

Veritas™ Resiliency Platform 2.1 Solutions for Virtual Business Services

VERITAS™

Veritas Resiliency Platform: Solutions for Virtual Business Services

Last updated: 2017-02-03

Document version: Document version: 2.1 Rev 0

Legal Notice

Copyright © 2017 Veritas Technologies LLC. All rights reserved.

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

This product may contain third party software for which Veritas is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the third party legal notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

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

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

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

Veritas Technologies LLC

500 E Middlefield Road
Mountain View, CA 94043

<http://www.veritas.com>

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Veritas account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The document version appears on page 2 of each guide. The latest documentation is available on the Veritas website:

<https://sort.veritas.com/documents>

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

doc.feedback@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

<http://www.veritas.com/community/>

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1	Overview of Resiliency Platform	6
	About Veritas Resiliency Platform	6
	About Resiliency Platform features and components	7
	About permissions for operations in the console	9
Chapter 2	Using Resiliency Platform for disaster recovery	10
	About disaster recovery using Resiliency Platform	10
	Understanding the role of resiliency groups in disaster recovery operations	11
Chapter 3	About virtual business services	12
	About virtual business services	12
	Understanding virtual business service tiers	13
	Creating a virtual business service	13
	Starting and stopping a virtual business service	15
	Displaying virtual business service details	16
	Editing a virtual business service	17
	Deleting a virtual business service	18
	Performing rehearsal on a virtual business service	18
	Performing cleanup rehearsal on a virtual business service	19
	Migrating a virtual business service	20
	Taking over a virtual business service	20
	Performing resync for a virtual business service	21
	Performing restore for a virtual business service	22
Chapter 4	Monitoring risks	24
	About risk insight	24
	Displaying risk information	25
	Predefined risks in Resiliency Platform	26
	Viewing the current risk report	32
	Viewing the historical risk report	33

Chapter 5	Managing activities and resiliency plans	34
	Managing activities	34
	Viewing activities	34
	Aborting a running activity	35
	Managing resiliency plans	36
	About resiliency plans	36
	Creating a new resiliency plan template	37
	Editing a resiliency plan template	40
	Deleting a resiliency plan template	41
	Viewing a resiliency plan template	41
	Creating a new resiliency plan	42
	Editing a resiliency plan	43
	Deleting a resiliency plan	44
	Executing a resiliency plan	44
	Viewing a resiliency plan	45
	Creating a schedule for a resiliency plan	45
	Editing a schedule for a resiliency plan	46
	Deleting a schedule for a resiliency plan	46
	Viewing a schedule for a resiliency plan	47
Chapter 6	Managing evacuation plans	48
	About evacuation plan	48
	Generating an evacuation plan	50
	Regenerating an evacuation plan	51
	Performing evacuation	52
	Performing rehearse evacuation	52
	Performing cleanup evacuation rehearsal	52
Appendix A	Troubleshooting	54
	Viewing events and logs in the console	54
Glossary		56
Index		58

Overview of Resiliency Platform

This chapter includes the following topics:

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

About Veritas Resiliency Platform

Veritas Resiliency Platform offers a unified solution that helps you proactively maintain business uptime across private, public, and hybrid clouds. Resiliency Platform gives you complete automation for all resiliency operations involving the virtual machines, applications, and multi-tier business-services in your data center. It safeguards the current technology investments by plugging into your existing environments and infrastructure.

For data replication, you can use the Veritas Data Mover or any third-party solution that is supported by Veritas Resiliency Platform. For a list of supported vendors and products, see *Veritas Resiliency Platform Hardware and Software Compatibility Guide*.

Resiliency Platform has the following core capabilities:

Security and Compliance

Veritas Resiliency Platform provides enhanced data encryption (for data-in-flight and data-at-rest) as well as choice of data residency.

Predictability	Customers can predictably meet critical business Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
Compliance	Customers can prove compliance to internal and external business continuity mandates with audit reporting and non-disruptive, real-time disaster recovery testing.
Automation	Customers get complete automation for all resiliency operations including recovery run books, and start and stop recovery orchestration for multi-tier applications. This reduces risk of downtime from human error.
Flexibility	Customers get the flexibility to keep their existing infrastructures and can innovate on their terms, with the flexibility that Resiliency Platform provides, to enable workload migration across sites and even to the cloud.

See [“About Resiliency Platform features and components”](#) on page 7.

About Resiliency Platform features and components

The following is a brief introduction to Veritas Resiliency Platform key components and their relationships. Administrators responsible for deploying and configuring the product 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.

Veritas InfoScale Operations Manager Management Server	<p>The component that allows discovery of InfoScale applications that are already configured in Veritas InfoScale Operations Manager. Also referred to as Veritas InfoScale Operations Manager server.</p> <p>You can manage the InfoScale applications that are already configured in Veritas InfoScale Operations Manager on Linux, Solaris, AIX as well as Windows platform.</p>
Replication Gateway	<p>The component of Veritas Resiliency Platform Data Mover that is deployed as a virtual appliance on both data centers and used to perform replication between the data centers.</p>
data center	<p>For a disaster recovery use case, the resiliency domain must contain at least two data centers in different locations, a production data center and recovery data center. Each data center has a Resiliency Manager and one or more IMSs.</p>
asset infrastructure	<p>The data center assets that you add to Resiliency Platform for discovery and monitoring by the IMS.</p> <p>The asset infrastructure can include hosts (Windows or Linux servers), virtualization servers for Hyper-V and VMware, and enclosures (storage arrays). Once the asset infrastructure is discovered by the IMS, the discovered virtual machines or applications are listed in the console as assets to manage or protect.</p>
resiliency group	<p>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.</p>
service objective	<p>A template to define the type of operations and technologies that are supported for a group of assets. You apply a service objective to each resiliency group.</p> <p>A template which identifies the characteristics of a service. These could be availability related characteristics such as local redundancy, and number of nodes in a cluster or DR characteristics such as remote recovery, Recovery Point Objective (RPO) SLAs, rehearsal support etc. Service objective is applied when a group of assets are being added to a resiliency group.</p> <p>Resiliency Platform monitors the resiliency groups based on the service objective definition and raises the risks as applicable.</p>

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 perform operations such as migrate, takeover, resync, rehearsal on 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 *Deployment Guide*.

Using Resiliency Platform for disaster recovery

This chapter includes the following topics:

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

About disaster recovery using Resiliency Platform

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

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

- Monitoring of data center assets - storage, virtual machines, and applications.
- Ability to group your virtual machines or applications in resiliency groups based on your production environment and business needs.
- Making business services more resilient by providing the ability to perform disaster recovery operations on virtual machines and applications. For example, migrate and take over.
- Ability to replicate data from virtual machines on source data centers to target data centers using Resiliency Platform Data Mover integrated with VMware API I/O filtering framework or array-based replication technologies provided by array vendors.
- Resiliency plan (a sequential execution of predefined steps) to automate site-level recovery operations on your IT infrastructure in the event of downtime.

- Auto-discovery and real-time tracking for recovery objectives.
- Ability to perform non-disruptive testing (rehearsal) on your virtual machines and applications to ensure that your infrastructure is adequately prepared for protection in the 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 11.

Understanding the role of resiliency groups in disaster recovery operations

To perform disaster recovery (DR) operations on virtual machines or applications, they must be configured for disaster recovery as part of a resiliency group, which is the unit of management and control in Veritas Resiliency Platform.

In the configuration wizard for resiliency groups, you apply a service objective to a resiliency group. When you apply the recover hosts service objective, the wizard prompts you for the additional information required for Resiliency Platform to configure the resiliency group for disaster recovery operations.

After disaster recovery configuration on a resiliency group is complete, you can proceed with DR-specific tasks on the resiliency group, such as migrate and take over.

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

About virtual business services

This chapter includes the following topics:

- [About virtual business services](#)
- [Creating a virtual business service](#)
- [Starting and stopping a virtual business service](#)
- [Displaying virtual business service details](#)
- [Editing a virtual business service](#)
- [Deleting a virtual business service](#)
- [Performing rehearsal on a virtual business service](#)
- [Performing cleanup rehearsal on a virtual business service](#)
- [Migrating a virtual business service](#)
- [Taking over a virtual business service](#)
- [Performing resync for a virtual business service](#)
- [Performing restore for a virtual business service](#)

About virtual business services

For a business service to work properly, it is important that all of its tiers and components are up and working together. From a business continuity point of view, it is important to not just ensure that individual tiers are up and running but also the entire business service.

A virtual business service (VBS) is a logical collection of resiliency groups that function together to perform a particular business service. A 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.

An Asymmetric VBS is a combination of resiliency groups having Recovery service objective and resiliency groups having Monitor service objective.

You can not create an asymmetrical virtual business service in which some of the resiliency groups have Copy service objective, while others have Monitor or Recovery service objective.

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.

Creating a virtual business service

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

To create a virtual business service

- 1 Prerequisites
 - Ensure that the required 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 13.
- 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.

Alternatively, you can select a resiliency group and then in the drop-down list, select the tier where you want to move the resiliency group.

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. Alternatively, you can click on the vertical ellipsis next to the resiliency group in the VBS tier and select **Remove**.
- 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 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.

You can use **Optional** only on a homogenous tier of resiliency groups.

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

6 Review the VBS configuration

On the **Plan View** page, click **Start Order** or **Stop Order** to review the sequence in which tiers start and stop.

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.

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 12.

See “[Creating a virtual business service](#)” on page 13.

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.

Displaying virtual business service details

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

The top left section lists the **Active Data Centers** and the VBS state. You can also view the current activity, last successful activity, and last unsuccessful activity below the active data center.

The top right section lists the **Risks** that are associated with the VBS. You can see the category wise distribution of risks and also view the details of these risks.

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.

For a resiliency group with InfoScale application, you can additionally view the details about the InfoScale product used in the Availability column. |
| 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.

On the rightmost side of the screen, you can see the menu options for operations that you can perform on the VBS.

See [“Editing a virtual business service”](#) on page 17.

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 13.

Deleting a virtual business service

When you delete 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 delete a virtual business service

1 Prerequisites

Determine the potential impact of deleting the VBS. 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 **Delete**.
- On the right side of the resiliency group row, click on the vertical ellipsis and select **Delete**.

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

Performing rehearsal on a virtual business service

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

To perform rehearsal 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 Perform rehearsal operation on the VBS.

Do one of the following:

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

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

Performing cleanup rehearsal on a virtual business service

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

To perform cleanup rehearsal 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 Perform cleanup rehearsal operation on the VBS.

Do one of the following:

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

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 **Management Operations** 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 to 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.

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**.

Performing resync for a virtual business service

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

Since the production data center is not working, the data replication between the two sites does not happen. After the production site is back up and running, you need to prepare the production site for the next failover or for a migration operation. This preparation includes cleaning up any residue and resuming the replication from the recovery to the production site.

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

To perform resync 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 Perform resync operation on the VBS.

Do one of the following:

- Right click on the VBS row and select **Resync**.
- On the right side of the VBS row, click on the vertical ellipsis and select **Resync**.
- Double click the VBS row, under **Management Operations** section, select **Resync**.

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

Performing restore for a virtual business service

Using Resiliency Platform console, you can recover virtual machine data that is protected with the Copy service definition. The most recent backup image is used for restoring the virtual machines within the virtual business service (VBS).

The virtual machine is restored using the selected backup image at the selected data center; before that the virtual machine in the other data center is stopped and unregistered. The network settings of the virtual machine are configured as per the subnet mapping, switch or port mapping as specified during the configure for remote recovery operation. Finally the virtual machine is up and running at the recovery data center.

Note: To restore a VBS, the resiliency groups must consist only of VMware virtual machines.

To restore a virtual business service at the recovery data center

1 Prerequisites

The resiliency group that contains the virtual machines must be protected using the Copy service definition.

2 Navigate



Assets > Virtual Business Services tab

3 Go to the details page of the VBS that you want to recover and select **Restore**.

4 In the **Restore Virtual Business Service** panel select the target data center and click **Next**.

5 Verify that the selected virtual machines are back online.

Monitoring risks

This chapter includes the following topics:

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

About risk insight

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

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

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

Risk insight generates two types of reports:

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

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

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

Table 4-1

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

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

Table 4-2

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

See [“Displaying risk information”](#) on page 25.

See [“Predefined risks in Resiliency Platform”](#) on page 26.

See [“Viewing the current risk report”](#) on page 32.



See [“Viewing the historical risk report”](#) on page 33.

Displaying risk information

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

You can display risks in the following ways:

Table 4-3 Ways to display risks

To display ...	Do the following:
A complete list of risks across the resiliency domain	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.

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

Predefined risks in Resiliency Platform

[Table 4-4](#) lists the predefined risks available in Resiliency Platform. These risks are reflected in the current risk report and the historical risk report.

Table 4-4 Predefined risks

Risks	Description	Risk detection time	Risk type	Affected operation	Fix if violated
Veritas Infoscale Operations Manager disconnected	Checks for Veritas Infoscale Operations Manager to Resiliency Manager connection state	1 minute	Error	All operations	Check Veritas Infoscale Operations Manager reachability Try to reconnect Veritas Infoscale Operations Manager
vCenter Password Incorrect	Checks if vCenter password is incorrect	5 minutes	Error	<ul style="list-style-type: none"> ■ On primary site: start or stop operations ■ On secondary site: migrate or takeover operations 	In case of a password change, resolve the password issue and refresh the vCenter configuration
VM tools not installed	Checks if VM Tools are not Installed. It may affect IP Customization and VM Shutdown.	Real time, when resiliency group is created	Error	<ul style="list-style-type: none"> ■ Migrate ■ Stop 	<ul style="list-style-type: none"> ■ In case of VMWare, install VMWare Tools ■ In case of Hyper-V, install Hyper-V Integration Tools
Snapshot removed from Virtual Machine	Checks if snapshot has been removed from virtual machine.	5 minutes	Error	Resiliency Platform Data Mover replication	Edit the resiliency group to refresh configuration
Snapshot reverted on Virtual Machine	Checks if snapshot has been reverted on virtual machine.	5 minutes	Error	Resiliency Platform Data Mover replication	Remove and re-add the virtual machine to the Resiliency group by editing Resiliency group

Table 4-4 Predefined risks (*continued*)

Risks	Description	Risk detection time	Risk type	Affected operation	Fix if violated
Data Mover Daemon Crash	Checks if VM Data Mover filter is not able to connect to its counterpart in ESX.	5 minutes	Error	Resiliency Platform Data Mover replication	In order to continue the replication, you can move (VMotion) the VM to a different ESX node in the cluster and either troubleshoot the issue with this ESX node or raise a support case with Veritas
Snapshot created on Virtual Machine	Checks if a snapshot has been created on Virtual machine.	5 minutes	Error	Resiliency Platform Data Mover replication	Edit the resiliency group to refresh configuration
DataMover virtual machine in noop mode	Checks if VM Data Mover filter is not able to connect to its counterpart in ESX.	5 minutes	Error	Resiliency Platform Data Mover replication	In order to continue the replication, you can move (VMotion) the VM to a different ESX node in the cluster and either troubleshoot the issue with this ESX node or raise a support case with Veritas
Resiliency group configuration drift	Checks if disk configuration of any of the assets in the resiliency group has changed.	30 minutes	Error	<ul style="list-style-type: none"> ■ Migrate ■ Resync 	Edit the resiliency group to first remove the impacted virtual machine from the resiliency group and then add it back to the resiliency group.
Global user deleted	Checks if there are no global users. In this case, the user will not be able to customize the IP for Windows machines in VMware environment.	Real time	Warning	<ul style="list-style-type: none"> ■ Migrate ■ Takeover 	Edit the resiliency group or add a Global user

Table 4-4 Predefined risks (*continued*)

Risks	Description	Risk detection time	Risk type	Affected operation	Fix if violated
Missing heartbeat from Resiliency Manager	Checks for heartbeat failure from a Resiliency Manager.	5 minutes	Error	All	Fix the Resiliency Manager connectivity issue
Infrastructure Management Server disconnected	Check for Infrastructure Management Server(IMS) to Resiliency Manager(RM) connection state.	1 minute	Error	All	Check IMS reachability Try to reconnect IMS
Storage Discovery Host down	Checks if the discovery daemon is down on the storage discovery host	15 minutes	Error	Migrate	Resolve the discovery daemon issue
DNS removed	Checks if DNS is removed from the resiliency group where DNS customization is enabled	real time	Warning	<ul style="list-style-type: none"> ■ Migrate ■ Takeover 	Edit the Resiliency Group and disable DNS customization
IOTap driver not configured	Checks if the IOTap driver is not configured	2 hours	Error	None	Configure the IOTap driver This risk is removed when the workload is configured for disaster recovery
VMware Discovery Host Down	Checks if the discovery daemon is down on the VMware Discovery Host	15 minutes	Error	Migrate	Resolve the discovery daemon issue
VM restart is pending	Checks if the VM has not been restarted after add host operation	2 hours	Error	Configure DR	Restart the VM after add host operation
New VM added to replication storage	Checks if a virtual machine that is added to a Veritas Replication Set on a primary site, is not a part of the resiliency group.	5 minutes	Error	<ul style="list-style-type: none"> ■ Migrate ■ Takeover ■ Rehearsal 	Add the virtual machine to the resiliency group.

Table 4-4 Predefined risks (*continued*)

Risks	Description	Risk detection time	Risk type	Affected operation	Fix if violated
Replication lag exceeding RPO	Checks if the replication lag exceeds the thresholds defined for the resiliency group. This risk affects the SLA for the services running on your production data center.	5 minutes	Warning	<ul style="list-style-type: none"> ■ Migrate ■ Takeover 	Check if the replication lag exceeds the RPO that is defined in the Service Objective
Replication state broken/critical	Checks if the replication is not working or is in a critical condition for each resiliency group.	5 minutes	Error	<ul style="list-style-type: none"> ■ Migrate ■ Takeover 	Contact the enclosure vendor.
Remote mount point already mounted	Checks if the mount point is not available for mounting on target site for any of the following reasons: <ul style="list-style-type: none"> ■ Mount point is already mounted. ■ Mount point is being used by other assets. 	<ul style="list-style-type: none"> ■ Native (ext3, ext4, NTFS): 30 minutes ■ Virtualization (VMFS, NFS): 6 hours 	Warning	<ul style="list-style-type: none"> ■ Migrate ■ Takeover 	Unmount the mount point that is already mounted or is being used by other assets.
Disk utilization critical	Checks if at least 80% of the disk capacity is being utilized. The risk is generated for all the resiliency groups associated with that particular file system.	<ul style="list-style-type: none"> ■ Native (ext3, ext4, NTFS): 30 minutes ■ Virtualization (VMFS, NFS): 6 hours 	Warning	<ul style="list-style-type: none"> ■ Migrate ■ Takeover ■ Rehearsal 	Delete or move some files or uninstall some non-critical applications to free up some disk space.
ESX not reachable	Checks if the ESX server is in a disconnected state.	5 minutes	Error	<ul style="list-style-type: none"> ■ On primary site: start or stop operations ■ On secondary site: migrate or takeover operations 	Resolve the ESX server connection issue.

Table 4-4 Predefined risks (*continued*)

Risks	Description	Risk detection time	Risk type	Affected operation	Fix if violated
vCenter Server not reachable	Checks if the virtualization server is unreachable or if the password for the virtualization server has changed.	5 minutes	Error	<ul style="list-style-type: none"> ■ On primary site: start or stop operations ■ On secondary site: migrate or takeover operations 	Resolve the virtualization server connection issue. In case of a password change, resolve the password issue.
Insufficient compute resources on failover target	Checks if there are insufficient CPU resources on failover target in a virtual environment.	6 hours	Warning	<ul style="list-style-type: none"> ■ Migrate ■ Takeover 	Reduce the number of CPUs assigned to the virtual machines on the primary site to match the available CPU resources on failover target.
Host not added on recovery data center	Checks if the host is not added to the IMS on the recovery data center.	30 minutes	Error	Migrate	Check the following and fix: <ul style="list-style-type: none"> ■ Host is up on recovery data center. ■ Host is accessible from recovery datacenter IMS. ■ Time is synchronized between host and recovery datacenter IMS.
NetBackup Notification channel disconnected	Checks for NetBackup Notification channel connection state	5 minutes	Error	Restore	Check if the NetBackup Notification channel is added to the NetBackup master server.

Table 4-4 Predefined risks (continued)

Risks	Description	Risk detection time	Risk type	Affected operation	Fix if violated
Backup image violates the defined RPO	Checks if the backup image violates the defined RPO	30 minutes	Warning	No operation	<ul style="list-style-type: none"> ■ Check the connection state of NetBackup Notification channel ■ Check for issues due to which backup images are not available
NetBackup master server disconnected	Checks if NetBackup master server is disconnected or not reachable	5 minutes	Error	Restore	Check if IMS is added as an additional server to the NetBackup master server
Assets do not have copy policy	Checks if the assets do not have a copy policy	3 hours	Warning	No operation	Set up copy policy and then refresh the NetBackup master server
Target replication is not configured	Checks if the target replication is not configured	3 hours	Warning	No operation	Configure target replication and then refresh the NetBackup master server

Viewing the current risk report

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

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

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

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

To view the current risk report

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

Viewing the historical risk report

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

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

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

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

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

To view the historical risk report

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

Managing activities and resiliency plans

This chapter includes the following topics:

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

Managing activities

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

See [“Viewing activities”](#) on page 34.

See [“Aborting a running activity”](#) on page 35.

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



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 35.

Aborting a running activity

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

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

To abort an activity

1 Navigate

Do one of the following:



Activities. Skip to [2](#)

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

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

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

See [“Viewing activities”](#) on page 34.

Managing resiliency plans

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

See [“About resiliency plans”](#) on page 36.

See [“Creating a new resiliency plan template”](#) on page 37.

See [“Editing a resiliency plan template”](#) on page 40.

See [“Deleting a resiliency plan template”](#) on page 41.

See [“Viewing a resiliency plan template”](#) on page 41.

See [“Creating a new resiliency plan”](#) on page 42.

See [“Editing a resiliency plan”](#) on page 43.

See [“Deleting a resiliency plan”](#) on page 44.

See [“Executing a resiliency plan”](#) on page 44.

See [“Viewing a resiliency plan”](#) on page 45.

See [“Creating a schedule for a resiliency plan”](#) on page 45.

See [“Editing a schedule for a resiliency plan”](#) on page 46.

See [“Deleting a schedule for a resiliency plan”](#) on page 46.

See [“Viewing a schedule for a resiliency plan”](#) on page 47.

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 virtual business service (VBS). Then you can add a VBS to the template to create a plan. You can create multiple plans using the same template.

You can create customized resiliency plans for performing all the disaster recovery operations such as migrate, takeover, rehearsal, cleanup rehearsal, and resync. You can also create customized resiliency plans for executing a manual task or a custom script.

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

You can schedule the resiliency plan to run at a particular time.

Using these predefined templates, you can create resiliency plans by adding assets to the template. You can then run these plans on a later date.

See [“Creating a new resiliency plan template”](#) on page 37.

See [“Creating a new resiliency plan”](#) on page 42.

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
See [“About manual task”](#) on page 38.
- Run a custom script
See [“About custom script”](#) on page 39.

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

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

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

To create a new resiliency plan template

- 1 Navigate
Automation Plans (menu bar) > **Resiliency Plans** 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 36.

About manual task

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

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

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

Using manual tasks in resiliency plans

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

To use a manual task in a resiliency plan

- 1 You can add a manual task to a resiliency plan template or to a resiliency plan.
See [“Creating a new resiliency plan template”](#) on page 37.
See [“Creating a new resiliency plan”](#) on page 42.
- 2 Drag and drop **Manual Task** into the canvas. Click the pencil icon in the action box to add the task details.
- 3 Provide a name for the manual task.
- 4 Describe the reason why you want to add this manual task to the resilient plan.
- 5 Select your choice for resuming the process manually or automatically. If you select the option for automatically resuming the process after a timeout, enter the duration of timeout in minutes. Click **Save**.

About custom script

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

Custom Script execution requires Resiliency Platform deployed on the Resiliency Manager, Infrastructure Management Server (IMS) and the hosts executing custom scripts. In addition, if you are using Resiliency Platform with Veritas InfoScale, the Veritas Resiliency Platform Enablement add-on has to be manually installed on applicable hosts.

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

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

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

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

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

Using custom scripts in resiliency plans

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

To use a custom script execution task in a resiliency plan

- 1 You can add a custom script execution task to a resiliency plan template or to a resiliency plan.

See “[Creating a new resiliency plan template](#)” on page 37.
See “[Creating a new resiliency plan](#)” on page 42.
- 2 Drag and drop **Custom Script** into the canvas. Click the pencil icon in the action box to add the task details.
- 3 Enter a name for the custom script.
- 4 Select the data center and the host where you want to execute the script. Click **Next**.
- 5 Enter the following details:
 - The relative path of the script on the specified host. The script path that you enter is taken as relative to the `VRTSsfmh InstallDir/vrp/scripts/` directory path.
For example, if you enter the path of the script as `myscripts/backup_scripts/script_name`, then the complete path considered by the system will be `VRTSsfmh InstallDir/vrp/scripts/myscripts/backup_scripts/script_name`.
 - Command-line arguments to the script. This is an optional input field.
 - Timeout for the script. By default, there is no timeout for the script execution. You can specify a timeout for the script execution. After the specified timeout expires, the script execution task in the resiliency plan is marked as failure but the script execution task is not stopped. The script execution may continue in the background. If you do not specify any timeout, the task will wait till the script is not completed.
- 6 Click **Save**.

Editing a resiliency plan template

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

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

To edit a resiliency plan template

- 1 Navigate
Automation Plans (menu bar) > **Resiliency Plans** 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 37.

Deleting a resiliency plan template

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

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

To delete a resiliency plan template

- 1 Navigate
Automation Plans (menu bar) > **Resiliency Plans** 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 37.

Viewing a resiliency plan template

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

To view a resiliency plan template

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

Creating a new resiliency plan

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

- Start and stop a virtual business service (VBS).
- Rehearsal and cleanup rehearsal of a resiliency group.
- Migrate and takeover a VBS.
- Manual task
See [“About manual task”](#) on page 38.
- Run a custom script
See [“About custom script”](#) on page 39.

Note: To create a plan for migrate, takeover, rehearsal, or cleanup rehearsal 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
Automation Plans (menu bar) > **Resiliency Plans** 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 36.

See ["Deleting a resiliency plan"](#) on page 44.

See ["Executing a resiliency plan"](#) on page 44.

Editing a resiliency plan

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

To edit a resiliency plan

- 1 Navigate
Automation Plans (menu bar) > **Resiliency Plans** 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 42.

Deleting a resiliency plan

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

To delete a resiliency plan

- 1 Navigate
Automation Plans (menu bar) > **Resiliency Plans** 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 42.

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
Automation Plans (menu bar) > **Resiliency Plans** 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 42.

Viewing a resiliency plan

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

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

See [“Editing a resiliency plan”](#) on page 43.

See [“Deleting a resiliency plan”](#) on page 44.

To view a resiliency plan

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

Creating a schedule for a resiliency plan

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

To create a schedule for a resiliency plan

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

- Select the row for which you want to create a schedule, click on the vertical ellipsis and select **Create Schedule**.

Editing a schedule for a resiliency plan

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

To edit a schedule for a resiliency plan

1 Navigate

Automation Plans (menu bar) > **Resiliency Plans** or **Quick Actions** > **Resiliency Plans**

2 In the **Saved Plans** list, do one of the following:

- Double click the row for which you want to edit a schedule. In the **Schedule** section of details page, click **Edit**.
- Select the row for which you want to create a schedule, right click and select **Edit Schedule**.
- Select the row for which you want to create a schedule, click on the vertical ellipsis and select **Edit Schedule**.

Deleting a schedule for a resiliency plan

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

To delete a schedule for a resiliency plan

1 Navigate

Automation Plans (menu bar) > **Resiliency Plans** or **Quick Actions** > **Resiliency Plans**

2 In the **Saved Plans** list, do one of the following:

- Double click the row for which you want to delete a schedule. In the **Schedule** section of details page, click **Delete**.
- Select the row for which you want to edit a schedule, right click and select **Delete Schedule**.
- Select the row for which you want to edit a schedule, click on the vertical ellipsis and select **Delete Schedule**.

Viewing a schedule for a resiliency plan

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

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

See [“Editing a schedule for a resiliency plan”](#) on page 46.

See [“Deleting a schedule for a resiliency plan”](#) on page 46.

To view a schedule for a resiliency plan

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

Managing evacuation plans

This chapter includes the following topics:

- [About evacuation plan](#)
- [Generating an evacuation plan](#)
- [Regenerating an evacuation plan](#)
- [Performing evacuation](#)
- [Performing rehearse evacuation](#)
- [Performing cleanup evacuation rehearsal](#)

About evacuation plan

An evacuation plan lets you evacuate all the assets from the production data center to the recovery data center with a single click operation.

Using the evacuation plan template you can define the sequence in which the virtual business services (VBS) should be migrated from the production data center to the recovery data center. Resiliency groups that do not belong to any VBSs, are appended at the end of the evacuation plan workflow after the VBS.

You can create an evacuation plan using only resiliency groups also. Having a VBS is not compulsory.

An evacuation plan has Priorities. You can add the VBSs to different priority levels. Ordering of resiliency groups is done by the Resiliency Platform.

If an asset within a VBS or a resiliency group fails to recover, the evacuation plan skips the asset and continues the process for the remaining assets. To do this you need to select the **Ignore failures** check box while creating the evacuation plan.

If the check box is not selected the evacuation plan stops, enabling you to fix the problem, and proceed ahead. If you choose to restart the workflow then the already executed steps are re-executed with the same results.

Only users with **Manage Evacuation Plans** permission can create and run the evacuation plans.

Prerequisites for a VBS or a resiliency group to belong to a plan

A VBS or a resiliency group should meet the following criteria to be a part of a plan.

- The VBSs and resiliency groups must be configured for disaster recovery. A resiliency group that is not configured for disaster recovery, or a VBS having such a resiliency group, cannot be added to the plan.
- A resiliency group must belong to only one VBS. Shared resiliency groups cannot be added.

An appropriate warning to exclude these assets is shown when you generate a plan.

On completing the evacuation plan, you can perform the following operations:

- Evacuate
- Rehearse evacuation
- Cleanup evacuation rehearsal
- Regenerate a plan

An alert is raised and you need to perform the **Regenerate evacuation plan** operation in the following scenarios:

- VBSs are added, modified, or deleted.
- Resiliency groups are added and configured for disaster recovery.
- Resiliency groups which were configured for disaster recovery are deleted.
- Existing resiliency group is configured for disaster recovery.

No action is required in the following scenarios:

- Resiliency groups are modified.
- Resiliency groups which are not configured for disaster recovery are deleted.

When you run the **Evacuate**, **Rehearse evacuation**, **Cleanup evacuation rehearsal**, or the **Regenerate evacuation plan** operation, you can view the workflow details in the **Activities** view.

See [“Generating an evacuation plan”](#) on page 50.

See [“Regenerating an evacuation plan”](#) on page 51.

See [“Performing evacuation”](#) on page 52.

See [“Performing rehearse evacuation”](#) on page 52.

See [“Performing cleanup evacuation rehearsal”](#) on page 52.

Generating an evacuation plan

Using the Resiliency Platform console you can generate an evacuation plan that lets you evacuate all the assets from the production data center to the recovery data center.

Using the evacuation plan template you can define the sequence in which the virtual business services (VBS) should be migrated from the production data center to the recovery data center. Resiliency groups that do not belong to any VBSs, are appended at the end of the evacuation plan workflow after the VBS.

By default only one priority group is created. To add more priority groups, click **Change Priority** and click the **+** button. You can drag and drop the VBSs into different priority groups.

Reset to Default removes all priority groups except one. All VBSs are moved into a single priority group.

If an asset within a VBS or a resiliency group fails to recover, the evacuation plan skips the asset and continues the process for the remaining assets. To do this you need to select the **Ignore failures** check box while creating the evacuation plan.

If any VBSs and resiliency groups do not fit the evacuation plan criteria, a message is displayed. We recommend that you fix the issues before creating the plan.

Only users with **Manage Evacuation Plans** permission can create and run the evacuation plans.

To generate an evacuation plan

1 Prerequisites

See [“About evacuation plan”](#) on page 48.

2 Navigate

Automation Plans (menu bar) > **Evacuation Plans**

- 3 Select **Evacuation Plans**.
- 4 For the required data center click **Generate Plan**.
- 5 Review the message if any and click **Next**.
- 6 Click **Change Priority** if you want to add more priority groups. Click **Submit**.

See [“Performing evacuation”](#) on page 52.

See [“Performing rehearse evacuation”](#) on page 52.

See [“Performing cleanup evacuation rehearsal”](#) on page 52.

See [“Regenerating an evacuation plan”](#) on page 51.

Regenerating an evacuation plan

After successfully creating an evacuation plan, if any of the following scenarios occur, you need to regenerate the evacuation plan.

- VBSs are added, modified, or deleted.
- Resiliency groups are added and configured for disaster recovery.
- Existing resiliency group is configured for disaster recovery.

No action is required in the following scenarios:

- Resiliency groups are added.
- Resiliency groups are modified.
- Resiliency groups which are not configured for disaster recovery are deleted.

To add more priority groups to the plan, click **Change Priority** and click the **+** button. You can drag and drop the VBSs into different priority groups. **Reset to Default** removes all priority groups except one. All VBSs are moved into a single priority group.

To regenerate an evacuation plan

- 1 Navigate
Automation Plans (menu bar) > **Evacuation Plans**
- 2 For the required data center click **Regenerate Plan**.
- 3 Review the message if any and click **Next**.
- 4 Click **Change Priority** if you want to add more priority groups or click **Reset to Default** if you want to have only one priority group. Click **Submit**.

See [“Generating an evacuation plan”](#) on page 50.

See [“Performing evacuation”](#) on page 52.

See [“Performing rehearse evacuation”](#) on page 52.

See [“Performing cleanup evacuation rehearsal”](#) on page 52.

Performing evacuation

Using the Resiliency Platform console, you can run an evacuation plan for a data center which lets you evacuate all the assets from the production data center to the recovery data center.

To run an evacuation plan

- 1 Navigate

Automation Plans (menu bar) > **Evacuation Plans**

- 2 For the required data center, click on the vertical ellipses and select **Evacuate** to run the evacuation plan.

See [“Performing rehearse evacuation”](#) on page 52.

See [“Performing cleanup evacuation rehearsal”](#) on page 52.

See [“Regenerating an evacuation plan”](#) on page 51.

Performing rehearse evacuation

Using the Resiliency Platform console, you can perform a rehearsal of an evacuation plan for a data center. This verifies whether all your assets from the production data center can evacuate to the recovery data center.

To perform a rehearsal of an evacuation plan

- 1 Navigate

Automation Plans (menu bar) > **Evacuation Plans**

- 2 For the required data center, click on the vertical ellipses and select **Rehearse Evacuation**.

See [“Performing cleanup evacuation rehearsal”](#) on page 52.

See [“Regenerating an evacuation plan”](#) on page 51.

Performing cleanup evacuation rehearsal

After you have performed the rehearse evacuation operation successfully to verify if all your assets from the production data center can evacuate to the recovery data

center, you can use the cleanup evacuation rehearsal operation to clean up the rehearsal virtual machines and its volumes in the VBS or resiliency groups.

All temporary objects that are created during the rehearse evacuation operation are now deleted.

During the rehearse evacuation operation, if any virtual machines are in ERROR state, then during the cleanup evacuation rehearsal operation, these virtual machines and their volumes are not deleted. You need to manually delete them. Similarly if the recovery data center is Cloud, then manually delete the instances which are in ERROR state.

To perform the cleanup rehearsal of an evacuation plan

- 1 Navigate
Automation Plans (menu bar) > **Evacuation Plans**
- 2 For the required data center, click on the vertical ellipses and select **Cleanup Evacuation Rehearsal**.

See [“Performing evacuation”](#) on page 52.

See [“Performing rehearse evacuation”](#) on page 52.

Troubleshooting

This appendix includes the following topics:

- [Viewing events and logs in the console](#)

Viewing events and logs in the console

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

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

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

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

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

To view events and logs

1 Navigate



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



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

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

Glossary

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.
klish	Command Line Interface SHell. Provides the command line menu on the virtual appliance for use after the initial bootstrap configuration.
data center	<p>A location that contains asset infrastructure to be managed by Veritas Resiliency Platform.</p> <p>For the disaster recovery use case, the resiliency domain must contain at least two data centers in different locations, a production data center and recovery data center. Each data center has a Resiliency Manager and one or more IMSs.</p>
host	<p>Physical servers, virtual machines, or Hyper-V servers that are added to the Infrastructure Management Server (IMS) as hosts.</p> <p>Adding the assets as hosts installs the host package that is used by the IMS for discovery and monitoring.</p>
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	<p>A zero-downtime test that mimics the configuration, application data, storage, and the failover behavior of the resiliency group.</p> <p>Rehearsal verifies the ability of the resiliency group to fail over to the recovery data center during a disaster.</p>
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.
take over	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	<p>An appliance that includes the operating system environment and the software application which are deployed together as a virtual machine.</p> <p>The Veritas Resiliency Platform virtual appliance is deployed as a virtual machine and then configured with basic settings and a role (for example, Resiliency Manager).</p>
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

A

- activities
 - abort 35
 - view 34

D

- disaster recovery
 - using Resiliency Platform 10
- disaster recovery operations
 - migrating 20
 - rehearsal 18
 - take over 20

E

- evacuation plan
 - about 48
 - cleanup evacuation rehearsal 52
 - evacuating 52
 - generating 50
 - regenerating 51
 - rehearse evacuation 52
- events 54

L

- logs
 - viewing in console 54

P

- permissions
 - about 9

R

- reports
 - current risk 32
 - historical risk 33
- resiliency groups
 - roles 11
- resiliency plan templates
 - create 37

- resiliency plan templates *(continued)*

- deleting 41
- editing 40
- viewing 41

- resiliency plans

- about 36
- create schedule 45
- creating 42
- custom script 39
- delete schedule 46
- deleting 44
- edit schedule 46
- editing 43
- executing 44
- manual task 38
- view schedule 47
- viewing 45

- Resiliency Platform

- features and components 7

- risk insight

- about 24

- risks

- current risk report 32
- description 26
- historical risk report 33
- view information 25

V

- VBS

- cleanup rehearsal 19
- resync 21

- Veritas Resiliency Platform

- about 6

- virtual business services

- about 12
- creating 13
- deleting 18
- displaying details 16
- editing 17
- migrating 20
- rehearsal 18

virtual business services *(continued)*

starting and stopping 15

take over 20

understanding tiers 13