Veritas™ Resiliency Platform 1.0: Solutions for Applications

July 2015

VERITAS™

Veritas Resiliency Platform: Solutions for Applications

Product version: 1.0

Document version: 1.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec 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 Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's 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 Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/index.jsp

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.symantec.com/business/support/contact_techsupp_static.jsp

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 Symantec
  - Recent software configuration changes and network changes

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/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
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

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

Asia-Pacific and Japan	customercare_apj@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec's enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

http://www.symantec.com/connect/storage-management

Documentation

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation

Contents

Chapter 1

Overview of Veritas Resiliency Platform

This chapter includes the following topics:

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 Resiliency Platform need to understand these in more detail.

resiliency domain	The logical scope of a Resiliency Platform deployment. It can extend across multiple data centers.
Resiliency Manager	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. The Resiliency Manager is deployed as a virtual appliance.
Infrastructure Management Server (IMS)	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. To achieve scale, multiple IMSs can be deployed in the same data center.
data center	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.
asset infrastructure	The data center assets that you add to the IMS for discovery and monitoring. 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.
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/takeover the entire VBS.

Resiliency Platform capabilities

Resiliency Platform helps you monitor and manage diaster 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 "Managing and monitoring applications" on page 19.
Displaying an overview of your resiliency domain including the number and health of your resiliency groups.	See "About the Resiliency Platform Dashboard" on page 31. See "Displaying resiliency group information and status" on page 23.
Starting and stopping resiliency groups for maintenance.	See "Starting a resiliency group" on page 28. See "Stopping a resiliency group" on page 29.
Configuring disaster recovery for a resiliency group	See "Configuring disaster recovery for a resiliency group of applications" on page 41.
Migrating a resiliency group	See "Migrating a resiliency group of applications" on page 44.
Taking over a resiliency group	See "Taking over a resiliency group of applications" on page 45.
Viewing reports	See "Viewing reports" on page 33.
Managing activities and resiliency plans	See "Managing activities" on page 46. See "Managing resiliency plans" on page 48.

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 *Veritas Resiliency Platform Deployment Guide*.

Chapter 2

Managing applications using Veritas Resiliency Platform

This chapter includes the following topics:

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 15.

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 16.

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 18.

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 32.

See “Managing and monitoring applications” on page 19.

See “About disaster recovery for applications” on page 37.

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:

Asset Type	Select application.
Data Center	Select the data center in which the application is located.
Application Type	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 19.

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 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).
  See *Veritas Resiliency Platform 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.

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 21.

See “Managing and monitoring applications” on page 19.

Chapter 3

Managing resiliency groups

This chapter includes the following topics:

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.

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. You can manage and monitor the group, start it, and stop it, edit it, and so on.
  See "Managing and monitoring applications" on page 19.
- You can create a resiliency group and enable disaster recovery for it. This is known as a protected resiliency group. You can work with this resiliency group just like a managed and monitored group, and you have additional features associated with disaster recovery.
  See "Protecting applications" on page 21.

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.

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 *Veritas Resiliency Platform Deployment Guide*.

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:

Asset Type	Select **Application**.
Data Center	The data center in which the application is located.
Application Type	Select the application type. See "Adding a custom application to Resiliency Platform" on page 16.

4 Filter the list of applications (optional)

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

Group By	Organize the applications by host name or replication consistency group.
Search	If you have a long list of applications, use the **Search** field to filter the list.
show assets in resiliency group	If you select this check box, the list of applications is updated with a **Resiliency Group** column. If an application is part of a resiliency group, it is listed in the table.

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.
- 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.

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:

Data Center	Select the data center in which the application is located.
Application Type	Select the application type. See "Adding a custom application to Resiliency Platform" on page 16.

4 Filter the list of applications (optional)

Group By	Organize the applications by the host on which they are installed or their replication consistency group.
Search	If you have a long list of applications, use the **Search** field to filter the list.
show assets in resiliency group	When you select this check box, the list of applications is updated with a **Resiliency Group** column. If an application is already a member of a resiliency group, this column displays the name of the 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. Select applications from the primary data center and the disaster 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 41.

- 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 3-1 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 "About the Resiliency Platform Dashboard" on page 31.
 **Assets** > **Resiliency Groups** 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 "Displaying resiliency group details" on page 26.

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	**Online** - The assets within the resiliency group are running.
	Partial - One or more of the assets in the resiliency group are offline.
	Offline - The assets in the resiliency group are powered off or not running.
DR Status	**Configured** - The resiliency group has been configured for disaster recovery.
	Not Configured - Disaster recovery is not configured for the group. Configure it as soon as possible.
Replication Type	Resiliency Platform supports several replication technologies.
	If no replication type is shown, consider configuring replication.
	See "Configuring disaster recovery for a resiliency group of applications" on page 41.

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 26.

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 resiliency group-specific screen is read-only. You can display and sort information on the screen, but you cannot update it. The screen is divided into the following areas:

Table 3-2 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.
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 **Name**, **Type**, or **State**.

Table 3-2 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.

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 31.
- 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 23.

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 41.

To modify resiliency group information

1 Prerequisites

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.

Starting a resiliency group

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

To start a resiliency group

1 Navigate

Assets > **Resiliency Groups** tab

2 Select

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

3 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**.

4 On the **Start Resiliency Group** screen, select the data center in which to start the group and click **Submit**.

5 Confirm

Click **Done**.

6 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 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

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**.

Chapter 4

Monitoring and reporting on assets status

This chapter includes the following topics:

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.
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.

You can use the Assets icon in the navigation pane to display more detailed information on resiliency groups.

See "Displaying resiliency group information and status" on page 23.

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.

Asset	Description
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. See "Viewing the Resiliency Groups by Datacenter report" on page 33.
Migrate and Takeover	Provides a summary report of the last migrate and takeover operations performed on the resiliency groups. See "Viewing the Migrate and Takeover report" on page 34.

Viewing the Resiliency Groups by Datacenter report

This report provides details about the resiliency groups in the data centers across all sites.

The **Resiliency Group Data Center Distribution** bar graph shows site wise distribution of the resiliency groups. It also shows the status such as online or offline.

The **Data Center Details** table displays the following information:

- Data center name
- Location details
- Name of the resiliency group
- Type of the resiliency group
- Replication status of the resiliency group
- Disaster recovery configuration status
- Status of the resiliency group such as online or offline.

To view the data center details report

1. Navigation

   Click **Reports** (menu bar) > **Inventory**.

2. Click **Run** or **Schedule** on the **Resiliency Groups by Datacenter** report to receive the report on the specified email address.

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

Viewing the Migrate and Takeover report

This report provides a summary of the last migrate and takeover operations that were performed on the resiliency groups.

The **Migrate and Takeover** pie chart shows the percentage of successful and failed operations.

The **Resiliency Groups at Risk** displays the list of resiliency groups on which the operations had failed. The **Last Migrate/Takeover Details** table displays the list of resiliency groups on which the operations were performed.

You can view the following information in these tables:

- Resiliency group name on which the operation was performed.
- Operation name; migrate or takeover.
- Start time of the operation.
- Duration of the operation.
- Target data center name.
- Source data center name.
- The data center on which the resiliency group is currently active.

To view the migrate and takeover report

1. Navigation

   Click **Reports** (menu bar) > **Risk Assessment**.

2. Click **Run** or **Schedule** on the **Migrate and Takeover Report** to receive the report on the specified email address.

For more information on configuring email settings, refer to the *Veritas Resiliency Platform Deployment Guide*.

See “Viewing reports” on page 33.

Chapter 5

Using Resiliency Platform for disaster recovery

This chapter includes the following topics:

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.

The 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.
- Making business services more resilient by providing the ability to perform disaster recovery operations on virtual machines and applications. For example, migrate, takeover, and rehearse.
- Ability to group your virtual machines or applications in resiliency groups based on your production environment and business needs.
- 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, such as replication lag.

- Ability to perform non-disruptive testing 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 36.

Understanding the role of resiliency groups in disaster recovery operations

To perform disaster recovery 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 start/stop operations on resiliency groups that are not enabled for DR. However, you cannot perform disaster recovery operations on a resiliency group without first enabling the resiliency group for disaster recovery. You can enable disaster recovery at the time you create the resiliency group, or later.

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.

See "About resiliency groups" on page 18.

Chapter 6

Managing disaster recovery for applications

This chapter includes the following topics:

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 44.

See "Taking over a resiliency group of applications" on page 45.

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 18.

See "About replication technologies used in disaster recovery of applications" on page 38.

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 6-1 Supported configurations using EMC Symmetrix Remote Data Facility (SRDF) replication

Operating System	Type of host	Clustering	Supported
Windows	Hyper-V virtual machine	Microsoft Failover Custering (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 6-1 Supported configurations using EMC Symmetrix Remote Data Facility (SRDF) 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 6-2 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 6-3 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.	See "Configuring application disaster recovery using EMC SRDF replication" on page 54. See "Configuring application disaster recovery using NetApp SnapMirror replication" on page 56.

Table 6-3 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 *Veritas Resiliency Platform Deployment Guide* .
Configure your assets for disaster recovery	Group the required applications in a resiliency group and enable disaster recovery for the resiliency group.	See "Managing and monitoring applications" on page 19. See " Modifying a resiliency group" on page 27. See "Protecting applications" on page 21. See "Configuring disaster recovery for a resiliency group of applications" on page 41.
DR operations	Perform the required DR operations: Migrate and takeover.	See "Migrating a resiliency group of applications" on page 44. See "Taking over a resiliency group of applications" on page 45.

Chapter 7

Preparing for disaster recovery operations

This chapter includes the following topics:

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 primary site and the DR site.
- 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 *Veritas Resiliency Platform 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.

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 21.

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 42.

See "Migrating a resiliency group of applications" on page 44.

See "Taking over a resiliency group of applications" on page 45.

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.

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 26.

Chapter 8

Performing disaster recovery operations

This chapter includes the following topics:

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**.

Chapter 9

Managing activities and resiliency plans

This chapter includes the following topics:

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 46.

See “Aborting a running activity” on page 47.

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 47.

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 approximately 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 task.

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 46.

Managing resiliency plans

Veritas Resiliency Platform provides a console for creating and customizing resiliency plans.

See "About resiliency plans" on page 48.

See "Creating a new resiliency plan template" on page 49.

See "Editing a resiliency plan template" on page 50.

See "Deleting a resiliency plan template" on page 50.

See "Creating a new resiliency plan" on page 51.

See "Editing a resiliency plan" on page 52.

See "Deleting a resiliency plan" on page 52.

See "Executing a resiliency plan" on page 53.

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. Then you can add a resiliency group 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

In addition to the above listed tasks, you can also add a **Manual** task in the resiliency plan. This task temporarily pauses the operation letting you perform a task before proceeding further or validating a step before proceeding.

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.

See "Creating a new resiliency plan template" on page 49.

See "Creating a new resiliency plan" on page 51.

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

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

In addition to the above listed tasks, you can also add a Manual task in the resiliency plan. This task temporarily pauses the operation letting you perform a task before proceeding further.

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 48.

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 49.

Deleting a resiliency plan template

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

You can add assets to these templates and create a customized resiliency plan. 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 49.

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

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 48.

See "Deleting a resiliency plan" on page 52.

See "Executing a resiliency plan" on page 53.

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 51.

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 51.

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 51.

Appendix A

Configuring applications for disaster recovery using replication

This appendix includes the following topics:

Configuring application disaster recovery using EMC SRDF replication

This section lists the pre-requisites to enable data replication using EMC SRDF. 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 as the array control host.

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

- Ensure to assign SRDF replicated LUNs to the respective systems. Do not attach replicated peer SRDF LUNs (that is R1 & R2) to the same system.
- The applications' data must be stored on disks that are replicated using EMC SRDF replication. The application installation and configuration files must be stored on non-replicated disk. Ensure that the replicated storage has only those LUNs, which are replicated using EMC SRDF replication and you have a corresponding device group created for them.

  Note: For VMware virtual machines, the applications' data must be stored on disks that are provisioned as RDM storage to the virtual machines.

- Keep the respective remote disks (Read only - RDF2 remote disk and snapshot) in the offline state on the systems at the DR 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 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.

Limitation: 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. The same export path should be used to mount the Netapp volume and Qtree on the application host. 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.
- Ensure you turn-on the following configurations in NetApp 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.

Appendix B

Troubleshooting

This appendix includes the following topics:

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.

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 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 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, than 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 *Veritas Resiliency Platform 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.

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, such as the `xprtld` process being down on the Control Host, require intervention and troubleshooting to resolve.

You can display risks in the following ways:

Table B-4 Ways to display risks

To display ...	Do the following:
A complete list of risks across the resiliency domain	1 On the menu bar, select  **More Views** > **Risks** 2 On the **Risk** page, double-click a risk in the table to display detailed information.

Table B-4 Ways to display risks *(continued)*

To display ...	Do the following:
Risks that are associated with a specific resiliency group or virtual business service	**1** On the navigation pane, select  (Assets) and the tab for either **Resiliency Groups** or **Virtual Business Services**. **2** On the tab, double-click a resiliency group or virtual business service to display detailed information. **3** On the details page, note any risks that are listed in the **At Risk** area, and double-click the risk for details.

Table B-5 describes each Resiliency Platform risk.

Table B-5 Risks and Descriptions

Risk	Description
CTRL_HOST_DOWN	The `xprtld` process is down on the Control Host, and configured resources are in unknown state. Discovered contents can be stale.
HOST_SFMH_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.

Glossary

activity	A task or an operation performed on a resiliency group.
add-on	An additional software package that can be installed on hosts by the Infrastructure Management Server (IMS) for specialized uses.
asset infrastructure	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.
assets	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.
CLISH	Command Line Interface SHell. Provides the command line menu on the Veritas Resiliency Platform virtual appliance for use after the initial bootstrap configuration..
data center	A location that contains asset infrastructure to be managed by Veritas Resiliency Platform. 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.
host	Physical servers, virtual machines, or Hyper-V servers that are added to the Infrastructure Management Server (IMS) as hosts. Adding the assets as hosts installs the host package that is used by the IMS for discovery and monitoring.
Infrastructure Management Server (IMS)	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.
migrate	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.
persona	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.
product role	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.
production data center	The data center that is normally used for business. See also recovery data center.
recovery data center	The data center that is used if a disaster scenario occurs. See also production data center.
rehearsal	A zero-downtime test that mimics the configuration, application data, storage, and the failover behavior of the resiliency group. Rehearsal verifies the ability of the resiliency group to fail over to the recovery data center during a disaster.
resiliency domain	The logical scope of a Resiliency Platform deployment. It can extend across multiple data centers.
resiliency group	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.
Resiliency Manager	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.
resiliency plan	A collection of tasks or operations, along with the relevant assets, which are performed in a predefined sequence.
resiliency plan template	A template defining the execution sequence of a collection of tasks or operations.
takeover	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.
tier	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.
virtual appliance	An appliance that includes the operating system environment and the software application which are deployed together as a virtual machine. 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).
virtual business service (VBS)	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.
web console	The web-based management console on the Resiliency Manager that is used to configure the settings for the resiliency domain and perform operations.

Index