

# Veritas™ Resiliency Platform 3.1 User Guide

Applicable for Veritas Resiliency  
Platform 3.1, Update 1, Update 2, and  
Update 3

# Veritas Resiliency Platform: User Guide

Last updated: 2018-04-24

Document version: Document version: 3.1 Rev 1

## Legal Notice

Copyright © 2018 Veritas Technologies LLC. All rights reserved.

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

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

<https://www.veritas.com/licensing/process>

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

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

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

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

<http://www.veritas.com>

## Technical Support

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

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

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

<https://my.veritas.com>

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

Worldwide (except Japan)

[CustomerCare@veritas.com](mailto:CustomerCare@veritas.com)

Japan

[CustomerCare\\_Japan@veritas.com](mailto:CustomerCare_Japan@veritas.com)

## Documentation

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

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

## Documentation feedback

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

[doc.feedback@veritas.com](mailto:doc.feedback@veritas.com)

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

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

## Veritas Services and Operations Readiness Tools (SORT)

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

[https://sort.veritas.com/data/support/SORT\\_Data\\_Sheet.pdf](https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf)

# Contents

Chapter 1	Recovery to cloud data center .....	5
	Recovering VMware virtual machines to AWS .....	5
	Recovering Hyper-V virtual machines to AWS .....	9
	Recovering VMware virtual machines to Azure .....	13
	Recovering Hyper-V virtual machines to Azure .....	17
	Recovering VMware virtual machines to vCloud Director .....	20
	Recovering Hyper-V virtual machines to vCloud Director .....	24
	Recovering VMware virtual machines to vCloud Director without adding vCenter server .....	28
	Recovering Hyper-V virtual machines to vCloud Director without adding Hyper-V server .....	32
	Recovering virtual machines from vCloud Director to vCloud Director .....	36
Chapter 2	Recovery to on-premises data center .....	40
	Recovering VMware virtual machines to on-premises data center using Resiliency Platform Data Mover .....	40
	Recovering VMware virtual machines using NetBackup .....	44
	Recovering VMware virtual machines using third-party replication technology .....	47
	Recovering Hyper-V virtual machines using third-party replication technology .....	50
	Recovering Applications using third-party replication technology .....	53
	Recovering InfoScale applications .....	56
Index .....		60

# Recovery to cloud data center

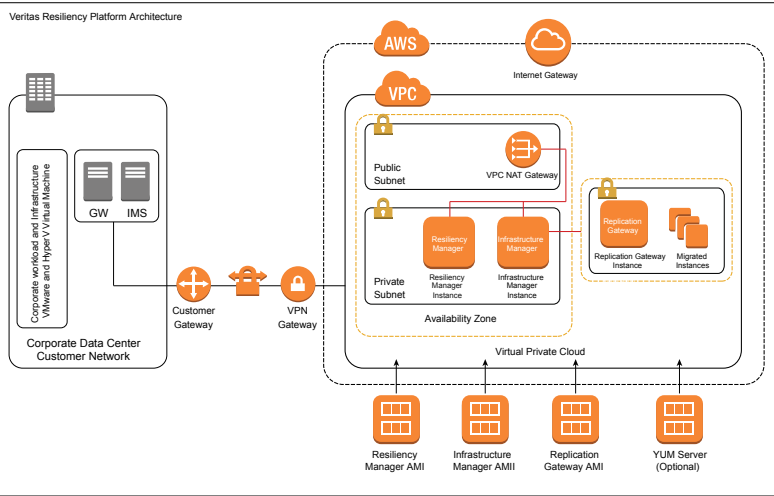
This chapter includes the following topics:

- [Recovering VMware virtual machines to AWS](#)
- [Recovering Hyper-V virtual machines to AWS](#)
- [Recovering VMware virtual machines to Azure](#)
- [Recovering Hyper-V virtual machines to Azure](#)
- [Recovering VMware virtual machines to vCloud Director](#)
- [Recovering Hyper-V virtual machines to vCloud Director](#)
- [Recovering VMware virtual machines to vCloud Director without adding vCenter server](#)
- [Recovering Hyper-V virtual machines to vCloud Director without adding Hyper-V server](#)
- [Recovering virtual machines from vCloud Director to vCloud Director](#)

## Recovering VMware virtual machines to AWS


Using Veritas Resiliency Platform 3.1, you can configure and protect your VMware virtual machines for recovery to AWS using the Resiliency Platform Data Mover.

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





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





Table 1-1 Recovering VMware virtual machines to AWS

Tasks	More information
<b>Plan your environment</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Overview and Planning Guide</a></li><li>■ <a href="#">Release Notes</a></li><li>■ <a href="#">Checklist for deployment and disaster recovery configuration</a></li></ul>

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



Tasks	More information
<b>Deploy and configure the virtual appliances</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Download the files required for deployment</a></li><li>■ <a href="#">About deploying the virtual appliances</a></li><li>■ Deploy the Resiliency Platform components in AWS by using one of the following methods:<ul style="list-style-type: none"><li>■ <a href="#">Using CloudFormation templates</a></li><li>■ <a href="#">Using OVA files</a></li></ul></li><li>■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the on-premises data center:<ul style="list-style-type: none"><li>■ <a href="#">Using VMware vSphere client</a></li></ul></li><li>■ Deploy Data Gateway in AWS environment (if you want to use Object Storage mode replication):<ul style="list-style-type: none"><li>■ <a href="#">Deploy Data Gateway</a></li></ul></li><li>■ Configure the virtual appliances as Veritas Resiliency Platform components:<ul style="list-style-type: none"><li>■ <a href="#">About configuring the virtual appliances</a></li><li>■ <a href="#">Prerequisites</a></li><li>■ <a href="#">Configuring Resiliency Manager or IMS</a></li><li>■ <a href="#">Configuring Replication Gateways</a></li></ul></li></ul>
<b>Set up the resiliency domain</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Create the resiliency domain using getting started wizard</a></li><li>■ Configure the settings for the resiliency domain:<ul style="list-style-type: none"><li>■ <a href="#">Add IMS</a></li><li>■ <a href="#">Add Replication Gateways</a></li><li>■ <a href="#">Add cloud data center</a> (if not done during getting started wizard)</li><li>■ <a href="#">Add Data Gateway</a> (only if you want to use Object Storage mode replication)</li><li>■ <a href="#">Manage user authentication and permission</a></li><li>■ <a href="#">Manage alerts, notifications, and other product settings</a></li></ul></li></ul>

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

Tasks	More information
<b>Add asset infrastructure</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Add VMware servers</a></li><li>■ <a href="#">Prepare host for replication</a></li><li>■ <a href="#">Create Replication Gateway pair</a></li><li>■ <a href="#">Add and map network objects</a></li><li>■ <a href="#">Add network groups</a> (Optional)</li><li>■ <a href="#">Create network pairs between data centers</a></li></ul>
<b>Create resiliency groups</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Configure resiliency groups for monitoring</a></li><li>■ <a href="#">Prerequisites for configuring resiliency groups for recovery to AWS</a></li><li>■ <a href="#">Configure resiliency groups for recovery to AWS</a></li></ul>
<b>Advanced features</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Virtual business services</a></li><li>■ <a href="#">Resiliency plans</a></li><li>■ <a href="#">Evacuation plans</a></li></ul>
<b>Perform remote recovery operations</b> 	<p>Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups.</p> <ul style="list-style-type: none"><li>■ <a href="#">Rehearsal</a></li><li>■ <a href="#">Cleanup rehearsal</a></li><li>■ <a href="#">Migrate</a></li><li>■ <a href="#">Take over</a></li><li>■ <a href="#">Resync</a></li></ul>



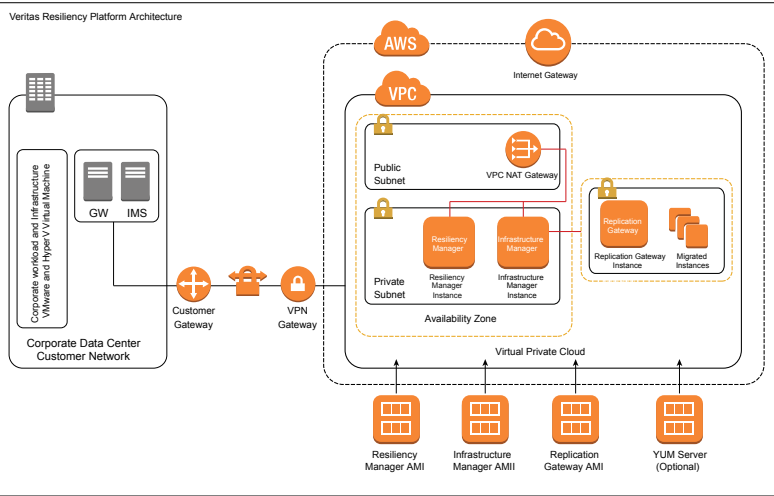
**Table 1-1** Recovering VMware virtual machines to AWS (*continued*)

Tasks	More information
<b>Monitor assets</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Risks</a></li><li>■ <a href="#">Reports</a></li><li>■ <a href="#">Activities</a></li></ul>
<b>Miscellaneous references</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Using klish</a></li><li>■ <a href="#">Troubleshooting</a></li><li>■ <a href="#">Updating</a></li><li>■ <a href="#">References</a></li></ul>

## Recovering Hyper-V virtual machines to AWS


Using Veritas Resiliency Platform 3.1, 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
<b>Plan your environment</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Overview and Planning Guide</a></li><li>■ <a href="#">Release Notes</a></li><li>■ <a href="#">Checklist for deployment and disaster recovery configuration</a></li></ul>



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

Tasks	More information
<b>Deploy and configure the virtual appliances</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Download the files required for deployment</a></li> <li>■ <a href="#">About deploying the virtual appliances</a></li> <li>■ Deploy the Resiliency Platform components in AWS by using one of the following methods: <ul style="list-style-type: none"> <li>■ <a href="#">Using CloudFormation templates</a></li> <li>■ <a href="#">Using OVA files</a></li> </ul> </li> <li>■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the on-premises data center: <ul style="list-style-type: none"> <li>■ <a href="#">Using Hyper-V Manager</a></li> </ul> </li> <li>■ Deploy Data Gateway in AWS environment (only if you want to use Object Storage mode replication): <ul style="list-style-type: none"> <li>■ <a href="#">Deploy Data Gateway</a></li> </ul> </li> <li>■ Configure the virtual appliances as Veritas Resiliency Platform components: <ul style="list-style-type: none"> <li>■ <a href="#">About configuring the virtual appliances</a></li> <li>■ <a href="#">Prerequisites</a></li> <li>■ <a href="#">Configuring Resiliency Manager or IMS</a></li> <li>■ <a href="#">Configuring Replication Gateways</a></li> </ul> </li> </ul>
<b>Set up the resiliency domain</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Create the resiliency domain using getting started wizard</a></li> <li>■ Configure the settings for the resiliency domain: <ul style="list-style-type: none"> <li>■ <a href="#">Add IMS</a></li> <li>■ <a href="#">Add Replication Gateways</a></li> <li>■ <a href="#">Add cloud data center</a> (if not done during getting started wizard)</li> <li>■ <a href="#">Add Data Gateway</a> (only if you want to use Object Storage mode replication)</li> <li>■ <a href="#">Manage user authentication and permission</a></li> <li>■ <a href="#">Manage alerts, notifications, and other product settings</a></li> </ul> </li> </ul>

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

Tasks	More information
<b>Add asset infrastructure</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Add Hyper-V servers</a></li><li>■ <a href="#">Prepare host for replication</a></li><li>■ <a href="#">Create Replication Gateway pair</a></li><li>■ <a href="#">Add and map network objects</a></li><li>■ <a href="#">Add network groups</a> (Optional)</li><li>■ <a href="#">Create network pairs between data centers</a></li></ul>
<b>Create resiliency groups</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Configure resiliency groups for monitoring</a></li><li>■ <a href="#">Prerequisites for configuring resiliency groups for recovery to AWS</a></li><li>■ <a href="#">Configure resiliency groups for recovery to AWS</a></li></ul>
<b>Advanced features</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Virtual business services</a></li><li>■ <a href="#">Resiliency plans</a></li><li>■ <a href="#">Evacuation plans</a></li></ul>
<b>Perform remote recovery operations</b> 	<p>Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups.</p> <ul style="list-style-type: none"><li>■ <a href="#">Rehearsal</a></li><li>■ <a href="#">Cleanup rehearsal</a></li><li>■ <a href="#">Migrate</a></li><li>■ <a href="#">Take over</a></li><li>■ <a href="#">Resync</a></li></ul>

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

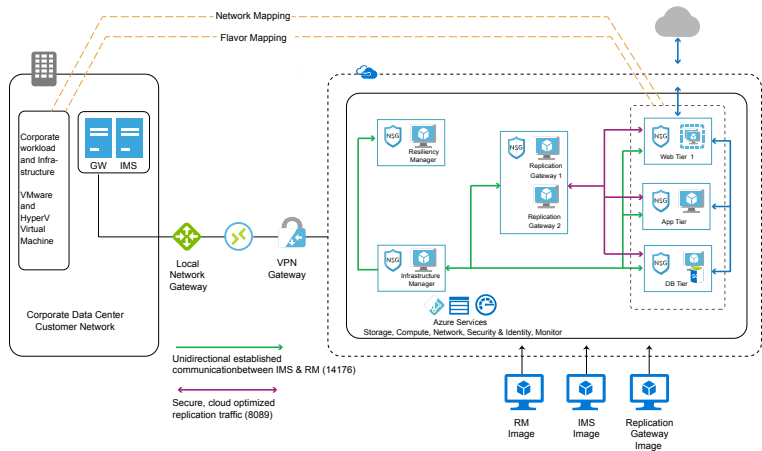
Tasks	More information
<b>Monitor assets</b> 	<p>You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page.</p> <ul style="list-style-type: none"><li>■ <a href="#">Risks</a></li><li>■ <a href="#">Reports</a></li><li>■ <a href="#">Activities</a></li></ul>
<b>Miscellaneous references</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Using klish</a></li><li>■ <a href="#">Troubleshooting</a></li><li>■ <a href="#">Updating</a></li><li>■ <a href="#">References</a></li></ul>

## Recovering VMware virtual machines to Azure

Using Veritas Resiliency Platform 3.1, you can configure and protect your VMware virtual machines for recovery to Azure using the Resiliency Platform Data Mover.


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

VRP: Basic Deployment Reference Architecture in Azure Cloud






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

Table 1-3 Recovering VMware virtual machines to Azure

Tasks	More information
<b>Plan your environment</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Overview and Planning Guide</a></li><li>■ <a href="#">Release Notes</a></li><li>■ <a href="#">Checklist for deployment and disaster recovery configuration</a></li></ul>

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

Tasks	More information
<b>Deploy and configure the virtual appliances</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Download the files required for deployment</a></li> <li>■ <a href="#">About deploying the virtual appliances</a></li> <li>■ Deploy the virtual appliances for Resiliency Manager, Infrastructure Management Server (IMS), and Replication Gateway in the Azure cloud data center: <ul style="list-style-type: none"> <li>■ <a href="#">Using Azure</a></li> </ul> </li> <li>■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the premises data center: <ul style="list-style-type: none"> <li>■ <a href="#">Using VMware vSphere client</a></li> </ul> </li> <li>■ Configure the virtual appliances as Veritas Resiliency Platform components: <ul style="list-style-type: none"> <li>■ <a href="#">About configuring the virtual appliances</a></li> <li>■ <a href="#">Prerequisites</a></li> <li>■ <a href="#">Configuring Resiliency Manager or IMS</a></li> <li>■ <a href="#">Configuring Replication Gateways</a></li> </ul> </li> </ul>
<b>Set up the resiliency domain</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Create the resiliency domain using getting started wizard</a></li> <li>■ Configure the settings for the resiliency domain: <ul style="list-style-type: none"> <li>■ <a href="#">Add IMS</a></li> <li>■ <a href="#">Add Replication Gateways</a></li> <li>■ <a href="#">Add cloud data center (if not done during getting started wizard)</a></li> <li>■ <a href="#">Manage user authentication and permission</a></li> <li>■ <a href="#">Manage alerts, notifications, and other product settings</a></li> </ul> </li> </ul>
<b>Add asset infrastructure</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Add VMware servers</a></li> <li>■ <a href="#">Prepare host for replication</a></li> <li>■ <a href="#">Create Replication Gateway pair</a></li> <li>■ <a href="#">Add and map network objects</a></li> <li>■ <a href="#">Create network pairs between data centers</a></li> </ul>

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





Tasks	More information
<b>Create resiliency groups</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Configure resiliency groups for monitoring</a></li> <li>■ <a href="#">Prerequisites for configuring resiliency groups for recovery to Azure</a></li> <li>■ <a href="#">Configure resiliency groups for recovery to Azure</a></li> </ul>
<b>Advance features</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Virtual business services</a></li> <li>■ <a href="#">Resiliency plans</a></li> <li>■ <a href="#">Evacuation plans</a></li> </ul>
<b>Perform remote recovery operations</b> 	<p>Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Rehearsal</a></li> <li>■ <a href="#">Cleanup rehearsal</a></li> <li>■ <a href="#">Migrate</a></li> <li>■ <a href="#">Take over</a></li> <li>■ <a href="#">Resync</a></li> </ul>
<b>Monitor assets</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Risks</a></li> <li>■ <a href="#">Reports</a></li> <li>■ <a href="#">Activities</a></li> </ul>



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

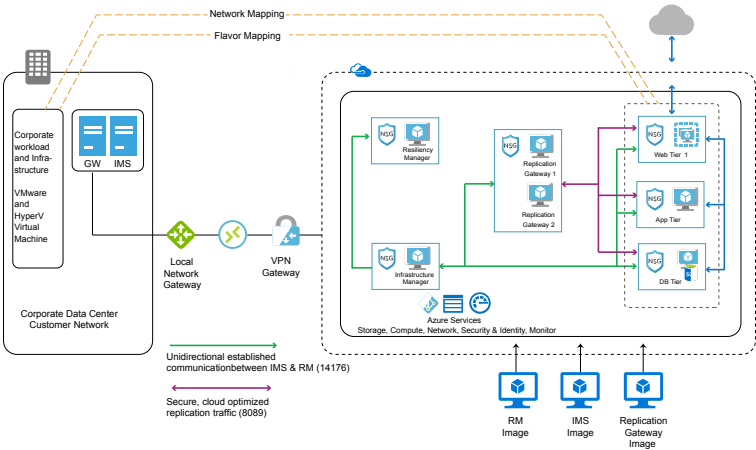
Tasks	More information
Miscellaneous references	<div>After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot.</div>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

# Recovering Hyper-V virtual machines to Azure

Using Veritas Resiliency Platform 3.1, you can configure and protect your Hyper-V virtual machines for recovery to Azure using the Resiliency Platform Data Mover.




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

VRP: Basic Deployment Reference Architecture in Azure Cloud







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



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

Tasks	More information
<b>Plan your environment</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Overview and Planning Guide</a></li> <li>■ <a href="#">Release Notes</a></li> <li>■ <a href="#">Checklist for deployment and disaster recovery configuration</a></li> </ul>
<b>Deploy and configure the virtual appliances</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Download the files required for deployment</a></li> <li>■ <a href="#">About deploying the virtual appliances</a></li> <li>■ Deploy the virtual appliances for Resiliency Manager, Infrastructure Management Server (IMS), and Replication Gateway in the Azure cloud data center: <ul style="list-style-type: none"> <li>■ <a href="#">Using Azure</a></li> </ul> </li> <li>■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the premises data center: <ul style="list-style-type: none"> <li>■ <a href="#">Using Hyper-V Manager</a></li> </ul> </li> <li>■ Configure the virtual appliances as Veritas Resiliency Platform components: <ul style="list-style-type: none"> <li>■ <a href="#">About configuring the virtual appliances</a></li> <li>■ <a href="#">Prerequisites</a></li> <li>■ <a href="#">Configuring Resiliency Manager or IMS</a></li> <li>■ <a href="#">Configuring Replication Gateways</a></li> </ul> </li> </ul>
<b>Set up the resiliency domain</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Create the resiliency domain using getting started wizard</a></li> <li>■ Configure the settings for the resiliency domain: <ul style="list-style-type: none"> <li>■ <a href="#">Add IMS</a></li> <li>■ <a href="#">Add Replication Gateways</a></li> <li>■ <a href="#">Add cloud data center (if not done during getting started wizard)</a></li> <li>■ <a href="#">Manage user authentication and permission</a></li> <li>■ <a href="#">Manage alerts, notifications, and other product settings</a></li> </ul> </li> </ul>

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

Tasks	More information
<b>Add asset infrastructure</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Add Hyper-V servers</a></li> <li>■ <a href="#">Prepare host for replication</a></li> <li>■ <a href="#">Create Replication Gateway pair</a></li> <li>■ <a href="#">Add and map network objects</a></li> <li>■ <a href="#">Create network pairs between data centers</a></li> </ul>
<b>Create resiliency groups</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Configure resiliency groups for monitoring</a></li> <li>■ <a href="#">Prerequisites for configuring resiliency groups for recovery to Azure</a></li> <li>■ <a href="#">Configure resiliency groups for recovery to Azure</a></li> </ul>
<b>Advance features</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Virtual business services</a></li> <li>■ <a href="#">Resiliency plans</a></li> <li>■ <a href="#">Evacuation plans</a></li> </ul>
<b>Perform remote recovery operations</b> 	<p>Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Rehearsal</a></li> <li>■ <a href="#">Cleanup rehearsal</a></li> <li>■ <a href="#">Migrate</a></li> <li>■ <a href="#">Take over</a></li> <li>■ <a href="#">Resync</a></li> </ul>

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

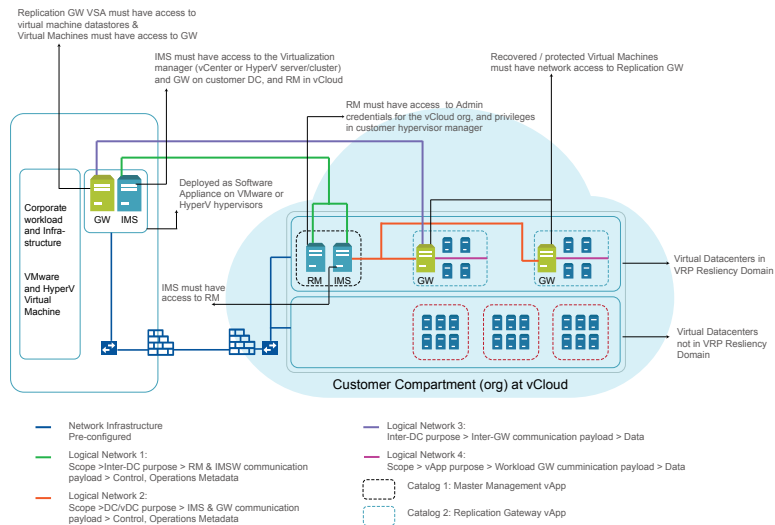
Tasks	More information
<b>Monitor assets</b> 	<p>You can monitor risks to the recoverability or continuity of your protected assets. Run various reports to view the status of the assets in your data center. And view details about operations such as the status (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed on the Activities page.</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Risks</a></li> <li>▪ <a href="#">Reports</a></li> <li>▪ <a href="#">Activities</a></li> </ul>
<b>Miscellaneous references</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Using klish</a></li> <li>▪ <a href="#">Troubleshooting</a></li> <li>▪ <a href="#">Updating</a></li> <li>▪ <a href="#">References</a></li> </ul>

# Recovering VMware virtual machines to vCloud Director

Using Veritas Resiliency Platform 3.1, you can configure and protect your VMware virtual machines for recovery to vCloud Director using the Resiliency Platform Data Mover.


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

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






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





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

Tasks	More information
<b>Plan your environment</b> 	<p>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.</p> <ul style="list-style-type: none"> <li><a href="#">Overview and Planning Guide</a></li> <li><a href="#">Release Notes</a></li> <li><a href="#">Checklist for deployment and disaster recovery configuration</a></li> </ul>


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

Tasks	More information
<b>Deploy and configure the virtual appliances</b>  	<p>Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in the premises as well as cloud data center.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Download the files required for deployment</a></li> <li>■ <a href="#">About deploying the virtual appliances</a></li> <li>■ 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: <ul style="list-style-type: none"> <li>■ <a href="#">Using vCloud Director</a></li> </ul> </li> <li>■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the on-premises data center: <ul style="list-style-type: none"> <li>■ <a href="#">Using VMware vSphere client</a></li> </ul> </li> <li>■ Configure the virtual appliances as Veritas Resiliency Platform components: <ul style="list-style-type: none"> <li>■ <a href="#">About configuring the virtual appliances</a></li> <li>■ <a href="#">Prerequisites</a></li> <li>■ <a href="#">Configuring Resiliency Manager or IMS</a></li> <li>■ <a href="#">Configuring Replication Gateways</a></li> </ul> </li> </ul>
<b>Set up the resiliency domain</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Create the resiliency domain using getting started wizard</a></li> <li>■ Configure the settings for the resiliency domain: <ul style="list-style-type: none"> <li>■ <a href="#">Add IMS</a></li> <li>■ <a href="#">Add Replication Gateways</a></li> <li>■ <a href="#">Add cloud data center (if not done during getting started wizard)</a></li> <li>■ <a href="#">Manage user authentication and permission</a></li> <li>■ <a href="#">Manage alerts, notifications, and other product settings</a></li> </ul> </li> </ul>
<b>Add asset infrastructure</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Add VMware servers</a></li> <li>■ <a href="#">Prepare host for replication</a></li> <li>■ <a href="#">Create Replication Gateway pair</a></li> <li>■ <a href="#">Create network pairs between data centers</a></li> </ul>

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

Tasks	More information
<b>Create resiliency groups</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Configure resiliency groups for monitoring</a></li> <li>■ <a href="#">Prerequisites for configuring virtual machines for remote recovery</a></li> <li>■ <a href="#">Manage resiliency groups for remote recovery</a></li> </ul>
<b>Advanced features</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Virtual business services</a></li> <li>■ <a href="#">Resiliency plans</a></li> <li>■ <a href="#">Evacuation plans</a></li> </ul>
<b>Perform remote recovery operations</b> 	<p>Once you have organized your assets into resiliency groups, you can perform migrate, takeover, or resync operations on the resiliency groups.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Migrate</a></li> <li>■ <a href="#">Take over</a></li> <li>■ <a href="#">Resync</a></li> </ul>
<b>Monitor assets</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Risks</a></li> <li>■ <a href="#">Reports</a></li> <li>■ <a href="#">Activities</a></li> </ul>

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

Tasks	More information
<b>Miscellaneous references</b> <div>  </div>	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Using klish</a></li> <li>■ <a href="#">Troubleshooting</a></li> <li>■ <a href="#">Updating</a></li> <li>■ <a href="#">References</a></li> </ul>

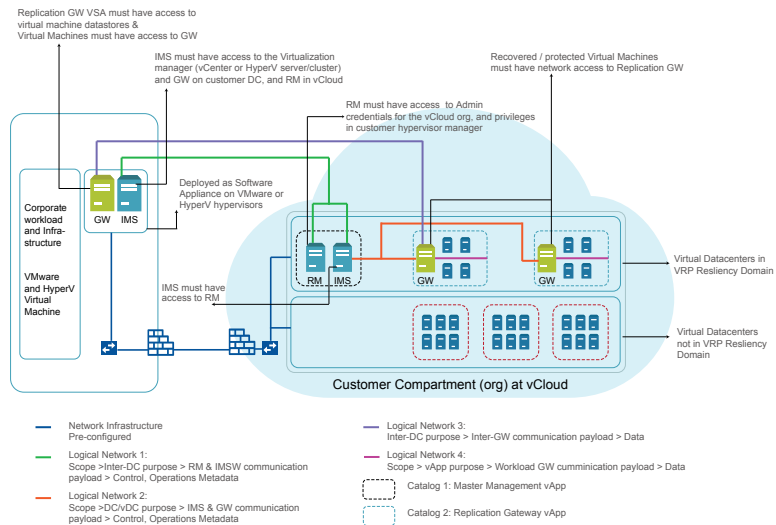
# Recovering Hyper-V virtual machines to vCloud Director

Using Veritas Resiliency Platform 3.1, you can configure and protect your Hyper-V virtual machines for recovery to vCloud Director using the Resiliency Platform Data Mover.

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



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






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

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

Tasks	More information
<b>Plan your environment</b> <div> </div>	<p>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.</p> <ul style="list-style-type: none"> <li><a href="#">Overview and Planning Guide</a></li> <li><a href="#">Release Notes</a></li> <li><a href="#">Checklist for deployment and disaster recovery configuration</a></li> </ul>

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

Tasks	More information
<b>Deploy and configure the virtual appliances</b>  	<p>Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in the premises as well as cloud data center.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Download the files required for deployment</a></li> <li>■ <a href="#">About deploying the virtual appliances</a></li> <li>■ 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: <ul style="list-style-type: none"> <li>■ <a href="#">Using vCloud Director</a></li> </ul> </li> <li>■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the on-premises data center: <ul style="list-style-type: none"> <li>■ <a href="#">Using Hyper-V Manager</a></li> </ul> </li> <li>■ Configure the virtual appliances as Veritas Resiliency Platform components: <ul style="list-style-type: none"> <li>■ <a href="#">About configuring the virtual appliances</a></li> <li>■ <a href="#">Prerequisites</a></li> <li>■ <a href="#">Configuring Resiliency Manager or IMS</a></li> <li>■ <a href="#">Configuring Replication Gateways</a></li> </ul> </li> </ul>
<b>Set up the resiliency domain</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Create the resiliency domain using getting started wizard</a></li> <li>■ Configure the settings for the resiliency domain: <ul style="list-style-type: none"> <li>■ <a href="#">Add IMS</a></li> <li>■ <a href="#">Add Replication Gateways</a></li> <li>■ <a href="#">Add cloud data center (if not done during getting started wizard)</a></li> <li>■ <a href="#">Manage user authentication and permission</a></li> <li>■ <a href="#">Manage alerts, notifications, and other product settings</a></li> </ul> </li> </ul>
<b>Add asset infrastructure</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Add Hyper-V servers</a></li> <li>■ <a href="#">Prepare host for replication</a></li> <li>■ <a href="#">Create Replication Gateway pair</a></li> <li>■ <a href="#">Create network pairs between data centers</a></li> </ul>

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






Tasks	More information
<b>Create resiliency groups</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Configure resiliency groups for monitoring</a></li> <li>■ <a href="#">Prerequisites for configuring virtual machines for remote recovery</a></li> <li>■ <a href="#">Manage resiliency groups for remote recovery</a></li> </ul>
<b>Advanced features</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Virtual business services</a></li> <li>■ <a href="#">Resiliency plans</a></li> <li>■ <a href="#">Evacuation plans</a></li> </ul>
<b>Perform remote recovery operations</b> 	<p>Once you have organized your assets into resiliency groups, you can perform migrate, takeover, or resync operations on the resiliency groups.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Migrate</a></li> <li>■ <a href="#">Take over</a></li> <li>■ <a href="#">Resync</a></li> </ul>
<b>Monitor assets</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Risks</a></li> <li>■ <a href="#">Reports</a></li> <li>■ <a href="#">Activities</a></li> </ul>

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

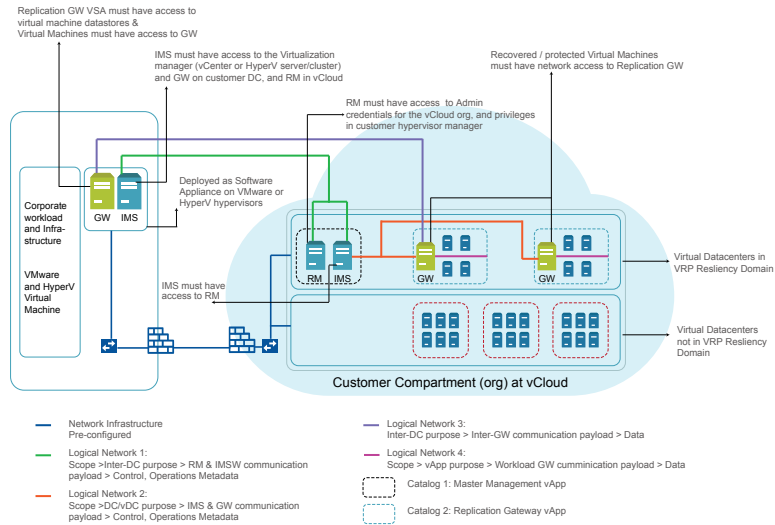
Tasks	More information
<div>Miscellaneous references</div> <div></div>	<div>After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. You can also use klish to update Resiliency Platform components.</div> <div><ul style="list-style-type: none"><li>■ <a href="#">Using klish</a></li><li>■ <a href="#">Troubleshooting</a></li><li>■ <a href="#">Updating</a></li><li>■ <a href="#">References</a></li></ul></div>

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

Using Veritas Resiliency Platform 3.1, you can configure and protect your VMware virtual machines for recovery to vCloud Director using the Resiliency Platform Data Mover without adding the vCenter server.


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

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






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

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

Tasks	More information
<b>Plan your environment</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Overview and Planning Guide</a></li> <li>■ <a href="#">Release Notes</a></li> <li>■ <a href="#">Checklist for deployment and disaster recovery configuration</a></li> </ul>

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

Tasks	More information
<b>Deploy and configure the virtual appliances</b> 	<p>Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in the premises as well as cloud data center.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Download the files required for deployment</a></li> <li>■ <a href="#">About deploying the virtual appliances</a></li> <li>■ 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: <ul style="list-style-type: none"> <li>■ <a href="#">Using vCloud Director</a></li> </ul> </li> <li>■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the on-premises data center: <ul style="list-style-type: none"> <li>■ <a href="#">Using VMware vSphere client</a></li> </ul> </li> <li>■ Configure the virtual appliances as Veritas Resiliency Platform components: <ul style="list-style-type: none"> <li>■ <a href="#">About configuring the virtual appliances</a></li> <li>■ <a href="#">Prerequisites</a></li> <li>■ <a href="#">Configuring Resiliency Manager or IMS</a></li> <li>■ <a href="#">Configuring Replication Gateways</a></li> </ul> </li> </ul>
<b>Set up the resiliency domain</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Create the resiliency domain using getting started wizard</a></li> <li>■ Configure the settings for the resiliency domain: <ul style="list-style-type: none"> <li>■ <a href="#">Add IMS</a></li> <li>■ <a href="#">Add Replication Gateways</a></li> <li>■ <a href="#">Add cloud data center (if not done during getting started wizard)</a></li> <li>■ <a href="#">Manage user authentication and permission</a></li> <li>■ <a href="#">Manage alerts, notifications, and other product settings</a></li> </ul> </li> </ul>
<b>Add asset infrastructure</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Prepare host for replication</a></li> <li>■ <a href="#">Create Replication Gateway pair</a></li> <li>■ <a href="#">Configure PXE Boot server on Replication Gateway</a></li> <li>■ <a href="#">Create network pairs between data centers</a></li> </ul>

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






Tasks	More information
<b>Create resiliency groups</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Prerequisites for configuring virtual machines for remote recovery</a></li> <li>■ <a href="#">Manage resiliency groups for remote recovery</a></li> </ul>
<b>Advanced features</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Virtual business services</a></li> <li>■ <a href="#">Resiliency plans</a></li> <li>■ <a href="#">Evacuation plans</a></li> </ul>
<b>Perform remote recovery operations</b> 	<p>Once you have organized your assets into resiliency groups, you can perform migrate, takeover, or resync operations on the resiliency groups.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Migrate</a></li> <li>■ <a href="#">Take over</a></li> <li>■ <a href="#">Resync</a></li> </ul>
<b>Monitor assets</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Risks</a></li> <li>■ <a href="#">Reports</a></li> <li>■ <a href="#">Activities</a></li> </ul>

Table 1-7

Recovering VMware virtual machines to vCloud Director without adding vCenter server *(continued)*

Tasks	More information
<div>Miscellaneous references</div> <div></div>	<div>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.</div> <div><ul style="list-style-type: none"><li>■ <a href="#">Using klish</a></li><li>■ <a href="#">Troubleshooting</a></li><li>■ <a href="#">Updating</a></li><li>■ <a href="#">References</a></li></ul></div>

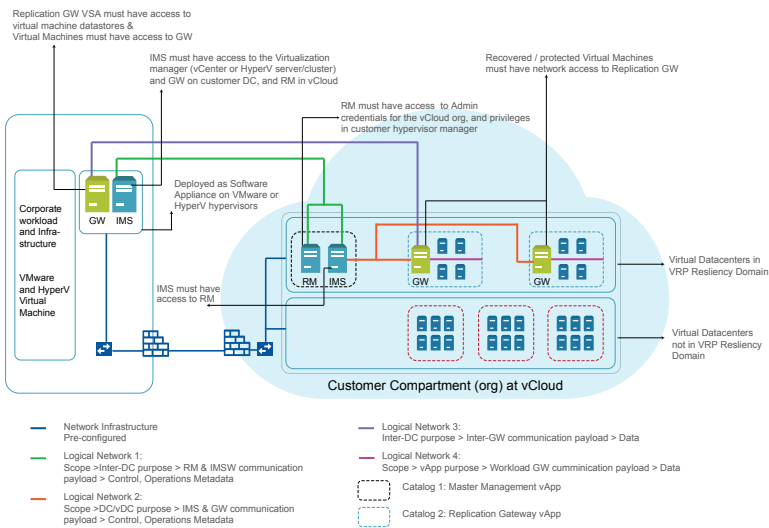
# Recovering Hyper-V virtual machines to vCloud Director without adding Hyper-V server

Using Veritas Resiliency Platform 3.1, you can configure and protect your Hyper-V virtual machines for recovery to vCloud Director using the Resiliency Platform Data Mover without adding Hyper-V server.

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




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






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

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

Tasks	More information
<div>Plan your environment</div> <div></div>	<div>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.</div> <div><ul style="list-style-type: none"><li>Overview and Planning Guide</li><li>Release Notes</li><li>Checklist for deployment and disaster recovery configuration</li></ul></div>

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

Tasks	More information
<b>Deploy and configure the virtual appliances</b> 	<p>Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in the premises as well as cloud data center.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Download the files required for deployment</a></li> <li>■ <a href="#">About deploying the virtual appliances</a></li> <li>■ 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: <ul style="list-style-type: none"> <li>■ <a href="#">Using vCloud Director</a></li> </ul> </li> <li>■ Deploy the virtual appliances for one or more IMS and Replication Gateway in the on-premises data center: <ul style="list-style-type: none"> <li>■ <a href="#">Using Hyper-V Manager</a></li> </ul> </li> <li>■ Configure the virtual appliances as Veritas Resiliency Platform components: <ul style="list-style-type: none"> <li>■ <a href="#">About configuring the virtual appliances</a></li> <li>■ <a href="#">Prerequisites</a></li> <li>■ <a href="#">Configuring Resiliency Manager or IMS</a></li> <li>■ <a href="#">Configuring Replication Gateways</a></li> </ul> </li> </ul>
<b>Set up the resiliency domain</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Create the resiliency domain using getting started wizard</a></li> <li>■ Configure the settings for the resiliency domain: <ul style="list-style-type: none"> <li>■ <a href="#">Add IMS</a></li> <li>■ <a href="#">Add Replication Gateways</a></li> <li>■ <a href="#">Add cloud data center (if not done during getting started wizard)</a></li> <li>■ <a href="#">Manage user authentication and permission</a></li> <li>■ <a href="#">Manage alerts, notifications, and other product settings</a></li> </ul> </li> </ul>
<b>Add asset infrastructure</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Prepare host for replication</a></li> <li>■ <a href="#">Create Replication Gateway pair</a></li> <li>■ <a href="#">Configure PXE Boot server on Replication Gateway</a></li> <li>■ <a href="#">Create network pairs between data centers</a></li> </ul>

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






Tasks	More information
<b>Create resiliency groups</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Prerequisites for configuring virtual machines for remote recovery</a></li> <li>■ <a href="#">Manage resiliency groups for remote recovery</a></li> </ul>
<b>Advanced features</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Virtual business services</a></li> <li>■ <a href="#">Resiliency plans</a></li> <li>■ <a href="#">Evacuation plans</a></li> </ul>
<b>Perform remote recovery operations</b> 	<p>Once you have organized your assets into resiliency groups, you can perform migrate, takeover, or resync operations on the resiliency groups.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Migrate</a></li> <li>■ <a href="#">Take over</a></li> <li>■ <a href="#">Resync</a></li> </ul>
<b>Monitor assets</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Risks</a></li> <li>■ <a href="#">Reports</a></li> <li>■ <a href="#">Activities</a></li> </ul>

Table 1-8

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

Tasks	More information
<div>Miscellaneous references</div> <div></div>	<div>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.</div> <div><ul style="list-style-type: none"><li>■ <a href="#">Using klish</a></li><li>■ <a href="#">Troubleshooting</a></li><li>■ <a href="#">Updating</a></li><li>■ <a href="#">References</a></li></ul></div>

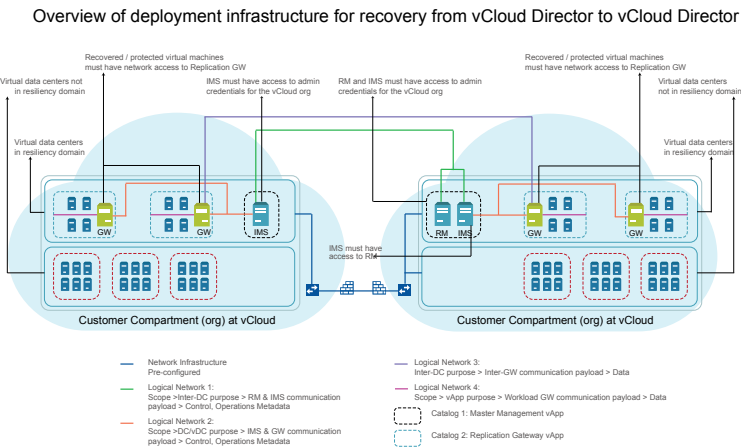
# Recovering virtual machines from vCloud Director to vCloud Director

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

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



Figure 1-9

Overview of deployment infrastructure for recovery from vCloud Director to vCloud Director







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




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

Tasks	More information
<b>Plan your environment</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Overview and Planning Guide</a></li> <li>■ <a href="#">Release Notes</a></li> <li>■ <a href="#">Checklist for deployment and disaster recovery configuration</a></li> </ul>
<b>Deploy and configure the virtual appliances</b> 	<p>Veritas Resiliency Platform is deployed as virtual appliances.</p> <p>Download and deploy the virtual appliances on source as well as on the target cloud data center.</p> <ul style="list-style-type: none"> <li>■ <b>For T-Systems:</b> <ul style="list-style-type: none"> <li>■ <a href="#">Download the files required for deployment</a></li> </ul> </li> <li>■ 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. <ul style="list-style-type: none"> <li>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: <ul style="list-style-type: none"> <li>■ <a href="#">About deploying the virtual appliances</a></li> <li>■ <a href="#">Deploy using vCloud Director</a></li> </ul> </li> </ul> </li> <li>■ Configure the virtual appliances as Veritas Resiliency Platform components: <ul style="list-style-type: none"> <li>■ <a href="#">About configuring the virtual appliances</a></li> <li>■ <a href="#">Prerequisites</a></li> <li>■ <a href="#">Configuring Resiliency Manager or IMS</a></li> <li>■ <a href="#">Configuring Replication Gateways</a></li> </ul> </li> </ul>

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

Tasks	More information
<b>Set up the resiliency domain</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Create the resiliency domain using getting started wizard</a></li> <li>■ Configure the settings for the resiliency domain: <ul style="list-style-type: none"> <li>■ <a href="#">Add IMS</a></li> <li>■ <a href="#">Add Replication Gateways</a></li> <li>■ <a href="#">Add another cloud data center</a></li> <li>■ <a href="#">Manage user authentication and permission</a></li> <li>■ <a href="#">Manage alerts, notifications, and other product settings</a></li> </ul> </li> </ul>
<b>Add asset infrastructure</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Prepare host for replication</a></li> <li>■ <a href="#">Create Replication Gateway pair</a></li> <li>■ <a href="#">Create network pairs between data centers</a></li> </ul>
<b>Create resiliency groups</b>  	<p>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.</p> <p>You can create a resiliency group either for basic monitoring (start or stop virtual machines) or for remote recovery.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Configure resiliency groups for basic monitoring</a></li> <li>■ <a href="#">Prerequisites for configuring virtual machines for recovery from vCloud Director to vCloud Director</a></li> <li>■ <a href="#">Manage resiliency groups for remote recovery</a></li> </ul>
<b>Advanced features</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Virtual business services</a></li> <li>■ <a href="#">Resiliency plans</a></li> <li>■ <a href="#">Evacuation plans</a></li> </ul>

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

Tasks	More information
<b>Perform remote recovery operations</b>  	<p>Once you have organized your assets into resiliency groups, you can perform migrate, takeover, or resync operations on the resiliency groups.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Migrate</a></li> <li>■ <a href="#">Take over</a></li> <li>■ <a href="#">Resync</a></li> </ul> <p>Note that, Rehearsal and Cleanup Rehearsal operations are not supported for recovery from vCloud Director to vCloud Director.</p>
<b>Monitor assets</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Risks</a></li> <li>■ <a href="#">Reports</a></li> <li>■ <a href="#">Activities</a></li> </ul>
<b>Miscellaneous references</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Using klish</a></li> <li>■ <a href="#">Troubleshooting</a></li> <li>■ <a href="#">Updating</a></li> <li>■ <a href="#">References</a></li> </ul>

# Recovery to on-premises data center

This chapter includes the following topics:

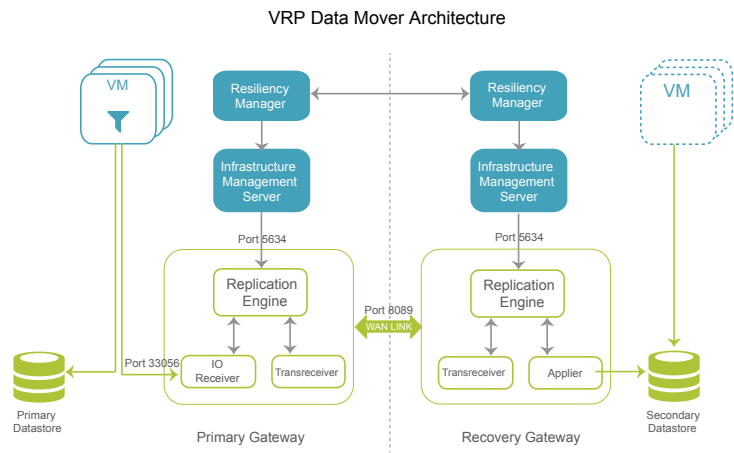
- [Recovering VMware virtual machines to on-premises data center using Resiliency Platform Data Mover](#)
- [Recovering VMware virtual machines using NetBackup](#)
- [Recovering VMware virtual machines using third-party replication technology](#)
- [Recovering Hyper-V virtual machines using third-party replication technology](#)
- [Recovering Applications using third-party replication technology](#)
- [Recovering InfoScale applications](#)

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

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




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






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

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

Tasks	More information
<div>Plan your environment</div> <div></div>	<div>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.</div> <div><ul style="list-style-type: none"><li>■ <a href="#">Overview and Planning Guide</a></li><li>■ <a href="#">Release Notes</a></li><li>■ <a href="#">Checklist for deployment and disaster recovery configuration</a></li></ul></div>

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

Tasks	More information
<b>Deploy and configure the virtual appliances</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Download the files required for deployment</a></li> <li>■ <a href="#">About deploying the virtual appliances</a></li> <li>■ <a href="#">Deploy the virtual appliances using VMware vSphere client</a></li> <li>■ <a href="#">Using VMware vSphere client</a></li> <li>■ Configure the virtual appliances as Veritas Resiliency Platform components: <ul style="list-style-type: none"> <li>■ <a href="#">About configuring the virtual appliances</a></li> <li>■ <a href="#">Prerequisites</a></li> <li>■ <a href="#">Configuring Resiliency Manager or IMS</a></li> <li>■ <a href="#">Configuring Replication Gateways</a></li> </ul> </li> </ul>
<b>Set up the resiliency domain</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Create the resiliency domain using getting started wizard</a></li> <li>■ Configure the settings for the resiliency domain: <ul style="list-style-type: none"> <li>■ <a href="#">Add IMS</a></li> <li>■ <a href="#">Add Replication Gateways</a></li> <li>■ <a href="#">Manage user authentication and permission</a></li> <li>■ <a href="#">Manage alerts, notifications, and other product settings</a></li> </ul> </li> </ul>
<b>Add asset infrastructure</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Add VMware virtualization servers</a></li> <li>■ <a href="#">Create Replication Gateway pair</a></li> <li>■ <a href="#">Add and map network objects</a> (Optional)</li> <li>■ <a href="#">Create network pairs between data centers</a> (Optional)</li> </ul>

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






Tasks	More information
<b>Create resiliency groups</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>For basic monitoring: <a href="#">Configure resiliency groups for monitoring</a></li> <li>For recovery to remote data center: <ul style="list-style-type: none"> <li><a href="#">Prepare cluster for replication</a></li> <li><a href="#">Prerequisites for configuring VMware virtual machines for recovery to on-premises data center</a></li> <li><a href="#">Configure VMware virtual machines for recovery to on-premises data center</a></li> </ul> </li> </ul>
<b>Advanced features</b> 	<p>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.</p> <ul style="list-style-type: none"> <li><a href="#">Virtual business services</a></li> <li><a href="#">Resiliency plans</a></li> <li><a href="#">Evacuation plans</a></li> </ul>
<b>Perform remote recovery operations</b> 	<p>Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups.</p> <ul style="list-style-type: none"> <li><a href="#">Rehearsal</a></li> <li><a href="#">Cleanup rehearsal</a></li> <li><a href="#">Migrate</a></li> <li><a href="#">Take over</a></li> <li><a href="#">Resync</a></li> </ul>
<b>Monitor assets</b> 	<p>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.</p> <ul style="list-style-type: none"> <li><a href="#">Risks</a></li> <li><a href="#">Reports</a></li> <li><a href="#">Activities</a></li> </ul>

Table 2-1

Recovering VMware virtual machines to on-premises data center using Resiliency Platform Data Mover *(continued)*

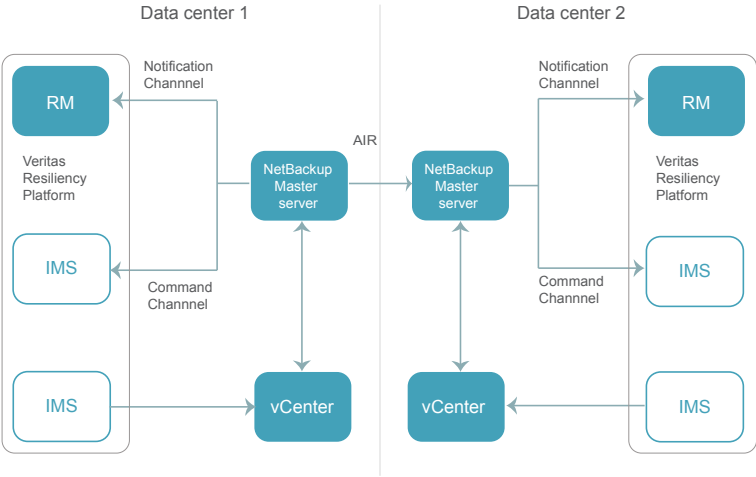
Tasks	More information
<div>Miscellaneous references</div> <div></div>	<div>After the virtual appliances are deployed and configured, you are given limited menu-based access to the operating system and the product. You need to use klish menu to manage the configuration-related changes to the product and to troubleshoot. You can also use klish to update Resiliency Platform components.</div> <div><ul style="list-style-type: none"><li>■ <a href="#">Using klish</a></li><li>■ <a href="#">Troubleshooting</a></li><li>■ <a href="#">Updating</a></li><li>■ <a href="#">References</a></li></ul></div>

# Recovering VMware virtual machines using NetBackup

Using the Veritas Resiliency Platform 3.1, you can restore VMware virtual machine from NetBackup generated backup images to the recovery data center. For more information on NetBackup and NetBackup Appliances, see [About NetBackup and NetBackup Appliances](#).

Figure 2-2




Deployment architecture for NetBackup master server







In the image, data center 1 is the production data center and data center 2 is recovery data center. Targeted Auto Image Replication, denoted as AIR in the below image, ensures that the backup images are available on NetBackup master server in the recovery data center. The image shows two Infrastructure Management Servers (IMS) although you can have only one IMS which discovers the vCenter and is also added as an additional server to NetBackup.

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



**Table 2-2** Recovering virtual machines using NetBackup images

Tasks	More information
<b>Plan your environment</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Overview and Planning Guide</a></li> <li>■ <a href="#">Release Notes</a></li> <li>■ <a href="#">Checklist for deployment and disaster recovery configuration</a></li> </ul>
<b>Deploy and configure the virtual appliances</b> 	<p>Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances for Resiliency Manager and IMS in both the data centers.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Download the files required for deployment</a></li> <li>■ <a href="#">About deploying the virtual appliances</a></li> <li>■ <a href="#">Deploy the virtual appliances using VMware vSphere client</a></li> <li>■ Configure the virtual appliances as Veritas Resiliency Platform components: <ul style="list-style-type: none"> <li>■ <a href="#">About configuring the virtual appliances</a></li> <li>■ <a href="#">Prerequisites</a></li> <li>■ <a href="#">Configuring Resiliency Manager or IMS</a></li> </ul> </li> </ul>
<b>Set up the resiliency domain</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Create the resiliency domain using getting started wizard</a></li> <li>■ Configure the settings for the resiliency domain: <ul style="list-style-type: none"> <li>■ <a href="#">Add IMS</a></li> <li>■ <a href="#">Manage user authentication and permission</a></li> <li>■ <a href="#">Manage alerts, notifications, and other product settings</a></li> </ul> </li> </ul>

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

Tasks	More information
<b>Add asset infrastructure</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Add VMware servers</a></li> <li>■ <a href="#">Add NetBackup master server</a></li> <li>■ <a href="#">Add IMS to NetBackup master server as an additional server</a></li> <li>■ <a href="#">Add and map network objects</a> (Optional)</li> <li>■ <a href="#">Create network pairs between data centers</a> (Optional)</li> </ul>
<b>Create resiliency groups</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Configure resiliency groups for basic monitoring</a></li> <li>■ <a href="#">Prerequisites for configuring VMware virtual machines for recovery using NetBackup images</a></li> <li>■ <a href="#">Manage VMware virtual machines for remote recovery using NetBackup images</a></li> </ul>
<b>Advanced features</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Virtual business services</a></li> <li>■ <a href="#">Resiliency plans</a></li> <li>■ <a href="#">Evacuation plans</a></li> </ul>
<b>Perform recovery operations</b> 	<p>Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform restore (local or remote) operations on the resiliency groups.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Rehearsal</a></li> <li>■ <a href="#">Cleanup rehearsal</a></li> <li>■ <a href="#">Restore virtual machines</a></li> </ul>

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

Tasks	More information
<b>Monitor assets</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Risks</a></li> <li>■ <a href="#">Reports</a></li> <li>■ <a href="#">Activities</a></li> </ul>
<b>Miscellaneous references</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Using klish</a></li> <li>■ <a href="#">Troubleshooting</a></li> <li>■ <a href="#">Updating</a></li> <li>■ <a href="#">References</a></li> </ul>





## Recovering VMware virtual machines using third-party replication technology

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

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





- EMC SRDF
- EMC Recoverpoint
- Netapp (cDOT) Snapmirror
- HP 3PAR Remote Copy
- Hitachi TrueCopy/HUR
- IBM SVC Global Mirror
- IBM XIV Remote Mirror

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


Tasks	More information
<b>Plan your environment</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Overview and Planning Guide</a></li> <li>■ <a href="#">Release Notes</a></li> <li>■ <a href="#">Checklist for deployment and disaster recovery configuration</a></li> </ul>
<b>Deploy and configure the virtual appliances</b> 	<p>Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances for Resiliency Manager and IMS in both the data centers.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Download the files required for deployment</a></li> <li>■ <a href="#">About deploying the virtual appliances</a></li> <li>■ <a href="#">Deploy the virtual appliances using VMware vSphere client</a></li> <li>■ Configure the virtual appliances as Veritas Resiliency Platform components: <ul style="list-style-type: none"> <li>■ <a href="#">About configuring the virtual appliances</a></li> <li>■ <a href="#">Prerequisites</a></li> <li>■ <a href="#">Configuring Resiliency Manager or IMS</a></li> </ul> </li> </ul>
<b>Set up the resiliency domain</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Create the resiliency domain using getting started wizard</a></li> <li>■ Configure the settings for the resiliency domain: <ul style="list-style-type: none"> <li>■ <a href="#">Add IMS</a></li> <li>■ <a href="#">Manage user authentication and permission</a></li> <li>■ <a href="#">Manage alerts, notifications, and other product settings</a></li> </ul> </li> </ul>
<b>Add asset infrastructure</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Add VMware virtualization servers</a></li> <li>■ <a href="#">Add enclosures</a></li> <li>■ <a href="#">Add and map network objects</a> (Optional)</li> <li>■ <a href="#">Create network pairs between data centers</a> (Optional)</li> </ul>



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

Tasks	More information
<b>Create resiliency groups</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Configure resiliency groups for basic monitoring</a></li> <li>■ <a href="#">Preparing virtual machines for recovery using array-based replication</a></li> <li>■ <a href="#">Manage resiliency groups for remote recovery</a></li> </ul>
<b>Advanced features</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Virtual business services</a></li> <li>■ <a href="#">Resiliency plans</a></li> <li>■ <a href="#">Evacuation plans</a></li> </ul>
<b>Perform remote recovery operations</b> 	<p>Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Rehearsal</a></li> <li>■ <a href="#">Cleanup rehearsal</a></li> <li>■ <a href="#">Migrate</a></li> <li>■ <a href="#">Take over</a></li> <li>■ <a href="#">Resync</a></li> </ul>
<b>Monitor assets</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Risks</a></li> <li>■ <a href="#">Reports</a></li> <li>■ <a href="#">Activities</a></li> </ul>

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

Tasks	More information
<b>Miscellaneous references</b> <div>  </div>	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Using klish</a></li> <li>■ <a href="#">Troubleshooting</a></li> <li>■ <a href="#">Updating</a></li> <li>■ <a href="#">References</a></li> </ul>





# Recovering Hyper-V virtual machines using third-party replication technology

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





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

- Hyper-V Replica
- EMC SRDF
- EMC Recoverpoint
- Netapp (cDOT) Snapmirror
- HP 3PAR Remote Copy
- Hitachi TrueCopy/HUR
- IBM SVC Global Mirror
- IBM XIV Remote Mirror


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

Tasks	More information
<b>Plan your environment</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Overview and Planning Guide</a></li> <li>■ <a href="#">Release Notes</a></li> <li>■ <a href="#">Checklist for deployment and disaster recovery configuration</a></li> </ul>
<b>Deploy and configure the virtual appliances</b> 	<p>Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in both the data centers.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Download the files required for deployment</a></li> <li>■ <a href="#">About deploying the virtual appliances</a></li> <li>■ Deploy the virtual appliances for Resiliency Manager and Infrastructure Management Server (IMS) <ul style="list-style-type: none"> <li>■ <a href="#">Using VMware vSphere client</a></li> <li>■ <a href="#">Using Hyper-V Manager</a></li> </ul> </li> <li>■ Configure the virtual appliances as Veritas Resiliency Platform components: <ul style="list-style-type: none"> <li>■ <a href="#">About configuring the virtual appliances</a></li> <li>■ <a href="#">Prerequisites</a></li> <li>■ <a href="#">Configuring Resiliency Manager or IMS</a></li> </ul> </li> </ul>
<b>Set up the resiliency domain</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Create the resiliency domain using getting started wizard</a></li> <li>■ Configure the settings for the resiliency domain: <ul style="list-style-type: none"> <li>■ <a href="#">Add IMS</a></li> <li>■ <a href="#">Manage user authentication and permission</a></li> <li>■ <a href="#">Manage alerts, notifications, and other product settings</a></li> </ul> </li> </ul>
<b>Add asset infrastructure</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Add Hyper-V servers</a></li> <li>■ <a href="#">Add enclosures</a></li> <li>■ <a href="#">Add and map network objects</a> (Optional)</li> <li>■ <a href="#">Create network pairs between data centers</a> (Optional)</li> </ul>

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

Tasks	More information
<b>Create resiliency groups</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Configure resiliency groups for basic monitoring</a></li> <li>■ <a href="#">Preparing virtual machines for recovery using array-based replication</a></li> <li>■ <a href="#">Manage resiliency groups for remote recovery</a></li> </ul>
<b>Advanced features</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Virtual business services</a></li> <li>■ <a href="#">Resiliency plans</a></li> <li>■ <a href="#">Evacuation plans</a></li> </ul>
<b>Perform remote recovery operations</b> 	<p>Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Rehearsal</a></li> <li>■ <a href="#">Cleanup rehearsal</a></li> <li>■ <a href="#">Migrate</a></li> <li>■ <a href="#">Take over</a></li> <li>■ <a href="#">Resync</a></li> </ul>
<b>Monitor assets</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Risks</a></li> <li>■ <a href="#">Reports</a></li> <li>■ <a href="#">Activities</a></li> </ul>

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

Tasks	More information
<b>Miscellaneous references</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Using klish</a></li><li>■ <a href="#">Troubleshooting</a></li><li>■ <a href="#">Updating</a></li><li>■ <a href="#">References</a></li></ul>


## Recovering Applications using third-party replication technology

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




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

- EMC SRDF
- EMC Recoverpoint
- Netapp (cDOT) Snapmirror
- HP 3PAR Remote Copy
- Hitachi TrueCopy/HUR

**Table 2-5** Recovering applications using third-party replication technology

Tasks	More information
<b>Plan your environment</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Overview and Planning Guide</a></li><li>■ <a href="#">Release Notes</a></li><li>■ <a href="#">Checklist for deployment and disaster recovery configuration</a></li></ul>

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

Tasks	More information
<b>Deploy and configure the virtual appliances</b>  	<p>Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances in both the data centers.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Download the files required for deployment</a></li> <li>■ <a href="#">About deploying the virtual appliances</a></li> <li>■ Deploy the virtual appliances for Resiliency Manager and Infrastructure Management Server (IMS) <ul style="list-style-type: none"> <li>■ <a href="#">Using VMware vSphere client</a></li> <li>■ <a href="#">Using Hyper-V Manager</a></li> </ul> </li> <li>■ Configure the virtual appliances as Veritas Resiliency Platform components: <ul style="list-style-type: none"> <li>■ <a href="#">About configuring the virtual appliances</a></li> <li>■ <a href="#">Prerequisites</a></li> <li>■ <a href="#">Configuring Resiliency Manager or IMS</a></li> </ul> </li> </ul>
<b>Set up the resiliency domain</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Create the resiliency domain using getting started wizard</a></li> <li>■ Configure the settings for the resiliency domain: <ul style="list-style-type: none"> <li>■ <a href="#">Add IMS</a></li> <li>■ <a href="#">Manage user authentication and permission</a></li> <li>■ <a href="#">Manage alerts, notifications, and other product settings</a></li> </ul> </li> </ul>
<b>Add asset infrastructure</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ Add virtualization servers: <ul style="list-style-type: none"> <li>■ <a href="#">VMware virtualization servers</a></li> <li>■ <a href="#">Hyper-V servers</a></li> </ul> </li> <li>■ <a href="#">Add host assets</a></li> <li>■ <a href="#">Add enclosures</a></li> <li>■ <a href="#">Add and map network objects</a> (Optional)</li> <li>■ <a href="#">Create network pairs between data centers</a> (Optional)</li> </ul>

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






Tasks	More information
<b>Create resiliency groups</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Managing applications</a></li> <li>■ <a href="#">Configure resiliency groups for basic monitoring</a></li> <li>■ <a href="#">Prerequisites for configuring applications for remote recovery</a></li> <li>■ <a href="#">Manage applications for remote recovery</a></li> </ul>
<b>Advanced features</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Virtual business services</a></li> <li>■ <a href="#">Resiliency plans</a></li> <li>■ <a href="#">Evacuation plans</a></li> </ul>
<b>Perform remote recovery operations</b> 	<p>Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Rehearsal</a></li> <li>■ <a href="#">Cleanup rehearsal</a></li> <li>■ <a href="#">Migrate</a></li> <li>■ <a href="#">Take over</a></li> <li>■ <a href="#">Resync</a></li> </ul>
<b>Monitor assets</b> 	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Risks</a></li> <li>■ <a href="#">Reports</a></li> <li>■ <a href="#">Activities</a></li> </ul>

Table 2-5

Recovering applications using third-party replication technology

(continued)

Tasks	More information
<div>Miscellaneous references</div> <div></div>	<div>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.</div> <div><ul style="list-style-type: none"><li>■ <a href="#">Using klish</a></li><li>■ <a href="#">Troubleshooting</a></li><li>■ <a href="#">Updating</a></li><li>■ <a href="#">References</a></li></ul></div>

## Recovering InfoScale applications

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

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

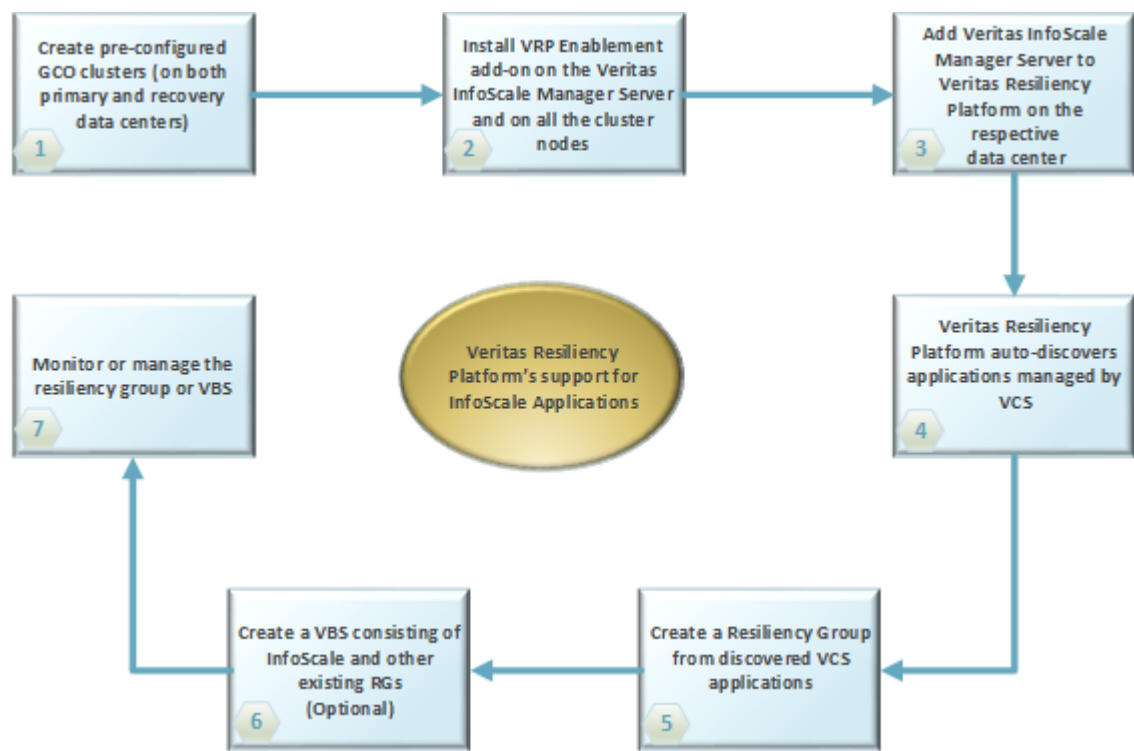
The InfoScale applications are automatically discovered in the Resiliency Platform when the Veritas InfoScale Operations Manager server is added to the resiliency domain. Veritas InfoScale Operations Manager users must download and install Veritas Resiliency Platform Enablement add-on to automatically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

A typical workflow of Veritas Resiliency Platform for InfoScale applications consists of a Veritas InfoScale Operation Manager server reporting to a Resiliency Manager. The InfoScale applications should be already configured in Veritas InfoScale Operations Management server. You can group the InfoScale applications into resiliency groups or VBSs to recover, monitor, visualize, and generate reports about these applications in the Resiliency Platform.


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







**Figure 2-3** A typical workflow for recovering managed InfoScale applications






**Table 2-6** Recovering InfoScale applications

Tasks	More information
<div>Plan your environment</div> <div></div>	<div>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.</div> <div><ul style="list-style-type: none"><li>■ <a href="#">Overview and Planning Guide</a></li><li>■ <a href="#">Release Notes</a></li><li>■ <a href="#">Checklist for deployment and disaster recovery configuration</a></li></ul></div>

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

Tasks	More information
<b>Deploy and configure the virtual appliances</b>  	<p>Veritas Resiliency Platform is deployed as virtual appliances. Download and deploy the virtual appliances for Resiliency Manager and IMS in both the data centers.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Download the files required for deployment</a></li> <li>■ <a href="#">About deploying the virtual appliances</a></li> <li>■ Deploy the virtual appliances for Resiliency Manager and Infrastructure Management Server (IMS) <ul style="list-style-type: none"> <li>■ <a href="#">Using VMware vSphere client</a></li> <li>■ <a href="#">Using Hyper-V Manager</a></li> </ul> </li> <li>■ <a href="#">About configuring the virtual appliances</a></li> <li>■ <a href="#">Prerequisites</a></li> <li>■ <a href="#">Configuring Resiliency Manager or IMS</a></li> </ul>
<b>Set up the resiliency domain</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Create the resiliency domain using getting started wizard</a></li> <li>■ Configure the settings for the resiliency domain: <ul style="list-style-type: none"> <li>■ <a href="#">Add InfoScale Operations Manager server</a></li> <li>■ <a href="#">Manage user authentication and permission</a></li> <li>■ <a href="#">Manage alerts, notifications, and other product settings</a></li> </ul> </li> </ul>
<b>Create resiliency groups</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Configure resiliency groups for basic monitoring</a></li> <li>■ <a href="#">Prerequisites for configuring InfoScale applications for remote recovery</a></li> <li>■ <a href="#">Manage applications for remote recovery</a></li> </ul>
<b>Advanced features</b>  	<p>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.</p> <ul style="list-style-type: none"> <li>■ <a href="#">Virtual business services</a></li> <li>■ <a href="#">Resiliency plans</a></li> <li>■ <a href="#">Evacuation plans</a></li> </ul>

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

Tasks	More information
<b>Perform remote recovery operations</b> 	<p>Once you have configured the resiliency groups for remote recovery, you can perform rehearsal and cleanup rehearsal operations on the resiliency groups. You can also perform migrate, takeover, or resync operations on the resiliency groups.</p> <ul style="list-style-type: none"><li>■ <a href="#">Rehearsal</a></li><li>■ <a href="#">Cleanup rehearsal</a></li><li>■ <a href="#">Migrate</a></li><li>■ <a href="#">Take over</a></li><li>■ <a href="#">Resync</a></li></ul>
<b>Monitor assets</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Risks</a></li><li>■ <a href="#">Reports</a></li><li>■ <a href="#">Activities</a></li></ul>
<b>Miscellaneous references</b> 	<p>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.</p> <ul style="list-style-type: none"><li>■ <a href="#">Using klish</a></li><li>■ <a href="#">Troubleshooting</a></li><li>■ <a href="#">Updating</a></li><li>■ <a href="#">References</a></li></ul>

# Index

## F

from vCloud Director to vCloud Director 36

## R

recover applications

    using third-party replication technology 53

recover Hyper-V

    to AWS 9

    to Azure 17

    to vCloud Director 24

    to vCloud Director without adding Hyper-V  
        server 32

    using third-party replication technology 50

recover InfoScale applications 56

recover virtual machines

    to vCloud Director 36

recover VMware

    to AWS 5

    to Azure 13

    to on-premises data center using Resiliency  
        Platform Data Mover 40

    to vCloud Director 20

    to vCloud Director without adding vCenter  
        server 28

    using NetBackup images 44

    using third-party replication technology 47