Veritas™ Resiliency Platform 1.0: Solutions for Virtual Business Services

July 2015

Veritas Resiliency Platform: Solutions for Virtual Business Services

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: 1.0

Document version: 1.0

Legal Notice

This Symantec product may contain third party software for which Symantec 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 Symantec product for more information on the Third Party Programs.

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. SYMANTEC CORPORATION 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 Symantec 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.

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

Overview of 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.

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

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 13.

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.

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.

Chapter 3

About virtual business services

This chapter includes the following topics:

About virtual business services

VBS is a logical collection of resiliency groups that function together to perform a particular service. A virtual business service (VBS) enables easy management of multi-tier business services. For example, you can group a web server resiliency group, a database resiliency group, and a payroll business logic resiliency group into a VBS called `payroll`. You can start, stop, monitor, manage, or recover that VBS as a single entity.

Asymmetric virtual business services

Asymmetric virtual business services contains a mixture of resiliency groups in which some of the resiliency groups are not DR configured. When a user creates such a VBS, the Configure DR option is disabled. If the user still wants to create an asymmetric VBS with DR configured, the user needs to toggle the Configure DR option value to **Yes**.

Understanding virtual business service tiers

Within a VBS, resiliency groups are arranged in tiers. Tiers represent the logical dependencies between the resiliency groups and determine the relative order in which the resiliency groups start and stop. For example, the database resiliency group must start before the application server resiliency group and the web server resiliency group, so the database resiliency group must go in the lowest tier. The application server resiliency group must start after the database resiliency group, so it goes in the next tier. The web server resiliency group must start last, so it goes into the top tier. Later, if you add a resiliency group to the VBS, you can manage it as part of the IT service by placing it in the appropriate tier.

Customizing a virtual business service

By default, each resiliency group in a VBS tier must start before the next tier is started. However, your VBS might not require that. For such a VBS, the following two advanced configuration options are available:

Optional

When a resiliency group has this setting, its state (whether online or offline) does not affect the overall state of the tier for start and stop operations. However the resiliency group state is taken into consideration before marking the VBS start or stop operation as completed.

For example, if you have a non-critical resiliency group within the tier and other resiliency groups in the next tier of the VBS do not depend on it for start or stop ordering, consider making it optional for the tier state. This potentially speeds up the VBS start or stop operation because other resiliency groups would start or stop without waiting for this resiliency group.

Starts after	By default, all the resiliency groups in a tier must start before any resiliency groups in the upper tier. Logically, however, a resiliency group may not require all the previous groups to start. For example, say tier 1 of a VBS contains two resiliency groups, `RG1` and `RG2`. Tier 2 contains a resiliency group, `database_app`, that requires `RG1` to be running, but not `RG2`. You can select `database_app` and specify that it can start any time after `RG1`. It does not have to wait for `RG2`.

See “Creating a virtual business service” on page 16.

Creating a virtual business service

Using the Veritas Resiliency Platform console, you can create a VBS.

To create a virtual business service

1 Prerequisites

- Determine the assets that constitute the IT Service. Ensure these assets have been organized into the appropriate resiliency groups.
- Make sure that you understand the tier model for creating VBSs and the dependencies between resiliency groups.
  See “Understanding virtual business service tiers” on page 15.

2 Navigate

Assets > **Virtual Business Services** > **Manage Multi-Tier Applications**

3 Create and populate VBS tiers

On the **Select Resiliency Groups** page, use the **Data Center** drop-down to select a data center and display its resiliency groups. You can enter text in the **Search** field to narrow your list.

Select a resiliency group and drag it to the VBS creation area on the right side of the screen. This area represents the first VBS tier. When you start the VBS, this tier starts first.

Do the following to create and populate the VBS tiers:

- Click **Add Tier** to add a tier and the **x** icon to remove a tier.

- You can drag resiliency groups from one tier to another, but you cannot change the order of the tiers.
- To remove a resiliency group from a VBS, drag it back to the resiliency group selection area.
- Add resiliency groups to tiers until you are done.

4. Do one of the following:
   - Optionally, fine-tune the VBS configuration. Continue with step 5.
   - If you have completed the VBS configuration, click **Next**.

5. Fine-tune the VBS configuration (optional).

   On the right side of the resiliency group, click on the vertical ellipsis, and select one or both of the following:

   Optional

   When a resiliency group has this setting, its state (whether online or offline) does not affect the overall state of the tier.

   For example, if you have a non-critical resiliency group within the tier and other resiliency groups in the VBS do not depend on it for start or stop ordering, consider making it optional for the tier state. This would potentially speed up the VBS start or stop operation because other resiliency groups would start or stop without waiting for this resiliency group.

   Starts after

   By default, all the resiliency groups in a tier must start before any resiliency groups in the next tier. Logically, however, a resiliency group may not require all the previous groups to start.

   For example, say tier 1 of a VBS contains two resiliency groups, `RG1` and `RG2`. Tier 2 contains a resiliency group, `database_app`, that requires `RG2` to be running, but not `RG2`. You can select `database_app` and specify that it can start any time after `RG1`. It does not have to wait for `RG2`.

   When you complete this step, click **Next**.

6. Review the VBS configuration

On the **Plan View** page, review the following:

- Use the **All** link or data center links to display all the resiliency groups or a site-specific set of groups.
- Click **Start Order** or **Stop Order** to review the sequence in which tiers start and stop.
- Note whether disaster recovery (DR) has been configured for the resiliency groups. If a resiliency group is configured for DR, its icon includes a check mark.

Plan View is a read-only page. To make changes, click **Back**; otherwise, click **Next**.

7 Complete VBS creation.

On the **Summary** screen, do the following:

- Make sure that the resiliency groups are in the proper tiers.
- Specify the name and description for the VBS.
- If one or more of the resiliency groups in the VBS is not configured for DR, decide whether you want to configure DR now.

When you are done, click **Submit**.

8 On the confirmation page, click **Done**.

Starting and stopping a virtual business service

When you start or stop a virtual business service (VBS), the resiliency groups within it start or stop based on the following:

- The tier they are in
- Any fine-tuning you may have specified using the **Start after** option

See “About virtual business services” on page 14.

See “Creating a virtual business service” on page 16.

Note: A resiliency group can be in multiple VBSs. When you start or stop a VBS, it affects all the VBSs in which the resiliency group appears.

To start or stop a Virtual Business Service

1. Navigate

   Assets > **Virtual Business Services** tab

2. Select

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

3. Start or stop the VBS.

   Do one of the following:

   - Right click on the VBS row and select **Start** or **Stop**.
   - On the right side of the VBS row, click on the vertical ellipsis and select **Start** or **Stop**

   Note: You need to provide the datacenter details on which the start or stop VBS operations are performed on.

Migrating a virtual business service

Migration refers to a planned activity involving graceful shutdown of the virtual business services at the production data center and starting them at the recovery data center.

To migrate a virtual business service

1. Navigate

   Assets > **Virtual Business Services** tab

2. Select

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

3. Migrate the VBS.

   Do one of the following:

   - Right click on the VBS row and select **Migrate**.

- On the right side of the VBS row, click on the vertical ellipsis and select **Migrate**.
- Double click the VBS row, under **DR Readiness** section, select **Migrate**.

On the confirmation screen, select the data center that you want to migrate, and click **Migrate**.

Taking over a virtual business service

Takeover is an activity initiated by a user when the production data center is down due any disaster or natural calamities, and the virtual business services (VBSs) need to be restored at the recovery data center in order to provide business continuity. The takeover operation brings up the VBSs at the recovery data center using the last recovered checkpoint.

To perform takeover operation on a virtual business service

1 Navigate

Assets > **Virtual Business Services** tab

2 Select

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

3 Take over the VBS.

Do one of the following:

- Right click on the VBS row and select **Takeover**.
- On the right side of the VBS row, click on the vertical ellipsis and select **Takeover**.
- Double click the VBS row, under DR Readiness section, select **Takeover**.

On the confirmation screen, select the data center that you want to take over, and click **Takeover**.

Displaying virtual business service details

The details screen shows the virtual business services (VBS) configuration and state information of the VBS.

The top section lists the **Active Data Centers** and the VBS state.

In the lower section, the VBS configuration is displayed. This section has the following tabs:

List The **List** tab lists the resiliency groups that are part of the VBS. Each row shows information about the type, active data centers, and states for the resiliency group. Depending on where the resiliency groups are located, you can click the links above the table to display all the resiliency groups or only the resiliency groups in a particular data center.

Tier View The **Tier View** tab lets you visualize how the resiliency groups are arranged into logical tiers.

Plan View The **Plan View** tab shows the relative start and stop ordering of the resiliency groups within the VBS.

This screen is read only.

See “Editing a virtual business service” on page 21.

Editing a virtual business service

The steps for editing a virtual business service are nearly identical to the steps for creating one.

To edit a virtual business service

1 Navigate

   Assets > **Virtual Business Services** tab

2 Select

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

4 Do one of the following:

   - Right click on the VBS row and select **Edit**.
   - On the right side of the VBS row, click on the vertical ellipsis and select **Edit**. The steps for editing a VBS are identical to creating it.
     After you edit your VBS, you need to manually refresh the page to view the latest VBS plan view.
     See “Creating a virtual business service” on page 16.

Removing a virtual business service

When you remove a virtual business service (VBS) from Resiliency Platform, the resiliency groups that make up the VBS are not affected. You can continue to manage and monitor them and organize them into other VBSs.

To remove a virtual business service

1. Prerequisites

   Determine the potential impact of removing the VBS. Will removing this service inconvenience your users?

   If necessary, notify users of the upcoming change.

2. Navigate

   Assets > **Virtual Business Services**

3. Select

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

4. Remove

   Do one of the following:

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

   On the confirmation screen, click **Submit**.

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 23.

See "Aborting a running activity" on page 24.

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 24.

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 23.

Managing resiliency plans

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

See “About resiliency plans” on page 25.

See “Creating a new resiliency plan template” on page 26.

See “Editing a resiliency plan template” on page 27.

See “Deleting a resiliency plan template” on page 27.

See “Creating a new resiliency plan” on page 28.

See “Editing a resiliency plan” on page 29.

See “Deleting a resiliency plan” on page 29.

See “Executing a resiliency plan” on page 30.

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 virtual business service (VBS).
- Stop a VBS.
- Migrate a VBS.
- Takeover a VBS.
- 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 26.

See “Creating a new resiliency plan” on page 28.

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 virtual business service (VBS).
- Migrate and takeover a VBS.
- 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 25.

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 26.

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 26.

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 virtual business service (VBS).
- Migrate and takeover a VBS.
- 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 25.

See "Deleting a resiliency plan" on page 29.

See "Executing a resiliency plan" on page 30.

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 28.

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 28.

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 28.

Troubleshooting

This appendix includes the following topics:

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 A-1 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.
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 A-2 describes each Resiliency Platform risk.

Table A-2 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