage array level. It replicates the contents of storage LUNs between associated sites.

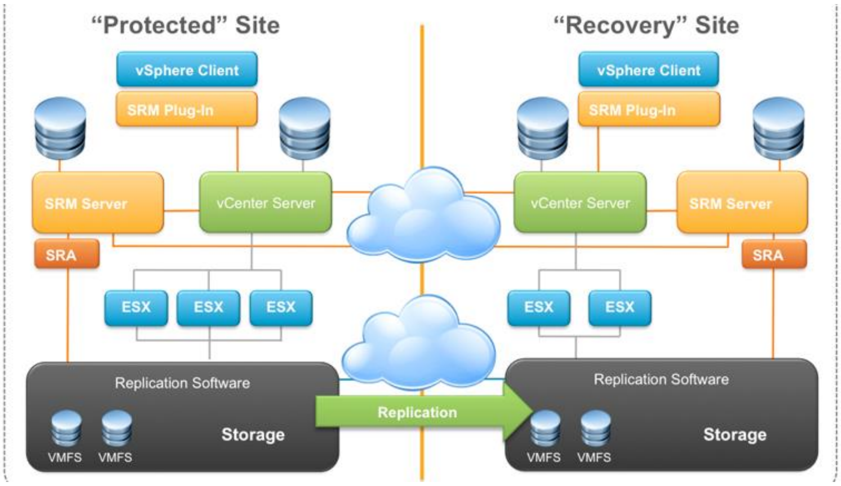


Figure 6. Array based Replication (Viltorious, 2015)

Planned Migration

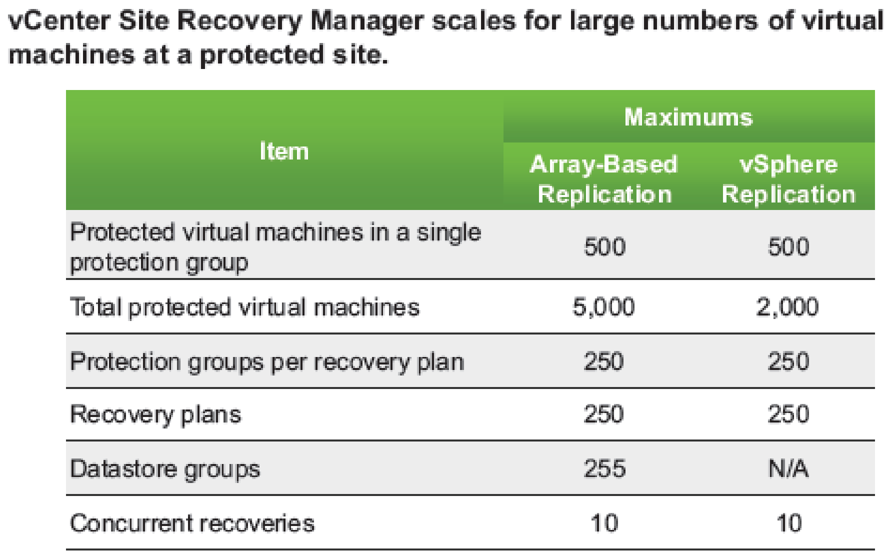
Planned migration is a vCenter Site Recovery Manager workflow that enables application-consistent migration of virtual machine workloads with zero data loss to a recovery site.

Automated Failback

Automated failback provides an automated workflow to migrate virtual machines back to a protected site after it is restored. For obvious reasons, automated failback cannot take place if the protected site is physically lost.

Scalability

Each vCenter Site Recovery Manager Server host supports up to a certain number of virtual machines, protection groups, datastore groups, and concurrent recoveries.



vCenter Site Recovery Manager scales for large numbers of virtual machines at a protected site.

Item	Maximums	
	Array-Based Replication	vSphere Replication
Protected virtual machines in a single protection group	500	500
Total protected virtual machines	5,000	2,000
Protection groups per recovery plan	250	250
Recovery plans	250	250
Datastore groups	255	N/A
Concurrent recoveries	10	10

Figure 7. vCenter Site Recovery Manager Scale (VMware n.d.n)

Various Disaster Recovery Topologies

- **Active-passive:** vCenter Site Recovery Manager supports the traditional active-passive disaster recovery scenario. In this scenario, a production site that is running applications is recovered at a second site that is idle until failover is required. Although this scenario is most common, it requires paying for a disaster recovery site that is idle most of the time.
- **Active-active:** vCenter Site Recovery Manager enables you to leverage your recovery site for other workloads when you are not using the site for disaster recovery. vCenter Site Recovery Manager can be configured to shut down or suspend virtual machines at the recovery site as part of the failover process. This configuration frees up compute capacity for the workloads being recovered (Finke, 2009).
- **Bi-directional:** vCenter Site Recovery Manager provides bidirectional failover protection so that you can run active production workloads at both sites and fail over to the other site in either direction. The spare capacity at the other site is used to run the virtual machines that are failed over.
- **Shared Recovery:** Shared recovery refers to the capability of recovering multiple protected sites (up to a maximum of 10 sites) to a single disaster recovery site. Shared recovery is useful if you are a disaster recovery provider offering disaster recovery services to remote offices or smaller companies.

Hardware and Software Requirements

- Two or more physical servers in each site.
- Two or more ESXi servers: At least one in primary site and one in disaster site.

- Two vCenter servers: one at primary site and one at disaster site.
- Two SRM servers: one at primary site and one at disaster site.
- Two storage arrays capable of array based replication.

vSphere and vCenter Server Requirements

- vCenter Server must be installed at both the protected site and the recovery site.
- VMware ESXi versions 4.x through 5.x are supported.
- VMware vSphere Replication requires ESXi 5 or higher.
- vCenter Site Recovery Manager supports the following vSphere Editions:
    - VMware vSphere Standard Edition
    - VMware vSphere Enterprise Edition
    - VMware vSphere Enterprise Plus Edition
    - VMware vSphere Essentials Plus Kit

vCenter Site Recovery Manager Server Requirements

VMware vCenter Site Recovery Manager Server is supported on the same Microsoft Windows operating systems as vCenter Server. The software requirements are as follows:

- A 64-bit Windows operating system is required.
- A vCenter Site Recovery Manager Server can be a physical server or a virtual machine.
- A 64-bit database source name (DSN) must be created for connecting to the vCenter Site Recovery Manager database.
- The vCenter Site Recovery Manager Server and the vCenter Server must be able to communicate over the network on all required ports.

- A vCenter Site Recovery Manager license is required to bring the server out of evaluation mode.
- The same vCenter Site Recovery Manager license should be installed on the vCenter Server instances at both sites.
- VMware Tools must be installed and updated in all protected virtual machines.
- Storage Replication Adapters (SRAs) must be configured if array-based replication is used.
- A non-replicated datastore is required at each recovery site to store placeholders for virtual machines.

vSphere Replication Agent

The vSphere Replication agent runs on each ESXi host that runs protected virtual machines. The vSphere Replication agent is a native component of an ESXi host and does not require additional installation or configuration.

The agent consists of two components:

- vSphere Replication service
- vSphere Replication filter

The vSphere Replication Service

- Schedules the creation and transfer of blocks modified by guest operating systems.
- Replicates the virtual machine’s metadata files (.vmx, .nvram, .vmxf).
- Stores a virtual machine’s replication configuration in the .vmx file.
- Coordinates group consistency for disks of a virtual machine.

The vSphere Replication Filter

- Attaches to the virtual device and intercepts all I/O to the virtual disk.
- Tracks changed blocks.
- Keeps the replication-specific state for individual disks.
- Transfers data to the vSphere Replication server.
- Implements logic necessary to guarantee data consistency.

Inventory Mappings

Inventory mappings provide a convenient way to specify how resources at the VMware vCenter Site Recovery Manager protected site are mapped to resources at the recovery site. These mappings are applied to all members of a protection group when the group is created (Sam Shouses Blog, 2014).

Resource Mappings

Resource mappings define which compute resources are used at the recovery site when virtual machines are recovered.

Folder Mappings

Folder hierarchies are used to help you organize which virtual machines are only local and which ones come from the protected site. These hierarchies also help you categorize virtual machines by their purpose, their recovery point and recovery time objectives, and other criteria.

High Availability and Disaster Recovery

High Availability has solutions to eliminate risks of a single-point failure by using secondary (redundant) sites or servers in the following ways:

- Real-time synchronization of data.

- Providing a quick response to hardware failures or unplanned outages based on real-time replication.
- Redundant servers.
- Replication over a local network.
- Localized Solution: disk redundancy, server redundancy, network interface and path redundancies, and redundant server power supplies.

Disaster recovery is a method for backing all the files and applications efficiently and making them immediately accessible after an outage or failure. Such an outage or failure can be caused by a natural disaster, power outage, human error, or deliberate attacks on a datacenter. A disaster recovery plan contains procedures and processes to protect resources and ensure quick recovery from an outage.

A Disaster Recovery Solution can be implemented in a physical datacenter or a virtual datacenter using solutions like those fromVMware. Implementing a DR in a physical datacenter presents distinct challenges:

- Requires identical hardware for recovery, which increases design complexity and cost.
- Requires significant amounts of time to orchestrate fail-over and fail-back in the case of an outage.
- Involves a slow and complex recovery process wherein different solutions will be used for different availability tiers and different storage types (Viltorius, 2015, VMware, n.d.f).

Advantages of Virtual Disaster Recovery

- Virtual machines are encapsulated into files, which are portable.
- Virtual machine hardware can be automatically configured.
- Failover and recovery plans can be easily tested.
- The requirement for identical hardware is virtually eliminated.
- Lower overall cost.

VMware High Availability

VMware vSphere High Availability is a feature which can protect virtual machines from unplanned downtime in the case of an ESXi server failure. HA is a cluster-level feature that allows up to 32 ESXi servers (vSphere 5.5) or 64 ESXi servers (vSphere 6) to be placed into a logical cluster. Once HA is enabled on a cluster under vCenter server, fault domain manager (FDM) agents are invoked on all cluster servers and an election process is held to choose a master node.

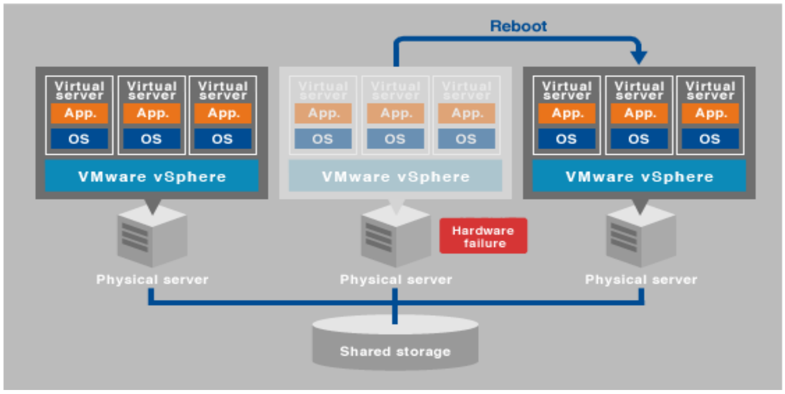


Figure 8. High Availability (Listwon, n.d.)

The master node will initially be chosen based on which one has the most connected datastores. In the case where there are two servers with same number of accessible datastores, vCenter will elect a master node based on the managed object ID (MOID), which is a unique identifier assigned to each ESXi host when it is added to vCenter. Once a master node is elected, the master will start monitoring all the ESXi hosts in the cluster for a failure. If a slave is not responding to the master node with regular “heartbeats,” the slave is considered either dead or isolated. The master node then checks on the datastore heartbeat of the slave and takes an appropriate action on the virtual machines currently running on the failed node.

If a server is dead, the master will simply restart the failed server’s virtual machines on another host in the same cluster. If a slave is still online but isolated for some reason, then the master will check on the host isolation response configured on the cluster and take an appropriate action. The potential responses in the case of an isolated host include leaving the powered-on VMs on the isolated server or, as in the case of a failed host, restarting them on another host.

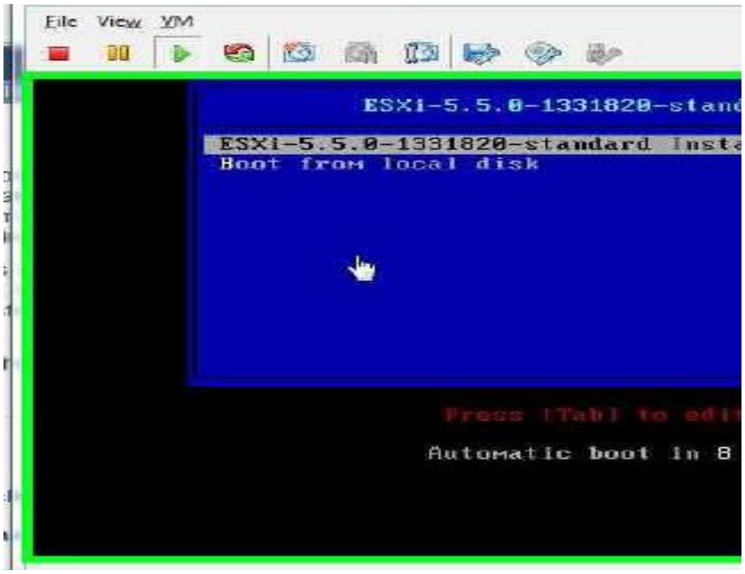
Chapter IV

IMPLEMENTATION

ESXi Installation

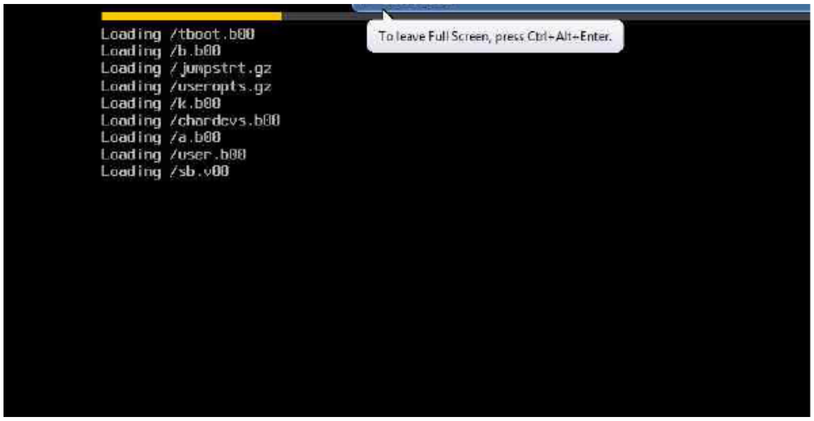
Installing ESXi on a physical server is a fairly straightforward process.

- Insert an ESXi 5.5 installation CD into the server's optical drive. Change the boot order in the system BIOS so that it boots to the optical drive first.



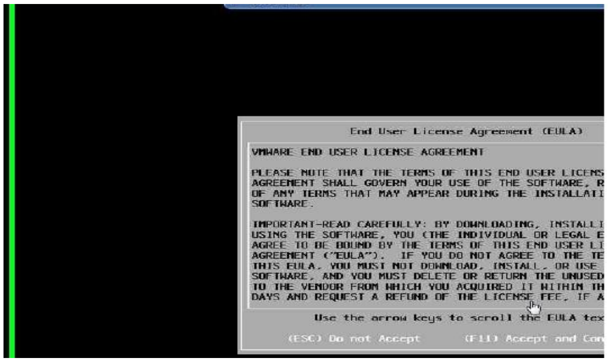
```
            ESXi-5.5.0-1331820-stand

 ESXi-5.5.0-1331820-standard Insta
 Boot from local disk

                         Press [Tab] to edi
                         Automatic boot in 8
```

- Wait 3-5 minutes for the installer to load.


To leave Full Screen, press Ctrl+Alt+Enter.

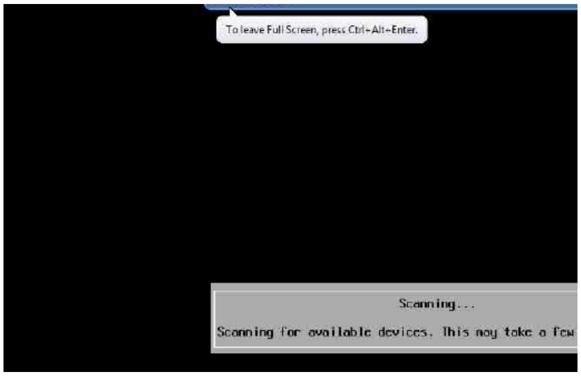
```
Loading /tboot.b00
Loading /b.b00
Loading /jumpstrt.gz
Loading /useropts.gz
Loading /k.b00
Loading /chardevs.b00
Loading /a.b00
Loading /user.b00
Loading /sb.v00
```

- Accept the End User License Agreement.



```
                    End User License Agreement (EULA)
VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENS
AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, R
OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATI
SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLI
USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL E
AGREE TO BE BOUND BY THE TERMS OF THIS END USER LI
AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TE
THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE
SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED
TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN TH
DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF A
            Use the arrow keys to scroll the EULA tex
      (ESC) Do not Accept        (F11) Accept and Con
```

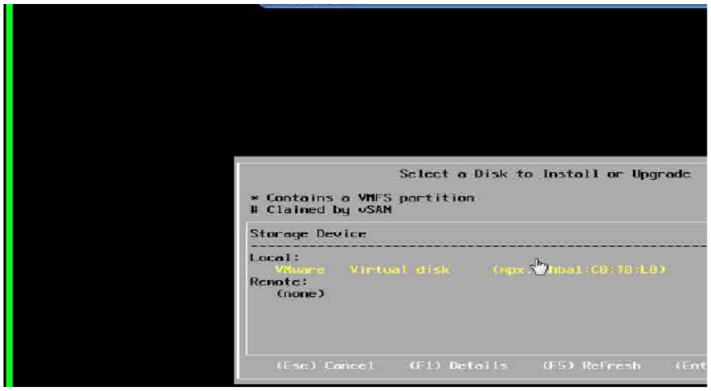
- The installer scans for attached hardware and loads the necessary drivers.



To leave Full Screen, press Ctrl+Alt+Enter.

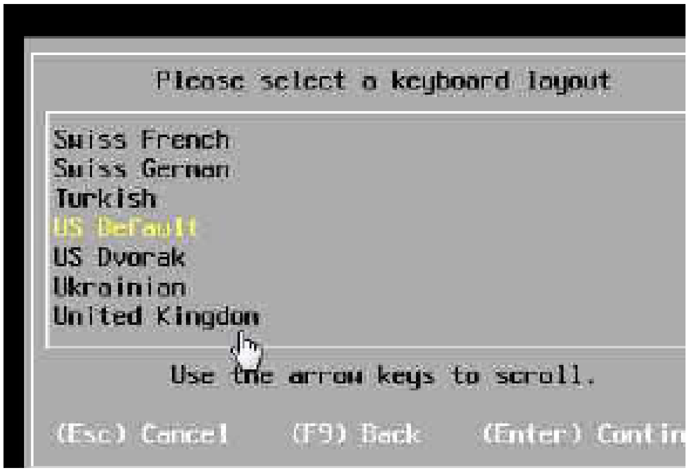
```
                Scanning...
Scanning for available devices. This may take a few
```

- The installer next scans for available storage devices and volumes. Select a local installation destination and continue.



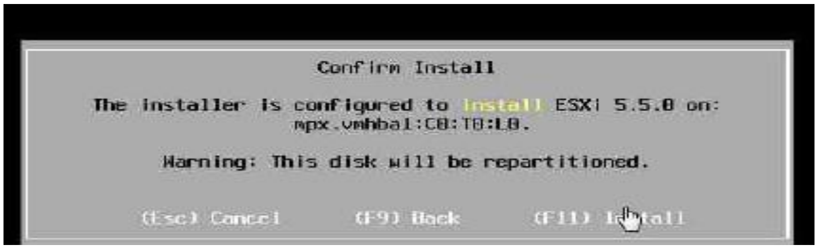
```
                     Select a Disk to Install or Upgrade
* Contains a VMFS partition
# Claimed by vSAN
Storage Device
-----------------------------------------------------------------
Local:
   VMware   Virtual disk     (mpx. hba1:C0:T0:L0)
Remote:
   (none)

   (Esc) Cancel    (F1) Details    (F5) Refresh    (Ent
```

- Select the desired keyboard layout.



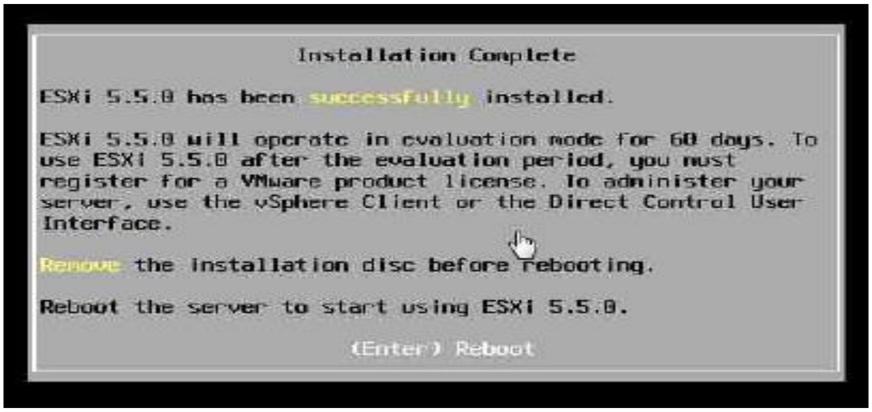
```
Please select a keyboard layout

Swiss French
Swiss German
Turkish
US Default
US Dvorak
Ukrainian
United Kingdom

Use the arrow keys to scroll.

(Esc) Cancel     (F9) Back     (Enter) Contin
```

- Enter F11 to begin the installation.



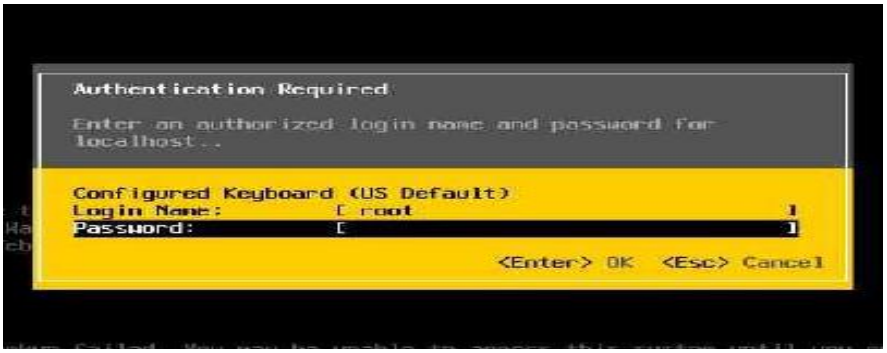
```
Confirm Install

The installer is configured to install ESXi 5.5.0 on:
mpx.vmhba1:C0:T0:L0.

Warning: This disk will be repartitioned.

(Esc) Cancel     (F9) Back     (F11) Install
```

- Once the installer has finished, press Enter to reboot the system.



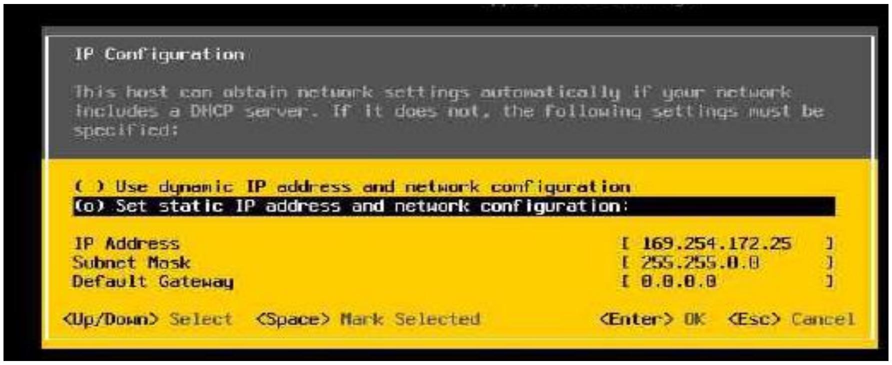
```
Installation Complete

ESXi 5.5.0 has been successfully installed.

ESXi 5.5.0 will operate in evaluation mode for 60 days. To
use ESXi 5.5.0 after the evaluation period, you must
register for a VMware product license. To administer your
server, use the vSphere Client or the Direct Control User
Interface.

Remove the installation disc before rebooting.

Reboot the server to start using ESXi 5.5.0.

(Enter) Reboot
```

- Press F2 and provide the root user credentials to start configuring the ESXi server.



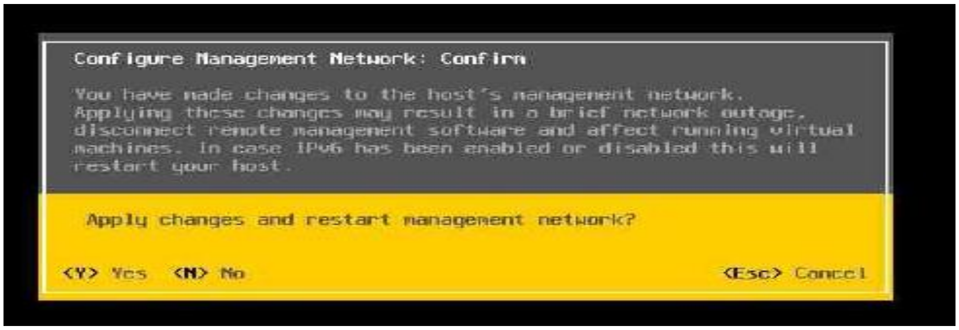
```
Authentication Required

Enter an authorized login name and password for
localhost..

Configured Keyboard (US Default)
Login Name:          [ root                              ]
Password:            [                                   ]

                                   <Enter> OK   <Esc> Cancel
```

- Select Configure Management Network and assign a static IP address to the server.



```
IP Configuration

This host can obtain network settings automatically if your network
includes a DHCP server. If it does not, the following settings must be
specified:

( ) Use dynamic IP address and network configuration
(o) Set static IP address and network configuration:

IP Address                                    [ 169.254.172.25   ]
Subnet Mask                                   [ 255.255.0.0      ]
Default Gateway                               [ 0.0.0.0          ]

<Up/Down> Select   <Space> Mark Selected          <Enter> OK   <Esc> Cancel
```

- Once the IP configuration is done, press “Y” to apply the changes and restart the management network.



```
Configure Management Network: Confirm

You have made changes to the host's management network.
Applying these changes may result in a brief network outage,
disconnect remote management software and affect running virtual
machines. In case IPv6 has been enabled or disabled this will
restart your host.

 Apply changes and restart management network?

<Y> Yes   <N> No                                    <Esc> Cancel
```

Log on to ESXi

To connect to an ESXi server we can use any of the following methods: (a) vSphere Client, (b) SSH client, (c) Shell or direct console on the server and (d) vCenter Server vSphere Client, SSH, and vCenter are all remote connectivity tools which allow administrators from different geographies to manage an ESXi server. The ESXi server shell can be used only if an administrator is physically in front of the server. If Lockdown Mode is enabled on a server, all remote access attempts will be blocked and the server can only be administered from the console or a vCenter Server instance. This helps increase the security of the ESXi server.

Shell and SSH access can be enabled from the DCUI of an ESXi server. To enable the shell, simply navigate to troubleshooting options on the ESXi customization screen, select troubleshooting options, and select ESXi shell from the menu. Once the shell is enabled, pressing ALT-F1 at the console will allow an administrator to type commands at the ESXi command line. To return to the DCUI interface, press the ALT-F2 hotkey combination.

To connect to an ESXi server using SSH, log into ESXi using the root account, navigate to troubleshooting options on the ESXi customization screen, and select ESXi SSH. Connecting to an ESXi server via SSH requires that the administrator have an SSH client application, such as PuTTY.

vCenter Server

vCenter server is a centralized management platform that can manage multiple ESXi servers and the virtual machines running on them. Two types of vCenter servers are available and, while they provide nearly identical feature sets, each has its own advantages and limitations.

Table 1

Significant Differences between Windows-based and Linux-based vCenter Deployments

Windows-Based vCenter Server	Linux-Based Virtual Appliance
Supports IPv6	Does not support IPv6
Can be installed either on a physical server or on a Virtual machine. VMware recommends running vCenter in a virtual machine	Can only be installed inside a VM
Supports Microsoft SQL Server, Oracle and IBM DB2 as external databases	Supports Oracle as an external database
The embedded database is a SQL Express instance. This Embedded database supports only 5 hosts and 50 virtual machines	PostgreSQL is the embedded database. Version 5.5 supports 300 hosts and 1,000 virtual machines, while version 6 supports 1,000 hosts and 10,000 virtual machines
Supports VMware Update Manager	Does not support VMware Update Manager
Linked mode configuration is supported	Does not support linked mode configuration
Available as a separate application. Supported operating systems include Windows Server 2008, Server 2008 R2, Server 2012, and Server 2012 R2	Embedded SUSE Linux Enterprise Server 11

vCenter Server Architecture

Before installing a vCenter Server, FOR instance, we need to install three prerequisite components: (a) Single Sign On, (b) Web Client, and (c) Inventory Service.

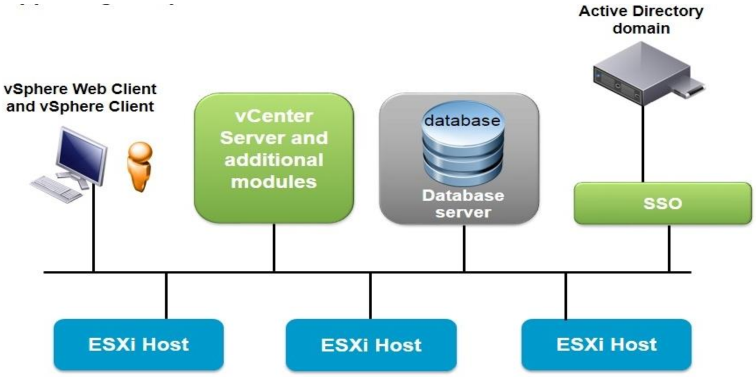


Figure 9. vCenter Server Architecture (VMware, n.d.n)

Single Sign On allows users to authenticate to vCenter and different modules with a single user name and password. To facilitate this, SSO depends on an existing Active directory, LDAP, or NIS infrastructure. Once SSO is installed, it creates its own internal domain (vSphere.local, by default).

Web Client can be used to connect to a vCenter Server instance in the same way as the traditional vSphere Client. However, the Web Client is the suggested method of administering vSphere infrastructures since version 5.5. In fact, there are new features added in versions 5.5 and 6.0 that are not available in the native vSphere Client.

The Inventory Service servers two primary roles: (a) It maintains the tags for Web Client, and (b) it acts as a proxy or cache for Web Client connections.

If users are connecting to a vCenter Server using the Web Client, all the connections will be cached by the Inventory Service. The next time the same users attempt to log into vCenter, the Inventory Service will look for and verify the connection details in the cache, thereby decreasing the load on the vCenter Server.

vCenter Server Specification Requirement

vCenter Server is a very critical component in the vSphere product suite. vCenter Server is a centralized management platform which can manage multiple ESXi servers. vCenter server can be installed on a supported Windows operating system or deployed as a Linux-based virtual appliance.

A single Windows-based vCenter Server instance can manage up to 1,000 ESXi servers and 10,000 powered-on virtual machines. vCenter Server requires a back-end database to store information about all of the ESXi servers it is managing.

Windows-based vCenter Server Requirements

Table 2

vCenter Server Requirements for Windows

RAM	Four GB (minimum)
CPU	Four cores (minimum)
Hard disk	Seven GB free disk space (minimum)
Operating System	Windows Server 2008, Server 2008 R2, Server 2012, Server 2012 R2
Installation Mode	Can be installed on a physical server or on a virtual machine. VMware recommends installing vCenter Server on a VM
OS Requirements	Operating system should be assigned a static IP address, should be a part of an Active Directory domain, and should have VMware Tools installed (if running as a VM). The vCenter installation should be performed using a domain administrator account.

Linux-based vCenter Server Requirements

Table 3

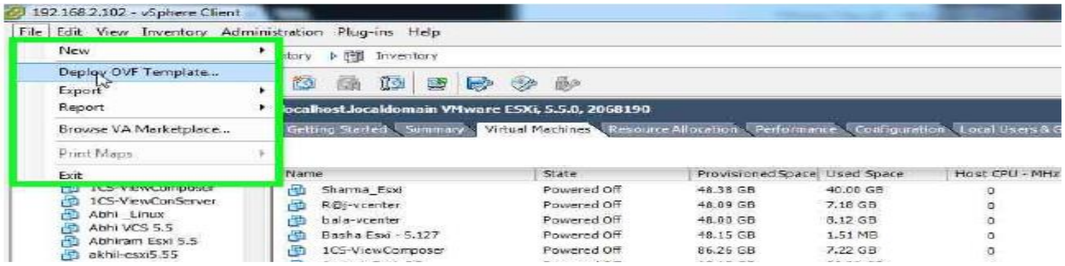
vCenter Server Requirements for Linux

RAM	Two GB (minimum)
CPU	Four cores (minimum)
Hard disk	Four GB (minimum)
Operating System	Comes as an OVA virtual appliance based on SUSE Linux
Installation Mode	Deployed into vCenter as a virtual appliance with pre-configured virtual hardware.

vCenter Server Installation

Installing vCenter Server as a Linux-based virtual appliance involves the following steps. In order to deploy the VCSA virtual appliance, the OVA file must first be downloaded from VMware.

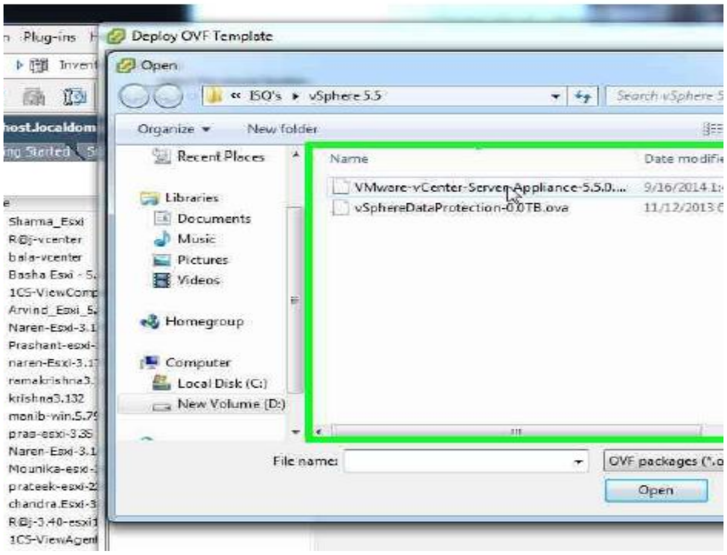
- Connect to an ESXi Server using vSphere Client. Click on File and select “Deploy OVF Template” from the menu.



localhost.localdomain VMware ESXi, 5.5.0, 2068190

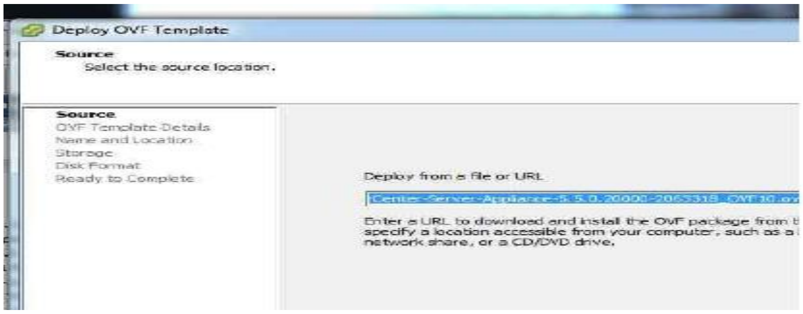
Name	State	Provisioned Space	Used Space	Host CPU - MHz
Sharma_Esxi	Powered Off	48.38 GB	40.00 GB	0
R@j-vcenter	Powered Off	48.09 GB	7.18 GB	0
bala-vcenter	Powered Off	48.00 GB	8.12 GB	0
Basha Esxi - 5.127	Powered Off	48.15 GB	1.51 MB	0
1CS-ViewComposer	Powered Off	86.26 GB	7.22 GB	0

- Locate and select the download OVA file. Click Next to continue.



Name	Date modifie
VMware-vCenter-Server-Appliance-5.5.0....	9/16/2014 1:
vSphereDataProtection-0.0TB.ova	11/12/2013

- On the next stage of the wizard it shows the description of the product. It is vCenter Server Appliance version 5.5 running on SUSE Linux Enterprise Server 11.

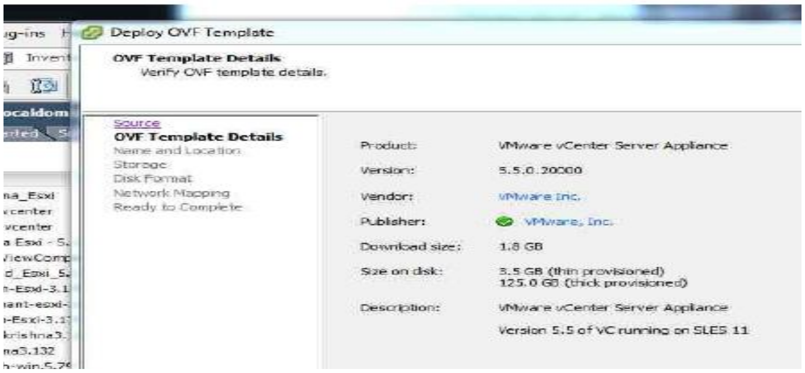


Source
Select the source location.

Deploy from a file or URL

Center-Server-Appliance-5.5.0.20000-2063318_OVF10.ov

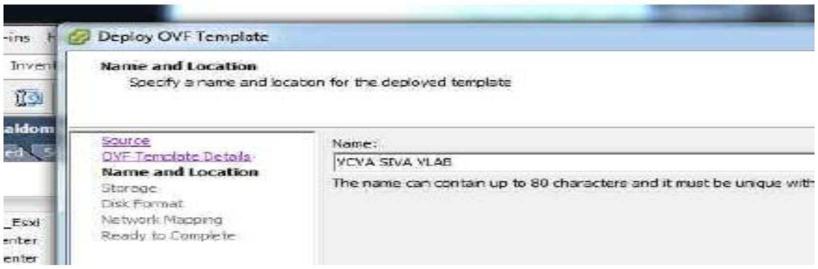
Enter a URL to download and install the OVF package from t
specify a location accessible from your computer, such as a l
network share, or a CD/DVD drive.



OVF Template Details
Verify OVF template details.

Product:	VMware vCenter Server Appliance
Version:	5.5.0.20000
Vendor:	VMware Inc.
Publisher:	VMware, Inc.
Download size:	1.8 GB
Size on disk:	3.5 GB (thin provisioned) 125.0 GB (thick provisioned)
Description:	VMware vCenter Server Appliance Version 5.5 of VC running on SLES 11

- Name the vCenter virtual appliance and click Next to continue.

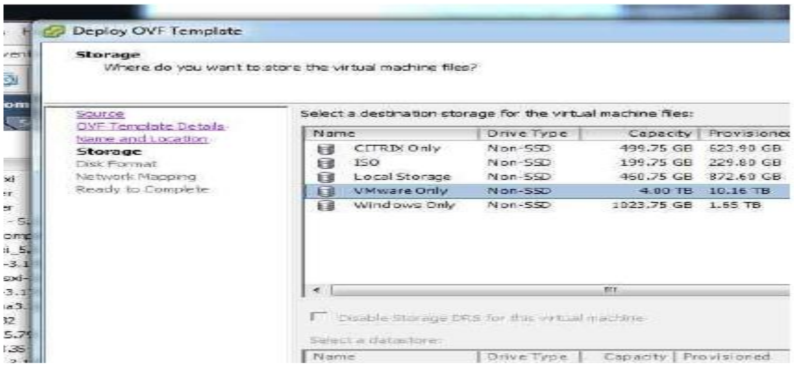


Name and Location
Specify a name and location for the deployed template

Name:
VCVA SIVA VLAB

The name can contain up to 80 characters and it must be unique with

- Select the datastore where the appliance should be stored and click Next.



Storage
Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

Name	Drive Type	Capacity	Provisioned
CITRIX Only	Non-SSD	499.75 GB	623.90 GB
ISO	Non-SSD	199.75 GB	229.80 GB
Local Storage	Non-SSD	460.75 GB	872.60 GB
VMware Only	Non-SSD	4.00 TB	10.16 TB
Windows Only	Non-SSD	1023.75 GB	1.65 TB

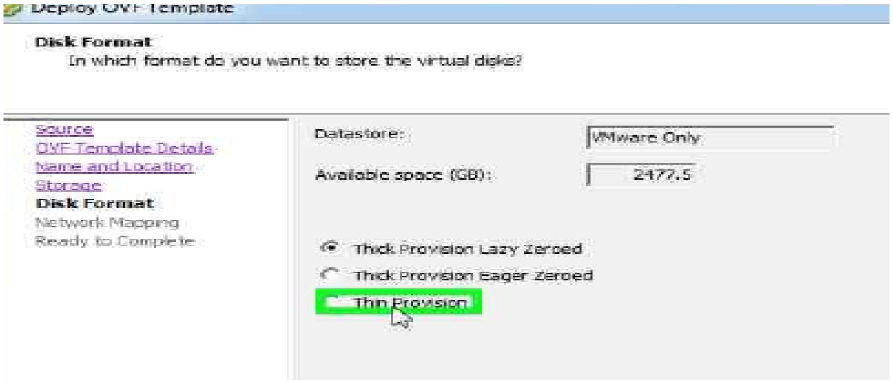
□ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Type	Capacity	Provisioned

Select the provisioning type for the appliance’s virtual hard disk. Three types of virtual disk provisioning are available:

- **Thick Provision Lazy Zeroed:** In this provisioning type, all storage space will be allocated immediately. However, the formatting of the hard disk will happen as needed.
- **Thick Provision Eager Zeroed:** In this provisioning type, all storage space will be allocated up-front. The formatting of the hard disk will take place immediately as well. This is the best option for running business-critical applications, as the applications need not wait for the formatting to take place.
- **Thin Provision:** In this provisioning type, virtual disk space is allocated on-demand up to a user-defined maximum. The primary benefit of thin provisioning is that there will be no wasted disk space. However, because a VM with a thin-provisioned virtual disk must wait for disk space to be allocated, there is a small performance degredation.

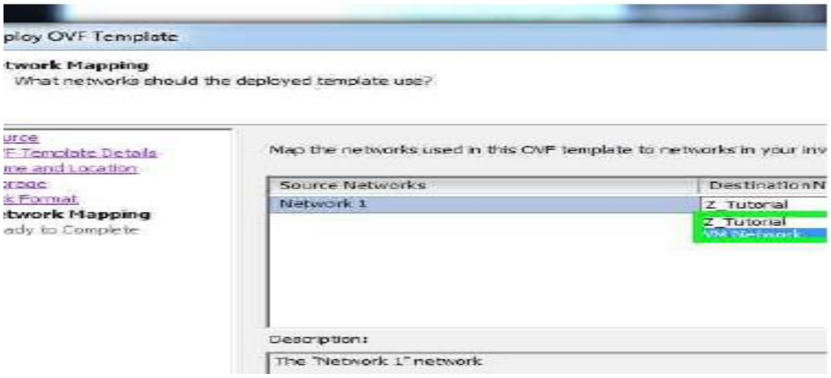


Disk Format
In which format do you want to store the virtual disks?

Datastore: VMware Only
Available space (GB): 2477.5

● Thick Provision Lazy Zeroed
○ Thick Provision Eager Zeroed
○ Thin Provision

Next, select the virtual network that the appliance should be connected to, and click Next to continue



ploy OVF Template

twork Mapping

What networks should the deployed template use?

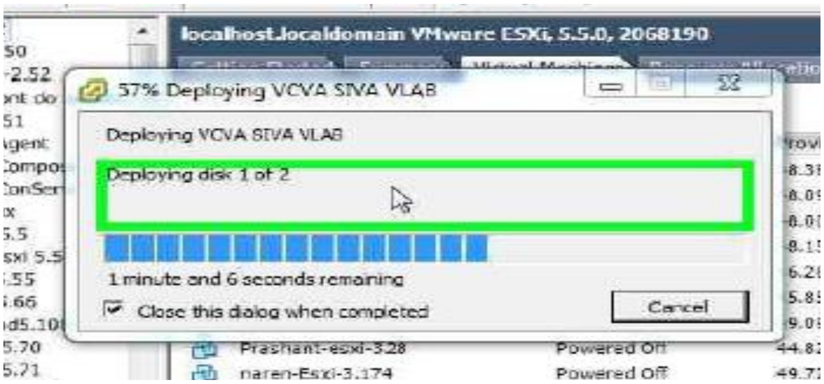
Map the networks used in this OVF template to networks in your inv

Source Networks	Destination N
Network 1	Z_Tutorial

Description:

The "Network 1" network

- The deployment of the virtual appliance will begin.



localhost.localdomain VMware ESXi, 5.5.0, 2068190

57% Deploying VCVA SIVA VLAB

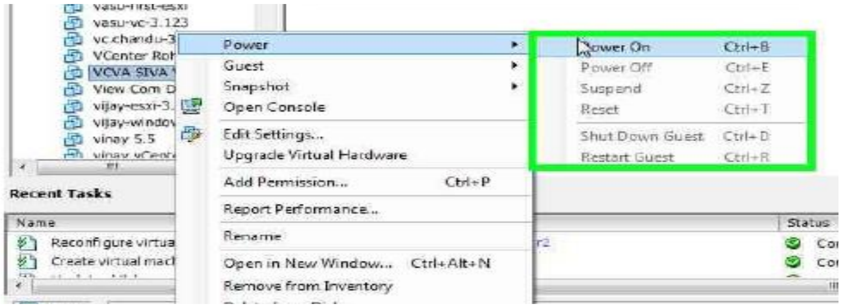
Deploying VCVA SIVA VLAB

Deploying disk 1 of 2

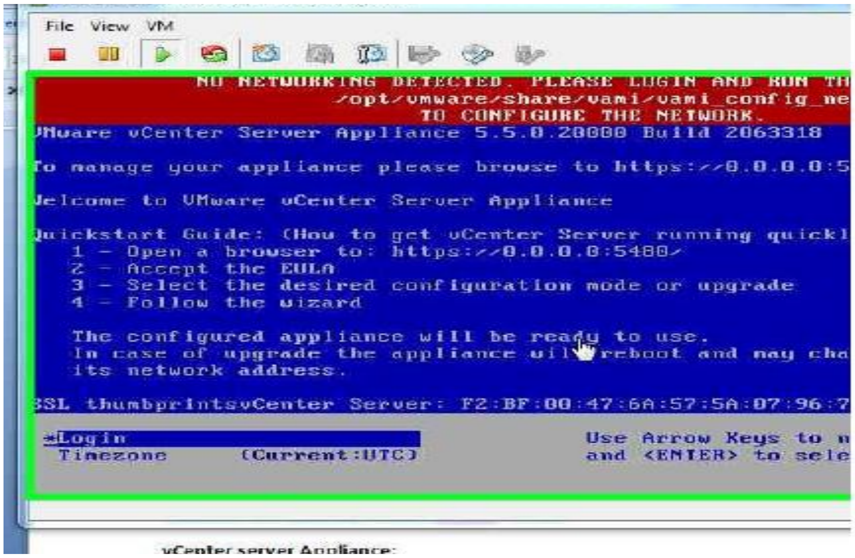
1 minute and 6 seconds remaining

☑ Close this dialog when completed

- Once the deployment is complete, select the vCenter Server VM and power it on.

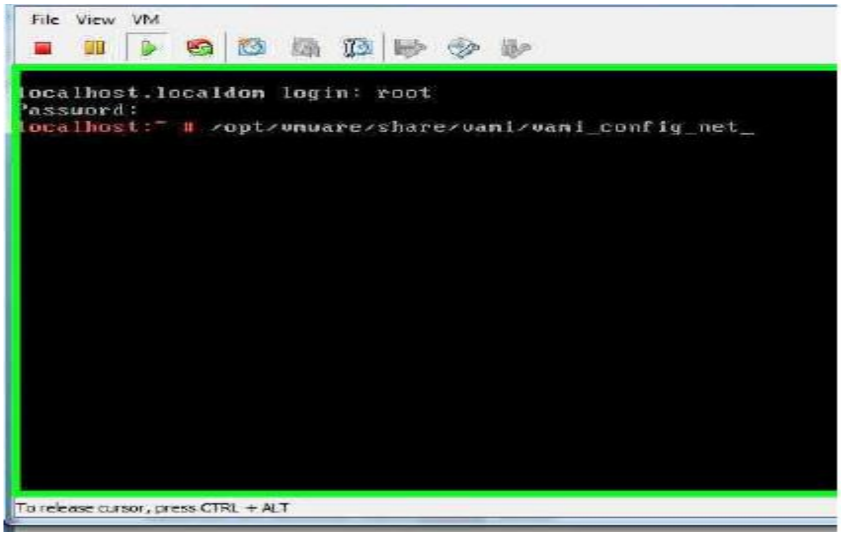


- Once the appliance finished booting, we next need to configure the management network interface, default gateway, and hostname of the appliance.



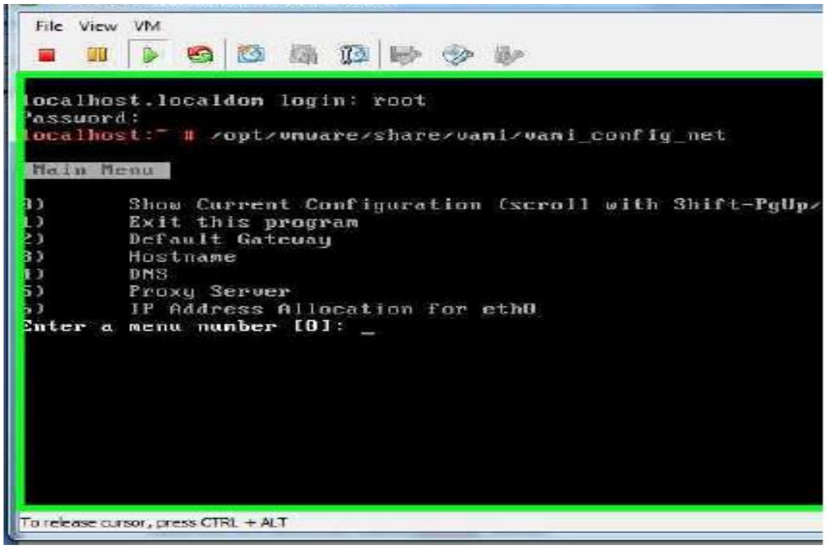
```
                       NO NETWORKING DETECTED. PLEASE LOGIN AND RUN TH
                                  /opt/vmware/share/vami/vami_config_ne
                                        TO CONFIGURE THE NETWORK.
VMware vCenter Server Appliance 5.5.0.20000 Build 2063318

To manage your appliance please browse to https://0.0.0.0:5

Welcome to VMware vCenter Server Appliance

Quickstart Guide: (How to get vCenter Server running quickl
   1 - Open a browser to: https://0.0.0.0:5480/
   2 - Accept the EULA
   3 - Select the desired configuration mode or upgrade
   4 - Follow the wizard

   The configured appliance will be ready to use.
   In case of upgrade the appliance will reboot and may cha
   its network address.

SSL thumbprintsvCenter Server: F2:BF:00:47:6A:57:5A:07:96:7

*Login                                        Use Arrow Keys to n
 Timezone        (Current:UTC)                and <ENTER> to sele
```

- Next, log into the manage console of the appliance using the default password "vmware" and run the command /opt/vmware/share/vami/vami_config_net to begin the post-installation configuration.



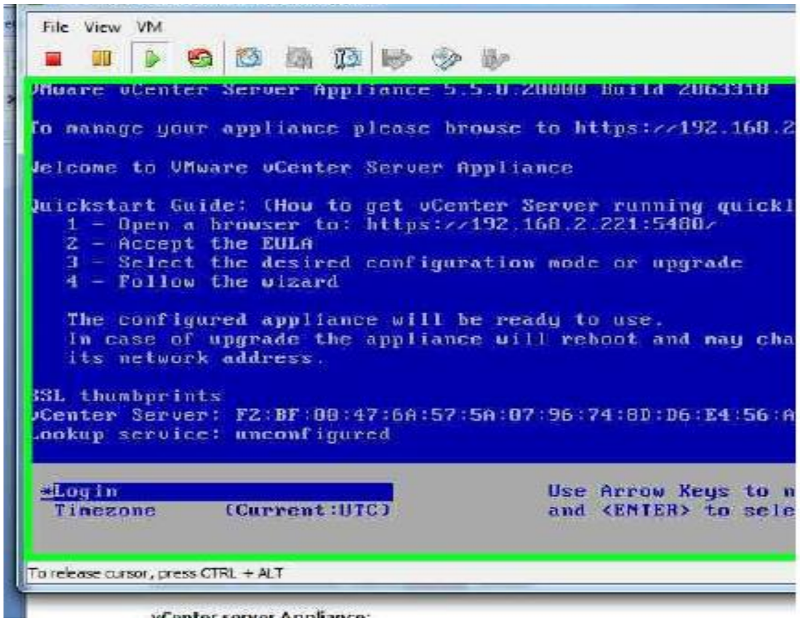
```
localhost.localdom login: root
Password:
localhost:~ # /opt/vmware/share/vami/vami_config_net_
```

- The vami_config_net command brings up a menu through which we can configure several aspects of the vCenter appliance.



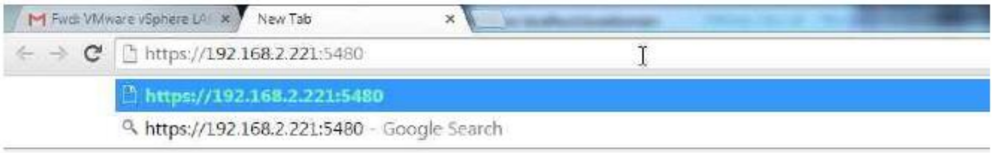
```
ocalhost.localdon login: root
assuord:
ocalhost:~ # /opt/vmuare/share/vami/vami_config_net

Main Menu

0)      Show Current Configuration (scroll with Shift-PgUp/
1)      Exit this program
2)      Default Gateuay
3)      Hostname
4)      DNS
5)      Proxy Server
6)      IP Address Allocation for eth0
Enter a menu number [0]: _
```

- Make any configuration changes necessary, and select option 2 to close the configuration menu.



```
VMuare vCenter Server Appliance 5.5.0.20000 Build 2063318

To manage your appliance please browse to https://192.168.2

Welcome to VMware vCenter Server Appliance

Quickstart Guide: (How to get vCenter Server running quickl
   1 - Open a brouser to: https://192.168.2.221:5480/
   2 - Accept the EULA
   3 - Select the desired configuration mode or upgrade
   4 - Follow the wizard

   The configured appliance will be ready to use.
   In case of upgrade the appliance will reboot and may cha
   its network address.

SSL thumbprints
vCenter Server: F2:BF:08:47:6A:57:5A:07:96:74:8D:D6:E4:56:A
Lookup service: unconfigured

 *Login                                    Use Arrow Keys to n
  Timezone      (Current:UTC)              and <ENTER> to sele
```

We can now access the web-based administration console. Open a supported web browser and enter the hostname of the appliance in the address bar. Be sure to specify port 5480 at the end of the address.

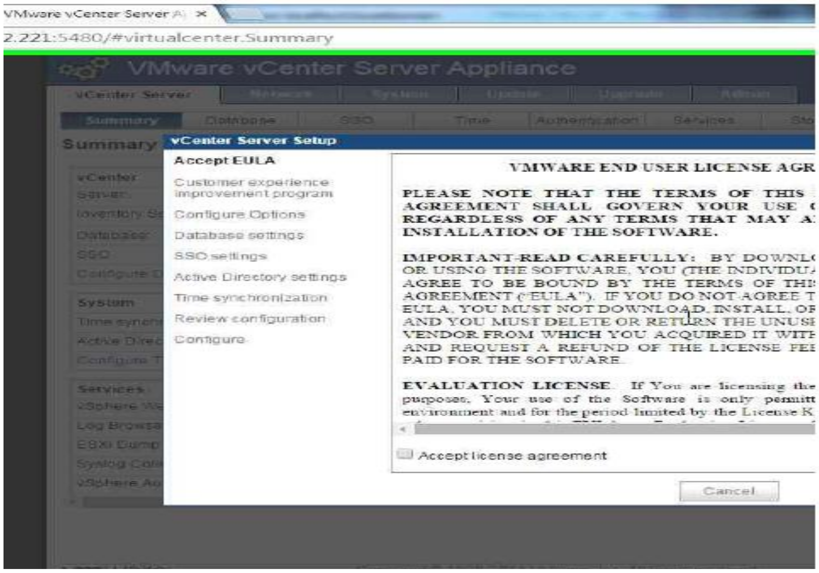


https://192.168.2.221:5480

https://192.168.2.221:5480

https://192.168.2.221:5480 - Google Search

- Accept the EULA and click Next to continue.



vCenter Server Setup

Accept EULA
Customer experience improvement program
Configure Options
Database settings
SSO settings
Active Directory settings
Time synchronization
Review configuration
Configure

VMWARE END USER LICENSE AGR

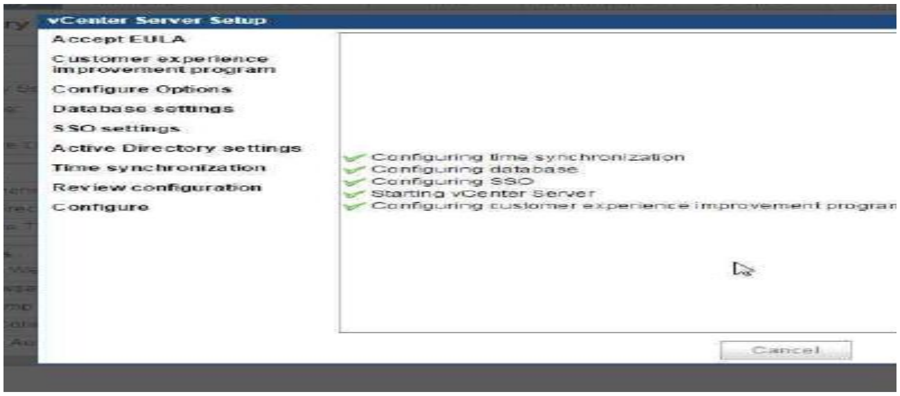
PLEASE NOTE THAT THE TERMS OF THIS
AGREEMENT SHALL GOVERN YOUR USE (
REGARDLESS OF ANY TERMS THAT MAY A
INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNL(
OR USING THE SOFTWARE, YOU (THE INDIVIDU
AGREE TO BE BOUND BY THE TERMS OF THI
AGREEMENT ("EULA"). IF YOU DO NOT AGREE T
EULA, YOU MUST NOT DOWNLOAD, INSTALL, OF
AND YOU MUST DELETE OR RETURN THE UNUSI
VENDOR FROM WHICH YOU ACQUIRED IT WITH
AND REQUEST A REFUND OF THE LICENSE FEI
PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If You are licensing the
purposes, Your use of the Software is only permitt
environment and for the period limited by the License K

☐ Accept license agreement

- Continue through the setup wizard, providing the appropriate information for the vCenter environment.

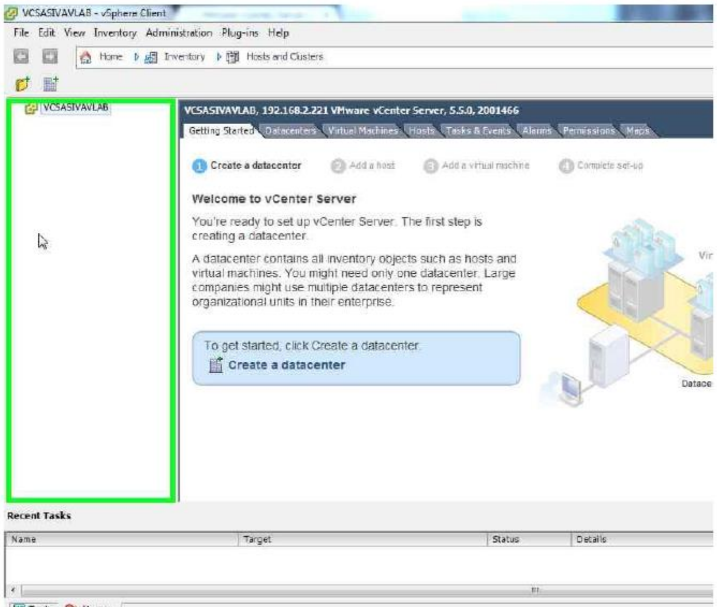


vCenter Server Setup

Accept EULA
Customer experience improvement program
Configure Options
Database settings
SSO settings
Active Directory settings
Time synchronization
Review configuration
Configure

✓ Configuring time synchronization
✓ Configuring database
✓ Configuring SSO
✓ Starting vCenter Server
✓ Configuring customer experience improvement program

- Now we can log into the vCenter Server appliance using the traditional vSphere Client by specifying the IP address of the appliance.



VCSASIVAVLAB, 192.168.2.221 VMware vCenter Server, 5.5.0, 2001466

Welcome to vCenter Server

You're ready to set up vCenter Server. The first step is creating a datacenter.

A datacenter contains all inventory objects such as hosts and virtual machines. You might need only one datacenter. Large companies might use multiple datacenters to represent organizational units in their enterprise.

To get started, click Create a datacenter.

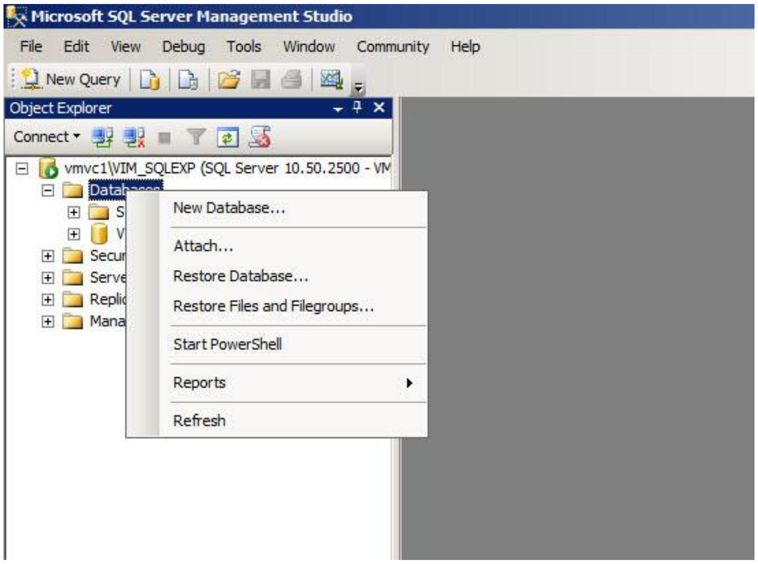
SRM Database Setup Using Microsoft SQL Server 2008 R2 Express

Download SQL Server Management Studio (SSMS) installation files (SQLManagementStudio_x64_ENU.exe / SQLManagementStudio_x86_ENU.exe) from the SQL Server download page depending on your server type (x64, x86), and keep it in a separate folder.

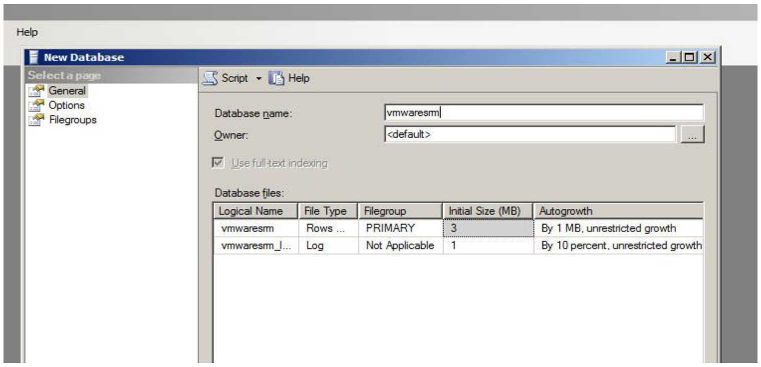
Once you downloaded the respective file as per your server type, you need to execute it. It will then take you to the SQL Server Installation Center, this is the primary installation of SQL Server. Other SQL server tools installations can be launched from there as well. Once you are on that screen, you need to select “New SQL Server stand-alone installation or add features to an existing installation” to proceed with the installation.

After Downloading and Installing SQL Server Management Studio (SSMS), open it and create a new database by following these steps.

- Right-click on the Databases folder and select New Database from the menu.



- Create a new database for System Resource Manager by completing the New Database wizard.



Database name: vmwaresm

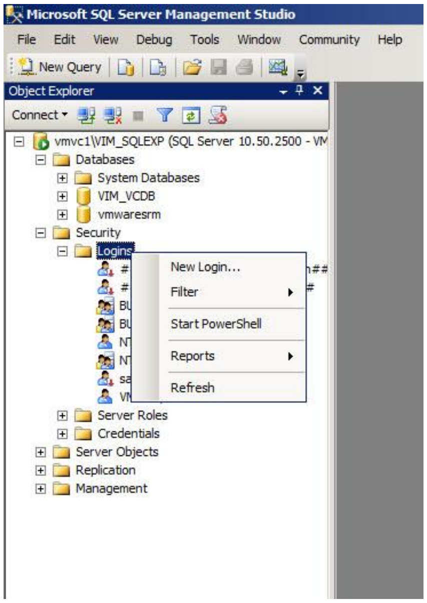
Owner: <default>

☑ Use full-text indexing

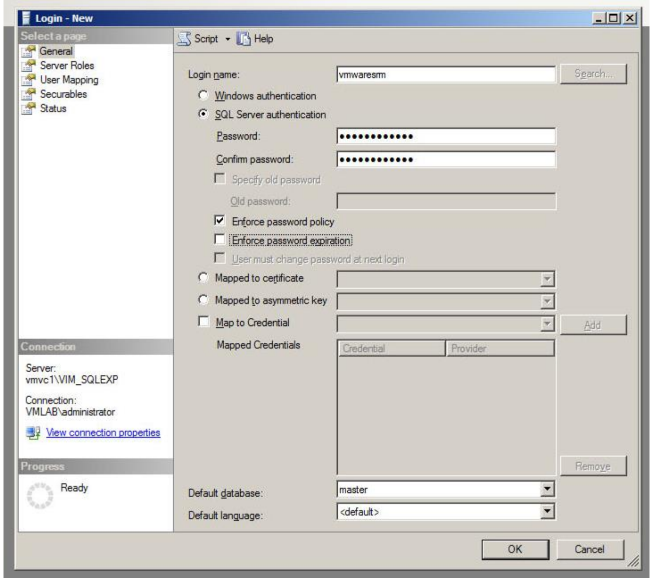
Database files:

Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth
vmwaresm	Rows ...	PRIMARY	3	By 1 MB, unrestricted growth
vmwaresm_l...	Log	Not Applicable	1	By 10 percent, unrestricted growth

- Create a new user for the database created in previous step by right-clicking on the Login option (under the Security node) and selecting New Login from the menu.



- Create a Login Name and Assign it a Password. Do not check the enforce Password Expiration Option as the Password has to be changed in 30 days.



Login name: vmwaresrm

○ Windows authentication

● SQL Server authentication

Password: ••••••••••••

Confirm password: ••••••••••••

□ Specify old password

Old password:

☑ Enforce password policy

□ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Default database: master

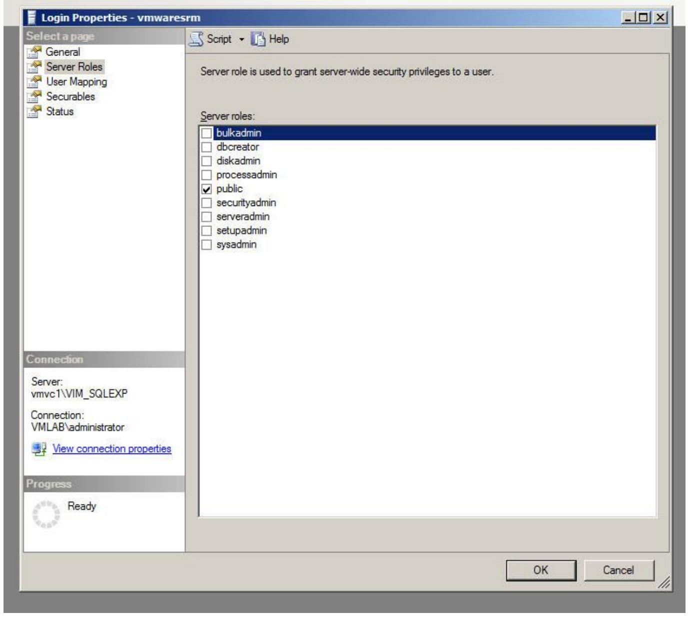
Default language: <default>

Connection

Server:
vmvc1\VIM_SQLEXP

Connection:
VMLAB\administrator

- Select the Public option from the list of server roles.



Login Properties - vmwaresrm

Server role is used to grant server-wide security privileges to a user.

Server roles:

- □ bulkadmin
- □ dbcreator
- □ diskadmin
- □ processadmin
- ☑ public
- □ securityadmin
- □ serveradmin
- □ setupadmin
- □ sysadmin

Connection

Server:
vmvc1\VIM_SQLEXP

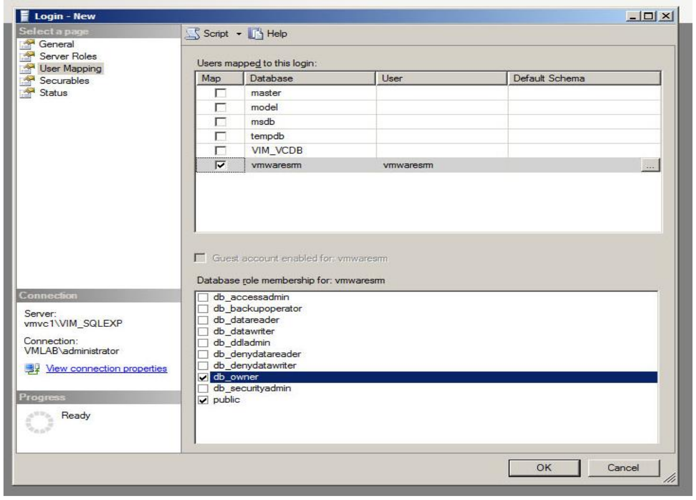
Connection:
VMLAB\administrator

View connection properties

Progress

Ready

- Next, map the user created in the previous step to the database by clicking on the user mapping, selecting the role membership as public and db_owner.



Login - New

Users mapped to this login:

Map	Database	User	Default Schema
□	master		
□	model		
□	msdb		
□	tempdb		
□	VIM_VCDB		
☑	vmwaresrm	vmwaresrm	...

□ Guest account enabled for: vmwaresrm

Database role membership for: vmwaresrm

- □ db_accessadmin
- □ db_backupoperator
- □ db_datareader
- □ db_datawriter
- □ db_ddladmin
- □ db_denydatareader
- □ db_denydatawriter
- ☑ db_owner
- □ db_securityadmin
- ☑ public

Connection

Server:
vmvc1\VIM_SQLEXP

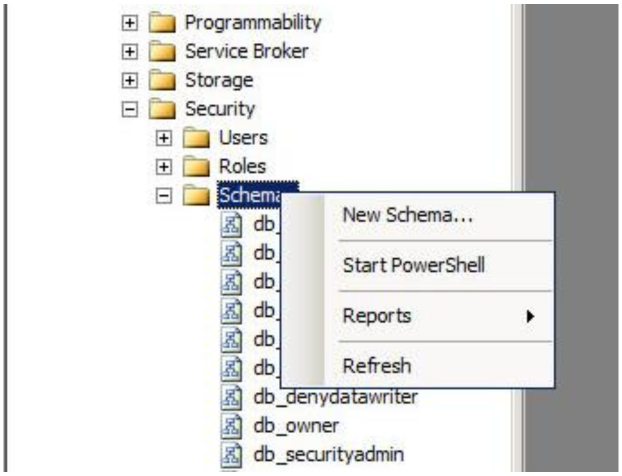
Connection:
VMLAB\administrator

View connection properties

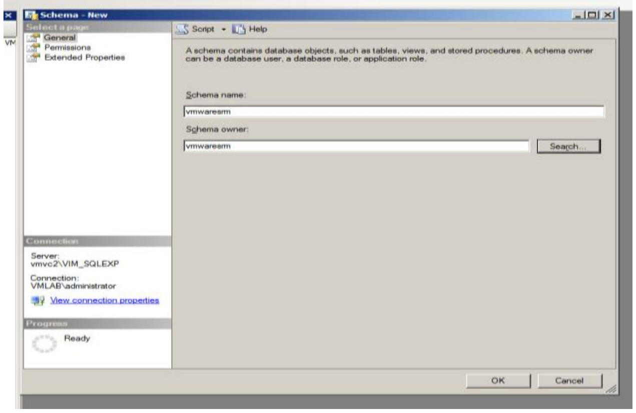
Progress

Ready

The next step involves creating a schema for SRM: Select databases, expand and select the new created database, click on Security, right-click on Schema, and select New Schema from the menu.



- Specify a name for the new schema and click OK to continue.



A schema contains database objects, such as tables, views, and stored procedures. A schema owner can be a database user, a database role, or application role.

Schema name: vmwaresrm

Schema owner: vmwaresrm

Connection

Server:
vmvc2\VIM_SQLEXP

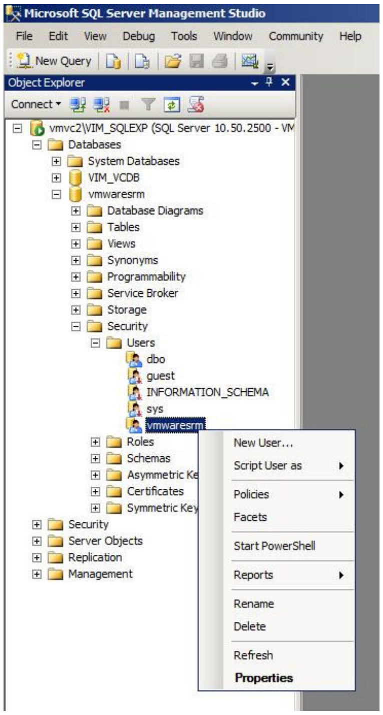
Connection:
VMLAB\administrator

View connection properties

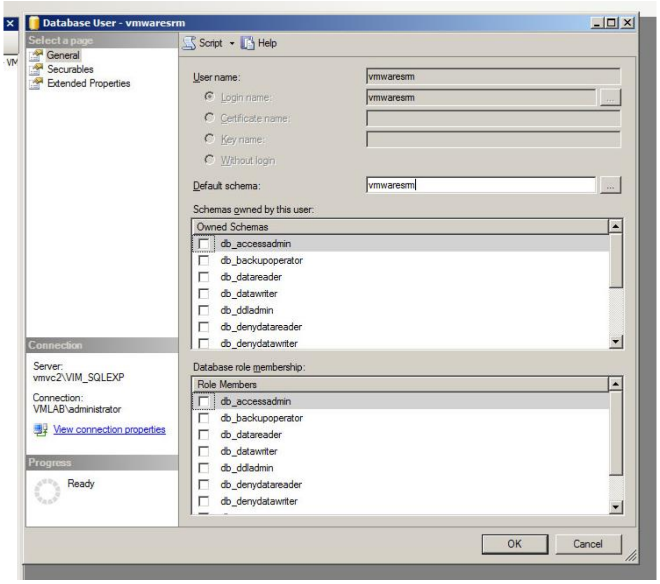
Progress

Ready

- Next, expand the Security folder under the database tree, right-click the new user account, and select Properties from the menu.



- Now on default schema option select the name that we have created. For this deployment, we used "vmwaresrm" as the name for the database, user account, and schema.



User name: vmwaresrm

● Login name: vmwaresrm

○ Certificate name:

○ Key name:

○ Without login

Default schema: vmwaresrm

Server: vmvc2\VIM_SQLEXP

Connection: VMLAB\administrator

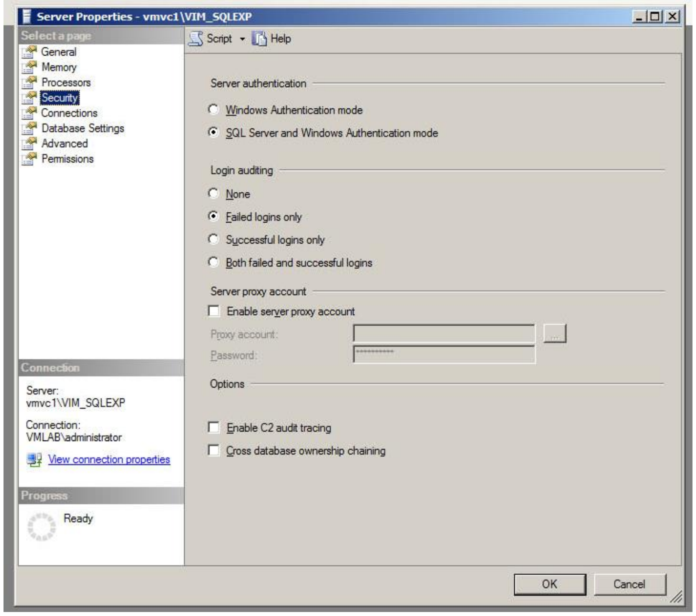
Schemas owned by this user:

Owned Schemas
□ db_accessadmin
□ db_backupoperator
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter

Database role membership:

Role Members
□ db_accessadmin
□ db_backupoperator
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter

Next, we have to make sure the database allows SQL Authentication. Right-click on the database and click on Properties from the menu. Navigate to Security Options and click on SQL and Windows Authentication mode. Restart the SQL Server database services to ensure that the authentication changes take effect.



Server: vmvc1\VIM_SQLEXP

Connection: VMLAB\administrator

Server authentication

○ Windows Authentication mode

● SQL Server and Windows Authentication mode

Login auditing

○ None

● Failed logins only

○ Successful logins only

○ Both failed and successful logins

Server proxy account

□ Enable server proxy account

Proxy account:

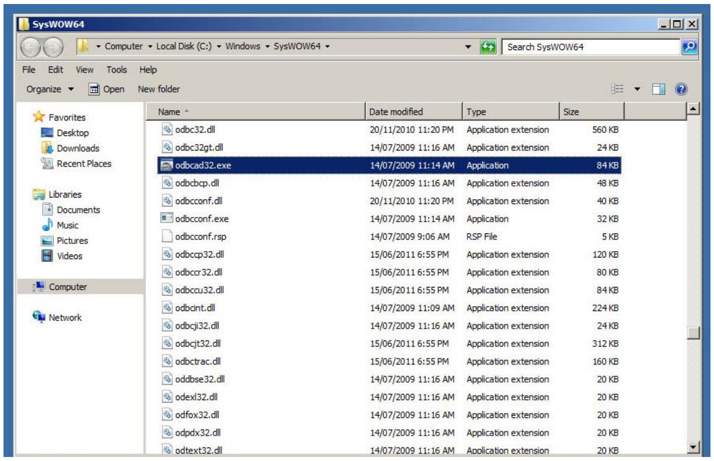
Password: **********

Options

□ Enable C2 audit tracing

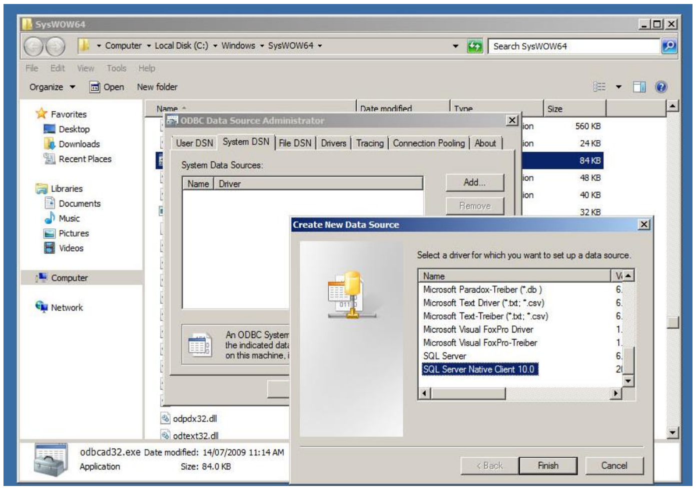
□ Cross database ownership chaining

- Next, we need to set up the 32-bit DSN for SRM so that SRM can connect to the database. Browse to C:\Windows\SysWOW64, select odbcad32.exe, and launch as shown in the following screenshot.



Name	Date modified	Type	Size
odbc32.dll	20/11/2010 11:20 PM	Application extension	560 KB
odbc32gt.dll	14/07/2009 11:16 AM	Application extension	24 KB
odbcad32.exe	14/07/2009 11:14 AM	Application	84 KB
odbcbcp.dll	14/07/2009 11:16 AM	Application extension	48 KB
odbcconf.dll	20/11/2010 11:20 PM	Application extension	40 KB
odbcconf.exe	14/07/2009 11:14 AM	Application	32 KB
odbcconf.rsp	14/07/2009 9:06 AM	RSP File	5 KB
odbccp32.dll	15/06/2011 6:55 PM	Application extension	120 KB
odbccr32.dll	15/06/2011 6:55 PM	Application extension	80 KB
odbccu32.dll	15/06/2011 6:55 PM	Application extension	84 KB
odbcint.dll	14/07/2009 11:09 AM	Application extension	224 KB
odbcji32.dll	14/07/2009 11:16 AM	Application extension	24 KB
odbcjt32.dll	15/06/2011 6:55 PM	Application extension	312 KB
odbctrac.dll	15/06/2011 6:55 PM	Application extension	160 KB
oddbse32.dll	14/07/2009 11:16 AM	Application extension	20 KB
odexl32.dll	14/07/2009 11:16 AM	Application extension	20 KB
odfox32.dll	14/07/2009 11:16 AM	Application extension	20 KB
odpdx32.dll	14/07/2009 11:16 AM	Application extension	20 KB
odtext32.dll	14/07/2009 11:16 AM	Application extension	20 KB

- Navigate to the System DSN tab and click the Add button. In the new window, select SQL Server Native Client Version 10.0, and click Finish.


SysWOW64
Computer ▸ Local Disk (C:) ▸ Windows ▸ SysWOW64
Search SysWOW64
File Edit View Tools Help
Organize Open New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name Date modified Type Size
ODBC Data Source Administrator
User DSN System DSN File DSN Drivers Tracing Connection Pooling About
Add...
Remove
Finish
Cancel
< Back

System Data Sources:

Name	Driver

An ODBC System the indicated data on this machine, i

odpdx32.dll
odtext32.dll

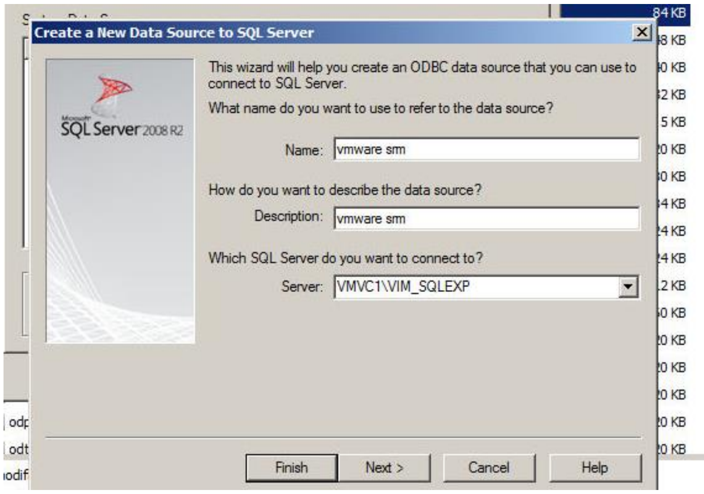
odbcad32.exe Date modified: 14/07/2009 11:14 AM
Application Size: 84.0 KB

Create New Data Source

Select a driver for which you want to set up a data source.

Name	V
Microsoft Paradox-Treiber (*.db)	6.
Microsoft Text Driver (*.txt; *.csv)	6.
Microsoft Text-Treiber (*.txt; *.csv)	6.
Microsoft Visual FoxPro Driver	1.
Microsoft Visual FoxPro-Treiber	1.
SQL Server	6.
SQL Server Native Client 10.0	2(

- Assign a name to the DSN and enter the correct and path for the server. For our deployment, we used the SQL Express embedded database included with the vCenter Server installation. The database name is VIM_SQLEXP.



Create a New Data Source to SQL Server

This wizard will help you create an ODBC data source that you can use to connect to SQL Server.

What name do you want to use to refer to the data source?

Name: vmware srm

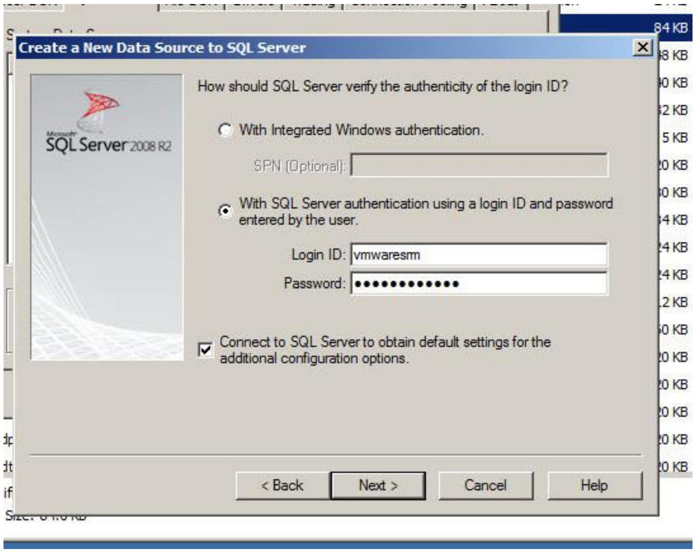
How do you want to describe the data source?

Description: vmware srm

Which SQL Server do you want to connect to?

Server: VMVC1\VIM_SQLEXP

- Select the radio button next to “With SQL Server authentication…” and specify the database login ID and password set earlier.



Create a New Data Source to SQL Server

How should SQL Server verify the authenticity of the login ID?

○ With Integrated Windows authentication.

SPN (Optional):

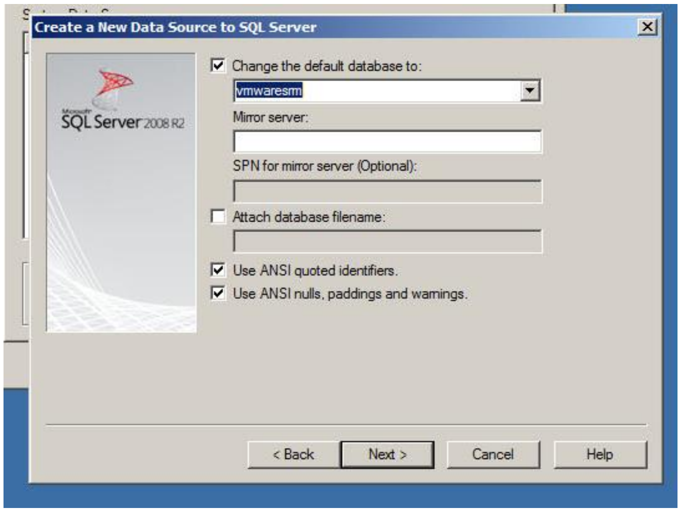
● With SQL Server authentication using a login ID and password entered by the user.

Login ID: vmwaresrm

Password: ●●●●●●●●●●●●●

☑ Connect to SQL Server to obtain default settings for the additional configuration options.

- Click on “Change the default database to:” and specify the name of the SRM database.



Create a New Data Source to SQL Server

☑ Change the default database to:

vmwaresrm

Mirror server:

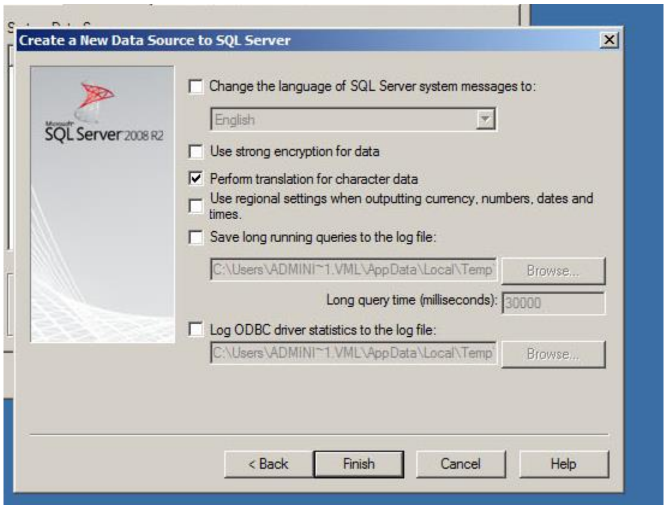
SPN for mirror server (Optional):

□ Attach database filename:

☑ Use ANSI quoted identifiers.

☑ Use ANSI nulls, paddings and warnings.

- Accept the defaults and click Finish.



Create a New Data Source to SQL Server

□ Change the language of SQL Server system messages to:

English

□ Use strong encryption for data

☑ Perform translation for character data

□ Use regional settings when outputting currency, numbers, dates and times.

□ Save long running queries to the log file:

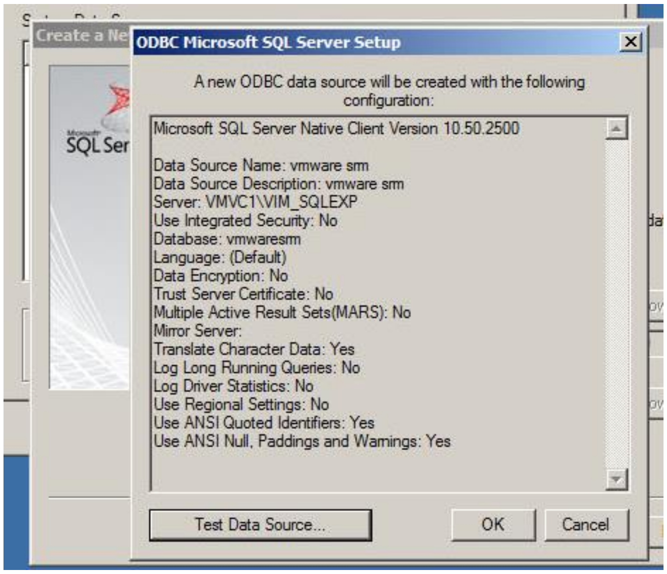
C:\Users\ADMINI~1.VML\AppData\Local\Temp Browse...

Long query time (milliseconds): 30000

□ Log ODBC driver statistics to the log file:

C:\Users\ADMINI~1.VML\AppData\Local\Temp Browse...

- All configured options will be displayed. Review them for correctness and click OK to complete the ODBC connector setup wizard.

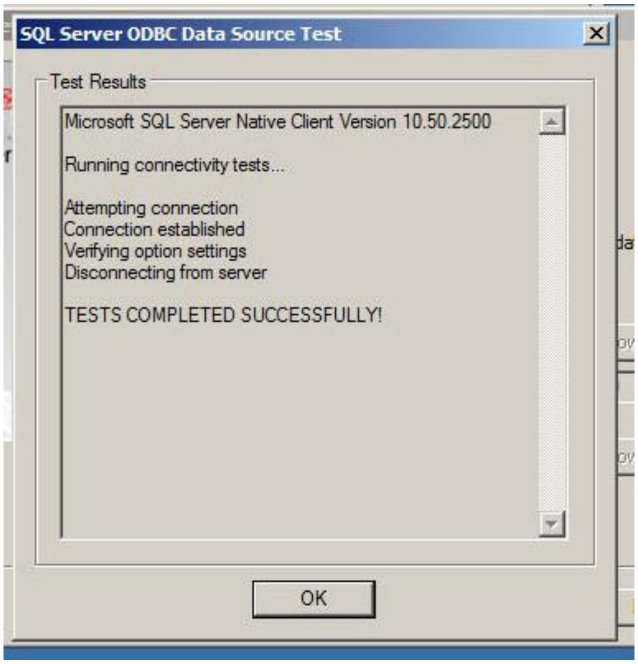


ODBC Microsoft SQL Server Setup

A new ODBC data source will be created with the following configuration:

```
Microsoft SQL Server Native Client Version 10.50.2500

Data Source Name: vmware srm
Data Source Description: vmware srm
Server: VMVC1\VIM_SQLEXP
Use Integrated Security: No
Database: vmwaresrm
Language: (Default)
Data Encryption: No
Trust Server Certificate: No
Multiple Active Result Sets(MARS): No
Mirror Server:
Translate Character Data: Yes
Log Long Running Queries: No
Log Driver Statistics: No
Use Regional Settings: No
Use ANSI Quoted Identifiers: Yes
Use ANSI Null, Paddings and Warnings: Yes
```

- Optionally, the DSN can be tested by clicking on the Test Data Source button. If everything was configured properly, the test should be successful as shown below.



```
Microsoft SQL Server Native Client Version 10.50.2500

Running connectivity tests...

Attempting connection
Connection established
Verifying option settings
Disconnecting from server

TESTS COMPLETED SUCCESSFULLY!
```

Chapter V

SITE RECOVERY MANAGER

Site Recovery Manager

Site Recovery Manager, aka SRM, is a Disaster Recovery Solutions from VMware. It makes use of either vSphere Replication or Storage Array Based Replication to Recover Virtual Machines from a Disaster (VMware, n.d.b).

Key Benefits of Using SRM

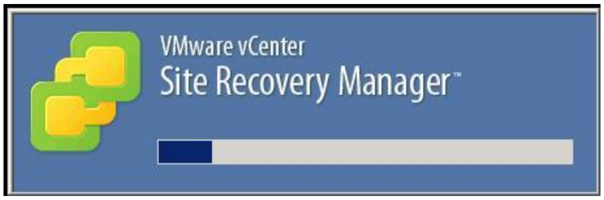
- SRM greatly simplifies and automates test and failover operations.
- Works along with VMware vSphere to enable faster, simpler, and more cost-effective disaster recovery.
- Allows failover configuration to be set on a per-VM basis.
- Administrator can expand disaster recovery protection to any application with minimal effort and cost.
- Allows for single-click recovery of hundreds of virtual machines, drastically reducing the time required for recovery.
- Eliminates hardware dependencies, as all components necessary for failover are virtualized.
- Simplifies the failover testing process to help ensure better preparedness in the case of an actual failure/disaster.
- Recovery and failover plans can be designed and modified dynamically in response to changing environments.
- Reduces capital and operating expenditures.

Installation of Site Recovery Manager (SRM)

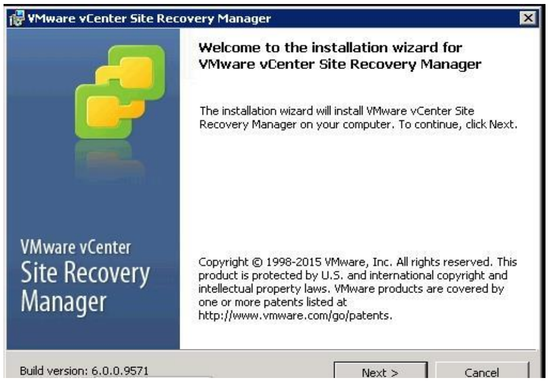
The installation media for Site Recovery Manager can be downloaded from the VMware website. To be able to download software from VMware, the user must first register for a VMware account and request a trial version of the product. We used the trial version in this paper.

Once the download is completed, start the installation on a machine which is running vCenter server or on a separate virtual machine running a supported Windows operating system. The installation of SRM should be carried out both in the protected and recovery sites.

- To begin the installation, mount the installation media and launch the included installer.



- Once the wizard starts, click Next and agree to the license agreement.



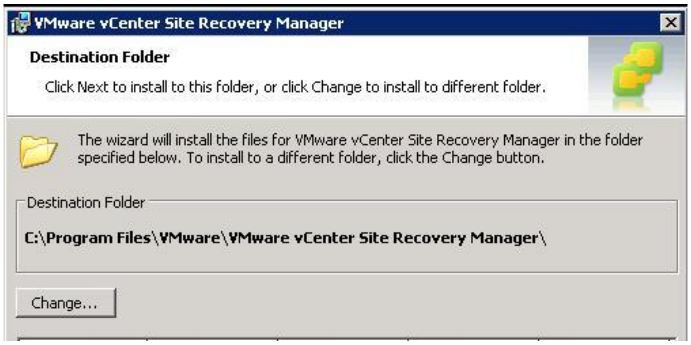
Welcome to the installation wizard for VMware vCenter Site Recovery Manager

The installation wizard will install VMware vCenter Site Recovery Manager on your computer. To continue, click Next.

Copyright © 1998-2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

Build version: 6.0.0.9571

- Specify an installation location and click Next to continue.



VMware vCenter Site Recovery Manager

Destination Folder

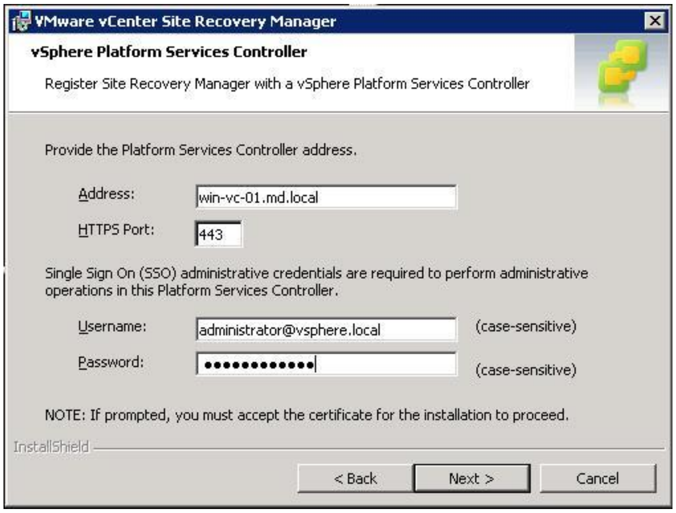
Click Next to install to this folder, or click Change to install to different folder.

The wizard will install the files for VMware vCenter Site Recovery Manager in the folder specified below. To install to a different folder, click the Change button.

Destination Folder

C:\Program Files\VMware\VMware vCenter Site Recovery Manager\

- Specify the vCenter Server Platform Services Controller address and port. The address must be a full-qualified host name or address. Also, specify the credentials of a Single Sign On account with administrative privileges, and click Next.



VMware vCenter Site Recovery Manager

vSphere Platform Services Controller

Register Site Recovery Manager with a vSphere Platform Services Controller

Provide the Platform Services Controller address.

Address: win-vc-01.md.local

HTTPS Port: 443

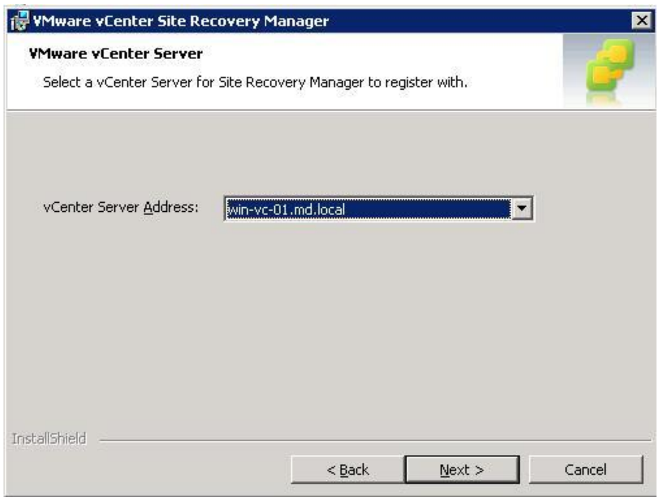
Single Sign On (SSO) administrative credentials are required to perform administrative operations in this Platform Services Controller.

Username: administrator@vsphere.local (case-sensitive)

Password: ••••••••••••• (case-sensitive)

NOTE: If prompted, you must accept the certificate for the installation to proceed.

- Select the vCenter Server instance for pairing up the SRM, and click Next to continue.



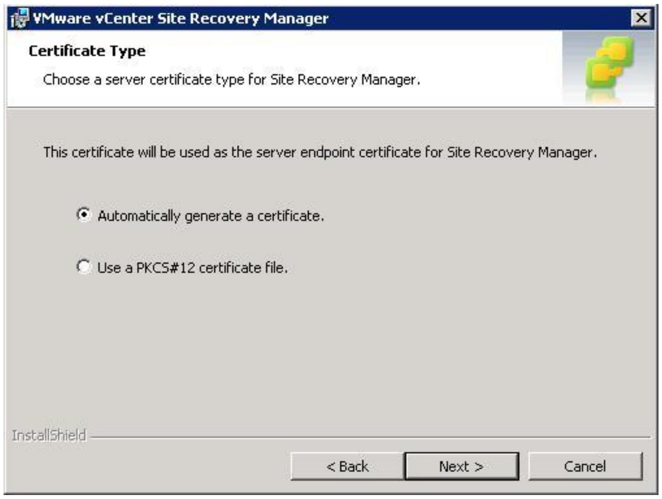
VMware vCenter Site Recovery Manager

VMware vCenter Server

Select a vCenter Server for Site Recovery Manager to register with.

vCenter Server Address: win-vc-01.md.local

- On the next stage of the wizard, specify a name for the site and an email address, and select the IP address of the host where SRM is installed.
- Let the wizard generate a SSL certificate. The certificate will be used to secure SRM traffic between servers.



VMware vCenter Site Recovery Manager

Certificate Type

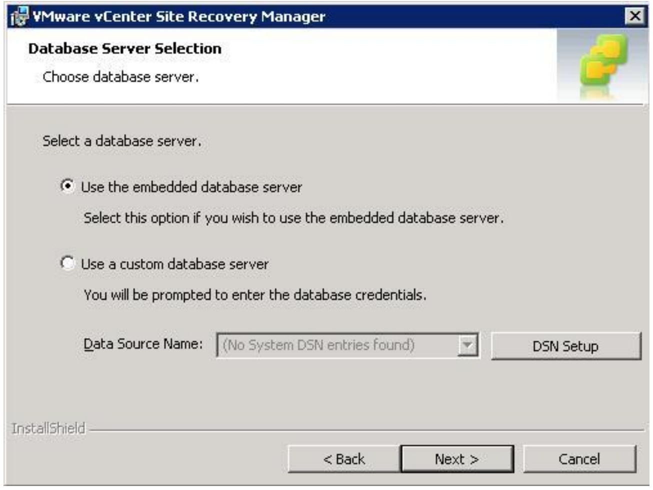
Choose a server certificate type for Site Recovery Manager.

This certificate will be used as the server endpoint certificate for Site Recovery Manager.

● Automatically generate a certificate.

○ Use a PKCS#12 certificate file.

- SRM server requires a database, which can be either a dedicated SQL Server database or the integrated database that comes bundled with SRM. It is recommended to have a separate, dedicated database in real production environments.



VMware vCenter Site Recovery Manager

Database Server Selection

Choose database server.

Select a database server.

● Use the embedded database server

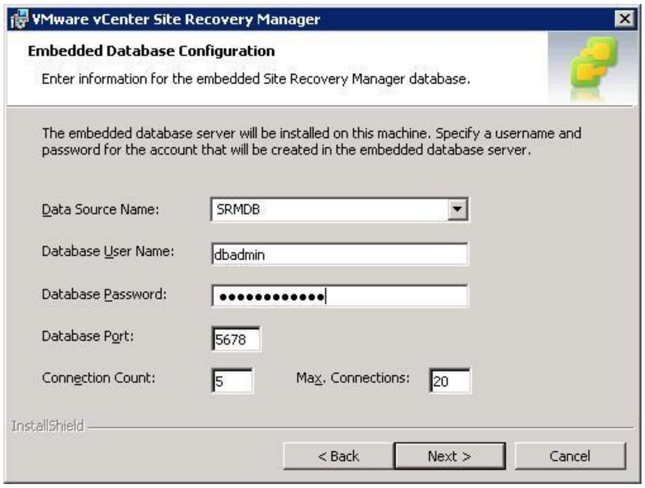
Select this option if you wish to use the embedded database server.

○ Use a custom database server

You will be prompted to enter the database credentials.

Data Source Name: (No System DSN entries found)

- Specify the DSN, database username and password, and port number for the database connection. The port will be 5678 by default, and it is recommended to not change it unless this port is being used by some other service. Finally, specify the database connection count and maximum connections limit, and click Next to continue.



VMware vCenter Site Recovery Manager

Embedded Database Configuration

Enter information for the embedded Site Recovery Manager database.

The embedded database server will be installed on this machine. Specify a username and password for the account that will be created in the embedded database server.

Data Source Name: SRMDB

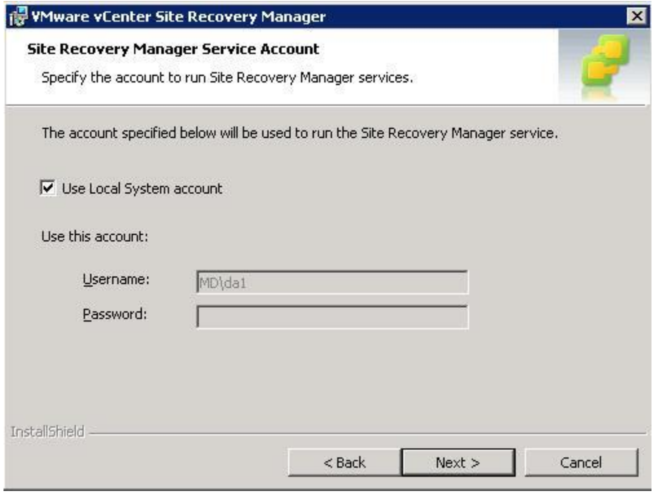
Database User Name: dbadmin

Database Password: ●●●●●●●●●●●●●

Database Port: 5678

Connection Count: 5 Max. Connections: 20

- Provide credentials for either a local system account or domain account under which the SRM service will be run.



VMware vCenter Site Recovery Manager

Site Recovery Manager Service Account

Specify the account to run Site Recovery Manager services.

The account specified below will be used to run the Site Recovery Manager service.

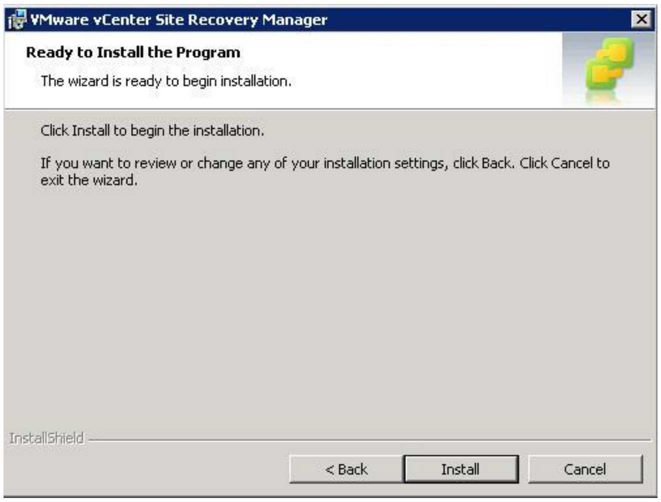
☑ Use Local System account

Use this account:

Username: MD\da1

Password:

- Once all steps of the wizard are complete, click Install to begin the SRM installation.



VMware vCenter Site Recovery Manager

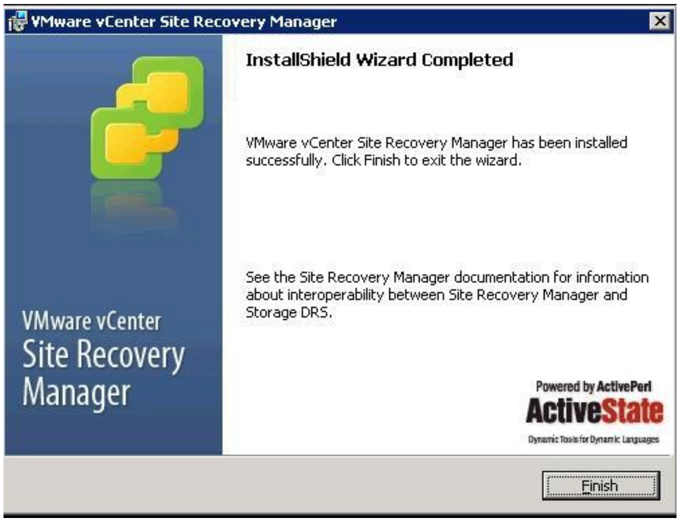
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

- Click Finish to complete the installation.



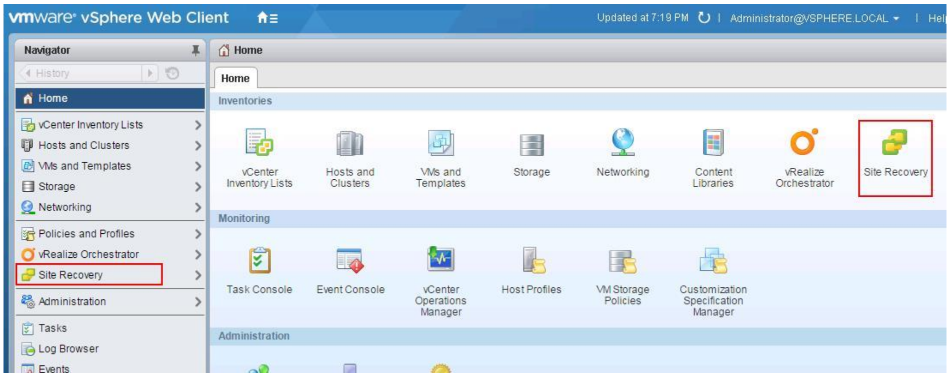
VMware vCenter Site Recovery Manager

InstallShield Wizard Completed

VMware vCenter Site Recovery Manager has been installed successfully. Click Finish to exit the wizard.

See the Site Recovery Manager documentation for information about interoperability between Site Recovery Manager and Storage DRS.

- Log into the vCenter Server in the primary/protected site using the vSphere Web Client and verify that Site Recovery is shown.



Repeat the same steps to install SRM at the secondary/recovery site. Once the installation is complete in the secondary site as well, log into the vCenter Server at the secondary site and verify that Site Recovery is present there as well.

Array-based Replication

Array-based Replication for business continuity can incorporate the creation of local copies of data within the same array as the source data, as well as the creation of remote copies in an array located elsewhere. Many enterprise storage vendors offer sophisticated technologies that provide this functionality, driven either from the arrays themselves -- via management hosts that control the direction and identity of replication -- or within a virtualization layer that operates in the SAN fabric or IP storage network.

Creating local and remote replicas of data gives an organization a limited form of business continuity and enhances its operational readiness by creating data copies that can be used for testing and development. Using storage technology, this is achieved at the volume level with features such as Quality of Service (QoS), priority controls, data consistency, source-target identity swaps, duplex data flow, protected copies, data queuing/batching, and full or pointer-based read/write.

The same functionality can be approximated at the host layer by using Logical Volume Manager (LVM) and plexes/mirrors as well as any "snap" functionality that may exist in the host LVM software. However, the feature set tends to be limited and management more painstaking due to the need to operate within LVM and in close logical proximity to the source data.

Creating local replicas for the purpose of business continuity is easily achieved using LVM when only one to three copies of that data are required. However, when four or more copies are required, and the business demands time-specific restore points, it is advisable to create replicas using the storage software. This is because there is a greater ability to create a large number of copies that can be synchronized and detached at specific intervals using advanced algorithms for incremental and full-data copy. This, combined with intelligent space management techniques such as copy on read/write, make the storage software offering highly effective.

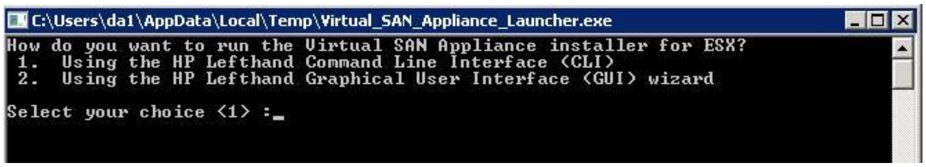
Installing HP SRA for SRM

For this research paper, we used an HP StoreVirtual (SV) storage appliance for VM storage. This provides array storage functionality for vSphere without requiring an external storage box. It makes a server’s internal storage available to ESXi servers as shared storage volumes. To download HP SV, registration is required on the HP website: https://www.hpe.com/us/en/storage/storevirtual.html.

Once HP SV is downloaded, the centralized management software should be downloaded as well. This additional software component is used to create storage LUNs and configure replication capabilities.

The steps required to install and configure HP SV are outlined below:

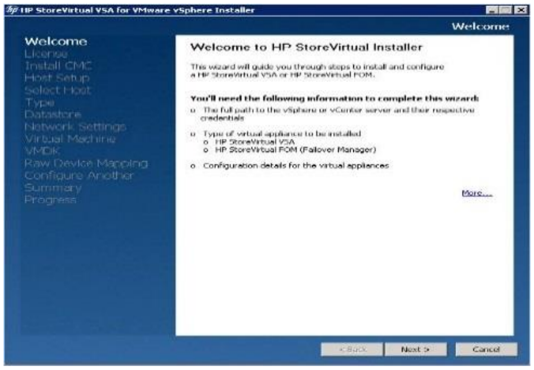
- Launch the downloaded installer and extract the files to a convenient location. Double-click Virtual_SAN_Appliance_launcher.exe and select option 2 to launch the graphical installation wizard.



C:\Users\da1\AppData\Local\Temp\Virtual_SAN_Appliance_Launcher.exe

```
How do you want to run the Virtual SAN Appliance installer for ESX?
 1.  Using the HP Lefthand Command Line Interface (CLI)
 2.  Using the HP Lefthand Graphical User Interface (GUI) wizard

Select your choice (1) :_
```

- A welcome message is displayed. Click Next to continue.



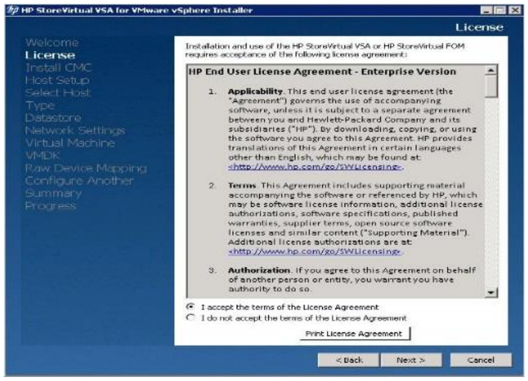
Welcome to HP StoreVirtual Installer

This wizard will guide you through steps to install and configure a HP StoreVirtual VSA or HP StoreVirtual FOM.

You'll need the following information to complete this wizard:

- The full path to the vSphere or vCenter server and their respective credentials
- Type of virtual appliance to be installed
  - HP StoreVirtual VSA
  - HP StoreVirtual FOM (Failover Manager)
- Configuration details for the virtual appliances

- Accept the license agreement and click Next to continue.



Installation and use of the HP StoreVirtual VSA or HP StoreVirtual FOM requires acceptance of the following license agreement:

HP End User License Agreement - Enterprise Version

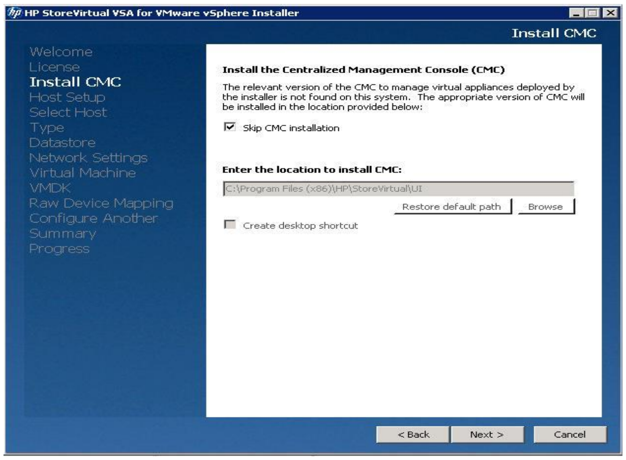
1. **Applicability**. This end user license agreement (the "Agreement") governs the use of accompanying software, unless it is subject to a separate agreement between you and Hewlett-Packard Company and its subsidiaries ("HP"). By downloading, copying, or using the software you agree to this Agreement. HP provides translations of this Agreement in certain languages other than English, which may be found at: <http://www.hp.com/go/SWLicensing>.

2. **Terms**. This Agreement includes supporting material accompanying the software or referenced by HP, which may be software license information, additional license authorizations, software specifications, published warranties, supplier terms, open source software licenses and similar content ("Supporting Material"). Additional license authorizations are at: <http://www.hp.com/go/SWLicensing>.

3. **Authorization**. If you agree to this Agreement on behalf of another person or entity, you warrant you have authority to do so.

● I accept the terms of the License Agreement
○ I do not accept the terms of the License Agreement

- Deselect the Skip CMC (Centralized Management Console) Installation option and click Next.



Install the Centralized Management Console (CMC)

The relevant version of the CMC to manage virtual appliances deployed by the installer is not found on this system. The appropriate version of CMC will be installed in the location provided below:

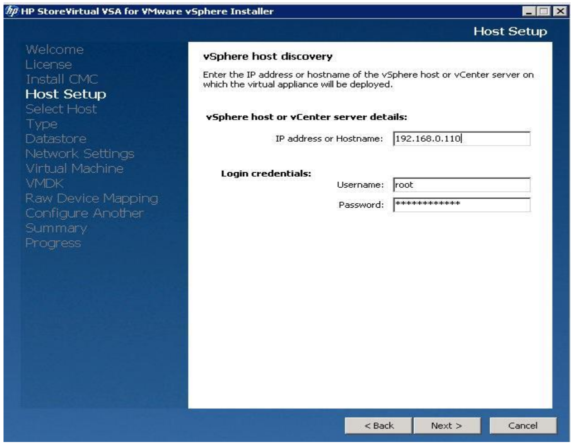
☑ Skip CMC installation

Enter the location to install CMC:

C:\Program Files (x86)\HP\StoreVirtual\UI

□ Create desktop shortcut

- Provide the IP address and root user credentials for the ESXi where the appliance should be deployed.



HP StoreVirtual VSA for VMware vSphere Installer

Host Setup

vSphere host discovery

Enter the IP address or hostname of the vSphere host or vCenter server on which the virtual appliance will be deployed.

vSphere host or vCenter server details:

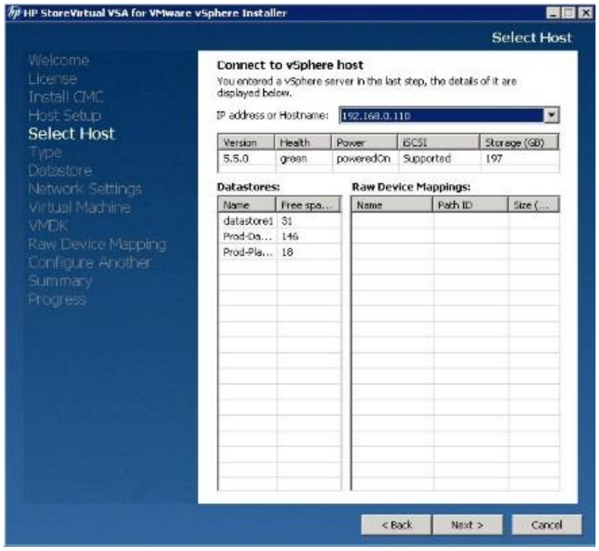
IP address or Hostname: 192.168.0.110

Login credentials:

Username: root

Password: *************

- Review the ESXi host and datastore information, and click Next to proceed.



HP StoreVirtual VSA for VMware vSphere Installer

Select Host

Connect to vSphere host

You entered a vSphere server in the last step, the details of it are displayed below.

IP address or Hostname: 192.168.0.110

Version	Health	Power	iSCSI	Storage (GB)
5.5.0	green	poweredOn	Supported	197

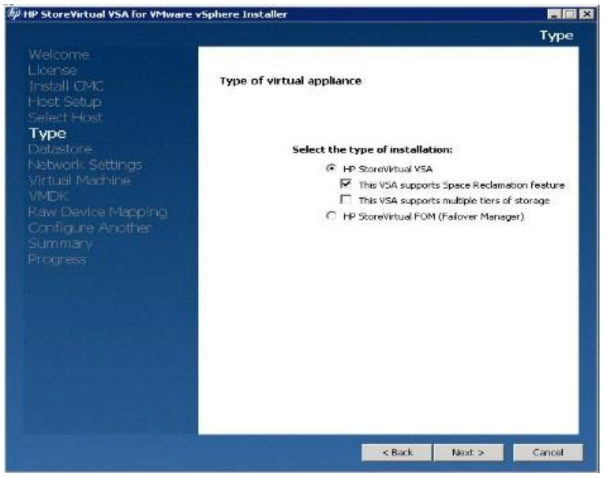
Datastores:

Name	Free spa...
datastore1	31
Prod-Da...	146
Prod-Pla...	18

Raw Device Mappings:

Name	Path ID	Size (...

- Select HP StoreVirtual VSA as the installation type. Additional options like Space Reclamation and multi-tiered storage support can be selected. Click Next to continue.



Type of virtual appliance

Select the type of installation:

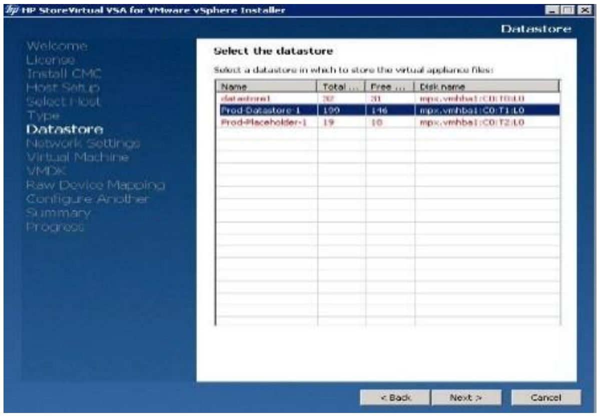
● HP StoreVirtual VSA

☑ This VSA supports Space Reclamation feature

☐ This VSA supports multiple tiers of storage

○ HP StoreVirtual FOM (Failover Manager)

- Select the datastore to deploy the HP SV appliance to, and click Next.

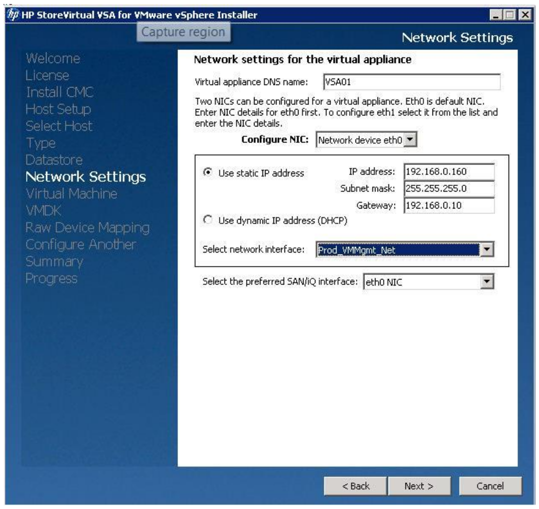


Select the datastore

Select a datastore in which to store the virtual appliance files:

Name	Total ...	Free ...	Disk name
datastore1	32	31	mpx.vmhba1:C0:T0:L0
Prod-Datastore-1	199	146	mpx.vmhba1:C0:T1:L0
Prod-Placeholder-1	19	10	mpx.vmhba1:C0:T2:L0

- Assign an IP address, DNS name and virtual machine port group to the appliance. Click Next to continue.



Network settings for the virtual appliance

Virtual appliance DNS name: VSA01

Two NICs can be configured for a virtual appliance. Eth0 is default NIC. Enter NIC details for eth0 first. To configure eth1 select it from the list and enter the NIC details.

Configure NIC: Network device eth0

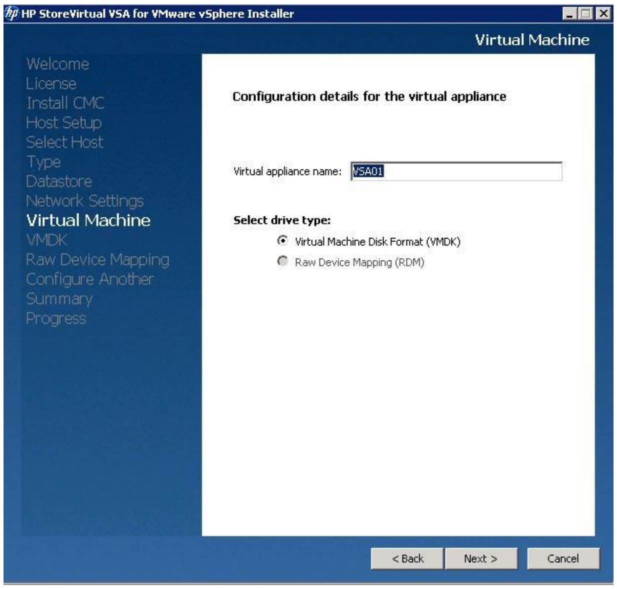
● Use static IP address
IP address: 192.168.0.160
Subnet mask: 255.255.255.0
Gateway: 192.168.0.10

○ Use dynamic IP address (DHCP)

Select network interface: Prod_VMMgmt_Net

Select the preferred SAN/iQ interface: eth0 NIC

- Specify a name for the virtual appliance, and select VMDK as the drive type. Click Next to continue.



Configuration details for the virtual appliance

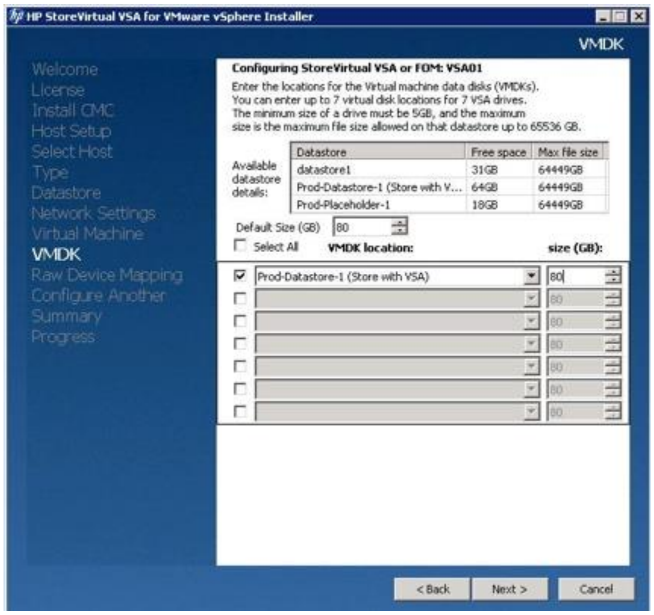
Virtual appliance name: VSA01

Select drive type:

● Virtual Machine Disk Format (VMDK)

○ Raw Device Mapping (RDM)

- Select a location for VMDK files on the ESXi server. This will be the storage destination presented to ESXi hosts as a datastore. Click Next to continue.



Configuring StoreVirtual VSA or FOM: VSA01

Enter the locations for the Virtual machine data disks (VMDKs).
You can enter up to 7 virtual disk locations for 7 VSA drives.
The minimum size of a drive must be 5GB, and the maximum
size is the maximum file size allowed on that datastore up to 65536 GB.

Available datastore details:

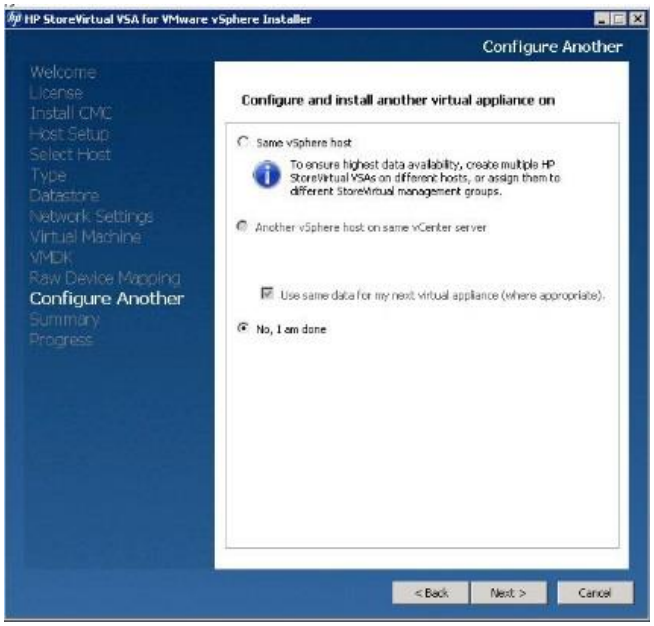
Datastore	Free space	Max file size
datastore1	31GB	64449GB
Prod-Datastore-1 (Store with V...	64GB	64449GB
Prod-Placeholder-1	18GB	64449GB

Default Size (GB) 80

□ Select All

	VMDK location:	size (GB):
☑	Prod-Datastore-1 (Store with VSA)	80
□		80
□		80
□		80
□		80
□		80
□		80

- If desired, a second virtual appliance can be deployed with the same wizard. Click on No, I am done click Next to continue with just the one SV appliance.



Configure and install another virtual appliance on

○ Same vSphere host

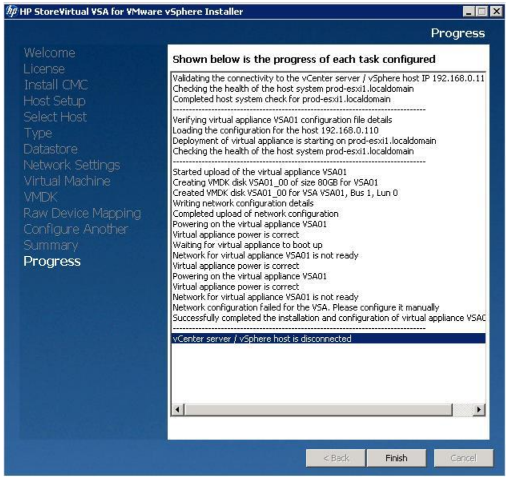
To ensure highest data availability, create multiple HP StoreVirtual VSAs on different hosts, or assign them to different StoreVirtual management groups.

○ Another vSphere host on same vCenter server

☑ Use same data for my next virtual appliance (where appropriate).

● No, I am done

- A progress screen will be displayed as the deployment proceeds. Once complete, click Finish.



Shown below is the progress of each task configured

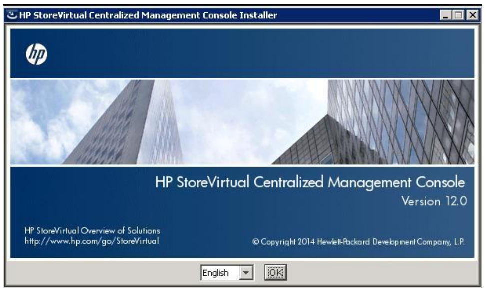
```
Validating the connectivity to the vCenter server / vSphere host IP 192.168.0.11
Checking the health of the host system prod-esxi1.localdomain
Completed host system check for prod-esxi1.localdomain
------------------------------------------------------------------------
Verifying virtual appliance VSA01 configuration file details
Loading the configuration for the host 192.168.0.110
Deployment of virtual appliance is starting on prod-esxi1.localdomain
Checking the health of the host system prod-esxi1.localdomain
------------------------------------------------------------------------
Started upload of the virtual appliance VSA01
Creating VMDK disk VSA01_00 of size 80GB for VSA01
Created VMDK disk VSA01_00 for VSA VSA01, Bus 1, Lun 0
Writing network configuration details
Completed upload of network configuration
Powering on the virtual appliance VSA01
Virtual appliance power is correct
Waiting for virtual appliance to boot up
Network for virtual appliance VSA01 is not ready
Virtual appliance power is correct
Powering on the virtual appliance VSA01
Virtual appliance power is correct
Network for virtual appliance VSA01 is not ready
Network configuration failed for the VSA. Please configure it manually
Successfully completed the installation and configuration of virtual appliance VSA0
------------------------------------------------------------------------
vCenter server / vSphere host is disconnected
```

Repeat the same steps to deploy the HP SV appliance at the secondary site, which can be used to map datastores to the ESXi servers in the secondary site. Once this process is complete, SRM uses those datastores for array-based replication.

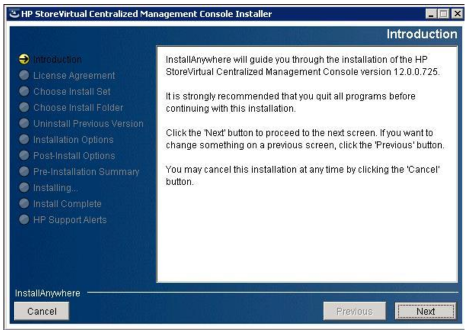
Configuring HP Virtual Storage Array.

Once our virtual storage appliances have been deployed, we need to perform some configuration steps to make the appliance's storage resources available to the VMware infrastructure. Log into the vCenter Server instance at the protected site and complete the following steps.

- Locate and launch the HP SV Centralized Management Console installer. Specify a language preference and click OK to continue.


HP StoreVirtual Centralized Management Console Installer
hp
HP StoreVirtual Centralized Management Console
Version 12.0
HP StoreVirtual Overview of Solutions
http://www.hp.com/go/StoreVirtual
© Copyright 2014 Hewlett-Packard Development Company, L.P.
English
OK

- On the Introduction screen, click Next to continue.



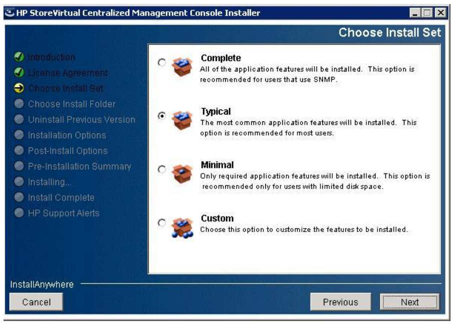
InstallAnywhere will guide you through the installation of the HP StoreVirtual Centralized Management Console version 12.0.0.725.

It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

- Select the Typical install set, and click Next to continue.



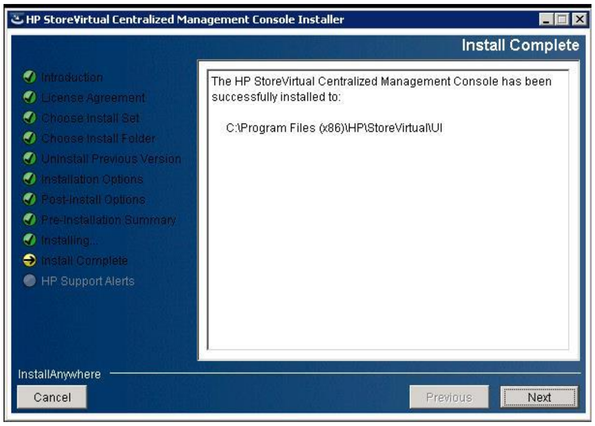
○ **Complete**
All of the application features will be installed. This option is recommended for users that use SNMP.

● **Typical**
The most common application features will be installed. This option is recommended for most users.

○ **Minimal**
Only required application features will be installed. This option is recommended only for users with limited disk space.

○ **Custom**
Choose this option to customize the features to be installed.

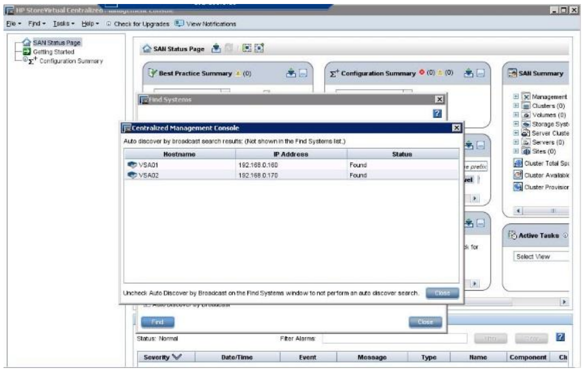
- The rest of the installation steps should not require any specific user input. Click Next as necessary to complete the wizard.



The HP StoreVirtual Centralized Management Console has been successfully installed to:

C:\Program Files (x86)\HP\StoreVirtual\UI

- Once the installation is complete, launch the HP CMC application. It should detect the HP SV appliance(s) that were deployed on the ESXi servers automatically. If the auto-detection fails, we can locate the HP SV appliance manually by clicking on the Find button.



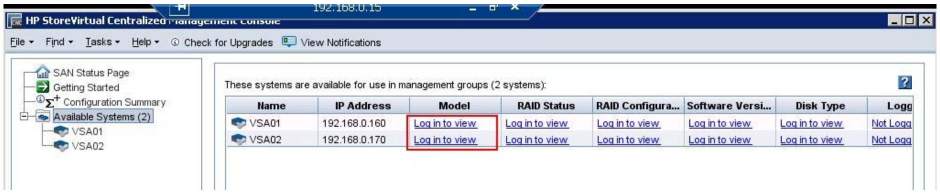
Centralized Management Console

Auto discover by broadcast search results: (Not shown in the Find Systems list.)

Hostname	IP Address	Status
VSA01	192.168.0.160	Found
VSA02	192.168.0.170	Found

Uncheck Auto Discover by Broadcast on the Find Systems window to not perform an auto discover search.

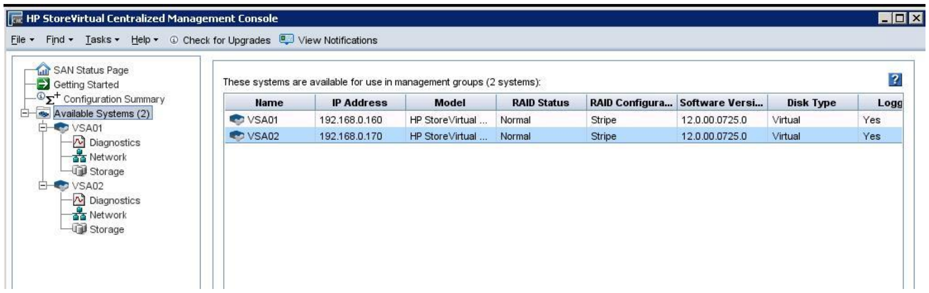
- Click on Login to view on the HP SV appliance that was deployed in the previous steps to review the storage appliance configuration.



These systems are available for use in management groups (2 systems):

Name	IP Address	Model	RAID Status	RAID Configura...	Software Versi...	Disk Type	Logg
VSA01	192.168.0.160	Log in to view	Log in to view	Log in to view	Log in to view	Log in to view	Not Logg
VSA02	192.168.0.170	Log in to view	Log in to view	Log in to view	Log in to view	Log in to view	Not Logg

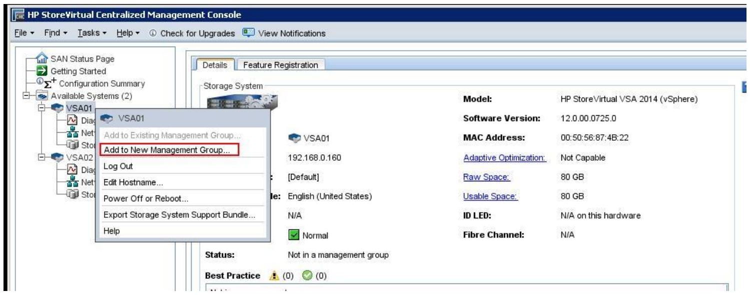
- After log in



These systems are available for use in management groups (2 systems):

Name	IP Address	Model	RAID Status	RAID Configura...	Software Versi...	Disk Type	Logg
VSA01	192.168.0.160	HP StoreVirtual ...	Normal	Stripe	12.0.00.0725.0	Virtual	Yes
VSA02	192.168.0.170	HP StoreVirtual ...	Normal	Stripe	12.0.00.0725.0	Virtual	Yes

- Next, we need to create a management group. Right-click the VSA node and select Add to New Management Group from the context menu. Create two management groups, one for the primary site and the other for the secondary site. These groups will be used by SRM for array-based replication.



VSA01

192.168.0.160

[Default]

English (United States)

N/A

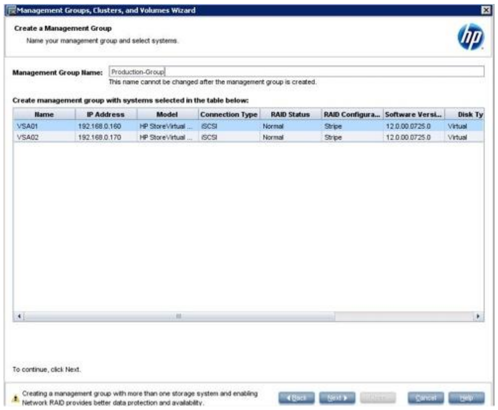
Normal

Status: Not in a management group

Best Practice (0) (0)

Model:	HP StoreVirtual VSA 2014 (vSphere)
Software Version:	12.0.00.0725.0
MAC Address:	00:50:56:87:4B:22
Adaptive Optimization:	Not Capable
Raw Space:	80 GB
Usable Space:	80 GB
ID LED:	N/A on this hardware
Fibre Channel:	N/A

- Specify a name for the management group and click on Next to continue.



Create a Management Group

Name your management group and select systems.

Management Group Name: Production-Group

This name cannot be changed after the management group is created.

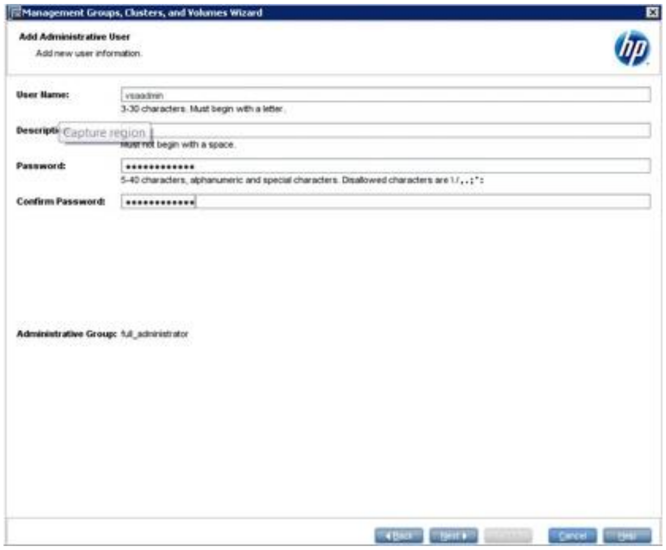
Create management group with systems selected in the table below:

Name	IP Address	Model	Connection Type	RAID Status	RAID Configura...	Software Versi...	Disk Ty
VSA01	192.168.0.160	HP StoreVirtual ...	iSCSI	Normal	Stripe	12.0.00.0725.0	Virtual
VSA02	192.168.0.170	HP StoreVirtual ...	iSCSI	Normal	Stripe	12.0.00.0725.0	Virtual

To continue, click Next.

Creating a management group with more than one storage system and enabling Network RAID provides better data protection and availability.

- Create an administrative user to manage the group. Click Next to continue.



Add Administrative User

Add new user information.

User Name: vsaadmin

3-30 characters. Must begin with a letter.

Descripti

Must not begin with a space.

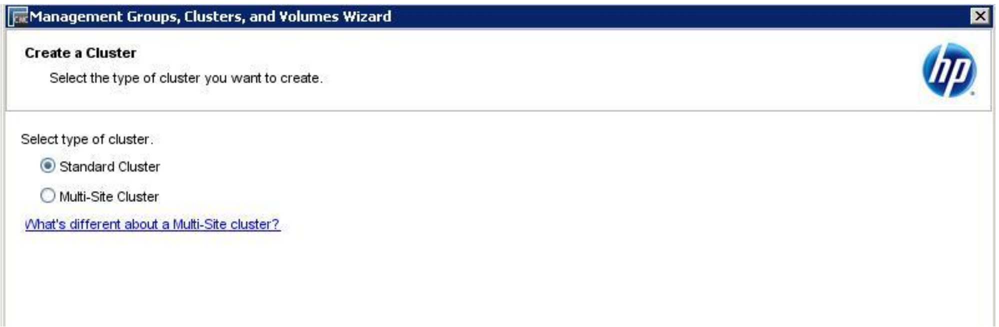
Password: ••••••••••••

5-40 characters, alphanumeric and special characters. Disallowed characters are \/,.;":

Confirm Password: ••••••••••••

Administrative Group: full_administrator

- Configure the time setting using a Network Time Protocol server, assign a DNS server, and select the cluster type as shown below. As one VSA is being used per site, select Standard Cluster.



Management Groups, Clusters, and Volumes Wizard

Create a Cluster

Select the type of cluster you want to create.

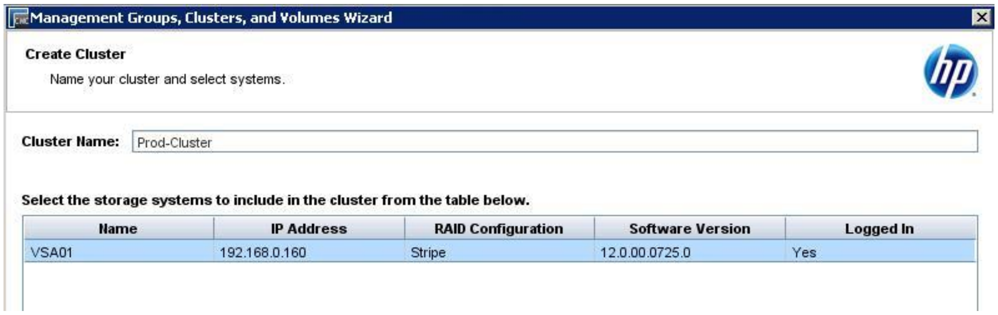
Select type of cluster.

● Standard Cluster

○ Multi-Site Cluster

What's different about a Multi-Site cluster?

- Provide a name for the cluster and add the first VSA.



Management Groups, Clusters, and Volumes Wizard

Create Cluster

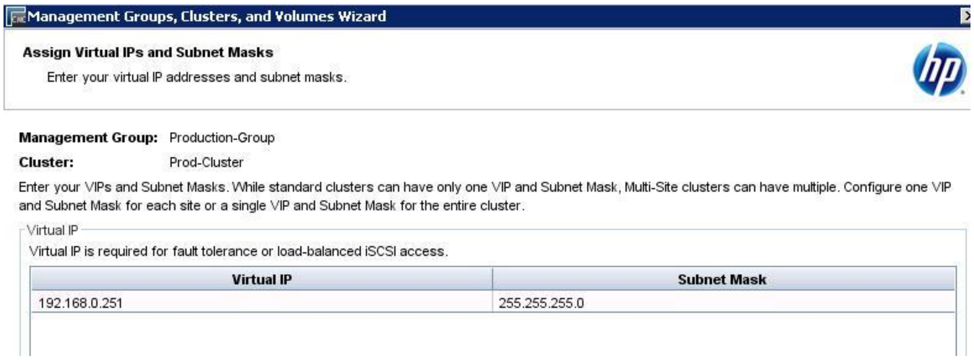
Name your cluster and select systems.

Cluster Name: Prod-Cluster

Select the storage systems to include in the cluster from the table below.

Name	IP Address	RAID Configuration	Software Version	Logged In
VSA01	192.168.0.160	Stripe	12.0.00.0725.0	Yes

- Assign an IP address and subnet mask to the cluster. This IP will be used as a storage target for the ESXi servers when adding a datastore.



Management Groups, Clusters, and Volumes Wizard

Assign Virtual IPs and Subnet Masks

Enter your virtual IP addresses and subnet masks.

Management Group: Production-Group

Cluster: Prod-Cluster

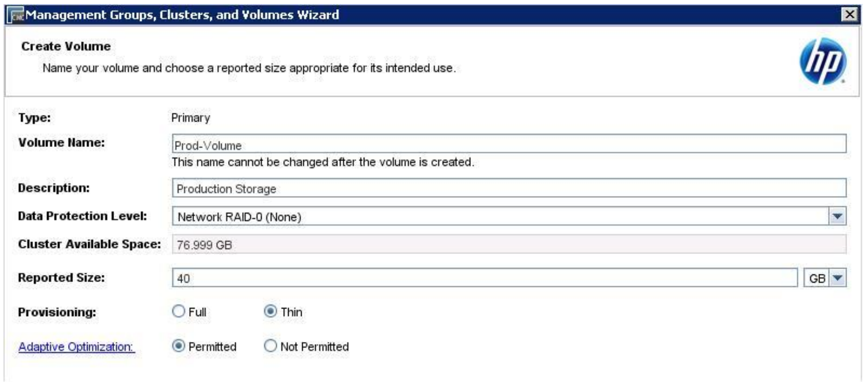
Enter your VIPs and Subnet Masks. While standard clusters can have only one VIP and Subnet Mask, Multi-Site clusters can have multiple. Configure one VIP and Subnet Mask for each site or a single VIP and Subnet Mask for the entire cluster.

Virtual IP

Virtual IP is required for fault tolerance or load-balanced iSCSI access.

Virtual IP	Subnet Mask
192.168.0.251	255.255.255.0

- We are now able to create a volume and provision space to it.



Management Groups, Clusters, and Volumes Wizard

Create Volume

Name your volume and choose a reported size appropriate for its intended use.

Type: Primary

Volume Name: Prod-Volume

This name cannot be changed after the volume is created.

Description: Production Storage

Data Protection Level: Network RAID-0 (None)

Cluster Available Space: 76.999 GB

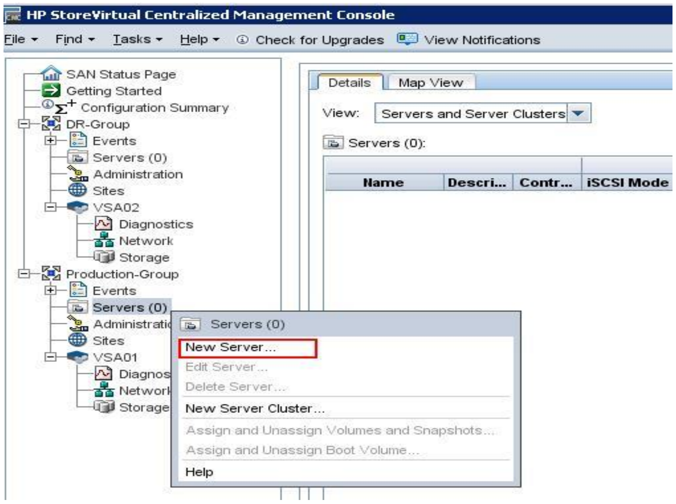
Reported Size: 40 GB

Provisioning: ○ Full ● Thin

Adaptive Optimization: ● Permitted ○ Not Permitted

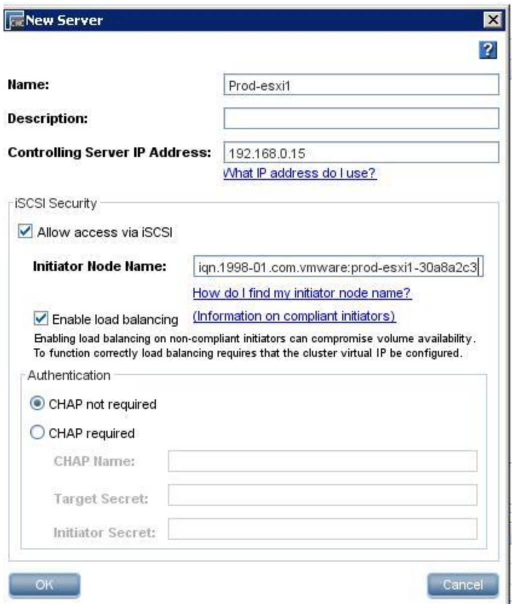
- Repeat the same steps to a create management group and provision storage for the secondary site.

Add the ESXi Server to the HP CMC. We can now see the datastores presented to the ESXi servers. Right-click on the Servers node and click on New Server from the context menu.



HP StoreVirtual Centralized Management Console

In the New Server dialog, we can configure details about the server that will be accessing the VSA storage. Provide a name and IP address for the vCenter Server instance. Specify an iSCSI IQN address, configure load balancing (if desired), and configure CHAP authentication for connections to the VSA.



New Server

Name: Prod-esxi1

Description:

Controlling Server IP Address: 192.168.0.15

What IP address do I use?

iSCSI Security

☑ Allow access via iSCSI

Initiator Node Name: iqn.1998-01.com.vmware:prod-esxi1-30a8a2c3

How do I find my initiator node name?

☑ Enable load balancing (Information on compliant initiators)

Enabling load balancing on non-compliant initiators can compromise volume availability. To function correctly load balancing requires that the cluster virtual IP be configured.

Authentication

● CHAP not required

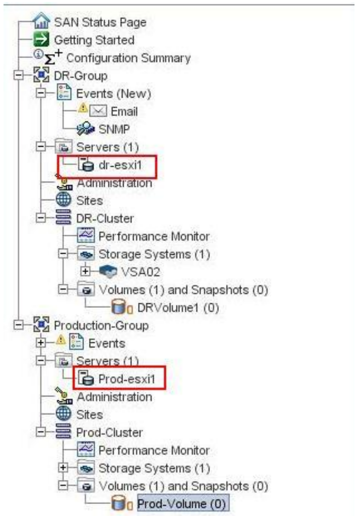
○ CHAP required

CHAP Name:

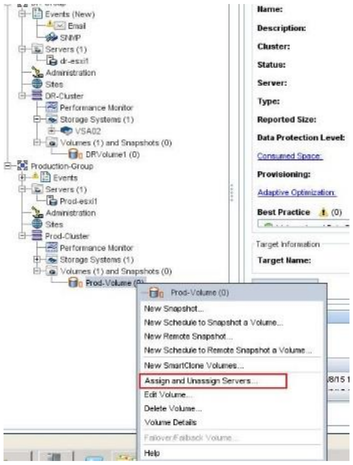
Target Secret:

Initiator Secret:

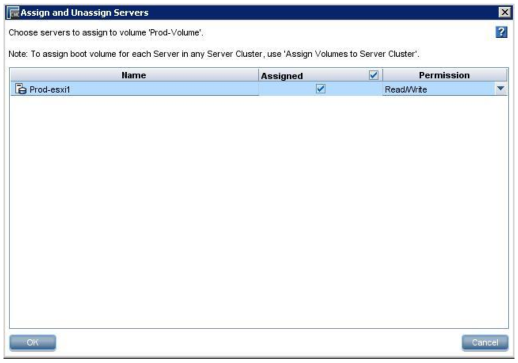
- Follow the same steps to add the server in the secondary site as well.



- As the ESXi hosts are already added to the management group, the next step is to make the ESXi servers access the storage volumes created in the earlier steps. To perform this operation, right-click on the storage volume and click on Assign and Unassigned Servers from the context menu.



- Locate the primary site ESXi server from the list and select the Assigned checkbox.



Assign and Unassign Servers

Choose servers to assign to volume 'Prod-Volume'.

Note: To assign boot volume for each Server in any Server Cluster, use 'Assign Volumes to Server Cluster'.

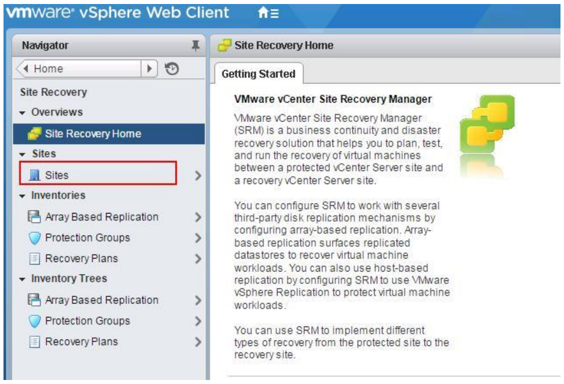
Name	Assigned ☑	Permission
Prod-esxi1	☑	Read/Write

Next, log into the ESXi server, click on Configuration, click on Storage Adapters under Hardware, click on click of the adapter and click on dynamic discovery and add the virtual IP of the management cluster created in the previous steps. Click OK.

Finally, complete the same steps for the secondary site.

Pairing Site Recovery Manager Servers

Once the HP SV appliance installation is complete and the SRM plugin appears in the vCenter Servers at both sites, we next need to pair the two sites so they can be used as a single DR group**.** Using the vSphere Web Client, log into the vCenter instance at the protected site, click on Site Recovery, and click on Sites as shown below. Complete the following steps to pair the two sites.



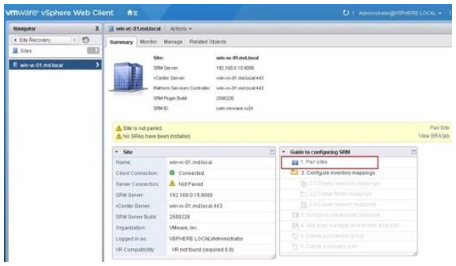
VMware vCenter Site Recovery Manager

VMware vCenter Site Recovery Manager (SRM) 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 site and a recovery vCenter Server site.

You can configure SRM to work with several third-party disk replication mechanisms by configuring array-based replication. Array-based replication surfaces replicated datastores to recover virtual machine workloads. You can also use host-based replication by configuring SRM to use VMware vSphere Replication to protect virtual machine workloads.

You can use SRM to implement different types of recovery from the protected site to the recovery site.

- On Sites, click on the Summary tab and then click on the Pair Sites option.

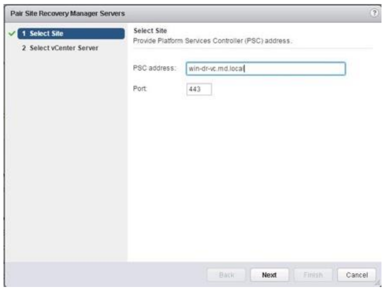


Site: win-vc-01.md.local
SRM Server: 192.168.0.15:9086
vCenter Server: win-vc-01.md.local:443
Platform Services Controller: win-vc-01.md.local:443
SRM Plugin Build: 2580226
SRM ID: com.vmware.vcDr

Site is not paired
No SRAs have been installed

Site
Name: win-vc-01.md.local
Client Connection: Connected
Server Connection: Not Paired
SRM Server: 192.168.0.15:9086
vCenter Server: win-vc-01.md.local:443
SRM Server Build: 2580226
Organization: VMware, Inc.
Logged in as: VSPHERE.LOCAL\Administrator
VR Compatibility: VR not found (required 6.0)

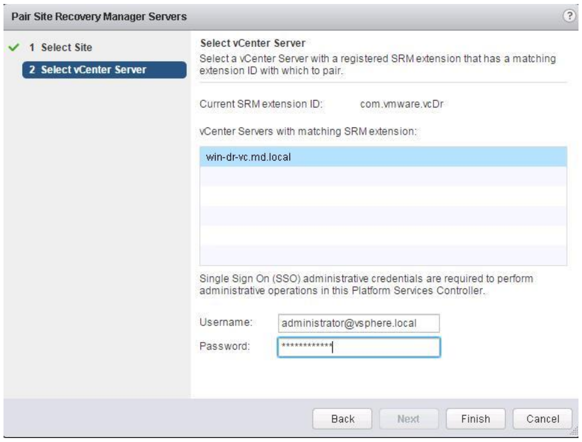
- Specify the IP address or fully-qualified domain name of the Platform Services Controller at the secondary site. Leave the port number at the default setting. Click Next to continue.



Select Site
Provide Platform Services Controller (PSC) address.

PSC address: win-dr-vc.md.local
Port: 443

- Once the PSC is specified, the wizard detects the vCenter Server associated with the PSC. Enter the Single Sign On credentials of the vCenter Server.



Select vCenter Server

Select a vCenter Server with a registered SRM extension that has a matching extension ID with which to pair.

Current SRM extension ID: com.vmware.vcDr

vCenter Servers with matching SRM extension:

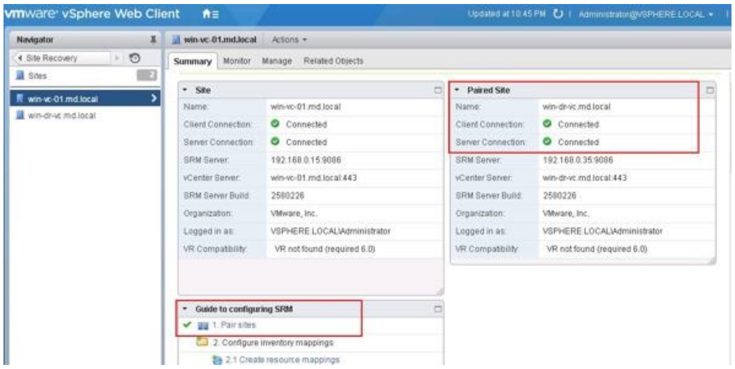
win-dr-vc.md.local

Single Sign On (SSO) administrative credentials are required to perform administrative operations in this Platform Services Controller.

Username: administrator@vsphere.local

Password: ************

- Once the pairing is complete, the wizard will automatically show the primary site and secondary site information as shown below.



Site	
Name:	win-vc-01.md.local
Client Connection:	Connected
Server Connection:	Connected
SRM Server:	192.168.0.15:9086
vCenter Server:	win-vc-01.md.local:443
SRM Server Build:	2580226
Organization:	VMware, Inc.
Logged in as:	VSPHERE.LOCAL\Administrator
VR Compatibility:	VR not found (required 6.0)

Paired Site	
Name:	win-dr-vc.md.local
Client Connection:	Connected
Server Connection:	Connected
SRM Server:	192.168.0.35:9086
vCenter Server:	win-dr-vc.md.local:443
SRM Server Build:	2580226
Organization:	VMware, Inc.
Logged in as:	VSPHERE.LOCAL\Administrator
VR Compatibility:	VR not found (required 6.0)

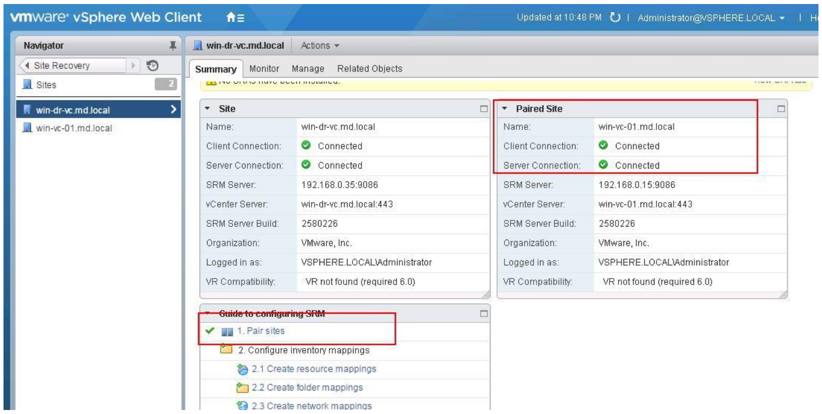
Guide to configuring SRM

✓ 1. Pair sites

2. Configure inventory mappings

2.1 Create resource mappings

- The configuration can also be verified by connecting to the vCenter Server instance at the secondary site. This pairing process need only be completed at one site, and will be reflected at both.



Site	
Name:	win-dr-vc.md.local
Client Connection:	Connected
Server Connection:	Connected
SRM Server:	192.168.0.35:9086
vCenter Server:	win-dr-vc.md.local:443
SRM Server Build:	2580226
Organization:	VMware, Inc.
Logged in as:	VSPHERE.LOCAL\Administrator
VR Compatibility:	VR not found (required 6.0)

Paired Site	
Name:	win-vc-01.md.local
Client Connection:	Connected
Server Connection:	Connected
SRM Server:	192.168.0.15:9086
vCenter Server:	win-vc-01.md.local:443
SRM Server Build:	2580226
Organization:	VMware, Inc.
Logged in as:	VSPHERE.LOCAL\Administrator
VR Compatibility:	VR not found (required 6.0)

Guide to configuring SRM

✓ 1. Pair sites

2. Configure inventory mappings

2.1 Create resource mappings

2.2 Create folder mappings

2.3 Create network mappings

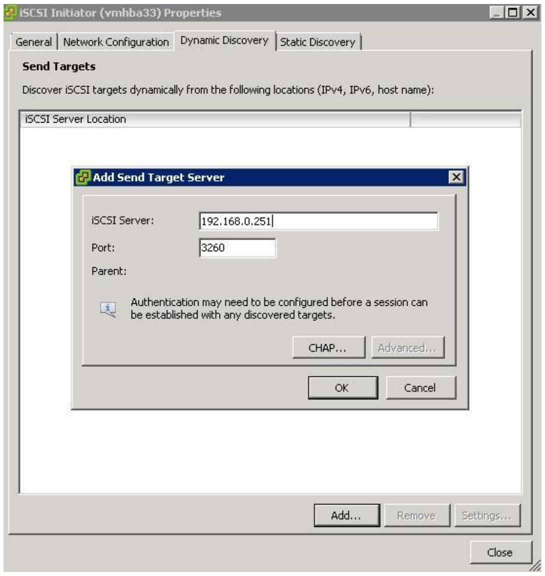
- Once the two sites are paired, we next need to configure the HP Array Manager at both sites.

HP SRA Array Manager for SRM.

The HP Array Configuration Utility (ACU) provides online, high availability configuration, management, and diagnostic capabilities in support of all Smart Array products and particular HP ProLiant Storage RAID Array Controllers. The software consistency of the related tools reduces the cost of training for each successive generation of product and takes much of the guesswork out of troubleshooting field problems. These tools lower the total cost of ownership by reducing training and technical expertise necessary to install and maintain HP server storage.

HP Array Configuration Utility 64-bit is a program developed by Hewlett-Packard. The software installer includes seven files and is usually about 5.55 MB (5,816,320 bytes). In comparison to the total number of users, most PCs are running the OS Windows 7 (SP1) as well as Windows 8 (Hewlett Packard, 20150.

Configuring the HP Array Manager at the primary and secondary sites.



Send Targets

Discover iSCSI targets dynamically from the following locations (IPv4, IPv6, host name):

iSCSI Server Location	

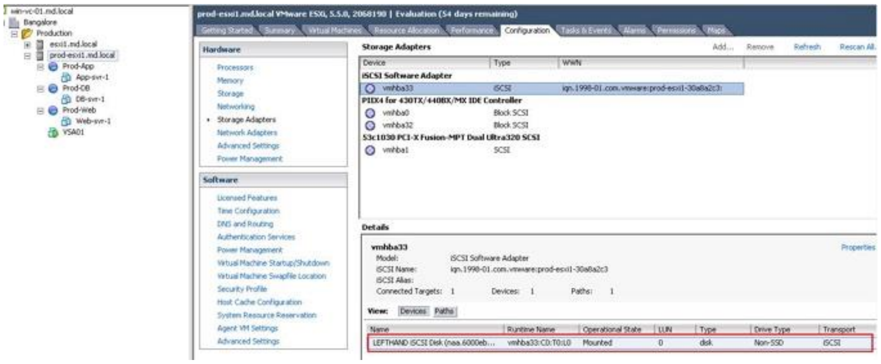
iSCSI Server: 192.168.0.251

Port: 3260

Parent:

Authentication may need to be configured before a session can be established with any discovered targets.

- Click on Rescan All. After a short wait, the storage LUNs provided by the VSA will be detected. Add the LUN as storage to the ESXi host.



prod-esxi1.md.local VMware ESXi, 5.5.0, 2068190 | Evaluation (54 days remaining)

Storage Adapters

Device	Type	WWN
iSCSI Software Adapter		
vmhba33	iSCSI	iqn.1998-01.com.vmware:prod-esxi1-30a8a2c3:
PIIX4 for 430TX/440BX/MX IDE Controller		
vmhba0	Block SCSI	
vmhba32	Block SCSI	
53c1030 PCI-X Fusion-MPT Dual Ultra320 SCSI		
vmhba1	SCSI	

Details

vmhba33

Model: iSCSI Software Adapter

iSCSI Name: iqn.1998-01.com.vmware:prod-esxi1-30a8a2c3

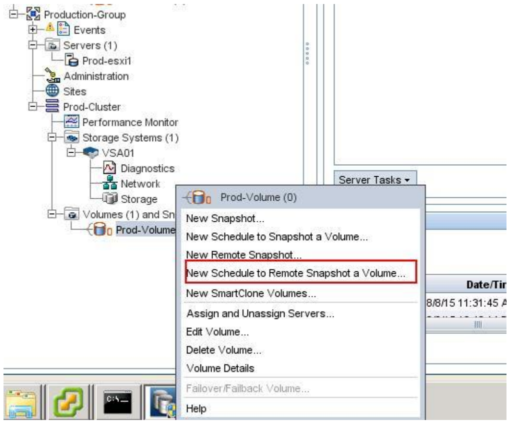
iSCSI Alias:

Connected Targets: 1 Devices: 1 Paths: 1

Name	Runtime Name	Operational State	LUN	Type	Drive Type	Transport
LEFTHAND iSCSI Disk (naa.6000eb...	vmhba33:C0:T0:L0	Mounted	0	disk	Non-SSD	iSCSI

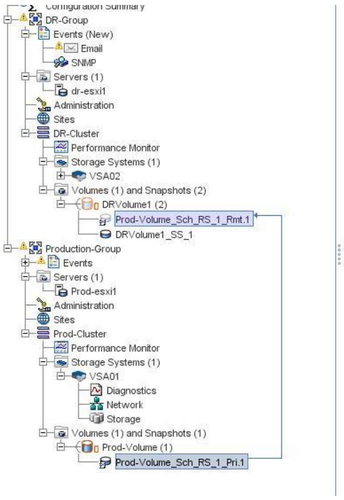
- Repeat the same steps to add the LUN to the ESXi at the secondary site as well.

Now that the primary and secondary sites are paired and have access to shared storage, we can configure replication between them. Storage replication allows the VMs on the shared storage volumes to replicate to the secondary site if something should happen to the primary site. To configure this, right-click on a volume at primary site and click on New Schedule to Remote Snapshot a Volume option, and proceed with the following steps.



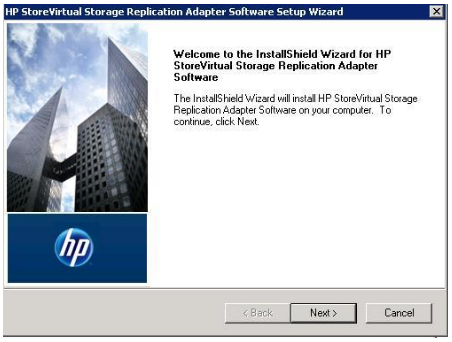
Assign a name to the replication schedule and add the secondary site management group and the volume of the secondary site under remote snapshot step. The retention time for the snapshot option can be selected, if required. Click OK to continue.

- Storage replication is now enabled between the primary and secondary sites.



VMware SRM has the capability to replicate data from a primary site to a DR site using array-based replication. For this to function, a Storage Replication Adapter (SRA) must be installed in both the primary and disaster sites so that the array manager on the SRM can do array-based replication. The steps to configure replication between sites are given below.

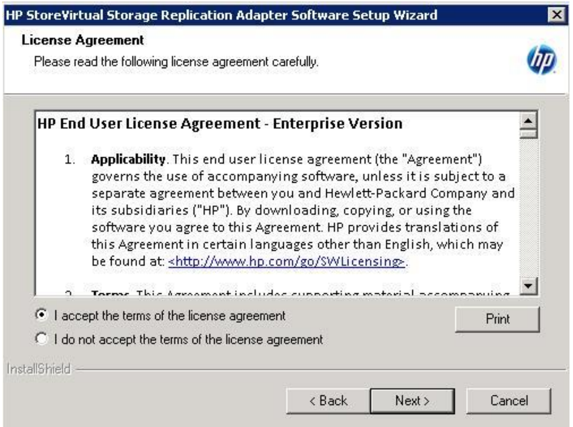
- Log into the server running the SRM instance at the protected site and download the SRA installer from the VMware website. Launch the installer to continue.


HP StoreVirtual Storage Replication Adapter Software Setup Wizard
< Back
Next >
Cancel

Welcome to the InstallShield Wizard for HP StoreVirtual Storage Replication Adapter Software

The InstallShield Wizard will install HP StoreVirtual Storage Replication Adapter Software on your computer. To continue, click Next.

- Accept the license and click Next.


HP StoreVirtual Storage Replication Adapter Software Setup Wizard
Print
InstallShield
< Back
Next >
Cancel

License Agreement

Please read the following license agreement carefully.

HP End User License Agreement - Enterprise Version

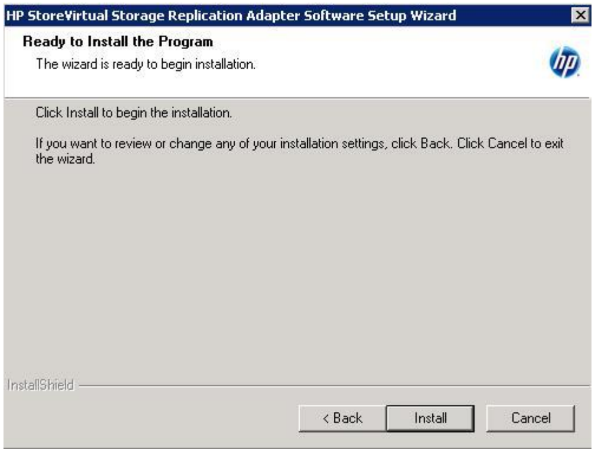
1. **Applicability**. This end user license agreement (the "Agreement") governs the use of accompanying software, unless it is subject to a separate agreement between you and Hewlett-Packard Company and its subsidiaries ("HP"). By downloading, copying, or using the software you agree to this Agreement. HP provides translations of this Agreement in certain languages other than English, which may be found at: <http://www.hp.com/go/SWLicensing>.

2. **Terms**. This Agreement includes supporting material accompanying

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

- Click on Install to begin the SRA installation.


HP StoreVirtual Storage Replication Adapter Software Setup Wizard
InstallShield
< Back
Install
Cancel

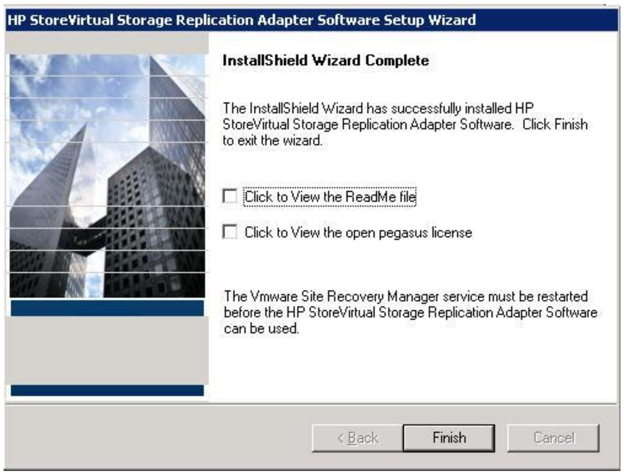
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

- Once the installation is complete, click Finish.



HP StoreVirtual Storage Replication Adapter Software Setup Wizard

InstallShield Wizard Complete

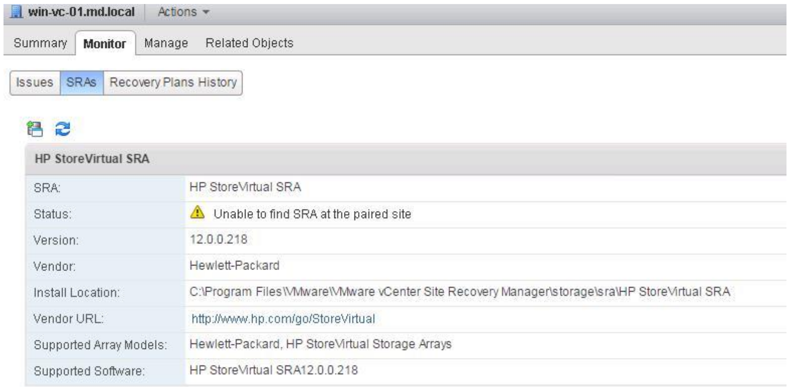
The InstallShield Wizard has successfully installed HP StoreVirtual Storage Replication Adapter Software. Click Finish to exit the wizard.

☐ Click to View the ReadMe file

☐ Click to View the open pegasus license

The Vmware Site Recovery Manager service must be restarted before the HP StoreVirtual Storage Replication Adapter Software can be used.

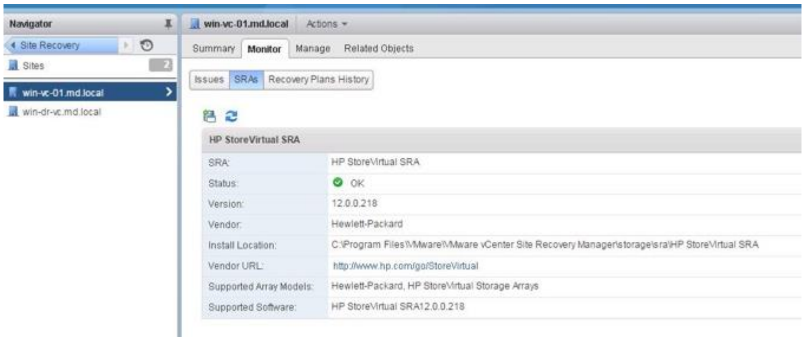
- The SRA installation will automatically be detected by the SRM server and can be seen within the vSphere Web Client as shown below.



HP StoreVirtual SRA

SRA:	HP StoreVirtual SRA
Status:	⚠ Unable to find SRA at the paired site
Version:	12.0.0.218
Vendor:	Hewlett-Packard
Install Location:	C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra\HP StoreVirtual SRA
Vendor URL:	http://www.hp.com/go/StoreVirtual
Supported Array Models:	Hewlett-Packard, HP StoreVirtual Storage Arrays
Supported Software:	HP StoreVirtual SRA12.0.0.218

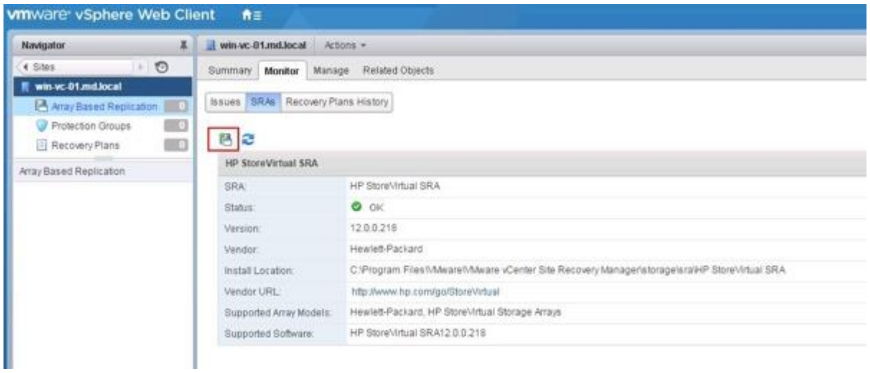
- Repeat the same steps to install the SRA at the second site.



HP StoreVirtual SRA

SRA:	HP StoreVirtual SRA
Status:	✓ OK
Version:	12.0.0.218
Vendor:	Hewlett-Packard
Install Location:	C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra\HP StoreVirtual SRA
Vendor URL:	http://www.hp.com/go/StoreVirtual
Supported Array Models:	Hewlett-Packard, HP StoreVirtual Storage Arrays
Supported Software:	HP StoreVirtual SRA12.0.0.218

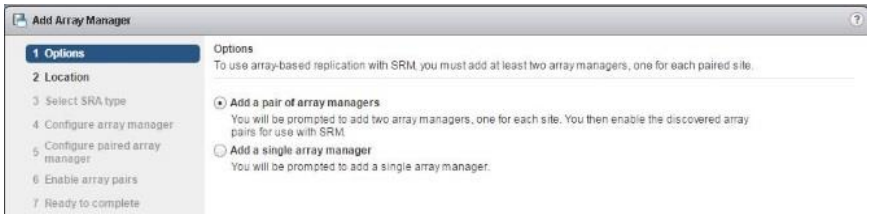
Next, we need to add the array manger on the Web Client. Click on SRM within the Web Client session, select the primary site, click array-based replication, and click on the icon shown below.



HP StoreVirtual SRA

SRA:	HP StoreVirtual SRA
Status:	✓ OK
Version:	12.0.0.218
Vendor:	Hewlett-Packard
Install Location:	C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra\HP StoreVirtual SRA
Vendor URL:	http://www.hp.com/go/StoreVirtual
Supported Array Models:	Hewlett-Packard, HP StoreVirtual Storage Arrays
Supported Software:	HP StoreVirtual SRA12.0.0.218

- Select the Add a pair of array mangers option to configure the array at both sites.



Options

To use array-based replication with SRM, you must add at least two array managers, one for each paired site.

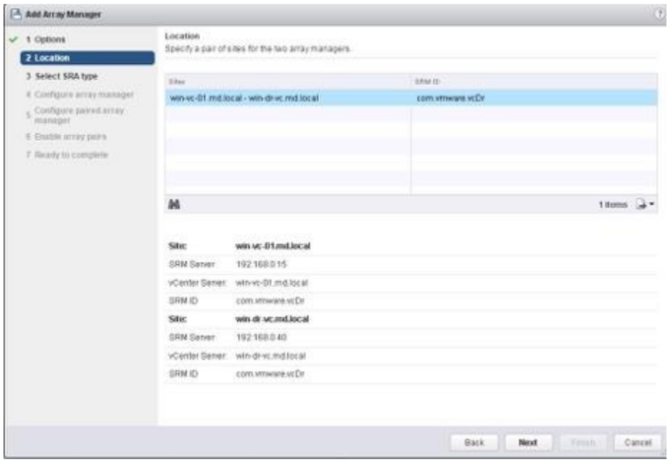
● Add a pair of array managers

You will be prompted to add two array managers, one for each site. You then enable the discovered array pairs for use with SRM.

○ Add a single array manager

You will be prompted to add a single array manager.

- Select the pair of sites, and click Next to continue.



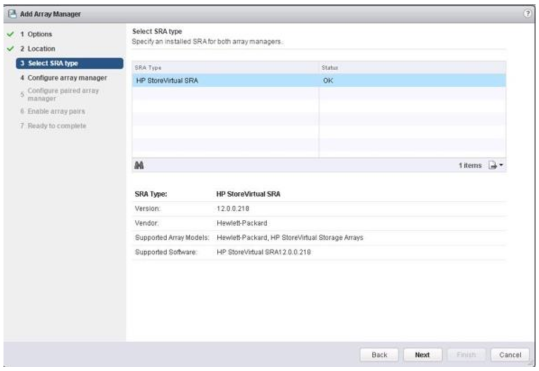
Location

Specify a pair of sites for the two array managers.

Sites	SRM ID
win-vc-01.md.local - win-dr-vc.md.local	com.vmware.vcDr

Site:	win-vc-01.md.local
SRM Server:	192.168.0.15
vCenter Server:	win-vc-01.md.local
SRM ID	com.vmware.vcDr
Site:	win-dr-vc.md.local
SRM Server:	192.168.0.40
vCenter Server:	win-dr-vc.md.local
SRM ID	com.vmware.vcDr

- The SRA will be automatically detected. Click Next to continue.

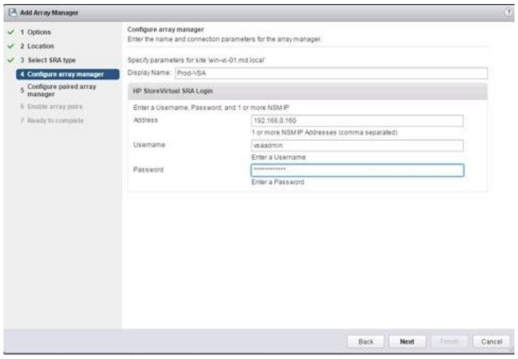


Select SRA type
Specify an installed SRA for both array managers.

SRA Type	Status
HP StoreVirtual SRA	OK

SRA Type:	**HP StoreVirtual SRA**
Version:	12.0.0.218
Vendor:	Hewlett-Packard
Supported Array Models:	Hewlett-Packard, HP StoreVirtual Storage Arrays
Supported Software:	HP StoreVirtual SRA12.0.0.218

- Provide a name for the new array, provide the credentials for the primary array manager, and click Next to continue.

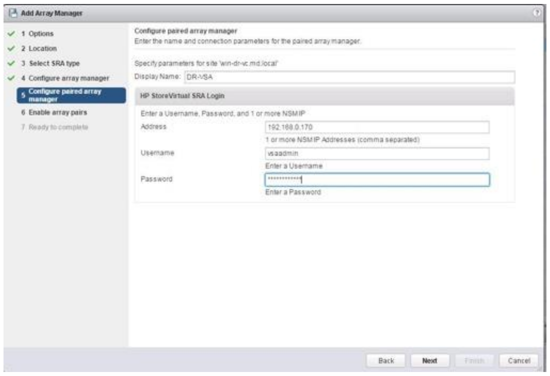


Configure array manager
Enter the name and connection parameters for the array manager.

Specify parameters for site 'win-vc-01.md.local'
Display Name: Prod-VSA

HP StoreVirtual SRA Login
Enter a Username, Password, and 1 or more NSM IP
Address: 192.168.0.160
1 or more NSM IP Addresses (comma separated)
Username: vsaadmin
Enter a Username
Password: ************
Enter a Password

- Provide the corresponding information for the secondary site as well.

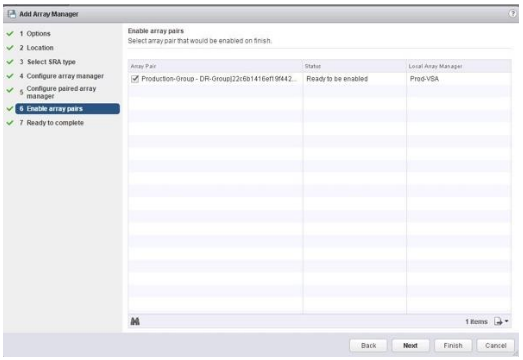


Configure paired array manager
Enter the name and connection parameters for the paired array manager.

Specify parameters for site 'win-dr-vc.md.local'
Display Name: DR-VSA

HP StoreVirtual SRA Login
Enter a Username, Password, and 1 or more NSM IP
Address: 192.168.0.170
1 or more NSM IP Addresses (comma separated)
Username: vsaadmin
Enter a Username
Password: ************
Enter a Password

- Select the array pair and click Next to continue.



Add Array Manager

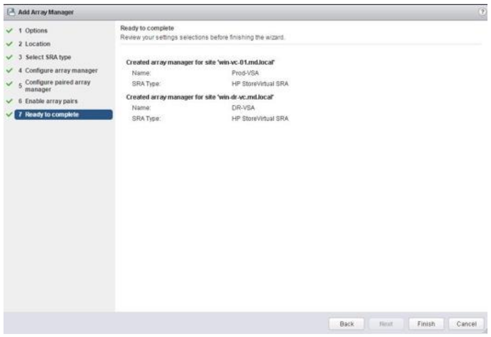
1 Options
2 Location
3 Select SRA type
4 Configure array manager
5 Configure paired array manager
6 Enable array pairs
7 Ready to complete

Enable array pairs
Select array pair that would be enabled on finish.

Array Pair	Status	Local Array Manager
☑ Production-Group - DR-Group|22c6b1416ef19f442...	Ready to be enabled	Prod-VSA

1 items

- Review the array configuration and click Finish.



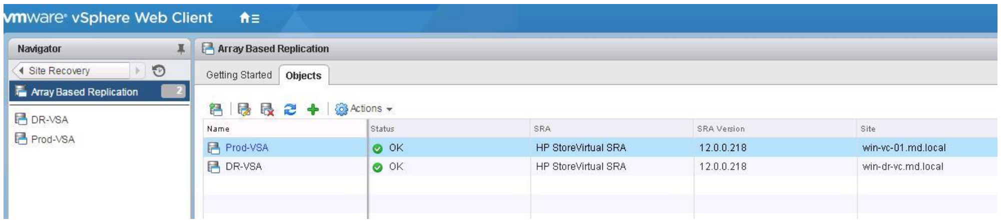
Add Array Manager

1 Options
2 Location
3 Select SRA type
4 Configure array manager
5 Configure paired array manager
6 Enable array pairs
7 Ready to complete

Ready to complete
Review your settings selections before finishing the wizard.

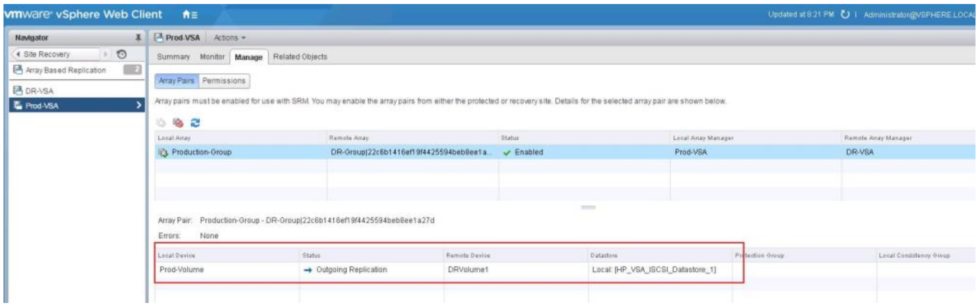
Created array manager for site 'win-vc-01.md.local'
Name: Prod-VSA
SRA Type: HP StoreVirtual SRA
Created array manager for site 'win-dr-vc.md.local'
Name: DR-VSA
SRA Type: HP StoreVirtual SRA

- Within the vSphere Web Client, click on Array Based Replication and navigate to the Objects tab. Confirm that an “OK” status is shown for both array managers.



Name	Status	SRA	SRA Version	Site
Prod-VSA	✓ OK	HP StoreVirtual SRA	12.0.0.218	win-vc-01.md.local
DR-VSA	✓ OK	HP StoreVirtual SRA	12.0.0.218	win-dr-vc.md.local

- Select one of the VSA in the left-hand pane. Replicated datastore information will be shown for the VSA pair.



Array pairs must be enabled for use with SRM. You may enable the array pairs from either the protected or recovery site. Details for the selected array pair are shown below.

Local Array	Remote Array	Status	Local Array Manager	Remote Array Manager
Production-Group	DR-Group|22c6b1416ef19f4425594beb8ee1a...	✓ Enabled	Prod-VSA	DR-VSA

Array Pair: Production-Group - DR-Group|22c6b1416ef19f4425594beb8ee1a27d

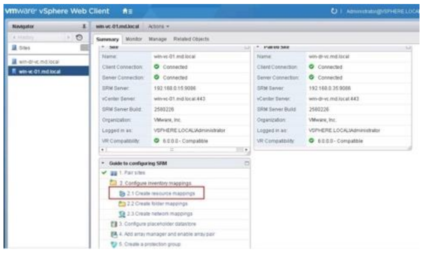
Errors: None

Local Device	Status	Remote Device	Datastore	Protection Group	Local Consistency Group
Prod-Volume	→ Outgoing Replication	DRVolume1	Local: [HP_VSA_ISCSI_Datastore_1]		

The next step involves configuring the inventory mapping between vCenter Servers at both sites. This will ensure that mappings exist between the clusters and resource pools at the primary and secondary sites, which is required by SRM to recover the virtual machines based on preferences set by the administrator. Once the mappings have been established, SRM will execute the recovery plan in the case of a disaster event, and the virtual machines will be restarted on the vSphere resources at the other site.

SRM Resource Mappings

- To create the necessary resource mappings, log into vCenter using the Web Client, click on SRM, select the protected site, and then click on Create resource mappings.

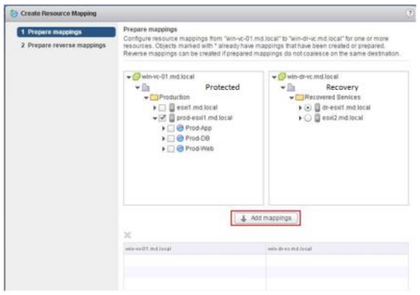


Name:	win-vc-01.md.local
Client Connection:	Connected
Server Connection:	Connected
SRM Server:	192.168.0.15:9086
vCenter Server:	win-vc-01.md.local:443
SRM Server Build:	2580226
Organization:	VMware, Inc.
Logged in as:	VSPHERE.LOCAL\Administrator
VR Compatibility:	6.0.0.0 - Compatible

Name:	win-dr-vc.md.local
Client Connection:	Connected
Server Connection:	Connected
SRM Server:	192.168.0.35:9086
vCenter Server:	win-dr-vc.md.local:443
SRM Server Build:	2580226
Organization:	VMware, Inc.
Logged in as:	VSPHERE.LOCAL\Administrator
VR Compatibility:	6.0.0.0 - Compatible

✓ 1. Pair sites
2. Configure inventory mappings
2.1 Create resource mappings
2.2 Create folder mappings
2.3 Create network mappings
3. Configure placeholder datastore
4. Add array manager and enable array pair
5. Create a protection group

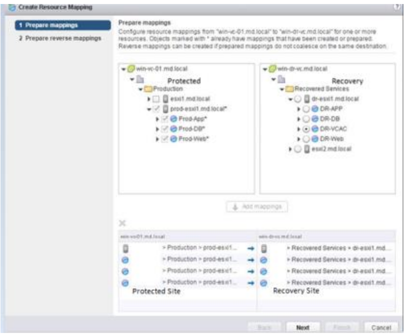
- Select the primary site, select the ESXi server at that site, select the newly-created mapping resources, and click on Add mappings.



Prepare mappings

Configure resource mappings from "win-vc-01.md.local" to "win-dr-vc.md.local" for one or more resources. Objects marked with * already have mappings that have been created or prepared. Reverse mappings can be created if prepared mappings do not coalesce on the same destination.

- Configure the mappings as per the folder structure required as shown below.

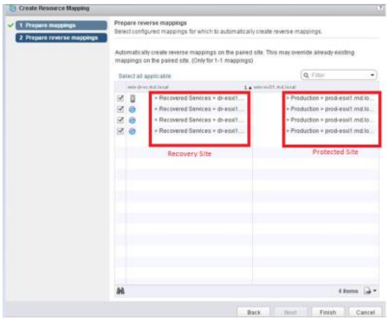


Prepare mappings

Configure resource mappings from "win-vc-01.md.local" to "win-dr-vc.md.local" for one or more resources. Objects marked with * already have mappings that have been created or prepared. Reverse mappings can be created if prepared mappings do not coalesce on the same destination.

win-vc01.md.local		win-dr-vc.md.local
> Production > prod-esxi1...	→	> Recovered Services > dr-esxi1.md...
> Production > prod-esxi1...	→	> Recovered Services > dr-esxi1.md...
> Production > prod-esxi1...	→	> Recovered Services > dr-esxi1.md...
> Production > prod-esxi1...	→	> Recovered Services > dr-esxi1.md...

- Select the objects for reverse mapping. This will create the reverse mappings automatically on the paired site. This is required to do a failover from the secondary site back to the primary site. Click on Select all applicable and click Finish.



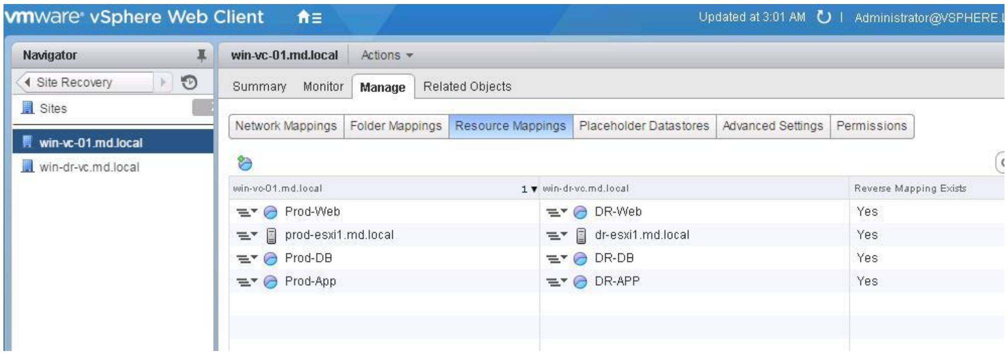
Prepare reverse mappings

Select configured mappings for which to automatically create reverse mappings.

Automatically create reverse mappings on the paired site. This may override already existing mappings on the paired site. (Only for 1-1 mappings)

	win-dr-vc.md.local	win-vc01.md.local
☑	> Recovered Services > dr-esxi1...	> Production > prod-esxi1.md.lo...
☑	> Recovered Services > dr-esxi1...	> Production > prod-esxi1.md.lo...
☑	> Recovered Services > dr-esxi1...	> Production > prod-esxi1.md.lo...
☑	> Recovered Services > dr-esxi1...	> Production > prod-esxi1.md.lo...

- To verify the resource mappings, click on the Manage tab on the primary site and navigate to the resource mappings tab as shown below.

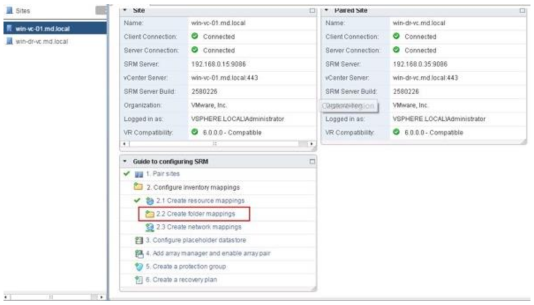


win-vc-01.md.local	win-dr-vc.md.local	Reverse Mapping Exists
Prod-Web	DR-Web	Yes
prod-esxi1.md.local	dr-esxi1.md.local	Yes
Prod-DB	DR-DB	Yes
Prod-App	DR-APP	Yes

SRM Folder Mappings

Once the necessary resource mappings have been configured, we need to map any organizational folders between the sites as well. This ensures that virtual resource organization is consistent between the two sites. The folder mapping procedure is described below.

- Click on SRM, select the primary site, and click on the Create folder mappings option under inventory, as shown below.



Site

Name:	win-vc-01.md.local
Client Connection:	Connected
Server Connection:	Connected
SRM Server:	192.168.0.15:9086
vCenter Server:	win-vc-01.md.local:443
SRM Server Build:	2580226
Organization:	VMware, Inc.
Logged in as:	VSPHERE.LOCAL\Administrator
VR Compatibility:	6.0.0.0 - Compatible

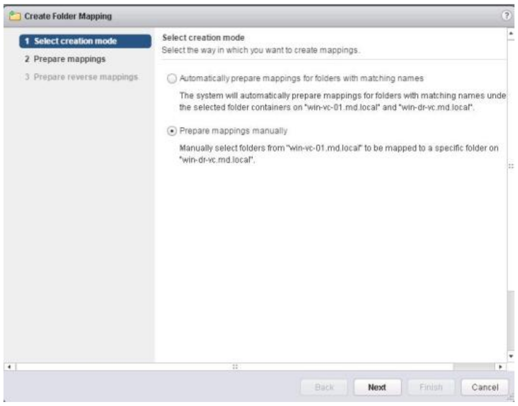
Paired Site

Name:	win-dr-vc.md.local
Client Connection:	Connected
Server Connection:	Connected
SRM Server:	192.168.0.35:9086
vCenter Server:	win-dr-vc.md.local:443
SRM Server Build:	2580226
Organization:	VMware, Inc.
Logged in as:	VSPHERE.LOCAL\Administrator
VR Compatibility:	6.0.0.0 - Compatible

Guide to configuring SRM

✓ 1. Pair sites
2. Configure inventory mappings
✓ 2.1 Create resource mappings
2.2 Create folder mappings
2.3 Create network mappings
3. Configure placeholder datastore
4. Add array manager and enable array pair
5. Create a protection group
6. Create a recovery plan

- These folder mappings can be done automatically and manually, select manual and click next.



Create Folder Mapping

1 Select creation mode

2 Prepare mappings

3 Prepare reverse mappings

Select creation mode

Select the way in which you want to create mappings.

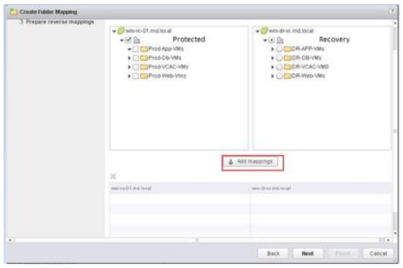
○ Automatically prepare mappings for folders with matching names

The system will automatically prepare mappings for folders with matching names unde the selected folder containers on "win-vc-01.md.local" and "win-dr-vc.md.local".

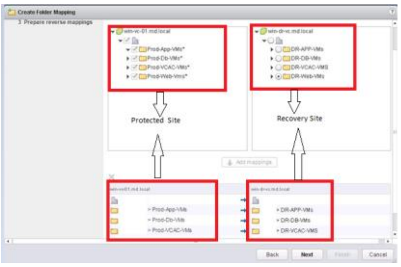
● Prepare mappings manually

Manually select folders from "win-vc-01.md.local" to be mapped to a specific folder on "win-dr-vc.md.local".

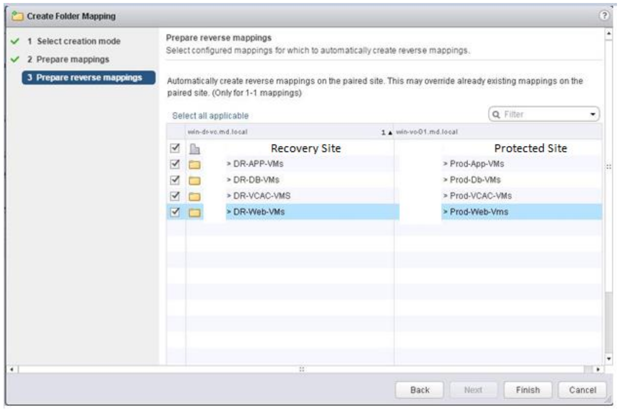
- Select the folders in the primary site and the corresponding folders on the recovery site and click on Add mappings to the create folder mappings.



- Select the folder mapping on the primary and secondary sites as shown below. Click Next to continue.



- Select all the required reverse mappings and this will automatically create the mappings between the paired sites. Click Finish.

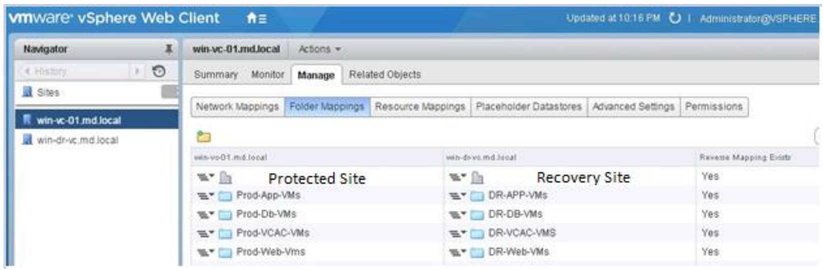


Prepare reverse mappings
Select configured mappings for which to automatically create reverse mappings.

Automatically create reverse mappings on the paired site. This may override already existing mappings on the paired site. (Only for 1-1 mappings)

		win-dr-vc.md.local	win-vc01.md.local
☑		Recovery Site	Protected Site
☑		> DR-APP-VMs	> Prod-App-VMs
☑		> DR-DB-VMs	> Prod-Db-VMs
☑		> DR-VCAC-VMS	> Prod-VCAC-VMs
☑		> DR-Web-VMs	> Prod-Web-Vms

- Once this process is complete, the configuration can be verified by clicking on the Manage tab on the site and navigating to folder mappings as shown below.

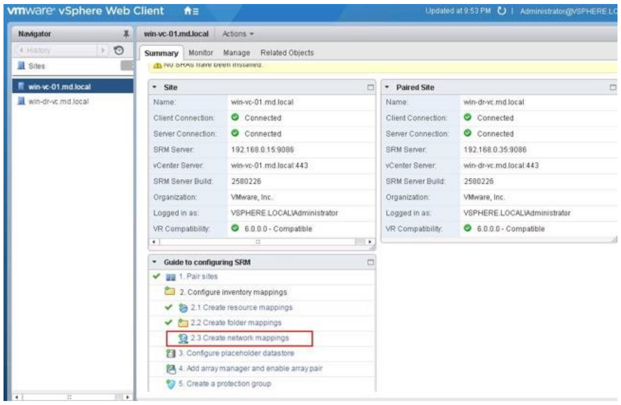


win-vc01.md.local	win-dr-vc.md.local	Reverse Mapping Exists
Protected Site	Recovery Site	Yes
Prod-App-VMs	DR-APP-VMs	Yes
Prod-Db-VMs	DR-DB-VMs	Yes
Prod-VCAC-VMs	DR-VCAC-VMS	Yes
Prod-Web-Vms	DR-Web-VMs	Yes

Next step involves the network mapping on the primary site to secondary site. This is required for the virtual machines powered on the disaster site should get connected to the network after a recovery plan is successfully executed by SRM. Select the virtual machine port groups on the primary site and map them with the port groups on the secondary site.

SRM Network Mappings

- Click on the SRM on the protected site by logging on to the vCenter Server. Click on summary tab and click on Create Network Mapping Option.



No SRAs have been installed.

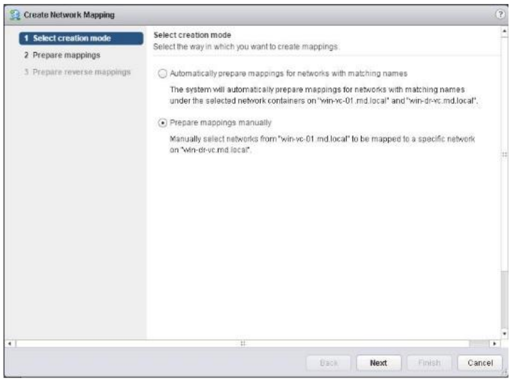
Site	
Name:	win-vc-01.md.local
Client Connection:	Connected
Server Connection:	Connected
SRM Server:	192.168.0.15:9086
vCenter Server:	win-vc-01.md.local:443
SRM Server Build:	2580226
Organization:	VMware, Inc.
Logged in as:	VSPHERE.LOCAL\Administrator
VR Compatibility:	6.0.0.0 - Compatible

Paired Site	
Name:	win-dr-vc.md.local
Client Connection:	Connected
Server Connection:	Connected
SRM Server:	192.168.0.35:9086
vCenter Server:	win-dr-vc.md.local:443
SRM Server Build:	2580226
Organization:	VMware, Inc.
Logged in as:	VSPHERE.LOCAL\Administrator
VR Compatibility:	6.0.0.0 - Compatible

Guide to configuring SRM

✓ 1. Pair sites
2. Configure inventory mappings
✓ 2.1 Create resource mappings
✓ 2.2 Create folder mappings
2.3 Create network mappings
3. Configure placeholder datastore
4. Add array manager and enable array pair
5. Create a protection group

- Just like folder mappings again, the same options are available. This network mapping can be done automatically o manually, click on manual and click next.



Select creation mode

Select the way in which you want to create mappings

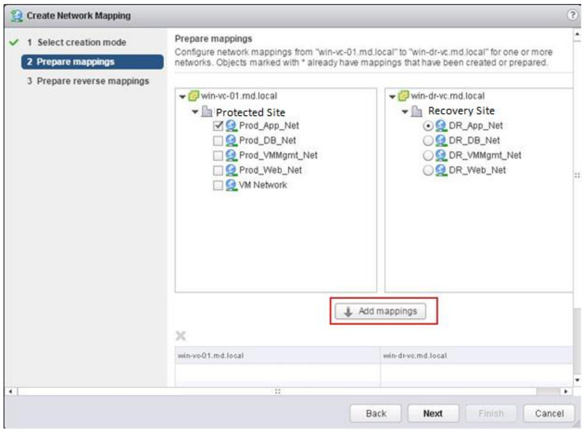
○ Automatically prepare mappings for networks with matching names

The system will automatically prepare mappings for networks with matching names under the selected network containers on "win-vc-01.md.local" and "win-dr-vc.md.local".

● Prepare mappings manually

Manually select networks from "win-vc-01.md.local" to be mapped to a specific network on "win-dr-vc.md.local".

- Select the virtual machine port groups on the primary site and map them with the port groups on the secondary site and then click on add mappings. Virtual machine port groups are where virtual machines get connected and can talk to each other.



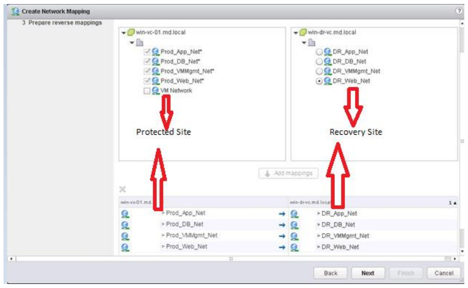
Prepare mappings

Configure network mappings from "win-vc-01.md.local" to "win-dr-vc.md.local" for one or more networks. Objects marked with * already have mappings that have been created or prepared.

win-vc-01.md.local
Protected Site
☑ Prod_App_Net
□ Prod_DB_Net
□ Prod_VMMgmt_Net
□ Prod_Web_Net
□ VM Network

win-dr-vc.md.local
Recovery Site
● DR_App_Net
○ DR_DB_Net
○ DR_VMMgmt_Net
○ DR_Web_Net

- Repeat the same and click next between the paired sites for different networks.



Create Network Mapping

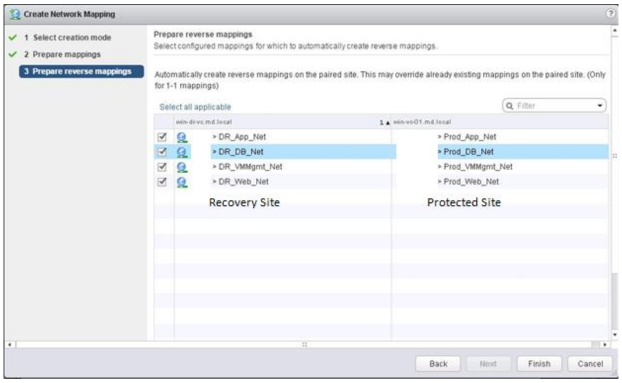
3 Prepare reverse mappings

win-vc-01.md.local
- ☑ Prod_App_Net*
- ☑ Prod_DB_Net*
- ☑ Prod_VMMgmt_Net*
- ☑ Prod_Web_Net*
- □ VM Network

win-dr-vc.md.local
- ○ DR_App_Net
- ○ DR_DB_Net
- ○ DR_VMMgmt_Net
- ● DR_Web_Net

win-vc-01.md.local		win-dr-vc.md.local
Prod_App_Net	→	DR_App_Net
Prod_DB_Net	→	DR_DB_Net
Prod_VMMgmt_Net	→	DR_VMMgmt_Net
Prod_Web_Net	→	DR_Web_Net

- Once all the networks are mapped click on finish.



Create Network Mapping

✓ 1 Select creation mode
✓ 2 Prepare mappings
3 Prepare reverse mappings

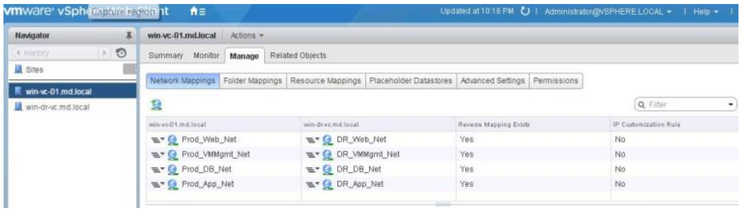
Prepare reverse mappings
Select configured mappings for which to automatically create reverse mappings.

Automatically create reverse mappings on the paired site. This may override already existing mappings on the paired site. (Only for 1-1 mappings)

Select all applicable

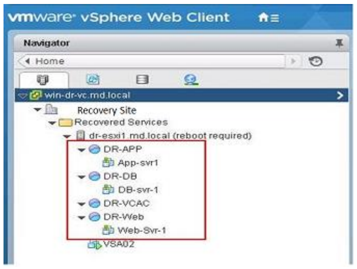
	win-dr-vc.md.local	win-vc-01.md.local
☑	DR_App_Net	Prod_App_Net
☑	DR_DB_Net	Prod_DB_Net
☑	DR_VMMgmt_Net	Prod_VMMgmt_Net
☑	DR_Web_Net	Prod_Web_Net

- The same can be verified by clicking on the SRM, click on primary site, click on manage, click on network mappings options.



win-vc-01.md.local	win-dr-vc.md.local	Reverse Mapping Exists	IP Customization Rule
Prod_Web_Net	DR_Web_Net	Yes	No
Prod_VMMgmt_Net	DR_VMMgmt_Net	Yes	No
Prod_DB_Net	DR_DB_Net	Yes	No
Prod_App_Net	DR_App_Net	Yes	No

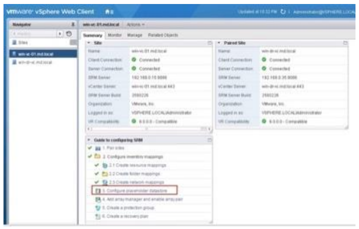
Next step involves creating a placeholder Datastore which will be used to place the virtual machines in the recovery site. It reserves the place for VM in recovery site inventory. These Datastores are to be seen by all severs in the cluster. These are to be created on both sites to enable failover to both sites. Place holder VM is a set of VM files that are created. Any VM added to recovery plan cannot be powered on. As soon as a VM is added to protection group, a placeholder VM will be created in the recovery site.



- win-dr-vc.md.local
  - Recovery Site
    - Recovered Services
      - dr-esxi1.md.local (reboot required)
        - DR-APP
          - App-svr1
        - DR-DB
          - DB-svr-1
        - DR-VCAC
        - DR-Web
          - Web-Svr-1
      - VSA02

SRM Placeholder Datastores

- To create a placeholder Datastore, click on configure placeholder Datastore under SRM.

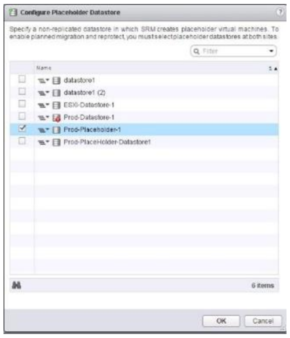


Site	
Name	win-vc-01.md.local
Client Connection	Connected
Server Connection	Connected
SRM Server	[illegible]
vCenter Server	win-vc-01.md.local:443
SRM Server Build	[illegible]
Organization	VMware, Inc.
Logged in as	VSPHERE.LOCAL\Administrator
VR Compatibility	6.0.0.0 - Compatible

Paired Site	
Name	win-dr-vc.md.local
Client Connection	Connected
Server Connection	Connected
SRM Server	[illegible]
vCenter Server	win-dr-vc.md.local:443
SRM Server Build	[illegible]
Organization	VMware, Inc.
Logged in as	VSPHERE.LOCAL\Administrator
VR Compatibility	6.0.0.0 - Compatible

Guide to configuring SRM
- ✓ 1. Pair sites
- ✓ 2. Configure inventory mappings
  - ✓ 2.1 Create resource mappings
  - ✓ 2.2 Create folder mappings
  - ✓ 2.3 Create network mappings
- 3. Configure placeholder datastore
- 4. Add array manager and enable array pair
- 5. Create a protection group
- 6. Create a recovery plan

- Net step involves selecting a Datastore to be used as a placeholder for the production virtual machines. Replicated LUN cannot be used for placeholder Datastore. Click OK

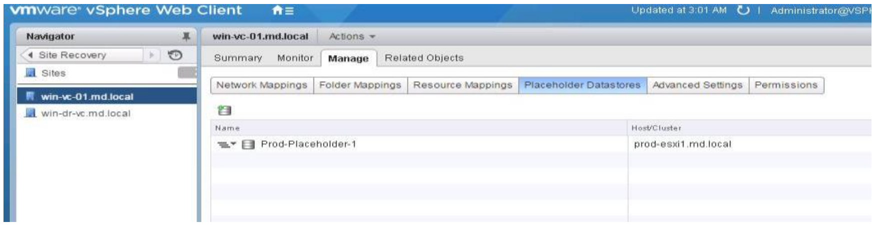

Configure Placeholder Datastore

Specify a non-replicated datastore in which SRM creates placeholder virtual machines. To enable planned migration and reprotect, you must select placeholder datastores at both sites.

	Name
□	datastore1
□	datastore1 (2)
□	ESXi-Datastore-1
□	Prod-Datastore-1
☑	Prod-Placeholder-1
□	Prod-PlaceHolder-Datastore1

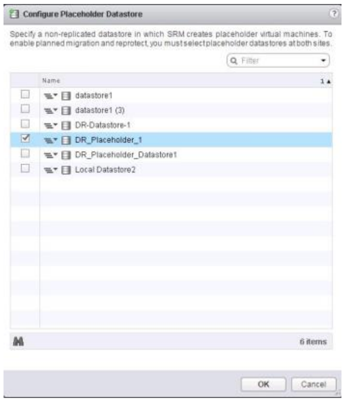
6 items

- Placeholder is configured and can be seen under manage, click on Placeholder Datastores.



Name	Host/Cluster
Prod-Placeholder-1	prod-esxi1.md.local

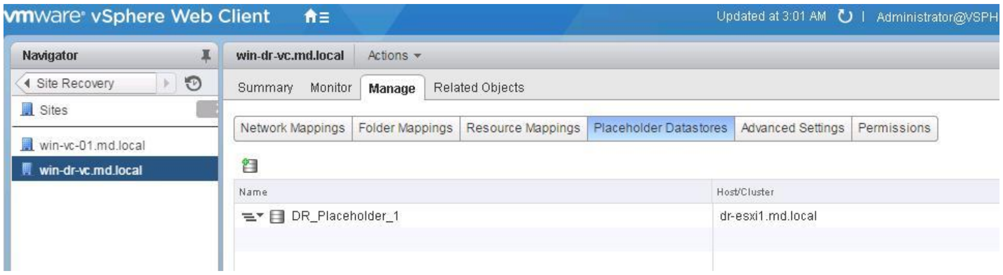
- Repeat the same steps on the secondary site as well. This has to be a non-replicated Datastore on the secondary site again. Click OK


Configure Placeholder Datastore

Specify a non-replicated datastore in which SRM creates placeholder virtual machines. To enable planned migration and reprotect, you must select placeholder datastores at both sites.

	Name
□	datastore1
□	datastore1 (3)
□	DR-Datastore-1
☑	DR_Placeholder_1
□	DR_Placeholder_Datastore1
□	Local Datastore2

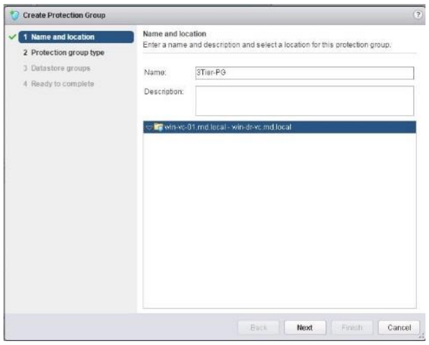
6 items



Name	Host/Cluster
DR_Placeholder_1	dr-esxi1.md.local

SRM Protection Group Creation

Next step involves creating a protection group, which is also a place to put the VM's that are to be protected by SRM. To create a protection group, click on create protection group under summary of SRM screen. Give a name and select the site.



Name and location

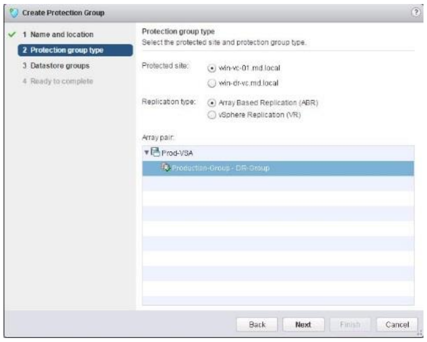
Enter a name and description and select a location for this protection group.

Name: 3Tier-PG

Description:

win-vc-01.md.local - win-dr-vc.md.local

- Select the primary site, the type of replication for the protected group created. Both vSphere replication and array based replication cannot be selected together, click next.



Protection group type

Select the protected site and protection group type.

Protected site: ● win-vc-01.md.local ○ win-dr-vc.md.local

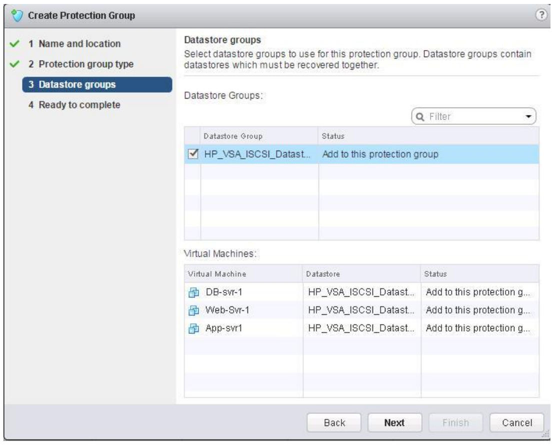
Replication type: ● Array Based Replication (ABR) ○ vSphere Replication (VR)

Array pair:

Prod-VSA

Production-Group - DR-Group

- Select the Datastores from the list to create a Datastore group. All the VMs on the Datastores will be recovered as part of the protection group. Click next.



Datastore groups

Select datastore groups to use for this protection group. Datastore groups contain datastores which must be recovered together.

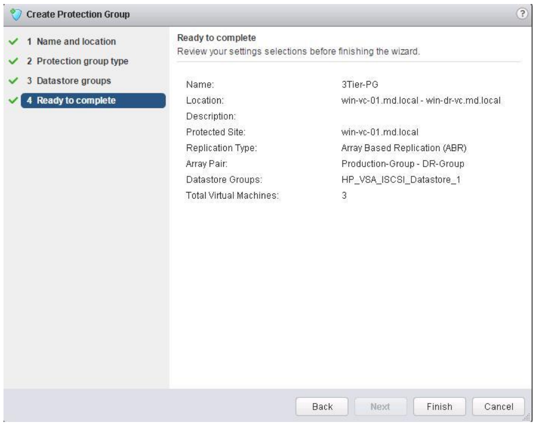
Datastore Groups:

	Datastore Group	Status
☑	HP_VSA_ISCSI_Datast...	Add to this protection group

Virtual Machines:

Virtual Machine	Datastore	Status
DB-svr-1	HP_VSA_ISCSI_Datast...	Add to this protection g...
Web-Svr-1	HP_VSA_ISCSI_Datast...	Add to this protection g...
App-svr1	HP_VSA_ISCSI_Datast...	Add to this protection g...

- Re-check and click Finish.



Ready to complete

Review your settings selections before finishing the wizard.

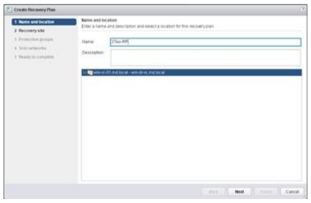
Name:	3Tier-PG
Location:	win-vc-01.md.local - win-dr-vc.md.local
Description:	
Protected Site:	win-vc-01.md.local
Replication Type:	Array Based Replication (ABR)
Array Pair:	Production-Group - DR-Group
Datastore Groups:	HP_VSA_ISCSI_Datastore_1
Total Virtual Machines:	3

Next step is to create a recover plan. Recovery plan is an automated plan for to recover the protected VMs in the recovery site should a disaster happen in the datacenter. A group of virtual machines can be included in multiple recovery plans. A recovery plan includes the list of virtual machines from all the protection groups in it. It also includes the startup priority of virtual machines should a disaster happen and also a customization to be followed after the virtual machine starts from recovery.

The customization includes IP for VMs after recovering, login scripts. Virtual machines which are recovered can be placed in to isolated network in order to make sure the production machines will not get effected.

SRM Recovery Plans

- To start creating a recovery plan, click on SRM, click on summary and then click on create a recovery plan, click ok



Name and location

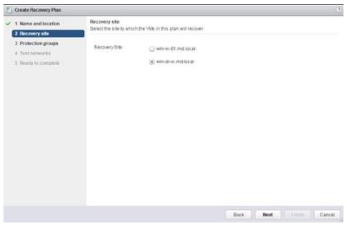
Enter a name and description and select a location for this recovery plan.

Name: 3Tier-RP

Description:

win-vc-01.md.local - win-dr-vc.md.local

- Select the site on to which virtual machines are to be restarted should a disaster occur, click next.

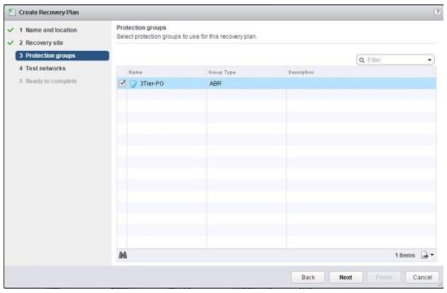


Recovery site

Select the site to which the VMs in this plan will recover.

Recovery Site: ○ win-vc-01.md.local ● win-dr-vc.md.local

- Select the protection groups, which are included in the recovery plan. Click next.



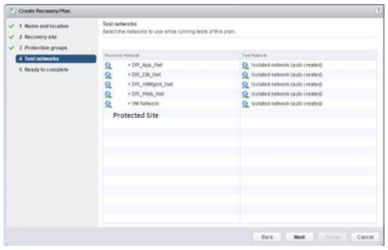
Protection groups

Select protection groups to use for this recovery plan.

	Name	Group Type	Description
☑	3Tier-PG	ABR	

1 items

Click on Next. Test networks can be specified on the recovery site if the admin wants the recovered virtual machines to be connected to the test network after a recovery in order to let the production virtual machine run without any disturbance, or the admin can make use of the automatically created test network for placing the recovered virtual machines. Click next.

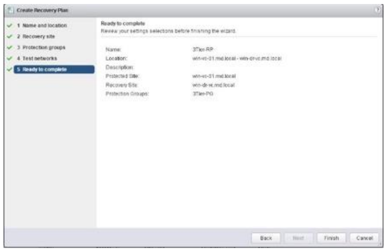


Test networks

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

Recovery Network	Test Network
DR_App_Net	Isolated network (auto created)
DR_DB_Net	Isolated network (auto created)
DR_VMMgmt_Net	Isolated network (auto created)
DR_Web_Net	Isolated network (auto created)
VM Network	Isolated network (auto created)

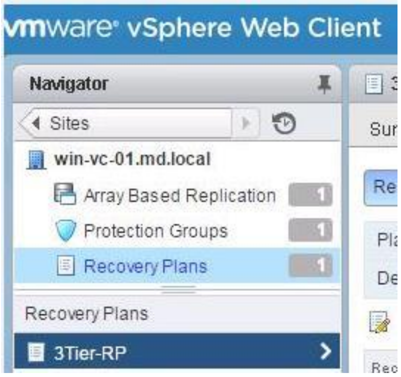
- Re-check all the settings specified and click finish.



Ready to complete
Review your settings selections before finishing the wizard.

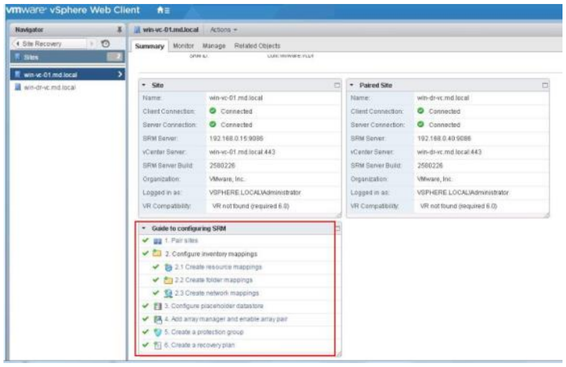
Name:	3Tier-RP
Location:	win-vc-01.md.local - win-dr-vc.md.local
Description:	
Protected Site:	win-vc-01.md.local
Recovery Site:	win-dr-vc.md.local
Protection Groups:	3Tier-PG

- Recovery plan created can be seen under the sites option on the web client. The recovery plan can be edited to change the VM priority and the networks.



SRM Testing and Failback

- Next step involves testing the recovery plan created. SRM ensures that a disruptive testing can be done without affecting the virtual machines which are already running on the server in both the sites.



Site

Name:	win-vc-01.md.local
Client Connection:	Connected
Server Connection:	Connected
SRM Server:	192.168.0.15:9086
vCenter Server:	win-vc-01.md.local:443
SRM Server Build:	2580226
Organization:	VMware, Inc.
Logged in as:	VSPHERE.LOCAL\Administrator
VR Compatibility:	VR not found (required 6.0)

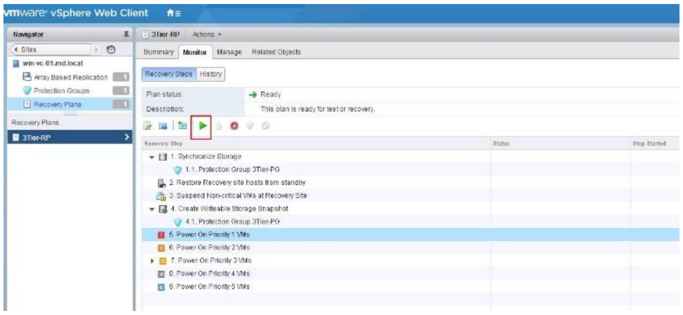
Paired Site

Name:	win-dr-vc.md.local
Client Connection:	Connected
Server Connection:	Connected
SRM Server:	192.168.0.40:9086
vCenter Server:	win-dr-vc.md.local:443
SRM Server Build:	2580226
Organization:	VMware, Inc.
Logged in as:	VSPHERE.LOCAL\Administrator
VR Compatibility:	VR not found (required 6.0)

Guide to configuring SRM

✓ 1. Pair sites
✓ 2. Configure inventory mappings
✓ 2.1 Create resource mappings
✓ 2.2 Create folder mappings
✓ 2.3 Create network mappings
✓ 3. Configure placeholder datastore
✓ 4. Add array manager and enable array pair
✓ 5. Create a protection group
✓ 6. Create a recovery plan

- To test a recovery plan, click on recovery plans options, then click on monitor tab, the click on recovery steps and then click on the play button as shown in the below screenshot.

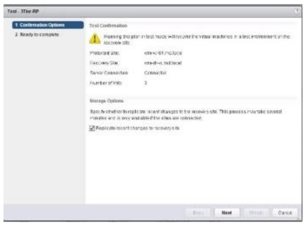


Plan status: Ready

Description: This plan is ready for test or recovery.

1. Synchronize Storage
1.1. Protection Group 3Tier-PG
2. Restore Recovery site hosts from standby
3. Suspend Non-critical VMs at Recovery Site
4. Create Writeable Storage Snapshot
4.1. Protection Group 3Tier-PG
5. Power On Priority 1 VMs
6. Power On Priority 2 VMs
7. Power On Priority 3 VMs
8. Power On Priority 4 VMs
9. Power On Priority 5 VMs

Once the play button is clicked on, the recovery will run in test mode without affecting the virtual machines already running on the servers on both the sites. Select the option replicate recent changes to the recovery site so as to get them replicated. Click next.



Test Confirmation

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

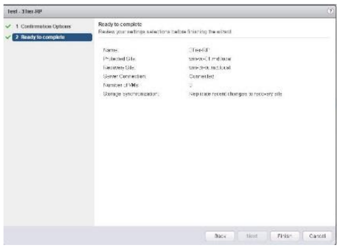
Protected site: win-vc-01.md.local
Recovery Site: win-dr-vc.md.local
Server Connection: Connected
Number of VMs: 3

Storage Options

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

☑ Replicate recent changes to recovery site

- Re-check the settings and click finish.

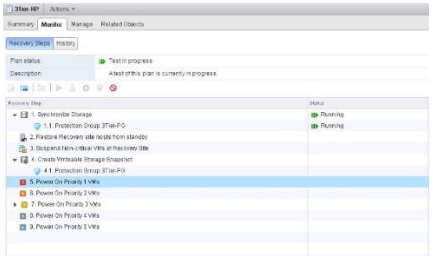


Ready to complete

Review your settings selections before finishing the wizard.

Name: 3Tier-RP
Protected Site: win-vc-01.md.local
Recovery Site: win-dr-vc.md.local
Server Connection: Connected
Number of VMs: 3
Storage synchronization: Replicate recent changes to recovery site

- Once test is being executed a series of steps can be seen on the recovery steps option.

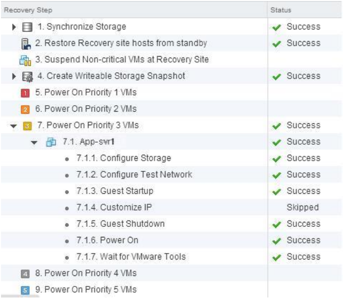


Plan status: Test in progress

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

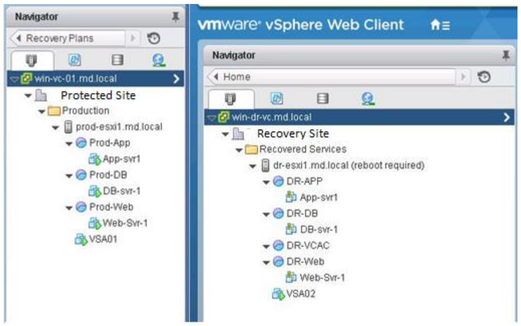
Recovery Step	Status
1. Synchronize Storage	Running
1.1. Protection Group 3Tier-PG	Running
2. Restore Recovery site hosts from standby	
3. Suspend Non-critical VMs at Recovery Site	
4. Create Writeable Storage Snapshot	
4.1. Protection Group 3Tier-PG	
5. Power On Priority 1 VMs	
6. Power On Priority 2 VMs	
7. Power On Priority 3 VMs	
8. Power On Priority 4 VMs	
9. Power On Priority 5 VMs	

- The status of the recovery plan can be seen once it is completed.



Recovery Step	Status
1. Synchronize Storage	✓ Success
2. Restore Recovery site hosts from standby	✓ Success
3. Suspend Non-critical VMs at Recovery Site	
4. Create Writeable Storage Snapshot	✓ Success
5. Power On Priority 1 VMs	
6. Power On Priority 2 VMs	
7. Power On Priority 3 VMs	✓ Success
7.1. App-svr1	✓ Success
7.1.1. Configure Storage	✓ Success
7.1.2. Configure Test Network	✓ Success
7.1.3. Guest Startup	✓ Success
7.1.4. Customize IP	Skipped
7.1.5. Guest Shutdown	✓ Success
7.1.6. Power On	✓ Success
7.1.7. Wait for VMware Tools	✓ Success
8. Power On Priority 4 VMs	
9. Power On Priority 5 VMs	

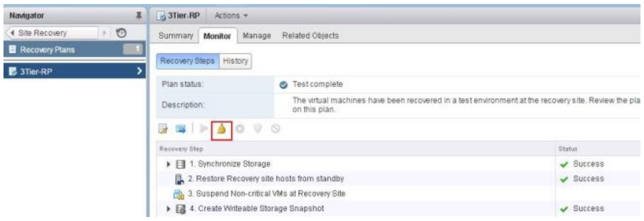
- Once the test is completed, the virtual machines the virtual machines can be seen running on both the sites.



win-vc-01.md.local
Protected Site
Production
prod-esxi1.md.local
Prod-App
App-svr1
Prod-DB
DB-svr-1
Prod-Web
Web-Svr-1
VSA01

win-dr-vc.md.local
Recovery Site
Recovered Services
dr-esxi1.md.local (reboot required)
DR-APP
App-svr1
DR-DB
DB-svr-1
DR-VCAC
DR-Web
Web-Svr-1
VSA02

- Clean up process is as important as creating a recovery plan. This can be done by click on the recovery plan, click on the brush symbol as shown below.

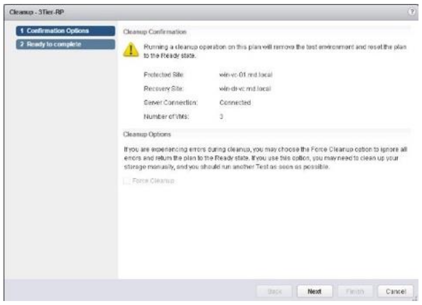


Plan status: Test complete

Description: The virtual machines have been recovered in a test environment at the recovery site. Review the pla on this plan.

Recovery Step	Status
1. Synchronize Storage	✓ Success
2. Restore Recovery site hosts from standby	✓ Success
3. Suspend Non-critical VMs at Recovery Site	
4. Create Writeable Storage Snapshot	✓ Success

- By click on the cleanup option the test environment will be removed completely and the sites will be back to normal functioning state.



Cleanup Confirmation

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

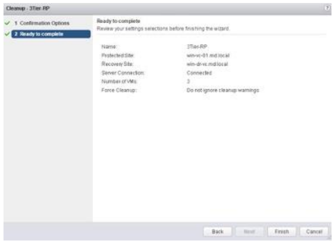
Protected Site:	win-vc-01.md.local
Recovery Site:	win-dr-vc.md.local
Server Connection:	Connected
Number of VMs:	3

Cleanup Options

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

□ Force Cleanup

- Re-Check and click on finish to start the cleanup.

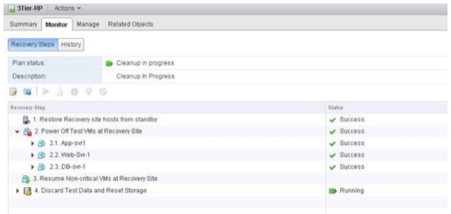


Ready to complete

Review your settings selections before finishing the wizard.

Name:	3Tier-RP
Protected Site:	win-vc-01.md.local
Recovery Site:	win-dr-vc.md.local
Server Connection:	Connected
Number of VMs:	3
Force Cleanup:	Do not ignore cleanup warnings

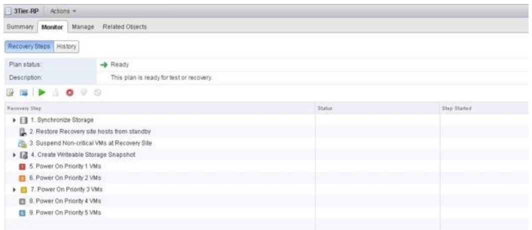
- Monitor the task and making sure that all the VM are up and running.



Plan status:	Cleanup in progress
Description:	Cleanup In Progress

Recovery Step	Status
1. Restore Recovery site hosts from standby	✓ Success
2. Power Off Test VMs at Recovery Site	✓ Success
2.1. App-svr1	✓ Success
2.2. Web-Svr-1	✓ Success
2.3. DB-svr-1	✓ Success
3. Resume Non-critical VMs at Recovery Site	
4. Discard Test Data and Reset Storage	Running

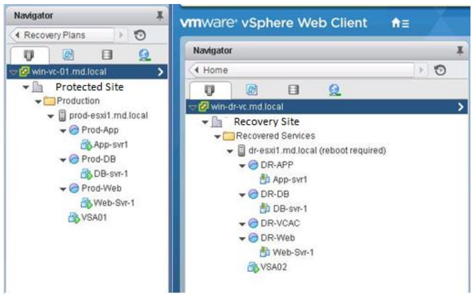
- It will now get everything back to a previous known state.



Plan status:	Ready
Description:	This plan is ready for test or recovery.

Recovery Step	Status	Step Started
1. Synchronize Storage		
2. Restore Recovery site hosts from standby		
3. Suspend Non-critical VMs at Recovery Site		
4. Create Writeable Storage Snapshot		
5. Power On Priority 1 VMs		
6. Power On Priority 2 VMs		
7. Power On Priority 3 VMs		
8. Power On Priority 4 VMs		
9. Power On Priority 5 VMs		

The virtual machines are now in a powered off state after the cleanup operation. We can now create another recovery plan if required and that also can be tested multiple times without affecting the running state of the virtual machines on both sites.



Chapter VI

TIMELINE

Table 4

Dates and Description of the Task

Task(s)			
Start Date	End Date	Description	Duration (Days)
4/16/2015	4/29/2015	Winding up the Data Collection	14
5/1/2015	5/7/2015	Acquiring Physical Servers	7
5/9/2015	5/20/2015	Required software's and OS licenses.	12
5/25/2015	6/15/2015	Installation and Configuration of Physicals Servers	11
6/20/2015	7/09/2015	All VMware and Necessary features will be installed	20
8/1/2015	8/10/2015	Implementing the replication.	10
8/11/2015	8/20/2015	Testing SRM	10
8/21/2015	9/15/2015	Complete report will be written on findings	25
9/16/2015	11/19/2015	Will be ready for final defense	45

I have met the estimated timeline as planned, though I have faced a few hurdles, it was all part of it.

Chapter VII

CONCLUSION AND FUTURE SCOPE

For Business Continuity and Disaster Recovery in a vSphere infrastructure, most customers make a choice of two options. Either use VMware Site Recovery Manager (SRM) or build a vSphere Metro Stretched Cluster.

Two datacenters in active/passive—one running production and the other test/dev. If production site fails, VMware Site Recovery Manager is used to perform an Orchestrated Recovery of the Virtual Machines in the recovery site. Tools used are vSphere Replication and Array Based Replication. This method is called as Disaster Recovery.

However, there is another method which is called as Disaster Avoidance—two datacenters, both running production in an active-active configuration with stretched storage and networking. We call this a vSphere Metro Stretched Cluster.

vSphere Metro Stretched Cluster is great for disaster avoidance, balancing of resources and planned maintenance. When IT knows in advance one of the datacenters might become unavailable because of a hurricane/downtime of power/SAN maintenance etc., virtual machines can be vMotion-ed to the alternate datacenter.

In case of an unplanned event like a fire or earthquake, VMware HA will take care of the restarts of virtual machine but the limitation is vMotion works well only in a round trip of 100ms. The advantage is that up-to-date virtual machine disk files are available in the recovery site so RPO as well as RTO is low.

However, VMware HA is not designed for large scale recovery of a complete site. VMware HA does not offer recovery plans for an automated recovery. It is not aware of application dependencies nor is it site aware. HA does not offer a granular control over VM start priority. Also a failover cannot be tested. So we cannot shutdown and reboot a VM without taking a production VM down.

Another restriction is that because of the synchronous replication of the storage layer, the distance between the two datacenters is limited to about 100km. A vSphere Metro Stretched Cluster is typically deployed in a metro area.

So, in the future, we may expect vSphere SRM will be improved to smoothly integrate with vSphere Metro Stretched Clusters.

References

Crump, G. (2011). *The downsides to array based data replication.* Retrieved from http://www.storage-switzerland.com/Blog/Entries/2011/11/22_The_Downsides_to_Array_Based_Data_Replication.html

Finke, A. (n.d.). *What are active-active and active-passive arrays, and what are the benefits of each*. Retrieved from http://www.computerweekly.com/answer/Active-active-array-vs-active-passive-array-Storage-arrays-explained

Galante, N. (2009). *VMware virtualization for business continuity and disaster recovery*. Retrieved from ftp://ftp.acs.it/documents/Event/WMWare-Nicolas%20Glanate.pdf.

Gordin, I. (2015). *Virtualizing real servers with unsupported OS by VMware vCenter Converter v6*. Retrieved from http://conference.roedu.net/index.php/roedunetconf/2015

Hewlett Packard. (2015). *Hewlett Packard Enterprise support center*. Retrieved from http://h20564.www2.hpe.com/hpsc/swd/public/detail?swItemId=MTX_4effd70562304a50b3be5c4b96#tab1

Khalsa, G. S. (2015). *VMware vSphere blog*. Retrieved from http://blogs.vmware.com/vsphere/2015/04/srm-abrvsvr.html

Listwon. (n.d.). *VMware high availability via vSphere.* Retrieved from http://www.listwow.com/vmware-high-availability-via-vsphere/

Mariusz. (2014). *Site recovery manager 5.8: Architecture overview and features.* Retrieved from http://www.settlersoman.com/site-recovery-manager-5-8-architecture-overview-and-features/

Raido. (n.d.). *Server virtualization*. Retrieved from http://www.raido.be/solutions/server-virtualization/

Sam Shouses Blog. (2014). *Site recovery manager site mappings.* Retrieved from http://samshouseblog.com/2014/08/26/vmware-site-recovery-manager-site-mappings/

Viltorious. (2015). *Disaster recovery.* Retrieved from http://www.viktorious.nl/2015/07/20/disaster-recovery-options-for-virtual-infrastructures/

VMware. (n.d.a). *Automated disaster recovery orchestration.* Retrieved from http://www.vmware.com/files/pdf/products/SRM/VMware_vCenter_Site_Recovery_Manager_5.8.pdf

VMware. (n.d.b). *VMware vCenter site recovery manager 5.5 documentation center* Retrieved from https://pubs.vmware.com/srm-55/index.jsp?topic=/com.vmware.srm.install_config.doc/GUID-ECDF095A-5CA4-4F62-A864-603E0FBA75E3.html

VMware. (n.d.c). *vCenter server*. Retrieved from http://www.vmware.com/files/pdf/products/vCenter/VMware-vCenter-Server-Datasheet.pdf

VMware. (n.d.d). *Esxi-hypervisor*. Retrieved from https://www.vmware.com/products/vsphere/features/esxi-hypervisor

VMware. (n.d.e). *Distributed switch.* Retrieved from http://www.vmware.com/products/vsphere/features/distributed-switch.html

VMware. (n.d.f). *High availability.* Retrieved from http://www.vmware.com/files/pdf/VMware-High-Availability-DS-EN.pdf

VMware. (n.d.g). *Site recovery manager.* Retrieved from www.VMWare.com/products/site-recovery-manager/features.html

VMware. (n.d.h). *vSphere and vSphere with operations management*. Retrieved from http://www.VMWare.com/products/vsphere

VMware. (n.d.i). *VMware Site Recovery Manager Documentation.* Retrieved from http://www.vmware.com/support/pubs/srm_pubs.html

VMware. (n.d.j). *Technology Network.* Retrieved from http://communities.vmware.com

VMware. (n.d.k). *VMware Education.* Retrieved from http://www.vmware.com/education

VMware. (n.d.l). *VMware vSphere documentation.* Retrieved from https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-serverpubs.html

VMware. (n.d.m). *VMware vSphere replication documentation.* Retrieved from https://www.vmware.com/support/pubs/vsphere-replication-pubs.html

VMware. (n.d.n). *VMware vCenter site recovery manager 5.1 documentation center.* Retrieved from https://pubs.vmware.com/srm-51/index.jsp?topic=%2Fcom.vmware.srm.admin.doc%2FGUID-0F7A37DF-30D5-4B04-87DB-6A4A4CF62A54.html

VMware White Paper. (2009). *VMware vCenter™ Site recovery manager performance and best practices for performance.* Retrieved from http://www.vmware.com/pdf/Perf_SiteRecoveryManager10_Best-Practices.pdf