

# **Dell RecoverPoint for Virtual Machines 6.0.3**

## vSphere HTML5 Plugin Administrator's Guide

## 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.

# Contents

<b>Figures.....</b>	<b>6</b>
<b>Tables.....</b>	<b>7</b>
<b>Preface.....</b>	<b>8</b>
<b>Chapter 1: Before you begin.....</b>	<b>10</b>
Create your license files.....	10
Launching RecoverPoint for VMs plugin.....	11
Add license.....	12
Flex to XML license conversion.....	12
Register for Customer Support.....	13
<b>Chapter 2: Protecting VMs.....</b>	<b>14</b>
Protect a VM in a new group.....	14
Protect a VM in an existing group.....	17
Protect multiple VMs in a new group.....	19
Protect multiple VMs in an existing group.....	21
Add a copy to an existing group.....	23
<b>Chapter 3: Monitoring protection.....</b>	<b>25</b>
RecoverPoint for VMs Dashboard.....	25
Monitor system alerts.....	30
Monitor system events.....	31
Monitor system limits.....	35
Monitor system components.....	37
Monitor group and copy protection.....	38
Reports.....	39
Reports vRPA Clusters.....	40
Reports Consistency Groups.....	40
Reports Copies.....	41
<b>Chapter 4: VM automation and orchestration.....</b>	<b>42</b>
Create a bookmark.....	42
Creating an Application-Consistent Bookmark using KVSS.....	43
Automation.....	45
Automatic protection of newly added VMDKs.....	45
Provisioning copy VMDKs.....	46
Excluding a VMDK from replication.....	46
Automatic replication of VM hardware changes.....	46
Orchestration.....	47
VM start-up sequence.....	47
Group start-up sequence.....	50
Create a group set.....	51
Re-IP rules.....	52

Failover networks.....	55
<b>Chapter 5: Recovering VMs.....</b>	<b>56</b>
Test a copy.....	56
Failover to a copy.....	60
Recover production from a copy.....	66
<b>Chapter 6: Monitoring recovery activities.....</b>	<b>71</b>
<b>Appendix A: Managing RecoverPoint for VMs.....</b>	<b>72</b>
Managing your RecoverPoint for VMs licenses.....	72
Managing the plugin server.....	72
Changing the plugin server certificate .....	73
Changing a registered plugin server certificate .....	73
Managing vCenter Server registration with plugin server.....	74
Managing linked vCenter Server registration.....	75
Displaying the plugin server info.....	80
Collecting plugin server logs.....	80
Upgrading the plugin server.....	81
Managing vRPA clusters.....	82
Managing system component registration.....	84
Register vCenter Server to vRPA cluster.....	84
Managing ESX cluster registration.....	85
Managing journal datastore registration.....	86
Managing external host registration.....	87
Manage Event Filters.....	87
Display all event filters.....	87
Create an event filter.....	87
Configure the transfer method.....	88
Configure Email event notification.....	89
Configure Syslog event notification.....	89
Configure SNMP event notification.....	90
Modify an existing event filter.....	90
Managing protected VMs.....	91
Managing VM protection policies.....	91
Stop protecting a VM.....	92
Managing consistency groups.....	92
Managing group protection policies.....	92
Managing group sets.....	97
Managing recovery activities.....	98
Manage testing.....	99
Manage failover and failback.....	103
Manage production recovery.....	107
Configuring email alerts and reports.....	108
<b>Appendix B: Troubleshooting.....</b>	<b>110</b>
Finding the vRPA cluster management IP.....	110
Collecting logs.....	110
Collecting logs from vRPA clusters.....	110

Collecting RecoverPoint for VMs splitter logs.....	112
Adding new VMDKs.....	113
Removing a VMDK.....	113
Automatically expanding copy VMDKs.....	113
Recovering from a cluster disaster.....	114
RecoverPoint for VMs licensing.....	114
XML license.....	115
Creating VMkernel ports.....	116
Load balancing.....	117
Copy VM network configuration guidelines.....	118
Changing the network adapter configuration of a protected VM.....	120

# Figures

1	vSphere Client.....	11
2	RecoverPoint for VMs Dashboard.....	25
3	RecoverPoint for VMs event logs.....	32
4	System limits.....	35
5	Consistency group limits.....	36
6	vRPA cluster limits.....	36
7	Splitter limits.....	37
8	Monitoring recovery activities.....	71
9	Plugin server vCenter Servers screen.....	75
10	Local linked vCenter example.....	77
11	Remote linked vCenter example.....	79
12	RecoverPoint for VMs Deployer 6.0.3.....	84
13	RecoverPoint for VMs Deployer 6.0.3.....	111

# Tables

1	Style conventions.....	8
2	Parameter Description.....	44
3	Event Filter settings.....	88
4	Email settings.....	89
5	Syslog settings.....	89
6	SNMP settings.....	90
7	Virtual machine network settings available through the GUI.....	118
8	Network settings only available through the JSON file.....	120

As part of an effort to improve product lines, revisions of software are periodically released. Therefore, some functions that are described in this document might not be applicable for all versions of the software in use. The product release notes provide the most up-to-date information about 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 [Dell Support Site](#) to ensure that you are using the latest version of this document.

## Purpose

This document includes conceptual information about managing a RecoverPoint for Virtual Machines system.

## Audience

This document is intended for use by vSphere administrators who are responsible for managing the RecoverPoint for VMs system.

## 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 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
<b>Bold</b>	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).
<i>Italic</i>	Used for full titles of publications referenced in text
Monospace	Used for: <ul style="list-style-type: none"><li>• System code</li><li>• System output, such as an error message or script</li></ul>

**Table 1. Style conventions (continued)**

Formatting	Description
	<ul style="list-style-type: none"><li>• Pathnames, filenames, prompts, and syntax</li><li>• Commands and options</li></ul>
<i>Monospace italic</i>	Used for variables
<b>Monospace bold</b>	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](#).

# Before you begin

Before you start protecting your data in RecoverPoint for Virtual Machines, perform the tasks in this section in the provided sequence.

This guide provides the procedures for protecting, recovering and managing VMs.

- This guide provides the procedures for protecting, recovering, and managing VMs with on-premises local and/or remote copies.

Before you begin:

- See the Dell RecoverPoint for Virtual Machines Product Guide for a detailed description of the vSphere HTML5 plugin and the vSphere HTML5 plugin server.
- System installation must be complete. See the *Dell RecoverPoint for Virtual Machines Installation and Deployment Guide* for more information.
- The plug-in server must be registered with the vCenter Server that you are connected to, or one linked to the vCenter you are connected to. See [Managing the plugin server](#) for more information.

## Topics:

- [Create your license files](#)
- [Launching RecoverPoint for VMs plugin](#)
- [Add license](#)
- [Flex to XML license conversion](#)
- [Register for Customer Support](#)

## Create your license files

When a RecoverPoint for VMs sales order is approved, an order confirmation email is automatically sent to the email addresses provided during order entry. The email provides the information you need to begin license activation.

### About this task

For more information about software licensing, see these resources:

- [Software licensing documentation](#)
- [Software Licensing Central Activation video](#)

### Steps

1. If you are starting from the [Dell Digital Locker](#), log in or create an account, search for your order, select your product, and click **Activate now**.  
This action takes you to the first step of the license activation wizard in the Software Licensing Center (described in step 3).
2. If you do not have the order confirmation email, you can activate your software directly from the [Software Licensing Center](#):
  - a. Click **ACTIVATE MY SOFTWARE**.
  - b. Provide information such as Licensing Authorization Code (LAC) or Sales Order #.
3. In the **SELECT PRODUCTS** step of the activation wizard, select the product you want to activate, and click **START THE ACTIVATION PROCESS**.
4. In the **SELECT A MACHINE** step:
  - a. If you are activating a new instance or rehosting to a new target machine, add a new machine name, and click **SAVE MACHINE & CONTINUE TO NEXT STEP**.
  - b. If you are increasing capacity on an existing machine, use the **SEARCH MACHINES** widget, select the wanted machine, and click **NEXT: ENTER DETAILS**.
5. In the **ENTER DETAILS** step, enter the quantity of entitlements that you want to activate and the vCenter ID. To learn how to obtain the vCenter ID, click **Machine Details FAQs** and select **RecoverPoint for Virtual Machines**.
6. In the **REVIEW** step, review your selections, and click **ACTIVATE**. This action generates the license keys.

7. In the **COMPLETE** step, view and download the license keys that you generated. To return to the Software Licensing Center home page, click **HOME**.

## Results

The entitlements are converted to license files.

## Next steps

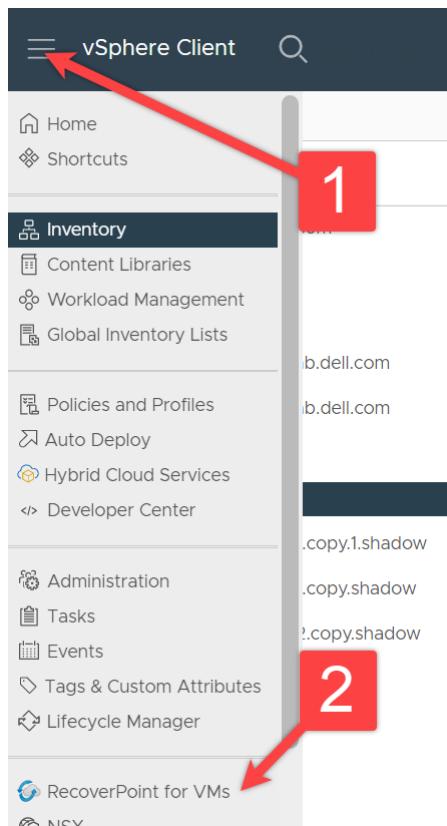
Transfer the license files to the computer from which you will be running RecoverPoint for VMs.

# Launching RecoverPoint for VMs plugin

Learn about how to launch the RecoverPoint for VMs plugin from vCenter Server.

## Steps

1. Connect to a vCenter Server hosting RecoverPoint for VMs components.
2. Click **LAUNCH VSphere CLIENT (HTML5)**. You can also launch the **vsphere Client (HTML5)** directly by entering `https://vCenter-IP or FQDN:/ui/` into your address bar.
3. Click the **vsphere Client Navigation** menu, and then click **RecoverPoint for VMs** to display the RecoverPoint for VMs plugin in the vsphere Client



**Figure 1. vSphere Client**

# Add license

Add a RecoverPoint for Virtual Machines license for each vCenter Server that is hosting a protected VM. Adding a license automatically registers the product and enables support.

## Prerequisites

[Create your license files](#). To learn more about the types of licenses that are available, see [RecoverPoint for VMs licensing](#).

## Steps

1. In the **RecoverPoint for Virtual Machines vSphere plug-in**, click **System > Licenses > Add**.

### Add a RecoverPoint for VMs License

X

Access your entitlements in the 'Software Licenses' section of support.dell.com or by clicking the link in the LAC email sent to the email address provided during order entry. Activate your entitlements and download your license (\*.xml) files from support.dell.com. Add a license for each vCenter Server that is protecting a VM or hosting a vRPA cluster. To learn more about the types of licenses that are available, see the RecoverPoint for VMs Administrator's Guide.

**i** When you add a socket-based license to a system with VM-based licenses, the system converts VM licenses to socket licenses at a ratio of 15 VMs per socket. When the ratio is not an even conversion, the value is rounded up.

Select a license (\*.xml) file 

CANCEL

ADD LICENSE

The **Add a RecoverPoint for Virtual Machines License** screen is displayed.

2. Click the browse icon, select a license file (\*.lic), and click **Add License**.

## Results

Your license is added to the RecoverPoint for Virtual Machines system, and its usage statistics and expiration are displayed in the **RecoverPoint for Virtual Machines Licenses** table. When both VM-based and socket-based licenses are added, the VM licenses are converted to socket licenses at a rate of 15 VMs to one socket.

An email with your license details is automatically sent to [emailalerts@dell.com](mailto:emailalerts@dell.com) to register your system.

# Flex to XML license conversion

After NDU from 6.x to 6.0.2 version, all the existing Flexera licenses must be converted to XML license.

## Steps

1. Upgrade vRPA clusters, splitter, and JAM VIBs to RecoverPoint for VMs version6.0.SP2.
2. Raise request for XML license conversion using VC UUIDs as Locking IDs.
3. In the vSphere Client, click **System > Licenses**.
4. Click **Add**, select the converted license, and click **Add license** to add the selected license.

**i** **NOTE:** The Qty is summed into a single <LicenseKey> if the component, feature, and key attributes are identical.

5. Delete all the licenses with license type as Flex.

**NOTE:** When moving from a version that supported Flex to a version that supports XML licensing, and choosing a fresh installation (not NDU), the user can typically choose either of the following:

Use a fresh XML license specifically for the fresh installation,

OR

Use a converted license, where the old Flex license is converted into the new XML format.

## Register for Customer Support

If the automatic registration email was not sent during license addition, or a change was made to your system follow the steps below. By ensuring that Customer Support has up-to-date information about the configuration of your system, you enable Dell Technologies to provide you with the most effective support possible.

### About this task

See the *RecoverPoint for VMs CLI Guide* for more detailed information.

### Steps

1. Create an SSH connection to a vRPA cluster management IP address, and use your RecoverPoint for VMs admin username and password to log in to the Admin CLI and, from there, open the Sysmgmt CLI.
2. In the Sysmgmt CLI, run the **set\_registration\_params** command, and provide all the requested information.

### Results

You should receive notification that your registration parameters have been successfully configured. Run the **get\_registration\_params** command if you want to confirm that the information in your system registration is correct.

# Protecting VMs

In RecoverPoint for VMs, consistency groups are used to protect virtual machines and replicate virtual machine application data to a consistent point in time. A consistency group is a logical entity that constitutes a container for virtual machines and all their copies.

Consistency groups can protect many VMs. If this is the first time you are using RecoverPoint for VMs, protect your VMs by creating new consistency groups for them. If you already have RecoverPoint for VMs consistency groups, you can protect your VMs by creating new consistency groups for them, or by adding them to an existing consistency group. You can also create a new copy to protect your production VMs, alongside your existing copy.

For additional information about VM management, including how to unprotect VMs, see [Managing protected VMs](#).

 **NOTE:** Protecting a virtual machine with fault tolerance enabled is not supported.

Before protecting your VMs, ensure you have:

- Completed the tasks that are described in [Before you begin](#).
- Powered on the virtual machines that you want to protect.
- Registered all linked vCenter Servers hosting production VMs and copy VMs as described in [Managing the plugin server](#).

## Topics:

- [Protect a VM in a new group](#)
- [Protect a VM in an existing group](#)
- [Protect multiple VMs in a new group](#)
- [Protect multiple VMs in an existing group](#)
- [Add a copy to an existing group](#)

## Protect a VM in a new group

Protect a virtual machine in a new consistency group.

### Prerequisites

Ensure that you have at least 6 GB space available in root volume for Windows VM and 250 MB for Linux.

### Steps

1. Connect to the vSphere Client of your production site.
2. Click the , and then click **Inventory**.
3. Click  to display the **VMs and Templates** view.
4. Right-click a powered-on VM, and select **RecoverPoint for Virtual Machines > Protect VM...**.  
The **Protect VM** dialog is displayed.

## Protect VM

X

Protected by

Production

Copies

+ ADD A COPY

CANCEL PROTECT

**NOTE:** In the **Protect VM** dialog, all the fields are prepopulated with sensible values, so you can safely click **PROTECT** now, and manage the protection policies later, if necessary.

5. (Optional) Click **Edit Settings** to change the default VM protection policy.

Hardware

Disk Provisioning Same as source

Replicate Hardware Changes

VMDKs (4 / 4)

VMDK	Size
Hard disk 1 - SCSI (0:0)	5 GB
Hard disk 2 - SCSI (0:1)	1 GB
Hard disk 3 - SCSI (0:2)	2 GB
Hard disk 4 - SCSI (0:3)	3 GB

**NOTE:** Replication of SR-IOV Passthrough Adapter is not supported. If the ESXi at a copy does not support the production VM version, no hardware changes are replicated.

- **Disk Provisioning:** Default is **Same as source**. Defines how the copy VMDKs are provisioned: **Same as source**, **Thick provision lazy zeroed**, **Thick provision eager zeroed** or **Thin provision**.
- **Replicate Hardware Changes:** Default is **Enabled**. Automatically replicates the hardware settings of all production virtual machines to their copy VMs whenever an image is accessed on the copy VMs. When enabled, RecoverPoint for Virtual Machines replicates the virtual machine version, CPU, memory, resource reservations, and network interface controller status and type, and MAC addresses (only to remote copy VMs).

**NOTE:** Replication of SR-IOV Passthrough Adapter is not supported. If the ESXi at a copy does not support the production VM version, no hardware changes are replicated.

- **VMDKs:** Displays the number of VMDKs that must be replicated, and their total size. Clear a VMDK check box to exclude the VMDK from replication.

6. (Optional) Change the default consistency group protection policies.

Protected by

Production

Consistency Group cg\_other\_os

vRPA Cluster Site1

Journal Datastore DEV\_RPVE34\_Site

**Consistency Group:** Default is **cg\_<vmname>**. Defines the consistency group name.

**vRPA Cluster:** Defines the vRPA cluster that is used to replicate and manage the production data to the copies.

- **Journal Datastore:** Defines the datastore that RecoverPoint for VMs automatically provisions a **3GB** VMDK on for the production journal. By default, RecoverPoint automatically registers up to 15 datastores for the production and copy journals and automatically selects the datastore with the most free space.

**NOTE:** RecoverPoint for Virtual Machines attempt to create the production journal on the selected datastore. If it cannot, the system attempts to create the production journal on another registered datastore. If you have more than 15 datastores and would like to register an additional datastore that is not in the list, register the other datastores according to [Managing journal datastore registration](#).

7. (Optional) Change the default copy protection policy.

Update the copy policies:

vRPA Cluster: Site2 (Remote Cop) | Sync:  RPO: 25 seconds | Async | vCenter Server: VM-RP-LAB-VC-28 | Target ESXi Cluster: Site 2 | Copy Datastore: DEV\_RPVE34\_Site |

- **vRPA Cluster:** Defines the vRPA cluster that is used to replicate and manage the production VM data to the storage at this copy.
- **Sync/Async:** Default is **Asynchronous** with **RPO** (Recovery Point Objective) of **25 Seconds**. The RPO is the point in time to which you are required to recover data, for a specific application, as defined by the organization. RPO defines the maximum lag that is allowed on a link.
- **vCenter Server and ESX Cluster:** Defines the vCenter Server and ESX cluster hosting the copy VMs.
- **Copy Datastore:** Defines the datastore to use for the copy VM data.

8. (Optional) Click the **Advanced Configuration** icon of the copy to update the advanced copy policies:



## Protect VM



vRPA Cluster: Darwin (Remote Cr) | Sync:  RPO: 25 seconds | Async | vCenter Server: VM-RP-Lab-H-134.r | Target ESXi Cluster: Darwin | Copy Datastore: DD\_StorageUnit\_E

### Advanced Copy Configuration

Journal Datastore: DD\_StorageUnit\_E | Journal Size: 10 GB

### Copy VM Creation

Production VM	Copy VM	<a href="#">RESET ALL TO DEFAULT</a>
Deploy_RPCenter_mgtariec_913	<input checked="" type="radio"/> Automatically create copy VM <input type="radio"/> Manually select copy VM	<a href="#">Select a Resource...</a>

- **Journal Datastore:** Defines the datastore that RecoverPoint for Virtual Machines automatically provisions a 10GB VMDK on for the copy journal, unless **Manually select copy VM** is selected as the **Copy VM Creation** method. By default, RecoverPoint automatically registers up to 15 datastores for the production and copy journals and automatically selects the datastore with the most free space.

**NOTE:** RecoverPoint for Virtual Machines attempt to create the copy journal on the selected datastore. If it cannot, the system attempts to create the copy journal on another registered datastore. If you have more than 15 datastores and would like to register an additional datastore that is not in the list, register the other datastores according to [Managing journal datastore registration](#).

- **Journal Size:** Default is **10GB**. The larger the copy journal, the more history can be saved.
  - **Copy VM Creation:** Default is **Automatically create copy VM**. You can:
    - Click **Select a Resource...** and select the ESXi host to host the copy VM.
    - Select **Manually select copy VM** > click **Select a VM...**, and select a VM from the list.
9. (Optional) For added protection, click **ADD A COPY** to protect the VM with an additional copy:
- Up to two copies can be created during VM protection. For additional protection, [Add a copy to an existing group](#) to create more copies.
  - After adding a copy, you can click **Delete Copy** to delete a copy. The last copy cannot be deleted.



10. Click **PROTECT**.

## Results

The specified virtual machine is protected, and the group production data starts being replicated to the copy VMs according to the specified policies. If an unregistered ESX cluster, or the VMware Resource Pool of an unregistered ESX cluster was selected to host a copy VM, the unregistered ESX cluster is automatically registered with the specified vRPA cluster, a splitter is installed on every ESXi host in the cluster, and replication is temporarily paused for all relevant VMs while the splitter is being installed.

## Next steps

- See [Managing VM protection policies](#) for additional VM protection policies.
- See [Managing group protection policies](#) for additional group and copy protection policies.
- For additional protection, [Add a copy to an existing group](#) to create more copies.

# Protect a VM in an existing group

Protect a virtual machine in an existing consistency group.

## About this task

The VM that you select to protect is added to an existing consistency group that is already protecting a VM. For best performance, you should only protect one VM per consistency group.

 **CAUTION:** If the image of the VM that you want to protect is larger than the journal size of the copy, the system automatically enters *one-phase distribution mode* upon protection.

## Steps

1. Connect to the vSphere Client of your production site.
  2. Click the , and then click **Inventory**.
  3. Click  to display the **VMs and Templates** view.
  4. Right-click a powered-on VM, and select **RecoverPoint for Virtual Machines > Protect VM in Existing Group...**
- The **Protect this VM in an Existing Group** dialog is displayed.

## Protect this VM in an Existing Group

X

Test-VM [Edit Settings](#)

Consistency Groups [HIDE](#)

'cg\_TVM-1' is selected.

Consistency Group	Production vCenter Server	Production vRPA Cluster	State
cg_TVM-1	VM-RP-Lab-H-213.hrz.lab.dell.com	VRPA_Test	Enabled

Copies

vCenter Server	Target ESXi Cluster	Copy Datastore	
vm-rp-lab-h-193.h...	London	RPVENV12_LONE	

Consistency Group	Production vCenter Server	Production vRPA Cluster	State
cg_TVM2	VM-RP-Lab-H-213.hrz.lab.dell.com	VRPA_Test	Enabled

[CANCEL](#) [PROTECT](#)

**NOTE:** All the fields are prepopulated with sensible values, so you can safely select the consistency group, and click **PROTECT** now. You can manage the VM protection settings later, if necessary, as described in [Managing VM protection policies](#).

5. Select the consistency group to protect your production VMs.

When a consistency group is selected, the group copies are displayed and you can change the **Target ESXi Cluster** and **Copy Datastore** of the group copy VMs.

6. (Optional) To change the VM creation settings, perform the following actions:

- Click . The **Copy VM creation** page appears.
- Copy VM** is set to **Automatically create copy VM** by default. To change the **Copy VM** setting, select the appropriate option. When **Automatically create copy VM** is selected, from the drop-down list, you can select the ESXi host to host the copy VM. When **Manually select copy VM** is selected, from the drop-down list you can select a VM.
- To reset all the **Copy VM Creation** setting values to the default values, click **RESET ALL TO DEFAULT**.
- To save your changes, click **BACK**.

7. (Optional) Click **Edit Settings** to change the default VM protection policies.

Hardware

Disk Provisioning [Same as source](#)

Replicate Hardware Changes

VMDKs (4 / 4)

Hard disk 1 - SCSI (0:0)	5 GB
Hard disk 2 - SCSI (0:1)	1 GB
Hard disk 3 - SCSI (0:2)	2 GB
Hard disk 4 - SCSI (0:3)	3 GB

See [Managing VM protection policies](#) for a detailed description of these VM protection policies, and others that cannot be defined during VM protection.

8. Click **PROTECT**.

## Results

The specified virtual machine is protected in the specified consistency group.

- A volume sweep occurs on the newly added VM, and a short initialization occurs on all other VMs in the consistency group.
- If an unregistered ESX cluster, or the VMware Resource Pool of an unregistered ESX cluster, was selected to host a copy VM, the unregistered ESX cluster is automatically registered with the specified vRPA cluster, a splitter is installed on every ESXi host in the cluster, and replication is temporarily paused for all relevant VMs while the splitter is being installed.
- RecoverPoint for VMs attempts to create the journals on the selected datastores. If for any reason journal creation fails, the system attempts to create the journal on another registered datastore.
- If the image of the VMs that you want to protect is larger than the journal size of the copy, the system automatically enters *one-phase distribution mode* upon protection.

## Protect multiple VMs in a new group

Protect multiple virtual machines hosted on an ESX cluster in a new consistency group.

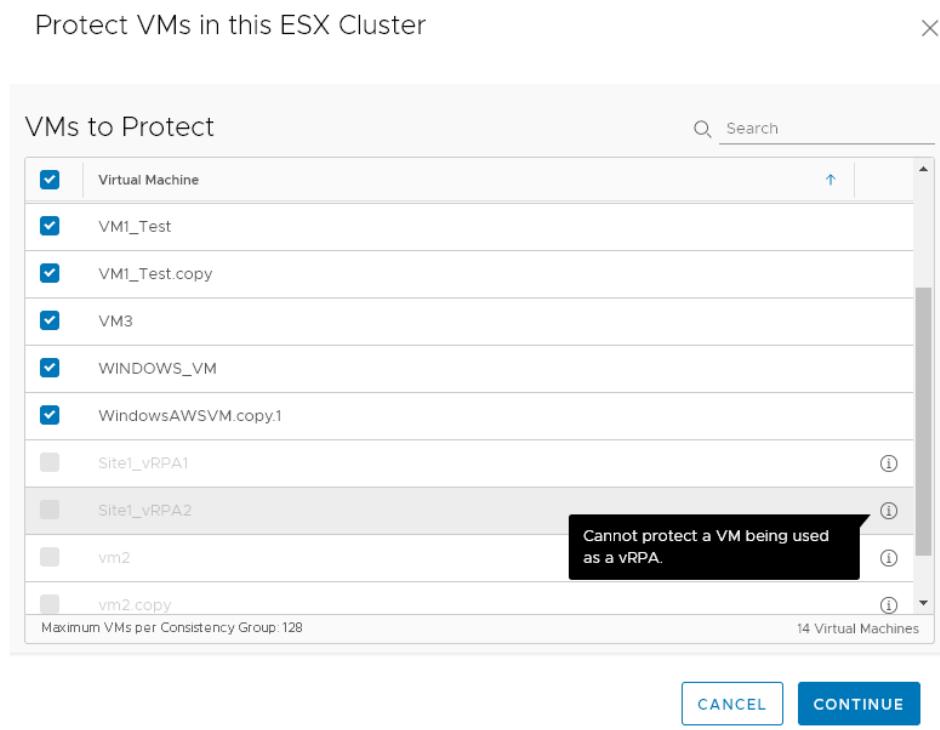
### About this task

All the VMs that you select in the following procedure are added to a single consistency group. For best performance, you should only protect one VM per consistency group.

### Steps

1. Connect to the vSphere Client of your production site.
2. Click the , and then click **Inventory**.
3. Click  to display the **Hosts and Clusters** view.
4. Right-click an ESX cluster, and select **RecoverPoint for VMs > Protect VMs....**

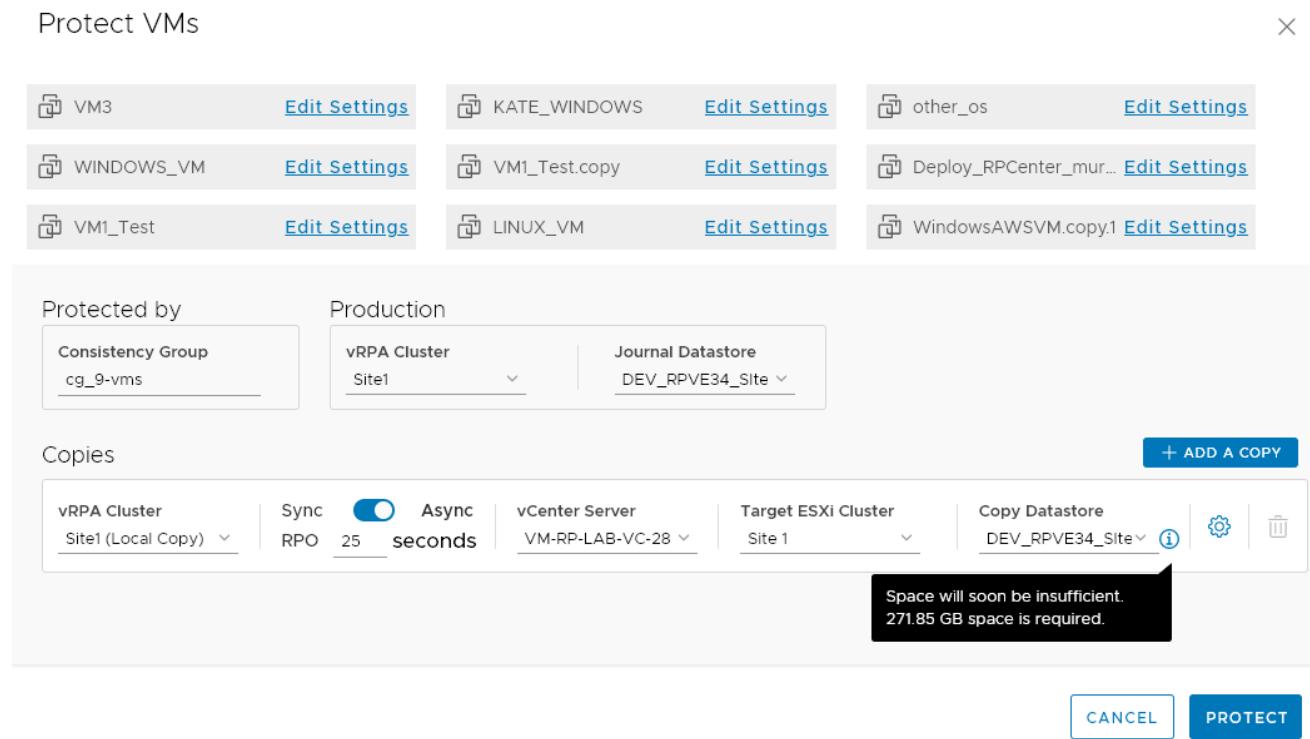
The **Protect VMs in this ESX Cluster** dialog is displayed.



RecoverPoint for VMs automatically detects if a VM is not able to be protected. Scroll to the bottom of the VM list and click the Info icon next to an excluded VM to display the reason for its exclusion.

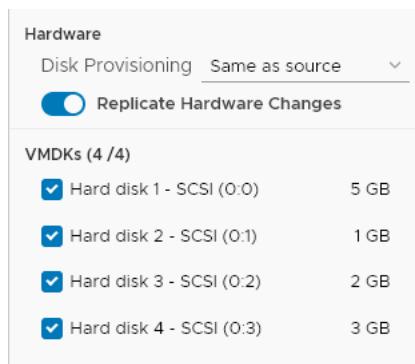
5. Select the VMs that you want to protect, and click **CONTINUE**.

The **Protect VMs** dialog is displayed.



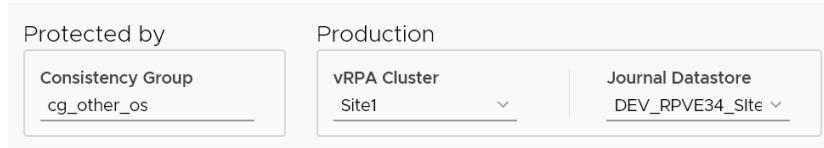
**NOTE:** In the **Protect VM** dialog, all the fields are prepopulated with sensible values, so you can safely click **PROTECT** now, and manage the protection settings later, if necessary, as described in [Managing VM protection policies](#) and [Managing group protection policies](#).

6. (Optional) Click **Edit Settings** to change the default VM protection policies.



See [Managing VM protection policies](#) for a detailed description of these VM protection policies, and others that cannot be defined during VM protection.

7. (Optional) Change the default consistency group and production protection policies.



See [Managing group protection policies](#) for a detailed description of these group protection policies, and others that cannot be defined during VM protection.

8. (Optional) Change the default copy protection policies.



See [Managing group protection policies](#) for a detailed description of these copy protection policies, and others that cannot be defined during VM protection.

9. (Optional) Update the advanced copy policies, see [Protect a VM in a new group](#) for details.
10. (Optional) For added protection, click **ADD A COPY** to protect the VMs with an additional copy:
  - Up to two copies can be created during VM protection. For additional protection, use [Add a copy to an existing group](#) to create additional copies.
  - After adding an additional copy, you can click the **Delete Copy** icon to delete a copy. The last copy cannot be deleted.



11. Click **PROTECT**.

## Results

The specified virtual machines are protected in a new consistency group.

- If an unregistered ESX cluster, or the VMware Resource Pool of an unregistered ESX cluster, was selected to host a copy VM, the unregistered ESX cluster is automatically registered with the specified VRPA cluster, a splitter is installed on every ESXi host in the cluster, and replication is temporarily paused for all relevant VMs while the splitter is being installed.
- RecoverPoint for VMs attempts to create the journals on the selected datastores. If for any reason journal creation fails, the system attempts to create the journal on another registered datastore.

# Protect multiple VMs in an existing group

Protect multiple virtual machines hosted on an ESX cluster in an existing consistency group.

## About this task

All the VMs that you select in the following procedure are added to a single consistency group. For best performance, you should only protect one VM per consistency group.

 **CAUTION:** If the image of the VMs that you want to protect is larger than the journal size of the copy, the system automatically enters *one-phase distribution mode* upon protection.

## Steps

1. Connect to the vSphere Client of your production site.
  2. Click the , and then click **Inventory**.
  3. Click  to display the **Hosts and Clusters** view.
  4. Right-click an ESX cluster, and select **RecoverPoint for VMs > Protect VMs in Existing Group...**
- The **Protect VMs in an Existing Group** dialog is displayed.

## Protect VMs in an Existing Group

X

VMs to Protect

	Virtual Machine
<input checked="" type="checkbox"/>	Virtual Machine
<input checked="" type="checkbox"/>	other_os
<input checked="" type="checkbox"/>	VM1_Test
<input checked="" type="checkbox"/>	VM1_Test.copy
<input checked="" type="checkbox"/>	VM3
<input checked="" type="checkbox"/>	WINDOWS_VM
<input checked="" type="checkbox"/>	WindowsAWSVM.copy1
<input type="checkbox"/>	Site1_vRPA1
<input type="checkbox"/>	Site1_vRPA2
<input type="checkbox"/>	vm2

Search

Cannot protect a VM being used as a vRPA.

Maximum VMs per Consistency Group: 128

14 Virtual Machines

**CANCEL** **CONTINUE**

RecoverPoint for VMs automatically detects if a VM is not able to be protected. Scroll to the bottom of the VM list and click the Info icon next to an excluded VM to display the reason for its exclusion.

5. Select the VMs that you want to protect, and click **CONTINUE**.

The **Protect these VMs in an Existing Group** dialog is displayed.

Protect this VM in an Existing Group

X

Test-VM [Edit Settings](#)

Consistency Groups [HIDE](#)

'cg\_TVM-1' is selected.

Consistency Group	Production vCenter Server	Production vRPA Cluster	State
cg_TVM-1	VM-RP-Lab-H-213.hrz.lab.dell.com	VRPA_Test	Enabled

Copies

vCenter Server	Target ESXi Cluster	Copy Datastore	
vm-rp-lab-h-193.h...	London	RPVENV12_LOND	

cg_TVM2	VM-RP-Lab-H-213.hrz.lab.dell.com	VRPA_Test	Enabled
---------	----------------------------------	-----------	---------

**CANCEL** **PROTECT**

**NOTE:** All the fields are prepopulated with sensible values, so you can safely select the consistency group, and click **PROTECT** now. You can manage the VM protection settings later, if necessary, as described in [Managing VM protection policies](#).

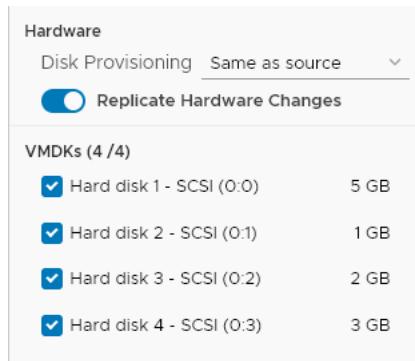
6. Select the consistency group to protect your production VMs.

When a consistency group is selected, the group copies are displayed and you can change the **Target ESXi Cluster** and **Copy Datastore** of the group copy VMs.

7. (Optional) To change the VM creation settings, perform the following actions:

- a. Click . The **Copy VM creation** page appears.
- b. **Copy VM** is set to **Automatically create copy VM** by default. To change the **Copy VM** setting, select the appropriate option. When **Automatically create copy VM** is selected, from the drop-down list, you can select the ESXi host to host the copy VM. When **Manually select copy VM** is selected, from the drop-down list you can select a VM.
- c. To reset all the **Copy VM Creation** setting values to the default values, click **RESET ALL TO DEFAULT**.
- d. To save your changes, click **BACK**.

8. (Optional) Click **Edit Settings** to change the default VM protection policies.



Hard disk	Size
Hard disk 1 - SCSI (0:0)	5 GB
Hard disk 2 - SCSI (0:1)	1 GB
Hard disk 3 - SCSI (0:2)	2 GB
Hard disk 4 - SCSI (0:3)	3 GB

See [Managing VM protection policies](#) for a detailed description of these VM protection policies, and others that cannot be defined during VM protection.

9. Click **PROTECT**.

## Results

The specified virtual machines are protected in the specified consistency group.

- A volume sweep occurs on the newly added VMs, and a short initialization occurs on all other VMs in the consistency group.
- If an unregistered ESX cluster, or the VMware Resource Pool of an unregistered ESX cluster, was selected to host a copy VM, the unregistered ESX cluster is automatically registered with the specified vRPA cluster, a splitter is installed on every ESXi host in the cluster, and replication is temporarily paused for all relevant VMs while the splitter is being installed.
- RecoverPoint for VMs attempts to create the journals on the selected datastores. If for any reason journal creation fails, the system attempts to create the journal on another registered datastore.
- If the image of the VMs that you want to protect is larger than the journal size of the copy, the system automatically enters *one-phase distribution mode* upon protection.

## Add a copy to an existing group

For added protection, add another copy to an existing consistency group.

### Steps

1. In the RecoverPoint for VMs plugin for vSphere Client, select **Protection > Consistency Groups**.
2. Select a group, and click the more group actions button (...) > **Add a copy**.
3. In the **Add a Copy** dialog:

## Add a Copy to 'MyGroup'

×



The screenshot shows the 'Add a Copy to 'MyGroup'' dialog box. It contains the following fields:

- vRPA Cluster:** WELL (Remote Co|) (Sync selected)
- RPO:** 25 seconds
- vCenter Server:** VM-RP-Lab-VC-154
- Target ESXi Cluster:** RPVENV8\_Site3
- Copy Datastore:** vsanDatastore (1.2.)
- Settings icon:** A gear icon in the top right corner of the dialog.

At the bottom of the dialog are two buttons: 'CANCEL' and 'ADD COPY'.

**NOTE:** All the fields are prepopulated with sensible values, so you can safely click **ADD COPY** now, and manage the protection policies later, if necessary.

### 4. (Optional) Change the default copy protection policy.

Update the copy policies:

- **vRPA Cluster:** Defines the vRPA cluster that is used to replicate and manage the production VM data to the storage at this copy.
- **Sync/Async:** Default is **Asynchronous** with **RPO** (Recovery Point Objective) of **25 Seconds**. The RPO is the point in time to which you are required to recover data, for a specific application, as defined by the organization. RPO defines the maximum lag that is allowed on a link.
- **vCenter Server and ESX Cluster:** Defines the vCenter Server and ESX cluster hosting the copy VMs.
- **Copy Datastore:** Defines the datastore to use for the copy VM data.

### 5. (Optional) Update the advanced copy policies, see [Protect a VM in a new group](#) for details.

### 6. Click **ADD COPY**.

## Results

A copy is added to the consistency group, and the group production data starts being replicated to the copy VMs according to the specified policies. If an unregistered ESX cluster, or the VMware Resource Pool of an unregistered ESX cluster, was selected to host a copy VM, the unregistered ESX cluster is automatically registered with the specified vRPA cluster, a splitter is installed on every ESXi host in the cluster, and replication is temporarily paused for all relevant VMs while the splitter is being installed.

## Next steps

See [Managing group protection policies](#) for additional copy protection policies.

# Monitoring protection

After protecting your VMs, use the **Dashboard** to monitor the number and status of protected VMs, consistency groups, group sets, vRPA clusters, system alerts and limits, as well as your RecoverPoint for VMs license usage.

## Topics:

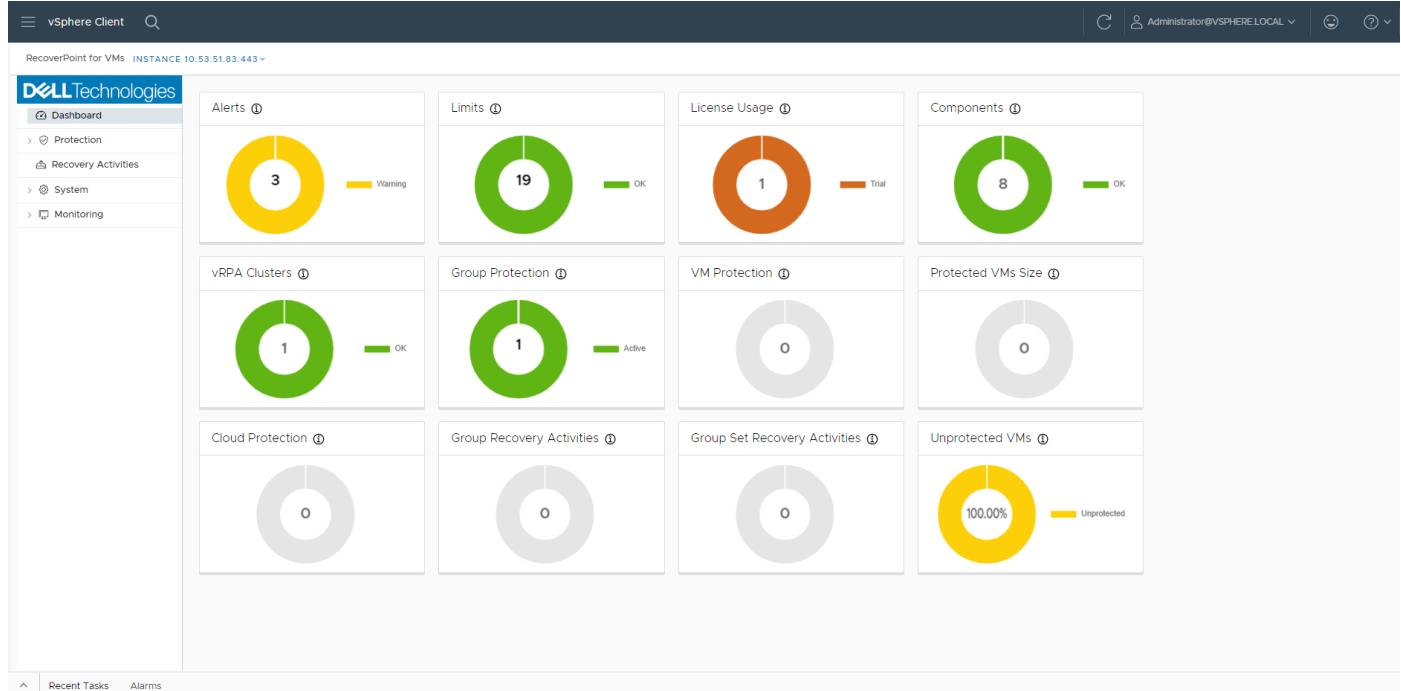
- RecoverPoint for VMs Dashboard
- Monitor system alerts
- Monitor system events
- Monitor system limits
- Monitor system components
- Monitor group and copy protection
- Reports

## RecoverPoint for VMs Dashboard

The RecoverPoint for VMs Dashboard presents a high level overview of the RecoverPoint for VMs system to help you analyze and monitor your system health.

### RecoverPoint for VMs Dashboard

The **Dashboard** is displayed every time that you log in to RecoverPoint for VMs. Use the **Dashboard** to monitor the status of your system licenses, limits, alerts, protected VMs, consistency groups, group sets, and recovery activities.

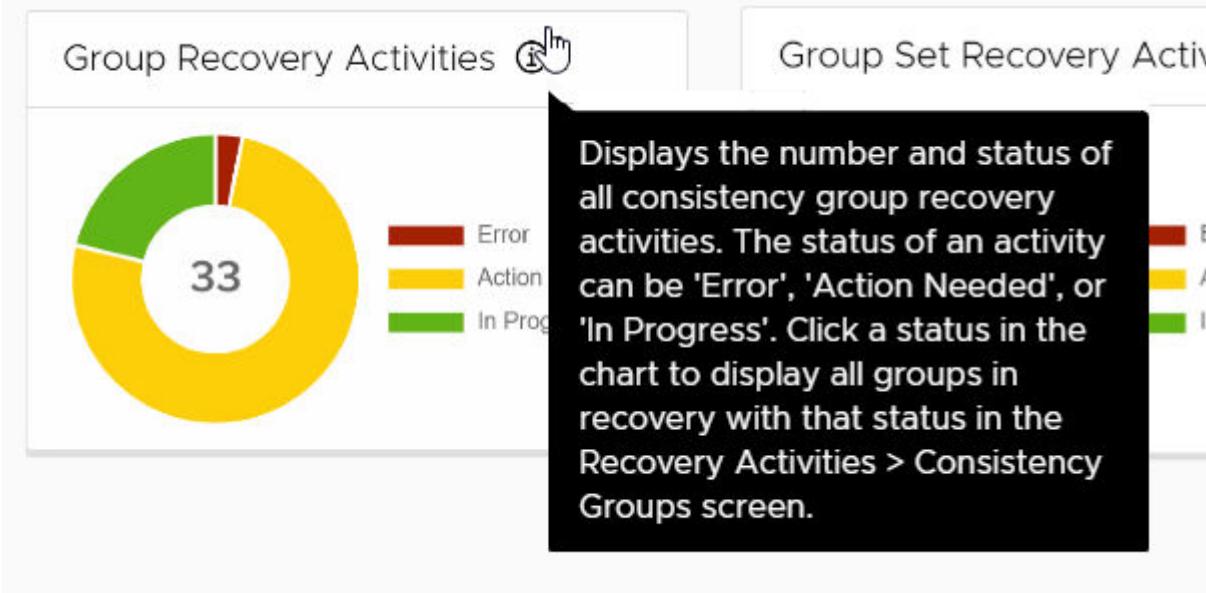


**Figure 2. RecoverPoint for VMs Dashboard**

In every **Dashboard widget**, you can:

- **Click the help icon** to display more detailed information about the widget system component or activity.

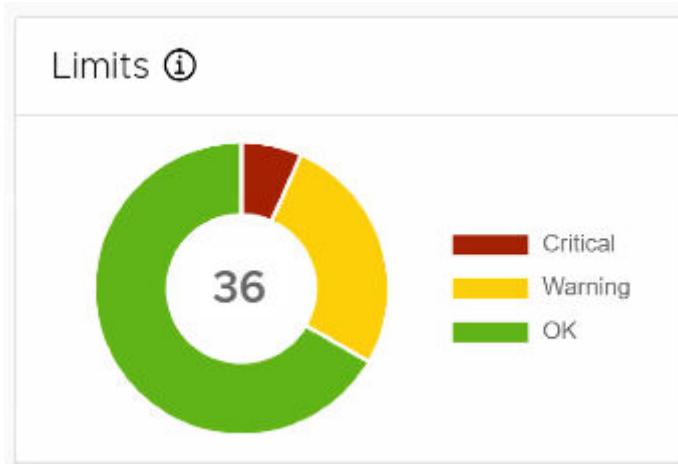
- **Click a status in a legend** (the colored bar or the label) to filter what is shown in the chart and display the number of system components with the status that you clicked. To clear the filter, click the status again.
- **Click a color of a status in a chart** to go to the relevant system component or activity screen, and display only the system component or activity in the clicked status.



## Widgets in RecoverPoint for VMs Dashboard

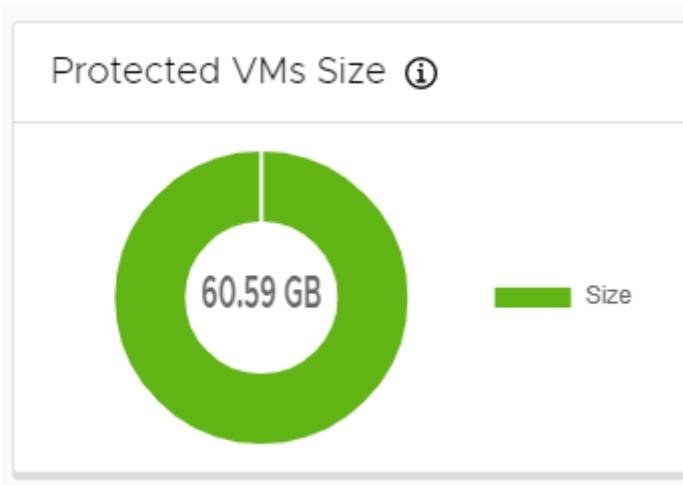
### Limits

- Displays the number and status of the limits that are imposed on system components like consistency groups, splitters, and vRPA clusters.
- The limit status of a system component can be '**Critical**', '**Warning**', or '**OK**'.
- Click a status in the chart to display all system components with that status in the **Monitoring > System Limits** screen.
- For more information, see how to [Monitoring System Limits](#).



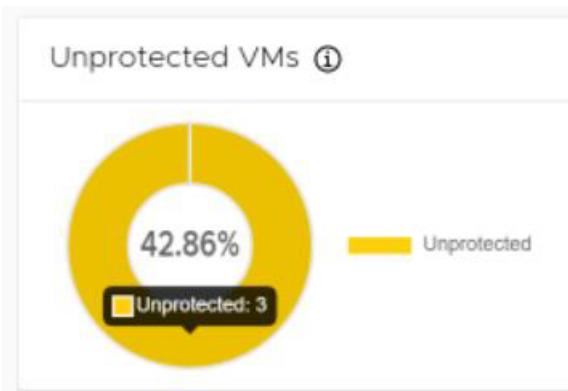
### Protected VMs Size

- Displays the total size (in GB) of all protected VMs on this vCenter Server
- For more information, see [Protecting VMs](#).



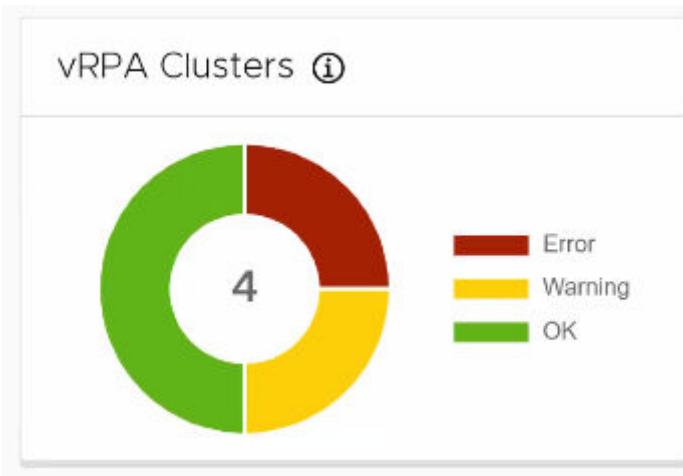
#### Unprotected VMs

- Displays the percentage of unprotected VMs.
- When you hover over the widget, the exact number of unprotected VMs appears. This widget displays the number of VMs that are unprotected and have to be protected to make data protection available.
- The number of unprotected VMs = total VMs - protected VMs - vRPAs - RPC - replica or shadow VMs.



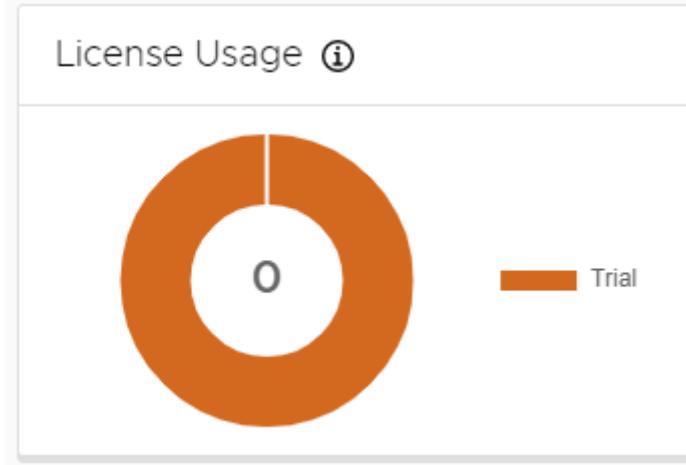
#### vRPA Clusters

- Displays the number and status of all registered vRPA clusters on all registered and linked vCenter Servers.
- The status of a vRPA cluster can be '**Error**', '**Warning**', or '**OK**'.
- Click a status in the chart to display all vRPA clusters with that status in the **System > Administration > vRPA Clusters** screen.
- For more information, see [Managing vRPA clusters](#) and [Collecting logs from vRPA clusters](#).



## License Usage

- Displays the number of protected sockets out of the total number of licensed sockets.
- The usage status of a system license can be '**Trial**', '**OK**', or '**Violated**'.
- Click a status in the chart to display all licenses with that status in the **System > Licenses** screen.
- For more information, see [Managing your RecoverPoint for VMs licenses](#).



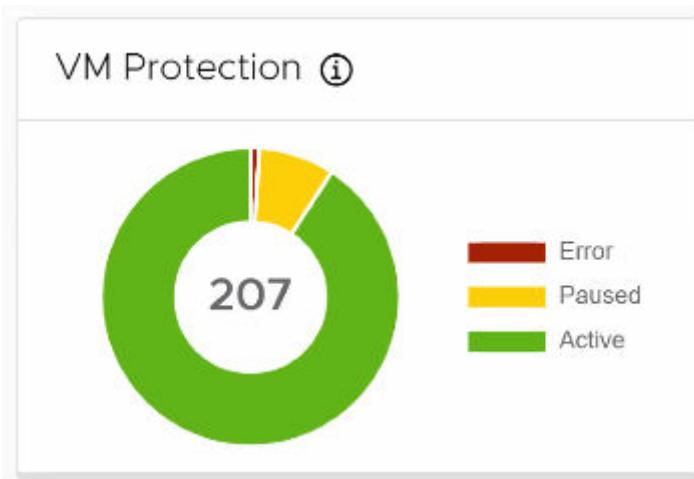
## Alerts

- Displays the number and types of alerts in the system.
- The type of an alert can be '**Error**' or '**Warning**'.
- Click an alert type in the chart to display all alerts of that type in the **Monitoring > Alerts** screen.
- For more information, see [Monitor system alerts](#).



## VM Protection

- Displays the number and status of protected VMs on the vCenter Server that you are connected to, or a registered vCenter Server that is linked to the vCenter that you are connected to.
- The status of a protected VM can be '**Active**', '**Error**', '**Initializing**', '**Inactive**', or '**Paused**'.
- Click a status in the chart to display all protected VMs with that status in the **Protection > Protected VMs** screen.
- For more information, see [Protecting VMs](#).



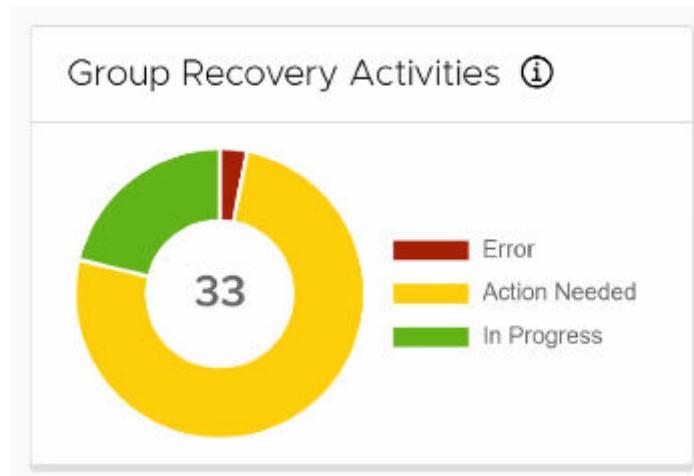
#### Group Protection

- Displays the number and status of all consistency groups in the system.
- The status of a consistency group can be '**Active**', '**Inactive**', '**Initializing**', '**Paused**', or '**Error**'.
- Click a status in the chart to display all groups with that status in the **Protection > Consistency Groups** screen.
- For more information, see [Protecting VMs](#).



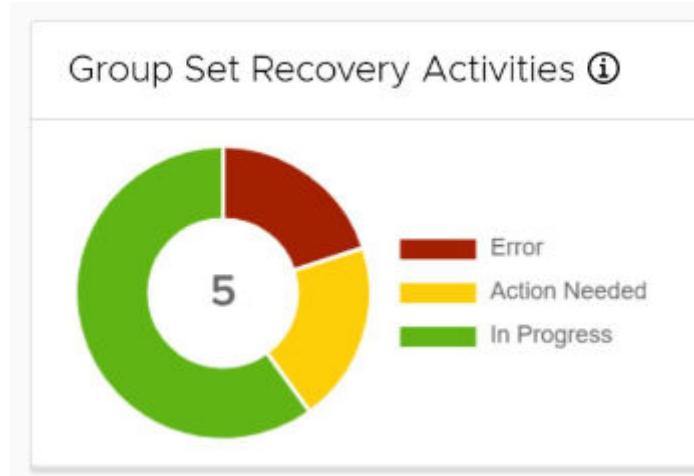
#### Group Recovery Activities

- Displays the number and status of all consistency group recovery activities.
- The status of an activity can be '**Error**', '**Action Needed**', or '**In Progress**'.
- Click a status in the chart to display all groups with that status in the **Recovery Activities > Consistency Groups** screen.
- For more information, see [Monitoring recovery activities](#).



#### Group Set Recovery Activities

- Displays the number and status of all group set recovery activities.
- The status of an activity can be 'Error', 'Action Needed', or 'In Progress'.
- Click a status in the chart to display all group sets with that status in the **Recovery Activities > Group Sets** screen.
- For more information, see [Monitoring recovery activities](#).



## Monitor system alerts

System alerts are a mechanism that enables vRPA clusters to send events about system components in real time. Monitor system alerts to troubleshoot your RecoverPoint for VMs environment.

### Prerequisites

Ensure you have performed the procedure for [Configuring email alerts and reports](#) and have added valid licenses as described in [Managing your RecoverPoint for VMs licenses](#).

### Steps

1. Click **Monitoring > Alerts** to monitor your system alerts.  
A system alert type can be Warning or Error.

Cluster	Category	Severity	Description
Vegas	System	Error	You are using the default password for the admin user. To change the default password, log in to the S...
	System	Warning	You are using an unlicensed trial version for non-commercial use only of Dell EMC RecoverPoint for VMs.
Belgrade	Consistency g...	Warning	The virtual RPA is running on the same ESX as the VM it is replicating. It is recommended not to have th...
Barcelona	RPA	Warning	At least two virtual RPAs are running on same ESX. It is recommended to run only one virtual RPA on a...
Vegas	Consistency g...	Warning	At least one virtual RPA is running on the same ESX as the VM it is replicating. It is recommended not t...

2. Alternatively, you can also monitor system alerts in the [RecoverPoint for VMs Dashboard](#).



## Monitor system events

Monitor system events to troubleshoot your RecoverPoint for VMs environment.

An event is a notification that a change has occurred in the state of a system component. Sometimes, the change indicates an error or warning condition for a system component. Multiple events can occur simultaneously on a single component, and a single incident can generate multiple events across multiple system components.

By default, the following information is displayed for every event in the **Event**:

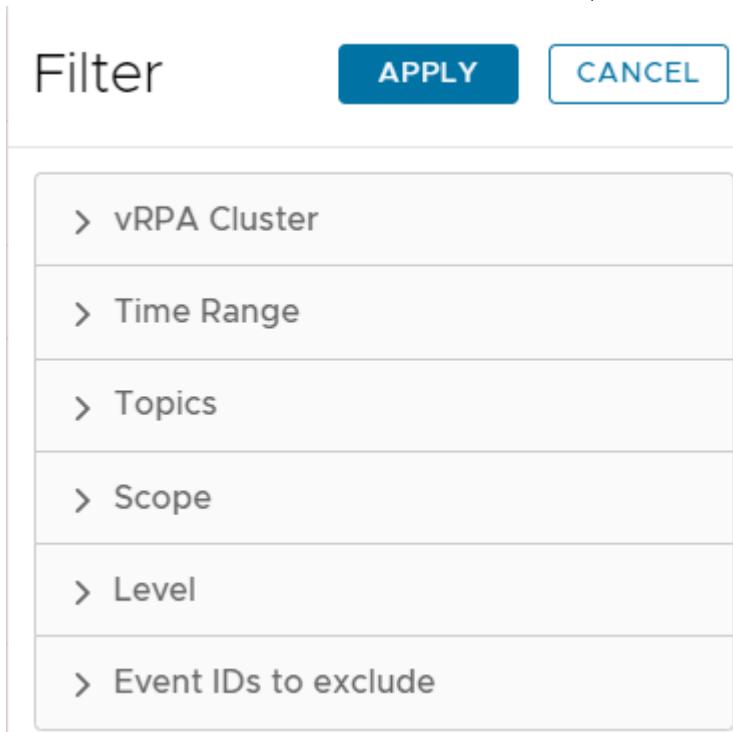
- **Level**, which can be: **Info**, **Warning**, or **Error**.
- **Scope**, which can be: **Normal**, **Root Cause**, or **Advanced**.
- **Time** and date that the event log was generated.
- **vRPA Cluster** reporting the event.
- **Event ID** that allows the event to be excluded from the events log using the event logs filter.
- **Topic**, which can be: **Splitter**, **Consistency Group**, **Management**, **Cluster**, **RPA**, or **Array**.
- **Summary** of the event.

To monitor your system events, click **Monitoring > Event**.

Event Logs						
Warnings and errors only from the last 24 hours						
Level	Scope	Time	vRPA Cluster	Event Id	Topic	Summary
> Transient Error	Root Cause	Jul 7, 2021 4:53:54 PM	TX-Cluster	16038	RPA	Brief group(s) journal volumes accessibility error co...
> Transient Error	Root Cause	Jul 7, 2021 4:54:11 PM	NY-Cluster	16014	RPA	The data path between all RPAs and all splitters (and storage) was briefly unavailable but the problem has been corrected.
> Transient Error	Root Cause	Jul 7, 2021 4:54:11 PM	NY-Cluster	16038	RPA	Brief group(s) journal volumes accessibility error co...
> Error	Normal	Jul 7, 2021 5:02:04 PM	NY-Cluster	4003	Consistency Group	Group capabilities problem
> Error	Normal	Jul 7, 2021 5:31:04 PM	NY-Cluster	4003	Consistency Group	Group capabilities problem
> Error	Normal	Jul 7, 2021 5:49:31 PM	NY-Cluster	4003	Consistency Group	Group capabilities problem
> Error	Normal	Jul 7, 2021 5:49:46 PM	NY-Cluster	4003	Consistency Group	Group capabilities problem
> Error	Normal	Jul 7, 2021 6:00:04 PM	NY-Cluster	4003	Consistency Group	Group capabilities problem
> Error	Normal	Jul 7, 2021 6:00:45 PM	NY-Cluster	4003	Consistency Group	Group capabilities problem
> Error	Normal	Jul 7, 2021 6:29:05 PM	NY-Cluster	4003	Consistency Group	Group capabilities problem

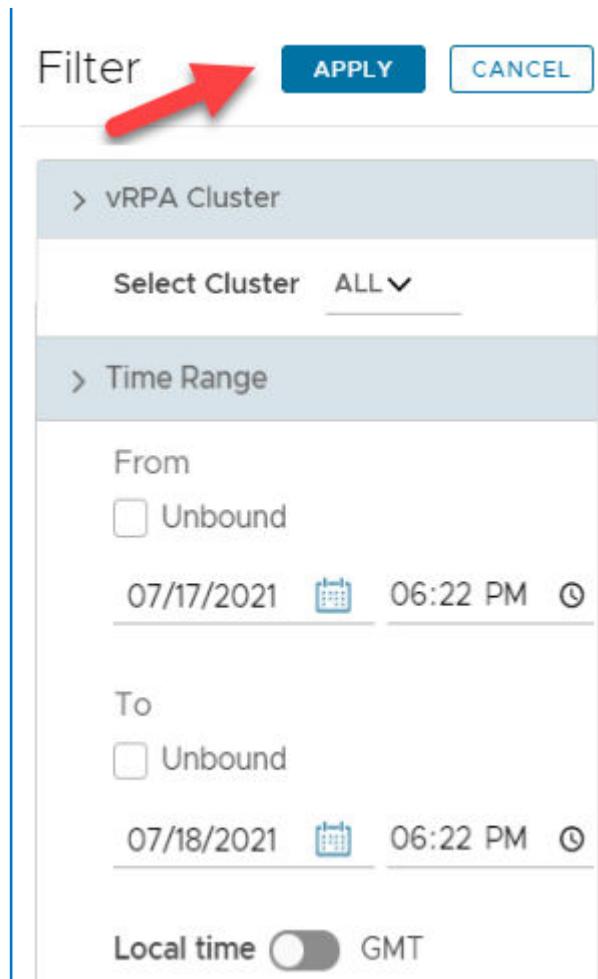
**Figure 3. RecoverPoint for VMs event logs**

1. Note the total number of events in the event logs.
2. Use the table controls to move to the next page, a previous page, or control the number of events that are displayed per page.
3. Click the **Event Filter** to control which events are displayed in the **Event** and which are hidden.

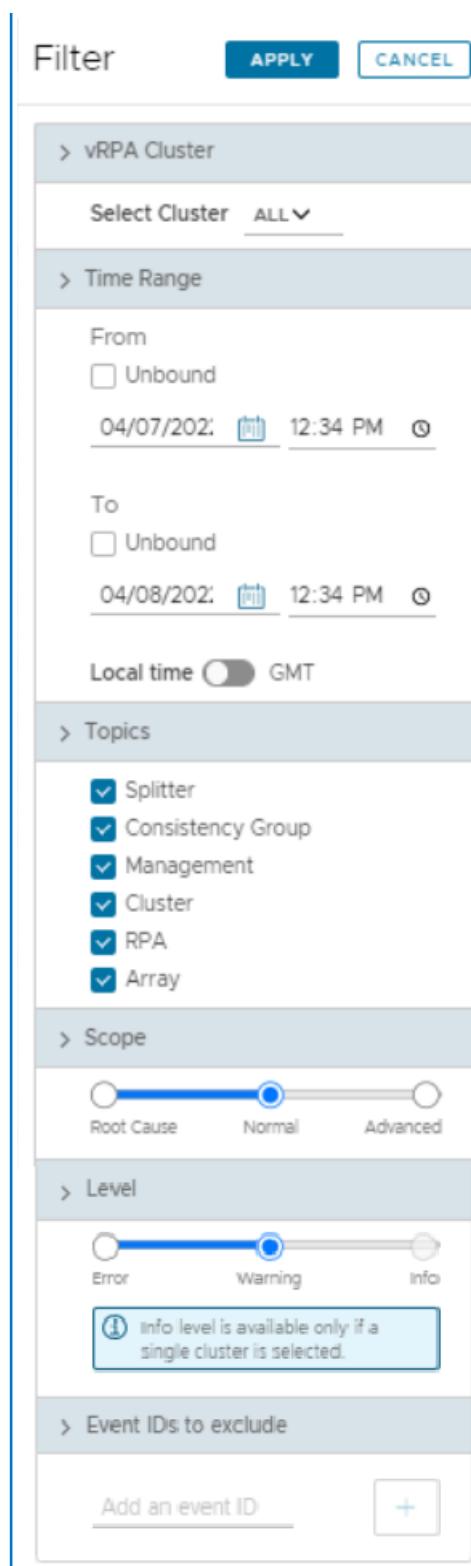


**NOTE:** Click **APPLY** after changing the event filter settings.

- Click **vRPA Cluster** to select the events for a specific vRPA cluster to display. By default, the events of all vRPA clusters are displayed.
- Click **Time Range** to select the events of a specific time period to display. Select **Unbound** to display all events. Display events based on your local time (the default) or GMT.



- Click **Topics** to hide or display events for specific system components. The event topic can be: **Splitter**, **Consistency Group**, **Management**, **Cluster**, **RPA**, or **Array**.
- Click **Scope** to hide or display logs of specific event scope. The event scope can be: **Normal**, **Root Cause**, or **Advanced**
- Click **Level** to hide or display events of a specific level. The event level can be **Info**, **Warning**, or **Error**.
- Click **Event IDs to exclude** to select the events to exclude from display in the events log.



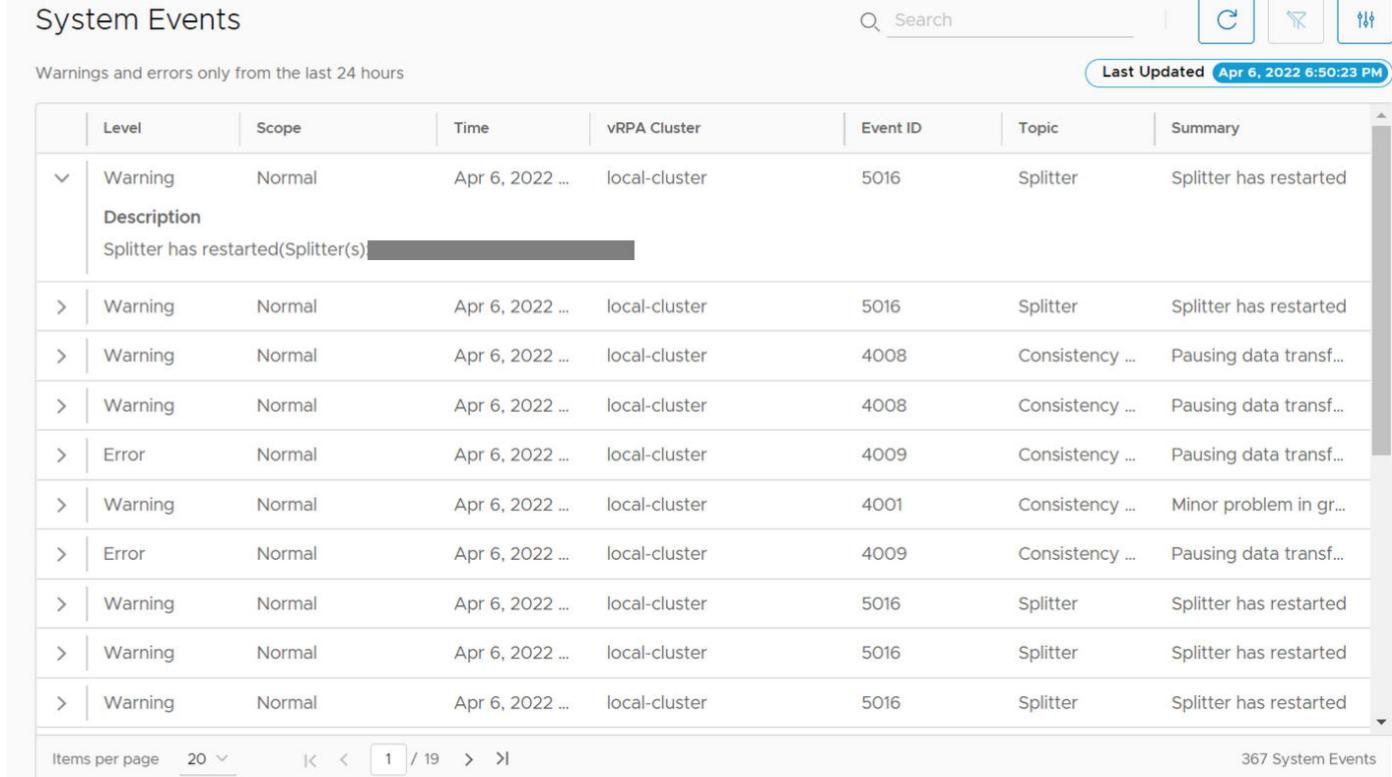
4. Note the date and time that the **Event Logs** were **Last Updated** and use the **Refresh** icon to update the **Event Logs**.
5. Hover over the **Summary** of an event with an ellipses (...) after it, to display hidden text.

While troubleshooting:

- Use the search bar to display only events that include specific text.



- Click the **Clear Filters** button to clear all event filters.
- Click an arrow to expand an event and display the event **Description** and **Details**.



System Events

Warnings and errors only from the last 24 hours

Last Updated Apr 6, 2022 6:50:23 PM

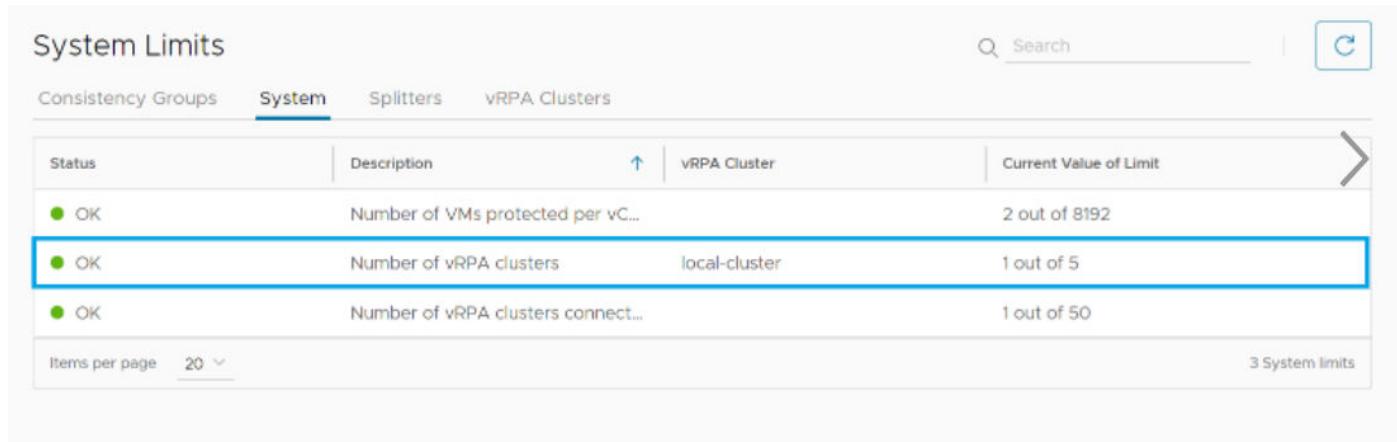
Level	Scope	Time	vRPA Cluster	Event ID	Topic	Summary	
Warning	Normal	Apr 6, 2022 ...	local-cluster	5016	Splitter	Splitter has restarted	
<b>Description</b> Splitter has restarted(Splitter(s))							
>	Warning	Normal	Apr 6, 2022 ...	local-cluster	5016	Splitter	Splitter has restarted
>	Warning	Normal	Apr 6, 2022 ...	local-cluster	4008	Consistency ...	Pausing data transf...
>	Warning	Normal	Apr 6, 2022 ...	local-cluster	4008	Consistency ...	Pausing data transf...
>	Error	Normal	Apr 6, 2022 ...	local-cluster	4009	Consistency ...	Pausing data transf...
>	Warning	Normal	Apr 6, 2022 ...	local-cluster	4001	Consistency ...	Minor problem in gr...
>	Error	Normal	Apr 6, 2022 ...	local-cluster	4009	Consistency ...	Pausing data transf...
>	Warning	Normal	Apr 6, 2022 ...	local-cluster	5016	Splitter	Splitter has restarted
>	Warning	Normal	Apr 6, 2022 ...	local-cluster	5016	Splitter	Splitter has restarted
>	Warning	Normal	Apr 6, 2022 ...	local-cluster	5016	Splitter	Splitter has restarted
Items per page	20	<	1 / 19	>	367 System Events		

## Monitor system limits

Monitor the limits that are imposed on your RecoverPoint for VMs system and system components to troubleshoot your system.

To monitor the state of your system limits, click **Monitoring > System Limits**. The **System Limits** screen displays the limits imposed on a system, or on consistency groups, vRPA clusters, or splitters in a system.

A system component's limit status can be '**Critical**', '**Warning**', or '**OK**'. Ensure an OK status is displayed for all of your system limits.



System Limits

Consistency Groups System Splitters vRPA Clusters

Status	Description	vRPA Cluster	Current Value of Limit
OK	Number of VMs protected per vC...		2 out of 8192
OK	Number of vRPA clusters	local-cluster	1 out of 5
OK	Number of vRPA clusters connect...		1 out of 50
Items per page	20	3 System limits	

Figure 4. System limits

System Limits					
Consistency Groups		System	Splitters	vRPA Clusters	
Status	Description	↑	vRPA Cluster	Consistency Group	Current Value of Limit
● OK	Lag (in seconds)		Site2	cg_Win5	1 out of 25
● OK	Lag (in seconds)		Site1	cg_Win1	0 out of 25
● OK	Lag (in seconds)		Site1	cg_Win1	1 out of 25
● OK	Number of non-production copies		Site1	cg_Win1	2 out of 4
● OK	Number of non-production copies		Site1	cg_Win5	1 out of 4
● OK	Number of VMs		Site1	cg_Win1	1 out of 128
● OK	Number of VMs		Site1	cg_Win5	1 out of 128

**Figure 5. Consistency group limits**

System Limits				
Consistency Groups		System	Splitters	vRPA Clusters
Status	Description	↑	vRPA Cluster	Current Value of Limit
● OK	Number of consistency groups		Site1	2 out of 512 groups
● OK	Number of ESX clusters		Site2	1 out of 8 clusters
● OK	Number of ESX clusters		Site1	1 out of 8 clusters
● OK	Number of ESX hosts with a splitter		Site2	2 out of 256
● OK	Number of ESX hosts with a splitter		Site1	2 out of 256
● OK	Number of protected VMDKs		Site2	4 out of 4096 protected VMDKs
● OK	Number of protected VMDKs		Site1	4 out of 4096 protected VMDKs
● OK	Number of protected VMs		Site2	2 out of 1024 protected VMs
● OK	Number of protected VMs		Site1	3 out of 1024 protected VMs
● OK	Number of vCenter Servers		Site1	1 out of 4 VCs
● OK	Number of vCenter Servers		Site2	1 out of 4 VCs

**Figure 6. vRPA cluster limits**

System Limits

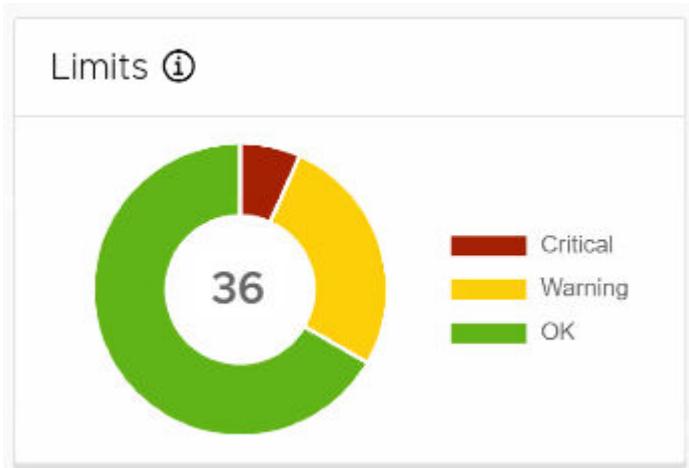
Consistency Groups   System   **Splitters**   vRPA Clusters

Search

Status	Description	Splitter	Current Value of Limit
● OK	Number of vRPA clusters attached to splitter	██████████	1 out of 128
● OK	Number of vRPA clusters attached to splitter	██████████	1 out of 128
● OK	Number of vRPA clusters attached to splitter	██████████	1 out of 128
● OK	Number of vRPA clusters attached to splitter	██████████	1 out of 128
● OK	Total number of VMDKs attached to splitter	██████████	4 out of 25000
● OK	Total number of VMDKs attached to splitter	██████████	4 out of 25000
● OK	Total number of VMDKs attached to splitter	██████████	6 out of 25000
● OK	Total number of VMDKs attached to splitter	██████████	6 out of 25000

Items per page  20 8 Splitter Limits

**Figure 7. Splitter limits**



## Monitor system components

Monitor RecoverPoint for VMs system components to better understand and troubleshoot your RecoverPoint for VMs environment.

To monitor the state of your system components, click **Monitoring > Components**. In the **System Components** screen, ensure an OK status is displayed next to each of your RecoverPoint for VMs system components.

## System Components

Search

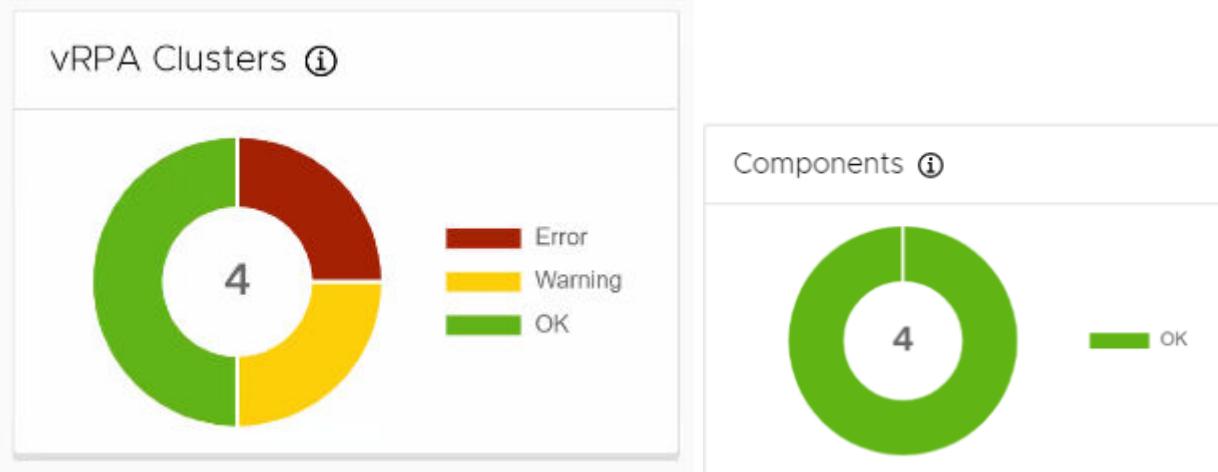


Status	Name	Type	vRPA Cluster	Version
● OK	VRPA1	vRPA	Site2	vRPA: 5.3.SP2(m.240)
● OK	VRPA2	vRPA	Site2	vRPA: 5.3.SP2(m.240)
● OK	██████████	ESX Splitter	Site2	SPLITTER: 5.3.SP2(m.222) JAM: 5.3.SP2(m.180)
● OK	██████████	ESX Splitter	Site2	SPLITTER: 5.3.SP2(m.222) JAM: 5.3.SP2(m.180)
● OK	VRPA2	vRPA	Site1	vRPA: 5.3.SP2(m.240)
● OK	VRPA1	vRPA	Site1	vRPA: 5.3.SP2(m.240)
● OK	██████████	ESX Splitter	Site1	SPLITTER: 5.3.SP2(m.222) JAM: 5.3.SP2(m.180)
● OK	██████████	ESX Splitter	Site1	SPLITTER: 5.3.SP2(m.222) JAM: 5.3.SP2(m.180)

Items per page  ▾

8 System Components

**(i) NOTE:** You can also monitor the state of **vRPA clusters** and **Components** in the [RecoverPoint for VMs Dashboard](#).



## Monitor group and copy protection

Monitor the status of replication for consistency groups and copies, when managing or troubleshooting your system.

### Steps

1. Select **Protection > Consistency Groups**.
2. Expand a group.
3. Note the **Transfer Status (1)** and **State (2)** of each consistency group and the **Status (3)** of each copy.

Consistency Groups					
PROTECTION POLICY		BOOKMARK	TEST A COPY	RECOVER PRODUCTION	FAILOVER
	Consistency Group	Production vCenter Server	Production vRPA Cluster	Protected Size	Transfer Status
○	cg_copyVmRemote	VM-RP-Lab-VC-12.rp.lcoe.lab.emc.com	Patagonia	40 MB	● Error
●	cg_newVm	VM-RP-Lab-VC-12.rp.lcoe.lab.emc.com	Patagonia	20.2 GB	● Active
Production					
>  Production		vRPA Cluster Patagonia			
Copies (3)					
>  Local Copy		vRPA Cluster Patagonia	Status  OK	⋮	
>  Remote Copy 1		vRPA Cluster Darwin	Status  OK	⋮	
>  Remote Copy 2		vRPA Cluster Darwin	Status  OK	⋮	
Items per page		20	▼	2 Consistency groups	

## Results

- The **Transfer Status (1)** of a consistency group can be:
  - Active**: Data is being transferred to a copy.
  - Initializing**: A copy is being initialized: volume sweep, short init, or full sweep.
  - High Load**: The system enters a temporary high-load state while data is being transferred to a copy, when the journal is full and cannot accept new writes. The system attempts to resolve the high-load state without user action.
  - Paused by System**: System paused replication so data is not being transferred. If this state occurs for long periods of time, check the system alerts and events in the **Dashboard** for more information.
  - Error**: An error has occurred.
  - Permanent High Load**: The system enters a permanent high-load state while data is being transferred to a copy. A permanent high-load can occur after a temporary high-load. The system pauses replication and waits for user action.
  - Paused**: User paused replication so data is not being transferred to a copy.
  - Disabled**: User disabled a copy so data is not being transferred.
- The **State (2)** of a consistency group can be:
  - Enabled**: A group is enabled for replication.
  - Failed over**: A multicity group has completed temporary failover.
  - Being recovered**: A group is in the process of recovering production.
  - Partially suspended**: Some of the copies of a group have been momentarily suspended while being upgraded.
  - Suspended**: All the copies of the group have been momentarily suspended while being upgraded.
  - Disabled**: A group is disabled for replication.
- The **Status (3)** of a copy can be:
  - OK**: Data can be transferred to the copy.
  - Initializing**: A copy is being initialized: volume sweep, short init, or full sweep.
  - High Load**: A copy enters a temporary high-load state while data is being transferred to the copy, when the journal is full and cannot accept new writes. The system attempts to resolve the high-load state for the copy without user action.
  - Paused by System**: System paused replication so data is not being transferred to a copy. If this state occurs for long periods of time, check the system alerts and events in the **Dashboard** for more information.
  - Error**: An error has occurred on the copy.
  - Permanent High Load**: A copy enters a permanent high-load state while data is being transferred to the copy. A permanent high-load can occur after a temporary high-load. The system pauses replication to the copy and waits for user action.
  - Paused**: User paused replication so data is not being transferred to a copy.
  - Disabled**: User disabled a copy so data is not being transferred.

## Reports

Reports menu option where a user can access a range of reports at different levels and for specific objects.

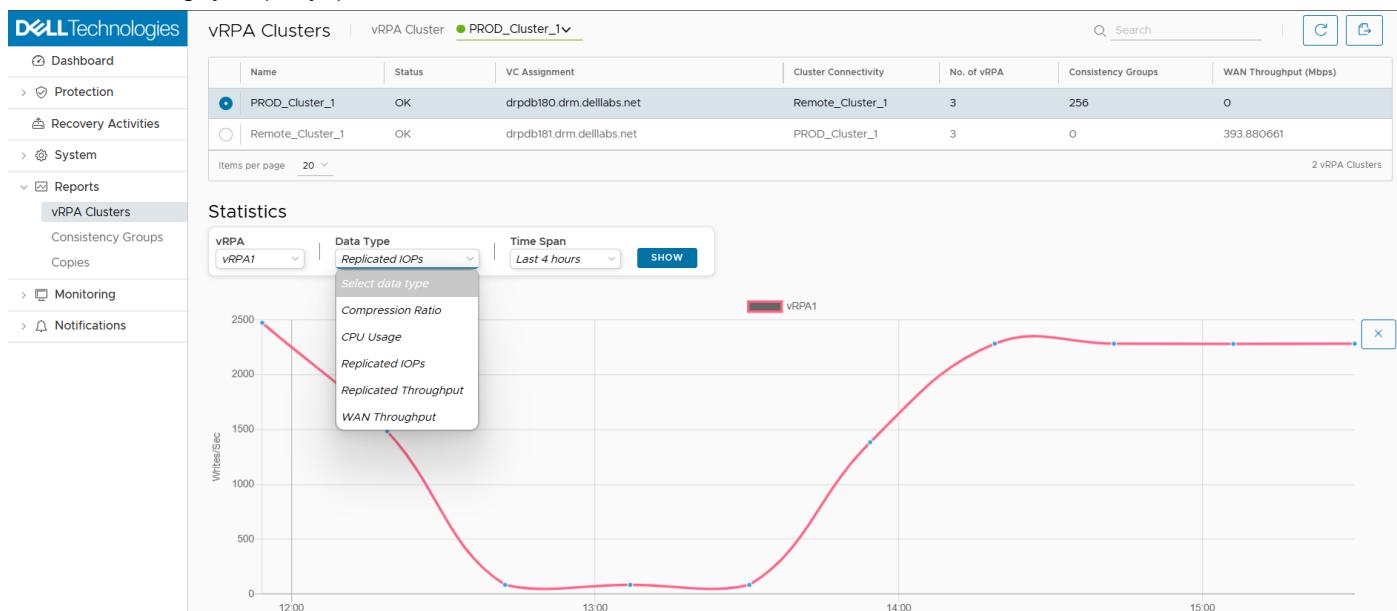
## Reports vRPA Clusters

This section contains details about Reports for vRPA cluster that are imposed on your RecoverPoint for VMs system to view a vRPA cluster health from RPC.

To view vRPA Cluster and its detailed statistics click **Reports > vRPA Clusters**.

By default in **vRPA Clusters** the following information displays,

- **Name:** which can be cluster name that is given at cluster creation.
- **Status:** which can be ok.
- **VC Assignment** name of the VC.
- **Cluster Connectivity** shows connected cluster.
- **No. Of vRPA** gives count of vRPAs in cluster.
- **Consistency Groups** gives count of consistency group in cluster.
- **WAN Throughput (Mbps)**



To view reports of vRPA Cluster in Statistics select **vRPA Clusters** and in Statistics click **vRPA > Data Type > Time Span > SHOW**, system displays the graphical representation of the system in a specified time span.

In Statistics, the **Data Type** drop down lists Compression Ratio, CPU Usage, Replicated IOPs, Replicated Throughput and WAN Throughput.

## Reports Consistency Groups

To view Consistency Groups and its detailed statistics click **Reports > Consistency Groups**, by default in **Consistency Groups** the following information displays,

- **Name:** which can be cluster name that is given at cluster creation.
- **Cluster** displays the cluster name.
- **Status:** which can be Enabled, Disabled, Pause depends on consistency group status.
- **RPA Assignment** displays the **vRPA** assigned to consistency group.
- **Copies** displays the number of copies for consistency group.

Consistency Groups | vRPA Cluster PROD\_Cluster\_1

Name	Cluster	Status	RPA Assignment	Copies
CG1	PROD_Cluster_1	Enabled	2	1
CG10	PROD_Cluster_1	Enabled	1	1

Items per page 20 | 1 / 13 | < > |

256 Consistency Groups

Statistics

Data Type: Incoming IOPs | Time Span: Last 4 hours | SHOW

Select data type: Incoming Throughput, Incoming IOPs, Links Init Traffic, Links Time Lag, Links Compression Ratio, Journal Lag.

Remote Copy

12:00 13:00 14:00 15:00

To view reports of Consistency Groups in Statistics select **Consistency Groups** and in Statistics click **Data Type>Time Span>SHOW**, system displays the graphical representation of the system in a specified time span.

In Statistics, the **Data Type** drop down lists Incoming Throughput, Incoming IOPs, Links init Traffic, Links Time Lag, Links Compression Ratio, and Journal Lag.

## Reports Copies

To view Copies and its detailed statistics click **Reports > Copies**

By default in **Copies** the following information displays,

- **Group Name** displays the name of consistency group.
- **Copy Name** displays the name of the copy.
- **Copy Role** displays the role of copies **Local Copy or Remote Copy**.
- **Transfer Status** displays the copies status.

**Replication Mode** which can be **Async**.

Copies | vRPA Cluster Remote\_Cluster\_1

Group Name	Copy Name	Copy Role	Transfer Status	Replication Mode
CG136	Replica_at_remote_cluster_1	Remote Copy	Active	Async
CG15	Replica_at_remote_cluster_1	Remote Copy	Active	Async
CG22	Replica_at_remote_cluster_1	Remote Copy	Active	Async
CG10	Replica_at_remote_cluster_1	Remote Copy	Active	Async
CG239	Replica_at_remote_cluster_1	Remote Copy	Active	Async
CG168	Replica_at_remote_cluster_1	Remote Copy	Active	Async
CG122	Replica_at_remote_cluster_1	Remote Copy	Active	Async
CG60	Replica_at_remote_cluster_1	Remote Copy	Active	Asvnc

Items per page 20 | 1 / 13 | < > |

256 Copies

Statistics

Current RPO	25 Seconds	Journal Capacity	7.71 GB
Retention Period	29 hours, 13 minutes, 43 Seconds	Journal Lag	0 B
Required Retention Period	NA	Image Access	No Access

To view reports of Copies in Statistics select **Copies** and in Statistics system displays Current RPO, Retention Period, Required Retention Period, Journal Capacity, Journal Lag, Image Access.

# VM automation and orchestration

RecoverPoint for Virtual Machines provides the following features that automate and orchestrate the recovery of your copy VMs.

## Topics:

- [Create a bookmark](#)
- [Creating an Application-Consistent Bookmark using KVSS](#)
- [Automation](#)
- [Orchestration](#)

## Create a bookmark

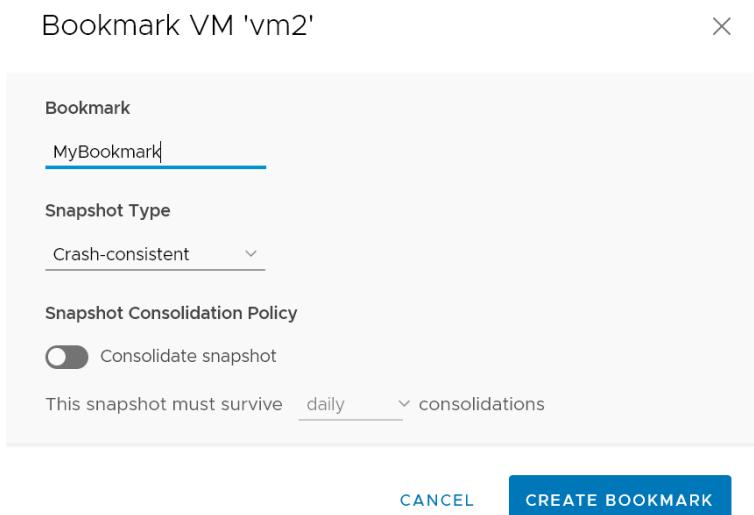
Label a snapshot of a virtual machine, a consistency group, or a group set, for identification during testing and recovery. RecoverPoint for Virtual Machines creates crash-consistent snapshots.

### About this task

Creating a bookmark on a protected VM creates a bookmark on all copy VMs of the group containing the protected VM. Creating a bookmark on a consistency group that is part of a group set creates a bookmark on all copy VMs of all groups in the group set.

### Steps

1. In the RecoverPoint for Virtual Machines plugin for vSphere Client:
  - To bookmark a snapshot of a consistency group, click **Protection > Consistency Groups**.
  - To bookmark a snapshot of a protected virtual machine, click **Protection > Protected VMs**.
  - To bookmark a snapshot of a group set, click **Protection > Group Sets**.
2. Select the consistency group, protected VM, or group set that you want to bookmark.
3. Click **BOOKMARK**.
4. In the **Bookmark** dialog:



- **Bookmark:** Enter a name for the snapshot. The bookmark is the name that is used to identify the snapshot during testing and recovery.

- **Snapshot Type:** Default is **crash-consistent**. Change this value to application-consistent only if you know this snapshot to be application consistent. Selecting **application-consistent** does not create an application-consistent snapshot, it only labels the snapshot as known to be application-consistent.
- **Snapshot Consolidation Policy**
  - **Consolidate snapshot:** Default is **disabled**.
  - **This snapshot must survive daily, weekly, or monthly consolidations:** Default is **daily**.
    - **Daily:** Snapshot survives daily consolidations but is consolidated weekly and monthly.
    - **Weekly:** Snapshot survives daily and weekly consolidations but is consolidated monthly.
    - **Monthly:** Snapshot survives daily, weekly, and monthly consolidations.

5. Click **CREATE BOOKMARK**.

### Results

A crash-consistent snapshot is created for the specified VM, group, or group set, with the specified label and consolidation policy.

If the bookmark was created on a:

- Protected VM, the system creates a bookmark on all copy VMs of the group containing the protected VM.
- Consistency group that is part of a group set, the system creates a bookmark on all copy VMs of all groups in the group set.

### Next steps

To display bookmarks, go to **Protection > Consistency Groups**, expand a group, and select **Snapshots** from the copy commands.

## Creating an Application-Consistent Bookmark using KVSS

KVSS bookmarks are created using the `kvss.exe bookmark` command. The working directory for running KVSS commands is: `%SystemDriver%/EMCRecoverPointVSSProvider/`

### Before you begin

#### Installation

- Download and extract KVSS Utility.
- Run `install-kvss-provider`.
- A folder with the name `EMCRecoverPointVssProvider` is created in `%SystemDriver%`, which is usually C:/ Drive.
- Verify the installation by running `kvss.exe version` command from `%SystemDriver%/EMCRecoverPointVSSProvider/`.

When using KVSS to apply bookmarks:

- Surround parameter values with quotation marks.
- Use the command `vssadmin list writers` to get a list of registered writers on the host virtual machine.
- Use the `kvss.exe list` command to display the components of each writer found using the `vssadmin list writers` command.
- Run the `kvss.exe set_credentials` command once per Windows user to define the IP, user, and password. This step removes the requirement to input these values repeatedly.
- You can specify multiple writers and groups simultaneously if separated by spaces.
- Ensure you run KVSS on the same virtual machine as the application to maintain application consistency.
- Upgrade Best Practice: Always upgrade vRPA clusters before upgrading KVSS. An older KVSS version works with newer vRPA clusters, but not conversely.

## Command Syntax

```
kvss.exe bookmark
bookmark=<bookmark_name>
  writers=<writer_name> [writer_name]
  [groups=<group_name> [group_name]]
  [consolidation_policy=never|survive_daily|survive_weekly|survive_monthly|always]

  [type=[FULL|COPY]]
  [ip=<RecoverPoint_cluster_management_ip_address>]
  [user=<RecoverPoint_username>]
  [password=<RecoverPoint_password>]
```

 **NOTE:** Parameters surrounded by [ ] are optional. Use the -version flag to check the KVSS version.

## Parameter Descriptions

**Table 2. Parameter Description**

Option	Description
writers	Specifies a VSS-aware host application.
groups	Defines the RecoverPoint consistency group.
bookmark	The name of the bookmark for identification.
consolidation_policy	Specifies the consolidation policy for snapshots: <ul style="list-style-type: none"><li>never: Snapshot is never consolidated.</li><li>survive_daily: Survives daily consolidations but consolidated in weekly, monthly, and manual processes.</li><li>survive_weekly: Survives daily/weekly consolidations but not monthly.</li><li>survive_monthly: Survives all but manual consolidations.</li><li>always: Consolidated in every process (default).</li></ul>
type	Defines shadow copy type: FULL or COPY (default = COPY).
ip	Specifies the vRPA cluster management IP.
user	The RecoverPoint for VMs username.
password	The RecoverPoint for VMs password.

## Procedure

### Creating a Bookmark for Microsoft Exchange (First Time)

1. Set credentials:

```
kvss.exe set credentials
  ip="10.10.0.145"
  user="admin"
  password="admin"
```

2. Create a bookmark:

```
kvss.exe bookmark
  writers="Microsoft Exchange Writer"
  groups="exchange\comp1" "exchange\comp2"
  bookmark="exchange hourly snapshot"
  consolidation_policy="survive_daily"
```

### Creating Subsequent Bookmarks for Microsoft Exchange

After setting the credentials once, use the following command:

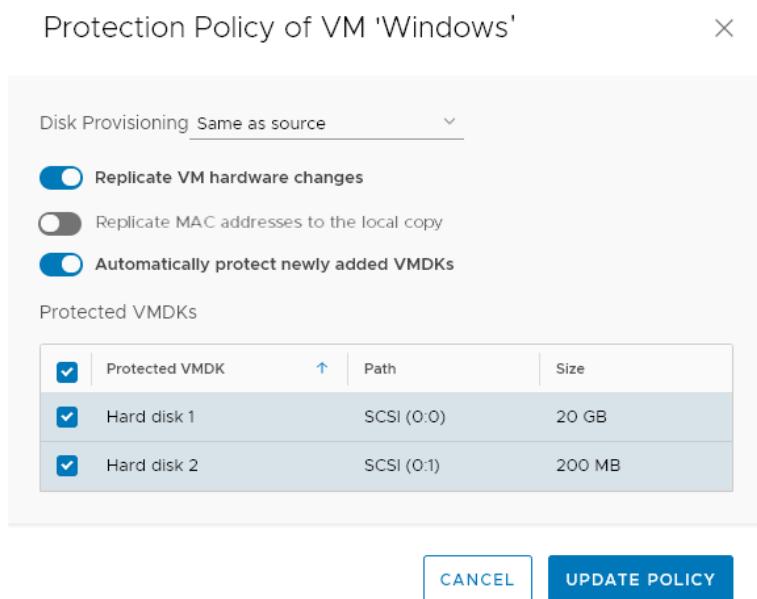
```
kvss.exe bookmark
writers="Microsoft Exchange Writer"
groups="exchange\comp1" "exchange\comp2"
bookmark="exchange hourly snapshot"
consolidation_policy="survive_daily"
```

## Automation

This section describes the RecoverPoint for Virtual Machines features for automating the replication of virtual machines and VMDKs.

VM automation can be defined when protecting VMs, or later through the VM protection policy.

To configure VM automation after protection, select **Protection > Protected VMs**, select a VM, and click **PROTECTION POLICY**.



## Automatic protection of newly added VMDKs

Define whether or not VMDKs that are added to a protected VM should automatically be protected.

### About this task

By default, all newly added VMDKs are automatically protected. Use this procedure to change the default behavior.

### Steps

1. Click **Protection > Protected VMs**.
2. Select the virtual machine for which you want to disable the automatic protection of any newly added VMDKs, in the future.
3. Click **PROTECTION POLICY**.
4. Disable or enable **Automatically protect newly added VMDKs**.
5. Click **UPDATE POLICY**.

### Results

The protection policy is updated and RecoverPoint for VMs will use the new policy the next time a VMDK is added to this VM.

## Provisioning copy VMDKs

Define the way copy VMs are provisioned, per consistency group.

### About this task

By default, copy VMDKs are provisioned **Same as source**. Use this procedure to change the default behavior.

### Steps

1. Click **Protection > Protected VMs**.
2. Select a protected VM.
3. Click **PROTECTION POLICY**.
4. In the **Disk Provisioning** drop-down, select **Same as source**, **Thick provision lazy zeroed**, **Thick provision eager**, or **Thin provision**.
5. Click **UPDATE POLICY**.

### Results

Newly added copy VMDKs are provisioned according to the specified settings. Copy VMDKs that were already provisioned will not be re-provisioned, and will keep the provisioning method defined during initial protection.

## Excluding a VMDK from replication

Include or exclude protected VMDKs from replication.

### About this task

Protected VMs containing nonpersistent VMDKs cannot be replicated. They should be excluded from replication or their VMDK type should be changed through vSphere Client.

- Excluded VMDKs are not replicated, but their corresponding copy VMDKs are not deleted. Excluded copy VMDKs are created at the copy, but writes going to excluded VMDKs are not replicated to their copy VMDKs.
- Copy VMDKs are created for any production VMDKs, both included and excluded. For most efficient use of storage resources, ensure that disk provisioning is configured as **Thin provision** (or **Same as source**, if production is thin provisioned) before adding the VMDK or upon VM protection.
- Changing the disk type of a nonpersistent VMDK to a persistent VMDK does not automatically include the VMDK in replication, even if **Automatically protect newly added VMDKs** is enabled.

### Steps

1. Click **Protection > Protected VMs**.
2. Select the VM whose VMDKs you want to exclude from replication.
3. Click **PROTECTION POLICY**.
4. Clear the check box next to each **Protected VMDK** that you want to exclude from replication.
5. Click **UPDATE POLICY**.

### Results

In the future, the excluded VMDKs are not displayed in the list of snapshots that you can select when [Recovering VMs](#) from a previous point in time, even when recovering snapshots from a time previous to the VMDK removal.

## Automatic replication of VM hardware changes

Enables or disables the automatic replication of hardware changes made to a protected VM.

### About this task

By default any hardware changes made to a protected VM through the vSphere Client VM Properties are replicated to all copy VMs. Use this procedure to change the default system behavior.

RecoverPoint for VMs replicates the protected VM **version**, **MAC address**, **CPU**, **memory**, **resource reservations**, **network adapter status**, and **network adapter type** to all copy VMs in the consistency group, upon image access.

**i** **NOTE:** Replication of the SR-IOV NIC type is not supported. If the ESXi at a copy does not support the production VM version, no hardware resources are replicated.

## Steps

1. Click **Protection > Protected VMs**.
2. Select a protected VM.
3. Click **PROTECTION POLICY**.
4. Switch **Replicate VM hardware changes** off.
5. Click **UPDATE POLICY**.

## Results

Replication of the protected VM hardware changes is enabled or disabled, as defined.

# Orchestration

This section describes the RecoverPoint for VMs features for orchestrating virtual machines and VMDKs.

## VM start-up sequence

Define the order in which VMs in a consistency group turns on during testing and recovery.

### Prerequisites

Install VMware Tools on every production VM. When VMware Tools is installed on a production VM, the VM is considered turned on only after its operating system loads. When VMware Tools is not installed on a production VM, the VM is considered turned on when it is turned on.

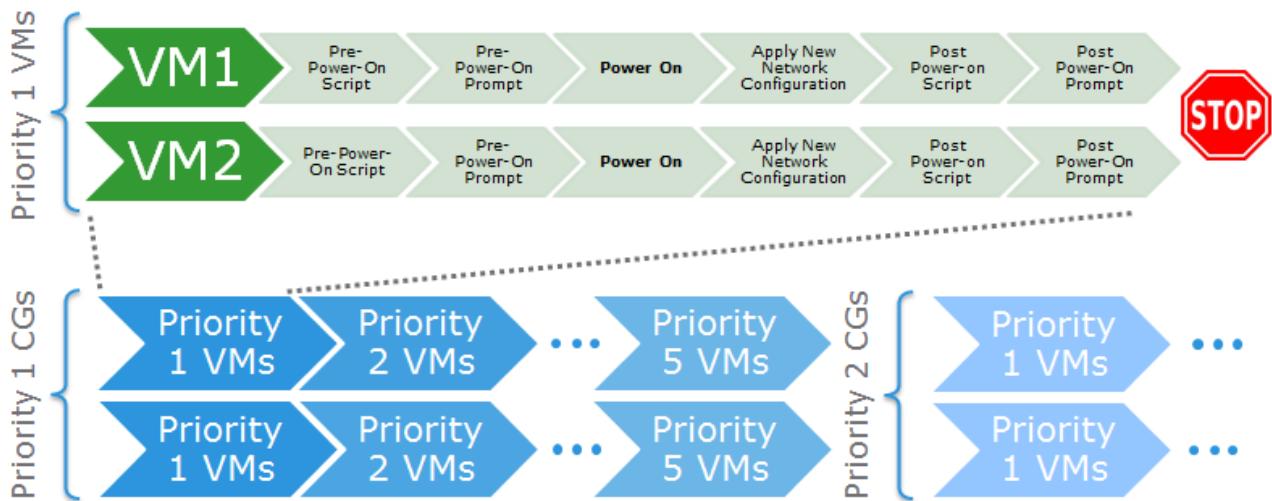
### About this task

The VM start-up sequence:

- Is initiated when a copy snapshot is accessed during testing or recovery.
- Moves to the next VM in the start-up sequence only when a VM is turned on.
- Enables you to define a VM as **Critical** to ensure that no other VMs turn on if the critical VM fails to turn on first.
- Can contain an **Operation**, with one **user script** and one **user prompt** that will run before VM power-on and after VM power-on. Operations run in a strict sequence: **script > prompt > power-up > script > prompt**.

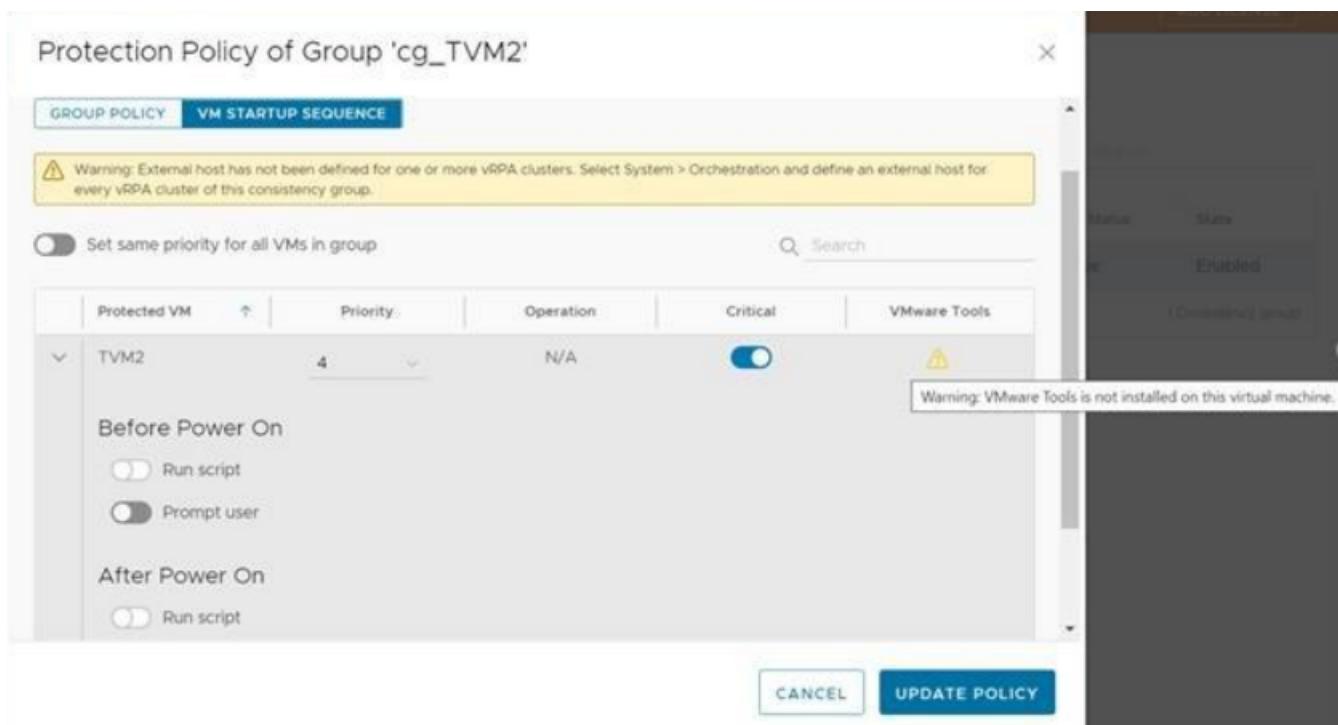
See [Defining user prompts](#) and [Defining user scripts](#) for more information.

The following diagram illustrates the order of sequences:



## Steps

1. Click **Protection > Consistency Groups**.
2. Select a consistency group, and click **PROTECTION POLICY**.  
The **Group Protection Policy** dialog is displayed.
3. In the **Group Protection Policy** dialog, click **General > VM STARTUP SEQUENCE**.



If the power-on sequence also performs an operation (contains scripts and prompts), a check mark is displayed in the **Operation** column. See [Defining user scripts](#) and [Defining user prompts](#) for more information.

4. Enable **Set same priority for all VMs in group**, or define a **Priority** for each VM in the group.  
By default, all priorities are set to 3.

Priority	Description
1	The first VMs to turn on in the group.

Priority	Description
2	The second VMs to turn on in the group.
3	The third VMs to turn on in the group.
4	The fourth VMs to turn on in the group.
5	The last VMs to turn on in the group.

5. Optionally, select each VM whose start-up sequence you want to stop if the VM does not turn on, and set it to **Critical**.
6. Click **UPDATE POLICY**.

## Results

During testing and recovery, the VMs in the group are turned on in the defined order of priority. All the VMs with the same priority turn on simultaneously.

## Defining user prompts

Define a message to display to the administrator that will perform VM copy testing and recovery. User prompts remind the administrator to perform specific tasks before continuing the start-up sequence.

### About this task

When defining a [VM start-up sequence](#), you can add a user prompt before power-on and a user prompt after power-on. Administrator's will have to dismiss the prompt before the start-up sequence continues. If a timeout is defined, the prompt is automatically dismissed when the time-out period passes. If no time-out is defined and a prompt is not dismissed, the start-up sequence does not continue until the prompt is dismissed.

### Steps

1. Select **Protection > Consistency Groups**, select a consistency group, and click **PROTECTION POLICY**.
2. In the **Protection Policy** dialog, select **General > VM STARTUP SEQUENCE**.
3. Expand a VM, and enable **Prompt user** before or after VM power-on.
4. Type a descriptive name for the prompt.
5. Type the prompt message.
6. Optionally, set the time-out period.

## Results

During testing and recovery, administrator's will have to dismiss the prompt before the start-up sequence continues, unless a timeout is defined.

## Defining user scripts

Run commands immediately before or after VMs are powered-on during testing and recovery.

### Prerequisites

- An external host must be configured. One external host can be defined per vRPA cluster. See [Managing external host registration](#) for more information.
- An SSH server must be installed on each external host.

### About this task

When defining a [VM start-up sequence](#), you can also define the scripts that will be run before or after VMs are powered-on.

- The scripts are run with ssh on the external host that you designate.
- Each script has a mandatory time-out period. The recovery flow is blocked until the script runs successfully. A prompt indicates if the script failed.
- You can define one user script before power-on, and one user script after power-on per VM.
- The maximum size of the script name and parameters is 1024 bytes.

## Steps

1. Select **Protection > Consistency Groups**, select a consistency group, and click **PROTECTION POLICY**.
2. In the **Protection Policy** dialog, select **General > VM STARTUP SEQUENCE**.
3. Expand a VM, and enable **Run script** before or after VM power-on.
4. Type a descriptive name for the script.
5. Type the script command, including parameters (separated by a space).
6. Set the time-out period (mandatory).
7. Specify the number of retries. If the script does not run within the set time or the script fails, the system retries the script this number of times.

## Results

During testing and recovery, these scripts will run before the start-up sequence continues.

## Group start-up sequence

Define the order in which VMs of each consistency group in a group set power-on during testing and recovery.

### Prerequisites

Install VMware Tools on every production VM. When VMware Tools is installed on a production VM, the VM is considered *turned on* only after its operating system loads. When VMware Tools is not installed on a production VM, the VM is considered *turned on* when it is turned on.

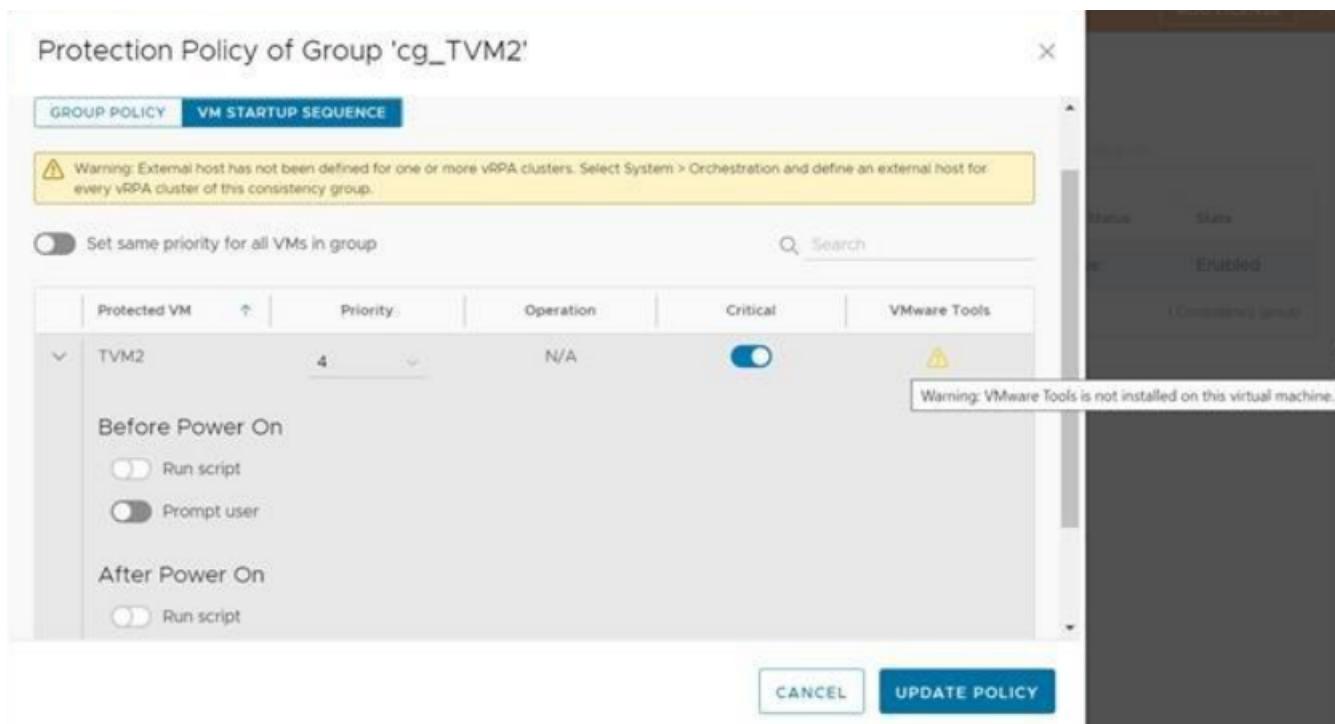
### About this task

The group start-up sequence:

- Is initiated when a copy snapshot is accessed during testing or recovery.
- Moves to the next group of VMs in the start-up sequence only when the last group of VMs are all *turned on*.

## Steps

1. Click **Protection > Group Sets**.
2. Select a group set.
3. Click **[...] > Group priority**, and define a **Priority** for each consistency group in the group set.



Priority	Description
1	The first group (VMs) to turn on in the group set.
2	The second (VMs) to turn on in the group set.
3	The third group (VMs) to turn on in the group set.
4	The fourth group (VMs) to turn on in the group set.
5	The last group (VMs) to turn on in the group set.

4. Click **SAVE**.

## Results

During testing and recovery, group VMs are turned on in the defined order of priority. All group VMs with the same priority turn on simultaneously.

## Create a group set

Add a group set to RecoverPoint for Virtual Machines.

### About this task

A group set is a collection of consistency groups that you can bookmark, enable, disable, pause and resume replication for, and test and recover as a group. You can also create parallel bookmarks on all groups in the group set, at a frequency that you define. Group sets are useful for consistency groups that rely on one another or that must work together as a single unit.

**i** **NOTE:** You cannot enable parallel bookmarking for a group set containing a group that is part of another group set that has parallel bookmarking enabled.

### Steps

1. Select **Protection > Group Sets**.  
The **Group Sets** screen is displayed.

Group Set	Consistency Groups	Parallel Bookmark Frequency	vRPA Cluster
My_GroupSet2	1	10 minutes	WELL
MyGroupSet	2	No parallel bookmarks	WELL

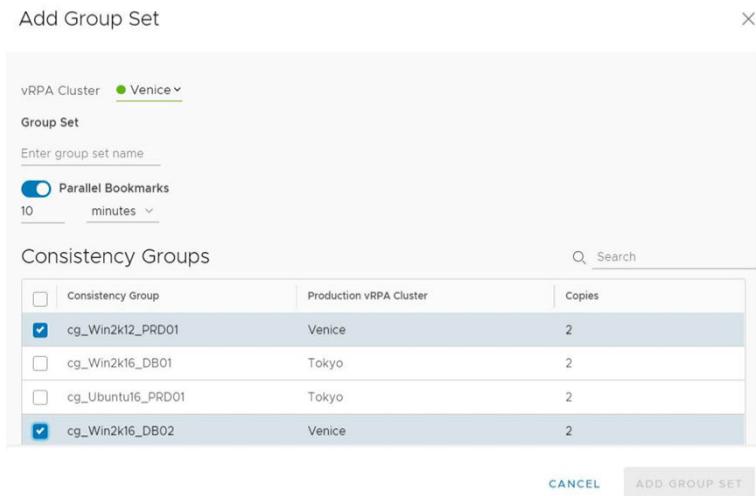
Consistency Group	Production vRPA Cluster	Copies
MyGroup2	WELL	2
MyGroup	ALLIS	3

2 Consistency groups in 'MyGroupSet'

Items per page: 20

2 Group sets

2. Click **ADD**.  
The **Add Group Set** dialog is displayed.
3. In the **Add Group Set** dialog:



- a. Choose the vRPA cluster that the consistency groups you want to add to the group set are replicating from. All groups in a group set must be replicating from the same vRPA cluster.
  - b. Enter a descriptive name for the group set.
  - c. (Optional) To create bookmarks for all consistency groups in the group set at the same interval, enable **Parallel Bookmarks** and set the required bookmark interval frequency.
  - d. Select the consistency groups to add to the group set.
4. Click **ADD GROUP SET**.

## Results

A new group set is created with the specified settings.

## Next steps

See [Managing group sets](#) for additional group set capabilities.

## Re-IP rules

Create Re-IP rules to update the network configuration of one or more copy VMs when *testing a copy, failing over, or recovering production*.

### Prerequisites

- See SSM always for any OS support .
- VMware Tools should be installed on each relevant production VM:
  - For Linux SLES12, automatic network configuration is not supported unless *Open VM Tools* version 9.4.0.25793 and **deployPkg** has been manually installed. See [VMWare KB article 2075048](#) for detailed information about how to install **deployPkg**.
  - For VMs running *Open VM Tools* versions lower than 9.10, automatic network configuration is not supported unless **deployPkg** has been manually installed. See [VMWare KB article 2075048](#) for detailed information about how to install **deployPkg**.
- Read the [Copy VM network configuration guidelines](#).
- Ensure you do not lose your production VM network configuration during failback by also creating re-ip rules for your production VMs.

### Steps

- You can specify the testing network of one or more VMs at a copy, or of all copy VMs in the system.

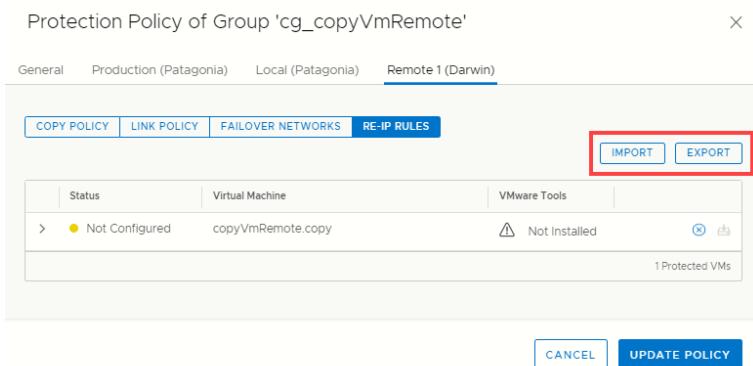
**NOTE:** Re-IP configuration using glue scripts is not available in the vSphere HTML5 plugin.

## Re-IP a few copy VMs

Update the network configuration of a few VMs at a copy.

### Steps

1. In the RecoverPoint for VMs plugin for vSphere Client, select **Protection > Consistency Groups**.
2. Select a consistency group, and click **PROTECTION POLICY**.  
The group **Protection Policy** dialog is displayed.
3. Select the tab of the **Production** or a **Copy** and click the **RE-IP RULES** tab.



4. To retrieve the network configuration of all copy VMs at all vRPA clusters in the system, click **Get values from production**.
5. Update the network values of each copy according to the [Copy VM network configuration guidelines](#).
6. Click **UPDATE POLICY**.

### Results

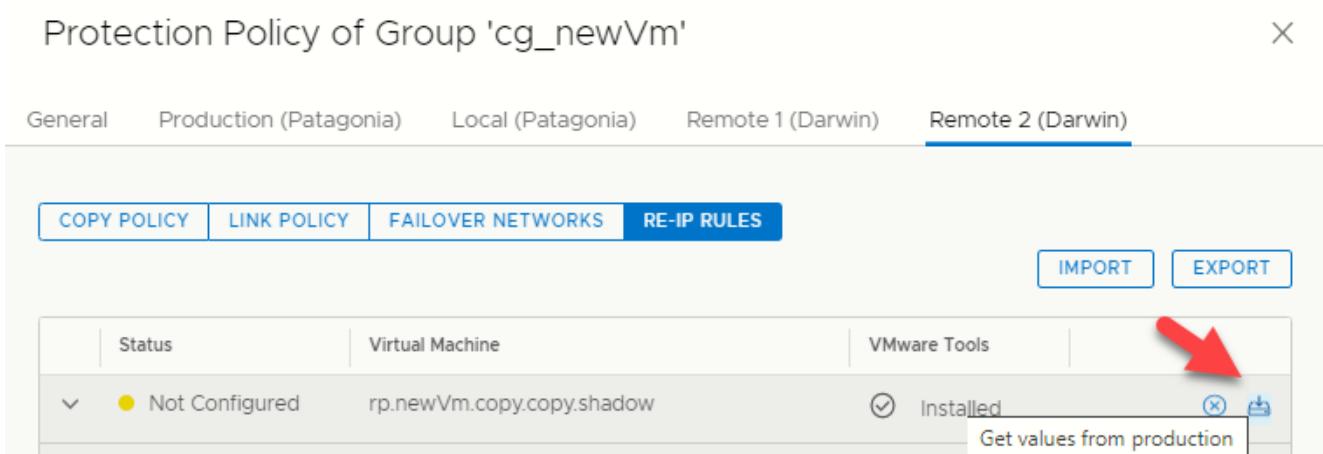
The new copy VM network configuration is used when testing a copy, failing over, or recovering production.

## Re-IP many copy VMs

Simultaneously update the network configuration of multiple VMs at a copy.

### Steps

1. In the RecoverPoint for Virtual Machines plugin for vSphere Client, select **Protection > Consistency Groups**.
2. Select a consistency group, and click **PROTECTION POLICY**.  
The group **Protection Policy** dialog is displayed.
3. Select the tab of the **Production** or a **Copy** and click the **RE-IP RULES** tab.
4. To retrieve the network configuration of all copy VMs at all vRPA clusters in the system, click **Get values from production**.



5. To facilitate populating JSON with the production values, click **UPDATE POLICY**.
6. Repeat steps 1-3.
7. To save the current network configuration of all virtual machines at the selected copy to a local JSON file, click **Export**.
8. Open the JSON file, and modify the network configuration of relevant virtual machines according to the [Copy VM network configuration guidelines](#).
9. To apply the new network configuration, click **Import** and select the modified JSON file .
10. Click **UPDATE POLICY**.

## Results

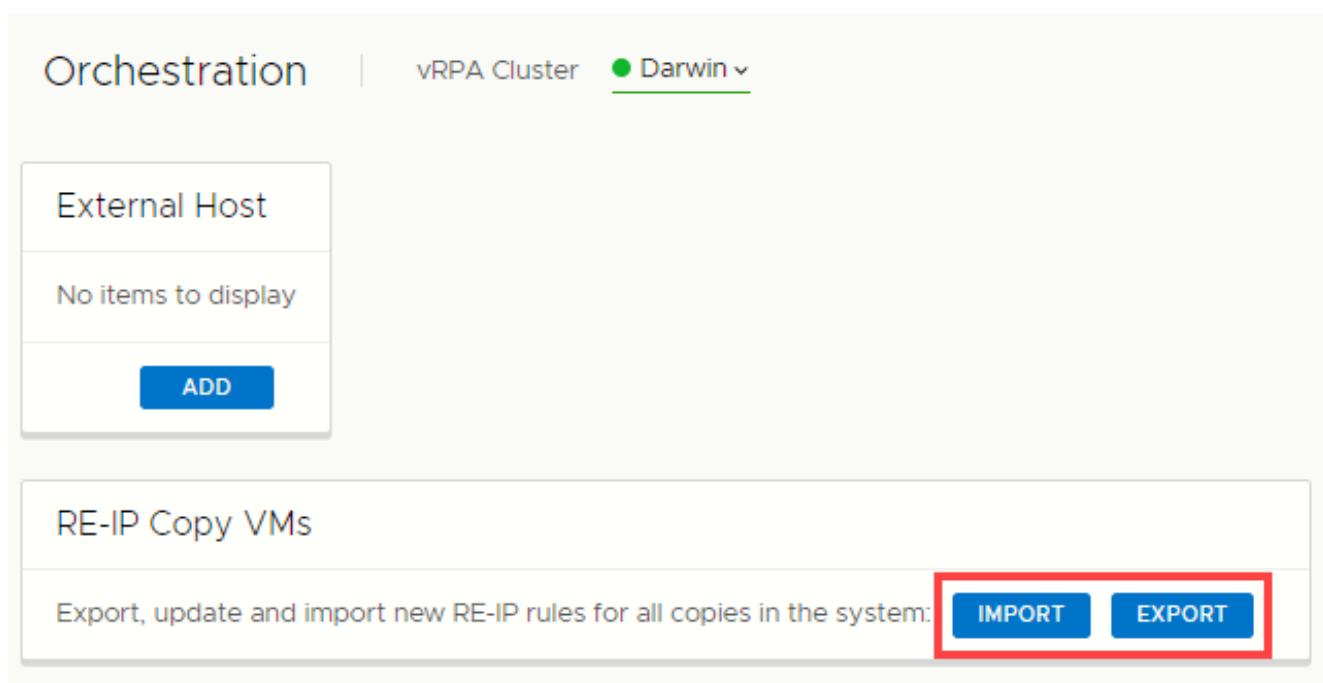
The new network configuration is used when testing a copy, failing over, or recovering production.

## Re-IP all copy VMs in the system

Simultaneously update the network configuration of all VMs of all copies in the system.

### Steps

1. In the RecoverPoint for Virtual Machines plugin for vSphere Client, select **System > Orchestration** and use the buttons in the **RE-IP Copy VMs** section to update your copy network settings.



The screenshot shows the 'Orchestration' interface in the vSphere Client. At the top, it displays 'Orchestration' and 'vRPA Cluster' with a dropdown set to 'Darwin'. Below this, there are two main sections: 'External Host' and 'RE-IP Copy VMs'. The 'External Host' section shows 'External Host' and 'No items to display' with an 'ADD' button. The 'RE-IP Copy VMs' section has a sub-header 'RE-IP Copy VMs' and a sub-instruction 'Export, update and import new RE-IP rules for all copies in the system:'. It features two buttons: 'IMPORT' and 'EXPORT', which are both highlighted with a red rectangular box.

2. To save the current network configuration to a local JSON file, click **Export**.
3. Open the JSON file, and modify the network configuration of relevant copy VMs according to the [Copy VM network configuration guidelines](#).
4. To apply the new network configuration to the system, click **Import** and select the modified JSON file.

## Results

The new network configuration is used when testing a copy, failing over, or recovering production.

# Failover networks

Automatically associate the VM network adapters (vNICs) of copy VMs with specific port groups upon failover, or during copy testing.

## About this task

Failover networks can be configured during or after VM protection. Configured failover networks are made available for selection during testing and failover.

## Steps

1. In the RecoverPoint for VMs vSphere Client plugin, click **Protection** > **Consistency Groups**, select a group, and click **PROTECTION POLICY**.  
The group **Protection Policy** dialog is displayed.
2. Select a copy and click **FAILOVER NETWORKS**.

Protection Policy of Group 'cg\_Win' X

General Production (NASA\_Site1) **Remote 1 (NASA\_Site2)**

**COPY POLICY** **LINK POLICY** **FAILOVER NETWORKS** **RE-IP RULES**

Search

Protected VM	Copy VM
> KATE_VM_1309	rp.KATE_VM_1309.copy.1.shadow
▼ Win	rp.Win.copy.shadow

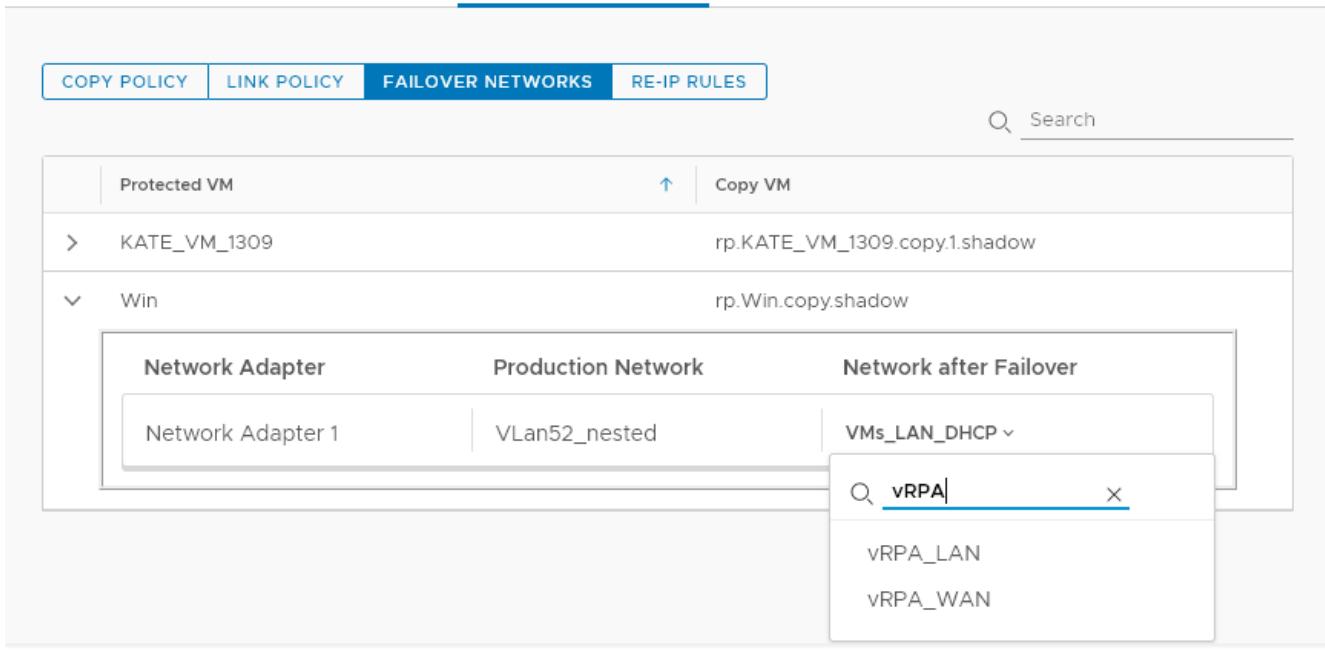
**Network Adapter** **Production Network** **Network after Failover**

Network Adapter	Production Network	Network after Failover
Network Adapter 1	VLAN52_nested	VMs_LAN_DHCP ▾

**vRPA** X

vrPA\_LAN  
vrPA\_WAN

**CANCEL** **UPDATE POLICY**



3. Expand a VM to display its network adapters, and for each adapter, select the network to be used after failover.  
Use the search filter to quickly identify the required network.
4. Click **UPDATE POLICY**.

## Results

The failover networks are configured.

## Next steps

Select **Preconfigured failover networks** when defining the **Testing Network** for copy testing, and when defining the **Target Network** before failing over.

# Recovering VMs

Periodically test copy images. In a disaster, fail over to a copy, or recover production to an earlier point-in-time.

Before recovering VMs, see the *Scale and Performance Guide* and the *Machines Release Notes* for information on how to scale your environment, and the limitations of this solution.

## Topics:

- [Test a copy](#)
- [Failover to a copy](#)
- [Recover production from a copy](#)

## Test a copy

Test a copy of a consistency group or a group set.

### Prerequisites

You may want to add journal volumes to a copy journal to ensure that you have ample space for copy testing. For detailed instructions on how to add journal volumes to a copy, see [Managing group protection policies](#).

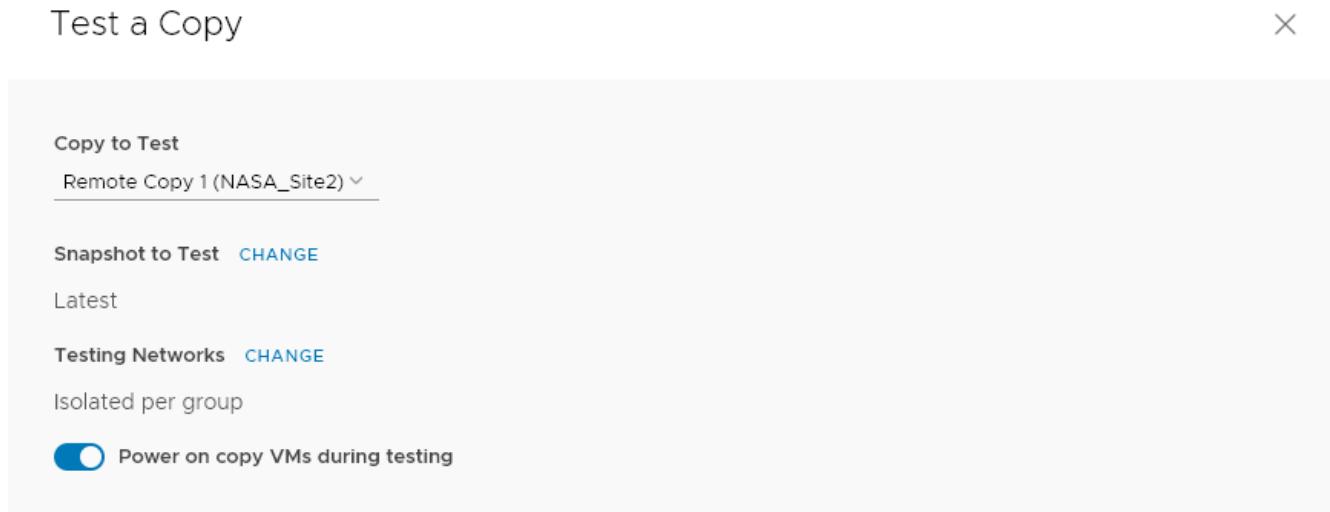
### About this task

From time to time, and especially before you begin recovery, test your copy snapshots to ensure they are appropriate for recovery. Then, [Create a bookmark](#) so that appropriate snapshots are quickly identifiable during recovery.

### Steps

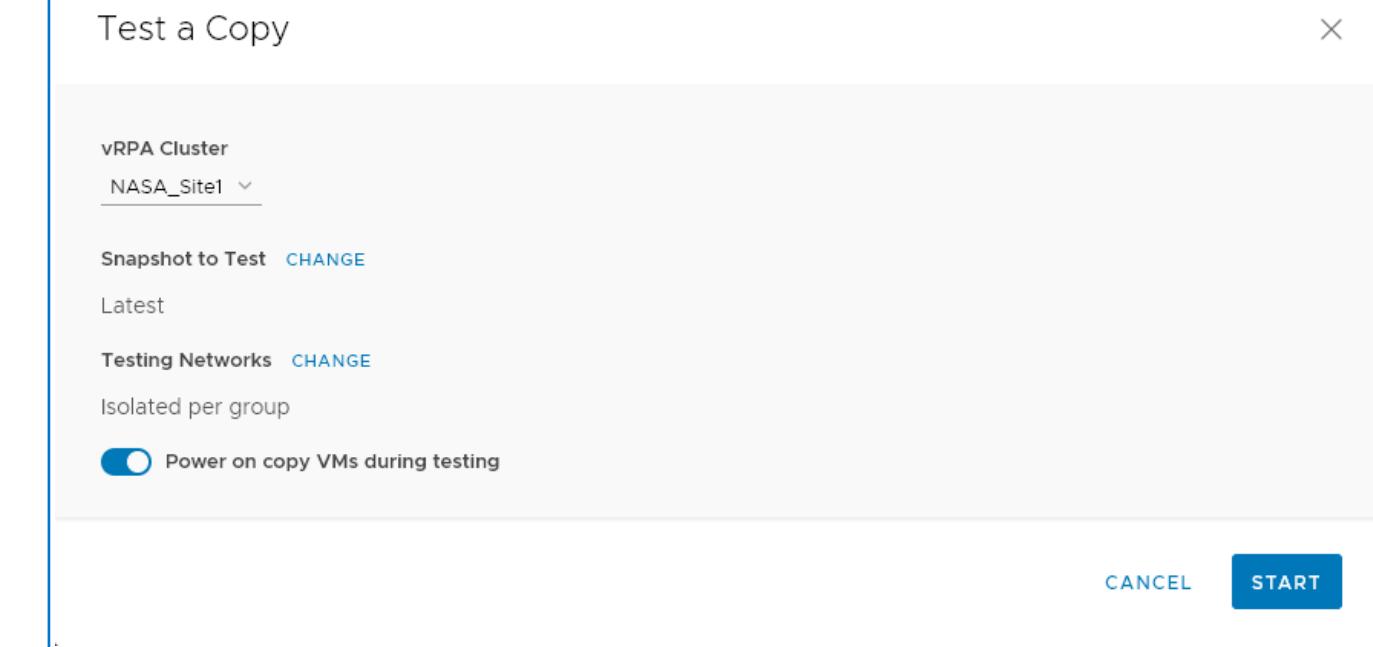
1. Depending on whether you want to test a copy of a consistency group or a group set, select **Protection > Consistency Groups** or **Protection > Group Sets**.
2. Select the group or group set whose copy you want to test, and click **TEST A COPY**.
3. In the **Test a Copy** dialog:

- If you selected a consistency group, select the **Copy to Test**. The vRPA cluster of the copy is displayed, for quick identification.



- If you selected a group set, select the **vRPA Cluster** containing a copy that you want to test. If there are multiple copies at the specified vRPA cluster, RecoverPoint for VMs automatically selects the copy to test. Consistency groups in the group set that do not have a copy at the specified vRPA cluster are excluded from the activity.

**NOTE:** To finish this activity, go to the **Recovery Activities** screen, **Consistency Groups** tab.

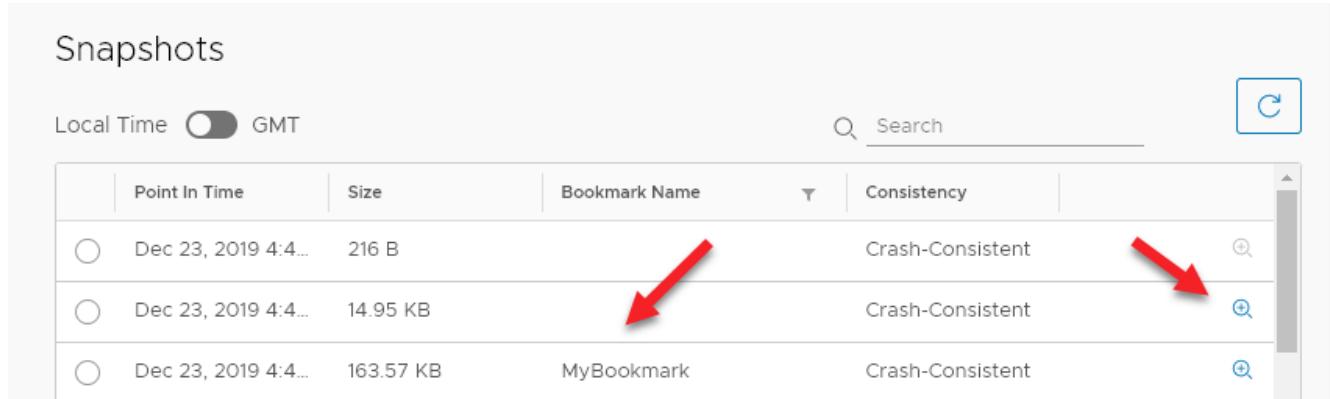


4. Select the copy **Snapshot to Test**.

Default is **latest**. When selecting a copy snapshot:

- You may want to start with the **Latest** (default) snapshot that is known to be valid.
- You can search for snapshots by name using the search field.

- You can select snapshots by **Bookmark** or **Point in Time**.



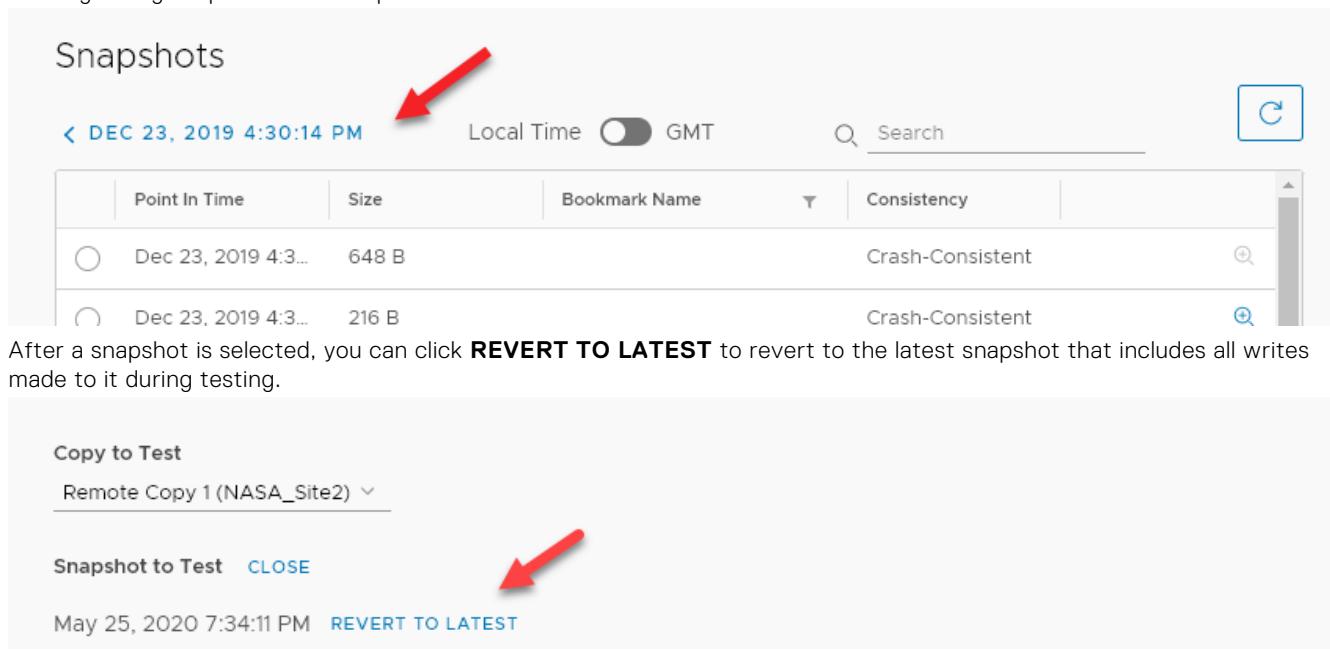
Snapshots

Local Time  GMT

Search

Point In Time	Size	Bookmark Name	Consistency
Dec 23, 2019 4:4...	216 B		Crash-Consistent
Dec 23, 2019 4:4...	14.95 KB		Crash-Consistent
Dec 23, 2019 4:4...	163.57 KB	MyBookmark	Crash-Consistent

- Use the **zoom in** icon to display all snapshots between the snapshot whose **zoom in** icon you clicked, and the previous snapshot. You can zoom into a snapshot up to four times. After zooming into a snapshot, you can zoom out by clicking the originating snapshot timestamp.



Snapshots

Local Time  GMT

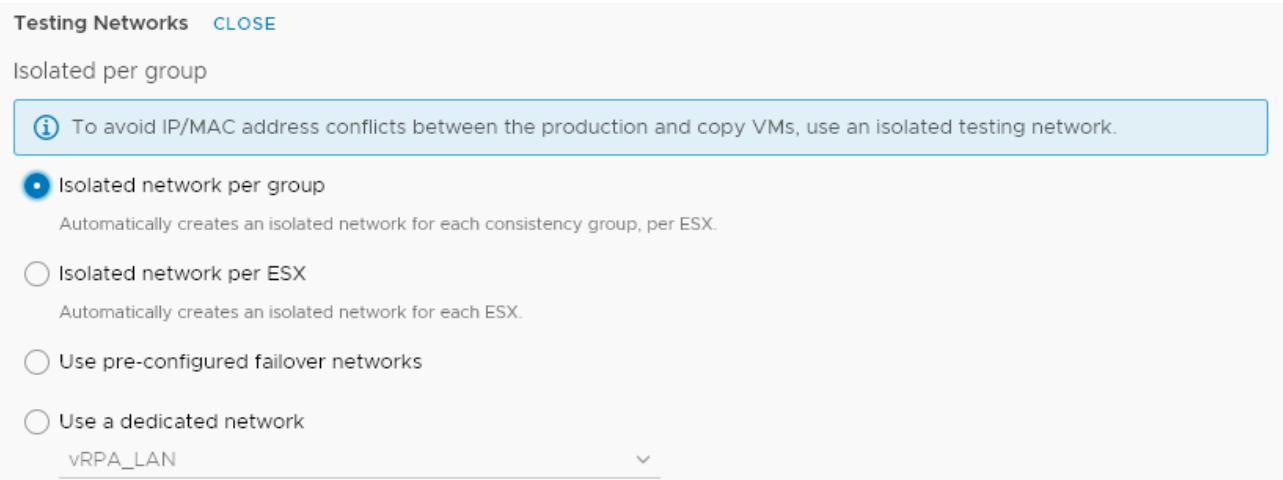
Search

Point In Time	Size	Bookmark Name	Consistency
Dec 23, 2019 4:3...	648 B		Crash-Consistent
Dec 23, 2019 4:3...	216 B		Crash-Consistent

**REVERT TO LATEST**

## 5. (Optional) Select the copy **Testing Networks**.

To avoid IP conflicts between the production and copy VMs, best practice is to use a dedicated testing network. Therefore, by default, RecoverPoint for VMs autoprovisions an isolated network for all VMs in the group or group set .



Testing Networks

Isolated per group

**ⓘ To avoid IP/MAC address conflicts between the production and copy VMs, use an isolated testing network.**

Isolated network per group  
Automatically creates an isolated network for each consistency group, per ESX.

Isolated network per ESX  
Automatically creates an isolated network for each ESX.

Use pre-configured failover networks

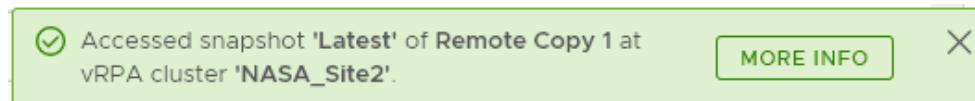
Use a dedicated network  
vRPA\_LAN

You can also:

- Create an isolated network for each ESX.
  - Use preconfigured [Failover networks](#).
  - Use a dedicated network.
6. Specify whether you want RecoverPoint for VMs to **Power on copy VMs during testing**. Default is **enabled**.
7. Click **START** to access the copy snapshot.

## Results

The specified snapshot is accessed, and a success message is displayed. You can now start testing the copy image.



**NOTE:** If you selected to test a copy of a group set, the success message identifies the copy that the system selected, at the vRPA cluster that you selected.

## Next steps

Click the **MORE INFO** link in the success message to go to the **Recovery Activities** screen, and display the activity progress and options. In the **Recovery Activities** screen:

- If you tested a copy of a consistency group:

Recovery Activity	Copy	Snapshot	Activity Start	Activity Status	Progress
Test Copy - cg_KATE_VM_13...	Local Copy (NASA_Site1)	Nov 23, 2020 11:55:47 AM	Nov 23, 2020 11:55:48 AM	Ready for next action	<div style="width: 100%;">100%</div>
<div style="display: flex; justify-content: space-between;"> <span>Image Access Log Capacity</span> <span>4%</span> </div> <div style="display: flex; justify-content: space-between;"> <span>UNDO WRITES</span> <span>ENABLE DIRECT ACCESS</span> </div> <div style="display: flex; justify-content: space-between;"> <span>Journal Capacity</span> <span>3%</span> </div>					

Items per page: 20

The **Consistency Group Recovery Activities** screen is displayed. The **Activity Status** and **Progress** columns indicate the progress of image access. After access is enabled to the copy snapshot, the **Activity Status** column displays **Ready for next action**, and you can:

**NOTE:** The **Image Access Log Capacity** progress bar indicates how long you can access the copy image before the image access log is full and all writes to the copy fail. If you need more time for testing, you can undo writes at the copy, enable direct access to the copy, or add journal volumes as described in [Managing group protection policies](#).

- Click **UNDO WRITES** to undo all writes that were made to the copy snapshot while write access was enabled, without disabling access to the copy volumes.
- Click **ENABLE DIRECT ACCESS** to write directly to the copy storage. Any changes that are made to the copy storage while directly accessing the copy cannot be automatically undone, because when a snapshot is directly accessed, the journal at the copy is deleted. However, direct access does not impose a limit to the amount of data that you can write to the copy storage volumes.

**CAUTION:** When direct access is enabled, replication stops to the copy, and a short initialization is required across all group volumes when direct access is disabled.

- Click **ACTIONS > Start new test** to select another snapshot to test, or to redefine the testing network.
- Click **ACTIONS > Stop activity** to roll back all writes that were made to the copy snapshot while write access was enabled to the snapshot volumes, and disable write access to the snapshot volumes.
- Click **ACTIONS > Promote image: Failover** to Failover to the copy image that you tested in step 8 without requiring to roll back the writes that were made to the copy snapshot while write access to the copy volumes was enabled.
- Click **ACTIONS > Promote image: Recover Production** to recover production from the copy image that you tested in step 8 without requiring to roll back the writes that were made to the copy snapshot while write access to the copy volumes was enabled.

- If you tested a copy of a group set:

Recovery Activities

Consistency Groups Groups Sets

Search

Recovery Activity	vRPA Cluster	Consistency Groups	Activity Start	Activity Status	Progress
Test Copy - group-set	NASA_Site2	2/2	May 25, 2020 6:21:50 PM	Ready for next action	100% <b>ACTIONS</b>
<b>Summary:</b> <b>Detailed Status</b> <b>OPEN</b> Excluded Groups: 0/2 Testing Network: Isolated per group Preparing snapshot...: 0/2 User Prompts: None Powering on VMs...: 0/2 Ready for next action: 2/2					

Items per page: 20 1 Recovery activity

- Click **OPEN** to display a **Detailed Status** for each group in the group set. The **Detailed Status** screen is displayed.

**i** **NOTE:** Groups in the group set without a copy at the specified vRPA cluster are excluded from the activity.

### Detailed Status of 'group-set'

Search

Consistency Groups	Copy	Snapshot	Status	Progress
cg_Win_286	Local Copy	May 25, 2020 6:17:0...	Ready for next action	100%
cg_Win	Remote Copy	May 25, 2020 6:17:0...	Ready for next action	100%

Items per page: 10 2 Detailed Statuses

CLOSE

- Click **ACTIONS** > **Stop activity** to roll back all writes that were made to the copy snapshot while access was enabled to the copy volumes, and disable access to the copy volumes.

**i** **NOTE:** After finding an appropriate snapshot, [Create a bookmark](#) to label the snapshot so it is quickly identifiable for recovery.

## Failover to a copy

Failover to a copy of a consistency group or a group set, and (optionally) failback to the production. You can failover (and failback) consistency groups or group sets.

### About this task

Failover consists of two stages:

- Testing the copy image
- Failover

Failback consists of the same stages.

Before failover, you have an opportunity to test your copy snapshots to ensure they are ready for failover.

In environments containing multiple RecoverPoint for VMs systems, to lessen the load on back-end storage arrays, best practice is to failover the consistency groups of up to seven systems concurrently.

## Steps

1. Depending on whether you want to failover a group or a group set, select **Protection > Consistency Groups** or **Protection > Group Sets**.
2. Select the group or group set that you want to failover, and click **FAILOVER**.
3. In the **Test a Copy for Failover** dialog:
  - If you selected a consistency group, select the copy and vRPA cluster that you want to failover to in the **Failover to Copy** field.



- If you selected a group set, select the **vRPA Cluster** containing a copy that you want to failover to. If there are multiple copies at the specified vRPA cluster, automatically selects the copy. Consistency groups in the group set that does not have a copy at the specified vRPA cluster are excluded from the activity.



4. Select the snapshot that you want to failover to by clicking **CHANGE** next to **Failover to Snapshot**. Default is the **Latest** snapshot.

When selecting a copy snapshot:

  - You may want to start with the **Latest** (default) snapshot that is known to be valid.
  - You can search for snapshots by name using the search field.

- You can select snapshots by **Bookmark** or **Point in Time**.

Point In Time	Size	Bookmark Name	Consistency
Dec 23, 2019 4:4...	216 B		Crash-Consistent
Dec 23, 2019 4:4...	14.95 KB		Crash-Consistent
Dec 23, 2019 4:4...	163.57 KB	MyBookmark	Crash-Consistent

- Use the **Zoom in** icon to display all snapshots between the snapshot whose **Zoom in** icon you clicked, and the previous snapshot. You can zoom into a snapshot up to four times. After, zooming into a snapshot you can zoom out by clicking the originating snapshot timestamp.

Point In Time	Size	Bookmark Name	Consistency
Dec 23, 2019 4:3...	648 B		Crash-Consistent
Dec 23, 2019 4:3...	216 B		Crash-Consistent

May 25, 2020 7:34:11 PM [REVERT TO LATEST](#)

## 5. (Optional) Select the copy **Testing Networks**.

To avoid IP conflicts between the production and copy VMs, best practice is to use a dedicated testing network. By default, autoprovisions an isolated network for all VMs in the group or group set .

Isolated network per group  
Automatically creates an isolated network for each consistency group, per ESX.

Isolated network per ESX  
Automatically creates an isolated network for each ESX.

Use pre-configured failover networks

Use a dedicated network  
vRPA\_LAN

You can also:

- Create an isolated network for each ESX.

- Use preconfigured **Failover networks**.
  - Use a dedicated network.
6. Click **START** to access the copy snapshot.
- The specified snapshot is accessed, and a success message is displayed.
- ✓ Accessed snapshot 'Latest' of Remote Copy 1 at VRPA cluster 'NASA\_Site2'.

MORE INFO X
- Click **MORE INFO** in the success message to go to the **Recovery Activities** screen.
- i **NOTE:** If you selected to test a copy of a group set, the success message identifies the copy that the system selected, at the vRPA cluster that you selected.
7. Test the copy image for failover:
- In the **Recovery Activities** screen, wait for the **Activity Status** to show **Ready for next action** and the **Progress** status bar, indicating the state of image access to reach 100%.
- Then:
- To select a consistency group for failover, ensure the **Consistency Groups** tab is selected.
- Recovery Activities

Consistency Groups Groups Sets

Q cg\_KATE\_VM\_1309 X

Recovery Activity	Copy	Snapshot	Activity Start	Activity Status	Progress	
▼ Failover - cg_KATE_VM_1309	Local Copy (NASA_Site1)	Nov 23, 2020 11:55:47 AM	Nov 23, 2020 5:24:50 PM	Ready for next action	<div style="width: 100%;">100%</div>	<span style="border: 1px solid #ccc; padding: 2px 10px; border-radius: 5px;">ACTIONS</span>
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <span style="color: blue;">■</span> Image Access Log Capacity 5% <span style="float: right;">UNDO WRITES ENABLE DIRECT ACCESS</span> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <span style="color: blue;">■</span> Testing Network: Isolated per group <span style="float: right;">Start transfer</span> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <span style="color: blue;">■</span> Failover Networks <input type="radio"/> Use current testing networks <span style="float: right;">User Prompts: None</span> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <span style="color: blue;">■</span> Use or edit pre-configured failover networks <span style="float: right;">Stop activity</span> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <span style="color: blue;">■</span> Start transfer <span style="float: right;">Failover</span> </div>						
Items per page: 20 ▾						
1 Recovery activity						
- i **NOTE:** By default, replication starts immediately after failover. In RecoverPoint for VMs 5.3.1 and later versions, disable **Start transfer** before failing over to pause replication after failover.
- Click **ACTIONS > Start new test** to select another snapshot to test, or to redefine the testing network.
  - Click **ACTIONS > Stop activity** to roll back all writes that were made to the copy snapshot while write access was enabled to the snapshot volumes, and disable write access to the snapshot volumes.
  - (Optional) Click **UNDO WRITES** to undo all writes that were made to the copy snapshot while write access was enabled, without disabling access to the copy volumes.
  - (Optional) Click **ENABLE DIRECT ACCESS** to write directly to the copy storage. Any changes that are made to the copy storage while directly accessing the copy cannot be automatically undone, because when a snapshot is directly accessed, the journal at the copy is deleted. On the other hand, direct access does not impose a limit to the amount of data that you can write to the copy storage volumes.
- ⚠ **CAUTION:** When direct access is enabled, replication stops to the copy, and a short initialization is required across all group volumes when direct access is disabled.
- In **Failover Networks**, you can use the default preconfigured failover networks, by keeping **Use or edit pre-configured failover networks** selected. You can also edit a preconfigured network, or choose to **Use current testing networks**.
- i **NOTE:** The **Image Access Log Capacity** progress bar indicates how long you can access the copy image before the image access log is full and all writes to the copy fail. If you need more time for testing, you can undo writes at the copy, enable direct access to the copy, or add journal volumes as described in [Managing group protection policies](#).

- To select a group set for failover, click the **Group Sets** tab.

Recovery Activities

Consistency Groups Groups Sets

Search

Recovery Activity	vRPA Cluster	Consistency Groups	Activity Start	Activity Status	Progress	ACTIONS
Failover - GS1	Site1	2/2	Jul 18, 2021 8:23:39 PM	Ready for next action	50%	<a href="#">Stop activity</a> <a href="#">Failover</a> 
<b>Summary:</b> Detailed Status <a href="#">OPEN</a> <b>Excluded Groups:</b> 0/2 Testing Network: Isolated per ESX <b>Preparing snapshot:</b> 0/2 <input checked="" type="button"/> Start transfer <b>User Prompts:</b> None <b>Powering on VMs:</b> 0/2 <b>Ready for next action:</b> 2/2						

Items per page: 10  1 Recovery activity

**NOTE:** By default, replication starts immediately after failover. In RecoverPoint for VMs 6.0.1, disable **Start transfer** before failing over to pause replication after failover.

- Click **OPEN** to display the **Detailed Status** of all consistency groups in the group set. After access is enabled to the copy snapshot, the **Status** column of all groups displays **Ready for next action**.

**NOTE:** Groups in the group set without a copy at the specified vRPA cluster are excluded from the activity.

### Detailed Status of 'group-set'

Search

Consistency Groups	Copy	Snapshot	Status	Progress
cg_Win_286	Local Copy	May 26, 2020 2:04:2...	Ready for next action	100%
cg_Win	Standalone	May 26, 2020 2:06:1...	Ready for next action	100%

Items per page: 10  2 Detailed Statuses

**CLOSE**

- Click **ACTIONS > Stop activity** to roll back all writes that were made to the copy snapshot while access was enabled to the copy volumes, and disable access to the copy volumes.

**NOTE:** After finding an appropriate snapshot, you may want to [Create a bookmark](#) to label the snapshot so it is identifiable during failover.

## 8. Failover to the copy.

Click **ACTIONS > Failover**.

### Results

- If the selected consistency group or group set has only one copy, failover starts.
  - The role of the **Production** becomes **Remote/Local Copy**.
  - The role of the **Remote/Local Copy** becomes **Production**.
  - The production VM and copy VM change roles, but their names do not change. Therefore, after failover, new production VMs will still be named `YourVMName.copy` and the new copy VMs are still named `YourVMName`.

- The production journal becomes the copy journal, and the copy journal becomes the production journal. You may want to add journal volumes as described in [Managing group protection policies](#).
- The marking information in the production journal is deleted, the copy journal is deleted, and the consistency group undergoes a full sweep.

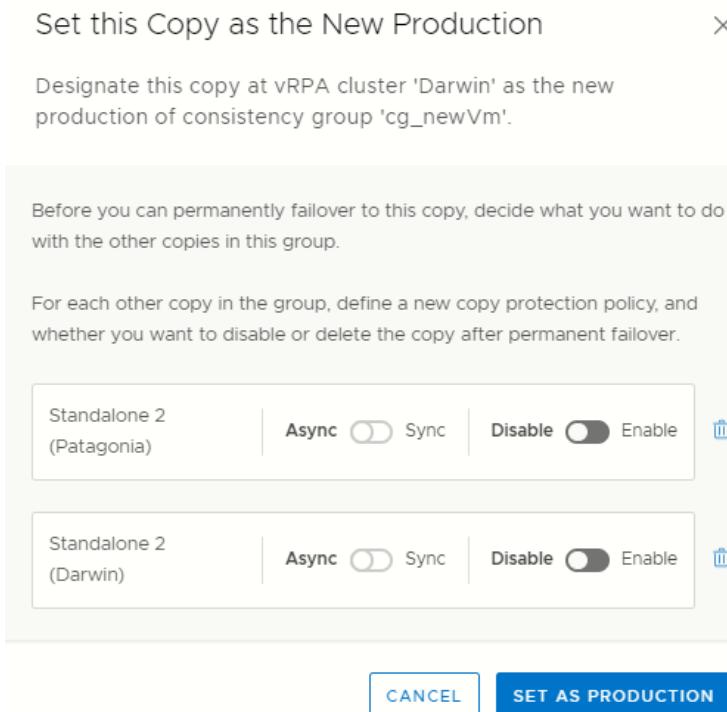
 **CAUTION: During the full sweep, data is not transferred synchronously.**

- If the consistency group or group set has copies other than the copy to which you are failing over (even if they are disabled or replication to them is paused), a temporary failover begins:
  - The role of the **Production** changes to **Temporary Production**.
  - The role of the **Remote/Local Copy** changes to **Temporary Remote/Local Copy**.
  - The roles of any other (unlinked) copies become **Standalone**.
  - Replication pauses for the other copies and the direction of replication between the production and the failed-over copy changes.

## Next steps

After temporary failover, if your consistency group or group set had more than one copy (even if they are disabled or replication to them is paused), in the **Recovery Activities** screen:

- **Failback to the original production.**
  - Select the recovery activity, click **ACTIONS > Test for failback** and run the above procedure beginning with step 3, substituting "failback" for "failover" throughout.
  - After failing back to the production, if you added volumes to the production journal after failover, to reset the production journal to its original size (by default, 3 GB) without triggering a full sweep click **Protection > Consistency Groups > PROTECTION POLICY**, select the **Production** copy of the group, and click **RESET SIZE** in the **Journal Volumes** section.
- **Set the copy as the new production.**
  - Select the recovery activity and click **ACTIONS > Set as production**. If there are stand-alone (unlinked) copies, the **Set this Copy as the New Production** dialog is displayed.
  - In the **Set this Copy as the New Production** dialog for consistency groups:



1. Configure each stand-alone copy for consistency groups (or all stand-alone copies for group sets). Standalone copies are not linked to the production, and you must decide how to handle them before failover. By default, RecoverPoint for VMs does not delete copy VMs but it does disable them. You can **Enable** any required stand-alone copies and select a replication mode (sync or async), or **Delete** them from the consistency group. Deleting a copy does not delete the VMs from storage.



**CAUTION:** Disabled copy VMs require a full sweep when they are reenabled.

2. Click **SET AS PRODUCTION** to permanently failover.
  - The role of the **Production** becomes **Remote/Local Copy**.
  - The role of the **Remote/Local Copy** becomes **Production**.
  - The stand-alone copies are handled as specified.
  - The production VM and copy VM change roles, but their names do not change. Therefore, after failover, new production VMs will still be named `YourVMName.copy` and the new copy VMs are still named `YourVMName`.
  - The production journal becomes the copy journal, and the copy journal becomes the production journal. The production journal does not contain the copy history, so it is by default, a smaller journal. Therefore, after failover, when the production becomes the copy, you may want to add journal volumes to the new copy journal to ensure that you have ample space for copy testing. For detailed instructions on how to add journal volumes to a copy journal, see [Managing group protection policies](#)
  - The marking information in the production journal is deleted, the journal of the copy to which you failed over is deleted, and the consistency group undergoes a full sweep.



**CAUTION:** During the full sweep, data is not transferred synchronously.

## Recover production from a copy

Production recovery corrects file or logical corruption by rolling the production back to a previous point-in-time. You can recover production of consistency groups or group sets.

### About this task

Before you begin recovery, you should test your copy snapshots to ensure they are ready for recovery.

Production recovery consists of two stages:

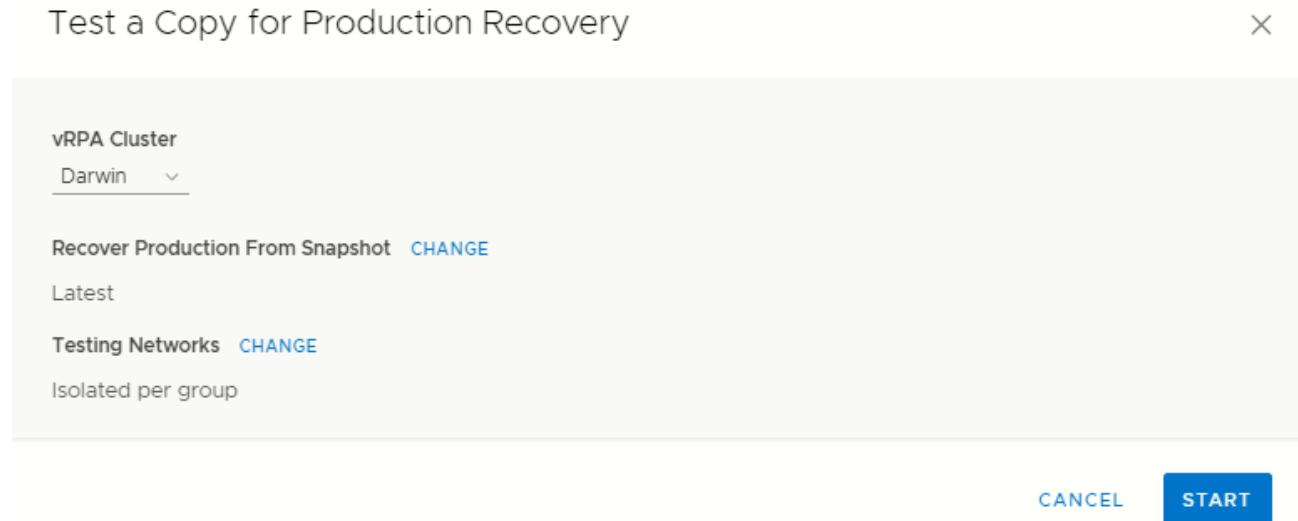
- Testing the copy image
- Recovering the production from the copy image

### Steps

1. Depending on whether you want to recover the production VMs of a group or a group set, select **Protection** > **Consistency Groups** or **Protection** > **Group Sets**.
2. Select the group or group set whose production VMs you want to recover and click **RECOVER PRODUCTION**.
3. In the **Test a Copy for Production Recovery** dialog:
  - If you selected a consistency group, select the copy and vRPA cluster from which you want to recover production in the **Recover Production From Copy** field.



- If you selected a group set, select the **vRPA Cluster** containing a copy from which you want to recover production. If there are multiple copies at the specified vRPA cluster, RecoverPoint for VMs automatically selects the copy. Consistency groups in the group set that do not have a copy at the specified vRPA cluster are excluded from the activity.



4. Select the snapshot from which you want to recover production by clicking **CHANGE** next to **Recover Production From Snapshot**. Default is the **Latest** snapshot.

When selecting a copy snapshot:

- You may want to start with the **Latest** (default) snapshot that is known to be valid.
- You can search for snapshots by name using the search field.
- You can select snapshots by **Bookmark** or **Point in Time**.

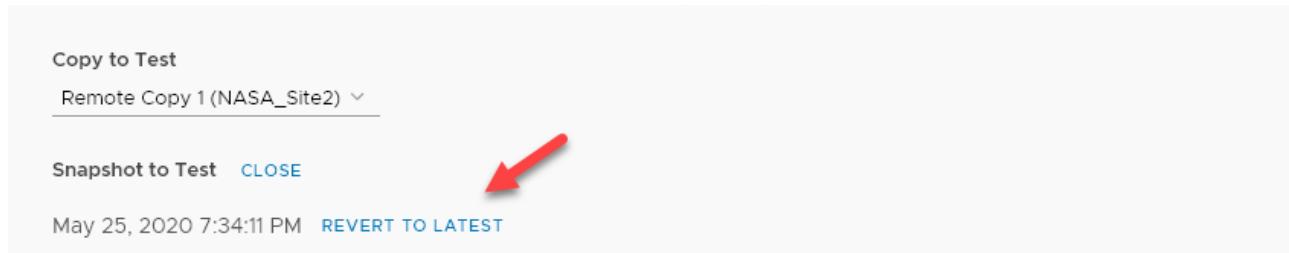
Point In Time	Size	Bookmark Name	Consistency
Dec 23, 2019 4:4...	216 B		Crash-Consistent
Dec 23, 2019 4:4...	14.95 KB		Crash-Consistent
Dec 23, 2019 4:4...	163.57 KB	MyBookmark	Crash-Consistent

- Use the **zoom in** icon to display all snapshots between the snapshot whose **zoom in** icon you clicked, and the snapshot before it. You can zoom into a snapshot up to four times. After zooming into a snapshot, you can zoom out by clicking the originating snapshot timestamp.

The screenshot shows the 'Snapshots' list view with a timestamp 'DEC 23, 2019 4:30:14 PM' highlighted by a red arrow. The 'Local Time' toggle is set to Local Time. The table columns are Point In Time, Size, Bookmark Name, and Consistency. The 'Point In Time' column is sorted.

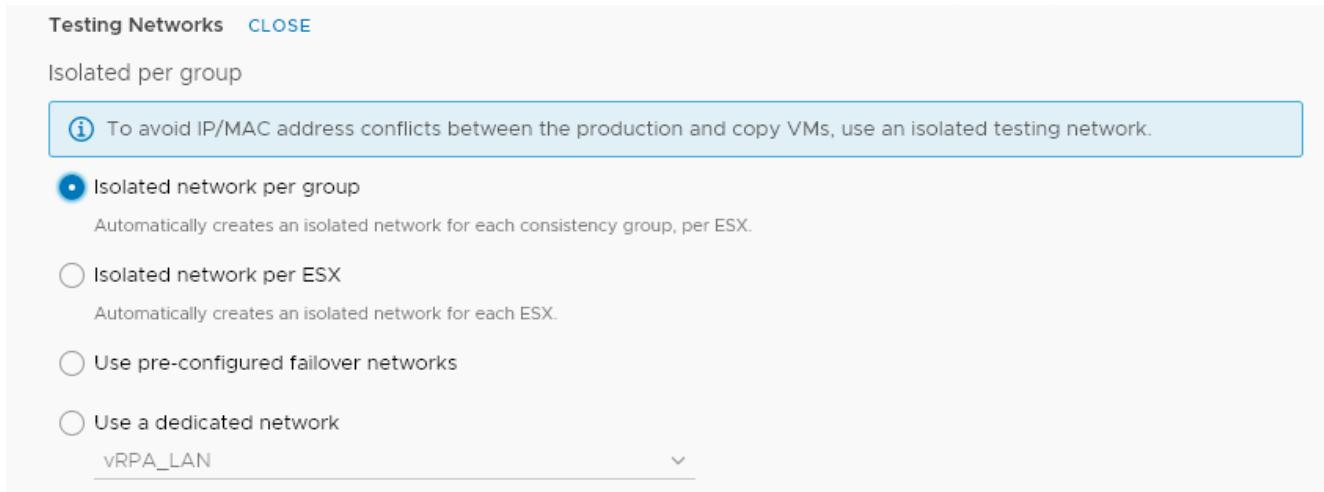
Point In Time	Size	Bookmark Name	Consistency
Dec 23, 2019 4:3...	648 B		Crash-Consistent
Dec 23, 2019 4:3...	216 B		Crash-Consistent

- After a snapshot is selected, you can click **REVERT TO LATEST** to revert to the latest snapshot that includes all writes made to it during testing.



5. (Optional) Select the copy **Testing Networks**.

To avoid IP conflicts between the production and copy VMs, best practice is to use a dedicated testing network. Therefore, by default, RecoverPoint for VMs autoprovisions an isolated network for all VMs in the group or group set .

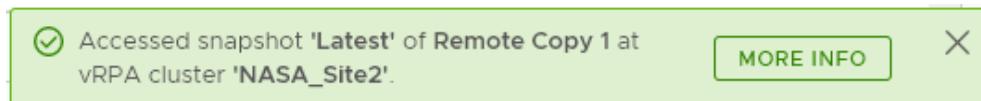


You can also:

- Create an isolated network for each ESX.
- Use preconfigured [Failover networks](#).
- Use a dedicated network.

6. Click **START** to access the copy snapshot.

The specified snapshot is accessed, and a success message is displayed.



Click **MORE INFO** in the success message to go to the **Recovery Activities** screen.

**(i) NOTE:** If you selected to test a copy of a group set, the success message identifies the copy that the system selected, at the vRPA cluster that you selected.

7. Test the copy image for production recovery:

In the **Recovery Activities** screen, wait for the **Activity Status** to show **Ready for next action** and the **Progress** status bar, indicating the state of image access to reach 100%.

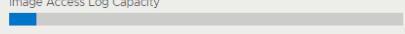
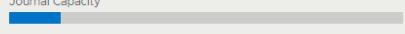
Then:

- To select a consistency group for production recovery, ensure the **Consistency Groups** tab is selected.

Recovery Activities

Consistency Groups Groups Sets

Search

Recovery Activity	Copy	Snapshot	Activity Start	Activity Status	Progress	ACTIONS
Recover Production - cg_ne...	Remote Copy 1 (Darwin)	Jul 20, 2020 1:23:01 PM	Jul 20, 2020 1:23:24 PM	Ready for next action	100%	<a href="#">Start new test</a> <a href="#">Stop activity</a> <a href="#">Recover production</a>
Image Access Log Capacity  7% <b>Testing Network:</b> Isolated per group <b>User Prompts:</b> None						<a href="#">UNDO WRITES</a> <a href="#">ENABLE DIRECT ACCESS</a>
Journal Capacity  13%						<a href="#">UNDO WRITES</a> <a href="#">ENABLE DIRECT ACCESS</a>
Items per page: 20						1 Recovery activity

- Click **ACTIONS > Start new test** to select another snapshot to test, or to redefine the testing network.
- Click **ACTIONS > Stop activity** to roll back all writes that were made to the copy snapshot while write access was enabled to the snapshot volumes, and disable write access to the snapshot volumes.
- (Optional) Click **UNDO WRITES** to undo all writes that were made to the copy snapshot while write access was enabled, without disabling access to the copy volumes.
- (Optional) Click **ENABLE DIRECT ACCESS** to write directly to the copy storage. Any changes that are made to the copy storage while directly accessing the copy cannot be automatically undone, because when a snapshot is directly accessed, the journal at the copy is deleted. However, direct access does not impose a limit to the amount of data that you can write to the copy storage volumes.

 **CAUTION:** When direct access is enabled, replication stops to the copy, and a short initialization is required across all group volumes when direct access is disabled.

 **NOTE:** The **Image Access Log Capacity** progress bar indicates how long you can access the copy image before the image access log is full and all writes to the copy fail. If you need more time for testing, you can undo writes at the copy, enable direct access to the copy, or add journal volumes as described in [Managing group protection policies](#).

- To select a group set for production recovery, click the **Group Sets** tab.

Recovery Activities

Consistency Groups Groups Sets

Search

Recovery Activity	vRPA Cluster	Consistency Groups	Activity Start	Activity Status	Progress	ACTIONS
Recover Production - Annas group set	Darwin	1/1	Jul 20, 2020 1:36:45 PM	Ready for next action	100%	<a href="#">Stop activity</a> <a href="#">Recover production</a>
<b>Summary:</b> Excluded Groups: 0/1 Preparing snapshot: 0/1 Powering on VMs: 0/1 Ready for next action: 1/1						<a href="#">OPEN</a>
<b>Detailed Status</b> Testing Network: Isolated per group User Prompts: None						<a href="#">OPEN</a>
Items per page: 20						1 Recovery activity

- Click **OPEN** to display the **Detailed Status** of all consistency groups in the group set. After access is enabled to the copy snapshot, the **Status** column of all groups displays **Ready for next action**.

 **NOTE:** Groups in the group set without a copy at the specified vRPA cluster are excluded from the activity.

## Detailed Status of 'group-set'

X

Q2 Detailed Statuses

Consistency Groups	Copy	Snapshot	Status	Progress
cg_Win_286	Local Copy	May 26, 2020 2:04:2...	Ready for next action	<div style="width: 100%;">100%</div>
cg_Win	Standalone	May 26, 2020 2:06:1...	Ready for next action	<div style="width: 100%;">100%</div>
Items per page <span>10</span> ▾				2 Detailed Statuses

CLOSE

- Click **ACTIONS > Stop activity** to roll back all writes that were made to the copy snapshot while access was enabled to the copy volumes, and disable access to the copy volumes.
8. Recover production from the copy.
- Click **ACTIONS > Recover production**.

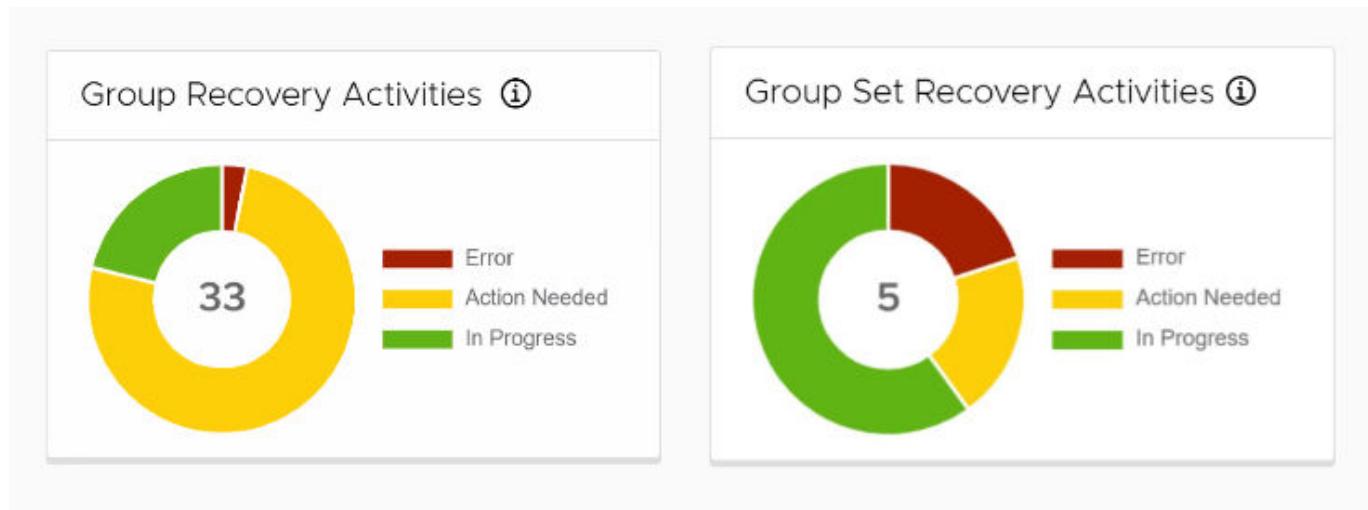
### Results

- Data transfer from the production to all copies is paused, and will resume only after production recovery is complete.
- Host access to the recovered production volumes and the recovering copy volumes is blocked.
- Recovered production volumes are overwritten. Any writes made to the copy during testing are transferred to the production, unless you clicked **UNDO WRITES** in step 7.
- The group undergoes a short initialization process to synchronize the new production data at the copy.

## Monitoring recovery activities

Monitor ongoing testing, failover, failback, and production recovery activities of consistency groups and group sets, using the **Dashboard**.

Use [RecoverPoint for VMs Dashboard](#) to monitor your recovery activities. The **Dashboard** provides an overview of all ongoing recovery activities in the system. Clicking the status of a recovery activity in a dashboard widget automatically displays the relevant system screen, displaying only the system components in the clicked status. To manage recovery activities, see [Managing recovery activities](#).



**Figure 8. Monitoring recovery activities**

# Managing RecoverPoint for VMs

This section describes how to use the **RecoverPoint for VMs vSphere plugin** to manage the components of the RecoverPoint for VMs , after initial system configuration.

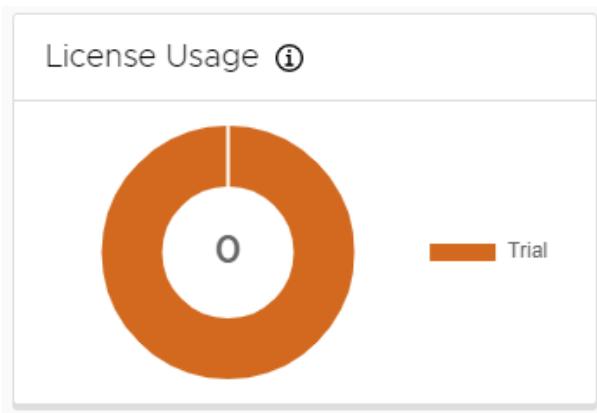
## Topics:

- Managing your RecoverPoint for VMs licenses
- Managing the plugin server
- Managing vRPA clusters
- Managing system component registration
- Manage Event Filters
- Managing protected VMs
- Managing consistency groups
- Managing group sets
- Managing recovery activities
- Configuring email alerts and reports

## Managing your RecoverPoint for VMs licenses

Manage RecoverPoint for VMs licenses.

To monitor your RecoverPoint for VMs license usage, use the RecoverPoint for VMs Dashboard. [RecoverPoint for VMs licensing](#) describes the licensing process.



To license RecoverPoint for VMs:

1. [Create your license files](#).
2. Add a license. For more information, see [Add license](#).

## Managing the plugin server

One RecoverPoint for VMs plugin server is supported per vCenter Server (or multiple linked vCenter Servers).

### Prerequisites

- Ensure you have a plugin server that is installed and registered with the vCenter Server that you are connected to. See the *Dell RecoverPoint for Virtual Machines Installation and Deployment Guide* for more information about installing plugin servers.

- Ensure you have consulted the *Dell RecoverPoint for Virtual Machines Product Guide* for a more detailed description of the plugin server, its architecture, installation, and functionality when vCenter Servers are linked.
- See [Managing linked vCenter Server registration](#).

## Steps

- In the **System > Administration** screen:
  1. The **vCenter Servers** tab displays all vCenter servers that are registered with the plugin server of the vCenter server that you are connected to.
  2. The **vRPA Clusters** tab displays all vRPA clusters that are hosted on all linked vCenter Servers that are registered with the plugin server of the vCenter Server that you are connected to.

## Changing the plugin server certificate

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

### About this task

Use this procedure, for instance, if you want to use a certificate that has been signed by your organization's internal certificate authority.

## 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" in the *RecoverPoint for VMs Installation and Deployment Guide*.

## 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 into 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 this procedure to change the plugin server certificate after the plugin server has already been configured using **Deployment Manager**.

### About this task

Use this procedure, for instance, if you want to use a certificate that has been signed by your organization's internal certificate authority.

## Steps

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

```
/etc/nginx/ssl/rpccenter.cert  
/etc/nginx/ssl/rpccenter.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 **rpccenter.cert** and the new key file to **rpccenter.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" in the *RecoverPoint for VMs Installation and Deployment Guide*.

8. Power on the plugin server VM.

9. Navigate to `https://RPCIP/ui`.

10. Click **Authorize** and enter the vCenter Server Credentials.

11. Navigate 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" in the *RecoverPoint for VMs Installation and Deployment Guide*.

## Results

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

## Next steps

 **NOTE:**

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

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

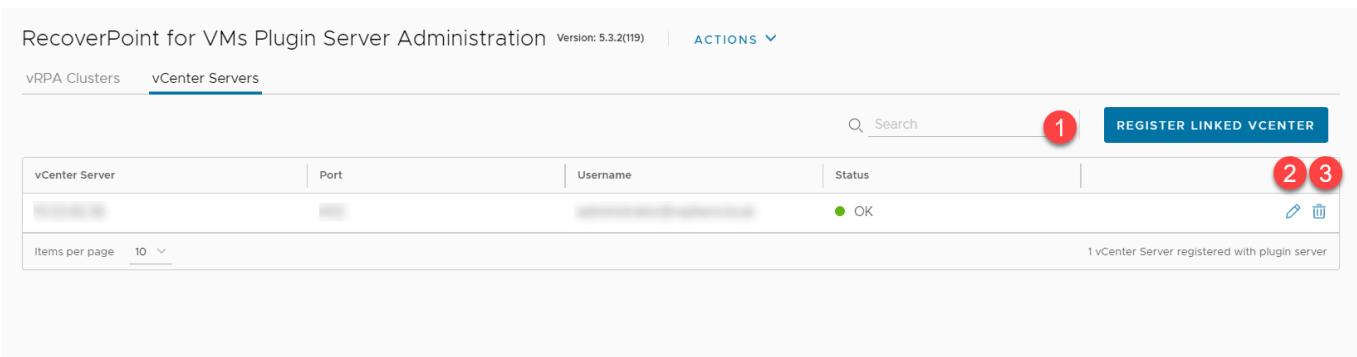
## Managing vCenter Server registration with plugin server

Manage the registration of linked vCenter Servers with the plugin server.

### About this task

Use the **System > Administration > vCenter Servers** tab to register linked vCenter Servers with the plugin server, update the registration of a vCenter Server with the plugin server, or unregister a vCenter Server from the plugin server.

 **NOTE:** The first vCenter Server is registered with the plugin server upon system deployment. See the *Dell RecoverPoint for Virtual Machines Installation and Deployment Guide* for more information.



**Figure 9. Plugin server vCenter Servers screen**

## Steps

1. To register a linked vCenter Server with the plugin server, click **Register Linked vCenter**.
2. To update the registration information of a vCenter Server that is already registered with the RecoverPoint for Virtual Machines plugin server (for instance, if the vCenter Server password expired, or if you changed the vCenter Server certificate or credentials), and the plugin server session is still active and you can still use the UI:
  - a. Click the **Edit** icon.
  - b. Reenter the vCenter Server credentials for the plugin server in the **System > Administration > vCenter Servers** tab, or for each vRPA cluster under **System > Administration > vRPA Clusters** tab.
  - c. Use the Sysmgmt CLI command **update\_vcenter\_server\_registration** to enter the new vCenter Server credentials for each relevant vRPA cluster. See the *Dell RecoverPoint for Virtual Machines CLI Reference Guide* for more details.
3. To unregister a vCenter Server from the plugin server, click the **Delete** icon.
4. Alternatively, if the plugin server session has expired and the UI is disconnected:
  - a. Use the Sysmgmt CLI command **update\_vcenter\_server\_registration** to enter the new vCenter Server credentials for each relevant vRPA cluster, see the *Dell RecoverPoint for Virtual Machines CLI Reference Guide* for more details.
  - b. Use the **Configure plugin server** option in the RecoverPoint for Virtual Machines Deployer for a vRPA cluster to update the plugin server with the new certificate, see the Configure plugin server procedure in the *Dell RecoverPoint for Virtual Machines Installation and Deployment Guide* for more details.

## Next steps

After unregistering a vCenter Server from the plugin server and after updating a plugin server with a new certificate, log out and log back into vSphere, or wait for the session to be reestablished.

## Managing linked vCenter Server registration

If you have vCenter Servers that are linked together using **vCenter Embedded Linked Mode**, you can see all vRPA clusters, protected VMs, copy VMs, and the plugin servers that reside on multiple vCenter Servers in a single vSphere **Inventory** view, and protect and recover VMs that reside on multiple vCenter Servers.

**(i) NOTE:** The first vCenter Server per site is registered during system deployment through the **RecoverPoint for VMs Deployer**. More linked and nonlinked vCenter Servers are registered through the **RecoverPoint for VMs vSphere plugin**.

RecoverPoint for VMs:

- Automatically registers the first vCenter Server when you install the first vRPA cluster.
- Supports up to 2 vCenter Servers that are linked together using **vCenter Embedded Linked Mode**.
- Uses one user authentication method for all linked vCenter Servers.

To register a linked system, after deploying the vRPA clusters:

1. Ensure you have used the **RecoverPoint for VMs Deployer > Install Plugin Server** button to install and register a plugin server with every vCenter Server hosting a protected VM, a copy VM, a plugin server, or a vRPA cluster. The plugin server installs the **vSphere HTML5 plugin** on every registered vCenter Server. When a vCenter Server is not registered with any plugin server, the **vSphere HTML5 plugin** interface is not available through the vSphere Client, and you cannot operate your RecoverPoint for VMs system. See the *RecoverPoint for VMs Installation and Deployment Guide* for more information about installing the plugin server.

2. Register all linked vCenter Servers and the plugin server through the **RecoverPoint for VMs vSphere plugin**:
  - Ensure you have registered all linked vCenter Servers with each vRPA cluster that is hosted on the linked vCenter Servers.
  - RecoverPoint for VMs automatically registers remote vRPA clusters when a local vRPA cluster is registered, but does not automatically register the vCenter Server on which the remote vRPA clusters are hosted.
  - When a vCenter Server is not registered with at least one vRPA cluster, the **RecoverPoint for VMs > Protect VMs...** menu is disabled, and you cannot protect VMs from the vSphere **Inventory**.
  - Click **System > Administration > vCenter Servers** and ensure you have registered all linked vCenter Servers with a plugin server.
  - When a vCenter Server is not registered with any plugin server, the **RecoverPoint for VMs > Protect VMs...** menu is disabled, and you cannot protect VMs from the vSphere **Inventory**.
3. Connect to a vCenter Server directly to:
  - Manage the plugin server of the linked vCenter Server.
  - Add a RecoverPoint for VMs license to the linked vCenter Server.
 License usage information is combined for all linked vCenter Servers.

To display all linked vCenter Servers in a linked RecoverPoint for VMs system, click the plugin server **INSTANCE** at the top of the RecoverPoint for VMs vSphere plugin.

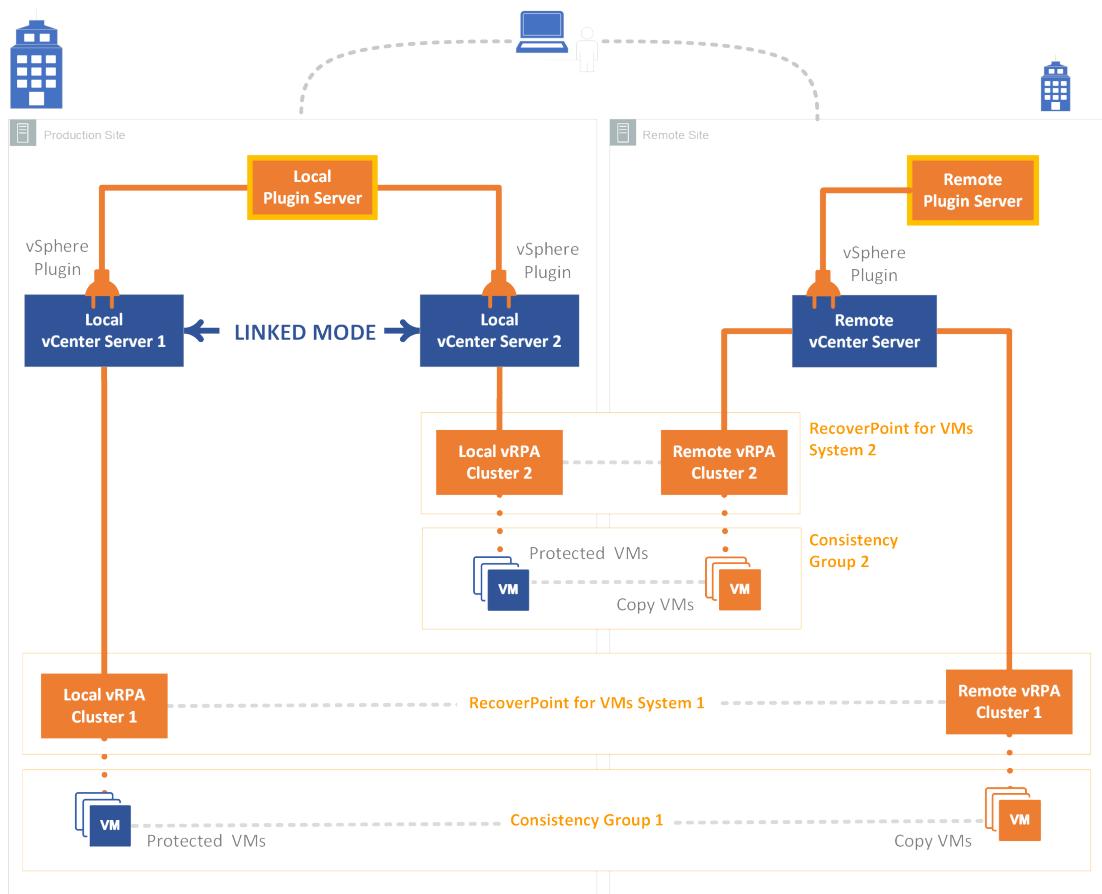
INSTANCE 10.10.10.10:123 ▾

Plugin Instance	Version	vCenter Server	
10.10.10.10:123	1.0.0	vc01.mydomain.com	Protected
10.10.10.11:123	1.0.0	vc02.mydomain.com	Active

More ▾

## Local linked vCenter Servers

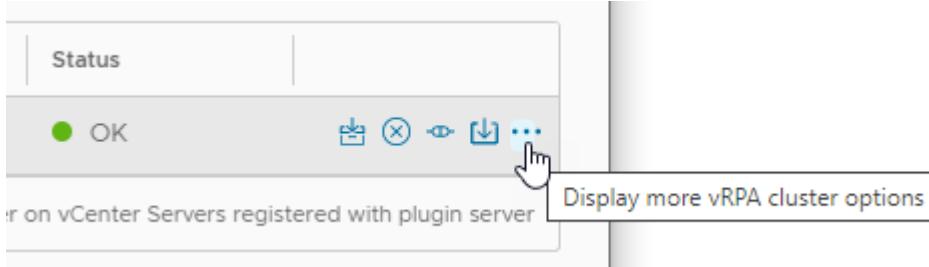
If you have local vCenter Servers that are linked together using **vCenter Embedded Linked Mode** and remote nonlinked vCenter Servers, you can connect to the local vCenter Servers to display all the production VMs and vRPA clusters at the production site in one vSphere Client inventory. When you connect to the remote vCenter Server, only the remote vRPA clusters and copy VMs are displayed in the vSphere Client inventory.



**Figure 10. Local linked vCenter example**

As illustrated in the [Local linked vCenter example](#), after installing your vRPA clusters:

1. Launch the **RecoverPoint for Virtual Machines Deployer** by clicking **System > Administration > vRPA Cluster** and clicking the **Display more vRPA cluster options** icon for a vRPA cluster that is registered to a linked vCenter:



2. Connect to **Local vCenter Server1** or **Local vCenter Server2** and register the vCenter with the **Local Plugin Server**.
3. Connect to the **Remote vCenter Server** and register it with the **Remote Plugin Server**.
4. In the **RecoverPoint for Virtual Machines vSphere plugin**:
  - When [Managing the plugin server](#), ensure the **System > Administration > Registered vCenter Servers** table displays linked **Local vCenter Server 2** is registered with the **Local Plugin Server**.
  - When [Managing vCenter Server registration with plugin server](#) of **Local vCenter Server1** and **Local vCenter Server2**:
    - Register **Local vCenter Server 1** with **Local vRPA Cluster 1**.
    - Register **Local vCenter Server 2** with **Local vRPA Cluster 2**.

- Click **INSTANCE** to display both the local and remote plugin servers and all linked and registered vCenter Servers at the production site.

INSTANCE 10.10.10.10:123 ▾

Plugin Instance	Version	vCenter Server	
10.10.10.10:123	1.0.0	vc01.mydomain.com	Protected
10.10.10.11:123	1.0.0	vc02.mydomain.com	Active

- When connected to the **Remote vCenter Server**:
  - When [Managing vCenter Server registration with plugin server](#), register **Remote vCenter Server** with **Remote vRPA Cluster 1** and **Remote vRPA Cluster 2**.
  - When [Managing the plugin server](#), register **Remote vCenter Server** with the **Remote Plugin Server**.
  - Click **INSTANCE** to display the remote plugin server and the remote vCenter Server.

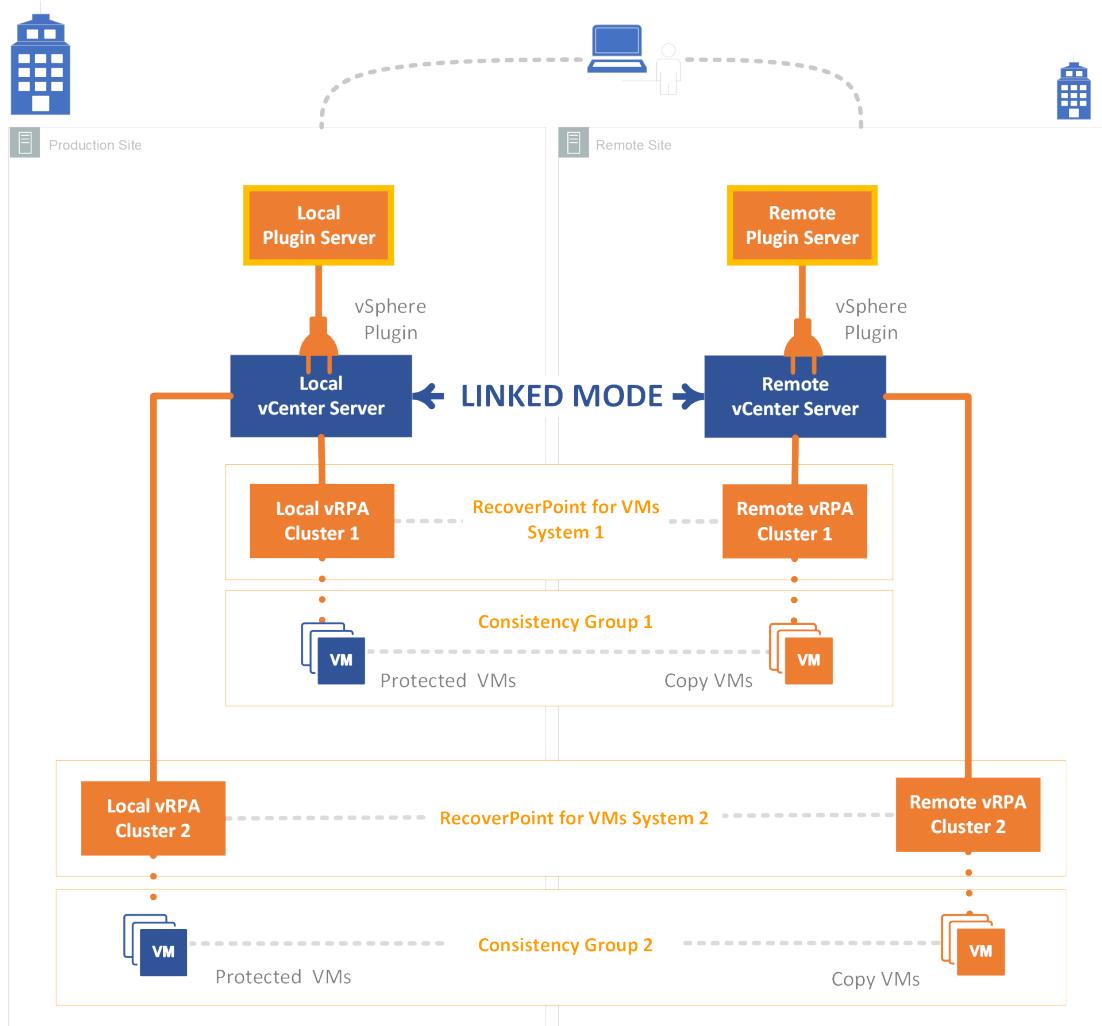
Plugin Instance	Version	vCenter Server
10.10.10.10:123	1.0.0	vc01.mydomain.com
		vc02.mydomain.com

**(i) NOTE:** In VMware Cloud Foundation (VCF) multitenancy environments (such as VxRail):

- It is best practice to register vRPA clusters with different vCenter Servers (see *Workload Domain* or *WLD* in VCF documentation).
- All VMs of all WLDs are displayed in the RecoverPoint for Virtual Machines plugin, no matter which user is logged in. For example, a user from a tenant on WLD 1 sees and can perform recovery on consistency groups from WLD 2. The RecoverPoint for Virtual Machines vSphere plugin does not currently support role-based authentication.
- You can see, manage, protect, and recover only the VMs of vRPA clusters that have been directly registered with a vCenter Server.

## Remote linked vCenter Servers

If you have vCenter Servers that are linked together using **vCenter Embedded Linked Mode**, you can display, manage, protect, and recover VMs hosted on multiple linked vCenter Servers, across remote sites.



**Figure 11. Remote linked vCenter example**

As illustrated in the [Remote linked vCenter example](#), after installing your vRPA clusters:

Register the vCenter Servers with the **Local Plugin Server** and **Remote Plugin Server** during system deployment using the **RecoverPoint for VMs Deployer**.

- Register the **Local vCenter Server** with the **Local Plugin Server**.
- Register the **Remote vCenter Server** with the **Remote Plugin Server**.

In the **vSphere plugin**, register linked vCenter (see [Managing vCenter Server registration with plugin server](#)).

- Register the **Local vCenter Server** with **Local vRPA Cluster 1** and **Local vRPA Cluster 2**.
- Register the **Remote vCenter Server** with **Remote vRPA Cluster 1** and **Remote vRPA Cluster 2**.

**NOTE:** To open the **Deployer** from the **vSphere plugin**, you can click **System > Administration > vRPA Clusters**, select a vRPA cluster, and click **Display more vRPA cluster options**. See the *RecoverPoint for VMs Installation and Deployment Guide* for more information.

When [Managing the plugin server](#), register the **Remote vCenter Server** with the **Remote Plugin Server**.

After registering your vCenter Servers with the plugin server and the vRPA clusters, you can see and protect VMs of both **System 1** and **System 2** from either vCenter Server.

Click **INSTANCE** to display both plugin server instances and both vCenter Servers are displayed when you are connected to the **RecoverPoint for VMs vSphere plugin** of either vCenter Server.

INSTANCE 10.10.10.10:123 ▾

Plugin Instance	Version	vCenter Server	
10.10.10.10:123	1.0.0	vc01.mydomain.com	Rotated
10.10.10.11:123	1.0.0	vc02.mydomain.com	Active

## Displaying the plugin server info

To display the plugin server, click the plugin server **INSTANCE** at the top of the **vSphere plugin**.

### Steps

- When vCenter Servers are linked, all [Managing linked vCenter Server registration](#) that have been registered with the plugin server are displayed. All plugin servers in the linked system are also displayed.

INSTANCE 10.10.10.10:123 ▾

Plugin Instance	Version	vCenter Server	
10.10.10.10:123	1.0.0	vc01.mydomain.com	Rotated
10.10.10.11:123	1.0.0	vc02.mydomain.com	Active

## Collecting plugin server logs

Collect plugin server logs for support purposes.

### About this task

This procedure collects logs from all vRPAs on all vCenter Servers that are registered with (or linked to one that is registered with) the plugin server, see [Collecting logs from vRPA clusters](#) to collect logs from specific vRPA clusters.

### Steps

- Click **System > Administration**

The **RecoverPoint for VMs Plugin Server Administration** screen is displayed.

RecoverPoint for VMs Plugin Server Administration Version: 5.3.2(119) | **ACTIONS** ▾

vRPA Clusters vCenter Servers

vRPA Cluster	Management IP Address	RecoverPoint for VMs Version	Remote vRF
Site1	██████████	5.3.SP2(m.240)	Site2

Items per page 20 ▾

Upgrading plugin server  
Collect plugin server logs   
Clear excluded vRPA clusters

OK    

1 vRPA cluster on vCenter Servers registered with plugin server

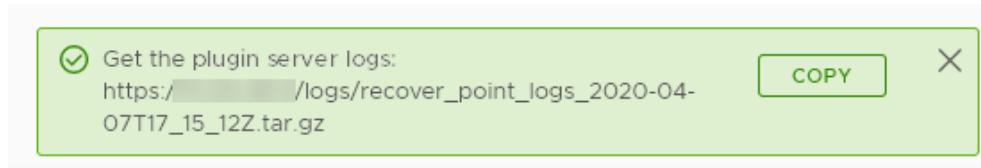
- Click **Actions > Collect plugin server logs**.

The collection of plugin server logs begins, and a status message is displayed.



## Results

When the collection process is complete, a success message is displayed with the location of the plugin server logs.



## Next steps

Click **Copy**, open a browser window, and paste the copied URL into the browser address bar to retrieve the files.

# Upgrading 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 the upgrade is complete.

**NOTE:** You can use the upgrade packages to upgrade services related to RP only, and not the SLES OS-related packages. If you want the plugin server with both RP and SLES packages, you should remove the older plugin server first. After that, download and deploy the latest plugin server OVA file, and then configure the plugin again.

## Steps

1. Click **System > Administration**.  
The **RecoverPoint for VMs Plugin Server Administration** screen is displayed.

RecoverPoint for VMs Plugin Server Administration			
vRPA Clusters		vCenter Servers	
Site1	Management IP Address	RecoverPoint for VMs Version	Remote vRP
5.3.SP2(m.240)	Site2	OK	

2. Click **Actions > Upgrade plugin server**.
3. Select the plugin server upgrade file that you downloaded from [Dell Support](#), and click **OK**.

## Results

During upgrade the RecoverPoint for VMs HTML5 plugin cannot be operated.

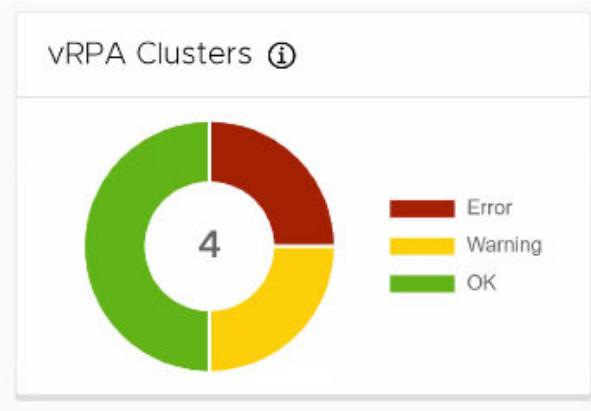
## Next steps

Wait for the upgrade to complete operating your RecoverPoint for VMs system.

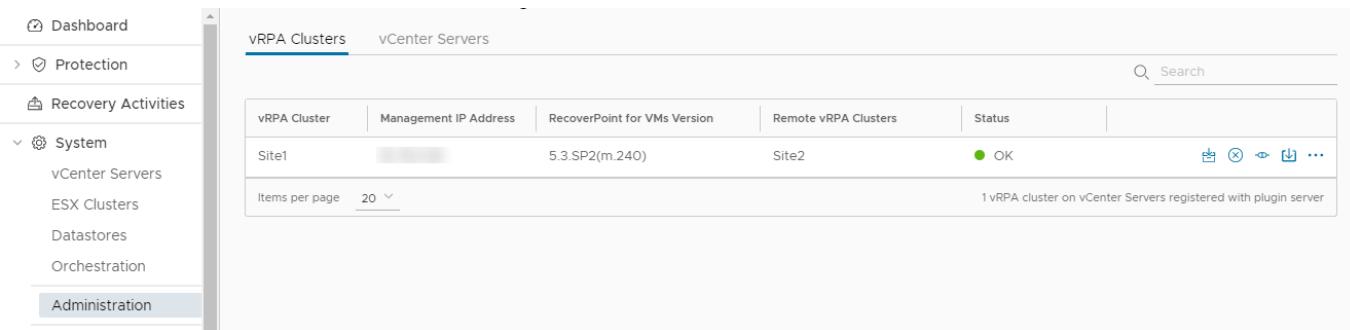
# Managing vRPA clusters

Manage the vRPA clusters on all vCenter Servers that are registered with (or Linked to a vCenter Server registered with) the plugin server.

Monitor the state of your **vRPA clusters** in the system in the RecoverPoint for VMs Dashboard.



Use the **System > Administration > vRPA Clusters** screen to collect logs from a vRPA cluster, exclude a vRPA cluster from plugin server management, connect a vRPA cluster to another vRPA cluster, upgrade a vRPA cluster, or display more vRPA cluster options.

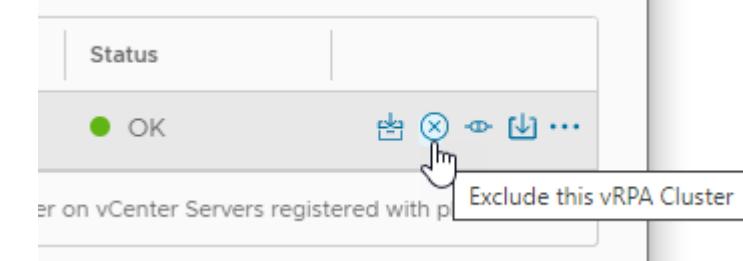


The screenshot shows the 'vRPA Clusters' tab selected in the navigation bar. The main table displays a single vRPA cluster named 'Site1' with the following details:

vRPA Cluster	Management IP Address	RecoverPoint for VMs Version	Remote vRPA Clusters	Status	Actions
Site1	[REDACTED]	5.3.SP2(m.240)	Site2	● OK	   

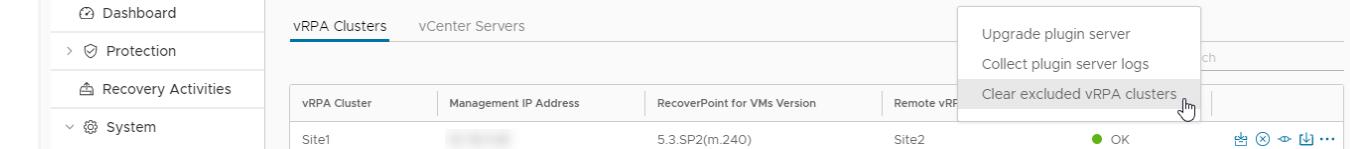
The sidebar on the left shows the navigation path: Dashboard, Protection, Recovery Activities, System (with sub-options: vCenter Servers, ESX Clusters, Datastores, Orchestration), and Administration (which is selected).

- To exclude a vRPA cluster from plugin server management, click the **exclude icon**.



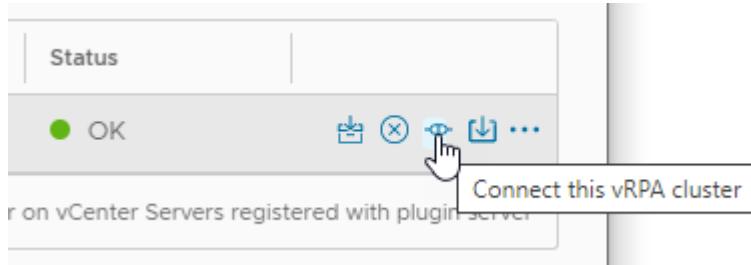
A close-up view of the vRPA cluster row in the table. A hand cursor is hovering over the 'Exclude' icon (a red circle with a white minus sign). A tooltip 'Exclude this vRPA Cluster' is displayed below the icon.

- To include all excluded vRPA clusters, click **ACTIONS > Clear excluded vRPA clusters**.

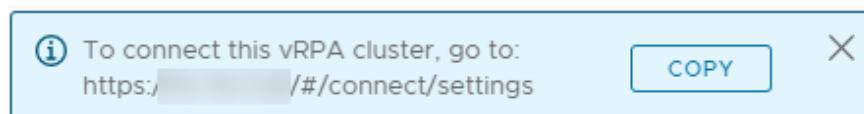


A screenshot of the 'vRPA Clusters' screen showing the 'Actions' menu open. The 'Clear excluded vRPA clusters' option is highlighted with a mouse cursor. The table below shows the same vRPA cluster data as the previous screenshot.

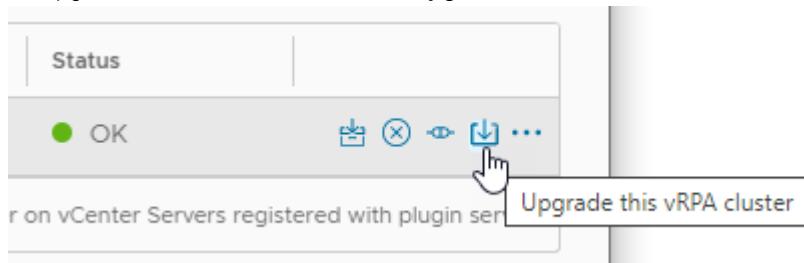
- To connect a vRPA cluster to another vRPA cluster, click the **Connect this vRPA cluster** icon.



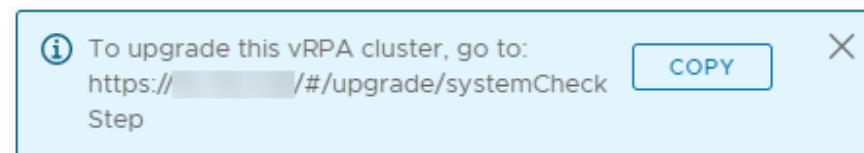
The following system message is displayed:



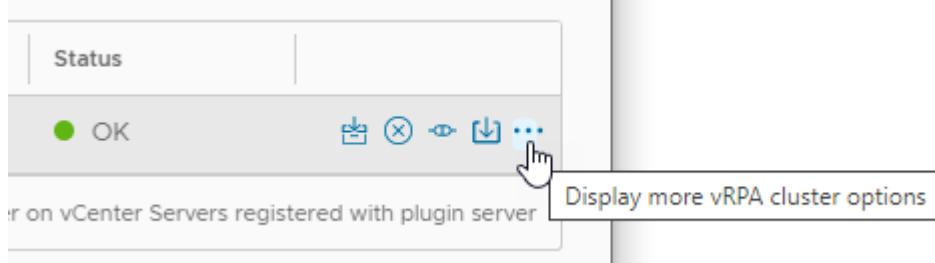
- To upgrade a vRPA cluster, click the **Upgrade this vRPA cluster** icon.



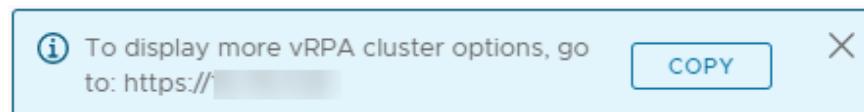
The following system message is displayed:



- To display more vRPA cluster options, click **[...]**.



The following system message is displayed:



In the system message that is displayed, click **Copy**, open a browser window, and paste the copied URL into the browser address bar.

The **RecoverPoint for VMs Deployer** is displayed.



**Figure 12. RecoverPoint for VMs Deployer 6.0.3**

In the **RecoverPoint for VMs Deployer** home screen, to complete:

- Click **Collect Logs**. To get the logs from the vRPA, click **Collect Logs** in the **Collect vRPA Logs** dialog box.
- Click **Connect vRPA clusters** and follow the on-screen instructions.
- Click **Upgrade a vRPA cluster** and follow the on-screen instructions.
- Other vRPA cluster options, select the required option under **More actions**.

For detailed information about how to perform all vRPA cluster actions, see the *RecoverPoint for VMs Installation and Deployment Guide*.

## Managing system component registration

This section describes how to manage the registration (and health) of the components of your RecoverPoint for Virtual Machines system, after the system has already been configured.

### Steps

- For a detailed description of how to deploy the RecoverPoint for Virtual Machines system, see the *Dell RecoverPoint for Virtual Machines Installation and Deployment Guide*.
- For a detailed description of how to initially configure the RecoverPoint for Virtual Machines system, see [Before you begin](#).

## Register vCenter Server to vRPA cluster

Use this procedure to register a vCenter Server to a vRPA cluster.

### Prerequisites

- All vCenter Servers that manage production VMs and copy VMs must be registered at the relevant vRPA cluster before you protect VMs.
- It is recommended to configure the vCenter Server to require a certificate, because once RecoverPoint has read the certificate, it does not need further access to the location.

For more information about the location of the security certificate, refer to VMware documentation at [www.vmware.com](http://www.vmware.com).

### Steps

1. Click **System > vCenter Server**, and select the vRPA cluster to which you want to register a vCenter Server.

Registered vCenter Servers		vRPA Cluster	Site1	Search	<b>ADD</b>	
vCenter Server	IP Address	Port	Username	Status		
		443		OK		
Items per page	20	▼	1 Registered vCenter Server with 'Site1'			

2. Click **ADD**.

Register vCenter Server X

---

**vCenter Server**  
Enter IP address or host name

**Port**  
443

**Username**  
Enter username

**Password**  
Enter username password

---

**CANCEL** **REGISTER**

3. Enter the IP and credentials of the vCenter Server to be registered.

4. Click **REGISTER**.

## Results

The specified vCenter Server is registered at the specified vRPA cluster. All ESX clusters hosted by the vCenter Server are automatically registered with the specified vRPA cluster, a splitter is installed on all ESXi hosts in the cluster, and replication is temporarily paused for all relevant VMs while the splitter is being installed.

## Next steps

Ensure that a plugin server is installed on the newly registered vCenter Server. For a linked vCenter Server, see [Managing vCenter Server registration with plugin server](#).

## Managing ESX cluster registration

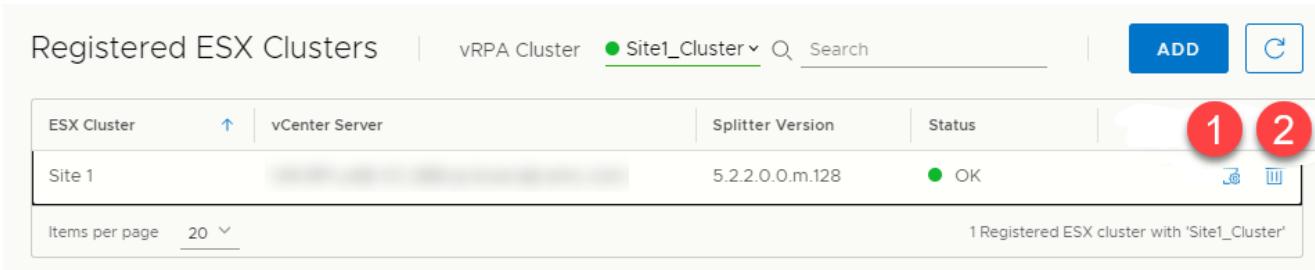
Registers the ESX cluster of a production VM or copy VM, at a vRPA cluster.

### About this task

By default, ESX clusters are automatically registered in RecoverPoint for Virtual Machines during VM protection and copy addition. Perform the steps below to register ESX clusters in the rare case that the system cannot automatically register an ESX cluster.

### Steps

1. In the **RecoverPoint for Virtual Machines vSphere plug-in**, select **System > ESX Clusters**.



ESX Cluster	vCenter Server	Splitter Version	Status
Site1	[REDACTED]	5.2.2.0.0.m.128	OK

Items per page  1 Registered ESX cluster with 'Site1\_Cluster'

2. If you are replicating remotely, select the vRPA cluster at which you want to register ESX clusters.
3. Click **ADD**.
4. In the **Register ESX Cluster** dialog box:
  - a. Select the ESX cluster that you want to register.
  - b. Click **REGISTER**.

## Results

The specified ESX cluster is registered at the specified vRPA cluster.

**NOTE:** When an ESX cluster of an unregistered vCenter Server is registered with a vRPA cluster, a splitter is installed on all ESXs in the cluster. The replication is temporarily paused for all relevant VMs while the splitter is being installed.

## Next steps

Registered ESX clusters can be (1) updated or (2) deleted.

## Managing journal datastore registration

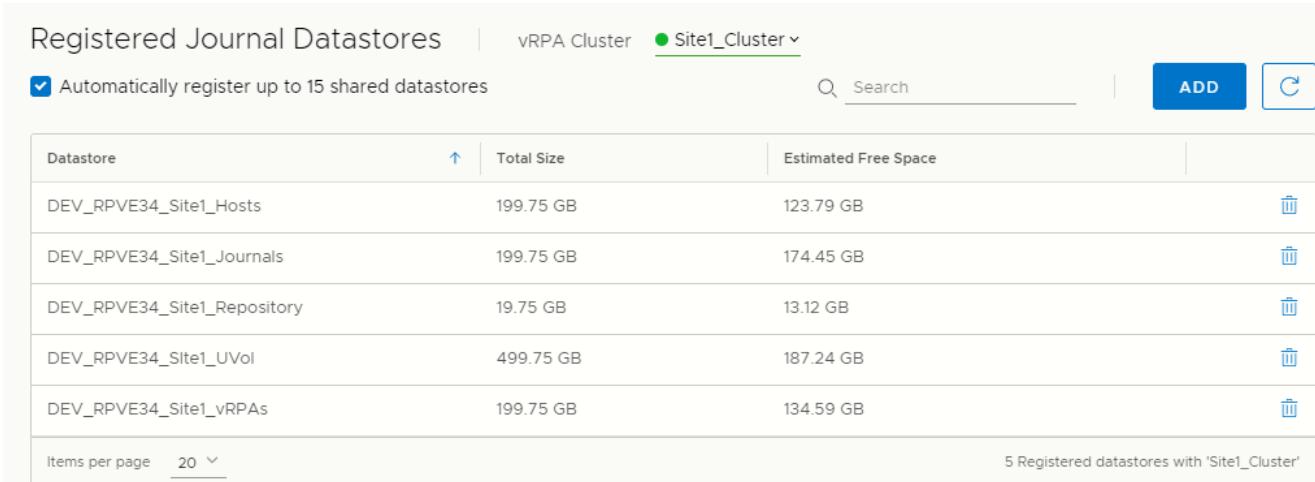
Register the datastores that are to contain the history of the data that you want to protect, at each vRPA cluster. Up to 15 shared datastores of ESX clusters running vRPAs are automatically registered in RecoverPoint for Virtual Machines. Use the following steps to register a datastore in the rare case that a datastore that you need is not automatically registered.

### About this task

**NOTE:** When you protect a consistency group, the **Protect VMs Wizard** automatically selects a datastore from the list of registered datastores, unless you specify a specific registered datastore to use. RecoverPoint for Virtual Machines attempts to create the journal on the selected datastore. If for any reason journal creation fails, the system attempts to create the journal on a different registered datastore.

### Steps

1. In the **RecoverPoint for Virtual Machines vSphere plug-in**, select **System > Datastores**.



Datastore	Total Size	Estimated Free Space
DEV_RPVE34_Site1_Hosts	199.75 GB	123.79 GB
DEV_RPVE34_Site1_Journals	199.75 GB	174.45 GB
DEV_RPVE34_Site1_Repository	19.75 GB	13.12 GB
DEV_RPVE34_Site1_UVol	499.75 GB	187.24 GB
DEV_RPVE34_Site1_vRPAs	199.75 GB	134.59 GB

Items per page  5 Registered datastores with 'Site1\_Cluster'

2. If you are replicating remotely, select the vRPA cluster at which you want to register datastores, and click **Add...**.

The **Register Datastore** dialog box is displayed.

**3.** In the **Register Datastore** dialog box:

- a.** Select one or more datastores to register.
- b.** Click **REGISTER**.

## Results

The datastore is registered at the specified vRPA cluster.

## Next steps

Registered journal datastores can be deleted.

 **NOTE:** A datastore with a scratch partition on its root path must not be used to host journals.

## Managing external host registration

Defines the external host on which user scripts are run during virtual machine start-up sequences.

### Prerequisites

- SSH must be installed on the external host.
- Only one external host can be configured per vRPA cluster.
- Define the external host before defining virtual machine start-up scripts in a virtual machine startup Sequence. For information on how to define start-up scripts, see [VM start-up sequence](#).

### Steps

1. In the vSphere HTML5 plugin, select **System > Orchestration**, and select the vRPA cluster for which you want to define an external host.
2. Click **ADD** under the **External Host** widget.
3. In the **Register External Host** dialog box, type the **Name**, **IP**, **User**, and **Password** of the external host for the selected vRPA cluster.
4. Optionally:
  - To verify connectivity with the external host, click **Check Connectivity**.
  - To unregister the external host from the specified vRPA cluster, click **Remove**.

## Manage Event Filters

Use **RecoverPoint for VMs > Notifications > Event Filters** to define and modify the settings for the outbound system events through email, SNMP, and Syslog.

### Display all event filters

#### About this task

To display all the event filters that are defined in the system, select **RecoverPoint for VMs > Notifications > Event Filters**.

### Create an event filter

#### Steps

1. Select **RecoverPoint for VMs > Notifications > Event Filters**.
2. Click **Add**. The **Define Filter** wizard is displayed.
3. In the **Define Filter** screen:
  - a.** Define the event filter settings according to the instructions in the following table.

**Table 3. Event Filter settings**

Setting	Description
Filter Name	Type a unique name of the event filter to be created.
Topic	Select the type of topic from the following options: <ul style="list-style-type: none"><li>• All Topics</li><li>• Array</li><li>• Cluster</li><li>• Consistency Group</li><li>• Management</li><li>• RPA</li><li>• Splitter</li></ul>
Groups to include	This table is displayed only when the 'Topic' is set to <i>All Topics</i> or <i>Consistency Group</i> .. Select the group names to include in the event filter . There is no default value for this parameter.
Level	<ul style="list-style-type: none"><li>• Info: The event is informative in nature, usually seeing changes in the configuration, or normal system state. When Level=Info, events of all levels are returned. There is no filtering of events as a result of the Level setting.</li><li>• Error: Event indicates an important event that is likely to disrupt normal system behavior and performance. When Level=Error, only events at the Error level are returned. Warning-level and Info-level events are filtered. The Error level includes Error Off and Brief Error events.</li><li>• Warning: Event indicates a warning, usually seeing a transient state or an abnormal condition that does not degrade system performance. When Level=Warning, all events with level of Warning or Error are returned. Info-level events are filtered. The Warning level includes Warning Off events.</li></ul>
Scope	<ul style="list-style-type: none"><li>• Advanced: In specific cases (for instance, for troubleshooting a problem) Customer Support may ask you to retrieve information from the advanced log events. These events contain information that is intended primarily for the technical support engineers.</li><li>• Normal: To report selected basic events and root-cause events. A root-cause event returns a single description for a system event that can spawn an entire set of <i>detailed</i> and <i>advanced</i> events. When Scope=Normal, all those <i>detailed</i> and <i>advanced</i> events are filtered out, leaving only the <i>normal</i> events. This is the default setting, and usually, it is sufficient for effective monitoring of system behavior.</li><li>• Detailed: This category includes all events (that is, <i>detailed</i> and <i>normal</i>), about all components that are generated for use by users.</li></ul>
Event IDs to exclude	The IDs of the <i>Events</i> that are not subject to this filter. Click the add icon to include more event ids.

- b. Click **Next Define Method of Transfer**.**
- 4. In the **Define Method of Transfer** screen, select one or more methods of transfer.**
  - Email—If you select this option, enter the following details:
    - Email Frequency—Select the frequency to send the events. The options available are **DAILY** and **IMMEDIATE**.
    - Email addresses of event recipients—Type the email addresses of the recipients. Click + to add multiple recipients.
  - SNMP
  - Syslog
- 5. Click **Finish** to save the event filter and exit the wizard.**
- 6. Configure the transfer method for each method of transfer that you defined.**

## Configure the transfer method

Events can be transferred to the specified servers or email addresses by email, syslog, or SNMP.

# Configure Email event notification

## About this task

Use the following table to enable the transfer of events by email.

## Steps

1. Select **RecoverPoint for VMs > Notifications > Event Filters**.
2. In the bottom pane, select the **Email** tab.
3. Enter the values for the fields in the **Email** tab according to the instructions in the following table.

**Table 4. Email settings**

Setting	Description
Enable Email Notifications	Select to enable the events defined in any event filters whose method of transfer is set to Email to be transferred to the specified server from the specified sender. <b>NOTE:</b> Selecting this checkbox also enables the sending of email alerts to the specified server address if you enabled both reports and alerts in the <b>Configure System Reports and Alerts</b> screen.
SMTP server address	Enter the IP address or DNS name of the server to which to send the emails. <b>NOTE:</b> When you click <b>Apply</b> , any change to this field automatically updates the SMTP server address field in the <b>Configure System Reports and Alerts</b> screen.
Sender address	Enter the email address that should appear in the sender field of all emails concerning sent to the specified server regarding event notifications.

4. Click **Apply**.

## Results

All the event filters whose Method of Transfer includes Email is transferred to the recipients defined in the filter (at the frequency defined in the filter) using the specified server address and sender.

# Configure Syslog event notification

## About this task

Use the following procedure to enable the transfer of events by syslog.

## Steps

1. Select **RecoverPoint for VMs > Notifications > Event Filters**.
2. In the bottom pane, select the **Syslog** tab.
3. Enter the values for the fields in the **Syslog** tab according to the following table.

**Table 5. Syslog settings**

Setting	Description
Enable Syslog Notifications	Select to enable the events defined in any event filters whose method of transfer is set to Syslog to be transferred to the specified servers with the specified label.
Facility	Select one of the available labels to be attached to all messages.
Specify a target host for	(Optional) Specify the syslog server at each RPA cluster to which you want to deliver notifications. The address may be either in IP or DNS format. A DNS address works only if a DNS server is configured in the RecoverPoint system.

4. Click **Apply**.

## Results

All the event filters whose Method of Transfer includes Syslog is transferred using the specified target host and facilities.

## Configure SNMP event notification

Use the following procedure to enable the transfer of events by SNMP.

### About this task

RecoverPoint supports the standard Simple Network Management Protocol (SNMP). RecoverPoint supports various SNMP queries and can be configured to generate SNMP traps (notification events), which are sent to designated network management systems.

### Steps

1. Select **RecoverPoint for VM** > **Notifications** > **Event Filters**.
2. In the bottom pane, select the **SNMP** tab.
3. Enter the values in the fields of the **SNMP** tab according to the following table.

**Table 6. SNMP settings**

Setting	Description
<b>Enable SNMP Agent</b>	Select this option to enable the RecoverPoint SNMP agent. It sends the events in the event filters whose method of transfer is set to SNMP to the specified servers with the specified label.  The RecoverPoint SNMP agent must be enabled in order to send SNMP traps (notification events) and to respond to host-initiated SNMP queries.
<b>Allow secure transports only</b>	When selected, only encrypted SNMP queries over secure transport are enabled; use of community strings and SNMP over an unsecured port is disabled.
<b>Send Event Traps</b>	When selected, sends SNMP traps (notification events) to the RecoverPoint SNMP agent according to your SNMP trap configuration. This option does not affect host queries.
<b>Specify trap destination for</b>	(Optional) The network management server to which you want to deliver notifications. The address may be either in IP or DNS format. A DNS address works only if a DNS server is configured in the RecoverPoint system.
<b>SNMP v1 RO community</b>	If you are using SNMP version 1, enter an SNMP v1 read-only community string to enable the use of SNMP v1 community strings. If not enabled, only SNMP v3 usernames with passwords or certificates are enabled.  <b>NOTE:</b> The read-only community string is transmitted in cleartext.

## Modify an existing event filter

### Steps

1. Select **RecoverPoint for VMs** > **Notifications** > **Event Filters**.
2. Click the **Edit** icon from the event row. The **Define Filter** wizard appears, with the current settings for the selected event filter.
3. Modify the event filter settings according to the instructions in [Create an event filter](#).
4. Click **Next Define Method of Transfer**.
5. Modify the methods of transfer if required. For each new method of transfer that you define, you must [Configure the transfer method](#).
6. Click **Finish** to save the new event filter settings and exit the wizard.

# Managing protected VMs

This section describes how to manage the protection of protected VMs.

## Steps

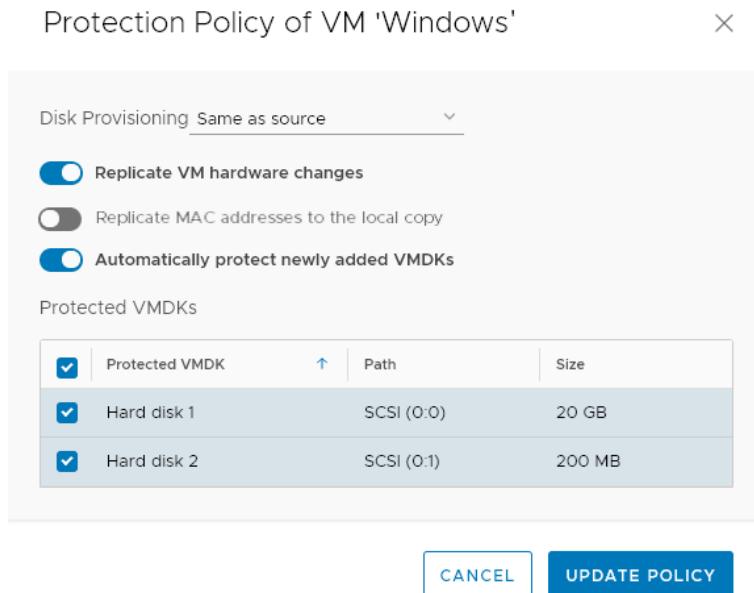
- After initial protection, use the RecoverPoint for Virtual Machines vSphere HTML5 plugin to manage VMs either through **Protection > Protected VMs** or **Protection > Consistency Groups**. For a detailed description of how to protect VMs, see [Protecting VMs](#).

## Managing VM protection policies

Update the protection policies of protected virtual machines.

## Steps

- In the RecoverPoint for Virtual Machines plugin for vSphere Client, select **Protection > Protected VMs**.
- Select a virtual machine, and click **PROTECTION POLICY**.  
The VM **Protection Policy** dialog is displayed.



- Update the VM protection policies:
  - Disk provisioning:** Default is **Same as source**. Defines the way in which the copy VMDKs are to be provisioned: **Same as source**, **Thick provision lazy zeroed**, **Thick provision eager zeroed** or **Thin provision**.
  - Replicate VM hardware changes:** Default is **Enabled**. Automatically replicates the hardware settings of all production virtual machines to their copy VMs whenever an image is accessed on the copy VMs. When enabled, RecoverPoint for VMs replicates the virtual machine version, MAC address, CPU, memory, resource reservations, and network adapter status and type. Replication of SR-IOV Passthrough Adapter is not supported. If the ESX at a copy does not support the production VM version, no hardware resources are replicated.
  - Replicate MAC addresses to local copy:** Default is **Disabled**. If two *remote copies* of the same production VM are on the same vCenter and in the same network, you cannot power on both copy VMs simultaneously, as they will both have the same MAC address. Therefore, by default, the MAC address of remote copy VMs network adapters (NICs) on a different vCenter than their production VMs are replicated to the copy. However:
    - When **Replicate VM hardware changes** is disabled, MAC address replication to the remote copies is also disabled.
    - To avoid IP conflicts, by default, the MAC addresses are not replicated to the local copy VMs on the same vCenter as their production VMs. If a local copy VM is not on the same network and ESX as its production VM, enable **Replicate MAC addresses to local copy** to replicate the MAC addresses.

- **Automatically protect newly added VMDKs:** Default is **Enabled**. Automatically includes any VMDKs that are added to a VM, after it is already protected.
- **Protected VMDKs:** Displays the number of VMDKs that will be replicated, their **Path**, and their total size. Clear a VMDK check box to exclude the VMDK from replication.

#### 4. Click **UPDATE POLICY**.

#### Results

The VM protection policies are updated.

## Stop protecting a VM

Unprotect a VM to stop replication and remove it from its consistency group.

#### Steps

1. In the RecoverPoint for VMs vSphere HTML5 plugin to manage VMs either through **Protection > Protected VMs**
2. Select the production VM that you want to stop protecting.
3. Click **UNPROTECT**

Alternatively, to unprotect all VMs in a consistency group, select **Protection > Consistency Groups**, select the consistency group, and from the [...] menu, select **Unprotect**.

#### Results

Replication stops and the virtual machine is removed from its consistency group. The copy VM is not automatically deleted. If there are no other virtual machines in the consistency group, the consistency group is removed.

## Managing consistency groups

This section describes how to manage existing consistency groups in the RecoverPoint for Virtual Machines system.

#### Steps

1. After initial protection, use the RecoverPoint for Virtual Machines plugin to manage consistency groups through the **Protection > Consistency Groups** screen.

## Managing group protection policies

Update the protection policies of consistency groups and their copies.

#### Steps

1. In the RecoverPoint for VMs plugin for **vSphere Client (HTML5)**, select **Protection > Consistency Groups**.
2. Select a consistency group, and click **PROTECTION POLICY**.  
The group **Protection Policy** dialog is displayed.

## Protection Policy of Group 'MyGroup'

X

General Production (Site1) Remote 1 (Site2)

GROUP POLICY VM STARTUP SEQUENCE

Consistency Group

MyGroup

Primary vRPA

vRPA 2 ▾

Bandwidth Priority

Normal ▾

CANCEL

UPDATE POLICY

### 3. Update the group policies:

#### a. Select **General** > **GROUP POLICY**.

- **Consistency Group:** The name of the consistency group in the RecoverPoint for VMs system. Default is `cg_<vmname>`.
- **Primary vRPA:** The vRPA that you prefer to replicate the consistency group. When the primary vRPA is not available, the consistency group switches to another vRPA in the vRPA cluster. When the primary vRPA becomes available, the consistency group switches back to it.

**(i) NOTE:** If your vRPA cluster is the only vRPA cluster in the system, it is a single point of failure in cases of disaster. Consider adding additional vRPAs to the vRPA cluster to ensure high availability.

- **Bandwidth Priority:** Only relevant for remote replication when two or more consistency groups are using the same **Primary vRPA**. Default is **Normal**. Select the bandwidth priority to assign to this consistency group. The priority determines the amount of bandwidth that is allocated to this group in relation to all other groups using the same primary vRPA.

#### b. To define the order in which VMs in a consistency group powers on during testing and recovery. Select **General** > **VM STARTUP SEQUENCE**, and see [VM start-up sequence](#).

### 4. Update the group production policies:

**(i) NOTE:** The production policies are only applied after failover.

Select the **Production** tab and click **PRODUCTION POLICY** and **RE-IP RULES** to define the production policies to be applied after failover (when the production becomes a copy). Refer to the next step for a detailed description of the production policies.

### 5. Update the group copy policies:

- Select a copy and click the **COPY POLICY** tab to update the copy protection settings:

Required retention policy  
7 days

Consolidate RecoverPoint for VMs snapshots  
Do not consolidate snapshots for at least: 2 days

Consolidate snapshots older than 2 days to one snapshot per day for: 5 days  indefinitely

Consolidate snapshots older than 1 weeks to one snapshot per week for: 8 weeks  indefinitely

**Info:** Snapshots older than 2 months 3 days will be consolidated to one snapshot per month.

- Required retention policy:** Default is **disabled**. Defines how far in time the copy image can be rolled back. Enable to define a retention policy in **minutes**, **hours**, **days**, **weeks**, or **months**. An alert is displayed if the copy image cannot be rolled back according to the required retention policy.
- Consolidate RecoverPoint for VMs snapshots:** Default is **disabled**. Automatic snapshot consolidation cannot be enabled for a group that is part of a group set.
  - Do not consolidate any snapshots for at least:** Default is **2 days**. Can be defined in **hours**, **days**, **weeks**, or **months**. Defines the period during which snapshot data is not to be consolidated. If no daily or weekly consolidations are specified, the remaining snapshots are consolidated monthly.
  - Consolidate snapshots that are older than x to one snapshot per day for y days:** Default is **5 days**. Snapshots are consolidated every 24 hours. Select **Indefinitely** to consolidate all subsequent snapshots in 24-hour intervals.
    - If **Indefinitely** is not selected, and no weekly consolidations are specified, the remaining snapshots are consolidated monthly.
    - If **Indefinitely** is selected, weekly, and monthly consolidations are disabled, and the remaining snapshots are consolidated daily.
  - Consolidate snapshots that are older than x to one snapshot per week for y weeks:** Default is **4 weeks**. Snapshots are consolidated every 7 days. Select **Indefinitely** to consolidate all subsequent snapshots in seven-day intervals.
    - If **Indefinitely** is not selected, the remaining snapshots are consolidated monthly.
    - If **Indefinitely** is selected, monthly consolidations are disabled, and the remaining snapshots are consolidated weekly.
- Journal Volumes:** Displays the size and datastore of each journal volume, and allows you to add or remove journal volumes.

Journal Volumes ADD

Journal Volume	Volume Size	Datastore	
IOFilter_JVOL_00003	10 GB	New_DS_Site2_XIO_X1_A07	

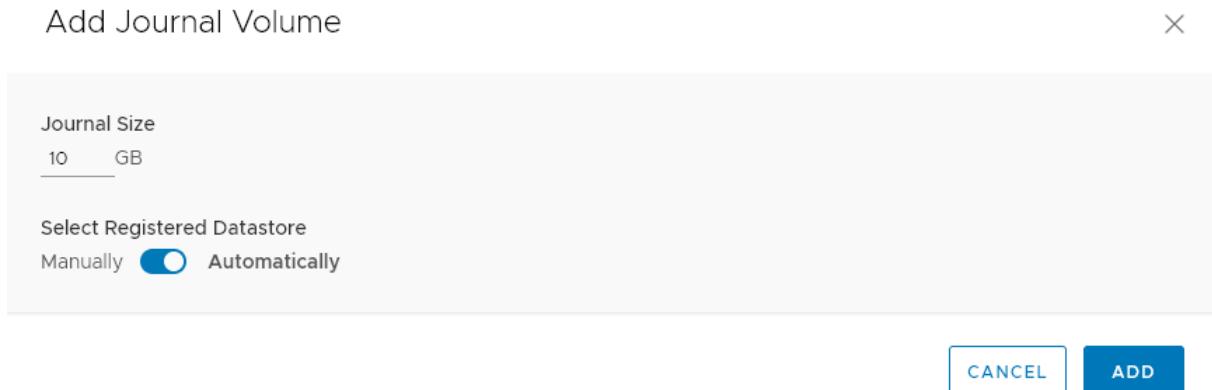
1 Journal volumes

- (Production journal only) This option is only displayed if more than one journal volume was added to the production journal. Click **RESET SIZE** if journal volumes were added to the production journal after a temporary failover. After failing back to production, use this button to reset the production journal to its original size (by default, **3GB**) without triggering a full sweep.
- Click the **delete icon** to remove a journal volume. The last journal volume at a copy cannot be deleted.

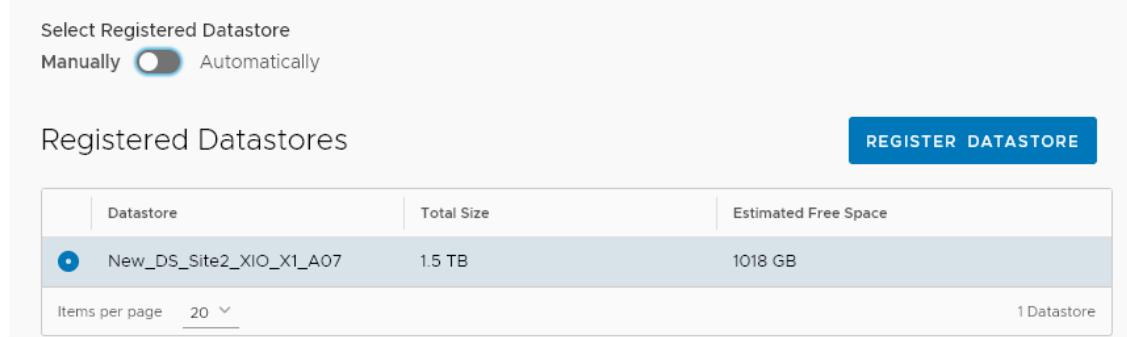
**CAUTION:** Removing a journal volume causes a full sweep on all VMs in the consistency group. The full sweep duration depends on the size of the data being replicated, network resources, and storage performance.

Click **ADD** to add volumes to the copy journal. The **Add Journal Volume** dialog is displayed.

**NOTE:** You can safely click **ADD** now, as the default settings provide a sensible configuration for most systems.

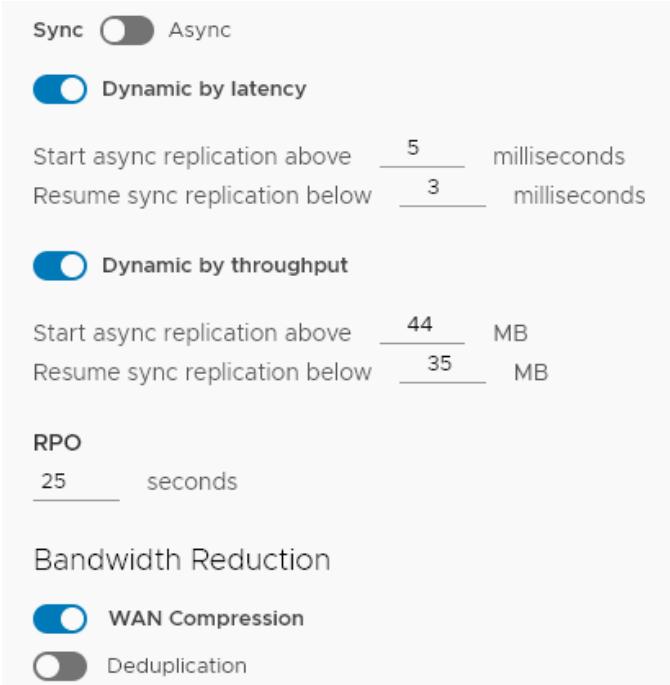


- **Journal Size:** Default is **10GB** for the copy journals and **3GB** for the production journal. The default size of the production journal is smaller, and in most cases does not require any additional volumes. The larger a copy journal, the more history can be saved.
- **Select Registered Datastore:** Default is **Automatically**. By default, RecoverPoint for VMs automatically registers up to 15 datastores for the production and copy journals and automatically selects the datastore with the most free space. When set to **Manually**:



- **Registered Datastores:** Select a registered datastore or register a new datastore for the journal. By default, RecoverPoint for Virtual Machines automatically registers up to 15 datastores for the group journals and automatically selects the datastore with the most free space. RecoverPoint for Virtual Machines attempts to create a journal volume on the selected datastore. If it cannot, the system attempts to create the journal volume on another registered datastore.
  - If you have more than 15 datastores and would like to register a datastore that is not in the list, click **REGISTER DATASTORE** to register an additional datastore.
- b. Select a copy and click the **RE-IP RULES** tab to create **Re-IP rules** to update the network configuration of copy VMs during testing and recovery.

- c. (Not relevant for the production) Select a copy and click the **LINK POLICY** tab to update the copy link protection



settings:

- **Async or Sync:** Default is **Async**. Defines how data is replicated from the production to the copy. Data can be replicated synchronously (**sync**) or asynchronously (**async**). When **sync** is selected, you can also define the following policies:
  - **Dynamic by latency:** Default is **disabled**. When enabled, RecoverPoint for VMs alternates between synchronous and asynchronous replication modes, as necessary, according to latency conditions.
    - **Start async replication above:** When the specified limit (in **milliseconds**) is reached, RecoverPoint for VMs automatically starts replicating asynchronously.
    - **Resume sync replication below:** When the specified limit (in **milliseconds**) is reached, RecoverPoint goes back to replicating synchronously.
  - **Dynamic by throughput** Default is **disabled**. When enabled, RecoverPoint for VMs alternates between synchronous and asynchronous replication modes, as necessary, according to throughput conditions.
    - **Start async replication above:** When the specified limit (in **MB**) is reached, RecoverPoint for VMs automatically starts replicating asynchronously.
    - **Resume sync replication below:** When the specified limit (in **MB**) is reached, RecoverPoint goes back to replicating synchronously.
- **RPO:** Defines the maximum lag that is allowed on a link.
- **WAN Compression:** Default is **enabled**. Only relevant for asynchronous remote replication. To compress data before transferring it to a remote vRPA cluster, select a level of compression. Enabling and disabling compression causes a short pause in transfer and a short initialization. Compression can reduce transfer time considerably, but increases the CPU utilization of the source vRPA.
- **Deduplication:** Default is **disabled**, but deduplication can be enabled whenever compression is enabled. Eliminates repetitive data before transferring the data to a remote vRPA cluster. Enabling and disabling deduplication causes a short pause in transfer and a short initialization. Deduplication can reduce transfer time considerably, but increases the CPU utilization of the source vRPA.

- d. (Not relevant for the production) Select a copy and click the **FAILOVER NETWORKS** tab to configure **Failover networks** to automatically associate the VM network adapters (vNICs) of a copy VM with specific port groups upon failover or during copy testing.

## 6. Click **UPDATE POLICY**.

### Results

The group protection policies are updated.

# Managing group sets

Manage group sets in RecoverPoint for VMs.

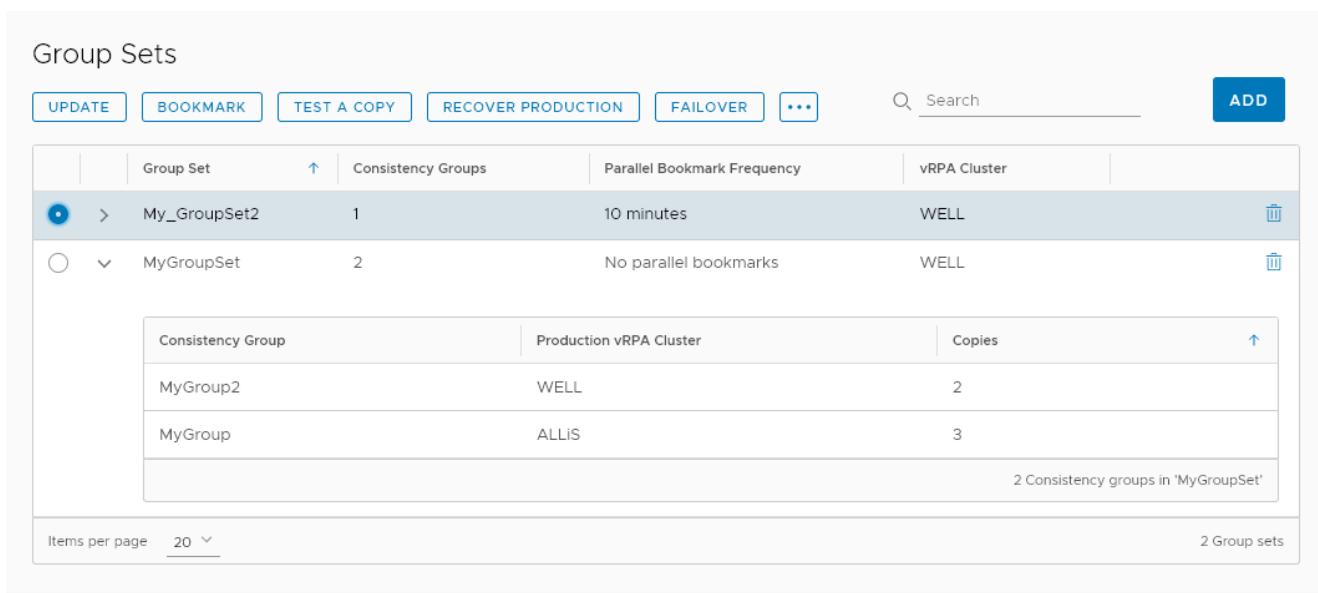
## About this task

A group set is a collection of consistency groups that you can bookmark, enable, disable, pause and resume replication for, and test and recover as a group. You can also create parallel bookmarks on all groups in the group set, at a frequency that you define. Group sets are useful for consistency groups that are dependent on one another or that must work together as a single unit.

## Steps

### 1. Select **Protection > Group Sets**.

The **Group Sets** screen is displayed.



Group Set	Consistency Groups	Parallel Bookmark Frequency	vRPA Cluster
My_GroupSet2	1	10 minutes	WELL
MyGroupSet	2	No parallel bookmarks	WELL

Consistency Group	Production vRPA Cluster	Copies
MyGroup2	WELL	2
MyGroup	ALLiS	3

2 Consistency groups in 'MyGroupSet'

Items per page 20 2 Group sets

### 2. In the **Group Sets** screen:

- Note the number of consistency groups in the group set, the parallel bookmarking status and the vRPA cluster from which all groups in the group set are replicating.
- Expand a group set to display the names of the consistency groups that are currently in the group set and their properties.
- Select a group set, and:
  - Click **ADD** to create another group set. See [Create a group set](#) for more information.
  - Click **UPDATE** to modify the group set configuration. See [Create a group set](#) for more information.
  - Click **BOOKMARK** to apply a label or consolidation policy to all copy VMs of all consistency groups in the group set. See [Create a bookmark](#) for more information.
  - Click **TEST A COPY**, **RECOVER PRODUCTION**, or **FAILOVER** to test a copy, failover, or recover production of all consistency groups in the group set. See [Recovering VMs](#) for more information.
  - Click the more commands **[...]** button to display additional group set commands:
    - **Group priority**: Set the power-on priority of all consistency groups in the group set. See [Group start-up sequence](#) for more information.
    - **Disable groups** or **Enable groups**: Disables or enables all copies of all consistency groups in the group set.

 **CAUTION:** Disabling a group stops all copy activities, and deletes all copy journals. A full sweep is required when transfer resumes.

- **Pause transfer** or **Resume transfer**: Pauses or resumes transfer of all copies of all consistency groups in the group set.

# Managing recovery activities

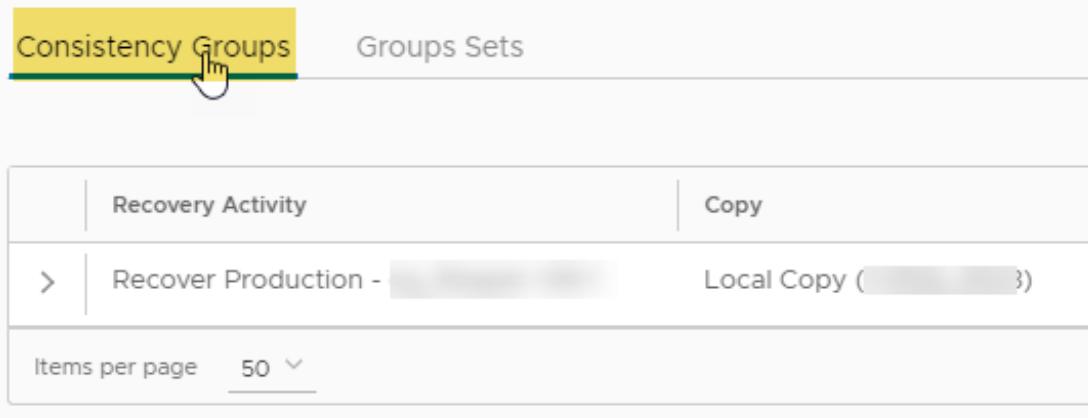
Manage ongoing testing, failover, failback, and production recovery activities using the **Recovery Activities** screen.

Use the **Recovery Activities** screen to:

- Manage testing.
- Manage failover and failback.
- Manage production recovery.

To manage an ongoing recovery activity of a consistency group, select **Recovery Activities** **Consistency Groups**.

## Recovery Activities

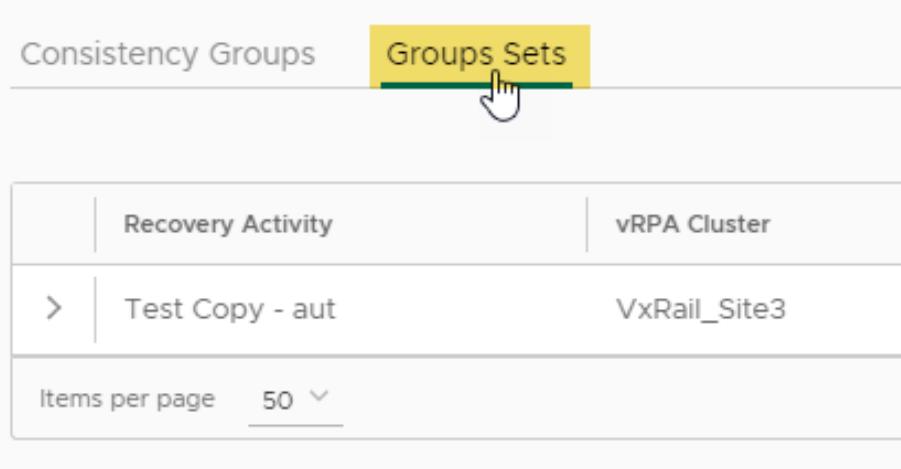


Recovery Activity	Copy
> Recover Production -	Local Copy ( 3 )

Items per page 50

To manage an ongoing recovery activity of a group set, select **Recovery Activities** **Group Sets**.

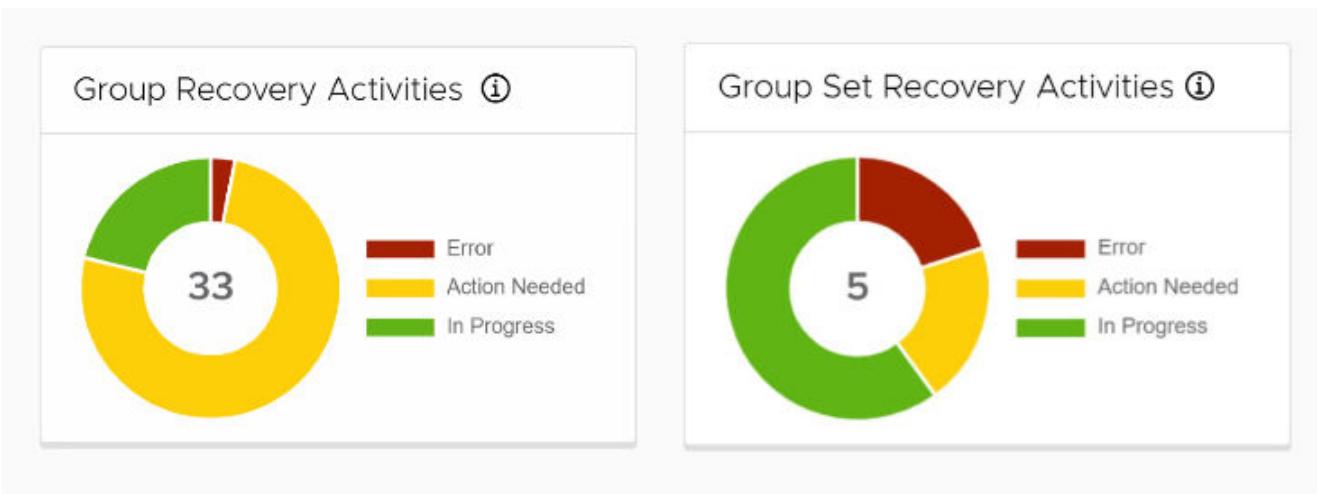
## Recovery Activities



Recovery Activity	vRPA Cluster
> Test Copy - aut	VxRail_Site3

Items per page 50

Use the [RecoverPoint for VMs Dashboard](#) to monitor the state of ongoing recovery activities, for both consistency groups and group sets.



## Manage testing

Manage the ongoing testing of a copy of a consistency group or group set using the **Recovery Activities** screen.

**NOTE:** When testing a copy, wait for the **Activity Status** to show **Ready for next action** and the **Progress status bar** to reach 100%, indicating the specified snapshot image has been accessed.

If you tested a copy of a consistency group:

Recovery Activity	Copy	Snapshot	Activity Start	Activity Status	Progress
Test Copy - cg_KATE_VM_13...	Local Copy (NASA_Site1)	Nov 23, 2020 11:55:47 AM	Nov 23, 2020 11:55:48 AM	Ready for next action	<div style="width: 100%;">100%</div>

Image Access Log Capacity: 4% (Progress bar)

Testing Network: Isolated per group

User Prompts: None

UNDO WRITES, ENABLE DIRECT ACCESS

Journal Capacity: 3% (Progress bar)

Items per page: 20

The **Consistency Group Recovery Activities** screen is displayed. The **Activity Status** and **Progress** columns indicate the progress of image access. After access is enabled to the copy snapshot, the **Activity Status** column displays **Ready for next action**, and you can:

**NOTE:** The **Image Access Log Capacity** progress bar indicates how long you can access the copy image before the image access log is full and all writes to the copy fail. If you need more time for testing, you can undo writes at the copy, enable direct access to the copy, or add journal volumes as described in [Managing group protection policies](#).

- Click **UNDO WRITES** to undo all writes that were made to the copy snapshot while write access was enabled, without disabling access to the copy volumes.
- Click **ENABLE DIRECT ACCESS** to write directly to the copy storage. Any changes that are made to the copy storage while directly accessing the copy cannot be automatically undone, because when a snapshot is directly accessed, the journal at the copy is deleted. Also direct access does not impose a limit to the amount of data that you can write to the copy storage volumes.

**CAUTION:** When direct access is enabled, replication stops to the copy, and a short initialization is required across all group volumes when direct access is disabled.

- Click **ACTIONS** > **Start new test** to select another snapshot to test, or to redefine the testing network.
- Click **ACTIONS** > **Stop activity** to roll back all writes that were made to the copy snapshot while write access was enabled to the snapshot volumes, and disable write access to the snapshot volumes.

- Click **ACTIONS > Promote image: Failover** to jump directly to the Failover stage of failover to the copy image that you tested now (step 8), without requiring to roll back the writes that were made to the copy snapshot while write access was enabled.
- Click **ACTIONS > Promote image: Recover Production** to jump directly to the production recovery stage of recovering production from the copy image that you tested earlier (step 8), without requiring to roll back the writes that were made to the copy snapshot while write access to the copy volumes was enabled.

If you tested a copy of a group set:

Recovery Activities

Consistency Groups Groups Sets

Search

Recovery Activity	vRPA Cluster	Consistency Groups	Activity Start	Activity Status	Progress
Test Copy - group-set	NASA_Site2	2/2	May 25, 2020 6:21:50 PM	Ready for next action	<div style="width: 100%;">100%</div>
<b>Summary:</b> <a href="#">Detailed Status OPEN</a> Excluded Groups: 0/2 Testing Network: Isolated per group Preparing snapshot...: 0/2 User Prompts: None Powering on VMs...: 0/2 Ready for next action: 2/2					

Items per page: 20

1 Recovery activity

- Click **OPEN** to display a **Detailed Status** for each group in the group set. The **Detailed Status** screen is displayed.

**i | NOTE:** Groups in the group set without a copy at the specified vRPA cluster are excluded from the activity.

### Detailed Status of 'group-set'

X

Search

Consistency Groups	Copy	Snapshot	Status	Progress
cg_Win_286	Local Copy	May 25, 2020 6:17:0...	Ready for next action	<div style="width: 100%;">100%</div>
cg_Win	Remote Copy	May 25, 2020 6:17:0...	Ready for next action	<div style="width: 100%;">100%</div>

Items per page: 10

2 Detailed Statuses

CLOSE

- Click **ACTIONS > Stop activity** to roll back all writes that were made to the copy snapshot while access was enabled to the copy volumes, and disable access to the copy volumes.

If you tested a copy of a consistency group:

Recovery Activities						
Consistency Groups		Groups Sets				
▼	Test Copy - cg_KATE_VM_13...	Copy	Snapshot	Activity Start	Activity Status	Progress
			Nov 23, 2020 11:55:47 AM	Nov 23, 2020 11:55:48 AM	Ready for next action	<div style="width: 100%;">100%</div>
						<b>ACTIONS</b> ▾
						<a href="#">Start new test</a>
						<a href="#">Stop activity</a>
						<a href="#">Promote Image</a>
						<a href="#">Failover</a>
						<a href="#">Recover Production</a>
	Items per page	20 ▾				

The **Consistency Group Recovery Activities** screen is displayed. The **Activity Status** and **Progress** columns indicate the progress of image access. After access is enabled to the copy snapshot, the **Activity Status** column displays **Ready for next action**, and you can:

**NOTE:** The **Image Access Log Capacity** progress bar indicates how long you can access the copy image before the image access log is full and all writes to the copy fail. If you need more time for testing, you can undo writes at the copy, enable direct access to the copy, or add journal volumes as described in [Managing group protection policies](#).

- Click **UNDO WRITES** to undo all writes that were made to the copy snapshot while write access was enabled, without disabling access to the copy volumes.
- Click **ENABLE DIRECT ACCESS** to write directly to the copy storage. Any changes that are made to the copy storage while directly accessing the copy cannot be automatically undone, because when a snapshot is directly accessed, the journal at the copy is deleted. Also direct access does not impose a limit to the amount of data that you can write to the copy storage volumes.

**CAUTION:** When direct access is enabled, replication stops to the copy, and a short initialization is required across all group volumes when direct access is disabled.

- Click **ACTIONS** > **Start new test** to select another snapshot to test, or to redefine the testing network.
- Click **ACTIONS** > **Stop activity** to roll back all writes that were made to the copy snapshot while write access was enabled to the snapshot volumes, and disable write access to the snapshot volumes.
- Click **ACTIONS** > **Promote image: Failover** to jump directly to the Failover stage of failover to the copy image that you tested now (step 8), without requiring to roll back the writes that were made to the copy snapshot while write access was enabled.
- Click **ACTIONS** > **Promote image: Recover Production** to jump directly to the production recovery stage of recovering production from the copy image that you tested now (step 8), without requiring to roll back the writes that were made to the copy snapshot while write access to the copy volumes was enabled.

If you tested a copy of a group set:

Recovery Activities						
Consistency Groups		Groups Sets				
▼	Test Copy - group-set	vRPA Cluster	Consistency Groups	Activity Start	Activity Status	Progress
		NASA_Site2	2/2	May 25, 2020 6:21:50 PM	Ready for next action	<div style="width: 100%;">100%</div>
						<b>ACTIONS</b> ▾
						<a href="#">Stop activity</a>
	Summary:	Detailed Status	OPEN			
	Excluded Groups: 0/2	Testing Network:	Isolated per group			
	Preparing snapshot...: 0/2	User Prompts:	None			
	Powering on VMs...: 0/2					
	Ready for next action: 2/2					
	Items per page	20 ▾				1 Recovery activity

- Click **OPEN** to display a **Detailed Status** for each group in the group set. The **Detailed Status** screen is displayed.

**NOTE:** Groups in the group set without a copy at the specified vRPA cluster are excluded from the activity.

Detailed Status of 'group-set'

Search

Consistency Groups	Copy	Snapshot	Status	Progress
cg_Win_286	Local Copy	May 25, 2020 6:17:0...	Ready for next action	<div style="width: 100%;">100%</div>
cg_Win	Remote Copy	May 25, 2020 6:17:0...	Ready for next action	<div style="width: 100%;">100%</div>

Items per page: 10 ▾ 2 Detailed Statuses

CLOSE

- Click **ACTIONS > Stop activity** to roll back all writes that were made to the copy snapshot while access was enabled to the copy volumes, and disable access to the copy volumes.

If you tested a copy of a consistency group:

Recovery Activities

Consistency Groups Groups Sets

cg\_KATE\_VM\_1309

Recovery Activity	Copy	Snapshot	Activity Start	Activity Status	Progress
Test Copy - cg_KATE_VM_13...	Local Copy (NASA_Site1)	Nov 23, 2020 11:55:47 AM	Nov 23, 2020 11:55:48 AM	Ready for next action	<div style="width: 100%;">100%</div>

Image Access Log Capacity: 4% Testing Network: Isolated per group  
UNDO WRITES ENABLE DIRECT ACCESS User Prompts: None

Journal Capacity: 3%

Items per page: 20 ▾

ACTIONS ▾

- Start new test
- Stop activity
- Promote Image
- Failover
- Recover Production

The **Consistency Group Recovery Activities** screen is displayed. The **Activity Status** and **Progress** columns indicate the progress of image access. After access is enabled to the copy snapshot, the **Activity Status** column displays **Ready for next action**, and you can:

**NOTE:** The **Image Access Log Capacity** progress bar indicates how long you can access the copy image before the image access log is full and all writes to the copy fail. If you need more time for testing, you can undo writes at the copy, enable direct access to the copy, or add journal volumes as described in [Managing group protection policies](#).

- Click **UNDO WRITES** to undo all writes that were made to the copy snapshot while write access was enabled, without disabling access to the copy volumes.
- Click **ENABLE DIRECT ACCESS** to write directly to the copy storage. Any changes that are made to the copy storage while directly accessing the copy cannot be automatically undone, because when a snapshot is directly accessed, the journal at the copy is deleted. Also direct access does not impose a limit to the amount of data that you can write to the copy storage volumes.

**CAUTION:** When direct access is enabled, replication stops to the copy, and a short initialization is required across all group volumes when direct access is disabled.

- Click **ACTIONS > Start new test** to select another snapshot to test, or to redefine the testing network.
- Click **ACTIONS > Stop activity** to roll back all writes that were made to the copy snapshot while write access was enabled to the snapshot volumes, and disable write access to the snapshot volumes.
- Click **ACTIONS > Promote image: Failover** to jump directly to the Failover stage of failover to the copy image that you tested now (step 8), without requiring to roll back the writes that were made to the copy snapshot while write access was enabled.

- Click **ACTIONS > Promote image: Recover Production** to jump directly to the production recovery stage of recovering production from the copy image that you tested now (step 8), without requiring to roll back the writes that were made to the copy snapshot while write access to the copy volumes was enabled.

If you tested a copy of a group set:

Recovery Activities

Consistency Groups Groups Sets

Search

Recovery Activity	vRPA Cluster	Consistency Groups	Activity Start	Activity Status	Progress
Test Copy - group-set	NASA_Site2	2/2	May 25, 2020 6:21:50 PM	Ready for next action	100%
<b>Summary:</b> Detailed Status <b>OPEN</b> Excluded Groups: 0/2 Testing Network: Isolated per group Preparing snapshot...: 0/2 User Prompts: None Powering on VMs...: 0/2 Ready for next action: 2/2					

Items per page: 20 1 Recovery activity

- Click **OPEN** to display a **Detailed Status** for each group in the group set. The **Detailed Status** screen is displayed.

**NOTE:** Groups in the group set without a copy at the specified vRPA cluster are excluded from the activity.

Detailed Status of 'group-set'

Search

Consistency Groups	Copy	Snapshot	Status	Progress
cg_Win_286	Local Copy	May 25, 2020 6:17:0...	Ready for next action	100%
cg_Win	Remote Copy	May 25, 2020 6:17:0...	Ready for next action	100%

Items per page: 10 2 Detailed Statuses

CLOSE

- Click **ACTIONS > Stop activity** to roll back all writes that were made to the copy snapshot while access was enabled to the copy volumes, and disable access to the copy volumes.

After finding an appropriate snapshot, [Create a bookmark](#) to label the snapshot so it is conveniently identifiable for recovery.

## Manage failover and fallback

Manage the ongoing failover or fallback of a copy of a consistency group or group set using the **Recovery Activities** screen.

**NOTE:** When failing over (or failing back) to a copy, wait for the **Activity Status** to show **Ready for next action** and the **Progress status bar** to reach 100%, indicating the specified snapshot image has been accessed.

When the **Activity Status** is **Ready for next action**, do one of the following:

To select a consistency group for failover, ensure the **Consistency Groups** tab is selected.

**i NOTE:** By default, replication starts immediately after failover. In RecoverPoint for Virtual Machines 5.3.1 and later versions, disable **Start transfer** before failing over to pause replication after failover.

- Click **ACTIONS** > **Start new test** to select another snapshot to test, or to redefine the testing network.
  - Click **ACTIONS** > **Stop activity** to roll back all writes that were made to the copy snapshot while write access was enabled to the snapshot volumes, and disable write access to the snapshot volumes.
  - (Optional) Click **UNDO WRITES** to undo all writes that were made to the copy snapshot while write access was enabled, without disabling access to the copy volumes.
  - (Optional) Click **ENABLE DIRECT ACCESS** to write directly to the copy storage. Any changes that are made to the copy storage while directly accessing the copy cannot be automatically undone, because when a snapshot is directly accessed, the journal at the copy is deleted. Also direct access does not impose a limit to the amount of data that you can write to the copy storage volumes.

 **CAUTION:** When direct access is enabled, replication stops to the copy, and a short initialization is required across all group volumes when direct access is disabled.

- In **Failover Networks**, you can use the default preconfigured failover networks, by keeping **Use or edit pre-configured failover networks** selected. You can also edit a preconfigured network, or choose to **Use current testing networks**.

**NOTE:** The **Image Access Log Capacity** progress bar indicates how long you can access the copy image before the image access log is full and all writes to the copy fail. If you need more time for testing, you can undo writes at the copy, enable direct access to the copy, or add journal volumes as described in [Managing group protection policies](#).

To select a group set for failover, click the **Group Sets** tab.

Recovery Activities						
Consistency Groups		Groups Sets		Actions		
	Recovery Activity	vRPA Cluster	Consistency Groups	Activity Start	Activity Status	Progress
▼	Failover - GS1	Site1	2/2	Jul 18, 2021 8:23:39 PM	Ready for next action	<div style="width: 100%;"> </div> 50%
	<strong>Summary:</strong>		<strong>Detailed Status</strong>	<strong>OPEN</strong>		
	Excluded Groups:	0/2	Testing Network:	Isolated per ESX		
	Preparing snapshot:	0/2	<input checked="" type="button"/> Start transfer			
	Powering on VMs:	0/2	User Prompts:	None		
	Ready for next action:	2/2				

- Click **OPEN** to display the **Detailed Status** of all consistency groups in the group set. After access is enabled to the copy snapshot, the **Status** column of all groups displays **Ready for next action**.

**i** **NOTE:** Groups in the group set without a copy at the specified vRPA cluster are excluded from the activity.

Detailed Status of 'group-set' X

Search

Consistency Groups	Copy	Snapshot	Status	Progress
cg_Win_286	Local Copy	May 26, 2020 2:04:2...	Ready for next action	<div style="width: 100%;">100%</div>
cg_Win	Standalone	May 26, 2020 2:06:1...	Ready for next action	<div style="width: 100%;">100%</div>

Items per page 10 2 Detailed Statuses

**CLOSE**

- Click **ACTIONS > Stop activity** to roll back all writes that were made to the copy snapshot while access was enabled to the copy volumes, and disable access to the copy volumes.

**i** **NOTE:** After finding an appropriate snapshot, you may want to [Create a bookmark](#) to label the snapshot so it is conveniently identifiable during failover.

Click **ACTIONS > Failover** to failover to the copy.

- If the selected consistency group or group set has only one copy, failover starts.
  - The role of the **Production** becomes **Remote/Local Copy**.
  - The role of the **Remote/Local Copy** becomes **Production**.
  - The production VM and copy VM change roles, but their names do not change. Therefore, after failover, new production VMs will still be named *YourVMName*.copy and the new copy VMs are still named *YourVMName*.
  - The production journal becomes the copy journal, and the copy journal becomes the production journal. You may want to add journal volumes as described in [Managing group protection policies](#).
  - The marking information in the production journal is deleted, the copy journal is deleted, and the consistency group undergoes a full sweep.

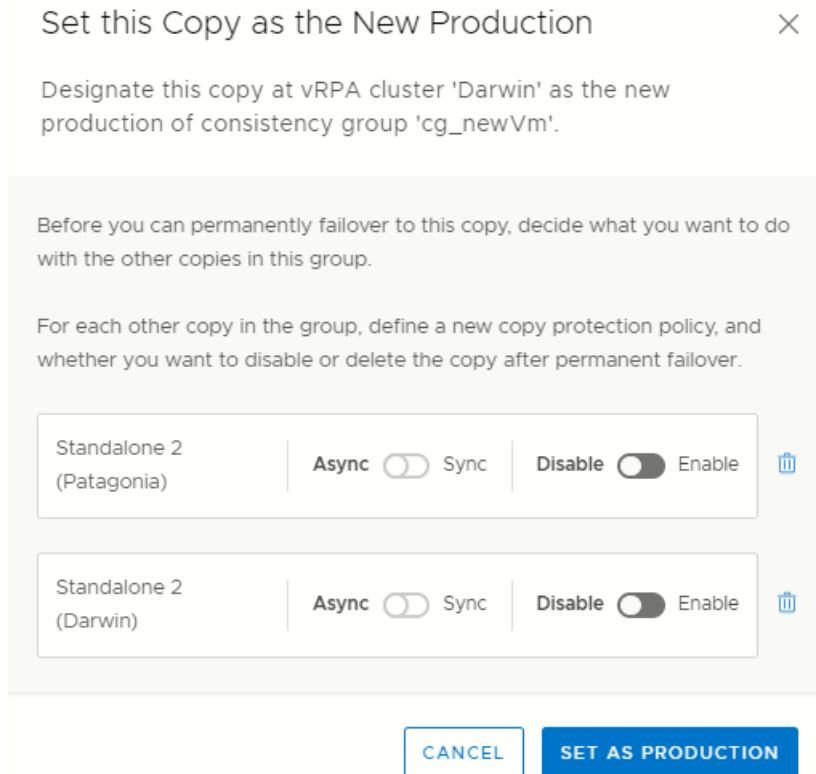
**⚠ CAUTION: During the full sweep, data is not transferred synchronously.**

- If the consistency group or group set has copies other than the copy to which you are failing over (even if they are disabled or replication to them is paused), a temporary failover begins:
  - The role of the **Production** changes to **Temporary Production**.
  - The role of the **Remote/Local Copy** changes to **Temporary Remote/Local Copy**.
  - The roles of any other (unlinked) copies become **Standalone**.
  - Replication pauses for the other copies and the direction of replication between the production and the failed-over copy changes.

After temporary failover, if your consistency group or group set had more than one copy (even if they are disabled or replication to them is paused), in the **Recovery Activities** screen:

- Fallback to the original production.**
  - Select the recovery activity, click **ACTIONS > Test for failback** and run the above procedure beginning with step 3, substituting "failback" for "failover" throughout.
  - After failing back to the production, if you added volumes to the production journal after failover, to reset the production journal to its original size (by default, 3 GB) without triggering a full sweep click **Protection > Consistency Groups > PROTECTION POLICY**, select the **Production** copy of the group, and click **RESET SIZE** in the **Journal Volumes** section.
- Set the copy as the new production.** Select the recovery activity and click **ACTIONS > Set as production**. If there are stand-alone (unlinked) copies, the **Set this Copy as the New Production** dialog is displayed.

In the **Set this Copy as the New Production** dialog for consistency groups:



1. Configure each stand-alone copy for consistency groups (or all stand-alone copies for group sets).

Standalone copies are not linked to the production, and you must decide how to handle them before failover. By default, RecoverPoint for Virtual Machines does not delete copy VMs but it does disable them. You can **Enable** any required standalone copies and select a replication mode (sync or async), or **Delete** them from the consistency group. Deleting a copy does not delete the VMs from storage.

**CAUTION:** Disabled copy VMs require a full sweep when they are reenabled.

2. Click **SET AS PRODUCTION** to permanently failover.

- The role of the **Production** becomes **Remote/Local Copy**.
- The role of the **Remote/Local Copy** becomes **Production**.
- The stand-alone copies are handled as specified.
- The production VM and copy VM change roles, but their names do not change. Therefore, after failover, new production VMs will still be named *YourVMName*.copy and the new copy VMs are still named *YourVMName*.
- The production journal becomes the copy journal, and the copy journal becomes the production journal. The production journal does not contain the copy history, so it is by default, a relatively smaller journal. Therefore, after failover, when the production becomes the copy, you may want to add journal volumes to the new copy journal to ensure that you have ample space for copy testing. For detailed instructions on how to add journal volumes to a copy journal, see [Managing group protection policies](#)
- The marking information in the production journal is deleted, the journal of the copy to which you failed over is deleted, and the consistency group undergoes a full sweep.

**CAUTION:** During the full sweep, data is not transferred synchronously.

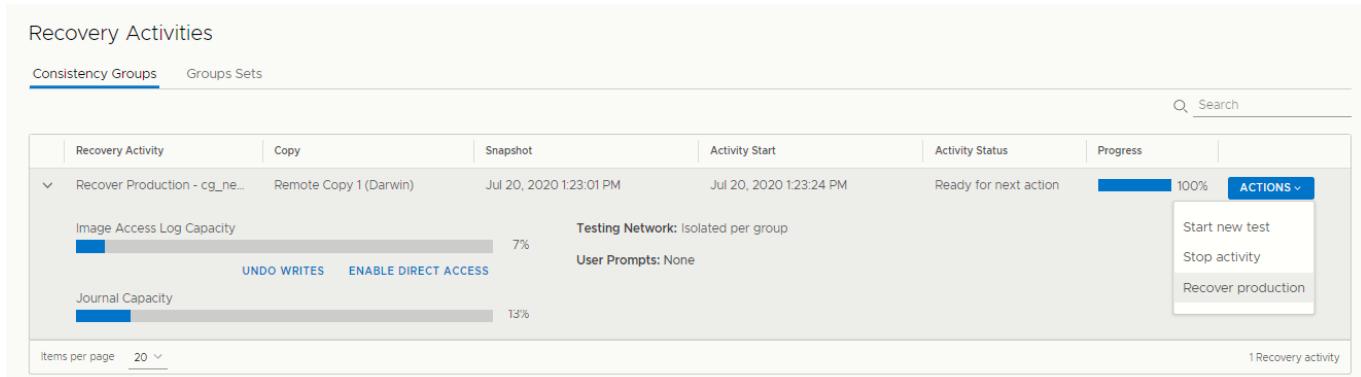
# Manage production recovery

Manage the ongoing recovery of a copy of a consistency group or group set from the production using the **Recovery Activities** screen.

**NOTE:** When recovering of a copy from the production, wait for the **Activity Status** to show **Ready for next action** and the **Progress status bar** to reach 100%, indicating the specified snapshot image has been accessed.

When the **Activity Status** is **Ready for next action**:

- To select a consistency group for production recovery, ensure the **Consistency Groups** tab is selected.



Recovery Activity	Copy	Snapshot	Activity Start	Activity Status	Progress
Recover Production - cg_ne...	Remote Copy 1 (Darwin)	Jul 20, 2020 1:23:01 PM	Jul 20, 2020 1:23:24 PM	Ready for next action	<div style="width: 100%;">100%</div>

Items per page: 20

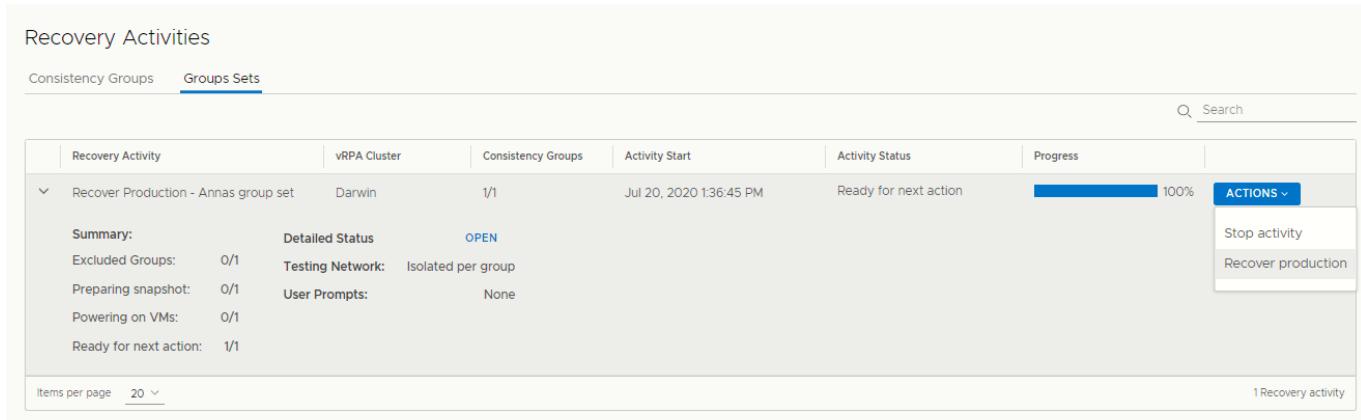
1 Recovery activity

- Click **ACTIONS** > **Start new test** to select another snapshot to test, or to redefine the testing network.
- Click **ACTIONS** > **Stop activity** to roll back all writes that were made to the copy snapshot while write access was enabled to the snapshot volumes, and disable write access to the snapshot volumes.
- (Optional) Click **UNDO WRITES** to undo all writes that were made to the copy snapshot while write access was enabled, without disabling access to the copy volumes.
- (Optional) Click **ENABLE DIRECT ACCESS** to write directly to the copy storage. Any changes that are made to the copy storage while directly accessing the copy cannot be automatically undone, because when a snapshot is directly accessed, the journal at the copy is deleted. On the other hand, direct access does not impose a limit to the amount of data that you can write to the copy storage volumes.

**CAUTION:** When direct access is enabled, replication stops to the copy, and a short initialization is required across all group volumes when direct access is disabled.

**NOTE:** The **Image Access Log Capacity** progress bar indicates how long you can access the copy image before the image access log is full and all writes to the copy fail. If you need more time for testing, you can undo writes at the copy, enable direct access to the copy, or add journal volumes as described in [Managing group protection policies](#).

- To select a group set for production recovery, click the **Group Sets** tab.



Recovery Activity	vRPA Cluster	Consistency Groups	Activity Start	Activity Status	Progress
Recover Production - Annas group set	Darwin	1/1	Jul 20, 2020 1:36:45 PM	Ready for next action	<div style="width: 100%;">100%</div>

Items per page: 20

1 Recovery activity

- Click **OPEN** to display the **Detailed Status** of all consistency groups in the group set. After access is enabled to the copy snapshot, the **Status** column of all groups displays **Ready for next action**.

**NOTE:** Groups in the group set without a copy at the specified vRPA cluster are excluded from the activity.

Detailed Status of 'group-set' X

Consistency Groups	Copy	Snapshot	Status	Progress
cg_Win_286	Local Copy	May 26, 2020 2:04:2...	Ready for next action	<div style="width: 100%;">100%</div>
cg_Win	Standalone	May 26, 2020 2:06:1...	Ready for next action	<div style="width: 100%;">100%</div>

Items per page: 10 ▼ 2 Detailed Statuses

CLOSE

- Click **ACTIONS > Stop activity** to roll back all writes that were made to the copy snapshot while access was enabled to the copy volumes, and disable access to the copy volumes.

To recover production from the copy click **ACTIONS > Recover production**.

**NOTE:**

- Data transfer from the production to all copies is paused, and will resume only after production recovery is complete.
- Host access to the recovered production volumes and the recovering copy volumes is blocked.
- Recovered production volumes are overwritten. Any writes made to the copy during testing are transferred to the production, unless you clicked **UNDO WRITES**.
- The group undergoes a short initialization process to synchronize the new production data at the copy.

## Configuring email alerts and reports

Run a series of **Sysmgmt CLI** commands to configure your system to send system alerts and reports to a specified email, in real time.

### Prerequisites

Create an SSH connection to a vRPA cluster management IP address, and use your R RecoverPoint for Virtual Machines **admin** username and password to log into the **Admin CLI > Sysmgmt CLI**.

### About this task

**NOTE:** For more information, see the *Dell RecoverPoint for Virtual Machines CLI Reference Guide*.

### Steps

1. Set up email access using the Sysmgmt CLI:
  - a. Run the **set\_smtp\_server** command, and enter the IP address or DNS name for sending email notifications. You should receive confirmation that the SMTP server has been configured successfully.
  - b. Run the **config\_email** command, and provide the requested information. You should receive confirmation that your email mechanism has been successfully configured.
  - c. Run the **enable\_email** command, and choose the **enable\_email** option. You should receive confirmation that email alerts have been enabled successfully.
2. (Optional) To add email users, run the **add\_email\_users** command, and provide the requested information. You should receive confirmation that email users have been added successfully.

### Results

Your email alerts and reports are configured.

## Next steps

See the [Monitor system alerts](#) for more information.

# Troubleshooting

Use the following information, features and tools to troubleshoot your RecoverPoint for VMs .

## Topics:

- [Finding the vRPA cluster management IP](#)
- [Collecting logs](#)
- [Adding new VMDKs](#)
- [Removing a VMDK](#)
- [Automatically expanding copy VMDKs](#)
- [Recovering from a cluster disaster](#)
- [RecoverPoint for VMs licensing](#)
- [XML license](#)
- [Creating VMkernel ports](#)
- [Load balancing](#)
- [Copy VM network configuration guidelines](#)
- [Changing the network adapter configuration of a protected VM](#)

## Finding the vRPA cluster management IP

Displays the vRPA cluster management IP of a specific vRPA cluster.

### Steps

1. In the vSphere HTML5 plugin, select **System > Administration**, and the **vRPA Clusters** tab.
2. Select the vRPA cluster.
3. Note the **Management IP Address** for the selected vRPA cluster.

## Collecting logs

Collecting logs is relevant only in support cases, and should be performed only when instructed to do so by Customer Support.

## Collecting logs from vRPA clusters

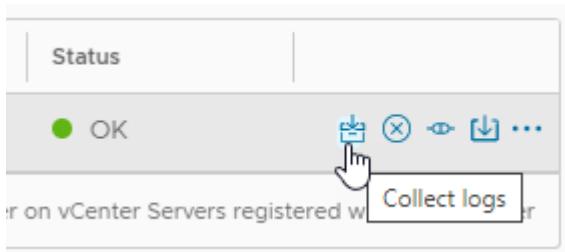
You can initiate the log collection process from within the RecoverPoint for VMs vSphere plugin.

### About this task

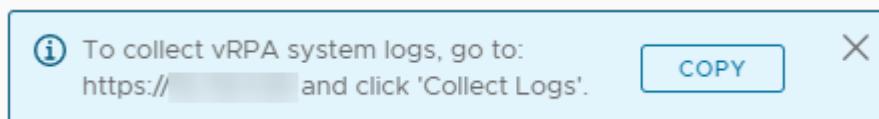
Logs can be collected from one or more vRPAs in multiple vRPA clusters, if they all reside on a vCenter Server registered with the plugin server, or a vCenter server that is linked to a vCenter Server that is registered with the plugin server.

### Steps

1. Click **System > Administration > vRPA Clusters**.
2. Select a vRPA cluster and click the **Collect logs** icon.



3. In the system notification that is displayed, click **Copy**, open a browser window, and paste the copied URL into the browser address bar.

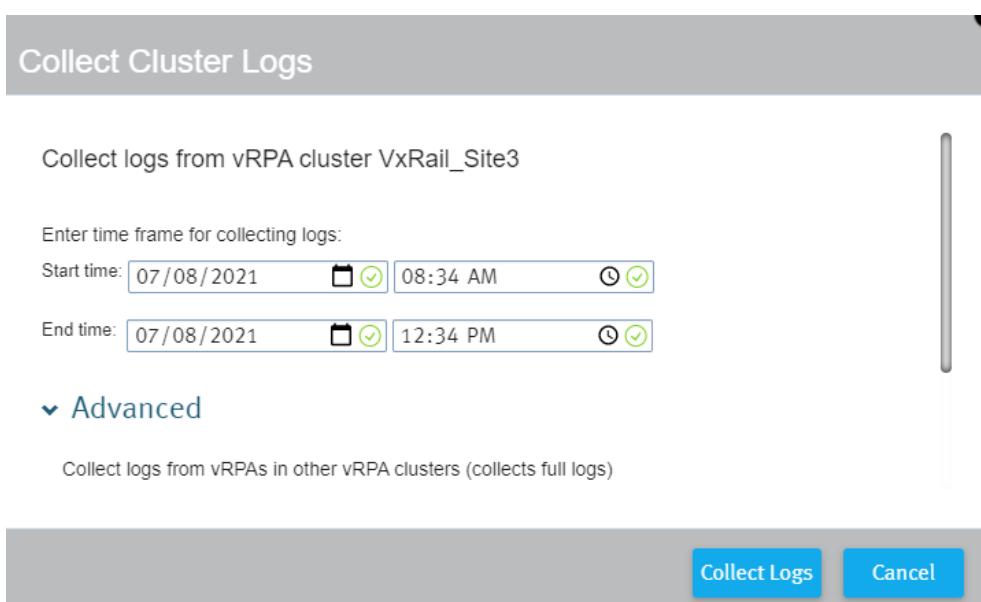


4. If prompted, type the login credentials for the **admin** user and click **Sign in**.
5. In the **RecoverPoint for VMs Deployer**, click **Collect Logs**.



**Figure 13. RecoverPoint for VMs Deployer 6.0.3**

The **Collect Cluster Logs** dialog is displayed.



In the **Collect Cluster Logs** dialog:

- a. Enter a time span for log collection.
- b. (Optional) Enter the IP addresses of other vRPA clusters from which to collect logs in the **Advanced** section.
- 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 (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
<a href="#">ic_report</a>	4.4 kb	Mon, 12 Jul 2021 15:32:29 GMT
<a href="#">sysInfo-incomplete-Site1_KBox-1-2-2021.07.12.15.29.35.tar</a>	198360.0 kb	Mon, 12 Jul 2021 15:32:29 GMT
<a href="#">long_term_stats/</a>		Mon, 12 Jul 2021 15:30:49 GMT

## Collecting RecoverPoint for VMs splitter logs

### About this task

RecoverPoint for VMs splitter logs are in the ESXi logs. To export the ESXi system logs, use the following procedure.

### Steps

1. In the vSphere Client, select **Menu > Home and Clusters**.
2. Right click on the desired vCenter, and select **Export System Logs....**
3. In the **Select hosts** pane of the **Export System Logs** screen:
  - a. Select the ESXi hosts for which you want to export the system logs.
  - b. (Optional) Select **Include vCenter and vSphere UI Client logs**.
  - c. Select the system logs to be exported
  - d. (Optional) Select **Gather performance data**, and specify a duration and interval
  - e. (Optional) Set a password with which to encrypt the collected log data.
4. In the **Select logs** pane of the **Export System Logs** screen:
  - a. Select the system logs to be exported
  - b. (Optional) Select **Gather performance data**, and specify a duration and interval
  - c. (Optional) Set a password with which to encrypt the collected log data.

5. Click **EXPORT LOGS**.

## Adding new VMDKs

Best practices and system behavior when adding new VMDKs to a protected VM.

### About this task

RecoverPoint for Virtual Machines automatically detects when a new VMDK is added to a protected VM through the vSphere Client VM Properties, and by default, automatically starts protecting each added VMDK.

### Steps

- To disable automatic protection for all VMDKs added to a protected VM in the future, see [Automatic protection of newly added VMDKs](#).
- To exclude specific VMDKs of a protected VM from protection, see [Excluding a VMDK from replication](#).

### Results

When a new VMDK is added to a protected VM, a volume sweep occurs on the added VMDK and a short initialization occurs on all other VMDKs in the consistency group, but no history is lost.

## Removing a VMDK

Defines how to handle a VMDK which was removed from a protected VM, at the copy.

### About this task

RecoverPoint for VMs automatically detects when a VMDK is removed from a protected VM through the vSphere Client, and displays an alert when there is hardware mismatch between a protected VM and its copy VM.

 **NOTE:** Removing VMDKs from a protected VM does not delete their copies and does not remove their history from the copy journal.

### Steps

- If the production VMDK removal was intentional, follow the instructions in [Excluding a VMDK from replication](#) to stop protecting it.
- If the production VMDK removal was unintentional, run [Recover production from a copy](#) to recover the removed VMDK. For recover production, select a snapshot that predates VMDK removal.

## Automatically expanding copy VMDKs

Best practices, troubleshooting, system behavior, and limitations of automatically expanding copy VMs when a protected VM is expanded.

### About this task

When a protected VMDK is expanded, RecoverPoint for Virtual Machines automatically expands all corresponding copy VMDKs, with the following limitations:

### Steps

- VMDKs can be expanded, but they cannot be shrunk.
- When a production VMDK is expanded, the system pauses replication of the consistency group while the system is busy resizing the corresponding copy VMDK.
- Automatic VMDK expansion fails if:
  - Replicating to VMDK. After expanding the production VMDK, you must manually expand the copy VMDK.
  - The datastore does not contain enough free space, and you should free up space in the copy VM datastore.

- A snapshot has been taken of the virtual machine containing the copy VMDK. Enable access to the copy containing the VMDK and use the vCenter snapshot manager to delete all snapshots before disabling image access.
- The version of the file system that you are running does not support the VMDK size. In this case, consider upgrading the file system version.
- The size of a copy VMDK is larger than the size of its corresponding production VMDK. In this case, to begin the automatic VMDK expansion process, you must manually expand the production VMDK. This manual expansion might be required if you failed over while automatic expansion was in progress, or if the copy VMDK was manually expanded.
- Replicating to VMDK. After expanding the production VMDK, you must manually expand the copy VMDK for replication to resume.
- A snapshot of a copy containing a VMDK marked for automatic expansion is selected during testing or recovery. In this case, you should disable image access for replication to resume.
- A protected VMDK is smaller than the size registered in the system settings. In this case, you should contact Customer Support. This instance occurs in situations when a production VMDK is removed and readded with a smaller size.
- One or more copy VMDKs have been marked for automatic expansion, but the system cannot automatically resize a RAW device. In this case, enable access to the copy VM with the problematic VMDK and manually expand it before disabling image access. If problem persists, contact Customer Support.

## Results

After fixing any of these issues, wait 15 minutes for the automatic expansion process to restart and the error to resolve itself. If the problem persists, try manually resizing the copy VMDKs or contact Customer Support.

## Recovering from a cluster disaster

After a full cluster disaster or a switch disaster, it may take 10 minutes or more for all the components of the vRPA system to restart, reconnect, and restore full operation.

## RecoverPoint for VMs licensing

RecoverPoint for VMs supports two types of licensing models; VM-based licensing and socket-based licensing .

### VM-based licensing

With VM-based licensing, licenses are based on the number of supported VMs per vCenter Server. Only production VMs are counted in the number of supported VMs per vCenter Server. Licensing is enforced using the vCenter Server ID.

All vCenter Servers must be registered in RecoverPoint for VMs before their licenses can be added. vCenter Server registration is performed in the RecoverPoint for VMs Deployer UI. See the *RecoverPoint for VMs Installation and Deployment Guide* for more information.

You can use the HTML5 plugin to register additional vCenter Servers. For details, see [Register vCenter Server to vRPA cluster](#).

When you reach the maximum number of VMs that the license supports for each vCenter Server, you cannot protect new VMs or enable disabled consistency groups. However, replication of existing VMs and consistency groups continues.

Failover has no effect on the license.

### Socket-based licensing

With socket-based licensing, licenses are based on the number of physical CPU sockets in the ESXi hosts that host the production VMs. A VM does not 'belong' to a specific socket.

When you reach the maximum number of sockets that the license supports for each vCenter Server, you cannot protect new VMs or enable disabled consistency groups. However, replication of existing VMs and consistency groups continues.

As with VM-based licensing, failover does not affect the socket-based license. However, vMotion of production VMs does affect the license and may cause a license violation due to an increase in the number of sockets being used. ESXi hosts that host the production VMs are the ones that count in a socket-based license. To avoid license violations, it is a best practice to license all ESXi hosts of the ESXi cluster.

## Adding a socket-based license to a system with VM-based licenses

When using VM-based licensing, license capacity is measured by the number of VMs. For example, when you view the license capacity in the UI, it may be listed as:

```
Capacity = 30 VMs
```

When using socket-based licensing, license capacity is measured by the number of sockets. For example, the license capacity may be listed as:

```
Capacity = 2 sockets
```

When a socket-based license is installed on a RecoverPoint for VMs system that has VM-based licenses, the system automatically converts VM-based licenses to socket-based licenses at a ratio of 15 VMs per socket. In this case, the license capacity would be listed as:

```
Capacity = 30 VMs (2 sockets)
```

In cases where the ratio does not result in an even conversion, the value is rounded up. For example:

```
Capacity = 31 VMs (3 sockets)
```

Since licenses are applied per vCenter, and not per vRPA cluster, multiple vRPA clusters with VMs or CPU sockets may count towards the same license.

**(i) NOTE:** On fresh deployment 6.0 SP2 only supports XML licenses. After NDU, all the existing Flexera licenses must be converted to XML license as mentioned in section Flex to XML license conversion.

## XML license

XML licenses are generated using unique Locking ID (VC UUID). Once a Locking ID is entered during initial activation, the Locking ID stays assigned to that machine for the life of that machine. It becomes its fingerprint.

If a user then tries to reuse that same Locking ID again, it is combined or appended to the existing license. It never creates a new license with an identical Locking ID.

### Feature codes in XML license

VMBL and SBL licenses are differentiated based on feature codes.

#### Codes :

VC.SYS.00 → VM-based licensing

VC.SYS.00-Socket → Socket-based licensing

### XML License type

1. Subscription License

2. Permanent License

3. Evaluation License

#### Subscription License

- **Subscription Start Date** – This is the date of order fulfillment/entitlement creation.

- **Subscription End Date** – Calculated based on the duration received from the order payload.

- **Grace Date** – Calculated 14 days from Subscription End Date.

In case of Subscription, the Qty is not summed and instead will have separate <LicenseKey> sections for possible SAME License <FeatureCode> components with their own unique subscription dates.

If the Start and end date are identical, then the Qty is summed into a single <LicenseKey>.

**i** **NOTE:** LicenseKeys are dropped from the license file if a license transaction is processed against a machine when the entitlement has passed the Grace Period date. If a renewal is activated to a machine with existing subscription LicenseKeys that have not yet reached the Grace Period, then all old + new renewal LicenseKeys will be listed within the license file.

A subscription license can be installed before the start date. It automatically becomes active on the start date.

VM- and socket-based licenses may be installed as subscriptions. Unlike a permanent license, a subscription license has a start date and an end date. The system sends an alert beginning 30 days before license expiration to indicate the number of days remaining. Subscription and permanent licenses may co-exist.

#### Permanent License

In case of Permanent, the Qty is summed into a single <LicenseKey> because the component/feature/key attributes are identical.

#### Evaluation License

In case of Evaluation, the license is raised with the Expiration date, that is the date after which the license expires.

**i** **NOTE:** Multiple License type is supported within the same entitlement, that is, Evaluation + Permanent + Subscription type license features within the same license file.

## Flex to XML license conversion

Steps:

1. Upgrade vRPA clusters, splitter, and JAM VIBs to RecoverPoint for VMs version 6.0.SP2.
2. Raise request for XML license conversion using VC UUIDs as Locking IDs.
3. In the vSphere Client, click **System > Licenses**.
4. Click **Add**, select the converted license, and click **Add license** to add the selected license.

**i** **NOTE:** The Qty is summed into a single <LicenseKey> if the component, feature, and key attributes are identical.

5. Delete all the licenses with license type as Flex.

## 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 to Remove Stale RP License Entries:

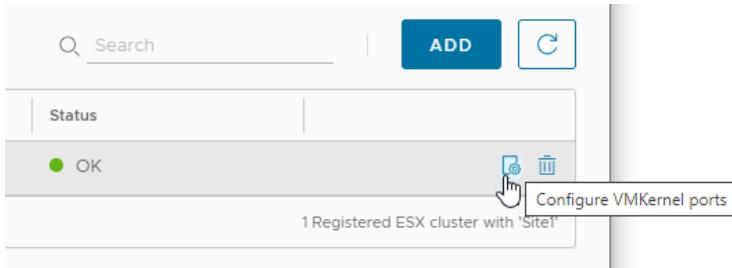
1. Verify and delete the custom attribute config.Recoverpoint\_LICENSES from VC:
  - Open **vSphere Client**.
  - Navigate to **Tags and Custom Attributes**.
  - Locate the custom attribute named config.Recoverpoint\_LICENSES.
  - Select this attribute and delete it.

## Creating VMkernel ports

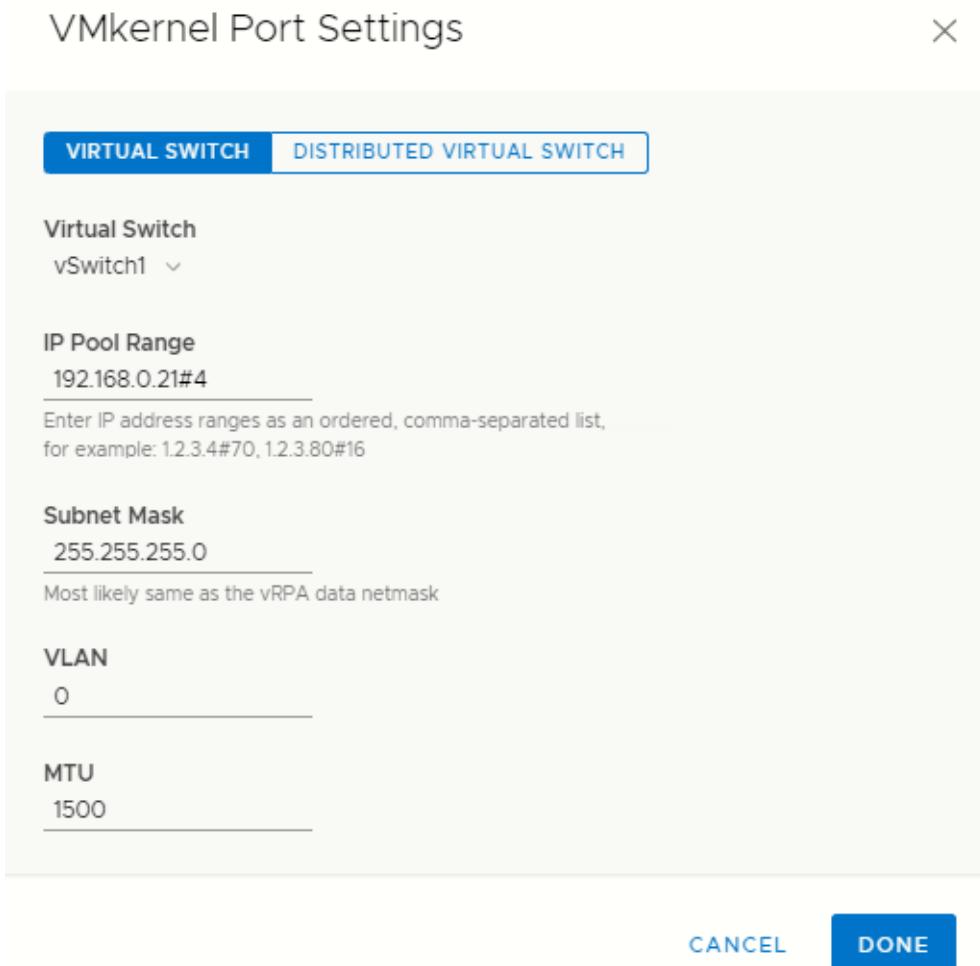
If before clicking **Protect** for VMs you received a warning regarding a potential communications problem, and after clicking **Protect**, transfer for the consistency group does not eventually reach the **Active** status, you must create VMkernel ports for all ESXi hosts in the cluster.

#### Steps

1. Select **System > ESX Clusters**, and click the **Configure VMkernel ports** icon of an ESXi cluster.



2. In the **VMkernel Port Settings** dialog box, specify the settings, including a range of available IPs, for creating VMkernel ports for all ESXi hosts in the cluster.



3. Click **DONE**

## Load balancing

### About this task

Load balancing is the process of assigning preferred vRPAs to consistency groups so that the preferred vRPA performs data transfer for that group. This is done to balance the load across the system and to prevent the system from entering a high-load state.

Perform load balancing:

- When a new consistency group is added to the system. Wait 1 week after the new group is added to accumulate enough traffic history before performing load balancing.
- When a new vRPA is added to a vRPA cluster. Perform load balancing immediately after the vRPA is added.

- If the system enters high load frequently. When load balancing is required, the event logs display a message indicating so. When you see this message, perform load balancing.
- Periodically, to ensure that the system is always handling distributing loads evenly. A script can be created to periodically perform load balancing.

### Steps

1. To balance the load on the vRPAs, use an ssh client to connect to the vRPA management IP address, and type the RecoverPoint `username` and `password` to log in to the CLI.
2. Run the `balance_load` command to balance the load. To view command parameters that can refine the search, run: `balance_load ?`

## Copy VM network configuration guidelines

Use the following guidelines for Re-IP rules

**Table 7. Virtual machine network settings available through the GUI**

Setting	Description	Guidelines
<b>(VM) Operating System</b>	The guest operating system of the specified VM.	<ul style="list-style-type: none"> <li>• Not customizable.</li> <li>• Automatically populated by the system.</li> <li>• Possible values are <i>Windows</i>, <i>Linux</i>, or <i>Unknown</i>.</li> </ul>
<b>(VM) Host Name</b>	The hostname of the specified VM.	<ul style="list-style-type: none"> <li>• Only mandatory for virtual machines with a Linux operating system.</li> <li>• Customizable.</li> <li>• Value can be retrieved from production VM using <b>Get Value from Production</b> or <b>Get All Values from Production</b>.</li> </ul>
<b>(VM) DNS Domain</b>	The DNS domain for the specified VM.	<ul style="list-style-type: none"> <li>• Only relevant (and mandatory) for virtual machines with a Linux operating system.</li> <li>• Value should be in the format <code>example.company.com</code>.</li> </ul>
<b>(VM) DNS Server(s)</b>	The global IP address that identifies one or more DNS servers for all adapters of the specified VM.	<ul style="list-style-type: none"> <li>• Only relevant for virtual machines with a Linux operating system.</li> <li>• Customizable.</li> <li>• Can be left blank.</li> <li>• This setting applies to all virtual network adapters of the specified VM.</li> <li>• Separate multiple values with a semicolon ( ; ).</li> <li>• Value can be retrieved from production VM using <b>Get Value from Production</b> or <b>Get All Values from Production</b>.</li> </ul>
<b>(VM) DNS Suffix(s)</b>	The global settings of the suffixes for the DNS servers of all adapters on both Windows and Linux virtual machines.	<ul style="list-style-type: none"> <li>• Customizable.</li> <li>• Can be left blank.</li> <li>• Value can be retrieved from production VM using <b>Get Value from Production</b> or <b>Get All Values from Production</b>.</li> </ul>
<b>(Adapter) IP Address</b>	IPv4 address for this virtual network adapter.	<ul style="list-style-type: none"> <li>• Can contain either a static IPv4 address or DHCP string.</li> <li>• Can be left blank when using IPv6.</li> <li>• Define one IPv4 address, one IPv6 address, or one of each, for the same virtual network adapter. Entering multiple IPv4 or IPv6 addresses for the same virtual network adapter is not supported.</li> <li>• Value can be retrieved from production VM using <b>Get Value from Production</b> or <b>Get All Values from Production</b>.</li> </ul>

**Table 7. Virtual machine network settings available through the GUI (continued)**

Setting	Description	Guidelines
<b>(Adapter) Subnet</b>	IPv4 subnet mask for this virtual network adapter.	<ul style="list-style-type: none"> <li>Mandatory when an <b>IP Address</b> is entered.</li> <li>Can be left blank when using IPv6.</li> <li>Value can be retrieved from production VM using <b>Get Value from Production</b> or <b>Get All Values from Production</b>.</li> </ul>
<b>(Adapter) Gateway(s)</b>	One or more IPv4 gateways for this virtual network adapter.	<ul style="list-style-type: none"> <li>Mandatory when an <b>IP Address</b> is entered.</li> <li>Can be left blank when using IPv6.</li> <li>Separate multiple values with a semicolon (;).</li> <li>Value can be retrieved from production VM using <b>Get Value from Production</b> or <b>Get All Values from Production</b>.</li> </ul>
<b>(Adapter) IPv6 Address</b>	IPv6 address for this virtual network adapter.	<ul style="list-style-type: none"> <li>Can contain either a static IPv6 address or its DHCP string.</li> <li>Can be left blank when using IPv4.</li> <li>Define one IPv4 address, one IPv6 address, or one of each, for the same virtual network adapter. Entering multiple IPv4 or IPv6 addresses for the same virtual network adapter is not supported.</li> <li>Value can be retrieved from production VM using <b>Get Value from Production</b> or <b>Get All Values from Production</b>.</li> </ul>
<b>(Adapter) IPv6 Subnet Prefix Length</b>	IPv6 subnet mask for this virtual network adapter.	<ul style="list-style-type: none"> <li>Customizable.</li> <li>Can be left blank when using IPv4.</li> <li>Value can be retrieved from production VM using <b>Get Value from Production</b> or <b>Get All Values from Production</b>.</li> </ul>
<b>(Adapter) IPv6 Gateway(s)</b>	One or more IPv6 gateways for this virtual network adapter.	<ul style="list-style-type: none"> <li>Customizable.</li> <li>Mandatory when an IPv6 format <b>IP Address</b> is entered.</li> <li>Can be left blank when using IPv4.</li> <li>Separate multiple values with a semicolon (;).</li> <li>Value can be retrieved from production VM using <b>Get Value from Production</b> or <b>Get All Values from Production</b>.</li> </ul>
<b>(Adapter) DNS Server(s)</b>	IP address of one or more DNS server(s) for this virtual network adapter.	<ul style="list-style-type: none"> <li>Can be left blank.</li> <li>Can contain one or more IPv4 DNS servers for each virtual network adapter (NIC).</li> <li>Applies only to the configured adapter when a value other than <b>Adapter ID 0</b> is defined.</li> <li>Separate multiple values with a semicolon (;).</li> <li>Value can be retrieved from production VM using <b>Get Value from Production</b> or <b>Get All Values from Production</b>.</li> </ul>
<b>(Adapter) NetBIOS</b>	Whether or not to activate NetBIOS on this virtual network adapter.	<ul style="list-style-type: none"> <li>Cannot be left blank.</li> <li>Only relevant for virtual machines running a Windows operating system.</li> <li>Default is <b>Enabled</b>.</li> <li>Net BIOS should be enabled.</li> <li>Valid values are <b>DISABLED</b>, <b>ENABLED</b>, <b>ENABLED_VIA_DHCP</b>.</li> </ul>
<b>(Adapter) Primary WINS</b>	Primary WINS server of this virtual network adapter.	<ul style="list-style-type: none"> <li>Relevant for windows virtual machines only.</li> <li>Customizable.</li> <li>Can be left blank.</li> </ul>

**Table 7. Virtual machine network settings available through the GUI (continued)**

Setting	Description	Guidelines
<b>(Adapter) Secondary WINS</b>	Secondary WINS server of this virtual network adapter.	<ul style="list-style-type: none"><li>• Relevant for windows virtual machines only.</li><li>• Customizable.</li><li>• Can be left blank.</li></ul>

**Table 8. Network settings only available through the JSON file**

Setting	Description	Guidelines
<b>CG ID</b>	The consistency group ID in the RecoverPoint for VMs system.	<ul style="list-style-type: none"><li>• Do not modify this field.</li><li>• Automatically populated by the system.</li><li>• Not customizable.</li><li>• Can be left blank.</li></ul>
<b>CG Name</b>	Name of the consistency group in the RecoverPoint for VMs system.	<ul style="list-style-type: none"><li>• Automatically populated by the system.</li><li>• Must be the name associated with the specified consistency ID in RecoverPoint for VMs.</li><li>• Customizable.</li><li>• Can be left blank.</li></ul>
<b>VC ID</b>	The vCenter Server ID in VMware.	<ul style="list-style-type: none"><li>• Do not modify this field.</li><li>• Automatically populated by the system.</li><li>• Not customizable.</li><li>• Can be left blank.</li></ul>
<b>VC Name</b>	The name of the vCenter Server hosting the virtual machine.	<ul style="list-style-type: none"><li>• Customizable.</li><li>• Can be left blank.</li></ul>
<b>VM ID</b>	The virtual machine ID that vCenter Server uses.	<ul style="list-style-type: none"><li>• Do not modify this field.</li><li>• Automatically populated by the system.</li><li>• Not customizable.</li><li>• Cannot be left blank.</li></ul>
<b>VM Name</b>	The name of the virtual machine.	<ul style="list-style-type: none"><li>• Customizable.</li><li>• Automatically populated by the system.</li><li>• Can be left blank.</li></ul>
<b>NIC Index in vCenter</b>	The index of the adapter in the order of virtual network adapters (NICs) in the virtual machine settings of the vCenter web client.	<ul style="list-style-type: none"><li>• Customizable.</li><li>• Cannot be left blank.</li><li>• Enter a numeric value.</li><li>• Enter a value of <b>0</b> to define the first virtual network adapter in the vSphere Web Client. Enter a value of <b>1</b> to define the next network adapter.</li></ul>

## Changing the network adapter configuration of a protected VM

When the virtual network adapter (NIC) configuration of a production VM changes, any pre-existing copy VM network configuration may be adversely affected and may require reconfiguration before it works.

### Steps

- After adding or removing NICs from a protected virtual machine, reconfigure the copy VM network using [Re-IP rules](#).
- If the NIC configuration of a production VM changes and the change is not reflected in the copy VM, ensure [Hardware changes](#) is enabled and [enable image access](#) by [Test a copy](#).