Dell RecoverPoint for Virtual Machines 6.0.3

Installation and Deployment Guide

October 2025
Rev. 02

Notes, cautions, and warnings

ⓘ **NOTE:** A NOTE indicates important information that helps you make better use of your product.

△ **CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

⚠ **WARNING: A WARNING indicates a potential for property damage, personal injury, or death.**

© 2020 - 2025 Dell Inc. or its subsidiaries. All rights reserved. Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Contents

Figures

Tables

Preface

As part of an effort to improve product lines, we periodically release revisions of software. Therefore, some functions described in this document might not be supported by all versions of the software 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** (Dell Support) to ensure that you are using the latest version of this document.

Purpose

This document describes how to install and configure a Dell 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:

- *Dell RecoverPoint for Virtual Machines Release Notes*
- *Dell RecoverPoint for Virtual Machines Quick Start Installation Poster*
- *Dell RecoverPoint for Virtual Machines Installation and Deployment Guide*
- *Dell RecoverPoint for Virtual Machines Scale and Performance Guide*
- *Dell RecoverPoint for Virtual Machines Product Guide*
- *Dell RecoverPoint for Virtual Machines HTML5 Plugin Administrator's Guide*
- *Dell RecoverPoint for Virtual Machines CLI Reference Guide*
- *Dell RecoverPoint for Virtual Machines Security Configuration Guide*
- *Dell RecoverPoint for Virtual Machines RESTful API* at Explore APIs

In addition to the core documents, we also provide white papers, technical notes, and demos.

Typographical conventions

This document uses the following style conventions:

Table 1. Style conventions

Formatting	Description
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

Table 1. Style conventions (continued)

Formatting	Description
	- 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 that is omitted from the example.

Product documentation

- For release notes and user guides, go to **Online Support** at Dell Support.
- For API documentation, see Dell Developer Portal.

Product information

For documentation, release notes, software updates, or information about products, go to **Online Support** at Dell Support.

Where to get help

Go to **Online Support** at Dell Support and click **Contact Support**. 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.

Where to find the support matrix

Consult the **Simple Support Matrix** for RecoverPoint for Virtual Machines at E-Lab Navigator.

Your comments

Your suggestions help Dell Technologies continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to Content Feedback Platform.

Internationalization and localization

The *HTML5 Plugin Administrator's Guide* is available only in English. The vSphere Web Client Flex plugin is also available only in English.

The following documents are available in English, Simplified Chinese, Japanese, Korean, German, French, Latin-American Spanish, and Brazilian Portuguese:

- *Dell RecoverPoint for Virtual Machines Installation and Deployment Guide*
- *Dell RecoverPoint for Virtual Machines Quick Start Installation Poster*
- *Dell RecoverPoint for Virtual Machines Release Notes* **New features** section.

1

Introduction to RecoverPoint for Virtual Machines

RecoverPoint for Virtual Machines is a virtualized solution that provides data replication, protection, and recovery within the VMware vSphere environment.

Definition of key terms and a system diagram helps you to understand the system operation.

Topics:

- RecoverPoint for VMs system

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. Create the vRPAs you need by using the vSphere Client or vSphere Web Client from the vCenter Server.

vRPA cluster
A group of up to 6 vRPAs that work together to replicate and protect data. You create the vRPA clusters, and then connect them to the system by using the RecoverPoint for VMs Deployer wizards.

RecoverPoint for VMs plug-in
The vSphere Client (HTML5). The HTML5 plug-in is installed after the plug-in server is deployed and configured.

RecoverPoint for VMs plug-in server
A dedicated VM deployed from an OVA template that provides replication management over one or more RecoverPoint for VMs systems that are hosted on the same vCenter Server. The plug-in server provides a single endpoint for the vSphere HTML5 plug-in, and the REAPER API.

RecoverPoint for VMs splitter
Proprietary software that is installed on every ESXi host in an ESX cluster that is involved in RecoverPoint replication or running virtual RPAs. It intercepts every write for a protected VM and sends a copy of the write to the assigned vRPA and then on to one or more designated storage volumes. The filter is automatically installed on every ESXi host in the ESX cluster where the vRPA cluster resides as part of the vRPA cluster deployment, or is automatically installed on ESXi hosts as part of any additional ESX clusters that are registered to the vRPA cluster.

RecoverPoint for VMs JIRAF
Proprietary software that is installed on every ESXi host in an ESX cluster running virtual RPAs. Journal I/O and Repository Access Filter (JIRAF) facilitates I/O access to the journal and repository VMDKs. The JIRAF filter is installed on every ESXi host in the ESX cluster where the vRPA cluster resides as part of the vRPA cluster deployment.

RecoverPoint for VMs system
One or more connected vRPA clusters.

RecoverPoint for VMs system provides a reference diagram that shows the vRPAs and vRPA clusters within the RecoverPoint for VMs system, including the RecoverPoint for VMs Plugin Servers. The diagram shows how these components interconnect within the VMware vSphere environment.

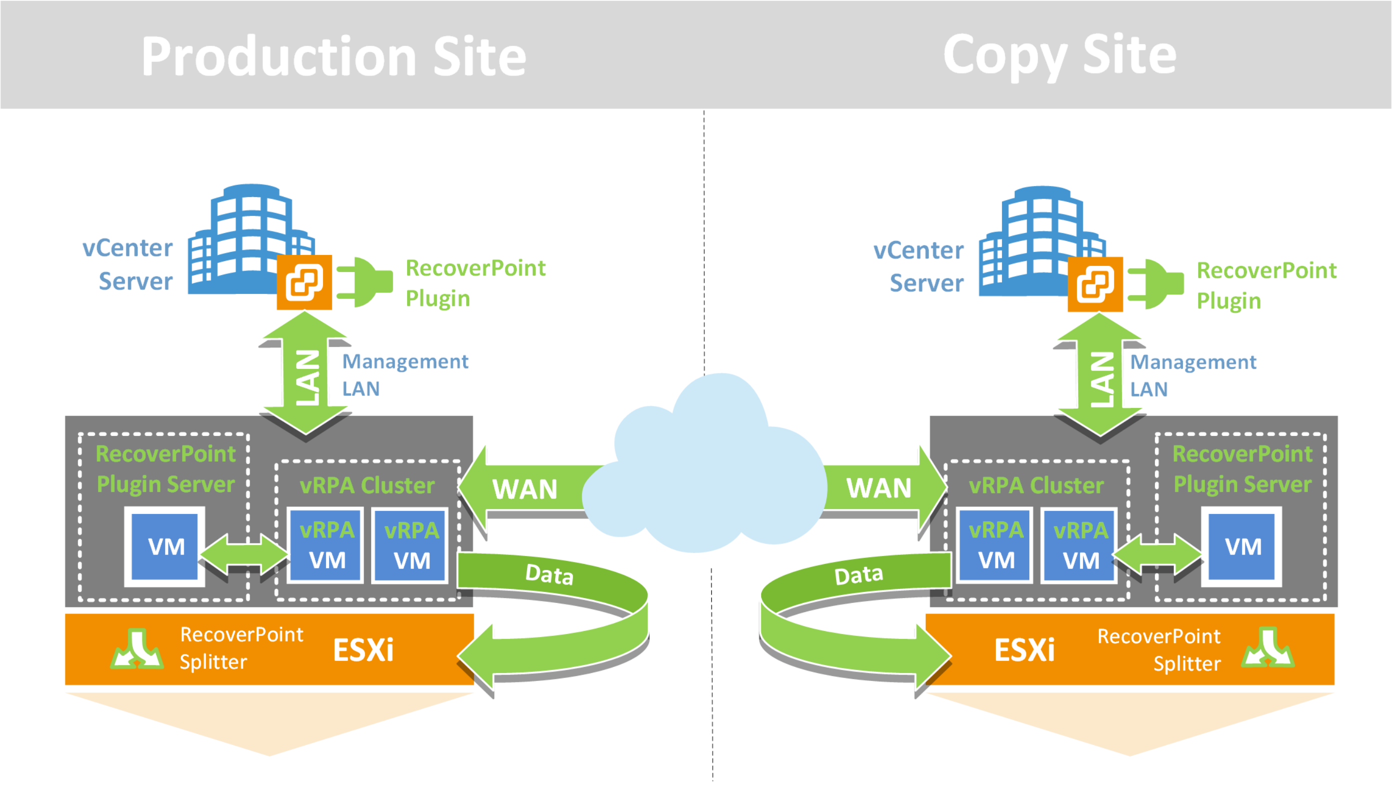


Figure 1. RecoverPoint for VMs system

2

Preparing to install RecoverPoint for VMs

Guidelines help you choose the number of vRPAs and vRPA clusters, vRPA performance profile, and network adapter topology.

Preparing the VMware network and determining storage capacity sets the stage for a successful installation.

Topics:

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, Networking example 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 help you to plan a system that meets your specific requirements.

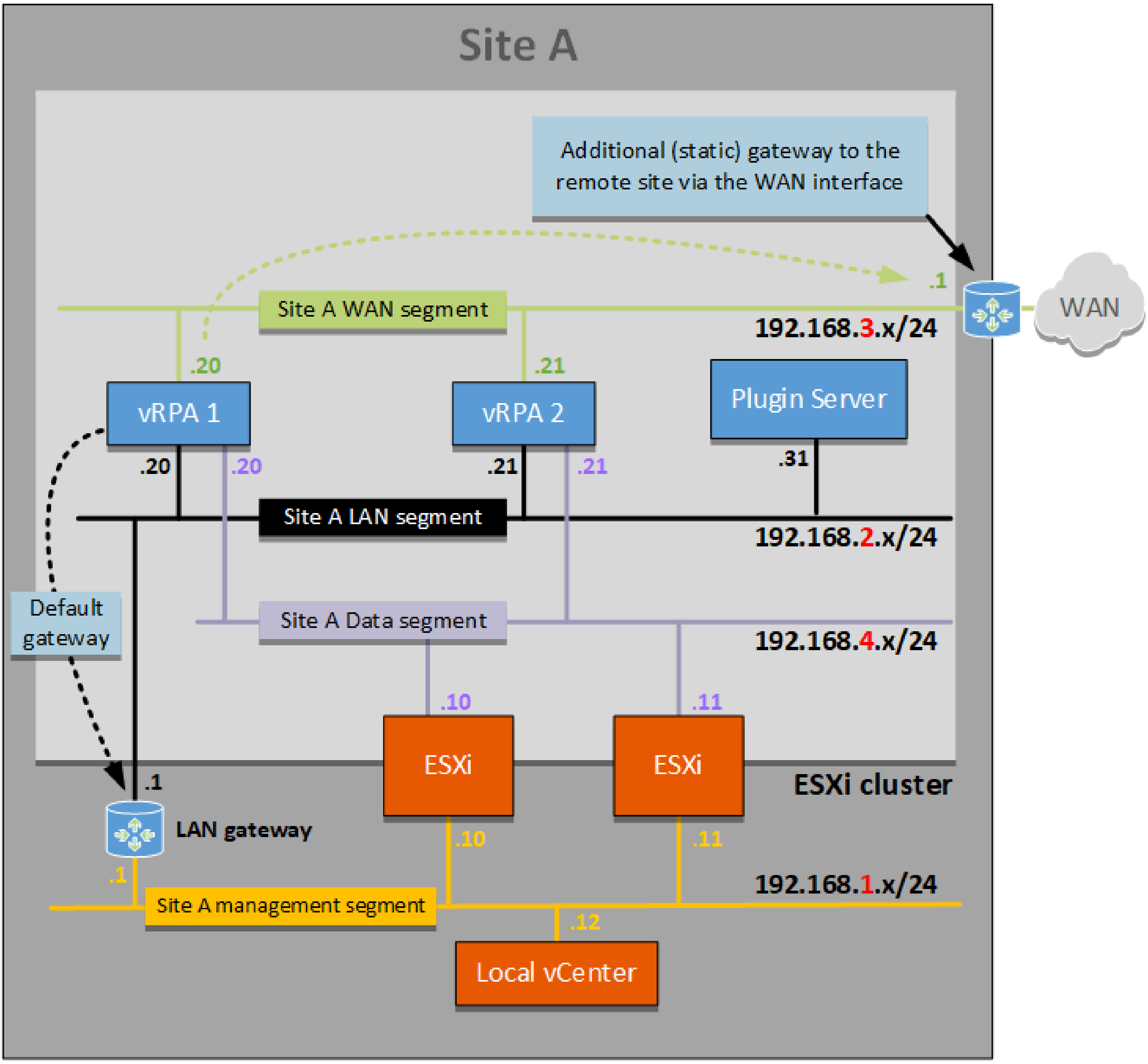


Figure 2. Networking example

System limitations

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

Successful operation of RecoverPoint for VMs depends on a persistent scratch location 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)
- An IP address for each VMkernel port
- An IP address for each plugin server
- An IP address for the NTP server (recommended)
- An IP address for the primary and secondary DNS servers (optional)

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 for examples.

Adhere to a consistent naming and numbering convention for the components of the RecoverPoint for VMs system. For example, use the following format for each vRPA:

*<vRPA_cluster_name>*_vRPA-*<n>*, where n=1, 2, ... 6, and where there are between 1 and 6 uniquely named clusters.

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 protection requirements, 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.

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.

How many vRPA clusters?

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

For most installations, you 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).

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 virtual CPUs and 16 GB 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 deploy a higher specification vRPA or change the resource allocation later by using the vSphere Client or vSphere Web Client.

Decide which of these vRPA performance profiles you need:

- 2x virtual CPUs / 16 GB RAM
- 4x virtual CPUs / 16 GB RAM
- 8x virtual CPUs / 16 GB RAM

For all profiles, each vRPA VM has a 70 GB VMDK capacity.

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

> **NOTE:** By default, all RAM is reserved and vCPU reservation is set to 3400MHz. Any change to these defaults may impact performance.

If required, you can add more memory and CPU resources after initial OVA deployment. For each vRPA, power off the vRPA, select Edit Settings for the vRPA VM, and add the needed resources.

I/O throttling

I/O throttling is used to slow down storage reads that are part of any initialization process including the initial full synchronization (full-sweep).

I/O throttling mitigates the negative impact of initialization on production performance. As a result, however, the initialization process may take longer than expected.

You can use the `config_io_throttling` Sysmgmt CLI command to set the I/O throttling setting.

For more information about I/O throttling, see the *RecoverPoint for Virtual Machines CLI Reference Guide*.

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, you should separate the LAN and WAN interfaces from the data interfaces (recommended for most installations). Place each network interface on a separate virtual switch and on a separate physical network interface for the highest performance.

When using multiple network adapters, each adapter should be assigned an IP on a different subnet. This is particularly relevant to the data interface(s). Assigning adapter IPs on the same subnet can cause connectivity issues that result in packets being sent through the wrong interface. If necessary, combine multiple adapters according to your preferred network topology.

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
Two network adapters (the	● WAN + LAN combined, Data separated ● Better performance, high availability

default and recommended configuration)	
Two network adapters	● LAN + Data combined, WAN separated ● Better performance, high availability ● DHCP for LAN is not supported.
Three network adapters	● WAN, LAN, and Data separated ● Better performance, high availability ● DHCP for LAN is not supported.
Four network adapters	● WAN and LAN separated, Data separated on two dedicated network adapters ● Compatible with previous releases ● Best performance and high availability. Use different subnet masks for the two Data IP addresses. ● DHCP for LAN is not supported.

NOTE: IPv6 is supported on vRPA LAN and WAN interfaces, but not on vRPA Data interfaces.

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 address.

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

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 Dell Support.

Preparing the network

The RecoverPoint for VMs splitter communicates with the vRPAs through a VMKernel port. Setting up separate 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. Avoid using the same subnet that is used also for high availability (vMotion) and hosts (applications).

Depending on your existing network, you may not need to configure any additional VMkernel ports, or if so, you can do so later from the RecoverPoint for VMs plug-in, even after you have protected VMs and are ready to begin replication. RecoverPoint for VMs informs you after protection if there are possible communication issues between vRPAs and splitters. When needed, RecoverPoint for VMs assists in automatically creating VMkernel ports for all the ESXi hosts in the ESX cluster. The procedure is described in the *RecoverPoint for Virtual Machines HTML Plugin Administrator's Guide*.

Alternatively, you can configure VMkernel ports manually by following the procedure in Configure 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.

Establishing vCenter-to-vRPA communication

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

Steps

- Ensure that you open port 443 between the vCenter Server and the vRPAs in both directions, and port 7225 in the vCenter Server-to-vRPAs direction only.
- Ensure that ESXi clusters can communicate with their vRPA targets. Configure the ESXi firewall profile to allow communication through the network.
- See *RecoverPoint for Virtual Machines Security Configuration Guide* for more information.

Plugin server communication

This topic contains checklists for setting up plugin server communication.

- Ensure that port 443 is open for bi-directional communication between the plugin server and the vCenter Server.
- Ensure you open port 9443 for plugin server-to-vRPA communication.

See *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, contact your Dell Technologies Account Team.

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
- 70 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 500 MB of free storage space on a permanently available persistent storage device.

NOTE: Each ESXi host should have its own dedicated datastore for the scratch directory.

For additional guidelines and sizing tools, contact Customer Support.

NOTE:

- RDM support is no longer available; instead, vRDM is supported.

Secure boot considerations

RecoverPoint for VMs version 6.0 supports secure boot. If secure boot is enabled on your ESXi hosts ensure that you install RecoverPoint for VMs 6.0 or later.

Understanding the installation flow

Understanding the stages of the installation work flow helps you to successfully install the RecoverPoint for VMs system, so that your system is ready for protecting VMs.

The Stages of installation flow figure shows the major stages of the installation flow. The Procedures in the installation flow table provides details of the required procedures for each stage of the installation flow.

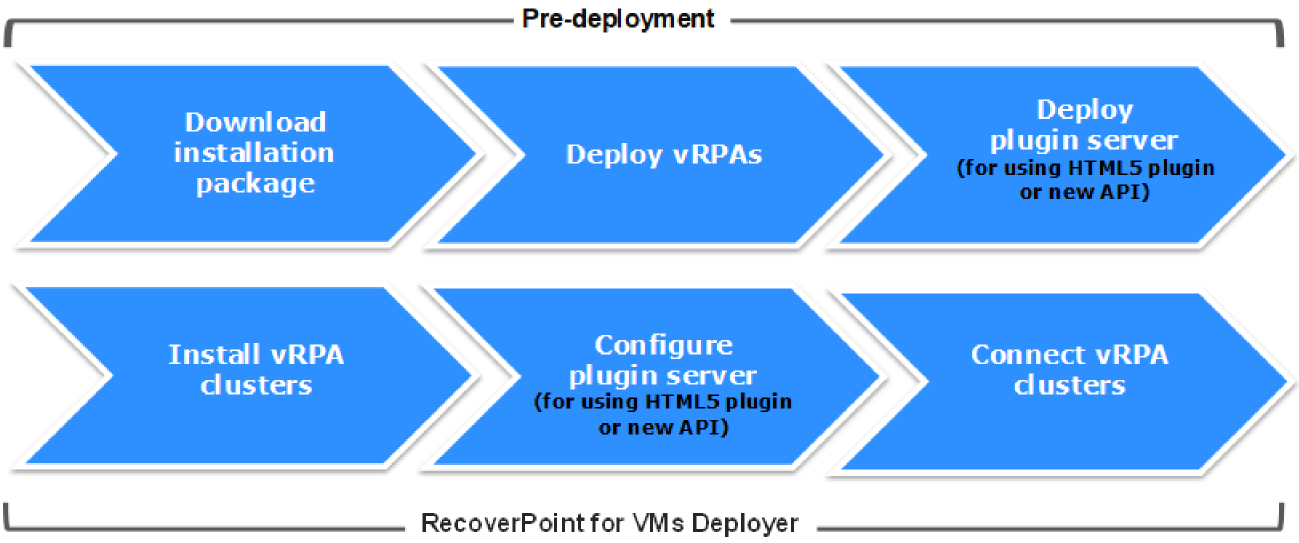

Pre-deployment
Download installation package
Deploy vRPAs
Deploy plugin server (for using HTML5 plugin or new API)
Install vRPA clusters
Configure plugin server (for using HTML5 plugin or new API)
Connect vRPA clusters
RecoverPoint for VMs Deployer

Figure 3. Stages of the installation flow

Table 2. Procedures in the installation flow

Stage of installation flow	Sequence of procedures in the installation flow	Interface
Download installation package.	Download the installation package	Online support site
Deploy vRPAs	Deploy vRPAs	vSphere Client, vSphere Web Client
Deploy plug-in server.	Deploy the plugin server	vSphere Client
Install vRPA clusters.	Install vRPA clusters	RecoverPoint for VMs Deployer
Configure plug-in server.	Configure plugin server	RecoverPoint for VMs Deployer
Connect vRPA clusters.	Connect vRPA clusters	RecoverPoint for VMs Deployer

Use the RecoverPoint for VMs plug-in for the vSphere Client (HTML5) to make final preparations for protecting VMs, including registering and licensing the system, and creating any required VMkernel ports (Completing installation of the RecoverPoint for VMs system).

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. In the RecoverPoint for VMs plugin for vSphere Client (HTML), it also involves installing and configuring a plugin server.

Topics:

Download the installation package

Download the installation software kit and extract the contents of the .zip file.

About this task

ⓘ **NOTE:** Try and Buy customers can download the latest RecoverPoint for VMs trial version from Software Downloads.

Steps

1. Browse to Dell Support.
2. Perform a search in the **Identify your product** 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. Extract the .zip file.

   The .zip file contains the OVA and ISO files that are needed for the installation.

   From RecoverPoint for Virtual Machines 6.0, SRO signature protects the OVA file and GPG signature protects the ISO file. If you want to verify a signature, see Verifying signatures.
5. Obtain documentation for RecoverPoint for Virtual Machines.
6. Continue to Deploy vRPAs.

Verifying signatures

Use the relevant procedure to verify a signature that is attached to an OVA or ISO file that you downloaded from the RecoverPoint for VMs downloads page.

Verifying the SRO signature of an OVA file

During deployment, the OVA deployment wizard automatically verifies the signature that was applied to the OVF package using the certification file provided by SRO.

You can verify the signature also manually in either of the following ways:

- Inspect the file, and compare with the signature.

- Run: `ovftool --machineOutput file.ova | grep -A40 CertValidate`

Verifying the GPG signature of an ISO file

Follow this procedure to verify the GPG signature on your ISO file:

1. To import the Public Key, run: `bash-4.4# gpg --import pubkey.gpg`
   - GPG acknowledges the successful import of the Public Key.
2. To verify the signature, run: `bash-4.4# gpg --verify rp.iso.sig rp.iso`
   - GPG confirms that the signature is good.

NOTE: It is not recommended to having a mixed version of RPA. Make sure to use the same version of RPA in al the sites.

Deploy vRPAs

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

Prerequisites

Ensure that you have completed:

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

Steps

1. In the vSphere Client (HTML5), right-click an ESX cluster, and select **Deploy OVF Template...**.
2. In the **Select an OVF template** screen, either enter a URL from which to download the OVF package from the Internet, or choose a location from which to access the file locally.
3. 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.
4. In the **Select Compute resource** screen, specify the vRPA OVF package location.
5. In the **Review details** screen, review the general properties of the OVF template. To accept, click **Next**.
6. In the **Accept License Agreements** screen, if you accept the terms of the End-User License Agreement, click **Accept** and **Next**.
7. In the **Select configuration** screen, select the desired vRPA performance profile.
8. If prompted to select a resource, in the **Select a resource** screen, select a cluster, host, or resource pool.
9. 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.

   Do not deploy the vRPA on a local datastore.
10. In the **Setup networks** screen, select a destination network for the **RecoverPoint Management Network**, and select an IP protocol.
11. 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.
12. 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.
13. Power on the vRPA VM.
14. To create additional vRPAs, repeat this procedure.

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.

Next steps

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

When you finish creating vRPAs, continue to "Deploy the plugin server".

Deploy the plugin server

Deploy an OVA to create a plugin server.

Prerequisites

Ensure that you have completed the preparations for installation.

Steps

1. Log in to the vSphere client, and then click **LAUNCH VPSHERE CLIENT** to launch the HTML5-based vSphere client.
2. In the vSphere Client, right-click the ESX cluster and select **Deploy OVF Template**.
   The Deploy OVF Template screen opens.
3. In the **Select an OVF template** screen, select an OVF template for the vSphere plugin server from a remote URL or local file system.
4. In the **Select a name and folder** screen, specify a unique name for the plugin server, and select the location of the virtual machine on which you want to deploy your plugin server.
5. In the **Select a compute resource** screen, select the destination compute resource for this operation.
6. In the **Review details** screen, review the general properties of the OVF template. To accept, click **Next**.
7. In the **Select storage** screen, select the storage for the configuration and disk files including the virtual disk format and VM storage policy.
8. In the **Select networks** screen, select a destination network for each source network.
9. In the **Customize template** screen, customize the deployment properties of this software solution.
   a. Select the time zone.
   b. The network management default is DHCP. If you are managing your network using static IP configuration, values for the gateway, netmask, and IP address are mandatory. Values for DNS and FQDN are optional, but entering a DNS address is recommended.
10. In the **Ready to complete** screen, review the details of the deployment and, when satisfied, click **FINISH** to create the plugin server.
    To track that the plugin server creation is successful, check for an OVF deployment in the Recent Tasks window of the vSphere Client.
11. Power on the plugin server VM.

Next steps

After installing a vRPA cluster, you should configure this plugin server with the vCenter on which the vRPA cluster resides.

Repeat the above steps to create a plugin server for another vCenter, either at this site or on a different site .

Install vRPA clusters

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

Prerequisites

- If you have changed the default plugin server certificate and have not yet configured the plugin server, perform Changing the plugin server certificate.
- If you have changed the default plugin server certificate and have already configured the plugin server, perform Changing a registered plugin server certificate.
- Get the Installation data forms that you created when planning the system ready so that when you are prompted to type data, you can consult them.

About this task

ⓘ **NOTE:** During vRPA cluster installation, the RecoverPoint for VMs splitter and jiraf are automatically installed on all ESXi hosts that belong to ESXi clusters on which vRPAs are running.

ⓘ **NOTE:** For RecoverPoint for Virtual Machine 6.0 or later deployment, do not use esxcli command to install, remove, or upgrade IOFilters from the ESXi.

ⓘ **NOTE:** Using the esxcli command for installing, removing, or upgrading IOFilters, corrupts the environment and may cause events like IOFilter crash.

Steps

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 Client or vSphere Web Client by selecting the vRPA and clicking the **Summary** tab.
2. If prompted, type the login credentials for the admin 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 must be validated manually to ensure that the system meets the requirements .

   On the Version Requirements page, the following options are prompted, select one of these options:

   - **Provide version requirements file manually**
   - **Do not check version requirements**

   If **Provide version requirements file manually** option is selected, users must manually download the `cca.xml` file from the support site and upload it to the WDM portal and click Next to continue.

   For the **Do not check version requirements** option, the user can click **Next** to continue.

   ⓘ **NOTE:** To obtain the version requirements file, browse through Dell Product Support. This page provides an option to download or email the `thea-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. Trust the VIB URL as displayed in WDM by seeing Trust Splitter and Jiraf vSphere Installation Bundle (VIB) URLs in vCenter. Click **Connect**.
6. 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 SSL certificate and click **Confirm**.
7. 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.
8. On the **Environment Settings** page, define the required settings.
   - Type a name for the vRPA cluster.
   - To align with security best practices, replace the default admin user password with a new unique password.

     ⓘ **NOTE:** The admin user (with the administrator role) is authorized with all access permissions for managing your RecoverPoint for VMs system. Use the same admin password for all vRPA clusters in a system, and all vRPA clusters under the same vCenter Server. The password for the admin user also serves as the password for the root user across all vRPAs in the system.

   - Type IP addresses for DNS and NTP servers.

     ⓘ **NOTE:** If you have a cloud copy, all vRPAs must be able to resolve amazonaws.com addresses, so all vRPA clusters require an appropriately configured DNS server. See the *RecoverPoint for VMs Cloud Solutions Guide* for more information.

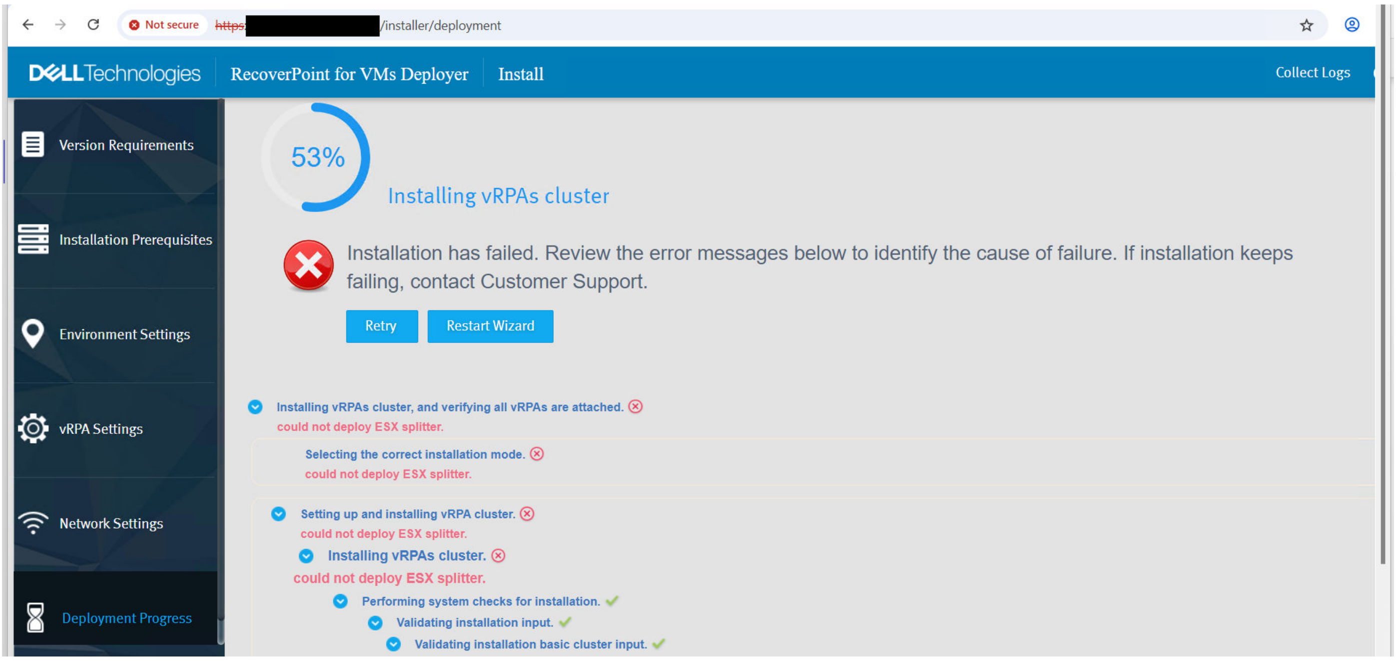
9. On the **vRPA Settings** page:

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.

10. 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 19191 for more information.
11. Click **Install** to initiate completion of the vRPA cluster installation.

    You can follow progress of the installation on the **Deployment progress** page.

NOTE: If a single image is enabled on the ESXi cluster where vRPA is deployed, the installation fails at 53%.

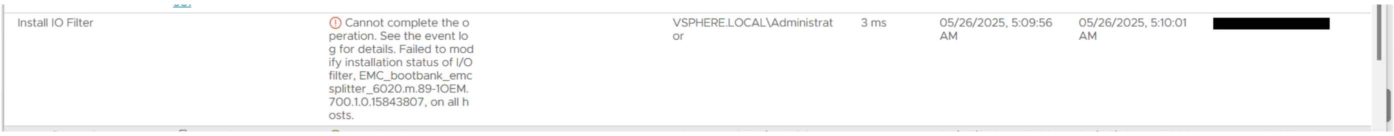


Installing vRPAs cluster

Installation has failed. Review the error messages below to identify the cause of failure. If installation keeps failing, contact Customer Support.

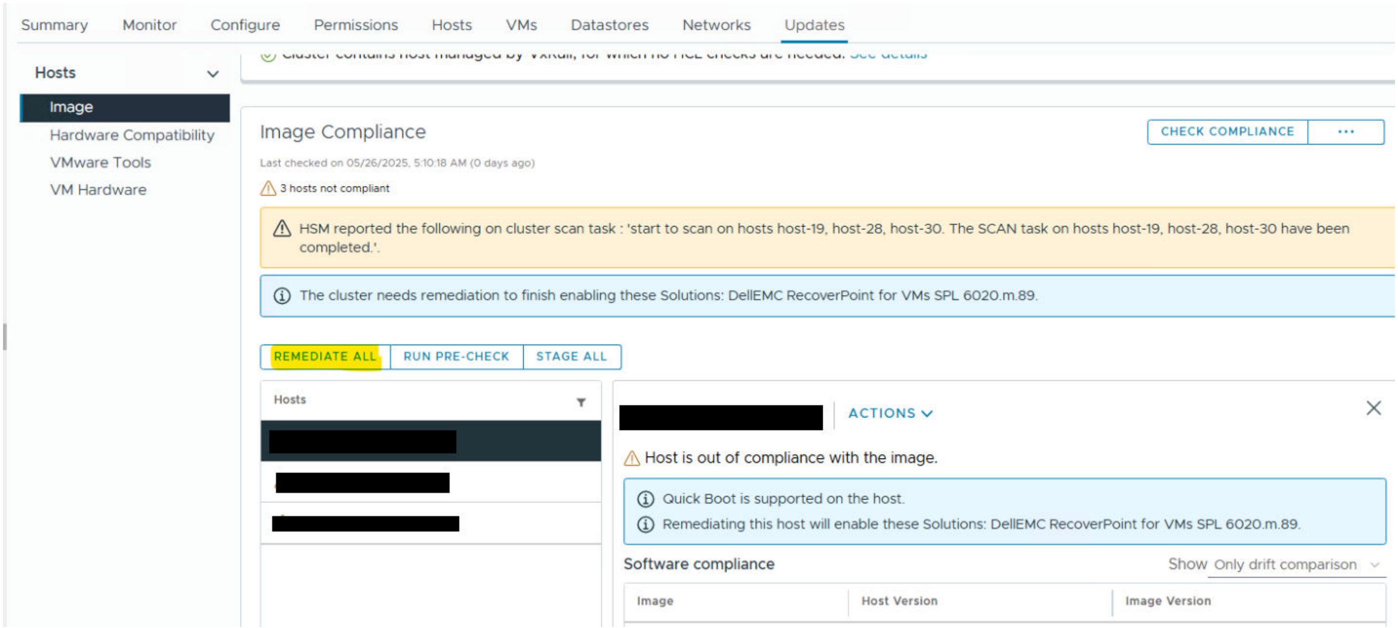
Installing vRPAs cluster, and verifying all vRPAs are attached. ⊗
could not deploy ESX splitter.
Selecting the correct installation mode. ⊗
could not deploy ESX splitter.
Setting up and installing vRPA cluster. ⊗
could not deploy ESX splitter.
Installing vRPAs cluster. ⊗
could not deploy ESX splitter.
Performing system checks for installation. ✓
Validating installation input. ✓
Validating installation basic cluster input. ✓

Also, from VC Recent task below error message shows up:



Install IO Filter	ⓘ Cannot complete the operation. See the event log for details. Failed to modify installation status of I/O filter, EMC_bootbank_emcsplitter_6020.m.89-1OEM.700.1.0.15843807, on all hosts.	VSPHERE.LOCAL\Administrator	3 ms	05/26/2025, 5:09:56 AM	05/26/2025, 5:10:01 AM	[redacted]

The next step to make the hosts compliant with the image is to remediate all hosts using the **Remediate All** option:`<ESX_cluster_name> → Updates → Hosts → Image → Remediate All`



Cluster contains host managed by VxRail, for which no HCL checks are needed. See details

Image Compliance

Last checked on 05/26/2025, 5:10:18 AM (0 days ago)

⚠ 3 hosts not compliant

⚠ HSM reported the following on cluster scan task : 'start to scan on hosts host-19, host-28, host-30. The SCAN task on hosts host-19, host-28, host-30 have been completed.'.

ⓘ The cluster needs remediation to finish enabling these Solutions: DellEMC RecoverPoint for VMs SPL 6020.m.89.

[redacted]

[redacted]

[redacted]

[redacted]

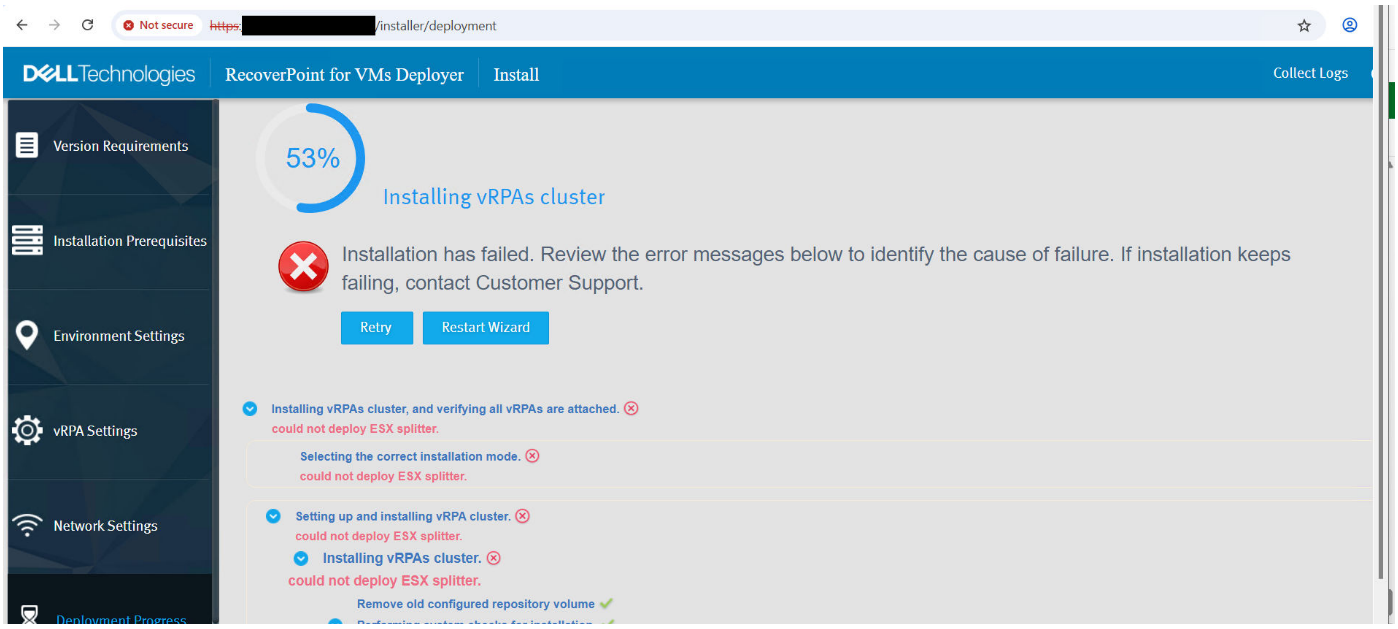
⚠ Host is out of compliance with the image.

ⓘ Quick Boot is supported on the host.

ⓘ Remediating this host will enable these Solutions: DellEMC RecoverPoint for VMs SPL 6020.m.89.

Once remediation completes successfully on all hosts, the Splitter should be installed on all ESXi servers.

The next step is to click the **Retry** button in the WDM. However, the installation fails again at 53% while installing Jiraf.



https:[redacted]/installer/deployment

Installing vRPAs cluster

Installation has failed. Review the error messages below to identify the cause of failure. If installation keeps failing, contact Customer Support.

Installing vRPAs cluster, and verifying all vRPAs are attached. ⊗
could not deploy ESX splitter.

Selecting the correct installation mode. ⊗
could not deploy ESX splitter.

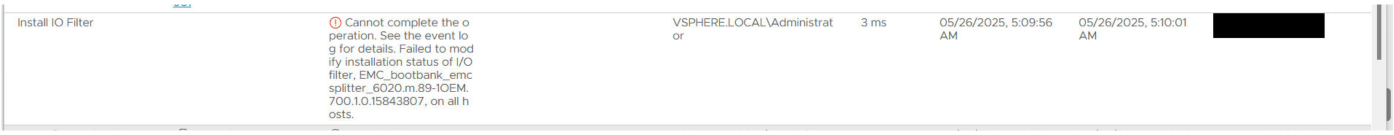
Setting up and installing vRPA cluster. ⊗
could not deploy ESX splitter.

Installing vRPAs cluster. ⊗
could not deploy ESX splitter.

Remove old configured repository volume ✓

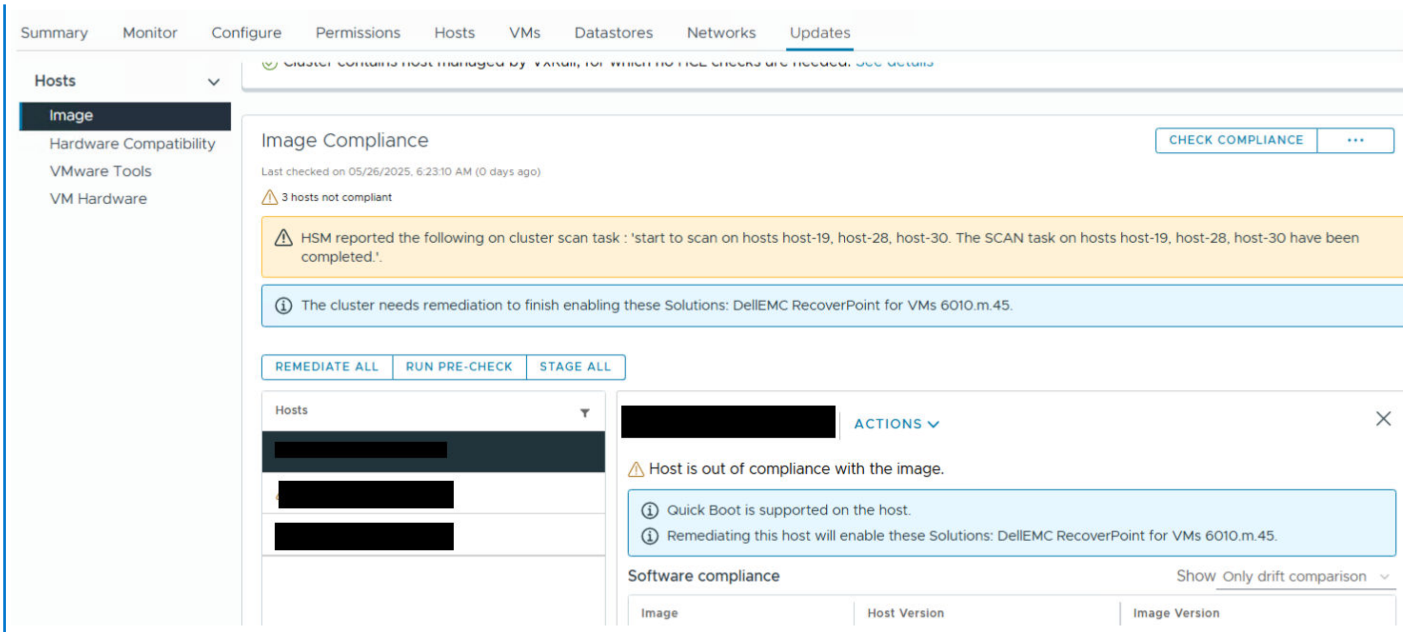
Performing system checks for installation ✓

Also from VC Recent task below error message shows :



Install IO Filter	ⓘ Cannot complete the operation. See the event log for details. Failed to modify installation status of I/O filter, EMC_bootbank_emcsplitter_6020.m.89-1OEM.700.1.0.15843807, on all hosts.	VSPHERE.LOCAL\Administrator	3 ms	05/26/2025, 5:09:56 AM	05/26/2025, 5:10:01 AM	[redacted]

The next step to make the hosts compliant with the image is to remediate all hosts using the **Remediate All** option:`<ESX_cluster_name> → Updates → Hosts → Image → Remediate All`



Cluster contains host managed by VxRail, for which no HCL checks are needed. See details

Image Compliance

Last checked on 05/26/2025, 6:23:10 AM (0 days ago)

3 hosts not compliant

HSM reported the following on cluster scan task : 'start to scan on hosts host-19, host-28, host-30. The SCAN task on hosts host-19, host-28, host-30 have been completed.'.

The cluster needs remediation to finish enabling these Solutions: DellEMC RecoverPoint for VMs 6010.m.45.

[redacted]

[redacted]

Host is out of compliance with the image.

Quick Boot is supported on the host.

Remediating this host will enable these Solutions: DellEMC RecoverPoint for VMs 6010.m.45.

Software compliance

Image	Host Version	Image Version

Once remediation completes successfully on all hosts, Jiraf should be installed on all ESXi servers.

The next step is to click the **Retry** button in the WDM to complete the installation.

During successful installation:

- The HTML5-based RecoverPoint for VMs vSphere plugin is installed after the plugin server is deployed and configured (see Configure the plugin server).
- Splitters and JIRAFs are pushed to all ESXi hosts in the ESXi cluster where the vRPAs are installed.

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 the installation continues to fail, contact Customer Support.

Results

If this vRPA cluster is the first vRPA cluster that is installed on the vCenter, click **Proceed to configure plugin server** now to configure your RecoverPoint for VMs plugin server for this vCenter. If you do not configure the plugin server now, you can configure it later using the **Configure plugin server** option in the RecoverPoint for VMs Deployer home screen.

To enable multisite replication, create additional vRPA clusters by repeating the above steps for each site.

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 that you have installed. You use it to restore the vRPA cluster settings after an installation failure (requiring the installation to be repeated).

When all vRPA clusters are created, continue to "Connect the vRPA clusters."

NOTE: The ESX cluster supports the deployment of RP4VMs clusters on a single ESXi host. For the upgrade, you need at least two ESXi hosts in the ESX cluster.

Next steps

For vSphere 8.0 U2b or later, trust the RPA cluster management IP VIB URL in VC as described in the section Trust Splitter and Jiraf vSphere Installation Bundle (VIB) URLs in vCenter

Configure the plugin server

You can configure the RecoverPoint for VMs vSphere plugin server from the **Configure plugin server** option on the RecoverPoint for VMs Deployer home screen. Alternatively, after using the Deployer installation wizard to successfully install a vRPA cluster on a vCenter, you can proceed directly to configure the plugin server in the Deployer.

Prerequisites

- Ensure that the admin user credentials are the same for all vRPA clusters on the vCenter that you are registering to the plugin server.
- If you want to use a certificate that has been altered, for example, one that has been signed by your organization's internal certificate authority, see "Changing the plugin server certificate" in the *RecoverPoint for VMs Administrator's Guide*.

About this task

Configure the plugin server for only one vRPA cluster that is hosted by the vCenter Server.

Steps

1. To start configuration of the RecoverPoint for VMs plugin server:
   a. Select **Configure plugin server** on the Deployer home page.
   b. Alternatively, immediately after successfully installing a vRPA cluster, click **Proceed to Configure plugin server**.
2. Enter the IP address for the plugin server.

   ⓘ **NOTE:** Use an IPv4 address only.

3. Confirm the SSL certificate of the vCenter Server (remote host).
4. Click **Configure**

Results

- The plugin server installs the HTML-based RecoverPoint for VMs plugin on the vCenter Server. Installation of the plugin usually occurs immediately, but it might take some time for the vCenter Server to identify the plugin. It is recommended to log out from the vSphere Client, and then to log in again. To access the plugin, navigate to RecoverPoint for VMs in the vSphere Client menu.
- The plugin server discovers and registers all vRPA clusters that are hosted by the vCenter Server and have the same admin user password, including vRPA clusters that may be added later. As a result, the plugin server knows how to direct API calls to the correct 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.

Prerequisites

- Do not exceed the maximum number of five vRPA clusters per system.
- (Recommended) Create Installation data forms.
- Ensure the remote vRPA cluster is not:
  - in maintenance mode.
  - an existing, configured vRPA cluster.
  - previously connected to a vRPA cluster.
  - installed on same VC where PROD vRPA cluster is installed.
- Ensure the remote vRPA cluster does not:
  - have protected VMs, consistency groups, or group sets.
  - have user or journal volumes.
  - have a license other than a vCenter license.
- If required, add a gateway for communication between vRPA clusters; add a gateway at each vRPA cluster before connecting the vRPA clusters.

- If you have changed the default plugin server certificate and have not yet configured the plugin server, perform Changing the plugin server certificate .
- If you have changed the default plugin server certificate and have already configured the plugin server, perform Changing a registered plugin server certificate .

ⓘ **NOTE:** A remote vRPA cluster that meets these requirements is called a "clean" cluster.

About this task

In the following steps, the "current" cluster is defined as the vRPA cluster to which the **Connect vRPA clusters** wizard is 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.

Steps

1. In a web browser, type `https://<cluster_management-ip-address>` 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. Ensure that you enter the WAN IP of one of the remote vRPAs.
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 is connected to your RecoverPoint for VMs system, and IP communication is enabled between the remote cluster and the current cluster.

   ⓘ **NOTE:** This connection does not enable communication between the remote cluster and any other clusters in your system. To enable communication between the remote cluster and additional clusters, follow the procedure in Enable communication between vRPA clusters.

6. Continue to the next section, "Register and license the system."

Completing installation of the RecoverPoint for VMs system

You can start protecting the VMs after completing the following tasks:

- Register and license the system.
- Create the required VMkernel ports.

ⓘ **NOTE:**

- For RecoverPoint for virtual machine 6.0 or later deployment, do not use `esxcli` command to install, remove, or upgrade IOFilters from the ESXi.
- Using the `esxcli` command for installing, removing, or upgrading IOFilters corrupts the environment and may cause events like IOFilter crash.

Follow the automatic procedure for installing, uninstalling, and upgrading IOFilters from the ESX cluster.

- Installation - Install vRPA clusters.
- Uninstallation - Uninstalling RecoverPoint for VMs.
- Upgrade - Upgrading the splitter with Admin CLI.

Register and license the system

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

Adding a license automatically enables support. See the "Before you begin" section of the *HTML5 Plugin Administrator's Guide*.

.

Create VMkernel ports

Before protecting VMs, create VMkernel ports for the ESXi hosts in the cluster.

See "Creating VMware ports" section in the *Dell RecoverPoint for Virtual Machines HTML5 Plugin Administrator's Guide*.

ⓘ **NOTE:** Use the following steps even If you are otherwise using the vSphere Web Client. There is one slight difference: In the first step of the procedure, select **Administration > vRPA Clusters > ESX Clusters**, before clicking the **Settings** icon for an ESXi cluster.

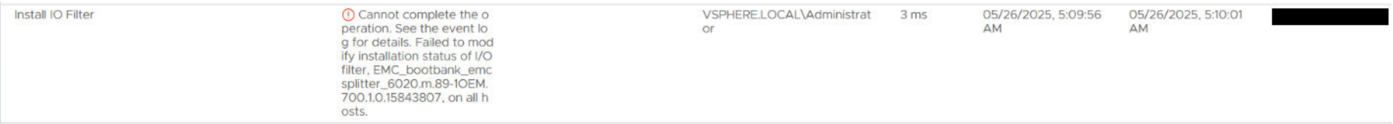
Protect VMs

The RecoverPoint for VMs system is ready for operation. Use the RecoverPoint for VMs plugin (HTML5-based) to begin protecting VMs. See the RecoverPoint for VMs HTML5 Administrator's Guide for instructions on protecting VMs and monitoring the system.

About this task

⚠ **CAUTION: When protecting a VM from the new ESX cluster that lacks I/O filters, it is important to ensure that the respective Site Controller RPA VIB URL has been trusted into the vCenter before initiating protection. You can find the detailed process in the section Trust Splitter and Jiraf vSphere Installation Bundle (VIB) URLs in vCenter. This guideline applies to ESX clusters that contain a copy VM as well.**

ⓘ **NOTE:** When protecting a VM from a new ESX cluster or placing a shadow VM on a new ESX cluster that has single image enabled but lacks I/O filters, RP attempts to install the filters but fails with the following error.



Install IO Filter	ⓘ Cannot complete the operation. See the event log for details. Failed to modify installation status of I/O filter, EMC_bootbank_emcsplitter_6020.m.89-1OEM.700.1.0.15843807, on all hosts.	VSPHERE.LOCAL\Administrator	3 ms	05/26/2025, 5:09:56 AM	05/26/2025, 5:10:01 AM	[redacted]

Manual remediation is then required to complete the installation of the Splitter on the ESXi hosts. To perform this, navigate to:`<ESX_Cluster_name> → Updates → Hosts → Image → Remediate All`

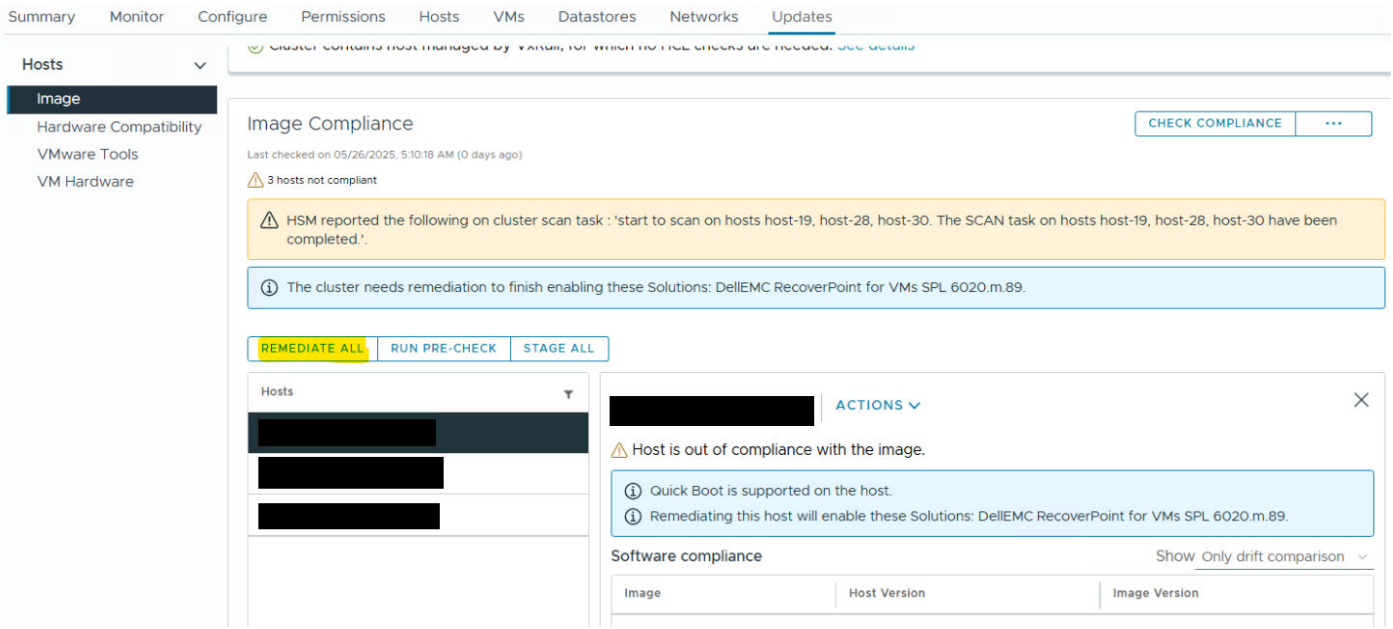


Image Compliance

Last checked on 05/26/2025, 5:10:18 AM (0 days ago)

⚠ 3 hosts not compliant

⚠ HSM reported the following on cluster scan task : 'start to scan on hosts host-19, host-28, host-30. The SCAN task on hosts host-19, host-28, host-30 have been completed.'.

ⓘ The cluster needs remediation to finish enabling these Solutions: DellEMC RecoverPoint for VMs SPL 6020.m.89.

[redacted]

[redacted]

⚠ Host is out of compliance with the image.

ⓘ Quick Boot is supported on the host.

ⓘ Remediating this host will enable these Solutions: DellEMC RecoverPoint for VMs SPL 6020.m.89.

Software compliance

Image	Host Version	Image Version

Once remediation is complete, the wanted Splitter is pushed to all ESXi hosts, and the CG will transition to the INIT and then active state.

Maintaining RecoverPoint for VMs

Maintaining the RecoverPoint for VMs system involves tasks such as collecting logs, modifying vRPA cluster network settings and topology, and adding, removing, or replacing vRPAs.

The topics in this chapter provide procedures for system maintenance.

Topics:

Register ESX clusters

By default, ESX clusters are registered automatically as part of the Protect VM procedure. Alternatively, you can register ESX clusters manually, using the RecoverPoint for VMs plug-in to the vSphere Client.

Steps

1. Access the vSphere Client.

   In the vSphere Client, click **System** > **ESX Clusters**.
2. Select the ESX cluster to be registered, and click **Add**. Verify that the connectivity status is OK. If there are connectivity issues with the cluster, click **Troubleshoot**.

Changing the IP Address of an I/O Filter MOB URL

This section describes the procedure to modify the I/O filter MOB URL IP address in the vSphere Web Client.

Prerequisites

It is essential to determine the state of the default I/O filters MOB URL IP address(s) before changing the IP address(s). Perform the following steps to verify the default I/O filters MOB URL IP address(s) state:

1. Check for the default I/O filter IP address(s) in the vSphere Web Client by selecting **ESX_Cluster_Name** > **Configure** > **Configuration** > **I/O Filters**.
   - The **I/O Filters** section displays the available filters and corresponding URLs under the **Filter Name** and **URL** columns, respectively.
2. Verify the RPA IP in the **URL** field from the previous step.

About this task

If the I/O filter MOB URL IP address(s) displayed in vSphere are down for various reasons, certain automated operations managed by vLCM may not work. These operations include:

- Removing filters from ESX when it is moved out of the cluster.
- Pushing filters to the newly added ESXi host.

Consider changing the IP address of the MOB URL to another active RPA IP by performing the following steps:

Steps

Obtaining the MOID of an ESX Cluster

1. Log in to **Managed Object Browser (MOB)** using the following URL format:

   ```
   https://<VC_IP>/mob
   ```

2. Type in your vSphere credentials in the `User Name` and `Password` fields.
3. Click **content** under **VALUE** in the **Properties** section.
4. Click the **rootFolder** property value from the **Properties** table on the next page.

   The **rootFolder** property may have different values for different users. For example, a property value *group-d1 (Datacenters)* is provided in the following table:

   Table 3. ServiceContent Properties Table

NAME	TYPE	VALUE
rootFolder	**ManagedObjectReference:Folder**	**group-d1 (Datacenters)**

5. Click the **childEntity** property value from the **Properties** table on the next page.

   The **childEntity** property may have different values for different users. For example, a property value *datacenter-3 (XXX_Remote)* is provided in the following table:

   Table 4. Datacenters Folder Properties Table

NAME	TYPE	VALUE
childEntity	**ManagedObjectReference:ManagedEntity[]**	**datacenter-3 (XXX_Remote)**

6. Click the **hostFolder** property value from the **Properties** table on the next page.

   The **hostFolder** property may have different values for different users. For example, a property value *group-h5 (host)* is provided in the following table:

   Table 5. Datacenter Properties Table

NAME	TYPE	VALUE
hostFolder	**ManagedObjectReference:Folder**	**group-h5 (host)**

7. Identify and note the *MOID* of the required ESX cluster from the **childEntity** property values.

   The **childEntity VALUE** column lists all ESX clusters and the corresponding MOIDs configured for a datacenter. For example, *domain-c10* is the *MOID* of the vRPA clusters as provided in the following table:

   Table 6. Host Folder Properties Table

NAME	TYPE	VALUE
childEntity	**ManagedObjectReference:ManagedEntity[]**	**domain-c10 (vRPAs_Cluster)**

Obtaining the I/O filter IDs and VIB URLs

8. Select **Home** > **Content** > **IoFilterManager** > **QueryIoFilterInfo**.
   This action displays the **QueryIoFilterInfo Parameters** table.
9. Replace the boilerplate text `MOID` with the one you noted from step 7 in the **VALUE** column, and click **Invoke Method**.
   This action invokes the **ClusterIoFilterInfo** table with all available I/O filter information.
10. Take note of the **id** and **vibUrl** values, without using any double quotations (`" "`), for the necessary I/O filter(s) from the table.
    Example:
    - **id**: EMC_bootbank_emcsplitter_6011.m.88-1OEM.700.1.0.15843807
    - **vibUrl**: https://10.0.0.1/RPResources/iof/esx8/EMC-RP4VMS-SPL_6011.M.88-1OEM.700.1.0.15843807.zip
11. Close the **QueryIoFilterInfo** page.

Updating the Existing IP Address with MOID, I/O Filter ID, and VIB URL

12. Select **Home** > **Content** > **IoFilterManager**.
    This action displays the **IoFilterManager** page.
13. Click the **UpgradeIoFilter_Task** return type from the **Methods** table.
    This action displays the **UpgradeIoFilter_Task** table.
14. Enter the filter ID, MOID, and VIB URL values in the **UpgradeIoFilter_Task** table, as described in the following steps:
    a. Enter the **filterId** parameter value that you previously noted.
    b. Replace the boilerplate text `MOID` in the **comRes** property value field with the one you previously noted.
    c. Enter the **vibUrl** property value that you previously noted, and type in the new IP address manually into the **VALUE** field. For example, you can manually update the existing IP address **`10.0.0.1`** of the VIB URL `https://10.0.0.1/RPResources/iof/esx8/EMC-RP4VMs-SPL_6011.m.88-1OEM.700.1.0.15843807.zip` into **`10.0.0.2`** to represent the new VIB URL `https://10.0.0.2/RPResources/iof/esx8/EMC-RP4VMs-SPL_6011.m.88-1OEM.700.1.0.15843807.zip`.

    NOTE: In vSphere 8.0 U2b or later, ensure that the new IP address provided in the MOB URL is trusted in VC using the procedure that is provided in Trust Splitter and Jiraf vSphere Installation Bundle (VIB) URLs in vCenter.

15. Click **Invoke Method** and the system creates a task for the requested changes.
16. Click the **task-XXXXXX** link **> info** and check the **state** property. If the **state** property value shows `success`, the requested changes were applied successfully.

    NOTE: The system may show a `Running` state for the task. Keep repeating this step until you see the `Success` state.

Verifying the Changed IP Address

17. Perform either of the following steps to verify the updated IP address:
    - Select **Home** > **Content** > **IoFilterManager** > **QueryIoFilterInfo** and replace the boilerplate text `MOID` with the one you previously noted. Click **Invoke Method** and the system displays the **vibUrl** field with the updated IP address.
    - Select **ESX_Cluster_Name** > **Configure** > **Configuration** > **I/O Filters** in the vSphere Web Client.

      The **I/O Filters** section displays the URL with the updated IP address under the **URL** column.

Results

The I/O filter MOB URL IP address has been successfully changed.

Next steps

Repeat this procedure for each I/O filter MOB URL separately to change the IP address of all the required I/O filters.

Add an ESXi host to a cluster

This section describes how to add an ESXi host to a vRPA cluster.

Prerequisites

CAUTION: Perform the following action to ensure that the MOB URL RPA IP displayed in the vSphere URL field is up:

In vSphere, select <ESX_Cluster_Name> > Configure > I/O Filters > URL

Steps

1. After you add an ESXi host to an ESX cluster, the RecoverPoint for VMs splitter is installed automatically on the new ESXi host.

   NOTE: Adding a Host to a Single Image-Enabled ESXi Cluster

   a. Place the ESXi host into maintenance mode before adding it to the cluster.
   b. Add the host to the cluster directly.
   c. Once added, go to the **Updates** tab of the cluster in vSphere.
   d. Click **Remediate All** to the new host.

e. Once the remediation is completed successfully, the ESXi host is fully added to the cluster.

> ⓘ **NOTE:** The ESXi host must be running the same version as the other hosts in the cluster because the cluster uses a single image version for all hosts.

2. The RecoverPoint for VMs jiraf is also installed automatically on the new ESXi host, when there are vRPA VMs running on the ESX cluster to which the ESXi host has been added.

Configure VMkernel ports

You can configure the VMKernel ports from the RecoverPoint for VMs plug-in UI, and they will be automatically created for all the ESXi hosts in the ESXi cluster. Alternatively, you can use this procedure to manually configure VMkernel ports.

Prerequisites

An ESXi must be registered (see Register ESX clusters) before you can configure VMkernel adapters on it.

Steps

1. For each ESXi host, click **Manage** > **Networking** > **VMkernel adapters**.
2. Add the VMkernel adapters.
   - Assign IP addresses that are on a routable subnet or on the same subnet as the vRPA data interfaces.

     It is recommended also that the VMkernel and vRPA data ports be on the same L2 network.
   - For a standard vSwitch, create a VMkernel port with the network label: **`RP-VM-Kernel-Port-Group`**
   - For a distributed vSwitch:
     - Create a VMkernel port on the relevant port group.
     - On the Ports tab of the Distributed Ports Group page, label each VMkernel port that is to be used for splitter-to-vRPA communication as **`RP-VM-Kernel-Port-Key`**.

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

Enable communication between vRPA clusters

Use this procedure to enable communication between pairs of vRPA clusters in your system.

About this task

Use the **Connect vRPA clusters** wizard in the RecoverPoint for VMs Deployer to add a vRPA cluster to your system, and to enable IP communication between that new cluster and one of the existing clusters. For more information, see Connect vRPA clusters.

Use the following procedure to enable communication between additional pairs of clusters.

Steps

1. Use an SSH client to connect as admin user to a cluster management vRPA of one of the pair of vRPA clusters between which you want to enable communication.
2. From the Admin CLI **Main Menu**, select **Cluster operations** > **Configure connection types to other clusters in the system** > **Configure cluster connection types**.
3. Select the vRPA cluster with which you want to enable communication.

Results

Bi-directional IP communication is enabled between the designated pair of vRPA clusters.

Repeat this procedure for each pair of vRPA clusters for which you want to enable communication.

Modify vRPA cluster network settings

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

Prerequisites

To modify the network adapter topology, refer to Modify the network topology.

Steps

1. In a web browser, type **`https://<cluster_management-ip-address>`** 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 admin 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.

Change the RPA communication security level

The default security level is to authenticate and encrypt all data between vRPA clusters. For information about the RPA communication security level, including a procedure for changing it, see the *RecoverPoint for Virtual Machines Security Configuration Guide*.

Modify the network topology

Use this procedure to modify the existing network topology.

Steps

1. Pause transfer between the production and copies of the consistency groups for the vRPA cluster that you are modifying.
2. From the vSphere Client or 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 the admin 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.

      ⓘ **NOTE:** If applicable, modify the port group using the vSphere client as needed.

   d. Attach the vRPA back to the cluster. From the **Main** menu, select **Cluster operations** > **Attach RPA to cluster**.
4. Repeat step 3 for each vRPA in the vRPA cluster.
5. Start transfer between the production and copies of the consistency groups for the modified vRPA cluster.

Upgrading the splitter with Admin CLI

Ensure that all vRPAs reside on ESXi hosts with a splitter installed. Splitters are installed automatically during system installation. You can use this procedure to upgrade splitters manually.

About this task

For information on upgrading splitters, see the section Upgrade Splitter and Jiraf for Entire ESX Cluster.

Add vRPAs to a vRPA cluster

Perform the following steps to add a vRPA to an existing vRPA cluster. A vRPA cluster can have up to 6 vRPAs, and all vRPAs in a cluster must run the same RecoverPoint for VMs version.

Prerequisites

If you are not using the default vRPA web server certificate, ensure that your certificate is the same for all vRPAs in the vRPA cluster.

> ⓘ **NOTE:** Before adding the extra RPA , ensure that the respective ESX cluster is already registered to RP cluster. If not, register the ESX cluster or protect the VM using the plugin.

Steps

1. In a web browser, type **`https://`*`<cluster_management-ip-address>`*** 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 admin 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 6 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.

Steps

1. In a web browser, type **`https://`*`<cluster_management-ip-address>`*** 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 admin 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.

Prerequisites

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.

ⓘ **NOTE:** Before replacing the RPA , ensure that the respective ESX cluster is already registered to RP cluster. If not, register the ESX cluster or protect the VM using the plugin.

About this task

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 admin user and select **Main Menu** > **Shutdown / Reboot operations** > **Shutdown RPA**.

Steps

1. In a web browser, type **`https://`*`<cluster_management-ip-address>`*** 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 admin 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.

   ⓘ **NOTE:** If you are replacing the Site Controller RPA (RPA1 or RPA2), the replaced RPA may not retain RP cluster settings. After logging in as an admin user, follow the procedure below to import the settings:

   a. Navigate to **Main Menu** > **Setup** > **Apply Settings**.
   b. Verify the RPA and cluster details.
   c. Follow the on-screen instructions and provide the required details.
   d. Enter the **`Cluster ID`** and the **`Replaced RPA ID`**.

   ⚠ **CAUTION: This action disconnects the RPA from the cluster based on your confirmation, and you must reconnect it.**

Collect logs

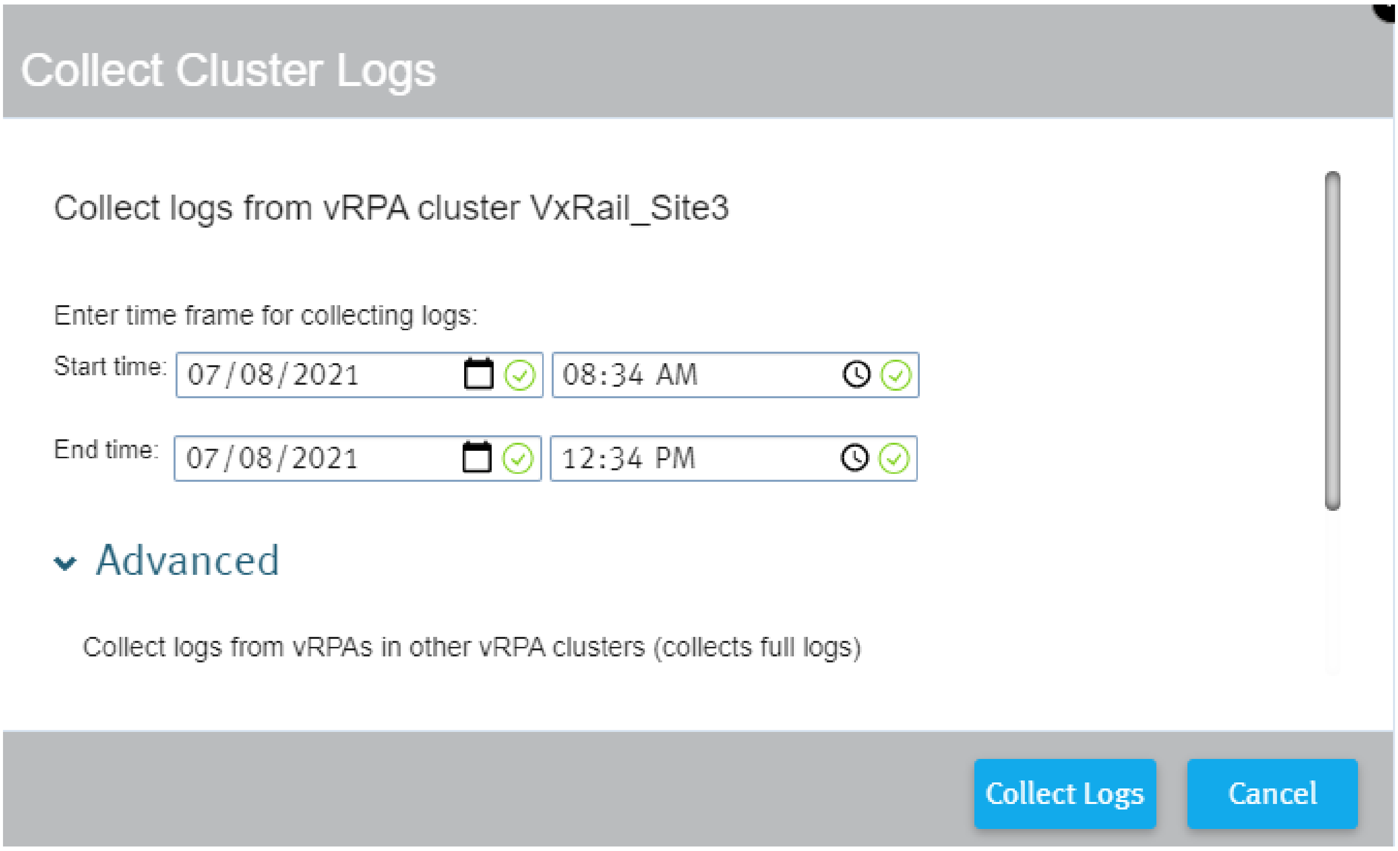
During deployment, collecting logs for the current vRPA cluster and its vRPAs provides information that may be helpful in troubleshooting the installation.

About this task

Logs can be collected from one or more vRPAs in multiple vRPA clusters, if they all reside on a vCenter Server registered with the plugin server, or a vCenter Server that is linked to a vCenter Server that is registered with the plugin server.

Steps

1. In a web browser, type **`https://<LAN-ip-address>`** where *<LAN-ip-address>* is the vRPA cluster management IP address. In the vRPA cluster home page, click **RecoverPoint for VMs Deployer**.
2. If prompted, type the login credentials for the **admin** user and click **Sign in**.
3. In the upper-right corner, click **Collect Logs** to display the log collection settings in the **RecoverPoint for VMs Deployer** home page.
4. In the **Collect Cluster Logs** dialog box:



Collect Cluster Logs

Collect logs from vRPA cluster VxRail_Site3

Enter time frame for collecting logs:

Start time: 07/08/2021 08:34 AM

End time: 07/08/2021 12:34 PM

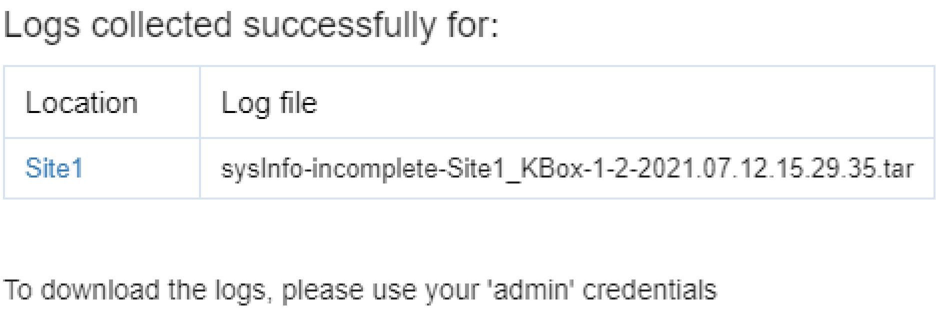
Advanced

Collect logs from vRPAs in other vRPA clusters (collects full logs)

   a. Enter a **Start time** and **End time** for log collection.
   b. (Optional) To simultaneously collect logs from vRPAs in other vRPA clusters, expand the **Advanced** section, and add another vRPA *<LAN-ip-address>*.
   c. Click **Collect Logs**.

Results

Depending on the size of the environment, log collection may take several minutes to complete. When the collection process is complete, a success message is displayed with the location (that is vRPA cluster) containing the logs.



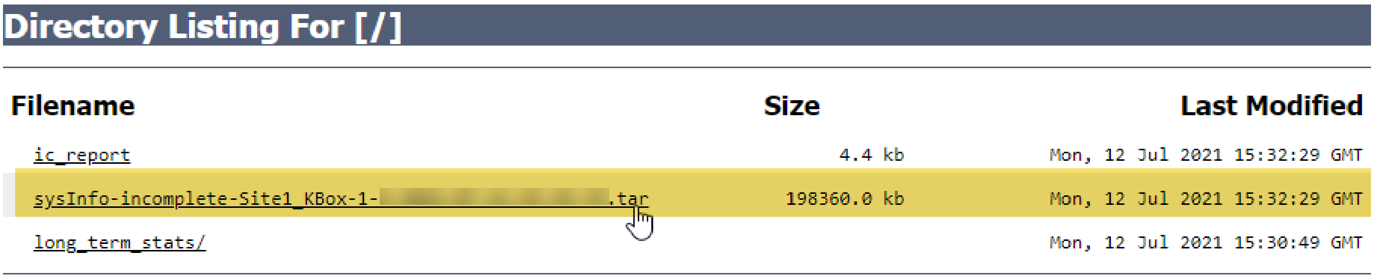
Logs collected successfully for:

Location	Log file
Site1	sysInfo-incomplete-Site1_KBox-1-2-2021.07.12.15.29.35.tar

To download the logs, please use your 'admin' credentials

Next steps

1. In the success message, click the name of a vRPA cluster to open a browser window to the location of the collected logs.
2. If prompted to, log in to the vRPA cluster with your **`admin`** user credentials.
3. Click a vRPA log name to download the vRPA log. The name of each vRPA log has a `*.tar` extension and it includes the `<clustername><vrpaname>` and `<vrpaip>` for quick identification. The log collection date is displayed under **Last Modified**.



Directory Listing For [/]

Filename	Size	Last Modified
ic_report	4.4 kb	Mon, 12 Jul 2021 15:32:29 GMT
sysInfo-incomplete-Site1_KBox-1-[redacted].tar	198360.0 kb	Mon, 12 Jul 2021 15:32:29 GMT
long_term_stats/		Mon, 12 Jul 2021 15:30:49 GMT

Upgrading RecoverPoint for Virtual Machines

Upgrading RecoverPoint for Virtual Machines requires downloading the upgrade package and sequentially upgrading vRPA clusters, splitter, JIRAF, and the RecoverPoint for Virtual Machines plugin.

ⓘ **NOTE:** RecoverPoint for Virtual Machines 6.0.3 supports upgrades from 5.3.4.1.

Topics:

Upgrade overview

Upgrade the RecoverPoint for VMs system by downloading the required upgrade package and then upgrading the relevant system components.

You can use the RecoverPoint for VMs vSphere plugin (**System** > **Administration** screen), API, or CLI (`get_versions` command) to determine what version of RecoverPoint for VMs system is currently installed.

In general, upgrading RecoverPoint for VMs includes the following activities:

- Download the upgrade package.
- Upgrade the vRPA clusters.
- Upgrade the RecoverPoint for VMs splitter filters.
- Upgrade the RecoverPoint for VMs JIRAF.
- Upgrade the RecoverPoint for VMs plugin.

You may upgrade the RecoverPoint for VMs plugin server whenever a later version of the plugin server is available.

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

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 that are required for the upgrade.

Download the RecoverPoint for VMs Upgrade and Maintenance Kit from Dell Support.

SRO signature protects the OVA file and GPG signature protects the ISO file. If you want to verify a signature, see Verifying signatures.

Upgrade a vRPA cluster

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

Prerequisites

If the vCenter Server SSL certificate has been changed, ensure that the new certificate is valid, and that RecoverPoint for VMs has been updated with it before beginning the upgrade.

About this task

- If you are upgrading a vRPA cluster with 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 the Deployer may become temporarily unavailable. When the vRPA completes its restart, you can log back into 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 vRPA. 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 simultaneously. This practice is not supported. Rather, upgrade connected vRPA clusters one cluster at a time until all the connected vRPA clusters are upgraded to the same release.**

Steps

1. In a web browser, type **`https://`*`<cluster_management-ip-address>`*** 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 admin 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.

   For the second option selected which is default option, users must manually download the ISO file from the support site and upload it to the WDM portal.
7. On the Version Requirements page, the version requirements file must be validated manually to ensure that the system meets the requirements.

   On the Version Requirements page, select one of the following options,

   - **Provide version requirements file manually**
   - **Do not check version requirements**

   If the first option is selected, users must manually download the `cca.xml` file from the support site and upload it to the WDM portal and click **Next** to continue.

   For the second option, click **Next** to continue.
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.

Results

All vRPAs in the vRPA cluster are upgraded.

Next steps

- If the upgrade fails, review the displayed error message to identify the cause of the failure.
- To correct any issues and retry the upgrade, click **Back**.
- If upgrading a vRPA continues to fail, contact Customer Support.

Upgrade Splitter and Jiraf for Entire ESXi Cluster

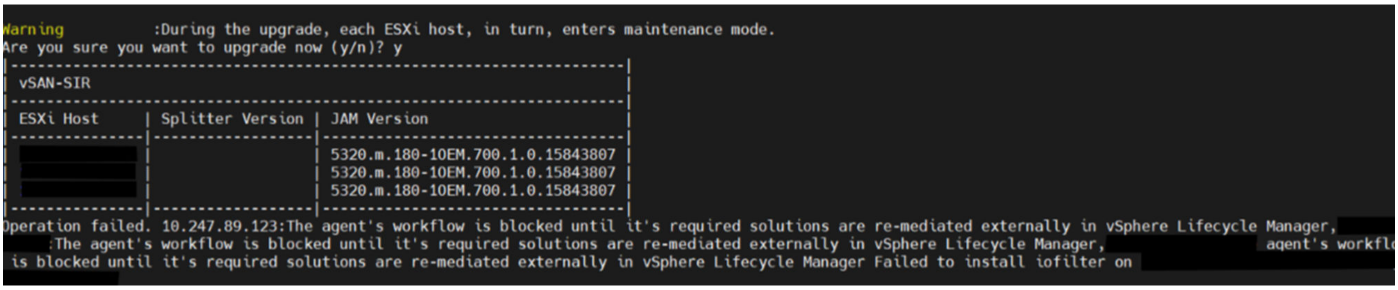
Perform the following procedure to upgrade splitter and jiraf on all ESXi hosts in an ESXi cluster.

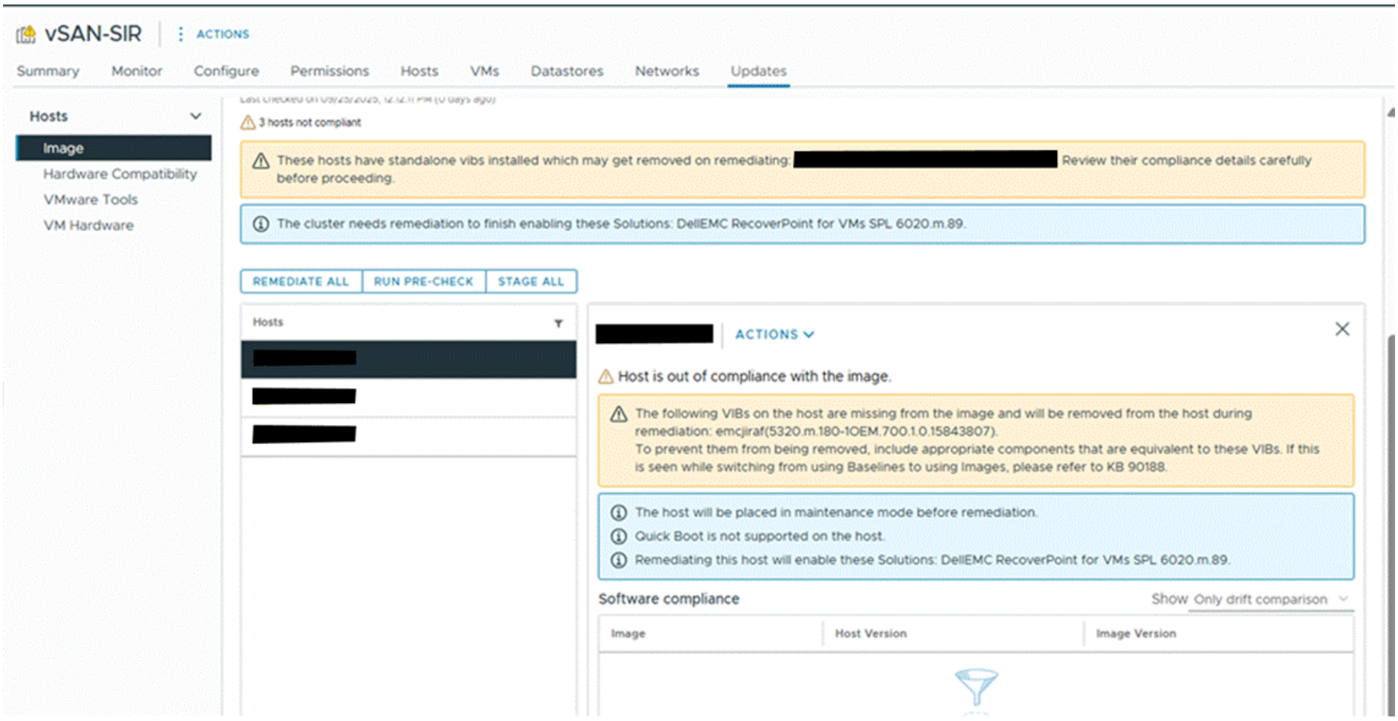
Prerequisites

- Ensure that you have completed the procedure to upgrade a vRPA cluster.
- The ESXi cluster must contain at least two ESXi hosts that are not already in maintenance mode before running the upgrade procedure.
- Ensure that DRS is enabled in automatic mode.

Steps

1. Use an SSH client to log in to the vRPA as the admin user.
2. From the Main menu, select **Setup** > **Advanced options** > **Splitter actions** > **Upgrade Splitter**.
3. Enter the requested information: vCenter Server IP address and TCP port number (if other than the default, 443), and the vCenter credentials.
4. Let the system provide the vCenter certificate automatically and, if the certificate is correct, approve the certificate.
5. Select the ESXi cluster on which to upgrade the RecoverPoint for VMs splitter and jiraf. The splitter and jiraf version that is currently installed on each of the ESXi hosts is listed, along with the splitter and jiraf version that the upgrade installs.
   For each of the ESXi hosts, the splitter and jiraf version that is installed and the version to be installed after the upgrade is listed.
6. For vSphere 8.0 U2b or later, trust the new VIB URL version for RP cluster management IPs. See Trust Splitter and Jiraf vSphere Installation Bundle (VIB) URLs in vCenter with URLs listed in the SU tool.
7. Type **y** to begin the upgrade.
   Each ESXi host enters maintenance mode, in turn, as its splitter and jiraf are upgraded. The table of splitter and jiraf versions is updated as the upgrade progresses. Ensure that the splitter and jiraf are upgraded to the required versions for all ESXi in the final result of the table.

   > **NOTE:** If upgrading from 5.3.4.1 and single image is enabled on the ESXi cluster, then admin CLI upgrade fails with the following error during the installation of splitter.
   >
   > 
   >
   > ```
   > Warning          :During the upgrade, each ESXi host, in turn, enters maintenance mode.
   > Are you sure you want to upgrade now (y/n)? y
   > |----------------------------------------------------------------|
   > | vSAN-SIR                                                       |
   > |----------------------------------------------------------------|
   > | ESXi Host     | Splitter Version | JAM Version                  |
   > |---------------|------------------|------------------------------|
   > | [redacted]    |                  | 5320.m.180-10EM.700.1.0.15843807 |
   > | [redacted]    |                  | 5320.m.180-10EM.700.1.0.15843807 |
   > | [redacted]    |                  | 5320.m.180-10EM.700.1.0.15843807 |
   > |---------------|------------------|------------------------------|
   > Operation failed. 10.247.89.123:The agent's workflow is blocked until it's required solutions are re-mediated externally in vSphere Lifecycle Manager, [redacted]
   > [redacted]:The agent's workflow is blocked until it's required solutions are re-mediated externally in vSphere Lifecycle Manager, [redacted] agent's workfl
   >  is blocked until it's required solutions are re-mediated externally in vSphere Lifecycle Manager Failed to install iofilter on [redacted]
   > ```
   >
   > Splitter entry might show as empty in the table as it was removed earlier.
   >
   > Make the hosts compliant with the image to remediate all hosts. Select **<ESXi_cluster_name>**, and then click **Updates** > **Hosts** > **Image** > **Remediate All**



3 hosts not compliant

These hosts have standalone vibs installed which may get removed on remediating: [redacted] Review their compliance details carefully before proceeding.

The cluster needs remediation to finish enabling these Solutions: DellEMC RecoverPoint for VMs SPL 6020.m.89.

[redacted]

Host is out of compliance with the image.

The following VIBs on the host are missing from the image and will be removed from the host during remediation: emcjiraf(5320.m.180-1OEM.700.1.0.15843807).
To prevent them from being removed, include appropriate components that are equivalent to these VIBs. If this is seen while switching from using Baselines to using Images, please refer to KB 90188.

The host will be placed in maintenance mode before remediation.
Quick Boot is not supported on the host.
Remediating this host will enable these Solutions: DellEMC RecoverPoint for VMs SPL 6020.m.89.

During remediation vLCM places each ESXi into maintenance mode to install splitter. After remediation is complete, following message is displayed.

```
Remediation completed successfully.
```

You might also see a remediate option to remove JIRAF which can be ignored and proceed to next step.

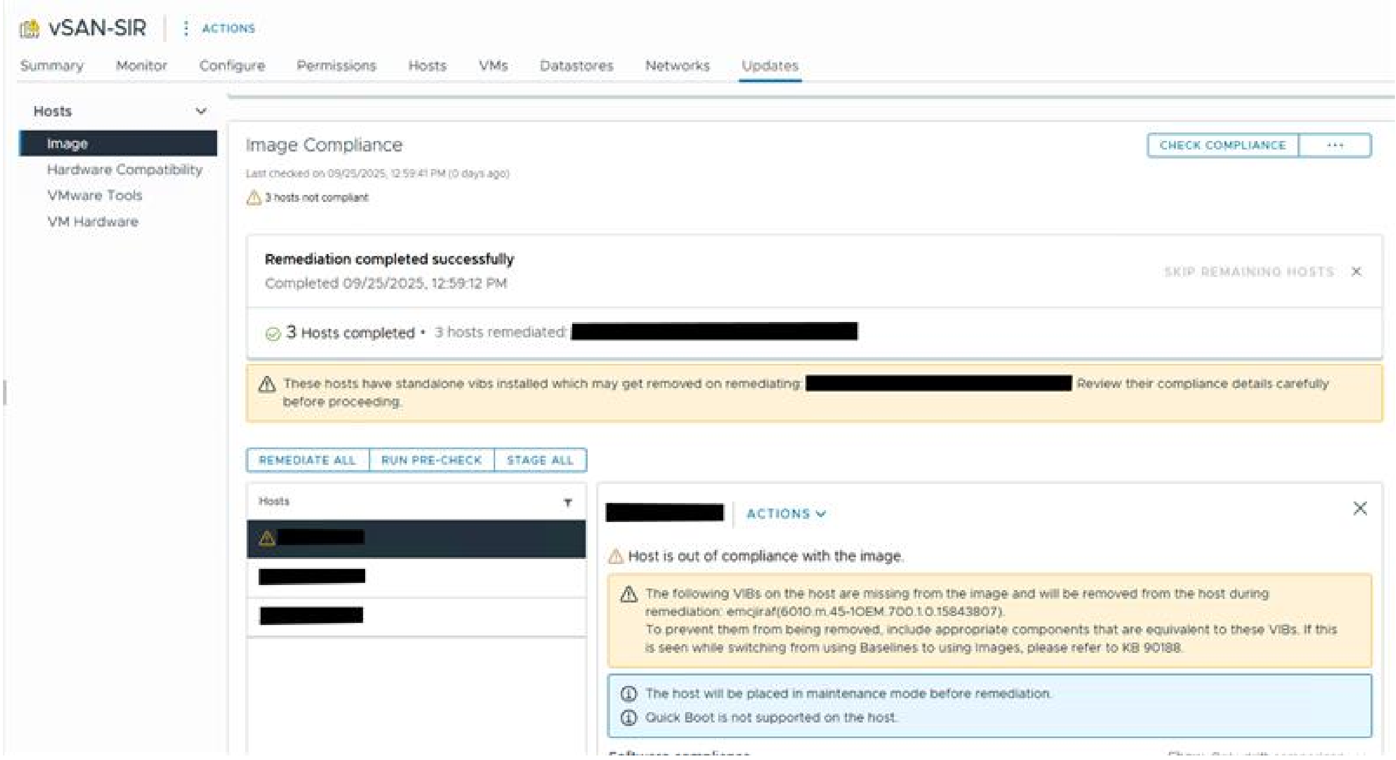


Image Compliance

Last checked on 09/25/2025, 12:59:41 PM (0 days ago)

3 hosts not compliant

Remediation completed successfully
Completed 09/25/2025, 12:59:12 PM

3 Hosts completed • 3 hosts remediated: [redacted]

These hosts have standalone vibs installed which may get removed on remediating: [redacted] Review their compliance details carefully before proceeding.

[redacted]

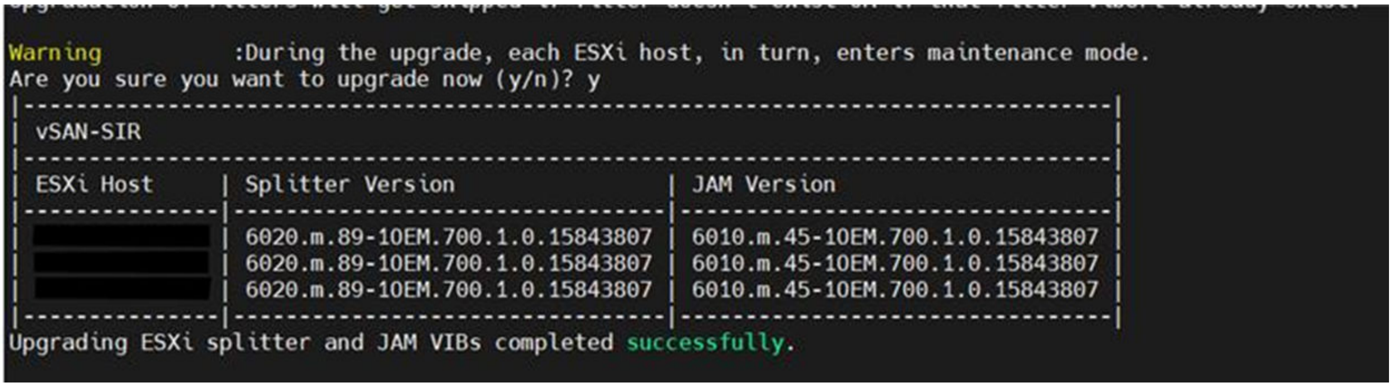
Host is out of compliance with the image.

The following VIBs on the host are missing from the image and will be removed from the host during remediation: emcjiraf(6010.m.45-1OEM.700.1.0.15843807).
To prevent them from being removed, include appropriate components that are equivalent to these VIBs. If this is seen while switching from using Baselines to using Images, please refer to KB 90188.

The host will be placed in maintenance mode before remediation.
Quick Boot is not supported on the host.

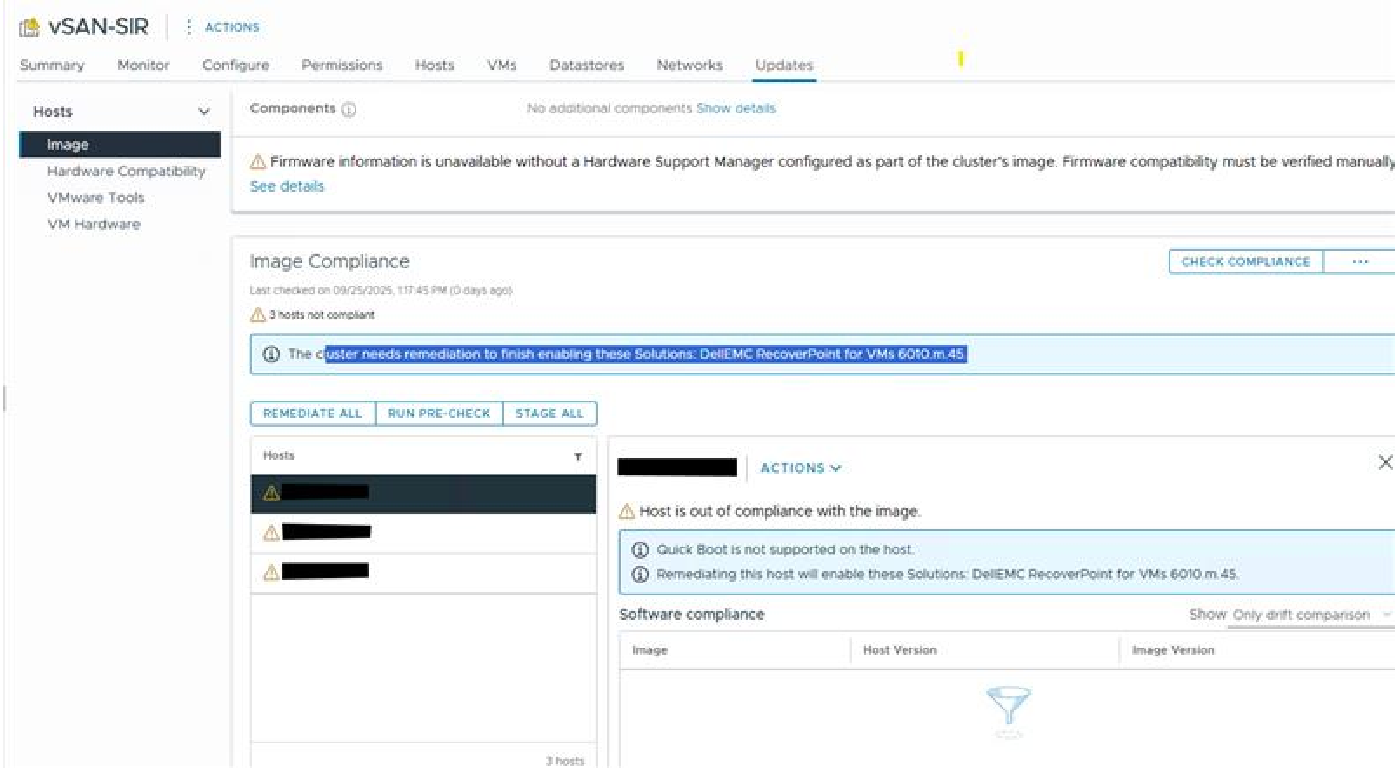
To successfully complete the upgrade, retry the upgrade again from admin CLI. Following message is displayed.

```
Upgrading ESXi splitter and JAM VIBs completed successfully.
```



```
Warning          :During the upgrade, each ESXi host, in turn, enters maintenance mode.
Are you sure you want to upgrade now (y/n)? y
|--------------------------------------------------------------------------------|
| vSAN-SIR                                                                       |
|--------------------------------------------------------------------------------|
| ESXi Host     | Splitter Version                | JAM Version                  |
|---------------|---------------------------------|------------------------------|
| [redacted]    | 6020.m.89-10EM.700.1.0.15843807 | 6010.m.45-10EM.700.1.0.15843807 |
| [redacted]    | 6020.m.89-10EM.700.1.0.15843807 | 6010.m.45-10EM.700.1.0.15843807 |
| [redacted]    | 6020.m.89-10EM.700.1.0.15843807 | 6010.m.45-10EM.700.1.0.15843807 |
|---------------|---------------------------------|------------------------------|
Upgrading ESXi splitter and JAM VIBs completed successfully.
```

However, to make the hosts compliant with the image, you must compliance check using **CHECK COMPLIANCE** and then remediate all hosts. Select **`<ESXi_cluster_name>`** and then click **Updates** > **Hosts** > **Image** > **Remediate All**.



No additional components Show details

Firmware information is unavailable without a Hardware Support Manager configured as part of the cluster's image. Firmware compatibility must be verified manually
See details

Image Compliance

Last checked on 09/25/2025, 1:17:45 PM (0 days ago)

3 hosts not compliant

The cluster needs remediation to finish enabling these Solutions: DellEMC RecoverPoint for VMs 6010.m.45

[redacted]

[redacted]

[redacted]

3 hosts

[redacted]

Host is out of compliance with the image.

Quick Boot is not supported on the host.

Remediating this host will enable these Solutions: DellEMC RecoverPoint for VMs 6010.m.45.

Show Only drift comparison

After remediation is complete in vSphere, following message is displayed.

```
Remediation completed successfully.
```

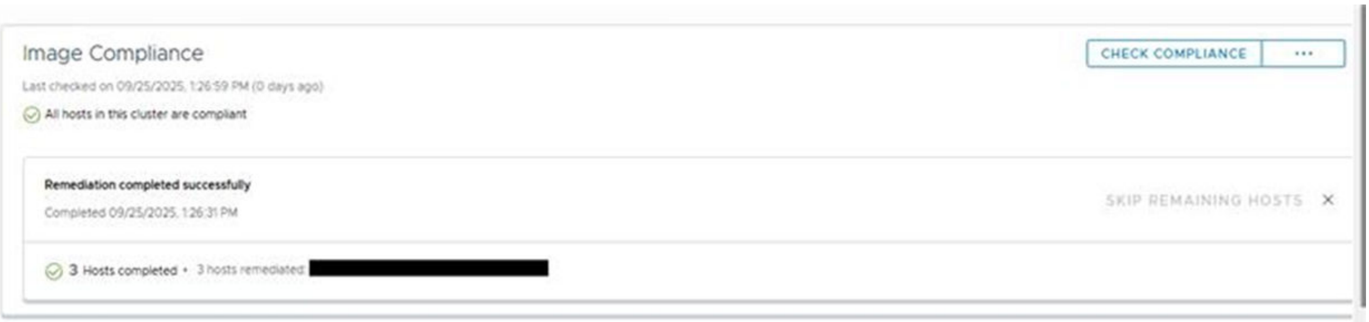


Image Compliance

Last checked on 09/25/2025, 1:26:59 PM (0 days ago)

All hosts in this cluster are compliant

Remediation completed successfully

Completed 09/25/2025, 1:26:31 PM

3 Hosts completed • 3 hosts remediated: [redacted]

Upgrade the plugin server

Upgrading the plugin server upgrades the HTML5 plugin and the API.

Prerequisites

Download a plugin server upgrade file from the RecoverPoint for VMs product support section of Dell Support.

About this task

Plugin server releases are not tied to RecoverPoint for VMs releases. Upgrade packages can upgrade all services running on the plugin server. When a plugin server is being upgraded, the vSphere HTML5 plugin is not functional until upgrade is complete.

> ⓘ **NOTE:** Plugin server upgrade packages do not contain the updated SLES versions of the plugin. After an upgrade, if security scans identify vulnerabilities associated with the plugin server, it is recommended that you uninstall the existing plugin server and re-install the plugin server using the latest OVA files. This ensures that the OS libraries and relevant packages are the latest versions. For more information, see Uninstall the plugin server.

Steps

1. In the RecoverPoint for VMs HTML5 plugin for vSphere Client, click **System** > **Plugin Server**
   The **RecoverPoint for VMs Plugin Server** screen is displayed.
2. Click **Actions** > **Upgrade plugin server**
3. Select the plugin server upgrade file that you downloaded from Dell Support, and click **OK**.

Results

Wait for upgrade to complete to operate your RecoverPoint for VMs system.

Upgrade from RecoverPoint for VMs 5.3.SP4 P1 to 6.0.SP3 and later

Perform the following procedure to upgrade your RecoverPoint for VMs from 5.3.SP4 P1 to 6.0.SP3 and later.

Prerequisites

Ensure that the vCenter version and ESXi version you are using is vSphere 7.0U3 to 8.0U2.

Ensure that your RPAs are running on RecoverPoint for VMs 5.3.SP4 P1.

Ensure that your current system matches the scale limits of RecoverPoint for VMs 6.0.SP3 and later defined in *RecoverPoint for Virtual Machines Scale and Performance Guide*.

If the vCenter Server SSL certificate is changed, ensure that the new certificate is valid, and that the RecoverPoint for VMs is updated.

Ensure that the VIB URLs are trusted. See the VMware KB93130 for more information.

You can enable secure boot after upgrading to 6.0.SP3 and later.

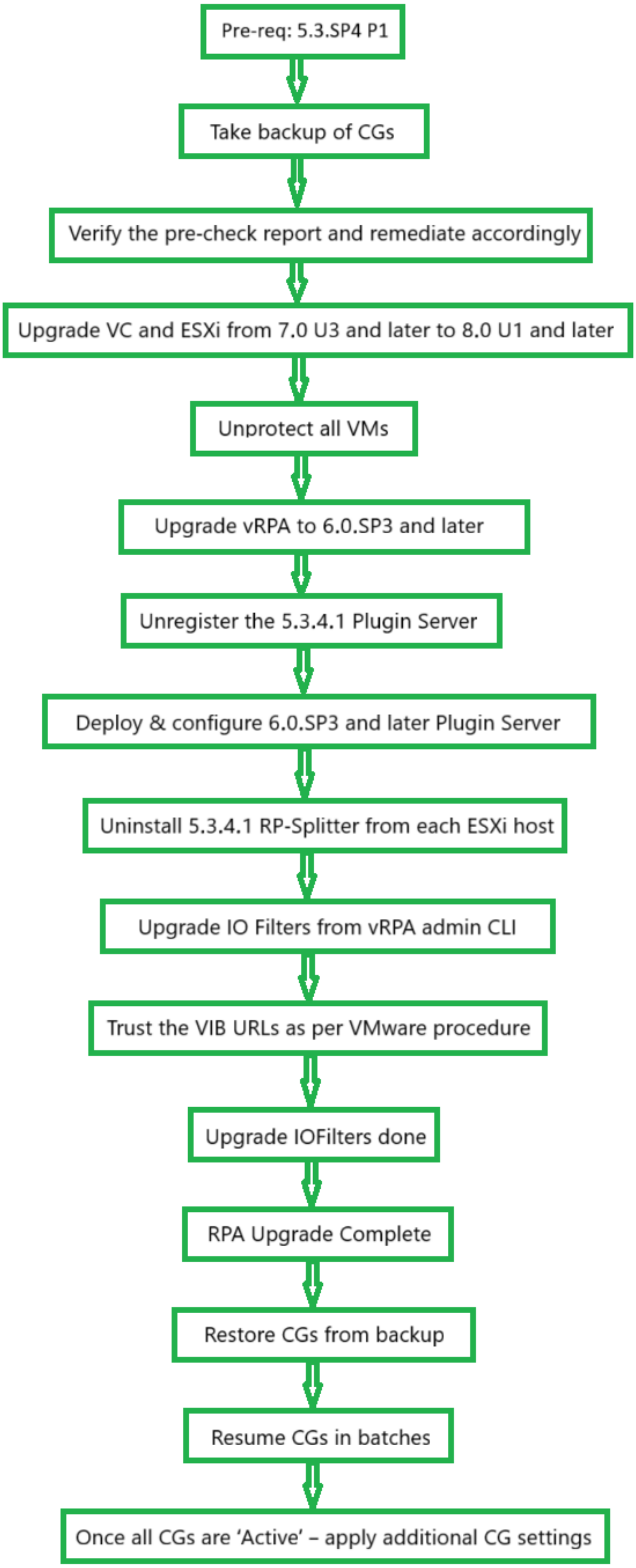
Ensure that there are no IDE disks available in the Virtual Machine that needs protection in your vSphere environment. RecoverPoint for VMs 6.0.SP1 and later does not support VM protection for IDE disk.

About this task

1. Backup:
   - Runs the pre-check automatically and creates a pre-check report.
   - Review the report manually and acknowledge.
   - Unprotect all CGs.
2. Upgrade or Migrate (5.3.4.1 → 6.0.3 and later) :
   - Follow the standard migration steps for migrating from the existing 5.3.4.1 version to 6.0.SP3 and later.
3. Restore
   - Deploy a binary patch to every RPA so that each CG restored thereafter begins in a paused state.

- Restore the compatible CGs from the backup automatically.
- Examine the restore-status report to spot any CGs that were skipped and may need manual handling.

4. Resume
    - Resume the CGs in batches (either using the script — random selection — or manually through the UI (based on user preference or priority)).
    - Limit each batch to ≤ 10 CGs to avoid high load problems in RPA.
5. Post-Restore Configuration
    - After all CGs show Active status, apply any additional CG settings that were backed up.
    - Revert the binary patch that was previously applied to all RPAs.



Pre-req: 5.3.SP4 P1

Take backup of CGs

Verify the pre-check report and remediate accordingly

Upgrade VC and ESXi from 7.0 U3 and later to 8.0 U1 and later

Unprotect all VMs

Upgrade vRPA to 6.0.SP3 and later

Unregister the 5.3.4.1 Plugin Server

Deploy & configure 6.0.SP3 and later Plugin Server

Uninstall 5.3.4.1 RP-Splitter from each ESXi host

Upgrade IO Filters from vRPA admin CLI

Trust the VIB URLs as per VMware procedure

Upgrade IOFilters done

RPA Upgrade Complete

Restore CGs from backup

Resume CGs in batches

Once all CGs are 'Active' – apply additional CG settings

Note: Do not attempt to upgrade multiple connected clusters at the same time.

Here are some key considerations and recommendations before proceeding:

- Do not run the script in parallel or on the same machine or on different machines. Running multiple instances can corrupt backup data or the CG configuration in the RP system.
- Always run only one instance at a time. If you restart or re-run the script, first terminate any existing script processes (close the script window or kill the process using Task Manager).
- Run the script from a Windows host on the same network as RPC or use a Windows VM as a host which is deployed in the VC.
- When re-running a backup, remove the previous backup folder or specify a new folder. Corruption of backup files or reports may occur.
- In a connected-cluster environment, use a single RPC IP for the backup and resume phases, and up to two RPC IP for the restore phase.
- After taking a backup in a connected-cluster setup, upgrade all clusters before initiating the restore. The backup-restore sequence should be performed only once.
- Pre-check before backup
  - The script runs a system pre-check and creates a precheck report that lists any limitations of RecoverPoint for Virtual Machines 6.0.SP3 and later depending upon the version which the user upgrades.
  - Review this report carefully; any parameter that exceeds the limits is skipped during restore and may require manual intervention.
  - The script cannot automatically verify every limitation. Refer to the Dell RecoverPoint for Virtual Machines Scale and Performance Guide, Dell RecoverPoint for Virtual Machines Release Notes to review the full list of limitations.
  - Resolve any non-compliant items (or make the environment RecoverPoint for Virtual Machines 6.0.3 and later compatible) before proceeding with the CG backup and restore.
- After the restore is complete, a detailed status report is generated. Review the status report after restore to identify any skipped CGs that need manual intervention.
- The script cannot restore VM priority or critical flags of consistency groups in the VM startup sequence. Note these settings before taking a backup and manually reassign the respective flags to each VM after the restore is complete.
- Resume CGs
  - CGs should be resumed in batches (recommended batch size <= 10CGs).
  - By default, the script uses a batch size of 10 and selects CGs randomly.
  - To manually resume CGs in the UI, keep the batch size under 10 to avoid excessive load on the RPAs.
- Post-restore configuration – Run the final script to apply any additional CG settings only after all CGs displays **Active** status.
- In large-scale environments, the whole process or only resuming CG process can take weeks or months, depending on factors such as VM size and protected CGs. Plan the process carefully by monitoring progress accordingly.
- The script does not work if datastores (where the protected VM resides) have space on their name.
- Protection or Unprotection does not work if a virtual machine has snapshots.

Steps

1. Download `migration_utility.zip` file from support site and extract to `backup_restore` directory on any Windows operating system. Change the directory to `backup_restore` and open Window command prompt or PowerShell prompt from that folder.

   NOTE: Extracted folder contains `cg_backup_restore_1.7.exe` and l`ibmanagement_libs-release.deb file`.

2. Take backup of CGs.
   a. Run the .exe in backup mode by entering the following command:

   ```
   cg_backup_restore_1.7 Script1 -a backup -i <RPC_IP> -u <USERERNAME> -p <PASSWORD>
   -o <BACKUP FOLDER NAME>
   ```

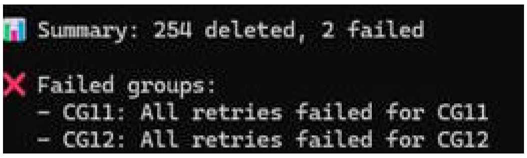
   Here `<USERERNAME>` and `<PASSWORD>` are VC username and password. `<RPC_IP>` is plugin server IP. For PowerShell, use `./cg_backup_restore_1.7`.

   b. Detailed `precheck_report.txt` is generated inside the backup folder for manual review.
3. If vCenter and ESXi are in 7.0U3, then first upgrade both to 8.0 U1 and later.
4. Unprotect all CGs.

a. Run the .exe in unprotect mode by entering the following command:

```
cg_backup_restore_1.7 Script1 -a unprotectall -i <RPC_IP> -u <USERERNAME> -p
<PASSWORD> -o <BACKUP FOLDER NAME>
```

i. Unprotection might fail for a few CGs with the error shown in the image here.



```
📊 Summary: 254 deleted, 2 failed

❌ Failed groups:
  - CG11: All retries failed for CG11
  - CG12: All retries failed for CG12
```

Verify if CG is still available in the plugin server UI. If CG is available, retry the unprotect command else ignore this error.

5. Upgrade from 5.3.4.1 to 6.0.3 and later.

a. Download the upgrade package. See the section The Upgrade and Maintenance package.

b. Upgrade vRPA clusters to 6.0.SP3 and later. See section Upgrade a vRPA cluster.

If there are multiple RP clusters that are installed in a VC, upgrade all RP Clusters.

When vRPA clusters are upgraded, older versions of RecoverPoint for VMs are shown under the vSphere summary section of vRPA virtual machine **vSphere Notes**. You can verify the upgraded RPA version from Plugin server UI or RecoverPoint CLI. If you want to see upgraded version in vSphere Notes, click **edit** button of vSphere Notes and update the new RecoverPoint for VMs version.

c. Uninstall the 5.3.SP4 P1 Plugin and Install the 6.0.SP3 and later plugin as follows:

i. In the RecoverPoint for VMs plugin for vSphere Client, select **System** > **vCenter Servers** > **Administration** > **vCenter Server**.

ii. Delete all vCenter Servers from the plugin server.

iii. Power off and remove the plugin server VM. See the section Uninstall the plugin server .

d. Deploy a new 6.0.SP3 and later plugin server. See the section Deploy the plugin server.

e. Configure the deployed plugin server. See the section Configure the plugin server.

f. Remove the 5.3.SP4 P1 Splitter from the hosts.

i. On the ESXi host, vMotion all VMs to another ESXi host.

ii. At ESXiCLI, enter maintenance mode. From the ESXi host console, use SSH to run the command `ESXicli system maintenanceMode set -e=true`

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

iii. To uninstall the splitter, enter the command `ESXicli software vib remove -n RP-Splitter`.

iv. Exit maintenance mode on the ESXi host by entering the command `ESXicli system maintenanceMode set -e=false`

g. Upgrade splitter and Jiraf for ESXi cluster. See the section Upgrade Splitter and Jiraf for Entire ESXi Cluster. This installs the 6.0.SP3 and later splitter and upgrades the Jiraf.

After removing the vSCSI Splitter from ESXi manually, the auto push mechanism may push the new RecoverPoint for VMs 6.0.3 and later Splitter to ESXi Cluster which is registered with RP.

After upgrade is complete, following message is displayed.

```
Upgrading ESXi splitter and JAM VIBs completed successfully
```

.

h. When the vRPAs, splitter, and Jiraf are migrated, check the ESXi cluster status. In the plugin, go to **System** > **ESXi Cluster** section.

Ensure that the ESXi cluster status is green. If the status is red:

i. Unregister the ESXi cluster. See the section Remove ESXi clusters from vRPA clusters.

ii. Reregister the removed ESXi cluster. See the section Register ESXi clusters.

6. Validate upgrade or migration.

a. After migration, ensure that all clusters are green in the dashboard and there are no critical errors.

7. Apply Binary patch fix on all RPAs.

a. Copy the `libmanagement_libs-release.deb` downloaded in Step1 to all the `/root` folder of RPA.

b. To perform backup of the original binary to /root, run the following command.

```
cp /usr/lib/recoverpoint/libmanagement_libs-release.so /root/libmanagement_libs-
release.so
```

c. To install the debug libs, run the following command in `/root`:

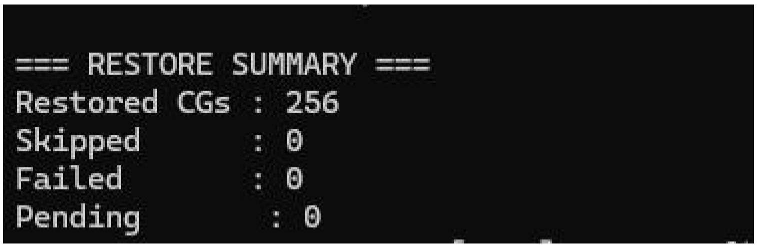
```
dpkg -i libmanagement_libs-release.deb
```

d. To kill the control process after lib replacement, do the following:
   i. Run the command `pkill -9 control_proces`
   ii. Wait until the dashboard returns to green status.

8. Restore all CGs.
   a. To run the .exe in restore mode, enter the following command:

```
cg_backup_restore_1.7 Script1 -a restore -i <RPC_IP> -u <USERERNAME> -p <PASSWORD>
-o <BACKUP FOLDER NAME> -e
```

   i. Give the same backup folder name as Step 2.
   ii. `-e` is required only when restoring Consistency Groups (CGs) using existing copy VMs. If you choose to create copy of VMs, this parameter is not needed in the command. However, the script may use the available datastores to create the replica copies.
   iii. Restored CGs are start in pause state.
   iv. For restore action, you can provide upto two RPC IP to manage restore load on the environment. For example : `-i 10.xx.xx.xx 10.xx.xx.xx` (space separated).
   v. In the restore summary shown here, if there are any pending CGs then do the following:



```
=== RESTORE SUMMARY ===
Restored CGs : 256
Skipped      : 0
Failed       : 0
Pending       : 0
```

   i. Open the `cg_status.txt` file generated inside the backup folder and check which Consistency Group (CG) entries have the status column marked as **PENDING**.
   ii. If the above CG is visible in the plugin server Consistency Groups list, it can be ignored. However, if it is not listed, retry the restore command.

9. Resume CGs in batches.
   a. To run the .exe in resume mode, enter the following command:

```
cg_backup_restore_1.7 Script2 -i <RPC_IP> -u <USERERNAME> -p <PASSWORD> -b 10
```

   b. The script selects 10 CGs based on ascending order of CG name list.
   c. 10 is the maximum number of CGs you can provide in a window.
   d. Script keeps all CGs in a queue and ensures that always 10 CGs are replicating in parallel.
   e. Detailed `cg_resume_status.txt` report is generated inside `resume_logs/resumereports` folder for manual review.

10. Apply post-restore configurations. Run this final script only if all CGs are in `Active` status.
   a. To run the .exe in post-restore mode, enter the following command:

```
cg_backup_restore_1.7 Script3 -i <RPC_IP> -u <USERERNAME> -p <PASSWORD> -o <BACKUP
FOLDER NAME>
```

   b. This command re-applies or restores additional CG settings such as:
      - Protection policies
      - Re-IP settings
      - Failover-network mappings

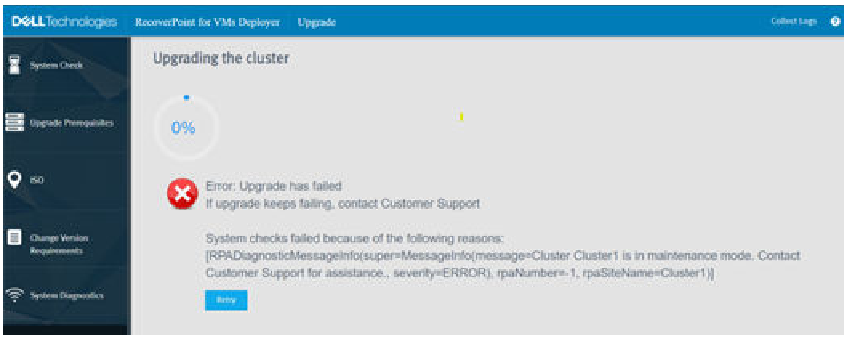
        - Copy policies
        - Additional remote copies
        - All Group Sets

11. Revert Binary patch fix applied in Step 7.
    a. To copy the backup binary back to the lib folder to revert the changes on all RPAs, do the following:
        i. Run the command `cp/root/libmanagement_libs-release.so /usr/lib/recoverpoint/`.
        ii. To kill the control process after lib replacement:
            i. Run the command `pkill -9 control_proces` .
        iii. Wait until the dashboard returns to green status.

Next steps

Troubleshoot the Migration Issues

- **Issue**: While removing the vSCSI splitter from the host, the error `can't remove '/tardisks/emcrpspl.t00' : Device or resource busy` appears.
    - **Resolution**: Use SSH to run the following commands from the ESXi host console:
        1. Put the host in maintenance mode: `ESXicli system maintenanceMode set -e=true`.
        2. Stop the splitter daemon manually: `/etc/init.d/rp-splitterd stop`.
        3. Remove the splitter: `ESXicli software vib remove -n RP-Splitter`.
        4. Exit the maintenance mode on the ESXi host: `ESXicli system maintenanceMode set -e=false`.
- **Issue**: In a multi cluster environment, when you upgrade all the vRPA cluster together, you can get **Upgrade has failed** error.



Error: Upgrade has failed
If upgrade keeps failing, contact Customer Support

System checks failed because of the following reasons:
[RPADiagnosticMessageInfo(super=MessageInfo(message=Cluster Cluster1 is in maintenance mode. Contact Customer Support for assistance., severity=ERROR), rpaNumber=-1, rpaSiteName=Cluster1)]

Figure 4. Cluster upgrade error

    - **Resolution**: Do not install the connected vRPA clusters together. Upgrade the connected clusters one after the other.
- **Issue**: Upgrade splitter fails with `Connection to server failed` error.
    - **Resolution**: Connection to the server can fail due to connectivity issue. Retry splitter upgrade. See the section Upgrade Splitter and Jiraf for Entire ESXi Cluster.
- **Issue**: Upgrade of Splitter and jiraf from the admin CLI fail with error `Operation failed. Failed getting vibs from ESXi <hostname>`.
    - **Resolution**: If any of the ESXi is still exiting maintenance mode, wait for it to complete and then retry upgrade from the admin CLI.
- **Issue**: Upgrade of JIRAF from admin CLI fails with error `Operation failed. Failed to install iofilter on <ESXi_hostname>`.
    - **Resolution**: Possible causes and their solutions are listed below:
        - If an error message is displayed for all ESXi, then rthe eason could be that VIB URLs are not trusted in VC. Trust the VIB URLs and retry the upgrade. See the section Trust Splitter and Jiraf vSphere Installation Bundle (VIB) URLs in vCenter
        - Maintenance mode issue can cause jiraf upgrade to fail in some ESXi. To confirm, check the table of splitter and jiraf versions that are displayed in the admin CLI. Follow the below steps to proceed,
            - From vSphere UI, check if problematic ESXi is still entering maintenance mode. If any maintenance tasks are running in the vSphere task console, wait for them to complete.
            - Identify why one or more ESXi servers are not moving into maintenance mode. To resolve this issue, manually move the problematic ESXi servers into maintenance mode.
            - After the above issue is resolved, vSphere Life-Cycle Manager (vLCM) triggers the task to upgrade the jiraf automatically.

- Log in to problematic ESXi and ensure that the jiraf is upgraded to the right version. Also verify the same at ESXi cluster level from vSphere using the path **ESXi Cluster** > **Configure** > **I/O Filters** > **URL**.
- If there is a mismatch of JIRAF version on ESXi server in above step, retry upgrade from admin CLI only after manually exiting from the maintenance mode on problematic ESXi.

6

Uninstalling RecoverPoint for VMs

You can uninstall a single vRPA cluster or all vRPA clusters from a vCenter.

The uninstaller tool scans the vCenter, datastores, and ESXi hosts. It removes vRPAs (production and copy VMs), configuration objects, and repository and journal volumes.

Topics:

Using the RecoverPoint for VMs uninstaller tool

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

Instructions for downloading the uninstaller tool are provided in Run the RecoverPoint for VMs uninstaller tool.

The uninstaller tool has the following 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.
- **`iof_uninstall`** - Uninstall iofilters (splitter and jiraf) from all provided VC's and their ESXi clusters.

Functions of uninstaller tool

The uninstaller tool removes vRPAs, shadow VMs, configuration objects, and repository and journal volumes.

Running the uninstaller 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.

The uninstaller tool does not remove plugin servers or splitter/JIRAFs. For further instructions, see Finishing up the uninstall.

NOTE: RP uninstaller tool internally uses a VMware API which puts multiple ESXi hosts into Maintenance Mode simultaneously while uninstalling the Splitter and JIRAF from all the hosts in the ESXI Cluster.

Preparing to uninstall vRPA clusters

Unprotect VMs

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

Steps

1. In the vSphere Web Client home page, click the **RecoverPoint for VMs Management icon** > **Protection** tab. Click **Virtual Machines**.

   Alternatively, in the vSphere Client home page, open the **RecoverPoint for VMs** menu, and click **Protection** > **Protected VMs**.
2. Select the VM you wish to stop replicating. Click the **Unprotect** icon. Repeat for each protected VM.

Remove ESX clusters from vRPA clusters

Unregister the ESX cluster of a production VM or copy VM, from a vRPA cluster.

Steps

1. Access the **plugin** in your vSphere client.

   Perform the following in the HTML5 plugin.
   a. Go to **System** > **ESX cluster**.
   b. To replicate remotely, select the vRPA cluster from which the ESX cluster must be unregistered.
2. Click the **Delete** icon next to each ESX cluster to unregister that ESX cluster from the specified vRPA cluster.

Results

The ESX cluster is unregistered from the specified vRPA cluster.

Uninstall a vRPA cluster

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

Prerequisites

- 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.

About this task

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 uninstaller tool.

Steps

1. In a web browser, type **`https://`*`<cluster_management-ip-address>`*** 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 admin 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 uninstaller tool

Download the uninstaller tool from Support as per the version being used, uncompress the *.bat* file, and run the tool in the command line.

Prerequisites

- Obtain the IP and TCP port number of the vCenter (or vCenters) you want to scan, the vCenter username (and domain name, if it exists), and the vCenter password.
- System requirements for the computer running the uninstaller tool:
  - Microsoft Windows
  - Java 8 or higher
- Ensure that DRS and vMotion are configured on the ESX cluster.

> **NOTE:** If a time difference of more than 30 minutes exists between the vRPA and the computer running the uninstaller tool, the tool may recognize the vRPA cluster as inactive when it is not. Different time zones do not influence the time difference.

Steps

1. Go 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.

   > **CAUTION: Use only the version of the uninstaller tool that is compatible with the RecoverPoint for VMs release that is installed on the vRPA cluster that you want to uninstall. For the latest support information, see the Simple Support Matrix for your version of RecoverPoint for VMs.**

2. From a computer with IP connectivity to the vCenters managing the RecoverPoint VMs you want to uninstall, extract the contents of the *.zip* file.
3. Double-click `uninstaller.bat`.
   The RecoverPoint for VMs uninstaller tool opens in a command line.
4. Perform one of the following actions:
   - Type **`uninstall`** to uninstall a single vRPA cluster from a vCenter.
   - Type **`full_rp_uninstall`** to uninstall all vRPA clusters from a vCenter.
   - Type **`--h`** after a command to view a description of that command.
   - Type **`help`** to view a brief description of all the available commands.
5. Enter the IP address of the vCenter.
6. Enter the TCP port number of the vCenter or press Enter for the default port (443).
7. Enter the username of the vCenter.
8. Enter the password of the vCenter.
   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 IP address of vCenter 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:
    - To uninstall 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`**).
    - To uninstall all vRPA clusters from a vCenter, type **`y`**.

11. If you have performed **`full_rp_uninstall`**, see Uninstall the RecoverPoint for VMs Splitter and Jiraf to uninstall *IOFilters* from VCs, and their ESXi clusters:

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.

The uninstaller tool does not remove the plug-in server.

- Do not remove a plug-in server that is still managing other vRPA clusters. Instead, *exclude* the vRPA cluster that you are uninstalling in order to stop the plug-in server from managing that vRPA cluster. For instructions on excluding a vRPA cluster (and clearing excluded clusters), see "Managing vRPA clusters on vCenters registered with the plug-in server" in the *RecoverPoint for VMs HTML5 Plugin Administrator's Guide*.
- If you want to uninstall the plug-in server, see Uninstall the plugin server.

Finishing up the uninstall

Perform the following tasks to complete the uninstall procedure.

Uninstall the plugin server

Use this procedure to uninstall the RecoverPoint for VMs plugin server.

Steps

1. In the RecoverPoint for VMs plugin for vSphere Client, select **System** > **Administration** > **vCenter Server**, and then select and delete.
2. Delete all vCenter Servers from the plugin server.
3. Power off and remove the plugin server VM.

Results

The plugin server is uninstalled.

Uninstall the RecoverPoint for VMs Splitter and Jiraf

Use the `uninstaller.bat` tool to uninstall the RecoverPoint for VMs splitter and jiraf.

Steps

1. Run `iof_uninstall`.

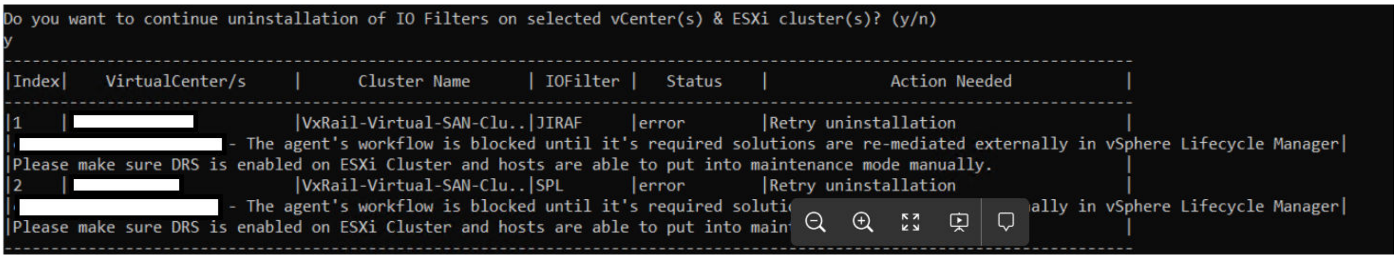
   This command removes splitter, and jiraf I/O filters completely from your vCenters and ESXi clusters.
2. A message is displayed `Would you like to proceed? (Y/N):`
   - Type **`Y`** if you want to continue to uninstall splitter and jiraf.
   - Type **`N`** to stop the uninstallation.
3. Enter the IP address of the vCenter.
4. Enter the TCP port number of vCenter or press **Enter** for the default port (443).
5. Enter the vCenter username.
6. Enter the vCenter password.
   A message is displayed `Checking vCenter connectivity vCenter is ready for scanning, do you want to add a new vCenter? (Y/N) or press Q to quit: .`
7. Type **`N`** if you do not want to add another vCenter to remove I/O filters or Type **`Y`** if you want.
   The scanning ESXi Clusters:

   (1) *<Cluster-Name>* v

   (2) All

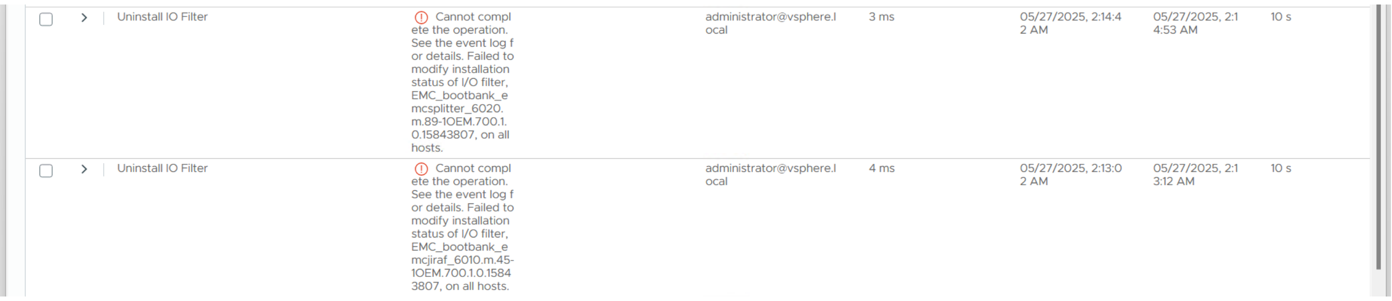
8. Ensure to enter a comma-separated ESXi cluster number (such as 1, 2) / All:
   A message is displayed `Do you want to continue uninstallation of IO Filters on selected vCenter(s) and ESXi cluster(s)? (Y/N).`
9. Type **Y** to complete the uninstallation.

   ⓘ **NOTE:** If a single image is enabled on esxi cluster then removal of splitter, and Jiraf will fail with the following error:

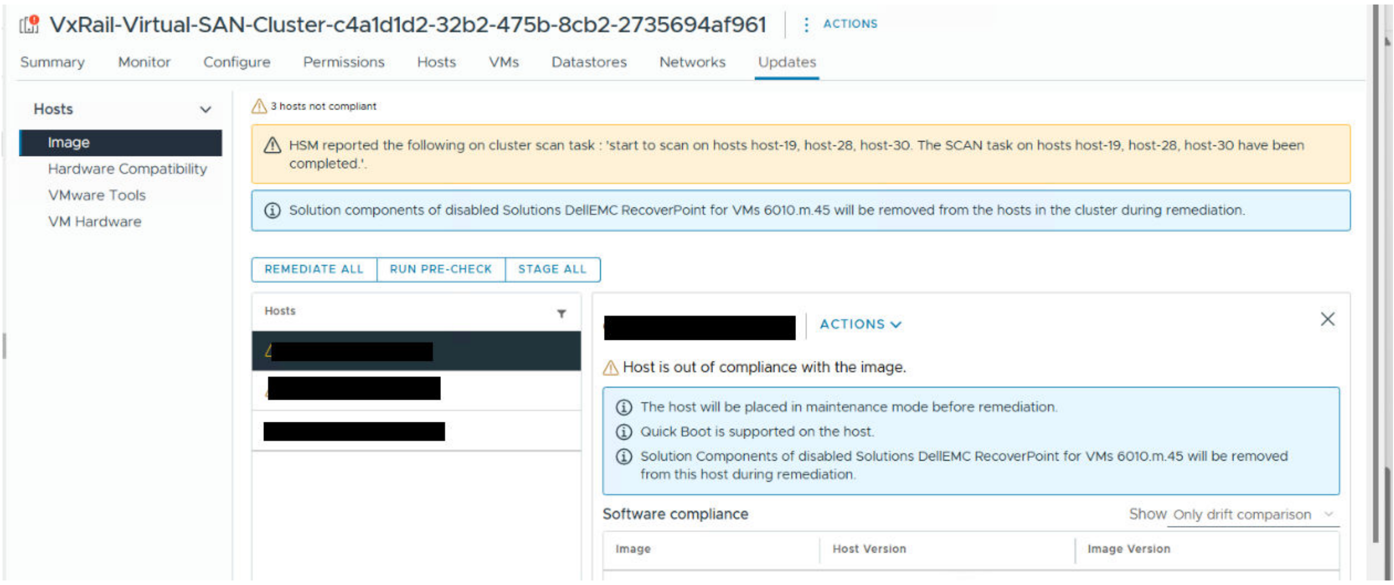
```
Do you want to continue uninstallation of IO Filters on selected vCenter(s) & ESXi cluster(s)? (y/n)
y
----------------------------------------------------------------------------------------------------------------------
|Index|    VirtualCenter/s      |       Cluster Name       | IOFilter |  Status     |            Action Needed         |
----------------------------------------------------------------------------------------------------------------------
|1    | [redacted]              |VxRail-Virtual-SAN-Clu..|JIRAF     |error        |Retry uninstallation              |
|[redacted]                      - The agent's workflow is blocked until it's required solutions are re-mediated externally in vSphere Lifecycle Manager|
|Please make sure DRS is enabled on ESXi Cluster and hosts are able to put into maintenance mode manually.                   |
|2    | [redacted]              |VxRail-Virtual-SAN-Clu..|SPL       |error        |Retry uninstallation              |
|[redacted]                      - The agent's workflow is blocked until it's required soluti                 ally in vSphere Lifecycle Manager|
|Please make sure DRS is enabled on ESXi Cluster and hosts are able to put into main                                         |
----------------------------------------------------------------------------------------------------------------------
```

   From the vSphere recent tasks the user sees below error.

□	>	Uninstall IO Filter	ⓘ Cannot complete the operation. See the event log for details. Failed to modify installation status of I/O filter, EMC_bootbank_emcsplitter_6020.m.89-1OEM.700.1.0.15843807, on all hosts.	administrator@vsphere.local	3 ms	05/27/2025, 2:14:42 AM	05/27/2025, 2:14:53 AM	10 s
□	>	Uninstall IO Filter	ⓘ Cannot complete the operation. See the event log for details. Failed to modify installation status of I/O filter, EMC_bootbank_emcjiraf_6010.m.45-1OEM.700.1.0.15843807, on all hosts.	administrator@vsphere.local	4 ms	05/27/2025, 2:13:02 AM	05/27/2025, 2:13:12 AM	10 s

   The next step is to make the host compliant with the image where we must remediate all the hosts using the **Remediate all** option :`<ESX_cluster_name> → Updates → Hosts → Image → Remediate All`

   ⚠ 3 hosts not compliant

   ⚠ HSM reported the following on cluster scan task : 'start to scan on hosts host-19, host-28, host-30. The SCAN task on hosts host-19, host-28, host-30 have been completed.'.

   ⓘ Solution components of disabled Solutions DellEMC RecoverPoint for VMs 6010.m.45 will be removed from the hosts in the cluster during remediation.

   [redacted]

   [redacted]

   [redacted]

   [redacted]

   ⚠ Host is out of compliance with the image.

   ⓘ The host will be placed in maintenance mode before remediation.

   ⓘ Quick Boot is supported on the host.

   ⓘ Solution Components of disabled Solutions DellEMC RecoverPoint for VMs 6010.m.45 will be removed from this host during remediation.

   This Remediation removes both Splitter and Jiraf from Esxi.

10. Follow the steps below to check if splitter and jiraf filters are removed from vSphere:
    a. At the cluster level, select **ESX_cluster_name** > **Configure** > **I/O Filters**
    b. At the ESXi host level, click an ESX, then select **Configure** > **I/O Filters**.

    - If you only see I/O filters at the cluster level, rerun the command `iof_uninstall` in the Uninstaller tool.

      Or,
    - If you only see I/O filters at the ESXi host level, you must manually remove the filters by performing the following steps.
      a. On the ESXi host, vMotion all VMs to another ESXi host.

b. At ESXCLI, enter **Maintenance** mode. From the ESXi host console, use SSH to run the following command:

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

> **NOTE:** This command requires an additional switch for vSAN environments. See the *vSphere documentation* for the vSphere version that you are using.

c. To uninstall the splitter, enter the following command:

```
esxcli software vib remove -n emcsplitter
```

Or,

To remove the JAM VIB (While still in **Maintenance** mode), run the following command:

```
esxcli software vib remove -n emcjiraf
```

d. Exit Maintenance mode on the ESXi host by entering the following command:

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

Removing Stale RecoverPoint (RP) License Entries from VC MOB

About this task

License entries are removed automatically post RP cluster uninstallation However, if stale license entries are still visible in the VC MOB, these must be removed manually.

Steps

Verify and delete the custom attribute config.Recoverpoint_LICENSES from VC:

- Open **vSphere Client**.
- Go to **Tags and Custom Attributes**.
- Locate the custom attribute named config.Recoverpoint_LICENSES.
- Select this attribute and delete it.

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.

The topics in this chapter provide procedures needed for installing RecoverPoint for VMs with VxRail.

Topics:

Deploying RecoverPoint for VMs in a VxRail™ environment

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

About this task

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, Deploy vRPAs, and Install vRPA clusters.

Downloading from the VxRail Marketplace

Download the latest qualified RecoverPoint for VMs release.

About this task

Download the latest RecoverPoint for VMs release from the VxRail manager marketplace or RecoverPoint for Virtual Machines download page.

Preparing the network for VxRail

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

About this task

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.

Steps

- 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. For this configuration, define two port groups: RP_WAN+LAN and RP_DATA.
- 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_DATA1, RP_DATA2.

Create vRPAs for VxRail

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

About this task

When creating vRPAs:

Steps

1. In the **Select storage** screen, in the **VM Storage Policy** drop down, select **VxRail-Virtual-SAN-Datastore**. The compatible VSAN datastore will be selected.
2. 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.

Steps

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.

   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:

Table 7. Traffic shaping values

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

Create a vRPA cluster for VxRail

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

About this task

When creating a vRPA cluster:

Steps

1. In the **Environment Settings** step, select the vSAN datastore from the table of available datastores.
2. In the **Network Settings** step of the wizard, specify the vRPA data 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.

About this task

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

Steps

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 data network adapters for enabling splitter-to-vRPA communication.
3. If you created a new ESXi cluster, register it 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.

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.

Steps

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 admin username and password to log in to the Admin CLI. Then select **System management CLI** to open the Sysmgmt CLI. Alternatively, if you have created a user with the sysmgmt role, use that user to log in directly to the Sysmgmt CLI. To check the cluster status, use the `get_system_status` Sysmgmt CLI command. Choose to retrieve the status of all categories.
3. 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.

Steps

1. Check the RecoverPoint for VMs dashboard for error events indicating that the vRPA cannot access storage or communicate with the splitters.
2. Create an SSH connection to a surviving vRPA, using your RecoverPoint for Virtual Machines admin username and password to log into the Admin CLI. Then select **System management CLI** to open the Sysmgmt CLI. Alternatively, if you have created a user with the sysmgmt role (RecoverPoint for Virtual Machines 5.2.0.2 or later), use that user to log in directly to the Sysmgmt CLI. Use the `get_system_status` Sysmgmt CLI command to check the cluster status. Choose to retrieve the status of all categories.
3. Confirm that the detached vRPA cannot be reached from the surviving vRPA.
4. Log in to the Admin CLI of the detached vRPA using admin username and password, 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.

Steps

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 iofltd-emcsplit`**
   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.

8

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.

These troubleshooting procedures use the vSphere Web Client.

Some commands that may be useful in troubleshooting can be run from the root user, including: ethtool, kps.pl, ping6, uptime, date, ssh, telnet, arping32, switch utils (Dell Technologies Customer Support only), netstat, arp, ping, top, and su.

Topics:

Troubleshooting RecoverPoint for VMs Deployment

The following table lists the error messages and their troubleshooting steps that you may encounter during RecoverPoint for VMs deployment.

Table 8. RecoverPoint for VMs deployment errors

Error message	Troubleshooting steps
`An error occurred during host configuration in the task console`	1. Identify the error in the **Tasks** Console of vSphere Client **Menu** > **Tasks** 2. Check for the error `An error occurred during host configuration` and identify the target hostname. 3. Keep the target host into **Maintenance** Mode. 4. Reboot the target host to discard the unfinished updates. 5. Go to **RecoverPoint of VMs Deployer** wizard page, and then click **Retry** to restart the cluster installation.
`The specified key, name, or identifier vibUrl already exists in the task console`	1. Identify the error in the **Task** console of vSphere Client. **Menu** > **Tasks** 2. Check for the error message `The specified key, name, or identifier vibUrl already exists.` 3. Uninstall the Splitter and jiraf from using RecoverPoint for VMs `uninstaller.bat` tool. For more

Table 8. RecoverPoint for VMs deployment errors (continued)

Error message	Troubleshooting steps
	information, see Uninstall the RecoverPoint for VMs Splitter and Jiraf . 4. After uninstallation, go to **RecoverPoint of VMs Deployer** wizard page, and then click **Retry** to restart the cluster installation.
The following errors are found in `esxupdate.log` file: - `esxupdate[13426927]: Download failed: <urlopen error [Errno -2] Name or service not known>, 1 retry left...` - `esxupdate[13426927]: An esxupdate error exception was caught:`	1. Select **ESXI host** > **Configure** > **TCP/IP Configuration** . 2. Click **Default** and edit the configuration. 3. Enter the following: - Preferred DNS server - Alternate DNS server - Domain 4. Click **Save** to save the setting. 5. Click **Retry from WDM** to continue the cluster installation.

`The operation is not allowed in the current state`
The `vpxd.log` file includes the following error messages:
`-->       msg =`
`""com.vmware.eam.security.trust.NotTrusted:`
`Suitable trust, not found!" caused by`
`"org.bouncycastle.tls.TlsFatalAlert:`
`certificate_unknown(46)" caused by`
`"java.security.cert.CertificateException:`
`Unable to construct a valid chain" caused by`
`"java.security.cert.CertPathBuilderException:`
`Unable to find certificate chain."`
`Please follow KB 93130"`
`-->    },`
`-->    faultMessage = <unset>,`
`-->    url = https://10.0.0.1/RPResources/iof/esx8/`
`EMC-RP4VMs-SPL_6011.m.64-1OEM.700.1.0.15843807.zip`
`-->    msg =`
`"Received SOAP response fault from`
`[<<cs p:00007fc3a425bc90, TCP:localhost:1080>, /eam/`
`sdk>]:`
`packageContent`
`--> "com.vmware.eam.security.trust.NotTrusted:`
`Suitable trust, not found!" caused by`
`"org.bouncycastle.tls.TlsFatalAlert:`
`certificate_unknown(46)" caused by`
`"java.security.cert.CertificateException:`
`Unable to construct a valid chain"`
`caused by`
`"java.security.cert.CertPathBuilderException:`
`Unable to find certificate chain.`
`" Please follow KB 93130"`
`--> }`
	1. Identify the error in the **Tasks** console of vSphere client. **Menu** > **Tasks**
	NOTE: Simultaneously, WDM displays a status of `53% failure with splitter deployment error.`
	2. This error may occur if you do not trust splitter and JAM URLs into VC as mentioned in the prerequisite of the section Install vRPA Clusters.
	3. Trust the URL and click **Restart Wizard** from WDM.

The RP cluster installation fails at 53% in the vSphere **Tasks** console and displays the following error:
`The operation is not allowed in the current state`
The `eam.log` file includes the following error message:
`024-02-13T10:08:31.186Z |  INFO | vim-monitor |`
`ExtensionSessionRenewer.java | 190 |`
`[Retry:Login:com.vmware.vim.eam:9a80e40bc4406cea] Re-`
	- The error may occur due to changes in the VC certificate, resulting in a sudden abortion of the VIB installation process. Follow VMware KB article 2112577

Table 8. RecoverPoint for VMs deployment errors (continued)

<table>
<tr><th>Error message</th><th>Troubleshooting steps</th></tr>
<tr><td>login to vCenter
because method: currentTime of managed object:
null::ServiceInstance:ServiceInstance failed due to
expired client session: null
2024-02-13T10:08:31.186Z | INFO | vim-monitor |
OpId.java | 37 |
[vim:loginExtensionByCertificate:bb9120d621eff4e8]
created from
[Retry:Login:com.vmware.vim.eam:9a80e40bc4406cea]
2024-02-13T10:08:31.779Z | ERROR | vlsi |
DispatcherImpl.java | 468 | Internal server error
during dispatch
com.vmware.vim.binding.eam.fault.EamServiceNotInitial
ized:
EAM is still loading from database.
Please try again later.
 at
com.vmware.eam.vmomi.EAMInitRequestFilter.handleBody(
EAMInitRequestFilter.java:57)
~[eam-server.jar:?]
 at
com.vmware.vim.vmomi.server.impl.DispatcherImpl$Singl
eRequestDispatcher.handleBody
(DispatcherImpl.java:373) [vlsi-server.jar:?]
 at
com.vmware.vim.vmomi.server.impl.DispatcherImpl$Singl
eRequestDispatcher.dispatch
(DispatcherImpl.java:290) [vlsi-server.jar:?]
 at
com.vmware.vim.vmomi.server.impl.DispatcherImpl.dispa
tch
(DispatcherImpl.java:246) [vlsi-server.jar:?]
 at
com.vmware.vim.vmomi.server.http.impl.CorrelationDisp
atcherTask.run
(CorrelationDispatcherTask.java:58) [vlsi-
server.jar:?]
 at
java.util.concurrent.ThreadPoolExecutor.runWorker
(ThreadPoolExecutor.java:1149) [?:1.8.0_341]
 at
java.util.concurrent.ThreadPoolExecutor$Worker.run(Th
readPoolExecutor.java:624)
[?:1.8.0_341]
        at java.lang.Thread.run(Thread.java:750)
[?:1.8.0_341]
2024-02-13T10:08:35.199Z | INFO | vim-async-1 |
OpIdLogger.java | 43 |
[vim:loginExtensionByCertificate:bb9120d621eff4e8]
Failed.
2024-02-13T10:08:35.199Z | WARN | vim-async-1 |
ExtensionSessionRenewer.java | 227 |
[Retry:Login:com.vmware.vim.eam:9a80e40bc4406cea] Re-
login failed, due to:
com.vmware.eam.security.NotAuthenticated: Failed to
authenticate extension
com.vmware.vim.eam to vCenter.
 at
com.vmware.eam.vim.security.impl.SessionManager.conve
rtLoginException
(SessionManager.java:295) ~[eam-server.jar:?]
 at
com.vmware.eam.vim.security.impl.SessionManager.lambd
a$loginExtension$4
(SessionManager.java:154) ~[eam-server.jar:?]
 at
com.vmware.eam.async.remote.Completion.onError
(Completion.java:86) [eam-server.jar:?]</td><td></td></tr>
</table>

Table 8. RecoverPoint for VMs deployment errors (continued)

Error message	Troubleshooting steps

`at`
`com.vmware.eam.vmomi.async.FutureAdapter.setException`
`(FutureAdapter.java:81) [eam-server.jar:?]`
`at`
`com.vmware.vim.vmomi.client.common.impl.MethodInvocat`
`ionHandlerImpl$`
`ClientFutureAdapter.setException`
`(MethodInvocationHandlerImpl.java:731) [vlsi-`
`client.jar:?]`
`at`
`com.vmware.vim.vmomi.client.common.impl.MethodInvocat`
`ionHandlerImpl$`
`RetryingFuture.fail`
`(MethodInvocationHandlerImpl.java:578) [vlsi-`
`client.jar:?]`	

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.

Steps

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 admin username and password to log in to the Admin CLI. Then select **System management CLI** to open the Sysmgmt CLI. Alternatively, if you have created a user with the sysmgmt role, use that user to log in directly to the Sysmgmt CLI. To check the cluster status, use the `get_system_status` Sysmgmt CLI command. Choose to retrieve the status of all categories.
3. 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.

Steps

1. Check the RecoverPoint for VMs dashboard for error events indicating that the vRPA cannot access storage or communicate with the splitters.
2. Create an SSH connection to a surviving vRPA, using your RecoverPoint for Virtual Machines admin username and password to log into the Admin CLI. Then select **System management CLI** to open the Sysmgmt CLI. Alternatively, if you have created a user with the sysmgmt role (RecoverPoint for Virtual Machines 5.2.0.2 or later), use that user to log in directly to

the Sysmgmt CLI. Use the `get_system_status` Sysmgmt CLI command to check the cluster status. Choose to retrieve the status of all categories.

3. Confirm that the detached vRPA cannot be reached from the surviving vRPA.
4. Log in to the Admin CLI of the detached vRPA using admin username and password, 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.

Steps

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 iofltd-emcsplit`**
   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 and investigate logs.

Steps

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 iofltd-emcsplit`**.
   b. Check the current status of splitter processes run: /etc/init.d/iofilterd-emcsplitter status.

      If splitter processes are not running, to start run: /etc/init.d/iofilterd-emcsplitter start.
3. To investigate the root cause of the splitter failure, collect logs.
4. If you are using a licensed version of RecoverPoint for VMs, contact Customer Support.

Troubleshooting Trust Splitter and Jiraf VIB URLs Issues

The following table presents error messages that may occur during the vCenter upgrade process and provides the necessary troubleshooting steps.

Table 9. Trust Splitter and Jiraf Issues

Error Messages	Troubleshooting Steps

You may encounter the following error while upgrading vCenter from 8.0 U1c to 8.0 U2b:
`Source ESX Agent Manager Configuration contains URLs`
`that are not trusted by the system!`
	- Trust the untrusted splitter and jiraf VIB URLs listed during the pre-check, as described in the Prerequisites subsection under vCenter Upgrade.

Troubleshooting Splitter and Jiraf Upgrade Issues

The following table presents error messages that may occur during the splitter and jiraf upgrade process and provides the necessary troubleshooting steps.

Table 10. Splitter and Jiraf Upgrade Issues

Error Messages	Troubleshooting Steps

The I/O filter upgrade task fails in vCenter 8.0 U2b or later and displays the following error in the vSphere **Tasks** console:
`The operation is not allowed in the current state.`
The `vpxd.log` file includes the following error messages:
`-->       msg =`
`""com.vmware.eam.security.trust.NotTrusted:`
`Suitable trust, not found!" caused by`
`"org.bouncycastle.tls.TlsFatalAlert:`
`certificate_unknown(46)" caused by`
`"java.security.cert.CertificateException:`
`Unable to construct a valid chain" caused by`
`"java.security.cert.CertPathBuilderException:`
`Unable to find certificate chain."`
`Please follow KB 93130"`
`-->    },`
`-->    faultMessage = <unset>,`
`-->    url = https://10.0.0.1/RPResources/iof/esx8/EMC-`
`RP4VMs-SPL_6011.m.64-1OEM.700.1.0.15843807.zip`
`-->    msg =`
`"Received SOAP response fault from`
`[<<cs p:00007fc3a425bc90, TCP:localhost:1080>, /eam/`
`sdk>]:`
`packageContent`
`--> "com.vmware.eam.security.trust.NotTrusted:`
`Suitable trust, not found!" caused by`
`"org.bouncycastle.tls.TlsFatalAlert:`
`certificate_unknown(46)" caused by`
`"java.security.cert.CertificateException:`
`Unable to construct a valid chain"`
`caused by`
`"java.security.cert.CertPathBuilderException:`
`Unable to find certificate chain.`
`" Please follow KB 93130"`
`--> }`
	- Trust splitter and upgrade the JAM VIB URLs as described in the section Trust Splitter and Jiraf vSphere Installation Bundles (VIBs) in vCenter. Follow KB article 93130 for more information.

Table 10. Splitter and Jiraf Upgrade Issues (continued)

Error Messages	Troubleshooting Steps
You may encounter the following error in both the SU tool and the vSphere **Tasks** console while upgrading the splitter and jiraf: `Cannot complete the operation. See the event log for details.`	1. Check the filter MOB URL version in vSphere by selecting **ESX Cluster Name** > **Configure** > **I/O Filters** 2. If the MOB URL appears with an upgraded filter version, put each ESX into **Maintenance** mode. vSphere Life Cycle Manager (vLCM) triggers the install agent task to upgrade the filters.
The splitter upgrade process fails and displays the following error in the SU tool: `The operation is not allowed in the current state.`	The ESXi image profile retains the older version even after upgrading to ESXi 8.0 U2b. It is advised to consider upgrading the ESXi image profile to the same version as a potential resolution for this error.
The splitter or jiraf upgrade fails and displays the following error in the SU tool: `Operation failed. Failed on ESXi VMs_Cluster: Operation timed out.`	1. Check the vSphere **Tasks** console to see if any **Maintenance** mode tasks are still running for any ESX. If any tasks are running, wait for them to finish. 2. Run the upgrade from the RPA SU tool again. 3. Manually exit **Maintenance** mode for any ESX that are still in it, once the upgrade completes. 4. Verify at the ESX cluster level in vSphere. Select **ESX Cluster** > **Configure** > **I/O Filters** > **URL** 5. Check the **URL** field to ensure that the vSphere has the upgraded version of splitter and jiraf.
Upgrade of Splitter / JIRAF from admin CLI fail with error `Operation failed. Failed to install iofilter on <ESX_hostname>`	Possible causes and their solutions are listed below: ● If error message coming for all ESX then reason could be VIB URLs are not trusted in VC. Trust the VIB URLs and retry the upgrade. See section Trust Splitter and Jiraf vSphere Installation Bundle (VIB) URLs in vCenter ● Maintenance mode issue can cause Splitter/jiraf upgrade to fail in some ESXi. To confirm, check the table of splitter and jiraf versions that are displayed in the admin CLI. Follow below steps to proceed, ○ From vSphere UI, check if problematic ESXi is still entering maintenance mode. If any maintenance tasks are running wait for them to complete. ○ Identify why one or more ESX servers are not moving into maintenance mode. To resolve this issue we can try to manually move the problematic

Table 10. Splitter and Jiraf Upgrade Issues (continued)

Error Messages	Troubleshooting Steps
	ESX servers into maintenance mode. ○ Once the above issue is resolved, vSphere Life-Cycle Manager (vLCM) triggers the task to upgrade the splitter/Jiraf automatically. ○ Manually exit problematic ESX from maintenance mode and Retry upgrade from admin CLI.

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

About this task

Go through the following steps until the problem is resolved:

Steps

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

About this task

Go through the following steps until the problem is resolved:

Steps

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.
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.

Changing the plugin server certificate

Use the following procedure to change the plugin server certificate before the plugin server has been configured using **Deployment Manager**.

About this task

Perform the following steps if you want to use a certificate that the internal certificate authority of your organization signs.

Steps

1. Connect to the plugin server with root permissions.
2. Create a backup of the existing certificate and key files:

   `/etc/nginx/ssl/rpcenter.cert`

   `/etc/nginx/ssl/rpcenter.key`
3. Disable the firewall on the plugin server.

   Run the command **`/sbin/SuSEfirewall2 off`**.
4. Upload the new certificate and key files to `/etc/nginx/ssl`.
5. Rename the new certificate file to **`rpcenter.cert`** and the new key file to **`rpcenter.key`**.
6. Reboot the plugin server VM.
7. In the **RecoverPoint for VMs Deployer**, click **Configure plugin server** home screen.

   Enter the **`plugin server IP address`** in IPv4 format, confirm the new certificate, and click **Configure**.

   For more information, see the Configure the plugin server.

Results

RecoverPoint for VMs is configured to use the new plugin server certificate.

Next steps

NOTE:

Check that the certificate is the same across all vRPAs of the same cluster before adding the vRPA to the cluster.

Log in to vSphere Client from the relevant vCenter Server and check that the RecoverPoint for VMs HTML5 plugin is displayed.

Changing a registered plugin server certificate

Use the following procedure to change the plugin server certificate after the plugin server has already been configured using **Deployment Manager**.

About this task

Perform the following steps if you want to use a certificate that the internal certificate authority of your organization has signed.

Steps

1. Connect to the plugin server with root permissions.
2. Create a backup of the existing certificate and key files:

   `/etc/nginx/ssl/rpcenter.cert`

   `/etc/nginx/ssl/rpcenter.key`
3. Disable the firewall on the plugin server.

   Run the command **`/sbin/SuSEfirewall2 off`**.
4. Upload the new certificate and key files to `/etc/nginx/ssl`.
5. Rename the new certificate file to **`rpcenter.cert`** and the new key file to **`rpcenter.key`**.
6. Power off the plugin server VM.

7. Unregister the RecoverPoint for VMs HTML5 plugin from the relevant vCenter Server.

   See Unregistering the plugin from the Managed Object Browser.
8. Power on the plugin server VM.
9. Go to `https://RPCIP/ui`.
10. Click **Authorize** and enter the vCenter Server Credentials.
11. Go to **DELETE /vcs/{vc-id}** near the bottom of the Swagger page.
12. Select **Try it Out**, enter the vCenter Server serial number, and select **Execute**.
    A 204 response is returned.
13. In the **RecoverPoint for VMs Deployer**, click **Configure plugin server** home screen.

    Enter the **`plugin server IP address`** in IPv4 format, confirm the new certificate, and click **Configure**.

    For more information, see the Configure the plugin server.

Results

RecoverPoint for VMs is configured to use the new plugin server certificate.

Next steps

NOTE:

Ensure that the certificate is the same across all vRPAs of the same cluster before adding the vRPA to the cluster.

Log in to vSphere Client from the relevant vCenter Server and check that the RecoverPoint for VMs HTML5 plugin is displayed.

Updating the certificate

Use this procedure to update the changed vCenter or vRPA certificates to RPC from WDM.

Steps

1. Click on **Update Certificate Information** in WDM.
2. You are prompted to switch to management server IP.
3. In the **Update Certificate wizard**, enter the plugin server IP and click on **Update Certificate Information**.

Results

Invalid certificates are removed, and new certificates are available in RPA and RPC.

Troubleshooting RecoverPoint for VMs replication

The topic describes how to troubleshoot these conditions:

- Consistency group is in a high-load transfer state, or initialization is not completing
- Consistency group is in error state
- Issue while unprotecting consistency group
- Consistency group in paused state during vmotion of VM between ESX clusters

CG in high-load transfer state or initialization not completing

Steps

1. If consistency groups are not balanced across vRPAs, create an SSH connection to the vRPA management IP address, and type the RecoverPoint admin username and password to log in to the Admin CLI. Then select **System management CLI** to open the Sysmgmt CLI. Alternatively, if you have created a user with the sysmgmt role, use that user to log in directly to the Sysmgmt CLI. Run the `balance_load` Sysmgmt CLI command and change consistency group assignments. For more information about load balancing, see the *RecoverPoint for Virtual Machines Administrator's Guide*.
2. 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.

3. Enabling deduplication when WAN compression is also enabled may overload the vRPA and therefore degrade replication performance.
    a. It is recommended to enable WAN and journal compression and disable deduplication.
    b. If the consistency group contains more than one VM, consider moving VMs to dedicated consistency groups and using group sets as needed.
    c. Review ESXi resources to ensure that there is no contention.
4. Create an SSH connection to the vRPA management IP address, and type the RecoverPoint admin username and password to log in to the Admin CLI. Then select **System management CLI** to open the Sysmgmt CLI. Alternatively, if you have created a user with the sysmgmt role, use that user to log in directly to the Sysmgmt CLI. Run the `config_io_throttling` command to slow down production storage reads during the full sweep process.

Consistency group is in Error state

Steps

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.

CG in paused state during vmotion of VM between ESX clusters

Table 11. CG in paused state during vmotion of VM between ESX clusters

Issue	Resolution
When a protected VM is vmotioned to a ESX cluster which is not registered to the current RP cluster , CG enters paused state.	To resolve this issue, manually register a new ESX cluster to RP cluster of protected VM using below steps. From the plugin server click **System** and then **Administration > select respective RP cluster from drop down** click **Add to add ESX cluster**

Issue While Unprotecting Consistency Group

- Issue : In RecoverPoint for VMs 6.0 or later if you unprotect a VM which already has snapshots, the RPC shows the error: `Please remove or consolidate the snapshots of all the VMs in the consistency group.`

  Resolution : Remove snapshots from the VM and unprotect it.

- Issue : After CG Unprotection , shadow VM is not getting converted to copy VM.

  Resolution :

  Follow the steps below:

  1. From vSphere for problematic shadow VM , Change from RP storage policy to “Datastore Default” policy using the path, right click **shadow VM > VM Policies > Edit VM Storage Policies >** select **VM Storage policy as Datastore Default >** click **OK**

     NOTE: Even if the storage policy is showing Datastore Default policy select the same again and click OK.

  2. Power off shadow VM. This should convert shadow VM to copy VM automatically in a few mins.
  3. If the above step is not working, then directly delete shadow VM.

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.

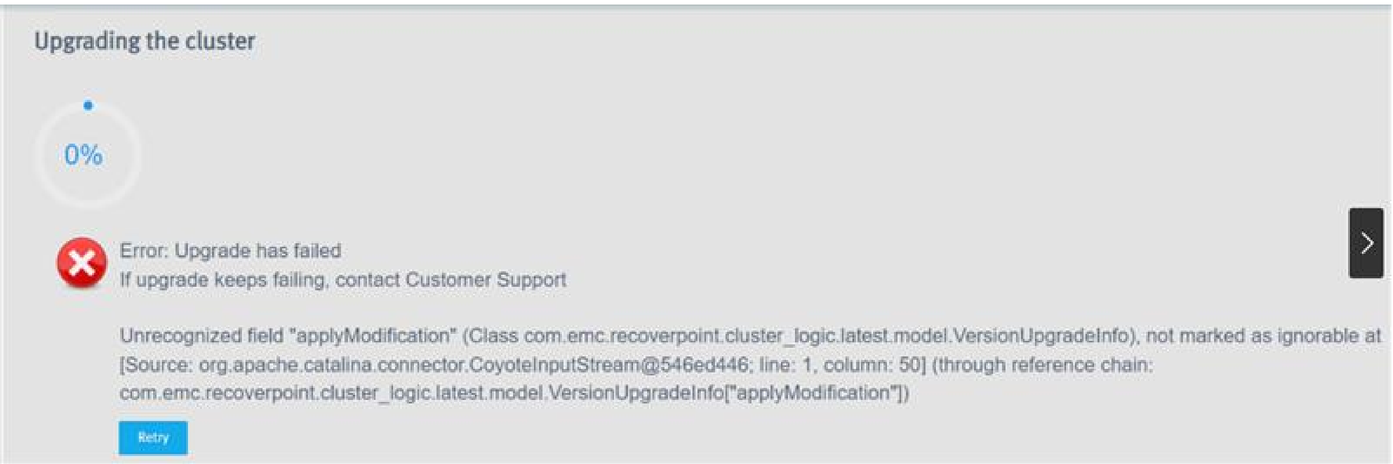
Troubleshooting RecoverPoint for VMs NDU

This section describes how to troubleshoot below condition.

After migrating from version 5.3.4.1 to 6.0.1.2 and subsequently performing an NDU to 6.0.2.1, the upgrade process may fail due to browser cache-related issues.

Symptoms

You may encounter an error during the upgrade (see screenshot below).



Error: Upgrade has failed
If upgrade keeps failing, contact Customer Support

Unrecognized field "applyModification" (Class com.emc.recoverpoint.cluster_logic.latest.model.VersionUpgradeInfo), not marked as ignorable at [Source: org.apache.catalina.connector.CoyoteInputStream@546ed446; line: 1, column: 50] (through reference chain: com.emc.recoverpoint.cluster_logic.latest.model.VersionUpgradeInfo["applyModification"])

Root Cause

Stale data from the browser cache can interfere with the upgrade flow, leading to unexpected failures.

Resolution

- Clear the browser cache and retry the upgrade.
- Alternatively, use the browser in incognito/private mode to avoid cache-related problems.

RecoverPoint for VMs installation form

The installation data form is a data sheet or a spreadsheet that lists the site specific values that you require to complete the installation successfully.

NOTE: To streamline the installation tasks, create the RecoverPoint for VMs installation forms during the planning phase.

Topics:

- Installation data forms

Installation data forms

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

The forms that are provided below 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 12. Example: vRPA cluster or site form

vRPA cluster	vRPA cluster 1	vRPA cluster 2	vRPA cluster 3	vRPA cluster 4	vRPA cluster 5
Cluster or site name					
Time zone					
Local domain					
Primary DNS server (optional)					
Secondary DNS server (optional)					
Primary NTP server (recommended)					
Secondary 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					

Table 12. Example: vRPA cluster or site form (continued)

vRPA cluster	vRPA cluster 1	vRPA cluster 2	vRPA cluster 3	vRPA cluster 4	vRPA cluster 5
vCenter credentials					
Plugin server (per vCenter Server)					
VMkernel IP pool					
ESXi 1					
_Data1 IP					
_Data2 IP					
_Management IP					
ESXi 2					
_Data1 IP					
_Data2 IP					
_Management IP					

Table 13. 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					

Table 13. Example: vRPA IP form (continued)

vRPA	vRPA IPs	Site: __________	Site: __________	Site: __________	Site: __________	Site: __________
	Data2 IP					
vRPA_7	LAN IP					
	WAN IP					
	Data1 IP					
	Data2 IP					
vRPA_8	LAN IP					
	WAN IP					
	Data1 IP					
	Data2 IP					

Table 14. Example: Site map

Site	Site1 (Prod)	Site2 (Remote)	Site2 (Remote)	Site3 (Remote)	Site3 (Remote)
Cluster	Cluster1	Cluster2	Cluster3	Cluster4	Cluster5
vCenter Server	*<name>* *<ip_address>*	*<name>* *<ip_address>*	*<name>* *<ip_address>*	*<name>* *<ip_address>*	*<name>* *<ip_address>*
Plugin server (per vCenter Server)	*<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

B

Topics:

- Trust Splitter and Jiraf vSphere Installation Bundle (VIB) URLs in vCenter

Trust Splitter and Jiraf vSphere Installation Bundle (VIB) URLs in vCenter

Perform the steps as outlined in this topic before installing or upgrading the splitter and jiraf filters in vCenter version 8.0 U2b or later.

About this task

Before installing or upgrading the splitter or jiraf VIB URLs in vCenter 8.0 U2b or later, VMware® requires that you trust the splitter and jiraf VIB URLs. You can see VMware KB93130 for more information.

Perform the following steps:

Steps

1. Log in to any RPA as a `root` user.

   NOTE: To determine which RPA to log in, depends upon the operation that is performed by user. For Example: installing splitter, Jiraf filter during RP cluster installation OR upgrading splitter, Jiraf etc. Kindly see the respective sections in the deployment guide to determine which RPA to use.

   To enable root access in vRPA, log in with an SSH client and **login as:** `admin`. Enter your admin password in the **Password** field. See *Table 2* in the *Security and Configuration Guide* for your default admin password.

   Select **Main Menu** > **Setup** > **Advanced options** > **Security options** > **Enable/Disable root access**, then enter `y` to enable root access.

   If you know the VIB URL, skip to step 3.

2. Navigate to the following paths and note the splitter and jiraf package names:
   - For jiraf, use `/home/kos/RPServers/jiraf/esx8`
   - For splitter, use `/home/kos/RPServers/iof/esx8`

   Following are the example of package names:
   - Jiraf : `EMC-RP4VMs-JAM_6010.m.45-1OEM.700.1.0.15843807_22162261.zip`
   - Splitter : `EMC-RP4VMs-SPL_6011.m.96-1OEM.700.1.0.15843807_24159168.zip`

3. Log in to VC as a root user and run the following command:

   ```
   #/usr/lib/vmware-eam/bin/eam-utility.py install-cert [VIB/OVF_URL]
   ```

   Use the following URL formats:
   - Jiraf URL: **`https://`*`{RPA_IP}`*`/RPResources/jiraf/esx8/`*`{jiraf_package_name}`***
   - Splitter URL: **`https://`*`{RPA_IP}`*`/RPResources/iof/esx8/`*`{splitter_package_name}`***

Example

- Jiraf: `/usr/lib/vmware-eam/bin/eam-utility.py install-cert https://10.0.0.1/RPResources/jiraf/esx8/EMC-RP4VMs-JAM_6010.m.45-1OEM.700.1.0.15843807_22162261.zip`
- Splitter: `/usr/lib/vmware-eam/bin/eam-utility.py install-cert https://10.0.0.1/RPResources/iof/esx8/EMC-RP4VMs-SPL_6011.m.96-1OEM.700.1.0.15843807_24159168.zip`

Next steps

- Confirm and mark the certificate as trusted for the URL.

```
root@XXX-XX-XX-XX [ ~ ]#/usr/lib/vmware-eam/bin/eam-
utility.py install-cert https://10.0.0.1/RPResources/jiraf/esx8/EMC-RP4VMs-
JAM_6010.m.45-1OEM.700.1.0.15843807_22162261.zip

2024-03-27 09:20:37 +0000 PEM encoding of certificate behind URL https://10.0.0.1/
RPResources/jiraf/esx8/EMC-RP4VMs-JAM_6010.m.45-1OEM.700.1.0.15843807_22162261.zip:

-----BEGIN CERTIFICATE-----

<...>

-----END CERTIFICATE-----
```

The system asks for the following confirmation:

```
Do you want to associate(pin) this certificate with this URL as a trusted certificate?
(enter "Y" to confirm):
```

Enter **Y** to confirm.

C

Support procedures for uninstalling vRPA clusters

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

The topics in this Appendix provide procedures for use in manually uninstalling a vRPA cluster.

Topics:

Uninstalling a single vRPA cluster from a vCenter manually

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

Prerequisites

Obtain the internal cluster name of the vRPA you are uninstalling by connecting to the vRPA Admin CLI as the admin user, and selecting **Main Menu** > **Setup** > **View Settings**.

About this task

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 instead of this one.

Steps

1. If the vRPA cluster is active:
    a. Unprotect the virtual machines. For more information, see Unprotect VMs.
    b. Remove all ESX clusters from the vRPA cluster. For more information, see Remove ESX 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.
   If the procedure Uninstall a vRPA cluster was successful, skip to step 6. If the procedure Uninstall a vRPA cluster failed, continue with the next step.
3. Detach the vRPAs from the cluster. For more information, see Detaching vRPAs.
4. Power off the vRPAs. For more information, see Powering off vRPAs.
5. 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.

6. Delete from all datastores the repository folder of the cluster you are uninstalling. For more information, see Deleting the repository folder.
7. Verify that the configuration parameters are empty. For more information, see Verifying that the configuration parameters are empty.

   > ⓘ **NOTE:** Perform this step only if you encountered problems when unprotecting the VMs. Performing this step requires downtime of the production VM.

8. Ensure that the vRPA virtual machines are powered off, and delete them.
9. 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 Splitter and Jiraf.

Uninstalling all vRPA clusters from a vCenter manually

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

Prerequisites

Obtain the internal cluster name of the vRPA you are uninstalling by connecting to the vRPA Admin CLI as the admin user, and selecting **Main Menu** > **Setup** > **View Settings**.

About this task

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

Steps

1. If the vRPA cluster is active:
   a. Unprotect the virtual machines. For more information, see Unprotect VMs.
   b. Remove all ESX clusters from the vRPA clusters. For more information, see Remove ESX 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.
   If the procedure Uninstall a vRPA cluster was successful, skip to step 6. If the procedure Uninstall a vRPA cluster failed, continue with the next step.
3. Detach the vRPAs from the cluster. For more information, see Detaching vRPAs.
4. Power off the vRPAs. For more information, see Powering off vRPAs.
5. 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.
6. Delete from all datastores the repository folders of all clusters. For more information, see Deleting the repository folder.
7. Verify that the configuration parameters are empty. For more information, see Verifying that the configuration parameters are empty.

   > ⓘ **NOTE:** Perform this step only if you encountered problems when unprotecting the VMs. Performing this step requires downtime of the production VM.

8. Ensure that the vRPA virtual machines are powered off, and delete them.
9. Unregister the plug-in from the Managed Object Browser. For more information, see Unregistering the plugin from the Managed Object Browser.
10. Uninstall the RecoverPoint for VMs splitter. For more information, see Uninstall the RecoverPoint for VMs Splitter and Jiraf.
11. Unregister the RecoverPoint extension from the Managed Object Browser. For more information, see Unregistering the plugin from the Managed Object Browser.
12. Remove the RecoverPoint datastore element. Delete the `RecoverPoint.flp` file located in the RecoverPoint folder.

Detaching vRPAs

Steps

1. Use an SSH client to connect to a vRPA and enter login credentials for the admin 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

Steps

1. In the vSphere Client or vSphere Web Client, select **Inventory**.
2. In the vSphere Client, select each vRPA, right-click and select **Power** > **Power Off** for each vRPA that is powered on.

   In the vSphere Web Client, select each vRPA, right-click and select **All vCenter Actions** > **Power** > **Power Off** for each vRPA that is powered on.

Deleting the repository folder

Steps

1. At the vSphere Web Client, select **Inventory** > **Datastore**.
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

About this task

ⓘ **NOTE:** Performing this task requires downtime of the production VM.

Steps

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 **Advanced** parameters to edit the advanced configuration parameters.
3. In the **Advanced 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 custom tokens from the Managed Object Browser

About this task

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.

Steps

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, RecoverPoint_TOKEN, for example, **`config.RecoverPoint_TOKEN;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 plugin from the Managed Object Browser

About this task

Unregister the RecoverPoint for VMs plugin from the Managed Object Browser at each vCenter Server that contains ESXi clusters that are hosting vRPA clusters. Unregister the plugin while the vRPAs are detached. Use this procedure also to unregister a RecoverPoint extension from the Managed Object Browser.

ⓘ **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.

Steps

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.dell.recoverpoint.vc.h5plugin`** (HTML5 value).

Uninstall the RecoverPoint for VMs Splitter or Jiraf

When the automated uninstaller tool is unavailable, you can manually uninstall the splitter of jiraf from the *Managed Object Browser (MOB)*.

Steps

1. Log in to the **Managed Object Browser (MOB)** using the URL format: `https://`*`<VC_IP>`*`/mob`.

   Ensure the vCenter credentials are configured correctly.
2. Click **Content > groud-d1 (Datacenter) > datacenter-3 (<Datastore-name>) > group-h5 (host)**.

3. Copy the required cluster name *MOID* from *childEntity*.

   For example: *domain-c8*
4. Click **Home > Content > IoFilterManager > QueryIoFilterInfo**.
5. Paste the *MOID* of cluster ex: `domain-c8` in place of `MOID` and click **Invoke Method**, to view the installed IO Filters: splitter or jiraf.
6. Copy the id value of splitter or jiraf without double quotations.

   Example:
   - Splitter id: `EMC_bootbank_emcsplitter_5330.m.169-1OEM.700.1.0.15843807`
   - Jiraf id: `EMC_bootbank_emcjiraf_5330.m.169-1OEM.700.1.0.15843807`
7. Run `UninstallIOFilter_Task`, **Home > Content > IoFilterManager > UninstallIOFilter_Task** .
8. Paste the ID of splitter or jiraf and give the *MOID* and click **Invoke Method** to run uninstallation of splitter or jiraf task.
9. To check the status of uninstallation task, go to **Task > info > TaskInfoState** running, repeat this step to refresh contents. Once the task gets complete, the *TaskInfoState* sets to `success`.

D

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.

Topics:

Upgrading vCenter

About this task

When upgrading the vCenter in a RecoverPoint for VMs system, the upgrade process should not change the **vCenter UUID** to ensure transparency for RecoverPoint.

During the upgrade:

- The vRPA clusters cannot be managed from the current vCenter. Make sure you have access to other vCenters.
- Data replication and Recovery Point Objective (RPO) might be affected.
- vCenters in Enhanced Linked Mode (ELM) might be affected (one vCenter at a time).
- The RecoverPoint for VMs plugin should remain intact.

⚠ **CAUTION: To avoid changing the vCenter UUID during the upgrade process, ensure that you select the Use existing inventory option.**

Steps

If you are upgrading to vSphere version 8.0 U3,

`Prerequisites:`

- Ensure that your RPA, splitter, and jiraf are all running on RecoverPoint for VMs 6.0.SP1.P2 or later.
- If you are in 8.0.u1c, ensure that you trust the splitter and jiraf VIB URLs into VC as described in the following steps:
  a. Log in to RPA as a root user.
  b. Navigate to the following paths and note the splitter and jiraf package names:
     - For jiraf, use `/home/kos/RPServers/jiraf/esx8`
     - For splitter, use `/home/kos/RPServers/iof/esx8`

     Following are the examples for package names:

     - Jiraf : `EMC-RP4VMs-JAM_6010.m.45-1OEM.700.1.0.15843807_22162261.zip`
     - Splitter : `EMC-RP4VMs-SPL_6011.m.96-1OEM.700.1.0.15843807_24159168.zip`
  c. Download and copy the `eam-utility.py` file to vCenter from KB Article 313026
  d. Log in to VC as a root user and run the following command:

     ```
     # python [script_location]/eam-utility.py install-cert [VIB/OVF_URL]
     ```

     Use the following URL formats:

     - Jiraf URL: **`https://{RPA_IP}/RPResources/jiraf/esx8/{jiraf_package_name}`**
     - Splitter URL: **`https://{RPA_IP}/RPResources/iof/esx8/{splitter_package_name}`**

     Examples:

     - Jiraf: `python /usr/lib/vmware-eam/bin/eam-utility.py install-cert https://10.0.0.1/RPResources/jiraf/esx8/EMC-RP4VMs-JAM_6010.m.45-1OEM.700.1.0.15843807_22162261.zip`

    - Splitter: `python /usr/lib/vmware-eam/bin/eam-utility.py install-cert https://10.0.0.1/RPResources/iof/esx8/EMC-RP4VMs-SPL_6011.m.96-1OEM.700.1.0.15843807_24159168.zip`

e. Confirm and mark the certificate as trusted for the URL.

```
root@XXX-XX-XX-XX [ ~ ]# python /usr/lib/vmware-eam/bin/eam-
utility.py install-cert https://10.0.0.1/RPResources/jiraf/esx8/EMC-RP4VMs-
JAM_6010.m.45-1OEM.700.1.0.15843807_22162261.zip

2024-03-27 09:20:37 +0000 PEM encoding of certificate behind URL https://10.0.0.1/
RPResources/jiraf/esx8/EMC-RP4VMs-JAM_6010.m.45-1OEM.700.1.0.15843807_22162261.zip:

-----BEGIN CERTIFICATE-----

<...>

-----END CERTIFICATE-----
```

The system asks for the following confirmation:

```
Do you want to associate(pin) this certificate with this URL as a trusted certificate?
(enter "Y" to confirm):
```

Enter **`Y`** to confirm.

Results

The vCenter Server is upgraded to the specified version.

Next steps

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.

Upgrading an ESXi host to 8.0 U3

Perform the following procedure on every ESXi host that is part of the ESXi cluster.

Prerequisites

- Before upgrading an ESX to 8.0 U3, ensure that vRPA clusters, splitter, and JAM VIBs are all running on RecoverPoint for VMs 6.0.SP1.P2 or later.
- Upgrade VC to 8.0 U3 build. See Upgrading vCenter for more details.

Steps

1. Enter **Maintenance** mode at EXCLI.
2. Use SSH to run the following command from the ESXi host console:

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

   NOTE: This command requires an additional switch for vSAN environments. See *vSphere documentation* for the vSphere version that you are using.

3. Perform the ESX upgrade.
4. Exit **Maintenance** mode.
5. Use SSH to run the following command from the ESXi host console :

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

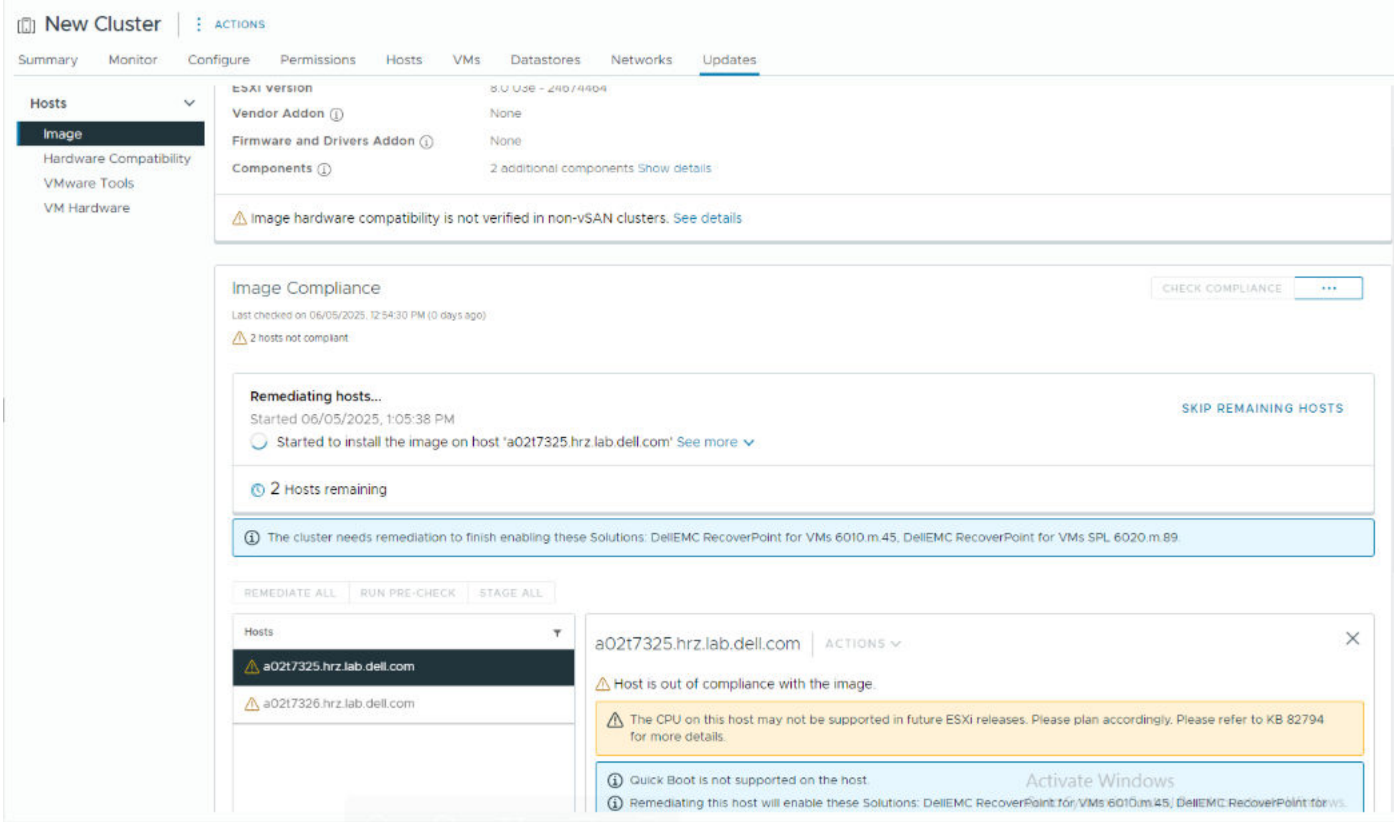
Next steps

Repeat this procedure on every ESXi which are part of the ESX cluster.

Enable Single Image on Already Deployed RP4VM System

If you have an RP cluster installed with a non-single image setup, you can convert the ESX cluster into a single image configuration by following these steps:

1. Go to **<ESX_cluster_name> → Updates → Setup Image Manually** and click **Save**
2. The system performs a compliance check.
3. If the cluster is compliant, the option to **Remediate All** becomes available.
4. Click **Remediate All** to apply the changes, then click **Finish** to complete the process.



ESXi Version 8.0 U3e - 24674464
Vendor Addon None
Firmware and Drivers Addon None
Components 2 additional components Show details

Image hardware compatibility is not verified in non-vSAN clusters. See details

Image Compliance
Last checked on 06/05/2025, 12:54:30 PM (0 days ago)
2 hosts not compliant

Remediating hosts...
Started 06/05/2025, 1:05:38 PM
Started to install the image on host 'a02t7325.hrz.lab.dell.com' See more
2 Hosts remaining

The cluster needs remediation to finish enabling these Solutions: DellEMC RecoverPoint for VMs 6010.m.45, DellEMC RecoverPoint for VMs SPL 6020.m.89.

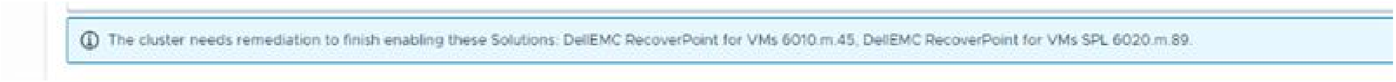
a02t7325.hrz.lab.dell.com
a02t7326.hrz.lab.dell.com

a02t7325.hrz.lab.dell.com
Host is out of compliance with the image.
The CPU on this host may not be supported in future ESXi releases. Please plan accordingly. Please refer to KB 82794 for more details.
Quick Boot is not supported on the host.
Remediating this host will enable these Solutions: DellEMC RecoverPoint for VMs 6010.m.45, DellEMC RecoverPoint for

Ideally, after the compliance check is completed, the remediate options for both **Splitter** and **Jiraf** should be visible on all hosts.

If the remediate options do not appear:

1. Click the **Finish Image Setup** button.
2. After clicking, you should see the following message:



The cluster needs remediation to finish enabling these Solutions: DellEMC RecoverPoint for VMs 6010.m.45, DellEMC RecoverPoint for VMs SPL 6020.m.89.

3. Once the message appears, the remediate options should become available