Veritas™ Resiliency Platform 3.1 Release Notes

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

Veritas Resiliency Platform: Release Notes

Last updated: 2018-07-22

Document version: Document version: 3.1 Rev 4

Legal Notice

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

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

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

https://sort.veritas.com/documents

Documentation feedback

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

doc.feedback@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 7 Known issues

Chapter 1

Overview of Veritas Resiliency Platform 3.1 Update 3

This chapter includes the following topics:

Issues fixed in Veritas Resiliency Platform 3.1 Update 3

This section lists the issues that have been fixed in the Veritas Resiliency Platform 3.1 Update 3 release.

Table 1-1 Issues fixed in Veritas Resiliency Platform 3.1 Update 3

Incident number	Abstract
14706	Resync operation always performs full synchronization of data
14627	Windows 2016 virtual machine fails to boot after migrating to the target data center
14668	Edit resiliency group operation fails if multiple disaster recovery operations were performed on the resiliency group
14661	Resync operation fails if resiliency group consists of a virtual machine with dependent and independent disks

Table 1-1 Issues fixed in Veritas Resiliency Platform 3.1 Update 3 *(continued)*

Incident number	Abstract
14550	If multiple create resiliency group operations are run simultaneously then it fails at the attach disks to gateway subtask

Chapter 2

Overview of Veritas Resiliency Platform 3.1 Update 2

This chapter includes the following topics:

- New feature in version 3.1 Update 2
- Known issues for Veritas Resiliency Platform 3.1 Update 2
- Issues fixed in Veritas Resiliency Platform 3.1 Update 2

New feature in version 3.1 Update 2

This release of Veritas Resiliency Platform includes the following new feature. Refer to the documentation for more details.

Recovery of assets from vCloud Director to vCloud Director

Veritas Resiliency Platform 3.1 Update 2 introduces, support for recovery of data center assets from vCloud Director to vCloud Director. You can configure and protect your virtual machines for recovery to vCloud 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 vCloud data centers.

Known issues for Veritas Resiliency Platform 3.1 Update 2

Following known issues are applicable for Veritas Resiliency Platform 3.1 Update 2:

DRL disk is not deleted when resiliency group is deleted (13797)

This issue is applicable if the recovery is from vCloud Director to vCloud Director.

When a resiliency group is deleted, the DRL disks are not removed from the virtual machine in the resiliency group. You need to manually delete them using the vCloud Director UI if you do not want to protect these machines on a later date. Else, when you create a new resiliency group with the same virtual machines, Veritas Resiliency Platform uses the same DRL disk.

Migrate or takeover operation may fail due to unavailability of independent disks on the vCloud Director (14639)

This issue is applicable if the recovery is from vCloud Director to vCloud Director.

The attach disk sub task may fail during the migrate or takeover operation as the independent disks are not available due to an internal error on the vCenter server.

Issues fixed in Veritas Resiliency Platform 3.1 Update 2

This section lists the issues that have been fixed in the Veritas Resiliency Platform 3.1 Update 2 release.

Table 2-1 Issues fixed in Veritas Resiliency Platform 3.1 Update 2

Incident number	Abstract
13836	Resync operation powers off the virtual machines on the active data center
13082	Support for vLans stretched across source and target data centers
12782	Prepare host for replication failed for Linux hosts with specific ssh settings

Table 2-1 Issues fixed in Veritas Resiliency Platform 3.1 Update 2 *(continued)*

Incident number	Abstract
NA	Primary NIC setting is not preserved for the virtual machines after disaster recovery operations

Chapter 3

Overview of Veritas Resiliency Platform 3.1 Update 1

This chapter includes the following topics:

New features and changes in version 3.1 Update 1

This release of Veritas Resiliency Platform includes the following new features, changes, and enhancements. Refer to the documentation for more details.

Support for migrate back of data center assets from AWS using Object Storage for replication

Veritas Resiliency Platform 3.1 Update 1 provides the ability to migrate back your data center assets from AWS using Object Storage for replication. Now you can perform disaster recovery operations such as migrate, migrate back, and resync on a resiliency group using Object Storage for replication.

Support for thin provisioned disks for VAIO based replication

Resiliency Platform version 3.1 Update 1 introduces the support for protecting the virtual machines with thin disks by provisioning corresponding thin disks on the target data center.

Resiliency Platform Data Mover replicates only the used blocks from the disks on the source data center to the disks on the target data center thereby maintaining the thin nature of the disks. Resiliency Platform Data Mover also replicates only the used blocks from a thick (lazy zero provisioned) disks to the disks on the target data center.

Support for replication tunables

Veritas Resiliency Platform 3.1 Update 1 provides the ability to tune the replication used by Resiliency Platform Data Mover by changing the size of the update set. You can change the size of the update set by using the `manage> datamover operation modify-updateset-size` klish command.

Support for downloading log files for Resiliency Manager

Using Veritas Resiliency Platform 3.1 Update 1, you can view and download the list of collected support log files for a Resiliency Manager. If you have multiple Resiliency Managers, you need to log on to each Resiliency Manager to view and download its logs. To download the log files, you must have *Resiliency Platform admin* persona with *Manage product settings* job assigned. These support logs are collected by running the `support > loggather` command using the klish menu.

Improvements for Veritas Replication VIB installation for VAIO based replication

Veritas Resiliency Platform 3.1 Update 1 has an improved and user-friendly way to install the Veritas Replication VIB (vSphere Installation Bundle). VIB is required for configuring the VMware virtual machines for recovery to on-premises data center. Prior to Update 1, VIB was installed as a part of create resiliency group operation.

Veritas Replication VIB validation scripts

Veritas Resiliency Platform 3.1 Update 1 is shipped with scripts that can validate the prerequisites for installation of Veritas Replication VIB. To run these scripts, you need to have access to the vCenter server and ESXi hosts. Veritas Replication VIB installation is required for configuring the VMware virtual machines for recovery to on-premises data center.

Asset discovery improvements

Veritas Resiliency Platform 3.1 Update 1 significant reduction in the time taken to discover the virtualization assets such as VMware vCenter server or Hyper-V server for the first time after being configured in resiliency Platform.

Performance improvement for better RTO in VMware environments

Veritas Resiliency Platform 3.1 Update 1 provides a significant performance improvement for better Recovery Time Objective (RTO) in VMware environments.

Changes in gateway to gateway encryption scheme

After upgrading to 3.1 Update 1, AES256-GCM-SHA384 is the only available encryption scheme. Hence if AES128-GCM-SHA256 is applied to any Replication Gateway, you need to modify. The encryption scheme can be modified after the Resiliency Manager is updated and must be done before Replication Gateway is updated.

Support for AES128-GCM-SHA256 has been dropped since it is no longer considered secure enough.

Security enhancements

Veritas Resiliency Platform 3.1 Update 1 provides security enhancements against vulnerabilities such as Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5753 & CVE-2017-5715).

Upgrading to Veritas Resiliency Platform 3.1 Update 1

Veritas Resiliency Platform 3.0 is the minimum version supported for upgrade to Veritas Resiliency Platform 3.1 Update 1.

About applying update to Resiliency Platform

Issues fixed in Veritas Resiliency Platform 3.1 Update 1

This chapter lists the issues that have been fixed in the Veritas Resiliency Platform 3.1 Update 1 release.

Table 3-1 Issues fixed in Veritas Resiliency Platform 3.1 Update 1

Incident number	Abstract
13063	Unable to rerun replace live Replication Gateway operation when it fails at a particular subtask
12644	When you perform DR operations on a VBS with multiple tiers, resiliency groups start in parallel instead of starting in the specified order
13220, 13015	Rehearsal of a resiliency group configured failed at IP customization stage
13190	Failed to create NIC during migrate operation in case of multiple DNS configured in Azure subnet
12951	Migrate step fails to mount the volume for RecoverPoint replication in Hyper-V environment
12891	Delete resiliency group failed to detach storage policy for VAIO based replication
12879	Create resiliency group operation for VAIO based replication fails at create storage policy task
12878	Create resiliency group operation for VAIO based replication fails at attach or delete disk
12805	Prepare host for replication operation fails on retry if the workflow is aborted
13048, 11716	Install Veritas Replication VIB on ESXi host failed during create resiliency group operation configured for VAIO based replication
11813	Add validations for Org/vApp network settings for recovery to vCloud Director
9275	After upgrade from 2.2HF1, migration fails to apply VLAN Map and then virtual machine cannot be powered on
12409	Migrate operation was not blocked even when the mount point was already in use on the target site
12381	Replication Lag incorrectly displayed when Data Mover network gets disconnected
12312	klish options `list-free-disk` and `add-disk` do not list newly added disk
13434	Proper error message not displayed if VIB is not installed

Table 3-1 Issues fixed in Veritas Resiliency Platform 3.1 Update 1 *(continued)*

Incident number	Abstract
13431	NBU master gets added but fails to connect to the IMS
13299	Cleanup rehearsal fails if you change the data center name after performing rehearsal
13240	Create gateway pair fails for recovery of Hyper-V virtual machines to Cloud
13638	Retry for delete resiliency group operation does not complete pending tasks
13408	Veritas replication VIB upgrade failed
12753	Operations time out in case of slow connection between the two Resiliency Managers
13693	Object name and data center name not shown on Activities Page for Rescan and Refresh Storage tasks
13912	IP gets changed as DHCP after migrating back from vCloud
13517	IP gets changed as DHCP after migrating back from Azure
9678	Subnet mapping gets deleted from console but not from the database
13683	VMware tools does not start after upgrade from 3.0U1 to 3.1
13316	Rehearsal cleanup operation is not idempotent for NetApp
13260	VAIO based replication gets slow if the disk size is multiple of 64GB
13065	No availability zone is displayed in technology customization page during edit resiliency group operation
12816	Edit resiliency group failed after performing replace gateway operation
12802	After Deleting a resiliency group, create resiliency group hangs at the attach volume step
10765	In case pof multiple Resiliency Managers in a data center, Resiliency Manager data does not get synchronized if one of the Resiliency Managers comes up after its downtime
12906	Incorrect rehearsal network pair displayed

Table 3-1 Issues fixed in Veritas Resiliency Platform 3.1 Update 1 *(continued)*

Incident number	Abstract
8326	Resiliency group details in the console displays stale vCloud virtual machine entries after migrating back a resiliency group to the premises site

Known issues for Veritas Resiliency Platform 3.1 Update 1

See "Replication stops if replace healthy Replication Gateway operation fails (13633)" on page 19.

See "Create resiliency group operation may fail with disk mismatch error for a virtual machine that gets migrated back from cloud to on-premises data center (13558)" on page 19.

Replication stops if replace healthy Replication Gateway operation fails (13633)

While data is being replicated, if you replace a healthy Replication Gateway with another for load balancing, and if the replace gateway operation fails. Then after fixing the failure issue, if you restart the replace gateway operation, the operation is completed successfully. But data replication is not resumed.

Workaround

You need to contact Veritas Support to resume the replication on peer Replication Gateway.

Create resiliency group operation may fail with disk mismatch error for a virtual machine that gets migrated back from cloud to on-premises data center (13558)

If you try to create a resiliency group with a virtual machine that had been migrated back from cloud to on-premises data center and then one of the following occurred:

- The virtual machine was removed from the resiliency group.
- The resiliency group containing the virtual machine was deleted.

In the above situation, the create resiliency group operation may fail with the following error:

Mismatch in the number of disks seen from the virtualization server and from guest. To fix this, rescan the virtual machine disks and then refresh the IMS discovery for the virtual machine and virtualization server.

Workaround:

- Refresh the vCenter server or Hyper-V server. Refresh the host.
- If the issue still persists, then remove the virtual machine and add it again to the IMS.

Chapter 4

Overview of Veritas Resiliency Platform 3.1

This chapter includes the following topics:

New features and changes in Veritas Resiliency Platform 3.1

This release of Veritas Resiliency Platform includes the following new features, changes, and enhancements. Refer to the documentation for more details about the new features.

Support for Object Storage mode replication for one-time migration to AWS

In Veritas Resiliency Platform 3.1, the Object Storage mode replication has been introduced to leverage the S3 Object Storage services provided by AWS. If you want to perform one-time migration of your data center assets to AWS, you have an option to choose Object Storage mode replication. To enable one-time migration of your assets to AWS using Object storage mode replication, you need to deploy a Data Gateway in AWS environment.

You can not migrate back your assets from AWS data center to the on-premises data center, if you use Object Storage mode replication.

Support for Multiple NICs for Replication Gateway appliance

Veritas Resiliency Platform 3.1 introduces support for configuring Replication Gateway with multiple Network Interface Cards (NIC). The Replication Gateway appliance is shipped with three NICs. You can configure these three NICs to be used for dedicated communication with Infrastructure Management Server (IMS), peer Replication Gateway, and the virtual machines to be protected. If you do not plan to use three separate networks, you can skip configuring all the three NICs and instead configure only one or two NICs.

Support for FIPS enablement for Replication Gateway

Federal Information Processing Standards (FIPS) are United States Government set of standards that are used for standardizing the cryptographic software. Veritas Resiliency Platform 3.1 supports FIPS compliance for the data encryption provided by Resiliency Platform Replication Gateway. You can enable the FIPS mode on a Replication Gateway at the time of bootstrap or by using the `manage > fips` option of klish menu.

Support for mapping one to multiple network groups for AWS

Veritas Resiliency Platform 3.1 supports creating network group using only subnets from Amazon Web Services (AWS) cloud data center. Network groups are created when you want your virtual machines in a resiliency group to be part of the different availability zones in AWS cloud.

Support for selecting multiple Replication Gateway pairs

Veritas Resiliency Platform 3.1 introduces the support to select multiple Replication Gateway pairs while configuring the resiliency group for recovery.

Edit resiliency group operation enhancements

Veritas Resiliency Platform 3.1 lets you edit a resiliency group, that is configured for disaster recovery, using different options for edits such as, customize the networks or edit the entire configuration.

Support for replacing a healthy Replication Gateway from a pair

Veritas Resiliency Platform 3.1 introduces the support to replace a Replication Gateway from a pair when both the gateways are in healthy state.

Infrastructure resiliency enhancements

Veritas Resiliency Platform 3.1 introduces the support to move Replication Gateways, replication hosts, and Hyper-V servers to a new Infrastructure Management Server (IMS) if the old IMS is unusable.

Support for Takeover operation from cloud data center

Veritas Resiliency Platform 3.1 introduces the support to take over a resiliency group from a cloud data center.

Support for bringing virtual machine online from storage for AWS and Azure

Veritas Resiliency Platform 3.1 lets you use the **Refresh storage, network, compute and customizations** option while starting a resiliency group if the resiliency group is configured for recovery to AWS or Azure. The operation helps bring the virtual machine online on active site when the virtual machine is not available due to failure of a DR operation at any step before or after replication. This option loads the storage, adds the virtual machine to the network, completes the IP customization, and starts the virtual machine. It is recommended to use this option if it is known that a refresh of the entire stack is needed.

RDM support for replication using Resiliency Platform Data Mover

Veritas Resiliency Platform 3.1 supports Raw Device Mapping (RDM) disk for replication using Resiliency Platform Data Mover. The RDM disk support for Resiliency Platform Data Mover is applicable to the following use-cases:

- Recovery to cloud data center: Support for RDM in virtual and physical compatibility mode
- Recovery to on-premises data center: Support for RDM in virtual compatibility mode

Azure Standard storage type supported for virtual machine size

Veritas Resiliency Platform 3.1 now supports Standard storage type for virtual machine size on Azure data center.

Changes in privileges required for adding a Windows host

Veritas Resiliency Platform 3.1 introduces some changes in the privileges required for adding a Windows host.

For adding a Windows host, It is recommended to use a domain user account with local administrative privileges on the Windows Install Host as well as on the host being added. If you cannot use a domain user account with local administrative privileges on both the hosts, you have an option to use an Administrator user or a user in local administrator group with certain prerequisites.

Support for Windows 16 as host operating system

Veritas Resiliency Platform 3.1 supports Windows 16 as operating system for virtual machines that can be protected using Resiliency Platform.

Internationalization support for Japanese language

In addition to the Internationalization support for German language, Veritas Resiliency Platform 3.1 provides Internationalization support for Japanese language. Starting with 3.1, you can see the localized version of the Resiliency Platform console if you are logging in from Japanese locale browser. The product can be used in a Japanese environment.

Upgrading to Veritas Resiliency Platform 3.1

Veritas Resiliency Platform 2.2 is the minimum version supported for upgrade to Veritas Resiliency Platform 3.1.

About applying update to Resiliency Platform

Using the product documentation

Table 4-1 lists the URLs for Veritas Resiliency Platform documentation and Table 4-2 lists the Veritas Resiliency Platform guides.

Table 4-1 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. 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.
https://www.veritas.com/support/en_US/article.100040713	The late breaking news that is related to this release.

Table 4-2 Names of Veritas Resiliency Platform guides

Title	Description
Veritas Resiliency Platform Hardware and Software Compatibility List (HSCL)	The list of hardware and software compatibility.
Veritas Resiliency Platform Release Notes	The release information such as main features, known issues, fixed issues, and limitations.
Veritas Resiliency Platform 3.1 Overview and Planning Guide	The information about the product, its features, and capabilities.
Veritas Resiliency Platform 3.1 User Guide	The information about deploying Resiliency Platform and using the product capabilities.
Veritas Resiliency Platform Third-Party Software License Agreements	The information about the third-party software that is used in Resiliency Platform.

Chapter 5

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, 6.0U1, 6.0U2, 6.0U2, 6.5
- vCenter Server 5.1, 5.5, 6.0, 6.0U1, 6.0U2, 6.0U2, 6.5

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 5-1 Minimum configurations

Component	Minimum configuration
Resiliency Manager	Disk space 60 GB RAM 32 GB Virtual CPU 8
Infrastructure Management Server (IMS)	Disk space 60 GB RAM 16 GB Virtual CPU 8
Replication Gateway	Disk space 40 GB RAM 16 GB Virtual CPU 8 Additional thick provisioned external disk of 50 GB
YUM repository server	Disk space 60 GB RAM 4 GB Virtual CPU 2

Table 5-1 Minimum configurations *(continued)*

Component	Minimum configuration
Hosts to be added to Veritas Resiliency Platform: ■ Windows Install host ■ Application host ■ Resiliency Platform Data Mover host ■ Storage discovery host ■ Hyper-V host **Note:** This section is not applicable for recovery of VMware virtual machines to on-premises data center.	Disk space 15 GB RAM 4 GB Dual processor CPU If you are using a single host for multiple purposes, add the disk space and RAM required for each purpose. For example, if you are using a single host as Windows Install host and as application host, then you need to have at least 30 GB disk space and 8 GB RAM. Note that you cannot use a single host as a Windows Install host as well as Resiliency Platform Data Mover host.

Note: You need to reserve the resources for Resiliency Manager and IMS to ensure that these resources do not get swapped in case of hypervisors 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 ports are used for Veritas Resiliency Platform:

- Recovery of assets to AWS
- Recovery of assets to Azure
- Recovery of assets to vCloud Director
- Recovery of assets to on-premises data center using Resiliency Platform Data Mover
- Recovery of assets to on-premises data center using third-party replication
- Recovery of assets using NetBackup
- Recovery of InfoScale applications

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 3.1 release.

Table 6-1 Issues fixed in Veritas Resiliency Platform 3.1

Incident number	Abstract
N/A	Disk utilization risk not resolved after DR operations
N/A	Disaster recovery (DR) configuration for resiliency group fails if Microsoft Hyper-V Replica is configured after you add a virtual machine in Resiliency Platform
N/A	The configure DR operation fails if virtual machines in the resiliency group belong to different servers
N/A	Login to the Resiliency Manager console fails at times
N/A	Previously configured network mapping may not work after re-adding a VMware vCenter server
N/A	In the VM Inventory report, instead of allocated memory, Resiliency Platform shows the total memory of the virtual machines
3721289	Certain validations do not work while creating a resiliency group of applications

Table 6-1 Issues fixed in Veritas Resiliency Platform 3.1 *(continued)*

Incident number	Abstract
3794650	Unknown state displayed for the Resiliency groups of dark sites that are part of VBS
3794105	VBS DR operations fail when an application resiliency group with unconfigured DR is added in VBS
3861929	Need to manually refresh all assets after a site recovery
3862253	Migrate operation becomes unresponsive if the operation is initiated from an unavailable site
8697	Replication information not discovered for Hyper-V virtual machines configured in Microsoft Failover Clustering environment using Non-English characters in the CSV path

Known issues

This chapter includes the following topics:

- Known issues: Generic
- Known issues: Recovery to Amazon Web services (AWS)
- Known issues: Recovery to Azure
- Known issues: Resiliency Platform Data Mover used for recovery to on-premises data center
- Known issues: Resiliency Platform Data Mover
- Known issues: Recovery using third-party replication
- Known issues: NetBackup integration
- Known issues: Multiple Resiliency Managers in a data center

Known issues: Generic

The following are the generic known issues applicable for Veritas Resiliency Platform:

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.

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 work as expected because of compatibility issues. 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.

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.

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.

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).

The disaster recovery operations may fail, if the Resiliency Manager is idle for few hours (13177)

Description: When the Resiliency Manager remains idle for some time, the disaster recovery operations may fail.

Workaround:

From the klish console of Resiliency Manager, go to the *manage* section and run the following command:

```
services restart core
```

Warning message may be displayed for network mapping (8644)

At times, even if the network mapping is set up in the environment, you may get a warning message for network mapping similar to the following while performing a disaster recovery operation:

```
Some virtual machines may not connect to network after migrate as
the required network mapping are not defined.
```

Workaround:

You need to click on Continue and the operation proceeds as expected.

Unable to rerun replace live Replication Gateway operation when it fails at a particular subtask (13063)

While replacing a live Replication Gateway, if the operation fails at “Unconfigure Veritas Replication Set from Veritas Replication Gateway” sub task, even if you re-run the operation is not executed. The workflow may be shown as complete on Recent Activities page, though the operation is not executed.

Workaround:

Contact Veritas Support.

Unable to map the network groups with the virtual machines in resiliency group that are created before upgrade to 3.1 (12978)

After upgrading to 3.1, the virtual machines in the existing resiliency groups cannot be mapped with network groups. You need to edit the resiliency group using the ‘Edit Configuration ‘ intent. Map the virtual machines to the network groups and submit the wizard. Or you can delete the resiliency group and recreate after mapping the virtual machines to network groups.

Migrate sub tasks continue to show as running even if Resiliency Manager is offline (13657)

Consider the following scenario if you have multiple Resiliency managers in your resiliency domain.

Using Resiliency Manager_1 you start to migrate your assets to any data center, and then Resiliency Manager_1 is shut down before the operation is complete. The other Resiliency Managers (Resiliency Manager_2 and Resiliency Manager_3) are still online. It is observed that the migrate workflow continues to show as running, but no tasks are executed. Only the workflow or the sub task state is shown as running.

Workaround:

Abort the operation from any of the Resiliency Managers that are online. Re-initiate the migrate operation.

DR operations fail if MAC and BIOS UUID change (13565)

If the MAC and BIOS UUID of a virtual machine that is already configured for disaster recovery (DR) changes, then the DR operations fail.

Workaround:

You need to remove the virtual machine from the resiliency group and add it back.

Virtual machine having duplicate disk IDs cannot be configured for disaster recovery (14188)

If virtual machines that are cloned or created from a template, have duplicate disk IDs, then they cannot be configured for disaster recovery.

Workaround:

Ensure that the virtual machines have unique disk IDs.

IDs displayed instead of object names in the console if you upgrade from a version prior to 3.0 (12131)

If you upgrade from any version prior to 3.0 to resiliency Platform 3.0 or later versions, ID strings are displayed instead of object names in the notifications and logs.

Default route option through klish changes on reboot (11788)

If you use the route command to set the default gateway in multiple NIC environment, the default route may get reset to the gateway of last NIC after you reboot the system or a network restart is done.

Workaround:

You need to explicitly delete the existing default route and again add the desired default route through klish.

Validations displayed while configuring resiliency group for remote recovery (10961)

Disk mismatch or disk correlation missing validations are displayed while configuring a resiliency group for remote recovery in the following situations:

- When you remove a virtual machine from an resiliency group having more than one virtual machine and try to add it again.
- In case of a resiliency group having a single virtual machine, if you delete and create the resiliency group again using the same virtual machine.

Workaround:

Wait for at least 40 minutes for the discovery of virtual machine to complete. Or you can manually refresh the virtual machine.

Known issues: Recovery to Amazon Web services (AWS)

In addition to the known issues applicable for recovery to AWS, the issues listed for Resiliency Platform Data Mover are also applicable:

See "Known issues: Resiliency Platform Data Mover" on page 40.

The following known issues are applicable only for recovery 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.

Migrate from cloud to on-premises date center fails if gateway pairs belong to the different modes (13069)

You have created Replication Gateways pairs having different modes such as Direct and Object Storage, and while configuring for recovery these are displayed on the panel. Irrespective of whether you have chosen gateway pairs with same modes or different modes, the migrate operation from cloud to on-premises data center fails.

Known issues: Recovery to Azure

In addition to the known issues applicable for recovery to Azure, the issues listed for Resiliency Platform Data Mover are also applicable:

See “Known issues: Resiliency Platform Data Mover” on page 40.

The following known issues are applicable only for recovery to Azure:

Incorrect options for choosing virtual machine size are displayed during Edit operation (13068)

While configuring a resiliency group for recovery to Azure, the virtual machine size chosen was Premium storage type supported. Now while editing the resiliency group, the drop-down list for choosing virtual machine size also displays options for Standard storage type supported virtual machine sizes.

If you choose Standard storage type supported virtual machine sizes then, the edit resiliency group operation is successfully completed without any errors, but the migrate or takeover operation fails.

Workaround:

Ensure that Premium storage type supported virtual machine size is selected.

Known issues: Resiliency Platform Data Mover used for recovery to on-premises data center

In addition to the known issues applicable for recovery to on-premises data center, the issues listed for Resiliency Platform Data Mover are also applicable:

See "Known issues: Resiliency Platform Data Mover" on page 40.

The following known issues are applicable to Resiliency Platform Data Mover used for recovery to on-premises data center:

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.

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.

Cannot delete a resiliency group after removing a virtual machine from the resiliency group configured for recovery of VMware virtual machines to on-premises data center (13209)

You may not be able to delete a resiliency group after removing a virtual machine from the resiliency group configured for recovery of VMware virtual machines to on-premises data center using Resiliency Platform Data Mover. This is due to a VMware limitation.

Workaround:

Attach the Storage Policy Based Manager (SPBM) policy to the virtual machine through vCenter Server console and then perform the delete resiliency group operation again.

Known issues: Resiliency Platform Data Mover

In addition to the issues listed under specific use-cases such as recovery to AWS, Azure, vCloud Director, or on-premises data center, the following known issues are generic for Resiliency Platform Data Mover used for recovery to any cloud data center or on-premises data center:

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

If you add a disk to the protected virtual machine or delete a disk from 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.

Recovery data center details are not displayed after upgrade (13024)

After upgrading to 3.1, while editing a resiliency group that is already configured for remote recovery, the details of recovery data center are not displayed in the **Review Environment** panel. This happens if the disk name is greater than 128 characters.

Workaround:

Contact Veritas support to start a full discovery on both the Replication Gateways.

Or you can delete the resiliency group and reconfigure it for recovery. Note that when you delete and reconfigure, full synchronization of data from production to recovery data center is done.

Known issues: Recovery using third-party replication

The following known issues are applicable for recovery using third-party replication:

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.

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.

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)

`Diskpart` command is used to clear the read only flag in Hyper-V SRDF replication environment. But the command may fail intermittently. Hence during rehearse operation, sometimes the snapshot disk may get mounted in read only mode.

Workaround:

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

Migrate operation for resiliency group using third-party replication may fail due to LUNs getting reported without WWN value (13235)

Migrate operation for resiliency group using third-party replication may fail at Load Storage step due to LUNs getting reported without WWN value.

Workaround:

Add the enclosure again.

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.

Restore operation may fail if the remote master server gets removed and is added again (8600)

Restore operation may fail if one of the associated NetBackup master servers has been removed and added again in Resiliency Platform console.

Workaround:

You need to remove and then add both the master servers again.

Websocket connection is disconnected after upgrade (12814)

After upgrading to version 3.1, the websocket connection with NetBackup master server gets disconnected.

Workaround:

To re-establish the connection you need to perform the edit operation, or remove and re-add the master server.

Known issues: Multiple Resiliency Managers in a data center

Following are the known issues applicable for multiple Resiliency Managers in a data center:

See “Newly added Resiliency Manager cannot remove the existing offline Resiliency Manager (10821)” on page 44.

See “In a cloud data center, DR operations need to be performed only from the Resiliency Manager associated with the cloud IMS (10895)” on page 44.

Newly added Resiliency Manager cannot remove the existing offline Resiliency Manager (10821)

If a new Resiliency Manager is added to a data center while any Resiliency Manager in the other data center is offline, then the newly added Resiliency Manager cannot remove the offline Resiliency Manager.

Workaround:

Log in to klish and use the following option of command to restart the database service:

```
services rm restart db
```

Now you can remove the offline Resiliency Manager.

In a cloud data center, DR operations need to be performed only from the Resiliency Manager associated with the cloud IMS (10895)

In a cloud deployment with multiple Resiliency Managers, you can perform the DR operations only from the Resiliency Manager that is associated with the cloud IMS.

Chapter 8

Limitations

This chapter includes the following topics:

Limitations when recovering from vCloud Director to vCloud Director.

After successful completion of Resync operation for the first time, independent disks are created. When you migrate back to the source data center, these independent disks are attached to the virtual machines. The following limitations, which are applicable to the independent disks of vCloud Director, are now applicable to the virtual machines created by Veritas Resiliency Platform:

- Cannot move the virtual machine to a different vApp.

- Cannot copy the virtual machine to a different vApp.
- Cannot resize or delete the independent disks.
- Cannot take snapshot of the virtual machines that have independent disks.
- Cannot add vApp to Catalog containing virtual machines having independent disks.
- Can delete a virtual machine but the independent disks are not deleted.
- Can upload the OVA file which is downloaded from a virtual machine having independent disks, to either the catalog or to MyCloud. But this creates a virtual machine with dependent disks.

Rehearse and cleanup rehearsal operations

Rehearse and cleanup rehearsal operations are not supported when recovering assets to vCloud Director. This applicable if the recovery is from on-premises data center to vCloud Director or from vCloud Director to vCloud Director.

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.

Limitations for on-premises Windows hosts for Resiliency Platform Data Mover replication

Following limitations are applicable only for on-premises hosts on Windows platform and the replication is Resiliency Platform Data Mover:

- To perform the Initialize Disk operation, consistency group must be in PAUSED or STOPPED state.
- If system recovery is done manually, then you need to first stop the replication and then start the replication using the CLI.
    - “C:\Program Files\Veritas\VRTSitrptap\cli\vxtapaction.exe” stop –cg <*CGID*>

- “C:\Program Files\Veritas\VRTSitrpptap\cli\vxtapaction.exe” start –cg <*CGID*> where *CGID* is the consistency group ID.

Hyper-V hosts having snapshots not supported for recovery to AWS

A Hyper-V host having snapshots is not supported for recovery to AWS.

Computer name of virtual machine on vCloud differs if the name exceeds permitted character limit

The maximum allowed character limit for a Computer name on vCloud is, 15 for Windows and 63 for Linux. If the host name part of the fully qualified domain name (FQDN) of a virtual machine exceeds the limit, then after performing migrate or take over operation the Computer name of the virtual machine on vCloud has a default name.

The name can be edited as required.

Localization of adding application type is not supported

Localization of adding applications type is not supported due to back-end limitations. The **Add Application Type** wizard in **Settings** > **Application Support** > **Uploaded** tab does not accept the inputs in non-English characters.

Localization related limitations

The following are a few localization related limitations applicable to Veritas Resiliency Platform 3.1:

- Resiliency Plan task names gets localized but after getting saved once, it does not change on browser locale
- Notification text does not get localized
- Email text does not get localized
- Activities task results does not get localized

- MH level tasks does not get localized
- For German AD, User's group name is mandatory
- If IP customization is done, then on the **Configuration of Resiliency Group** page, **IP Customization Details** table is displayed. This table is not displayed in Japanese and German localized UI.
- Some fields in the **Schedule Report** and **Saved Plans** panel are not displayed in Japanese localized UI.

Virtual machine name limited to 35 characters

If recovery is on Azure then the virtual machine name should not exceed 35 characters.