Veritas™ Resiliency Platform 3.0 User Guide

VERITAS™

Veritas Resiliency Platform: User Guide

Last updated: 2017-09-21

Document version: Document version: 3.0 Rev 0

Legal Notice

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

Recovery to cloud data center

This chapter includes the following topics:

- Recovering VMware virtual machines to AWS

- Recovering Hyper-V virtual machines to AWS

- Recovering VMware virtual machines to Azure

- Recovering Hyper-V virtual machines to Azure

- Recovering VMware virtual machines to vCloud Director

- Recovering Hyper-V virtual machines to vCloud Director

- Recovering VMware virtual machines to vCloud Director without adding vCenter server

- Recovering Hyper-V virtual machines to vCloud Director without adding Hyper-V server

Recovering VMware virtual machines to AWS

Using Veritas Resiliency Platform 3.0, you can configure and protect your VMware virtual machines for recovery to AWS using the Resiliency Platform Data Mover.

Figure 1-1   Overview of deployment Infrastructure for recovery to AWS

The following table provides the summary for deployment, configuration, and recovery of virtual machines to a data center on AWS.

Table 1-1   Recovering VMware virtual machines to AWS

Tasks	More information
Plan your environment	Refer to the Release Notes for release information such as main features, known issues, and limitations. Ensure that the configuration details in your environment matches the requirements mentioned in the System resources and Hardware and software list. ■ Release Notes ■ Hardware and software list ■ System resources ■ List of ports

Table 1-1 Recovering VMware virtual machines to AWS *(continued)*

Tasks	More information

Deploy and configure the virtual appliances
 	
	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in the AWS cloud data center as well as in the premises data center.
	
	■ Download the files required for deployment
	■ About deploying the virtual appliances
	■ Deploy the virtual appliances for Resiliency Manager, Infrastructure Management Server (IMS), and Replication Gateway in the AWS cloud data center:
	  ■ Using AWS
	■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the premises data center:
	  ■ Using VMware vSphere client
	■ Configure the virtual appliances as Veritas Resiliency Platform components:
	  ■ About configuring the virtual appliances
	  ■ Prerequisites
	  ■ Configuring Resiliency Manager or IMS
	  ■ Configuring Replication Gateways

Set up the resiliency domain
 	
	Set up the infrastructure and basic settings of the Veritas Resiliency Platform resiliency domain. These tasks are performed after you configure the Resiliency Manager and log in to the web console.
	
	■ Create the resiliency domain:
	  ■ Using getting started wizard
	■ Configure the settings for the resiliency domain:
	  ■ Add IMS
	  ■ Add Replication Gateways
	  ■ Add cloud data center (if not done during getting started wizard)
	  ■ Manage user authentication and permission
	  ■ Manage alerts, notifications, and other product settings

Add asset infrastructure 	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console. ■ Add VMware servers ■ Prepare host for replication ■ Create Replication Gateway pair ■ Map production network to rehearsal network ■ Setup network mapping between data centers

Table 1-1   Recovering VMware virtual machines to AWS *(continued)*

Tasks	More information
Create resiliency groups	After adding the assets to Resiliency Platform, you organize the related assets into a resiliency group that you can protect and manage as a single entity. You can create a resiliency group either for basic monitoring (start or stop virtual machines) or for remote recovery. ■ Configure resiliency groups for basic monitoring ■ Prerequisites for configuring resiliency groups for recovery to AWS ■ Configure resiliency groups for recovery to AWS
Advanced features	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets. ■ Virtual business services ■ Resiliency plans ■ Evacuation plans
Perform remote recovery operations	Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Resync ■ Take over
Monitor assets	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page. ■ Risks ■ Reports ■ Activities

| | **Table 1-1** | Recovering VMware virtual machines to AWS *(continued)* |

Tasks	More information
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. You can also use klish to update Resiliency Platform components. ■ Using klish ■ Troubleshooting ■ Updating ■ References

Recovering Hyper-V virtual machines to AWS

Using Veritas Resiliency Platform 3.0, you can configure and protect your VMware and Hyper-V virtual machines for recovery to AWS using the Resiliency Platform Data Mover.

Figure 1-2   Overview of deployment Infrastructure for recovery to AWS

The following table provides the summary for deployment, configuration, and recovery of virtual machines to a data center on AWS.

Table 1-2 Recovering Hyper-V virtual machines to AWS

Tasks	More information
Plan your environment	Refer to the Release Notes for release information such as main features, known issues, and limitations. Ensure that the configuration details in your environment matches the requirements mentioned in the System resources and Hardware and software list. ■ Release Notes ■ Hardware and software list ■ System resources ■ List of ports
Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in the AWS cloud data center as well as in the premises data center. ■ Download the files required for deployment ■ About deploying the virtual appliances ■ Deploy the virtual appliances for Resiliency Manager, Infrastructure Management Server (IMS), and Replication Gateway in the AWS cloud data center: 　　■ Using AWS ■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the premises data center: 　　■ Using Hyper-V Manager ■ Configure the virtual appliances as Veritas Resiliency Platform components: 　　■ About configuring the virtual appliances 　　■ Prerequisites 　　■ Configuring Resiliency Manager or IMS 　　■ Configuring Replication Gateways
Set up the resiliency domain	Set up the infrastructure and basic settings of the Veritas Resiliency Platform resiliency domain. These tasks are performed after you configure the Resiliency Manager and log in to the web console. ■ Create the resiliency domain: 　　■ Using getting started wizard ■ Configure the settings for the resiliency domain: 　　■ Add IMS 　　■ Add Replication Gateways 　　■ Add cloud data center (if not done during getting started wizard) 　　■ Manage user authentication and permission 　　■ Manage alerts, notifications, and other product settings

Table 1-2 Recovering Hyper-V virtual machines to AWS *(continued)*

Tasks	More information
Add asset infrastructure	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console.
	■ Add Hyper-V servers
	■ Prepare host for replication
	■ Create Replication Gateway pair
	■ Map production network to rehearsal network
	■ Setup network mapping between data centers
Create resiliency groups	After adding the assets to Resiliency Platform, you organize the related assets into a resiliency group that you can protect and manage as a single entity. You can create a resiliency group either for basic monitoring (start or stop virtual machines) or for remote recovery.
	■ Configure resiliency groups for basic monitoring
	■ Prerequisites for configuring resiliency groups for recovery to AWS
	■ Configure resiliency groups for recovery to AWS
Advanced features	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets.
	■ Virtual business services
	■ Resiliency plans
	■ Evacuation plans
Perform remote recovery operations	Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups.
	■ Rehearsal
	■ Cleanup rehearsal
	■ Migrate
	■ Resync
	■ Take over

| Table 1-2 | Recovering Hyper-V virtual machines to AWS *(continued)* |

Tasks	More information
Monitor assets	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page.
	■ Risks
	■ Reports
	■ Activities
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot.
	■ Using klish
	■ Troubleshooting
	■ Updating
	■ References

Recovering VMware virtual machines to Azure

Using Veritas Resiliency Platform 3.0, you can configure and protect your VMware virtual machines for recovery to Azure using the Resiliency Platform Data Mover.

Figure 1-3   Overview of deployment Infrastructure for recovery to Azure

The following table provides the summary for deployment, configuration, and recovery of virtual machines to a data center on Azure.

Table 1-3   Recovering VMware virtual machines to Azure

Tasks	More information
Plan your environment	Refer to the Release Notes for release information such as main features, known issues, and limitations. Ensure that the configuration details in your environment matches the requirements mentioned in the System resources and Hardware and software list.
	■ Release Notes
	■ Hardware and software list
	■ System resources
	■ List of ports

Table 1-3 Recovering VMware virtual machines to Azure *(continued)*

Tasks	More information
Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in the Azure cloud data center as well as in the premises data center. ■ Download the files required for deployment ■ About deploying the virtual appliances ■ Deploy the virtual appliances for Resiliency Manager, Infrastructure Management Server (IMS), and Replication Gateway in the Azure cloud data center: 　■ Using Azure ■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the premises data center: 　■ Using VMware vSphere client ■ Configure the virtual appliances as Veritas Resiliency Platform components: 　■ About configuring the virtual appliances 　■ Prerequisites 　■ Configuring Resiliency Manager or IMS 　■ Configuring Replication Gateways
Set up the resiliency domain	Set up the infrastructure and basic settings of the Veritas Resiliency Platform resiliency domain. These tasks are performed after you configure the Resiliency Manager and log in to the web console. ■ Create the resiliency domain: 　■ Using getting started wizard ■ Configure the settings for the resiliency domain: 　■ Add IMS 　■ Add Replication Gateways 　■ Add cloud data center (if not done during getting started wizard) 　■ Manage user authentication and permission 　■ Manage alerts, notifications, and other product settings
Add asset infrastructure	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console. ■ Add VMware servers ■ Prepare host for replication ■ Create Replication Gateway pair ■ Map production network to rehearsal network ■ Setup network mapping between data centers

Table 1-3   Recovering VMware virtual machines to Azure *(continued)*

Tasks	More information
Create resiliency groups	After adding the assets to Resiliency Platform, you organize the related assets into a resiliency group that you can protect and manage as a single entity. You can create a resiliency group either for basic monitoring (start or stop virtual machines) or for remote recovery. ■ Configure resiliency groups for basic monitoring ■ Prerequisites for configuring resiliency groups for recovery to Azure ■ Configure resiliency groups for recovery to Azure
Advance features	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets. ■ Virtual business services ■ Resiliency plans ■ Evacuation plans
Perform remote recovery operations	Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Resync ■ Take over
Monitor assets	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page. ■ Risks ■ Reports ■ Activities

| Table 1-3 | Recovering VMware virtual machines to Azure *(continued)* |

Tasks	More information
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot.
	■ Using klish
	■ Troubleshooting
	■ Updating
	■ References

Recovering Hyper-V virtual machines to Azure

Using Veritas Resiliency Platform 3.0, you can configure and protect your Hyper-V virtual machines for recovery to Azure using the Resiliency Platform Data Mover.

Figure 1-4   Overview of deployment Infrastructure for recovery to Azure

The following table provides the summary for deployment, configuration, and recovery of virtual machines to a data center on Azure.

Table 1-4   Recovering Hyper-V virtual machines to Azure

Tasks	More information
Plan your environment	Refer to the Release Notes for release information such as main features, known issues, and limitations. Ensure that the configuration details in your environment matches the requirements mentioned in the System resources and Hardware and software list. ■ Release Notes ■ Hardware and software list ■ System resources ■ List of ports
Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in the Azure cloud data center as well as in the premises data center. ■ Download the files required for deployment ■ About deploying the virtual appliances ■ Deploy the virtual appliances for Resiliency Manager, Infrastructure Management Server (IMS), and Replication Gateway in the Azure cloud data center: ■ Using Azure ■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the premises data center: ■ Using Hyper-V Manager ■ Configure the virtual appliances as Veritas Resiliency Platform components: ■ About configuring the virtual appliances ■ Prerequisites ■ Configuring Resiliency Manager or IMS ■ Configuring Replication Gateways
Set up the resiliency domain	Set up the infrastructure and basic settings of the Veritas Resiliency Platform resiliency domain. These tasks are performed after you configure the Resiliency Manager and log in to the web console. ■ Create the resiliency domain: ■ Using getting started wizard ■ Configure the settings for the resiliency domain: ■ Add IMS ■ Add Replication Gateways ■ Add cloud data center (if not done during getting started wizard) ■ Manage user authentication and permission ■ Manage alerts, notifications, and other product settings

Table 1-4   Recovering Hyper-V virtual machines to Azure *(continued)*

Tasks	More information
Add asset infrastructure	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console. ■ Add Hyper-V servers ■ Prepare host for replication ■ Create Replication Gateway pair ■ Map production network to rehearsal network ■ Setup network mapping between data centers
Create resiliency groups	After adding the assets to Resiliency Platform, you organize the related assets into a resiliency group that you can protect and manage as a single entity. You can create a resiliency group either for basic monitoring (start or stop virtual machines) or for remote recovery. ■ Configure resiliency groups for basic monitoring ■ Prerequisites for configuring resiliency groups for recovery to Azure ■ Configure resiliency groups for recovery to Azure
Advance features	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets. ■ Virtual business services ■ Resiliency plans ■ Evacuation plans
Perform remote recovery operations	Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Resync ■ Take over

Table 1-4   Recovering Hyper-V virtual machines to Azure *(continued)*

Tasks	More information
Monitor assets	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page. ■ Risks ■ Reports ■ Activities
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. ■ Using klish ■ Troubleshooting ■ Updating ■ References

Recovering VMware virtual machines to vCloud Director

Using Veritas Resiliency Platform 3.0, you can configure and protect your VMware virtual machines for recovery to vCloud Director using the Resiliency Platform Data Mover.

Before starting the product deployment in your data center, ensure that the cloud tenant is created for you and you have the cloud credentials to access it.

Figure 1-5 Overview of deployment infrastructure for recovery to vCloud Director

The following table provides the summary for deployment, configuration, and recovery of virtual machines to a data center on vCloud Director. These operations can be performed by the end user or the service subscriber.

Table 1-5 Recovering VMware virtual machines to vCloud Director

Tasks	More information
Plan your environment	Refer to the Release Notes for release information such as main features, known issues, and limitations. Ensure that the configuration details in your environment matches the requirements mentioned in the System resources and Hardware and software list. ■ Release Notes ■ Hardware and software list ■ System resources ■ List of ports

| Table 1-5 | Recovering VMware virtual machines to vCloud Director *(continued)* |

Tasks	More information

Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in the premises as well as cloud data center.
	
	 ■ Download the files required for deployment
	 ■ About deploying the virtual appliances
	 ■ Deploy the virtual appliances in vCloud Director for Resiliency Manager, Infrastructure Management Server (IMS), and Replication Gateway. Each virtual data center in vCloud is represented as an individual data center in Resiliency Platform. If you have multiple virtual data centers, you need to create multiple data centers in Resiliency Platform and then deploy Resiliency Manager and IMS in one virtual data center and only IMS in rest of the virtual data centers:
	   ■ Using vCloud Director
	 ■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the premises data center:
	   ■ Using VMware vSphere client
	 ■ Configure the virtual appliances as Veritas Resiliency Platform components:
	   ■ About configuring the virtual appliances
	   ■ Prerequisites
	   ■ Configuring Resiliency Manager or IMS
	   ■ Configuring Replication Gateways

Set up the resiliency domain	Set up the infrastructure and basic settings of the Veritas Resiliency Platform resiliency domain. These tasks are performed after you configure the Resiliency Manager and log in to the web console.
	
	 ■ Create the resiliency domain:
	   ■ Using getting started wizard
	 ■ Configure the settings for the resiliency domain:
	   ■ Add IMS
	   ■ Add Replication Gateways
	   ■ Add cloud data center (if not done during getting started wizard)
	   ■ Manage user authentication and permission
	   ■ Manage alerts, notifications, and other product settings

Table 1-5   Recovering VMware virtual machines to vCloud Director
(continued)

Tasks	More information
Add asset infrastructure	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console. ■ Add VMware servers ■ Prepare host for replication ■ Create Replication Gateway pair ■ Setup network mapping between data centers
Create resiliency groups	After adding the assets to Resiliency Platform, you organize the related assets into a resiliency group that you can protect and manage as a single entity. You can create a resiliency group either for basic monitoring (start or stop virtual machines) or for remote recovery. ■ Configure resiliency groups for basic monitoring ■ Prerequisites for configuring virtual machines for remote recovery ■ Manage resiliency groups for remote recovery
Advanced features	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets. ■ Virtual business services ■ Resiliency plans ■ Evacuation plans
Perform remote recovery operations	Once you have organized your assets into resiliency groups, you can perform migrate, takeover, or resync operations on the resiliency groups. ■ Migrate ■ Resync ■ Take over

| | Table 1-5 | Recovering VMware virtual machines to vCloud Director *(continued)* |

Tasks	More information
Monitor assets	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page. ■ Risks ■ Reports ■ Activities
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. ■ Using klish ■ Troubleshooting ■ Updating ■ References

Recovering Hyper-V virtual machines to vCloud Director

Using Veritas Resiliency Platform 3.0, you can configure and protect your Hyper-V virtual machines for recovery to vCloud Director using the Resiliency Platform Data Mover.

Before starting the product deployment in your data center, ensure that the cloud tenant is created for you and you have the cloud credentials to access it.

Figure 1-6   Overview of deployment infrastructure for recovery to vCloud Director

The following table provides the summary for deployment, configuration, and recovery of virtual machines to a data center on vCloud Director. These operations can be performed by the end user or the service subscriber.

Table 1-6   Recovering Hyper-V virtual machines to vCloud Director

Tasks	More information
Plan your environment	Refer to the Release Notes for release information such as main features, known issues, and limitations. Ensure that the configuration details in your environment matches the requirements mentioned in the System resources and Hardware and software list. ■ Release Notes ■ Hardware and software list ■ System resources ■ List of ports

Table 1-6   Recovering Hyper-V virtual machines to vCloud Director
(continued)

Tasks	More information

Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in the premises as well as cloud data center.
	
	■ Download the files required for deployment
	■ About deploying the virtual appliances
	■ Deploy the virtual appliances in vCloud Director for Resiliency Manager, Infrastructure Management Server (IMS), and Replication Gateway. If you have multiple virtual data centers, deploy Resiliency Manager and IMS in one virtual data center and only IMS in rest of the virtual data centers:
	  ■ Using vCloud Director
	■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the premises data center:
	  ■ Using Hyper-V Manager
	■ Configure the virtual appliances as Veritas Resiliency Platform components:
	  ■ About configuring the virtual appliances
	  ■ Prerequisites
	  ■ Configuring Resiliency Manager or IMS
	  ■ Configuring Replication Gateways

Set up the resiliency domain	Set up the infrastructure and basic settings of the Veritas Resiliency Platform resiliency domain. These tasks are performed after you configure the Resiliency Manager and log in to the web console.
	
	■ Create the resiliency domain:
	  ■ Using getting started wizard
	■ Configure the settings for the resiliency domain:
	  ■ Add IMS
	  ■ Add Replication Gateways
	  ■ Add cloud data center (if not done during getting started wizard)
	  ■ Manage user authentication and permission
	  ■ Manage alerts, notifications, and other product settings

Add asset infrastructure	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console. ■ Add Hyper-V servers ■ Prepare host for replication ■ Create Replication Gateway pair ■ Setup network mapping between data centers

Table 1-6   Recovering Hyper-V virtual machines to vCloud Director
(continued)

Tasks	More information
Create resiliency groups	After adding the assets to Resiliency Platform, you organize the related assets into a resiliency group that you can protect and manage as a single entity. You can create a resiliency group either for basic monitoring (start or stop virtual machines) or for remote recovery. ■ Configure resiliency groups for basic monitoring ■ Prerequisites for configuring virtual machines for remote recovery ■ Manage resiliency groups for remote recovery
Advanced features	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets. ■ Virtual business services ■ Resiliency plans ■ Evacuation plans
Perform remote recovery operations	Once you have organized your assets into resiliency groups, you can perform migrate, takeover, or resync operations on the resiliency groups. ■ Migrate ■ Resync ■ Take over
Monitor assets	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page. ■ Risks ■ Reports ■ Activities

Table 1-6 Recovering Hyper-V virtual machines to vCloud Director *(continued)*

Tasks	More information
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. You can also use klish to update Resiliency Platform components. ■ Using klish ■ Troubleshooting ■ Updating ■ References

Recovering VMware virtual machines to vCloud Director without adding vCenter server

Using Veritas Resiliency Platform 3.0, you can configure and protect your VMware virtual machines for recovery to vCloud Director using the Resiliency Platform Data Mover without adding the vCenter server.

Before starting the product deployment in your data center, ensure that the cloud tenant is created for you and you have the cloud credentials to access it.

Figure 1-7   Overview of deployment infrastructure for recovery to vCloud Director

The following table provides the summary for deployment, configuration, and recovery of virtual machines to a data center on vCloud Director. These operations can be performed by the end user or the service subscriber.

Table 1-7   Recovering VMware virtual machines to vCloud Director without adding vCenter server

Tasks	More information
Plan your environment	Refer to the Release Notes for release information such as main features, known issues, and limitations. Ensure that the configuration details in your environment matches the requirements mentioned in the System resources and Hardware and software list.
	■ Release Notes
	■ Hardware and software list
	■ System resources
	■ List of ports

Table 1-7 Recovering VMware virtual machines to vCloud Director without adding vCenter server *(continued)*

Tasks	More information
Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in the premises as well as cloud data center. ■ Download the files required for deployment ■ About deploying the virtual appliances ■ Deploy the virtual appliances in vCloud Director for Resiliency Manager, Infrastructure Management Server (IMS), and Replication Gateway. If you have multiple virtual data centers, deploy Resiliency Manager and IMS in one virtual data center and only IMS in rest of the virtual data centers: ■ Using vCloud Director ■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the premises data center: ■ Using VMware vSphere client ■ Configure the virtual appliances as Veritas Resiliency Platform components: ■ About configuring the virtual appliances ■ Prerequisites ■ Configuring Resiliency Manager or IMS ■ Configuring Replication Gateways
Set up the resiliency domain	Set up the infrastructure and basic settings of the Veritas Resiliency Platform resiliency domain. These tasks are performed after you configure the Resiliency Manager and log in to the web console. ■ Create the resiliency domain: ■ Using getting started wizard ■ Configure the settings for the resiliency domain: ■ Add IMS ■ Add Replication Gateways ■ Add cloud data center (if not done during getting started wizard) ■ Manage user authentication and permission ■ Manage alerts, notifications, and other product settings
Add asset infrastructure	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console. ■ Prepare host for replication ■ Create Replication Gateway pair ■ Configure PXE Boot server on Replication Gateway ■ Setup network mapping between data centers

Table 1-7   Recovering VMware virtual machines to vCloud Director without adding vCenter server *(continued)*

Tasks	More information
Create resiliency groups	After adding the assets to Resiliency Platform, you organize the related assets into a resiliency group that you can protect and manage as a single entity. ■ Prerequisites for configuring virtual machines for remote recovery ■ Manage resiliency groups for remote recovery
Advanced features	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets. ■ Virtual business services ■ Resiliency plans ■ Evacuation plans
Perform remote recovery operations	Once you have organized your assets into resiliency groups, you can perform migrate, takeover, or resync operations on the resiliency groups. ■ Migrate ■ Resync ■ Take over
Monitor assets	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page. ■ Risks ■ Reports ■ Activities

Table 1-7	Recovering VMware virtual machines to vCloud Director without adding vCenter server *(continued)*
Tasks	**More information**
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. ■ Using klish ■ Troubleshooting ■ Updating ■ References

Recovering Hyper-V virtual machines to vCloud Director without adding Hyper-V server

Using Veritas Resiliency Platform 3.0, you can configure and protect your Hyper-V virtual machines for recovery to vCloud Director using the Resiliency Platform Data Mover without adding Hyper-V server.

Before starting the product deployment in your data center, ensure that the cloud tenant is created for you and you have the cloud credentials to access it.

Figure 1-8   Overview of deployment infrastructure for recovery to vCloud
Director

The following table provides the summary for deployment, configuration, and
recovery of virtual machines to a data center on vCloud Director. These operations
can be performed by the end user or the service subscriber.

Table 1-8   Recovering Hyper-V virtual machines to vCloud Director without
adding Hyper-V server

Tasks	More information
Plan your environment	Refer to the Release Notes for release information such as main features, known issues, and limitations. Ensure that the configuration details in your environment matches the requirements mentioned in the System resources and Hardware and software list. ■ Release Notes ■ Hardware and software list ■ System resources ■ List of ports

Table 1-8   Recovering Hyper-V virtual machines to vCloud Director without adding Hyper-V server *(continued)*

Tasks	More information

Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in the premises as well as cloud data center.
	
	■ Download the files required for deployment
	■ About deploying the virtual appliances
	■ Deploy the virtual appliances in vCloud Director for Resiliency Manager, Infrastructure Management Server (IMS), and Replication Gateway. If you have multiple virtual data centers, deploy Resiliency Manager and IMS in one virtual data center and only IMS in rest of the virtual data centers:
	   ■ Using vCloud Director
	■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the premises data center:
	   ■ Using Hyper-V Manager
	■ Configure the virtual appliances as Veritas Resiliency Platform components:
	   ■ About configuring the virtual appliances
	   ■ Prerequisites
	   ■ Configuring Resiliency Manager or IMS
	   ■ Configuring Replication Gateways

Set up the resiliency domain	Set up the infrastructure and basic settings of the Veritas Resiliency Platform resiliency domain. These tasks are performed after you configure the Resiliency Manager and log in to the web console.
	
	■ Create the resiliency domain:
	   ■ Using getting started wizard
	■ Configure the settings for the resiliency domain:
	   ■ Add IMS
	   ■ Add Replication Gateways
	   ■ Add cloud data center (if not done during getting started wizard)
	   ■ Manage user authentication and permission
	   ■ Manage alerts, notifications, and other product settings

Add asset infrastructure	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console. ■ Prepare host for replication ■ Create Replication Gateway pair ■ Configure PXE Boot server on Replication Gateway ■ Setup network mapping between data centers

Table 1-8   Recovering Hyper-V virtual machines to vCloud Director without adding Hyper-V server *(continued)*

Tasks	More information
Create resiliency groups	After adding the assets to Resiliency Platform, you organize the related assets into a resiliency group that you can protect and manage as a single entity. ■ Prerequisites for configuring virtual machines for remote recovery ■ Manage resiliency groups for remote recovery
Advanced features	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets. ■ Virtual business services ■ Resiliency plans ■ Evacuation plans
Perform remote recovery operations	Once you have organized your assets into resiliency groups, you can perform migrate, takeover, or resync operations on the resiliency groups. ■ Migrate ■ Resync ■ Take over
Monitor assets	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page. ■ Risks ■ Reports ■ Activities

	Table 1-8	Recovering Hyper-V virtual machines to vCloud Director without adding Hyper-V server *(continued)*

Tasks	More information
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. You can also use klish to update Resiliency Platform components. ■ Using klish ■ Troubleshooting ■ Updating ■ References

Recovery to on-premises data center

This chapter includes the following topics:

- Recovering VMware virtual machines to on-premises data center using Resiliency Platform Data Mover

- Recovering VMware virtual machines using NetBackup

- Recovering VMware virtual machines using 3rd party replication technology

- Recovering Hyper-V virtual machines using 3rd party replication technology

- Recovering Applications using 3rd party replication technology

- Recovering InfoScale applications

Recovering VMware virtual machines to on-premises data center using Resiliency Platform Data Mover

Using Veritas Resiliency Platform, you can recover VMware virtual machine to on-premises data center using Resiliency Platform Data Mover. Resiliency Platform Data Mover uses VMware VAIO (vSphere APIs for IO Filter) interfaces published and supported by VMware.

The following table provides the summary for deployment, configuration, and recovery of VMware virtual machines to on-premises data center using data mover.

Table 2-1 Recovering VMware virtual machines using VMware VAIO

Tasks	More information
Plan your environment	Refer to the Release Notes for release information such as main features, known issues, and limitations. Ensure that the configuration details in your environment matches the requirements mentioned in the System resources and Hardware and software list. ■ Release Notes ■ Hardware and software list ■ System resources ■ List of ports
Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances for Resiliency Manager, IMS, and Replication Gateway in both the data centers. ■ Download the files required for deployment ■ About deploying the virtual appliances ■ Deploy the virtual appliances using VMware vSphere client ■ Configure the virtual appliances as Veritas Resiliency Platform components: ■ About configuring the virtual appliances ■ Prerequisites ■ Configuring Resiliency Manager or IMS ■ Configuring Replication Gateways
Set up the resiliency domain	Set up the infrastructure and basic settings of the Veritas Resiliency Platform resiliency domain. These tasks are performed after you configure the Resiliency Manager and log in to the web console. ■ Create the resiliency domain: ■ Using getting started wizard ■ Configure the settings for the resiliency domain: ■ Add IMS ■ Add Replication Gateways ■ Manage user authentication and permission ■ Manage alerts, notifications, and other product settings
Add asset infrastructure	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console. ■ Add VMware virtualization servers ■ Create Replication Gateway pair ■ Map production network to rehearsal network (Optional) ■ Setup network mapping between data centers (Optional)

Table 2-1 Recovering VMware virtual machines using VMware VAIO
(continued)

Tasks	More information
Create resiliency groups	After adding the assets to Resiliency Platform, you organize the related assets into a resiliency group that you can protect and manage as a single entity. You can create a resiliency group either for basic monitoring (start or stop virtual machines) or for recovery to remote data center. ■ Configure resiliency groups for basic monitoring ■ Prerequisites for configuring VMware virtual machines for recovery to on-premises data center ■ Configure VMware virtual machines for recovery to on-premises data center
Advanced features	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets. ■ Virtual business services ■ Resiliency plans ■ Evacuation plans
Perform remote recovery operations	Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Resync ■ Take over
Monitor assets	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page. ■ Risks ■ Reports ■ Activities

| | Table 2-1 | Recovering VMware virtual machines using VMware VAIO *(continued)* |

Tasks	More information
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. You can also use klish to update Resiliency Platform components. ■ Using klish ■ Troubleshooting ■ Updating ■ References

Recovering VMware virtual machines using NetBackup

Using the Veritas Resiliency Platform 3.0, you can restore VMware virtual machine from NetBackup generated backup images to the recovery data center. For more information on NetBackup and NetBackup Appliances,

Figure 2-1 Deployment architecture for NetBackup master server

In the image, data center 1 is the production data center and data center 2 is recovery data center. Targeted Auto Image Replication, denoted as AIR in the

below image, ensures that the backup images are available on NetBackup master server in the recovery data center. The image shows two Infrastructure Management Servers (IMS) although you can have only one IMS which discovers the vCenter and is also added as an additional server to NetBackup.

The following table provides the summary for deployment, configuration, and recovery of virtual machines from NetBackup generated backup images.

Table 2-2   Recovering virtual machines using NetBackup images

Tasks	More information
Plan your environment	Refer to the Release Notes for release information such as main features, known issues, and limitations. Ensure that the configuration details in your environment matches the requirements mentioned in the System resources and Hardware and software list.
	■ Release Notes
	■ Hardware and software list
	■ System resources
	■ List of ports
Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances for Resiliency Manager and IMS in both the data centers.
	■ Download the files required for deployment
	■ About deploying the virtual appliances
	■ Deploy the virtual appliances using VMware vSphere client
	■ Configure the virtual appliances as Veritas Resiliency Platform components:
	■ About configuring the virtual appliances
	■ Prerequisites
	■ Configuring Resiliency Manager or IMS
Set up the resiliency domain	Set up the infrastructure and basic settings of the Veritas Resiliency Platform resiliency domain. These tasks are performed after you configure the Resiliency Manager and log in to the web console.
	■ Create the resiliency domain:
	■ Using getting started wizard
	■ Configure the settings for the resiliency domain:
	■ Add IMS
	■ Manage user authentication and permission
	■ Manage alerts, notifications, and other product settings

Table 2-2   Recovering virtual machines using NetBackup images *(continued)*

Tasks	More information
Add asset infrastructure	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console. ■ Add VMware servers ■ Add NetBackup master server ■ Add IMS to NetBackup master server as an additional server ■ Map production network to rehearsal network ■ Setup network mapping between data centers
Create resiliency groups	After adding the assets to Resiliency Platform, you organize the related assets into a resiliency group that you can protect and manage as a single entity. You can create a resiliency group either for basic monitoring (start or stop virtual machines) or for recovery on local or remote data center. ■ Configure resiliency groups for basic monitoring ■ Prerequisites for configuring VMware virtual machines for recovery using NetBackup images ■ Manage VMware virtual machines for remote recovery using NetBackup images
Advanced features	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets. ■ Virtual business services ■ Resiliency plans ■ Evacuation plans
Perform recovery operations	Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform restore (local or remote) operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Restore virtual machines

Table 2-2   Recovering virtual machines using NetBackup images *(continued)*

Tasks	More information
Monitor assets	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page. ■ Risks ■ Reports ■ Activities
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. ■ Using klish ■ Troubleshooting ■ Updating ■ References

Recovering VMware virtual machines using 3rd party replication technology

When you configure VMware virtual machines for disaster recovery, Veritas Resiliency Platform lets you select the replication technology to replicate data from a production data center to a recovery data center.

Veritas Resiliency Platform supports the following replication technologies. Depending on your environment, select the replication technology that best fits your business needs.

■ EMC SRDF

■ EMC Recoverpoint

■ Netapp (cDOT) Snapmirror

■ HP 3PAR Remote Copy

■ Hitachi TrueCopy/HUR

■ IBM SVC Global Mirror

■ IBM XIV Remote Mirror

Table 2-3	Recovering VMware virtual machines using 3rd party replication technology

Tasks	More information
Plan your environment	Refer to the Release Notes for release information such as main features, known issues, and limitations. Ensure that the configuration details in your environment matches the requirements mentioned in the System resources and Hardware and software list. ■ Release Notes ■ Hardware and software list ■ System resources ■ List of ports

Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances for Resiliency Manager and IMS in both the data centers.
	
	 ■ Download the files required for deployment
	 ■ About deploying the virtual appliances
	 ■ Deploy the virtual appliances using VMware vSphere client
	 ■ Configure the virtual appliances as Veritas Resiliency Platform components:
	    ■ About configuring the virtual appliances
	    ■ Prerequisites
	    ■ Configuring Resiliency Manager or IMS

Set up the resiliency domain	Set up the infrastructure and basic settings of the Veritas Resiliency Platform resiliency domain. These tasks are performed after you configure the Resiliency Manager and log in to the web console.
	
	 ■ Create the resiliency domain:
	    ■ Using getting started wizard
	 ■ Configure the settings for the resiliency domain:
	    ■ Add IMS
	    ■ Manage user authentication and permission
	    ■ Manage alerts, notifications, and other product settings

Add asset infrastructure	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console. ■ Add VMware virtualization servers ■ Add enclosures ■ Map production network to rehearsal network (Optional) ■ Setup network mapping between data centers (Optional)

Table 2-3 Recovering VMware virtual machines using 3rd party replication technology *(continued)*

Tasks	More information
Create resiliency groups	After adding the assets to Resiliency Platform, you organize the related assets into a resiliency group that you can protect and manage as a single entity. You can create a resiliency group either for basic monitoring (start or stop virtual machines) or for recovery on local or remote data center. ■ Configure resiliency groups for basic monitoring ■ Preparing virtual machines for recovery using array-based replication ■ Manage resiliency groups for remote recovery
Advanced features	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets. ■ Virtual business services ■ Resiliency plans ■ Evacuation plans
Perform remote recovery operations	Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Resync ■ Take over
Monitor assets	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page. ■ Risks ■ Reports ■ Activities

Table 2-3	Recovering VMware virtual machines using 3rd party replication technology *(continued)*
Tasks	**More information**
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. ■ Using klish ■ Troubleshooting ■ Updating ■ References

Recovering Hyper-V virtual machines using 3rd party replication technology

When you configure Hyper-V virtual machines for disaster recovery, Veritas Resiliency Platform lets you select the replication technology to replicate data from a production data center to a recovery data center.

Veritas Resiliency Platform supports the following replication technologies. Depending on your environment, select the replication technology that best fits your business needs.

■ Hyper-V Replica

■ EMC SRDF

■ EMC Recoverpoint

■ Netapp (cDOT) Snapmirror

■ HP 3PAR Remote Copy

■ Hitachi TrueCopy/HUR

■ IBM SVC Global Mirror

■ IBM XIV Remote Mirror

Table 2-4   Recovering Hyper-V virtual machines using 3rd party replication
                      technology

Tasks	More information
Plan your environment	Refer to the Release Notes for release information such as main features, known issues, and limitations. Ensure that the configuration details in your environment matches the requirements mentioned in the System resources and Hardware and software list. ■ Release Notes ■ Hardware and software list ■ System resources ■ List of ports
Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in both the data centers. ■ Download the files required for deployment ■ About deploying the virtual appliances ■ Deploy the virtual appliances for Resiliency Manager and Infrastructure Management Server (IMS) ■ Using VMware vSphere client ■ Using Hyper-V Manager ■ Configure the virtual appliances as Veritas Resiliency Platform components: ■ About configuring the virtual appliances ■ Prerequisites ■ Configuring Resiliency Manager or IMS
Set up the resiliency domain	Set up the infrastructure and basic settings of the Veritas Resiliency Platform resiliency domain. These tasks are performed after you configure the Resiliency Manager and log in to the web console. ■ Create the resiliency domain: ■ Using getting started wizard ■ Configure the settings for the resiliency domain: ■ Add IMS ■ Manage user authentication and permission ■ Manage alerts, notifications, and other product settings

Table 2-4   Recovering Hyper-V virtual machines using 3rd party replication technology *(continued)*

Tasks	More information
Add asset infrastructure	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console. ■ Add Hyper-V servers ■ Add enclosures ■ Map production network to rehearsal network (Optional) ■ Setup network mapping between data centers (Optional)
Create resiliency groups	After adding the assets to Resiliency Platform, you organize the related assets into a resiliency group that you can protect and manage as a single entity. You can create a resiliency group either for basic monitoring (start or stop virtual machines) or for recovery on local or remote data center. ■ Configure resiliency groups for basic monitoring ■ Preparing virtual machines for recovery using array-based replication ■ Manage resiliency groups for remote recovery
Advanced features	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets. ■ Virtual business services ■ Resiliency plans ■ Evacuation plans
Perform remote recovery operations	Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Resync ■ Take over

	Table 2-4	Recovering Hyper-V virtual machines using 3rd party replication technology *(continued)*

Tasks	More information
Monitor assets	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page. ■ Risks ■ Reports ■ Activities
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. ■ Using klish ■ Troubleshooting ■ Updating ■ References

Recovering Applications using 3rd party replication technology

When you configure applications for disaster recovery, Veritas Resiliency Platform lets you select the replication technology to replicate data from a production data center to a recovery data center.

Veritas Resiliency Platform supports the following replication technologies. Depending on your environment, select the replication technology that best fits your business needs.

■ EMC SRDF

■ EMC Recoverpoint

■ Netapp (cDOT) Snapmirror

■ HP 3PAR Remote Copy

■ Hitachi TrueCopy/HUR

	Table 2-5	Recovering applications using 3rd party replication technology

Tasks	More information
Plan your environment	Refer to the Release Notes for release information such as main features, known issues, and limitations. Ensure that the configuration details in your environment matches the requirements mentioned in the System resources and Hardware and software list. ■ Release Notes ■ Hardware and software list ■ System resources ■ List of ports

Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in both the data centers.
	
	■ Download the files required for deployment
	■ About deploying the virtual appliances
	■ Deploy the virtual appliances for Resiliency Manager and Infrastructure Management Server (IMS)
	  ■ Using VMware vSphere client
	  ■ Using Hyper-V Manager
	■ Configure the virtual appliances as Veritas Resiliency Platform components:
	  ■ About configuring the virtual appliances
	  ■ Prerequisites
	  ■ Configuring Resiliency Manager or IMS

Set up the resiliency domain	Set up the infrastructure and basic settings of the Veritas Resiliency Platform resiliency domain. These tasks are performed after you configure the Resiliency Manager and log in to the web console.
	
	■ Create the resiliency domain:
	  ■ Using getting started wizard
	■ Configure the settings for the resiliency domain:
	  ■ Add IMS
	  ■ Manage user authentication and permission
	  ■ Manage alerts, notifications, and other product settings

Table 2-5 Recovering applications using 3rd party replication technology *(continued)*

Tasks	More information
Add asset infrastructure	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console. ■ Add virtualization servers: ■ VMware virtualization servers ■ Hyper-V servers ■ Add host assets ■ Add enclosures ■ Map production network to rehearsal network (Optional) ■ Setup network mapping between data centers (Optional)
Create resiliency groups	After adding the assets to Resiliency Platform, you organize the related assets into a resiliency group that you can protect and manage as a single entity. You can create a resiliency group either for basic monitoring (start or stop virtual machines) or for recovery on local or remote data center. ■ Managing applications ■ Configure resiliency groups for basic monitoring ■ Prerequisites for configuring applications for remote recovery ■ Manage applications for remote recovery
Advanced features	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets. ■ Virtual business services ■ Resiliency plans ■ Evacuation plans
Perform remote recovery operations	Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Take over ■ Resync

Table 2-5   Recovering applications using 3rd party replication technology *(continued)*

Tasks	More information
Monitor assets 	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page. ■ Risks ■ Reports ■ Activities
Miscellaneous references 	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. ■ Using klish ■ Troubleshooting ■ Updating ■ References

Recovering InfoScale applications

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

Veritas Resiliency Platform lets you manage the InfoScale applications that are already configured in Veritas InfoScale Operations Manager. You cannot add or modify InfoScale applications through Resiliency Platform. They can be added or modified only by an administrator through Veritas InfoScale Operations Manager.

The InfoScale applications are automatically discovered in the Resiliency Platform when the Veritas InfoScale Operations Manager server is added to the resiliency domain. Veritas InfoScale Operations Manager users must download and install Veritas Resiliency Platform Enablement add-on to automatically discover the InfoScale applications. You can download the add-on from Veritas Services and Operations Readiness Tools (SORT).

A typical workflow of Veritas Resiliency Platform for InfoScale applications consists of a Veritas InfoScale Operation Manager server reporting to a Resiliency Manager. The InfoScale applications should be already configured in Veritas InfoScale

Operations Management server. You can group the InfoScale applications into resiliency groups or VBSs to recover, monitor, visualize, and generate reports about these applications in the Resiliency Platform.

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

Figure 2-2   A typical workflow for recovering managed InfoScale applications

Table 2-6   Recovering InfoScale applications

Tasks	More information
Plan your environment	Refer to the Release Notes for release information such as main features, known issues, and limitations. Ensure that the configuration details in your environment matches the requirements mentioned in the System resources and Hardware and software list. ■ Release Notes ■ Hardware and software list ■ System resources ■ List of ports ■ Support matrix for InfoScale applications

Table 2-6   Recovering InfoScale applications *(continued)*

Tasks	More information
Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances for Resiliency Manager and IMS in both the data centers.

	■ Download the files required for deployment
	■ About deploying the virtual appliances
	■ Deploy the virtual appliances for Resiliency Manager and Infrastructure Management Server (IMS)
	  ■ Using Hyper-V Manager
	  ■ Using VMware vSphere client

	Configure the virtual appliances as Veritas Resiliency Platform components:
	■ About configuring the virtual appliances ■ Prerequisites ■ Configuring Resiliency Manager or IMS
Set up the resiliency domain	Set up the infrastructure and basic settings of the Veritas Resiliency Platform resiliency domain. These tasks are performed after you configure the Resiliency Manager and log in to the web console.

	■ Create the resiliency domain:
	  ■ Using getting started wizard
	■ Configure the settings for the resiliency domain:
	  ■ Add InfoScale Operations Manager server
	  ■ Manage user authentication and permission
	  ■ Manage alerts, notifications, and other product settings

Create resiliency groups	After adding the assets to Resiliency Platform, you organize the related assets into a resiliency group that you can protect and manage as a single entity. You can create a resiliency group either for basic monitoring (start or stop virtual machines) or for recovery on local or remote data center.
	■ Configure resiliency groups for basic monitoring ■ Prerequisites for configuring InfoScale applications for remote recovery ■ Manage applications for remote recovery
Advanced features	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets.
	■ Virtual business services ■ Resiliency plans ■ Evacuation plans

| Table 2-6 | Recovering InfoScale applications *(continued)* |

Tasks	More information
Perform remote recovery operations	Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Take over ■ Resync
Monitor assets	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page. ■ Risks ■ Reports ■ Activities
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. ■ Using klish ■ Troubleshooting ■ Updating ■ References

R

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	A location that contains asset infrastructure to be managed by Veritas Resiliency Platform.
	For the disaster recovery use case, the resiliency domain must contain at least two data centers in different locations, a production data center and recovery data center. Each data center has a Resiliency Manager and one or more IMSs.
host	Physical servers, virtual machines, or Hyper-V servers that are added to the Infrastructure Management Server (IMS) as hosts.
	Adding the assets as hosts installs the host package that is used by the IMS for discovery and monitoring.
Infrastructure Management Server (IMS)	The Veritas Resiliency Platform component that discovers, monitors, and manages the asset infrastructure within a data center. The IMS transmits information about the asset infrastructure to the Resiliency Manager.
migrate	A planned activity involving graceful shutdown of virtual machines at the production data center and starting them at the recovery data center. In this process, replication ensures that consistent virtual machine data is made available at the recovery data center.
persona	A user role that has access to a predefined set of jobs (operations). Used to assign permissions to users and groups for Veritas Resiliency Platform web console operations.
product role	The function configured for a Veritas Resiliency Platform virtual appliance.

For example, a virtual appliance can be configured as a Resiliency Manager, Infrastructure Management Server (IMS) or both.

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