Dell EMC RecoverPoint for Virtual Machines

Version 5.1

Installation and Deployment Guide

P/N 302-003-968

REV 05

DELL EMC

Published November 2018

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

FIGURES

TABLES

Preface

As part of an effort to improve product lines, we periodically release revisions of software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your technical support professional if a product does not function properly or does not function as described in this document.

Note

This document was accurate at publication time. Go to Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Purpose

This document describes how to install and configure a Recoverpoint for Virtual Machines system.

Audience

This document is intended for Virtualization Administrators who manage, maintain and scale their virtual environments, and Application Administrators who monitor application performance.

Related documentation

The following publications provide additional information:

- *RecoverPoint for Virtual Machines Release Notes*
- *RecoverPoint for Virtual Machines Quick Start Installation Poster*
- *RecoverPoint for Virtual Machines Basic Configuration Installation Guide*
- *RecoverPoint for Virtual Machines Installation and Deployment Guide*
- *RecoverPoint for Virtual Machines Product Guide*
- *RecoverPoint for Virtual Machines Administrator's Guide*
- *RecoverPoint for Virtual Machines CLI Reference Guide*
- *RecoverPoint for Virtual Machines Deployment REST API Programming Guide*
- *RecoverPoint for Virtual Machines REST API Programmer's Guide*
- *RecoverPoint for Virtual Machines Security Configuration Guide*
- *RecoverPoint for Virtual Machines Scale and Performance Guide*
- *RecoverPoint for Virtual Machines FAQ*
- *Recoverpoint for Virtual Machines Simple Support Matrix*

In addition to the core documents, we also provide White papers and Technical Notes on applications, arrays, and splitters.

Typographical conventions

This document uses the following style conventions:

Bold	Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)

Italic	Used for full titles of publications referenced in text
`Monospace`	Used for: • System code • System output, such as an error message or script • Pathnames, filenames, prompts, and syntax • Commands and options
Monospace italic	Used for variables
`Monospace bold`	Used for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

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

Product information

For documentation, release notes, software updates, or information about products, go to Online Support at https://support.emc.com.

Technical support

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

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to techpubcomments@emc.com.

CHAPTER 1

Introduction to RecoverPoint for VMs

RecoverPoint for VMs is a virtualized solution that provides data replication, protection, and recovery within the VMware vSphere environment. Definition of key terms and a system diagram help you to understand the system operation.

RecoverPoint for VMs system

Key components of the RecoverPoint for VMs system are defined and illustrated.

Key system components that are involved in this installation include:

vRPA

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

vRPA cluster

A group of up to 8 vRPAs that work together to replicate and protect data. You will create the vRPA clusters and connect them to the system by using the RecoverPoint for VMs Deployer wizards.

RecoverPoint for VMs plug-in

The vSphere Web Client user interface for managing VM replication. Automatically installed after you create the vRPA cluster.

RecoverPoint for VMs splitter

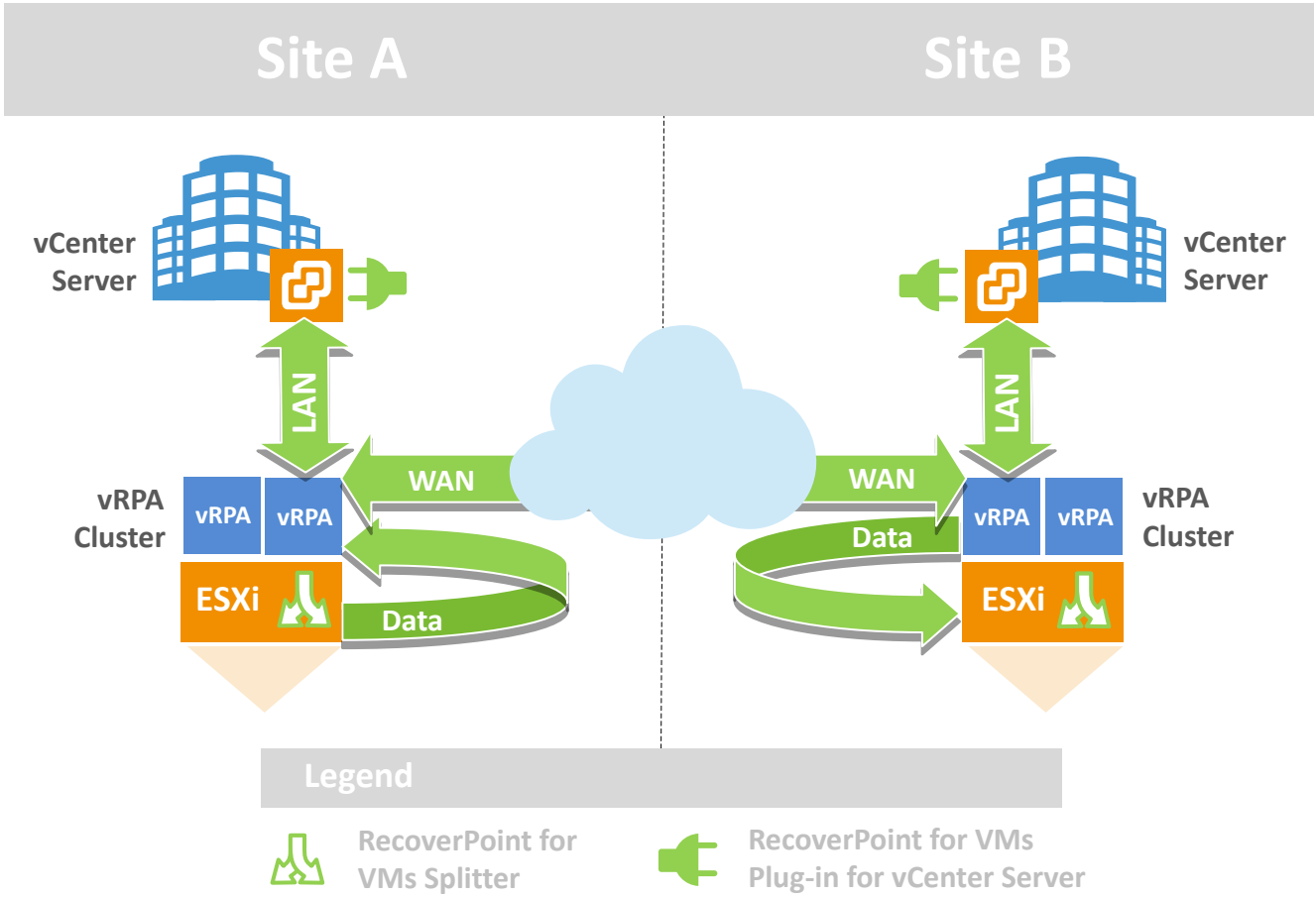
Proprietary software installed on every ESXi host in an ESXi cluster involved in RecoverPoint replication or running virtual RPAs. Splits every write to the VMDK and sends a copy of the write to the vRPA and then to the designated storage volumes. Automatically installed after you register the ESXi cluster.

RecoverPoint for VMs system

One or more connected vRPA clusters.

Figure 1 on page 15 provides a reference diagram that shows the vRPA and vRPA clusters within the RecoverPoint for VMs system. The diagram shows how these components interconnect within the VMware vSphere environment.

Figure 1 RecoverPoint for VMs system



CHAPTER 2

Preparing to install RecoverPoint for VMs

Guidelines help you choose the number of vRPAs and vRPA clusters, vRPA performance profile, splitter communication mode (IP is preferred), and network adapter topology. Preparing the VMware network and determining storage capacity sets the stage for a successful installation.

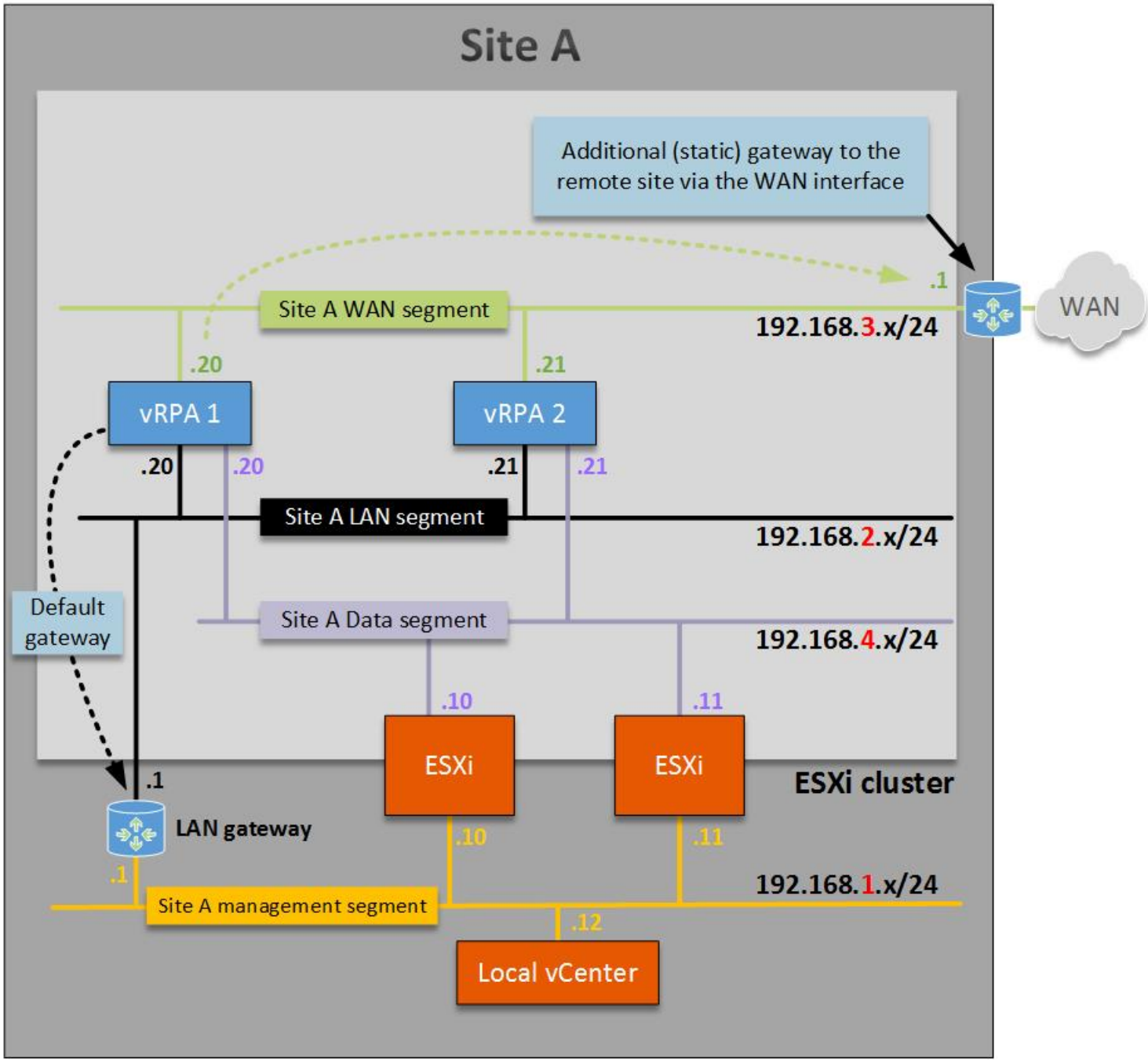
RecoverPoint for VMs networking example

A reference diagram is a valuable tool for planning your RecoverPoint for VMs system. The diagram shows an example of the network that interconnects key system components.

For clarity, Figure 2 on page 19 shows the components and interconnections of only one site in a small system. The IP addresses are for illustration purposes only.

The remaining sections of this chapter will help you to plan a system that meets your specific requirements.

Figure 2 Networking example



Planning your system

System limitations

Understanding system limitations facilitates the installation of the RecoverPoint for VMs system.

Successful operation of RecoverPoint for VMs depends on a persistent vSphere deployment.

For a comprehensive and up-to-date list of system limitations, see the *RecoverPoint for Virtual Machines Release Notes*.

Allocating IP addresses

Knowing how many IP addresses you need for the RecoverPoint for VMs system helps you to allocate the IP addresses before the installation is scheduled.

The RecoverPoint for VMs system requires these IP addresses:

- Cluster management IP address for each vRPA cluster
- An IP address for each vRPA network adapter (see Choosing a network adapter topology on page 22)
- An IP address for each VMkernel port

To allocate the necessary IP addresses for the RecoverPoint for VMs system, consult with the network administrator.

Document these addresses in an installation data form or spreadsheet before you begin the installation.

Documenting the installation settings

Creating an inventory of the RecoverPoint for VMs system ensures that you have all the required settings before the installation begins.

As you perform the required planning, create an installation data form or spreadsheet to record the values that you type during the installation. See Installation data forms on page 74 for examples.

Adhere to a consistent naming and numbering convention for the components of the RecoverPoint for VMs system. For example:

- For vRPAs: *<vRPA_name>*`_1`, *<vRPA_name>*`_2`, ... *<vRPA_name>*`_8`
- For vRPA clusters: *<vRPA_cluster_site_name_1>*, *<vRPA_cluster_site_name_2>* (for example: `London_1` or `New York_2`)

Choosing a vRPA topology

The first step in planning the RecoverPoint for VMs system is to determine how many vRPAs you need in each vRPA cluster and how many vRPA clusters you need in the system.

How many vRPAs?

Determining the number of vRPAs in the system is based on existing storage capacity, VMware infrastructure, and replication requirements such as high availability or product evaluation.

For typical installations, two vRPAs per vRPA cluster is sufficient. Two vRPAs per vRPA cluster provide the high availability that most production environments require.

For production environments that do not require high availability or for product evaluation in non-production environments, a single vRPA per cluster is also possible.

To scale up and support higher throughput, you may non-disruptively add vRPAs (up to 8) to each vRPA cluster.

All vRPA clusters in a system must have the same number of vRPAs.

The actual number of vRPAs that you need for each vRPA cluster depends on the capabilities of your storage, network, ESXi hosts, and the scale and performance requirements of your system.

For specific details and examples, refer to the *RecoverPoint for Virtual Machines Scale and Performance Guide*.

How many vRPA clusters?

The number of vRPA clusters you need is based on whether you require local or remote replication, or both.

For most installations, you will install two vRPA clusters in your RecoverPoint for VMs system.

For local replication, you need only one vRPA cluster. To support remote replication, two vRPA clusters are required. The maximum number of vRPA clusters in a system is five.

A vRPA cluster is confined to a single ESXi cluster. All vRPAs in a vRPA cluster must be in the same ESXi cluster.

A vRPA cluster protects VMs on the same or a different ESXi cluster. This capability requires connections between the vRPA cluster and the ESXi hosts (see Preparing the network on page 24).

For specific details and examples, refer to the *RecoverPoint for Virtual Machines Scale and Performance Guide*.

Choosing a vRPA performance profile

The vRPA performance profile defines the number of virtual CPUs, RAM, and VMDK capacity allocated to each vRPA. You choose a performance profile depending on the number of protected VMs and expected throughput.

For most installations, 2 CPUs and 4 GB of RAM is sufficient.

The actual vRPA performance profile that you need depends on these factors:

- IOPS and throughput of protected VMs
- The number of VMs protected by the vRPA cluster

You can change the resource allocation later by using the vSphere vCenter Web Client.

Decide which of these vRPA performance profiles you need:

Bronze, low performance, < 256 VMs

2 virtual CPUs

4 GB RAM

35 GB VMDK capacity

Bronze +, low performance, 256+ VMs

2 virtual CPUs

8 GB RAM

35 GB VMDK capacity

Silver, medium performance, 256+ VMs

4 virtual CPUs

8 GB RAM

35 GB VMDK capacity

Gold, high performance, 256+ VMs

8 virtual CPUs

8 GB RAM

35 GB VMDK capacity

This selection is made when you create vRPAs from the OVF wizard in the vSphere Web Client.

NOTICE

By default, all RAM is reserved and vCPU reservation is set to 3400MHz.

If required, memory and CPU resources can be added after OVA deployment by submitting a service request for scaled environments.

For details and examples, refer to the *RecoverPoint for Virtual Machines Scale and Performance Guide*.

Splitter communication mode

RecoverPoint for VMs supports TCP/IP or iSCSI communication modes between the splitters and the vRPAs. IP splitter communication mode is preferred.

The IP splitter communication mode requirements include:

- vCenter must be version 6.0 or later
- ESXi clusters or hosts to be protected must be at ESXi version 6.0 or later.
- Splitters and connected vRPA clusters must be at RecoverPoint for VMs version 5.1.1 or later.
- The preceding requirements must be enforced when adding ESXi clusters or hosts to be protected.

For new installations, the **Install a vRPA cluster** wizard in the RecoverPoint for VMs Deployer automatically validates the environment to determine if it supports the IP splitter communication mode. If validations succeed, the IP splitter communication mode is selected by default with an option to choose iSCSI mode, if desired. If validations fail, the environment is not IP-ready, and the splitter communication mode defaults to iSCSI.

For existing iSCSI installations, the user may choose to non-disruptively migrate the iSCSI environment to the IP splitter communication mode. A migration wizard and procedure are provided. The migration automatically pauses consistency groups and resumes them with the IP communication mode active. When you successfully migrate from iSCSI to IP communication mode, all communication occurs over IP, and iSCSI communication is rejected. iSCSI paths and targets are automatically removed from the ESXi iSCSI software adapters, and iSCSI configurations (for example, VMkernel port binding) can be removed.

Choosing a network adapter topology

RecoverPoint for VMs supports LAN, WAN, and data interfaces distributed across multiple network adapters or combined into one. The choice depends on the requirements for high availability and performance.

Combining multiple interfaces on one network adapter is recommended for small environments. The advantage is a smaller network footprint and ease of installation and management.

Where high availability and performance are desired, separate the LAN and WAN interfaces from the data interfaces (recommended for most installations). For even better performance, place each network on a separate virtual switch.

Decide which of these network adapter topologies you need:

One network adapter

WAN + LAN + data combined

Fewer IP addresses to create and manage

Not for high availability solutions

IPv6 is not supported for data.

Two network adapters (the default and recommended configuration)

WAN + LAN combined, Data separated

Better performance, high availability

IPv6 is not supported for data.

Two network adapters

LAN + data combined, WAN separated

Better performance, high availability

DHCP for LAN is not supported

IPv6 is not supported for data.

Three network adapters

WAN, LAN, and data separated

Better performance, high availability

DHCP for LAN is not supported

IPv6 is not supported for data.

Four network adapters

WAN and LAN separated, Data separated on two dedicated network adapters

Compatible with previous releases

Best performance and high availability

DHCP for LAN is not supported

IPv6 is not supported for data.

This selection is made when you run the Install a vRPA cluster wizard in the RecoverPoint for VMs Deployer.

For high-availability deployments in which clients have redundant physical switches, route each data card to a different virtual switch with a separate network adapter.

For each network adapter, you have the option to assign a dynamic or static IP addresses.

When using Dynamic Host Configuration Protocol (DHCP):

- Separating WAN and LAN interfaces on different network adapters is supported only when using static IP addresses for the LAN interface

- Redundant, highly available DHCP servers in the network ensure that when a vRPA restarts, it acquires an IP address

Preparing the VMware environment

Supported vSphere versions

For the most up-to-date information on supported VMware vCenter and vSphere versions, refer to the *Simple Support Matrix* available online at https://support.emc.com.

Preparing the network

To enable communications between the ESXi hosts and the vRPAs in the RecoverPoint for VMs system, you must prepare the VMware network.

If you are using IP communication, you are required only to set up the VMkernel ports.

The number of VMkernel ports you need is based on the network adapter topology you previously selected. If you decided to use four network adapters for the topology, create two VMkernel ports. Otherwise, one VMkernel port is required.

If you require iSCSI communication, the preparation requires adding iSCSI software adapters, then setting up VMkernel ports, and optionally binding the ports to the adapters. See Configuring iSCSI communication on page 91.

Set up VMkernel ports

Setting up VMkernel ports is the best practice for isolating splitter traffic from other network traffic. You isolate the traffic by placing the vRPA data interface and a dedicated VMkernel port on a private (separate) subnet. Do not use the same subnet for high availability (vMotion) and hosts (applications).

Procedure

1. For each ESXi host, click **Manage** > **Networking** > **VMkernel adapters**.
2. Add/edit the VMkernel adapters.
   - Assign IP addresses that are on a routable subnet or on the same subnet as the vRPA data interfaces.
   - Configure each VMkernel port on each vSwitch/dvSwitch.
   - If you encounter messages about the VMkernel port teaming policy, refer to VMware KB2009119.
   - Ensure that all ESXi HBA drivers and firmware are up to date and supported by VMware and respective storage vendors. See VMware KB1002598.

   The vRPA data IP addresses are assigned when deploying the vRPA cluster.

Establishing vCenter-to-vRPA communication

During installation, the vCenter server communicates to the vRPAs over port 443 to acquire the RecoverPoint for VMs plug-in. The ESXi clusters communicate over the network with the vRPA targets.

Procedure

- Ensure that you open port 443 between the vCenter and the vRPAs.

- Ensure that ESXi clusters can communicate with their vRPA targets. Configure the ESXi firewall profile to allow communication through the network.
- See the *RecoverPoint for Virtual Machines Security Configuration Guide* for more information.

Preparing the storage

Determining the amount and types of storage you need requires careful planning, guidelines, and sizing tools.

RecoverPoint for VMs replicates VMs on any type of storage that VMware supports including VMFS, NFS, vSAN, and VVols.

Ensure that all ESXi hosts in the cluster where the vRPAs reside share the datastore for the repository VMDK.

RecoverPoint for VMs requires additional storage for journal VMDKs to store point-in-time history. This storage is needed at local and remote sites. The amount of journal storage you need depends on site-specific installation and replication requirements and requires careful planning. A general guideline is to begin with a number that is 15–25 % of the total protected VM capacity. If required, you may add additional storage later. To size the system according to estimated workloads, use the RecoverPoint Sizer tool. See https://help.psapps.emc.com/display/HELP/RecoverPoint+Sizer.

The total storage capacity that is required includes:

- Storage for production VMs at the production site
- Storage for replica VMs at the replica site
- Storage for journal VMDKs
- 35 GB for each vRPA in the RecoverPoint for VMs system

A persistent scratch location on the 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.

For more details and examples, refer to the *RecoverPoint for Virtual Machines Scale and Performance Guide*.

For additional guidelines and sizing tools, contact Customer Support.

Note

Shared virtual disks (VMDK/RDM) are not supported.

Note

The vSCSI splitter does not support using VVols for journal storage.

Disabling delayed ACK

Disabling delayed acknowledgement (ACK) on ESXi servers that are used in the RecoverPoint for VMs system is recommended.

Disable delayed ACK on all ESXi servers in all ESXi clusters that may be hosting vRPAs and/or protected VMs. For more information and for instructions on disabling delayed ACK, refer to VMware KB1002598.

Understanding the installation flow

The complete work flow includes installation and protection. Understanding the stages of the work flow helps you to successfully install the RecoverPoint for VMs system and protect VMs.

Figure 3 on page 26 shows the major stages of the installation flow. Table 1 on page 26 provides details of the required procedures for each stage of the installation flow. Table 2 on page 26 lists the tasks that are performed in the RecoverPoint for VMs plug-in to protect VMs.

Figure 3 Stages of the installation flow

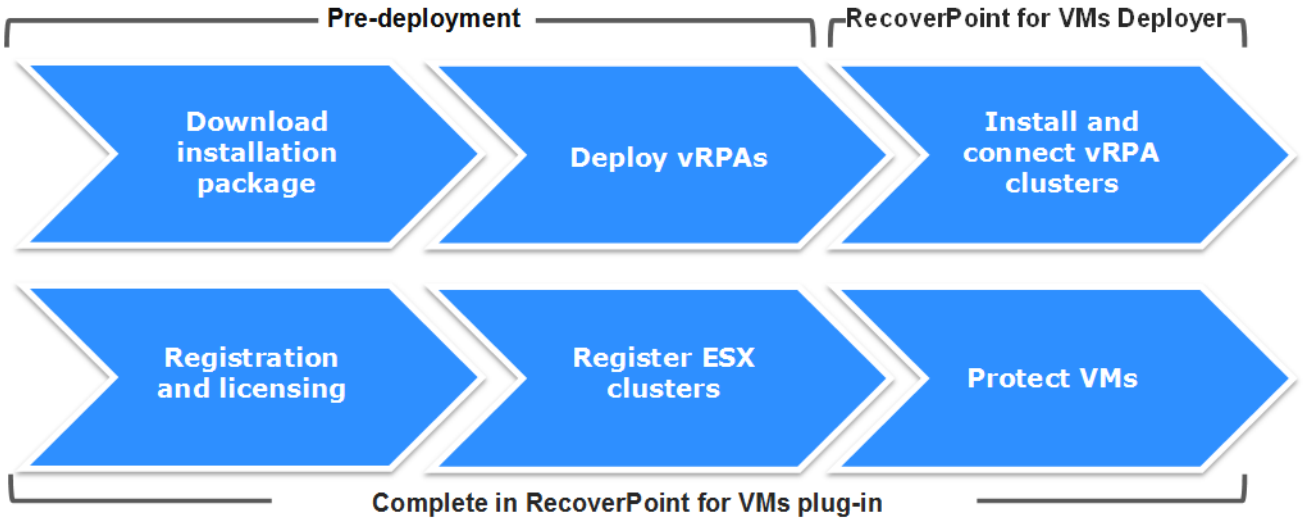


Table 1 Procedures in the installation flow

Stage of installation flow	Sequence of procedures in the installation flow	Interface
Download installation package	Download the installation package on page 30	Online support site
Deploy vRPAs	Deploy vRPAs on page 30	vSphere Web Client
Install and connect vRPA clusters	Install vRPA clusters on page 31 Connect vRPA clusters on page 33	RecoverPoint for VMs Deployer

Table 2 Procedures in the protection flow

RecoverPoint for VMs plug-in step	Sequence of procedures	Interface
Registration and licensing	Register and license the system on page 35	**vSphere Web Client** > **RecoverPoint for VMs plug-in**

Table 2 Procedures in the protection flow (continued)

RecoverPoint for VMs plug-in step	Sequence of procedures	Interface
Register ESXi clusters	Register ESXi clusters on page 35	**vSphere Web Client** > **RecoverPoint for VMs plug-in**
Protect VMs	Protect VMs on page 36	**vSphere Web Client** > **RecoverPoint for VMs plug-in**

CHAPTER 3

Installing the RecoverPoint for VMs system

Installing the RecoverPoint for VMs system involves deploying the vRPAs, installing the vRPA clusters, and connecting the vRPA clusters together. You register and license the system, register the ESXi clusters, and then begin protecting VMs.

Download the installation package

Download the installation software kit and uncompress the `.zip` file.

Note

To complete a registration form requesting a download for evaluation, Try and Buy customers should go to http://www.emc.com/products-solutions/trial-software-download/recoverpointforvms.htm.

Procedure

1. Browse to https://support.emc.com/downloads.
2. Perform a search in the **Type a Product Name** text box for **`RecoverPoint for Virtual Machines`**.
3. Locate and download **`RecoverPoint for Virtual Machines <version> Installation Kit`**.

   Example of downloaded file:
   `RecoverPoint_for_Virtual_Machines_<version>_Installation_Kit_<md5_checksum>.zip`
4. Uncompress the `.zip` file.

   The `.zip` file contains the OVA file that is needed for the installation.
5. (Recommended) Obtain documentation for RecoverPoint for VMs.
6. Continue to the next section, "Deploy vRPAs."

Deploy vRPAs

Deploy a standard OVA to create vRPAs for RecoverPoint for VMs.

Before you begin

Ensure that you have completed:

- Preparations for installation.
- Installation data form or spreadsheet to facilitate entering requested information (recommended). See Installation data forms on page 74.

Procedure

1. In the vSphere Web Client, right-click an ESXi host and select **Deploy OVF Template...**.
2. In the **Select source** screen, specify the vRPA OVF package location.
3. In the **Review details** screen, review the general properties of the OVF template. To accept, click **Next**.
4. In the **Accept License Agreements** screen, if you accept the terms of the End-User License Agreement, click **Accept** and **Next**.
5. In the **Select name and folder** screen, type a name for this vRPA and select a folder or data center.

   If you type the name of an existing vRPA, you are not permitted to continue.
6. In the **Select configuration** screen, select the desired vRPA performance profile.

7. If prompted to select a resource, in the **Select a resource** screen, select a cluster, host, or resource pool.
8. In the **Select storage** screen, select a disk format, storage policy, and high-performance datastore (best practice) to host the vRPA virtual machine files.

   All ESXi hosts in the cluster where the vRPAs reside must share the datastore where the repository VMDK resides.
9. In the **Setup networks** screen, select a destination network for the **RecoverPoint Management Network**, and select an IP protocol.
10. In the **Customize template** screen, type these vRPA LAN settings: IP address, subnet mask, and gateway.

    Follow instructions on the screen for using DHCP or static IP addresses depending on the network adapter topology.
11. The **Ready to Complete** screen summarizes all the selections. Select **Power on after deployment**. To create the vRPA, click **Finish**.

    The **Deploying vRPA** screen appears, showing the progress.
12. To create additional vRPAs, repeat this procedure.
13. When you finish creating vRPAs, continue to the next section, "Install vRPA clusters."

Results

When a vRPA is created, the **vRPA Summary** tab shows the vRPA package contents as specified. The selected IP policy is implemented automatically when the vRPA is powered on.

After you finish

To enable redundancy in case an ESXi host or datastore fails, ensure that vRPAs do not share the same ESXi host or datastore.

Install vRPA clusters

Follow the **Install a vRPA cluster** wizard to create one or more vRPA clusters for RecoverPoint for VMs.

When you are prompted to type data, consult the installation data form or spreadsheet that you created when planning the system (recommended). See Installation data forms on page 74.

Procedure

1. In a web browser, type `https://<LAN-ip-address>` where *<LAN-ip-address>* is the LAN IP address of vRPA 1 or vRPA 2 in the cluster you are installing. In the home page, click **RecoverPoint for VMs Deployer**.

   If you are using DHCP, obtain the LAN IP address from the vSphere Web Client by selecting the vRPA and clicking the **Summary** tab.
2. If prompted, type the login details for the boxmgmt user and click **Sign in**.

   The **RecoverPoint for VMs Deployer** home page appears.
3. Select the **Install a vRPA cluster** wizard.
4. On the **Version Requirements** page, the version requirements file is automatically downloaded and validated to ensure that the system meets the

requirements. If you have a `.json` configuration file that you want to import, click the **Settings** icon and then click **Import**.

If version requirements verification is successful, click **Next** to continue. If issues are found, analyze and fix blocking issues before continuing.

If the version requirements file fails to download, you are prompted to select one of these options:

- **Retry downloading the up-to-date requirements from EMC Online Support**
- **Provide version requirements file manually**
- **Do not check version requirements**

Note

To obtain the version requirements file for offline installation, browse to https://rplicense.emc.com/download. This page provides an option to download or email the `a-cca.xml` file. If this option is not available, open a Service Request with Customer Support Services (severity level 3). In the request, ask for the latest version requirements file for the RecoverPoint for VMs Deployer. The file is provided within one (1) business day and must be used within 30 days.

5. On the **Installation Prerequisites** page, type the requested information for the vCenter on which the current vRPA is running, and then click **Connect**.

   If the **SSL Certificate** window appears, verify the vCenter's SSL certificate and click **Confirm**.

6. Review the **Pre-installation Validation Results** area. If validation errors are listed, fix them before proceeding.

   If an error can be automatically fixed, the **Fix** button appears in the **Auto-Fix** column.

7. On the **Environment Settings** page, define the required settings.
   - Type a name for the vRPA cluster.
   - For better security, select the **Authenticated and encrypted communication between vRPAs** checkbox (recommended). For better performance, clear this checkbox.
   - Ensure that the splitter communication mode that you require is selected. (If the environment does not support the communication mode, the option is unavailable.)
   - Type IP addresses for DNS and NTP servers.

8. On the **vRPA Settings** page:
   a. Select the vRPAs for the vRPA cluster and click the **Apply Selection** button.
   b. Select a repository volume from the list. All ESXi hosts in the cluster where the vRPAs reside must share this volume.

9. On the **Network Settings** page, provide the requested settings for the vRPA cluster and its vRPAs.
   - In the **Network Adapters Configuration** area, keep the default setting or click **Edit** to choose a different network adapter topology.

- In the **Network Mapping** area, for each network adapter, select a value and whether to use DHCP. Type a Cluster Management IP address.
- In the **vRPA Settings** area, type the requested IP addresses. If the network configuration requires gateways to communicate with remote vRPA clusters, click **Add** to insert each gateway. For each gateway that you add at the current cluster, add a gateway at the remote cluster.
- In the **Advanced Settings** area, change the **MTU** values only if required. MTU values must be consistent across the communication interface from source to target. See KB article 484259 for more information.

10. On the **Deployment progress** page, on reaching 100%, click **Finish** to return to the home page. To export a configuration file of the vRPA cluster settings, click the **Settings** icon (upper right), and then click **Export**. This file provides a record of the vRPA cluster configuration for the major version you have installed. You use it to restore the vRPA cluster settings after an installation failure (requiring the installation to be repeated).

    If installation fails:

    - To identify the cause of failure, review the displayed error messages.
    - To return to the step in the wizard where you can fix the problem, click **Back**. Fix the problem and retry the installation.
    - Alternatively, you can retry the operation that failed by clicking **Retry the operation**.
    - If installation continues to fail, contact Customer Support.

11. To enable multi-site replication, create additional vRPA clusters by repeating this procedure for each site.
12. When all vRPA clusters are created, continue to the next section, "Connect the vRPA clusters."

Results

Installation of the RecoverPoint for VMs plug-in for vSphere vCenter is initiated.

The plug-in installation usually occurs immediately, but it might take some time for the vCenter to identify the plug-in. If you experience issues with the RecoverPoint for VMs plug-in, log out and log in again to the vSphere Web Client as described in "Troubleshooting the RecoverPoint for VMs plug-in."

Splitters are pushed to all ESXi hosts in the ESXi cluster where the vRPAs are installed.

Post-deployment, ensure that TCP port 7225 is open, to enable the plug-in residing on the vCenter to communicate with the relevant vRPA cluster.

Connect vRPA clusters

To enable replication between any two vRPA clusters, use the **Connect vRPA clusters** wizard to establish a connection between them.

Before you begin

In this procedure, the "current" cluster is defined as the vRPA cluster to which the **Connect vRPA clusters** wizard is currently pointed. The "remote" cluster is the vRPA cluster at a remote site. This wizard helps you to connect a remote vRPA cluster to the current vRPA cluster.

The remote vRPA cluster must not:

- Be in maintenance mode.
- Be an existing, configured vRPA cluster.
- Have protected VMs, consistency groups, or group sets.
- Have user or journal volumes.
- Have a license other than a vCenter license.
- Have been previously connected to a vRPA cluster

Note

A remote vRPA cluster that meets these requirements is called a "clean" cluster.

Ensure that you have a completed installation data form or spreadsheet (recommended).

Do not exceed the maximum number of five vRPA clusters per system.

If you require a gateway for communication between vRPA clusters, add a gateway at each vRPA cluster before connecting between the clusters.

Procedure

1. In a web browser, type `https://<cluster_management-ip-address>/WDM` for the vRPA cluster that you want to connect.
2. In the RecoverPoint for VMs Deployer home page of the current cluster, select the **Connect vRPA clusters** wizard.
3. On the **Environment Settings** page, type the requested information for the remote cluster.
4. In the **Current Cluster Settings** area, review the list of gateways that are configured for this vRPA cluster. If required, add one or more gateways on the current vRPA cluster. Remember that for each additional gateway at the current cluster, you must add a gateway at the remote cluster.
5. On the **Add Cluster Progress** page, the remote cluster connects to the current cluster.
6. To connect additional vRPA clusters, repeat this procedure.
7. Continue to the next section, "Change default passwords."

Change default passwords

To align with security best practices, change the default passwords of your RecoverPoint for VMs system.

Procedure

1. Connect to the RecoverPoint for VMs CLI by using SSH and the cluster management IP address.

   For more details, see the *RecoverPoint for Virtual Machines CLI Reference Guide*.
2. Log in with `security-admin` credentials (user/password).

User	Default password
admin	admin
boxmgmt	boxmgmt

User	Default password
security-admin	security-admin

Note

For RecoverPoint for VMs 5.1.1.4 and later, your admin user password serves also as the root password; follow your organization's password policy to set a strong password for these users. For earlier versions of RecoverPoint for VMs, contact Customer Support for assistance with changing the default root password; see Dell EMC Knowledge Base Article 520937 for details.

3. Run the `set_user` command to change the default passwords for the admin and boxmgmt users.
4. Run the `set_password` command to change the default password for the security-admin user.
5. Continue to the next section, "Register and license the system."

Register and license the system

Use the RecoverPoint for VMs plug-in to register and license your system. Registration and licensing enables support and provides important product updates to keep your system running optimally.

Procedure

1. Ensure that you activate your entitlements.

   This procedure is in the "Activating your entitlements" section of the *RecoverPoint for Virtual Machines Administrator's Guide*.

2. Use the **Getting Started Wizard** to add licenses and register your RecoverPoint for VMs system.

   This procedure is in the "Licensing, support, and registration" section of the *RecoverPoint for Virtual Machines Administrator's Guide*.

3. Continue to the next section, "Register ESXi clusters."

Register ESXi clusters

Use the RecoverPoint for VMs plug-in to register ESXi clusters. You cannot protect VMs unless you first register the ESXi clusters.

Procedure

1. To register an ESXi cluster:

   a. In the vSphere Web Client home page, select **RecoverPoint for VMs** > **Administration** > **vRPA Clusters**.

   b. Select the vRPA cluster at which you want to register ESXi clusters.

   c. Select the **ESX Clusters** tab.

   d. Click **Add**.

   e. In the **Register ESX Clusters** dialog box, select the ESXi cluster that you want to register, and then click **OK**.

The system validates the ESXi cluster for communication compliance.

2. If using iSCSI communication mode, and the cluster detects connectivity issues, click **Validate**. See "Validating ESXi connectivity."
3. Repeat this procedure for each vRPA cluster.
4. Continue to the next section, "Protect VMs."

Results

The RecoverPoint for VMs splitter automatically installs on all ESXi hosts of registered ESXi clusters.

Protect VMs

The RecoverPoint for VMs system is ready for operation. Use the RecoverPoint for VMs plug-in to begin protecting VMs.

Procedure

1. Protect the VMs by right-clicking each VM and selecting the protection option. Detailed instructions are in the *RecoverPoint for Virtual Machines Administrator's Guide*.
2. After protection is enabled, monitor the system as described in the *RecoverPoint for Virtual Machines Administrator's Guide*.

CHAPTER 4

Maintaining RecoverPoint for VMs

Maintaining the RecoverPoint for VMs system involves tasks such as collecting logs, migrating from iSCSI to IP communication mode, modifying vRPA cluster network settings and topology, and adding, removing, or replacing vRPAs.

Collect logs

During deployment, collecting logs for the current cluster and its vRPAs provides information that may be helpful in troubleshooting the installation.

Procedure

1. In a web browser, type `https://<LAN-ip-address>` where *<LAN-ip-address>* is the LAN IP address of the first vRPA in the cluster. In the vRPA home page, click **RecoverPoint for VMs Deployer**.
2. If prompted, type the login details for the boxmgmt user and click **Sign in**.
3. At the upper right of the home page, click the Settings icon, and then click **Collect Logs**.
4. In the **Collect Cluster Logs** dialog box, type start and end times for log collection.
5. If required, under the Advanced section, you may add one or more vRPAs from other clusters to the log collection.
6. To begin the log collection, click **Collect Logs**.

   Depending on the size of the environment, log collection may take several minutes to complete. A message in the **Collect Cluster Logs** dialog box indicates when the log collection is complete. Collected logs are stored in the vRPA file system.
7. To download a log file, click the name of the cluster in the **Location** column of the **Collect Cluster Logs** dialog box.

   This action opens a browser window to the downloadable log file. To download it, click the `.tar` file.

Migrate to IP communication mode

After upgrading to Release 5.1.1 (or later), you can migrate an existing RecoverPoint for VMs iSCSI environment to the IP communication mode.

Before you begin

For more information about the IP communication mode, review the information in the "Splitter communication mode" topic in the planning section of this guide.

Procedure

1. In a web browser, type `https://<cluster_management-ip-address>`. In the vRPA home page, click **RecoverPoint for VMs Deployer**.
2. If prompted, type the login details for the boxmgmt user and click **Sign in**.
3. From the RecoverPoint for VMs Deployer home page, click **Changing splitter communication mode to IP**.
4. In the **Migrate to IP communication mode** dialog box, verify that the listed prerequisites are satisfied. If the environment:
   - Does not satisfy the listed prerequisites, click **Cancel**, and perform the necessary upgrades.
   - Satisfies the listed prerequisites, click **OK**.

   Deployer tries to migrate the environment to IP communication mode.

5. If the migration is:
   - Successful, click **Close**.
   - Not successful, fix the errors that are listed, and retry the migration procedure. If still unsuccessful, collect logs and contact Customer Support.

Results

The environment has successfully migrated to IP communication mode. RecoverPoint for VMs no longer requires iSCSI adapters on the ESXi and you may remove them.

Modify vRPA cluster network settings

Use the Modify vRPA cluster network wizard to change network settings.

Before you begin

To modify the network adapter topology, refer to Modify the network topology on page 39.

Procedure

1. In a web browser, type `https://<cluster_management-ip-address>/WDM` for the vRPA cluster that you want to modify.
2. In the home page, click **RecoverPoint for VMs Deployer**.
3. If prompted, type the login credentials for the boxmgmt user and click **Sign in**.
4. Under **More actions**, select **Modify vRPA cluster network**.
5. Make the desired changes to the **Environment Settings** page. If you have a `.json` configuration file that you want to import, hover over the **Settings** icon and click **Import**.
6. Make the desired modifications changes to the **Network Settings** page.

   Some settings cannot be modified.
7. To apply the changes, click **Modify**. To export a configuration file of the vRPA cluster settings, click the **Settings** icon (upper right), and then click **Export**. This file provides a record of the vRPA cluster configuration.

Modify the network topology

Use this procedure to modify the existing network topology.

Procedure

1. Pause transfer between the production and copies of the consistency groups for the vRPA cluster that you are modifying.
2. From the vSphere Web Client, add the vNIC on all vRPA VMs. Ensure that the type is VMXNET3.
3. Use an SSH client to log in to the vRPA as a boxmgmt user.
   a. Detach the vRPA from the vRPA cluster. From the **Main** menu, select **Cluster operations** > **Detach RPA from cluster**.
   b. From the **Main** menu, select **Setup** > **Modify settings** > **Enter cluster details** > **Network Interface and IPs Configuration**.
   c. Select the network topology that you want to use.

d. Attach the vRPA back to the cluster. From the **Main** menu, select **Cluster operations** > **Attach RPA to cluster**.

4. Repeat step 3 on page 39 for each vRPA in the vRPA cluster.
5. Start transfer between the production and copies of the consistency groups for the modified vRPA cluster.

Add vRPAs to a vRPA cluster

Use this procedure to add a vRPA to an existing vRPA cluster. A vRPA cluster can have up to 8 vRPAs, and new vRPAs must have the same RecoverPoint for VMs ISO image as existing vRPAs.

Procedure

1. In a web browser, type `https://<cluster_management-ip-address>/WDM` for the vRPA cluster to which you want to add vRPAs.
2. In the home page, click **RecoverPoint for VMs Deployer**.
3. If prompted, type the login credentials for the boxmgmt user and click **Sign in**.
4. Under **More actions**, click **Add vRPAs to vRPA cluster**.
5. In the **Add Prerequisites** step, acknowledge that you have met the listed conditions by selecting the checkbox.
6. In the **Add vRPAs** step, select one or more VMs/vRPAs to add to the cluster.
   - New vRPAs must have the same RecoverPoint software ISO image as the existing vRPAs in the cluster.
   - A cluster can have a maximum of 8 vRPAs.
7. In the **vRPA Cluster Settings** and **vRPA Settings** sections, type required information for the vRPAs you are adding.
8. In the **Add vRPAs Progress** step, on reaching 100%, click **Finish** to return to the Home Page.

   If adding a vRPA fails:

   - To identify the cause of failure, review the displayed error messages.
   - To return to the step in the wizard where you can fix the problem, click **Back**. Fix the problem, and then retry the installation wizard from that point.
   - Alternatively, you can retry the operation that failed by clicking **Retry the operation**.
   - If adding a vRPA continues to fail, contact Customer Support.

Remove a vRPA from a vRPA cluster

Use this procedure to remove a vRPA from a vRPA cluster. You cannot remove a vRPA if the cluster has 2 or fewer vRPAs.

Procedure

1. In a web browser, type `https://<cluster_management-ip-address>/WDM` for the vRPA cluster from which you want to remove a vRPA.
2. In the home page, click **RecoverPoint for VMs Deployer**.

3. If prompted, enter the login credentials for the boxmgmt user and click **Sign in**.
4. Under **More actions**, click **Remove vRPA from vRPA cluster**.
   - The highest numbered vRPA (the last one added) will be removed.
   - The consistency groups of the removed vRPA will be non-disruptively moved to a different vRPA.
   - The preferred vRPA setting for those consistency groups will be automatically updated.

Replace a vRPA

Use this procedure and wizard to replace a vRPA with a different vRPA.

Before you begin

This wizard does not support replacing a vRPA within a vRPA cluster that has only one vRPA. If you must replace a vRPA in a single-vRPA cluster, contact Customer Support.

Deploy the new, replacement vRPA with the same IP settings as the faulty vRPA you want to replace. Ensure that the replacement vRPA is shut down. To shut down the replacement vRPA, login as boxmgmt user and select **Main Menu** > **Shutdown / Reboot operations** > **Shutdown RPA**.

Procedure

1. In a web browser, type `https://<cluster_management-ip-address>/WDM` for the vRPA cluster in which you want to replace a vRPA.
2. In the home page, click **RecoverPoint for VMs Deployer**.
3. If prompted, type the login credentials for the boxmgmt user and click **Sign in**.
4. Under **More actions**, click **Replace vRPA**.
5. In the **Prerequisites** step, acknowledge that you have met the listed conditions by selecting the checkbox.
6. In the **Replace vRPA** step, select the vRPA that you want to replace.
7. Select the vRPA you want to add as a replacement.
8. In the **Replacement Progress** step, on reaching 100% click **Finish** to return to the home page.

   If replacing a vRPA fails:

   - To identify the cause of failure, review the displayed error messages.
   - To return to the step in the wizard where you can fix the problem, click **Back**. Fix the problem, and then retry the installation wizard from that point.
   - Alternatively, you can retry the operation that failed by clicking **Retry the operation**.
   - If replacing a vRPA continues to fail, contact Customer Support.

CHAPTER 5

Upgrading RecoverPoint for VMs

Upgrading RecoverPoint for VMs involves downloading the upgrade package and sequentially upgrading the vRPA clusters, the splitters, and the RecoverPoint for VMs plug-in.

Upgrade overview

Upgrade the RecoverPoint for VMs system to a later version by downloading the desired upgrade package. Then upgrade the vRPA clusters, splitters, and RecoverPoint for VMs plug-in.

When upgrading RecoverPoint for VMs, all existing RecoverPoint for VMs settings are preserved. There is no journal loss and no full sweep.

Upgrading RecoverPoint for VMs consists of:

- Downloading the upgrade package
- Upgrading the vRPA clusters
- Upgrading the RecoverPoint for VMs splitters
- Upgrading RecoverPoint for VMs plug-in

After completing the upgrade, observe the following:

- Force the browser to reload updated files. From the Deployer home page, type **CTRL** + **F5**.
- If the environment meets requirements, you can migrate vSCSI splitter-based clusters from iSCSI to IP communication mode.
- Shadow VMs are not required. The copy VM is used in low resources mode. After upgrading to Release 5.1 and later, shadow VMs are automatically removed.

The Upgrade and Maintenance package

Download the RecoverPoint for VMs Upgrade and Maintenance Kit. The Upgrade and Maintenance Kit is a zip file that consists of multiple components required for the upgrade.

Download the RecoverPoint for VMs Upgrade and Maintenance Kit from http://support.emc.com.

Upgrade a vRPA Cluster

The RecoverPoint for VMs Deployer supports non-disruptive upgrades for clusters with two or more vRPAs and enables upgrading an ISO image without re-protecting VMs.

Before you begin

If you are upgrading a cluster that has only one vRPA, the upgrade is disruptive to replication, but the upgrade occurs without full sweep or journal loss. Also, during the vRPA restart, the Upgrade Progress report may not update, and Deployer may become temporarily unavailable. When the vRPA completes its restart, the user can log back in to Deployer and observe the Upgrade Progress to completion.

When you upgrade a cluster that has two or more vRPAs and is connected to a cluster with a single vRPA, a partially disruptive upgrade occurs. When the first vRPA is upgraded, all consistency groups move to another RPA. However, for consistency groups that are replicated in the single vRPA, replication stops while the first vRPA is upgraded.

⚠ CAUTION

Do not attempt to upgrade multiple connected clusters at the same time. This practice is not supported. Rather, upgrade connected vRPA clusters one cluster at a time until all of the connected vRPA clusters are upgraded to the same release.

Procedure

1. In a web browser, type `https://<cluster_management-ip-address>/WDM` for the vRPA cluster that you want to upgrade.
2. In the home page, click **RecoverPoint for VMs Deployer**.
3. If prompted, type the login credentials for the boxmgmt user, and click **Sign in**.
4. Click **Upgrade a vRPA cluster**.

   The wizard performs a system check.
5. In the **Upgrade Prerequisites** step, ensure that you meet the conditions that are listed on the screen. Select the checkbox: **I have fulfilled these conditions**.
6. In the **ISO** step, choose how you want to provide the ISO image for upgrading RecoverPoint for VMs.
7. In the **Change Version Requirements** step, the version requirements file is automatically downloaded and validated to ensure that the system meets the requirements. If the version requirements file fails to download, select one of these options:
   - **Retry downloading the up-to-date requirements from Online Support**
   - **Provide version requirements file manually**
   - **Do not check version requirements**

   Issues that are found are displayed for you to analyze. It is recommended that you fix blocking issues before continuing.
8. In the **System Diagnostics** step, Deployer checks for tweak modifications and signed scripts on the vRPAs. If discovered, these modifications are collected and the user is prompted to send the modifications file to Customer Support for analysis.
9. In the **Upgrade Progress** step, the progress bar displays the replacement progress. On reaching 100%, click **Finish** to return to the Deployer home page.
10. If upgrading fails, review the displayed error message to identify the cause of the failure. To correct the issue and retry the upgrade, click **Back**.

    If upgrading a vRPA continues to fail, contact Customer Support.

Upgrade splitters

Use this procedure to upgrade splitters on the ESXi host.

Before you begin

You may need to enable ESXi Shell and SSH access before proceeding. Refer to VMware documentation for more information.

To keep vRPAs working during the splitter upgrade, ensure that at least two ESXi hosts have an installed splitter.

Procedure

1. On the ESXi host, vMotion all VMs to another ESXi host.
2. At the ESXCLI, enter maintenance mode. From the ESXi host console, use SSH to run the following command:

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

   Note

   For VSAN environments, this command requires an additional switch (refer to the vSphere documentation for the vSphere version that you are using).

3. Remove the old RecoverPoint vSphere Installation Bundle on the ESXi host.

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

4. Install the splitter by using this method:

   a. To copy the RecoverPoint VIB to the `tmp` directory, use an SSH client with secure copy protocol:

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

   NOTICE

   Do not erase the `/scratch` space during the upgrade.

   Example:

   ```
   scp kdriver_RPESX-00.5.0.0.0.0.h.152.000.vib
   root@10.10.10.10:/scratch
   ```

   b. To install the splitter, in the ESXi host console, run the following command:

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

   If installation is successful, the following message appears:

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

   c. Confirm installation of the splitter in the ESXi host console by using 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.

5. On the ESXi host, exit maintenance mode by running the following command:

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

6. vMotion the VMs back to this ESXi host.
7. Repeat this procedure for each ESXi host.

Upgrade the RecoverPoint for VMs plug-in

Use the vSphere Web Client to upgrade the RecoverPoint for VMs plug-in.

Before you begin

The vRPA is backward-compatible, but the RecoverPoint for VMs plug-in is not. New vRPAs work with older plug-ins, but a new RecoverPoint for VMs plug-in might not be able to communicate with older vRPAs. Therefore, the RecoverPoint for VMs plug-in version must correspond with the version of the oldest vRPA cluster.

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

Procedure

1. Access the vSphere Web Client at: `https://<vCenter-ip-address>:9443/vsphere-client/`. In the vSphere Web Client home page, click the **RecoverPoint for VMs** icon.
2. Click the **Help...** link at the top right of the **RecoverPoint for VMs Management** screen, and select **Upgrade RecoverPoint for VMs**.
3. In the **Upgrade RecoverPoint for VMs** window, select the upgrade version and click **OK**.
4. Log out all active user sessions of the vSphere Web Client, and log back in. Verify that the RecoverPoint for VMs plug-in is listed under **Inventories**.
5. If the RecoverPoint for VMs plug-in is not listed under **Inventories**, restart the vCenter Web Client service to ensure that all active user sessions are disconnected.

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

CHAPTER 6

Uninstalling RecoverPoint for VMs

You can uninstall a single vRPA cluster or all vRPA clusters from a vCenter. The uninstall tool scans the vCenter, datastores, and ESXi hosts. It removes vRPAs (production and copy VMs), configuration objects, and repository and journal volumes.

Using the RecoverPoint for VMs Uninstall tool

The Uninstall tool removes vRPA clusters and their configuration entities from a vCenter.

The Uninstall tool has two options:

- `uninstall` - Uninstalls a single vRPA cluster from a vCenter. Use this option to:
  - Replace a Try and Buy or Beta version with a supported production version
  - Remove a vRPA cluster (after data migration)
  - Remove unwanted elements from the vCenter environment
- `full_rp_uninstall` - Uninstalls all vRPA clusters from a vCenter. Use this option to completely remove all RecoverPoint entities and clusters from the vCenter.

What the RecoverPoint for VMs uninstall tool does

The RecoverPoint fo VMs uninstall tool removes vRPAs, shadow VMs, configuration objects, and repository and journal volumes.

Running the RecoverPoint for VMs Uninstall tool does the following:

1. Scans the vCenter, datastores, and ESXi hosts.
2. Displays a list of all detected vRPA clusters and marks them either active or suspected inactive. Active clusters are clusters that have registered vCenter tokens during the last hour.
3. After you select which vRPA clusters the tool should uninstall, the tool removes the following from the selected vRPA clusters: production and replica VMs that were running vRPAs, shadow VMs (if they exist), RecoverPoint configuration objects, and the repository and journal volumes.

In addition to all the actions performed when uninstalling one vRPA cluster, uninstalling all vRPAs removes all vRPA clusters on the selected vCenter with all related elements. It also removes from the vCenter RecoverPoint elements not belonging to a specific vRPA cluster, such as the RecoverPoint vCenter plug-in.

Preparing to uninstall vRPA clusters

Unprotect VMs

To stop replication for a vRPA, unprotect the associated VM.

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.

Remove ESXi clusters from vRPA clusters

Use the vSphere Web Client and this procedure to remove a ESXi cluster from a vRPA cluster.

Procedure

1. In the vSphere Web Client home page, click the **RecoverPoint for VMs Management icon** > **Administration** tab.
2. Click **vRPA Clusters**.
3. Select the relevant vRPA cluster.
4. Click the **ESX Clusters** tab.
5. Click the garbage can icon next to each ESXi cluster to remove that ESXi cluster from the selected vRPA cluster.

Uninstall a vRPA cluster

The Uninstall a vRPA cluster from this system wizard guides you in uninstalling a vRPA cluster. Use the uninstall tool to uninstall the last vRPA cluster.

Before you begin

- You cannot uninstall a cluster from a single-cluster system.
- After you uninstall a vRPA cluster, you cannot reuse the cluster or its vRPAs.
- When you uninstall a vRPA cluster, the vRPAs are shut down and cannot be restored.
- If required, collect logs before you uninstall the cluster. Log collection for the cluster is not possible later.

If you want to remove only one vRPA cluster from a system with two or more clusters, perform these steps from a vRPA cluster that is remaining in the system (and not from the cluster that you want to remove).

If you want to remove all of the vRPA clusters, perform these steps from one of the clusters. The last remaining cluster must be removed by using the uninstall tool.

Procedure

1. In a web browser, type `https://<cluster_management-ip-address>/WDM` for the vRPA cluster that you want to uninstall.
2. In the home page, click **RecoverPoint for VMs Deployer**.
3. If prompted, type the login credentials for the boxmgmt user and click **Sign in**.
4. Under **More actions**, click **Uninstall a vRPA cluster from this system**.
5. Select the vRPA cluster that you want to remove. Click **OK**.

   If cluster removal does not succeed, try again. If cluster removal fails, contact Customer Support.

Results

The vRPA cluster is successfully uninstalled. Continue to the next procedure.

Run the RecoverPoint for VMs uninstall tool

Download the uninstall tool, uncompress the .bat file, and run the tool in the command line.

Before you begin

Obtain the IP and TCP port number of the vCenter (or vCenters) you want to scan, the vCenter username (and domain name, if one exists), and the vCenter password.

System requirements for the computer running the Uninstall tool:

- Microsoft Windows
- Java 7 or higher

Note

If a time difference of more than 30 minutes exists between the vRPA and the computer running the Uninstall tool, the tool may recognize the vRPA cluster as inactive when it is not. (The time difference is not influenced by different time zones.)

Procedure

1. Navigate to the RecoverPoint for Virtual Machines download page under the Tools & Utilities section and click the **RecoverPoint for Virtual Machines Uninstaller Tool** link. The link is also referenced from the Customer Installation kit.
2. From a computer with IP connectivity to the vCenters managing the RecoverPoint VMs you want to uninstall, unzip the zip file.
3. Double click on `uninstaller.bat`.

   The RecoverPoint for VMs Uninstall Tool opens in a command line.
4. Perform one of the following actions:

Option	Description
If uninstalling a single vRPA cluster from a vCenter	...type `uninstall`.
If uninstalling all vRPA clusters from a vCenter	...type `full_rp_uninstall`.

   Type `--h` after a command to view an explanation of that command. Type `help` to view a short explanation of all available commands.
5. Enter the IP address of the vCenter.
6. Enter the vCenter's TCP port number or press Enter for the default port (443).
7. Enter the vCenter's username.
8. Enter the vCenter's password.

   The tool tests connectivity and logs in to the vCenter.
9. Type `y` if you want to add another vCenter. Type `n` if you do not.

   If you have remote vRPA clusters connected to a different vCenter, type that vCenter's IP address if you want to uninstall that cluster as well.

   The tool displays a list of detected vRPA clusters.

10. Perform one of the following actions:

Option	Description
If uninstalling a single vRPA cluster from a vCenter	Type the index number of the vRPA cluster that you want to uninstall. To remove more than one cluster, type the index numbers separated by commas (for example: `1,4,9`).
If uninstalling all vRPA clusters from a vCenter	Type `y` to perform the uninstallation.

Results

The tool begins to scan and uninstall the cluster (or clusters).
If the process notifies you that it did not uninstall all objects, you may run the uninstall operation again.

RecoverPoint splitters are not removed by the uninstall tool. They can be manually removed from each ESXi host. For instructions, see Uninstall the RecoverPoint for VMs splitters on page 53.

Finishing up the uninstall

Uninstall the RecoverPoint for VMs splitters

Use the ESXCLI to uninstall the RecoverPoint for VMs splitters.

Procedure

1. Use ESXCLI to obtain a list of all installed vSphere Installation Bundles (VIBs):

   ```
   esxcli software vib list
   ```

2. Ensure that a bundle named *RP-Splitter* is installed.
3. On the ESXi host, enter maintenance mode:

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

   Note

   For VSAN environments, this command requires an additional switch (refer to the vSphere documentation for the vSphere version that you are using).

4. To uninstall the splitter, type:

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

5. On the ESXi host, exit maintenance mode:

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

Removing unused directories

From the vCenter, remove RecoverPoint for VMs plug-in directories which are no longer being used.

Procedure

1. Connect to the vCenter server (using a local network mapping or Remote Desktop Connection). Delete the following folder:

- vCenter 5.5 and Windows vCenter: `C:\ProgramData\VMware\vSphere Web Client\vc-packages\vsphere-client-serenity\com.emc.recoverpoint.vwc-<version>`
- vCenter 5.5 and vCSA: `/var/lib/vmware/vsphere-client/vc-packages/vsphere-client-serenity/com.emc.recoverpoint.vwc-<version>`
- vCenter 6.0/6.5 and Windows vCenter: `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\com.emc.recoverpoint.vwc-<version>`
- vCenter 6.0/6.5 and vCSA: `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/com.emc.recoverpoint.vwc-<version>`

2. Restart the vSphere Web Client. For instructions, refer to VMware KB1003895 (Windows), VMware KB2109887 (Linux - vCenter 6.x), or VMware KB2147152 (Linux - vCenter 6.5).

CHAPTER 7

Installing in VxRail environments

Installing RecoverPoint for VMs in VxRail environments is similar to a standard installation but includes a few specific requirements for preparing the network, configuring VMkernel ports, creating vRPAs and vRPA clusters, and adding VxRail appliances or nodes.

Deploying RecoverPoint for VMs in a VxRail™ environment

Follow specific guidelines when deploying Recoverpoint for VMs in a VxRail environment.

When deploying RecoverPoint for VMs on VxRail appliances, follow the guidelines in this chapter along with the instructions that are listed in Preparing the network on page 24, Deploy vRPAs on page 30, and Install vRPA clusters on page 31.

Downloading from the VxRail market place

Download the latest qualified RecoverPoint for VMs release from the VxRail manager marketplace.

Preparing the network for VxRail

Prepare the network for the VxRail environment by choosing a network adapter topology and defining the required ports.

VxRail supports adding a PCIe NIC to the node in E, P, S, and V Series. VxRail initialization does not impact the PCIe NIC. You can connect unused ports to the VxRail system vSphere Distributed switch. Alternatively, you can create a vSphere Standard Switch (VSS)/vSphere Distributed switch and connect the unused ports after initialization. The ports are available for uses such as RecoverPoint traffic. VxRail G-Series 2x10G models have only 2x10G ports.

In VxRail 4.0 and later, vSphere Network I/O Control (NIOC) is enabled during initialization, and vSAN traffic has the highest priority to consume the bandwidth in contention. If NIOC is enabled with the default VxRail setting, you can use the vSAN port for other traffic.

The configuration described here uses the G-Series 2x10G model uplink configuration and VxRail system vSphere Distributed switch default name ("VMware HCIA Distributed Switch") as an example. Choose a vSwitch and uplink name according to the VxRail model and uplink configuration.

Prepare the required port groups on the VMware HCIA Distributed Switch.

Procedure

- Use the default configuration of two network adapters (WAN + LAN on one adapter and data on the other) unless required to use a different network adapter topology.
- If using a single network adapter, define one port group: RP_ALL.
- If using four network adapters, define four port groups: RP_WAN, RP_LAN, RP_iSCSI1, RP_iSCSI2.

Create vRPAs for VxRail

Use the OVA file and guidelines in this procedure to create vRPAs for VxRail environments.

When creating vRPAs:

Procedure

- In the **Select storage** screen, in the **VM Storage Policy** drop down, select **MARVIN-STORAGE-PROFILE**. The compatible VSAN datastore will be selected.

- Deploy two vRPAs and configure VM-Host affinity rules to avoid running both vRPAs on the same ESXi node (recommended).

Create and configure VMkernel ports for VxRail

Create and configure VMkernel ports for VxRail environments.

Best practice recommends VxRail deployments use vSCSI splitter with the IP communication mode.
If you are using:

- IP communication mode, do not configure software iSCSI adapters
- iSCSI communication mode, configure software iSCSI adapters on all ESXi nodes

Procedure

1. Create one or two VMkernel ports on each ESXi node by selecting an existing distributed vSwitch "VMware HCIA Distributed Switch."

   A single VMkernel port is required when using the default of two network adapters (WAN + LAN on one network adapter and data on the other network adapter). This configuration is standard. Two VMkernel ports are required when you are using two network adapters for data.

2. To select one network adapter (uplink) as active, override the NIC teaming policy. The other network adapter should be marked as unused.

   When using a single VMKernel port, assign uplink1 to the port and, if using iSCSI communication mode, bind it to the software iSCSI adapter.

   When using two VMkernel ports:

   - Assign uplink1 to one VMkernel port and uplink2 to the second VMkernel port.
   - For uplink2, use traffic shaping to limit bandwidth to no more than 1Gb/s (if NIOC is enabled with the default VxRail setting, traffic shaping is optional):

     a. Locate the port group, right-click it, and select **Edit Settings**.

     b. In the **Edit Settings** window, change traffic shaping for the port group:

Traffic shaping	Field	Value
Ingress	Peak bandwidth (kb/s)	1048576
	Burst size (KB)	102400
Egress	Status	Enabled
	Average bandwidth (kb/s)	1048576
	Peak bandwidth (kb/s)	1048576
	Burst size (KB)	102400

3. If using iSCSI communication mode, bind the VMkernel ports to the software iSCSI adapter.

Create a vRPA cluster for VxRail

Use the Install a vRPA cluster wizard to create a vRPA cluster for the VxRail environment.

When creating a vRPA cluster:

Procedure

- In the **Environment Settings** step, select the vSAN datastore from the table of available datastores.
- In the **Network Settings** step of the wizard, specify the vRPA iSCSI network addresses (and not the VMkernel port IP addresses that were created earlier).

Adding VxRail appliances or nodes

Adding a VxRail appliance or node requires verifying the node addition, configuring ESXi nodes, registering the new ESXi clusters, and adjusting VM-host affinity rules.

After adding a VxRail appliance or a node to an existing appliance:

Procedure

1. Verify that the nodes are added into the same vSAN cluster and under the same vCenter.
2. Configure each ESXi node with the required iSCSI network adapters for enabling splitter-to-vRPA communication.
3. Register the new ESXi clusters within the vRPA cluster.

   This action installs the RecoverPoint for VMs splitters on the new ESXi nodes.
4. Adjust VM-host affinity rules for the vRPAs to ensure that they are running on separate ESXi servers.

CHAPTER 8

Installing in VxRack environments

When deploying Recoverpoint for VMs in a VxRack SDDC environment, follow the specific guidelines in this chapter along with the instructions that are listed in "Preparing the network" on page 24, "Deploy vRPAs" on page 30, and "Install vRPA clusters" on page 31.

See also the instructions in Preparing the network on page 24, Deploy vRPAs on page 30, and Install vRPA clusters on page 31.

Deployment

Note these guidelines when deploying RecoverPoint for VMs in a VxRack environment.

- Provide a dedicated vRPA cluster for each Workload Domain that contains VMs that are to be replicated.
  vRPA clusters can be configured also on the Management Domain.
- Configure the network with three network adapters: LAN, WAN, and Data.

  NOTICE

  Communication between splitters and vRPAs must use IP communication mode.

  - The WAN network must be routed out of the workload domain, to be used for transferring data to a remote copy.
  - The vRPA LAN network adapters must be in the Management network, which is not routable.
    LAN network adapters must communicate with vCenter.
  - The Data network port group must be created on the existing distributed vSwitch. There is one distributed vSwitch per Workload Domain.
    The Data network should not be routable.
  - A single VMkernel port must be configured for each ESXi host, and must be on a separate subnet. It must be associated with the designated Data port group.
  - The VMkernel port must communicate with the vRPA Data network adapters.
  - Overriding the failover and NIC-teaming policy is not required.
- For remote replication, MTU must be consistent end-to-end for network adapters across the WAN network.
  MTU for all vRPA network adapters must be the same as that set by VxRack, which by default is 9000.
- Guidelines that should be followed when deploying the vRPAs in VxRack clusters.
- Configure an anti-affinity rule for each Workload Domain that contains a vRPA cluster.
  The rule ensures that vRPAs will reside on separate hosts, improving both availability of the cluster and resource distribution within the cluster.
- DRS or frequent migration of the vRPAs may have a negative impact on replication performance.
  If your performance needs are high, or your application is very latency-sensitive, configure your DRS policy to minimize vRPA migrations.
- After vRPA cluster creation:
  - In the RecoverPoint for VMs plug-in, register all vCenters in the VxRack SDDC environment.
    This is necessary because VxRack SDDC leverages enhanced link mode.
  - Register the vRPA cluster with the Workload Domain.

Protecting VMs

- Currently, with vSAN, a journal volume has a maximum size of 250 GB. If a consistency group needs a larger journal, you can add volumes to that journal.
- Because vRPAs always reside on the same ESXi cluster with the protected or replica VMs, the journals should be configured on the vSAN datastore of the Workload Domain.

SDDC life cycle procedures

SDDC manager provides an integrated Life Cycle Manager (LCM) utility to orchestrate upgrades of the system components within the environment. LCM is integrated with Dell EMC to enable validated software bundles to be downloaded and staged within the SDDC software repository until they are sheduled for use in updating the systems.

Table 3 on page 61provides a summary of the SDDC components and the impact each has on the RecoverPoint for VMs protection.

Table 3 VxRack Life Cycle Management and RecoverPoint for VMs

SDDC System	Scope of the upgrade	Impact
vCenter	RecoverPoint for VMs UI management	vCenter and primary vRPA management is unavailable during the upgrade process. No impact on protection. Management is possible via Secondary vCenter, if necessary.
Platform Services Controller	Identity access management.	Temporary loss of vCenter access. No impact to protection.
SDDC manager	VCF Management.	No impact to RecoverPoint for VMs.
ESXi	ESXi impacts resources.	Resource limitation during rolling host upgrades. No impact on protection.
vSAN	Resource limitations because hosts are placed into maintenance mode and restarted.	Similar to host upgrade.

Adding a node

Follow this procedure if you want to add compute resources.

Procedure

1. Create a new VMkernel address, and assign it to the RecoverPoint for VMs Data port group.

The Data port group is used by the vRPAs and other ESXi hosts in the environment.

2. Assign an IP address from the defined network to ensure network connectivity between the splitters and vRPAs.

   The splitter is deployed on the host automatically.

3. Connect to vCenter to monitor the host status for the splitter update.

Replacing a node

Follow this procedure to replace a faulty node, or as part of an upgrade.

Procedure

1. Replace the system and re-image with the VMware Imaging Assistance (VIA) using the previously assigned node information.
2. Run Adding a node on page 61 on the new node.

Removing a protected Workload Domain

Use this procedure when reconfiguring or upgrading.

Procedure

1. Because VxRack uses enhanced linked mode, uninstall the vRPA cluster from all vCenters.
2. If the vRPA cluster is connected to other vRPA clusters, disconnect it using the RecoverPoint for VMs Deployer.
3. Uninstall RecoverPoint for VMs. For instructions, see Uninstalling RecoverPoint for VMs on page 49
4. Remove the splitters from the ESXi hosts.
5. If you are removing also a parallel Workload Domain at another VxRack SDDC system, perform the same operation for that VxRack SDDC.

Password rotation

SDDC Manager enforces password rotation policies, especially for the vCenter administrator user. It is therefore advised to create a dedicated RecoverPoint for VMs administrator with vCenter admin role, and to use that user during RecoverPoint for VMs deployment. vCenter credentials can be changed using the RecoverPoint for VMs plug-in.

CHAPTER 9

Troubleshooting RecoverPoint for VMs installation

When the RecoverPoint for VMs installation is not successful, knowing how to troubleshoot the vRPAs, splitters, RecoverPoint for VMs plug-in, and replication helps you to fix the problem.

Troubleshooting vRPAs

This section describes how to troubleshoot these vRPA conditions:

- vRPA is down
- vRPA is detached from cluster
- vRPA does not see storage or splitter

vRPA is down

If a vRPA is down (powered off), check for vRPA errors, vRPA cluster status, and conflicts in the vRPA resource reservation. To investigate the root cause, collect and analyze logs. From the vSphere Web Client, power on the vRPA.

Procedure

1. Check the RecoverPoint for VMs dashboard for Error events indicating that the vRPA is not online.
2. Log in to a surviving vRPA and type the RecoverPoint username and password to log in to the CLI. To check the cluster status, use the `get_system_status` command. Choose to retrieve the status of all categories.
3. Use SSH to log in to the failed vRPA with boxmgmt credentials. Confirm that the failed vRPA cannot be reached.
4. Check any conflicts in the vRPA resource reservation that might have led to the vRPA being powered off. Resolve any issues before proceeding.
5. In the vSphere Web Client, right-click the vRPA that is down and select **All vCenter Actions** > **Power** > **Power On**.
6. To ensure that the vRPA was powered on successfully, monitor the vRPA console in the vSphere Web Client.
7. To investigate the root cause of the vRPA failure, collect logs.

vRPA is detached from the vRPA cluster

If the vRPA is detached from the vRPA cluster, check for vRPA errors and cluster status. Use the boxmgmt menu to log in to the detached vRPA and attach it to the cluster.

Procedure

1. Check the RecoverPoint for VMs dashboard for Error events indicating that the vRPA cannot access storage or communicate with the splitters.
2. Log in to a surviving vRPA and type the RecoverPoint username and password to log in to the CLI. Use the `get_system_status` command to check the cluster status. Choose to retrieve the status of all categories.
3. From the surviving vRPA, use SSH to try logging in to the failed vRPA with boxmgmt credentials.
   a. From the boxmgmt **Main Menu**, select **Diagnostics** > **Run internal command**.
   b. At the prompt, type: **ssh boxmgmt@*<ip_address_of_detached_vrpa>***
   c. Confirm that the vRPA cannot be reached.

4. Log in to the detached vRPA using boxmgmt and select **Cluster operations** > **Attach RPA to Cluster**. To ensure that the vRPA was powered on successfully, monitor the vRPA console in the vSphere Web Client.
5. To investigate the root cause of the vRPA detachment from the cluster, collect logs.
6. If you are using a licensed version of RecoverPoint for VMs, contact Customer Support.

vRPA cannot detect storage or splitter

When a vRPA cannot detect the storage or the splitters, investigate the status of the vRPA and splitters. Collect and analyze the logs.

Procedure

1. Ensure the vRPA is online.
2. Ensure the vRPA is attached to the cluster.
3. Verify that the splitters are running:
   a. Login to ESXi hosts.
   b. Run: `ps |grep kdriver`
   c. Ensure that splitter processes are running.
4. To investigate the root cause of why the vRPA went down, collect logs.
5. If you are using a licensed version of RecoverPoint for VMs, contact Customer Support.

Troubleshooting splitters

The section describes how to troubleshoot the splitter when it is not visible or is in error state.

Splitter is not visible or in error state

To determine why the splitter is not visible or in error, check splitter processes, verify iSCSI software adapter configuration, and investigate logs.

Procedure

1. If possible, vMotion any protected VMs from ESXi hosts with splitters in error state continue or resume replication.
2. Ensure that the splitter processes are running on the host you are troubleshooting:
   a. Login to the ESXi host and use the following command: `ps |grep kdriver`
   b. If processes are not running, place the ESXi node in maintenance mode and restart.
3. Verify Software iSCSI Adapter configuration:
   a. Ensure that the VMkernel ports are bound to the Software iSCSI Adapter on every host in the ESXi cluster.
   b. Verify that the Software iSCSI Adapter sees all paths and vRPA iSCSI targets.

c. Verify that the iSCSI paths to the vRPAs are active and used.

4. Verify that the vRPAs can ping the Software iSCSI VMkernel ports:
   a. Log in to boxmgmt and select **Diagnostics** > **Run Internal Command** > **ping -I eth2 (or eth3)** *<VMkernel IP address>*
   b. If the ping tests fail, validate the IP address, netmask, and gateway assignments on the vRPA iSCSI interfaces and on the Software iSCSI Adapter VMkernel ports.
5. To investigate the root cause of the splitter failure, collect logs.
6. If you are using a licensed version of RecoverPoint for VMs, contact Customer Support.

Troubleshooting the RecoverPoint for VMs plug-in

This section describes how to troubleshoot these conditions:

- vSphere Web client does not contain plug-in
- Plug-in does not see the vRPA cluster

vSphere Web client does not contain plug-in

Go through the following steps until the problem is resolved:

Procedure

1. Log out of vSphere Web client and log back in. Check if the RecoverPoint for VMs plug-in is listed under **Inventories**.
2. If the RecoverPoint for VMs plug-in is not listed, close all active vSphere Web client user sessions. Then check if the RecoverPoint for VMs plug-in is listed under **Inventories**.
3. If the RecoverPoint for VMs plug-in is still not listed, restart the vCenter Web Client service.
4. If the plug-in is still not visible in the vSphere Web Client, validate the vCenter Credentials configuration. You may need to reconfigure vCenter credentials. Consult Customer Support if protected VMs exist.
5. 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.

Plug-in does not detect the vRPA cluster

Go through the following steps until the problem is resolved:

Procedure

1. Log out of the vSphere Web Client and log back in.
2. Refresh the vSphere Web Client.
3. Log out all users from the vSphere Web Client.
4. Restart the vSphere Web Client.
5. Log in to the Managed Object Browser at `https://<vSphere Web Client>/mob`. Ensure the vCenter credentials are configured correctly.

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

6. Restart vRPA1.
7. Restart vRPA2.
8. To investigate the root cause of the vRPA failure, collect logs.
9. If you are using a licensed version of RecoverPoint for VMs, contact Customer Support.

Troubleshooting RecoverPoint for VMs replication

This section describes how to troubleshoot these conditions:

- Consistency group is in high-load transfer state or initialization is not completing
- Consistency group is in error state

CG in high-load transfer state or initialization not completing

Procedure

1. Create an SSH connection to the vRPA management IP address, and type the RecoverPoint username and password to log in to 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 about detecting bottlenecks, see the *RecoverPoint for Virtual Machines Administrator's Guide*.
2. Resolve issues that are highlighted by the `detect_bottlenecks` reports such as WAN or journal issues.
3. If consistency groups are not balanced across vRPAs, create an SSH connection to the vRPA management IP address, and type the RecoverPoint username and password to log in to the CLI. Run the `balance_load` command and change consistency group assignments. For more information about load balancing, see the *RecoverPoint for Virtual Machines Administrator's Guide*.
4. 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 requirements.
5. Check link policies such as compression and deduplication. These policies can add additional load on the vRPA. For more information about these link policies, see the *RecoverPoint for Virtual Machines Administrator's Guide*.
   a. If the consistency group contains more than one VM, consider moving VMs to dedicated consistency groups and using group sets as needed.
   b. Consider adding vRPAs (up to 8) to the vRPA cluster for additional resources.
   c. Review ESXi resources to ensure that there is no contention.
6. If needed, create an SSH connection to the vRPA management IP address, and type the RecoverPoint username and password to log in to the CLI. Run the `config_io_throttling` command to slow down production storage reads during full sweep process.

Consistency group is in Error state

Procedure

1. Perform all of the procedures suggested for a consistency group in high-load state.

2. If the consistency group is still in Error state, try the following:
   a. Check if the image access buffer is full. If so, disable image access.
   b. Resolve any WAN issues.
   c. Check if the consistency group is in a permanent high-load state.
3. To investigate why the consistency group is in error state, collect logs.
4. If you are using a licensed version of RecoverPoint for VMs, contact Customer Support.

Validating ESXi connectivity

During ESXi cluster registration, you can validate iSCSI connectivity issues by clicking the **Validate** wizard. IP connectivity issues are not part of these validations.

Table 4 Validation tests and fixes

Validation test	Description	Fix (manual or automatic)
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 from that node and retry.
All ESXis 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 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: Manually upgrade the ESXi.
Persistent scratch locations are available on all ESXis 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.
iSCSI software adapter that is installed on the ESXi.	To allow the ESXi host to communicate with vRPAs, a software iSCSI adapter is needed on each ESXi host that is running vRPAs.	Pass: There is an iSCSI software adapter that is installed on the ESXi. Error: There is no iSCSI software adapter that is installed on the ESXi. Fix: Automatically install an iSCSI software adapter on the ESXi.

Table 4 Validation tests and fixes (continued)

Validation test	Description	Fix (manual or automatic)
Sufficient vNIC ports available on the ESXi.	Ensure that each ESXi host has a VMkernel port available for iSCSI communication.	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.
Ping to the splitter on the ESXi cluster.	Verifies that there is connectivity to the ESXi's iSCSI VM kernel ports.	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.
No conflicting iSCSI ports binding on all ESXis in the ESXi cluster.	Verifies that there is a supported iSCSI port binding configuration on each ESXi host.	Pass: For each ESXi host, either no port binding is configured or port binding is configured with a single broadcast domain in the target list. Error: for some ESXi hosts, port binding is configured with more than one broadcast domain in the target list. Fix: Manually fix the port biding configuration for relevant ESX hosts (either by removing port binding or by changing targets list).
Splitter connectivity status	Verifies iSCSI connectivity to each ESXi host.	Pass: Successfully communicated with all ESXi hosts in the cluster. Error: Failed to communicate with one or more ESXi hosts in the cluster. Fix: Manually check the iSCSI configuration for all ESXi hosts and/or vRPAs to identify the communication problem.

ESXi UUID duplication

In the VMware environment, each ESXi host is assigned a Universally Unique ID (UUID). RecoverPoint for VMs uses these UUIDs to maintain the integrity of replicated copies and protect the ESXi hosts from data corruption.

However, in some cases, a UUID might change with results that include:

- More than one ESXi host within a cluster reporting the same UUID.
- A single ESXi host reporting a different UUID after host restart (or similar operations).
- A single ESXi host reporting a degenerated UUID with all 0's or F's.

These cases can occur when using hardware that is not certified by VMware because the UUID is based on the BIOS UUID reported by the underlying server hardware. For more information about duplicate UUIDs, see VMware Knowledgebase Article 2006865.

Duplicate or degenerated UUIDs can cause the following:

- The RecoverPoint cluster can experience reboot regulation (vRPAs restarting over and over again until they detach from the cluster).
- The RecoverPoint consistency groups may not be able to recognize, connect to, or communicate with the splitter on the affected ESXi hosts.

RecoverPoint for VMs replaces the use of VMware's ESXi host UUID and creates its own unique identifier, which ensures that no duplicate or degenerated UUIDs exist in the system. The substitution occurs only if the:

- vRPA cluster version supports this feature
- Splitter version supports this feature

For versions that do not support this feature, RecoverPoint for VMs displays a warning about the condition.

Working with vCenter Server Linked Mode

Multiple vCenter Servers can be linked together to share information. The vCenter Server Linked Mode enables users to view and manage inventories of the linked vCenter servers.

When working with vCenter Server Linked Mode, ensure that:

- All vCenter Servers are registered on all vRPA clusters in your RecoverPoint for VMs system.
- ESXi cluster registration is based on the connectivity between vRPA clusters and ESXi clusters in your RecoverPoint for VMs system.

When working with vCenters in Linked Mode, some users may need to run the `register_storage` CLI command to manually register their vCenter. This method requires knowledge of the vCenter certificate locations in Table 5 on page 70:

Table 5 Certificate locations

Version	Certificate location
Windows vCenter 5.1/5.5	`C:\ProgramData\VMware\VMware Virtual Center\ssl\rui.crt`
Windows vCenter 6.0/6.5	`C:\ProgramData\VMware\vCenterServer\cfg\vmware-vpx\ssl\rui.crt`
Linux vCenter 5.1/5.5	`/etc/vmware-vpx/ssl/rui.crt`
Linux vCenter 6.0/6.5	`/etc/vmware-vpx/ssl/rui.crt`

To follow best practices for working with vCenter Server Linked Mode, refer to VMware KB2005481.

To resolve issues related to vCenter Server Linked Mode, refer to VMware KB2031115.

Getting help

Support, product, and licensing information can be obtained as follows:

- Product information — For documentation, release notes, software updates, or information about products, access Online Support at: https://support.emc.com
- Technical support — Access to Online Support and click Service Center. You will see several options for contacting Technical Support. Note that to open a service

request, you must have a valid support agreement. Contact your sales representative for details about obtaining a valid support agreement or with questions about your account.

APPENDIX A

RecoverPoint for VMs installation form

To streamline the installation tasks, create the RecoverPoint for VMs installation form during the planning phase. The installation form is a data sheet or spreadsheet that lists the site-specific values that you require to successfully complete the installation.

Installation data forms

The best practice for successful installations is to collect and document required data before the installation.

The forms that are provided in this section are examples of the types of information you should collect before installation. You can create a planning spreadsheet that matches specific requirements (number of vRPA clusters, network topology, and so forth).

You are directed to type the data from these forms (or similar data sheet) during the installation process.

Table 6 Example: vRPA cluster/site form

vRPA cluster	vRPA cluster 1	vRPA cluster 2	vRPA cluster 3	vRPA cluster 4	vRPA cluster 5
Cluster/site name					
Time zone					
Local domain					
Primary DNS server (optional)					
Secondary DNS server (optional)					
NTP server (recommended)					
Cluster management IP					
Management default gateway IP					
Management subnet mask IP					
WAN default gateway					
WAN subnet mask					
SMTP (optional)					
vCenter IP					
vCenter credentials					
vCenter credentials					
ESXi 1					
_Data1 IP					
_Data2 IP					
_Management IP					
ESXi 2					

Table 6 Example: vRPA cluster/site form (continued)

vRPA cluster	vRPA cluster 1	vRPA cluster 2	vRPA cluster 3	vRPA cluster 4	vRPA cluster 5
_Data1 IP					
_Data2 IP					
_Management IP					

Table 7 Example: vRPA IP form

vRPA	vRPA IPs	Site: _____	Site: _____	Site: _____	Site: _____	Site: _____
vRPA_1	LAN IP					
	WAN IP					
	Data1 IP					
	Data2 IP					
vRPA_2	LAN IP					
	WAN IP					
	Data1 IP					
	Data2 IP					
vRPA_3	LAN IP					
	WAN IP					
	Data1 IP					
	Data2 IP					
vRPA_4	LAN IP					
	WAN IP					
	Data1 IP					
	Data2 IP					
vRPA_5	LAN IP					
	WAN IP					
	Data1 IP					
	Data2 IP					
vRPA_6	LAN IP					
	WAN IP					
	Data1 IP					
	Data2 IP					
vRPA_7	LAN IP					
	WAN IP					
	Data1 IP					

Table 7 Example: vRPA IP form (continued)

vRPA	vRPA IPs	Site: _____	Site: _____	Site: _____	Site: _____	Site: _____
	Data2 IP					
vRPA_8	LAN IP					
	WAN IP					
	Data1 IP					
	Data2 IP					

Table 8 Example: Site map

Site	Site1 (Prod)	Site2 (Remote)	Site2 (Remote)	Site3 (Remote)	Site3 (Remote)
Cluster	Cluster1	Cluster2	Cluster3	Cluster4	Cluster5
vCenter	*<name>* *<ip_address>*	*<name>* *<ip_address>*	*<name>* *<ip_address>*	*<name>* *<ip_address>*	*<name>* *<ip_address>*
ESXi 1	*<name>* *<ip_address>*	*<name>* *<ip_address>*	*<name>* *<ip_address>*	*<name>* *<ip_address>*	*<name>* *<ip_address>*
ESXi 2	*<name>* *<ip_address>*	*<name>* *<ip_address>*	*<name>* *<ip_address>*	*<name>* *<ip_address>*	*<name>* *<ip_address>*
vRPA 1	*<ip_address>*	*<ip_address>*	*<ip_address>*	*<ip_address>*	*<ip_address>*
vRPA 2	*<ip_address>*	*<ip_address>*	*<ip_address>*	*<ip_address>*	*<ip_address>*
Cluster Mgmt	*<ip_address>*	*<ip_address>*	*<ip_address>*	*<ip_address>*	*<ip_address>*
NIC1 IP (WAN)	*<ip_address>* RPA1 *<ip_address>* RPA2	*<ip_address>* RPA1 *<ip_address>* RPA2	*<ip_address>* RPA1 *<ip_address>* RPA2	*<ip_address>* RPA1 *<ip_address>* RPA2	*<ip_address>* RPA1 *<ip_address>* RPA2
Data 1	*<ip_address>* RPA1 *<ip_address>* RPA2	*<ip_address>* RPA1 *<ip_address>* RPA2	*<ip_address>* RPA1 *<ip_address>* RPA2	*<ip_address>* RPA1 *<ip_address>* RPA2	*<ip_address>* RPA1 *<ip_address>* RPA2
Data 2	*<ip_address>* RPA1 *<ip_address>* RPA2	*<ip_address>* RPA1 *<ip_address>* RPA2	*<ip_address>* RPA1 *<ip_address>* RPA2	*<ip_address>* RPA1 *<ip_address>* RPA2	*<ip_address>* RPA1 *<ip_address>* RPA2

APPENDIX B

Support procedures for uninstalling vRPA clusters

When the automated uninstall tool is unavailable, you can manually uninstall a vRPA cluster by using support procedures to guide you.

Uninstalling a single vRPA cluster from a vCenter manually

Perform this procedure to uninstall one vRPA cluster from a vCenter.

Before you begin

Obtain the internal cluster name and iSCSI IP addresses of the vRPA you are uninstalling by connecting to the vRPA as a boxmgmt user and selecting **Main Menu** > **Setup** > **View Settings**.

You must perform this procedure for each vRPA cluster you want to uninstall.

If removing the last vRPA cluster on the vCenter, use the procedure Uninstalling all vRPA clusters from a vCenter manually on page 79 instead of this one.

Procedure

1. If the vRPA cluster is active:
   a. Unprotect the virtual machines. For more information, see Unprotect VMs on page 80.
   b. Remove all ESX clusters from the vRPA cluster. For more information, see Removing ESXi clusters from vRPA clusters. Repeat this step for all ESX clusters in the vRPA cluster.
2. If you are removing just one vRPA cluster from a system with at least two clusters, perform the following procedure: Uninstall a vRPA cluster on page 51.

   If the procedure Uninstall a vRPA cluster on page 51 was successful, skip to step 7 on page 78. If the procedure Uninstall a vRPA cluster on page 51 failed, continue with the next step.
3. Detach the vRPAs from the cluster. For more information, see Detaching vRPAs on page 81.
4. Power off the vRPAs. For more information, see Powering off vRPAs on page 81.
5. Delete the vRPA iSCSI IP addresses of the vRPA you are uninstalling. For more information, see Removing the vRPA iSCSI IPs on page 82.
6. Remove the custom tokens that correspond to the RecoverPoint for VMs cluster ID. For more information, see Removing custom tokens from the Managed Object Browser on page 82.
7. Delete from all datastores the repository folder of the cluster you are uninstalling. For more information, see Deleting the repository folder on page 81.
8. Verify that the configuration parameters are empty. For more information, see Verifying that the configuration parameters are empty on page 81.

   Note

   Perform this step only if you encountered problems when unprotecting the VMs. Performing this step requires downtime of the production VM.
9. Ensure that the vRPA virtual machines are powered off, and delete them.
10. If the ESX cluster you are removing is not registered to any other vRPA cluster, you can uninstall the RecoverPoint for VMs splitter on that ESXi host. For more information, see Uninstall the RecoverPoint for VMs splitters on page 53.

Uninstalling all vRPA clusters from a vCenter manually

Perform this procedure to uninstall all vRPA clusters from a vCenter.

Before you begin

Obtain the internal cluster name and iSCSI IP addresses of the vRPA you are uninstalling by connecting to the vRPA as a boxmgmt user and selecting **Main Menu** > **Setup** > **View Settings**.

You must perform this procedure for each vRPA cluster you want to uninstall.

Procedure

1. If the vRPA cluster is active:
   a. Unprotect the virtual machines. For more information, see Unprotect VMs on page 80.
   b. Remove all ESX clusters from the vRPA clusters. For more information, see Removing ESXi clusters from vRPA clusters. Repeat this step for all ESX clusters in all vRPA clusters.
2. If you are removing just one vRPA cluster from a system with at least two clusters, perform the following procedure: Uninstall a vRPA cluster on page 51.

   If the procedure Uninstall a vRPA cluster on page 51 was successful, skip to step 7 on page 79. If the procedure Uninstall a vRPA cluster on page 51 failed, continue with the next step.
3. Detach the vRPAs from the cluster. For more information, see Detaching vRPAs on page 81.
4. Power off the vRPAs. For more information, see Powering off vRPAs on page 81.
5. Delete the vRPA iSCSI IP addresses of the vRPA you are uninstalling. For more information, see Removing the vRPA iSCSI IPs on page 82.
6. Remove the custom tokens that correspond to the RecoverPoint for VMs Internal cluster name. For more information, see Removing custom tokens from the Managed Object Browser on page 82.
7. Delete from all datastores the repository folders of all clusters. For more information, see Deleting the repository folder on page 81.
8. Verify that the configuration parameters are empty. For more information, see Verifying that the configuration parameters are empty on page 81.

   Note

   Perform this step only if you encountered problems when unprotecting the VMs. Performing this step requires downtime of the production VM.
9. Ensure that the vRPA virtual machines are powered off, and delete them.
10. Unregister the plug-in from the Managed Object Browser. For more information, see Unregistering the plug-in from the Managed Object Browser on page 83.
11. Uninstall the RecoverPoint for VMs splitter. For more information, see Uninstall the RecoverPoint for VMs splitters on page 53.

12. Unregister the RecoverPoint extension from the Managed Object Browser. For more information, see Unregistering the RP extension from the Managed Object Browser on page 83.
13. Remove the RecoverPoint datastore element. Delete the `RecoverPoint.flp` file located in the RecoverPoint folder.

Unprotect VMs

To stop replication for a vRPA, unprotect the associated VM.

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.

Remove ESXi clusters from vRPA clusters

Use the vSphere Web Client and this procedure to remove a ESXi cluster from a vRPA cluster.

Procedure

1. In the vSphere Web Client home page, click the **RecoverPoint for VMs Management icon** > **Administration** tab.
2. Click **vRPA Clusters**.
3. Select the relevant vRPA cluster.
4. Click the **ESX Clusters** tab.
5. Click the garbage can icon next to each ESXi cluster to remove that ESXi cluster from the selected vRPA cluster.

Remove a vRPA from a vRPA cluster

Use this procedure to remove a vRPA from a vRPA cluster. You cannot remove a vRPA if the cluster has 2 or fewer vRPAs.

Procedure

1. In a web browser, type `https://<cluster_management-ip-address>/WDM` for the vRPA cluster from which you want to remove a vRPA.
2. In the home page, click **RecoverPoint for VMs Deployer**.
3. If prompted, enter the login credentials for the boxmgmt user and click **Sign in**.
4. Under **More actions**, click **Remove vRPA from vRPA cluster**.
   - The highest numbered vRPA (the last one added) will be removed.
   - The consistency groups of the removed vRPA will be non-disruptively moved to a different vRPA.
   - The preferred vRPA setting for those consistency groups will be automatically updated.

Detaching vRPAs

Procedure

1. Use an SSH client to connect to a vRPA and enter login credentials for the boxmgmt user.
2. From the **Main Menu**, select **Cluster Operations** > **Detach from Cluster**.

   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**.
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 **Home** > **Storage** > **Manage**.
2. Select the datastore where the repository folder was created.
3. In the list of files displayed in the **Files** subtab, locate and open the `RPvStorage` folder.
4. Within the `RPvStorage` folder, delete all folders and/or files that include the Internal cluster name.

Verifying that the configuration parameters are empty

Note

Performing this task requires downtime of the production VM.

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 not exist or 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 iSCSI IP addresses 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 Internal cluster name. The custom field may have the Internal cluster name in either hexadecimal format, for example, `RecoverPoint.0x2a9c2643b0e5d27a.rpasIscsiDiscoverySet` or decimal format, for example, `config.RecoverPoint_TOKEN; 3070371118132351610` and: `config.RecoverPoint_MeteringInfo; 3070371118132351610`.
5. Click **Invoke Method**.
6. If you are reinstalling several clusters, repeat steps 3 through 5 for each custom field listed in the **Properties** table that corresponds to the Internal cluster names.

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 hosts that are 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-5.0.<x.y>`
   - vCenter 5.1/5.5 and vCSA: `/var/lib/vmware/vsphere-client/vc-packages/vsphere-client-serenity/com.emc.recoverpoint.vwc-5.0.<x.y>`
   - vCenter 6.0 and Windows vCenter: `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\com.emc.recoverpoint.vwc-5.0.<x.y>`
   - vCenter 6.0 and vCSA: `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/com.emc.recoverpoint.vwc-5.0.<x.y>`
6. Restart the vSphere Web Client. For instructions, refer to VMware KB1003895 (Windows), VMware KB2109887 (Linux - vCenter 6.x), or VMware KB2147152 (Linux - vCenter 6.5).

Unregistering the plug-in from the Managed Object Browser

Unregister the RecoverPoint for VMs plug-in from the Managed Object Browser at each vCenter that contains ESXi hosts hosting vRPA clusters. Unregister the plug-in while the vRPAs are detached.

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 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`** for the value and click **Invoke Method**.

Removing unused directories

From the vCenter, remove RecoverPoint for VMs plug-in directories which are no longer being used.

Procedure

1. Connect to the vCenter server (using a local network mapping or Remote Desktop Connection). Delete the following folder:
   - vCenter 5.5 and Windows vCenter: `C:\ProgramData\VMware\vSphere Web Client\vc-packages\vsphere-client-serenity\com.emc.recoverpoint.vwc-<version>`
   - vCenter 5.5 and vCSA: `/var/lib/vmware/vsphere-client/vc-packages/vsphere-client-serenity/com.emc.recoverpoint.vwc-<version>`
   - vCenter 6.0/6.5 and Windows vCenter: `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\com.emc.recoverpoint.vwc-<version>`
   - vCenter 6.0/6.5 and vCSA: `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/com.emc.recoverpoint.vwc-<version>`
2. Restart the vSphere Web Client. For instructions, refer to VMware KB1003895 (Windows), VMware KB2109887 (Linux - vCenter 6.x), or VMware KB2147152 (Linux - vCenter 6.5).

Uninstall the RecoverPoint for VMs splitters

Use the ESXCLI to uninstall the RecoverPoint for VMs splitters.

Procedure

1. Use ESXCLI to obtain a list of all installed vSphere Installation Bundles (VIBs):

   `esxcli software vib list`

2. Ensure that a bundle named *RP-Splitter* is installed.
3. On the ESXi host, enter maintenance mode:

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

   Note

   For VSAN environments, this command requires an additional switch (refer to the vSphere documentation for the vSphere version that you are using).

4. To uninstall the splitter, type:

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

5. On the ESXi host, exit maintenance mode:

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

APPENDIX C

vSphere upgrades

You may be required to upgrade a vCenter or an ESXi host that is used in the RecoverPoint for VMs system. Information about these tasks helps you to successfully perform these upgrades.

Upgrading vCenter

The vCenter upgrade is transparent to RecoverPoint for VMs provided that the upgrade process does not cause a change in the vCenter UUID.

Use this procedure when you need to upgrade the vCenter within a RecoverPoint for VMs system.

During the upgrade:

- vRPA clusters cannot be managed from this vCenter. Ensure you have access to other vCenters.
- Recovery time objective (RTO) and data replication might be affected.
- vCenters in Enhanced Linked Mode might be impacted (one vCenter at a time).
- RecoverPoint for VMs plug-in should remain intact.

Procedure

1. If you are upgrading to vCenter 5.5, follow these best practices: Upgrading to vCenter Server 5.5 best practices.
2. If you are upgrading to vCenter 6.0, follow these best practices: Upgrading to vCenter Server 6.0 best practices.
3. If you are upgrading to vCenter 6.5, follow these best practices: Upgrading to vCenter Server 6.5 best practices.

Results

⚠ CAUTION

If RecoverPoint for VMs is in an error state after you upgrade the vCenter, check if the vCenter UUID has changed. If it has, contact Customer Support to obtain a workaround for restoring normal RecoverPoint for VMs operation.

Upgrading ESXi

Use this procedure when you need to upgrade the ESXi within a RecoverPoint for VMs system. This procedure provides pre-upgrade and post-upgrade instructions when upgrading ESXi. Reference to VMware documentation is provided.

Procedure

1. On the ESXi host, use vMotion to migrate all VMs to a different ESXi host.
2. At the ESXCLI, enter maintenance mode. From the ESXi host console, use SSH to run the following command:

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

   Note

   For VSAN environments, this command requires an additional switch (refer to the vSphere documentation for the vSphere version that you are using).

3. Remove the ESXi host from the cluster.
4. Uninstall the splitter from the ESXi host. Run the following command:

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

5. (Optional) Verify the ESXi version before the upgrade:

   ```
   vmware -lv
   ```

   ```
   VMware ESXi 6.0.0 build-2494585
   VMware ESXi 6.0.0 GA
   ```

6. Login to ESXi KVM.
7. Mount the ISO file to the DVD drive.
8. Reboot the ESXi host (boot it from the mounted DVD).
9. Follow VMware instructions for ESXi upgrade.

Upgrading to 5.5	Methods for upgrading to ESXi 5.5
Upgrading to 6.0	Methods for upgrading to VMware ESXi 6.0
Upgrading to 6.5	Upgrading ESXi hosts (to ESXi 6.5)

10. (Optional) Verify the ESXi version after the upgrade:

    ```
    vmware -lv
    ```

11. Move the ESXi back to the ESXi cluster.
12. Confirm that the splitter is installed. From the ESXi host console, use SSH to run this command:

    ```
    esxcli software vib list
    ```

    The RecoverPoint for VMs splitter installation bundle name appears at the top of the list.
13. Use vMotion to migrate the VMs back to this ESXi host.

APPENDIX D

Configuring iSCSI communication

If the environment supports it, IP communication mode is preferred. Otherwise, iSCSI mode is required. Tasks involved in configuring iSCSI communication include adding iSCSI software adapters, setting up VMkernel ports, and optionally binding the ports to the adapters.

Adding the iSCSI software adapter

Adding an iSCSI software adapter is the first step in establishing iSCSI communication between the splitters and the vRPAs.

Procedure

1. At the vSphere Web Client, under **Inventory Trees**, select **Hosts and Clusters**.
2. For each ESXi host, click **Manage** > **Storage** > **Storage Adapters**.
3. To add an iSCSI software adapter, click the **Add** icon and confirm the selection.

   The iSCSI software adapter appears in the list of storage adapters. The vRPA iSCSI target ports will automatically be discovered after RecoverPoint for VMs has been installed and the ESXi cluster is registered.

After you finish

Set up the VMkernel ports. See Set up VMkernel ports on page 24.

Binding VMkernel ports to iSCSI software adapters

If VMkernel ports and vRPA iSCSI ports are on the same broadcast domain and IP subnet, you must bind the VMkernel ports to the iSCSI software adapters.

Before you begin

Set up the VMkernel ports. See Set up VMkernel ports on page 24.

For more information about iSCSI VMkernel port binding, refer to VMware KB2038869.

Procedure

1. Determine whether port binding is needed. If the iSCSI VMkernel ports and the vRPA iSCSI ports are on:

Option	Description
Different subnets/broadcast domains Example: vRPA iSCSI vNICs on subnet 192.168.1.x and ESXi VMkernel ports subnet 172.30.90.x	Do not use port binding. Skip this procedure.
The same subnet/broadcast domain Example: vRPA iSCSI vNICs on subnet 192.168.1.x and ESXi VMkernel ports also on subnet 192.168.1.x	Bind the VMkernel ports to the software iSCSI adapter. Continue to use this procedure.

2. If port binding is needed, bind the VMkernel ports to the software iSCSI adapters:
   a. In the vSphere Web client, select the ESXi host and click **Manage** > **Storage** > **Storage Adapters**.
   b. Select the iSCSI software adapter. In the **Adapter Details** section, select the **Network Port Binding** tab, and click the **Add** icon.
   c. Select a VMkernel adapter to bind with the iSCSI adapter and click **OK**.

d. Perform a full rescan on the ESXi host.

e. Repeat this step for each ESXi host in the ESXi cluster.

Results

VMkernel ports are bound to the iSCSI software adapters. 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 RecoverPoint for VMs is installed. The targets are automatically added when the ESXi cluster is registered.

APPENDIX E

Installing on Nutanix

Before you can install RecoverPoint for VMs on Nutanix, you must manually edit the settings for storage containers that are to be used by RecoverPoint for VMs.

Installing RecoverPoint for VMs on Nutanix

You must manually modify settings for Nutanix containers that will be used by RecovePoint for VMs before you install your RecoverPoint for VMs system.

Before you begin

RecoverPoint for VMs is supported by Nutanix AOS 4.7.5 or 5.0.2, or later. If necessary, upgrade your Nutanix installation to one of those versions.

Procedure

1. To properly modify the Nutanix container settings, follow the instructions in Dell EMC Knowledge Base Article 495379 and its attachments.
2. Perform a normal Installlation of your RecoverPoint for VMs system, version 5.1.1 or later.