Veritas™ Resiliency Platform 10.4 Release Notes

VERITAS™

Veritas™ Resiliency Platform Release Notes

Last updated: 2024-09-29

Document version: Document version: 10.4 Rev 0

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

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 10.4

This release of Veritas Resiliency Platform includes security fixes as well as other software fixes.

Using the product documentation

The below table lists the URL where you can find the product documentation and videos related to Resiliency Platform. 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.

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 10.4 Overview and planning Guide	The information about the product, its features, and capabilities.
Veritas Resiliency Platform 10.4 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.
Veritas Resiliency Platform Install and Upgrade Guide	The information about installing and upgrading the Resiliency Platform

More information

- The supported upgrade path is Veritas Resiliency Platform 3.5 and above.
- From version 3.6, only Oracle databases (among non-InfoScale applications) can be configured in resiliency groups for monitoring and DR activities.

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:

Table 2-1 Minimum configurations

Component	Minimum configuration
Resiliency Manager	Disk space 50GB RAM 32 GB Virtual CPU 8 Additional external thick provisioned disk of 100 GB
Infrastructure Management Server (IMS)	Disk space 30 GB RAM 16 GB Virtual CPU 8 Additional external thick provisioned disk of 40 GB

Table 2-1 Minimum configurations *(continued)*

Component	Minimum configuration
Replication Gateway	Disk space 50GB RAM 16 GB Virtual CPU 4 Additional external thick provisioned disk of 50 GB This staging storage is the minimum needed by Replication Gateway Appliance and up to 8 virtual machines can be configured with this default configuration. Additional virtual machines can be configured by extending this staging storage with the size of 6 GB per virtual machine.
Minimum VMware hardware version for Resiliency Platform appliances	13 (ESXi 6.5 and above)
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 CPU 4 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 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 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

Fixed issues

This chapter includes the following topics:

Fixed issues

This chapter lists the issues that have been fixed.

Table 3-1 Fixed issue list

Incident number	Abstract
30039	RM UI appears to be hanged or un-responsive.
30129	Rehearsal and Cleanup rehearsal operation fails if Windows DNS server is only configured for production and Bind DNS server for both production and rehearsal purpose.
30219	Even after the date and time on the Resiliency Manager are in sync, NTP time sync failed risk is raised.
31829	Assets unregistered error may occur while creating resiliency group.
31788	Takeover operation failed as ERS went into read-only mode.
29924	Create resiliency group failed at install PV driver step if the host is configured as domain controller.
31856	DR operation fails if we select volume type as IOPS1/IOPS2 while creating a resiliency group.
14639	Migrate or takeover operation may fail due to unavailability of independent disks on the vCloud Director.

Table 3-1 Fixed issue list *(continued)*

Incident number	Abstract
31606	Sometimes unable to maintain the data consistency (send - receive data) by protected workloads to Replication Gateway.
30055	Create or edit resiliency group fails on a partially upgraded setup using Data Mover with in-guest replication.
31597, 31644	Replication Gateway pairs status changes faulted state after upgrade if only if the Replication Gateway of the gateway pair is upgraded to Resiliency Platform 3.6.
31917	Unable to sync data between Resiliency Managers while upgrading from version 3.4 to 3.5.
29973	Upgrade fails while attempting to upgrade more than 2 RMs in a single data center.
29972	In the NAT setups, the upgrade process is stuck while syncing the data between the Resiliency Managers.
23989	Try different password special characters wherever applicable in Veritas Resiliency Platform.
30672	The error message "1102 = Internal error during licensing check" needs to be improved to address specific issue.
30905	Disable OPTIONS for IMS 14161 port.
30859	Heap dump on resiliency-service due to log statement
30425	Veritas Resiliency Platform changes should not be in base MH files - Snapshot discovery
31720	Severity filter doesn't work in Japanese environment.
30409	Validate that application have application_instance relations while creating resiliency group and raise risk if this happens at later point of time
30603	IP address configuration failed
31399	Failed to register Windows VMware virtual machines in Resiliency Platform version 3.5 rehearsal operation
27678	Replication process is stuck for longer duration
30354	Need help with crash dump analysis for virtual protected by Resiliency Platform.

Table 3-1 Fixed issue list *(continued)*

Incident number	Abstract
30769	Application impacted during snapshot deletion - VMX dump generated
30772	Virtual machine protected by Resiliency Platform reporting hang situation when taking snapshots for them
30935	Resiliency Platform VMware platform resiliency group state hang in configuration state
25711	Differential sync cycle is getting triggered frequently
30963	Veritas Resiliency Platform Data Mover service is crashing on RM in customer environment
30411	Executable permission to the files not getting set while applying hotfix using hotfix framework.
24048	Hyper-V server allowed to be added to 2 IMS on same the data center.
26471	Add message in configure DNS wizard related to key tab to direct to doc for any error
29533	Upgrade process failed at validation step
30369	RHEL7.5 virtual machine does not boot in premise when it is upgraded, while virtual machine is running in cloud and later migrated back to premise after upgrade.
29845	On upgrading the Resiliency Platform to version 3.5, the VBS may be found in configuration failed state.
25722	Replication becomes inactive after performing the Replace Gateway operation when the gateway has workload's snapshot disks attached.
29597	Block replace Replication Gateway in case any peer gateway has any consistency group (CG) in admin wait state.
29632	On upgrading Resiliency Platform to version 3.4 or onwards, followed by replace Replication Gateway on target data centre, replication may become inactive after migration.
33872	Single rule is processed for an event.
33943	Create resiliency group is failing at Start Replication task for multiple resiliency group.

Table 3-1 Fixed issue list *(continued)*

Incident number	Abstract
36113	On triggering "Resync resiliency group" operation, database was unresponsive.
35927	Rehearsal virtual machines are failing to boot up.
35715	Update Error message "vmware tools not found" with more details in case of failure of add application host operation if required ports are not open.
35465	Creating Hyper-V based resiliency group fail with Error: None of the selected Gateway pairs have access to disks on source or target datacenter.
35393	While selecting datastores on IOTAP, create resiliency group fails.
35356	Failed to orchestrate the workflow as the replication is not present in either source or target datacenter.
34022	Heapdumps generated for the ers-query service.
31681	Virtual machine hanged and forcely rebooted by VMwareHA.
34118	[Vmware -> AWS] Edit resiliency group does not have the validation if disk is not accessible to the Replication Gateway.
34116	SRDF SYMCLI : Rehearsal operation failed in Mount datastore step.
34114	Resiliency group should not get stuck in "Configuring" state but recovery should be automated.
33510	Customer should be forced to edit or delete the resiliency group as it gets stuck in "Configuring" state.
34107	Error:"Invalid host name, user name or password." when adding Windows Infoscale Cluster.
34083	Copydata service is not creating the tar bundle.
34073	Add klish option to validate state of CIM and daemon.
34069	Out-of-order processing of IMS updates.
33952	Resiliency group is stuck at "Configuring" state.

Chapter 4

Known issues

This chapter includes the following topics:

General known issues

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

See “Certain links in the help point to an older help version” on page 21.

See “Abruptly powering off the Resiliency Manager resulted into services going in stopped state (27740)” on page 21.

See “Replication lag exceeding RPO risk getting raise/clear frequently (30234)” on page 21.

See “DR operations fail if ESXi server is moved from one vCenter server to another (16287)” on page 22.

See “On performing the recover operation when the risk Existing disk is detached from virtual machine is present on the resiliency group, resync operation may fail.(33645)” on page 22.

See “Migrate operation failed in Post register(veritassr) task (34078).” on page 22.

See “Notification bell icon is not getting updated automatically when risks are raised. (36054)” on page 23.

See “Creating resiliency group for the first time on Windows 2012 and Windows2012 R2 failed.(35858, 35600)” on page 32.

See “Resiliency Platform Datamover operations may fail on the ESXi with error. (36121)” on page 24.

See “While executing reports in pdf format, the reports are stuck. (35885) ” on page 24.

See “Resync operation after recovering the virtual machine may fail with error. (36136)” on page 24.

See “Maintenance mode issue for Suse 12.5 & 15.2. (35454)” on page 24.

See “Risk History report for large amount of data might show errors in the report and count of new or/and closed risks data might be blank. (36080)” on page 25.

See “Enabling secure boot mode after creating the resiliency group is not supported. (36654)” on page 25.

See “Resiliency group with in-guest replication and addition of 100GB disk hits memory cap issue. (9985)” on page 25.

See “Some DR operations for resiliency group like rehearsal, migrate or recovery operations failed for RHEL 8.x and 9.0. (36921) ” on page 26.

See “Activity of adding Cloud Recovery Server (CRS) to Resiliency Manager is not displayed under Activity tab. ” on page 26.

See “Veritas Resiliency Platform integration with Recovery vault version 10.2 and above is not supported. (36923) ” on page 26.

See “Prepare host failed for RHEL version 9.1. (36077)” on page 26.

See “Performed RabbitMQ major version upgrade for version 10.4 (PVM-3772)” on page 26.

See “Session times out in the between the bootstrap process. (36986)” on page 27.

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_10.0&locale=en_US, to access the latest product documentation.

Abruptly powering off the Resiliency Manager resulted into services going in stopped state (27740)

Description: In multiple RM environment, when RM are abruptly powered off it impacts some of critical services and user is unable to login to RM UI.

Resolution:

This would need to be resolved with support user access, hence contact Veritas Support for further assistance.

Replication lag exceeding RPO risk getting raise/clear frequently (30234)

Description: This issue may be seen in the environment where there are multiple RMs deployed; when there are lot of changes in the vCenter server and ESX server configured in Resiliency Platform where large data would get reported by discovery of assets.

Resiliency Manager may take few minutes to process this large discovered data. During this time frame, Resiliency Manager may generate false risks for replication lag as the required inputs from Replication Gateway may take few minutes to get processed.

Workaround: You need to wait for 5-10 minutes for all the false replication lag risks to get cleared. You can login to recovery data center Replication Gateway as admin user and use below Klish command to check actual replication lag.

```
monitor> datamover repl-sets
```

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.

On performing the recover operation when the risk Existing disk is detached from virtual machine is present on the resiliency group, resync operation may fail.(33645)

Resync operation after recover might fail as there is no disk on the source data center, and editing or recreating a resiliency group is not allowed. Due to this, the virtual machine would be stuck in the cloud and there is no simple way to migrate back to the premise using Resiliency Platform console.

Workaround: Need to follow the below steps to resolve this issue.

1. Fetch the disk ID, disk name, and disk size from the database for the disk which is removed.
2. Create the same size disk on the source data center datastore.
3. Change the disk ID of the new disk from IMS to the disk ID of the disk which is removed.
4. Rename the disk from vCenter server to the name of the disk which is removed.
5. Perform resync operation from Resiliency Platform console. Perform migrate operation to source data center. After migration, detach disk risk will be raised on the resiliency group.
6. Perform full edit operation on the resiliency group. Risk is resolved after the edit operation.

Migrate operation failed in Post register(veritassr) task (34078).

Description: If error "Name or service not known" cause any of the DR operations in Resiliency Platform to fail, then perform following steps:

Workaround:

- Check the reason for name resolution failures in the environment and rectify it.
- Retry the failed DR operation.

Notification bell icon is not getting updated automatically when risks are raised. (36054)

Description: It may happen that notifications such as IMS disconnect that does not update bell icon.

Workaround: You need to refresh the page or re-login to display the notification. You can check the notifications on clicking the bell icon or from Notifications UI.

Creating resiliency group for the first time on Windows 2012 and Windows2012 R2 failed.(35858, 35600)

Description: While creating resiliency group for the first time on Windows 2012 and Windows2012 R2, it failed with following error:

```
"Drivers required for target technology [GCP] could not be installed
on this host". These drivers are required to boot this instance on
target data center. Installation failed because of the following
error: Command exit code [255]Global symbol $ver requires explicit
package name (did you forget to declare my $ver?) at
C:ProgramDataVeritasVRTSsfmhspooladdonsstoreVRTSitrptap-9.1.2.0GCPPVDriverinstall_gcp_driver.pl
line 91.Global symbol $ver requires explicit package name (did you
forget to declare my $ver?) at
C:ProgramDataVeritasVRTSsfmhspooladdonsstoreVRTSitrptap-9.1.2.0GCPPVDriverinstall_gcp_driver.pl
line 93.Execution of
C:ProgramDataVeritasVRTSsfmhspooladdonsstoreVRTSitrptap-9.1.2.0GCPPVDriverinstall_gcp_driver.pl
aborted due to compilation errors."
```

Workaround:

- Open below location in Explorer for Windows 2012
  `C:\ProgramData\Veritas\VRTSsfmh\spool\addons\store\VRTSitrptap-9.1.2.0\GCPPVDriver\win6.2.`
- Open below location in Explorer for Windows 2012 R2
  `C:\ProgramData\Veritas\VRTSsfmh\spool\addons\store\VRTSitrptap-9.1.2.0\GCPPVDriver\win6.3.`
- Right click on `vioscsi.inf` .
- Click on **Install**.
- Windows security pop-up confirming about install device driver appears. Click on **Yes** with **Always trust software from "Google LLC** and then perform a DR operation.

Resiliency Platform Datamover operations may fail on the ESXi with error. (36121)

Description: While performing any Resiliency Platform Datamover operations, subtasks may fail at ESXi server with error:

```
<operation name> operation on CG <cgid> failed due to error :
processProviderInvocationRequests: Too many queued requests alr".
```

Workaround:

1. Restart CIM server on ESXi `/etc/init.d/sfcbd-watchdog restart`.
2. Restart IOFilter daemon on ESXi `/etc/init.d/iofilterd-vtstap restart`.

While executing reports in pdf format, the reports are stuck. (35885)

Description: While executing the 'Risk History Report' in pdf format, report get stuck in running state. This happens in case data size for past risks are very large. The reports that are stuck in running state does not have any impact on performance or on the resources.

Workaround: Try to run the reports in other formats (html, csv).

Resync operation after recovering the virtual machine may fail with error. (36136)

Description: This issue may occur when you add or remove(s) disks on source center, migrate resiliency group to the target data center, again add or remove the disks on target data center and migrate or recover back to the different ESX in cluster other than source data center.

This issue may occur in case of multi-node cluster. This scenario is very rare and may hit only in case of you modify the disk configuration on both data center. This issue may not occur in case of single node cluster.

Workaround: Delete the resiliency group and create it again.

Maintenance mode issue for Suse 12.5 & 15.2. (35454)

Description: After performing DR operation, the workload sometimes goes into maintenance mode while booting up on the target site. This issue is similar to the following known issues for SUSE linux -

Devices time out at boot time but appear later

Systemd-udev-settle timing out

Workaround: On the source data center, before performing the DR operation, update following entry in `/etc/default/grub` file of the workload machine as below:

```
GRUB_CMDLINE_LINUX=”rd.udev.event-timeout=300 console=ttyS0
earlyprintk=ttyS0 rootdelay=300
```

You may need to update the grub by `grub2-mkconfig -o /boot/grub2/grub.cfg` command & reboot the workload machine after this.

If the virtual machine on the target data center is already in maintenance mode, perform reboot multiple times, eventually, it will boot normally. Upon the successful reboot, perform above steps to update the grub & reboot.

Note: "console=ttyS0 earlyprintk=ttyS0 rootdelay=300" this setting is just for the investigation purpose to gain the VM console on a cloud.

Risk History report for large amount of data might show errors in the report and count of new or/and closed risks data might be blank. (36080)

Description: Risk History report for large amount of data might show errors in the report and count of new or/and closed risks data might be blank.

Resolution: Use appropriate filters on the risks report to fetch the data.

Enabling secure boot mode after creating the resiliency group is not supported. (36654)

Description: After creating a resiliency group with secure boot mode on, DR operations may fail.

Resiliency group with in-guest replication and addition of 100GB disk hits memory cap issue. (9985)

Description: After creating resiliency group with in-guest replication and adding up 100GB disk, edit the resiliency group. On completing the edit operation, the resiliency group memory_cap error occurs.

Resolution: There are 3 options to clear the cache without interrupting any process or service:

- **1. Clear PageCache only.**

  ```
  sync; echo 1 > /proc/sys/vm/drop_caches
  ```

- **2. Clear dentries and inodes.**

```
sync; echo 2 > /proc/sys/vm/drop_caches
```

- **3. Clear pagecache, dentries, and inodes**

```
.sync; echo 3 > /proc/sys/vm/drop_caches
```

Some DR operations for resiliency group like rehearsal, migrate or recovery operations failed for RHEL 8.x and 9.0. (36921)

Description: On performing rehearsal operation on the resiliency group with RHEL8.x and 9.0, the rehearsal operation failed and the rehearsed virtual machine failed with error occurred: Wait for property [guest.toolsRunningStatus] value to become [guestToolsRunning] has timed out.

Activity of adding Cloud Recovery Server (CRS) to Resiliency Manager is not displayed under Activity tab.

Description: Even after adding Cloud Recovery Server (CRS) to Resiliency Manager, the activity is not displayed in Activities tab.

Veritas Resiliency Platform integration with Recovery vault version 10.2 and above is not supported. (36923)

Description: Recovery vault configuration in NetBackup removed the support of cloud storage account access key. Instead of access key, Recovery Vault team generates ‘Refresh Token’ to configure Recovery Vault in NetBackup primary server.

Discovery of Veritas Resiliency Platform fully depends on access key and the new method of ‘refresh token’ is breaking the current configuration. This new change is from NetBackup version 10.2.

Prepare host failed for RHEL version 9.1. (36077)

Description: The Prepare host step failed as RHEL version 9.1 is not supported.

Performed RabbitMQ major version upgrade for version 10.4 (PVM-3772)

Description: RabbitMQ major version as upgraded in 10.4. Due to this, the RabbitMQ cookie and its associated data folder is cleared as part of this process. To ensure that there is no data loss, no DR operations or discovery operations must be running at the time of upgrade.

Session times out in the between the bootstrap process. (36986)

Description: When you try to bootstrap an appliance on the VMware vCenter server console, the admin session logs out in between the operations.

Resolution: Login to tty1 session using `Alt + F2` and proceed with bootstrap.

Known issues: Recovery to Amazon Web services (AWS)

The following known issues are applicable to AWS:

See " Resiliency group remains offline even after deep start at target data center. (31786)" on page 27.

See "Resync is failed at Start Replication on Windows Host. (34091) " on page 28.

See "After migrating Hyper-V virtual machines to AWS cloud data center with ENA based flavour, resync operation failed. (36177)" on page 28.

See "After migration, on AWS based virtualization target region, you may see inactive replication state for RHEL9.0 workloads. (9984)" on page 28.

See "Create RG fails on AWS for SLES 12.5 with older version of kernel. (36675)" on page 29.

See "Windows 22 IOTAP exited into critical condition after migrate back from AWS to premise data center. " on page 29.

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

See "Known issues: Resiliency Platform Data Mover" on page 33.

Resiliency group remains offline even after deep start at target data center. (31786)

Description: Even after takeover operation is failed in between, try retry operation or perform the deep start on the target data center only. In case of deep start, if source data center is selected, then the resiliency group goes in offline state and to recover from it you need to contact to Veritas Support.

Resolution: To recover from the above mentioned state, you need to contact to Veritas Support.

Resync is failed at Start Replication on Windows Host. (34091)

Description: For a protected workload; respective target instance copy on AWS could be of NVMe type built on a nitro system. If such target is selected for Windows workload especially for W2k12R2; then you may see replication state being inactive post migration.

Resolution:

1. Get IP of the migrated instance from AWS Console. Log in to the instance remotely and verify if target instance fall among following list. Instances built on the Nitro System
2. Check the replication state.
3. Perform a machine restart. Once machine is up and running; login to instance remotely again. Machine should be configured with respective with Consistency Group. Verify the replication state using following command.`vxtapinfo.exe status`
4. Perform Resync on respective resiliency group. This would trigger full synchronization for the workload to maintain data integrity.

After migrating Hyper-V virtual machines to AWS cloud data center with ENA based flavour, resync operation failed. (36177)

Description: On ENA based instance on AWS; the data disks get detached in a boot path for short duration. Disks gets reattached later but it tampers the replication configuration. Hence, the resiliency group is un-configured after boot up with error `No CG configured for W2K16.`

Workaround: Contact Veritas Support to resolve the issue.

After migration, on AWS based virtualization target region, you may see inactive replication state for RHEL9.0 workloads. (9984)

Description: For a protected workload of RHEL 9.0, on the migrated instance on AWS region the replication state is seen as inactive on resiliency group details and instance status check as 1/2 on the AWS console.

Resolution: From the resiliency group details page, stop and start the resiliency group. The replication resumes once the instance is successfully up with network connectivity and the status check is in 2/2 state.

Create RG fails on AWS for SLES 12.5 with older version of kernel. (36675)

Description: While a resiliency group is getting created, the task "Install Extra Drivers on Host" fails for SLES 12.5 virtual machines in case of AWS cloud.

Resolution: You need to update the virtual machines to latest kernel version in 4.12.14-122.XX series.

Windows 22 IOTAP exited into critical condition after migrate back from AWS to premise data center.

Description: For a non-ENA based Windows Server 2022 (W2K22) EC2 instances there were I/O issues on the boot disk in the absence of the DRL disk. This may lead to a data integrity issue.

Workaround: Initiate a resync operation for the respective resiliency group containing the Windows Server 2022 workload. This resync process shall ensure a full synchronisation automatically, thereby ensuring data integrity.

Known issues: Recovery from AWS region to AWS region

The following known issues are applicable to while recovering from AWS region to AWS region:

Reverse replication is not working after migrate back if the instance type is selected as ENA. (146721)

After migration, inactive replication state is seen on AWS based virtualization.(8575)

Reverse replication is not working after migrate back if the instance type is selected as ENA. (146721)

Description: For a protected workload of the respective target instance copy on AWS region of Linux workload; the replication state might be inactive after migration and the instance status check might show as failed. Also the virtual machine screen shot displays virtual machine in emergency mode and the system log shows XFS corruption warning.

Note: This is a known Issue for Linux workloads with XFS filesystem. link

---

Workaround:

1. Perform the steps provided in the below article.
2. Check the instance and replication state after performing above steps.

After migration, inactive replication state is seen on AWS based virtualization.(8575)

Description: For a protected workload for the respective target instance copy on AWS region of Windows workload; they may become inactive post migration.

Workaround:

1. Fetch the IP address of the migrated instance from AWS Console and the log in to the instance remotely.
2. Check for the replication state. It should be mentioned as STOPPED.
3. Perform the resync operation on the respective resiliency group. This would trigger full synchronization for the workload to maintain the data integrity.

Known issues: Recovery to Azure using NetBackup MSDP-C

The following known issues are applicable to while recovering to Azure using MSDP-C:

Restore operation might fail if NetBackup Cloud Recovery Server has version less that 10.1.

Risks related to config drift disk and NetBackup Cloud Recovery Server readiness bundle do not resolve automatically.

See “While upgrading Resiliency Manager to version 10.4, the deployment failed for initial upgrade validation.(36985)” on page 32.

Restore operation might fail if NetBackup Cloud Recovery Server has version less that 10.1.

Description: If you have deployed NetBackup Cloud Recovery Server with less than version 10.1, restore operation might fail.

Resolution: You need to upgrade NetBackup Cloud Recovery Server to version 10.1 or above.

Risks related to config drift disk and NetBackup Cloud Recovery Server readiness bundle do not resolve automatically.

Description: After the restore operation is performed, the risks related to config drift disk and NetBackup Cloud Recovery server readiness bundle risks do not resolve automatically.

Note: After Edit Resiliency group existing backup(s) won't be available for restore.

Resolution: You need to clear the risks by editing the resiliency group and take the backup.

While upgrading Resiliency Manager to version 10.4, the deployment failed for initial upgrade validation.(36985)

Description: The deployment for initial upgrade failed while upgrading Resiliency Manager to version 10.4.

Resolution: You need to restart the Azure Resiliency Manager virtual machine for successful Resiliency Manage upgrade.

Known issues: Recovery to Azure

The following known issue is applicable to Azure:

See “Routing tables are not getting updated properly, hence the host is not getting added to IMS.(33994)” on page 31.

See “On upgrading Resiliency Platform to version 10.0 and above, refresh cloud operations fails.” on page 32.

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

Routing tables are not getting updated properly, hence the host is not getting added to IMS.(33994)

After the migrate operation, the host is not added to the target IMS. Also due to the missing route, host might not reach to other subnets.

Workaround:

You may need to remove the entries *GATEWAY* and *GATEWAYDEV* from the `/etc/sysconfig/network` file since those entries are not required after migrate operation. If the entries are not required, you can remove them when the virtual machine is on the source data center itself, before performing migrate operation.

You may need to start the *xprtld* service using CLI `/opt/VRTSsfmh/adm/xprtldctrl start` command.

Also trigger the *local_ims_attach* script using CLI `/opt/VRTSsfmh/bin/perl /opt/VRTSsfmh/adm/local_ims_attach.pl`.

On upgrading Resiliency Platform to version 10.0 and above, refresh cloud operations fails.

After upgrading to version 10.0 and above, the refresh cloud operations fails.

Workaround: You need to edit the cloud data center operation if any data center is edited in version 4.0.

While upgrading Resiliency Manager to version 10.4, the deployment failed for initial upgrade validation.(36985)

Description: The deployment for initial upgrade failed while upgrading Resiliency Manager to version 10.4.

Resolution: You need to restart the Azure Resiliency Manager virtual machine for successful Resiliency Manage upgrade.

Known issues: Google Cloud Platform

The following known issues are applicable to Google Cloud Platform:

See "Creating resiliency group for the first time on Windows 2012 and Windows2012 R2 failed.(35858, 35600)" on page 32.

Creating resiliency group for the first time on Windows 2012 and Windows2012 R2 failed.(35858, 35600)

Description: While creating resiliency group for the first time on Windows 2012 and Windows2012 R2, it failed with following error:

```
"Drivers required for target technology [GCP] could not be installed on this host". These drivers are required to boot this instance on target data center. Installation failed because of the following error: Command exit code [255]Global symbol $ver requires explicit package name (did you forget to declare my $ver?) at C:ProgramDataVeritasVRTSsfmhspooladdonsstoreVRTSitptap-9.1.2.0GCPPVDriverinstall_gcp_driver.pl line 91.Global symbol $ver requires explicit package name (did you forget to declare my $ver?) at
```

```
C:ProgramDataVeritasVRTSsfmhspooladdonsstoreVRTSitrptap-9.1.2.0GCPPVDriverinstall_gcp_driver.pl
line 93.Execution of
C:ProgramDataVeritasVRTSsfmhspooladdonsstoreVRTSitrptap-9.1.2.0GCPPVDriverinstall_gcp_driver.pl
aborted due to compilation errors."
```

Workaround:

- Open below location in Explorer for Windows 2012
  `C:\ProgramData\Veritas\VRTSsfmh\spool\addons\store\VRTSitrptap-9.1.2.0\GCPPVDriver\win6.2.`
- Open below location in Explorer for Windows 2012 R2
  `C:\ProgramData\Veritas\VRTSsfmh\spool\addons\store\VRTSitrptap-9.1.2.0\GCPPVDriver\win6.3.`
- Right click on `vioscsi.inf .`
- Click on **Install**.
- Windows security pop-up confirming about install device driver appears. Click on **Yes** with **Always trust software from "Google LLC** and then perform a DR operation.

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 Replication Block Tracking (RBT) disk gets deleted from a protected asset, then edit resiliency group and delete resiliency group gets stuck stop replication on IOTAP. (23266)” on page 34.

See “Hyper-V virtualization: State of Replication Gateway is incorrectly reflected in Veritas Resiliency Platform (22888)” on page 34.

See “Refresh VCenter discovery if inaccessible or template virtual machines are present (27564)” on page 35.

See “Cloned virtual machine configured for DR operation, leads to data corruption on the target data center. (30176)” on page 35.

See “False risk may appear for all the configured disks of the resiliency group after Resiliency Manager is upgraded from version 3.4 to 3.6. (31827)” on page 35.

See “Duplicate risks are removed after successful Resiliency Manager and IMS upgrade.” on page 35.

See “ VIB installation fails on vLCM enabled cluster on vSphere 7.0.(31266)” on page 36.

See “Replication Gateway pair may appear in Faulty state even if the individual Replication Gateway state is Healthy. (31898) ” on page 36.

See “No validation message occurs in edit wizard if the Replication Gateway disk capacity exceeds.(118855)” on page 37.

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 Replication Block Tracking (RBT) disk gets deleted from a protected asset, then edit resiliency group and delete resiliency group gets stuck stop replication on IOTAP. (23266)

Description: If Replication Block Tracking (RBT) disk is accidentally deleted from a protected asset, then edit resiliency group and delete resiliency group gets stuck in the **Stop replication on IOTAP** task.

Workaround:

Check the **Continue on failure** flag while editing or deleting the resiliency group in this case.

Hyper-V virtualization: State of Replication Gateway is incorrectly reflected in Veritas Resiliency Platform (22888)

Veritas Resiliency Platform expects virtual machines to have unique VM ID in Hyper-V virtualization environment.

Resolution:

Ensure that the hypervisor has unique ID for all the virtual machines.

Refresh VCenter discovery if inaccessible or template virtual machines are present (27564)

Description: In case a virtual machine in vCenter server has become inaccessible or has been converted to template, those virtual machines will be removed from the Resiliency Platform database after scheduled VMware discovery.

Resolution: You need to refresh the vCenter server if inaccessible or the template virtual machines are present or you want to reflect those changes in Resiliency Platform immediately.

Cloned virtual machine configured for DR operation, leads to data corruption on the target data center. (30176)

Description: In the VMware environment other than VMware on-premises data center , if a virtual machine configured for DR operation is cloned, it leads to data corruption for that virtual machine's replicated data on the target data center. This issue in not applicable for VMware virtual machines on on-premises data center.

Resolution: For such VMware environment excluding the on-premises data center, a protected virtual machines should not be cloned.

False risk may appear for all the configured disks of the resiliency group after Resiliency Manager is upgraded from version 3.4 to 3.6. (31827)

Description: After Resiliency Manager gets upgraded from version 3.4 to 3.6, false risk “Existing disk is detached from virtual machine” may appear for all configured disks of resiliency groups.

Resolution: These risks immediately get cleared after successful IMS upgrade from 3.4 to 3.6 version.

Duplicate risks are removed after successful Resiliency Manager and IMS upgrade.

Description: If there are existing “New disk is attached to virtual machine” risks on version 3.4 then, after successful Resiliency Manager and IMS upgrade, duplicates for all such risks remain for max 30 minutes.

Resolution: Wait for 30 mins for duplicate risks to get removed.

VIB installation fails on vLCM enabled cluster on vSphere 7.0.(31266)

Description: VIB installation fails on vLCM enabled cluster on vSphere 7.0 with error "The agents workflow is blocked until its required solutions are re-mediated externally in vSphere Lifecycle Manager".

Resolution: To resolve this error, perform the below mentioned steps:

1. Manually remediate the cluster hosts from vCenter server to enable Veritas Resiliency Platform Data Mover on the cluster.
2. Refresh the vCenter server from Resiliency Platform.
3. Refer to documentation to create "vtstap" storage policy from vCenter server.

Note: For more references, https://www.veritas.com/support/en_US/article.100044886

Replication Gateway pair may appear in Faulty state even if the individual Replication Gateway state is Healthy. (31898)

Description: Replication Gateway pair state may appear as "Faulted" even when individual Replication Gateways state is showing as "Healthy" in the Data Mover card.

Workaround: Perform below steps:

1. Using Klish menu, stop `txrx` service from any one of the Replication Gateway using below command:

   ```
   manage > services stop txrx
   ```

2. Refresh the same Replication Gateway from the Resiliency Manager web console Data Mover card of the data center.
3. Using Klish menu, start `txrx` service of the Replication Gateway using below command:

   ```
   manage > services start txrx
   ```

4. Refresh the same Replication Gateway from the Resiliency Manager web console Data Mover card of the data center. The Replication Gateway pair state should change to "Connected".

No validation message occurs in edit wizard if the Replication Gateway disk capacity exceeds.(118855)

For a Replication Gateway with disk capacity full, attaching a disk and then detaching a disk on the same Replication Gateway might fail.

Workaround:

You need to manually detach the target side data disk.

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 37.

See “Replace Gateway fails at suspend replication task with error cg-admin error. (29597)” on page 38.

See “After correcting virtual mode RDM disk paths, VMware NRT causes false updates (30201)” on page 38.

See “Recover operation failed while configuration drift on the resiliency group. (33735)” on page 38.

See “Unable to apply IP customization for resiliency group due to subnet for IP not found error. (36184)” on page 38.

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

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.

Replace Gateway fails at suspend replication task with error cg-admin error. (29597)

Description: The replace gateway operation fails at the suspend replication task with error cg-admin error.

Resolution: Try to check if the replication task fails for CG having admin wait and try to resolve it. Try to check the peer gateway for the particular or same CG and replace it first if required.

After correcting virtual mode RDM disk paths, VMware NRT causes false updates (30201)

Description: For a resiliency group having virtual machine with virtual mode RDM disks, after DR operation, the disks attached to the virtual machine could be temporarily in incorrect order.

This order is corrected as part of the DR workflow itself. However, in some cases, the NRT updates are received because of the incorrect order of disks may raise false risks about 'existing disk detached' or 'disk size changed'.

Workaround: You need to refresh the vCenter server.

Recover operation failed while configuration drift on the resiliency group. (33735)

If configuration drift risk is raised on the resiliency group before upgrading to version v4.0, and if you perform recover operation before resolving the configuration drift through edit operation, recover operation fails.

Workaround:

- If a disk is added, recover operation would fail at start virtual machine step. You may need to edit the virtual machine in vCenter server, remove the missing disk controller and start the virtual machine.
- If in case disk is removed, recover operation would fail at attach policy step. Delete and recreate the resiliency group.

Unable to apply IP customization for resiliency group due to subnet for IP not found error. (36184)

Description: This issue is applicable for recovering VMware virtual machines using Resiliency Platform Data Mover in Hypervisor mode. In case of configuring a virtual machine for recovery using Resiliency Platform Data Mover in Hypervisor mode, if the virtual machine has been prepared for replication earlier and then unprepared

before configuring the virtual machine into resiliency group, IP customization cannot be applied for that virtual machine due to subnet for IP address not found error.

Resolution: Remove and re-add the vCenter server before applying IP customization for virtual machine.

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 physical machines with multiple NICs 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 host.

Resolution:

To rectify this issue, do the following:

- Provide the appropriate routes after the migration of physical machines with multiple NICs 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:

See "Hyper-V with 3rd party replication: After creating or editing the resiliency group, immediate DR operations may fail. (28704)" on page 40.

See “Error occurred for while migrating resiliency group configured with IBM replication array.(36971)” on page 40.

See “Error occurred for resiliency group configured with IBM replication array. (36978)” on page 41.

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 Recover 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.

Hyper-V with 3rd party replication: After creating or editing the resiliency group, immediate DR operations may fail. (28704)

Immediately after the resiliency group is created or edited, on invoking any DR operations, it may fail with error "Failed to load [<vm_id>.vmcx] file".

Resolution: You need to check the respective replication interval of the 3rd party replication and wait to replicate the configuration files on the target data center.

Error occurred for while migrating resiliency group configured with IBM replication array.(36971)

Description: An error occurred while migrating the resiliency group configured with IBM replication array with error - "Resiliency group does not have replication information, unable to continue."

Workaround: To resolve the risk, remove the IBM Replication array and re-add to the source datacenter of Resiliency Manager.

Error occurred for resiliency group configured with IBM replication array. (36978)

Description: An error occurred for resiliency group configured with IBM replication array as - `One or more replication consistency groups that are part of this resiliency group no longer has any virtual machine consuming storage from it.`

Workaround: To resolve the risk, remove the IBM Replication array and re-add to the source data center of Resiliency Manager.

Known issues: NetBackup integration

See "A virtual machine backed up by multiple NetBackup primary servers gets mapped with only one primary server in the console (7608) " on page 41.

See "Resiliency group task name shows TAKEOVER during evacuation (16466)" on page 42.

See " Avoid creating or editing the resiliency group for the virtual machines on which backup jobs are running in NetBackup (30210)" on page 42.

See "Avoid executing migrate, recover using replicated data, resync, rehearsal using replicated data or cleanup rehearsal operation for the virtual machines on which backup jobs are running in NetBackup. (36061)" on page 42.

See "In case of multiple active data centers for a resiliency group, only single data center name is displayed instead of showing names of all the active data centers in the UI. (36183)." on page 42.

See "Resiliency Plan scheduled execution failed at Clear Outage for VBS task.(36182)" on page 43.

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

If a virtual machine gets backed up by multiple NetBackup primary servers, it is mapped with only one primary server in the Resiliency Manager console. You can create resiliency group or restore virtual machine only with the mapped primary 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 Recover operation is performed. But in the **Activities** panel, the task name is displayed as TAKEOVER instead of RESTORE.

Avoid creating or editing the resiliency group for the virtual machines on which backup jobs are running in NetBackup (30210)

Description: If backup jobs are running for any Virtual Machine in NetBackup, NetBackup snapshots those virtual machines. As a result, creation/editing of resiliency group during this time will be impacted due to the snapshot state of the Virtual machines. Also, check the VMDKs of the virtual machine while creating or editing a resiliency group in the wizard to ensure that the correct VMDKs are selected by the resiliency group.

Once your backups are complete then you can do edit or create resiliency group operations on those virtual machines.

Workaround: Wait for the backup jobs to complete and then proceed to create / edit resiliency group for the virtual machines.

Avoid executing migrate, recover using replicated data, resync, rehearsal using replicated data or cleanup rehearsal operation for the virtual machines on which backup jobs are running in NetBackup. (36061)

Description: If backup jobs are being executed for any virtual machine in NetBackup, NetBackup takes snapshots of these virtual machines. As a result any replication based operation might be impacted due to the snapshot state of the virtual machines.

Workaround: Wait for the backup jobs to complete and then proceed for the operations.

In case of multiple active data centers for a resiliency group, only single data center name is displayed instead of showing names of all the active data centers in the UI. (36183).

Description: In case of multiple active data centers for resiliency group, only single data center name is displayed instead of showing names of all the active data

centers in the UI. This might be a temporary state for multiple active data centers or if the source data center virtual machines are brought up after recover operation which results in displaying both the data centers as active.

Workaround: There is no impact on the functionality as it is a UI issue. There are no resolution steps.

Resiliency Plan scheduled execution failed at Clear Outage for VBS task.(36182)

Description: If a resiliency plan contains Clear Outage for VBS task, the scheduled execution of resiliency plan fails if user session is used while creating a schedule and that schedule has expired before resiliency plan schedule is executed.

Resolution: Execute the clear outage operation on virtual business service.

Known issues: Upgrade

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

See "For VC 6.5, VIB upgrade fails because of ESX maintenance mode (22493)" on page 43.

See "Notifications of some events that are generated during upgrade process are not shown in the UI. (36204)" on page 43.

See "During upgrade process, upgrade of hosts of SLES 12.4 may hang for more than 3 hours. (36150)" on page 44.

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.

Notifications of some events that are generated during upgrade process are not shown in the UI. (36204)

Description: Events are raised when upgrade is in progress. These events are missed from getting displayed in Notifications Bell in UI because of uninitialized ERS service.

Workaround: To view the events raised during upgrade process, you can go to **Logs** view in the UI and see the notifications log.

During upgrade process, upgrade of hosts of SLES 12.4 may hang for more than 3 hours. (36150)

Description: While upgrading the hosts, the hosts of SLES 12.4 may hang for more than 3 hours.

Resolution: Retry performing the upgrade on the same host.

Known issues: InfoScale clusters

Following is the known issue applicable for InfoScale clusters:

See "Due to the application dependency changes and the discovered top level application service group are no longer at the top level on the InfoScale cluster, the application goes in deleted or unavailable state. (29475)" on page 44.

See "Dashboard view card displays incorrect information for OS count on Hosts by Platform and OS card. (33766)" on page 45.

See "Sometimes there are no risk/notifications if the cluster name configuration is changed. (7156)" on page 45.

See "Adding InfoScale 8.x cluster in Resiliency Platform failed with error. " on page 45.

Due to the application dependency changes and the discovered top level application service group are no longer at the top level on the InfoScale cluster, the application goes in deleted or unavailable state. (29475)

Description: If the application dependency changes on the InfoScale cluster and the discovered top level application service group is no longer at top level, the application goes into deleted / unavailable state.

Resolution: You need to delete the resiliency group and create a new one with the top level application.

Dashboard view card displays incorrect information for OS count on Hosts by Platform and OS card. (33766)

When InfoScale is protected in Resiliency Platform and the setup is upgraded to 4.0 version, the dashboard view card "Hosts by Platform and OS" may show incorrect OS counts.

Workaround:

Reconfigure the clusters without changing any settings. After reconfiguration is successful, the correct count is reflected.

Sometimes there are no risk/notifications if the cluster name configuration is changed. (7156)

Description: If cluster information (i.e name) is changed or needs to be changed in InfoScale while resiliency group is configured or cluster is just added but resiliency group is not configured, then the following steps should be performed.

Workaround: There are two main cases where this issue might appear:

Case: 1 Change the cluster name.

1. Firstly remove the resiliency group, then remove the cluster from the Resiliency Platform.
2. Change the cluster name. (Refer to the *Configuring InfoScale clusters in Resiliency Platforms* topic to change the name.)
3. Add the cluster to Resiliency Platform and then create resiliency group.

Case: 2 If cluster name had been changed while resiliency group was configured.

1. Delete the resiliency group and then delete the cluster from cluster list.
2. Add the cluster again using the cluster host and the create the resiliency group.

Adding InfoScale 8.x cluster in Resiliency Platform failed with error.

Description: While adding InfoScale 8.x cluster in Resiliency Platform, it failed with error "Version of VRTSsfmh package on the host is not supported. Install VRTSsfmh package of version 7.2 or above on the host."

For Resiliency Platform v10.0, InfoScale 8.x is not supported.

Known issues : Continuous Data Protection (CDP)

The following known issue is applicable to CDP in Resiliency Platform:

See “Recover operation of CDP enabled resiliency groups may fail at takeover replication step with error - Could not find recovery point with UUID. (29618)” on page 46.

Recover operation of CDP enabled resiliency groups may fail at takeover replication step with error - Could not find recovery point with UUID. (29618)

Description: It may happen that the selected recovery point may get deleted or converted to larger recovery point by the time recover operation reaches to Replication Data Mover. Hence, the stop replication step may fail for resiliency group where CDP is enabled as it could not find the recovery point with the UUID.

Workaround: Launch the recover operation wizard again and submit by selecting different recovery point.

Known issue: VMware vSphere 7.0 support

The following known issue is applicable to VMware vSphere 7.0 support:

See “On creating resiliency group using VMware VAIO on vSphere 7.0, make sure there are no snapshots of protected virtual machines. (30216)” on page 46.

See “Installation of VIB on vLCM enabled cluster on VMware vSphere 7.0 fails (31266)” on page 47.

See “Storage vMotion fails for Resiliency Platform appliances.(33880)” on page 47.

On creating resiliency group using VMware VAIO on vSphere 7.0, make sure there are no snapshots of protected virtual machines. (30216)

Description: Using VMware VAIO based resiliency group created on vSphere 7.0, before doing migrate or recover operations on it, make sure there are no snapshots of the protected virtual machines.

If there were snapshots for any of the protected virtual machines and rehearsal operation is performed on that data center, it may fail with following error: "Invalid or unsupported virtual machine configuration."

Workaround: Make sure you do not take any snapshots of protected vSphere 7.0 virtual machines before migrate or recover operations to other data centers.

Installation of VIB on vLCM enabled cluster on VMware vSphere 7.0 fails (31266)

Installation of VIB on vLCM enabled cluster on VMware vSphere 7.0 fails with error "The agent's workflow is blocked until it's required solutions are re-mediated externally in vSphere Lifecycle Manager".

Resolution: To resolve this error, perform the below mentioned steps:

1. Manually resolve the cluster hosts from vCenter server to enable Resiliency Platform Data Mover on the cluster.
2. Refresh the vCenter server from Resiliency Platform.
3. Refer Resiliency Platform documentation to create "vtstap" storage policy from the vCenter server.

   KB article

Storage vMotion fails for Resiliency Platform appliances.(33880)

In case of VMware 7.0 or above storage vMotion might fail for any Resiliency Platform appliance. This happens because of the lower hardware version vmx-10 is used to create the appliance.

Workaround:

Power off the appliance and update the hardware version to 14 or above and power on the appliance. It is recommended to use 6.7 above supported Data Mover appliances for VMware 7.0 and above. Refer section Downloading the Veritas Resiliency Platform virtual appliances.

Known issue: Managing security certificates and SSH host keys

See “Add storage enclosure may fail with error “Unable to fetch SSH host key for the host HOSTNAME”. (31790)” on page 47.

Add storage enclosure may fail with error “Unable to fetch SSH host key for the host HOSTNAME”. (31790)

Description: Sometimes **Add storage enclosure** fails with error “Unable to fetch SSH host key for the host HOSTNAME” when **Peer verification** is enabled.

Workaround: You may have to restart the web server on Infrastructure Management Server (IMS) when you are trying to add the enclosure. Follow below steps or Contact Veritas Support for further assistance.

- Login to Infrastructure Management Server (IMS) with support user credentials.
- Execute the command: `/opt/VRTSsfmcs/bin/vomsc --restart web`
- Try to add enclosure again.

Known issues: Recovery of resiliency groups configured using multiple recovery points

See "Delete VM directory task in recover operation using Copy (NetBackup) may fail. " on page 48.

Delete VM directory task in recover operation using Copy (NetBackup) may fail.

In some cases the 'Delete VM Directory' task in recover operation using Copy (NetBackup) may fail due to the disks from that directory are attached to the Replication Gateway. But the overall recover operation does not fail and it should get completed successfully.

Since the original folder is not removed the restore operation from NetBackup primary server creates the different folder with different name. After above situation , any remote recover operation using Copy (NetBackup) to same datacenter without executing the resync/repair operation in between might create new folders and older folder are not deleted.

Workaround:

It is recommended that after every restore operation the resync/repair should be executed to reconfigure the broken replication and to avoid such folders pile up.

Chapter 5

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 virtual machine. If you want to take a snapshot of the virtual 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 virtual machines

Virtual 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.

NVMe controllers in VMware virtual machines are not supported by Resiliency Platform. (30154)

Virtual machines having virtual disks attached to NVMe controllers can be used in Resiliency Platform to create copy based resiliency group if those virtual machines are backed-up by NetBackup. Such virtual machines are not supported for any other type of resiliency group configured in Resiliency Platform.

Resiliency Platform does not support VMware virtual machines which have same BIOS ID as that of any virtual appliances (RM, IMS and Replication Gateway). (26630)

Some of the VMware virtual machines have same BIOS ID and are unable to be uniquely identify the appliance virtual machines. Due to this behavior, they are unable to protect these assets which use these appliances.

Recover point datastores are discovered as type VMFS instead of VMFS6. (30153)

For some datastores, the type is discovered as VMFS even if the actual type is VMFS6. This is seen only with vSphere 7.0 and does not have any impact on any of the DR operations.

The rehearsal operation is not supported from AWS to VMware. (31529)

In 3.6, rehearsal operation from AWS to VMware in case of NetBackup Image Sharing to AWS is not supported, but rehearsal operation from VMware to AWS will be supported as it was earlier.

Infinidat enclosure configuration for VMware and Hyper-V servers

Below are the limitations for VMware and Hyper-V servers:

1. Active-Active replication configurations are not supported.
2. Multi-target replication configuration is not supported.

Risk signature unable to detect the changes made on the target Replication Gateway during upgrade process. (31827)

The “Existing disk is detached from the gateway” risk signature will not be able to detect the changes made on target Replication Gateway during upgrade process.

Resiliency Platform supports only dependent persistent mode for VMware virtual disk. (31695)

Resiliency Platform currently supports only dependent persistent mode for VMware virtual disk. This is applicable to RDM as well and non-RDM disks.

Evacuation plan rehearsal is not getting invoked due to Request timed out error in the wizard due to resiliency group count is increased.

Evacuation plans supports resiliency groups upto 400 only.

Limitations: Recovery to AWS

Resiliency Platform is unable to perform automatic DR for virtual machines from VMware to AWS, if backups are taken by policies which uses ‘storage unit groups’.

If the backups are taken using the policies using 'storage unit group', Resiliency Platform is unable to perform the automatic DR operations for recovery to AWS.

Limitations: Recovery from AWS region to AWS region

Recover operation fails if xls is added as user data in case of data migration of a virtual machine.

While creating resiliency group with user data type as xls, recover operation is failing while migrating the data.

Limitations: Recovery to Azure

Virtual machine with shared disk is not supported. (33027)

The configuration of a shared disk is not supported in Resiliency Platform. More details can be found on About share disk.

Replication Gateway or to be protected virtual machine having boot diagnostic enabled with pre-provisioned storage account managed by Microsoft, operations of Resiliency Platform might fail. (31983)

Boot diagnostics can be used with a custom storage account or with a pre-provisioned storage account managed by Microsoft. If any Replication Gateway or to be protected virtual machine having boot diagnostic enabled with pre-provisioned storage account which is managed by Microsoft; operations of Resiliency Platform might fail.

It is recommended to change this setting either by disabling the boot diagnostic or enable with custom storage account which can be done from Azure console.

Limitations: Recovery to Azure using NetBackup MSDP-C

Multiple NetBackup Cloud Recovery Server in Resiliency Platform is not supported.

Adding multiple NetBackup Cloud Recovery Sever in Resiliency Platform for recovery is not supported.

Storage accounts configured for NetBackup CRS and Resiliency Platform Azure datacenter should be under same Azure subscription.

Storage accounts configured for NetBackup Cloud Recovery Server and Resiliency Platform Azure datacenter should be under same Azure subscription.

Throttling the notification for asset disk configuration drift risk is not supported.

For resiliency groups configured for recovery to Azure using MSDP-C, the risks generated due to asset disk configuration on these resiliency group cannot be throttled.

Limitations: Recovery of resiliency groups configured using multiple recovery points

Following limitations are applicable only for resiliency groups configured using multiple recovery points:

See “Limitations: Recovery of resiliency groups configured using multiple recovery points with Instant Access” on page 54.

See “Limitations: Resync/repair replication for resiliency groups ” on page 55.

See “Limitations: For selective disk restore operation on local and remote data centers. ” on page 56.

See “Limitation: For NetBackup CDP protected virtual machines” on page 56.

Limitations: Recovery of resiliency groups configured using multiple recovery points with Instant Access

Following limitations are applicable only for resiliency groups configured using multiple recovery points with Instant Access:

In recover operation with Copy(NetBackup) path using Instant Access, the target Replication Gateway disks are removed by default.

In recover operation with Copy(NetBackup) path using Instant Access, the target Replication Gateway disks are removed by default as there is no option to preserve them.

Rehearsal operation with Copy(NetBackup) using Instant Access is not supported.

The rehearsal operation with Copy(NetBackup) using Instant Access is not supported and the operation is always completed using full sync of restored virtual machine.

Limitations: Resync/repair replication for resiliency groups

For resiliency groups which are recovered using backup path i.e Copy (Netbackup) technology, you need to perform resync/repair operation to reconfigure the replication for those resiliency groups. Below are the scenarios where resync operation is not supported after **performing the restore operation from NetBackup console**.

- Virtual machines that are restored on the local data center with new instance or BIOS UUID with **Overwrite VM settings**, the current protected virtual machine is deleted.
- Virtual machines that are restored on the local data center with new instance or BIOS UUID with **Do not overwrite VM settings**, the current protected virtual machine is intact.
- Virtual machines that are that are restored with same instance or BIOS UUID on local data center and the disk count or size or SCSI locations are changed.
- Virtual machines that are restored on remote data center with new instance or BIOS UUID, the current protected virtual machine remains intact on local data center.
- Virtual machines that are restored with same instance or BIOS UUID on remote data center, resiliency group displays the restored virtual machine as active on source and target data centers. This behavior is not supported.

Even though the above mentioned points are limitations, there are workaround for the limitations. Refer *Troubleshooting: Resync/repair replication issues for resiliency group configured using Multi-RPO recovery of hosts service objective* for more details.

Limitations: For selective disk restore operation on local and remote data centers.

Below are the scenarios which may occur for selective disk restore operation on local and remote data centers:

Selective disk restore operation on local data center

Configuration drift risk is raised on the resiliency group. It is recommended to edit the resiliency. Refer documentation for handling configuration drift risk details.

Selective disk restore operation on remote data center

Replication with current protected virtual machine will be intact and there will be no impact on current resiliency group. If you want to protect the new virtual with restored disks, create a new resiliency group.

Limitation: For NetBackup CDP protected virtual machines

Unable to select NetBackup CDP protected virtual machines when creating a resiliency group with service objective that supports both NetBackup and Resiliency Platform Data Mover recovery points or the service objective that supports only Resiliency Platform Data Mover recovery points.

A validation error would prevent this configuration if the corresponding NetBackup primary server is configured in Resiliency Platform. So, it is recommended to configure the respective NetBackup primary servers in Resiliency Platform for better visibility and validation of configuration options. If a NetBackup primary server is not configured in Resiliency Platform, it cannot detect the NetBackup CDP protection for virtual machines in that primary server and configuring the Resiliency Platform Data Mover replication for such virtual machines would remove the NetBackup CDP configuration on the ESX servers for those virtual machines.

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 (19641)

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 (19437)

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 (19633)

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 (20112)

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 (19165)

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.

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.

For Replication Gateway, disable the Keep VMDKs together setting in below two cases: (25263)

1. **Replication Gateway is deployed in a datastore cluster:** Immediately after deploying the Replication Gateway, you can create a VM override rule.
2. **Replication Gateway is outside the datastore cluster:** If you select a datastore cluster as target while creating a resiliency group, then after creating the resiliency group apply the rule on the Replication Gateway.

Rehearsal operation failed for virtual machines having SCSI controller with bus sharing (29710)

If a VMware VAIO based resiliency group having virtual machines includes SCSI controller with SCSI bus sharing mode as physical or virtual, then you are unable to perform rehearsal operation on such a resiliency group. For the rehearsal operation, Veritas Resiliency Platform needs to take a snapshot of the virtual machine; if such virtual machine has SCSI controller in SCSI bus sharing mode as physical/virtual then VMware vSphere does not allow snapshot of such a virtual machine. VMware Knowledge Base

The space validation on target datastore may be incorrect if the virtual machines are getting removed while editing a resiliency group. (25232)

While adding new virtual machines to a resiliency group which is protected using Resiliency Platform Data Mover, the space requirements and required space validations on target datastore(s) may not be correct if virtual machines are also getting removed from the resiliency group while editing the same resiliency group. It is recommended to first edit the resiliency group to remove the virtual machines and then edit it again to add new virtual machines.

Datastore cluster not supported if Resiliency Platformis installed using express install. (31895)

In the VMware vSphere environment, if Resiliency Platform is installed using the express install, datastore cluster is not supported.

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.

RDM disk pointer file present on non-replicated storage is not supported (29764)

Resiliency group cannot be configured for remote recovery if it consists of a virtual machine having RDM disk pointer file present on non-replicated storage.

For Infinidat NFS based resiliency group, different export path on source and target data center for qtree is not supported.

While creating Infidata NFS based resiliency group, providing different export path for qtree on source and target data center is not supported.

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: InfoScale

Collecting loggather support for InfoScale hosts from RM is not supported. (34000)

Using Resiliency Platform console, you can gather logs from the Logs->Support page of RM for all the appliances. In case of InfoScale environment, the InfoScale hosts are also listed on this page, and if you select InfoScale host to gather logs, it may fail.

Limitations: Localization

The following are a few localization related limitations applicable to Veritas Resiliency Platform 10.4:

- 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.

Limitation: NetBackup

Resiliency group created with virtual machines from different NetBackup primary server of same version is not supported. (33930)

Resiliency Platform does not support resiliency groups that are created using different NetBackup primary server of same versions.