Using the vRealize Orchestrator Plug-In for Site Recovery Manager 6.1

Site Recovery Manager 6.1

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-002144-01

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2017 VMware, Inc. All rights reserved. Copyright and trademark information.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Using the Site Recovery Manager Plug-In 1

Using the vRealize Orchestrator Plug-In for Site Recovery Manager provides information and instructions about configuring and using the VMware® vRealize Orchestrator plug-in for VMware Site Recovery Manager.

Intended Audience

The information in *Using the vRealize Orchestrator Plug-In for Site Recovery Manager* is intended for experienced administrators who want to automate protection configuration tasks on a vSphere environment using the Site Recovery Manager plug-in. The information is written for experienced users who are familiar with virtual machine technology, with vRealize Orchestrator workflow development, and with VMware Site Recovery Manager.

For more information about vRealize Orchestrator, see http://www.vmware.com/support/pubs/orchestrator_pubs.html.

For more information about Site Recovery Manager, see http://www.vmware.com/support/pubs/srm_pubs.html.

Updated Information

This *Using the vRealize Orchestrator Plug-In for Site Recovery Manager* document is updated with each release of the product or when necessary.

This table provides the update history of the *Using the vRealize Orchestrator Plug-In for Site Recovery Manager* document.

Revision	Description
EN-002144-01	■ Updated the information in "Limitations of the Site Recovery Manager Plug-In," on page 27.
EN-002144-00	Initial release.

Automated Operations That the vRealize Orchestrator Plug-In for Site Recovery Manager Provides

2

With the vRealize Orchestrator plug-in for Site Recovery Manager, you can automate the creation of your Site Recovery Manager infrastructure to add virtual machines to protection groups and configure recovery settings of virtual machines.

With the vRealize Orchestrator plug-in for Site Recovery Manager you can protect virtual machines by adding them to array-based replication or to vSphere Replication protection groups. The plug-in does not automate the configuration of vSphere Replication on virtual machines. You can use the vRealize Orchestrator Plug-In for vSphere Replication to configure vSphere Replication on virtual machines, or configure vSphere Replication manually. For information about the vRealize Orchestrator Plug-In for vSphere Replication, see the release notes of the vRealize Orchestrator Plug-In for vSphere Replication.

The vRealize Orchestrator plug-in for Site Recovery Manager includes vRealize Orchestrator actions, workflows, policy templates to trigger actions when certain events occur, and scripting objects to expose selected elements of the Site Recovery Manager API to workflows.

- The plug-in provides actions and workflows that create a Site Recovery Manager infrastructure:
  - Create array-based protection groups and vSphere Replication protection groups
  - Create inventory mappings between matching objects
  - Add protection groups to existing recovery plans
- The plug-in provides actions and workflows that protect virtual machines:
  - Protect a virtual machine by using an existing array-based replication protection group
  - Protect a virtual machine by using an existing vSphere Replication protection group
- The plug-in provides actions and workflows that configure recovery settings on virtual machines:
  - Set the recovery priority
  - Configure virtual machine recovery settings
  - Create per-virtual machine recovery steps
  - Set the final power state of a recovered virtual machine
- The plug-in provides actions and workflows that orchestrate recovery of virtual machines:
  - Start test, cleanup, failover, and reprotect a recovery plan
  - Cancel the currently running recovery plan

Note The plugin starts test, cleanup, failover, reprotect, and cancel and immediately finishes the workflow. You can monitor the plan progress in the vSphere Web Client.

- The plug-in provides actions and workflows that obtain information from Site Recovery Manager Server:
  - List protected datastores
  - List protection groups and recovery plans
  - Find array-based protection groups by datastore
  - Get unassigned replication datastores and recovery plan states
- The plug-in provides a workflow to configure a local site:
  - Search the local site's LookupService for the local Site Recovery Manager URL
  - Connect to the local Site Recovery Manager Server and retrieve the local Site Recovery Manager certificate
  - Prompt you to examine and import the Site Recovery Manager certificate into the vRealize Orchestrator trust store or not import if the certificate is incorrect
- The plug-in provides a workflow to configure a remote site:
  - Obtain the RemoteSite LookupService URL from the local Site Recovery Manager extapi
  - Retrieve the remote site LookupService's SSL certificate
  - Prompt you to examine, import, or reject the LookupService certificate
  - After accepting the remote LookupService SSL certificate, search the remote site LookupService for the remote vCenter Server URL
  - Connect to the remote VC and retrieve its SSL certificate
  - Examine and import or reject this certificate

Note The workflows to configure local and remote sites assume that the vRealize Orchestrator trust store already contains the local site infrastructure node's SSL certificate and the local sitevCenter Server SSL certificate. In an embedded configuration, the vRealize Orchestrator trust store contains only one certificate. You must rerun the appropriate workflows if an administrator updates any of the SSL certificates.

Installing and Configuring the Site Recovery Manager Plug-In

3

If you want to create and run workflows on the protected and recovery Site Recovery Manager sites, you must install and configure the Site Recovery Manager plug-in on both sites.

This chapter includes the following topics:

Site Recovery Manager Plug-In Functional Prerequisites

To install and use the Site Recovery Manager plug-in, your system must meet certain functional prerequisites.

Site Recovery Manager

Verify that the version of your Site Recovery Manager plug-in is compatible with your Site Recovery Manager.

For information about the compatibility between the Site Recovery Manager plug-in and Site Recovery Manager, see *vRealize Orchestrator plug-in for Site Recovery Manager 6.1 Release Notes*.

For information about setting up Site Recovery Manager, see the *Site Recovery Manager Installation and Configuration* documentation.

vRealize Orchestrator

Verify that you have a running instance of Orchestrator and its version is compatible with the versions of your Site Recovery Manager and Site Recovery Manager plug-in.

For information about the compatibility between Site Recovery Manager and Orchestrator, see the *vRealize Orchestrator plug-in for Site Recovery Manager 6.1 Release Notes* and *Compatibility Matrixes for Site Recovery Manager 6.1* documentation.

For information about setting up Orchestrator, see *the Installing and Configuring VMware vRealize Orchestrator* documentation.

Other Prerequisites

Verify that you have installed a vCenter Server plug-in. See the *Using the vCenter Server Plug-In* topic in the vRealize Orchestrator documentation.

Installing, Upgrading, and Uninstalling the Site Recovery Manager Plug-In

You can use the Site Recovery Manager plug-in after you install it on a Orchestrator instance. The version of the Site Recovery Manager plug-in must be compatible with your Site Recovery Manager and Orchestrator.

Installing the Site Recovery Manager Plug-In

You can install the Site Recovery Manager plug-in if your Site Recovery Manager sites are paired and your Orchestrator instance is configured to work with your vSphere environment.

You must configure Orchestrator to use the vSphere configuration by configuring Component Manager, vCenter Server Single Sign-On, and the vCenter Server plug-in.

For information about how to configure your Orchestrator to work with a vSphere environment, see the *Configuring vRealize Orchestrator* section in the *Installing and Configuring VMware Realize Orchestrator* documentation.

You can download the Site Recovery Manager plug-in installation `.vmoapp` file from the download page of Site Recovery Manager.

You can install the Site Recovery Manager plug-in by using the `http://your_orchestrator_server:8283/vco-config` configuration interface. For information about how to install the `.vmoapp` file on your Orchestrator instance, see the *Install a New Plug-In Distributed as a VMOAPP File* topic in the *Installing and Configuring VMware Realize Orchestrator* documentation.

Upgrading and Uninstalling the Site Recovery Manager Plug-In

You can upgrade your Site Recovery Manager plug-in by uninstalling your plug-in and installing the new version.

You can uninstall your Site Recovery Manager plug-in by using the `http://your_orchestrator_server:8283/vco-config` configuration interface. For more information about how to uninstall your Site Recovery Manager plug-in, see the Uninstall a Plug-in topic in the *Installing and Configuring VMware Realize Orchestrator* documentation and the following KB : http://kb.vmware.com/kb/2064575, *Uninstalling a plug-in from VMware vRealize Orchestrator 5.5.x, 6.0.x, and 7.0.0* .

Configure the Site Recovery Manager Plug-In

Before you run other Site Recovery Manager workflows, you must configure the plug-in by running the Site Recovery Manager configuration workflows.

Procedure

1. Log in to the Orchestrator client as an administrator and select **Design** or **Run** from the drop-down menu in the left upper corner.
2. Click the **Workflows** view.
3. Select **Library > SRM > Configuration**.
4. Run the **Configure Local Sites** workflow.

   The workflow registers the Site Recovery Manager certificates, so that you can access the Site Recovery Manager inventory.

   a. Right-click the workflow and select **Start workflow**.

   b. Select whether to install the SSL certificates automatically without user confirmation and click **Submit**.

5 Run the **Configure Remote Site** workflow.

The workflow registers the Site Recovery Manager certificates on the remote vCenter Server or Platform Services Controller, so that you can log in to the remote site.

a Right-click the workflow and select **Start workflow**.

b Click **Not set** and, from the inventory tree, select the local site.

c Select whether to install the SSL certificates automatically without user confirmation and click **Submit**.

6 Run the **Login Remote Site** workflow.

The workflow logs you to the remote site, so that you can run other Site Recovery Manager workflows.

a Right-click the workflow and select **Start workflow**.

b Click **Not set** and, from the inventory tree, select the local site.

c Provide a user name and password for the site and click **Submit**.

Note You must run this workflow once per Orchestrator client session. The Orchestrator logs out of Site Recovery Manager when you log out of the Orchestrator client.

What to do next

Perform the procedure on the opposite Site Recovery Manager site to create and run workflows on both sites.

Using the Site Recovery Manager Plug-In Workflows

4

The Site Recovery Manager plug-in workflow library contains workflows that you can use to automate Site Recovery Manager tasks. With the predefined workflows you can run tests and cleanup, run recoveries and reprotect, and cancel recovery plans. You can use the predefined workflows to create custom workflows.

You can use the **Inventory** view in the Orchestrator client to manage the available Site Recovery Manager resources. You can use the scripting API of the plug-in to create custom workflows.

This chapter includes the following topics:

Using the Site Recovery Manager Plug-In Inventory

You can use the Inventory view to run workflows on Site Recovery Manager objects.

To display the workflows that are available for an inventory object, navigate to **Tools > User preferences > Inventory** and select the **Use contextual menu in inventory** check box. After the option is enabled, when you right-click an object in the Orchestrator inventory, all available workflows for the object are displayed.

Prerequisites for Using the Site Recovery Manager Plug-In

To use the Site Recovery Manager plug-in, your environment must meet certain requirements.

- Verify that you have Site Recovery Manager server instances installed on both sites and that they are paired.
- Verify that your Orchestrator instance is configured to work with the vSphere infrastructure. See the *Configure Orchestrator to Work with the vSphere 6.0* infrastructure topic in the vRealize Orchestrator documentation.

User Scenario: Create, Test, and Run a Recovery Plan with the Site Recovery Manager Plug-In and by Using Array-Based Replication

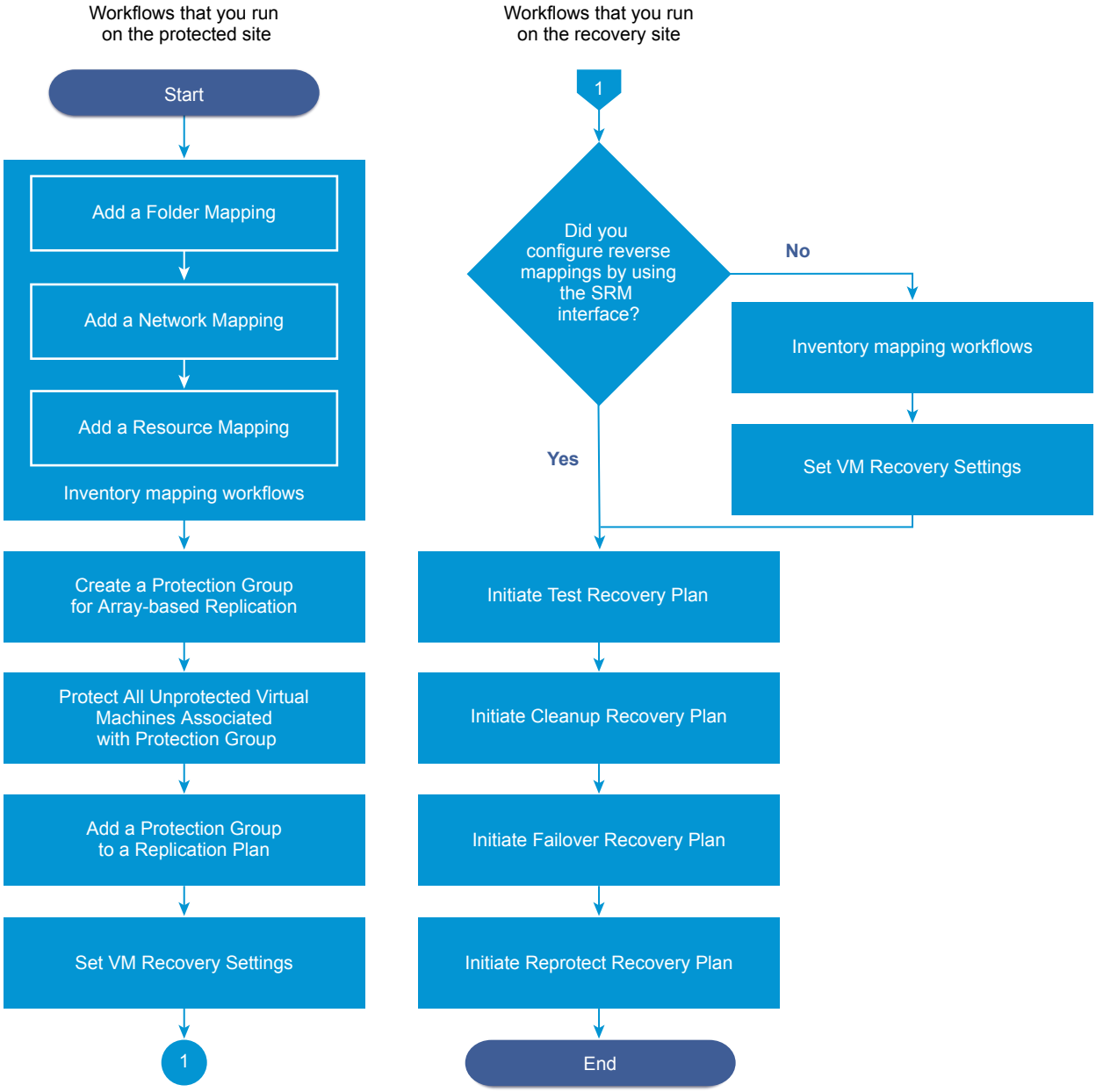
As an administrator you want to protect the YourCo company website environment. In this scenario, you use array-based replication to protect the virtual machines from Protected Site A to Recovery Site B and reprotect them back.

In each site you have vCenter Server instances, paired Site Recovery Manager instances, and the following components.

Table 4-1. YourCo Environment Details

Object	Description
Datastore A	A datastore on Protected Site A, configured for array-based replication with Datastore B on Recovery Site B.
Production A	A network on Protected Site A, used by the virtual machines on Protected Site A.
Host A	A host on Protected Site A.
Folder A	A folder that contains the virtual machines on Protected Site A.
YourCo DB VM	A virtual machine on Protected Site A that contains the database for the YourCo website environment.
YourCo App VM	A virtual machine on Protected Site A that contains the application services for the YourCo website.
YourCo Web VM	A virtual machine on Protected Site A that contains the web services for the YourCo website.
Datastore B	A datastore on Recovery Site B, configured for array-based replication with Datastore A.
Production B	A network on Recovery Site B.
Host B	A host on Recovery Site B.
Folder B	A folder on Recovery Site B.

In the current user scenario, you use the Site Recovery Manager plug-in workflows shown in the following figure to create inventory mappings, a protection group for array-based replication, and test and run a recovery plan. After you run the recovery plan, you run a workflow to restore your environment on the protected site.



Prerequisites

- Verify that you have Site Recovery Manager server instances installed on both sites and that they are paired.
- Verify that you have array pairing configured for the datastores you want to protect.
- Verify that you installed and configured vRealize Orchestrator on each Site Recovery Manager site.
- Verify that you installed and configured your vRealize Orchestrator plug-in for Site Recovery Manager plug-in on each Site Recovery Manager site.

Procedure

1 User Scenario: Configure Inventory Mappings on page 18

You run inventory mappings workflows to specify how Site Recovery Manager maps the resources on Protected Site A to resources on Recovery Site B.

2 User Scenario: Create a Protection Group for Array-Based Replication on page 20

You specified how Site Recovery Manager maps the resources between the two sites. The next step is to create protection groups to enable Site Recovery Manager to protect virtual machines.

3 User Scenario: Protect All Unprotected Virtual Machines Associated with a Protection Group on page 21

You created the protection group with Datastore A. To protect your virtual machines when you use array-based replication, you must configure the protection of your virtual machines that reside on Datastore A. The next step is to configure the protection of your virtual machines by running the Protect All Unprotected Virtual Machines Associated with the Protection Group workflow.

4 User Scenario: Add a Protection Group to a Recovery Plan on page 21

You protected the virtual machines in Datastore A and created a recovery plan using the Site Recovery Manager interface. The next step is to add the protection group to a recovery plan to include it in a recovery run.

5 User Scenario: Set Virtual Machine Recovery Settings on page 22

You added the protection group to the recovery plan. The next step is to configure the virtual machine recovery settings such as priority, power state, and recovery prompt messages. The priority defines the order in which Site Recovery Manager plug-in powers the virtual machines on or off.

6 User Scenario: Test a Recovery Plan on page 23

You set the recovery priority setting of the virtual machines. The next step is to test the recovery plan. Testing the recovery plan ensures that the virtual machines in the plan recover correctly to the recovery site.

7 User Scenario: Clean up a Recovery Plan on page 24

You tested the recovery plan with a test workflow. The next step is to run a cleanup workflow to return the recovery plan to the Ready state. You must complete the cleanup operation before you can run a failover or another test.

8 User Scenario: Run a Recovery Plan on page 25

You used the cleanup workflow to return the recovery plan to the Ready state after the test. The next step is to run a failover recovery plan workflow to perform a disaster recovery of all virtual machines to the recovery site.

9 User Scenario: Reprotect Your Resources After Recovery on page 26

You used the failover workflow to perform a disaster recovery. The next step is to run the Initiate Reprotect Recovery Plan workflow to reconfigure the protection groups and recovery plan to work in the opposite direction.

User Scenario: Configure Inventory Mappings

You run inventory mappings workflows to specify how Site Recovery Manager maps the resources on Protected Site A to resources on Recovery Site B.

In this scenario you map the virtual machines in Folder A, Production A network, and Host A on the Protected Site A to the corresponding folder, network, and host resources on Recovery Site B.

Note You run the current workflows on Protected Site A.

To configure the reverse mappings, you can run the following procedure on Recovery Site B by using the opposite source and destination resources or you can configure the reverse mappings by using the Site Recovery Manager interface.

Prerequisites

Connect to Protected Site A by using the Orchestrator client.

- Verify that you ran the Login Remote Site workflow for the current Orchestrator client session.
- Verify that Folder A is not mapped to any folder. You can check the folder mappings by using the Site Recovery Manager interface.
- Verify that the Production A network and Host A are not mapped to another network and host. You can check the existing network and resource mappings by running the Get Network Mappings and Get Resource Mapping workflows or by using the Site Recovery Manager interface.

Verify that you ran the Login Remote Site workflow for the current Orchestrator client session.

Procedure

1. Log in to the Orchestrator client as an administrator and select **Design** or **Run** from the drop-down menu in the upper-left corner.
2. Click the **Workflows** view in the Orchestrator client left pane.
3. Select **Library > SRM > Inventory Mappings**.
4. Run the **Add a Folder Mapping** workflow.
   a. Right-click the workflow and select **Start workflow**.
   b. Under Site setting, click **Not set** and from the inventory tree select **Protected Site A** .
   c. Under Local Folder setting, click **Not set** and select virtual machines **Folder A**.
   d. Under Remote Folder setting, click **Not Set** and select remote virtual machines **Folder B** to map.
   e. Click **Submit**.
5. Run the **Add a Network Mapping** workflow.
   a. Right-click the workflow and select **Start workflow**.
   b. Under Site setting, click **Not set** and from the inventory tree select **Protected Site A**.
   c. Under Local Network setting, click **Not set** and select **Production A** network.
   d. Under Remote Network setting, click **Not Set** and select remote **Production B** network to map.
   e. Click **Submit**.
6. Run the **Add a Resource Mapping** workflow.
   a. Right-click the workflow and select **Start workflow**.
   b. Under Site setting, click **Not set** and from the inventory tree select **Protected site A**.
   c. Under Local Resource setting, click **Not set** and select **Host A**.
   d. Under Remote Resource setting, click **Not Set** and select the remote **Host B** to map.
   e. Click **Submit**.

What to do next

Create a protection group for array-based replication. See "User Scenario: Create a Protection Group for Array-Based Replication," on page 20.

User Scenario: Create a Protection Group for Array-Based Replication

You specified how Site Recovery Manager maps the resources between the two sites. The next step is to create protection groups to enable Site Recovery Manager to protect virtual machines.

In this scenario you create a protection group for Datastore A to protect YourCo Web VM, YourCo App VM, and YourCo DB VM.

NOTE You run the current workflow on Protected Site A.

Prerequisites

- Connect to Protected Site A by using the Orchestrator client.
- Verify that you ran the Login Remote Site workflow for the current Orchestrator client session.
- Verify that you ran the inventory mapping workflows. See "User Scenario: Configure Inventory Mappings," on page 18.
- Verify that YourCo ABR Protection Group does not exist by running the List Protection Groups workflow .
- Verify that Datastore A is not part of an existing protection group. You can run the Find ABR Protection Group by Datastore, Get Unassigned Replicated Datastores, and List Protected Datastores workflows to check which protection group the Datastore A is assigned to.

Procedure

1 In the Orchestrator client left pane, click the **Workflows** view.

2 Select **Library > SRM > Protection Groups**.

3 Run the **Create Protection Group for Array Based Replication** workflow.

   a Right-click the workflow and select **Start workflow**.

   b Under the Protection Folder setting click **Not set** and select the **Protections Group** folder.

   c Enter a name and description.

   For this scenario enter, **`YourCo ABR Protection Group`**.

   d Under the Datastores setting click **Not Set**, click **Insert value**, and select **Datastore A**.

   You can select Datastore A if it is not assigned to another protection group.

   e Click **Submit**.

What to do next

Protect the virtual machines associated with the protection group. See "User Scenario: Protect All Unprotected Virtual Machines Associated with a Protection Group," on page 21.

User Scenario: Protect All Unprotected Virtual Machines Associated with a Protection Group

You created the protection group with Datastore A. To protect your virtual machines when you use array-based replication, you must configure the protection of your virtual machines that reside on Datastore A. The next step is to configure the protection of your virtual machines by running the Protect All Unprotected Virtual Machines Associated with the Protection Group workflow.

By running the workflow, you apply the configured inventory mappings to your virtual machines and create placeholder virtual machines on the placeholder Datastore B on Recovery Site B. For information about applying inventory mappings to your virtual machines, see the *Apply Inventory Mappings to All Members of a Protection Group* topic in the *Site Recovery Manager Administration* documentation.

In this scenario all virtual machines in Datastore A are unprotected.

Note You run the current workflow on Protected Site A.

Prerequisites

- Connect to Protected Site A by using the Orchestrator client.
- Verify that you ran the Login Remote Site workflow for the current Orchestrator client session.
- Create a protection group for array-based replication. See "User Scenario: Create a Protection Group for Array-Based Replication," on page 20.

Procedure

1. In the Orchestrator client left pane, click the **Workflows** view.
2. Select **Library > SRM > Protection Groups**.
3. Run the **Protect All Unprotected Virtual Machines Associated with Protection Group** workflow.
   a. Right-click the workflow and select **Start workflow**.
   b. Under the Protection Group setting click **Not Set** and select **YourCo ABR Protection Group**.
   c. Click **Submit**.

What to do next

1. Create a recovery plan called YourCo RP by using the Site Recovery Manager interface in the vSphere Web Client. See the *Create a Recovery Plan* topic in the *Site Recovery Manager Administration* documentation.
2. Add the protection group to the recovery plan. See "User Scenario: Add a Protection Group to a Recovery Plan," on page 21.

User Scenario: Add a Protection Group to a Recovery Plan

You protected the virtual machines in Datastore A and created a recovery plan using the Site Recovery Manager interface. The next step is to add the protection group to a recovery plan to include it in a recovery run.

In this scenario you add the YourCo ABR Protection Group to the YourCo RP recovery plan.

Note You run the current workflow on Protected Site A.

Prerequisites

- Connect to Protected Site A by using the Orchestrator client.

- Verify that you ran the Login Remote Site workflow for the current Orchestrator client session.
- Protect the virtual machines associated with the protection group. See "User Scenario: Protect All Unprotected Virtual Machines Associated with a Protection Group," on page 21.
- Create a recovery plan called YourCo RP using the Site Recovery Manager interface in the vSphere Web Client. See the Create a Recovery Plan topic in the Site Recovery Manager documentation center. You can run the List Recovery Plans workflow to check whether YourCo RP exists.

Procedure

1 In the Orchestrator client left pane, click the **Workflows** view.

2 Select **Library > SRM > Recovery Plans**.

3 Run the **Add Protection Group to Recovery Plan** workflow.

   a Right-click the workflow and select **Start workflow**.

   b Under the Recovery Plan setting click **Not set** and select **YourCo RP**.

   c Under the Protection Group setting click **Not Set** and select **YourCo ABR Protection Group** to add.

   d Click **Submit**.

What to do next

Configure the virtual machines recovery settings. See "User Scenario: Set Virtual Machine Recovery Settings," on page 22.

User Scenario: Set Virtual Machine Recovery Settings

You added the protection group to the recovery plan. The next step is to configure the virtual machine recovery settings such as priority, power state, and recovery prompt messages. The priority defines the order in which Site Recovery Manager plug-in powers the virtual machines on or off.

In this scenario you set the power on order of the virtual machines and pre-power on prompt messages. YourCo App VM and YourCo Web VM depend on the database, so YourCo DB VM must power on first , YourCo App VM second, and YourCo Web VM last.

Note You run the current workflow on Protected Site A.

Prerequisites

- Connect to Protected Site A by using the Orchestrator client.
- Verify that you ran the Login Remote Site workflow for the current Orchestrator client session.
- Add the protection group to the recovery plan. See "User Scenario: Add a Protection Group to a Recovery Plan," on page 21.

Procedure

1 In the Orchestrator client left pane, click the **Workflows** view.

2 Select **Library > SRM > Recovery Plans**.

3 Run the **Set VM Recovery Settings** workflow for YourCo DB VM, YourCo App VM, and YourCo Web VM.

   a Right-click the workflow and select **Start workflow**.

   b Under the Recovery Plan setting, click **Not set** and select **YourCo RP**.

   c Under the VM setting, click **Not Set**, select the virtual machine that you want to configure, and click **Next**.

d Under the Power setting, click **Not Set**, in the Filter text box type **`powered`**, and select **poweredOn** for the replicated virtual machine final power state.

To use this feature, your VMs must use VMware Tools.

e Click **Next**.

f Under Priority Group setting click **Not Set**, in the **Filter** text box type **`priority`**, and select the priority for the virtual machine.

Set the following priority for the virtual machines.

Virtual Machine Name	Priority Group
YourCo DB VM	Priority 1
YourCo App VM	Priority 2
YourCo Web VM	Priority 3

g Click **Next**.

h (Optional) Set a pre power on step to prompt users or Site Recovery Manager to perform tasks on the virtual machine before Site Recovery Manager powers it on.

Ask user to check the free disk space on Datastore B with the following prompt text.

```
Verify that the datastore has 100 GB free disk space.
```

To use this feature, your VMs must use VMware Tools. For information about writing command steps, see the Guidelines for Writing Command Steps and Environment Variables for Command Steps topics in the Site Recovery Manager documentation center.

i (Optional) Set a post power on steps to prompt users or Site Recovery Manager to perform tasks on the virtual machine after Site Recovery Manager powers it on.

To use this feature, your VMs must use VMware Tools. For information about writing command steps, see the Guidelines for Writing Command Steps and Environment Variables for Command Steps topics in the Site Recovery Manager documentation center.

j Click **Submit**.

What to do next

Start a test recovery plan workflow. See "User Scenario: Test a Recovery Plan," on page 23.

User Scenario: Test a Recovery Plan

You set the recovery priority setting of the virtual machines. The next step is to test the recovery plan. Testing the recovery plan ensures that the virtual machines in the plan recover correctly to the recovery site.

In this scenario you test the YourCo RP recovery plan. The virtual machines on Protected Site A stay powered on.

Note You run the current workflow on Recovery Site B.

You can observe the progress of the recovery process in your Site Recovery Manager interface. To get a detailed record of the recovery process, you can use the Site Recovery Manager interface to generate a report.

Prerequisites

- Connect to Recovery Site B by using the Orchestrator client.
- Verify that you ran the Login Remote Site workflow for the current Orchestrator client session.

- Configure the virtual machines recovery settings. See "User Scenario: Set Virtual Machine Recovery Settings," on page 22.
- Verify that the recovery plan is in the Ready state. You can check the state of your recovery plan by running the Get Recovery State workflow or by using the Site Recovery Manager interface. For information about the states of recovery plans, see the *Recovery Plan Status Reference* topic in the Site Recovery Manager documentation center and the RecoveryPlanGetInfo section in *Site Recovery Manager API Developer's Guide* documentation.

Procedure

1. Log in to the Orchestrator client as an administrator and select **Design** or **Run** from the drop-down menu in the upper-left corner.
2. Click the **Workflows** view in the Orchestrator client left pane.
3. Select **Library > SRM > Recovery Plans**.
4. Run the **Initiate Test Recovery Plan** workflow.
   a. Right-click the workflow and select **Start workflow**.
   b. Under Plan setting, click **Not set** and select the **YourCo RP** recovery plan on Recovery Site B to run.
   c. Click **Submit**.

What to do next

Run an Initiate Cleanup Recovery Plan workflow. See "User Scenario: Clean up a Recovery Plan," on page 24.

User Scenario: Clean up a Recovery Plan

You tested the recovery plan with a test workflow. The next step is to run a cleanup workflow to return the recovery plan to the Ready state. You must complete the cleanup operation before you can run a failover or another test.

In this scenario you run the Initiate Cleanup Recovery Plan workflow for the YourCo RP recovery plan.

NOTE You run the current workflow on Recovery Site B.

You can observe the progress of the recovery process in your Site Recovery Manager interface. To get a detailed record of the cleanup process, you can use the Site Recovery Manager interface to generate a report.

Prerequisites

- Connect to Recovery Site B by using the Orchestrator client.
- Verify that you ran the Login Remote Site workflow for the current Orchestrator client session.
- Verify that you tested the recovery plan. See "User Scenario: Test a Recovery Plan," on page 23.
- Verify that the recovery plan is in the Test complete or in the needsCleanup state. You can check the state of your recovery plan by running the Get Recovery State workflow or by using the Site Recovery Manager interface. For information about the states of recovery plans, see the *Recovery Plan Status Reference* topic in the Site Recovery Manager documentation center and the RecoveryPlanGetInfo section in *Site Recovery Manager API Developer's Guide* documentation.

Procedure

1. Log in to the Orchestrator client as an administrator and select **Design** or **Run** from the drop-down menu in the left upper corner.
2. Click the **Workflows** view in the Orchestrator client left pane.

3 Select **Library > SRM > Recovery Plans**.

4 Run the **Initiate Cleanup Recovery Plan** workflow.

   a Right-click the workflow and select **Start workflow**.

   b Under Plan setting click **Not set** and select the **YourCo RP** recovery plan on Recovery Site B to run.

   c Click **Submit**.

What to do next

Run an Initiate Failover Recovery Plan workflow. See "User Scenario: Run a Recovery Plan," on page 25.

User Scenario: Run a Recovery Plan

You used the cleanup workflow to return the recovery plan to the Ready state after the test. The next step is to run a failover recovery plan workflow to perform a disaster recovery of all virtual machines to the recovery site.

In this scenario you run the YourCo RP recovery plan to perform disaster recovery of the resources on Protected Site A to Recovery Site B.

Note You run the current workflow on Recovery Site B.

You can observe the progress of the recovery process in your Site Recovery Manager interface. To get a detailed record of the recovery process, you can use the Site Recovery Manager interface to generate a report .

For information about the disaster recovery, see the *Performing a Planned Migration or Disaster Recovery By Running a Recovery Plan* topic in the Site Recovery Manager documentation center.

Prerequisites

- Connect to Recovery Site B by using the Orchestrator client.
- Verify that you ran the Login Remote Site workflow for the current Orchestrator client session.
- Verify that you ran a recovery plan cleanup. See "User Scenario: Clean up a Recovery Plan," on page 24.
- Verify that the recovery plan is in a Ready state. You can check the state of your recovery plan by running the Get Recovery State workflow or by using the Site Recovery Manager interface. For information about the states of recovery plans, see the *Recovery Plan Status Reference* topic in the Site Recovery Manager documentation center and the RecoveryPlanGetInfo section in *Site Recovery Manager API Developer's Guide* documentation.

Procedure

1 Log in to the Orchestrator client as an administrator and select **Design** or **Run** from the drop-down menu in the left upper corner.

2 Click the **Workflows** view in the Orchestrator client left pane.

3 Select **Library > SRM > Recovery Plans**.

4 Run the **Initiate Failover Recovery Plan** workflow.

   a Right-click the workflow and select **Start workflow**.

   b Under Plan setting click **Not set** and select the **YourCo RP** recovery plan on Recovery Site B to run.

   c Click **Submit**.

What to do next

Start a Reprotect Recovery Plan workflow. See "User Scenario: Reprotect Your Resources After Recovery," on page 26

User Scenario: Reprotect Your Resources After Recovery

You used the failover workflow to perform a disaster recovery. The next step is to run the Initiate Reprotect Recovery Plan workflow to reconfigure the protection groups and recovery plan to work in the opposite direction.

In this scenario you run the Initiate Reprotect Recovery Plan workflow to reverse the protection direction and reconfigure the YourCo ABR Protection Group and YourCo RP recovery plan to work for replication from Recovery Site B to Protected Site A.

Note You run the current workflow on Recovery Site B.

You can observe the progress of the reprotect process on your Site Recovery Manager interface. To get a detailed record of the reprotect process, you can use the Site Recovery Manager interface to generate a report.

For information about the reprotect states, see the *Reprotect States* topic in the Site Recovery Manager documentation center and the RecoveryPlanGetInfo section in *Site Recovery Manager API Developer's Guide*.

For information about the reprotection with array-based replication, see the *How Site Recovery Manager Reprotects Virtual Machines with Array Based Replication* topic in the Site Recovery Manager documentation center.

Prerequisites

- Connect to Recovery Site B by using the Orchestrator client.
- Verify that you ran the Login Remote Site workflow for the current Orchestrator client session.
- Verify that you ran a recovery plan failover workflow. See "User Scenario: Run a Recovery Plan," on page 25.
- Verify that you configured reverse mapping by running the Inventory Mappings workflows with reversed source and destination resources on Recovery Site B or by using the Site Recovery Manager interface. See "User Scenario: Configure Inventory Mappings," on page 18.
- Verify that you satisfied the preconditions for performing reprotect, see the *Preconditions for Performing Reprotect* topic in the Site Recovery Manager documentation center.
- Verify that you performed a successful planned migration by using the API, by creating a custom workflow in Orchestrator, or by using the Site Recovery Manager interface.
- Verify that the recovery plan is in the Recovery complete or in the failedOver state. You can check the state of your recovery plan by running the Get Recovery State workflow or by using the Site Recovery Manager interface. For information about the states of recovery plans, see the *Recovery Plan Status Reference* topic in the Site Recovery Manager documentation center and the RecoveryPlanGetInfo section in the*Site Recovery Manager API Developer's Guide* documentation.

Procedure

1. Log in to the Orchestrator client as an administrator and select **Design** or **Run** from the drop-down menu in the left upper corner.
2. Click the **Workflows** view in the Orchestrator client left pane.
3. Select **Library > SRM > Recovery Plans**.

4 Run the **Initiate Reprotect Recovery Plan** workflow.

   a Right-click the workflow and select **Start workflow**.

   b Under Plan setting click **Not set** and select the YourCo RP recovery plan to run.

   c Click **Submit**.

   Recovery Site B is the protected Site Recovery Manager site and Protected Site A is the recovery Site Recovery Manager site. The recovery plan on Protected Site A is in the Ready state .

What to do next

After a reprotect operation, you can reverse the protected and recovery sites back to the initial recovery direction.

1 Run an Initiate Test Recovery Plan workflow on Protected Site A. Use "User Scenario: Test a Recovery Plan," on page 23 and select the recovery plan on Protected Site A.

2 Run an Initiate Cleanup Recovery Plan workflow on Protected Site A. Use "User Scenario: Clean up a Recovery Plan," on page 24 and select the recovery plan on Protected Site A.

3 Run an Initiate Failover Recovery Plan workflow. Use "User Scenario: Run a Recovery Plan," on page 25 and select the recovery plan on Protected Site A.

4 Run an Initiate Reprotect Recovery Plan workflow, to restore the original configuration of the protected and recovery sites. Use "User Scenario: Run a Recovery Plan," on page 25 and select the recovery plan on Protected Site A.

Limitations of the Site Recovery Manager Plug-In

Site Recovery Manager plug-in is subject to limitations.

When working with the Site Recovery Manager plug-in, consider the following limitations:

- You cannot create, edit, or delete recovery plans.
- You cannot add or remove test network mapping to a recovery plan.
- You cannot rescan storage to discover newly added replicated devices.
- You cannot delete folder, network, and resource pool mappings.
- You cannot delete protection groups.
- You cannot customize IP settings by using the Site Recovery Manager plug-in.
- The `unassociateVms` and `unrotectVms` methods are not available in the plug-in. You can use them by using the Site Recovery Manager public API.

Index