## FIGURES

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RecoverPoint for VMs Deployer Home Page displaying cluster overview</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>Installation overview</td>
<td>14</td>
</tr>
</tbody>
</table>
TABLES

1. The vRPA performance profile matrix ................................................................. 16
2. Pre-deployment validations and fixes ................................................................. 19
3. Troubleshooting tests and fixes ......................................................................... 22
4. Comparison of vSCSI splitter and IO splitter ..................................................... 23
5. RecoverPoint for VMs Upgrade and Maintenance package components .......... 26
6. IP & SAN vRPA Cluster Setup Details ............................................................... 44
7. IP & SAN vRPA Setup Details ............................................................................ 45
CHAPTER 1

New Features and Limitations

- Product description........................................................................................................ 10
- RecoverPoint for VMs Deployer overview...................................................................... 10
- RecoverPoint for VMs limitations.................................................................................. 12
Product description

RecoverPoint for Virtual Machines allows replicating virtual machines with virtual machine level granularity. This solution runs in VMware virtual environments and does not depend on any specific hardware.

RecoverPoint for VMs enables users to replicate virtual machines simply and easily and to manage virtual machine replication from within vSphere Web Client using the RecoverPoint plug-in. Users will also be able to use RecoverPoint features such as point-in-time access, failover, and testing. For more information on RecoverPoint for VMs, see the *EMC RecoverPoint for Virtual Machines 4.3 Product Guide* and the *EMC RecoverPoint for Virtual Machines 4.3 Administrator’s Guide*.

RecoverPoint for VMs 4.3.1 introduces the RecoverPoint for VMs Deployer, a new tool for installing vRPA clusters, connecting vRPA clusters, modifying vRPA cluster network settings, and for upgrades to future versions of RecoverPoint for VMs.

RecoverPoint for VMs Deployer overview

The RecoverPoint for VMs Deployer, introduced in RecoverPoint for VMs 4.3.1, gives you control over your RecoverPoint for VMs infrastructure and allows you to install, connect, upgrade, and maintain your vRPA clusters. The installation process is simplified and includes pre-deployment validations to ensure that your environment is set up appropriately for a smooth and error-free installation. You can also import and export configuration files with saved setup details in JSON format. Importing a saved configuration file when rerunning a Deployer wizard populates all of the fields in the Deployer with the saved data to make process quick and easy.

Once one vRPA cluster has been installed, the Home Page displays the RecoverPoint for VMs system cluster overview, including the vRPA cluster’s status and its connection to vCenter. Each vRPA cluster is displayed with its cluster name and management IP address. Expanding the cluster will display all of the vRPAs in the cluster with their IP address, status, and RecoverPoint for VMs version. When additional vRPA clusters are added, they are also be displayed in the Home Page.
Deployer System Requirements

The Deployer has the following environment and system requirements:

- vRPAs are first created by deploying the OVA template in vSphere and the vRPAs must be powered on to run the Deployer.
- One of the following web browsers should be installed on the computer running the Deployer: Chrome version 47 or later, Internet Explorer version 11 or later, or Firefox version 43 or later.
New Features and Limitations

- The web browser should have caching enabled.
- The vRPAs being installed, connected, upgraded, or modified by the Deployer must be running RecoverPoint for VMs 4.3.1 or later.
- Internet access is needed to download some files used in the Deployer (such as the ISO or the Configuration Procedures file), however, if the files are available locally, Internet access is not required.

RecoverPoint for VMs limitations

For the current release of RecoverPoint for VMs, the following limitations apply:

- Only RecoverPoint-for-Virtual-Machines-to-RecoverPoint-for-Virtual-Machines replication is supported.
- For scale limitations, refer to the *EMC RecoverPoint for Virtual Machines 4.3 Scale and Performance Guide*.
- Upgrading VMware tools on the vRPAs is not supported. As such, upgrades of vRPAs’ VMware tools are blocked.
- RecoverPoint for VMs 4.3.x system does not support 4.2.x vRPA clusters.
- The vSphere scratch location (on the ESX host in /scratch/log, see VMware documentation) must have at least 400 MB of free storage space on a permanently available persistent storage device.
- IO Filter splitter can be installed only with vCenter version 6.0 U2 and later with ESX servers 6.0 U2 or later.
- VMware VVol support: When using vSCSI splitter, the vRPA repositories and journals should be provisioned on non-VVol datastores.
CHAPTER 2

Installing RecoverPoint for VMs 4.3.1

- Installation overview ................................................................. 14
- The installation package ............................................................ 14
- Configuring networking .............................................................. 15
- Deploying vRPAs using the OVA file ........................................... 16
- Creating additional vRPAs ....................................................... 18
- Installing a VRPA cluster ......................................................... 18
- Connecting VRPA clusters ..................................................... 21
- Registering ESXi clusters ....................................................... 22
- About the IO Filter splitter .................................................... 23
- Modifying a VRPA cluster's network settings ......................... 24
Installation overview

Setting up your RecoverPoint for VMs environment consists of the following steps:

Pre-deployment:
1. Downloading the installation package on page 14.
2. Deploying vRPAs using the OVA file in vSphere on page 16.

Deployment using the RecoverPoint for VMs Deployer:
1. Installing a vRPA cluster on page 18.

Completing installation using the RecoverPoint for VMs plug-in:
1. Registering and licensing RecoverPoint for VMs in the RecoverPoint for VMs plug-in. For more information on these procedures, see the EMC RecoverPoint for Virtual Machines 4.3 Administrator's Guide.
2. Registering ESXi clusters in the RecoverPoint for VMs plug-in on page 22.

Post-installation:
- Modifying a vRPA cluster's network settings on page 24.

The installation package

The RecoverPoint for VMs installation package can be downloaded from http://support.emc.com. Try & Buy users can download the installation package from http://www.emc.com. The RecoverPoint for VMs installation package contains the RecoverPoint for VMs release in Open Virtualization Appliance format. This OVA file is used to deploy vRPAs.
Configuring networking

Before you begin

- The VMkernel ports must be able to communicate with the vRPA iSCSI ports.
- Best practice is to configure both iSCSI (vRPA and VMkernel) networks on the same subnet.

To allow the ESXi server to communicate with vRPAs, create a software iSCSI adapter and then two VMkernel ports per ESXi node on each ESXi server that will run the vRPAs or protected virtual machines. One VMkernel port is required; however, best practice is to set up two VMkernel ports. One software iSCSI adapter is required.

NOTICE

Installation of RecoverPoint for VMs can proceed without configuring networking; however, you will need to configure the software iSCSI adapters and VMkernel ports in order for the ESXi clusters to be successfully registered in RecoverPoint for VMs. After registering ESXi clusters in the RecoverPoint for VMs plug-in, the network settings will be validated. If the validations fail, you should configure the network settings as directed below:

Procedure

1. Set up one or two VMkernel ports. Assign IP addresses that are on a routable subnet or on the same subnet as the vRPA iSCSI interfaces. The vRPA iSCSI IP addresses will be assigned when deploying the vRPA cluster. Each VMkernel port should be configured on each iSCSI vSwitch/dvSwitch.

   - When the iSCSI VMkernel ports and the vRPA iSCSI ports are on the same broadcast domain, it is recommended to bind the VMkernel ports to the software iSCSI adapter. For example, the vRPA’s iSCSI vNICs are on subnet 192.168.1.x and the ESX VMkernel ports are also on subnet 192.168.1.x.

   - When the iSCSI VMkernel ports and the vRPA iSCSI ports are on different broadcast domains, it is recommended not to use port binding. For example, the vRPA’s iSCSI vNICs are on subnet 192.168.1.x and the ESX VMkernel ports are on subnet 172.30.90.x.

IPv6 addresses are not supported on iSCSI interfaces.

For more information on iSCSI VMkernel, refer to VMware KB2038869.

NOTICE

If iSCSI is used for storage connectivity, consult the storage vendor for the recommendations and best practices.

When using VMkernel port binding to iSCSI, the active-active and active-standby NIC teaming policy cannot be used on distributed vSwitches. For more information on NIC teaming policy, refer to VMware KB2009119.

Ensure that all ESXi HBA drivers and firmwares are up to date and supported by VMware and respective storage vendors.

2. At the vSphere Web Client, in Inventory, select Hosts and Clusters. Select an ESXi server (host), click the Manage tab > Storage > Storage Adapters and create a software iSCSI adapter. Click Add and confirm that you want to add the software iSCSI adapter.
The software iSCSI adapter appears in the list of storage adapters. The vRPA iSCSI target ports will automatically be discovered after RecoverPoint for VMs has been installed.

3. If port binding is needed, as explained above, bind the VMkernel ports to the software iSCSI adapters.

4. Verify that the Port Group Policy for every VMkernel you created is Compliant and that at least one of them is Active.

The paths will become active after deployment of RecoverPoint for VMs has been accomplished. The targets will be automatically added during installation.

Deploying vRPAs using the OVA file

Before you begin
- Ensure you are running VMware vCenter 5.1 U1 or later with at least one registered vSphere 5.1, 5.5, or 6.0.
- To install IO Filter splitters, you must be running vCenter 6.0 U2 and ESXi 6.0 U2 and later. Refer to About the IO Filter splitter on page 23.
- Ensure you have a copy of the vRPA OVA file. This is included in the installation package.
- Assign enough resources (CPU, memory, disk) for the virtual system, as listed in the vRPA performance profile matrix on page 16. When using 4CPU/4GB or 8CPU/8GB configurations to run vRPA, the best practice is to reserve all RAM for RecoverPoint for VMs.

Table 1 The vRPA performance profile matrix

<table>
<thead>
<tr>
<th>vRPA Profile Feature</th>
<th>2xCPU/4GB</th>
<th>4xCPU/4GB</th>
<th>8xCPU/8GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual CPUs</td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>RAM</td>
<td>4GB</td>
<td>4GB</td>
<td>8GB</td>
</tr>
<tr>
<td>VMDK capacity</td>
<td>44GB</td>
<td>44GB</td>
<td>44GB</td>
</tr>
</tbody>
</table>

Memory reservation:
- When using 4CPU/4GB or 8CPU/8GB configurations to run vRPA, the best practice is to reserve all RAM for RecoverPoint for VMs.

Multiple vRPAs sharing the same vSphere host:
To allow redundancy in case an ESXi server fails, vRPAs should not share the same ESXi server. When resources are so scarce (temporarily) that vRPAs must run on the same host, sufficient resources must be made available:
- CPU and memory: total resources available on a shared host must be at least the sum of resources required by each of the individual vRPAs on the server.
- Network bandwidth must be sufficient to handle the I/Os of all vRPAs.
- Ensure that the total CPU and memory resources available on the shared host is the sum of resources required by each of the individual vRPAs on the server and that the network bandwidth is sufficient to handle the I/Os of all vRPAs.

Configuring virtual networks for vRPA:
- In low-traffic or non-production deployments, all four virtual network cards may be placed on the same virtual network (on a single vSwitch).
Where high availability and performance is desired, separate LAN and WAN traffic from iSCSI traffic. For even better performance, place each network (LAN, WAN, iSCSI1, and iSCSI2) on a separate switch.

For high-availability deployments, in which clients have redundant physical switches, the best practice is to route each iSCSI card to a different physical switch. This involves creating one VMkernel port on every vSwitch and dVswitch dedicated for iSCSI.

vMotion and storage vMotion:
- Any online or offline migration of vRPAs is supported without affecting high availability.
- Suspend and resume operations on vRPAs are strictly unsupported and can lead to unexpected results (especially if the vRPA is the cluster leader).

iSCSI bandwidth:
Since the vRPA relies on virtual networks, the bandwidth that you expose to the vRPA iSCSI vSwitches will determine the performance that the vRPA can achieve. You can configure vSphere hosts with quad port NICs and present them to the vRPAs as single or dual iSCSI networks; or implement VLAN tagging to logically divide the network traffic among multiple vNICs.

It is recommended that protected VMs run on a different ESXi server than the vRPAs replicating these VMs.

The first vRPA must be created using the OVA package file. The OVA package can be deployed only from the VMware vCenter management, not from the ESX management. There must be a minimum of two vRPAs per cluster; this procedure should be repeated for each vRPA being deployed. Alternatively, the first vRPA can be cloned on page 18.

Procedure
1. In the vSphere Web Client, right-click on an ESX host and select Deploy OVF Template....
   The Deploy OVF Template wizard appears.
2. In the Source screen, specify the vRPA OVA package location.
3. In the OVF template details screen, review the general properties of this OVA package. To accept, click Next.
4. In the EMC End-User License Agreement screen, if you accept the terms of the EMC End-User License Agreement, click Accept and Next.
5. In the Name and Location screen, enter the name you wish to assign to this vRPA. If you enter the name of an existing vRPA, you will not be permitted to continue.
6. In the Deployment Configuration screen, select the desired configuration profile (refer to Table 1 on page 16).
7. In the Storage screen, select the vRPA storage (datastore) that will be used to host the vRPA virtual machine files. The best practice is to select a high-performance datastore.
8. In the Disk Format screen, select Thin Provision or Thick Provision disk format.
9. In the Network Mapping screen, map the four required vRPA Ethernet ports (Source Networks) to the available vSphere virtual networks (Destination Networks). Do not select the internal VMware iSCSI network (iSCSI Network option).
10. In the IP address allocation screen, the Fixed IP option is selected. Enter required IP Properties.
11. The Ready to Complete screen summarizes all your selections. Click Finish to create this instance of the vRPA.
The Deploying vRPA screen appears, showing the progress.

Results
When the vRPA is created, the vRPA Summary tab shows the vRPA package contents as specified. The new vRPA is ready to be powered on. The selected IP policy will be implemented automatically when the vRPA is powered up.

Creating additional vRPAs

Before you begin
- The best practice is to create each vRPA instance from the OVA, as described in Creating vRPAs with the OVA package file on page 16.
- It is possible to create multiple vRPAs by cloning or copying an existing vRPA. Cloning has no effect on the source vRPA.
- Cloning an existing vRPA can be performed by various methods including: vCenter, ESX CLI, vSphere API and more. If needed, edit the settings of the new vRPA, change its network assignments, and input the new IP addresses. IPv6 addresses are not supported on iSCSI interfaces.

To complete installation of the vRPA cluster:
- If the vRPA cluster has not yet been installed and all vRPAs for that cluster are already created or cloned, use the RecoverPoint for VMs Deployer to install the vRPA cluster on page 18.
- If you wish to add the cloned vRPA to an existing vRPA cluster, use the RecoverPoint Deployment Manager and run the Add new RPAs wizard.

Installing a vRPA cluster

Before you begin
- Ensure that all vRPAs to be included in this cluster have already been created using the OVA or by cloning an existing vRPA.
- The boxmgmt user for each vRPA to be included in the cluster must share the same password.
- Ensure you have the credentials to the vCenter.
- Note that the Deployer tool is only supported on HTTPS.

Use the RecoverPoint for VMs Deployer to install each vRPA cluster. During installation, the RecoverPoint for VMs splitter is installed on all ESXi in the ESXi cluster hosting the vRPA cluster. After the vRPA clusters are installed, use the Connect a vRPA Cluster wizard to connect two clusters. If you have previously exported a configuration file with setup details, you can click Import to populate the fields in the installation wizard with those details.

Procedure
1. In a web browser, enter https://<ip-address> where <ip-address> is the IP address of a vRPA in the cluster you are installing. Once the vRPA’s landing page loads in the web browser, click the RecoverPoint for VMs Deployer link.
   The RecoverPoint for VMs Deployer Home Page loads in the web browser.
2. If requested, enter the login details for RecoverPoint for VMs user boxmgmt and click Sign in.
3. Select the **Install a vRPA cluster** wizard.

4. In the **Configuration Procedures** step, provide the configuration file. After completing the Configuration Procedures, select **I have completed the Configuration Procedures**.

   The configuration file is an XML file containing up-to-date configuration information relevant to your specific installation environment and is supplied by EMC Customer Support. After evaluating the information, a list of configuration procedures are displayed. These procedures must be completed before proceeding with installation.

5. In the **Prerequisites** step, provide the vCenter information and click **Retrieve SSL certificate** to verify the vCenter’s SSL certificate.

   The **SSL Certificate** window appears.

6. In the **SSL Certificate** window, verify the vCenter’s SSL certificate and click **Ok**.

7. Click **Run Validations** to run the pre-deployment validations. Review the **Pre-deployment Validation Results**. If any of the validations result in an error, these must be fixed before proceeding with the next step in installation. If the error can be fixed by the Deployer, the *Fix* button is displayed in the *Auto-Fix* column. The following table offers detailed descriptions of each validation and suggestions for manually fixing errors that cannot be automatically fixed by the Deployer. Once the errors have been corrected, run the Install a vRPA cluster wizard again.

   **Table 2** Pre-deployment validations and fixes

<table>
<thead>
<tr>
<th>Pre-deployment validation title</th>
<th>Description</th>
<th>Result and Fix (manual or automatic)</th>
</tr>
</thead>
</table>
| No old RecoverPoint splitters installed on any ESXi in the ESXi      | All ESXi hosts are ready for a new splitter installation. This test validates that no splitters exist on any of the ESXi nodes or, if there is an installed splitter, that its version matches (such as when deploying a second vRPA cluster on the same ESXi cluster). | Pass: No splitters are installed or the installed splitters match the new version.  
Warning: A 4.3 splitter is installed.  
Error: A 4.2 splitter is installed.  
Fix: If an ESXi node is listed, manually remove the splitter on page 48 from that node and retry. |
| cluster where the vRPA cluster is being deployed.                   |                                                                             |                                                                                                                                 |
| All ESXi in the ESXi cluster are communicating with the vCenter.    | All hosts on the ESXi cluster are connected to the vCenter.                 | Pass: All ESXi hosts are connected to the vCenter.  
Warning: There is at least one ESXi host that is disconnected from the vCenter.  
Fix: Manually ensure that all hosts in the ESXi cluster are connected to the vCenter. |
| vCenter inventory does not exceed VM limit.                         | For best results, there should be less than 10K VMs in the vCenter inventory, although a maximum of 15K VMs is permitted. | Pass: There are less than 10K VMs in the vCenter.  
Warning: There are more than 10K VMs in the vCenter.  
Error: There are more than 15K VMs in the vCenter.  
Fix: Manually ensure that the vCenter inventory is less than 15K VMs, or 10K VMs for optimal results. |
| All ESXi clusters have candidate datastores for repositories.       | All ESXi clusters have at least one shared datastore that can be used as a repository. | Pass: There is at least one shared datastore with at least 6 GB of available space.  
Error: There is no shared datastore with at least 6 GB available space.  
Fix: Manually add a shared datastore with sufficient space or clear space from an existing shared datastore. |
### Table 2 Pre-deployment validations and fixes (continued)

<table>
<thead>
<tr>
<th>Pre-deployment validation title</th>
<th>Description</th>
<th>Result and Fix (manual or automatic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported ESXi versions in the ESXi cluster.</td>
<td>All ESXi hosts meet the minimum supported version for RecoverPoint for VMs.</td>
<td>Pass: All ESXis in the ESXi cluster meet the minimum required version. Error: There exists an ESXi whose version is less than 5.1 Update 1. Fix: Upgrade the ESXi servers.</td>
</tr>
<tr>
<td>Persistent scratch locations are available on all ESXis in the ESXi cluster.</td>
<td>A persistent scratch location was found for each ESXi in the cluster.</td>
<td>Pass: A persistent scratch location is configured on all ESXi nodes. Error: There is a non-persistent scratch location configured. Fix: Adjust the vSphere deployment to configure a persistent scratch location.</td>
</tr>
<tr>
<td>No pre-existing vSphere client RecoverPoint plugin installed.</td>
<td>No RecoverPoint for VMs Web Client Plugin is registered on the vCenter.</td>
<td>Pass: There is no Plugin installed. Warning: There is a previous version of the Plugin installed. If there is a 4.2 vRPA cluster running in this vCenter, the <strong>Fix</strong> button can be used to upgrade the Plugin to the current version. If there are earlier versions of the current release installed, the Plugin will not be upgraded during installation. Fix: After installation is finished, manually upgrade an earlier version of this Plugin on page 29 if it is for release 4.3.0.x.</td>
</tr>
<tr>
<td>Supported vCenter version.</td>
<td>The vCenter meets the minimum supported version for RecoverPoint for VMs.</td>
<td>Pass: The vCenter version is at least 5.1 Update 1. Error: The vCenter version is less than 5.1 Update 1. Fix: Manually upgrade the vCenter.</td>
</tr>
</tbody>
</table>

8. In the **Connectivity Settings** step, define the vRPA cluster IP configurations and vRPA IP addresses. IPv6 addresses are not supported on iSCSI interfaces. In the **Advanced** section, if can choose to define custom MTU values for the vRPA cluster. To add additional gateways, click **Add Route**.

9. In the **Environment Settings** step, define the RecoverPoint for VMs cluster settings, including the name of the RecoverPoint for VMs cluster you are installing, the time zone of the cluster, the IP addresses of DNS servers and NTP servers, and the vRPA communication security level. To include more than one DNS server IP address, separate additional IP addresses with a semicolon.

<table>
<thead>
<tr>
<th>vRPA Communication Security Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessible</td>
<td>Communication between vRPA clusters is not authenticated or encrypted. vRPA clusters can communicate with each other only by adhering to the RecoverPoint proprietary protocol.</td>
</tr>
<tr>
<td>Authenticated</td>
<td>vRPA clusters use certificates to authenticate each other before communicating. This option minimally impacts vRPA performance.</td>
</tr>
<tr>
<td>Authenticated and encrypted</td>
<td>vRPA clusters use certificates to authenticate each other before communicating. All communication between vRPA clusters is also encrypted. This option moderately impacts vRPA performance. This security level is FIPS compliant.</td>
</tr>
</tbody>
</table>
10. In the Environment Settings step, in the vRPA Repository Configuration section, select a datastore on which to place the vRPA repository. The datastore for the virtual repository must be mapped to every ESXi capable of running vRPAs. A minimum of 6 GB of storage is required for the repository.

11. It is recommended to export a configuration file with the setup details saved in JSON format. To export the configuration file, click Export.

12. In the Deployment Progress step, the progress bar displays the deployment progress. Upon reaching 100%, click Finish to return to the Home Page.

If installation fails, review the displayed error messages to identify the cause of failure. Click Back to return to the step in the wizard where you can fix the problem and try continuing the installation wizard from that point. Alternatively, you can try running the operation that failed again by clicking Retry the operation. If installation continues to fail, contact EMC Customer Support.

13. Repeat this installation procedure for each vRPA cluster in your system.

**Connecting vRPA clusters**

After installing all vRPA clusters using the Install a vRPA cluster wizard in the RecoverPoint for VMs Deployer, use the Connect vRPA clusters wizard to connect the clusters. The vRPA cluster that the Deployer is being run on is referred to as "the existing cluster," while the cluster being connected to it is called "the cluster to connect." When adding an additional cluster to an existing system, the cluster must be clean, meaning that no configuration changes, including license installations, have been made to the new cluster.

**Procedure**

1. In the RecoverPoint for VMs Deployer Home Page, select the Connect vRPA clusters wizard.

2. In the Prerequisites step, read the prerequisites. Once you have ensured that the conditions are met, select I have fulfilled the conditions for preparing the new cluster.

3. In the Environment Settings step, in the Cluster to Connect Settings section, enter the WAN IP and login credentials of the new vRPA cluster. To determine the WAN IP of the vRPA cluster you are connecting:
   - Use an SSH connection to connect to one of the vRPAs with your RecoverPoint credentials. Run the CLI command get_rpa_settings.
   - Alternatively, use an SSH connection to connect to one of the vRPAs with the boxmgmt credentials. In boxmgmt, select Setup > View Settings > View cluster settings.

4. In the Current Cluster Settings section, if needed, gateways must be added on both clusters.

5. In the Add Cluster Progress step, the cluster to connect is connected to the current cluster and the progress is displayed on the screen.

6. Repeat this procedure to connect additional remote vRPA clusters.

7. When you are done connecting all vRPA clusters, complete the procedure for registering ESXi clusters in the RecoverPoint for VMs plug-in.
Registering ESXi clusters

Before beginning to use your RecoverPoint for VMs environment, you must register any ESXi clusters that will be hosting protected VMs or their copies. Registering ESXi clusters is performed in the RecoverPoint for VMs plug-in in the vSphere Web Client. During registration, the RecoverPoint for VMs splitter is installed on the ESXi cluster.

Procedure

1. Access the vSphere Web Client at: https://<vCenter-ip-address>:9443/vsphere-client/

   where: <vCenter-ip-address> is the IP address of the vCenter. In the vSphere Web Client home page, click RecoverPoint for VMs Management > Administration > vRPA Clusters.

2. Select the ESXi Clusters tab.

3. Click Add to register an ESXi cluster. Verify that the connectivity status is good. If there are connectivity issues with the cluster, click Troubleshoot to open the Troubleshooting on page 22 wizard.

Troubleshooting Connectivity

After registering ESXi clusters, you can troubleshoot connectivity issues using the Troubleshooting wizard.

Table 3 Troubleshooting tests and fixes

<table>
<thead>
<tr>
<th>Troubleshooting test</th>
<th>Description</th>
<th>Fix (manual or automatic)</th>
</tr>
</thead>
</table>
| No old RecoverPoint splitters installed on any ESXi in the ESXi cluster where the vRPA cluster is deployed. | All ESXi hosts are ready for a new splitter installation. This test validates that no splitters exist on any of the ESXi nodes or, if there is an installed splitter, that its version matches (such as when deploying a second vRPA cluster on the same ESXi cluster). | Pass: No splitters are installed or the installed splitters match the new version.  
Warning: A 4.3 splitter is installed.  
Error: A 4.2 splitter is installed.  
Fix: If an ESXi node is listed, manually remove the splitter on page 48 from that node and retry. |
| All ESXi in the ESXi cluster are communicating with the vCenter. | All hosts on the ESXi cluster are connected to the vCenter. | Pass: All ESXi hosts are connected to the vCenter.  
Warning: There is at least one ESXi host that is disconnected from the vCenter.  
Fix: Manually ensure that all hosts in the ESXi cluster are connected to the vCenter. |
| Supported ESXi versions in the ESXi cluster. | All ESXi hosts meet the minimum supported version for RecoverPoint for VMs. | Pass: All ESXi in the ESXi cluster meet the minimum required version.  
Error: There exists an ESXi whose version is less than 5.1 Update 1.  
Fix: Manually upgrade the ESXi. |
| Persistent scratch locations are available on all ESXi in the ESXi cluster. | A persistent scratch location was found for each ESXi in the cluster. | Pass: A persistent scratch location is configured on all ESXi nodes.  
Error: There is a non-persistent scratch location configured.  
Fix: Adjust the vSphere deployment to configure a persistent scratch location. |
### Table 3 Troubleshooting tests and fixes (continued)

<table>
<thead>
<tr>
<th>Troubleshooting test</th>
<th>Description</th>
<th>Fix (manual or automatic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>iSCSI software adapter installed on the ESXi.</td>
<td>To allow the ESXi server to communicate with vRPAs, a software iSCSI adapter is needed on each ESXi server that are running vRPAs.</td>
<td>Pass: There is an iSCSI software adapter installed on the ESXi. Error: There is no iSCSI software adapter installed on the ESXi. Fix: Automatically install an iSCSI software adapter on the ESXi.</td>
</tr>
<tr>
<td>Sufficient vNIC ports available on the ESXi.</td>
<td>Ensure that each ESXi server has a VMkernel port available for iSCSI communication.</td>
<td>Pass: All ESXs have at least two VMkernel ports. Warning: Some ESXs have only one VMkernel port. Error: Some ESXs have no VMkernel ports. Fix: Manually add VMkernel ports to the relevant ESXs. For more information, see Configuring networking on page 15.</td>
</tr>
<tr>
<td>Ping to the splitter on the ESXi cluster.</td>
<td>Verifies that there is connectivity to the ESXi’s IP address.</td>
<td>Pass: There is connectivity to the ESXi’s IP address. Error: There is no connectivity to the ESXi’s IP address. Fix: Determine why there is no connectivity to the IP address.</td>
</tr>
<tr>
<td>No conflicting iSCSI ports binding on all ESXIs in the ESXi cluster.</td>
<td>Verifies that there is a supported iSCSI port binding configuration on each ESXi server.</td>
<td>Pass: For each ESXi server, either no port binding is configured or port binding is configured with a single broadcast domain in the target list. Error: for some ESXs, port binding is configured with more than one broadcast domain in the target list. Fix: Manually fix the port binding configuration for relevant ESXs (either by removing port binding or by changing targets list). For more information, see Configuring networking on page 15.</td>
</tr>
<tr>
<td>Splitter connectivity status</td>
<td>Verifies iSCSI connectivity to each ESXi server.</td>
<td>Pass: Successfully communicated with all ESXi servers in the cluster. Error: Failed to communicate with one or more ESXi servers in the cluster. Fix: Manually check the iSCSI configuration for all ESXIs and/or vRPAs to identify the communication problem.</td>
</tr>
</tbody>
</table>

### About the IO Filter splitter

IO Filter splitter uses the vSphere APIs for I/O filtering to intercept and split writes to protected virtual machines. IO Filter requires vSphere 6.0 Upgrade 2 or later and each vRPA in the cluster must be running RecoverPoint for VMs 4.3.1.3.

### Table 4 Comparison of vSCSI splitter and IO Filter splitter

<table>
<thead>
<tr>
<th></th>
<th>vSCSI splitter</th>
<th>IO Filter splitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation</td>
<td>automated, using VIB</td>
<td>automated, using VIB</td>
</tr>
<tr>
<td>vSphere minimum version</td>
<td>5.1 U1</td>
<td>6.0 U2 (best to use U2 ep6 or later)</td>
</tr>
<tr>
<td>ESXi</td>
<td>5.1</td>
<td>6.0 U2</td>
</tr>
<tr>
<td>vRPA control path connectivity</td>
<td>iSCSI</td>
<td>iSCSI and LAN</td>
</tr>
</tbody>
</table>
Table 4 Comparison of vSCSI splitter and IO splitter (continued)

<table>
<thead>
<tr>
<th></th>
<th>vSCSI splitter</th>
<th>IO Filter splitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>iRPAs data path connectivity</td>
<td>iSCSI</td>
<td>iSCSI</td>
</tr>
<tr>
<td>Raw Device Mapping supported</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>

To request additional information and to enable the IO Filter splitter, use the following mailing list: mailto: io.filter.request.rp4vms@emc.com.

Modifying a vRPA cluster's network settings

**Before you begin**

The boxmgmt user for each vRPA in the cluster must share the same password.

Use the Network modifications wizard in the RecoverPoint for VMs Deployer to modify the network settings of the vRPA cluster.

**Procedure**

1. In a web browser, enter https://<ip-address> where <ip-address> is the IP address of a vRPA in the cluster you are installing. Once the vRPA’s landing page loads in the web browser, click the RecoverPoint for VMs Deployer link.

   The RecoverPoint for VMs Deployer Home Page loads in the web browser.

2. If prompted to, enter the login details for RecoverPoint for VMs user boxmgmt and click Sign in.

3. Under More actions:, select the vRPA cluster network modifications wizard.

4. In the Connectivity Settings step, modify the gateway or iSCSI IP addresses you wish to change. IPv6 addresses are not supported on iSCSI interfaces.

5. In the Advanced Settings section, you can define custom MTU values for the vRPA cluster, as needed. To add additional gateways, click Add Route.

6. Click Modify.

7. In the Modifications Progress screen, the vRPA cluster is modified according to the settings selected in the wizard.
CHAPTER 3

Upgrading RecoverPoint for VMs 4.3.x to 4.3.1

- Upgrade overview ........................................................................................................ 26
- The Upgrade and Maintenance package ................................................................ 26
- Upgrading the vRPA clusters ................................................................................ 27
- Upgrading the RecoverPoint for VMs splitters ...................................................... 28
- Upgrading the RecoverPoint for VMs plug-in ........................................................ 29
Upgrade overview

Note
RecoverPoint for VMs 4.3 clusters and RecoverPoint for VMs 4.2 clusters cannot co-exist on the same vCenter. RecoverPoint for VMs 4.3 clusters and RecoverPoint for VMs 4.3.1 clusters can co-exist on the same vCenter, however, the 4.3.1 plugin does not support 4.3 clusters. If you need to use functionality that is only available in the 4.3.1 plugin, all clusters will need to be upgraded to RecoverPoint for vMs 4.3.1.

Upgrading RecoverPoint for VMs 4.3 to 4.3 SP1 consists of the following steps:

1. Downloading the Upgrade and Maintenance package from EMC online support on page 26.
2. Upgrading the vRPA clusters using the RecoverPoint Deployment Manager on page 27.
3. Upgrading the RecoverPoint for VMs splitters on every ESXi server in the RecoverPoint for VMs system on page 28.
4. Upgrading the RecoverPoint for VMs plug-in on page 29.

Note
If you are currently running RecoverPoint for VMs 4.2 and wish to upgrade to RecoverPoint for VMs 4.3.1, you must follow the procedure detailed in Upgrading RecoverPoint for VMs 4.2 to 4.3.1 on page 32.

The Upgrade and Maintenance package

The RecoverPoint for VMs Upgrade and Maintenance package should be downloaded from http://support.emc.com. The Upgrade and Maintenance package consists of the following components:

Table 5 RecoverPoint for VMs Upgrade and Maintenance package components

<table>
<thead>
<tr>
<th>Component</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>RecoverPoint Deployment Manager</td>
<td>RecoverPoint Deployment Manager ZIP archive file. RecoverPoint Deployment Manager is used to upgrade to RecoverPoint for VMs 4.3.1 and to add new vRPAs to an existing RecoverPoint for VMs environment.</td>
</tr>
<tr>
<td>ISO file</td>
<td>RecoverPoint for VMs release ISO.</td>
</tr>
<tr>
<td>VIB file</td>
<td>vSphere Installation Bundle. ESXi splitter installation in a vSphere Installation Bundle format. The ESXi splitter needs to be manually deployed when upgrading to RecoverPoint for VMs 4.3.1.</td>
</tr>
<tr>
<td>RecoverPoint for VMs Web Client plug-in</td>
<td>RecoverPoint for VMs Web Client plug-in. The RecoverPoint for VMs plug-in needs to be manually deployed when upgrading to RecoverPoint for VMs 4.3.1.</td>
</tr>
<tr>
<td>KVSS</td>
<td>Optional KVSS ZIP archive file. KVSS is a component that aids in creating VSS-based application consistent bookmarks for applications residing on protected VMs.</td>
</tr>
</tbody>
</table>
Upgrading the vRPA clusters

Before you begin
To use the RecoverPoint for VMs Deployment Manager, you must have a version of Java™ 7 (update 13 or higher), 32-bit, installed on the computer running the RecoverPoint for VMs Deployment Manager. It is highly recommended to have the latest Java 7 update installed.

Use the RecoverPoint for VMs Deployment Manager to upgrade the vRPA cluster.

Procedure
1. Launch the RecoverPoint Deployment Manager and select **Upgrade RecoverPoint for Virtual Machines**. Click **Login**.
2. In the **Select upgrade step** screen, select **Prepare for Upgrade** to prepare the vRPA cluster for upgrading.
3. In the **Prepare for upgrade** screen, read the list of conditions. Once you have ensured that the conditions are met, select **I have fulfilled the conditions for upgrading the cluster**.
4. In the **Login credentials** screen, enter the RecoverPoint for VMs cluster management IP address and the installation and administrator credentials to connect to the cluster.
5. In the **Login credentials summary** screen, review the results of the connectivity test.
6. In the **Update RecoverPoint release** screen, select **Update with an ISO image available locally**.
7. In the **ISO file information** screen, select **Upload from local machine** and browse to locate the ISO file.
8. In the **ISO file distribution summary** screen, review the results of the distribution of the ISO image file to all of the vRPAs in the RecoverPoint for VMs environment.
9. In the **System diagnostics** screen, review the results of the system diagnostic tests. If errors are detected, you must correct them before you are able to continue. Once errors are resolved, click **Refresh** to rerun the system diagnostics process.
10. In the **Save system files** screen, specify a path and filename to save the configuration file and the system modifications file.
11. In the **Apply upgrade configuration** screen, import the system modifications file that may have been provided to you by EMC Customer Support. If no system modifications were found, clear the **Modifications file** checkbox and click **Yes** when the **No system modifications file imported** window appears.
12. In the **Cluster diagnostics** screen, review the results of the environment diagnostics test. It is strongly recommended to resolve any warnings or errors that may be found before proceeding.

Before clicking **Next**, note that applying the upgrade may take a number of hours to complete, depending on the size of the environment you are upgrading (number of vRPAs, number of consistency groups, number of VMs, and so on).
13. In the **Apply upgrade summary** screen, the system applies the upgrade to all the vRPAs. During this step, the system goes into maintenance mode and the RecoverPoint for VMs plug-in can only be used to monitor the system; modifications cannot be made. Once the upgrade is completed, the system exists maintenance mode.
14. Repeat this procedure for all other vRPA clusters in your RecoverPoint for VMs system.
Upgrading the RecoverPoint for VMs splitters

Upgrading the splitters on the ESXis must be done gradually; there must always be at least one ESXi with an installed splitter for the vRPAs to keep working. In order to prevent a full sweep, the splitter upgrade procedure can continue only when all of the consistency groups are active. Before installing the new splitter, the existing splitter must be removed:

Procedure
1. On the ESXi host, enter maintenance mode to vMotion all VMs from the ESXi server. To enter maintenance mode, at the ESXCLI, enter the following command:

   `esxcli system maintenanceMode set -e=true`

2. To remove the old RecoverPoint vSphere Installation Bundle on the ESXi, in the ESXi host console, use ssh to run the following command:

   `esxcli software vib remove -n "RP-Splitter"

3. Verify that `/usr/lib/vmware/vmkmod/esx_splitter` has been deleted.

4. The new splitter can be installed with either of the following methods, documented below:
   - Installing the splitter with the RecoverPoint for VMs VIB installer
   - Installing the splitter with boxmgmt

Installing the splitter with the RecoverPoint for VMs VIB installer

If you chose to install the splitter with the VIB installer, you must repeat these steps for all ESXi hosts being updated. If you are using ESXi 6.x, you may need to enable shell access in ESXi 6.x before proceeding.

Procedure
1. Use an SSH client with secure copy protocol to copy the RecoverPoint VIB to the tmp directory. Use the following command:

   `scp <vib name> <username>@<ESXi host IP>:/scratch`

   For example:
   `scp kdriver_RPESX-00.4.3.1.0.0.h.152.000.vib root@10.10.10.10:/scratch`

2. To install the new RecoverPoint vSphere Installation Bundle on the ESXi, in the ESXi host console, run the following command:

   `esxcli software vib install -v /<vib_full_path> --no-sig-check`

   The following message appears if installation is successful:

   **Installation Result**
   
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: EMC_Recoverpoint_bootbank_RP-Splitter_RPS-<version number>
   VIBs Removed:
   VIBs Skipped:

3. To confirm installation of the splitter, in the ESXi host console, use ssh to run the following command:

   `esxcli software vib list`
The RecoverPoint for VMs splitter installation bundle name should appear at the top of the list.

4. On the ESXi host, exit maintenance mode by running the following command at the ESXCLI:

   ```
esxcli system maintenanceMode set -e=false
   ```

5. vMotion the VMs back to this ESXi host.

6. Repeat the entire procedure for every ESXi server in every ESXi cluster in the system.

**Installing the splitter with boxmgmt**

If you chose install the splitter with boxmgmt, you must ensure that all vRPAs reside on ESXis with a splitter installed.

**Procedure**

1. Use an SSH client to connect to a vRPA and log in with boxmgmt credentials.
2. From the Main Menu, select **Setup > Advanced options > Splitter actions > Install Splitter.** Provide the following vCenter Server credentials: IP, username, password, and certificate location. Review and approve the certificate.

   All ESXis in the vCenter that do not have splitters installed are listed.
3. Select the ESXis on which to deploy the splitter. The splitter can be deployed on individual ESXis or on all ESXis in the vCenter.

   The RecoverPoint for VMs splitter is installed on the selected ESXis.

**Upgrading the RecoverPoint for VMs plug-in**

Upgrade the RecoverPoint for VMs plug-in for each vCenter in your system.

**Procedure**

1. Access the vSphere Web Client at: https://<vCenter-ip-address>:9443/vsphere-client/
   where: `<vCenter-ip-address>` is the IP address of the vCenter. In the vSphere Web Client home page, click the **RecoverPoint for VMs** icon.
2. Click the **Help...** link at the top right corner of the **RecoverPoint for VMs Management** screen and select **Upgrade RP for VMs plug-in** from the drop-down box.
3. In the **Upgrade RP for VMs plug-in** window, select a version to upgrade to.
4. Log out of the vCenter and then log back in to complete the upgrade of the plug-in.

   After upgrading the plug-in, you will not be able to access vRPA clusters that are running earlier versions of RecoverPoint for VMs.
CHAPTER 4

Upgrading RecoverPoint for VMs 4.2 to 4.3.1

- Upgrade overview .......................................................... 32
- Upgrading vRPAs from 4.2 to 4.3.1 .................................. 32
- Upgrading the RecoverPoint for VMs splitters ............. 33
Upgrade overview

Note
RecoverPoint for VMs 4.3.x clusters and RecoverPoint for VMs 4.2 clusters cannot co-exist on the same vCenter.

When upgrading from RecoverPoint for VMs 4.2.x to 4.3.1, all existing RecoverPoint for VMs settings are preserved by RecoverPoint for VMs 4.3.1. There is no journal loss and no full sweep. However, replication is stopped temporarily to complete the upgrade process.

The upgrade procedure requires a minimum of 2 ESXi hosts with installed splitters; the vRPAs will continue running on one host while the other host's splitter is being upgraded. In order to have a copy of the configuration settings for future reference, it is recommended to run the `save_settings` command in the CLI before starting the upgrade procedure. Use an SSH client to connect to the cluster management IP, log in as user admin and run the `save_settings` command.

Before upgrading the RecoverPoint for VMs splitters, all vRPA clusters attached to the splitter must be upgraded to RecoverPoint for VMs 4.3.1.

Upgrading from RecoverPoint for VMs 4.2 to 4.3.1 consists of the following procedures:

- Upgrading vRPAs
- Upgrading the RecoverPoint for VMs splitters

Upgrading vRPAs from 4.2 to 4.3.1

To upgrade the RecoverPoint for VMs environment, perform the following procedures on all vRPAs in the system:

1. Detaching vRPAs on page 32
2. Unregistering the RP extension from the Managed Object Browser on page 49
3. Installing the new ISO on vRPAs on page 33
4. Completing the vRPA upgrade on page 33

Detaching vRPAs

Procedure

1. Use an ssh client to connect to a vRPA and log in as user boxmgmt.
2. From the Main Menu, select Cluster Operations ➔ Detach from Cluster.

   The vRPA detaches from the cluster. All replication is paused.
3. Repeat this procedure on all vRPAs in all vRPA clusters in the system.

Unregistering the plug-in from the Managed Object Browser

The RecoverPoint for VMs plug-in should be unregistered from the Managed Object Browser at each vCenter that contains ESXi hosting vRPA clusters. It is recommended to unregister while the vRPAs are detached and before they are reattached to the cluster. All vRPAs in the vRPA cluster must be detached before unregistering the plug-in.
Upgrading RecoverPoint for VMs 4.2 to 4.3.1

**Note**

Access to the Managed Object Browser is disabled by default in vSphere 6.0. For instructions on how to enable access, refer to VMware KB2108405.

**Procedure**

1. In a web browser, enter the fully-qualified domain name (or IP address) for the ESXi or vCenter Server system:
   
   `https://hostname.yourcompany.com/mob/?moid=ExtensionManager`

2. Log in using your vCenter login credentials.

3. In the **Methods** table, select **UnregisterExtension**.
   
   A new browser window opens with **void UnregisterExtension** command displayed.

4. In the **Parameters** table, enter `com.emc.recoverpoint.vwc` in the value field and click **Invoke Method**.

**Installing the new ISO on vRPAs**

**Procedure**

1. Use an ssh client to connect to a vRPA and log in as user boxmgmt.

2. From the **Main Menu**, select **Installation > Upgrade > Download ISO (get from FTP server)**.

3. From the **Main Menu**, select **Installation > Upgrade > Apply downloaded ISO**.
   
   The ISO is applied to the vRPA and the vRPA reboots.

4. Repeat this procedure on all vRPAs in all vRPA clusters in the system.

**Completing the vRPA upgrade**

**Procedure**

1. Use an SSH client to connect to a vRPA and log in as user boxmgmt.

2. When prompted to configure a temporary IP, select **No**.

3. From the **Main Menu**, select **Installation > Upgrade > Auto Upgrade**. When prompted, "Have you converted the repository volume from the previous version to the current version?", select **No** for the first vRPA in each vRPA cluster.

4. Once the auto upgrade of the first vRPA in each cluster has completed, repeat the vRPA upgrade on each additional vRPA in the system. When prompted, "Have you converted the repository volume from the previous version to the current version?", select **Yes** for all subsequent vRPAs.

**Results**

The RecoverPoint for VMs plug-in will install automatically when you log into the vSphere Web Client.

**Upgrading the RecoverPoint for VMs splitters**

Upgrading the splitters on the ESXi must be done gradually; there must always be at least one ESXi with an installed splitter for the vRPAs to keep working. In order to prevent a full sweep, the splitter upgrade procedure can continue only when all of the consistency groups are active. Before installing the new splitter, the existing splitter must be removed:
Procedure

1. On the ESXi host, enter maintenance mode to vMotion all VMs from the ESXi server. To enter maintenance mode, at the ESXCLI, enter the following command:

   ```bash
   esxcli system maintenanceMode set -e=true
   ```

2. To remove the old RecoverPoint vSphere Installation Bundle on the ESXi, in the ESXi host console, use ssh to run the following command:

   ```bash
   esxcli software vib remove -n "RP-Splitter"
   ```

3. Verify that `/usr/lib/vmware/vmkmod/esx_splitter` has been deleted.

4. The new splitter can be installed with either of the following methods, documented below:
   - Installing the splitter with the RecoverPoint for VMs VIB installer
   - Installing the splitter with boxmgmt

Installing the splitter with the RecoverPoint for VMs VIB installer

If you chose to install the splitter with the VIB installer, you must repeat these steps for all ESXi hosts being updated. If you are using ESXi 6.x, you may need to enable shell access in ESXi 6.x before proceeding.

Procedure

1. Use an SSH client with secure copy protocol to copy the RecoverPoint VIB to the tmp directory. Use the following command:

   ```bash
   scp <vib name> <username>@<ESXi host IP>:/scratch
   ```
   
   For example:

   ```bash
   scp kdriver_RPESX-00.4.3.1.0.0.h.152.000.vib root@10.10.10.10:/scratch
   ```

2. To install the new RecoverPoint vSphere Installation Bundle on the ESXi, in the ESXi host console, run the following command:

   ```bash
   esxcli software vib install -v /<vib_full_path> --no-sig-check
   ```

   The following message appears if installation is successful:

   ```markdown
   Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: EMC_Recoverpoint_bootbank_RP-Splitter_RPS-<version number>
   VIBs Removed: 
   VIBs Skipped:
   ```

3. To confirm installation of the splitter, in the ESXi host console, use ssh to run the following command:

   ```bash
   esxcli software vib list
   ```

   The RecoverPoint for VMs splitter installation bundle name should appear at the top of the list.

4. On the ESXi host, exit maintenance mode by running the following command at the ESXCLI:

   ```bash
   esxcli system maintenanceMode set -e=false
   ```

5. vMotion the VMs back to this ESXi host.
6. Repeat the entire procedure for every ESXi server in every ESXi cluster in the system.

**Installing the splitter with boxmgmt**

If you chose install the splitter with boxmgmt, you must ensure that all vRPAs reside on ESXis with a splitter installed.

**Procedure**

1. Use an SSH client to connect to a vRPA and log in with boxmgmt credentials.
2. From the Main Menu, select **Setup** › **Advanced options** › **Splitter actions** › **Install Splitter**. Provide the following vCenter Server credentials: IP, username, password, and certificate location. Review and approve the certificate.

   All ESXis in the vCenter that do not have splitters installed are listed.
3. Select the ESXis on which to deploy the splitter. The splitter can be deployed on individual ESXis or on all ESXis in the vCenter.

   The RecoverPoint for VMs splitter is installed on the selected ESXis.
CHAPTER 5

Troubleshooting

- Troubleshooting issues with vRPAs ............................................................... 38
- Troubleshooting issues with splitters ............................................................ 39
- Troubleshooting issues with the RecoverPoint for VMs plug-in ...................... 40
- Troubleshooting issues with RecoverPoint for VMs replication ..................... 40
- Getting help .................................................................................................... 41
Troubleshooting issues with vRPAs

vRPA is down

- Check the RecoverPoint for VMs dashboard for Error events indicating that the vRPA is not online.
- Login to the surviving vRPA and enter your RecoverPoint username and password to log into the CLI. Check the cluster status using the `get_system_status` command and when prompted, choose to retrieve the status of all categories.
- Confirm that the vRPA cannot be reached using SSH by trying to log into boxmgmt.
- Check any conflicts in the vRPA resource reservation which might have led to the vRPA being powered off. Resolve any issues before proceeding.
- In the vSphere Web Client, right click on the vRPA that is down and select All vCenter Actions > Power > Power On
- Monitor the vRPA console in vSphere Web Client to ensure that the vRPA was powered on successfully.
- Collect logs to investigate the root cause of why the vRPA went down. For more information on collecting logs, see “Collecting system information” and “Collecting RecoverPoint for VMs splitter logs” in the *EMC RecoverPoint for Virtual Machines Administrator’s Guide*.

Note

If you are using a licensed version of RecoverPoint for VMs, contact EMC Customer Support.

vRPA is detached from the cluster

- Check the RecoverPoint for VMs dashboard for Error events indicating that the vRPA cannot access storage or communicate with the splitter(s).
- Login to the surviving vRPA and enter your RecoverPoint username and password to log into the CLI. Check the cluster status using the `get_system_status` command and when prompted, choose to retrieve the status of all categories.
- Confirm that the vRPA can be reached using SSH by trying to log into boxmgmt.
- Login to the vRPA using boxmgmt and select Cluster operations > Attach RPA to Cluster. Monitor the vRPA console in vSphere Web Client to ensure that the vRPA was powered on successfully.
- Collect logs to investigate the root cause of why the vRPA is detached from the cluster. For more information on collecting logs, see “Collecting system information” and “Collecting RecoverPoint for VMs splitter logs” in the *EMC RecoverPoint for Virtual Machines Administrator’s Guide*.

Note

If you are using a licensed version of RecoverPoint for VMs, contact EMC Customer Support.

vRPA does not see Storage or Splitter

- Ensure the vRPA is online.
- Ensure the vRPA is attached to the cluster.
**Troubleshooting issues with splitters**

**Splitter is not visible or is in error state**

- If possible, vMotion any protected VMs from ESXi hosts with splitters in error state in order to continue or resume replication.
- Ensure the splitter processes are running:
  1. Login to the ESXi server and validate that the splitter processes are running using the following command: `ps |grep kdriver`
  2. If processes are not running, place the ESXi node in maintenance mode and reboot.
- Validate Software iSCSI Adapter configuration:
  - Ensure that the VMkernel ports are bound to the Software iSCSI Adapter on every host in the ESXi cluster.
  - Validate that the Software iSCSI Adapter sees all paths and vRPA iSCSI targets.
  - Validate that the iSCSI paths to the vRPAs are active and used.
- Validate that the vRPAs are able to ping the Software iSCSI VMkernel ports:
  - To ping the Software iSCSI VMkernel ports from vRPA, login to boxmgmt and select `Diagnostics > Run Internal Command > ping -I eth2 (or eth3) <VMkernel IP address>`
  - If the ping tests fail, validate the IP address, netmask and gateway assignments on the vRPA iSCSI interfaces as well as on the Software iSCSI Adapter VMkernel ports.
- Collect logs to investigate the root cause of why the splitter is not visible or is in error state. For more information on collecting logs, see “Collecting system information” and “Collecting RecoverPoint for VMs splitter logs” in the *EMC RecoverPoint for Virtual Machines Administrator’s Guide*.

**Note**

If you are using a licensed version of RecoverPoint for VMs, contact EMC Customer Support.
Troubleshooting issues with the RecoverPoint for VMs plug-in

vSphere Web Client does not contain plug-in
Proceed through the following steps until the problem is resolved:

- Log out of vSphere Web Client and log back in. Check if the RecoverPoint for VMs plug-in is listed under Inventories.
- If the RecoverPoint for VMs plug-in is not listed, restart the vCenter Web Client service.
- Validate the vCenter Credentials configuration. You may need to reconfigure vCenter credentials. Consult EMC Customer Support if protected VMs exist.
- If the plug-in is still not visible in the vSphere Web Client, collect logs to investigate the root cause of why the plug-in is not visible. For more information on collecting logs, see “Collecting system information” and “Collecting RecoverPoint for VMs splitter logs” in the EMC RecoverPoint for Virtual Machines Administrator’s Guide.

Plug-in does not see the vRPA cluster
Proceed through the following steps until the problem is resolved:

- Log out of the vSphere Web Client and log back in.
- Refresh the vSphere Web Client.
- Restart the vSphere Web Client.
- Log into the Managed Object Browser at https://<vSphere Web Client>/mob. Ensure the vCenter credentials are configured properly.

Note
Access to the Managed Object Browser is disabled by default in vSphere 6.0. For instructions on how to enable access, refer to VMware KB2108405.

- Reboot vRPA1 and then reboot vRPA2.
- Collect logs to investigate the root cause of why the vRPA is not visible. For more information on collecting logs, see “Collecting system information” and “Collecting RecoverPoint for VMs splitter logs” in the EMC RecoverPoint for Virtual Machines Administrator’s Guide.

Note
If you are using a licensed version of RecoverPoint for VMs, contact EMC Customer Support.

Troubleshooting issues with RecoverPoint for VMs replication

Consistency Group is in High-load transfer state or initialization is not completing

- Create an SSH connection to the vRPA management IP address, and enter your RecoverPoint username and password to log into the CLI. Run the detect_bottlenecks command and collect the created reports to determine the root cause of the high-load condition. For more information on detecting bottlenecks, see “Detecting bottlenecks” in the EMC RecoverPoint for Virtual Machines Administrator’s Guide.
- Resolve issues highlighted by the detect_bottlenecks reports such as WAN or journal issues.
Troubleshooting

- If consistency groups are not balanced across vRPAs, create an SSH connection to the vRPA management IP address, and enter your RecoverPoint username and password to log into the CLI. Run the `balance_load` command and change consistency group assignments accordingly. For more information on load balancing, see “Load balancing” in the *EMC RecoverPoint for Virtual Machines Administrator’s Guide*.

- If the throughput required by a consistency group exceeds the availability on a single vRPA, review the vRPA profile to see if additional resources can be added to meet higher IOPS and throughput requirements.

- Check link policies such as compression, and deduplication as these can add additional load on the vRPA. For more information on these link policies, see “Editing group or link policies” in the *EMC RecoverPoint for Virtual Machines Administrator’s Guide*.
  - If the consistency group contains more than one VM, consider moving VMs to dedicated consistency groups and using group sets as needed.
  - Consider adding vRPAs (up to 8) to the vRPA cluster for additional resources.
  - Review ESXi resources to ensure there is no contention.

- If needed, create an SSH connection to the vRPA management IP address, and enter your RecoverPoint username and password to log into the CLI. Run the `config_io_throttling` command to slow down production storage reads during full sweep process.

Consistency group is in Error state

- Perform all of the procedures suggested for when the consistency group is in High-load state. If the consistency group is still in Error state, try the following:
  - Check if the image access buffer is full. If so, disable image access.
  - Resolve any WAN issues.
  - Check if the consistency group is in a permanent high-load state.

- Collect logs to investigate the root cause of why the consistency group is in error state. For more information on collecting logs, see “Collecting system information” and “Collecting RecoverPoint for VMs splitter logs” in the *EMC RecoverPoint for Virtual Machines Administrator’s Guide*.

---

**Note**

If you are using a licensed version of RecoverPoint for VMs, contact EMC Customer Support.

---

**Getting help**

EMC support, product, and licensing information can be obtained as follows:

- **Product information** — For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at: [https://support.emc.com](https://support.emc.com)

- **Technical support** — Go to EMC Online Support and click Service Center. You will see several options for contacting EMC Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.
Troubleshooting
APPENDIX A

IP & SAN setup details template

- IP & SAN setup details template ............................................................................ 44
IP & SAN setup details template

Use the IP & SAN setup details template for vRPA clusters to collect relevant infrastructure data prior to installation.

A RecoverPoint for VMs installation requires at least two designated IP addresses per vRPA, one for Management (LAN) and the other for WAN. Two additional IP addresses are required for iSCSI for each vRPA. Each ESXi host VMkernel port requires an IP address. Finally, an additional cluster management IP is required per cluster, for use by one of the vRPAs for management activities.

A RecoverPoint for VMs installation requires Management (LAN) and WAN default gateways and subnet masks.

Use of NTP, DNS, SMTP, and SNMP services, is optional according to your preference, however, use of NTP services is highly recommended.

In addition to the details in the template below, it is recommended to document the following values:

- ESXi cluster
- vRPA Profile: min, med, max
- vRPA datastore

### Table 6 IP & SAN vRPA Cluster Setup Details

<table>
<thead>
<tr>
<th>IP &amp; SAN vRPA Cluster Details</th>
<th>vRPA cluster #1</th>
<th>vRPA cluster #2</th>
<th>vRPA cluster #3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time zone</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local domain</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary DNS server (optional)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secondary DNS server (optional)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP server (optional, but highly recommended)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cluster management IPv4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management default gateway IPv4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management subnet mask IPv4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAN default gateway</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAN subnet mask</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP (optional)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vCenter IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vCenter credentials</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP &amp; SAN vRPA Details</td>
<td>vRPA cluster #1</td>
<td>vRPA cluster #2</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>vRPA 1:</td>
<td>vRPA management IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vRPA WAN IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iSCSI1 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iSCSI2 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ESXi server iSCSI VMkernel port 1 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ESXi server iSCSI VMkernel port 2 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vRPA 2:</td>
<td>vRPA management IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vRPA WAN IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iSCSI1 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iSCSI2 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ESXi server iSCSI VMkernel port 1 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ESXi server iSCSI VMkernel port 2 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vRPA 3 (optional):</td>
<td>vRPA management IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vRPA WAN IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iSCSI1 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iSCSI2 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ESXi server iSCSI VMkernel port 1 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ESXi server iSCSI VMkernel port 2 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vRPA 4 (optional):</td>
<td>vRPA management IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vRPA WAN IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iSCSI1 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iSCSI2 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ESXi server iSCSI VMkernel port 1 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ESXi server iSCSI VMkernel port 2 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vRPA 5 (optional):</td>
<td>vRPA management IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vRPA WAN IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iSCSI1 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iSCSI2 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ESXi server iSCSI VMkernel port 1 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ESXi server iSCSI VMkernel port 2 IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vRPA 6 (optional):</td>
<td>vRPA management IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vRPA WAN IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP &amp; SAN vRPA Details</td>
<td>vRPA cluster #1</td>
<td>vRPA cluster #2</td>
<td>vRPA cluster #3</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>vRPA 7 (optional):</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iSCSI1 IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iSCSI2 IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESXi server iSCSI VMkernel port 1 IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESXi server iSCSI VMkernel port 2 IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vRPA management IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vRPA WAN IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iSCSI1 IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iSCSI2 IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESXi server iSCSI VMkernel port 1 IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESXi server iSCSI VMkernel port 2 IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vRPA 8 (optional):</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vRPA management IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vRPA WAN IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iSCSI1 IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iSCSI2 IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESXi server iSCSI VMkernel port 1 IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESXi server iSCSI VMkernel port 2 IP</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX B

Cleaning up the RecoverPoint for VMs system for reinstallation

Use the following procedures to clean up the RecoverPoint for VMs environment before reinstalling. Note that RecoverPoint for VMs 4.3 clusters and RecoverPoint for VMs 4.2 clusters cannot co-exist on the same vCenter. RecoverPoint for VMs 4.3 clusters and RecoverPoint for VMs 4.3.1 clusters can co-exist on the same vCenter, however, the 4.3.1 plug-in does not support 4.3 clusters. If you need to use functionality that is only available in the 4.3.1 plug-in, all clusters will need to be upgraded to RecoverPoint for VMs 4.3.1.

- Unprotecting VMs..................................................................................................48
- Removing the vRPA cluster from the RecoverPoint for VMs system......................... 48
- Uninstalling the RecoverPoint for VMs splitter....................................................... 48
- Detaching vRPAs....................................................................................................48
- Powering off vRPAs..............................................................................................48
- Deleting the repository folder................................................................................49
- Unregistering the RP extension from the Managed Object Browser.........................49
- Verifying that the configuration parameters are empty...........................................50
- Removing the vRPA iSCSI IPs...............................................................................50
- Removing custom tokens from the Managed Object Browser.................................50
- Cleaning up the vRPAs...........................................................................................51
Unprotecting VMs

Procedure

1. In the vSphere Web Client home page, click the RecoverPoint for VMs Management icon > Protection tab. Click Virtual Machines.
2. Select the VM you wish to stop replicating. Click the Unprotect icon. Repeat for each protected VM.

Removing the vRPA cluster from the RecoverPoint for VMs system

If there is more than one vRPA cluster in the RecoverPoint for VMs system that you are uninstalling, you must remove each vRPA cluster from the system. If you wish to remove just one vRPA cluster from a system with at least two clusters, the following procedure should be performed from a vRPA cluster that is remaining in the system (and not from the cluster being removed).

Procedure

1. Use an ssh client to connect to a vRPA in the cluster and log in as user boxmgmt.
2. From the Main Menu, select Cluster operations > Remove a cluster from this system.

Uninstalling the RecoverPoint for VMs splitter

Procedure

1. Use an ssh client to obtain a list of all installed vSphere Installation Bundles (VIB) on each ESXi host. Use the following command:

   esxcli software vib list

2. Extract the name of the VIBs to uninstall from the displayed list (usually listed as “RP-Splitter”). Use the following command to remove the VIB:

   esxcli software vib remove -n "<vib name>" --maintenance-mode

3. Repeat this procedure for every vRPA cluster in the RecoverPoint for VMs system.

Detaching vRPAs

Procedure

1. Use an ssh client to connect to a vRPA and log in as user boxmgmt.
2. From the Main Menu, select Cluster Operations > Detach from Cluster.
   
   The vRPA detaches from the cluster. All replication is paused.
3. Repeat this procedure on all vRPAs in all vRPA clusters in the system.

Powering off vRPAs

Procedure

1. At the vSphere Web Client, in Inventory, select VMs and Templates.
Cleaning up the RecoverPoint for VMs system for reinstallation

2. Select each vRPA, right-click and select All vCenter Actions > Power > Power Off.

Deleting the repository folder

**Procedure**

1. At the vSphere Web Client, select vCenter > Datastores > Manage. Select the datastore where the repository folder was created.
2. In the list of files displayed in the Files subtab, locate the RPvStorage folder. Right-click and select Delete File.

Unregistering the RP extension from the Managed Object Browser

The RecoverPoint extension should be unregistered from the Managed Object Browser at each vCenter that contains ESXi hosting vRPA clusters.

**Note**

Access to the Managed Object Browser is disabled by default in vSphere 6.0. For instructions on how to enable access, refer to VMware KB2108405.

**Procedure**

1. In a web browser, enter the fully-qualified domain name (or IP address) for the ESXi or vCenter Server system:
   
   `https://hostname.yourcompany.com/mob/?moid=ExtensionManager`

2. Log in using your vCenter login credentials.
3. In the Methods table, select UnregisterExtension.
   
   A new browser window opens with void UnregisterExtension command displayed.
4. In the Parameters table, enter `com.emc.recoverpoint.vwc` in the value field and click Invoke Method.
5. Connect to the vCenter server (using a local network mapping or Remote Desktop Connection). Delete the following folder:
   
   - **vCenter 5.1/5.5 and Windows vCenter:**
     
     `C:\ProgramData\VMware\vSphere Web Client\vc-packages\vsphere-client-serenity\com.emc.recoverpoint.vwc-4.3.<x.y>`
   
   - **vCenter 5.1/5.5 and vCSA:**
     
     `/var/lib/vmware/vsphere-client/vc-packages/vsphere-client-serenity/com.emc.recoverpoint.vwc-4.3.<x.y>`
   
   - **vCenter 6.0 and Windows vCenter:**
     
     `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity/com.emc.recoverpoint.vwc-4.3.<x.y>`
   
   - **vCenter 6.0 and vCSA:**
     
     `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/com.emc.recoverpoint.vwc-4.3.<x.y>`
6. Restart the vSphere Web Client.
Verifying that the configuration parameters are empty

Procedure

1. At the vSphere Web Client, in Inventory, select Hosts and Clusters. Select a VM that was protected by RecoverPoint for VMs. Power off the VM. Right-click and select Edit Settings...
2. In the Edit Settings dialog box, select the VM Options tab. Expand the Advanced column. In the Configuration Parameters row, click Edit Configuration... to edit the advanced configuration parameters.
3. In the Configuration Parameters window, ensure that all configuration parameters with "RecoverPoint" or "ESX splitter" in the name have empty values.
   The following parameters must have empty values:
   - RecoverPoint RPA number
   - RecoverPoint CGUID
   - RecoverPoint Cluster ID
   - esx_splitter.globalOptions
   - esx_splitter.scsi0:1.options

Removing the vRPA iSCSI IPs

Procedure

1. At the vSphere Web Client, in Inventory, select Hosts and Clusters. Select the ESXi host.
2. Select Manage > Storage > Storage Adapters > iSCSI Software Adapter > Targets.
3. Delete the vRPA targets of the vRPA you are uninstalling.
4. Run Rescan storage adapter afterwards.

Removing custom tokens from the Managed Object Browser

The custom tokens that correspond to the RecoverPoint for VMs cluster ID need to be removed from the cluster(s) being reinstalled for all previously used vCenters.

Note
Access to the Managed Object Browser is disabled by default in vSphere 6.0. For instructions on how to enable access, refer to VMware KB2108405.

Procedure

1. In a web browser, enter the fully-qualified domain name (or IP address) of the vCenter Server system:
   https://hostname.yourcompany.com/mob/?moid=CustomFieldsManager
2. Log in using your vCenter login credentials.
3. In the Methods table, select RemoveCustomFieldDef.
   A new browser window opens with the void RemoveCustomFieldDef command displayed.
4. In the Parameters table, enter the value of a custom field listed in the Properties table that corresponds to the RecoverPoint for VMs cluster ID. Click Invoke Method.

5. If you are reinstalling several clusters, repeat step 3 and step 4 for each custom field listed in the Properties table that corresponds to the cluster IDs.

Cleaning up the vRPAs

Before installing a newer build of your release of RecoverPoint for VMs, remove all installed components. If you are planning to do a fresh installation, it is recommended to use fresh vRPAs. Otherwise, vRPA cleanup is required:

Procedure

1. Right click on the vRPA and select Edit Settings... In the Edit Settings dialog box, remove Hard disk 2 (10 MB).

2. Remove references to ESXi splitter in the configuration parameters.
Cleaning up the RecoverPoint for VMs system for reinstallation
APPENDIX C

Deploying in a VxRAIL environment

- Deploying in a VxRAIL environment

54
Deploying in a VxRAIL environment

Before you begin
When adding additional VxRAIL appliances:

- The new ESXi nodes have the RecoverPoint for VMs splitter installed and are configured with the proper software iSCSI adapter, VMkernel ports, and port groups.
- You have adjusted any VM-host affinity rules for the vRPA to ensure that they are running on separate ESXis.
- The new nodes are added into the same VSAN cluster and under the same vCenter.
- The maximum configuration is four VxRAIL appliances, which support up to 400 VMs.

Follow the instructions for Configuring networking on page 15, Deploying vRPAs using the OVA file on page 16, and Installing a vRPA cluster on page 18 using the following additional guidelines.

Deploying vRPAs using the OVA file
When Deploying vRPAs using the OVA file on page 16, in the Deploy OVF Template wizard:

Procedure

- In the Select storage screen, in the VM Storage Policy drop down, select MARVIN-STORAGE-PROFILE. The compatible VSAN datastore will be selected.
- After the vRPAs have been created, it is recommended to configure VM-Host affinity rules to avoid running vRPA1 and vRPA2 on the same ESXi node.

Configuring networking
When Configuring networking on page 15, as you configure software iSCSI adapters on all four ESXi nodes:

Procedure

1. Create two VMkernel ports on each ESXi node by selecting an existing standard vSwitch “vSwitch0”.
2. Override the NIC teaming policy to select one network adapter (vmnic) as active; the other should be marked as unused. VxRAIL uses vmnic2 exclusively for VSAN. It is recommended to assign vmnic1 to both VMkernel ports.
3. Bind the VMkernel ports to the software iSCSI adapter. It is also possible to configure a single VMkernel port which uses vmnic1 and bind it to the software iSCSI adapter.
4. It is recommended to create four port groups on vSwitch0: RP_WAN, RP_LAN, RP_iSCSI1, RP_iSCSI2.

Installing a vRPA cluster
When Installing a vRPA cluster on page 18 in the Connect a vRPA Cluster wizard:

Procedure

- In the Connectivity Settings step of the Install a vRPA cluster wizard, specify the vRPA iSCSI addresses (and not the VMkernel port IP addresses that were created earlier).
• In the **Environment Settings** step, select the VSAN datastore from the table of available datastores.
Deploying in a VxRAIL environment