

# Veritas™ Resiliency Platform 1.2: Solutions for Applications

# Veritas Resiliency Platform: Solutions for Applications

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: 1.2

Document version: 1.2 Rev 0

## Legal Notice

Copyright © 2016 Veritas Technologies LLC. All rights reserved.

Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third party software for which Veritas is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC  
500 E Middlefield Road  
Mountain View, CA 94043

<http://www.veritas.com>

# Technical Support

Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within the company to answer your questions in a timely fashion.

Our support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about our support offerings, you can visit our website at the following URL:

[www.veritas.com/support](http://www.veritas.com/support)

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

## Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

[www.veritas.com/support](http://www.veritas.com/support)

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information

- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Technical Support
  - Recent software configuration changes and network changes

## Licensing and registration

If your product requires registration or a license key, access our technical support Web page at the following URL:

[www.veritas.com/support](http://www.veritas.com/support)

## Customer service

Customer service information is available at the following URL:

[www.veritas.com/support](http://www.veritas.com/support)

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Advice about technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

## Support agreement resources

If you want to contact us regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Worldwide (except Japan)

[CustomerCare@veritas.com](mailto:CustomerCare@veritas.com)

Japan

[CustomerCare\\_Japan@veritas.com](mailto:CustomerCare_Japan@veritas.com)

# Contents

Technical Support	4	
Chapter 1	Overview of Resiliency Platform	11
	About Veritas Resiliency Platform	11
	About Resiliency Platform features and components	12
	Resiliency Platform capabilities	13
	About permissions for operations in the console	14
Chapter 2	Managing applications using Resiliency Platform	15
	Managing applications using Resiliency Platform	15
	Providing inputs for partially discovered applications	17
	Adding a custom application to Resiliency Platform	18
	Deleting a custom application	19
	Uploading application bundle to the Resiliency Manager	20
	Removing an application bundle	21
	Installing an application bundle on selected hosts	21
	Uninstalling an application bundle from selected hosts	22
	Enabling and disabling application bundle on selected hosts	23
	Managing auto-deploy for an application bundle	23
	Editing the discovery schedule for an application type	24
	Viewing the details of application types	25
	Viewing the applicable host details	25
Chapter 3	Managing InfoScale applications using Resiliency Platform	27
	About Veritas InfoScale Operations Manager	27
	Resiliency Platform support for InfoScale applications	27
	Managing InfoScale applications using Resiliency Platform	28
Chapter 4	Managing resiliency groups	30
	About resiliency groups	30
	Prerequisites for creating resiliency groups with applications	31

	Prerequisites for creating resiliency groups with InfoScale applications .....	31
	Managing and monitoring applications .....	31
	Protecting applications .....	33
	Displaying resiliency group information and status .....	36
	Viewing InfoScale applications details .....	38
	Displaying resiliency group details .....	40
	Modifying a resiliency group .....	41
	Starting a resiliency group .....	42
	Stopping a resiliency group .....	43
	Deleting a resiliency group .....	44
<b>Chapter 5</b>	<b>Monitoring and reporting on assets status .....</b>	<b>46</b>
	About the Resiliency Platform Dashboard .....	46
	Understanding asset types .....	48
	Viewing reports .....	48
<b>Chapter 6</b>	<b>Using Resiliency Platform for disaster recovery .....</b>	<b>50</b>
	About disaster recovery using Resiliency Platform .....	50
	Understanding the role of resiliency groups in disaster recovery operations .....	51
<b>Chapter 7</b>	<b>Managing disaster recovery for applications .....</b>	<b>52</b>
	About disaster recovery for applications .....	52
	Pre-requisites for disaster recovery of applications .....	53
	About replication technologies used in disaster recovery of applications .....	53
	An overview of key steps required for disaster recovery of applications .....	54
<b>Chapter 8</b>	<b>Preparing for disaster recovery operations .....</b>	<b>56</b>
	Configuring disaster recovery for a resiliency group of applications .....	56
	Viewing the details of a disaster recovery-enabled resiliency group .....	57



<b>Chapter 9</b>	<b>Rehearsing DR operations to ensure DR readiness .....</b>	<b>59</b>
	Ensuring the disaster recovery readiness of your Resiliency Platform	
	assets using the rehearse operation .....	59
	Rehearse operations for applications .....	60
	Performing rehearsal cleanup .....	62
<b>Chapter 10</b>	<b>Monitoring risks .....</b>	<b>63</b>
	About risk insight .....	63
	Setting up replication lag threshold .....	64
	Displaying risk information .....	65
	Predefined risks in Resiliency Platform .....	65
	Viewing the current risk report .....	68
	Viewing the historical risk report .....	69
<b>Chapter 11</b>	<b>Performing disaster recovery operations .....</b>	<b>70</b>
	Migrating a resiliency group of applications .....	70
	Taking over a resiliency group of applications .....	71
	Performing the resync operation .....	71
<b>Chapter 12</b>	<b>Managing activities and resiliency plans .....</b>	<b>73</b>
	Managing activities .....	73
	Viewing activities .....	73
	Aborting a running activity .....	74
	Managing resiliency plans .....	75
	About resiliency plans .....	75
	Creating a new resiliency plan template .....	76
	Editing a resiliency plan template .....	79
	Deleting a resiliency plan template .....	80
	Viewing a resiliency plan template .....	80
	Creating a new resiliency plan .....	81
	Editing a resiliency plan .....	82
	Deleting a resiliency plan .....	83
	Executing a resiliency plan .....	83
	Viewing a resiliency plan .....	83
	Creating a schedule for a resiliency plan .....	84
	Editing a schedule for a resiliency plan .....	84
	Deleting a schedule for a resiliency plan .....	85
	Viewing a schedule for a resiliency plan .....	85

Appendix A	Configuring applications for disaster recovery using replication .....	87
	Configuring application disaster recovery using EMC SRDF replication .....	87
	Configuring application disaster recovery using NetApp SnapMirror replication .....	90
	Configuring application disaster recovery using EMC RecoverPoint replication .....	91
Appendix B	Troubleshooting .....	95
	Troubleshooting discovery of assets .....	95
	Viewing events and logs in the console .....	97
Glossary	.....	99
Index	.....	101

# Overview of Resiliency Platform

This chapter includes the following topics:

- [About Veritas Resiliency Platform](#)
- [About Resiliency Platform features and components](#)
- [Resiliency Platform capabilities](#)
- [About permissions for operations in the console](#)

## About Veritas Resiliency Platform

Veritas Resiliency Platform offers a unified approach for visibility and control of IT service continuity for applications, virtual machines, and complex, multi-tier business services across a global landscape.

Resiliency Platform has the following core capabilities:

Recovery	Resiliency Platform provides a disaster recovery (DR) solution using data centers on premises in different geographical locations. The management console simplifies recovery, with single-click rehearsal and recovery operations.
Visibility	The console Dashboard provides visibility into the health of applications, virtual machines, and multi-tier business services.
Orchestration	Resiliency Platform can assist in data center day-to-day workload automation activities. For instance, virtual machines or IT services can be started and stopped for maintenance.

# About Resiliency Platform features and components

The following is a brief introduction to Veritas Resiliency Platform key components and features. Administrators responsible for deploying and configuring the product need to understand these in more detail.

resiliency domain	<p>The logical scope of a Resiliency Platform deployment.</p> <p>It can extend across multiple data centers.</p>
Resiliency Manager	<p>The component that provides resiliency capabilities within a resiliency domain. It is composed of loosely coupled services, a distributed data repository, and a management console.</p> <p>The Resiliency Manager is deployed as a virtual appliance.</p>
Infrastructure Management Server (IMS)	<p>The component that discovers, monitors, and manages the asset infrastructure within a data center. The IMS transmits information about the asset infrastructure to the Resiliency Manager. The IMS is deployed as a virtual appliance.</p> <p>To achieve scale, multiple IMSs can be deployed in the same data center.</p>
Veritas InfoScale Operations Manager Management Server	<p>The component that allows discovery of InfoScale applications that are already configured in Veritas InfoScale Operations Manager. Also referred to as Veritas InfoScale Operations Manager server.</p> <p>See <a href="#">“Managing InfoScale applications using Resiliency Platform”</a> on page 28.</p>
data center	<p>For a disaster recovery use case, the resiliency domain must contain at least two data centers in different locations, a production data center and recovery data center. Each data center has a Resiliency Manager and one or more IMSs.</p>
asset infrastructure	<p>The data center assets that you add to the IMS for discovery and monitoring.</p> <p>The asset infrastructure can include hosts (Windows or Linux servers), virtualization servers for Hyper-V and VMware, and enclosures (storage arrays). Once the asset infrastructure is discovered by the IMS, the discovered virtual machines or applications are listed in the console as assets to manage or protect.</p>

resiliency group	The unit of management and control in Resiliency Platform. You organize related assets into a resiliency group and manage and monitor them as a single entity.
Virtual Business Service (VBS)	A multi-tier business service where each VBS tier hosts one or more resiliency groups. A VBS lets you group multiple services as a single unit for visualization, automation, and controlled start and stop in the desired order. VBS uses the vertical grouping mechanism to group the multiple services. You can also migrate or takeover the entire VBS.

## Resiliency Platform capabilities

Resiliency Platform helps you monitor and manage disaster recovery across multiple data centers. It provides the following capabilities.

**Table 1-1** Resiliency Platform capabilities

Capability	More information
Protecting and managing applications as a single entity.	See <a href="#">“Managing and monitoring applications”</a> on page 31.
Displaying an overview of your resiliency domain including the number and health of your resiliency groups.	See <a href="#">“About the Resiliency Platform Dashboard”</a> on page 46. See <a href="#">“Displaying resiliency group information and status”</a> on page 36.
Starting and stopping resiliency groups for maintenance.	See <a href="#">“Starting a resiliency group”</a> on page 42. See <a href="#">“Stopping a resiliency group”</a> on page 43.
Configuring disaster recovery for a resiliency group	See <a href="#">“Configuring disaster recovery for a resiliency group of applications”</a> on page 56.
Monitoring risks for protected assets	See <a href="#">“About risk insight”</a> on page 63.
Rehearsing disaster recovery	See <a href="#">“Ensuring the disaster recovery readiness of your Resiliency Platform assets using the rehearse operation”</a> on page 59.
Migrating a resiliency group	See <a href="#">“Migrating a resiliency group of applications”</a> on page 70.
Taking over resiliency groups	See <a href="#">“Taking over a resiliency group of applications”</a> on page 71.
Viewing reports	See <a href="#">“Viewing reports”</a> on page 48.

**Table 1-1** Resiliency Platform capabilities (*continued*)

Capability	More information
Managing activities and resiliency plans	See <a href="#">“Managing activities”</a> on page 73. See <a href="#">“Managing resiliency plans”</a> on page 75.

# About permissions for operations in the console

Users that are configured for Resiliency Platform have permission by default to view the web console but not to perform any operations. Permissions for operations must be assigned separately by a Resiliency Platform administrator, who assigns the appropriate personas to users or groups. A persona is a role with access to a set of operations. The administrator can further limit the scope of some operations by selecting the objects, such as resiliency groups, to which the user has access.

For example, an administrator can assign one user the permission to perform operations on resiliency group RG1 and assign another user the permission to perform operations on RG2. If more resiliency groups are added later, the administrator needs to update permissions to assign access to the new resiliency groups.

Some objects, such as resiliency plans or virtual business services, can include multiple resiliency groups. To perform an operation on such an object, a user must have access to all its resiliency groups. Otherwise, the operation fails.

For more information on setting up user access to operations, refer to the *Deployment Guide*.

# Managing applications using Resiliency Platform

This chapter includes the following topics:

- [Managing applications using Resiliency Platform](#)
- [Providing inputs for partially discovered applications](#)
- [Adding a custom application to Resiliency Platform](#)
- [Deleting a custom application](#)
- [Uploading application bundle to the Resiliency Manager](#)
- [Removing an application bundle](#)
- [Installing an application bundle on selected hosts](#)
- [Uninstalling an application bundle from selected hosts](#)
- [Enabling and disabling application bundle on selected hosts](#)
- [Managing auto-deploy for an application bundle](#)
- [Editing the discovery schedule for an application type](#)
- [Viewing the details of application types](#)
- [Viewing the applicable host details](#)

## Managing applications using Resiliency Platform

You can use the Veritas Resiliency Platform to manage and protect your applications that are configured in the resiliency domain. For more information on supported

applications and their versions refer to *Hardware and Software Compatibility List (HSCL)*. The Resiliency Platform supports application discovery on physical hosts as well as VMware and Hyper-V virtual machines, provided that the `VRTSsfmh` host package is installed on the virtual machine.

When hosts are added to and discovered by the Infrastructure Management Server (IMS), applications residing on those hosts are displayed on the Resiliency Platform. They are listed on the **Unmanaged** tab. Note that for discovering Oracle instances, the `oratab` file must be present and must contain the entries for oracle applications.

For certain application instances, you need to provide additional information such as application database file path, or user name and password to complete the discovery. These are also listed on the **Unmanaged** tab with a **Pending Inputs** warning.

See [“Providing inputs for partially discovered applications”](#) on page 17.

By default, Resiliency Platform discovers Microsoft SQL Server (MSSQL) and Oracle applications. To discover, manage, and protect other applications, you need to add them using the **Add Custom Application** wizard.

See [“Adding a custom application to Resiliency Platform”](#) on page 18.

You can also discover and manage applications using the Application Enablement Software Development Kit (SDK). You can create a bundle with predefined Perl APIs and upload the same on the Resiliency Manager. You can either auto deploy the bundle on all the associated hosts in your data center or do it manually by selecting the managed hosts. The Perl scripts in the bundle developed using the SDK discover and report the applications on the Resiliency Platform console. For more information about developing the bundle, refer to *Veritas Resiliency Platform 1.2: Application Enablement SDK* guide.

See [“Uploading application bundle to the Resiliency Manager”](#) on page 20.

Resiliency Platform lets you manage applications by grouping them into resiliency groups. Some examples of Resiliency Platform operations are create a resiliency group, edit the resiliency group to add or remove applications, start and stop the resiliency groups and so on. Applications must be completely discovered to add them into resiliency groups.

See [“About resiliency groups”](#) on page 30.

Resiliency Platform provides disaster recovery (DR) specific operations to protect your applications that are grouped into a resiliency group. For example you can configure disaster recovery for the resiliency group and also migrate the resiliency group to another data center.

See [“Understanding asset types”](#) on page 48.

See [“Managing and monitoring applications”](#) on page 31.



See [“About disaster recovery for applications”](#) on page 52.

# Providing inputs for partially discovered applications

When hosts are added to and discovered by the Infrastructure Management Server (IMS), applications residing on those hosts are displayed on the Resiliency Platform web console. But certain application instances are not completely discovered until you provide additional information such as application database file path, or user name and password.

Using the Resiliency Platform console, you can provide inputs to such partially discovered applications to enable complete discovery. Complete discovery of applications is essential to group them into a resiliency group and thereby perform the disaster recovery operations.

For partially discovered applications, a **Pending Inputs** warning is displayed on the **Unmanaged** tab, in the **Discovery Status** column.

After an application is completely discovered and if any of the previous provided inputs have changed, the **Pending Inputs** warning is displayed again on the **Unmanaged** tab.

## To provide inputs for partially discovered applications

- 1 Navigate



**Assets > Unmanaged** tab.

- 2 Use one or more of the following drop-downs to filter your list of applications:

<b>Asset Type</b>	Select application.
<b>Data Center</b>	Select the data center in which the application is located.
<b>Application Type</b>	Select the application type.

- 3 Right-click the partially discovered application and select **Enter Inputs**.
- 4 In the **Enter Inputs** panel, enter the required information, and click **Submit**.

See [“Managing and monitoring applications”](#) on page 31.

# Adding a custom application to Resiliency Platform

By default, Resiliency Platform discovers Microsoft SQL Server (MSSQL) and Oracle applications. In certain circumstances, however, some Oracle applications may not be discovered. In addition, you may want to add other applications to Resiliency Platform. To manage and protect applications that are not discovered by default, you need to add them using the **Add Custom Application** wizard.

---

**Note:** Adding custom applications using Microsoft Failover Cluster nodes is not recommended and not supported.

---

## To add a custom application to Resiliency Platform

### 1 Prerequisites

Do the following:

- Create a script to start, stop, and monitor the application. Resiliency Platform interacts with the application using these scripts. The scripts should reside on the same host as the application.
- Note the directory path to each script.
- Determine the user who should run the script. Often, this is the admin user or root user. Note the password of this user.
- Identify which data directory paths the application uses.
- Ensure that the host where the application resides is added to the Infrastructure Management Server (IMS).

For more information, see the *Deployment Guide*.

### 2 Navigate



**Assets > Unmanaged tab**

- 3 On the **Unmanaged** tab, use the **Asset Type** drop-down list to select **Application**.
- 4 Click **Add Custom Application**.
- 5 On the **Type and Host Selection** page, do the following:
  - On the **Application Type** drop-list, select **Custom Application**.

- On the **Data Center** drop-list, select the data center in which the application's host system resides.
  - In the host name list, use the check box to select the host.
  - Click **Next**.
- 6** On the **Application Inputs** page, do the following:
- Verify that you select the correct data center and host.
  - Use the information you collected in step [1](#) to complete the form.
  - Specify the instance name.

Note that if you selected Oracle as **Application Type** in step 5, you need to specify same name (SID) in both the Instance name fields. If you specify different names for both the instance name fields, your application may not be discovered.

- 7** Click **Submit**.

---

**Note:** After adding a custom application successfully, you cannot edit the information. If you enter any application parameters incorrectly or later the application information changes, you must delete the application and add it again with the correct information.

---

After you add a custom application, you organize it with other applications into a resiliency group.

See [“Protecting applications”](#) on page 33.

See [“Managing and monitoring applications”](#) on page 31.

## Deleting a custom application

Using the Resiliency Platform console you can delete a custom application.

### To delete a custom application

- 1** Navigate



**Assets > Unmanaged** tab

- 2** On the **Unmanaged** tab, use the **Asset Type** drop-down list to select **Application**.

- 3 Right-click the application and select **Delete**
- 4 In the **Delete Application** panel, review the select and click **OK**.

## Uploading application bundle to the Resiliency Manager

Using the Resiliency Platform console you can manage the discovered applications that are installed in your data center. For some applications such as MS SQL and Oracle the discovery scripts are pre-bundled with the Resiliency Platform. For others, you can create a bundle using the Application Enablement SDK to discover and manage the applications. A sample bundle is available for downloading on the **Application Types** page in **Infrastructure Settings**.

You can upload this bundle on the Resiliency Manager and install it on all the applicable hosts that are associated with the Resiliency Platform. You can also choose to install the bundle on selected hosts.

The bundle should be in `.tar.gz` format.

For more information on how to create the bundle, refer to *Veritas Resiliency Platform 1.2: Application Enablement SDK* guide.

After you upload the bundle, you can view the following information on the **Application Types** page:

- Application type
- Application category
- Version
- Platform
- Whether the application bundle is enabled for auto deploy.
- The Status column displays the installed versus applicable hosts data.

### To upload application bundle to the Resiliency Manager

- 1 Navigate



**Settings** (menu bar)

Under **Infrastructure Settings**, click **Application Support**.

- 2 On the **Application Types** page, click **Add**.

- 3 In the **Add Application Type** panel, click **Browse** to select the application bundle. You can upload only one file at a time. Click **Upload**.
- 4 Review the application information in the table.
- 5 Do the following and click **Submit**.
  - You can choose to auto deploy the applications on all the associated hosts.
  - If an application type with the same version already exists, then you can choose to overwrite it. If the lower version of the application exists, you can choose to upgrade to the higher version.

See [“Installing an application bundle on selected hosts”](#) on page 21.

## Removing an application bundle

Using the Resiliency Platform console, you can remove the application bundle from the Resiliency Manager.

You cannot remove an application bundle that is installed if the managed host is disconnected from the Infrastructure Management Server (IMS).

### To remove the application bundle

- 1 Navigate



**Settings** (menu bar)

Under **Infrastructure Settings**, click **Application Support**.

- 2 On the **Application Types** page, select the application which you want to remove, and click **Remove**.
- 3 In the **Remove Application Type** panel, review your selection and click **Submit**.

See [“Uploading application bundle to the Resiliency Manager”](#) on page 20.

## Installing an application bundle on selected hosts

Using the Resiliency Platform console, you can install the application bundle on selected hosts.

### To install the application bundle on selected hosts

#### 1 Navigate



**Settings** (menu bar)

Under **Infrastructure Settings**, click **Application Support**.

- 2 On the **Application Types** page, on the **Uploaded** tab, double-click on the application which you want to install on selected hosts.
- 3 On the application type details page, select the hosts on which you want to install the bundle and click **Install**.
- 4 On the **Install Application Type** panel, review your selection, and click **Submit**.

See [“Enabling and disabling application bundle on selected hosts”](#) on page 23.

See [“Managing auto-deploy for an application bundle”](#) on page 23.

## Uninstalling an application bundle from selected hosts

Using the Resiliency Platform console, you can uninstall the application bundle from the selected hosts.

### To uninstall the application bundle from selected hosts

#### 1 Navigate



**Settings** (menu bar)

Under **Infrastructure Settings**, click **Application Support**.

- 2 On the **Application Types** page, on the **Uploaded** tab, double-click on the application which you want to uninstall.
- 3 On the application type details page, select the hosts from which you want to uninstall the bundle and click **Uninstall**.
- 4 On the **Uninstall Application Type** panel, review your selection, and click **Submit**.

See [“Uploading application bundle to the Resiliency Manager”](#) on page 20.

# Enabling and disabling application bundle on selected hosts

Using the Resiliency Platform console, you can enable and disable the application bundle on the selected hosts to resume or pause the discovery of the application instances.

When you disable the application bundle, the application discovery is paused. The current state of the application is not displayed on the Resiliency Platform console.

## To enable or disable application bundle on selected hosts

### 1 Navigate



**Settings** (menu bar)

Under **Infrastructure Settings**, click **Application Support**.

- 2 On the **Application Types** page, on the **Uploaded** tab, double-click on the application type which you want to enable or disable.
- 3 On the application details page, select the hosts on which you want to enable or disable the bundle and click the appropriate menu option.
  - **Enable**
  - **Disable**
- 4 On the **Application Type** panel, review your host selection, and click **Submit**.

See [“Installing an application bundle on selected hosts”](#) on page 21.

# Managing auto-deploy for an application bundle

Using the Resiliency Platform console, you can auto deploy the selected application bundle on all the applicable managed hosts. If the application bundle is enabled for auto-deploy during the initial deployment process, then every time you add a new managed host to your data center the bundle is deployed on that host. You can choose to disable this auto-deploy facility.

## To manage auto-deploy for an application bundle

### 1 Navigate



**Settings** (menu bar)

Under **Infrastructure Settings**, click **Application Support**.

- 2 On the **Application Types** page, on the **Uploaded** tab, right-click the application type and select **Set/Unset Auto-Deploy**.
- 3 On the **Set/Unset Auto-Deploy** page click **Submit**.

See [“Enabling and disabling application bundle on selected hosts”](#) on page 23.

See [“Editing the discovery schedule for an application type”](#) on page 24.

# Editing the discovery schedule for an application type

Using the Resiliency Platform console, you can edit the discovery schedule for an application type. Application discovery is of two types: deep and probe. Deep discovers the entire application and its components including files. Probe only checks the status of the application instances. For example whether the application is online or offline.

The discovery frequency for deep can range from 240 minutes to 1440 minutes. For probe, the range is one minute to 60 minutes.

The default discovery frequencies for deep and probe are 360 and 10 minutes respectively.

## To edit the discovery schedule for an application type

### 1 Navigate



**Settings** (menu bar)

Under **Infrastructure Settings**, click **Application Support**.

- 2 On the **Application Types** page, on the **Uploaded** tab, right-click the application type and select **Properties**.
- 3 On the **Properties** page, click on the **Frequency** column to change the discovery schedule for Deep and Probe, and click **Submit**.



See [“Installing an application bundle on selected hosts”](#) on page 21.

## Viewing the details of application types

Using the Resiliency Platform console you can view the details of the application types.

You can view the following information on the **Uploaded** tab:

- Application type
- Category such as database
- Version
- Platform information
- Whether the application bundle is enabled or disabled for auto deploy on all the applicable hosts.
- The **Status** column displays the installed versus applicable hosts data.

You can view the following information on the **Pre-bundled** tab:

- Application type
- Category such as database
- Whether the application is enabled or disabled for auto deploy on all the applicable hosts.

### To view the details of application types

- ◆ Navigate



**Settings** (menu bar)

Under **Infrastructure Settings**, click **Application Support**.

See [“Uploading application bundle to the Resiliency Manager”](#) on page 20.

See [“Installing an application bundle on selected hosts”](#) on page 21.

See [“Managing auto-deploy for an application bundle”](#) on page 23.

## Viewing the applicable host details

Using the Resiliency Platform web console you can view the details of the hosts on which an application bundle can be installed.

You can view the following information of the hosts in this view:

- Host name
- Platform
- Family
- Architecture
- Status of the bundle on the host. Whether it is enabled, disabled, or not installed.

### To view the applicable host details

#### 1 Navigate



**Settings** (menu bar)

Under **Infrastructure Settings**, click **Application Support**.

#### 2 On the **Application Type** view, double-click on an application.

See [“Uploading application bundle to the Resiliency Manager”](#) on page 20.

See [“Installing an application bundle on selected hosts”](#) on page 21.

See [“Managing auto-deploy for an application bundle”](#) on page 23.

# Managing InfoScale applications using Resiliency Platform

This chapter includes the following topics:

- [About Veritas InfoScale Operations Manager](#)
- [Resiliency Platform support for InfoScale applications](#)
- [Managing InfoScale applications using Resiliency Platform](#)

## About Veritas InfoScale Operations Manager

Veritas InfoScale Operations Manager gives you a single, centralized management console for the Veritas InfoScale products. You can use it to monitor, visualize, and manage storage and cluster resources, and generate reports about these components in the Management Server domain. Veritas InfoScale Operations Manager helps administrators centrally manage diverse data center environments.

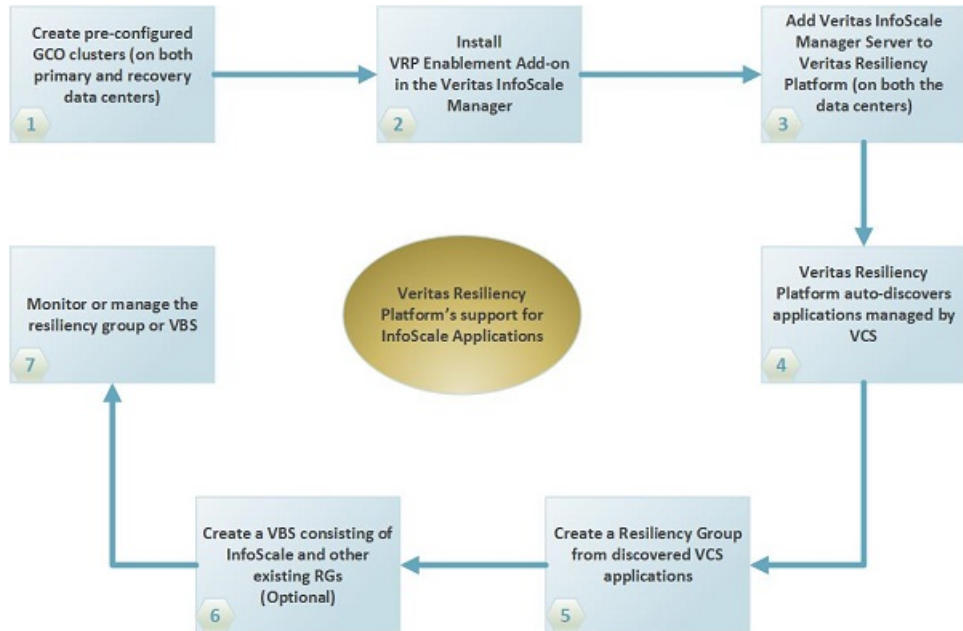
## Resiliency Platform support for InfoScale applications

A typical workflow of Veritas Resiliency Platform for InfoScale applications consists of a Veritas InfoScale Operation Manager server reporting to a Resiliency Manager. The InfoScale applications should be already configured in Veritas InfoScale Operations Management server. You can group the InfoScale applications into resiliency groups or VBSs to recover, monitor, visualize, and generate reports about these applications in the Resiliency Platform.

**Note:** Applications that are only managed by InfoScale Availability (VCS) are supported in Veritas Resiliency Platform.

The following diagram depicts the general workflow of configuring the InfoScale applications for recovery using Resiliency Platform.

**Figure 3-1** A typical workflow for recovering managed InfoScale applications



## Managing InfoScale applications using Resiliency Platform

Veritas Resiliency Platform lets you manage the InfoScale applications that are already configured in Veritas InfoScale Operations Manager Management Server. The InfoScale applications are automatically discovered in the Resiliency Platform when the Veritas InfoScale Operations Manager server is added to the resiliency domain. They are listed on the **Assets** page under the **Unmanaged** tab. You can filter the InfoScale applications using the **InfoScale applications** check box under the **More Options** drop-down menu.

For more information on adding a Veritas InfoScale Operations Manager server to the Resiliency Domain, refer to *Veritas Resiliency Platform Deployment Guide*.

Veritas InfoScale Operations Manager users must download and install Veritas Resiliency Platform Enablement add-on to automatically discover the InfoScale applications. You can download the add-on from [Veritas Services and Operations Readiness Tools](#) (SORT). You cannot add or modify InfoScale applications through Resiliency Platform. They can be added or modified only by an administrator through Veritas InfoScale Operations Manager.

# Managing resiliency groups

This chapter includes the following topics:

- [About resiliency groups](#)
- [Managing and monitoring applications](#)
- [Protecting applications](#)
- [Displaying resiliency group information and status](#)
- [Viewing InfoScale applications details](#)
- [Displaying resiliency group details](#)
- [Modifying a resiliency group](#)
- [Starting a resiliency group](#)
- [Stopping a resiliency group](#)
- [Deleting a resiliency group](#)

## About resiliency groups

In Veritas Resiliency Platform, you organize related assets into a resiliency group that you can protect and manage as a single entity. Before you create a resiliency group, you must add the assets to Resiliency Platform.

For example, you can organize several applications into a resiliency group and name it `SQL_Server_Group`. Then, when you perform an operation on `SQL_Server_Group` from the Resiliency Platform console, all the applications in the group are affected. For example, if you start `SQL_Server_Group`, all the applications

in the group start. Similarly, you can organize virtual machines into a resiliency group and perform operations that affect all the virtual machines in the group.

---

**Note:** A resiliency group must contain similar types of objects, either all applications or all virtual machines. It cannot contain a mix of the two.

---

You can create a resiliency group in the following ways:

- You can create a resiliency group without enabling disaster recovery for it. See [“Managing and monitoring applications”](#) on page 31.
- You can create a resiliency group and enable disaster recovery for it. This is known as a protected resiliency group. See [“Protecting applications”](#) on page 33.

## Prerequisites for creating resiliency groups with applications

Following prerequisites are for creating resiliency groups with applications:

- They must be members of the same consistency group.
- They must use the same replication technology.
- Applications must be completely discovered.
- For Microsoft SQL Server, the **Guest** user must have **Connect** permission on all the databases, to create a resiliency group.

## Prerequisites for creating resiliency groups with InfoScale applications

Following prerequisites are for creating resiliency groups with InfoScale applications:

- You cannot add both InfoScale and non-InfoScale applications within a same resiliency group.
- The selected InfoScale applications in the resiliency group should be from the same Global Cluster Option (GCO) pair. You cannot add InfoScale applications from different GCO pairs.
- The InfoScale applications in the resiliency group should be from different data centers.

## Managing and monitoring applications

To manage and monitor applications, create a resiliency group of applications.

To manage and monitor applications

- 1 Prerequisites
- The asset infrastructure must be added to the Infrastructure Management Server (IMS) and IMS discovery of the applications must be complete. For more information on adding asset infrastructure, refer to the *Deployment Guide*.

■

For InfoScale applications, the asset infrastructure must be added to the Veritas InfoScale Operations Manager and the discovery of the applications must be complete. For more information, refer to the Veritas InfoScale Operations Manager documentation.

2 Navigate



**Assets > Resiliency Groups** tab > **Manage & Monitor Virtual Machines or Applications**

3 Display a list of applications

On the **Select Assets** page, use one or more of the following drop-downs to filter your list of applications:

<b>Asset Type</b>	Select <b>Application</b> .
<b>Data Center</b>	The data center in which the application is located.
<b>Application Type</b>	Select the application type.  See <a href="#">“Adding a custom application to Resiliency Platform”</a> on page 18.

4 Filter the list of applications (optional)

Use one or more of the following to filter your list of applications:

<b>Group By</b>	Organize the applications by host name or replication consistency group.
<b>Search</b>	If you have a long list of applications, use the <b>Search</b> field to filter the list.



**More Options**

Lets you select the following options from the drop-down menu:

- Infoscale applications: Lets you filter the InfoScale applications from the total list of applications.
- Assets in RG: Lets you filter the applications that are already part of a resiliency group.

**5** Select the applications

To include an application in your new resiliency group, drag it from the list and drop in the **Selected Instances** area. If you change your mind, you can drag it back to the application list. Click **Next**.

**6** Create the resiliency group

On the **Summary** page, review the list of applications that form your new resiliency group. If you need to make any changes, click **Back** to return to the **Select Assets** page. When you are ready, name the resiliency group and click **Submit**.

**7** On the confirmation screen, click **Done**

Resiliency Platform displays detailed information about the new resiliency group. It includes the following:

- The active data centers, replication type, and replication state.
- Controls to modify, delete, start, and stop the resiliency group.
- A list of the applications in the resiliency group.
- The disaster recovery readiness of the resiliency group. You can configure disaster recovery from this screen.
- A list of risks (if any) to the resiliency group.

To display a record and a graphic representation of what you did, click the **Recent Activities** at the bottom of the page, find your task, and click **Details**.

## Protecting applications

The Resiliency Platform provides a single wizard to protect your applications across data centers by creating a resiliency group and setting up disaster recovery (DR) for the group.

## To protect applications

### 1 Prerequisites

Before you configure DR for a resiliency group, make sure of the following:

- The applications should be running.
- For InfoScale applications, Veritas Cluster Servers (6.0 onwards) with Global Cluster Option (GCO) should be enabled.
- They must be members of the same consistency group.
- They must use the same replication technology.
- Application binaries should be stored on local storage and data files on replicated storage.
- The DNS server settings should be configured for both data centers. DNS settings are required for binding a host name to different IP addresses on the DR site. This is required only if you plan to use the Resiliency Platform for performing DNS updates.

For more information on configuring DNS server settings, see the *Veritas Resiliency Platform Deployment Guide*.

- If Failover Clustering is not used, you must plumb the application IP addresses on all the systems across the data centers. The Resiliency Platform console does not manage plumbing or unplumbing of IP address for applications.
- Ensure that you have disabled the 'Quick removal' policy for disks in Windows Server 2008 R2 and disabled the 'write-cache' policy for disks in Windows Server 2012 R2.

### 2 Navigate



**Assets > Resiliency Groups tab > Protect Applications**

### 3 Display a list of applications

On the **Select Assets** page, use one or more of the following drop-downs to filter your list of applications:

<b>Data Center</b>	Select the data center in which the application is located.
<b>Application Type</b>	Select the application type.  See <a href="#">“Adding a custom application to Resiliency Platform”</a> on page 18.

#### 4 Filter the list of applications (optional)

<b>Group By</b>	Organize the applications by the host on which they are installed or their replication consistency group.
<b>Search</b>	If you have a long list of applications, use the <b>Search</b> field to filter the list.
<b>More Options</b>	Lets you select the following options from the drop-down menu: <ul style="list-style-type: none"> <li>■ <b>Infoscale applications</b>: Lets you can filter the InfoScale applications from the total list of applications.</li> <li>■ <b>Assets in RG</b>: Lets you filter the applications that are already part of a resiliency group.</li> </ul>

#### 5 Select the applications

To include an application in your new resiliency group, drag it from the list and drop in the **Selected Instances** area. If you change your mind, you can drag it back to the application list. Select applications from the production data center and the recovery data center. The application must be online on one of the data centers. When you select all the assets you need, click **Next**.

#### 6 Create the resiliency group

On the **Manage Assets** page, review the list of applications that form your new resiliency group. If you need to make any changes, click **Back** return to the **Select Assets** page. When you are ready, name the resiliency group and click **Next**.

#### 7 On the **Configure DR** page, decide whether to configure disaster recovery now or later. Do one of the following:

- To configure disaster recovery later, click **Done**.  
See [“Configuring disaster recovery for a resiliency group of applications”](#) on page 56.
- To configure disaster recovery now, click **Submit**, and continue with step 8.

#### 8 Review your selections in the **Selected Assets** page. Click **Next**.

#### 9 On the **Selected Assets** page, review assets in each data center. The page should show two data centers, each with identical applications. If it doesn't, click **Back** until you return the **Select Assets** page and update the resiliency group. If the data centers each contain the same applications, click **Next**.

- 10** On the **DNS Settings for Primary DC** page, specify whether you want to manage the DNS record setting for the resiliency group on the primary data center. Select **Yes** to manage the DNS setting.

You can use this page to do the following:

- Remove the DNS mappings for any hosts in the data center that do not need to be updated on the DNS server.
- Specify whether or not Resiliency Platform creates pointer (PTR) records for the host. A PTR record resolves the IP address to the host name. It is used for reverse DNS lookups.
- Specify whether you want to abort the migrate workflow if the DNS settings fail.

When you complete your selections, click **Next**.

- 11** On the **DNS Settings for DR DC** page, update the DNS settings for the resiliency group at the disaster recovery data center. You can use this page update the host name or remove the mapping.

When you complete your updates, click **Next**.

- 12** On the **Summary** screen, verify the information and click **Submit**.


## Displaying resiliency group information and status

You can display resiliency group information and status in the following ways:

**Table 4-1** Displaying resiliency group information and status

Location	Level of detail	Useful for
Resiliency Platform Dashboard	Lowest. Displays the number of resiliency groups under Resiliency Platform control and the total number of groups in error, at risk, and healthy.	Getting a quick overview of the resiliency group population and health throughout Resiliency Platform.  See <a href="#">“About the Resiliency Platform Dashboard”</a> on page 46.

Table 4-1      Displaying resiliency group information and status *(continued)*

Location	Level of detail	Useful for
 <b>Assets &gt; Resiliency Groups</b> tab	Medium. Lists all your resiliency groups in one place.	Seeing what is in each of your data centers, the state of the groups, whether disaster recovery is configured, and so on.
Resiliency group-specific screen	Highest. Lists each asset in the resiliency group, their type, and state.	Getting detailed information on a resiliency group and its underlying assets. This screen can help you decide whether to start, stop, edit, or delete a group.  See <a href="#">“Displaying resiliency group details”</a> on page 40.

This section discusses the second method of displaying resiliency group information and status: using the **Assets** page. The **Assets** page gives you a quick overview of all your resiliency groups.

To display resiliency group information and status

1    Navigate



**Assets > Resiliency Groups** tab

2    Review information and status

- For a quick health check of your resiliency groups, review the colored boxes above the table. Click on a box to show only the resiliency groups in that category; for example, click the green square to display only the resiliency groups that are healthy.

Blue	The total number of resiliency groups
Yellow	The number of resiliency groups at risk
Green	The number of resiliency groups that are healthy

By default, the table lists all resiliency groups. Use the drop-list and search field to filter your results, and click on a table heading to sort the groups. In the table, the key fields are **State**, **DR Status**, and **Replication Type**. Possible states are:

State	<p><b>Online</b> - The assets within the resiliency group are running.</p> <p><b>Partial</b> - One or more of the assets in the resiliency group are offline.</p> <p><b>Offline</b> - The assets in the resiliency group are powered off or not running.</p>
DR Status	<p><b>Configured</b> - The resiliency group has been configured for disaster recovery.</p> <p><b>Not Configured</b> - Disaster recovery is not configured for the group. Configure it as soon as possible.</p>
Replication Type	<p>Resiliency Platform supports several replication technologies.</p> <p>If no replication type is shown, consider configuring replication.</p> <p>See <a href="#">“Configuring disaster recovery for a resiliency group of applications”</a> on page 56.</p>
Type	<p>Application Group: The resiliency group comprises applications.</p> <p>Virtual Machine Group: The resiliency group comprises virtual machines.</p>

### 3 Display detailed information on a resiliency group (optional)

To display detailed information about a resiliency group, click its row in the table.

See [“Displaying resiliency group details”](#) on page 40.

## Viewing InfoScale applications details

Veritas Resiliency Platform lets you manage the InfoScale applications that are added in Veritas InfoScale Operations Manager (7.0 onwards).

## To view InfoScale applications information

### 1 Navigate



**Assets > Unmanaged tab**

### 2 Use one or more of the following drop-downs to filter your list of applications:

<b>Asset Type</b>	Select application.
<b>Data center</b>	Select the data center in which the application is located.
<b>Application Type</b>	<p>Select the application type.</p> <p>In InfoScale applications, Application Type resources with service group dependencies are considered as a single application.</p> <p><b>Note:</b> Only the service group with resources that are of Application type are discovered under the Unmanaged tab.</p>

### 3 Under **More Options** drop-down menu, select **InfoScale applications**.

### 4 At the end of the InfoScale application row,



Click the vertical ellipsis, and select **More Information**.

### 5 In the **More Information** window, you can view the following InfoScale details:

<b>Details</b>	It displays the Application Name along with its Host Name, and State (Offline or Online). It also provides the type of the application.
<b>Availability</b>	It displays the type of availability product used, name, and type of the service group. It also provides the system list, cluster details of the application and fire drill service related information.
<b>Data protection</b>	It displays detailed information about the replication details, such as Replication Type, Replication availability, of the application.

# Displaying resiliency group details

You can display detailed information on each of your resiliency groups. You can use a resiliency group-specific screen to answer questions as such the following:

- What is the overall health of the resiliency group?
- Is it configured for disaster recovery (DR)?
- What are its underlying assets and their current state?
- If DR is configured for the resiliency group, what is the replication lag time between sites?

## To display details on a single resiliency group

1    Navigate



**Assets > Resiliency Groups** tab

2    Sort and select your resiliency group

On the **Resiliency Groups** tab, use the drop-down list, **Search** field, and table headings to filter your list of resiliency groups.

3    Display the resiliency group-specific screen

Double-click the table row for the resiliency group you are interested in.

The screen is divided into the following areas:

**Table 4-2**            Resiliency group details screen

This part of the screen ...	Displays ...
Top	Resiliency group's health and status.  It identifies the data centers at which the resiliency group is active, its replication state and type, and whether the resiliency group is configured for disaster recovery. This part of the screen displays the number of alerts that are associated with the resiliency group. And also verifies whether the resiliency group is part of any VBS or not.
Middle	A table with the assets that make up the resiliency group. You can use links above the table to sort the assets by data center, and you can use the table headings to sort the assets by <b>Name</b> , <b>Type</b> , or <b>State</b> .



**Table 4-2** Resiliency group details screen (*continued*)

This part of the screen ...	Displays ...
Bottom	If the resiliency group is configured for disaster recovery, this portion of the screen displays the replication lag between the production data center and the recovery data center, and the recovery time. Note that the recovery time is available only after the rehearse operation is complete.

For resiliency group with InfoScale applications, you can view **Availability Details** in the resiliency group details page. Under this option, you find the details of the InfoScale applications, such as availability type, service group's name, type, and system list.

You also can display information on your resiliency groups in the following ways:

- For a high-level view of resiliency group health, use the Resiliency Platform Dashboard.  
See [“About the Resiliency Platform Dashboard”](#) on page 46.
- For a list of your resiliency groups and a quick view of which ones are up, configured, and so on, use the **Assets > Resiliency Group** tab.  
See [“Displaying resiliency group information and status”](#) on page 36.

## Modifying a resiliency group

You can modify resiliency group information including the group name as well as change the underlying assets on which the resiliency group is based.

---

**Note:** If you modify a resiliency group that has been configured for disaster recovery, you must reconfigure it.

See [“Configuring disaster recovery for a resiliency group of applications”](#) on page 56.

---

### To modify resiliency group information

#### 1 Prerequisites

- After you configure a resiliency group for disaster recovery, you cannot edit the resiliency group. You must first unconfigure disaster recovery for the resiliency group, edit it, and then configure disaster recovery again.
- Determine the potential impact modifying the resiliency group may have on users. If necessary, notify users of the upcoming change.

## 2 Navigate



**Assets > Resiliency Groups** tab

## 3 Select

Use the on-screen filters, **Search** field, and table heading sort feature to locate your resiliency group.

## 4 Edit

Do one of the following:

- Right click on the resiliency group row and select **Modify**.
- On the right side of the resiliency group row, click on the vertical ellipsis and select **Modify**.

The steps for editing the resiliency group are the same as creating it.

When you edit a resiliency group made up of virtual machines, note the following:

- If the resiliency group is configured for disaster recovery, Resiliency Platform proceeds to the Protect VM wizard.
- When the number of virtual machines on the replicated volume changes, edit the resiliency group to add or remove the virtual machines.

---

**Note:** If you add or remove virtual machines from a resiliency group after you have configured DR for that particular resiliency group, the DR functionality may not work as expected. You need to reconfigure DR for the resiliency group with the current set of virtual machines.

---

# Starting a resiliency group

When you start a resiliency group, you start all the underlying assets in it.

### To start a resiliency group

- 1 Prerequisites  
Create a resiliency group.
- 2 Navigate



**Assets > Resiliency Groups** tab

- 3 Select  
Use the on-screen filters, **Search** bar, and table heading sort feature to locate your resiliency group.
- 4 Start the resiliency group.  
Do one of the following:
  - Right click on the resiliency group row and select **Start**.
  - On the right side of the resiliency group row, click on the vertical ellipsis and select **Start**.
- 5 On the **Start Resiliency Group** screen, select the data center in which to start the group and click **Submit**.
- 6 Confirm  
Click **Done**.
- 7 Notify  
If necessary, notify users after you start the resiliency group.

To display a record and a graphic representation of what you did, click the **Recent Activities** at the bottom of the page, find your task, and click **Details**.

## Stopping a resiliency group

When you stop a resiliency group, you stop all the assets that make up the group.

A typical reason for stopping a resiliency group would be to update or perform maintenance in one of the underlying assets.

### To stop a resiliency group

- 1 Prerequisites
  - Make sure that you are aware of all the assets in the resiliency group, and the potential affect on users if you shut them down.

- Choose a time for stopping the resiliency group that minimizes any disruption of service.
- If necessary, notify users before stop the resiliency group.

## 2 Navigate



**Assets > Resiliency Groups** tab

## 3 Select

Use the on-screen filters, **Search** field, and table heading sort feature to locate your resiliency group.

## 4 Stop the resiliency group.

Do one of the following:

- Right click on the resiliency group row and select **Stop**.
- On the right side of the resiliency group row, click on the vertical ellipsis and select **Stop**

## 5 On the **Stop Resiliency Group** screen, select the data center in which to stop the resiliency group and click **Submit**.

## 6 Confirm

Click **Done**.

To display a record and a graphic representation of what you did, click the **Recent Activities** at the bottom of the page, find your task, and click **Details**.

# Deleting a resiliency group

When you delete a resiliency group from Resiliency Platform management, you can no longer monitor, manage, or protect it from the Resiliency Platform console. Deleting the resiliency group from Resiliency Platform has no affect on the underlying assets.

## To delete a resiliency group

### 1 Prerequisites

- Determine the potential affect of deleting the resiliency group. What is the benefit (if any) to deleting it from Resiliency Platform management? Does this benefit outweigh the fact that the group can no longer be monitored, managed, or protected through Resiliency Platform?

- If the resiliency group is configured for disaster recovery, you cannot remove it. You must unconfigure disaster recovery before you can remove the group.
- If necessary, notify users of the upcoming change.

## 2 Navigate



**Assets > Resiliency Groups** tab

## 3 Select

Use the state drop-down list, **Search** field, and table heading sort feature to locate the resiliency group.

## 4 Remove

To remove the resiliency group, do one of the following:

- Right click on the resiliency group row and select **Delete**.
- On the right side of the resiliency group row, click on the vertical ellipsis and select **Delete**.

On the **Delete Resiliency Group** screen, click **Submit**. On the confirmation screen, click **Done**.

# Monitoring and reporting on assets status

This chapter includes the following topics:

- [About the Resiliency Platform Dashboard](#)
- [Understanding asset types](#)
- [Viewing reports](#)

## About the Resiliency Platform Dashboard

The Resiliency Platform Dashboard gives you an overview of your resiliency domain. Use the Dashboard to answer questions such as the following:

- Which of my data centers have Resiliency Platform managed assets?
- What is the mix of my assets by type and platform?
- Which assets are configured for disaster recovery?

The Dashboard has the following areas:

**Global View**

A world map that identifies the data centers that contain Resiliency Platform managed assets.

Lines between data centers indicate that replication takes place between the locations.

Mouse over an icon for basic Resiliency Platform platform configuration and asset configuration information for that data center. Click **More** for detailed information and recent activity.

**Resiliency Groups and Virtual Business Services** summaries

The upper right section of the dashboard displays total number of resiliency groups and virtual business services in the resiliency domain, as well as those at risk and normal.

Click a square in either the **Resiliency Groups** or **Virtual Business Services** summary to display a tab of detailed information.

**Virtual Machines by Type and Platform**

Displays a summary of virtual machines in all data centers or information on a single data center. Use the drop-down list to filter your results. The summary lists the virtual machine types by percentage and the platform types by number.

**Application environment**

Displays the number of applications and the application types. The chart shows the number of applications that are managed by InfoScale and those that are not managed by InfoScale.

**Applications by Type**

Displays a summary of application types in all data centers or in a single data center. Use the drop-down list to filter your results.

**Top Resiliency Groups by Replication Lag**

Ranks the resiliency groups according to how long it takes the recovery data center to be in sync with the active data center.

**Virtual Machines and Applications by Recovery Readiness**

Displays the percentage of virtual machines and applications that are unprotected or unmanaged.

Use the drop-down list to filter your results.

See [“Displaying resiliency group information and status”](#) on page 36.

# Understanding asset types

On the Resiliency Platform console Assets page, assets are classified as follows.

Asset	Description
Resiliency Group	A group of applications or virtual machines under Resiliency Platform control. You can use Resiliency Platform to start and stop the resiliency group, as well as protect and manage it.
Virtual Business Service	A collection of resiliency groups logically grouped for a specific business purpose.
Unmanaged	An application or virtual machine that Resiliency Platform discovers in your environment, but that is not under Resiliency Platform management. You cannot use any Resiliency Platform features with these assets until they become a part of a resiliency group.

# Viewing reports

Veritas Resiliency Platform provides a console for viewing the following reports:

Resiliency Groups by Datacenter	Provides details about the resiliency groups in the data centers across all sites.
Migrate and Takeover	Provides a summary of the last migrate and takeover operations that were performed on the resiliency groups. A pie chart shows the percentage of successful and failed operations.

## To view a report

- 1
- Navigation
- Click **Reports** (menu bar).
- 2
- Do one of the following:
- Click **Run** to receive the report on the specified email address in HTML or PDF format, or as a comma separated (.CSV) file. You can also view the saved report on the console.



- Click **Schedule** to create a report generation schedule.

For more information on configuring email settings and scheduling reports, refer to the *Deployment Guide*.

# Using Resiliency Platform for disaster recovery

This chapter includes the following topics:

- [About disaster recovery using Resiliency Platform](#)
- [Understanding the role of resiliency groups in disaster recovery operations](#)

## About disaster recovery using Resiliency Platform

A comprehensive disaster recovery strategy ensures that your mission-critical IT functions can continue during and after a disaster and any unforeseen risk can be mitigated to the extent possible.

Veritas Resiliency Platform lets you perform disaster recovery operations on your critical IT services. This section introduces you to the key features of Resiliency Platform:

- Monitoring of data center assets - storage, virtual machines, and applications.
- Ability to group your virtual machines or applications in resiliency groups based on your production environment and business needs.
- Making business services more resilient by providing the ability to perform disaster recovery operations on virtual machines and applications. For example, migrate and takeover.
- Resiliency plan (a sequential execution of predefined steps) to automate site-level recovery operations on your IT infrastructure in an event of downtime.
- Auto-discovery and real-time tracking for recovery objectives.

- Ability to perform non-disruptive testing (rehearsal) on your virtual machines and applications to ensure that your infrastructure is adequately prepared for protection in an event of disaster.
- Reporting capabilities providing details about resiliency health of applications and virtual machines.

See [“Understanding the role of resiliency groups in disaster recovery operations”](#) on page 51.

## Understanding the role of resiliency groups in disaster recovery operations

To perform disaster recovery (DR) operations on virtual machines or applications, first they must be placed in a resiliency group, which is the unit of failover in Veritas Resiliency Platform.

You can configure resiliency groups without enabling them for disaster recovery. You can perform the start or stop operations on resiliency groups that are not enabled for DR. However, you cannot perform DR operations on a resiliency group without first enabling the resiliency group for disaster recovery. You can enable disaster recovery when you create the resiliency group, or at a later point of time you can select the resiliency group and perform the **Configure DR** operation.

After you enable and configure disaster recovery on a resiliency group, you can proceed with DR-specific tasks on the resiliency group, such as migrate and takeover.

A Virtual Business Service (VBS) lets you further group these resiliency groups in a vertical grouping mechanism, and lets you perform controlled start, stop and recovery operations on these resiliency groups.

See [“About resiliency groups”](#) on page 30.

# Managing disaster recovery for applications

This chapter includes the following topics:

- [About disaster recovery for applications](#)
- [Pre-requisites for disaster recovery of applications](#)
- [About replication technologies used in disaster recovery of applications](#)
- [An overview of key steps required for disaster recovery of applications](#)

## About disaster recovery for applications

You can use Veritas Resiliency Platform to perform disaster recovery operations for the applications in your data center. For more information on supported applications and their versions refer to *Hardware and Software Compatibility List (HSCL)*.

Create a resiliency group with the required applications, configure disaster recovery on the resiliency group, and then perform the following operations.

- **Migrate:** A planned activity involving graceful shutdown of applications at the production data center and starting them at the recovery data center. In this process, replication ensures that consistent application data is made available at the recovery data center.
- **Takeover:** An activity initiated when the production data center is down due to any disaster or natural calamities, and the applications need to be restored at the recovery data center in order to provide business continuity.

See [“Migrating a resiliency group of applications”](#) on page 70.

See [“Taking over a resiliency group of applications”](#) on page 71.

# Pre-requisites for disaster recovery of applications

To be able to perform disaster recovery (DR) operations on the applications in the data center, ensure that the following requirements are met.

- You have set-up replication for the applications.
- You have preconfigured the applications at the DR data center.
- You have grouped the applications in a resiliency group.
- You have configured disaster recovery for the resiliency group.

See [“About resiliency groups”](#) on page 30.

See [“About replication technologies used in disaster recovery of applications”](#) on page 53.

## About replication technologies used in disaster recovery of applications

For a successful disaster recovery operation of applications, you need to ensure that the data is synchronized between the primary and the secondary data centers. This is achieved using data replication.

The following tables list the supported configurations based on array replication and clustering:

**Table 7-1** Supported configurations using EMC Symmetrix Remote Data Facility (SRDF) and RecoverPoint replication

Operating System	Type of host	Clustering	Supported
Windows	Hyper-V virtual machine	Microsoft Failover Clustering (MS FoC)	No
Windows	VMware virtual machine	MS FoC	No
Windows	Physical systems	MS FoC	Yes
Windows	Hyper-V virtual machine	Non - MS FoC	Yes
Windows	VMware virtual machine	Non - MS FoC	Yes

**Table 7-1** Supported configurations using EMC Symmetrix Remote Data Facility (SRDF) and RecoverPoint replication (*continued*)

Operating System	Type of host	Clustering	Supported
Windows	Physical systems	Non - MS FoC	Yes
Linux	Hyper-V virtual machine	NA	No
Linux	VMware virtual machine	NA	Yes
Linux	Physical systems	NA	Yes

**Table 7-2** Supported configurations using NetApp SnapMirror replication

Operating System	Type of host	Supported
Linux	Hyper-V virtual machine	No
Linux	VMware virtual machine	Yes
Linux	Physical systems	Yes

## An overview of key steps required for disaster recovery of applications

This section lists the key steps required to configure the disaster recovery for applications using Resiliency Platform.

**Table 7-3** Disaster recovery for applications - an overview of key steps

Action	Description	Refer to
Set up your replication environment	Configuration before you install Resiliency Platform. It includes configuring applications on physical and virtual machines, configuring replication and so on.	<p>See <a href="#">“Configuring application disaster recovery using EMC SRDF replication”</a> on page 87.</p> <p>See <a href="#">“Configuring application disaster recovery using NetApp SnapMirror replication”</a> on page 90.</p> <p>See <a href="#">“Configuring application disaster recovery using EMC RecoverPoint replication”</a> on page 91.</p>

**Table 7-3** Disaster recovery for applications - an overview of key steps  
*(continued)*

Action	Description	Refer to
Add the asset infrastructure	Add the asset infrastructure to the Infrastructure Management Server (IMS) using the Resiliency Platform web console.	Refer to the <i>Deployment Guide</i> .
Configure your assets for disaster recovery	Group the required applications in a resiliency group and enable disaster recovery for the resiliency group.	See <a href="#">“Managing and monitoring applications”</a> on page 31. See <a href="#">“ Modifying a resiliency group”</a> on page 41. See <a href="#">“Protecting applications”</a> on page 33. See <a href="#">“Configuring disaster recovery for a resiliency group of applications”</a> on page 56.
DR operations	Perform the required DR operations: Migrate and takeover.	See <a href="#">“Migrating a resiliency group of applications”</a> on page 70. See <a href="#">“Taking over a resiliency group of applications”</a> on page 71.

# Preparing for disaster recovery operations

This chapter includes the following topics:

- [Configuring disaster recovery for a resiliency group of applications](#)
- [Viewing the details of a disaster recovery-enabled resiliency group](#)

## Configuring disaster recovery for a resiliency group of applications

Before you configure disaster recovery (DR) for a resiliency group of applications, make sure of the following:

- The selected resiliency group must have applications from the production data center and the recovery data center.
- Application binaries should be stored on local storage and data files on replicated storage.
- The DNS server settings should be configured for both data centers. DNS settings are required for binding a host name to different IP addresses on the DR site. This is required only if you plan to use the Resiliency Platform for performing DNS updates.

For more information on configuring DNS server settings, see the *Deployment Guide*.

- For applications on Windows with Failover Clustering, you may have to plumb or unplumb the IP addresses using appropriate Failover Clustering roles. If Failover Clustering is not used, you must plumb the application IP addresses on all the systems across the data centers. The Resiliency Platform console does not manage plumbing or unplumbing of IP address for applications.



- Ensure that you have disabled the 'Quick removal' policy for disks in Windows Server 2008 R2 and disabled the 'write-cache' policy for disks in Windows Server 2012 R2.

A successful DR configuration enables takeover and migrate operations.

You can also protect your applications by creating a resiliency group and setting up disaster recovery for the group in a single wizard panel.

See [“Protecting applications”](#) on page 33.

### To configure disaster recovery for a resiliency group of applications

#### 1 Navigate



**Assets** (navigation pane)

#### Resiliency Groups

- 2 Double-click the desired resiliency group.
- 3 In the resiliency group details page, click **Configure DR**.
- 4 In the **Selected Assets** page, review the applications on the primary site and the DR site. Click **Next**.
- 5 The **DNS Setting for Primary and DR DC** pages let you map the host names to IP addresses for individual sites.
- 6 Review your selections and click **Submit**.

When the configuration is complete, a notification is displayed and the **DR Status** column on the resiliency group listing page displays the status as **Configured**.

See [“Viewing the details of a disaster recovery-enabled resiliency group”](#) on page 57.

See [“Migrating a resiliency group of applications”](#) on page 70.

See [“Taking over a resiliency group of applications”](#) on page 71.

## Viewing the details of a disaster recovery-enabled resiliency group

The Veritas Resiliency Platform console provides information about a resiliency group for which disaster recovery (DR) operation is configured successfully. The information includes the state of the replication for the resiliency group (for example, synchronized), used replication technology (for example, EMC SRDF), associated alerts, the details about the applications or the virtual machines in the resiliency group, replication lag, recovery time, and so on.

From this view, you can also set the replication lag threshold. For more information on setting the threshold, see:

See [“Setting up replication lag threshold”](#) on page 64.

Note that for virtual machines, the recovery time is available only after the rehearse operation is complete.

### To view the details of a disaster recovery-enabled resiliency group

#### 1 Navigate



**Assets** (navigation pane)

#### Resiliency Groups

- 2 On the resiliency groups tab, double-click the resiliency group for which disaster recovery is already configured. That is, the **DR Status** column shows the status of the resiliency group as **Configured**.

See [“Displaying resiliency group details”](#) on page 40.

# Rehearsing DR operations to ensure DR readiness

This chapter includes the following topics:

- [Ensuring the disaster recovery readiness of your Resiliency Platform assets using the rehearse operation](#)
- [Rehearse operations for applications](#)
- [Performing rehearsal cleanup](#)

## Ensuring the disaster recovery readiness of your Resiliency Platform assets using the rehearse operation

Use the **Rehearse** option on the Resiliency Platform console to perform the disaster recovery rehearsal, which verifies the ability of your configured resiliency group to fail over to the disaster recovery (DR) data center during disaster. A rehearsal is a zero-downtime test that mimics the configuration, application data, storage, replication, and the fail over behavior of your resiliency group.

---

**Note:** You can perform the Rehearsal operation only on the recovery data center.

---

**To perform the rehearse operation****1** Navigate**Assets** (navigation pane)**Resiliency Groups**

- 2** Double-click the resiliency group for which DR is already configured. That is, the DR Status column shows the status of the resiliency group as CONFIGURED.
- 3** On the resiliency group details page, click **Rehearse**.
- 4** Select the recovery data center and then click **Submit**.

Before you perform the rehearse operation again, you need to ensure that the previous rehearsal is cleaned up by running the Rehearse Cleanup operation.

See [“Performing rehearsal cleanup”](#) on page 62.

## Rehearse operations for applications

**Rehearse operations with EMC SRDF based replication:**

- Device group should be associated with the snapshot LUNs. Veritas Resiliency Platform supports Timefinder Snap and Timefinder Mirror (BCV).
- Rehearsal operations for resiliency groups that are replicated using EMC SRDF technology in Asynchronous mode cannot be performed using TimeFinder Snap technology (VDEV devices). You need to configure Timefinder Mirrors (BCV devices) to perform the rehearsal operations on such resiliency groups.
- When the rehearse operation is initiated, the Resiliency Platform creates point in time snapshots as a part of the rehearsal operations, since it cannot work with the existing snapshots.

---

**Note:** If there are any active snapshots that are in progress, you need to terminate the snapshots and refresh the asset discovery.

---

- The snapshot disks are enabled on the DR hosts.
- For Linux hosts, the logical volume manager (LVM) volume group (VG) is imported using the snapshot disks. The LVM volume, on the snapshot VG, is then mounted on a mount point. This mount point is same as that of the VG on the DR host if you were to perform the takeover or migrate operation.

- For Windows host, the snapshot disk is assigned a drive letter. This drive letter is the same as that of the replicated disk if you were to perform the takeover or migrate operation.
- The application is then started on the DR hosts. The application starts to consume storage from the snapshot disks instead of the replicated disks.
- During the Rehearse cleanup operation, the above tasks are reversed and the snapshots are terminated, bringing the system back to the original state.

**Rehearse operations with NetApp SnapMirror based replication:**

- NetApp SnapMirror based replication uses FlexClone for the Rehearse operation and so NetApp storage server must be enabled with the FlexClone license.
- When the rehearse operation is initiated, the Resiliency Platform creates a point in time volume snapshot as a part of the rehearsal operation. The snapshot volume is exported and mounted on the DR host.

---

**Note:** Rehearse operation breaks any ongoing replication between the source storage server and the destination storage server as the FlexClone operation cannot be performed on the destination read-only volume. SnapMirror replication resumes after the rehearsal cleanup operation is complete.

---

- The application is then started on the DR hosts. The application starts to consume storage from the snapshot disks instead of the replicated disks.
- During the Rehearse cleanup operation, the above tasks are reversed and the snapshots are terminated, bringing the system back to the original state.

**Rehearse operations with EMC RecoverPoint based replication:**

- When the rehearse operation is initiated, the Resiliency Platform creates a point in time volume snapshot as a part of the rehearsal operation. The snapshot volume is exported and mounted on the DR host.

---

**Note:** If there are any active snapshots, you need to terminate the snapshots and refresh the asset discovery.

---

- The application is then started on the DR hosts. The application starts to consume storage from the snapshot disks instead of the replicated disks.
- During the Rehearse cleanup operation, the above tasks are reversed and the snapshots are terminated, bringing the system back to the original state.

# Performing rehearsal cleanup

After you have performed the rehearse operation successfully to verify the ability of your configured resiliency group to fail over on to the disaster recovery data center, you can use the rehearsal cleanup operation to clean up the rehearsal virtual machines or applications in the resiliency group. All temporary objects created during the rehearsal operation are now deleted.

## To perform rehearsal cleanup

- 1 Navigate



**Assets** (navigation pane)

**Resiliency Groups**

- 2 Select the data center, and then click **Submit**.
- 3 Double-click the resiliency group for which DR is already configured. That is, the DR Status column shows the status of the resiliency group as CONFIGURED.
- 4 Click **Rehearse Cleanup**.
- 5 Select the data center and click **Submit**.

See [“Ensuring the disaster recovery readiness of your Resiliency Platform assets using the rehearse operation”](#) on page 59.

# Monitoring risks

This chapter includes the following topics:

- [About risk insight](#)
- [Displaying risk information](#)
- [Predefined risks in Resiliency Platform](#)
- [Viewing the current risk report](#)
- [Viewing the historical risk report](#)

## About risk insight

The objective of the Risk Insight feature is to notify you about the vulnerabilities that might impact the recoverability or continuity of your protected assets.

Risk Insight detects the changes to the state and configuration of your protected assets. It identifies if there is a risk to the recoverability or continuity of your protected assets.

Veritas Resiliency Platform also enables you to set up the replication lag threshold or service level threshold. Risk insight alerts you when the replication lags beyond the threshold that you specified.

See [“Setting up replication lag threshold”](#) on page 64.

Risk insight generates two types of reports:

- **Current risk reports:** Provides the summary and detail information about all the current risks in your data center.
- **Historical risk reports:** Provides a summary and a detailed analysis of information about the risks in your environment during the specified period.

These reports help you take actions to prevent such risks. The historical risk data is purged after a period of two years.

The risks covered by risk insight can be classified into three main categories:

**Table 10-1**

Risk Type	Description
Recoverability	Risks that may impact the ability to recover and run the application on the recovery site.
Continuity	Risks that may impact the ability to run your applications without disruption either on your production site or on your recovery site.
SLA	Risks that may impact the ability to fulfill the service level agreements (SLA) for your applications.

On the basis of criticality, the risks can be classified into two types:

**Table 10-2**

Risk type	Description
Error	A risk that disrupts any stated goals of the product. An error must be fixed to make the product work as expected.
Warning	A risk that jeopardizes any stated goals of the product. A warning alerts you about a potential problem in your environment.

## Setting up replication lag threshold

Veritas Resiliency Platform enables you to set up the replication lag or service level agreement (SLA) threshold.

### To set up replication lag threshold

#### 1 Navigate



**Assets > Resiliency Groups** tab

- 2 On the resiliency groups tab, double-click the resiliency group for which disaster recovery is already configured. The next page provides the details about the resiliency group.
- 3 Under **Replication**, enter the value for **Replication lag threshold**. Select the unit of time, and click **Save**.

See [“About risk insight”](#) on page 63.





# Displaying risk information

Resiliency Platform identifies and flags several risks that may occur during data center operations. Some of these risks are transient. They are temporary and resolve themselves without your intervention. Other risks require intervention and troubleshooting to resolve.

You can display risks in the following ways:

**Table 10-3** Ways to display risks

To display ...	Do the following:
A complete list of risks across the resiliency domain	<ol style="list-style-type: none"><li>1 On the menu bar, select  <b>More Views &gt; Risks</b></li><li>2 On the <b>Risk</b> page, double-click a risk in the table to display detailed information.</li></ol>
Risks that are associated with a specific resiliency group or virtual business service	<ol style="list-style-type: none"><li>1 On the navigation pane, select  (Assets) and the tab for either <b>Resiliency Groups</b> or <b>Virtual Business Services</b>.</li><li>2 On the tab, double-click a resiliency group or virtual business service to display detailed information.</li><li>3 On the details page, note any risks that are listed in the <b>At Risk</b> area, and double-click the risk for details.</li></ol>

In addition to the above mentioned views, the **More views > Logs > All** view and the **More views > Logs > Notification** view also includes the notification about the risks in your environment. You can double-click any row to view the detailed description of the error and suggested resolution for the error.

## Predefined risks in Resiliency Platform

Table 10-4 lists the predefined risks available in Resiliency Platform. These risks are reflected in the current risk report and the historical risk report.

**Table 10-4**      Predefined risks

Risks	Description	Risk detection time	Risk type	Affected operation	Fix if violated
New VM added to replication storage	Checks if a virtual machine that is added to a consistency group on a primary site, is not a part of the resiliency group.	5 minutes	Error	<ul style="list-style-type: none"> <li>■ Migrate</li> <li>■ Takeover</li> <li>■ Rehearse</li> </ul>	Add the virtual machine to the resiliency group.
Replication lag exceeding threshold	Checks if the replication lag exceeds the thresholds that are defined by the user for each resiliency group.	5 minutes	Warning	<ul style="list-style-type: none"> <li>■ Migrate</li> <li>■ Takeover</li> </ul>	Contact the appropriate administrator
Replication state broken/critical	Checks if the replication is not working or is in a critical condition for each resiliency group.	5 minutes	Error	<ul style="list-style-type: none"> <li>■ Migrate</li> <li>■ Takeover</li> </ul>	Contact the enclosure vendor.
Remote mount point already mounted	Checks if the mount point is not available for mounting on target site for any of the following reasons: <ul style="list-style-type: none"> <li>■ Mount point is already mounted.</li> <li>■ Mount point is being used by other assets.</li> </ul>	<ul style="list-style-type: none"> <li>■ Native (ext3, ext4,NTFS ): 30 minutes</li> <li>■ Virtualization (VMFS, NFS): 6 hours</li> </ul>	Warning	<ul style="list-style-type: none"> <li>■ Migrate</li> <li>■ Takeover</li> </ul>	Unmount the mount point that is already mounted or is being used by other assets.
Disk utilization critical	Checks if at least 80% of the disk capacity is being utilized. The risk is generated for all the resiliency groups associated with that particular file system.	<ul style="list-style-type: none"> <li>■ Native (ext3, ext4,NTFS ): 30 minutes</li> <li>■ Virtualization (VMFS, NFS): 6 hours</li> </ul>	Warning	<ul style="list-style-type: none"> <li>■ Migrate</li> <li>■ Takeover</li> <li>■ Rehearse</li> </ul>	Delete or move some files or uninstall some non-critical applications to free up some disk space.
Control host not reachable	Checks if the discovery daemon is down on the Control Host.	15 minutes	Error	<ul style="list-style-type: none"> <li>■ Migrate</li> </ul>	Resolve the discovery daemon issue.

**Table 10-4** Predefined risks (*continued*)

Risks	Description	Risk detection time	Risk type	Affected operation	Fix if violated
ESX not reachable	Checks if the ESX server is in a disconnected state.	5 minutes	Error	<ul style="list-style-type: none"><li>■ On primary site: start or stop operations</li><li>■ On secondary site: migrate or takeover operations</li></ul>	Resolve the ESX server connection issue.
vCenter Server not reachable	Checks if the virtualization server is unreachable or if the password for the virtualization server has changed.	5 minutes	Error	<ul style="list-style-type: none"><li>■ On primary site: start or stop operations</li><li>■ On secondary site: migrate or takeover operations</li></ul>	Resolve the virtualization server connection issue.  In case of a password change, resolve the password issue.
Insufficient compute resources on failover target	Checks if there are insufficient CPU resources on failover target in a virtual environment.	6 hours	Warning	<ul style="list-style-type: none"><li>■ Migrate</li><li>■ Takeover</li></ul>	Reduce the number of CPUs assigned to the virtual machines on the primary site to match the available CPU resources on failover target.

[Table 10-5](#) describes some risks that are displayed in Resiliency Platform console, but these risks are not reflected in the risk reports.

Table 10-5 Other risks

Risk	Description
HOST_SFMMH_REINSTALLED	The host is disconnected. The probable cause is that the host has been reinstalled. Changes you make after this condition are not reflected on the Resiliency Manager. To correct this issue, remove and re-add this host to the Infrastructure Management Server (IMS).
HOST_DISCONNECTED_MAC_CHANGED	The host is disconnected. The probable cause is that the media access code (MAC) address of host has changed. Changes you make after this condition are not reflected on the Resiliency Manager. To correct this issue, remove and re-add this host to the Infrastructure Management Server (IMS).
VMWARE_DISCOVERY_FAILED	VMware discovery failed.
FS_FILESYSTEM_FULL	The file system is at 100% usage.

## Viewing the current risk report

This report provides the summary and detail information about all the current risks in your data center. The high-level summary shows the total number of risks and its distribution by severity.

The **Distribution by type** chart displays the severity-wise distribution for recoverability, continuity, and service level agreement (SLA).

The **Unresolved risks** chart shows the risks that are unresolved for more than one month, for last one month, and for last one week. The **Recent Risks** chart shows the recent risks that are generated in the last 24 hours.

The **Current risks details by type** table provides detailed information such as the name of the resiliency group which is at risk, the name of the risk, its description, object at which the risk is generated, severity, and date and time on which the risk was generated.

### To view the current risk report

- 1 Navigation:  
Click **Reports**(menu bar).
- 2 In the **Risk > Current Risk Report** section, click **Run** or **Schedule** to receive the report on the specified email address.

# Viewing the historical risk report

This report provides a summary and a detailed analysis of information about the risks in your environment during the specified period.

The high-level summary shows the total number of risks and its distribution by the time the risks have been open. The information is categorized under various headings such as **Carried forward**, **New**, **Closed**, and **Still open**.

Within these categories, you can see severity wise distribution (high or low) and category wise distribution (recoverability, continuity, and service level agreement) of the risks.

The detailed analysis is displayed in the form of various charts:

- The various charts under **Risk by Category** display the open risks and new risks in the recoverability, continuity, and SLA categories at specific points of time within the duration specified by you.
- The **Resolving time chart** shows the average time to resolve the risk within the recoverability, continuity, and SLA categories.
- The **5 risks that took the longest time to resolve** chart shows the top 5 risks that took the longest time to be resolved, within the recoverability, continuity, and SLA categories. This information is displayed per resiliency group or per Virtual Business Service (VBS).

## To view the historical risk report

- 1 Navigation:  
Click **Reports**(menu bar).
- 2 In the **Risk > Risk History Report** section, click **Run** or **Schedule** to receive the report on the specified email address.

# Performing disaster recovery operations

This chapter includes the following topics:

- [Migrating a resiliency group of applications](#)
- [Taking over a resiliency group of applications](#)
- [Performing the resync operation](#)

## Migrating a resiliency group of applications

A typical application migration involves the following steps. These steps are performed automatically by the Resiliency Platform as a part of the migrate operation.

- At the primary data center, stop the application and storage.
- Reverse the replication role.
- At the recovery data center, start the storage and application.
- Update the DNS resource records.

### To migrate applications

#### 1 Navigate



**Assets** (navigation pane)

**Resiliency Groups**

#### 2 Do one of the following:

- Double-click the resiliency group for which DR is already configured. Skip to Step 3
  - Right-click the resiliency group for which DR is already configured, and select **Migrate**.
  - Click the vertical ellipses and select **Migrate**.
- 3 On the resiliency group details page, click **Migrate**.
  - 4 Select the target data center and then click **Submit**.

## Taking over a resiliency group of applications

Takeover is an activity initiated when the production data center is down due to any disaster or natural calamities, and the applications need to be restored at the recovery data center to provide business continuity.

### To perform takeover operation on applications

- 1 Navigate



**Assets** (navigation pane)

**Resiliency Groups**

- 2 Do one of the following:
  - Double-click the resiliency group for which DR is already configured. Skip to Step 3
  - Right-click the resiliency group for which DR is already configured, and select **Takeover**.
  - Click the vertical ellipses and select **Takeover**.
- 3 On the resiliency group details page, click **Takeover**.
- 4 Select the target data center, and then click **Submit**.

## Performing the resync operation

When disaster strikes on a production data center, the Takeover operation is invoked to start the resiliency groups on the recovery data center.

Since the production data center is not working the data replication between the two sites does not happen. Later when the production site is up and running you

need to prepare the site for next failover or migrate operation. This includes cleaning up any residue and resuming the replication from recovery to production site.

Use the Resync operation on the Resiliency Platform console to automate these steps for the required resiliency groups. This operation cleans up the residue which includes stopping applications and virtual machines, deregistering virtual machines, unmounting file systems, datastores, etc.

Resync operation can be performed only if the last Takeover operation was successfully completed.

---

**Note:** Resync operation must be performed at an individual resiliency group level.

---

### Performing the resync operation

#### 1 Navigate



**Assets** (navigation pane)

**Resiliency Groups**

- 2 Double click the resiliency group for which DR is already configured. That is, the DR Status column shows the status of the resiliency group as **Configured**.
- 3 On the resiliency group details page, click **Resync**.
- 4 In the **Resync** panel, select the production data center name from the drop-down list, and click **Submit**.



# Managing activities and resiliency plans

This chapter includes the following topics:

- [Managing activities](#)
- [Managing resiliency plans](#)

## Managing activities

Using the Veritas Resiliency Platform console, you can view the sub task information for a task or an operation that is performed on the console.

See [“Viewing activities”](#) on page 73.

See [“Aborting a running activity”](#) on page 74.

## Viewing activities

Using the Veritas Resiliency Platform console, you can view the sub task information for a task or an operation that is performed on the console. You can view the details on the **Activities** page. Details such as the status of the operation (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed are displayed. You can view these details for a currently running task and for the completed tasks. On the **Current** page you can abort a running task.

Click on a currently running task, to view the details in a graphical representation. The steps that are completed are shown in green color along with the success icon. The ongoing steps are in blue color with the loader image, and the future steps are in gray. Expand **Execution Details** to view all the sub-tasks that comprise the task.

**To view activities****1** Navigate

Do one of the following:



**Activities** (menu bar).

**2** Choose either of the following:

- Select **Current** to view the currently running tasks.
- Select **Completed** to view the historical tasks.

To view recent activities, click **Recent Activities** on the bottom pane.

See [“Aborting a running activity”](#) on page 74.

## Aborting a running activity

Using the Veritas Resiliency Platform console, you can abort a task or an operation which is currently running. You can abort an operation that is executed using a resiliency plan or from the console. When you abort an operation, the sub task which is in progress is completed and then the process is aborted. The status of the sub tasks which were already completed does not change.

For example, the migrate resiliency group operation has six sub tasks. If you abort the operation while the first sub task, Stop Virtual Machine, is in progress, then the Stop Virtual Machine sub task is completed and the remaining sub tasks are skipped. If you restart the migrate operation, it starts from the beginning.

**To abort an activity****1** Navigate

Do one of the following:



**Activities**. Skip to Step [2](#)

**Recent Activities (bottom pane)**. Click **Abort** on the required activity.

**2** In the **Current** activities page, place your cursor on the activity that you want to abort. Do one of the following:

- Right click your mouse and click **Abort**.
- Click on the vertical ellipsis and select **Abort**

See [“Viewing activities”](#) on page 73.

## Managing resiliency plans

Veritas Resiliency Platform provides a console for creating and customizing resiliency plans. The following topics cover how to create, edit, delete resiliency plan templates and resiliency plans and how to execute resiliency plans.

See [“About resiliency plans”](#) on page 75.

See [“Creating a new resiliency plan template”](#) on page 76.

See [“Editing a resiliency plan template”](#) on page 79.

See [“Deleting a resiliency plan template”](#) on page 80.

See [“Viewing a resiliency plan template”](#) on page 80.

See [“Creating a new resiliency plan”](#) on page 81.

See [“Editing a resiliency plan”](#) on page 82.

See [“Deleting a resiliency plan”](#) on page 83.

See [“Executing a resiliency plan”](#) on page 83.

See [“Viewing a resiliency plan”](#) on page 83.

See [“Creating a schedule for a resiliency plan”](#) on page 84.

See [“Editing a schedule for a resiliency plan”](#) on page 84.

See [“Deleting a schedule for a resiliency plan”](#) on page 85.

See [“Viewing a schedule for a resiliency plan”](#) on page 85.

## About resiliency plans

Using the Veritas Resiliency Platform console you can create customized resiliency plans. A resiliency plan is a customized set of tasks that you can run as a single operation. You add each task and the particular assets on which to run the task. If you intend to use the same sequence of tasks on different assets, you can create a resiliency template. You can save the template and use it to create multiple resiliency plans.

For example, you can create a resiliency plan template to migrate a resiliency group or virtual business service (VBS). Then you can add a resiliency group or VBS to the template to create a plan. You can create multiple plans using the same template.

You can create customized resiliency plans for the following tasks:

- Start a resiliency group.

- Stop a resiliency group.
- Migrate a resiliency group.
- Takeover a resiliency group.
- Manual task
- Run a custom script

You do not have to create a template in order to create a resiliency plan. Resiliency plans can be created using blank templates.

---

**Note:** To create a plan for migrate, takeover, rehearse, or cleanup operation, configure disaster recovery task must be successful on the selected resiliency group or VBS.

---

See [“Creating a new resiliency plan template”](#) on page 76.

See [“Creating a new resiliency plan”](#) on page 81.

## Creating a new resiliency plan template

Using the Veritas Resiliency Platform console, you can create a customized resiliency plan template for the following operations:

- Start and stop a resiliency group.
- Migrate and takeover a resiliency group.
- Manual task  
See [“About manual task”](#) on page 77.
- Run a custom script  
See [“About custom script”](#) on page 78.

To create a template, you need to drag and drop the required operation from the stencil into the canvas below. The arrow lets you connect various operations in the canvas.

For example, if you want to create a template to perform the Start Resiliency Group task, drag the operation from the top bar into the canvas. Now click on the arrow on the **Start** action box and drag the mouse to the **Start Resiliency** In addition to the above listed tasks, you can also add a custom script Manual task in the resiliency plan. This task temporarily pauses the operation letting you perform a task before proceeding further.

**Group** action box. Similarly you can drag the arrow from the **Start Resiliency Group** action box to the **End** action.

### To create a new resiliency plan template

- 1 Navigate  
**Resiliency Plans** (menu bar) or **Quick Actions > Resiliency Plans**
- 2 In the **Templates** section, click **New**.
- 3 In the **Create New Template** wizard panel, enter a name and a description for the template.
- 4 Drag and drop the required operation into the canvas. Connect the **Start** and **Stop** actions to the operation.
- 5 Click **Create**.

See [“About resiliency plans”](#) on page 75.

## About manual task

Using the Resiliency Platform console, you can add a manual task in the resiliency plan. The purpose of including this task in resiliency plan is to temporarily pause the operation of the resiliency plan to perform a task or validate a step before you proceed further.

You can specify a timeout for the manual task. After the specified timeout expires, the manual task in the resiliency plan is marked as complete and the resiliency plan proceeds further.

Alternatively, you can opt for manually resuming the process. In this case, the resiliency plan enters into a pause state. You need to go to the **Inbox** in Resiliency Platform console and click **Resume** on the corresponding entry in the **Inbox**. You can also resume the resiliency plan by right-clicking the corresponding entry in **Activities > Current Activities** and selecting **Resume**.

## Using manual tasks in resiliency plans

Using the Resiliency Platform console, you can add a manual task in the resiliency plan.

### To use a manual task in a resiliency plan

- 1 You can add a manual task to a resiliency plan template or to a resiliency plan.  
See [“Creating a new resiliency plan template”](#) on page 76.  
See [“Creating a new resiliency plan”](#) on page 81.
- 2 Drag and drop **Manual Task** into the canvas. Click the pencil icon in the action box to add the task details.
- 3 Provide a name for the manual task.

- 4 Describe the reason why you want to add this manual task to the resilient plan.
- 5 Select your choice for resuming the process manually or automatically. If you select the option for automatically resuming the process after a timeout, enter the duration of timeout in minutes. Click **Save**.

## About custom script

Using the Resiliency Platform console, you can add a custom script execution task in the resiliency plan. You can use the custom script execution task to perform customized operations before executing the next step of the resiliency plan such as repurposing capacity on the recovery site, orchestrate network changes, or any kind of post-processing.

Custom Script execution requires Resiliency Platform 1.1 or later on the Resiliency Manager, Infrastructure Management Server (IMS) and the hosts executing custom scripts. In addition, if you are using VRP together with Veritas InfoScale, the Resiliency Platform Enablement Add-on have to be manually installed on applicable hosts.

The custom script can be in any format that can be directly executed on a shell on the target host. For the Linux hosts, it may be an executable or a script that specifies the interpreter on the shebang line such as a shell or a Perl script. For Windows hosts, it may be an executable or a script with known extension such as a bat file or a PowerShell script. The Script is executed as root user on a UNIX host or as Local System on a Windows host. You may use `sudo` or `RunAs` commands to execute some other scripts from these custom scripts.

Before you can execute the script as part of the resiliency plan, you need to manually copy the script to the `VRTSsfmh InstallDir\vrp/scripts` directory on the host.

Where, `VRTSsfmh InstallDir` is `/opt/VRTSsfmh` on the Unix/Linux hosts and `SystemDrive/Program Files/VERITAS/VRTSsfmh` on the Windows hosts. Copying the script to these specific folders enforces the security policy for running a custom script since these folders can be accessed only by a root user or a Local System.

Exit code from script execution determines the success or failure of the task in the resiliency plan workflow. An exit code of zero means the script execution was successful while a non-zero exit code means the script execution failed. If you select the option to ignore the exit code, the script task is always marked as successful after completion of the script. You can select this option, if your script does not return any exit code. You can view the output of the script in activity details for the resiliency plan in Resiliency Platform console.

If you uninstall the host package from the host where you have copied your custom script, the custom script is removed from the host as part of the uninstallation process.

## Using custom scripts in resiliency plans

Using the Resiliency Platform console, you can add a custom script execution task in the resiliency plan.

### To use a custom script execution task in a resiliency plan

- 1 You can add a custom script execution task to a resiliency plan template or to a resiliency plan.  
  
See [“Creating a new resiliency plan template”](#) on page 76.  
  
See [“Creating a new resiliency plan”](#) on page 81.
- 2 Drag and drop **Custom Script** into the canvas. Click the pencil icon in the action box to add the task details.
- 3 Enter a name for the custom script.
- 4 Select the data center and the host where you want to execute the script. Click **Next**.
- 5 Enter the following details:
  - The relative path of the script on the specified host. The script path that you enter is taken as relative to the `VRTSsfmh InstallDir/vrp/scripts/` directory path.  
For example, if you enter the path of the script as `myscripts/backup_scripts/script_name`, then the complete path considered by the system will be `VRTSsfmh InstallDir/vrp/scripts/myscripts/backup_scripts/script_name`.
  - Command-line arguments to the script. This is an optional input field.
  - Timeout for the script. By default, there is no timeout for the script execution. You can specify a timeout for the script execution. After the specified timeout expires, the script execution task in the resiliency plan is marked as failure but the script execution task is not stopped. The script execution may continue in the background. If you do not specify any timeout, the task will wait till the script is not completed.
- 6 Click **Save**.

## Editing a resiliency plan template

Using the Veritas Resiliency Platform console, you can edit an existing resiliency plan template.

You can add assets to these templates and create a customized resiliency plan. Any changes to the template do not affect the existing resiliency plans that you created from the template.

### To edit a resiliency plan template

- 1    Navigate  
     **Resiliency Plans** (menu bar) or **Quick Actions > Resiliency Plans**
  - 2    In the **Templates** list, place your cursor on the row which you want to edit. Do one of the following:
    - Right click your mouse and click **Edit**.
    - Click on the vertical ellipsis and select **Edit**.
  - 3    In the **Edit Template** wizard panel, edit the required actions and click **Save**.  
     The steps for editing the plan are the same as creating it.
- See [“Creating a new resiliency plan template”](#) on page 76.

## Deleting a resiliency plan template

Using the Veritas Resiliency Platform console you can delete an existing resiliency plan template.

Deleting the template does not affect the existing resiliency plans that you created from the template.

### To delete a resiliency plan template

- 1    Navigate  
     **Resiliency Plans** (menu bar) or **Quick Actions > Resiliency Plans**
  - 2    In the **Templates** list, place your cursor on the row which you want to delete. Do one of the following:
    - Right click your mouse and click **Delete**.
    - Click on the vertical ellipsis and select **Delete**.
  - 3    In the **Delete Template** panel click **Delete**.
- See [“Creating a new resiliency plan template”](#) on page 76.

## Viewing a resiliency plan template

Using the Veritas Resiliency Platform console, you can view the details of a resiliency plan template. To view the details of the resiliency plan templates, you need to have at least guest persona assigned to you.



### To view a resiliency plan template

- 1 Navigate  
**Resiliency Plans** (menu bar) or **Quick Actions > Resiliency Plans**
- 2 In the **Templates** list, do one of the following:
  - Double click the row that you want to view.
  - Select the row that you want to view, right click and select Details.
  - Select the row that you want to view, click on the vertical ellipsis and select Details.
- 3 You can now view the details of the resiliency plan template.

## Creating a new resiliency plan

Using the Veritas Resiliency Platform console, you can create a new resiliency plan for the following operations. Resiliency plans can be created using an existing template or with a blank template. When you create a plan using a blank template, you need to create the plan and add the assets at the same time.

- Start and stop a resiliency group.
- Migrate and takeover a resiliency group.
- Manual task  
 See [“About manual task”](#) on page 77.
- Run a custom script  
 See [“About custom script”](#) on page 78.

---

**Note:** To create a plan for migrate, takeover, rehearse, or cleanup operation, disaster recovery must be configured successfully on the selected resiliency group or the VBS.

---

### To create a new resiliency plan using blank template

- 1 Navigate  
**Resiliency Plans** (menu bar) or **Quick Actions > Resiliency Plans**
- 2 In the **Saved Plans** section, click **New**.
- 3 In the **Create Saved Plan - Select Template** wizard panel, select **Blank Template**, and click **Next**.
- 4 In the **Add Assets** panel, enter name and description.

- 5 Drag and drop the required operation into the canvas. Connect the **Start** and **Stop** actions to the operation.
- 6 Click the pencil icon in the action box to add relevant assets. Select the data center whose assets you want to add to the template. Click **Add**.
- 7 Click **Submit**.

#### To create a new resiliency plan using predefined template

- 1 Navigate  
**Resiliency Plans** (menu bar) or **Quick Actions > Resiliency Plans**
- 2 In the **Saved Plans** section, click **New**.
- 3 In the **Create Saved Plan - "Select Template"** wizard panel, select **Pre-defined Template**.
- 4 Select a template from the list and click **Next**.
- 5 In the **Add Assets** panel, name and description are pre-populated.
- 6 Click the pencil icon in the action box to add relevant assets. Select the data center whose assets you want to add to the template. Click **Add**.
- 7 Click **Submit**.

See ["About resiliency plans"](#) on page 75.

See ["Deleting a resiliency plan"](#) on page 83.

See ["Executing a resiliency plan"](#) on page 83.

## Editing a resiliency plan

Using the Veritas Resiliency Platform console, you can edit a resiliency plan.

#### To edit a resiliency plan

- 1 Navigate  
**Resiliency Plans** (menu bar) or **Quick Actions > Resiliency Plans**
- 2 In the **Saved Plans** list, place your cursor on the row which you want to edit. Do one of the following:
  - Right click your mouse and click **Edit**.
  - Click on the vertical ellipsis and select **Edit**.
- 3 In the **Edit Saved Plan** wizard panel, edit the required actions and click **Submit**.  
The steps for editing the plan are the same as creating it.

See ["Creating a new resiliency plan"](#) on page 81.

## Deleting a resiliency plan

Using the Veritas Resiliency Platform console, you can delete a resiliency plan.

### To delete a resiliency plan

- 1 Navigate  
**Resiliency Plans** (menu bar) or **Quick Actions > Resiliency Plans**
- 2 In the **Saved Plans** list, place your cursor on the row which you want to delete. Do one of the following:
  - Right click your mouse and click **Delete**.
  - Click on the vertical ellipsis and select **Delete**.
- 3 In the **Delete Saved Plan** panel click **Delete**.

See [“Creating a new resiliency plan”](#) on page 81.

## Executing a resiliency plan

Using the Veritas Resiliency Platform console, you can execute a resiliency plan. After executing the resiliency plan, you can navigate to the **Activities** page to view the progress of the plan.

### To execute a resiliency plan

- 1 Navigate  
**Resiliency Plans** (menu bar) or **Quick Actions > Resiliency Plans**
- 2 In the **Saved Plans** list, place your cursor on the row which you want to execute. Do one of the following:
  - Right click your mouse and click **Execute**.
  - Click on the vertical ellipsis and select **Execute**.
- 3 In the **Execute Saved Plan** panel click **Execute**.

See [“Creating a new resiliency plan”](#) on page 81.

## Viewing a resiliency plan

Using the Veritas Resiliency Platform console, you can view the details of a resiliency plan. To view the details of the resiliency plans, you need to have at least guest persona assigned to you.

You can also launch operations such as edit a resiliency plan or delete a resiliency plan from this view.

See [“Editing a resiliency plan”](#) on page 82.

See [“Deleting a resiliency plan”](#) on page 83.

### To view a resiliency plan

- 1 Navigate  
**Resiliency Plans** (menu bar) or **Quick Actions > Resiliency Plans**
- 2 In the **Saved Plans** list, do one of the following:
  - Double click the row that you want to view.
  - Select the row that you want to view, right click and select **Details**.
  - Select the row that you want to view, click on the vertical ellipsis and select **Details**.
- 3 You can now view the details of the resiliency plan. Click the watch icon to see the details of the components of a resiliency plan such as a custom script or a manual task.

## Creating a schedule for a resiliency plan

Using the Veritas Resiliency Platform console, you can create a schedule for a resiliency plan.

### To create a schedule for a resiliency plan

- 1 Navigate  
**Resiliency Plans** (menu bar) or **Quick Actions > Resiliency Plans**
- 2 In the **Saved Plans** list, do one of the following:
  - Double click the row for which you want to create a schedule. In the **Schedule** section of details page, click **New**.
  - Select the row for which you want to create a schedule, right click and select **Create Schedule**.
  - Select the row for which you want to create a schedule, click on the vertical ellipsis and select **Create Schedule**.

## Editing a schedule for a resiliency plan

Using the Veritas Resiliency Platform console, you can edit a schedule for a resiliency plan.

### To edit a schedule for a resiliency plan

- 1 Navigate  
**Resiliency Plans** (menu bar) or **Quick Actions > Resiliency Plans**
- 2 In the **Saved Plans** list, do one of the following:
  - Double click the row for which you want to edit a schedule. In the **Schedule** section of details page, click **Edit**.
  - Select the row for which you want to create a schedule, right click and select **Edit Schedule**.
  - Select the row for which you want to create a schedule, click on the vertical ellipsis and select **Edit Schedule**.

## Deleting a schedule for a resiliency plan

Using the Veritas Resiliency Platform console, you can delete a schedule for a resiliency plan.

### To delete a schedule for a resiliency plan

- 1 Navigate  
**Resiliency Plans** (menu bar) or **Quick Actions > Resiliency Plans**
- 2 In the **Saved Plans** list, do one of the following:
  - Double click the row for which you want to delete a schedule. In the **Schedule** section of details page, click **Delete**.
  - Select the row for which you want to edit a schedule, right click and select **Delete Schedule**.
  - Select the row for which you want to edit a schedule, click on the vertical ellipsis and select **Delete Schedule**.

## Viewing a schedule for a resiliency plan

Using the Veritas Resiliency Platform console, you can view a schedule for a resiliency plan. To view the details of the resiliency plans, you need to have at least guest persona assigned to you.

You can also launch operations such as edit a schedule or delete a schedule from this view.

See [“Editing a schedule for a resiliency plan”](#) on page 84.

See [“Deleting a schedule for a resiliency plan”](#) on page 85.

### To view a schedule for a resiliency plan

- 1 Navigate  
**Resiliency Plans** (menu bar) or **Quick Actions > Resiliency Plans**
- 2 In the **Saved Plans** list, do one of the following:
  - Double click the row for which you want to view a schedule.
  - Select the row for which you want to view a schedule, right click and select **Details**.
  - Select the row for which you want to view a schedule, click on the vertical ellipsis and select **Details**.
- 3 In the **Schedule** section of details page, view the details of the schedule.

# Configuring applications for disaster recovery using replication

This appendix includes the following topics:

- [Configuring application disaster recovery using EMC SRDF replication](#)
- [Configuring application disaster recovery using NetApp SnapMirror replication](#)
- [Configuring application disaster recovery using EMC RecoverPoint replication](#)

## Configuring application disaster recovery using EMC SRDF replication

This appendix includes the following scenarios:

- See [the section called “Configuring application disaster recovery using EMC SRDF with Microsoft Failover Clustering”](#) on page 87.
- See [the section called “Configuring application disaster recovery using EMC SRDF without Microsoft Failover Clustering”](#) on page 89.

### **Configuring application disaster recovery using EMC SRDF with Microsoft Failover Clustering**

This section lists the pre-requisites to enable data replication using EMC SRDF when the hosts are a part of a Microsoft failover cluster. For EMC SRDF-based replication, all applications consuming storage from a consistency group must belong to the same resiliency group. A consistency group is a collection of Symmetrix LUNs that helps in maintaining write consistency during replication.

- Ensure that EMC Symmetrix Solutions Enabler (version v7.4, or later) is installed on a host and the SRDF device groups are already set up for the replication between the primary and remote arrays.
- Ensure that EMC Symmetrix Gatekeeper device is present on the array control host. You can designate any host including the Hyper-V server as the array control host.

---

**Note:** The SRDF R1 and R2 LUNs must be on different hosts from different data centers.

---

- Ensure to enable the Failover Cluster roles on the Windows Server 2012R2 hosts at the production and recovery data centers.
- Ensure that you have created Microsoft failover cluster using the required nodes at the production and recovery data centers.
- Ensure that you have created the cluster shared volume (CSV) on the replicated shared disk (R1) on the application server at the production data center. On the application hosts configured at the recovery data center, re-scan the storage on all the Microsoft failover cluster nodes.
- Configure application on the production data center's Microsoft failover cluster with their data on the replicated CSVs.

Once you have performed the necessary configurations, proceed with disaster recovery specific tasks.

#### **Veritas Resiliency Platform configurations:**

- Add Windows 2012 R2 hosts to the Infrastructure Management Server (IMS) using the **Add Hosts** operation.
- Add the array control host where the SRDF device groups are configured, to the each IMS using the **Add Hosts** operation.
- Add Symmetrix enclosure using the **Add Enclosure** option. Provide the discovery host name and the SYMCLI location on this discovery host. This operation returns the list of Symmetrix arrays (local and remote) accessible to the host. To configure disaster recovery for applications, select one or more local arrays.

Default SymCLI location on Linux host      /opt/emc/SYMCLI/bin/

Default SymCLI location on Windows host   C:\Program Files\EMC\SYMCLI\bin



---

**Note:** Any physical or virtual machine can be designated as the array control host, including the virtual machine inside VMware ESX server that has EMC Symmetrix Gatekeeper device visibility.

---

- Perform add host and add enclosure operations for the IMS at the disaster recovery data center as well.

## **Configuring application disaster recovery using EMC SRDF without Microsoft Failover Clustering**

This section lists the pre-requisites to enable data replication using EMC SRDF when the hosts are not a part of a Microsoft failover cluster.

- Ensure that EMC Symmetrix Solutions Enabler (version v7.4, or later) is installed on a host and the SRDF device groups are already set up for the replication between the primary and remote arrays.
- Ensure that EMC Symmetrix Gatekeeper device is present on the array control host. You can designate any host including the Hyper-V server as the array control host.

---

**Note:** The replicated and primary LUNs must be on different hosts from different data centers.

---

- Ensure that you have created the volumes on the primary Hyper-V host where the LUNs are read and write enabled. Veritas Resiliency Platform supports only one volume per replicated disk. Windows Storage Space Storage Pool is not supported.
- Ensure that you have configured application at the production data centre under the Hyper-V Manager and kept the data files on the replicated volumes.
- Ensure that the respective remote disks (Read only - R2 remote disk and snapshot) are in the offline state on the Hyper-V server at the recovery data center. And also verify that no drive letter is assigned to the volumes present on these offline disks.

---

**Note:** To perform the Rehearse operation, you must add the snapshot devices to the SRDF device group at the recovery data center, and thereafter map them to the application hosts at the recovery data center.

---

Once you have performed the necessary configurations, proceed with disaster recovery specific tasks.

### Veritas Resiliency Platform configurations:

- Add the host where the SRDF device groups are configured, to the Infrastructure Management Server (IMS) using the **Add Hosts** operation.
- Add Symmetrix enclosure using the **Add Enclosure** option. Provide the discovery host name and the SYMCLI location on this discovery host. This operation returns the list of Symmetrix arrays (local and remote) accessible to the host. To configure disaster recovery for applications, select one or more local arrays.

Default SymCLI location on Linux host     /opt/emc/SYMCLI/bin/

Default SymCLI location on Windows host   C:\Program Files\EMC\SYMCLI\bin

---

**Note:** Any physical or virtual machine can be designated as the array control host, including the virtual machine inside VMware ESX server that has EMC Symmetrix Gatekeeper device visibility.

---

- Perform add host and add enclosure operations for the IMS at the disaster recovery data center as well.

### Limitations

- EMC SRDF LUN-based replication, without device group, and replication in the adaptive copy mode are not supported.
- If the application hosts are inside the virtual machines, the replicated data disks must be mapped to these hosts in Raw mode only. Virtual disks are not supported.
- Logical grouping of disks, Windows Server Storage space storage pool, is not supported.

## Configuring application disaster recovery using NetApp SnapMirror replication

This section lists the pre-requisites to enable the data replication using NetApp SnapMirror. For NetApp SnapMirror based replication, all applications that consume storage from a NetApp volume must belong to the same resiliency group.

- Ensure the NetApp volumes are already setup for replication between the primary and remote NetApp storage systems, and the replication has a replication schedule associated with it. The same export path should be used to mount the Netapp volume and Qtree on the application host. In case of NetApp clusters,

ensure that the junction path is '/' and the junction name is same as the volume name. And you must mount array volumes and Qtree in NFS mode only.

- Ensure to mount NetApp SnapMirror replicated volumes on the respective servers in both the sites. Do not mount the replicated peer NetApp Volumes on the same server.

NetApp share can be mounted with array IP or FQDN. For storage to application correlation to work successfully, ensure that the mount entry is consistent in the fstab.

- Change the permission to **Grant root access to all hosts** on the replicated volumes at both the production and recovery sites.
- Ensure you turn-on the following configurations for NetApp 7 Mode enclosure, `httpd.admin.enable` and `httpd.enable`. These are required for NetApp SnapMirror operations.

And also ensure that the MultiStore license is installed and enabled.

Once you have performed the necessary configurations, proceed with Resiliency Platform specific tasks.

#### **Resiliency Platform configurations:**

- Ensure that all the application hosts are added and discovered completely by the Infrastructure Management Server (IMS).
- Add NetApp enclosure using the **Add Enclosure** option.  
Provide the discovery host name, NetApp storage system name or IP, and credentials.

---

**Note:** While configuring NetApp array, you must use IMS as discovery host.

---

- Ensure that all the application hosts are added and discovered completely by IMS at the disaster recovery (DR) site.
- Perform add enclosure operations for the IMS at the DR data center as well.

## **Configuring application disaster recovery using EMC RecoverPoint replication**

This appendix includes the following scenarios:

- See [the section called “Configuring application disaster recovery using EMC RecoverPoint with Microsoft Failover Clustering”](#) on page 92.

- See [the section called “Configuring application disaster recovery using EMC RecoverPoint without Microsoft Failover Clustering”](#) on page 93.

## **Configuring application disaster recovery using EMC RecoverPoint with Microsoft Failover Clustering**

This section lists the pre-requisites to enable data replication using EMC RecoverPoint when the hosts are a part of a Microsoft failover cluster. For RecoverPoint-based replication, all applications consuming storage from a consistency group must belong to the same resiliency group. A consistency group is a collection of LUNs that helps in maintaining write consistency during replication.

- Ensure that RecoverPoint consistency groups are set up on the control host for the replication between the primary and remote arrays.
- Ensure that EMC RecoverPoint groups are set up for the CRR replication between the primary and Secondary RecoverPoint Appliance.
- Ensure to enable the Failover Cluster roles on the Windows Server 2012R2 hosts at the production and recovery data centers.
- Ensure that you have created Microsoft failover cluster using the required nodes at the production and recovery data centers.
- Ensure that you have created the cluster shared volume (CSV) on the replicated shared disk on the application server at the production data center. On the application hosts configured at the recovery data center, re-scan the storage on all the Microsoft failover cluster nodes.
- Configure application on the production data center's Microsoft failover cluster with their data on the replicated CSVs.

Once you have performed the necessary configurations, proceed with disaster recovery specific tasks.

### **Veritas Resiliency Platform configurations:**

- Add Windows 2012 R2 hosts to the Infrastructure Management Server (IMS) using the **Add Hosts** operation.
- Add the array control host where the RecoverPoint consistency groups are configured, to the each IMS using the **Add Hosts** operation.
- Add Symmetrix, CLARiiON, or VNX enclosure using the **Add Enclosure** option. Provide the discovery host name and the SYMCLI, NaviSecCLI, or Navisphere CLI location on this discovery host. This operation returns the list of Symmetrix, CLARiiON, or VNX arrays (local and remote) that are accessible to the host. To configure disaster recovery for applications, select one or more local arrays.

---

**Note:** Any physical or virtual machine can be designated as the array control host, including the virtual machine inside VMware ESX server.

---

- Add RecoverPoint appliance for replication using the **Add RecoverPoint** operation.
- Perform add host, add RecoverPoint appliance, and add enclosure operations for the IMS at the disaster recovery data center as well.

## Configuring application disaster recovery using EMC RecoverPoint without Microsoft Failover Clustering

This section lists the pre-requisites to enable data replication using EMC RecoverPoint when the hosts are not a part of a Microsoft failover cluster.

- Ensure that RecoverPoint consistency groups are setup on the control host for the replication between the primary and remote arrays.

---

**Note:** The replicated and primary LUNs must be on different hosts from different data centers.

---

- Ensure that EMC RecoverPoint groups are set up for the CRR replication between the primary and Secondary RecoverPoint Appliance.
- Ensure that you have created the volumes on the primary Hyper-V host where the LUNs are read and write enabled. Veritas Resiliency Platform supports only one volume per replicated disk. Windows Storage Space Storage Pool is not supported.
- Ensure that you have configured application at the production data centre under the Hyper-V Manager and kept the data files on the replicated volumes.
- Ensure that the respective remote disks are in the offline state on the Hyper-V server at the recovery data center. And also verify that no drive letter is assigned to the volumes present on these offline disks.

Once you have performed the necessary configurations, proceed with disaster recovery specific tasks.

### Veritas Resiliency Platform configurations:

- Add the host where the RecoverPoint consistency groups are configured, to the Infrastructure Management Server (IMS) using the **Add Hosts** operation.
- Add Symmetrix, CLARiiON, or VNX enclosure using the **Add Enclosure** option. Provide the discovery host name and the SYMCLI, NaviSecCLI, or Navisphere CLI location on this discovery host. This operation returns the list of Symmetrix,

CLARiiON, or VNX arrays (local and remote) that are accessible to the host. To configure disaster recovery for applications, select one or more local arrays.

---

**Note:** Any physical or virtual machine can be designated as the array control host, including the virtual machine inside VMware ESX server.

---

- Add RecoverPoint appliance for replication using the **Add RecoverPoint** operation.
- Perform add host, add RecoverPoint appliance, and add enclosure operations for the IMS at the disaster recovery data center as well.

#### Limitations

- If the application hosts are inside the virtual machines, the replicated data disks must be mapped to these hosts in Raw mode only. Virtual disks are not supported.
- Logical grouping of disks, Windows Server Storage space storage pool, is not supported.

# Troubleshooting

This appendix includes the following topics:

- [Troubleshooting discovery of assets](#)
- [Viewing events and logs in the console](#)

## Troubleshooting discovery of assets

When asset infrastructure is added to the Infrastructure Management Server (IMS), or when changes are made to the infrastructure, the IMS discovers and correlates the asset information and displays the information on the Assets page of the Resiliency Platform console. The discovery can take some time before the information is updated on the console. Until discovery is complete, some information needed to configure resiliency groups may be missing from the Assets page on the console.

If changes have been made to the asset infrastructure, you can use the Refresh operation on assets in the IMS to speed up discovery so that updated asset information is displayed more quickly in the console. To use the Refresh operation, display the asset infrastructure page for the IMS, select the asset type, right-click the asset and select Refresh.

---

**Note:** Occasionally, the data discovered from the Infrastructure Management server (IMS) may not be updated properly in the Resiliency Manager database. This situation may result in displaying incorrect information about the resiliency group state, replication state, and replication type. In such a case, refresh the appropriate assets on the IMS in both the data centers.

---

If you are configuring replication using storage arrays in a VMware vCenter Server environment, you can use the following guidelines to speed up discovery or to troubleshoot information that is not being updated:

**Table B-1**      Configuring asset infrastructure in IMS for storage arrays in VMware environment

Situation	Troubleshooting/best practices
Adding storage arrays as enclosures to IMS	Ensure that the storage arrays that are added to the IMS are the ones that provide storage to the ESX servers managed by the vCenter Server that is added to the IMS.
More than one IMS in data center	Ensure that the vCenter Server that is managing the ESX servers, and the enclosure providing storage to those servers, are added to the same IMS.
Refreshing the IMS after a change in infrastructure	Ensure that you use the Refresh operation on the correct vCenter Servers and enclosures where the change was made.
Refreshing the IMS after a change in infrastructure, where there is more than one IMS	Ensure that you use the Refresh operation in the correct IMS.

In the VMware and EMC SRDF and RecoverPoint environment, the general guideline is to add/refresh the enclosure before adding/refreshing the VMware vCenter Server.

**Table B-2**      Configuring or refreshing asset infrastructure in IMS for VMware and EMC SRDF and RecoverPoint environment

Situation	Recommended sequence
You have not yet added the asset infrastructure.	Add the enclosure information in the IMS and let the discovery complete before adding the vCenter Server to the IMS.
You later provision new storage from an enclosure that is already configured in the IMS and mount datastores from the new storage.	Refresh the enclosure in the IMS, let the refresh task on the enclosure complete, and then refresh the vCenter Server in the IMS.
You provision storage from a new enclosure.	Add the new enclosure in the IMS and then refresh the vCenter Server after the enclosure discovery completes.
You are provisioning storage from an enclosure that is already configured in the IMS to new ESX servers managed by a vCenter Server.	Refresh the enclosure first, then add the vCenter Server to the IMS or refresh it if it is already added to the IMS.



In the VMware and NetApp SnapMirror environment, the general guideline is add/refresh the vCenter Server first, then add/refresh the NetApp enclosure.

**Table B-3** Configuring or refreshing asset infrastructure in IMS for storage arrays in VMware and NetApp SnapMirror environment

Situation	Recommended sequence
You have not yet added the asset infrastructure.	Add the vCenter Server to the IMS first and let the discovery complete before you add the NetApp enclosure.
You later provision storage from an existing NetApp enclosure and mount NFS datastores on ESX servers.	Refresh the vCenter Server first in the IMS, let the discovery complete and then refresh the NetApp enclosure.
You later provision storage from a new NetApp enclosure and mount NFS datastores on that ESX servers.	Refresh the vCenter Server first in the IMS, wait for the vCenter Server discovery to complete, and then add the new NetApp enclosure.

The recommended sequence for adding or modifying asset infrastructure for application discovery in the NetApp SnapMirror replication environment is as follows: Ensure that discovery of the hosts is complete before you add or refresh the NetApp enclosures.

For more information on adding asset infrastructure and on the refresh operation in the IMS, refer to the *Deployment Guide*.

## Viewing events and logs in the console

Veritas Resiliency Platform maintains the following types of logs that can be viewed in the web console:

**System logs:** System logs are typically the result of a user performing an operation in the console.

**Audit logs:** Audit logs are primarily used for security audits. They leave a chronological trail of activities performed on the system. They identify user, activity, affected objects, etc. They help track the individuals responsible for activities and detect security violations.

**Event and notification logs:** Event and notification logs are not necessarily related to user activity; they can include information such as a server going down. Events can be public or private. Rules can be configured to notify users by email of selected public events. Private events are typically unrelated to user-initiated operations.

Private events are displayed in the console for troubleshooting but are not available to include in rules for notification.

By default, logs and SNMP traps are retained for 2 years. This retention period can be modified in the product settings in the console.

### To view events and logs

#### 1 Navigate



**More Views** (menu bar) > **Logs**



You can also view new notifications from the **Notifications** icon.

#### 2 To view logs by type (System, Audit, or Notification) select the appropriate tab. You can filter by the product service and by severity (information, warning, or errors) or type (public, private), depending on the tab.

# Glossary

<b>activity</b>	A task or an operation performed on a resiliency group.
<b>add-on</b>	An additional software package that can be installed on hosts by the Infrastructure Management Server (IMS) for specialized uses.
<b>asset infrastructure</b>	The data center assets that can be added to the Infrastructure Management Server (IMS) for IMS discovery and monitoring. For example, virtual machines or virtualization servers.
<b>assets</b>	In Veritas Resiliency Platform, the virtual machines or applications that have been discovered by the Infrastructure Management Server (IMS) and that can be grouped into resiliency groups.
<b>CLISH</b>	Command Line Interface SHell. Provides the command line menu on the virtual appliance for use after the initial bootstrap configuration.
<b>data center</b>	<p>A location that contains asset infrastructure to be managed by Veritas Resiliency Platform.</p> <p>For the disaster recovery use case, the resiliency domain must contain at least two data centers in different locations, a production data center and recovery data center. Each data center has a Resiliency Manager and one or more IMSs.</p>
<b>host</b>	<p>Physical servers, virtual machines, or Hyper-V servers that are added to the Infrastructure Management Server (IMS) as hosts.</p> <p>Adding the assets as hosts installs the host package that is used by the IMS for discovery and monitoring.</p>
<b>Infrastructure Management Server (IMS)</b>	The Veritas Resiliency Platform component that discovers, monitors, and manages the asset infrastructure within a data center. The IMS transmits information about the asset infrastructure to the Resiliency Manager.
<b>migrate</b>	A planned activity involving graceful shutdown of virtual machines at the production data center and starting them at the recovery data center. In this process, replication ensures that consistent virtual machine data is made available at the recovery data center.
<b>persona</b>	A user role that has access to a predefined set of jobs (operations). Used to assign permissions to users and groups for Veritas Resiliency Platform web console operations.
<b>product role</b>	The function configured for a Veritas Resiliency Platform virtual appliance.

	For example, a virtual appliance can be configured as a Resiliency Manager, Infrastructure Management Server (IMS) or both.
<b>production data center</b>	The data center that is normally used for business. See also recovery data center.
<b>recovery data center</b>	The data center that is used if a disaster scenario occurs. See also production data center.
<b>rehearsal</b>	<p>A zero-downtime test that mimics the configuration, application data, storage, and the failover behavior of the resiliency group.</p> <p>Rehearsal verifies the ability of the resiliency group to fail over to the recovery data center during a disaster.</p>
<b>resiliency domain</b>	The logical scope of a Resiliency Platform deployment. It can extend across multiple data centers.
<b>resiliency group</b>	The unit of management and control in Veritas Resiliency Platform. Related assets are organized into a resiliency group and managed and monitored as a single entity.
<b>Resiliency Manager</b>	The Veritas Resiliency Platform component that provides resiliency capabilities within a resiliency domain. It is composed of loosely coupled services, a distributed data repository, and a management console.
<b>resiliency plan</b>	A collection of tasks or operations, along with the relevant assets, which are performed in a predefined sequence.
<b>resiliency plan template</b>	A template defining the execution sequence of a collection of tasks or operations.
<b>takeover</b>	An activity initiated by a user when the production data center is down due to a disaster and the virtual machines need to be restored at the recovery data center to provide business continuity.
<b>tier</b>	<p>Within a virtual business service (VBS), resiliency groups are arranged as tiers. Tiers represent the logical dependencies between the resiliency groups and determine the relative order in which the resiliency groups start and stop.</p>
<b>virtual appliance</b>	<p>An appliance that includes the operating system environment and the software application which are deployed together as a virtual machine.</p> <p>The Veritas Resiliency Platform virtual appliance is deployed as a virtual machine and then configured with basic settings and a role (for example, Resiliency Manager).</p>
<b>virtual business service (VBS)</b>	A multi-tier IT service where each VBS tier hosts one or more resiliency groups. A VBS groups multiple services as a single unit for visualization, automation, and controlled start and stop in the desired order. You can also migrate/takeover the entire VBS.
<b>web console</b>	The web-based management console on the Resiliency Manager that is used to configure the settings for the resiliency domain and perform operations.

# Index

## A

- activities
  - abort 74
  - view 73
- application bundle file
  - editing discovery schedule 24
  - enabling and disabling on selected hosts 23
  - installing on selected hosts 21
  - managing auto-deploy 23
  - removing 21
  - uninstalling from selected hosts 22
  - uploading 20
  - viewing applicable host details 25
  - viewing details 25
- applications
  - about managing 15
  - adding custom application 18
  - deleting custom application 19
  - managing and monitoring using resiliency groups 31
  - partially discovered 17
  - protecting with resiliency groups 33
- applications disaster recovery
  - about 52
  - EMC RecoverPoint 91
  - EMC SRDF 87
  - NetApp SnapMirror 90
  - pre-requisites 53
  - replication technologies 53
- asset infrastructure
  - troubleshooting discovery of assets 95

## D

- dashboard 46
- disaster recovery operations
  - about 50
  - configure 56
  - key steps 54
  - migrate applications 70
  - rehearsal cleanup 62
  - rehearse 59

- disaster recovery operations *(continued)*
  - rehearse operations 60
  - takeover applications 71

## E

- events 97

## I

- Infrastructure Management Server
  - troubleshooting discovery of assets 95

## L

- logs
  - viewing in console 97

## P

- permissions
  - about 14

## R

- replication lag 40
- Replication lag threshold 64
- reports
  - viewing 48
- resiliency groups
  - about 30
  - creating from applications 31
  - creating from applications 33
  - deleting 44
  - displaying detailed information 40
  - displaying information and status 36
  - modifying 41
  - roles 51
  - starting 42
  - stopping 43
  - viewing details 57
- resiliency plan template
  - viewing 80

- resiliency plan templates
  - create 76
  - deleting 80
  - editing 79
- resiliency plans
  - about 75
  - create schedule 84
  - creating 81
  - custom script 78
  - delete schedule 85
  - deleting 83
  - edit schedule 84
  - editing 82
  - executing 83
  - manual task 77
  - view schedule 85
  - viewing 83
- Resiliency Platform
  - capabilities 13
  - features and components 12
- resync
  - performing 71
- risk information
  - view 65
- risk insight
  - about 63
- risks
  - description 65

## S

- SLA threshold 64