Veritas™ Resiliency Platform Release Notes

3.4

VERITAS™

Veritas Resiliency Platform: Release Notes

Last updated: 2019-09-08

Document version: Document version: 3.4 Rev 0

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

Chapter 1

Release overview

This chapter includes the following topics:

New features and changes in Veritas Resiliency Platform 3.4

This release of Veritas Resiliency Platform includes the following new feature:

See “Support for NetBackup Instant Access to recover a resiliency group” on page 7.

See “Support for NetBackup CloudCatalyst for recovery of virtual machines to AWS ” on page 8.

See “Support for Orange Recovery Engine ” on page 8.

See “Support for recovery from physical to virtual/cloud environment ” on page 8.

See “Enhancements for preparing hosts for replication ” on page 9.

Support for NetBackup Instant Access to recover a resiliency group

Veritas Resiliency Platform 3.4 supports the NetBackup Instant Access feature that supports faster access to data from the backup. When creating or editing a Resiliency Group, you can choose to use the NetBackup Instant Access feature to rehearse and restore assets that are part of the resiliency group.

Using the NetBackup Instant Access feature for rehearsal or recovery of assets provides the following benefits:

- Significant reduction in the recovery time objective during rehearsal
- Zero storage overhead storage usage for test workload instances
- Ability to achieve almost instant startup of test workload instances

For detailed information about managing VMware virtual machines for remote recovery using NetBackup images, see Using NetBackup Instant Access to recover a resiliency group.

Support for NetBackup CloudCatalyst for recovery of virtual machines to AWS

Veritas Resiliency Platform 3.4 supports the recovery of VMware virtual machines to AWS cloud using NetBackup images stored in AWS S3 buckets by the on premises NetBackup CloudCatalyst with Automated DR feature. This functionality is supported in Resiliency Platform only with NetBackup version 8.2 onwards.

To configure recovery of virtual machines to a cloud data center using NetBackup CloudCatalyst with Automated DR, see the following topics:

Prerequisites for integrating NetBackup with Resiliency Platform

Adding NetBackup Cloud Recovery Server (CRS)

Managing VMware virtual machines for remote recovery to AWS cloud using NetBackup images

Support for Orange Recovery Engine

Veritas Resiliency Platform now supports Orange Recovery Engine, which is a public cloud solution. This feature facilitates the following:

- Ability to support Orange Recovery Engine as a target for VMware virtual machines
- Support for recovery/migration from Physical environment to Cloud environment

Support for recovery from physical to virtual/cloud environment

Veritas Resiliency Platform is now enhanced to recover/migrate physical machines to target virtual/cloud environment, which facilitates the following:

- Migrate/Recover a physical workload from an on-premise environment to AWS, Orange Recovery Engine, vCloud Director, and on-premises VMware target environments
- Failback/recover workload from the target environment to the original physical host

- Rehearsal on the target environment

Enhancements for preparing hosts for replication

Veritas Resiliency Platform (VRP) now allows more ways and flexibility to prepare hosts or virtual machines for replication. You can choose any of the available methods, suitable in your environment, to prepare hosts or virtual machines for replication using the Resiliency Platform Data Mover. These enhancements support the following functionalities:

- Select an already discovered virtual machine to prepare it for replication
- Use a non-root privileged user account that has appropriate sudo privileges to prepare Linux workloads for replication
- Deploy and configure Resiliency Platform host agent and replication driver packages manually, on both Windows and Linux workloads, and later prepare them for replication without providing user credentials
- Add, both Linux and Windows workloads, together in the same wizard flow

Using the product documentation

The below table lists the URL where you can find the product documentation, the videos related to Resiliency Platform, and the late break news. The second table lists the various documents that you can refer to along with a brief description of their contents.

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.
https://www.veritas.com/community/business-continuity/videos	The list of Resiliency Platform videos.
https://www.veritas.com/support/en_US/article. 100042657	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 3.4 Overview and planning Guide	The information about the product, its features, and capabilities.
Veritas Resiliency Platform 3.4 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.

More information

- Disaster Recovery to OpenStack is in Tech Preview mode.
- Physical To VMWare (P2V) is in Tech Preview mode.
- The supported upgrade path is Veritas Resiliency Platform 3.2 and later to Veritas Resiliency Platform 3.3.2.

Chapter 2

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.

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

Table 2-1 Minimum configurations

Component	Minimum configuration
Resiliency Manager	Disk space 150 GB RAM 32 GB Virtual CPU 8
Infrastructure Management Server (IMS)	Disk space 60 GB RAM 16 GB Virtual CPU 8

Table 2-1 Minimum configurations *(continued)*

Component	Minimum configuration
Replication Gateway	Disk space 40 GB RAM 16 GB Virtual CPU 8 Additional external thick provisioned disk of 50 GB This staging storage is the minimum needed by Replication Gateway Appliance and up to 4 virtual machines can be configured with this default configuration. Additional virtual machines can be configured by extending this staging storage with the size of 12 GB per virtual machine.
YUM repository server	Disk space 60 GB RAM 4 GB Virtual CPU 2
Hosts to be added to Veritas Resiliency Platform: ■ Application host (applications to be protected) ■ Resiliency Platform Data Mover host (virtual machines to be protected) ■ 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 storage discovery host and as application host, then you need to have at least 30 GB disk space and 8 GB RAM.

Note: You need to reserve the resources for Resiliency Manager, IMS, and Replication Gateway. It ensures 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 HUAWEI CLOUD
- Recovery of physical machines to on-premises data center
- 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

Known issues

This chapter includes the following topics:

General known issues

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

See “A network group becomes faulted if any of its network member is unavailable (VRP-25636)” on page 15.

See “Rehearsal virtual machine Identifier is not same as workload virtual machine Identifier on an upgraded setup (22369)” on page 15.

See “Replace gateway configuration may not get updated in virtual machine’s configuration after Veritas Resiliency Platform is upgraded from 3.3.2 to 3.4 (VRP-25508)” on page 16.

See “Replication becomes inactive after performing the Replace Gateway operation when the gateway has workload's snapshot disks attached (25722)” on page 16.

See “Certain links in the help point to an older help version” on page 16.

A network group becomes faulted if any of its network member is unavailable (VRP-25636)

When any of the network member in a network group is unavailable, the network group becomes faulted. This issue does not get resolved despite editing the network group, and it fails to restore to a normal state.

Workaround:

To resolve the risk associated with impacted Resiliency Groups and faulty Network Group do the following:

1. Update the network member list of the faulted network group by editing the Network Group.
2. Edit all the impacted Resiliency Groups which have Risk "Network Group is in faulted state" associated with them, using the **Edit Configuration or Customize Network** option.

HTML format is not supported for large sized reports (VRP-25649)

In Veritas Resiliency Platform, if the report size is large, typically more than 32MB, then HTML format of that report cannot be generated. This issue occurs because of the database setting of the maximum commit size.

Workaround:

You can generate such reports in PDF or CSV format, as these formats are relatively small in size.

Rehearsal virtual machine Identifier is not same as workload virtual machine Identifier on an upgraded setup (22369)

On an upgraded setup, rehearsal virtual machine Identifier is not same as workload virtual machine Identifier.

Workaround

Edit the Resiliency group to resolve this issue.

Replace gateway configuration may not get updated in virtual machine's configuration after Veritas Resiliency Platform is upgraded from 3.3.2 to 3.4 (VRP-25508)

Replace gateway configuration may not get updated in virtual machine's configuration after Veritas Resiliency Platform is upgraded to 3.4

This occurs in the following scenarios:

- Environment is on prior to 3.4
- Virtual Machine or workloads are migrated or taken-over to target datacenter
- Upgrade to 3.4 is successful as per the upgrade matrix
- Replace gateway is done before taking-over or migrating to the source

Workaround

Migrate the virtual machine/workload back to the source after upgrading to 3.4. After that you can perform the replace gateway operation.

Replication becomes inactive after performing the Replace Gateway operation when the gateway has workload's snapshot disks attached (25722)

If snapshots have been taken on a protected virtual machine and you perform **Replace Gateway** operation for its Replication Gateway appliance, then after a disaster recovery operation on this Resiliency Group, replication state for this protected virtual machine is shown as *Inactive* on the **Resiliency Group Details** page.

Workaround

Perform the Resync operation on the Resiliency Group which will do a full data sync and replication state will be *Active* again.

Certain links in the help point to an older help version

Certain hyperlinks in the Resiliency Platform help may point to topics in a previous version of the help. As a workaround, search for the desired topic in the latest help set.

Navigate to http://help.veritas.com/Welcome?context=VRP_3.4&locale=en_US, to access the latest product documentation.

Known issues: Recovery to Amazon Web services (AWS)

The issues listed for Resiliency Platform Data Mover are also applicable recovery to AWS.

See “Known issues: Resiliency Platform Data Mover” on page 18.

Known issues: Recovery to Azure

The following known issues are applicable to Azure:

See “ Re-sync operation failed with error (25625) ” on page 17.

Re-sync operation failed with error (25625)

The re-sync operation fails with the following error on a SLES machine - No CG configured to perform this action. [52] Command failed.

In an SLES environment, the re-sync operation may sometimes fail due to “No CG configured to perform this action.”. The SLES virtual machine if the system root device is not on multipath. it is possible for multipath to be included in the initramfs. This causes in guest replication CG not be loaded while booting up on migrated virtual machine

Workaround

Manually power off all the migrated virtual machines of the resiliency group and then boot with the parameter multipath=off. Perform Resync operation on migrated CG.

Known issues: Recovery to vCloud

The following known issues are applicable to recovery to vCloud:

In addition to the above listed known issues, the issues listed for Resiliency Platform Data Mover are also applicable.

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.

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 using the **Edit Configuration** intent. 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 (16458)

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 or on-premises data center:

See "If DRL disk gets deleted from a protected asset, then edit RG and delete RG gets stuck stop replication on iotap. (23266)" on page 19.

See "State of Replication Gateway is incorrectly reflected in Veritas Resiliency Platform (22888)" on page 19.

Configuring resiliency group for remote recovery fails during Add disk task (16245)

While configuring a resiliency group for remote recovery the operation sometimes fails during the Add disk task. This happens because VMware updates the instanceUUID of the virtual machine hosting the Replication Gateway. The instanceUUID discovered by Resiliency Platform does not match the current instanceUUID and hence the task fails.

Workaround:

To fix this, complete the following steps in the order mentioned:

1. Delete the resiliency group which was unsuccessfully created.
2. Create a new Replication Gateway pair.
3. Create a new resiliency group using the above gateway pair.

This issue is applicable when the replication technology used is Resiliency Platform Data Mover and Resiliency Platform Data Mover with VMware VAIO (vSphere APIs for IO Filter) interfaces.

If DRL disk gets deleted from a protected asset, then edit RG and delete RG gets stuck stop replication on iotap. (23266)

If DRL disk is accidentally deleted from a protected asset, then edit RG and delete RG gets stuck in the **Stop replication on iotap** task.

Workaround

If DRL disk is accidentally deleted from a protected asset, then edit RG and delete RG gets stuck in the "Stop replication on iotap" task.

State of Replication Gateway is incorrectly reflected in Veritas Resiliency Platform (22888)

Veritas Resiliency Platform expects virtual machines to have unique VM ID.

Workload

Ensure that the hypervisor has unique ID for all the Virtual Machines.

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 "Veritas Replication VIB installation, Upgrade, Resolve & Verify, Create RG, or any DR operation may fail on ESX with errors (22585)" on page 20.

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

vtstap storage policy may be displayed as Incompatible (18287)

On the vCenter server's virtual machine storage policies page, vtstap storage policy may be displayed as Incompatible for some of the datastores of the cluster.

Workaround:

The product functionality is not affected due to this error. However, you can reboot the ESX servers of the cluster to resolve this issue.

Configuring resiliency group for remote recovery fails during Add disk task (16245)

While configuring a resiliency group for remote recovery the operation sometimes fails during the Add disk task. This happens because VMware updates the instanceUUID of the virtual machine hosting the Replication Gateway. The instanceUUID discovered by Resiliency Platform does not match the current instanceUUID and hence the task fails.

Workaround:

To fix this, complete the following steps in the order mentioned:

1. Delete the resiliency group which was unsuccessfully created.
2. Create a new Replication Gateway pair.
3. Create a new resiliency group using the above gateway pair.

This issue is applicable when the replication technology used is Resiliency Platform Data Mover and Resiliency Platform Data Mover with VMware VAIO (vSphere APIs for IO Filter) interfaces.

Veritas Replication VIB installation, Upgrade, Resolve & Verify, Create RG, or any DR operation may fail on ESX with errors (22585)

Veritas Replication VIB installation, Upgrade, Resolve & Verify, Create RG, or any DR operation may fail on ESX with following errors:

"operation failed due to error: Internal error - -1, result: 1" Or “Provider not found or not loadable”

Workaround

Resolution is to restart CIM service either through vCenter or through ESX. Once service is restarted, retry the failed operation through Veritas Resiliency Platform.

Known issues: Recovery from physical environment to virtual machines

The following known issues are applicable to recovery from physical environment to virtual machines:

The sequence of NICs is not maintained during recovery from a physical environment to a virtual machine (VRP-25439)

This issue is applicable if the recovery is from a physical environment to a virtual machine.

In case of recovering from a physical environment to a virtual machine, when multiple NIC IOTAP are migrated to VMware, then there is a possibility that the sequence of NIC is not as same as it was on the on-premise device.

Workaround:

To rectify this issue, do the following:

- Provide the appropriate routes after the migration of IOTAP to VMware is complete.
- Remove the existing gateway rule, if any, and add a rule for default gateway with appropriate NIC.
  For example:
  - *ip route del default via {default_gateway}*
  - *ip route add default via {default_gateway}*

Known issues: Recovery using third-party replication

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

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.

Hyper-V Replica does not replicate any new assets (19084)

Hyper-V Replica does not replicate any new assets such as disks, NICs that are added after the initial configuration of Replica is done. Also no risk is raised for the resiliency group in such a scenario.

Workaround

You can either reinitialize the replication or allow Hyper-V Replica to continue replicating only the initially configured assets.

Known issues: NetBackup integration

See “A virtual machine backed up by multiple NBU master servers gets mapped with only one master server in the console (7608) ” on page 22.

See “Resiliency group task name shows TAKEOVER during evacuation (16466)” on page 22.

See “Issue with support for restoring of UEFI-enabled virtual machines from Netbackup ” on page 23.

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.

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.

Issue with support for restoring of UEFI-enabled virtual machines from Netbackup

Veritas Resiliency Platform does not support restoring of UEFI-enabled virtual machines from Netbackup master server with versions 8.1 and 8.1.1.

Restoring of virtual machines through Veritas Resiliency Platform may fail under certain conditions

Restoring of virtual machines through Veritas Resiliency Platform may fail if all of the below conditions are met:

- The virtual machine contains more than one hard disk.
- Netbackup master server used during the restore operation is at version 8.1 or 8.1.1
- SCSI attachments of hard disk are in out-of-order fashion. For example. Hard disk0 is attached to scsi0:1 while Hard disk1 is attached to scsi0:0.

Known issues: Upgrade

The following known issue is applicable during upgrading of Resiliency Platform:

See “Replace gateway configuration may not get updated in virtual machine’s configuration after Veritas Resiliency Platform is upgraded from 3.3.2 to 3.4 (VRP-25508)” on page 16.

See ““Asset disk configuration changed” risk with description “New disk is attached to virtual machine” may come for RBT disk after upgrade to 3.3.2.0 (23118)” on page 24.

See “Kernel RPM package cannot be recovered if partially installed on VSA during upgrade (22625) ” on page 24.

See “For VC 6.5, VIB upgrade fails because of ESX maintenance mode (22493)” on page 24.

See “New UI alignment is not updated after upgrade in same tab or session (22240)” on page 24.

“Asset disk configuration changed” risk with description “New disk is attached to virtual machine” may come for RBT disk after upgrade to 3.3.2.0 (23118)

After upgrade to 3.3.2.0, “Asset disk configuration changed” risk with description “New disk is attached to virtual machine” may come for RBT disk.

Workaround

If Resiliency group is active for on-premises data center, upgrade respective host’s packages, refresh all hosts, vCenter servers, Hyper-V servers and cloud discovery. After refresh, probe the risk. After performing these steps even if the risk still exists, suppress it before DR operation. If Resiliency group is active on Cloud data center, suppress the risk before DR operation.

Kernel RPM package cannot be recovered if partially installed on VSA during upgrade (22625)

Consider a scenario in which the appliance is rebooted or shut down at **Started upgrade from current_version to update_version** step and new **kernel** RPM package is partially installed on the appliance. In this scenario, bootstrap loader fails to load **kernel** in memory and the appliance fails to boot and directly grub command line is shown to user. All other partially installed RPM packages except kernel package on the appliance can be recovered during upgrade at system start time. If kernel RPM package gets corrupted due to system reboot or shutdown during upgrade, we cannot recover it as boot process of the system fails. Appliance goes in unrecoverable state due to corrupt kernel in it.

New UI alignment is not updated after upgrade in same tab or session (22240)

After upgrade from VRP 3.2 to VRP 3.3.2, New UI alignment is not updated after upgrade.

Workaround

Browser caches HTML to save network bandwidth. You need to relaunch browser or new tab or clear cache to get latest HTML.

For VC 6.5, VIB upgrade fails because of ESX maintenance mode (22493)

In VC 6.5 version if the ESX is in maintenance mode then VIB upgrade fails and manual intervention is needed to resolve this issue.

Workaround

First resolve the ESX maintenance mode issue manually on the VirtualCenter and then rerun the failed VIB upgrade workflow.

False risk of GW is not upgraded popup is shown while performing DR operation after upgrade (22768)

False risk of GW is not upgraded popup is shown while performing DR operation after upgrade.

Workaround

From Resiliency Manager user interface, go to **Settings > Updates**. Select the server and click on **Refresh** button.

Chapter 4

Limitations

This chapter includes the following topics:

General limitations

Hyper-V hosts having snapshots not supported for recovery

A Hyper-V host having snapshots is not supported for recovery on all cloud platforms.

Resiliency Platform does not support disaster recovery operation of HyperV virtual machines, if snapshots are taken on this virtual machine. Resiliency Platform blocks the **Create Resiliency Group** operation if it finds a snapshot of HyperV VM. If you want to take a snapshot of the virutal machine for any reason, after creating a Resiliency Group, then perform the Resiliency Platform disaster recovery operation only after deleting the snapshots.

Restore operation non-functional for 8 hours

If a vCenter server is configured in NetBackup using Java console, then you may not be able to perform a restore operation for next 8 hours.

Windows operating system installed across multiple disks is not supported

If you have Windows Operating System (OS) installed over multiple disks ("system reserved" on disk 0 and OS on disk 1), then such configuration is not supported.

Change of network pairing on target data center is not honored

Change of network pairing is not honored on target data center if resiliency group is active on the target data center. The network pair change is not honored for recovery using Resiliency Platform Data Mover with in-guest replication and NetBackup Cloud DR.

Single NIC having multiple IP addresses of same type are not supported

Single NIC having multiple IP addresses of same type attached to a single virtual machine are not supported.

Snapshot of Resiliency Manager and IMS virtual appliances is supported only for recovering from upgrade failure

In normal circumstances, taking snapshots and restoring from those snapshots is not supported for any of the Resiliency Platform virtual appliances. Resiliency Platform supports taking snapshot of the Resiliency Manager and IMS virtual appliances and restoring from those snapshots only in a situation where something goes wrong during upgrade and the previous state of the appliances needs to be restored.

Taking snapshot and restoring from the snapshot is not supported for Replication Gateway even in the case of an upgrade failure.

DNS customization does not work if FQDN is not defined

If FQDN is not defined for virtual machines running on Hyper-V platform (Linux and Windows), DNS customization does not work.

vLan mapping compulsory for DRS enabled VMware virtual machines having distributed port groups

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.

NIC bonding / NIC teaming is not supported for protected workloads

Workloads under Veritas Resiliency Platform control are expected not to have NIC binding / NIC teaming configured.

Moving an IMS from one datacenter to another is not supported for cloud platforms

Veritas Resiliency Platform does not support moving an Infrastructure Management Server (IMS) from one datacenter or region to another.

Limitations: Recovery to vCloud Director

Resync operation always performs full synchronization of data

The Resync operation performs incremental synchronization when possible. Otherwise, the operation performs full synchronization of data. In the subsequent Resync operations, only incremental synchronization is done. But in case of recovery to vCloud Director, full synchronization of data is done during every Resync operation.

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.

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.

Limitations: Recovery of physical machines to VMware virtual machines

NICs do not get created if subnets are not mapped to VLAN on target data center

If a physical machine on the source data center has multiple NICs, Subnets of all those NICs need to be mapped to a vLAN on the target data center. If you do not map all the subnets to vLAN, then NICs without mapping may not be created for the virtual machine on the target site .

Hosts with gatekeeper devices having duplicate IDs are not supported

If physical machines have gatekeeper devices associated with them and these gatekeeper devices have duplicate IDs, then those physical machines cannot be protected using Resiliency Platform.

CD-ROM attached to the virtual machine does not get deleted

If a physical machine without a CD-ROM gets migrated to a VMware virtual machine, the CD-ROM attached to the virtual machine does not get deleted even after migration of the physical server.

German Operating System not supported

Physical machines with German Operating Systems are not supported for protection using Resiliency Platform.

Limitations: Recovery of VMware virtual machines to on-premises data center using Resiliency Platform Data Mover

Veritas Resiliency Platform cannot protect a virtual machine having same disk UUID for more than one disk of the same VM

Veritas Resiliency Platform cannot distinguish between disks of a virtual machine, if more than one disk share the same disk UUID. Protecting such a machine using Veritas Resiliency Platform will result in failure of DR operations. You can validate this by monitoring the disk count on Veritas Resiliency Platform UI, when creating a Resiliency Group. The disk count shown in Veritas Resiliency Platform UI will be less than that of the actual number of disks of VM.

vSAN storage policy not blocked for virtual machines configured on VMFS

While configuring resiliency groups, you can select vSAN storage policy even for the virtual machines that are configured on VMware VMFS (Virtual Machine File system). In such cases, replication remains in **Inactive (Connected, Inconsistent)** state and does not work.

An incorrect disk entry may be displayed after you attach or detach a disk to the appliance

If you remove a disk and then attach a new disk of different size to the appliance, the size of the previous disk may be displayed instead of the new disk size. In such a scenario where incorrect disk information is displayed, a disk detach operation removes the disk from the appliance but the respective disk entry may still be displayed.

Though the disk information is displayed incorrectly, it does not affect any operation and the operations use the valid disk with correct size.

Kernel version upgrade on SLES 11.4 virtual machine is not supported

Veritas Resiliency Platform does not support kernel version upgrade of SLES 11.4 host managed by Veritas Resiliency Platform. If you upgrade the kernel then the host needs to be reconfigured.

Limitations: Recovery of VMware virtual machines to on-premises data center using third party replication

Long SRDF device group names are not discovered

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

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.

Colon character (:) is not allowed in datastore name

Datastore name should not contain colon character (:) in its name if you want to protect Virtual Machines which are configured on that datastore.

Limitations: Windows hosts for Resiliency Platform Data Mover replication

Following limitations are applicable only for 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 the consistency group is not in **PAUSED** or **STOPPED** state then you need to perform the following steps before initializing the disk:
  - Move the consistency group in maintenance mode.
  - Verify that the consistency group is in **PAUSED | FLOW CONTROL** state on the Windows hosts running the following command on the host:

    `%PROGRAMFILES%\Veritas\VRTSitrptap\cli\vxtapinfo status`
- 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.

Limitations: Localization

The following are a few localization related limitations applicable to Veritas Resiliency Platform 3.4:

- VRP API browser supports English locale only.
- Resiliency Plan task names gets localized but after getting saved once, it does not change on browser locale.
- Email text does not get localized.
- Activities task results do not get localized.
- MH level tasks do not get localized.
- 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.