Veritas™ Resiliency Platform 3.2 User Guide

Veritas Resiliency Platform: User Guide

Last updated: 2018-05-30

Document version: Document version: 3.2 Rev 0

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

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

https://sort.veritas.com/documents

Documentation feedback

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

doc.feedback@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1

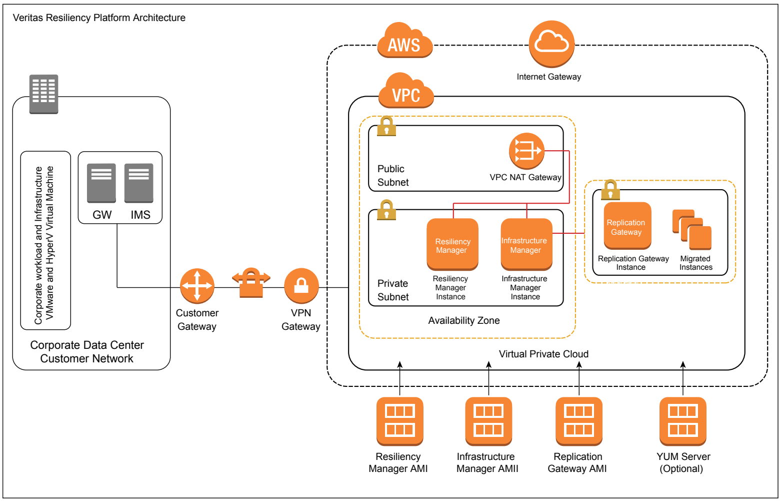
Recovery to cloud data center

This chapter includes the following topics:

Recovering VMware virtual machines to AWS

Using Veritas Resiliency Platform 3.2, 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 Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

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 Resiliency Platform components in AWS by using one of the following methods: ■ Through AWS marketplace using CloudFormation templates ■ Using OVA files ■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the premises data center: ■ Using VMware vSphere client ■ Deploy Data Gateway in AWS environment if you want to do one-time migration of your assets and choose to use Object Storage for replication: ■ Deploy Data Gateway ■ 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) ■ Add Data Gateway (only if you want to use Object Storage mode of replication) ■ Manage user authentication and permission ■ Manage alerts, notifications, and other product settings

Table 1-1 Recovering VMware 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 VMware servers ■ Prepare host for replication ■ Create Replication Gateway pair ■ Add and map network objects ■ Add network groups (Optional) ■ Create network pairs 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 ■ Take over ■ Resync

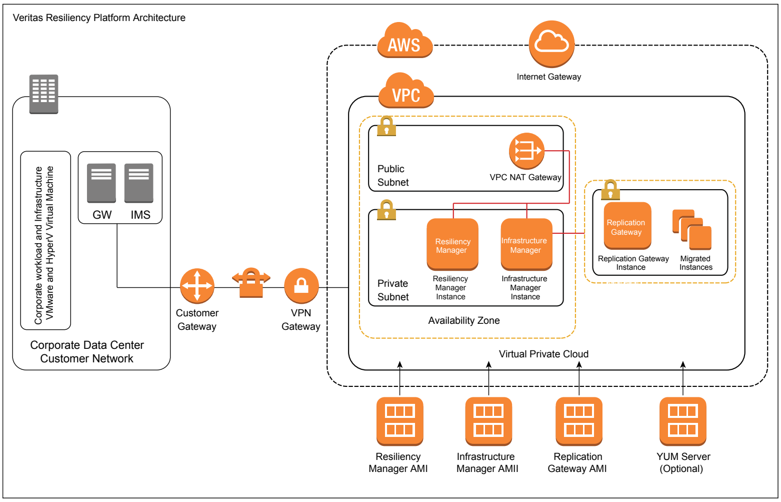
Table 1-1 Recovering VMware virtual machines to AWS *(continued)*

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. 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 3.2, 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 Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

Table 1-2 Recovering Hyper-V 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 Resiliency Platform components in AWS by using one of the following methods: ■ Through AWS marketplace using CloudFormation templates ■ Using OVA files ■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the premises data center: ■ Using Hyper-V Manager ■ Deploy Data Gateway in AWS environment if you want to do one-time migration of your assets and choose to use Object Storage for replication: ■ Deploy Data Gateway ■ 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) ■ Add Data Gateway (only if you want to use Object Storage mode of replication) ■ 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 ■ Add and map network objects ■ Add network groups (Optional) ■ Create network pairs 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 ■ Take over ■ Resync

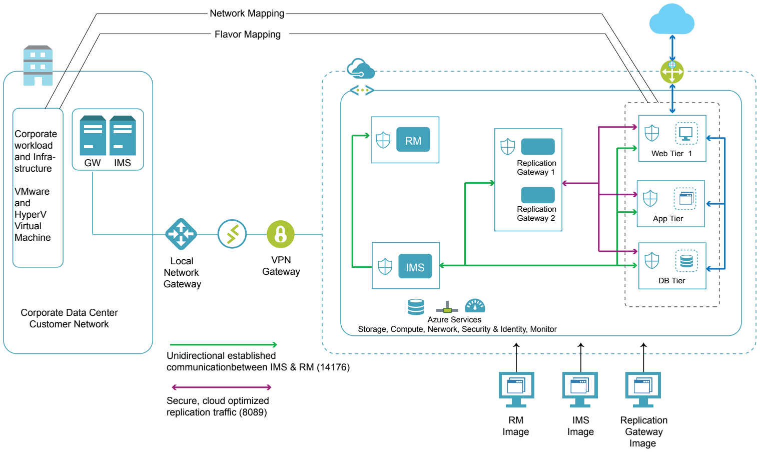
Table 1-2 Recovering Hyper-V virtual machines to AWS *(continued)*

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 3.2, 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


Network Mapping
Flavor Mapping
Corporate workload and Infra-structure
VMware and HyperV Virtual Machine
GW
IMS
Corporate Data Center
Customer Network
Local Network Gateway
VPN Gateway
RM
IMS
Replication Gateway 1
Replication Gateway 2
Web Tier 1
App Tier
DB Tier
Azure Services
Storage, Compute, Nerwork, Security & Identity, Monitor
Unidirectional established communicationbetween IMS & RM (14176)
Secure, cloud optimized replication traffic (8089)
RM Image
IMS Image
Replication Gateway Image

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 Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

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 ■ Add and map network objects ■ Create network pairs 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 ■ 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

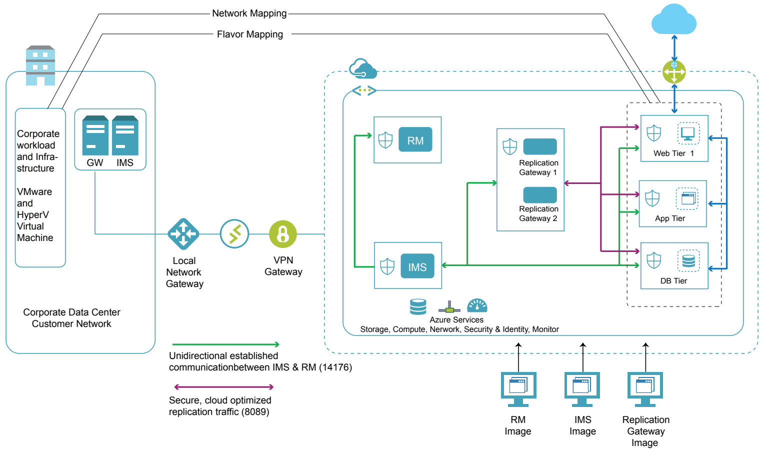
Table 1-3 Recovering VMware virtual machines to Azure *(continued)*

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 3.2, 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


Network Mapping
Flavor Mapping
Corporate workload and Infra-structure
VMware and HyperV Virtual Machine
GW
IMS
Corporate Data Center
Customer Network
Local Network Gateway
VPN Gateway
RM
IMS
Replication Gateway 1
Replication Gateway 2
Web Tier 1
App Tier
DB Tier
Azure Services
Storage, Compute, Network, Security & Identity, Monitor
Unidirectional established communicationbetween IMS & RM (14176)
Secure, cloud optimized replication traffic (8089)
RM Image
IMS Image
Replication Gateway Image

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 Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration
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 ■ Add and map network objects ■ Create network pairs 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 ■ Take over ■ Resync

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

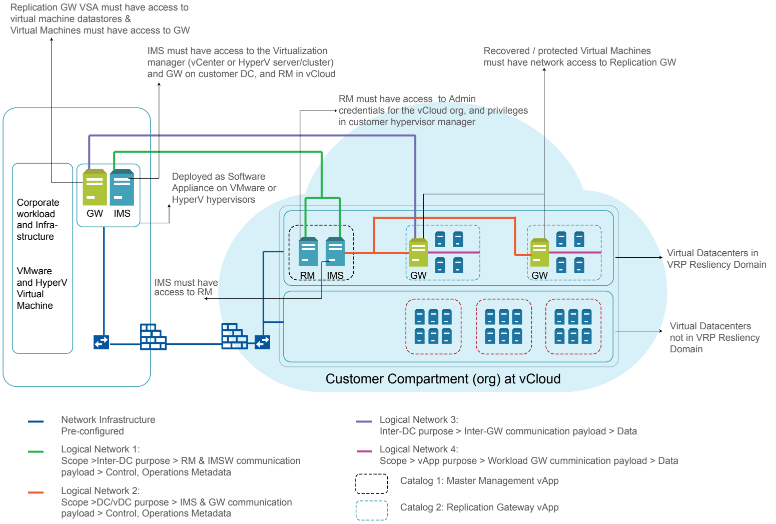
Tasks	More information
Monitor assets	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, 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 3.2, 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


Replication GW VSA must have access to virtual machine datastores & Virtual Machines must have access to GW
IMS must have access to the Virtualization manager (vCenter or HyperV server/cluster) and GW on customer DC, and RM in vCloud
Recovered / protected Virtual Machines must have network access to Replication GW
RM must have access to Admin credentials for the vCloud org, and privileges in customer hypervisor manager
Corporate workload and Infra-structure
VMware and HyperV Virtual Machine
GW
IMS
Deployed as Software Appliance on VMware or HyperV hypervisors
IMS must have access to RM
RM
IMS
GW
GW
Virtual Datacenters in VRP Resliency Domain
Virtual Datacenters not in VRP Resliency Domain
Customer Compartment (org) at vCloud
Network Infrastructure Pre-configured
Logical Network 1: Scope >Inter-DC purpose > RM & IMSW communication payload > Control, Operations Metadata
Logical Network 2: Scope >DC/vDC purpose > IMS & GW communication payload > Control, Operations Metadata
Logical Network 3: Inter-DC purpose > Inter-GW communication payload > Data
Logical Network 4: Scope > vApp purpose > Workload GW cumminication payload > Data
Catalog 1: Master Management vApp
Catalog 2: Replication Gateway vApp

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 Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

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 ■ Add and map network objects ■ Create network pairs 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 ■ Take over ■ Resync Note that, Rehearsal and Cleanup Rehearsal operations are not supported for recovery to vCloud Director.

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

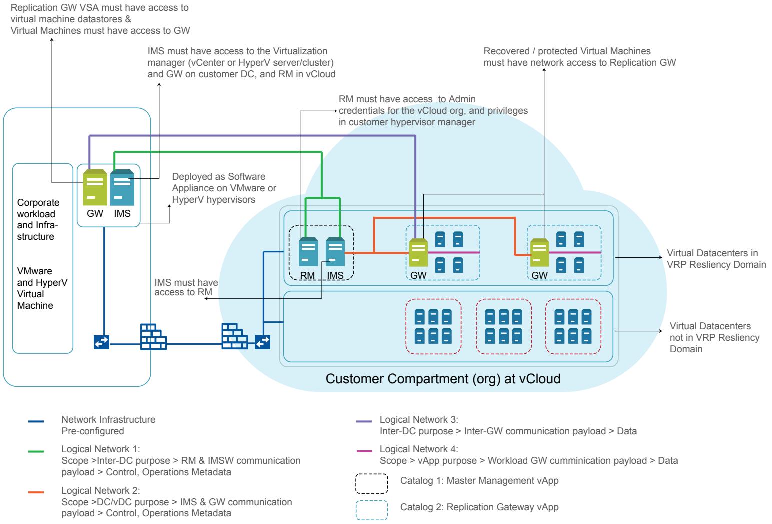
Tasks	More information
Monitor assets	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, 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 3.2, 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


Replication GW VSA must have access to virtual machine datastores & Virtual Machines must have access to GW
IMS must have access to the Virtualization manager (vCenter or HyperV server/cluster) and GW on customer DC, and RM in vCloud
Recovered / protected Virtual Machines must have network access to Replication GW
RM must have access to Admin credentials for the vCloud org, and privileges in customer hypervisor manager
Deployed as Software Appliance on VMware or HyperV hypervisors
Corporate workload and Infra-structure
VMware and HyperV Virtual Machine
GW
IMS
IMS must have access to RM
RM
IMS
GW
GW
Virtual Datacenters in VRP Resliency Domain
Virtual Datacenters not in VRP Resliency Domain
Customer Compartment (org) at vCloud
Network Infrastructure Pre-configured
Logical Network 1: Scope >Inter-DC purpose > RM & IMSW communication payload > Control, Operations Metadata
Logical Network 2: Scope >DC/vDC purpose > IMS & GW communication payload > Control, Operations Metadata
Logical Network 3: Inter-DC purpose > Inter-GW communication payload > Data
Logical Network 4: Scope > vApp purpose > Workload GW cumminication payload > Data
Catalog 1: Master Management vApp
Catalog 2: Replication Gateway vApp

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 Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ▪ Overview and Planning Guide ▪ Release Notes ▪ Checklist for deployment and disaster recovery configuration

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 ■ Create network pairs 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 ■ Take over ■ Resync Note that, Rehearsal and Cleanup Rehearsal operations are not supported for recovery to vCloud Director.
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)*

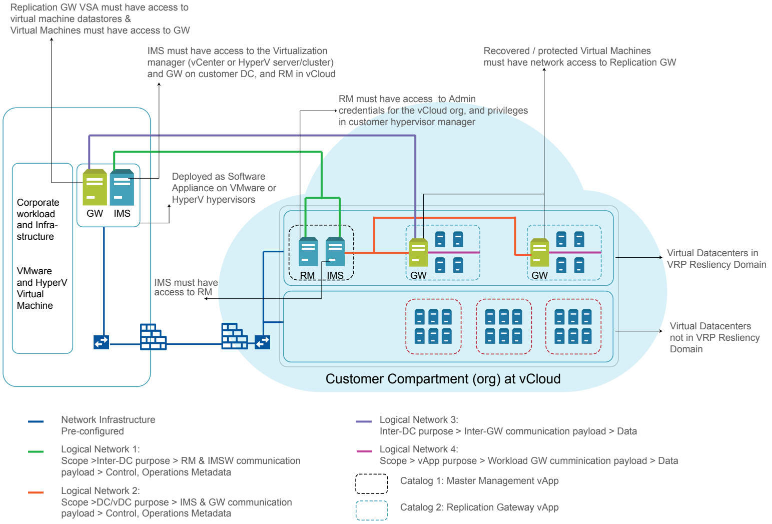
Tasks	More information
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. You can 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 3.2, 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


Replication GW VSA must have access to virtual machine datastores & Virtual Machines must have access to GW
IMS must have access to the Virtualization manager (vCenter or HyperV server/cluster) and GW on customer DC, and RM in vCloud
Recovered / protected Virtual Machines must have network access to Replication GW
RM must have access to Admin credentials for the vCloud org, and privileges in customer hypervisor manager
Corporate workload and Infra-structure
GW
IMS
Deployed as Software Appliance on VMware or HyperV hypervisors
VMware and HyperV Virtual Machine
IMS must have access to RM
RM
IMS
GW
GW
Virtual Datacenters in VRP Resliency Domain
Virtual Datacenters not in VRP Resliency Domain
Customer Compartment (org) at vCloud
Network Infrastructure Pre-configured
Logical Network 1: Scope >Inter-DC purpose > RM & IMSW communication payload > Control, Operations Metadata
Logical Network 2: Scope >DC/vDC purpose > IMS & GW communication payload > Control, Operations Metadata
Logical Network 3: Inter-DC purpose > Inter-GW communication payload > Data
Logical Network 4: Scope > vApp purpose > Workload GW cumminication payload > Data
Catalog 1: Master Management vApp
Catalog 2: Replication Gateway vApp

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 Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

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 ■ Create network pairs 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 ■ Take over ■ Resync Note that, Rehearsal and Cleanup Rehearsal operations are not supported for recovery to vCloud Director.
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)*

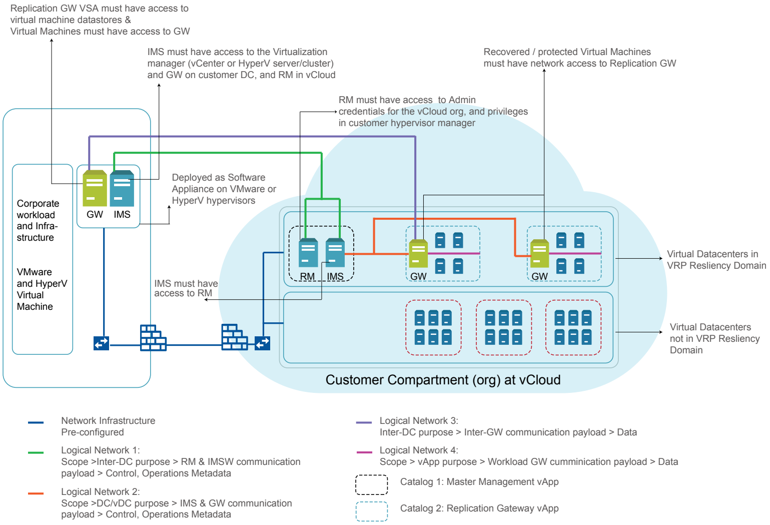
Tasks	More information
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. ■ Using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

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

Using Veritas Resiliency Platform 3.2, 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


Replication GW VSA must have access to virtual machine datastores & Virtual Machines must have access to GW
IMS must have access to the Virtualization manager (vCenter or HyperV server/cluster) and GW on customer DC, and RM in vCloud
Recovered / protected Virtual Machines must have network access to Replication GW
RM must have access to Admin credentials for the vCloud org, and privileges in customer hypervisor manager
Corporate workload and Infra-structure
VMware and HyperV Virtual Machine
GW
IMS
Deployed as Software Appliance on VMware or HyperV hypervisors
IMS must have access to RM
RM
IMS
GW
GW
Virtual Datacenters in VRP Resliency Domain
Virtual Datacenters not in VRP Resliency Domain
Customer Compartment (org) at vCloud
Network Infrastructure Pre-configured
Logical Network 1: Scope >Inter-DC purpose > RM & IMSW communication payload > Control, Operations Metadata
Logical Network 2: Scope >DC/vDC purpose > IMS & GW communication payload > Control, Operations Metadata
Logical Network 3: Inter-DC purpose > Inter-GW communication payload > Data
Logical Network 4: Scope > vApp purpose > Workload GW cumminication payload > Data
Catalog 1: Master Management vApp
Catalog 2: Replication Gateway vApp

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 Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

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 ■ Create network pairs 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 ■ Take over ■ Resync Note that, Rehearsal and Cleanup Rehearsal operations are not supported for recovery to vCloud Director.
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)*

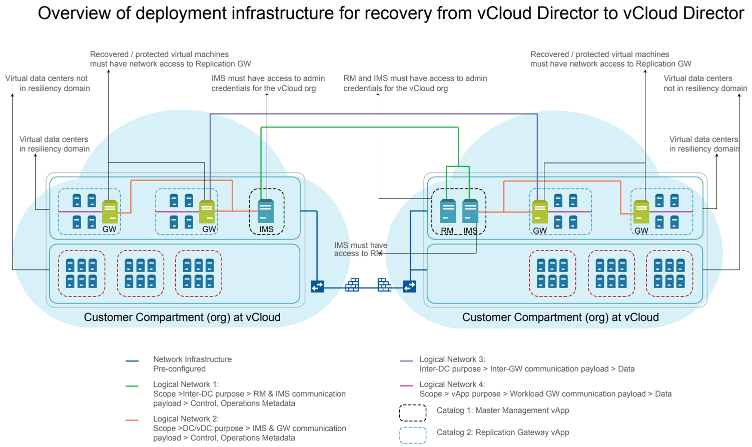
Tasks	More information
Miscellaneous references	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. You can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

Recovering virtual machines from vCloud Director to vCloud Director

Using Veritas Resiliency Platform , you can configure and protect your virtual machines for recovery from vCloud Director 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 1-9 Overview of deployment infrastructure for recovery from vCloud Director to vCloud Director


Overview of deployment infrastructure for recovery from vCloud Director to vCloud Director
Recovered / protected virtual machines must have network access to Replication GW
Virtual data centers not in resiliency domain
IMS must have access to admin credentials for the vCloud org
RM and IMS must have access to admin credentials for the vCloud org
Recovered / protected virtual machines must have network access to Replication GW
Virtual data centers not in resiliency domain
Virtual data centers in resiliency domain
Virtual data centers in resiliency domain
GW
GW
IMS
RM
IMS
GW
GW
IMS must have access to RM
Customer Compartment (org) at vCloud
Customer Compartment (org) at vCloud
Network Infrastructure Pre-configured
Logical Network 1: Scope >Inter-DC purpose > RM & IMS communication payload > Control, Operations Metadata
Logical Network 2: Scope >DC/vDC purpose > IMS & GW communication payload > Control, Operations Metadata
Logical Network 3: Inter-DC purpose > Inter-GW communication payload > Data
Logical Network 4: Scope > vApp purpose > Workload GW communication payload > Data
Catalog 1: Master Management vApp
Catalog 2: Replication Gateway vApp

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

Table 1-9 Recovering virtual machines from vCloud Director to vCloud Director

Tasks	More information
Plan your environment	Refer to the Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration
Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances on source as well as on the target cloud data center. ■ Download the files required for deployment ■ Deploy the virtual appliances for Infrastructure Management Server (IMS) and Replication Gateway in vCloud Director on both the cloud data centers. Resiliency Manager should be deployed either on source or on target data center. If you have multiple virtual data centers, deploy Resiliency Manager , IMS and Replication Gateway in one virtual data center and only IMS and Replication Gateway in rest of the virtual data centers: ■ About deploying the virtual appliances ■ Deploy using vCloud Director ■ Configure the virtual appliances as Veritas Resiliency Platform components: ■ About configuring the virtual appliances ■ Prerequisites ■ Configuring Resiliency Manager or IMS ■ Configuring Replication Gateways

Table 1-9 Recovering virtual machines from vCloud Director to vCloud Director *(continued)*

Tasks	More information
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 ■ Create network pairs 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 recovery from vCloud Director to vCloud Director ■ 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

Table 1-9 Recovering virtual machines from vCloud Director to vCloud Director *(continued)*

Tasks	More information
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 ■ Take over ■ Resync Note that, Rehearsal and Cleanup Rehearsal operations are not supported for recovery from vCloud Director to vCloud Director.
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 OpenStack

Using Veritas Resiliency Platform 3.2, you can configure and protect your VMware virtual machines for recovery to OpenStack using Resiliency Platform Data Mover. You have the option to configure your OpenStack based cloud as a cloud data center, or as a private cloud instance within your on-premises data center.

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

Table 1-10 Recovering VMware virtual machines to OpenStack

Tasks	More information
Plan your environment	Refer to the Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration
Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in OpenStack cloud data center as well as in the on-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 OpenStack cloud data center using any of the following methods: ■ Using OpenStack dashboard ■ Using volumes ■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the on-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

Table 1-10 Recovering VMware virtual machines to OpenStack *(continued)*

Tasks	More information
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 - - For adding public cloud data center Add cloud data center (if not done during getting started wizard) - For adding private cloud instances Add OpenStack private cloud instance - 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 - Add and map network objects - Create network pairs 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 OpenStack - Configure resiliency groups for recovery to OpenStack
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 1-10 Recovering VMware virtual machines to OpenStack *(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 Note that Resync, Takeover operation, and migrating back from target to source data center is not supported.
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. You can also use klish to update Resiliency Platform components. ■ Using klish ■ Troubleshooting ■ Updating ■ References

Recovering Hyper-V virtual machines to OpenStack

Using Veritas Resiliency Platform 3.2, you can configure and protect your Hyper-V virtual machines for recovery to OpenStack using Resiliency Platform Data Mover. You have the option to configure your OpenStack based cloud as a cloud data center, or as a private cloud instance within your on-premises data center.

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

Table 1-11 Recovering Hyper-V virtual machines to OpenStack

Tasks	More information
Plan your environment	Refer to the Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration
Deploy and configure the virtual appliances	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in the OpenStack cloud data center as well as in the on-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 OpenStack cloud data center using any of the following methods: ■ Using OpenStack dashboard ■ Using volumes ■ 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

Table 1-11 Recovering Hyper-V virtual machines to OpenStack *(continued)*

Tasks	More information
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 ■ ■ For adding public cloud data center Add cloud data center (if not done during getting started wizard) ■ For adding private cloud instances Add OpenStack private cloud instance ■ 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 ■ Add and map network objects ■ Create network pairs 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 OpenStack ■ Configure resiliency groups for recovery to OpenStack
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

Table 1-11 Recovering Hyper-V virtual machines to OpenStack *(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 Note that Resync, Takeover operation, and migrating back from target to source data center is not supported.
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

Chapter 2

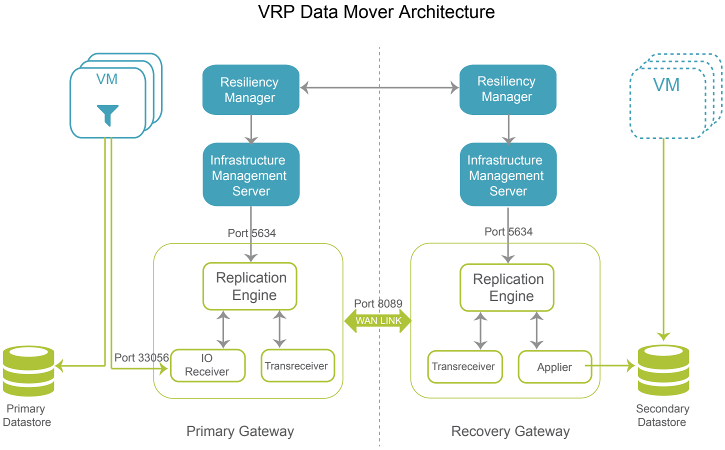
Recovery to on-premises data center

This chapter includes the following topics:

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

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

Figure 2-1 Overview of deployment Infrastructure for recovery using Resiliency Platform Data Mover



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 Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

Table 2-1 Recovering VMware virtual machines using VMware VAIO *(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, 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 ■ Add and map network objects (Optional) ■ Create network pairs 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 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

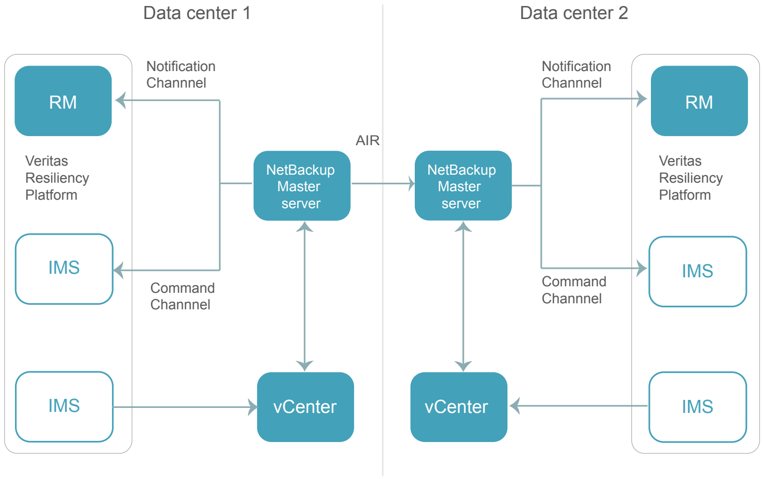
Table 2-1 Recovering VMware virtual machines using VMware VAIO *(continued)*

Tasks	More information
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
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. 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 3.2, you can restore VMware virtual machine from NetBackup generated backup images to the recovery data center. For more information on NetBackup and NetBackup Appliances, see About NetBackup and NetBackup Appliances.

Figure 2-2 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 Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration
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 servers ■ Add NetBackup master server ■ Add IMS to NetBackup master server as an additional server ■ Add and map network objects ■ Create network pairs between data centers

Table 2-2 Recovering virtual machines using NetBackup images *(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 ■ 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
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 2-2 Recovering virtual machines using NetBackup images *(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 VMware virtual machines using third-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 third-party replication technology

Tasks	More information
Plan your environment	Refer to the Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ▪ Overview and Planning Guide ▪ Release Notes ▪ Checklist for deployment and disaster recovery configuration
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 ▪ Add and map network objects (Optional) ▪ Create network pairs between data centers (Optional)

Table 2-3 Recovering VMware virtual machines using third-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 ■ 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

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

Tasks	More information
Plan your environment	Refer to the Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration
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 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
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 ■ Add and map network objects (Optional) ■ Create network pairs between data centers (Optional)

Table 2-4 Recovering Hyper-V virtual machines using third-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 - 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

Table 2-4 Recovering Hyper-V virtual machines using third-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 Applications using third-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 third-party replication technology

Tasks	More information
Plan your environment	Refer to the Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ▪ Overview and Planning Guide ▪ Release Notes ▪ Checklist for deployment and disaster recovery configuration

Table 2-5 Recovering applications using third-party replication technology *(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 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
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 ■ Add and map network objects (Optional) ■ Create network pairs between data centers (Optional)

Table 2-5 Recovering applications using third-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. - 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
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 2-5 Recovering applications using third-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 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 2-3 A typical workflow for recovering managed InfoScale applications

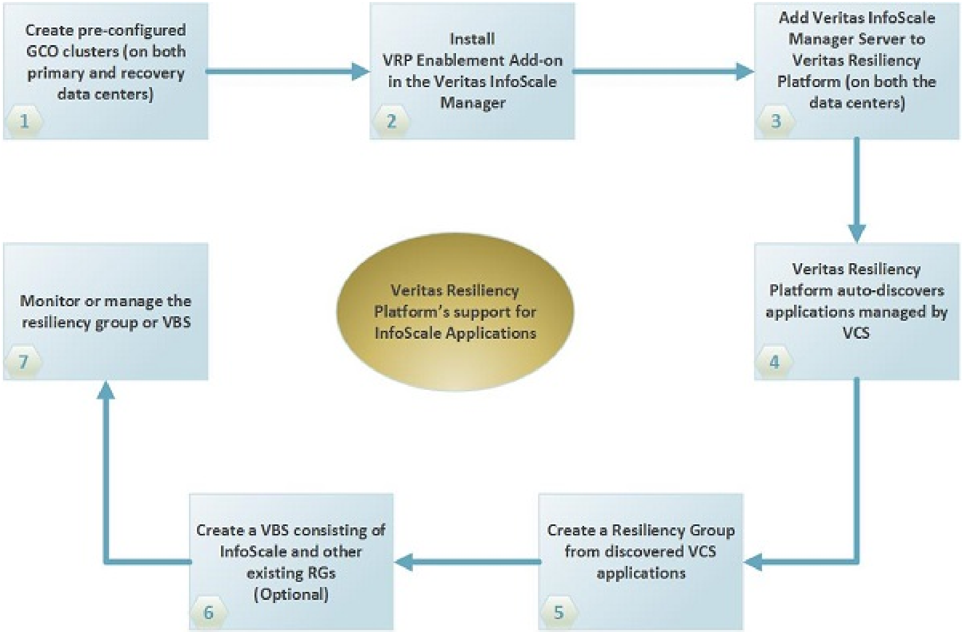

Create pre-configured GCO clusters (on both primary and recovery data centers)
1
Install VRP Enablement Add-on in the Veritas InfoScale Manager
2
Add Veritas InfoScale Manager Server to Veritas Resiliency Platform (on both the data centers)
3
Veritas Resiliency Platform auto-discovers applications managed by VCS
4
Create a Resiliency Group from discovered VCS applications
5
Create a VBS consisting of InfoScale and other existing RGs (Optional)
6
Monitor or manage the resiliency group or VBS
7
Veritas Resiliency Platform's support for InfoScale Applications

Table 2-6 Recovering InfoScale applications

Tasks	More information
Plan your environment	Refer to the Overview and Planning Guide to know about the product, its components, features, and capabilities. 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 checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

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 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 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

Index