Managing VMware vCenter Site Recovery Manager

This chapter contains the following sections:

About 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. The following terms are important for fully understanding SRM technology.

Array-based replication (ABR)

Replication of virtual machines that is managed and executed by the storage subsystem itself, rather than from inside the virtual machines, the vmkernel or the Service Console.

Failback

Reversal of direction of replication, and automatic reprotection of protection groups.

Failover

Event that occurs when the recovery site takes over operation in place of the protected site after the declaration of a disaster.

Protection group

A group of virtual machines that will be failed over together to the recovery site during testing or recovery.

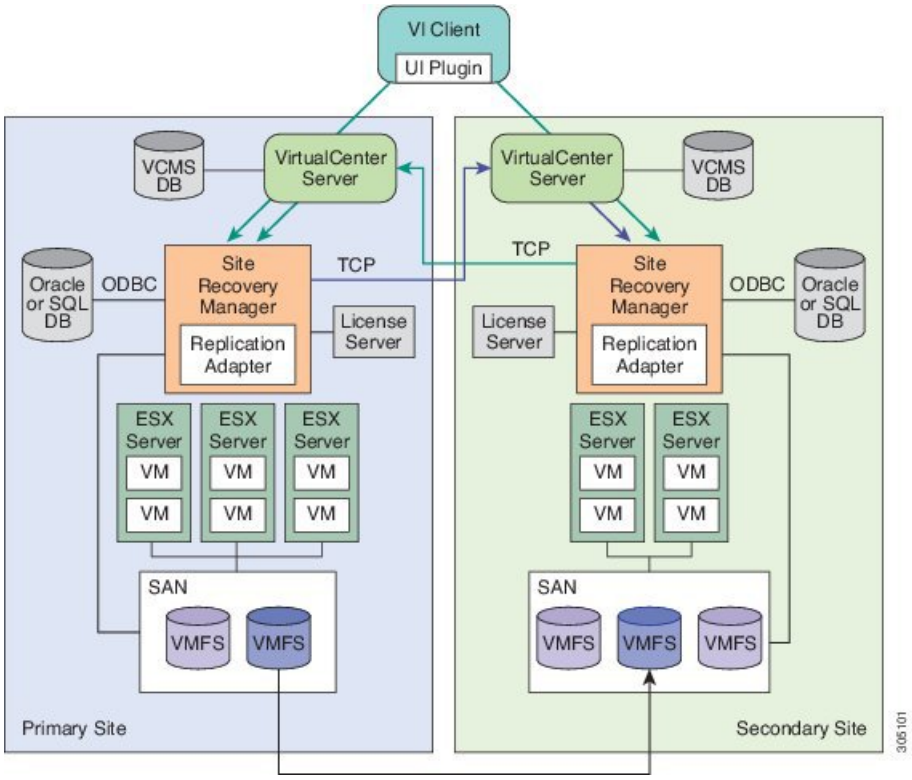
Protected site

The primary site that contains the virtual machines to be protected.

Recovery site

The secondary site to which virtual machines will fail over.

Figure 1: SRM Architecture



Overview of SRM Configuration

Configuring SRM after installation on the protected and recovery site involves the following steps:

1. Configure array managers in SRM: Array managers are identities of the storage systems at both the protected and recovery sites. Once SRM is installed, it interrogates the array managers and discovers which datastores have been marked for replication.
2. Define inventory mappings: Inventory mappings build a relationship between the folders, resource pools and networks between the protected site and recovery site. These mappings ensure that VMs are recovered to the correct location in the vCenter environment.
3. Create protection groups: Protection Groups are pointers to the replicated vSphere datastores that contain collections of virtual machines that will be failed over from the protected site to the recovery site.
4. Create recovery plans: A recovery plan is like an automated runbook. It controls every step of the recovery process, including the order in which virtual machines are powered off or powered on, the network addresses that recovered virtual machines use, and so on. A recovery plan applies to one or more protection groups. The protection groups use the inventory mappings to determine the location of placeholder VMs. These placeholder VMs are used in Recovery Plans to indicate when and where they should be recovered and allows for advanced features such as VM dependencies and scripting callouts.

Integrating SRM with Cisco UCS Director

The integration of SRM with Cisco UCS Director involves discovering and enabling the existing SRM environment in Cisco UCS Director. The various interlinked components in the SRM environment, such as inventory mappings, protection groups, and recovery plans, need to be identified and enabled in Cisco UCS Director. Identifying and enabling these components allows for the seamless communication between the primary site and recovery site when a disaster occurs.

Cisco UCS Director integration with the SRM API lets you create protection groups and initiate test, recovery, reprotect, or revert operations and collect the results. You can create a protection group, protect a VM, unprotect a VM, and add a protection group to a recovery plan using orchestration workflow tasks.

Prerequisites for Integrating SRM

Ensure that the following prerequisites are met prior to integrating SRM with Cisco UCS Director:

- Inventory mappings between protected and recovery sites, specifically resource pools, folders and networks have been configured.

  You can create folder, resource pool, and network mappings using Cisco UCS Director workflow tasks.

- Protection groups for the protected site have been created.

Note Currently, you can configure SRM to work with Cisco UCS Director by configuring array-based replication. Array-based replication surfaces replicated datastores to recover virtual machine workloads.

- A recovery plan has been created on the recovery site.

Enabling SRM in Cisco UCS Director

The following table describes the process of enabling SRM in Cisco UCS Director. Prior to completing the tasks below, ensure that the prerequisites are met. See Prerequisites for Integrating SRM, on page 3.

Task	Description
Add an SRM account	See Adding an SRM Account, on page 4.
Enable Resource Pool Mappings	Enable the resource pool mappings between protected and recovery sites in Cisco UCS Director. See Enabling Resource Pool and Folder Mappings, on page 5.
Enable Folder Mappings	Enable the folder mappings between protected and recovery sites in Cisco UCS Director. See Enabling Resource Pool and Folder Mappings, on page 5.

Task	Description
Enable Network Mappings	Enable the network mappings between protected and recovery sites in Cisco UCS Director. See Enabling Network Mappings, on page 6.
Enable Protection Groups	Enable the protected groups created in the protected site in Cisco UCS Director. See Mapping Datastores, on page 7.
Enable policies in the Virtual Datacenter (VDC)	Enable policies (computing, network and storage) in the VDC. See Enabling Policies in VDC, on page 8.

Adding an SRM Account

Before you begin

Ensure that the protection and recovery sites are configured properly.

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 On the **Virtual Accounts** page, click **Virtual Accounts**.

Step 3 Click **Add**.

Step 4 On the **Add Cloud** screen, choose VMware as the cloud type and complete the required fields.

Step 5 In the **Cloud Name** field, enter the name for the cloud.

Each cloud requires a unique name in Cisco UCS Director. The name cannot include single quotes. Once a cloud has been added, all reports refer to the cloud using the Cloud Name.

Step 6 Choose one of the following options to specify the VMware datacenter and/or VMware cluster:

a) Check **Use Credential Policy** and select a credential policy that includes an associated VMware datacenter.

b) In the **VMware Datacenter** field, enter the data center name on the vCenter account and in the **VMware Cluster** field, enter the cluster name.

The VMware datacenter name allows you to discover, monitor, and manage the specified pod's resources. Leave the field blank if the entire vCenter account is managed by Cisco UCS Director.

When you enter a cluster name, the vCenter account displays data center cluster-level information.

c) Check **Discover Datacenters / Clusters** to discover and use any VMware datacenters and associated VMware clusters. Any associated datacenters and clusters are displayed in the **Select Datacenters / Clusters** field.

Note Either a datacenter within the credential policy or the VMware datacenter and VMware cluster can be selected. Specifying the datacenter on the **Add Cloud** screen as well as in the credential policy form results in an error.

Step 7 Check **Enable SRM**.

Step 8 Choose the converged infrastructure pod from the **Pod** drop-down list.

When you choose a pod name, the VMware cloud account appears in the converged infrastructure stack.

Step 9 Click **Add**.

Enabling Resource Pool and Folder Mappings

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Computing**.

Step 2 On the **Computing** page, click **VMware Computing Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Computing Policy** screen, complete the fields, including the following:

a) In the **Policy Name** field, enter the name of the policy.

This name is used during catalog definition.

b) In the **Host Node/Cluster Scope** drop-down list, choose the scope of deployment.

Note You can narrow the scope of deployment by specifying whether to use all, include chosen, or exclude chosen options. Depending on the choices, a new field appears where the required hosts or clusters can be chosen.

c) In the **Filter Conditions** field, check the boxes for one or more conditions that the hosts should match.

Any hosts that do not meet these criteria are excluded from consideration. If more than one condition is chosen, all of the chosen conditions must match.

d) Check **Override Template** to override the template properties.

You are provided with options to enter custom settings for CPU and memory. The specified number of vCPUs for a VM should not exceed the total cores for the chosen scope of host nodes or clusters. The CPU reservation for the VM depends upon the number of vCPUs specified. The CPU limit is based on the chosen scope of host nodes or clusters. The CPU shares determine which VM gets CPU resources when there is competition among VMs.

e) Check **Allow Resizing of VM** to allow VM resizing before provisioning, or to resize an existing VM.

You are provided with options to enter custom settings for CPU and memory. The **Permitted Values for vCPUs** field is the range of vCPUs to use while provisioning a VM or resizing an existing VM. A range of more than 8 is visible during VM provisioning or resizing, only if the chosen cloud (vCenter) is 5 or above and has VM version 8. Only the values specified in the box are visible.

The **Permitted Values for Memory in MB** field is the range of memory to use while provisioning a VM or resizing an existing VM. For example: 512, 768, 1024, 1536, 2048, 3072, 4096, and so on. Only the values specified in the box are visible.

The VMs created using this policy can be deployed into a custom folder. Cisco UCS Director allows automatic creation of folder names from group names or from the available Macro provided by Cisco UCS Director.

For more information, see the Cisco UCS Director Orchestration Guide.

By specifying ${GROUP_NAME}, folders are created from the group name that uses this policy. You can specify a new or existing folder name.

If the **Enable protection** option is checked, only the folders that are mapped to the recovery site are listed in the drop-down folder.

Step 5 Click **Submit**.

Enabling Network Mappings

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.

Step 2 On the **Network** page, click **VMware Network Policy**.

Step 3 Click **Add**.

Step 4 On the **Network Policy Information** screen, complete the fields.

Step 5 Click **Add** in the VM Networks section to add and configure multiple vNICs. These vNICs are applicable to the VM that is provisioned using this policy.

Note To add or replace vNICs for provisioned or discovered VMs using VM actions, you must configure the vNICs.

Step 6 On the **Add Entry to VM Networks** screen, complete the fields, including the following:

a) If **Allow end user to select optional NICs** in the **Network Policy** dialog box is checked, the **Mandatory** check box is pre-selected. If the **Network Policy** dialog box was not selected, and **Allow end user to select optional NICs** is not checked, then the **NIC Alias** field is optional.

Note At least one of the NICs should have the **Mandatory** option selected. The NICs that have the **Mandatory** field selected are used in VM provisioning, and you will not have the option to select the NIC during VM service request creation.

b) In the **Adapter Type** drop-down list, choose the adapter type.

Note This option is not visible if the **Copy Adapter from Template** option is chosen.

Step 7 Click **Add (+)** in the **Port Groups** section. The **Add Entry to Port Groups** screen displays.

Step 8 Click **Select** to choose the port group name.

Note All the port groups mapped in the protection site to the corresponding recovery site are displayed here.

Step 9 From the **Select IP Address Type** drop-down field, choose **DHCP** (default) or **Static**.

a) If you choose **Static**, the **Select IP Address Source** drop-down field appears. Choose **IP Pool Policy** (default) or **Inline IP Pool**.

If you choose IP Pool Policy, the **Static IP Pool** field appears. In the **Select** dialog box, choose from the list of preconfigured static IP pool(s). If no preconfigured static IP pools exist, see the Adding a Static IP Policy topic in the Cisco UCS Director Administration Guide.

b) If you choose **Inline IP Pool**, complete the fields.

Step 10 Click **Submit**.

Step 11 Click **Submit** on the **Add Entry to VM Networks** screen.

Step 12 Click **Submit** on the **Network Policy Information** screen.

Viewing SRM Protection Group Reports

You can view the collected inventory for SRM resource mappings, protection groups, and recovery plans.

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **SRM Sites**.

Step 4 Click the row with the SRM site.

Step 5 Click **View Details** to see the details of the SRM site.

Step 6 Click **Protection Groups**.

Step 7 Click the row with the protection group.

Step 8 Click **View Details** to see the details of the SRM protection group.

By default, the **Unassigned Replicated VMs** page appears. You can also view the associated datastores, VMs, and recovery plans by clicking **Datastores**, **VMs**, or **Recovery Plans**.

Mapping Datastores

SRM protection groups let you group VMs to fail over from the protected site to the recovery site together as part of your recovery plan. You can enable protection groups when creating a new SRM storage policy, or when editing an existing SRM storage policy. The available datastores that you can map to your SRM storage policy is filtered based on the selected protection group. The recovery site VMs are provisioned on the selected protection group datastore.

For more information on adding a storage policy, see the Cisco UCS Director Administration Guide.

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Storage**.

Step 2 On the **Storage** page, click **VMware Storage Policy**.

Step 3 Do one of the following:

- Click **Add**.
- Choose the SRM storage policy on which you want to enable protection groups and click **Edit**.

Step 4 On the **Add Storage Resource Allocation Policy** screen, check **Enable Protection**.

Note If you are adding a new SRM storage policy, you must select an SRM cloud from the **Cloud Name** drop-down list for this option to appear.

Step 5 In the **Protection Group** field, click **Select**.

Step 6 Check the protection groups that you want to add to the storage policy, and click **Select**.

Step 7 On the **System Disk Policy** screen, if necessary, complete the required fields, and click **Next**.

Step 8 On the **Additional Disk Policies** screen, if necessary, configure a disk policy, and click **Next**.

Step 9 On the **Hard Disk Policy** screen, if necessary, specify the number of physical disks that you want to create during VM provisioning.

Step 10 Click **Submit**.

Enabling Policies in VDC

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Virtual Data Centers**.

Step 2 On the **Virtual Data Centers** page, click **vDC**.

Step 3 Click **Add**.

Step 4 On the **Add VDC** screen, select the cloud type, and click **Submit**.

Step 5 On the **Add VDC** screen, complete the fields, including:

a) Check **VDC Locked** to deny the use of the VDC for any further deployments.

Actions on existing VMs, within this VDC, are disabled. Uncheck **VDC Locked** to allow the use of the VDC for further deployments.

b) Check **Enable Protection** to enable protection.

If checked, all the policies for this account (compute, storage and network) that have SRM enabled are displayed here.

c) In the **User Action Policy** drop-down list, choose the policy that is used for execution of orchestration workflow post-provisioning of the VMs.

The chosen workflow appears as an action button for VMs within the VDC.

d) In the **Delete after Inactive VM days** drop-down list, choose the number of days to wait before deleting an inactive VM.

A VM that is in the inactive state is not powered-on.

Note Ensure that **Delete Inactive VMs Based on VDC Policy** is checked on the **Advanced Controls** screen under **Administration > System** for this choice to work as expected. For more information, see Enabling Advanced Controls.

Step 6 Click **Add**.