

Veritas™ Resiliency Platform 3.3.1 Overview and Planning Guide

Veritas Resiliency Platform: Overview and Planning Guide

Last updated: 2018-09-26

Document version: Document version: 3.3.1 Rev 0

Legal Notice

Copyright © 2018 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/licensing/process>

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:

vrpdocs@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	5
	About Veritas Resiliency Platform	5
	About Resiliency Platform features and components	6
	About Resiliency Manager	9
	About Infrastructure Management Server (IMS)	9
	About Replication Gateways	10
	About Data Gateway	11
	About resiliency domain	11
Chapter 2	Planning your Resiliency Platform environment	13
	Replication in a Resiliency Platform deployment	13
	About Object Storage mode replication	14
	Recovery options using Resiliency Platform	14
	Planning a resiliency domain for efficiency and fault tolerance	16
	Simplified trialware deployment experience	17
	On-boarding with Resiliency Platform	17
Index		19
Glossary		20

Overview of Resiliency Platform

This chapter includes the following topics:

- [About Veritas Resiliency Platform](#)
- [About Resiliency Platform features and components](#)

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 Resiliency Platform 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 Data Mover is a separately licensable feature of Veritas Resiliency Platform. It provides data replication between geographically separated data centers facilitating an effective disaster recovery solution. The Resiliency Platform Data Mover can be used for the following purposes:

- For recovery of VMware virtual machines to VMware virtual machines
- For recovery of Linux and Windows physical machines to VMware virtual machines
- For recovery of VMware and Hyper-V virtual machines to cloud data center

Resiliency Platform has the following core capabilities:

Security and Compliance	Veritas Resiliency Platform provides enhanced data encryption for data-in-flight.
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 6.

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 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.
--------------------	---

See [“About Resiliency Manager”](#) on page 9.

Infrastructure Management Server (IMS)	<p>The component that discovers, monitors, and manages the asset infrastructure within a data center. The IMS transmits information about the asset infrastructure to the Resiliency Manager. The IMS is deployed as a virtual appliance.</p> <p>To achieve scale, multiple IMSs can be deployed in the same data center.</p> <p>See “About Infrastructure Management Server (IMS)” on page 9.</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> <p>If you plan to use any third party replication technology, you do not need to deploy Replication Gateway.</p> <p>See “About Replication Gateways” on page 10.</p>
Data Gateway	<p>The component of Veritas Resiliency Platform that is deployed in AWS data center to enable replication using Object Storage. You need to deploy this component only if you plan to use Object Storage replication for recovery of your data center assets to AWS data center.</p> <p>See “About Data Gateway” on page 11.</p>
resiliency domain	<p>The logical scope of a Resiliency Platform deployment.</p> <p>It can extend across multiple data centers.</p> <p>See “About resiliency domain” on page 11.</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. If you are using Resiliency Platform Data Mover for replication, each data center must also have at least one Replication Gateway.</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>
NetBackup Server	<p>The component that allows restoration of virtual machines to a local or remote data center using NetBackup generated backup images.</p> <p>You need to add this component only if you want to restore the virtual machines using NetBackup generated backup images.</p>
Veritas InfoScale Operations Manager Management Server	<p>The component that allows discovery of InfoScale applications that are already configured in Veritas InfoScale Operations Manager, also referred to as Veritas InfoScale Operations Manager server. 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> <p>You need to add this component only if you want to manage and recover the Infoscale applications that are already configured in Veritas InfoScale Operations Manager.</p>
Virtual Business Service (VBS)	<p>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 perform the disaster recovery operations on the entire VBS.</p>

About Resiliency Manager

The Resiliency Manager includes a set of loosely coupled services, a distributed data repository, and a management web console. The Resiliency Manager provides the services required for protecting assets, such as virtual machines, within a resiliency domain. It also provides workload automation services.

You start by deploying one Resiliency Manager and creating the resiliency domain. You can then add more Resiliency Managers to the resiliency domain for efficiency of local access and for fault tolerance. You can deploy multiple Resiliency Managers in the same data center or in separate geographical locations.

The Resiliency Manager discovers and manages information about data center assets from an Infrastructure Management Server (IMS), which is another required Resiliency Platform component. The Resiliency Manager stores the asset information in its data repository and displays the information in its management console.

Multiple Resiliency Managers that are part of the same domain synchronize their databases using built-in replication. Each Resiliency Manager has its own web console but because the data is synchronized, all consoles show the same data. Operations can be performed from any console and the results show in all the consoles in the resiliency domain.

See [“About resiliency domain”](#) on page 11.

See [“About Infrastructure Management Server \(IMS\)”](#) on page 9.

About Infrastructure Management Server (IMS)

Each Resiliency Manager requires one or more Infrastructure Management Servers (IMSs). An IMS discovers and monitors assets within a data center. You use the web console to add the asset infrastructure to Resiliency Platform so that assets can be discovered and monitored by an IMS.

The asset infrastructure can include objects such as hosts, virtualization servers, and enclosures (storage arrays).

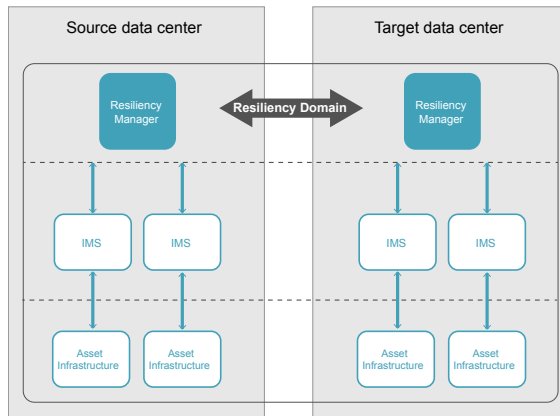
The IMS sends information about the assets to the Resiliency Manager so that the Resiliency Manager can manage the assets. Management operations on assets (for example, starting or stopping virtual machines) that you initiate from the web console are carried out by the IMS.

If there are multiple data centers in different geographical locations, a separate IMS is deployed and configured for each geographical data center location.

Each IMS connects to only one Resiliency Manager at a time. If a Resiliency Manager failure occurs, an IMS can automatically connect to another Resiliency Manager within the same domain.

You can also configure multiple Infrastructure Management Servers in the same data center. For example, to achieve scale, you can add a separate IMS for a separate business unit such as Human Resources or Finance. More than one IMS can be managed by the same Resiliency Manager.

Figure 1-1 Multiple Infrastructure Management Servers in a data center



See [“About resiliency domain”](#) on page 11.

See [“About Resiliency Manager”](#) on page 9.

About Replication Gateways

If you plan to use Resiliency Platform Data Mover for replication of data in your environment, you need to deploy and configure at least one Replication Gateway in your source as well as target data center.

The Replication Gateway component of Veritas Resiliency Platform is a staging server that aggregates and batches data from multiple virtual machines during replication. The Gateway also performs data optimization like local deduplication and compression. The Gateway on source data center is always paired with a Gateway on target data center. The target data center Gateway is a staging server that applies the data on the source data center storage.

Each Replication Gateway includes the following components:

- I/O receiver
Receives the application I/Os that were tapped and sent by the application host in a continuous fashion.
- Transceiver
Transfers and receives data over the WAN link periodically.

- **Applier**
Applies the data to the storage after it is received on the cloud Gateway.
- **Scheduler**
Manages the jobs and policies in the Gateway.
- **Engine**
Maintains the state of replication and also coordinates with all other components.

About Data Gateway

If you want to choose Object Storage replication mode for migration of your assets to AWS, you need to deploy a Data Gateway in AWS environment.

The Data Gateway acts like a communication channel between the on-premises Replication Gateway and cloud Replication Gateway. The data being replicated from the on-premises data center gets compressed and stored in S3 bucket in the form of objects. The cloud Replication Gateway pulls this data from S3 bucket, decompresses it and applies to the target disk.

You can use a single Data Gateway for replicating data between multiple Replication Gateways.

To deploy the Data Gateway in AWS, you need to download a zip file that is shipped along with Veritas Resiliency Platform.

A few resources get created in AWS when you deploy a Data Gateway in the AWS environment. You must not delete these resources while the Data Gateway is in use as it may impact the functionality of the feature and the product. These resources automatically get deleted when you delete the Data Gateway.

About resiliency domain

A resiliency domain is the management domain of a Veritas Resiliency Platform deployment. It represents the scope of the deployment, which can spread across multiple data centers and can include multiple Resiliency Managers and other components, along with the infrastructure that is being managed and protected. Within the resiliency domain, Resiliency Platform can protect assets, for example, virtual machines and applications, and orchestrate automation of workload tasks for the assets.

The resiliency domain is a logical object that you create from the web console after you deploy the Resiliency Manager.

For disaster recovery, the resiliency domain must contain at least two data centers, a production data center and a recovery data center that can be on-premises or in the cloud.

A resiliency domain can optionally be implemented at a single data center for automation of workload tasks.

See [“About Resiliency Manager”](#) on page 9.

See [“About Infrastructure Management Server \(IMS\)”](#) on page 9.

Planning your Resiliency Platform environment

This chapter includes the following topics:

- [Replication in a Resiliency Platform deployment](#)
- [Recovery options using Resiliency Platform](#)
- [Planning a resiliency domain for efficiency and fault tolerance](#)
- [On-boarding with Resiliency Platform](#)

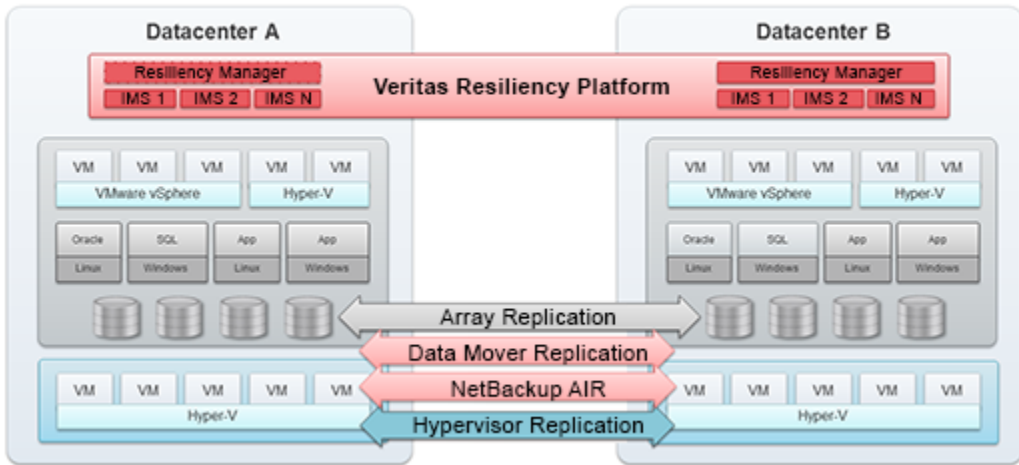
Replication in a Resiliency Platform deployment

Veritas Resiliency Platform supports several forms of replication for data recovery from your source data center to your target data center.

- Array-based replication (block-based replication) using supported arrays
- Hypervisor-based replication using Hyper-V Replica
- NetBackup Auto Image Replication (AIR)
- Resiliency Platform Data Mover (separately licensable feature of Resiliency Platform)

For details on supported replication hardware and software, refer to the *Hardware and Software Compatibility List*.

Figure 2-1 Replication in a Resiliency Platform deployment



About Object Storage mode replication

If you want to migrate your data center assets to AWS, you have an option to choose between Object Storage mode replication and Direct mode replication.

In Resiliency Platform, the Object Storage mode replication is used to leverage the S3 Object Storage services provided by AWS. The following are some of the advantages of using the Object Storage mode replication in Resiliency Platform:

- Automatically scales according to the requirements of the user by utilizing the AWS services to achieve scalability.
- Facilitates resiliency for the Replication Gateway. Since the data keeps getting replicated and stored in S3 bucket, failure of replication gateway in the cloud does not hamper the replication.

To enable the Object Storage mode replication, you need to deploy a Data Gateway in AWS environment.

See [“About Data Gateway”](#) on page 11.

Recovery options using Resiliency Platform

There are various recovery options available with Resiliency Platform. You can use any of the supported third-party replication technologies, NetBackup, or Resiliency

Platform Data Mover to replicate and recover your data across data centers. You can also recover your InfoScale applications using Resiliency Platform.

Table 2-1

Category	Recovery options
Using third-party replication	Recovery to on-premises data center: <ul style="list-style-type: none"> Recovery of VMware virtual machines to on-premises data center Recovery of Hyper-V virtual machines to on-premises data center Recovery of applications to on-premises data center
Using NetBackup	Recovery to local and remote data center: <ul style="list-style-type: none"> Recovery of VMware virtual machines to local and remote data center
Using Resiliency Platform Data Mover	<ul style="list-style-type: none"> Recovery to on-premises data center: <ul style="list-style-type: none"> Recovery of VMware virtual machines to on-premises data center using VAIO Recovery to AWS data center: <ul style="list-style-type: none"> Recovery of VMware virtual machines to AWS data center Recovery of Hyper-V virtual machines to AWS data center Recovery to vCloud data center: <ul style="list-style-type: none"> Recovery of VMware virtual machines to vCloud data center Recovery of Hyper-V virtual machines to vCloud data center Recovery of VMware virtual machines to vCloud data center without adding the vCenter Server Recovery of Hyper-V virtual machines to vCloud data center without adding the Hyper-V Server Recovery to Azure data center: <ul style="list-style-type: none"> Recovery of VMware virtual machines to Azure data center Recovery of Hyper-V virtual machines to Azure data center Recovery to OpenStack data center: <ul style="list-style-type: none"> Recovery of VMware virtual machines to OpenStack data center Recovery of Hyper-V virtual machines to OpenStack data center
Using Veritas InfoScale Management Server	Recovery to on-premises data center: <ul style="list-style-type: none"> Recovery of InfoScale applications to on-premises data center

Planning a resiliency domain for efficiency and fault tolerance

Before you deploy Veritas Resiliency Platform, you should plan how to scale the deployment for efficiency and fault tolerance.

Although a resiliency domain requires only one Resiliency Manager, you can add multiple Resiliency Managers instances to the domain. For example, you can distribute Resiliency Managers geographically for efficiency of local access. For resiliency, you can even have multiple Resiliency Managers in one data center.

If you have multiple Resiliency Managers in the resiliency domain, the recommended WAN latency between two Resiliency Managers is recommended to be less than 30 milliseconds. The maximum WAN latency allowed between the two Resiliency Managers is 50 milliseconds. This latency requirement applies to any two Resiliency Managers - within a single data center or across two different data centers.

The recommended minimum deployment for disaster recovery to on-premises data center in production environment would be four virtual appliances: a Resiliency Manager and Infrastructure Management Servers (IMS) in the production data center and a Resiliency Manager and IMS in the recovery data center. In a test environment, you can have only one Resiliency Manager at the target data center.

The recommended minimum deployment for disaster recovery to cloud data center would be three virtual appliances: an IMS in the production data center and a Resiliency Manager and IMS in the recovery data center.

The source and target data centers do not require a one-on-one mapping of IMSs. For example, you can have two IMSs in the source data center and one IMS in the target data center.

You can add multiple Infrastructure Management Servers (IMS) to a resiliency domain. For example, if there are multiple data centers in different geographical locations to be managed, you configure a separate IMS for each geographical data center location. You can also configure more than one IMS in the same data center.

If you plan to use Resiliency Platform data mover for replication, then additionally you need minimum one Replication Gateway in each data center. Resiliency Platform supports asymmetric pairing of Replication Gateways. This feature facilitates deployment of only the required number of Gateways on each side, based on data transfer rate and technology specific limits. One Gateway on production site can be paired with multiple Gateways on recovery site and vice versa. One Gateway can be paired with up to 16 gateways on the peer site.

Table 2-2

For more information on.....	Refer to....
Network	About FIPS enablement About NAT support About IPv6 support
Capacity planning for Resiliency Platform replication appliances	VMware vSphere environment VMware vSphere and Azure environment VMware vSphere and AWS environment
Network objects and mapping of network objects required across data centers	About network objects About purpose Creating network pairs between data centers

See [“About resiliency domain”](#) on page 11.

See [“About Resiliency Manager”](#) on page 9.

See [“About Infrastructure Management Server \(IMS\)”](#) on page 9.

Simplified trialware deployment experience

Veritas Resiliency Platform 3.2 introduces a simplified trialware or Proof of Concept (POC) deployment experience for a new user. You get use case based resources that include zip files to be used for deployment and configuration, a configuration planner, and a Quick Start guide explaining the entire flow along with the documentation link.

On-boarding with Resiliency Platform

The following table describes the various steps that are involved in the customer on-boarding with Resiliency Platform and what to expect during each of these steps:

Table 2-3 On-boarding with Resiliency Platform

Step	Description
Deploy	<ul style="list-style-type: none"> ■ Deploy Resiliency Platform virtual appliances and configure them as Resiliency Manager, Infrastructure Management Server (IMS), or Replication Gateway ■ Define the resiliency domain through Getting Started wizard ■ Add assets to your resiliency domain for discovery: <ul style="list-style-type: none"> ■ Virtual machines ■ Applications ■ Storage enclosures
Discover	<ul style="list-style-type: none"> ■ Resiliency Platform's deep discovery enables identification of the following: <ul style="list-style-type: none"> ■ Virtual machines ■ Applications ■ Storage enclosures ■ Software/hardware replication ■ Virtual networks (vSwitches)
Define service level objective	<ul style="list-style-type: none"> ■ Configure service level objective based on the intended Recovery Point Objective (RPO). service level objective driven configuration enables the following capabilities: <ul style="list-style-type: none"> ■ Basic monitoring of assets ■ Recovery of assets ■ Recovery of multi-tier business services (VBS) ■ Health status reporting of assets ■ Risk alerts and notifications for protected assets
Manage	<ul style="list-style-type: none"> ■ Single-click rehearsal for resiliency groups and VBS validates disaster readiness: <ul style="list-style-type: none"> ■ Automated rehearsal ■ Automated rehearsal cleanup ■ Option of network isolation for workloads during rehearsal ■ Single-click recovery or migration of resiliency groups and VBS: <ul style="list-style-type: none"> ■ Automated recovery or migration based on the service level objective ■ Recovery with predefined network customization ■ Recovery based on predefined grouping or order ■ Controlled recovery using Resiliency Plans ■ Single-click evacuation plan for resiliency groups and VBS: <ul style="list-style-type: none"> ■ Option of defining priority levels for VBS ■ Automated rehearsal or cleanup rehearsal for evacuation plan

Index

D

- Data Gateway 14
- deployment
 - replication 13

O

- overview
 - Data Gateway 11
 - IMS 9
 - Replication Gateways 10
 - resiliency domain 11
 - Resiliency Manager 9

R

- replication
 - Object Storage 14
- Resiliency Platform
 - about 5
 - features and components 6

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, virtualization servers, virtual machines, enclosures, and applications.
assets	The virtual machines, physical 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 source data center and target data center. Each data center has a Resiliency Manager and one or more IMSs.</p>
host	In Veritas Resiliency Platform, hosts means Windows Install host, Application host, Resiliency Platform Data Mover host, Storage discovery host, VMware Discovery host, and Hyper-V host.
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 assets at the source data center and starting them at the target data center. In this process, replication ensures that consistent data is made available at the target 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.
source data center	The data center that is normally used for business.
target data center	The data center that is used if a disaster scenario occurs.

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 to be 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 web 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 source data center is down due to a disaster and the assets need to be restored at the target 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 operations are performed on the resiliency groups.
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 recovery in case of a disaster in the desired order.
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.