Veritas™ Resiliency Platform 3.3.1 Release Notes

VERITAS™

Veritas Resiliency Platform: Release Notes

Last updated: 2018-09-26

Document version: Document version: 3.3.1 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 8

New features and changes in Veritas Resiliency Platform 3.3.1 8
Support for IPv6 networks 8
Using the product documentation 9

Chapter 2 System requirements 10

System resource requirements for Resiliency Platform 10
Network and firewall requirements 12

Chapter 3 Known issues 13

General known issues 13
Static IP customization may not work under certain conditions (3862916, 3862237) 14
DNS customization changes are not updated while editing resiliency group (12946) 14
Migrate operation in VMware environment may sometimes fail due to timeout (12642) 14
DR operations fail if ESXi server is moved from one vCenter server to another (16287) 14
False configuration drift related risk raised during certain operations (16803) 15
Validations displayed while configuring resiliency group for remote recovery (10961) 15
Data availability missing for some resiliency groups after a DR operation (19305) 15
Scheduled scan does not clear the risk when the vCenter server is removed and re-added into the IMS (19885) 16
IMS disconnected risk does not get resolved immediately after adding new IMS (19859) 16
Risk or notification is not generated for IP or subnet changes done on source data center (19201) 16
Windows host may appear to be disconnected after migrate back to on-premises data center (19949) 17
Known issues: Recovery to Amazon Web services (AWS) 17

Some DHCP enabled NICs are not present on Cloud after migrate (7407) 17
One or more NICs of a migrated Windows virtual machine may not be visible (7718) 17
Cloud IPs get added to on-premise NICs after migrate back to the on-premise site and reboot (7713) 18
Migrate or takeover operations fail at the Add Network for AWS task and Create Network Interface sub-task (7719) 18
Sometimes network comes up on only one NIC although there are multiple NICs (8232) 19
Delete resiliency group operation fails at Detach volume sub task (19268) 19
Configuring resiliency group for disaster recovery fails at Attach Disk to Replication Gateway sub task (19268) 19
Known issues: Recovery to vCloud 19
Resiliency group details in the console displays stale vCloud virtual machine entries after migrating back a resiliency group to the premises site (8326) 20
Migrate or takeover operation may fail due to unavailability of independent disks on the vCloud Director (14639) 20
After migrating back, the storage profile selection for the existing virtual machine may be incorrect (16901) 20
After migrating back, the IP and MAC addresses assigned to a NIC are displayed incorrect on using Customize Network intent (16885) 20
Known issues: Resiliency Platform Data Mover 20
Recovery data center details are not displayed after upgrade (13024) 21
Replication Gateway pair may appear in faulted state after upgrade (19896) 21
Sometimes replication gets stuck after upgrade or restart of Replication Gateway (19818) 21
Known issues: Resiliency Platform Data Mover used for recovery to on-premises data center 23
Virtual Machine protection using Data Mover has a few policy related limitations (5181) 23
Data Mover virtual machine in no op mode risk cannot be resolved (5183) 23
Cannot delete a resiliency group after editing the resiliency group configured for recovery of VMware virtual machines to on-premises data center (13209) 24
vtstap storage policy may be displayed as Incompatible (18287) 24

Configuring resiliency group for remote recovery fails during Add disk task (16245) 24
Known issues: Recovery using third-party replication 25
DR operations may fail for virtual machines with NFS datastore mounted from a NetApp volume with substring vol 25
In the Hyper-V guest environment, the writable disk is shown in the Read-Only state (3785911) 25
Resiliency groups for Hitachi enclosures are not displayed on dashboard under Top RG by replication lag chart (3861173) 25
Snapshot disk is read only after rehearse operation is performed in Hyper-V with SRDF replication (3862088) 25
Migrate operation for resiliency group using third-party replication may fail due to LUNs getting reported without WWN value (13235) 26
Migrate and resync operations fail when there are stale objects on the source data center (13775) 26
After upgrade to 3.2, create or edit resiliency group operation may fail for applications or Hyper-V virtual machines using 3PAR for replication (16441) 26
Hyper-V Replica does not replicate any new assets (19084) 26
Known issues: NetBackup integration 27
MAC address starting with 00:0c:29 not supported for VMware virtual machines (7103) 27
A virtual machine backed up by multiple NBU master servers gets mapped with only one master server in the console (7608) 27
A transient virtual machine remains in the ESX server in one scenerio (7413) 27
Restore operation may fail if the remote master server gets removed and added again (8600) 27
Resiliency group task name shows TAKEOVER during evacuation (16466) 28
Known issues: Recovery of physical machines 28
Veritas Replication Set information does not get deleted from physical machines when you delete a resiliency group from target data center (19634) 28
Known issues: Recovery of InfoScale applications 28
Remote cluster group dependencies not validated before migrate (3863082) 28
Known issues: Multiple Resiliency Managers in a data center 29
Newly added Resiliency Manager cannot remove the existing offline Resiliency Manager (10821) 29

Data sync fails when multiple Resiliency Managers are configured using IPv6 and IPV4 networks (20505) 29
Known issues: Upgrade 29
Upgrade of Replication Gateway fails if a Veritas Replication Set is in stopping state (19976) 30

Chapter 4 Limitations 31

General limitations 31
Limitations: Recovery to AWS 32
Limitations: Recovery to vCloud Director 33
Limitations: Recovery of physical machines to VMware virtual machines 34
Limitations: Recovery of VMware virtual machines to on-premises data center using Resiliency Platform Data Mover 35
Limitations: Recovery of VMware virtual machines to on-premises data center using third party replication 35
Limitations: Windows hosts for Resiliency Platform Data Mover replication 35
Limitations: Localization 36

Chapter 1

Release overview

This chapter includes the following topics:

- New features and changes in Veritas Resiliency Platform 3.3.1
- Using the product documentation

New features and changes in Veritas Resiliency Platform 3.3.1

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

See "Support for IPv6 networks" on page 8.

Support for IPv6 networks

Resiliency Platform 3.3.1 enables IPv6 network support for configuration of virtual appliances, discovery hosts, VMware vCenter servers, and storage enclosures. All these virtual appliances, hosts, servers, and enclosures can now be configured using both IPv4 and IPv6 addresses. You can also create and map the IPv6 subnets across the data centers for IP customization.

This support for IPv6 networks is limited to the following recovery scenarios:

- Recovery of VMware virtual machines using NetBackup
- Recovery of VMware virtual machines to on-premises data center using Resiliency Platform Data Mover replication technology
- Recovery of VMware virtual machines using the following third-party replication technologies:
  - HPE 3PAR Remote Copy
  - EMC RecoverPoint

- NetApp SnapMirror

There is no upgrade support available for Resiliency Platform 3.3.1. You need to do a fresh installation of Resiliency Platform 3.3.1 in your environment to get the support for IPv6 networks.

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 3.3.1 Overview and planning Guide	The information about the product, its features, and capabilities.
Veritas Resiliency Platform 3.3.1 User Guide	The information about deploying Resiliency Platform and using the product capabilities.
Veritas Resiliency Platform Third-Party Software License Agreements	The information about the third-party software that is used in Resiliency Platform.

Chapter 2

System requirements

This chapter includes the following topics:

- System resource requirements for Resiliency Platform
- Network and firewall requirements

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
YUM repository server	Disk space 60 GB RAM 4 GB Virtual CPU 2
Hosts to be added to Veritas Resiliency Platform: ■ Windows Install host ■ Application host (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 Windows Install host and as application host, then you need to have at least 30 GB disk space and 8 GB RAM. Note that you cannot use a single host as a Windows Install host as well as Resiliency Platform Data Mover host.

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

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

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

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

- Startup memory and minimal memory should be equal to or greater than the amount of memory that the distribution vendor recommends.
- If you are using dynamic memory on a Windows Server 2012 operating system, specify Startup memory, Minimum memory, and Maximum memory parameters

in multiples of 128 megabytes (MB). Failure to do so can lead to dynamic memory failures, and you may not see any memory increase in a guest operating system. Even if you are using dynamic memory, the above mentioned minimum configuration should be met.

Network and firewall requirements

The following ports are used for Veritas Resiliency Platform:

- Recovery of assets to AWS
- Recovery of assets to Azure
- Recovery of assets to vCloud Director
- Recovery of assets to OpenStack
- Recovery of assets to 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
- Known issues: Recovery to Amazon Web services (AWS)
- Known issues: Recovery to vCloud
- Known issues: Resiliency Platform Data Mover
- Known issues: Resiliency Platform Data Mover used for recovery to on-premises data center
- Known issues: Recovery using third-party replication
- Known issues: NetBackup integration
- Known issues: Recovery of physical machines
- Known issues: Recovery of InfoScale applications
- Known issues: Multiple Resiliency Managers in a data center
- Known issues: Upgrade

General known issues

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

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

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

Workaround:

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

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

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

Workaround:

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

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

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

Workaround:

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

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

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

Workaround:

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

False configuration drift related risk raised during certain operations (16803)

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

Scenarios:

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

Workaround:

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

Generic known issue

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

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

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

Workaround:

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

Data availability missing for some resiliency groups after a DR operation (19305)

After performing any DR operation such as migrate or takeover on a resiliency group, the resiliency group details page may not display the data availability for that resiliency group if the resiliency group consists of VMware virtual machines. This may happen because of some stale data in Resiliency Platform database.

Workaround:

go to **Settings -> Infrastructure> Virtualization** and look for the currently active data center for the resiliency group. Select the VCenter server associated with the VMware virtual machine and refresh it.

Scheduled scan does not clear the risk when the vCenter server is removed and re-added into the IMS (19885)

A risk is raised when the vCenter server is removed from the Infrastructure Management Server (IMS). When you re-add the vCenter server to the IMS, the risk is not cleared in the scheduled scan which is done every 3o minutes.

Workaround

If the risk is not cleared from the scheduled scan, you have to probe the risk.

IMS disconnected risk does not get resolved immediately after adding new IMS (19859)

If an IMS Disconnected Risk is raised on some resiliency groups, the risk does not get resolved even after you add a new IMS and then remove the old IMS after moving the assets to the new IMS. Probe on risk does not work in this situation.

Workaround:

You need to wait for 30 minutes, the risk gets resolved after the next scheduled scan.

Risk or notification is not generated for IP or subnet changes done on source data center (19201)

After a resiliency group is configured for disaster recovery, if any changes are done in the IP address or to the subnets on the source data center, no risk or notification is generated.

Workaround

You need to perform the Edit resiliency group operation using the **Edit Configuration** intent so that the data is reflected on the web console. It is recommended that you wait for the hypervisor and the host discoveries to be complete before editing the resiliency group. Or you can refresh the hypervisor and the host using the Resiliency Manager console, and then run the Edit resiliency group operation.

Windows host may appear to be disconnected after migrate back to on-premises data center (19949)

After migrate back to the source data center, the protected Windows host of the resiliency group sometimes may appear to be disconnected from the IMS at source data center.

Workaround

Run the following command on the Windows host:

```
sc query xprtld
```

If the status of the `xprtld` service is displayed as STOPPED, then start the service by running the following command:

```
sc start xprtld
```

Known issues: Recovery to Amazon Web services (AWS)

The following known issues are applicable to AWS:

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

See "Known issues: Resiliency Platform Data Mover" on page 20.

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

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

Workaround:

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

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

After migration, one or more network interface cards (NIC) associated with a Windows virtual machine may not be visible from the operating system. You may

not be able to connect to the migrated virtual machine using the IP address assigned to these invisible NICs.

Workaround:

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

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

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

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

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

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

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

Workaround:

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

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

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

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

Workaround:

Start the virtual machine and manually remove the cloud IPs.

Refresh the host and vCenter server or Hyper-V.

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

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

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

Workaround

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

Delete resiliency group operation fails at Detach volume sub task (19268)

The delete operation fails at “Detach Replicated Disk From Target Gateway" sub task with a timeout error. This happens because in the AWS cloud data center, the volume attached to the Replication Gateway is stuck in ‘detaching’ state.

Workaround

Refer to AWS documentation to resolve the blocked state.

Configuring resiliency group for disaster recovery fails at Attach Disk to Replication Gateway sub task (19268)

While configuring the resiliency group for disaster recovery, the operation fails at “Attach Disk to Replication Gateway” sub task with timeout error. This happens because in the AWS cloud data center, the volume attached to the Replication Gateway is stuck in ‘attaching’ state.

Workaround

Refer to the article on AWS knowledge center to resolve the blocked state.

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.

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

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

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 (16885)

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

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

Known issues: Resiliency Platform Data Mover

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

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

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

Workaround

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

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

Replication Gateway pair may appear in faulted state after upgrade (19896)

At times, the Replication Gateway pair may appear in faulted state after upgrade.

Workaround:

- Using the following klish command, check if any of the gateway services is down:
  `manage services status all`
- If yes, restart the service using the following command:
  `manage services start <service_name>`
- Restart the Replication Gateway.

Sometimes replication gets stuck after upgrade or restart of Replication Gateway (19818)

Sometimes when network between the peer gateways is very slow, the source site gateway enforces flow control on the replication host and pauses the replication for some time. If the gateway is restarted or upgraded during this time when replication is paused, replication is not resumed afterwards and gets stuck in inactive state.

Workaround

To fix the issue and resume the replication

1. Check if the protected host is stuck in flow control mode by running the following command on the host:

   ```
   /opt/VRTSitrptap/bin/vxtapinfo status
   ```

2. If the output is displayed as FLOW CONTROL, then the protected host is in the flow control mode. Perform the following steps to recover the host from flow control and resume the replication:

   - Run the following commands on a Linux protected host:
     - Find Veritas Replication Set ID (CGID) of the resiliency group:
       `/opt/VRTSitrptap/bin/vxtapinfo config`
     - Find the RBT disk or DRL disk (DRL_DISK) :
       `/opt/VRTSitrptap/bin/vxtapdrlfind`
     - Find the current site (SITE_ID) of the resiliency group:
       `/opt/VRTSitrptap/bin/vxtapdrlsign site -drl_dev` *`DRL_DISK`*
     - Pause the replication:
       `/opt/VRTSitrptap/bin/vxtapaction pause -cg` *`CGID`*
     - Modify the source gateway IP of the Veritas Replication Set:
       `/opt/VRTSitrptap/bin/vxtapconfigure modgw -cg` *`CGID`* `-gateway` *`SOURCE_GW_IP`* `:33056 -site` *`SITE_ID`*
     - Persist the configuration:
       `/opt/VRTSitrptap/bin/vxtapconfigure persist`
     - Resume the replication of the Veritas Replication Set:
       `/opt/VRTSitrptap/bin/vxtapaction resume -cg` *`CGID`*
   - Run the following commands on a Windows protected host:
     - Find Veritas Replication Set ID (CGID) of the resiliency group:
       `c:\Program Files\Veritas\VRTSitrptap\cli\vxtapinfo config`
     - Find the RBT disk or DRL disk (DRL_DISK) :
       `c:\Program Files\Veritas\VRTSitrptap\cli\vxtapdrlfind`
     - Find the current site (SITE_ID) of the resiliency group:
       `c:\Program Files\Veritas\VRTSitrptap\cli\vxtapdrlsign site -drl_dev` *`DRL_DISK`*
     - Pause the replication:
       `c:\Program Files\Veritas\VRTSitrptap\cli\vxtapaction pause -cg` *`CGID`*

- Modify the source gateway IP of the Veritas Replication Set:
  `c:\Program Files\Veritas\VRTSitrptap\cli\vxtapconfigure modgw -cg CGID -gateway SOURCE_GW_IP :33056 -site SITE_ID`
- Persist the configuration:
  `c:\Program Files\Veritas\VRTSitrptap\cli\vxtapconfigure persist`
- Resume the replication of the Veritas Replication Set:
  `c:\Program Files\Veritas\VRTSitrptap\cli\vxtapaction resume -cg CGID`

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:

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

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

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

Workaround:

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

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

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

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

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

Workaround:

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

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.

Known issues: Recovery using third-party replication

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

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

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

Workaround:

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

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

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

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

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

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

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

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

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

Workaround:

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

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

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

Workaround:

Add the enclosure again.

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

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

Workaround:

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

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

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

Workaround:

Remove the assets from Resiliency Platform and then re-add. Retry the create or edit resiliency group operation.

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

The following known issues are applicable to NetBackup integration:

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

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

Workaround:

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

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

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

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

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

Workaround:

Restart the services on the vCenter server.

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

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

Workaround:

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

Resiliency group task name shows TAKEOVER during evacuation (16466)

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

Known issues: Recovery of physical machines

Following is the known issue applicable for recovery of physical machines to VMware environment:

Veritas Replication Set information does not get deleted from physical machines when you delete a resiliency group from target data center (19634)

If a resiliency group is deleted from the target data center, the corresponding Veritas Replication set information does not get deleted from the physical machines at source data center.

Workaround

You need to manually cleanup the corresponding Veritas Replication set information on the physical machine and unsign the Replication Block Tracking (RBT) disk.

Known issues: Recovery of InfoScale applications

The following known issue is applicable when recovering InfoScale applications:

Remote cluster group dependencies not validated before migrate (3863082)

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

Known issues: Multiple Resiliency Managers in a data center

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

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

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

Workaround:

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

```
services rm restart db
```

Now you can remove the offline Resiliency Manager.

Data sync fails when multiple Resiliency Managers are configured using IPv6 and IPV4 networks (20505)

Consider the following scenario in which there are multiple Resiliency Managers configured in a resiliency domain:

NIC of Resiliency Manager 1 has IPV6 network and that of Resiliency Manager 2 has IPV4 and IPV6 networks or Resiliency Manager 2 has IPv6 network only. Resiliency Manager 2 is joined or connected to existing Resiliency Manager 1, powered off, and then powered on. The state of data on Resiliency Manager 2 is displayed as Connected (Data sync failed). The Data resync operation also fails to synchronize the data.

Workaround:

Contact Veritas support.

Known issues: Upgrade

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

Upgrade of Replication Gateway fails if a Veritas Replication Set is in stopping state (19976)

While upgrading a Replication Gateway, the operation fails if one or more Veritas Replication Sets are in ‘stopping’ state.

Workaround

Identify the Veritas Replication Sets associated with the Replication Gateway which are in ‘stopping’ state. Abort the replication for these sets and then retry to upgrade the gateway. You can abort the process using the KLISH menu: Datamover->Operation-> Abort.

Chapter 4

Limitations

This chapter includes the following topics:

- General limitations
- Limitations: Recovery to AWS
- Limitations: Recovery to vCloud Director
- Limitations: Recovery of physical machines to VMware virtual machines
- Limitations: Recovery of VMware virtual machines to on-premises data center using Resiliency Platform Data Mover
- Limitations: Recovery of VMware virtual machines to on-premises data center using third party replication
- Limitations: Windows hosts for Resiliency Platform Data Mover replication
- Limitations: Localization

General limitations

NICs having multiple IP addresses is not supported

NICs having multiple IP addresses attached to a single virtual machine is not supported.

Pairing of subnets having same ID is not supported

If you pair two subnets having same ID, the subnet pairing is completed without any error but the pairing does not work.

Virtual machines of Hyper-V servers are discovered even when Hyper-V server is added as Windows Install host

In Veritas Resiliency Platform, a Hyper-V server is expected to be added as a Virtualization server. But even if the Hyper-V server gets added as a Replication host or Windows Install host, the virtual machines of that hyper-V servers get listed under **Unmanaged** tab in the resiliency Manager console. These virtual machines cannot be protected using Resiliency Platform.

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.

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

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

Limitations: Recovery to AWS

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

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

Limitations: Recovery to vCloud Director

Resync operation always performs full synchronization of data

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

Manual cleanup required on physical machine if resiliency group is deleted from target data center

If a resiliency group is deleted from target data center, you need to manually cleanup the corresponding Veritas Replication set information on the physical machine and unsign the Replication Block Tracking (RBT) disk.

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.

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.

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

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.

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.

Limitations: Windows hosts for Resiliency Platform Data Mover replication

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

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

Limitations: Localization

The following are a few localization related limitations applicable to Veritas Resiliency Platform 3.3.1:

- Resiliency Plan task names gets localized but after getting saved once, it does not change on browser locale.
- Notification text does not get localized.
- Email text does not get localized.
- Activities task results do not get localized.
- MH level tasks do not get localized.
- For German AD, User's group name is mandatory.
- If IP customization is done, then on the **Configuration of Resiliency Group** page, **IP Customization Details** table is displayed. This table is not displayed in Japanese and German localized UI.
- Some fields in the **Schedule Report** panel are not displayed in Japanese localized UI.
- 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.