Veritas™ Resiliency Platform 3.3.2 Release Notes

VERITAS™

Veritas Resiliency Platform: Release Notes

Last updated: 2019-02-03

Document version: Document version: 3.3.2 Rev 0

Legal Notice

Copyright © 2019 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, Veritas InfoScale, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party (“Third-Party Programs”). Some of the Third-Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the third-party legal notices document accompanying this Veritas product or available at:

https://www.veritas.com/licensing/process

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

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

https://sort.veritas.com/documents

Documentation feedback

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

vrpdocs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1

Release overview

This chapter includes the following topics:

New features and changes in Veritas Resiliency Platform 3.3.2

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

See “Removal of Windows Install Hosts” on page 8.

See “Monitoring API support” on page 8.

See “Replace faulty or healthy gateway” on page 8.

See “Simplified licensing” on page 8.

See “Extended In-Guest IOTAP” on page 8.

See “Mark Resiliency Group in maintenance mode” on page 8.

See “Collect logs from Veritas Resiliency Platform appliances from the user interface” on page 8.

See “Service pack delivery mechanism” on page 8.

See “Localization support is extended to Chinese language” on page 9.

See “Improved user interface” on page 9.

See “Separate Security Group for rehearsal and disaster recovery operations” on page 9.

See “Introduced new risk signatures” on page 9.

Removal of Windows Install Hosts

Veritas Resiliency Platform does not need Windows Install Hosts to add Windows hosts anymore. Any existing Windows Install Hosts that are added to Veritas Resiliency Platform can be safely removed from the resiliency manager console.

Monitoring API support

Monitoring API support to meet your need of integrating Veritas Resiliency Platform into your monitoring dashboards and automation tools.

Replace faulty or healthy gateway

Ability to replace faulty or healthy gateway without affecting the Recovery Time Objective.

Simplified licensing

Simplified licensing by consolidating SKU for Per-GB license under Per-Virtual Machine.

Extended In-Guest IOTAP

Extended In-Guest IOTAP support to:

- CentOS 6.x,7.0 to 7.4
- SUSE 11.4, 12.2, 12.3

Mark Resiliency Group in maintenance mode

Customers are enabled to mark Resiliency Group in maintenance mode to avoid doing disaster recovery operations accidentally and raising false risks.

Collect logs from Veritas Resiliency Platform appliances from the user interface

Ability to collect logs from various Veritas Resiliency Platform appliances from the user interface.

Service pack delivery mechanism

Ability to apply hotfixes easily with enhanced service pack delivery mechanism.

Localization support is extended to Chinese language

Localization support is extended to Chinese language to facilitate users in China region.

Improved user interface

Improved user interface with enhanced charts on dashboard. The user interface also reflects near real time Cloud Discovery state.

Separate Security Group for rehearsal and disaster recovery operations

Ability to have separate Security Group for rehearsal and disaster recovery operations for AWS.

Introduced new risk signatures

Introduced new risk signatures to detect changes in the network configuration like subnet mapping changed, IP changed on the source.

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 3.3.2 Overview and planning Guide	The information about the product, its features, and capabilities.
Veritas Resiliency Platform 3.3.2 User Guide	The information about deploying Resiliency Platform and using the product capabilities.
Veritas Resiliency Platform Third-Party Software License Agreements	The information about the third-party software that is used in Resiliency Platform.

More information

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

Chapter 2

System requirements

This chapter includes the following topics:

System resource requirements for Resiliency Platform

The amount of virtual CPUs, memory, and disk space that Veritas Resiliency Platform requires are listed in this section.

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

Table 2-1 Minimum configurations

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

Table 2-1 Minimum configurations *(continued)*

Component	Minimum configuration
Replication Gateway	Disk space 40 GB RAM 16 GB Virtual CPU 8 Additional external thick provisioned disk of 50 GB This staging storage is the minimum needed by Replication Gateway Appliance and up to 4 virtual machines can be configured with this default configuration. Additional virtual machines can be configured by extending this staging storage with the size of 12 GB per virtual machine.
YUM repository server	Disk space 60 GB RAM 4 GB Virtual CPU 2
Hosts to be added to Veritas Resiliency Platform: ■ Application host (applications to be protected) ■ Resiliency Platform Data Mover host (virtual machines to be protected) ■ Storage discovery host ■ Hyper-V host	Disk space 15 GB RAM 4 GB Dual processor CPU If you are using a single host for multiple purposes, add the disk space and RAM required for each purpose. For example, if you are using a single host as storage discovery host and as application host, then you need to have at least 30 GB disk space and 8 GB RAM.

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

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

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

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

- Startup memory and minimal memory should be equal to or greater than the amount of memory that the distribution vendor recommends.
- If you are using dynamic memory on a Windows Server 2012 operating system, specify Startup memory, Minimum memory, and Maximum memory parameters in multiples of 128 megabytes (MB). Failure to do so can lead to dynamic memory failures, and you may not see any memory increase in a guest operating system.
  Even if you are using dynamic memory, the above mentioned minimum configuration should be met.

Network and firewall requirements

The following ports are used for Veritas Resiliency Platform:

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

Chapter 3

Fixed issues

This chapter includes the following topics:

Fixed issues

This chapter lists the issues that have been fixed in the Veritas Resiliency Platform 3.3.2 release.

Table 3-1 Issues fixed in Veritas Resiliency Platform 3.3.2

Incident number	Abstract
12946	DNS customization changes are not updated while editing resiliency group
19305	Data availability missing for some resiliency groups after a DR operation
19885	Scheduled scan does not clear the risk when the vCenter server is removed and re-added into the IMS
19859	IMS disconnected risk does not get resolved immediately after adding new IMS
19949	Windows host may appear to be disconnected after migrate back to on-premises data center
7407	Some DHCP enabled NICs are not present on Cloud after migrate
8232	Sometimes network comes up on only one NIC on virtual machines having multiple NICs

Table 3-1 Issues fixed in Veritas Resiliency Platform 3.3.2 *(continued)*

Incident number	Abstract
8326	Resiliency group details in the console displays stale vCloud virtual machine entries after migrating back a resiliency group to the premises site
13024	Recovery data center details are not displayed after upgrade if the disk name is greater than 128 characters
19818	Sometimes replication gets stuck after upgrade or restart of Replication Gateway
5181	Virtual machine protection using Resiliency Platform Data Mover has a few policy related limitations
5183	Data Mover virtual machine in no op mode risk cannot be resolved
10821	Newly added Resiliency Manager cannot remove the existing offline Resiliency Manager

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 “Migrate operation in VMware environment may sometimes fail due to timeout (12642)” on page 17.

See “RG creation for Virtual machines that replicated by NetApp SnapMirror, fails with error (23189)” on page 17.

See “Rehearsal virtual machine Identifier is not same as workload virtual machine Identifier on an upgraded setup (22369)” on page 17.

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.

RG creation for Virtual machines that replicated by NetApp SnapMirror, fails with error (23189)

It may occur if Veritas Resiliency Platform setup was upgraded from some version before 3.3.2. Veritas Resiliency Platform communicates with NetApp Array using ONTAP APIs. The data that NetApp Array returns is sometimes inconsistent in the number of records. It causes Veritas Resiliency Platform to think that some objects such as SnapMirror configurations or LUN maskings are deleted from the array. The issue is fixed in Veritas Resiliency Platform 3.3.2, but the data that was deleted from Veritas Resiliency Platform cannot be reconstructed automatically by Veritas Resiliency Platform after upgrade to 3.3.2.

Workaround

Remove the NetApp configuration from Veritas Resiliency Platform and add it back.

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

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

Workaround

Edit the Resiliency group to resolve this issue.

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 19.

Delete resiliency group operation fails at Detach volume sub task (12804)

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 (12804)

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.

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

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

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

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

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

Workaround

To fix this, verify the storage profile of the existing virtual machine using the **Edit Configuration** intent. If the storage profile displayed is incorrect, change it to the appropriate value.

After migrating back, the IP and MAC addresses assigned to a NIC are displayed incorrect on using Customize Network intent (16458)

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

Workaround

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

Known issues: Resiliency Platform Data Mover

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

See "If DRL disk gets deleted from a protected asset, then edit RG and delete RG gets stuck stop replication on iotap. (23266)" on page 20.

See "State of Replication Gateway is incorrectly reflected in Veritas Resiliency Platform (22888)" on page 20.

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

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

Workaround:

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

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

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

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

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

Workaround

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

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

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

Workload

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

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

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

See “Veritas Replication VIB installation, Upgrade, Resolve & Verify, Create RG, or any DR operation may fail on ESX with errors (22585)” on page 21.

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

vtstap storage policy may be displayed as Incompatible (18287)

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

Workaround:

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

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

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

Workaround:

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

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

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

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

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

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

Workaround

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

Known issues: Recovery using third-party replication

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

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

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

Workaround:

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

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

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

Workaround

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

Known issues: NetBackup integration

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.

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 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: Upgrade

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

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

See "Kernel RPM package cannot be recovered if partially installed on VSA during upgrade (22625) " on page 25.

See "For VC 6.5, VIB upgrade fails because of ESX maintenance mode (22493)" on page 25.

See "New UI alignment is not updated after upgrade in same tab or session (22240)" on page 25.

See "False risk of GW is not upgraded popup is shown while performing DR operation after upgrade (22768)" on page 25.

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.

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

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

Workaround

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

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

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

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

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

Workaround

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

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

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

Workaround

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

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

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

Workaround

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

Chapter 5

Limitations

This chapter includes the following topics:

General limitations

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

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

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

In normal circumstances, taking snapshots and restoring from those snapshots is not supported for any of the Resiliency Platform virtual appliances. Resiliency Platform supports taking snapshot of the Resiliency Manager and IMS virtual

appliances and restoring from those snapshots only in a situation where something goes wrong during upgrade and the previous state of the appliances needs to be restored.

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

DNS customization does not work if FQDN is not defined

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

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

If vSphere DRS is enabled for a VMware HA cluster and virtual machine has port group attached from distributed switch, then you must do vLan mapping for successfully performing the migrate operation. This is applicable only to vCenter server and ESXi version lower than 6.5.

NIC bonding / NIC teaming is not supported for protected workloads

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

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

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

Limitations: Recovery to 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 .

Hosts with gatekeeper devices having duplicate IDs are not supported

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

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

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

German Operating System not supported

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

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

vSAN storage policy not blocked for virtual machines configured on VMFS

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

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

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

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

Kernel version upgrade on SLES 11.4 virtual machine is not supported

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

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

Long SRDF device group names are not discovered

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

Rehearsal is not supported if volume is configured using asynchronous replication in IBM XIV enclosure

If the consistency group or the volume is configured using asynchronous replication in IBM XIV array, then the snapshot operation is not supported by XIV enclosure. Hence if the resiliency group is configured with virtual machines that are using asynchronous consistency group or volume-based replication, then the rehearsal operation fails at the ‘create snapshot’ step.

Colon character (:) is not allowed in datastore name

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

Limitations: Windows hosts for Resiliency Platform Data Mover replication

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

- To perform the Initialize Disk operation, consistency group must be in PAUSED or STOPPED state.
- If the consistency group is not in **PAUSED** or **STOPPED** state then you need to perform the following steps before initializing the disk:
  - Move the consistency group in maintenance mode.

    - Verify that the consistency group is in **PAUSED | FLOW CONTROL** state on the Windows hosts running the following command on the host:

      `/opt/VRTSitrptap/bin/vxtapinfo status`

- If system recovery is done manually, then you need to first stop the replication and then start the replication using the CLI.
    - “C:\Program Files\Veritas\VRTSitrptap\cli\vxtapaction.exe” stop –cg <*CGID*>
    - “C:\Program Files\Veritas\VRTSitrptap\cli\vxtapaction.exe” start –cg <*CGID*> where *CGID* is the consistency group ID.

Limitations: Localization

The following are a few localization related limitations applicable to Veritas Resiliency Platform 3.3.2:

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