Veritas™ Resiliency Platform 3.2 Release Notes

Last updated: 2018-07-25

Document version: Document version: 3.2 Rev 1

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:

vrpdocs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Release overview

This chapter includes the following topics:

- New features and changes in Veritas Resiliency Platform 3.2
- Using the product documentation

New features and changes in Veritas Resiliency Platform 3.2

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

See "Recovery of assets from vCloud Director to vCloud Director" on page 10.

See "Automated disaster recovery and migration support for OpenStack" on page 10.

See "Support for multiple NICs for Resiliency Manager and IMS appliances" on page 10.

See "Support for VMware Storage vMotion" on page 11.

See "Enhanced support for replication tunables" on page 11.

See "Guided help for Veritas Resiliency Platform configuration" on page 11.

See "Simplified trialware deployment experience" on page 11.

See "Improved handling of VMware vSphere virtual machine snapshots" on page 12.

See "Real-time monitoring of configuration files" on page 12.

See "Veritas Replication VIB enhancements" on page 12.

See "View data replication status" on page 12.

See "Support for NetBackup 8.1 and 8.1.1" on page 13.

See "Change in licensing model" on page 13.

See "Support for mapping one network to multiple cross-site networks in VMware environment" on page 13.

See "Support for probing and suppressing the risks" on page 13.

See "Pausing the Migrate and Takeover operations" on page 14.

See "Abort the takeover operation" on page 14.

See "Pre-upgrade check" on page 14.

Recovery of assets from vCloud Director to vCloud Director

Veritas Resiliency Platform 3.2 introduces the 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.

Automated disaster recovery and migration support for OpenStack

Veritas Resiliency Platform 3.2 introduces the support for recovery of the data center assets to OpenStack cloud data center. You can configure and protect your VMware and Hyper-V virtual machines for recovery to OpenStack using the Resiliency Platform Data Mover.

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

Recovery to OpenStack is a technical preview feature.

Support for multiple NICs for Resiliency Manager and IMS appliances

Veritas Resiliency Platform 3.2 introduces support for configuring Resiliency Manager and IMS appliances with two Network Interface Cards (NIC) each. Both these appliances are shipped with two NICs. You can configure these two NICs to be used for dedicated communication. If you do not plan to use two separate networks, you can skip configuring the two NICs and instead configure only one NIC.

For the Replication Gateway appliance, support for multiple (three) NICs was added in Veritas Resiliency Platform 3.1 release.

Support for VMware Storage vMotion

Veritas Resiliency Platform 3.2 supports VMware Storage vMotion. With Storage vMotion, you can migrate a virtual machine from one datastore to another while the virtual machine is running. This lets you move the virtual machines off the arrays for maintenance or for upgrade.

Enhanced support for replication tunables

Veritas Resiliency Platform 3.2 enables the Resiliency Platform Data Mover users to tune the replication performance, RPO, as well as the number of virtual machines that can be protected using a particular gateway. This can be done by tuning the following parameters:

- **Update set size:** You can tune the performance of the replication by changing the update set size.
- **Replication Frequency:** You can tune the RPO for all the resiliency groups configured on a gateway by changing the replication frequency.
- **Quota per Veritas Replication Set:** You can tune the maximum number of virtual machines that can be protected using a gateway by changing the quota per Veritas Replication Set.

You can change the values for all the three parameters using the klish commands:

Guided help for Veritas Resiliency Platform configuration

Veritas Resiliency Platform 3.2 introduces a guided help for configuration and protection tasks. **Guide Me**, the guided help, begins right after deployment of the product. It guides you through the Resiliency Manager console to perform the operations related to asset configuration and protection.

Guide Me automatically detects the steps being performed in the Resiliency Manager console and directs you towards the next step. It also provides the context-sensitive help for the steps being performed.

Simplified trialware deployment experience

Veritas Resiliency Platform 3.2 introduces a simplified trialware or Proof of Concept (POC) deployment experience for a new user. You get use case based resources that include zip files to be used for deployment and configuration, a configuration planner, and a Quick Start guide explaining the entire flow along with the documentation link.

Improved handling of VMware vSphere virtual machine snapshots

Veritas Resiliency Platform 3.2 now supports improved handling of VMware vSphere virtual machine snapshots. When snapshots are created or deleted no user action is required, but when reverted, minimum user action is required to resync the changes.

When a resiliency group is created and protected for disaster recovery, the virtual disk paths are recorded. When snapshots are created, deleted, or reverted these paths change. Such changes are detected and automatically recorded by Resiliency Platform thereby ensuring seamless disaster recovery operations.

Real-time monitoring of configuration files

Veritas Resiliency Platform 3.2 now monitors the configuration files (vmx files) of VMware virtual machines that belong to a resiliency group.

When the resiliency group is configured for disaster recovery (DR) using Resiliency Platform Data Mover replication technology, then any configuration changes for these virtual machines are monitored. These changes are updated in near real-time in the Resiliency Platform database. This latest copy of the configuration file is used in the subsequent DR operations such as Migrate, Takeover, and Rehearsal.

Veritas Replication VIB enhancements

Veritas Resiliency Platform 3.2 provides significant enhancements to the operations involving Veritas Replication VIB. Veritas Replication VIB can now be installed, upgraded, or uninstalled using the Resiliency Manager console. You can also verify the status of the Veritas Replication VIB installation on the ESXi clusters and try to resolve the installation issues, if any.

View data replication status

Data replication starts when you add your assets to a resiliency group and configure it for disaster recovery. Incremental replication also happens in certain scenarios. Using the Resiliency Platform 3.2 console, you can view the status of data replication on the resiliency group details page. Details such as time required to complete synchronization, percentage of data replicated. The progress is also displayed on a status bar.

You can also view the size of the protected data, which is the total data of the virtual machines within the resiliency group.

Support for NetBackup 8.1 and 8.1.1

Veritas Resiliency Platform 3.2 provides support for NetBackup 8.1 and 8.1.1 with secure communication. NetBackup 8.0 is no longer supported with Resiliency Platform version 3.2.

If you have NetBackup master server version 8.0 added to Resiliency Platform and you upgrade to Resiliency Platform 3.2, you must upgrade your master server to NetBackup 8.1 or 8.1.1. After upgrading the master server to 8.1, you need to re-add the master server to the Resiliency Platform.

Change in licensing model

Veritas Resiliency Platform 3.2 supports one to one mapping of license subscription with a resiliency group. You can create multiple resiliency groups using one license but you cannot use multiple licenses of same meter type for a resiliency group. You can remove the unused licenses from the licensing view. If there are any licenses which are expired and used, in nightly schedule run, these licenses will be automatically replaced with new valid licenses of same meter type where the license is unused and sufficient meters are available.

Support for mapping one network to multiple cross-site networks in VMware environment

Veritas Resiliency Platform 3.2 supports creating network group using port groups of same VLAN ID within a cluster.

When you create and pair network groups, and perform a disaster recovery operation, the virtual machines in same cluster that are connected to different port groups can be migrated to the same network on target data center.

Support for probing and suppressing the risks

Using the risk insight feature, you can analyze the risks that may exist in the application and take corrective actions to fix those risks. There are risks raised when the Resiliency Platform components are either unreachable or unavailable from the configuration. Veritas Resiliency Platform 3.2 supports probing and suppressing these risks.

Probing a risk is a way of evaluating a risk to check whether the risk is eliminated or still exists.

Suppressing a risk is a way of dodging a risk for some specific time.

Pausing the Migrate and Takeover operations

Resiliency Platform 3.2 lets you pause the Migrate and Takeover operation at certain predefined stages. This gives you time to perform any manual tasks on the assets if required. On completion of your tasks, you can resume the operation from Activities or Recent Activities menu. You select the pause or the manual intervention points while configuring a resiliency group or a Virtual Business Service (VBS) for disaster recovery.

Abort the takeover operation

Resiliency Platform 3.2 adds the support to abort the takeover operation in case of data loss. During the takeover operation, if Resiliency Platform detects a probability of data loss while shutting down the virtual machines, then you have the option to abort the takeover operation to avoid any data loss. A checkbox is displayed on the Takeover operation wizard.

Pre-upgrade check

If you are using Veritas Resiliency Platform 3.1 and any Resiliency Manager or IMS in your resiliency domain is in disconnected state, you must not upgrade to 3.2. Contact Veritas support to fix the issue before you upgrade the Resiliency Platform components in your resiliency domain.

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. Online help portal. The help content is also available from the product console.
Veritas Resiliency Platform videos and articles	The list of Resiliency Platform videos and other articles.
Veritas Resiliency Platform 3.2 LBN	The late breaking news that is related to this release.

Table 1-2 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, and limitations.
Veritas Resiliency Platform 3.2 Overview and planning Guide	The information about the product, its features, and capabilities.
Veritas Resiliency Platform 3.2 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.

System requirements

This chapter includes the following topics:

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.

Table 2-1 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

Table 2-1 Minimum configurations *(continued)*

Component	Minimum configuration
YUM repository server	Disk space 60 GB RAM 4 GB Virtual CPU 2
Hosts to be added to Veritas Resiliency Platform: ■ Windows Install host ■ Application host ■ Resiliency Platform Data Mover host ■ Storage discovery host ■ Hyper-V host	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 OpenStack
- 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

Chapter 3

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 3.2 release.

Table 3-1 Issues fixed in Veritas Resiliency Platform 3.2

Incident number	Abstract
6886	Risks not generated after taking snapshot of virtual machine replicated using Data Mover
13633	Replication stops if replace healthy Replication Gateway operation fails
13889	The risk "Host not added to IMS" does not get resolved if virtual machine is migrated to vCloud Director
13903	Configure DR operation fails with error "Invalid virtualization server error" if the vCenter server is added to an IMS that is being reused without proper cleanup
13956	Refresh operation fails with error that are unable to find IMS
14126	Network group VMware environment is not supported
13990	Virtual machine network did not show up after migrating back from cloud data center
14151	Unable to reconnect to Resiliency Manager if IMS is removed

Table 3-1 Issues fixed in Veritas Resiliency Platform 3.2 *(continued)*

Incident number	Abstract
14418	Disaster recovery operations fail to update DNS entry with error "TSIG error with server: tsig verify failure"
15175	Deleting the resiliency group after takeover operation does not completely clear the cloud environment
15291	Retry button of deep start only tries to start the virtual machine and does not perform deep start
15451	Delete resiliency group operation for on-premises recovery of VMware virtual machines using Resiliency Platform data Mover does not completely unconfigure the DR
15277	Unable to perform operation on resiliency group as IMS is in disconnected state
15414	Network pairing is not displayed when you upgrade from 3.0.1 to 3.1.1
15620	Risk does not get resolved even after deleting the resiliency group
15860	Resiliency group operation fails at DNS task with 'TSIG error' while deleting the DNS entry
13991	Virtual machine network is not available during migrate back from any cloud to VMware environment after performing multiple round trip across sites.
16180	Leave domain operation fails for Resiliency Manager
11046	On re-adding the IMS to the cloud data center, the old cloud configuration does not get cleared
14228	YUM server configuration is not supported if there are no new updates
14488	Klish option 'poweroff' does not shutdown the Replication Gateway virtual machine
14403	If a virtual appliance upgrade hangs and you retry the update after restarting the appliance, the subsequent update fails
13491	Migrate or takeover operation fails due to incomplete networking information of the resiliency group
13836	Resync operation shuts down the protected virtual machine on the active data center

Table 3-1 Issues fixed in Veritas Resiliency Platform 3.2 *(continued)*

Incident number	Abstract
13837	Windows Install Host cannot be removed after upgrade
13266	Unable to add new staging disk to the gateway after the resiliency group is migrated to the target data center
13179	Prepare Host for Replication operation hangs due to pop up window appearing on the Windows virtual machine
13203	NBU Master server fails to connect after being added into Veritas Resiliency Platform
12882	Validate CIM server status for resiliency group disaster recovery (DR) operation
12884	Veritas Replication VIB installation failed after new IMS being added to the vCenter server

Chapter 4

Known issues

This chapter includes the following topics:

Known issues: Generic

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

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.

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.

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).

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.

vLan mapping compulsory for DRS enabled Vmware virtual machines (10322)

If vSphere DRS is enabled for a VMware HA cluster and virtual machine has port group attached from distributed switch, then you must do vLan mapping for successfully performing the migrate operation.

This is applicable only to vCenter server and ESXi version lower than 6.5.

DNS customization changes are not updated while editing resiliency group (12946)

When you edit a resiliency group using the **Customize Network** intent, any changes that are made in the DNS customization check boxes are not saved. The edit resiliency group operation is successfully completed without these changes.

Workaround:

To fix this, edit the resiliency group using the **Edit Configuration** intent.

Replace Replication Gateway operation fails at a subtask (13049)

Replace Replication Gateway operation fails at the following subtask.

Subtask: Create the Veritas Replication Set on the Replication Gateway

This error is displayed in the following scenarios:

Scenario 1:

A resiliency groups, consisting of Windows virtual machines, is migrated to a cloud data center without enabling the Enable reverse replication check box. After migrate if you try to replace the Replication Gateway on the on-premises data center which is healthy. The replace gateway operation fails.

Scenario 2:

A resiliency groups, consisting of Windows virtual machines, is migrated to a cloud data center without enabling the Enable reverse replication check box. After migrate if you try to replace the Replication Gateway on the on-premises data center which is in faulted state. The replace gateway operation fails.

Workaround for scenario 1:

Perform the resync operation and then replace the Replication Gateway.

Workaround for scenario 2:

Contact Veritas Support.

Unable to map the network groups with the virtual machines in resiliency group which 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.

DR operations fail after editing the resiliency group using Customize Network intent (16804)

When you migrate back to the source data center and edit the resiliency group using the **Customize Network** intent, the subsequent disaster recovery (DR) operations such as migrate, takeover, or resync fails with error `VserverID not found`.

Workaround:

Do one of the following:

- After migrating back, avoid using **Customize Network** intent to edit the resiliency group, instead use the**Edit Configuration** intent to update the network mappings.
- If you have used the **Customize Network** intent to edit the resiliency group, manually attach the NIC networks to the virtual machines, and then power on the virtual machines. Refresh the vCenter server from Resiliency Manager console.

Warning message is displayed if the subnets are not mapped using Create Pair wizard but are selected while creating a resiliency group (16564)

A network group consisting of port groups is created and mapped across the data centers, and the subnets are not mapped using **Create Pair** wizard but are selected on the **Network Customization** panel while creating a resiliency group. Following message is displayed when you invoke any disaster recovery operation on such resiliency group:

```
No mapping is found for any workload in the resiliency group. Edit
the resiliency group to view the configuration for network mapping
details.
```

Workaround:

Ignore the message and continue with the operation.

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.

Asset unavailable risk raised while removing a virtual machine from a resiliency group (16966)

While removing an already added virtual machine from a resiliency group which is configured for disaster recovery, asset unavailable risk is raised.

If the edit resiliency group operation is successful, the risk is resolved automatically. But if the edit resiliency group operation fails while the virtual machine is been removed, the risk exists.

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.

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.

Migrate operation in VMware environment may sometimes fail due to timeout (12642)

In VMware environment, migrate operation may sometimes fail due to failure in properly shutting down the virtual machine. The virtual machine operating system gets shut down but the virtual machine remains powered on. This results in failure of migrate operation.

Workaround:

Manually power off all the virtual machines of the resiliency group and then retry the migrate operation.

DR operations fail if ESXi server is moved from one vCenter server to another (16287)

If you remove an ESXi server from one vCenter server and add it to another vCenter server, DR operations fail.

Workaround:

Edit the earlier vCenter server and remove the ESXi server entry associated for discovery.

Ignore the configuration drift related risk raised during various operations (16803)

"Disk configuration for asset(s) in the Resiliency Group has changed. This is a configuration drift.”, this risk is raised in the following scenarios. There is no user action required, the risk is cleared after the next discovery cycle is complete which is 30 minutes.

Scenarios:

- While migrating back from AWS or Azure cloud data center.
- While migrating to an on-premises data center using Resiliency Platform Data Mover replication technology.
- While configuring the resiliency group for recovery to vCloud Director.

Workaround:

If the risk is not cleared in 30 minutes then, you need to remove the virtual machine from the resiliency group. Re-add the virtual machine using the Edit resiliency group operation.

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.

DR operations may fail at create disk step (16919)

If Create Disk operation on vCenter server takes more than 5 minutes, the disaster recovery (DR) operations such as rehearsal, take over, or migrate, may fail.

Workaround:

Retry the DR operation.

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)

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: Recovery to Azure

The following known issue is applicable 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.

Work around

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

Known issues: Recovery to vCloud

The following known issues are applicable to recovery to vCloud:

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

After migrating back a resiliency group to the premises site, the details page of resiliency group in the console may show stale vCloud virtual machine entries in some cases. The operation succeeds and there is no harmful side effect otherwise.

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.

Resync operation always performs full synchronization of data (14706)

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

The Resync operation when performed for the first time does full synchronization of data. In the subsequent Resync operations, only incremental synchronization is done. But in this scenario, full synchronization of data is done during every Resync operation.

After migrating back, the storage profile selection for the existing virtual machine may be incorrect (16901)

When you migrate back to the source data center, and edit the resiliency group using **Edit Configuration** intent, it may happen that for the existing virtual machines the storage profile displayed is incorrect.

Workaround: To fix this, verify the storage profile of the existing virtual machine. If the storage profile displayed is incorrect, change it to the appropriate value.

After migrating back, the IP and MAC addresses assigned to a NIC are displayed incorrect on using Customize Network intent (16885)

After migrating back, if you edit a resiliency group using the **Customize Network** intent, then the IP address is blank and incorrect MAC address is displayed for the NIC. This issue occurs even though the correct IP and MAC addresses are assigned to a NIC.

Workaround: To fix this, do not use **Customize Network** to edit the resiliency group. Instead use the **Edit Configuration** intent.

Known issues: Resiliency Platform Data Mover

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

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.

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

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.

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

You may not be able to delete the resiliency group after editing the resiliency group for the use case of recovery of VMware virtual machines to on-premises data center. This is due to a VMware limitation.

Workaround:

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

Known issues: Recovery using third-party replication

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

DR operations may fail for virtual machines with NFS datastore mounted from a NetApp volume with substring vol

If a VMware datastore is mounted from a NetApp replicated volume and the volume name contains the substring vol, DR operation such as Migrate and Takeover may fail for the corresponding resiliency groups.

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)

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.

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.

Migrate and resync operations fail when there are stale objects on the source data center (13775)

If the source data center is down, and the Takeover operation is performed, there may be some stale entries of workloads and datastores on the source side after the data center is functional. If these entries are in inaccessible state on the vCenter console, then Resync operation is unable to clean the entries. And hence when you migrate back the Migrate operation fails.

Workaround:

Before you migrate back to the source data center, you need to manually cleanup the stale entries.

After upgrade to 3.2, create or edit resiliency group operation may fail for applications or Hyper-V virtual machines using 3PAR Remote Copy for replication (16441)

After upgrading from any lower Resiliency Platform version to version 3.2 or above, you may face issue while creating or editing a resiliency group of applications or Hyper-V virtual machines if 3PAR Remote Copy is being used for replication.

Workaround:

- Remove the following assets from Resiliency Platform and then re-add:
  - For a resiliency group consisting Hyper-V virtual machines, remove HyperV servers.
  - For a resiliency group consisting Applications, remove Application hosts.
- Retry the create or edit resiliency group operation.

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 added again (8600)

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

Resiliency group task name shows TAKEOVER during evacuation (16466)

When you run the evacuation operation for an Evacuation plan, which consists of resiliency groups that are protected using NetBackup, the Restore operation is performed. But in the **Activities** panel, the task name is displayed as TAKEOVER instead of RESTORE.

Known issues: Multiple Resiliency Managers in a data center

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

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 disaster recovery (DR) operations only from the Resiliency Manager that is associated with the cloud IMS.

Known issues: Guide Me tool

Following are the known issues applicable for the Guide me tool:

Add Data Center task not detected if data centers are already added (17111)

If more than two data centers are added before launching Guide Me, then the tool does not detect the data centers. The Add Data Center tasks does not show as completed.

Workaround:

Select the **Task Completed** checkbox to proceed with further tasks, and manually navigate to the data center details instead of using hyperlinks within Guide Me.

Install Veritas Replication VIB step incorrectly marked as complete (17115, 17160)

Guide Me incorrectly marks the Install Veritas Replication VIB step as complete. This happens if the state of Veritas Replication VIB is Partially Installed or if you launch Guide Me after adding the vCenter server.

Workaround:

Ensure that Veritas Replication VIB is installed properly.

Guide Me does not detect completion of Veritas Replication VIB installation(17137)

If vCenter Server is added and Veritas Replication VIB installation is complete before launching Guide Me, then the tool does not show the task as complete.

Workaround:

Select the **Task Completed** checkbox to proceed with further tasks.

Guide Me fails to detect completion of some tasks (17112)

If you add the IMS to another data center instead of the one mentioned by Guide Me, then the task completion is not detected immediately.

Create gateway pair task is followed by create network pair. Instead of following the sequence if you to create network pair first and then create a gateway pair, then create gateway pair task is marked as complete. Create network pair is not marked as complete.

Workaround:

Either you can select the **Task Completed** checkbox to proceed with further tasks, or you can close Guide Me and relaunch again to see the relevant steps marked as complete.

Chapter 5

Limitations

This chapter includes the following topics:

Limitations when recovering from vCloud Director to vCloud Director.

Resiliency Platform creates independent disks and when you migrate to the target data center, these independent disks get 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.

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\VRTSitrptap\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.

Replication gateways having snapshot are not supported

If a replication gateway has snapshots, then the disaster recovery operations for those resiliency groups that are using the gateway fail.

Snapshot is not supported for Resiliency Manager and IMS virtual appliances

Taking or reverting of snapshot for Resiliency Manager and IMS virtual appliances is not supported.

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.

Virtual machine name limited to 35 characters

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

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 3.2:

- 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 do not get localized.
- MH level tasks do 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** panel are not displayed in Japanese localized UI.
- Guide Me tool does not get localized.

NICs having multiple IP addresses

NICs having multiple IP addresses attached to a single virtual machine is not supported. This is applicable when you are recovering to any supported cloud data centers.