Dell EMC RecoverPoint for Virtual Machines

Version 5.2

Basic Configuration Installation Guide

P/N 302-004-998
REV 02
January 2019

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
02	January 2019	Published with release of RecoverPoint for VMs 5.2.1.
01	July 2018	First release of RecoverPoint for VMs 5.2.

Purpose of the basic configuration installation

Thank you for choosing RecoverPoint for Virtual Machines, a virtualized solution that provides data replication, protection, and recovery within the VMware vSphere environment. This guide provides a step-by-step explanation for installing a basic configuration to replicate virtual machines between two sites. This installation is targeted at low-scale environments with minimal redundancy and can be used to show proof of concept.

Using this guide, you create RecoverPoint for VMs clusters and connect them to form a working replication system.

For more advanced installations, refer to the *RecoverPoint for Virtual Machines Installation and Deployment Guide*. For larger scale configuration information, refer to the *RecoverPoint for Virtual Machines Scale and Performance Guide*. These guides may be found at https://support.emc.com/.

Terminology

If you are new to RecoverPoint or VMware architectures, review these definitions before continuing.

vRPA

The virtual RecoverPoint Appliance is a data appliance that manages data replication. You create the vRPAs you need by using the vSphere web Client from the vCenter Server.

vRPA cluster

A group of up to 8 vRPAs in the same cluster that work together to replicate and protect data. In this installation process, you create 2 vRPA clusters with 2 vRPAs in each cluster.

RecoverPoint for VMs plug-in

The vSphere web client user interface for managing VM replication. The plug-in is installed automatically after the vRPA cluster has been installed.

RecoverPoint for VMs splitter

Proprietary software that is installed on every ESXi host in an ESXi cluster that is involved in RecoverPoint for VMs replication or running virtual RPAs. The splitter splits every write to the VMDK and sends a copy of the write to the vRPA and then to the designated storage volumes. It is installed automatically after you register the ESXi cluster.

RecoverPoint for VMs system

One or more connected vRPA clusters. Use this document to configure a RecoverPoint for VMs system that connects two vRPA clusters, one at each of two sites.

vRPA LAN network

vRPA cluster management network that is used for communication between vRPAs and to other entities such as the vCenter.

vRPA WAN network

vRPA inter-cluster network that is used for communication between vRPA clusters. The basic configuration uses a unified topology: a single WAN+LAN network. This topology does not require an additional gateway to communicate between sites.

vRPA data (IP) network

Data network that is used for traffic between the vRPA and the ESXi splitter.

Reference architecture

For ease of deployment and proof of concept, this guide uses a reference architecture that features a basic configuration that includes:

- Two vRPA clusters, one at Site A and one at Site B
- Two vRPAs at each vRPA cluster
- Two vCenters
- Two ESXi hosts on each vCenter
- Two vNICs per vRPA, one for LAN + WAN and the other for data (IP) communication
- One VMkernel port for each ESXi

Note

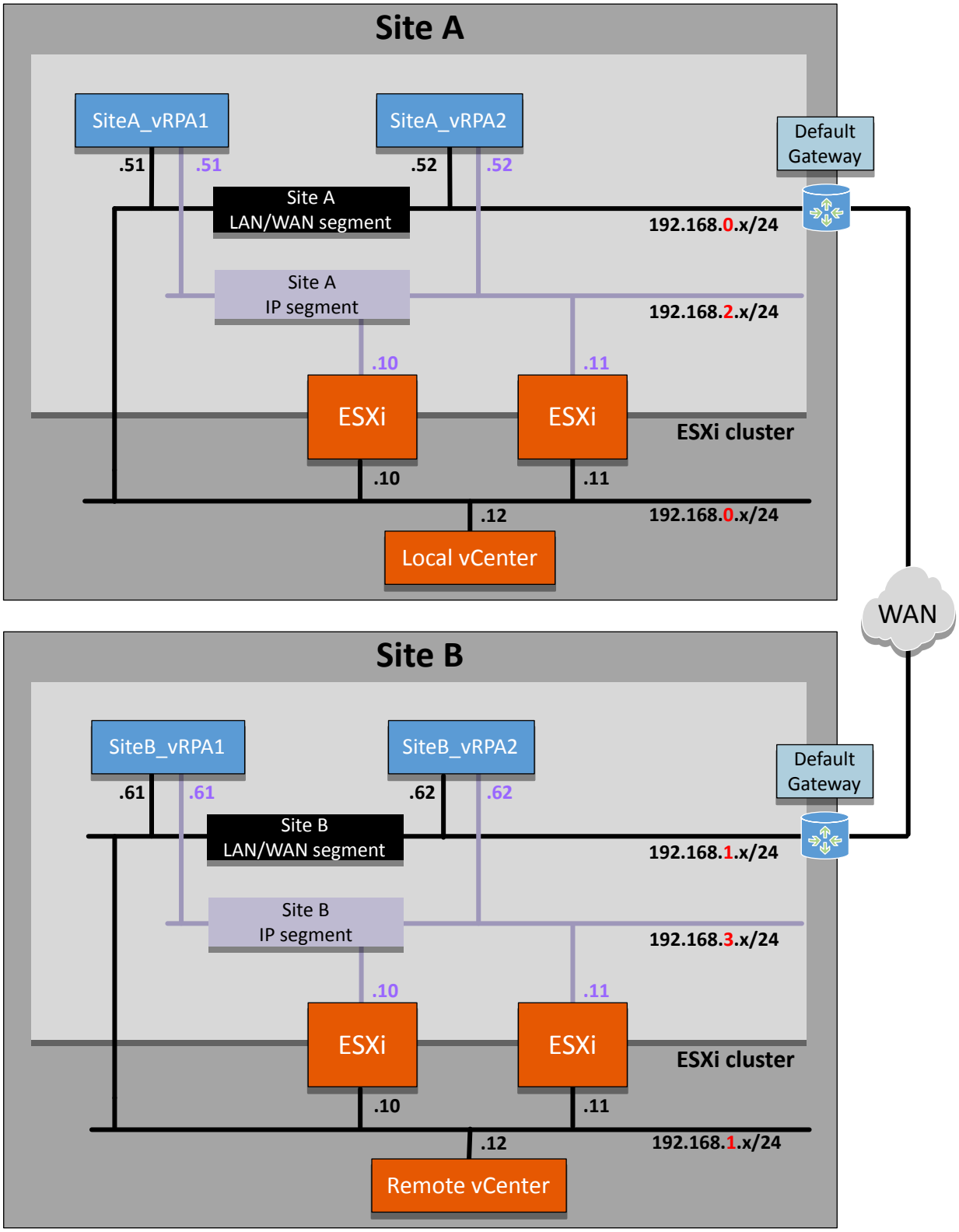
Other network topologies can be deployed. For more information, refer to the RecoverPoint for Virtual Machines Installation and Deployment Guide.

The goal of this guide is to establish replication by deploying a single consistency group between Site A and Site B.

The steps include creating two vRPAs in a vRPA cluster at each site and connecting these two vRPA clusters to enable replication between the sites.

The examples in this guide are based on the reference architecture in Figure 1 on page 5.

Figure 1 Reference architecture for the basic configuration



Assumptions

This procedure provides a limited installation of RecoverPoint for proof of concept. The procedure assumes various environmental characteristics.

- You have installed the latest version of Google Chrome, Firefox, or Internet Explorer browser on the workstation that you use for this installation.
- Screenshots in this document are taken from a vSphere 6 Update 2 environment. Screens may appear slightly different when using a different version.
- RecoverPoint for VMs Release 5.2 supports the vSphere versions that are listed in the Simple Support Matrix, which is available at https://elabnavigator.emc.com and contains the most up-to-date information.
- This guide assumes IP communication between the ESXi hosts and the vRPAs. The IP communication mode requires vSphere 6.0 and later.
- vSphere Web Client is available on both vCenters.

Before you begin

Before you begin this installation make sure that you prepare for the installation.

- Download the vRPA OVA file for RecoverPoint for VMs from https://support.emc.com/downloads.
  1. Perform a search in the **Type a Product Name** text box for **`RecoverPoint for Virtual Machines`**.
  2. Locate and download **RecoverPoint for Virtual Machines 5.2 Installation Kit**. Ensure that you select version 5.2.
     Example of downloaded file: `RecoverPoint_for_Virtual_Machines_5.2_Installation_Kit_md5_checksum.zip`
  3. Extract the `.zip` file that contains the OVA file that is needed for the installation.
- Select an IP segment from which IPs are allocated for ESXi hosts and vRPAs (recommended on a dedicated VLAN).
- Select a network segment— any standard VLAN with three unassigned IPs for each cluster. This network segment is used for management of vRPAs, vRPA cluster management, and data transfer between the clusters.
- For each vRPA, open firewall ports for inbound and outbound TCP/IP communication. Ports 5020, 5040, 5042, 5044, and 5050 are required for communication between the vRPAs and the ESXi splitter. For more detailed information, refer to the *RecoverPoint for Virtual Machines Security Configuration Guide*.
- If you have a network firewall installed in the environment, open firewall ports 443 and 7225 between vCenter and vRPA.
- Ensure that you have at least one VM for protection in Site A.
- Ensure that you have datastores with free space, as follows:
  - Site A

  - 100 GB for system usage (not including protected VM)
  - 3 GB per protected VM, for journaling
    These datastores must be shared between the ESXi hosts within the ESXi cluster that hosts the vRPAs.
- Site B
  - 100 GB for system usage
  - Size of Site A protected VMs
  - 10 GB per protected VM, for journaling
    These datastores must be shared between the ESXi hosts within the ESXi cluster that hosts the vRPAs.

- Plan for 8 GB memory and 8000 MHz CPU in each ESXi cluster for each site. This requirement assumes using a Bronze vRPA (2 vCPU and 4GB). For larger deployments, use the *RecoverPoint for Virtual Machines Installation and Deployment Guide*.
- Ensure that vSphere Web Client with Client Integration Plug-in is installed (see high-level steps in Appendix A: Install vSphere Client Integration Plug-in).
- Ensure that all server clocks, including ESXi hosts and vCenters, are synchronized using NTP. Time differences may affect VMware vCenter certificate authentication resulting in possible installation failure.
- A persistent scratch location on each ESXi host is required for storing splitter configuration information. The scratch location (/scratch/log) requires at least 50 MB of free storage space on a permanently available persistent storage device.
- Related RecoverPoint for VMs guides are available at https://support.emc.com/:
  - *RecoverPoint for Virtual Machines Scale and Performance Guide*
  - *RecoverPoint for Virtual Machines Security Configuration Guide*
  - *RecoverPoint for Virtual Machines Installation and Deployment Guide*
  - *RecoverPoint for Virtual Machines Administrator's Guide*

Overview of the basic configuration installation flow

The basic installation flow that is described in this guide includes these high-level steps:

Table 2 Installation flow

Order of installation flow	Section of this guide
Gather the necessary data.	Data preparation
Deploy the OVA for Site A vRPA 1, and repeat for Site A vRPA 2.	Deploy vRPA OVA on page 9
Configure the vRPA cluster for Site A and verify successful deployment.	• Configure vRPA cluster on page 13 • Verify deployment success on page 18
Deploy the OVA and configure the vRPA cluster for the remote site, Site B.	Deploy vRPA OVA on page 9 • Configure vRPA cluster on page 13 • Verify deployment success on page 18

Table 2 Installation flow (continued)

Order of installation flow	Section of this guide
Connect the vRPA clusters between Site A and Site B.	Connect Site A and Site B vRPA clusters on page 19
Establish and verify replication between production copy at Site A and remote copy at Site B.	• Protect a virtual machine on page 21 • Verify replication status on page 25
Register the RecoverPoint for VMs system	Final RecoverPoint for VMs installation steps on page 28

Data preparation

Before beginning this installation, use these forms to collect data that is required for the installation.

Table 3 Common to all vRPAs

Property	Site A	Site B	Notes
vCenter IP address			
Cluster name			
Datastore name			System usage - use of several datastores is optional.
Time zone			
Local domain (optional)			
Primary DNS server IP (optional)			
Secondary DNS Server IP (Optional)			
NTP server (recommended)			
vRPA cluster management IP			
vCenter credentials			
WAN + LAN/subnet mask			
IP subnet mask			
VMkernel IP pool range			

Table 4 For each vRPA

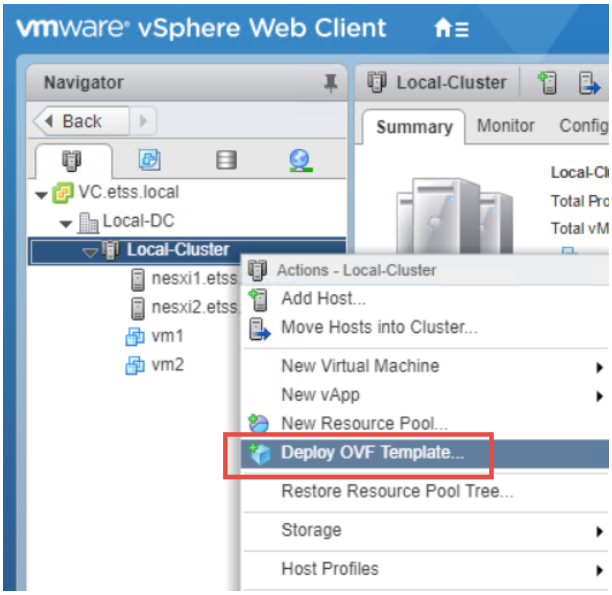
Property	SiteA_vRPA1	SiteA_vRPA2	SiteB_vRPA1	SiteB_vRPA2	Notes
WAN + LAN IP					
Data IP					

Deploy vRPA OVA

Deploy the OVA on two virtual Machines at Site A, then power on the vRPAs.

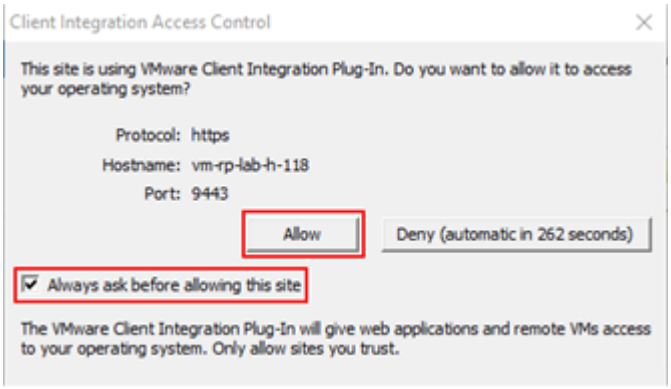
Procedure

1. Connect to the vSphere Web Client.
2. In the Navigator, click **Hosts and Clusters**.
3. Select the ESXi cluster or specific ESXi host on which to deploy the vRPA VM.
4. To deploy the OVA, right-click the cluster or host, and select **Deploy OVF template**.



The vRPA reserves the virtual machine resources to ensure that the targeted environment has enough resources.

5. After selecting **Deploy OVF template**, you might receive the following pop-up. Clear the **Always ask before allowing this site** checkbox, and then click **Allow**.

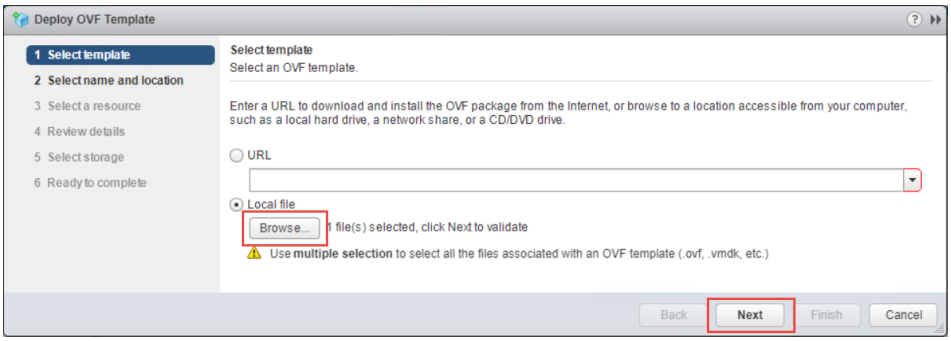


6. In the **Select template** step of the Deploy OVF Template wizard:

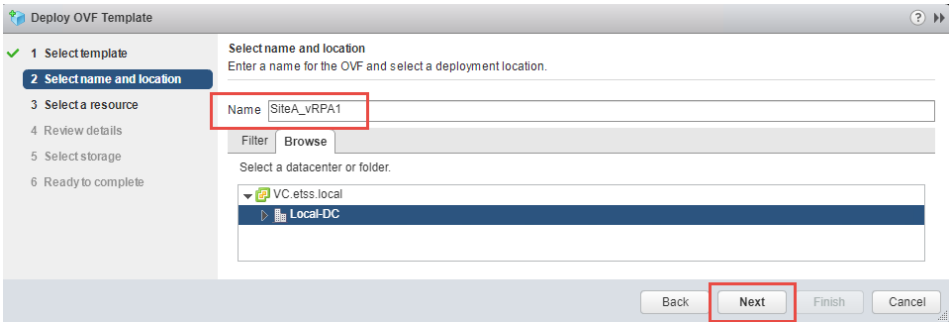
   a. Click **Browse**.

   b. Locate the OVA file, and then click **OK**.

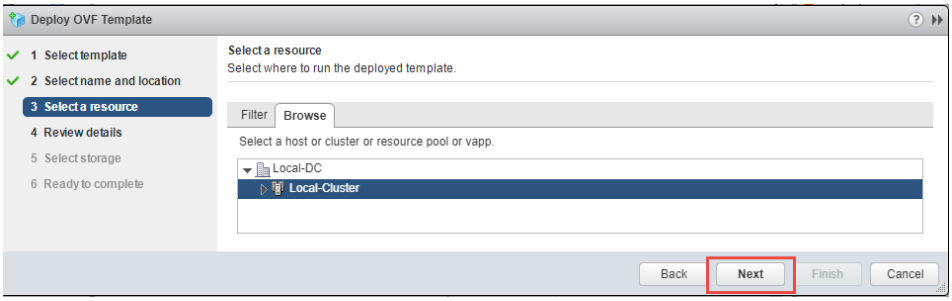
   c. Click **Next**.



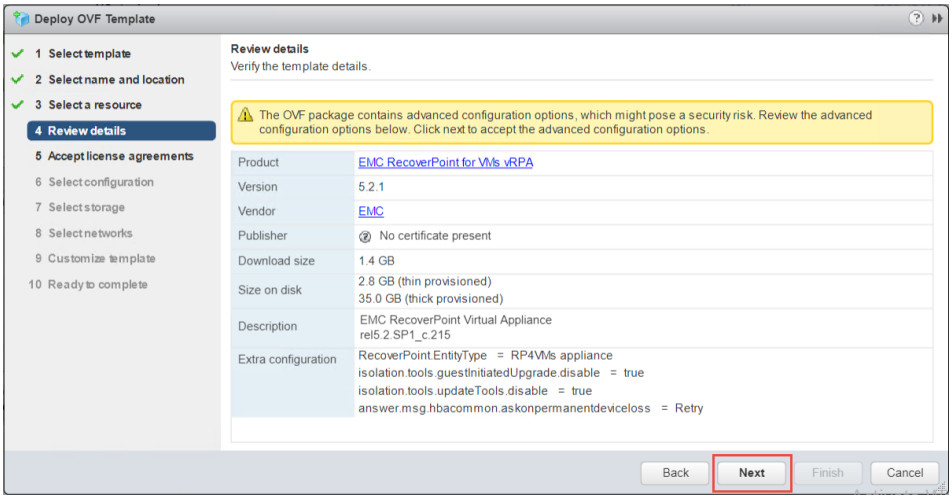
7. In the **Select name and location** step, select a VM folder in which to locate the vRPA, and type a meaningful name (to replace the filename). For example:



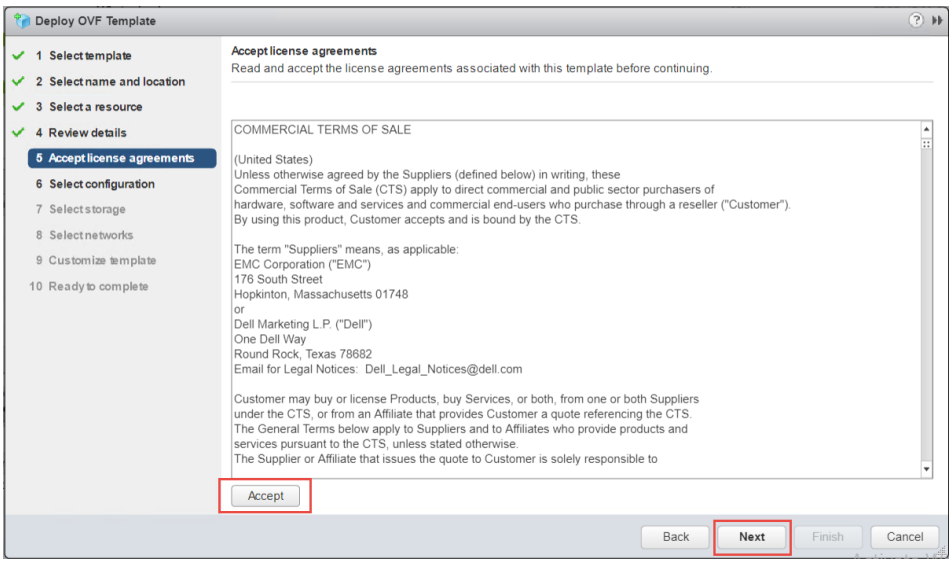
8. In the **Select a resource** step, select where to run the template.



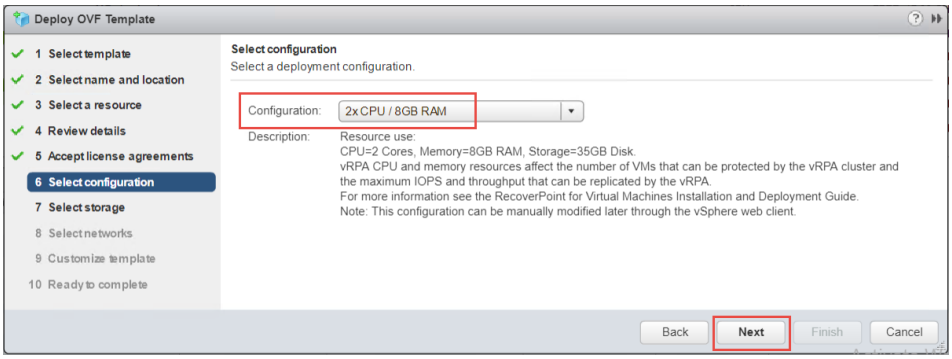
9. In the **Review details** step, click **Next**.



10. Scroll to the bottom of the **Accept License Agreements** window. If you accept the terms, click **Accept**, and click **Next**.

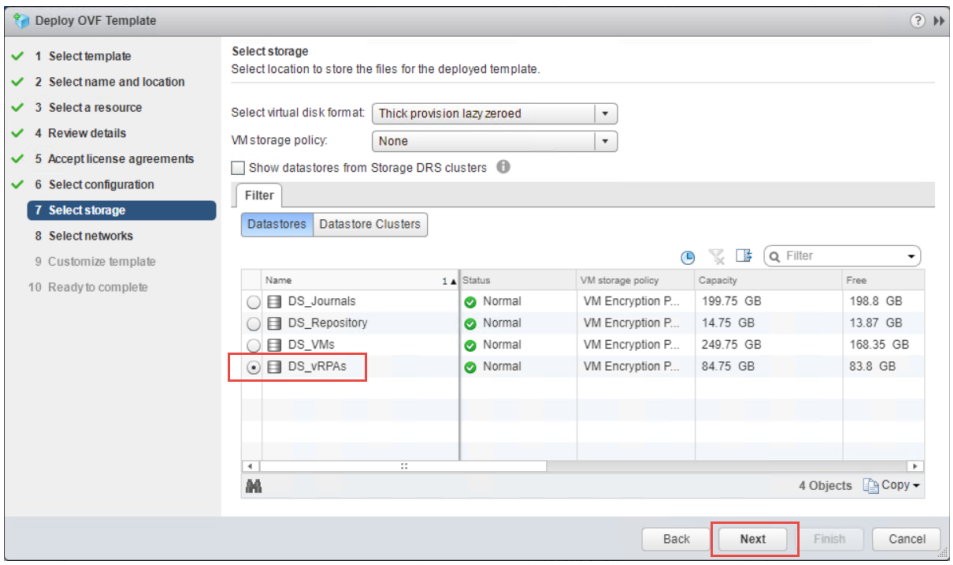


11. Select the desired deployment configuration. The default configuration is 2x CPU/8 GB RAM, but for this installation, the smaller configuration (as shown) is adequate. Click **Next**.

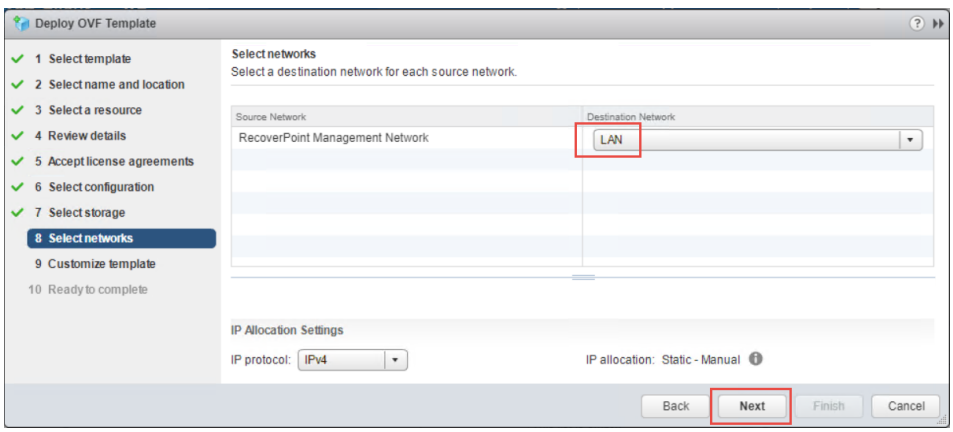


12. In the Select Storage step, select a datastore (see "Data Preparation") on which to deploy the vRPA.

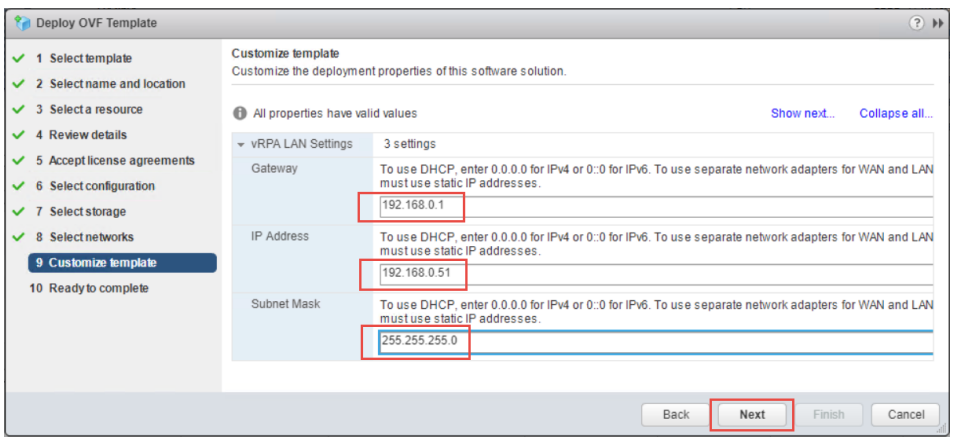
If you are using storage policies, select a policy that is based on the requirements. These requirements might include redundancy, speed, and back-up, among others.
Click **Next**



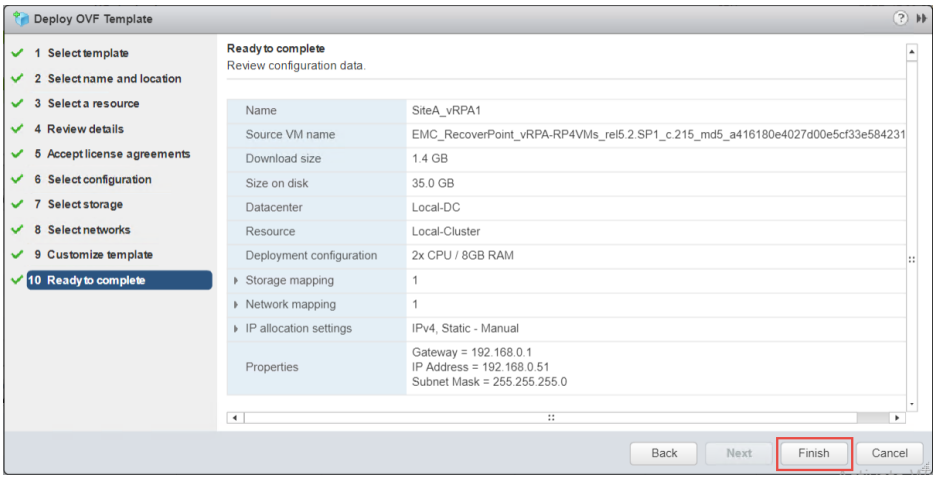
13. Select the port group for the vRPA management network, also known as the LAN network. This network is used also for the WAN network (see reference architecture). Click **Next**.



14. Type the **IP address**, **Subnet Mask**, and **Gateway**. Click **Next**.



15. Review the summary, and click **Finish**.



16. Repeat steps 4-15 for SiteA_vRPA2.
17. When finished, ensure that both vRPAs are powered on. If not, power them on.

Results

You have finished deploying the vRPAs and are ready to configure the vRPA clusters.

Configure vRPA cluster

Use the RecoverPoint for VMs Deployer to configure both vRPAs of the cluster.

Procedure

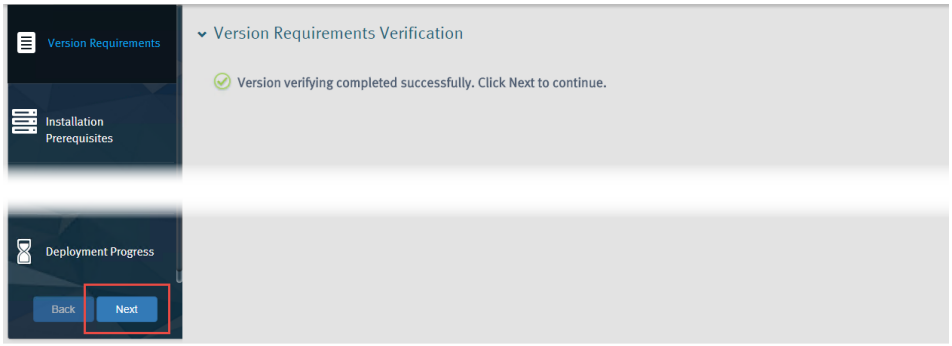
1. Connect to the RecoverPoint for VMs Deployer by opening a web browser and entering the address of the first vRPA:

```
https://first_vRPA_IP
```

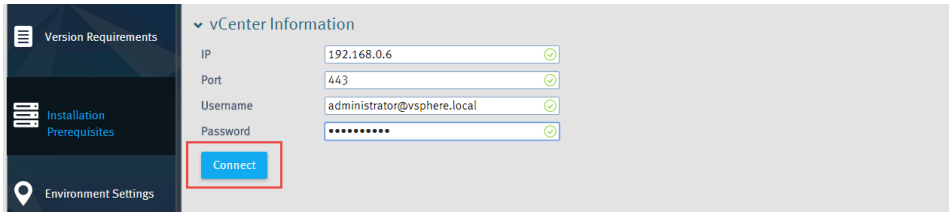
2. At the bottom of the page, click **Install a vRPA cluster**.

The Deployer tries to connect automatically to the repository for the Version Requirements file.

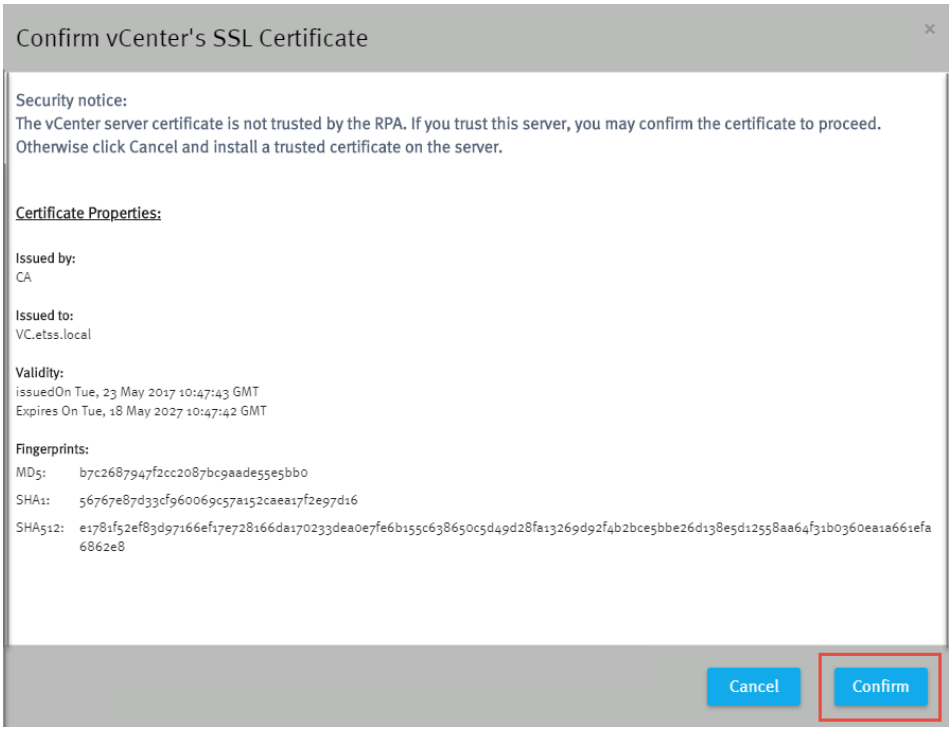
3. In the Version Requirements Verification window, click **Next**.



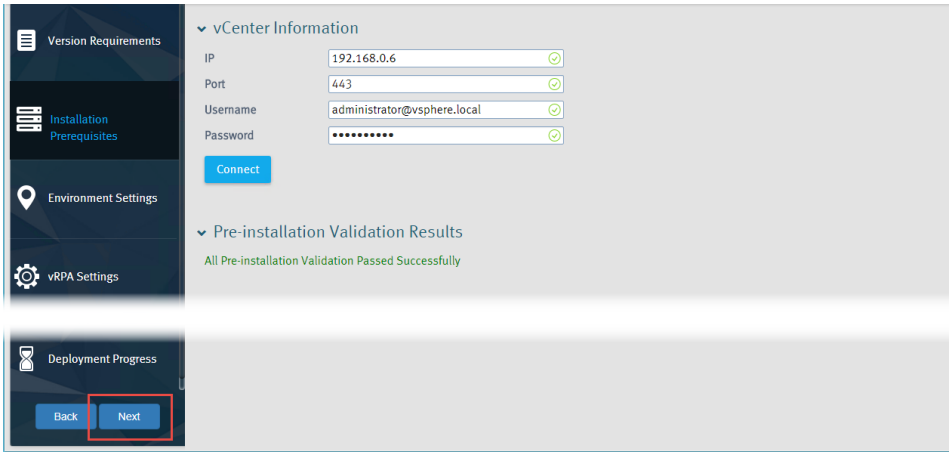
4. Type user credentials with administrator privilegies, and connect to the vCenter by clicking **Connect**.



5. A pop-up may prompt you to confirm the SSL certificate. Accept the certificate by clicking **Confirm**.



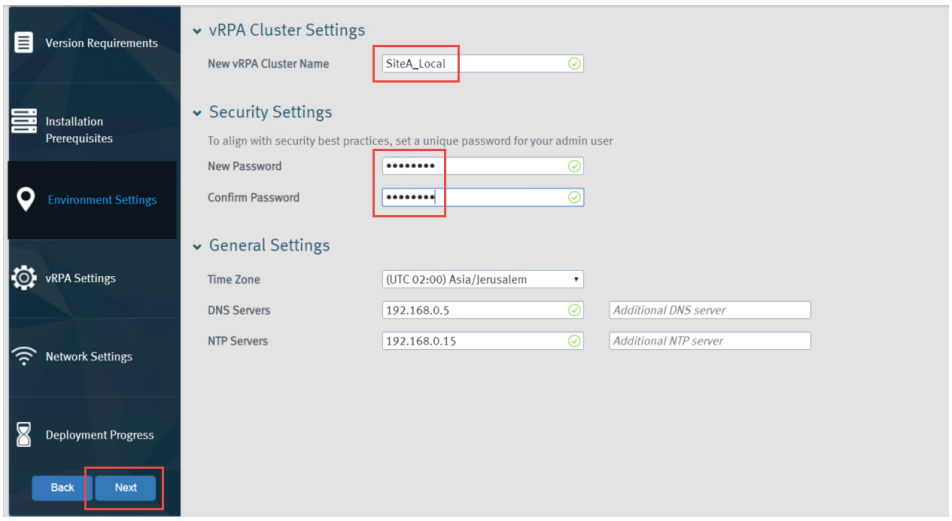
6. Verify the **Pre-installation Validation Results**, and ensure that all results are positive (as shown). Click **Next**.



7. Configure the **Environment Settings** according to the data from "Data preparation."

   a. Type a name for the new vRPA cluster. For example: Site A_Local.

   b. Type and confirm a password to replace the default admin user password.

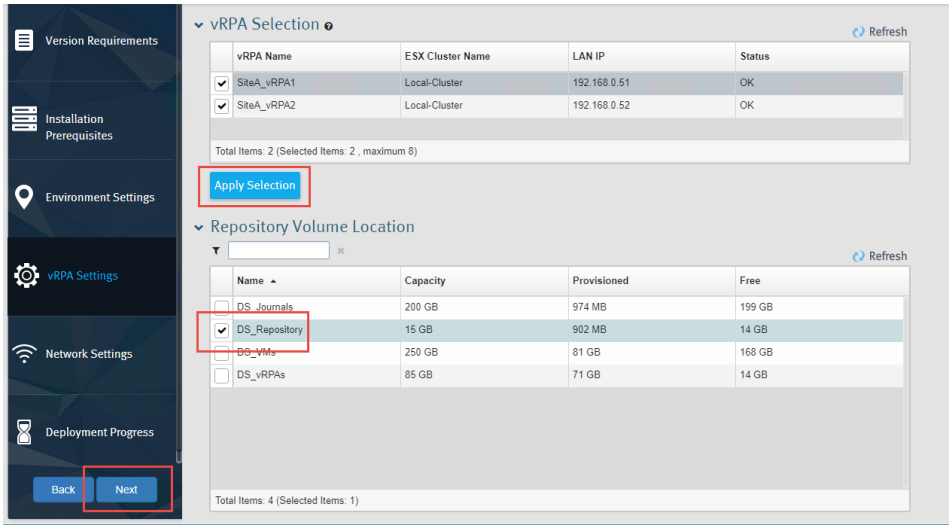


8. Configure **vRPA Settings** according to the data from "Data preparation."

   a. Select both vRPAs by clicking the checkmark at the left side of the vRPA names.

   b. Click **Apply Selection**.

   c. Select a datastore for the shared repository data between the vRPAs. Click **Next**.



This action creates a VMDK file under a folder that is named **RPvStorage**, which is used for shared persistent storage by the vRPAs.

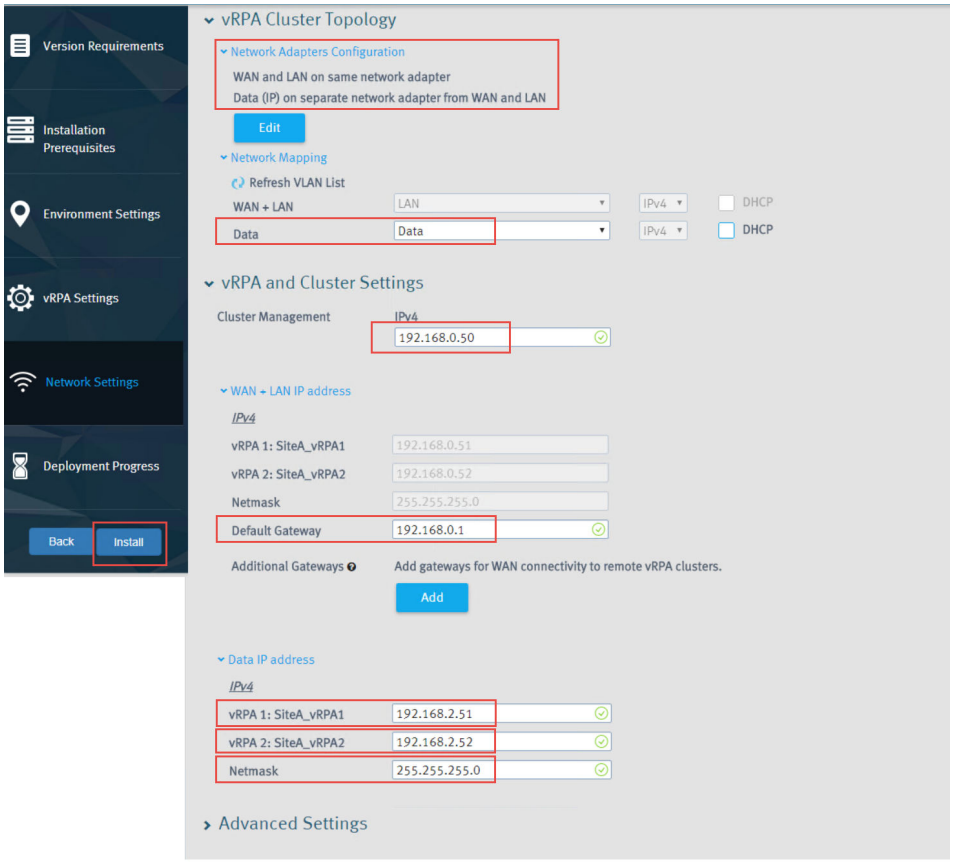
9. Configure the **vRPA Cluster Topology** and **vRPA and Cluster Settings** sections according to the data from "Data preparation."

   a. Use the default network adapter topology, which places WAN and LAN on the same network adapter and Data on a separate network adapter.

   b. Select the Data network (in this example, Data).

   c. In the **Data IP address** section, in the **IPv4**text boxes, type the IP address of the vRPAs.

   d. In the **Netmask** text box, type the netmask of the IP network.



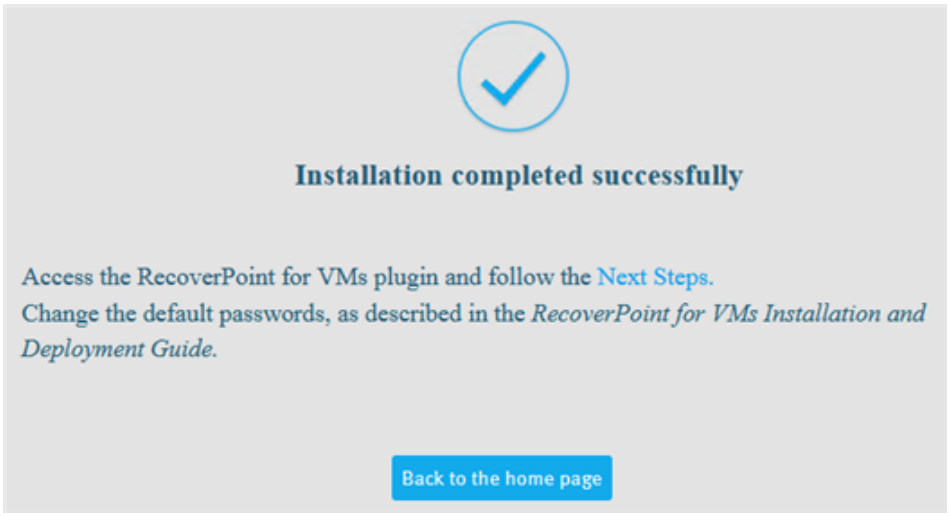
Note

The **IPv4** text boxes in the **WAN + LAN IP address** section are disabled because the IP address is automatically retrieved from vRPA properties.

e. When finished typing the data, click **Install**.

10. Observe the installation progress as the settings are applied. The installation may take a while to complete.

11. When the vRPA cluster configuration is complete, in the **Deployment Progress** window, click **Finish**.



Results

You have finished configuring the vRPA cluster and are ready to verify the deployment success.

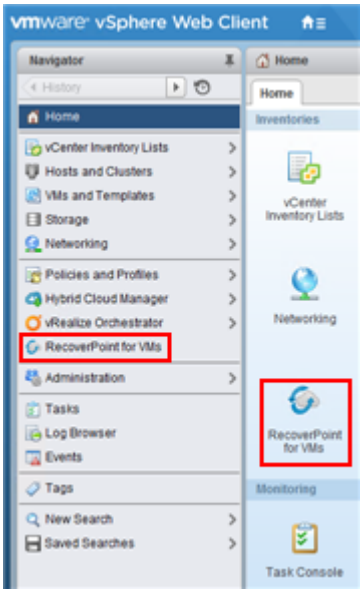
Verify deployment success

After configuring the vRPAs, ensure that the deployment was successful by finding the RecoverPoint for VMs plug-in in the vSphere Web Client.

Procedure

1. If you are already logged in to vSphere Web Client, log out and log in again to force vSphere Web Client to refresh.

2. In the vSphere Web Client Navigator, ensure that **RecoverPoint for VMs** appears.



Results

You have finished verifying deployment success and are ready to deploy vRPAs and configure the cluster at the remote site.

Deploy and configure remote site

At the remote site, repeat all steps in the Deploy vRPA OVA and Configure vRPA cluster sections for SiteB_vRPA1 and SiteB_vRPA2. Use the data that is listed in the "Data preparation" section.

Results

When you have finished deploying and configuring the remote site, connect Site A and Site B vRPA clusters.

Connect Site A and Site B vRPA clusters

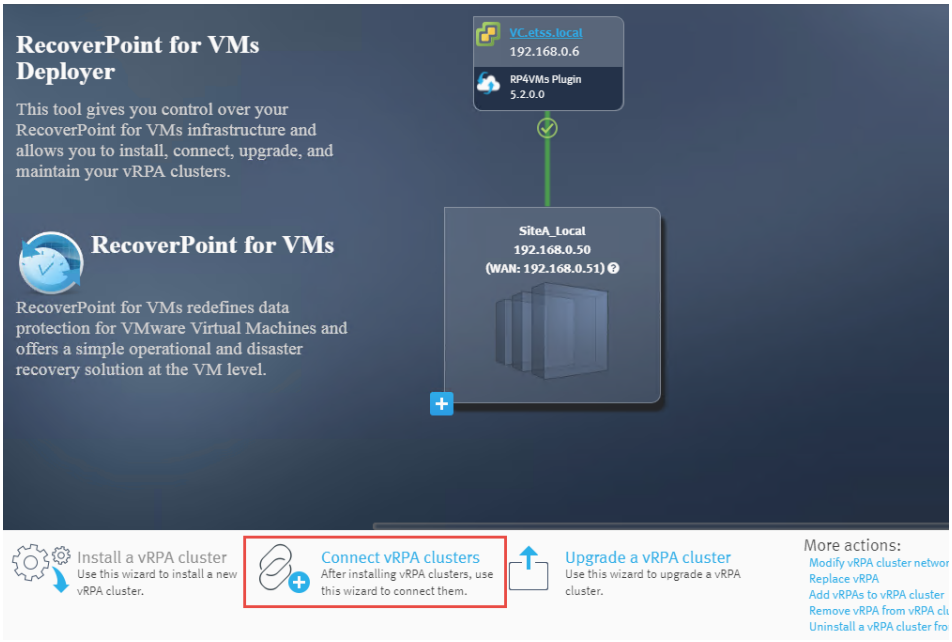
Use the RecoverPoint for VMs Deployer to connect the two sites so that RecoverPoint for VMs can replicate data from Site A to Site B.

Procedure

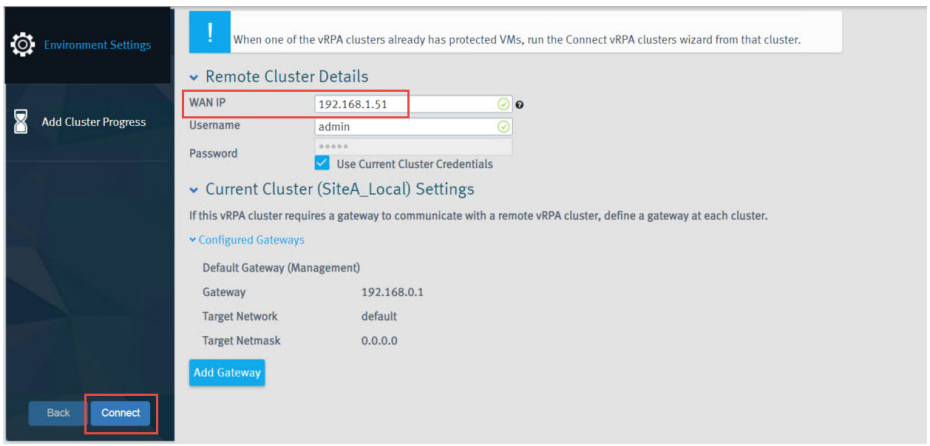
1. Connect to the RecoverPoint for VMs Deployer home page by browsing to `https://SiteA_cluster_management_IP`.

   For example, `https://192.168.0.50`

2. In the RecoverPoint for VMs Deployer home page, click **Connect vRPA clusters**.

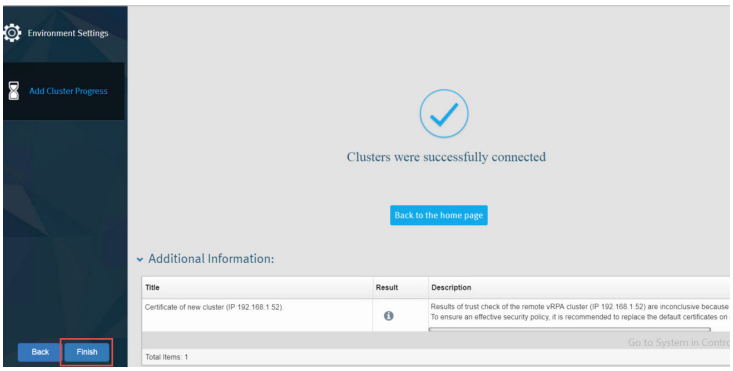


3. In the Remote Cluster Details section, type the WAN IP address of one of the vRPAs at the remote (Site B) cluster. Use the data from the "Data preparation" section.



4. Click **Connect**. Observe the progress of the connection between the vRPA clusters.

5. Ensure that the clusters connect successfully. Then click **Finish**.



Results

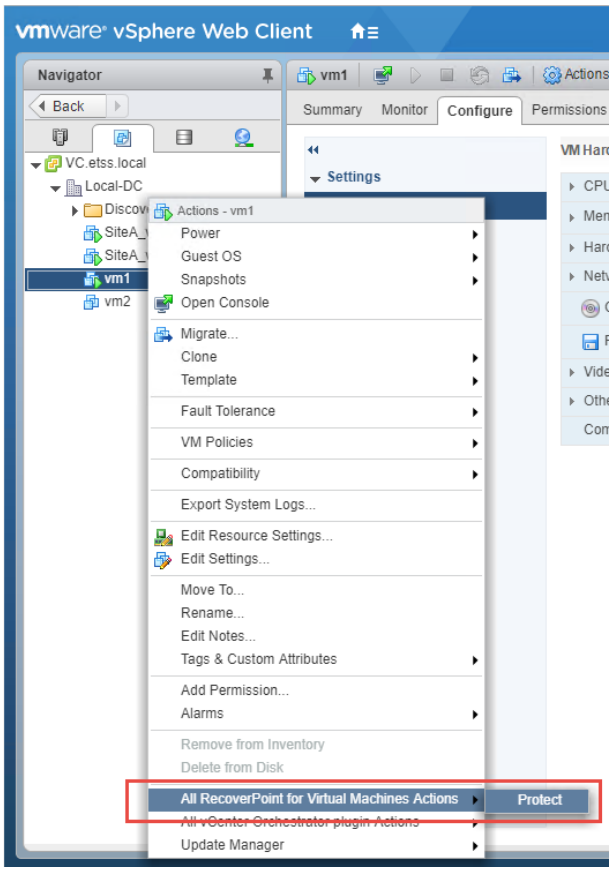
You have finished connecting Site A and Site B vRPA clusters and are ready to register the ESXi cluster for replication.

Protect a virtual machine

Production VMs are protected using the RecoverPoint for VMs **Protect VMs wizard**.

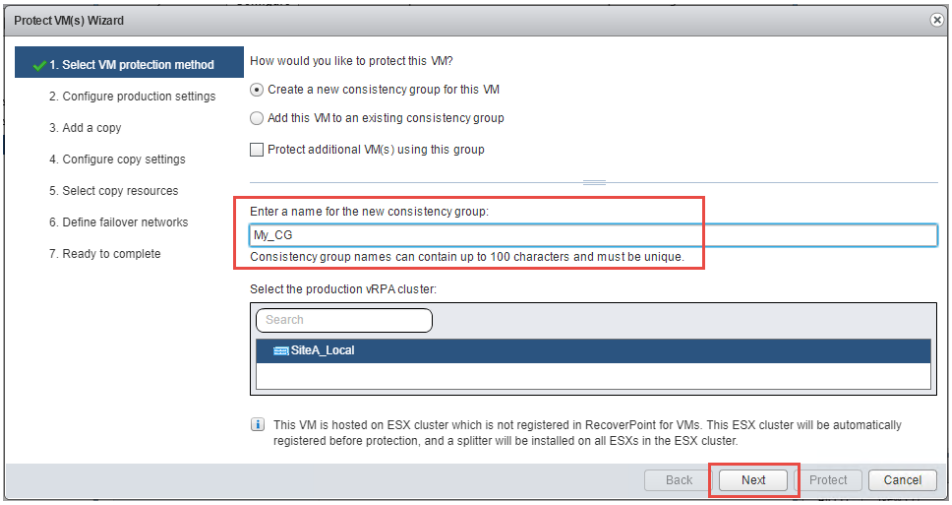
Procedure

1. Connect to the vSphere Web Client of Site A.
2. Select **VMs and Templates** view.
3. Power on the virtual machine that you want to protect.
4. Right-click on the virtual machine and select **All RecoverPoint for Virtual Machines Actions** > **Protect**.



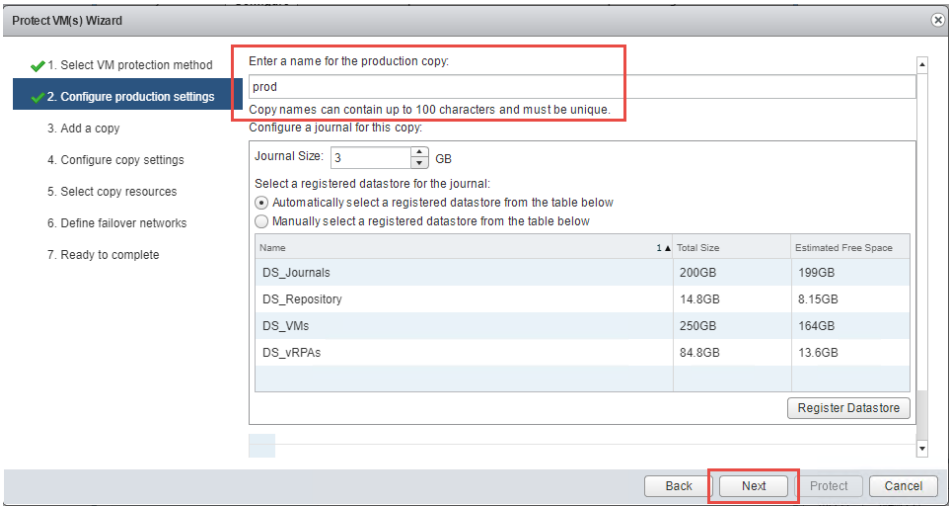
5. Enter a name for the new consistency group, and click **Next**.

   Best practice is to use the VM or application name as your consistency group name.



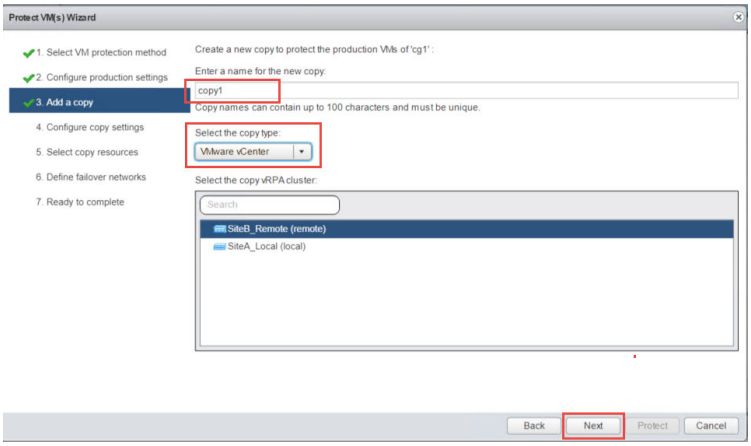
6. Enter a name for the production copy, and click **Next**.

   Best practice is to differentiate the production copy name from the replica copy name (for example, use "Production" or the production site location). By default, RecoverPoint automatically selects a datastore for the production journal. However, if you want to use a specific datastore for the production journal and you don't see it in the list of datastores, click **Register Datastore** and select the datastore before clicking **Next**.



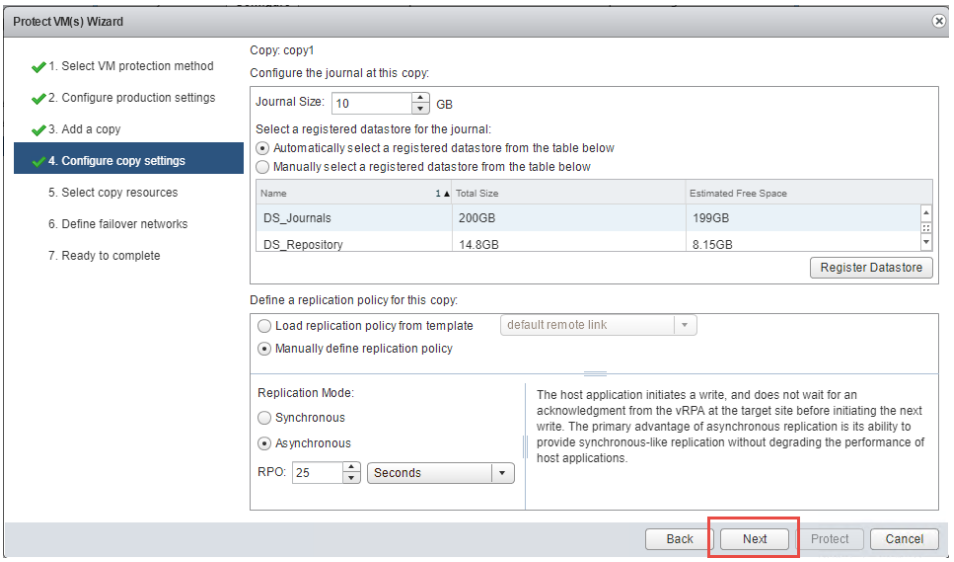
7. Enter a name for the replica copy, and ensure that the copy type is VMware vCenter. Then, click **Next**.

   Best practice is differentiate the replica copy name from the production copy name (for example, use "Remote Copy" or the copy site location).

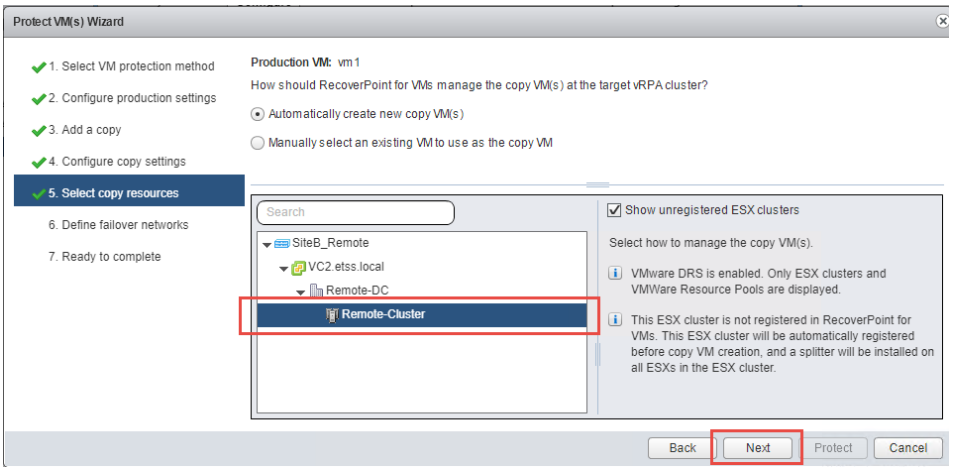


8. Accept the default copy settings, and click **Next**.

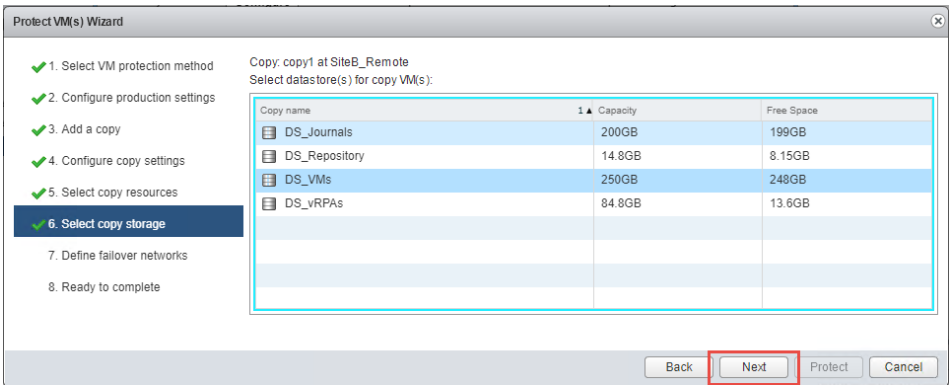
   By default, RecoverPoint automatically selects a datastore for the copy journal. However, if you want to use a specific datastore for the copy journal and you don't see it in the list of datastores, click **Register Datastore** and select the datastore before clicking **Next**.



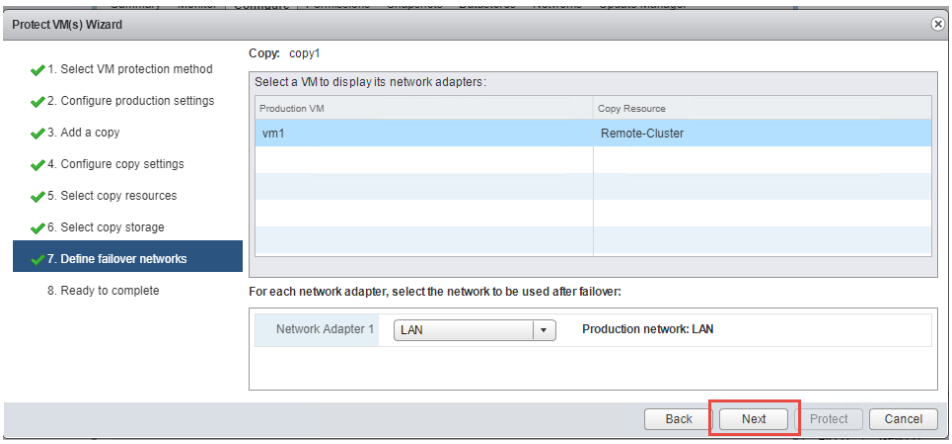
9. Select the ESX cluster, VMWare Resource Pool, or ESX that will manage the copy VM, and click **Next**.



10. Select the datastore(s) that will contain the copy data, and click **Next**.

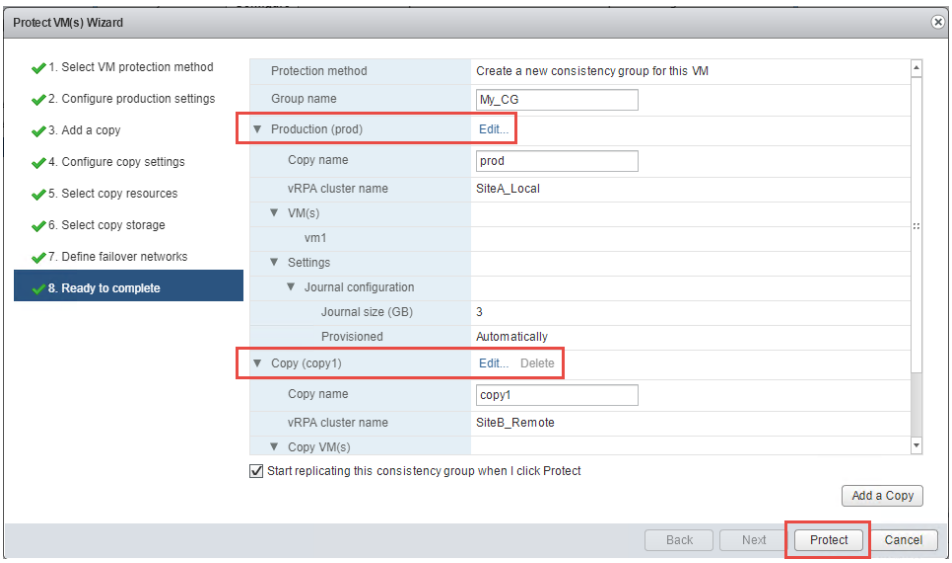


11. (Optionally) For each network adapter of all production VMs, select the network to use after failover, and click **Next**.



12. Expand the **Production** and **Copy** settings to ensure that they are correct, note if a warning is displayed regarding a potential communications problem (no action required at this time), and click **Protect**.

    If need be, click **Edit** to change a setting before clicking **Protect**.



Results

You have finished protecting the virtual machine.

Note

If an unregistered ESX cluster, or an ESX host or VMware Resource Pool of an unregistered ESX cluster were selected to manage the copy, the unregistered cluster is automatically registered with the specified vRPA cluster, a splitter is installed on all ESXs in the cluster, and replication is temporarily paused for all relevant VMs while the splitter is being installed.

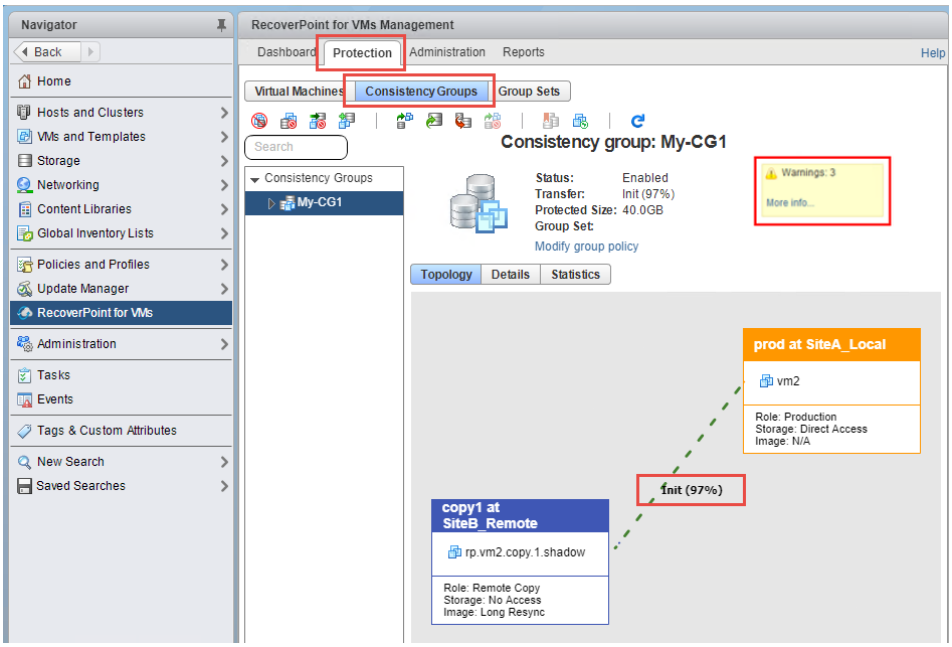
Verify replication status

From the RecoverPoint for VMs plug-in, verify the status of the replication.

Procedure

1. Select **RecoverPoint for VMs Management** > **Protection** > in the **Consistency Groups** tab, select the *CG Name*.

   You might encounter temporary warnings and alerts as shown in this screen and the alert messages that follow:



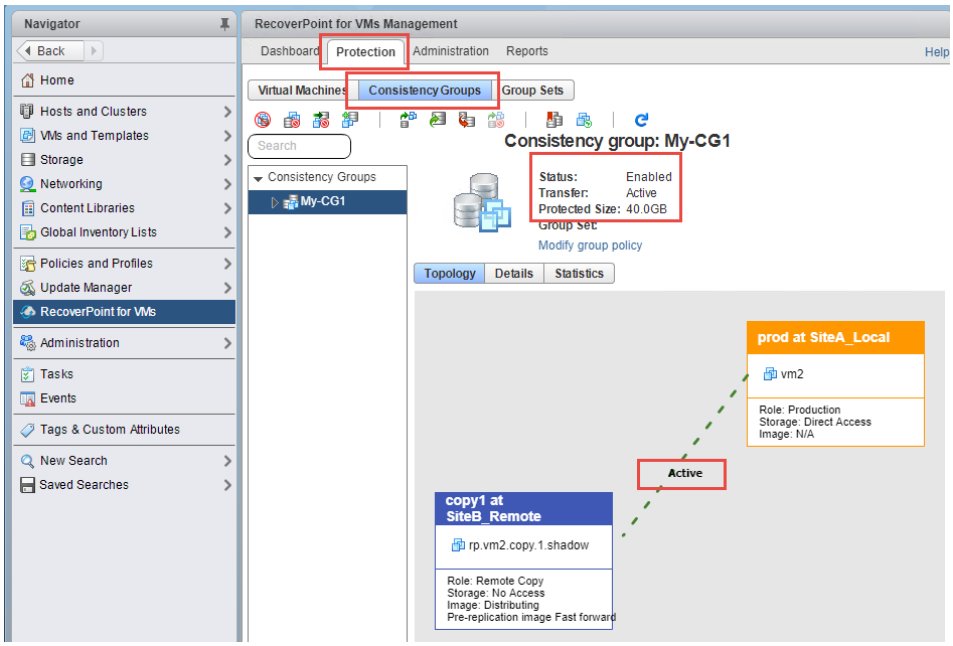
   Alerts:

```
One or more volumes are currently being provisioned for copy
[CG1, Remote_copy.
```

```
One or more volumes are currently being provisioned for copy
[CG1, prod_Copy]
```

```
Accessibility of volume [CG1, prod_Copy], CG_RSET_SiteA_VM
copy_0_0] by splitter Local-Cluster is unknown.
```

After a few minutes, the final status shows that protection is enabled and the transfer is active:



If warnings and alerts do not disappear after 10-15 minutes, contact Customer Support.

Note

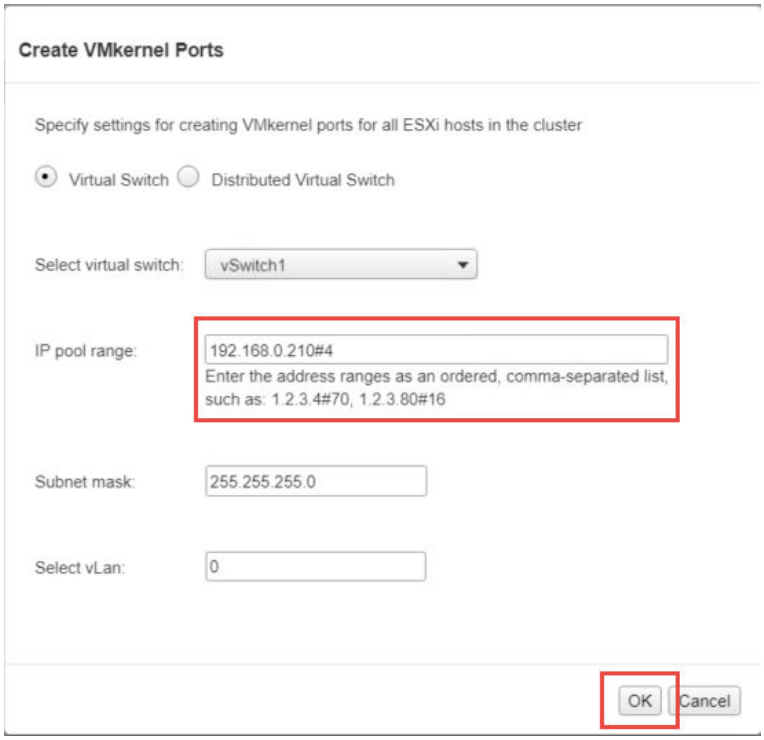
- If the environment is configured in a way that causes one or both of the vRPAs to reside on the same ESXi with the replicated virtual machine, one warning remains as a notification:

```
At least one virtual RPA is running on the same ESX as the VM it
is replicating. It is recommnded not to have the virtual RPA that
replicates a VM running on the same ESX as the replicated VM. Use
vMotion to move one of them to another ESX.
```

- The replication process might require several minutes and initialization might require up to several hours depending on the size of the virtual disks and the speed of the data transfer between the two sites.

---

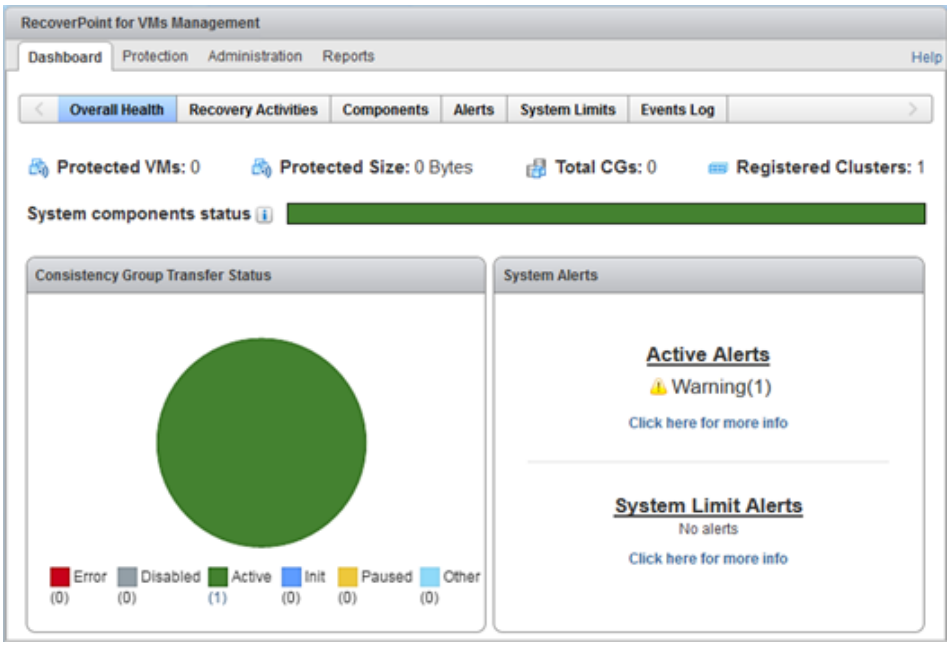
2. If previously (before clicking **Protect** in the **Protect VMs wizard**) you received a warning regarding a potential communications problem, and transfer is still not active, you may need to create VMkernel ports.
   a. At **Administation > vRPA Clusters > ESX Clusters**, click the **Settings** icon for an ESXi cluster.
   b. On the Create VMkernel Ports screen, specify the settings for creating VMkernel ports for all ESXi hosts in the cluster.



c. Click **OK**

Repeat for each ESXi cluster that is listed.

3. Monitor the health of the system from the RecoverPoint for VMs plug-in **Dashboard** tab.



Results

You have finished verifying replication status and are ready to perform the final steps.

Final RecoverPoint for VMs installation steps

Licensed users should activate their entitlements, add licenses, register their RecoverPoint for VMs system, and establish communication between their system and the System Reports database.

Steps to complete these tasks are in the "Getting started" section of the *RecoverPoint for Virtual Machines Administrator's Guide*, which is available at https://support.emc.com.

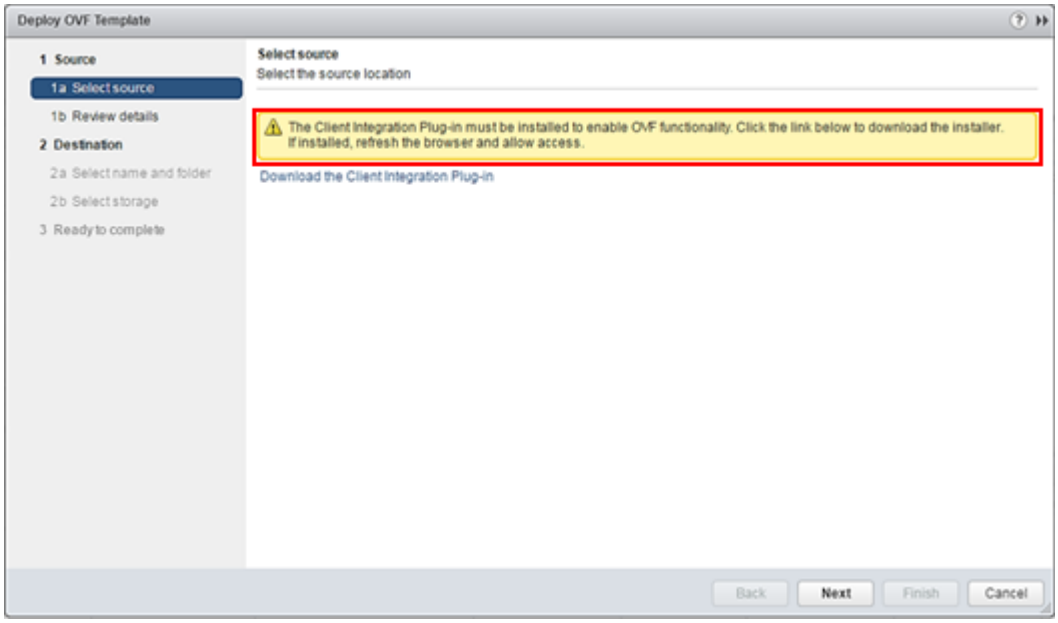
Install vSphere Client Integration Plug-in

Ensure that you have installed the Client Integration Plug-in for the vSphere web client; this plug-in is required for deploying OVF functionality.

Note

This procedure is required only when running vSphere versions earlier than 6.5.

When you try to enable OVF functionality without the plug-in, this message appears:

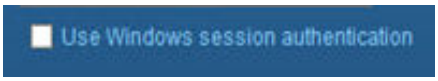


Procedure

1. If the Client Integration Plug-in is not installed, notice this option at the bottom of the vSphere web client login page (`https://vc ip or fqdn:9443`).

2. To install the Client Integration Plug-in, close all web browsers, click **Download Client Integration Plugin**, and select the default installation
3. After successful plug-in installation, ensure that the browser detects and enables the plug-in. If the plug-in is browser-enabled, you notice this option at the login screen:


Use Windows session authentication

Published January 2019