

Veritas™ Resiliency Platform 2.1 Release Notes

Veritas Resiliency Platform: Release Notes

Last updated: 2017-03-16

Document version: Document version: 2.1 Rev 1

Legal Notice

Copyright © 2017 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/about/legal/license-agreements>

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

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

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

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

<http://www.veritas.com>

Technical Support

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

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

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

<https://my.veritas.com>

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

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

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

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

Documentation feedback

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

doc.feedback@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1	Overview	8
	About Veritas Resiliency Platform	8
	About Resiliency Platform features and components	9
	New features and changes in Veritas Resiliency Platform 2.1	11
	Recovery of assets in Amazon Web Services (AWS)	11
	Integration with NetBackup and NetBackup Appliances	11
	Asymmetric pairing of Replication Gateways	11
	Virtual appliance for YUM repository	12
	CLISH changed to klish	12
	Version 2.1.0.100 supports IBM SVC and XIV replication technologies	12
	What is not supported?	12
	Using the product documentation	13
Chapter 2	System requirements	15
	Supported hypervisors for deploying Resiliency Platform virtual appliance	15
	System resource requirements for Resiliency Platform	16
	Network and firewall requirements	17
Chapter 3	Fixed issues	20
	Fixed issues	20
Chapter 4	Known issues	21
	Disaster recovery (DR) configuration for resiliency group fails if Microsoft Hyper-V Replica is configured after you add a virtual machine in Resiliency Platform	23
	In the VM Inventory report, instead of allocated memory, Resiliency Platform shows the total memory of the virtual machines	23
	Certain validations do not work while creating a resiliency group of applications (3721289)	23
	Rehearsal does not work after being aborted	24
	The configure DR operation fails if virtual machines in the resiliency group belong to different servers	24

For resiliency groups containing VMware virtual machines with NFS datastore mounted from a NetApp volume with substring vol, Migrate or takeover operations may fail	24
The license expiry status is inconsistent on Resiliency Managers configured on different time zones	24
In the Hyper-V guest environment, the writable disk is shown in the Read-Only state (3785911)	25
Long SRDF device group names are not discovered (3786826)	25
Multiple repository paths on the same host are not allowed for the repository server (3734149)	25
Unknown state displayed for the Resiliency groups of dark sites that are part of VBS (3794650)	25
An Oracle custom application is not discovered if the instance names do not match (3796579)	25
VBS DR operations fail when an application resiliency group with unconfigured DR is added in VBS (3794105)	26
Expired resiliency plan cannot be executed even after editing the schedule (3861955)	26
Resiliency groups for Hitachi enclosures are not displayed on dashboard under Top RG by replication lag chart (3861173)	26
Snapshot disk is read only after rehearse operation is performed in Hyper-V with SRDF replication (3862088)	26
Static IP customization may not work under certain conditions (3862916, 3862237)	27
Need to manually refresh all assets after a site recovery (3861929)	27
Disk utilization risk not resolved after DR operations	27
Migrate operation becomes unresponsive if the operation is initiated from an unavailable site (3862253)	28
Remote cluster group dependencies not validated before migrate (3863082)	28
VBS migrate operation cannot be performed after failure (3862124)	28
Resiliency group state does not get updated when production site is down (3863081)	28
Replication information error (5170)	29
DNS customization does not work if FQDN is not defined (5037)	29
Some versions of VMware Tools are not supported (4969)	29
Refresh operation for EMC SRDF enclosure does not work (7709)	29
Remove DNS operation fails if DNS customization done by editing resiliency group (7704)	29
Login to the Resiliency Manager console fails at times	30

VLAN pairing for distributed port group gets deleted after upgrade (7717) 30

Known issues: Resiliency Platform Data Mover 30

 Virtual Machine protection using Data Mover has a few policy related limitations (5181) 30

 lofilter bundle not removed from ESX hosts even after unconfiguring virtual machines (5178) 31

 Storage policy needs to be manually removed after all the virtual machines are unconfigured (5180) 31

 VMDK and VMX files need to be in the same folder(5167) 31

 Edit resiliency group operation may fail after rehearsal or cleanup rehearsal (5092) 31

 Replication gets paused if you perform add disk operation (5182) 31

 Cannot perform any operation after deleting disk from virtual machine (5182) 32

 Data Mover virtual machine in no op mode risk cannot be resolved (5183) 32

 Risks not generated after taking snapshot of virtual machine replicated using Data Mover(6886) 32

Known issues: Recovery to Amazon Web services (AWS) 32

 Some DHCP enabled NICs are not present on Cloud after migrate (7407) 32

 One or more NICs of a migrated Windows virtual machine may not be visible (7718) 33

 Cloud IPs get added to on-premise NICs after migrate back to the on-premise site and reboot (7713) 33

 Migrate or takeover operations fail at the Add Network for AWS task and Create Network Interface sub-task (7719) 33

 Sometimes network comes up on only one NIC although there are multiple NICs (8232) 34

Known issues: NetBackup integration 34

 MAC address starting with 00:0c:29 not supported for VMware virtual machines (7103) 34

 A virtual machine backed up by multiple NBU master servers gets mapped with only one master server in the console (7608) 34

 A transient virtual machine remains in the ESX server in one scenario (7413) 35

Chapter 5	Limitations	36
	Rehearsal is not supported if volume is configured using asynchronous replication in IBM XIV enclosure	36
Appendix A	Virtual appliance security features	37
	Operating system security	37
	Management Security	37
	Network security	38
	Access control security	38
	Physical security	38

Overview

This chapter includes the following topics:

- [About Veritas Resiliency Platform](#)
- [About Resiliency Platform features and components](#)
- [New features and changes in Veritas Resiliency Platform 2.1](#)
- [What is not supported?](#)
- [Using the product documentation](#)

About Veritas Resiliency Platform

Veritas Resiliency Platform offers a unified solution that helps you proactively maintain business uptime across private, public, and hybrid clouds. Resiliency Platform gives you complete automation for all resiliency operations involving the virtual machines, applications, and multi-tier business-services in your data center. It safeguards the current technology investments by plugging into your existing environments and infrastructure.

For data replication, you can use the Veritas Data Mover or any third-party solution that is supported by Veritas Resiliency Platform. For a list of supported vendors and products, see *Veritas Resiliency Platform Hardware and Software Compatibility Guide*.

Resiliency Platform has the following core capabilities:

Security and Compliance	Veritas Resiliency Platform provides enhanced data encryption (for data-in-flight and data-at-rest) as well as choice of data residency.
-------------------------	-------------------------------------------------------------------------------------------------------------------------------------------

Predictability	Customers can predictably meet critical business Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
Compliance	Customers can prove compliance to internal and external business continuity mandates with audit reporting and non-disruptive, real-time disaster recovery testing.
Automation	Customers get complete automation for all resiliency operations including recovery run books, and start and stop recovery orchestration for multi-tier applications. This reduces risk of downtime from human error.
Flexibility	Customers get the flexibility to keep their existing infrastructures and can innovate on their terms, with the flexibility that Resiliency Platform provides, to enable workload migration across sites and even to the cloud.

See [“About Resiliency Platform features and components”](#) on page 9.

About Resiliency Platform features and components

The following is a brief introduction to Veritas Resiliency Platform key components and their relationships. Administrators responsible for deploying and configuring the product need to understand these in more detail.

resiliency domain	The logical scope of a Resiliency Platform deployment. It can extend across multiple data centers.
Resiliency Manager	The component that provides resiliency capabilities within a resiliency domain. It is composed of loosely coupled services, a distributed data repository, and a management console. The Resiliency Manager is deployed as a virtual appliance.
Infrastructure Management Server (IMS)	The component that discovers, monitors, and manages the asset infrastructure within a data center. The IMS transmits information about the asset infrastructure to the Resiliency Manager. The IMS is deployed as a virtual appliance. To achieve scale, multiple IMSs can be deployed in the same data center.

Veritas InfoScale Operations Manager Management Server	<p>The component that allows discovery of InfoScale applications that are already configured in Veritas InfoScale Operations Manager. Also referred to as Veritas InfoScale Operations Manager server.</p> <p>You can manage the InfoScale applications that are already configured in Veritas InfoScale Operations Manager on Linux, Solaris, AIX as well as Windows platform.</p>
Replication Gateway	<p>The component of Veritas Resiliency Platform Data Mover that is deployed as a virtual appliance on both data centers and used to perform replication between the data centers.</p>
data center	<p>For a disaster recovery use case, the resiliency domain must contain at least two data centers in different locations, a production data center and recovery data center. Each data center has a Resiliency Manager and one or more IMSs.</p>
asset infrastructure	<p>The data center assets that you add to Resiliency Platform for discovery and monitoring by the IMS.</p> <p>The asset infrastructure can include hosts (Windows or Linux servers), virtualization servers for Hyper-V and VMware, and enclosures (storage arrays). Once the asset infrastructure is discovered by the IMS, the discovered virtual machines or applications are listed in the console as assets to manage or protect.</p>
resiliency group	<p>The unit of management and control in Resiliency Platform. You organize related assets into a resiliency group and manage and monitor them as a single entity.</p>
service objective	<p>A template to define the type of operations and technologies that are supported for a group of assets. You apply a service objective to each resiliency group.</p> <p>A template which identifies the characteristics of a service. These could be availability related characteristics such as local redundancy, and number of nodes in a cluster or DR characteristics such as remote recovery, Recovery Point Objective (RPO) SLAs, rehearsal support etc. Service objective is applied when a group of assets are being added to a resiliency group.</p> <p>Resiliency Platform monitors the resiliency groups based on the service objective definition and raises the risks as applicable.</p>

Virtual Business Service (VBS)

A multi-tier business service where each VBS tier hosts one or more resiliency groups. A VBS lets you group multiple services as a single unit for visualization, automation, and controlled start and stop in the desired order. VBS uses the vertical grouping mechanism to group the multiple services. You can also perform operations such as migrate, takeover, resync, rehearsal on the entire VBS.

For more information on the above components, refer to the Deployment Guide.

New features and changes in Veritas Resiliency Platform 2.1

This release of Veritas Resiliency Platform includes the following new features, changes, and enhancements.

Recovery of assets in Amazon Web Services (AWS)

Veritas Resiliency Platform 2.1 introduces the support for recovery of the data center assets to AWS. You can configure and protect your VMware and Hyper-V virtual machines for recovery to AWS using the Resiliency Platform Data Mover. You will need one license for Veritas Resiliency Platform and one license for Resiliency Platform Data Mover.

You can use Resiliency Platform to seamlessly move your single-tiered or multi-tiered workloads between on-premises data center and AWS. Resiliency Platform provides controlled recovery options for the recovery of your on-premises workload to AWS.

Integration with NetBackup and NetBackup Appliances

NetBackup and NetBackup Appliances can be integrated with Veritas Resiliency Platform 2.1. The integrations lets you configure the VMware virtual machines for remote recovery by applying the service objective for copy based recovery. The Restore operation lets you choose the backup image and restore the virtual machines on the recovery data center.

NetBackup version 8.0 and NetBackup Appliances (5200 or 5300 Series) version 3.0 are supported.

Asymmetric pairing of Replication Gateways

Starting from version 2.1, Resiliency Platform supports the asymmetric pairing of Replication Gateways. This feature facilitates deployment of only the required

number of gateways on each side, based on the data transfer rate and technology specific limits.

One Gateway on production site can be paired with multiple Gateways on recovery site and vice versa. One gateway can be paired with up to 16 gateways on the peer site.

Virtual appliance for YUM repository

Veritas Resiliency Platform 2.1 introduces the use of a virtual appliance as a YUM server. This feature of Resiliency Platform makes it easier to setup a YUM server. If you do not use the YUM virtual appliance, you will be required to manually install all the required perl modules to setup the repository server.

The YUM server virtual appliance is available in VHD and OVA formats.

CLISH changed to klish

The command line interface shell used for logging in to the Veritas Resiliency Platform virtual appliances has changed from CLISH to klish. klish is an improved version of CLISH with better support and enhancements. All the commands and options available with CLISH are now available with klish.

Version 2.1.0.100 supports IBM SVC and XIV replication technologies

Veritas Resiliency Platform version 2.1.0.100 supports remote recovery of VMware and Hyper-V virtual machines using the following replication technologies:

- IBM SVC Global Mirror
- IBM XIV Remote Mirror

For the updated list of virtual appliances file names, refer to *Deployment Guide*.

What is not supported?

Veritas Resiliency Platform does not support the following features:

- In case of recovery to AWS, takeover operation from cloud data center to on-premise data center.
- In case of recovery to AWS, any volume other than simple volume.
- Executing a custom script on a host that is not actively reporting to Resiliency Platform environment through Infrastructure Management Server (IMS) or Infoscale Operations Manager Management Server.

- Database user authentication for Oracle applications.
- Rehearse and cleanup rehearsal operations for applications on Microsoft Failover Cluster.
- Rehearse and cleanup rehearsal operations for applications inside virtual machines having data on raw disks mapped to virtual machines and data replicated through 3PAR RemoteCopy or NetApp SnapMirror through fibre channel.
- Configuring resiliency group for remote recovery using Data Mover fails if a virtual machine has snapshots. Remove all snapshots before proceeding with the operation.
- VMware fault tolerant virtual machines.
- Raw device mapping (RDM) is not supported for virtual machine disaster recovery using Resiliency Platform Data Mover.

Array-based replication does not support the following:

- Raw device mapping (RDM) mapped replicated LUNs are not supported for virtual machine disaster recovery.
- Combination of replicated and non-replicated storage to virtual machines is not supported.
- Combination of storage from multiple array technologies is not supported.

Using the product documentation

[Table 1-1](#) lists the URLs for Veritas Resiliency Platform documentation and [Table 1-2](#) lists the Veritas Resiliency Platform guides.

Table 1-1 URLs for Veritas Resiliency Platform documentation

URL	Description
https://sort.veritas.com/documents	The latest version of the product documentation: Product guides in PDF format and HTML format. Online help portal. The help content is also available from the product console.
https://www.veritas.com/community/business-continuity/videos	The list of Resiliency Platform videos.
http://www.veritas.com/docs/000116615	The late breaking news that is related to this release.

Table 1-2 Names of Veritas Resiliency Platform guides

Title	Description
<i>Veritas Resiliency Platform Getting Started Guide</i>	An overview of processes of deployment, configuration, and disaster recovery in Resiliency Platform.
<i>Veritas Resiliency Platform Hardware and Software Compatibility List (HSCL)</i>	The list of hardware and software compatibility.
<i>Veritas Resiliency Platform Release Notes</i>	The release information such as main features, known issues, and limitations.
<i>Veritas Resiliency Platform: Deployment Guide</i> <i>Veritas Resiliency Platform: Solutions for Applications</i> <i>Veritas Resiliency Platform: Solutions for Microsoft Hyper-V</i> <i>Veritas Resiliency Platform: Solutions for VMware</i> <i>Veritas Resiliency Platform: Solutions for Virtual Business Services</i> <i>Veritas Resiliency Platform: Application Enablement SDK</i>	The information about deploying Resiliency Platform and using the solutions.
<i>Veritas Resiliency Platform Third-Party Software License Agreements</i>	The information about the third-party software that is used in Resiliency Platform.

System requirements

This chapter includes the following topics:

- [Supported hypervisors for deploying Resiliency Platform virtual appliance](#)
- [System resource requirements for Resiliency Platform](#)
- [Network and firewall requirements](#)

Supported hypervisors for deploying Resiliency Platform virtual appliance

This section lists the hypervisor versions that are supported for Resiliency Platform virtual appliance.

Microsoft Hyper-V:

- Windows Server 2012 with Hyper-V
- Windows Server 2012 R2 with Hyper-V

VMware:

- ESXi 5.1, 5.5, 6.0
- vCenter Server 5.1, 5.5, 6.0

Note: The lists of supported platforms for deployment of virtual appliance and for disaster recovery of virtual machines are different. For information on platform support for disaster recovery of virtual machines, see the *Veritas Resiliency Platform Hardware and Software Compatibility List*.

System resource requirements for Resiliency Platform

The amount of virtual CPUs, memory, and disk space that Veritas Resiliency Platform requires are listed in this section.

The minimum configuration that is recommended for a virtual appliance for Resiliency Manager, Infrastructure Management Server (IMS), Replication Gateway, and YUM repository server:

Table 2-1 Minimum configurations

Component	Minimum configuration
Resiliency Manager	Disk space 60 GB RAM 16 GB Virtual CPU 8
Infrastructure Management Server (IMS)	Disk space 60 GB RAM 16 GB Virtual CPU 8
Gateway	Disk space 40 GB RAM 16 GB Virtual CPU 8 Additional external disk of 50 GB

Note: You need to reserve the resources for Resiliency Manager and IMS to ensure that these resources do not get swapped in case of the hypervisor getting overloaded.

If the virtual appliance does not meet the minimum configuration, you get a warning during the bootstrap of the virtual appliance and you are required to confirm if you want to continue with the current configuration.

If you plan not to use the YUM virtual appliance, you need a Linux server with a minimum of 50-GB disk space, to be configured as the repository server. Provisioning for the repository server is optional, it is required to install the Veritas Resiliency Platform patches or updates in the future.

If you want to enable dynamic memory on Hyper-V, make sure that the following prerequisites are met:

- Startup memory and minimal memory should be equal to or greater than the amount of memory that the distribution vendor recommends.
- If you are using dynamic memory on a Windows Server 2012 operating system, specify Startup memory, Minimum memory, and Maximum memory parameters in multiples of 128 megabytes (MB). Failure to do so can lead to dynamic memory failures, and you may not see any memory increase in a guest operating system. Even if you are using dynamic memory, the above mentioned minimum configuration should be met.

Network and firewall requirements

The following are the network requirements for Veritas Resiliency Platform:

- Before you use the hostname and the IP address in the **Network settings**, you need to register them with the DNS server.
- Before you use the hostname and the IP address in the **Network settings**, make sure that the reverse lookup for that IP works.
- The hostname that you use for a virtual appliance must not start with a digit and must not contain the underscore (_) character.
- Veritas Resiliency Platform supports only Internet protocol version (IPV) 4.

The following ports are used for Veritas Resiliency Platform:

Table 2-2 Ports used for Resiliency Manager

Ports used	Purpose	For communication between	Direction	Protocol
443	Used for SSL communication	Resiliency Manager and web browser	Browser to Resiliency Manager	TCP
14176	Used for communication between the Resiliency Manager and Infrastructure Management Server (IMS)	Resiliency Manager and IMS Resiliency Managers of the two data centers	Bi-directional	TCP
7001	Used for database replication	Resiliency Managers of the two data centers	Bi-directional	TCP

Table 2-2 Ports used for Resiliency Manager (*continued*)

Ports used	Purpose	For communication between	Direction	Protocol
22	Used for communication between remote host to the appliance klish access	Appliance and the hosts	Bi-directional	TCP
123	Used for NTP synchronization	Appliance and the NTP server	Bi-directional	TCP

Table 2-3 Ports used for Infrastructure Management Server (IMS)

Ports used	Description	For communication between	Direction	Protocol
14176	Used for communication between the Resiliency Manager and Infrastructure Management Server (IMS)	Resiliency Manager and IMS Resiliency Managers of the two data centers	Bi-directional	TCP
5634	Used for IMS configuration	IMS and the hosts	Bi-directional	TCP
14161	Used for running the IMS console	Resiliency Manager and IMS	Resiliency Manager to IMS	TCP
22	Used for communication between remote host to the appliance klish access Used for remote deployment of the packages on remote Unix host from IMS	IMS and the hosts	Bi-directional	TCP
135	Used for remote deployment on client computer (inbound)	Host and remote Windows hosts	Bi-directional	TCP
123	Used for NTP synchronization	Appliance and the NTP server	Bi-directional	TCP

Table 2-4 Ports used for Resiliency Platform Replication Gateways

Ports used	Description	For communication between	Direction	Protocol
33056	Used for replication	ESX server and Replication Gateway	Uni-directional	TCP
5634	Used for communication with IMS	IMS and Replication Gateway	Bi-directional	TCP
8089	Used for replication	Replication Gateways in different data centers	Bi-directional	TCP

Fixed issues

This chapter includes the following topics:

- [Fixed issues](#)

Fixed issues

This chapter lists the issues that have been fixed in the Veritas Resiliency Platform 2.1.

Table 3-1

Incident number	Abstract
5172	The virtual machine console may display the buffer IO error sometimes

Known issues

This chapter includes the following topics:

- Disaster recovery (DR) configuration for resiliency group fails if Microsoft Hyper-V Replica is configured after you add a virtual machine in Resiliency Platform
- In the VM Inventory report, instead of allocated memory, Resiliency Platform shows the total memory of the virtual machines
- Certain validations do not work while creating a resiliency group of applications (3721289)
- Rehearsal does not work after being aborted
- The configure DR operation fails if virtual machines in the resiliency group belong to different servers
- For resiliency groups containing VMware virtual machines with NFS datastore mounted from a NetApp volume with substring vol, Migrate or takeover operations may fail
- The license expiry status is inconsistent on Resiliency Managers configured on different time zones
- In the Hyper-V guest environment, the writable disk is shown in the Read-Only state (3785911)
- Long SRDF device group names are not discovered (3786826)
- Multiple repository paths on the same host are not allowed for the repository server (3734149)
- Unknown state displayed for the Resiliency groups of dark sites that are part of VBS (3794650)
- An Oracle custom application is not discovered if the instance names do not match (3796579)

- VBS DR operations fail when an application resiliency group with unconfigured DR is added in VBS (3794105)
- Expired resiliency plan cannot be executed even after editing the schedule (3861955)
- Resiliency groups for Hitachi enclosures are not displayed on dashboard under Top RG by replication lag chart (3861173)
- Snapshot disk is read only after rehearse operation is performed in Hyper-V with SRDF replication (3862088)
- Static IP customization may not work under certain conditions (3862916, 3862237)
- Need to manually refresh all assets after a site recovery (3861929)
- Disk utilization risk not resolved after DR operations
- Migrate operation becomes unresponsive if the operation is initiated from an unavailable site (3862253)
- Remote cluster group dependencies not validated before migrate (3863082)
- VBS migrate operation cannot be performed after failure (3862124)
- Resiliency group state does not get updated when production site is down (3863081)
- Replication information error (5170)
- DNS customization does not work if FQDN is not defined (5037)
- Some versions of VMware Tools are not supported (4969)
- Refresh operation for EMC SRDF enclosure does not work (7709)
- Remove DNS operation fails if DNS customization done by editing resiliency group (7704)
- Login to the Resiliency Manager console fails at times
- VLAN pairing for distributed port group gets deleted after upgrade (7717)
- Known issues: Resiliency Platform Data Mover
- Known issues: Recovery to Amazon Web services (AWS)
- Known issues: NetBackup integration

Disaster recovery (DR) configuration for resiliency group fails if Microsoft Hyper-V Replica is configured after you add a virtual machine in Resiliency Platform

This issue applies to the disaster recovery (DR) configuration for a resiliency group. The DR configuration operation fails if a Hyper-V Replica is configured on the Hyper-V virtual machine after you add the virtual machine to the Infrastructure Management Server (IMS).

Workaround:

Use the Resiliency Platform console to refresh the Hyper-V host manually. It discovers the Hyper-V Replica information, and the configuration DR operation functions as expected.

In the VM Inventory report, instead of allocated memory, Resiliency Platform shows the total memory of the virtual machines

In the VM Inventory report, for the virtual machines on the Hyper-V Server, the Resiliency Platform console displays the total memory instead of their allocated memory.

Certain validations do not work while creating a resiliency group of applications (3721289)

When you create a resiliency group of applications, the following validations do not work:

- Check if the Resiliency Platform Applications Enablement add-on is deployed on the host. If the Veritas Resiliency Platform Applications Enablement add-on is not correctly installed on the managed host, the create resiliency group operation for application fails. In such situation, you need to install the add-on on the host before creating the resiliency group for applications.
- If the workflow fails, resiliency group should not get created.

Rehearsal does not work after being aborted

If you abort a rehearsal operation, that rehearsal operation does not work afterwards.

Workaround:

Run cleanup rehearsal operation before performing Rehearsal again.

The configure DR operation fails if virtual machines in the resiliency group belong to different servers

If you try to configure disaster recovery (DR) for a resiliency group with multiple virtual machines that belong to different servers, the configure DR operation fails.

For resiliency groups containing VMware virtual machines with NFS datastore mounted from a NetApp volume with substring vol, Migrate or takeover operations may fail

If a VMware datastore is mounted from a NetApp replicated volume and the volume name contains the substring **vol**, the corresponding resiliency groups may fail to migrate across data centers.

Workaround:

Rename the NetApp volume to remove the substring **vol** from the name.

The license expiry status is inconsistent on Resiliency Managers configured on different time zones

If Resiliency Managers are configured on different time zones, then the license on one Resiliency Manager may expire before the license on the other Resiliency Manager. This behavior is seen on the second Resiliency Manager for almost 12 hours.

In the Hyper-V guest environment, the writable disk is shown in the Read-Only state (3785911)

In the Hyper-V guest environment, if a disk is writable but the disk manager or any other Windows utility shows that the disk is in the Read-only state, you need to restart the Hyper-V guest machine.

This can occur in the recovery data center during the migrate and takeover operation.

Long SRDF device group names are not discovered (3786826)

Symmetrix Remote Data Facility (SRDF) device groups with names longer than 18 characters cannot be discovered in the Resilience Manager web console.

Multiple repository paths on the same host are not allowed for the repository server (3734149)

While you add a repository server, you cannot add multiple repository paths on the same host as multiple entries for repository server.

Unknown state displayed for the Resiliency groups of dark sites that are part of VBS (3794650)

If a virtual business service (VBS) contains a resiliency group that belongs to dark sites, the state of the individual resiliency group is displayed as unknown if it is not online.

An Oracle custom application is not discovered if the instance names do not match (3796579)

When you add an Oracle custom application, Resiliency Platform to discover, the **Application Inputs** screen includes two **Instance name** fields. You must specify the same name in each field; otherwise, the application is not discovered.

VBS DR operations fail when an application resiliency group with unconfigured DR is added in VBS (3794105)

User cannot perform disaster recovery operations when the VBS consists of an application resiliency group which is not configured for DR.

Expired resiliency plan cannot be executed even after editing the schedule (3861955)

Once a resiliency plan schedule expires, it cannot be executed even after editing the schedule. No error is encountered when you try to edit the schedule, but the plan is not executed on edited schedule.

Workaround:

Delete the previous resiliency plan schedule and create a new resiliency plan schedule.

Resiliency groups for Hitachi enclosures are not displayed on dashboard under Top RG by replication lag chart (3861173)

In case of Hitachi enclosures, the resiliency groups are not displayed on the dashboard under Top RG by replication lag since replication lag for Hitachi enclosures is reported in percentage and the chart being displayed on the dashboard uses *HH:MM:SS* format.

[However, resiliency group details page displays the replication lag for a specific resiliency group.]

Snapshot disk is read only after rehearse operation is performed in Hyper-V with SRDF replication (3862088)

We use `Diskpart` command to clear read only flag. But the command does not work intermittently. Hence during rehearse operation in Hyper-V SRDF replication environment, sometimes the snapshot disk gets mounted in read only mode.

Static IP customization may not work under certain conditions (3862916, 3862237)

Workaround:

- Take the disk offline and then bring it online.
- Power on the virtual machine.

Static IP customization may not work under certain conditions (3862916, 3862237)

Hyper-V provides Linux Integration Services(LIS) which allows static IP customization for Linux guest. However sometimes the operation does not succeed even though the operation reports success. In such cases, the IP is not assigned to the Linux guest.

Workaround:

Log in to the virtual machine console and manually assign the IP address.

Need to manually refresh all assets after a site recovery (3861929)

After a primary site is recovered, you need to manually refresh all the asset configurations such as configurations of enclosures, virtual machines, discovery host.

Following is the order in which the asset configuration needs to be refreshed:

- For EMC VNX, EMC RecoverPoint and Hitachi, refresh the discovery host first, then refresh the enclosures, and then finally refresh the VMware vCenter servers.
- For NetApp, first refresh the VMware vCenter server and then refresh the enclosures.

Disk utilization risk not resolved after DR operations

The disk utilization risk is not resolved if the disk is made available after the resiliency group associated with the risk, is migrated to the recovery site.

Migrate operation becomes unresponsive if the operation is initiated from an unavailable site (3862253)

Migrate operation becomes unresponsive if the operation is initiated from an unavailable site (3862253)

If you try to perform the migrate operation instead of the takeover operation from a site which is currently not available, the operation becomes unresponsive indefinitely.

Remote cluster group dependencies not validated before migrate (3863082)

Veritas Resiliency Platform allows you to migrate a global service group which is mapped as a resiliency group and has dependent service groups on DR cluster which are not online. As a result, the start resiliency group operation on the recovery site may fail.

VBS migrate operation cannot be performed after failure (3862124)

If the workflow fails during a VBS migrate operation, then migrate operation cannot be retried for the VBS.

Workaround:

Fix the issue which caused the failure and then bring the VBS online on production site and then perform the Migrate operation. You can also try to perform migrate operation on individual resiliency group after fixing the issue which caused the failure.

Resiliency group state does not get updated when production site is down (3863081)

If the production site where a resiliency group is online, goes down, the state of the resiliency group does not change. However, the state of the application changes to display **Online(Stale)** to reflect that the online state of the resiliency group is stale and may not be recent.

Replication information error (5170)

For virtual machines or applications, at times you may encounter an error as **No replication information found**.

Workaround:

Remove the associated appliance, enclosure, or discovery host and add it back.

DNS customization does not work if FQDN is not defined (5037)

This issue occurs if FQDN is not defined for virtual machines running on Hyper-V platform (Linux and Windows).

Some versions of VMware Tools are not supported (4969)

Resiliency Platform uses vSphere web service API, `ValidateCredentialsInGuest()`, which does not work with some versions of VMware Tools that are installed in guest virtual machine. This issue may lead to failure in IP customization of Windows virtual machines in vSphere environment.

Workaround

Install the latest version of VMware Tools.

vSphere web service API, `ValidateCredentialsInGuest()`, works with VMware Tools version 9.4.10.2092844.

Refresh operation for EMC SRDF enclosure does not work (7709)

Refresh operation for EMC SRDF enclosure from the console does not work as expected, though the scheduled discovery after every 6 hours works as expected.

Remove DNS operation fails if DNS customization done by editing resiliency group (7704)

If you customize the DNS through edit resiliency group operation, then remove DNS operation gets aborted while migrating the resiliency group.

Workaround:

Log in to the production and recovery site Resiliency Manager consoles through Klish. Go to the manage option and restart the workflow service by running the following command:

```
manage> services rm restart wf
```

Login to the Resiliency Manager console fails at times

Sometimes, login to the Resiliency Manager console fails.

Workaround:

Stop the Resiliency Manager instance and then restart it.

VLAN pairing for distributed port group gets deleted after upgrade (7717)

If you create a VLAN pairing for distributed port group in Veritas Resiliency Platform 2.0 environment and then upgrade the Resiliency Manager and IMS to 2.1, the VLAN pairing gets deleted after the upgrade.

Workaround:

In case VLAN pairing gets deleted for the distributed port group after upgrade of Resiliency Manager and Infrastructure Management, you can re-create the network pairing from **Disaster Recovery Settings** page.

Known issues: Resiliency Platform Data Mover

The following known issues are applicable to Resiliency Platform Data Mover:

Virtual Machine protection using Data Mover has a few policy related limitations (5181)

Virtual Machine protection using Data Mover has SPBM (Storage Policy Based Management) from VMware related limitations. You may not be able to protect your virtual machines if it has any non-default policy attached that does not have vtstap filter.

Workaround:

You need to apply the policy with vtstap filter as one of the rules in it.

iofilter bundle not removed from ESX hosts even after unconfiguring virtual machines (5178)

In case you are using Resiliency Platform Data Mover, even after you unconfigure all the virtual machines in the cluster that were configured for recovery, iofilter bundle does not get removed from the cluster.

Storage policy needs to be manually removed after all the virtual machines are unconfigured (5180)

The storage policy for virtual machines does not automatically get removed After all the protected virtual machines in the VMware vSphere server are unconfigured. It needs to be manually removed from virtual machine's storage policies.

VMDK and VMX files need to be in the same folder(5167)

Protection of virtual machines using Resiliency Platform Data Mover does not work if it has vmdk and vmx files in two different folder.

Workaround:

Put the vmdk and vmx files in the same folder.

Edit resiliency group operation may fail after rehearsal or cleanup rehearsal (5092)

The edit resiliency group operation may fail after performing a rehearsal or cleanup rehearsal operation.

Workaround:

Refresh the vCenter on the datacenter where rehearsal is performed after rehearsal or cleanup rehearsal operation.

Replication gets paused if you perform add disk operation (5182)

If you add a disk to the protected virtual machine, replication is paused and you are not able to perform any operation on the associated resiliency group.

Workaround:

Edit the resiliency group to remove the affected virtual machine and then add it back.

Cannot perform any operation after deleting disk from virtual machine (5182)

If you delete a disk from a virtual machine, you cannot perform any operation on the associated resiliency group.

Workaround:

Edit the resiliency group to remove the affected virtual machine and add it back.

Data Mover virtual machine in no op mode risk cannot be resolved (5183)

The **Data mover virtual machine in no op mode** risk cannot be resolved once it gets generated.

Risks not generated after taking snapshot of virtual machine replicated using Data Mover(6886)

If you take a snapshot of the virtual machine that is a part of a Resiliency Group that gets replicated using Resiliency Platform Data Mover, the risks are not generated after taking the snapshot.

Workaround:

You need to perform edit Resiliency Group operation after you take the snapshot of any virtual machine.

Known issues: Recovery to Amazon Web services (AWS)

The following known issues are applicable to AWS:

Some DHCP enabled NICs are not present on Cloud after migrate (7407)

If DHCP is enabled for NICs but network pairing is not complete, then during the migrate operation these NICs are ignored.

Workaround

Create a network pair for the DHCP enabled NICs so that the IP addresses are shown on AWS Cloud. Or you need to manually create the network interface after migrate operation is successfully completed.

One or more NICs of a migrated Windows virtual machine may not be visible (7718)

After migration, one or more network interface cards (NIC) associated with a Windows virtual machine may not be visible from the operating system. You may not be able to connect to the migrated virtual machine using the IP address assigned to these invisible NICs.

Workaround:

In device manager, under network connections, all the NICs are listed. The NICs that are not visible in Network Connections are also listed here, but they show an error similar to the following:

```
Windows could not load drivers for this interface.
```

Right click on the network interface that is showing the error and click on Uninstall Device.

After the uninstallation, scan for hardware changes in the device manager. The NIC gets installed properly and is visible.

Cloud IPs get added to on-premise NICs after migrate back to the on-premise site and reboot (7713)

After the successful migration to the production site (on-premise) and reboot of the Windows virtual machines, the cloud IP addresses get associated with the on-premise NICs.

This is because of some issue in networking script that causes the cloud IPs to be added to premise NICs on reboot after migrate back.

Workaround:

You need to manually remove the additional IPs from the on-premise NIC.

Migrate or takeover operations fail at the Add Network for AWS task and Create Network Interface sub-task (7719)

Due to some error, the cloud IPs get added to the on-premise NICs after migrating back to the premise. After that, if you perform the edit resiliency group operation or delete and again create the resiliency group, the migrate and takeover operations fail with the following error:

```
An error occurred (InvalidParameterValue) when calling the  
CreateNetworkInterface operation: invalid value for parameter address:  
[]
```

Workaround:

Start the virtual machine and manually remove the cloud IPs.

Refresh the host and vCenter server or Hyper-V.

Edit the resiliency group and then retry the migrate or takeover operation.

Sometimes network comes up on only one NIC although there are multiple NICs (8232)

Sometimes the RHEL virtual machines having multiple NICs are accessible using only one NIC IP after performing disaster recovery (DR) operations such as migrate, take over, and rehearsal. It happens because the DHCP client is unable to get the DHCP offer from the server which prevents the routing table to get the load. Hence, the virtual machines are not accessible by other NIC IPs.

Workaround

Using the available IP, access the virtual machine, and restart the network services.

Known issues: NetBackup integration

The following known issues are applicable to NetBackup integration:

MAC address starting with 00:0c:29 not supported for VMware virtual machines (7103)

If you want to restore an image on a VMware virtual machine with MAC address starting with 00:0c:29, the machine does not get powered on.

Workaround:

You need to edit the virtual machine settings and change the MAC address type of the Network adapter to Automatic. This changes the MAC address of the machine. You can then power on the virtual machine again.

A virtual machine backed up by multiple NBU master servers gets mapped with only one master server in the console (7608)

If a virtual machine gets backed up by multiple NBU master servers, it is mapped with only one master server in the Resiliency Manager console. You can create resiliency group or restore virtual machine only with the mapped master server.

A transient virtual machine remains in the ESX server in one scenerio (7413)

If you restore a resiliency group from site A to site B and then restore it back to site A, then two virtual machines are seen on the ESX server of site A.

Workaround:

Restart the services on the vCenter server.

Limitations

This chapter includes the following topics:

- [Rehearsal is not supported if volume is configured using asynchronous replication in IBM XIV enclosure](#)

Rehearsal is not supported if volume is configured using asynchronous replication in IBM XIV enclosure

If the consistency group or the volume is configured using asynchronous replication in IBM XIV array, then the snapshot operation is not supported by XIV enclosure. Hence if the resiliency group is configured with virtual machines that are using asynchronous consistency group or volume-based replication, then the rehearsal operation fails at the 'create snapshot' step.

Virtual appliance security features

This appendix includes the following topics:

- [Operating system security](#)
- [Management Security](#)
- [Network security](#)
- [Access control security](#)
- [Physical security](#)

Operating system security

Veritas Resiliency Platform appliance operating system is hardened against potential security exploitation by removing the operating system packages that are not used by the Resiliency Platform. All the default yum repository files that are shipped with the operating system are removed.

The Control + Alt + Delete key combination has been disabled to avoid any accidental reboot of the virtual appliance. Exec-shield is enabled to protect the virtual appliance from stack, heap, and integer overflows.

Management Security

Only two users are available on the appliance: admin user and support user. These two user accounts are used to access the appliance based on the requirement.

Only admin login is available for the appliance. The password policy of admin login is modified to prompt the user to change the password on the first login.

If the admin user password is lost, you need to contact Veritas support for resetting the admin user password.

On successful completion of the product bootstrap, admin user can only access a limited menu of commands through klish. Besides admin user, support user is also supported in the appliance but remote login of support user is disabled. To access the support user, one need to login as an admin and go through **klish**. An option `support > shell` is provided in the **klish** menu to switch the user to support and access the bash shell of support. After selecting this option, the support user is given superuser privileges. Using this option is not recommended and it should be used only with the assistance of technical support.

Timeout of the bash shells of all users is set to 900 seconds.

Network security

The TCP timestamp responses are disabled in Resiliency Platform virtual appliance. Another network security feature of the appliance is that during the product bootstrap process, only those ports that are used by the product for communication and data transfer, are opened through the firewall and all the other communications are blocked.

Uncommon network protocols such as DCCP, SCTP, RDC, TIPC have been disabled so that any process cannot load them dynamically.

See [“Network and firewall requirements”](#) on page 17.

Access control security

Resiliency Platform virtual appliance implements certain access control measures. The umask is set to 0700 across the appliance. The access permissions of some of the files such as home folder of root, the log directory etc. is restricted. All the security and the authorization messages are logged into the appliance.

Physical security

In the Resiliency Platform virtual appliance, the USB storage access is disabled.