Veritas™ Resiliency Platform 4.0 User Guide

VERITAS™

Veritas™ Resiliency Platform User Guide

Last updated: 2021-06-07

Document version: Document version: 4.0 Rev 0

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

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

https://sort.veritas.com/documents

Documentation feedback

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

vrpdocs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1

Recovery to cloud data center

This chapter includes the following topics:

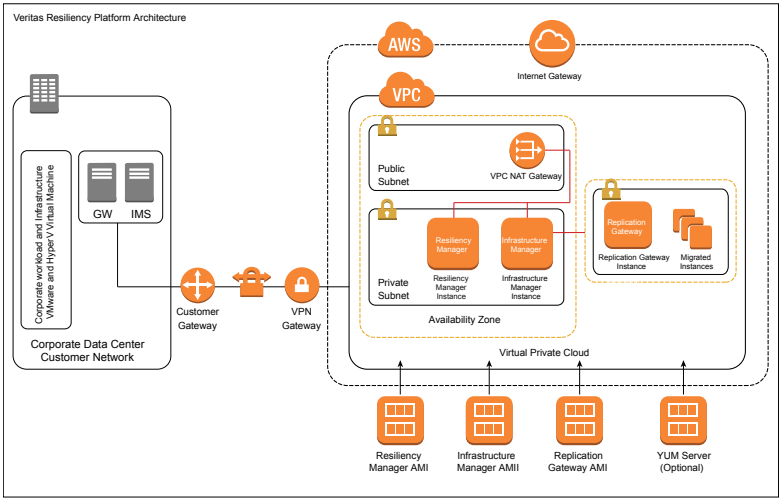
- Recovering physical machines to Orange Recovery Engine using Resiliency Platform Data Mover
- Recovering physical machines to Azure using Resiliency Platform Data Mover

Recovering VMware virtual machines to AWS

Using Veritas Resiliency Platform 4.0, you can configure and protect your VMware virtual machines for recovery to AWS using the Resiliency Platform Data Mover.

Instance MetaData Service v2 (IMDSv2) is introduced by AWS as security enhancement over IMDSv1. From version 4.0 of Resiliency Platform, while configuring resiliency group for disaster recovery, the wizard has an option to specify metadata access using **Enforce IMDSv2** option per virtual machine. If this option is true, the virtual machine when migrated to AWS, should use only IMDSv2 mechanism.

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 are compatible with 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 AWS cloud data center as well as in the premises data center. Refer to the following topics: Download the files required for deployment About deploying the virtual appliances Deploy the Resiliency Platform components in AWS 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 Deploy Data Gateway in AWS environment if you want to use Object Storage for replication Configure the virtual appliances as Veritas Resiliency Platform components

Table 1-1 Recovering VMware virtual machines to AWS *(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. Refer to the following topics: Getting started with a new Resiliency Platform configuration Configure the settings for the resiliency domain: Adding an IMS Adding a Replication Gateway Adding AWS cloud data center (if not done during getting started wizard) Adding a Data Gateway (only if you want to use Object Storage mode of replication) Managing user authentication and permissions Adding, modifying, or deleting email 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
Infrastructure Pairing	For recovering assets to AWS you have to do following infrastructure pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ Create Network group of Cloud Subnets, refer Add network groups (Optional). ■ For DNS customization, refer Add DNS servers. ■ Create network mappings, refer Network pairs for recovering virtual machines to AWS.

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

Tasks	More information
Create resiliency groups 	After adding the assets to Resiliency Platform, you organize the related assets into a resiliency group that you can protect and manage as a single entity. You can create a resiliency group either for basic monitoring (start or stop virtual machines) or for remote recovery. ■ Configuring a resiliency group 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. ■ Managing virtual business services ■ Managing resiliency plans ■ About evacuation plan
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, recover, or resync operations on the resiliency groups. ■ Performing the rehearsal operation for virtual machines ■ Performing cleanup rehearsal for virtual machines ■ Migrating a resiliency group ■ Recovering resiliency group of virtual machines ■ Performing the resync operation for 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. ■ About risks ■ About reports ■ Managing activities

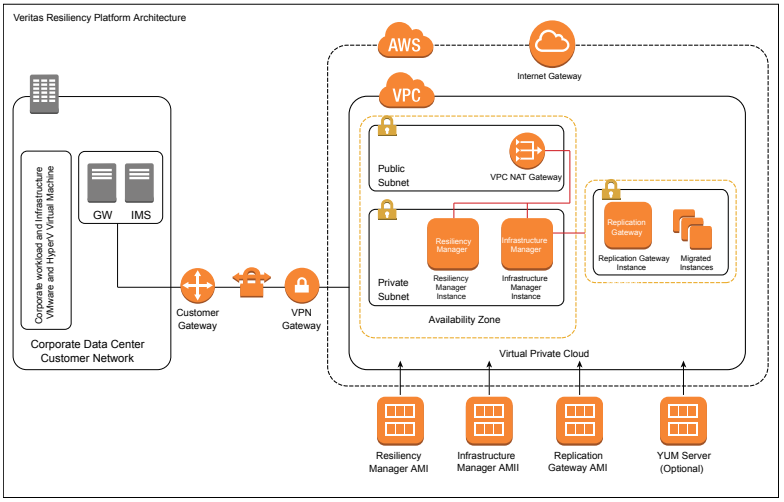
Table 1-1 Recovering VMware virtual machines to AWS *(continued)*

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

Recovering Hyper-V virtual machines to AWS

Using Veritas Resiliency Platform 4.0, you can configure and protect your VMware and Hyper-V virtual machines for recovery to AWS using the Resiliency Platform Data Mover.

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



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

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

Tasks	More information
Plan your environment 	Refer to the 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 are compatible with 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 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 use Object Storage for replication:
	  ■ Deploy Data Gateway
	■ Configure the virtual appliances as Veritas Resiliency Platform components:
	  ■ About configuring the virtual appliances
	  ■ Configuring Resiliency Manager or IMS
	  ■ Configuring Replication Gateways

Table 1-2 Recovering Hyper-V virtual machines to AWS *(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) ■ 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
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
Infrastructure Pairing	For recovering assets to AWS you have to do following infrastructure pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ Create Network group of Cloud Subnets, refer Add network groups (Optional). ■ For DNS customization, refer Add DNS servers. ■ Create network mappings, refer Network pairs for recovering virtual machines to AWS.
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 ■ Configure resiliency groups for recovery to AWS

Table 1-2 Recovering Hyper-V virtual machines to AWS *(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, recover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Recover ■ 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

Recovering virtual machines from VMware to AWS using NetBackup Image Sharing

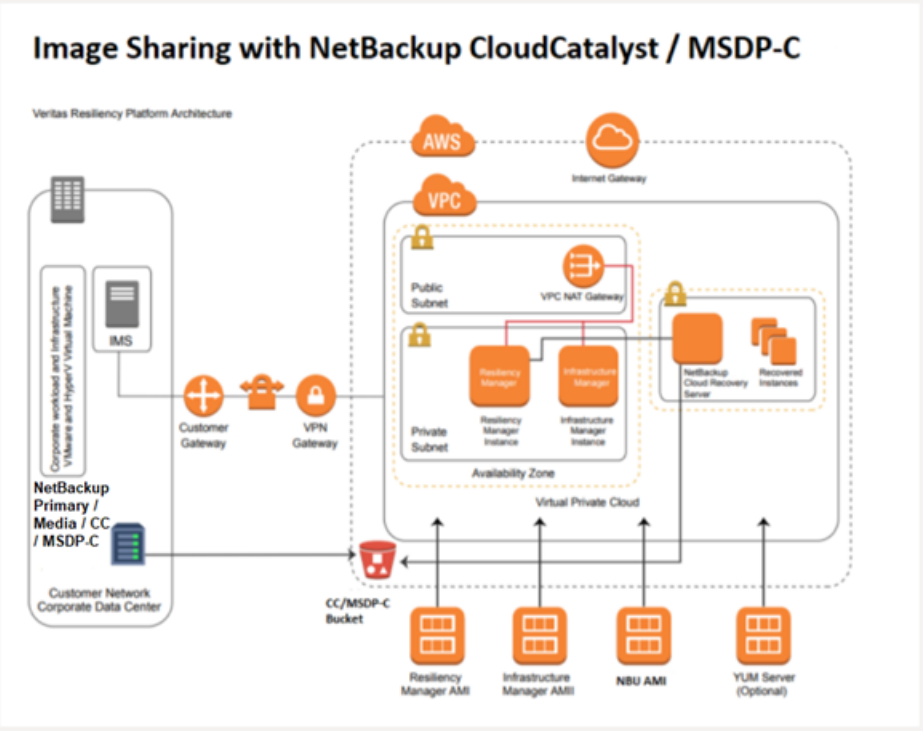
Using the Resiliency Platform, you can recover VMware virtual machine from NetBackup generated backup images that are stored into AWS S3 buckets to the AWS cloud target data center.

In figure the on-premises data center is the source data center and the target data center is an AWS cloud region. The Infrastructure Management Server (IMS) in the on-premises data center discovers the vCenter server and the backup configuration from the NetBackup primary server. NetBackup with the Image Sharing feature, which is available from NetBackup version 8.2 onwards, backs up the virtual machine images along with the image metadata from the on-premise data center into the designated S3 bucket.

For backing up the data in AWS S3 bucket, either NetBackup CloudCatalyst or MSDP-C configuration can be used.

The recovery using these backup images is achieved using a NetBackup Cloud Recovery Server (CRS) virtual appliance that is deployed in the cloud data center. The image metadata stored in the S3 bucket allows the NetBackup CRS to read the image information and create an Amazon Machine Image (AMI). This AMI is then used to provision cloud instances in the cloud data center during the recover operation.

Figure 1-3 Image Sharing with NetBackup CloudCatalyst / MSDP-C



The following table provides the summary of deployment, configuration, and recovery of virtual machines to cloud using NetBackup generated backup images that are stored in S3 bucket using the Image Sharing feature.

Table 1-3 Recovering virtual machines using NetBackup images

Tasks	More information
Plan your environment	Refer to the *Veritas Resiliency Platform Overview and Planning Guide* to know about the product, its components, features, and capabilities. Refer to the *Veritas Resiliency Platform Release Notes* for release information such as main features, known issues, and limitations. Overview and Planning Guide Release Notes Ensure that the configuration details in your environment match the requirements mentioned in the checklist. Checklist for recovery of VMware virtual machines to AWS cloud using NetBackup

Table 1-3 Recovering virtual machines using NetBackup images *(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 Downloading the Veritas Resiliency Platform virtual appliances ■ About deploying the virtual appliances About deploying the Resiliency Platform virtual appliances ■ Deploy the Resiliency Platform components in AWS by using one of the following methods: ■ Deploying the virtual appliances in AWS through AWS Marketplace ■ Deploying the virtual appliances in AWS using OVA files ■ Deploy the virtual appliances for one or more IMS in the premises data center: ■ Deploying the virtual appliance through VMware vSphere Client ■ Configure the virtual appliances as Veritas Resiliency Platform components: ■ About configuring the Resiliency Platform components ■ Prerequisites for configuring Resiliency Platform components ■ Deploy the Cloud Recovery Server (CRS) Deploy CRS
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. ■ Getting started with a new Resiliency Platform configuration ■ Configure the settings for the resiliency domain: ■ Adding an IMS ■ Adding AWS cloud data center ■ Managing user authentication and permissions ■ For secure communication, refer Managing security
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. ■ Adding VMware virtualization servers ■ Adding NetBackup primary server ■ Adding NetBackup Cloud Recovery Server (CRS)

Table 1-3 Recovering virtual machines using NetBackup images *(continued)*

Tasks	More information
Infrastructure Pairing	For recovering assets to VMware you have to do following Infrastructure Pairing: ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ Create Network group of cloud subnets. Adding a network group ■ Customize DNS Configuring DNS server settings for a data center ■ Create network mappings. Network pairs for recovering virtual machines to AWS
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. ■ Configuring a resiliency group for basic monitoring ■ Managing VMware virtual machines for remote recovery to AWS cloud 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. ■ Managing virtual business services ■ Managing resiliency plans ■ About evacuation plan
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 recover (local or remote) operations on the resiliency groups. **Note:** The rehearsal operation is not supported from AWS to VMware. ■ Performing the rehearsal operation on virtual machines from VMware to AWS using NetBackup Image Sharing ■ Performing cleanup rehearsal for virtual machines ■ Recovering virtual machines to cloud (AWS) using NetBackup Image Sharing

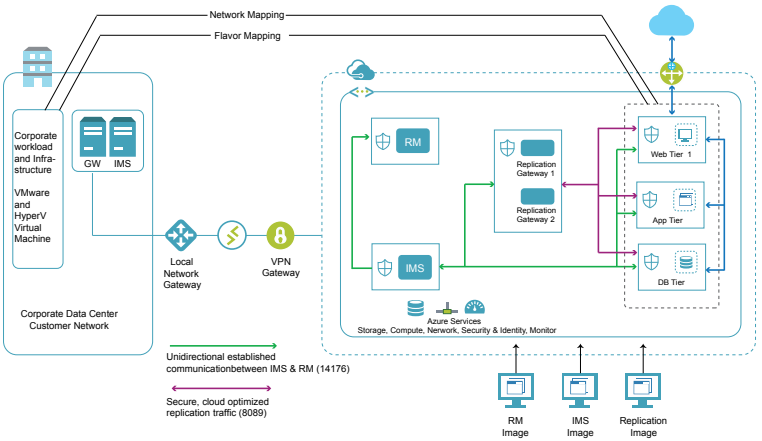
Table 1-3 Recovering virtual machines using NetBackup images *(continued)*

Tasks	More information
Monitor assets 	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page. ■ About risks ■ About reports ■ Managing 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. ■ About klish ■ Troubleshoot ■ About applying updates to Resiliency Platform ■ References

Recovering VMware virtual machines to Azure

Using Veritas Resiliency Platform 4.0, you can configure and protect your VMware virtual machines for recovery to Azure using the Resiliency Platform Data Mover.

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



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

Table 1-4 Recovering 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 are compatible with the requirements mentioned in the checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

Table 1-4 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 any of the following options:
	■ 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
	  ■ 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

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

Tasks	More information
Infrastructure Pairing	For recovering assets to Azure you have to do following Infrastructure Pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ For DNS customization, refer Add DNS servers. ■ Create network mappings, refer Network pairs for recovering virtual machines to Azure.
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 ■ 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, recover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Recover ■ Resync

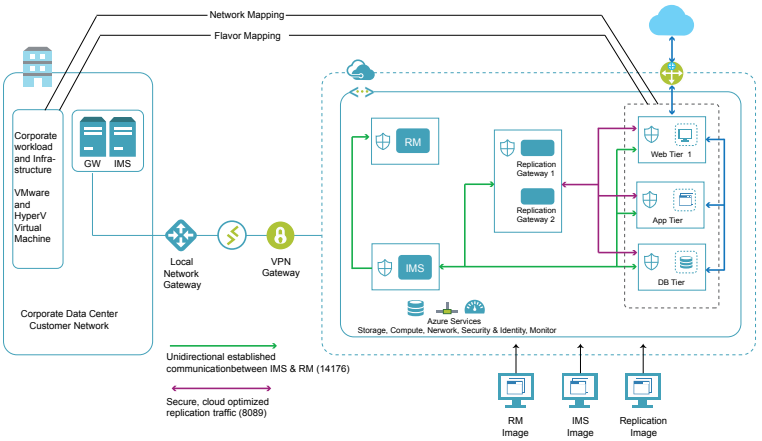
Table 1-4 Recovering VMware virtual machines to Azure *(continued)*

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 Hyper-V virtual machines to Azure

Using Veritas Resiliency Platform 4.0, you can configure and protect your Hyper-V virtual machines for recovery to Azure using the Resiliency Platform Data Mover.

Figure 1-5 Overview of deployment Infrastructure for recovery to Azure



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

Table 1-5 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 are compatible with the requirements mentioned in the checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

Table 1-5 Recovering Hyper-V 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 any of the following options:
	■ 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
	  ■ 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

Table 1-5 Recovering Hyper-V virtual machines to Azure *(continued)*

Tasks	More information
Infrastructure Pairing	For recovering assets to Azure you have to do following Infrastructure Pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ For DNS customization, refer Add DNS servers. ■ Create network mappings, refer Network pairs for recovering virtual machines to Azure.
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 ■ 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, recover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Recover ■ Resync

Table 1-5 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 virtual machines from Azure / Azure Stack to Azure / Azure Stack

Using Veritas Resiliency Platform 4.0, you can configure and protect your virtual machines for recovery from Azure to Azure using the Resiliency Platform Data Mover which includes combination of :

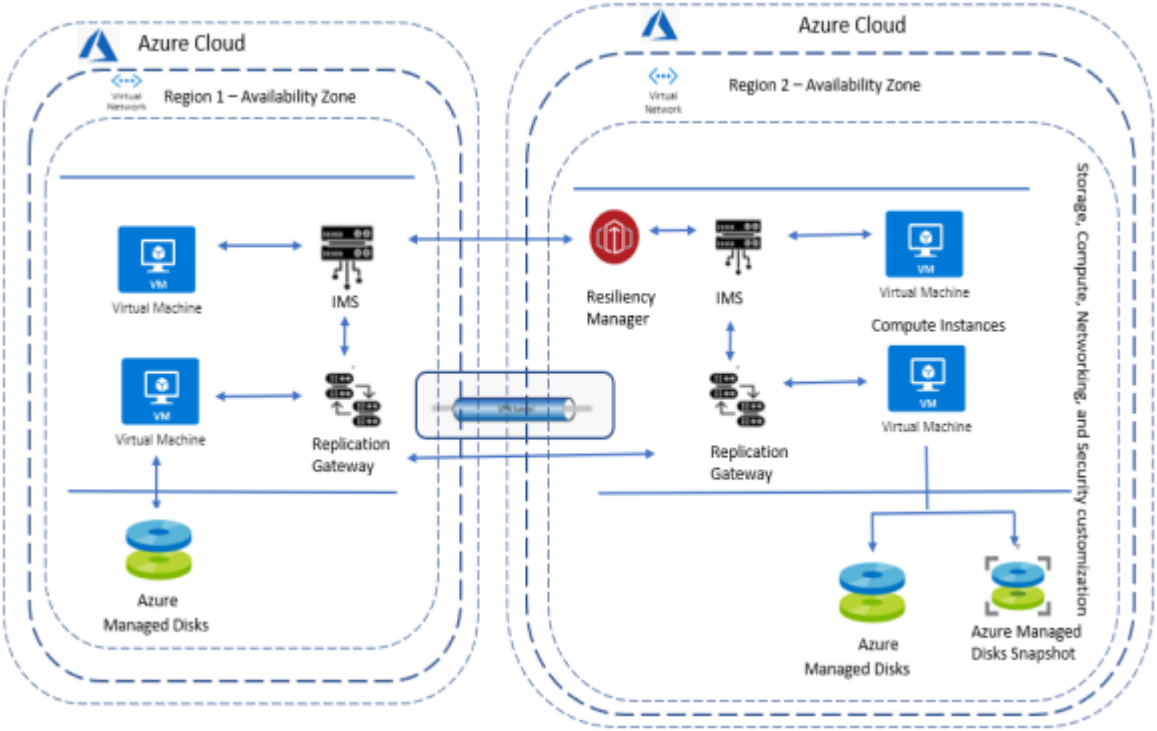
- Azure Stack to Azure Stack
- Azure Stack to Azure region
- Azure region to Azure region
- Azure region to Azure Stack

You can use the same or different Azure cloud subscriptions for using the Azure resources. Following are the features supported for this use case:

1. NRT discovery support is enabled for the virtual machines which are present at the target data center. Using NRT, the real-time updates related to network and virtual machines are discovered.
2. You can now edit the migrated virtual machine, add/ remove the virtual machine from a resiliency group on the target data center.

3. Rehearsal operation is enabled when target data center is Azure and vice versa.
4. Network customization feature is added where you can enable or disable IP customization on both source and target data center.

Figure 1-6 Overview of deployment Infrastructure for recovery from Azure to Azure



The following table provides the summary for deployment, configuration, and recovery of virtual machines to a data center on Azure to Azure which includes (Azure Stack to Azure Stack, Azure Stack to Azure region, Azure region to Azure region and Azure region to Azure Stack).

Table 1-6 Recovering virtual machines from Azure 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 are compatible with 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 on source and target data centers.
	■ Download the files required for deployment
	■ Deploy the virtual appliances Infrastructure Management Server (IMS) and Replication Gateway on Azure cloud at both the data centers using any one of the following options. Resiliency Manager should be deployed either on source or on target data center.
	■ Configure the virtual appliances as Veritas Resiliency Platform components:
	  ■ About configuring the virtual appliances
	  ■ Prerequisites for configuring the virtual appliances
	  ■ 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 another cloud data center
	  ■ Manage user authentication and permission
	  ■ Manage alerts, notifications, and other product settings
	Using the Resiliency Platform console, you can add one or more Azure Stack private cloud instances to the non-cloud datacenter (premise) at source, or at target or both data centers. Azure Stack private cloud can be added to non-cloud datacenter only.
	■ Adding Azure Stack private cloud instance
	■ For secure communication, refer Managing security

Table 1-6 Recovering virtual machines from Azure 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. ■ Prepare host for replication
Infrastructure Pairing	For recovering assets to Azure you have to do following Infrastructure Pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ For DNS customization, refer Add DNS servers. ■ Create network mappings, refer Network pairs for recovering virtual machines to Azure.
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 ■ Configure resiliency groups for recovery from Azure cloud to Azure cloud
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. ■ Evacuation plans

Table 1-6 Recovering virtual machines from Azure to Azure *(continued)*

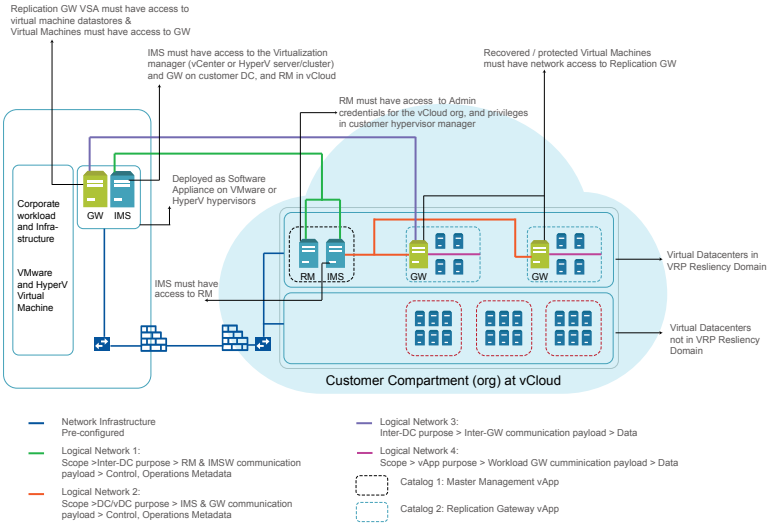
Tasks	More information
Perform remote recovery operations 	Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, recover, or resync operations on the resiliency groups. From version 4.0, Resiliency Platform supports rehearsal operation from Azure region to Azure region along with (Azure Stack to Azure Stack, Azure Stack to Azure region, and Azure region to Azure Stack) . ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Recover ■ 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

Recovering VMware virtual machines to vCloud Director

Using Veritas Resiliency Platform 4.0, you can configure and protect your VMware virtual machines for recovery to vCloud Director using the Resiliency Platform Data Mover.

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

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



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

Table 1-7 Recovering VMware virtual machines to vCloud Director

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 *(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
	  ■ 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

Table 1-7 Recovering VMware virtual machines to vCloud Director *(continued)*

Tasks	More information
Infrastructure Pairing	For recovering assets to vCloud Director you have to do following Infrastructure Pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ Create Network group of vLAN/Port Group, refer Add network groups (Optional). ■ For DNS customization, refer Add DNS servers. ■ Create network mappings, refer Network pairs for recovering virtual machines to vCloud Director.
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 ■ 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, recover, or resync operations on the resiliency groups. ■ Migrate ■ Recover ■ Resync Note that, Rehearsal and Cleanup Rehearsal operations are not supported for recovery to vCloud Director.

Table 1-7 Recovering VMware virtual machines to vCloud Director *(continued)*

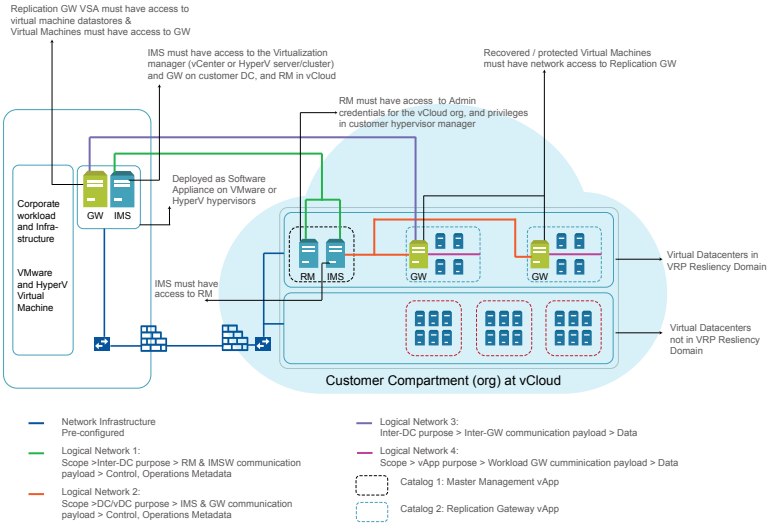
Tasks	More information
Monitor assets 	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, 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 4.0, you can configure and protect your Hyper-V virtual machines for recovery to vCloud Director using the Resiliency Platform Data Mover.

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

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



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

Table 1-8 Recovering Hyper-V virtual machines to vCloud Director

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 are compatible with 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 *(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
	  ■ 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

Table 1-8 Recovering Hyper-V virtual machines to vCloud Director *(continued)*

Tasks	More information
Infrastructure Pairing	For recovering assets to vCloud Director you have to do following Infrastructure Pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ Create Network group of vLAN/Port Group, refer Add network groups (Optional). ■ For DNS customization, refer Add DNS servers. ■ Create network mappings, refer Network pairs for recovering virtual machines to vCloud Director.
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 ■ 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, recover, or resync operations on the resiliency groups. ■ Migrate ■ Recover ■ Resync Note that, Rehearsal and Cleanup Rehearsal operations are not supported for recovery to vCloud Director.

Table 1-8 Recovering Hyper-V virtual machines to vCloud Director *(continued)*

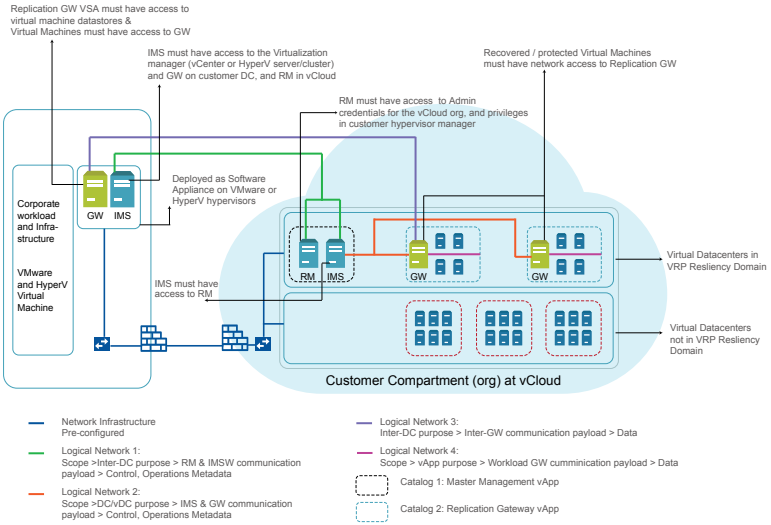
Tasks	More information
Monitor assets 	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, 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. 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 4.0, you can configure and protect your VMware virtual machines for recovery to vCloud Director using the Resiliency Platform Data Mover without adding the vCenter server.

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

Figure 1-9 Overview of deployment infrastructure for recovery to vCloud Director



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

Table 1-9 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 are compatible with the requirements mentioned in the checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

Table 1-9 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
	  ■ 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

Table 1-9 Recovering VMware virtual machines to vCloud Director without adding vCenter server *(continued)*

Tasks	More information
Infrastructure Pairing	For recovering assets to vCloud Director you have to do following Infrastructure Pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ For DNS customization, refer Add DNS servers. ■ Create network mappings, refer Network pairs for recovering virtual machines to vCloud Director.
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. ■ 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, recover, or resync operations on the resiliency groups. ■ Migrate ■ Recover ■ Resync Note that, Rehearsal and Cleanup Rehearsal operations are not supported for recovery to vCloud Director.

Table 1-9 Recovering VMware virtual machines to vCloud Director without adding vCenter server *(continued)*

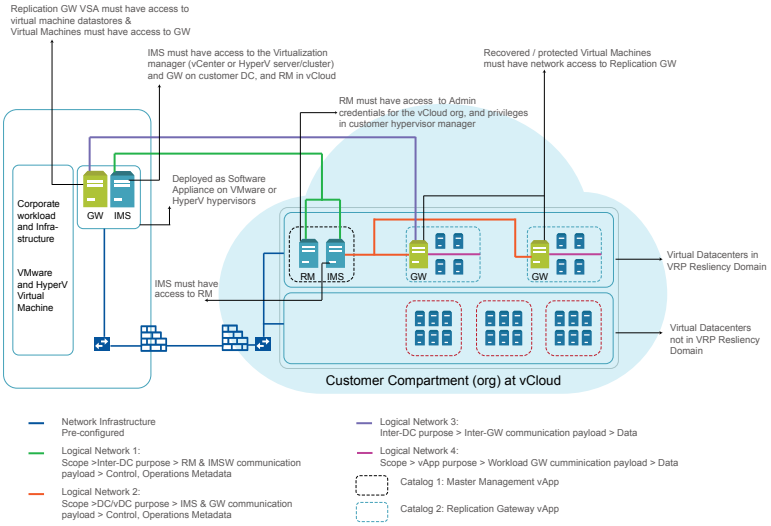
Tasks	More information
Monitor assets 	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, 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 without adding Hyper-V server

Using Veritas Resiliency Platform 4.0, you can configure and protect your Hyper-V virtual machines for recovery to vCloud Director using the Resiliency Platform Data Mover without adding Hyper-V server.

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

Figure 1-10 Overview of deployment infrastructure for recovery to vCloud Director



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

Table 1-10 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 are compatible with the requirements mentioned in the checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

Table 1-10 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
	  ■ 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

Table 1-10 Recovering Hyper-V virtual machines to vCloud Director without adding Hyper-V server *(continued)*

Tasks	More information
Infrastructure Pairing	For recovering assets to vCloud Director you have to do following Infrastructure Pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ For DNS customization, refer Add DNS servers. ■ Create network mappings, refer Network pairs for recovering virtual machines to vCloud Director.
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. ■ 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, recover, or resync operations on the resiliency groups. ■ Migrate ■ Recover ■ Resync Note that, Rehearsal and Cleanup Rehearsal operations are not supported for recovery to vCloud Director.

Table 1-10 Recovering Hyper-V virtual machines to vCloud Director without adding Hyper-V server *(continued)*

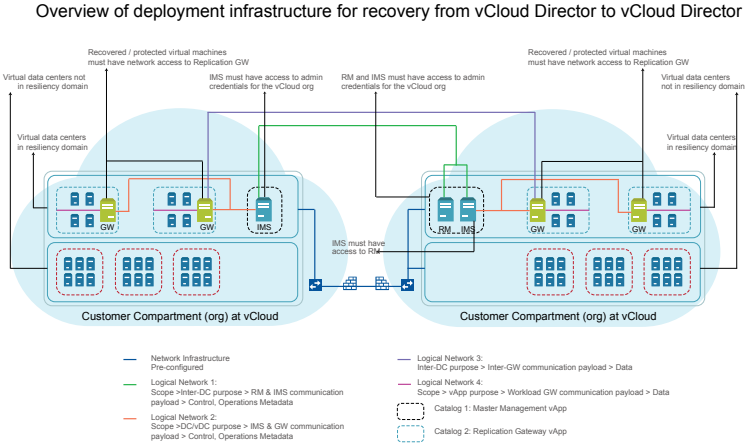
Tasks	More information
Monitor assets 	You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, 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 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 1-11 Overview of deployment infrastructure for recovery from vCloud Director to vCloud Director



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 1-11 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 are compatible with the requirements mentioned in the checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

Table 1-11 Recovering virtual machines from vCloud Director 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 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 ■ Using vCloud Director ■ Configure the virtual appliances as Veritas Resiliency Platform components: ■ About configuring the virtual appliances ■ 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 another cloud data center ■ 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

Table 1-11 Recovering virtual machines from vCloud Director to vCloud Director *(continued)*

Tasks	More information
Infrastructure Pairing	For recovering assets from vCloud Director to vCloud Director you have to do following Infrastructure Pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ For DNS customization, refer Add DNS servers. ■ Create network mappings, refer Network pairs for recovering from vCloud Director to vCloud Director.
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 ■ 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, recover, 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.

Table 1-11 Recovering virtual machines from vCloud Director 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 VMware virtual machines to Orange Recovery Engine

Using Veritas Resiliency Platform, you can recover VMware virtual machines to Orange Recovery Engine.

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

Table 1-12 Recovering VMware virtual machines to Orange Recovery Engine

Tasks	More information
Plan your environment 	Refer to the *Veritas Resiliency Platform Overview and Planning Guide* to know about the product, its components, features, and capabilities. Refer to the *Veritas Resiliency Platform Release Notes* for release information such as main features, known issues, and limitations. Overview and Planning Guide Release Notes Ensure that the configuration details in your environment are compatible with the requirements mentioned in the checklist. ■ 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 Orange Recovery Engine 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 Orange Recovery Engine data center:
	  ■ Using Orange Recovery Engine
	■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the premises data center:
	  ■
	■ Configure the virtual appliances as Veritas Resiliency Platform components:
	  ■
	  ■
	  ■

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 1-12 Recovering VMware virtual machines to Orange Recovery Engine *(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
Infrastructure Pairing	For recovering assets to Orange Recovery Engine you have to do following Infrastructure Pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, referAdd and map network objects ■ For DNS customization, refer Add DNS servers ■ For NIC teaming / bonding, refer Support for NIC teaming / bonding for physical machines ■ Create network mappings, referNetwork pairs for recovering virtual machines to Orange Recovery Engine
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 ■ Configuring resiliency groups for recovery to Orange Recovery Engine
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 1-12 Recovering VMware virtual machines to Orange Recovery Engine *(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, recover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup Rehearsal ■ Migrate ■ Recover ■ 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. ■ Risk ■ 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 physical machines to AWS using Resiliency Platform Data Mover

Using Veritas Resiliency Platform, you can recover physical machines to AWS using Resiliency Platform Data Mover.

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

Table 1-13 Recovering physical machines to AWS using Resiliency Platform Data Mover

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 are compatible with 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 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 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

Table 1-13 Recovering physical machines to AWS using Resiliency Platform Data Mover *(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) ■ 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
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
Infrastructure Pairing	For recovering assets to AWS you have to do following infrastructure pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ Create Network group of Cloud Subnets, refer Add network groups (Optional). ■ For DNS customization, refer Add DNS servers. ■ For NIC teaming / bonding, refer Support for NIC teaming / bonding for physical machines ■ For creating network mapping, refer Network pairs for recovering virtual machines to AWS

Table 1-13 Recovering physical machines to AWS using Resiliency Platform Data Mover *(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. ■ Managing physical machines for remote recovery (DR) using Resiliency Platform Data Mover
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, recover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Recover ■ 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 1-13 Recovering physical machines to AWS using Resiliency Platform Data Mover *(continued)*

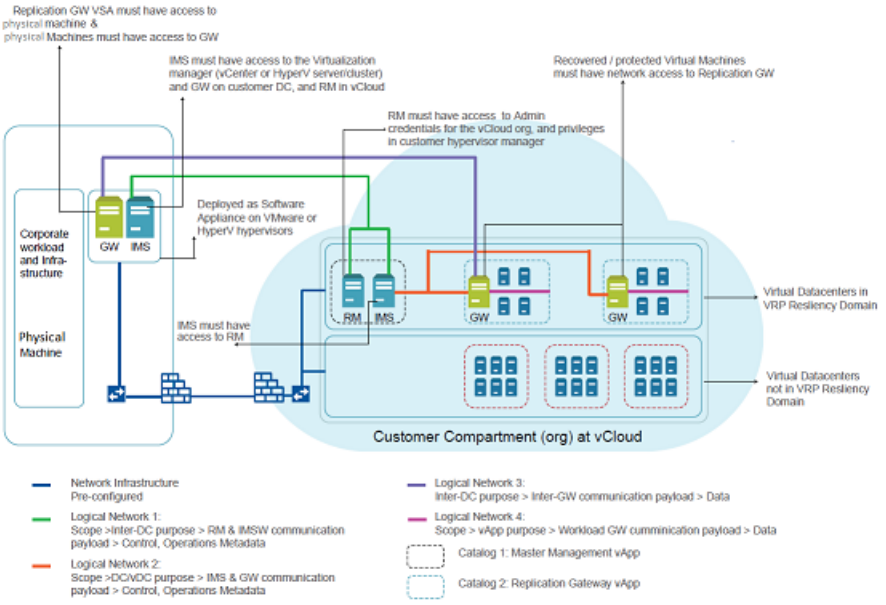
Tasks	More information
Miscellaneous references 	After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. You can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

Recovering physical machines to vCloud Director using Resiliency Platform Data Mover

Using Veritas Resiliency Platform, you can you can recover physical machines to vCloud Director using 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 1-12 Overview of deployment infrastructure for recovery to vCloud Director



The following table provides the summary for deployment, configuration, and recovery of physical machines to a data center on vCloud Director. End user or the service subscriber can perform these operations.

Table 1-14 Recovering machines to vCloud Director using Resiliency Platform Data Mover

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 is compatible with the requirements mentioned in the checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

Table 1-14 Recovering machines to vCloud Director using Resiliency Platform Data Mover *(continued)*

Tasks	More information

Deploy and configure the virtual appliances
 
	Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in the AWS cloud data center as well as in the premises data center.
	■ Download the files required for deployment
	■ About deploying the virtual appliances
	■ Deploy the virtual appliances 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
	  ■ 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

Table 1-14 Recovering machines to vCloud Director using Resiliency Platform Data Mover *(continued)*

Tasks	More information
Infrastructure Pairing	For recovering assets to vCloud Director you have to do following Infrastructure Pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ Create Network group of vLAN/Port Group, refer Add network groups (Optional). ■ For DNS customization, refer Add DNS servers. ■ For NIC teaming / bonding, refer Support for NIC teaming / bonding for physical machines ■ Create network mappings, refer Network pairs for recovering virtual machines to vCloud Director.
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. ■ Configure physical machines for recovery to on-premises data center
Advanced features 	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets. ■ Virtual business services ■ Resiliency plans ■ Evacuation plans
Perform remote recovery operations 	Once you have organized your assets into resiliency groups, you can perform migrate, recover, or resync operations on the resiliency groups. ■ Migrate ■ Recover ■ Resync

Table 1-14 Recovering machines to vCloud Director using Resiliency Platform Data Mover *(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 physical machines to Orange Recovery Engine using Resiliency Platform Data Mover

Using Veritas Resiliency Platform, you can recover physical machines to Orange Recovery Engine using Resiliency Platform Data Mover.

The following table provides the summary for deployment, configuration, and recovery of physical machines to Orange Recovery Engine using Resiliency Platform Data Mover.

Table 1-15 Recovering physical machines to Orange Recovery Engine using Resiliency Platform Data Mover

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 is compatible with 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 Orange Recovery Engine 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 Orange cloud data center using one of the following methods:
	  ■ Using Orange Recovery Engine
	■ 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 1-15 Recovering physical machines to Orange Recovery Engine using Resiliency Platform Data Mover *(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. ■ Prepare host for replication
Infrastructure Pairing	For recovering assets to VMware, do following Infrastructure Pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ For DNS customization, refer Add DNS servers. ■ For NIC teaming / bonding , refer Support for NIC teaming / bonding for physical machines ■ Create network mappings, refer Network pairs for recovering physical machines to Orange Recovery Engine.
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. ■ Managing physical machines for remote recovery (DR) using Resiliency Platform Data Mover
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 1-15 Recovering physical machines to Orange Recovery Engine using Resiliency Platform Data Mover *(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, recover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Recover ■ 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 physical machines to Azure using Resiliency Platform Data Mover

Using Veritas Resiliency Platform, you can recover physical machines to Azure using Resiliency Platform Data Mover.

The following table provides the summary for deployment, configuration, and recovery of physical machines to Azure using Resiliency Platform Data Mover.

Table 1-16 Recovering physical machines to Azure using Resiliency Platform Data Mover

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 are compatible with 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:
	  ■ Deploy using Azure PowerShell
	  ■ Through Azure Marketplace
	■ 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

Table 1-16 Recovering physical machines to Azure using Resiliency Platform Data Mover *(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 Using the Resiliency Platform console, you can add one or more Azure Stack private cloud instances to the non-cloud datacenter (premise) at source, or at target or both data centers. Azure Stack private cloud can be added to non-cloud datacenter only. Adding Azure Stack private cloud configuration
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
Infrastructure Pairing	For recovering assets to Azure you have to do following Infrastructure Pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ For DNS customization, refer Add DNS servers. ■ Create network mappings, refer Network pairs for recovering physical machines to Azure

Table 1-16 Recovering physical machines to Azure using Resiliency Platform Data Mover *(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. ■ Managing physical machines for remote recovery (DR) using Resiliency Platform Data Mover
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, recover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Recover ■ 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 1-16 Recovering physical machines to Azure using Resiliency Platform Data Mover *(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 product_name_short components. ■ Using klish ■ Troubleshooting ■ Updating ■ References

Chapter 2

Recovery to on-premises data center

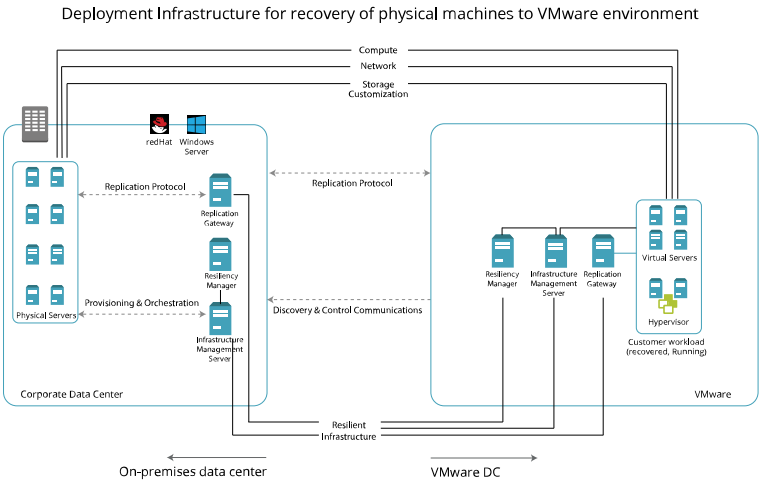
This chapter includes the following topics:

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

Using Veritas Resiliency Platform, you can recover physical machines to VMware virtual machines on an on-premises data center using Resiliency Platform Data Mover.

Note: SD card and USB disks on physical hosts with Veritas Resiliency Platform data mover are not supported.

Figure 2-1 Overview of deployment Infrastructure for recovery of physical machines to VMware virtual machines



The following table provides the summary for deployment, configuration, and recovery of physical machines to on-premises data center using Resiliency Platform Data Mover.

Table 2-1 Recovering physical machines to on-premises data center using Resiliency Platform Data Mover

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 are compatible with the requirements mentioned in the checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

Table 2-1 Recovering physical machines to on-premises data center using Resiliency Platform Data Mover *(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
	  ■ 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
	  ■ Configuring Replication Gateway as a PXE Boot server and DHCP server
	  ■ 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 ■ Prepare host for replication

Table 2-1 Recovering physical machines to on-premises data center using Resiliency Platform Data Mover *(continued)*

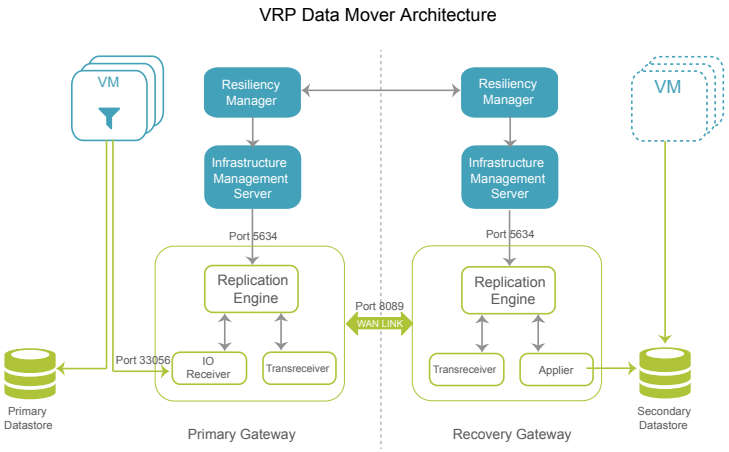
Tasks	More information
Infrastructure Pairing	For recovering assets to VMware you have to do following Infrastructure Pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ For DNS customization, refer Add DNS servers. ■ For NIC teaming / bonding, refer Support for NIC teaming / bonding for physical machines ■ Create network mappings, refer Network pairs for recovering physical machines to VMware.
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. ■ Configure physical machines for recovery to on-premises data center
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 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.

Veritas Resiliency Platform now supports Continuous Data Protection (CDP) mechanism to recover from the current or a point in past known as Recovery Point. This support is available from version 3.5 and is now supported only for recovering VMware virtual machines to on-premises data center using Resiliency Platform Data Mover using VMware VAIO (vSphere APIs for IO Filter) interfaces. CDP is enabled when you create or edit a resiliency group while selecting the Replication Gateway pair.

Figure 2-2 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 2-2 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 are compatible with 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, 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
	  ■ 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
	■ For secure communication with VMware vCenter server, install the root CA certificate. Refer Managing security

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

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

Tasks	More information
Infrastructure Pairing	For recovering assets to VMware you have to do following Infrastructure Pairing: ■ Navigate to **Infrastructure Pairing > Replication Appliance**, refer Create Replication Gateway pair. ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ For DNS customization, refer Add DNS servers. ■ Create network mappings, refer Network pairs for recovering machines to on-premises data center.
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. From version 3.5, CDP storage mechanism is provided to the resiliency groups. While configuring the resiliency group for disaster recovery, in the Replication Gateway pair selection wizard, you can enable the CDP storage and can provide the % of the CDP storage to be used on the source and target data centers. ■ Configure resiliency groups for monitoring ■ Configure VMware virtual machines for recovery to on-premises data center
Advanced features 	Virtual business services, resiliency plans, and evacuation plans are some of the features of Veritas Resiliency Platform that you can additionally use to customize the process of recovery of your assets. ■ Virtual business services ■ Resiliency plans ■ Evacuation plans
Perform remote recovery operations 	Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, recover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Recover ■ Resync

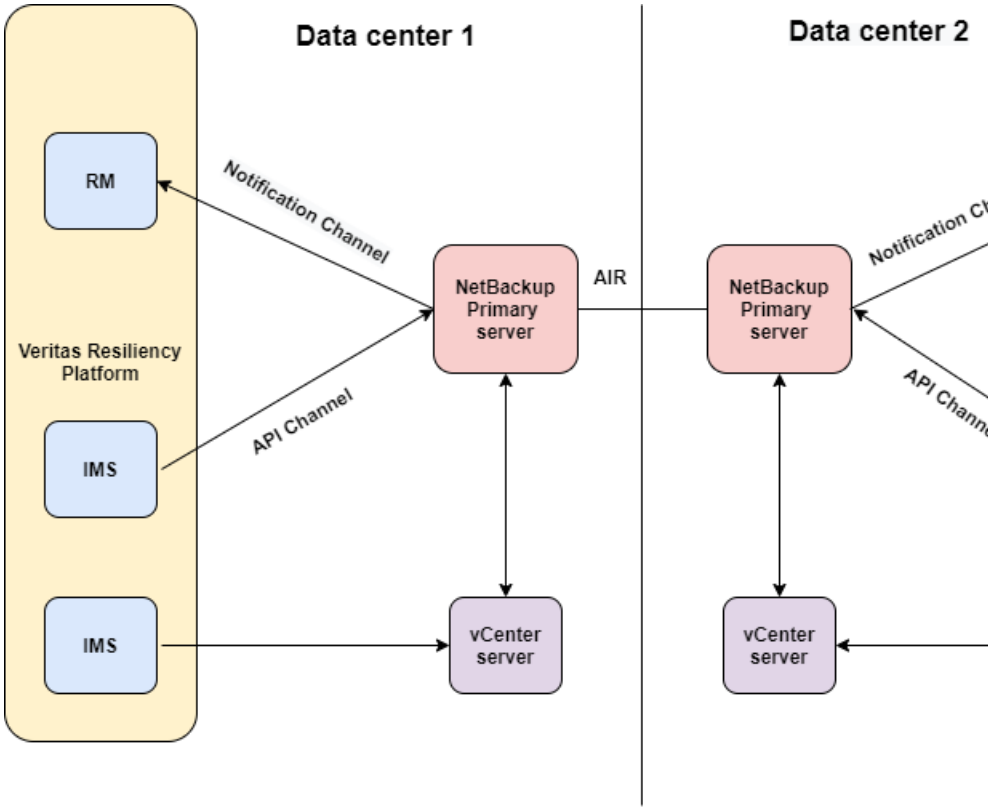
Table 2-2 Recovering VMware virtual machines using VMware VAIO *(continued)*

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 VMware virtual machines from VMware to VMware using NetBackup

Using the Veritas Resiliency Platform 4.0, you can restore VMware virtual machine from NetBackup generated backup images to the target data center. For more information on NetBackup and NetBackup Appliances, see About NetBackup and NetBackup Appliances.

Figure 2-3 Deployment architecture for NetBackup primary server



In the image, data center 1 is the source data center and data center 2 is target data center. Targeted Auto Image Replication, denoted as AIR in the below image, ensures that the backup images are available on NetBackup primary server in the target 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 2-3 Recovering virtual machines using NetBackup images

Tasks	More information
Plan your environment 	Refer to the *Veritas Resiliency Platform Overview and Planning Guide* to know about the product, its components, features, and capabilities. Refer to the *Veritas Resiliency Platform Release Notes* for release information such as main features, known issues, and limitations. Overview and Planning Guide Release Notes Ensure that the configuration details in your environment matches the requirements mentioned in the checklist.

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
	  ■ 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
	■ For secure communication, refer Managing security

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 primary server ■ Add IMS to NetBackup primary server as an additional server

Table 2-3 Recovering virtual machines using NetBackup images *(continued)*

Tasks	More information
Infrastructure Pairing	For recovering assets to VMware you have to do following Infrastructure Pairing: ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ For DNS customization, refer Add DNS servers. ■ Create network mappings, refer Network pairs for recovering machines to on-premises data center.
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 ■ 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 recover (local or remote) operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Recover virtual machines

Table 2-3 Recovering virtual machines using NetBackup images *(continued)*

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

Recovering virtual machines from VMware to AWS using NetBackup Image Sharing

Using the Resiliency Platform, you can recover VMware virtual machine from NetBackup generated backup images that are stored into AWS S3 buckets to the AWS cloud target data center.

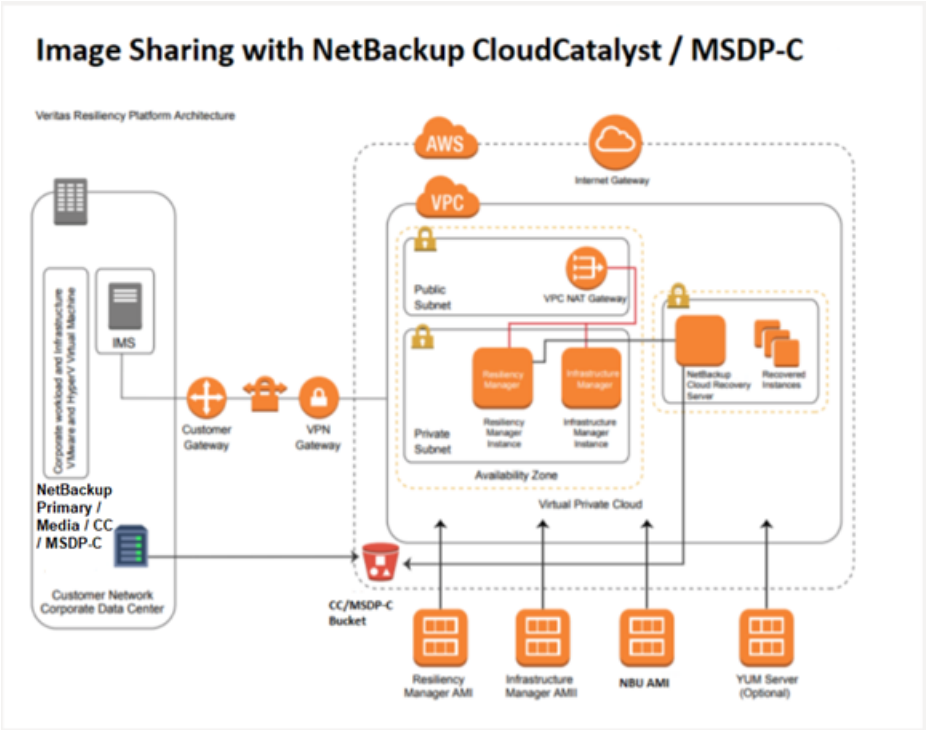
In figure the on-premises data center is the source data center and the target data center is an AWS cloud region. The Infrastructure Management Server (IMS) in the on-premises data center discovers the vCenter server and the backup configuration from the NetBackup primary server. NetBackup with the Image Sharing feature, which is available from NetBackup version 8.2 onwards, backs up the virtual machine images along with the image metadata from the on-premise data center into the designated S3 bucket.

For backing up the data in AWS S3 bucket, either NetBackup CloudCatalyst or MSDP-C configuration can be used.

The recovery using these backup images is achieved using a NetBackup Cloud Recovery Server (CRS) virtual appliance that is deployed in the cloud data center. The image metadata stored in the S3 bucket allows the NetBackup CRS to read the image information and create an Amazon Machine Image (AMI). This AMI is

then used to provision cloud instances in the cloud data center during the recover operation.

Figure 2-4 Image Sharing with NetBackup CloudCatalyst / MSDP-C



The following table provides the summary of deployment, configuration, and recovery of virtual machines to cloud using NetBackup generated backup images that are stored in S3 bucket using the Image Sharing feature.

Table 2-4 Recovering virtual machines using NetBackup images

Tasks	More information
Plan your environment 	Refer to the *Veritas Resiliency Platform Overview and Planning Guide* to know about the product, its components, features, and capabilities. Refer to the *Veritas Resiliency Platform Release Notes* for release information such as main features, known issues, and limitations. Overview and Planning Guide Release Notes Ensure that the configuration details in your environment match the requirements mentioned in the checklist. Checklist for recovery of VMware virtual machines to AWS cloud using NetBackup
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 Downloading the Veritas Resiliency Platform virtual appliances ■ About deploying the virtual appliances About deploying the Resiliency Platform virtual appliances ■ Deploy the Resiliency Platform components in AWS by using one of the following methods: ■ Deploying the virtual appliances in AWS through AWS Marketplace ■ Deploying the virtual appliances in AWS using OVA files ■ Deploy the virtual appliances for one or more IMS in the premises data center: ■ Deploying the virtual appliance through VMware vSphere Client ■ Configure the virtual appliances as Veritas Resiliency Platform components: ■ About configuring the Resiliency Platform components ■ Prerequisites for configuring Resiliency Platform components ■ Deploy the Cloud Recovery Server (CRS) Deploy CRS
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. ■ Getting started with a new Resiliency Platform configuration ■ Configure the settings for the resiliency domain: ■ Adding an IMS ■ Adding AWS cloud data center ■ Managing user authentication and permissions ■ For secure communication, refer Managing security

Table 2-4 Recovering virtual machines using NetBackup images *(continued)*

Tasks	More information
Add asset infrastructure 	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console. ■ Adding VMware virtualization servers ■ Adding NetBackup primary server ■ Adding NetBackup Cloud Recovery Server (CRS)
Infrastructure Pairing	For recovering assets to VMware you have to do following Infrastructure Pairing: ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ Create Network group of cloud subnets. Adding a network group ■ Customize DNS Configuring DNS server settings for a data center ■ Create network mappings. Network pairs for recovering virtual machines to AWS
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. ■ Configuring a resiliency group for basic monitoring ■ Managing VMware virtual machines for remote recovery to AWS cloud 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. ■ Managing virtual business services ■ Managing resiliency plans ■ About evacuation plan

Table 2-4 Recovering virtual machines using NetBackup images *(continued)*

Tasks	More information
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 recover (local or remote) operations on the resiliency groups. **Note:** The rehearsal operation is not supported from AWS to VMware. ■ Performing the rehearsal operation on virtual machines from VMware to AWS using NetBackup Image Sharing ■ Performing cleanup rehearsal for virtual machines ■ Recovering virtual machines to cloud (AWS) using NetBackup Image Sharing
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. ■ About risks ■ About reports ■ Managing 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. ■ About klish ■ Troubleshoot ■ About applying updates to Resiliency Platform ■ 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 2-5 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 are compatible with 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
	  ■ Configuring Resiliency Manager or IMS

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

Table 2-5 Recovering VMware virtual machines using third-party replication technology *(continued)*

Tasks	More information
Add asset infrastructure 	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console. ■ Add VMware virtualization servers ■ Add enclosures
Infrastructure Pairing	For recovering assets to VMware you have to do following Infrastructure Pairing: ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ For DNS customization, refer Add DNS servers. ■ Create network mappings, refer Network pairs for recovering machines to on-premises data center.
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 ■ 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 2-5 Recovering VMware virtual machines using third-party replication technology *(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, recover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Recover ■ 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

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
- Infinidat

Table 2-6 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 are compatible with 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 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
	  ■ Configuring Resiliency Manager or IMS

Table 2-6 Recovering Hyper-V virtual machines using third-party replication technology *(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
	  ■ 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
Infrastructure Pairing	For recovering assets to Hyper-V you have to do following Infrastructure Pairing: ■ Navigate to **Settings > Infrastructure > Access Profile > Network** to mark purpose of the networks, refer Add and map network objects. ■ For DNS customization, refer Add DNS servers. ■ Create network mappings, refer Network pairs for recovering machines to on-premises data center.
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 ■ Manage resiliency groups for remote recovery

Table 2-6 Recovering Hyper-V virtual machines using third-party replication technology *(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, recover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Recover ■ 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

Recovering Applications using third-party replication technology

Veritas Resiliency Platform supports following replication technology for recovery of the applications:

- DataGuard

Table 2-7 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 are compatible with 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 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
	  ■ Configuring Resiliency Manager or IMS

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

Table 2-7 Recovering applications using third-party replication technology *(continued)*

Tasks	More information

Add asset infrastructure
 
	Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to Veritas Resiliency Platform. The IMS then discovers the asset information for monitoring and operations in the console.
	■ Add virtualization servers:
	  ■ Add VMware virtualization servers
	  ■ Hyper-V servers
	■ Add host assets
	■ Add enclosures
	■ Add DNS servers

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 ■ 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, recover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Recover ■ Resync

Table 2-7 Recovering applications using third-party replication technology *(continued)*

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

Recovering InfoScale applications

Veritas Resiliency Platform lets you manage the InfoScale applications by configuring the corresponding clusters into Infrastructure Management Servers (IMS). The InfoScale applications are automatically discovered in the Resiliency Platform. You can group the InfoScale applications into resiliency groups or VBS to recover, monitor, visualize, and generate reports about these applications in the Resiliency Platform. Before version 3.5, you were required to add Veritas InfoScale Operations Manager into Veritas Resiliency Platform to manage the InfoScale applications. From version 3.5 there is no need to use Veritas InfoScale Operations Manager to manage the InfoScale applications. If you are upgrading from version 3.4 or earlier version where you had configured Veritas InfoScale Operations Manager, then refer to topic for how to configure those clusters into Infrastructure Management Servers.

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

Figure 2-5 A typical workflow for recovering managed InfoScale applications

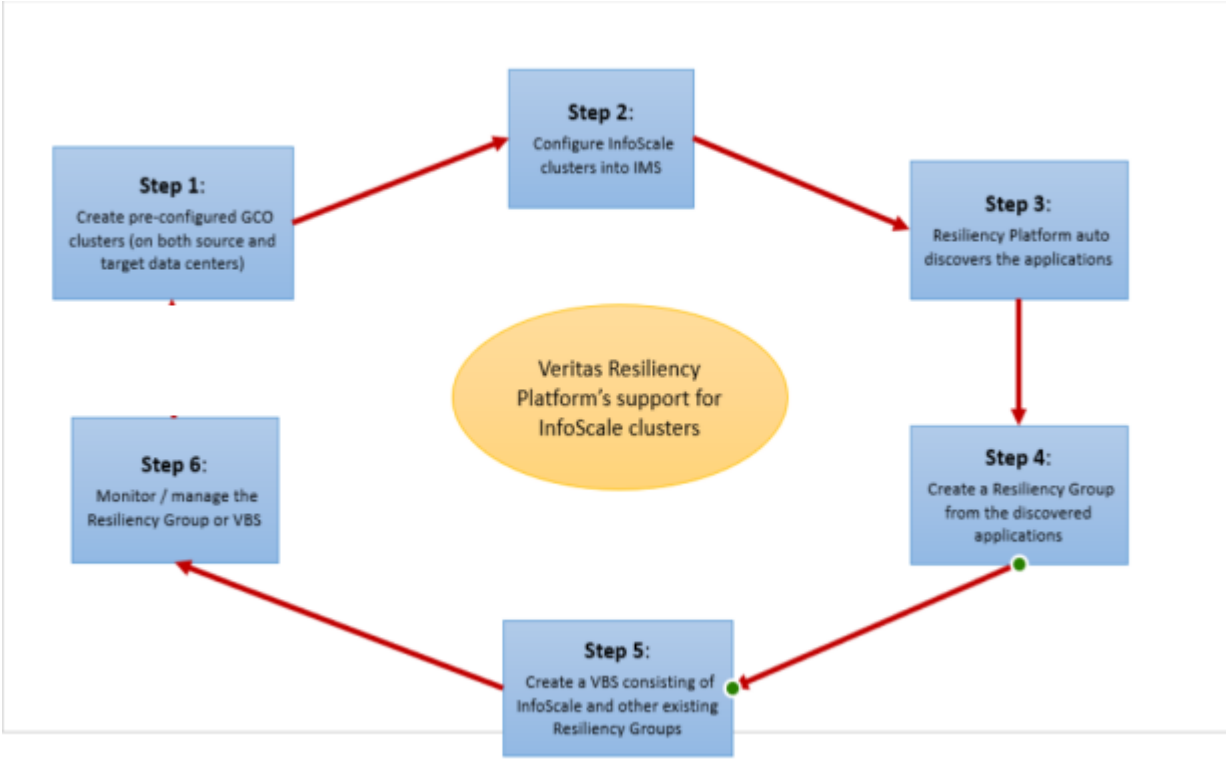


Table 2-8 Recovering InfoScale applications

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 are compatible with the requirements mentioned in the checklist. ■ Overview and Planning Guide ■ Release Notes ■ Checklist for deployment and disaster recovery configuration

Table 2-8 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
	■ About configuring the virtual appliances
	■ 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
	  ■ Add InfoScale cluster
	  ■ 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 ■ 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 2-8 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, recover, or resync operations on the resiliency groups. ■ Rehearsal ■ Cleanup rehearsal ■ Migrate ■ Recover ■ 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

Glossary

activity	A task or an operation performed on a resiliency group.
add-on	An additional software package that can be installed on hosts by the Infrastructure Management Server (IMS) for specialized uses.
asset infrastructure	The data center assets that can be added to the Infrastructure Management Server (IMS) for IMS discovery and monitoring. For example, virtualization servers, virtual machines, enclosures, and applications.
assets	The virtual machines, physical machines, or applications that have been discovered by the Infrastructure Management Server (IMS) and that can be grouped into resiliency groups.
data center	A location that contains asset infrastructure to be managed by Veritas Resiliency Platform. For the disaster recovery use case, the resiliency domain must contain at least two data centers in different locations, a source data center and target data center. Each data center has a Resiliency Manager and one or more IMSs.
host	In Veritas Resiliency Platform, the term hosts means Application host, Resiliency Platform Data Mover host, Storage discovery host, VMware Discovery host, and Hyper-V host.
Infrastructure Management Server (IMS)	The Veritas Resiliency Platform component that discovers, monitors, and manages the asset infrastructure within a data center. The IMS transmits information about the asset infrastructure to the Resiliency Manager.
klish	Command Line Interface SHell. Provides the command line menu on the virtual appliance for use after the initial bootstrap configuration.
migrate	A planned activity involving graceful shutdown of assets at the source data center and starting them at the target data center. In this process, replication ensures that consistent data is made available at the target data center.
persona	A user role that has access to a predefined set of jobs (operations). Used to assign permissions to users and groups for Veritas Resiliency Platform web console operations.
rehearsal	A zero-downtime test that mimics the configuration, application data, storage, and the failover behavior of the resiliency group.

	Rehearsal verifies the ability of the resiliency group to fail over to the recovery data center during a disaster.
Replication Gateway	The Veritas Resiliency Platform component that performs data replication between the source and the target data center.
resiliency domain	The logical scope of a Resiliency Platform deployment. It can extend across multiple data centers.
resiliency group	The unit of management and control in Veritas Resiliency Platform. Related assets are organized into a resiliency group to be managed and monitored as a single entity.
Resiliency Manager	The Veritas Resiliency Platform component that provides resiliency capabilities within a resiliency domain. It is composed of loosely coupled services, a distributed data repository, and a management web console.
resiliency plan	A collection of tasks or operations, along with the relevant assets, which are performed in a predefined sequence.
resiliency plan template	A template defining the execution sequence of a collection of tasks or operations.
Resiliency Platform Data Mover Replication host	To enable replication using Resiliency Platform Data Mover replication technology, you need to add an asset and prepare it for replication. Asset can be a physical machine or a virtual machine.
source data center	The data center that is normally used for business.
take over	An activity initiated by a user when the source data center is down due to a disaster and the assets need to be restored at the target data center to provide business continuity.
target data center	The data center that is used if a disaster scenario occurs.
tier	Within a virtual business service (VBS), resiliency groups are arranged as tiers. Tiers represent the logical dependencies between the resiliency groups and determine the relative order in which operations are performed on the resiliency groups.
VAIO framework	VMware framework consisting of vSphere APIs for I/O Filtering. This framework enables Veritas Resiliency Platform to run filters on ESXi servers and intercept any I/O requests from a guest operating system to a virtual disk.
virtual appliance	An appliance that includes the operating system environment and the software application which are deployed together as a virtual machine. The Veritas Resiliency Platform virtual appliance is deployed as a virtual machine and then configured with basic settings and a role (for example, Resiliency Manager).

virtual business service (VBS)	A multi-tier IT service where each VBS tier hosts one or more resiliency groups. A VBS groups multiple services as a single unit for visualization, automation, and recovery in case of a disaster in the desired order.
Veritas Replication Set	A virtual machine, which belongs to the resiliency group, is termed as Veritas Replication Set. All the disks attached to this virtual machine, including the boot and data disk, constitute a Veritas Replication Set. The write order fidelity is maintained across all disks in a given replication set.
web console	The web-based management console on the Resiliency Manager that is used to configure the settings for the resiliency domain and perform operations.