Veritas™ Resiliency Platform 3.0 Release Notes

VERITAS™

Veritas Resiliency Platform: Release Notes

Last updated: 2017-08-15

Document version: Document version: 3.0 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:

doc.feedback@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

Overview

This chapter includes the following topics:

About Veritas Resiliency Platform

Veritas Resiliency Platform offers a unified solution that helps you proactively maintain business uptime across private, public, and hybrid clouds. Resiliency Platform gives you complete automation for all resiliency operations involving the virtual machines, applications, and multi-tier business-services in your data center. It safeguards the current technology investments by plugging into your existing environments and infrastructure.

For data replication, you can use the Resiliency Platform Data Mover or any third-party solution that is supported by Veritas Resiliency Platform. For a list of supported vendors and products, see *Veritas Resiliency Platform Hardware and Software Compatibility Guide*.

Resiliency Platform Data Mover is a separately licensed feature of Veritas Resiliency Platform. It provides data replication between geographically separated data centers facilitating an effective disaster recovery solution. The Resiliency Platform Data Mover can be used for the following purposes:

- For recovery of VMware virtual machines to on-premises data center
- For recovery of VMware and Hyper-V virtual machines to cloud data center

Resiliency Platform has the following core capabilities:

Security and Compliance	Veritas Resiliency Platform provides enhanced data encryption for data-in-flight.
Predictability	Customers can predictably meet critical business Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
Compliance	Customers can prove compliance to internal and external business continuity mandates with audit reporting and non-disruptive, real-time disaster recovery testing.
Automation	Customers get complete automation for all resiliency operations including recovery run books, and start and stop recovery orchestration for multi-tier applications. This reduces risk of downtime from human error.
Flexibility	Customers get the flexibility to keep their existing infrastructures and can innovate on their terms, with the flexibility that Resiliency Platform provides, to enable workload migration across sites and even to the cloud.

See "About Resiliency Platform features and components" on page 9.

About Resiliency Platform features and components

The following is a brief introduction to Veritas Resiliency Platform key components and their relationships. Administrators responsible for deploying and configuring the product need to understand these in more detail.

Resiliency Manager	The component that provides resiliency capabilities within a resiliency domain. It is composed of loosely coupled services, a distributed data repository, and a management console. The Resiliency Manager is deployed as a virtual appliance.
Infrastructure Management Server (IMS)	The component that discovers, monitors, and manages the asset infrastructure within a data center. The IMS transmits information about the asset infrastructure to the Resiliency Manager. The IMS is deployed as a virtual appliance. To achieve scale, multiple IMSs can be deployed in the same data center.

Veritas InfoScale Operations Manager Management Server	The component that allows discovery of InfoScale applications that are already configured in Veritas InfoScale Operations Manager, also referred to as Veritas InfoScale Operations Manager server. You can manage the InfoScale applications that are already configured in Veritas InfoScale Operations Manager on Linux, Solaris, AIX as well as Windows platform. You need to add this component only if you want to manage and recover the Infoscale applications that are already configured in Veritas InfoScale Operations Manager.
NetBackup Server	The component that allows restoration of virtual machines to a local or remote data center using NetBackup generated backup images. You need to add this component only if you want to restore the virtual machines using NetBackup generated backup images.
Replication Gateway	The component of Veritas Resiliency Platform Data Mover that is deployed as a virtual appliance on both data centers and used to perform replication between the data centers. If you plan to use any third party replication technology, you do not need to deploy Replication Gateway.
resiliency domain	The logical scope of a Resiliency Platform deployment. It can extend across multiple data centers.
data center	For a disaster recovery use case, the resiliency domain must contain at least two data centers in different locations, a production data center and recovery data center. Each data center has a Resiliency Manager and one or more IMSs. If you are using Resiliency Platform Data Mover for replication, each data center must also have at least one Replication Gateway.
asset infrastructure	The data center assets that you add to Resiliency Platform for discovery and monitoring by the IMS. The asset infrastructure can include hosts (Windows or Linux servers), virtualization servers for Hyper-V and VMware, and enclosures (storage arrays). Once the asset infrastructure is discovered by the IMS, the discovered virtual machines or applications are listed in the console as assets to manage or protect.

resiliency group	The unit of management and control in Resiliency Platform. You organize related assets into a resiliency group and manage and monitor them as a single entity.
service objective	A template to define the type of operations and technologies that are supported for a group of assets. You apply a service objective to each resiliency group. A template which identifies the characteristics of a service. These could be availability related characteristics such as local redundancy, and number of nodes in a cluster or DR characteristics such as remote recovery, Recovery Point Objective (RPO) SLAs, rehearsal support etc. Service objective is applied when a group of assets are being added to a resiliency group. Resiliency Platform monitors the resiliency groups based on the service objective definition and raises the risks as applicable.
Virtual Business Service (VBS)	A multi-tier business service where each VBS tier hosts one or more resiliency groups. A VBS lets you group multiple services as a single unit for visualization, automation, and controlled start and stop in the desired order. VBS uses the vertical grouping mechanism to group the multiple services. You can perform the disaster recovery operations on the entire VBS.

New features and changes in Veritas Resiliency Platform 3.0

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

Automated disaster recovery and migration support for Microsoft Azure

Veritas Resiliency Platform 3.0 introduces the support for recovery of the data center assets to Microsoft Azure. You can configure and protect your VMware and Hyper-V virtual machines for recovery to Azure using the Resiliency Platform Data Mover.

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

Enhanced support for vCloud Director

Resiliency Platform 3.0 introduces the support for recovery of VMware and Hyper-V virtual machines to vCloud Director without adding the vCenter server or Hyper-V servers. This feature can help you perform disaster recovery of virtual machines even without accessing the VMware or Hyper-V servers.

Internationalization support for German language

In addition to the Internationalization support introduced in Resiliency Platform 2.2, Resiliency Platform 3.0 provides some additional Internationalization support for German language. Starting with 3.0, you can see the localized version of the Resiliency Platform Console if you are logging in from German locale browser. The product can be used in a German environment.

For Internationalization support introduced in Resiliency Platform 2.2, refer to *Veritas Resiliency Platform 2.2 Release Notes.*

Support for multiple Resiliency Managers in a data center

Resiliency Platform 3.0 introduces support for multiple Resiliency Managers in a data center. Multiple Resiliency Managers in a data center helps in maintaining resiliency and fault tolerance in the data center.

What is not supported?

Veritas Resiliency Platform does not support the following features:

- EFI (Extensible Firmware Interface) enabled Hyper-V Generation 2 virtual machines are not supported if replication technology is Resiliency Platform Data Mover.
- VMware fault tolerant virtual machines.
- Executing a custom script on a host that is not actively reporting to Resiliency Platform environment through Infrastructure Management Server (IMS) or Infoscale Operations Manager Management Server.
- Database user authentication for Oracle applications.
- Rehearse and cleanup rehearsal operations for applications on Microsoft Failover Cluster.
- Rehearse and cleanup rehearsal operations for applications inside virtual machines having data on raw disks mapped to virtual machines and data replicated through 3PAR RemoteCopy or NetApp SnapMirror through fibre channel.

- Rehearse and cleanup rehearsal operations if the recovery data center is in vCloud.
- Takeover operation from a cloud data center to on-premises data center.
- Raw device mapping (RDM) is not supported for virtual machine disaster recovery using Resiliency Platform Data Mover.
- Replacing the Replication Gateway on the on-premises data center is not supported for the use case of recovery of virtual machines to vCloud Director without adding the vCenter server or Hyper-V server.
- Starting and stopping of resiliency groups is not supported for the use case of recovery of virtual machines to vCloud Director without adding the vCenter server or Hyper-V server.

Array-based replication does not support the following:

- Combination of replicated and non-replicated storage to virtual machines is not supported.
- Combination of storage from multiple array technologies is not supported.

Using the product documentation

Table 1-1 lists the URLs for Veritas Resiliency Platform documentation and Table 1-2 lists the Veritas Resiliency Platform guides.

Table 1-1 URLs for Veritas Resiliency Platform documentation

URL	Description
https://sort.veritas.com/documents	The latest version of the product documentation: Product guides in PDF format. Online help portal. The help content is also available from the product console.
https://www.veritas.com/community/business-continuity/videos	The list of Resiliency Platform videos.
https://www.veritas.com/support/en_US/article.000127401	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.

Table 1-2 Names of Veritas Resiliency Platform guides *(continued)*

Title	Description
Veritas Resiliency Platform Release Notes	The release information such as main features, known issues, and limitations.
Veritas Resiliency Platform 3.0 Overview and Planning Guide	The information about the product, its features, and capabilities.
Veritas Resiliency Platform 3.0 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:

Supported hypervisors for deploying Resiliency Platform virtual appliance

This section lists the hypervisor versions that are supported for Resiliency Platform virtual appliance.

Microsoft Hyper-V:

- Windows Server 2012 with Hyper-V
- Windows Server 2012 R2 with Hyper-V

VMware:

- ESXi 5.1, 5.5, 6.0, 6.0U1, 6.0U2, 6.5
- vCenter Server 5.1, 5.5, 6.0, 6.0U1, 6.0U2, 6.5

Note: The lists of supported platforms for deployment of virtual appliance and for disaster recovery of virtual machines are different. For information on platform support for disaster recovery of virtual machines, see the *Veritas Resiliency Platform Hardware and Software Compatibility List*.

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 60 GB RAM 32 GB Virtual CPU 8
Infrastructure Management Server (IMS)	Disk space 60 GB RAM 16 GB Virtual CPU 8
Replication Gateway	Disk space 40 GB RAM 16 GB Virtual CPU 8 Additional external 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 ■ Resiliency Platform Data Mover host ■ Storage discovery host ■ Hyper-V host	Disk space 15 GB RAM 4 GB Dual processor CPU If you are using a single host for multiple purposes, add the disk space and RAM required for each purpose. For example, if you are using a single host as Windows Install host and as application host, then you need to have at least 30 GB disk space and 8 GB RAM. Note that you cannot use a single host as a Windows Install host as well as Resiliency Platform Data Mover host.

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

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

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

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

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

Network and firewall requirements

The following are the network requirements for Veritas Resiliency Platform:

- Before you use the hostname and the IP address in the **Network settings**, you need to register them with the DNS server.
- The hostname or the IP address which is used for product configuration, should not have multiple entries in the DNS server. For example, the IP address should not be associated with multiple hostnames, or the hostname should not be associated with multiple IP addresses.
- Ensure that ports 88 and 750 on DNS server are open for communication with IMS.
- In case of recovery to cloud, ensure that port 53 on DNS server is open for bi-directional communication with the cloud data center.
- The hostname that you use for a virtual appliance must not start with a digit and must not contain the underscore (_) character.
- Veritas Resiliency Platform supports only Internet protocol version 4 (IPV4).

- If you plan to use the DHCP server, the DHCP server should be in the same subnet where you plan to deploy the product.

The following ports are used for Veritas Resiliency Platform:

Table 2-2 Ports used for Resiliency Manager

Ports used	Purpose	For communication between	Direction	Protocol
443	Used for SSL communication	Resiliency Manager and web browser	Browser to Resiliency Manager	HTTPS, TLS v1.1+
14176	Used for communication between the Resiliency Manager and Infrastructure Management Server (IMS)	Resiliency Manager and IMS	Bi-directional	HTTPS, TLS v1.1+
7001	Used for database replication	Resiliency Manager and IMS In case of multiple Resiliency Managers, between Resiliency Managers	Bi-directional	TCP with SSL/TLS1.1+
389	Used for communication with LDAP/AD server	Resiliency Manager and LDAP/AD server	Bi-directional	TCP, user provided
636	Used for communication with LDAP/AD server	Resiliency Manager and LDAP/AD server	Bi-directional	TCP with SSL/TLS, user provided
22	Used for communication between remote host to the appliance klish access	Appliance and the hosts	Bi-directional	TCP
123	Used for NTP synchronization	Appliance and the NTP server	Bi-directional	TCP
14180	Used for accessing API service	Resiliency Manager and the API service	Bi-directional	HTTS, TLSv1.1+

Table 2-3 Ports used for on-premises IMS and in-cloud IMS

Ports used	Description	For communication between	Direction	Protocol
14176	Used for communication between the Resiliency Manager and Infrastructure Management Server (IMS)	Resiliency Manager and IMS	Bi-directional	HTTPS, TLSv1.1+
5634	Used for IMS configuration	IMS and the hosts	Bi-directional	HTTPS, TLSv1.1+
14161	Used for running the IMS console	Resiliency Manager and IMS	Resiliency Manager to IMS	HTTPS, TLSv1.1+
22	Used for communication between remote host to the appliance klish access Used for remote deployment of the packages on remote UNIX host from IMS	IMS and the hosts	Bi-directional	TCP
135	Used for remote deployment on client computer (inbound)	Host and remote Windows hosts	Bi-directional	TCP
123	Used for NTP synchronization	Appliance and the NTP server	Bi-directional	TCP

Table 2-4 Ports used for on-premises Replication Gateway and in-cloud Replication Gateway

Ports used	Description	For communication between	Direction	Protocol
33056	Used for replication	On-premises virtual machine and Replication Gateway/Storage Proxy		TCP

Table 2-4 Ports used for on-premises Replication Gateway and in-cloud Replication Gateway *(continued)*

Ports used	Description	For communication between	Direction	Protocol
5634	Used for communication with IMS	IMS and Replication Gateway/Storage Proxy	Bi-directional	HTTPS, TLSv1.1+
8089	Used for replication	in-cloud component and on-premises component	Bi-directional	TCP

Table 2-5 Ports used for target Gateway in resync operation

Ports used	Description	For communication between	Direction	Protocol
67	BOOTP server	Target Gateway enabled with DHCP role and host	Uni-directional	UDP
68	BOOTP client	Target Gateway enabled with DHCP role and host	Uni-directional	UDP
69	TFTP protocol	Target Gateway enabled with PXE role and host	Uni-directional	TCP/UDP

Table 2-6 Ports used for virtual machines

Ports used	Description	For communication between	Direction	Protocol
22	Used for communication between remote host to the appliance klish access Used for remote deployment of the packages on remote UNIX host from IMS	IMS and the hosts	Bi-directional	TCP

Table 2-6 Ports used for virtual machines *(continued)*

Ports used	Description	For communication between	Direction	Protocol
5634	Used for communication with IMS	IMS and the hosts	Bi-directional	HTTPS, TLSv1.1+
33056	Used for replication	Virtual machine and Replication Gateway		TCP

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 3.0 release.

Table 3-1 Issues fixed in Veritas Resiliency Platform 3.0

Incident number	Abstract
5170	Replication information error
8465	Resiliency group and VBS names in charts are displayed incorrectly in Japanese and Chinese
8433	Cannot edit application discovery frequency for the uploaded application bundles from console
8617	Metering report does not work for third-party replication technologies
5167	VMDK and VMX files need to be in the same folder
5092	Edit resiliency group operation may fail after rehearsal or cleanup rehearsal
8654	Previously configured network mapping may not work after re-adding a VMware vCenter server
8697	Replication information not discovered for Hyper-V virtual machines configured in Microsoft Failover Clustering environment using Non-English characters in the CSV path

Table 3-1 Issues fixed in Veritas Resiliency Platform 3.0 *(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

Chapter 4

Known issues

This chapter includes the following topics:

- VBS DR operations fail when an application resiliency group with unconfigured DR is added in VBS (3794105)
- Expired resiliency plan cannot be executed even after editing the schedule (3861955)
- Resiliency groups for Hitachi enclosures are not displayed on dashboard under Top RG by replication lag chart (3861173)
- Snapshot disk is read only after rehearse operation is performed in Hyper-V with SRDF replication (3862088)
- Static IP customization may not work under certain conditions (3862916, 3862237)
- Need to manually refresh all assets after a site recovery (3861929)
- Disk utilization risk not resolved after DR operations
- Migrate operation becomes unresponsive if the operation is initiated from an unavailable site (3862253)
- Remote cluster group dependencies not validated before migrate (3863082)
- VBS migrate operation cannot be performed after failure (3862124)
- Resiliency group state does not get updated when production site is down (3863081)
- DNS customization does not work if FQDN is not defined (5037)
- Some versions of VMware Tools are not supported (4969)
- Login to the Resiliency Manager console fails at times
- Warning message may be displayed for network mapping (8644)
- Newly added NIC information is not displayed (10856)
- Validations displayed while configuring resiliency group for remote recovery (10961)
- An operation may fail if invoked at a time when virtual machine is being migrated using Vmotion (6476)
- vLan mapping compulsory for DRS enabled Vmware virtual machines (10322)
- Create resiliency group operation displays error for RHEL 7.0 and RHEL 7.1 virtual machines with open-vm-tools version 9.4.X (8479)

- DR operations fail if the data disk count of virtual machines at cloud data center and on-premises data center is same (10982)
- Rehearsal operation does not get launched for cloud data center immediately after you edit resiliency group to remove one virtual machine (10992)
- Removing Windows Data Mover virtual machine does not uninstall the Replication add-on(11024)
- Known issues: Resiliency Platform Data Mover
- Known issues: Recovery to Amazon Web services (AWS)
- Known issues: Recovery to vCloud Director
- Known issues: NetBackup integration
- Known issues: Multiple Resiliency Managers in a data center

Disaster recovery (DR) configuration for resiliency group fails if Microsoft Hyper-V Replica is configured after you add a virtual machine in Resiliency Platform

This issue applies to the disaster recovery (DR) configuration for a resiliency group. The DR configuration operation fails if a Hyper-V Replica is configured on the Hyper-V virtual machine after you add the virtual machine to the Infrastructure Management Server (IMS).

Workaround:

Use the Resiliency Platform console to refresh the Hyper-V host manually. It discovers the Hyper-V Replica information, and the configuration DR operation functions as expected.

In the VM Inventory report, instead of allocated memory, Resiliency Platform shows the total memory of the virtual machines

In the VM Inventory report, for the virtual machines on the Hyper-V Server, the Resiliency Platform console displays the total memory instead of their allocated memory.

Certain validations do not work while creating a resiliency group of applications (3721289)

When you create a resiliency group of applications, the following validations do not work:

- Check if theResiliency Platform Applications Enablement add-on is deployed on the host. If the Veritas Resiliency Platform Applications Enablement add-on is not correctly installed on the managed host, the create resiliency group operation for application fails. In such situation, you need to install the add-on on the host before creating the resiliency group for applications.
- If the workflow fails, resiliency group should not get created.

Rehearsal does not work after being aborted

If you abort a rehearsal operation, that rehearsal operation does not work afterwards.

Workaround:

Run cleanup rehearsal operation before performing Rehearsal again.

The configure DR operation fails if virtual machines in the resiliency group belong to different servers

If you try to configure disaster recovery (DR) for a resiliency group with multiple virtual machines that belong to different servers, the configure DR operation fails.

For resiliency groups containing VMware virtual machines with NFS datastore mounted from a NetApp volume with substring vol, Migrate or takeover operations may fail

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.

The license expiry status is inconsistent on Resiliency Managers configured on different time zones

If Resiliency Managers are configured on different time zones, then the license on one Resiliency Manager may expire before the license on the other Resiliency Manager. This behavior is seen on the second Resiliency Manager for almost 12 hours.

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

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

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

Long SRDF device group names are not discovered (3786826)

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

Multiple repository paths on the same host are not allowed for the repository server (3734149)

While you add a repository server, you cannot add multiple repository paths on the same host as multiple entries for repository server.

Unknown state displayed for the Resiliency groups of dark sites that are part of VBS (3794650)

If a virtual business service (VBS) contains a resiliency group that belongs to dark sites, the state of the individual resiliency group is displayed as unknown if it in not online.

An Oracle custom application is not discovered if the instance names do not match (3796579)

When you add an Oracle custom application, Resiliency Platform to discover, the **Application Inputs** screen includes two **Instance name** fields. You must specify the same name in each field; otherwise, the application is not discovered.

VBS DR operations fail when an application resiliency group with unconfigured DR is added in VBS (3794105)

User cannot perform disaster recovery operations when the VBS consists of an application resiliency group which is not configured for DR.

Expired resiliency plan cannot be executed even after editing the schedule (3861955)

Once a resiliency plan schedule expires, it cannot be executed even after editing the schedule. No error is encountered when you try to edit the schedule, but the plan is not executed on edited schedule.

Workaround:

Delete the previous resiliency plan schedule and create a new resiliency plan schedule.

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.

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.

Need to manually refresh all assets after a site recovery (3861929)

After a primary site is recovered, you need to manually refresh all the asset configurations such as configurations of enclosures, virtual machines, discovery host.

Following is the order in which the asset configuration needs to be refreshed:

- For EMC VNX, EMC RecoverPoint and Hitachi, refresh the discovery host first, then refresh the enclosures, and then finally refresh the VMware vCenter servers.
- For NetApp, first refresh the VMware vCenter server and then refresh the enclosures.

Disk utilization risk not resolved after DR operations

The disk utilization risk is not resolved if the disk is made available after the resiliency group associated with the risk, is migrated to the recovery site.

Migrate operation becomes unresponsive if the operation is initiated from an unavailable site (3862253)

If you try to perform the migrate operation instead of the takeover operation from a site which is currently not available, the operation becomes unresponsive indefinitely.

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.

VBS migrate operation cannot be performed after failure (3862124)

If the workflow fails during a VBS migrate operation, then migrate operation cannot be retried for the VBS.

Workaround:

Fix the issue which caused the failure and then bring the VBS online on production site and then perform the Migrate operation. You can also try to perform migrate operation on individual resiliency group after fixing the issue which caused the failure.

Resiliency group state does not get updated when production site is down (3863081)

If the production site where a resiliency group is online, goes down, the state of the resiliency group does not change. However, the state of the application changes to display **Online(Stale)** to reflect that the online state of the resiliency group is stale and may not be recent.

DNS customization does not work if FQDN is not defined (5037)

This issue occurs if FQDN is not defined for virtual machines running on Hyper-V platform (Linux and Windows).

Some versions of VMware Tools are not supported (4969)

Resiliency Platform uses vSphere web service API, ValidateCredentialsInGuest(), which does not work with some versions of VMware Tools that are installed in guest virtual machine. This issue may lead to failure in IP customization of Windows virtual machines in vSphere environment.

Workaround

Install the latest version of VMware Tools.

vSphere web service API, ValidateCredentialsInGuest(), works with VMware Tools version 9.4.10.2092844.

Login to the Resiliency Manager console fails at times

Sometimes, login to the Resiliency Manager console fails.

Workaround:

Stop the Resiliency Manager instance and then restart it.

Warning message may be displayed for network mapping (8644)

At times, even if the network mapping is set up in the environment, you may get a warning message for network mapping similar to the following while performing a disaster recovery operation:

```
Some virtual machines may not connect to network after migrate as
the required network mapping are not defined.
```

Workaround:

You need to click on Continue and the operation proceeds as expected.

Newly added NIC information is not displayed (10856)

If a network interface card (NIC) is attached to a virtual machine and the following conditions are met, then the new NIC is not listed on the **Network customization** panel when you configure the resiliency group for remote recovery.

- The virtual machine belongs to a resiliency group.
- **Apply IP customization** is enabled.
- IPs addresses are edited.

Workaround:

Edit the resiliency group to uncheck the **Apply IP customization** check box, and submit the wizard.

Again edit the resiliency group and select the **Apply IP customization** check box. The information of the new NIC is displayed for IP customization.

This issue does not occur if IP address are not edited.

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.

An operation may fail if invoked at a time when virtual machine is being migrated using Vmotion (6476)

In case a virtual machine is being migrated through VMotion or through DRS and at the same time, any VRP operation is invoked on that particular virtual machine, the operation may fail as the resources are in transient state.

Workaround:

You need to re-launch the operation once the migration of the virtual machine completes.

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

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

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

Create resiliency group operation displays error for RHEL 7.0 and RHEL 7.1 virtual machines with open-vm-tools version 9.4.X (8479)

If you try to configure a resiliency group with RHEL 7.0 and 7.1 virtual machines having open-vm-tools version 9.4.X, the operation displays the following error:

```
Unable to determine filesystem used size for virtual machine for
licensing
```

Workaround:

Install open-vm-tools version 9.10.X and above on those RHEL 7.0 and RHEL 7.1 virtual machines and then try to configure resiliency group.

DR operations fail if the data disk count of virtual machines at cloud data center and on-premises data center is same (10982)

If the selected cloud virtual machine's size has exactly the same data disks count as that of on-premise virtual machine data disks count, the DR operations fail with the following error:

```
The maximum number of data disks allowed to be attached to a VM of
this size is 'x'.", "code": 409, "message_id": "OperationNotAllowed"
```

Workaround:

while configuring for DR, add one extra disk to the data disk count of the on-premises virtual machine and then select the cloud virtual machine size accordingly.

Rehearsal operation does not get launched for cloud data center immediately after you edit resiliency group to remove one virtual machine (10992)

If your target data center is a cloud data center and you have removed a virtual machine by editing the resiliency group, then you may not be able to launch the rehearsal operation.

Workaround:

Refresh the cloud discovery and then edit the resiliency group again.

Removing Windows Data Mover virtual machine does not uninstall the Replication add-on(11024)

When you remove a Windows virtual machine listed in the **Prepare host for replication** view, the Resiliency Platform Replication add-on does not get uninstalled from that host.

Workaround:

You need to manually uninstall the `Veritas Resiliency Platform SR IO Tap Driver` package from the Control Panel of the virtual machine.

Known issues: Resiliency Platform Data Mover

The following known issues are applicable to Resiliency Platform Data Mover:

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

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

Workaround:

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

Iofilter bundle not removed from ESX hosts even after unconfiguring virtual machines (5178)

In case you are using Resiliency Platform Data Mover, even after you unconfigure all the virtual machines in the cluster that were configured for recovery, iofilter bundle does not get removed from the cluster.

Storage policy needs to be manually removed after all the virtual machines are unconfigured (5180)

The storage policy for virtual machines does not automatically get removed After all the protected virtual machines in the VMware vSphere server are unconfigured. It needs to be manually removed from virtual machine's storage policies.

Replication gets paused if you perform add disk operation (5182)

If you add a disk to the protected virtual machine, replication is paused and you are not able to perform any operation on the associated resiliency group.

Workaround:

Edit the resiliency group to remove the affected virtual machine and then add it back.

Cannot perform any operation after deleting disk from virtual machine (5182)

If you delete a disk from a virtual machine, you cannot perform any operation on the associated resiliency group.

Workaround:

Edit the resiliency group to remove the affected virtual machine and add it back.

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.

Risks not generated after taking snapshot of virtual machine replicated using Data Mover(6886)

If you take a snapshot of the virtual machine that is a part of a Resiliency Group that gets replicated using Resiliency Platform Data Mover, the risks are not generated after taking the snapshot.

Workaround:

You need to perform edit Resiliency Group operation after you take the snapshot of any virtual machine.

Known issues: Recovery to Amazon Web services (AWS)

The following known issues are applicable to AWS:

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

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

Workaround

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

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

After migration, one or more network interface cards (NIC) associated with a Windows virtual machine may not be visible from the operating system. You may not be able to connect to the migrated virtual machine using the IP address assigned to these invisible NICs.

Workaround:

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

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

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

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

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

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

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

Workaround:

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

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

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

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

Workaround:

Start the virtual machine and manually remove the cloud IPs.

Refresh the host and vCenter server or Hyper-V.

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

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

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

Workaround

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

Known issues: Recovery to vCloud Director

The following known issues are applicable to recovery to vCloud Director:

Migrate back of VBS from vCloud Director to on-premises data center fails (10975)

If you try to migrate back a VBS from vCloud Director to the on-premises data center, the operation fails.

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.

Operations for virtual machine do not work if the remote master server gets reconfigured (8600)

If the remote master server is reconfigured, the remote master association for the virtual machine gets detached and no operation works for the virtual machine.

Workaround:

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

Known issues: Multiple Resiliency Managers in a data center

The following known issues are applicable if you have multiple Resiliency Managers in a data center:

In a cloud data center, DR operations need to be performed only from the Resiliency Manager associated with the cloud IMS (10895)

In a cloud deployment with multiple Resiliency Managers, you can perform the DR operations only from the Resiliency Manager that is associated with the cloud IMS.

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.

Chapter 5

Limitations

This chapter includes the following topics:

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

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

Limitations for on-premises Windows hosts for Resiliency Platform Data Mover replication

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

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

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

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

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.

Localization of adding application type is not supported

Localization of adding applications type is not supported due to back-end limitations. The **Add Application Type** wizard in **Settings** > **Application Support** > **Uploaded** tab does not accept the inputs in non-English characters.

Localization related limitations

The following are a few localization related limitations applicable to Veritas Resiliency Platform 3.0:

- Resiliency Plan task name does not change on changing the browser locale.
- Notification text does not get localized
- Email text does not get localized
- Activities task result does not get localized
- Host level task does not get localized
- For German AD, User's group name is mandatory
- Main task of workflow for resiliency groups created before upgrade does not get localized
- Workflow performed before upgrade does not get localized
- State of Resiliency Manager, IMS, or InfoScale Operations Manager server displayed in the Resiliency Platform console does not get localized.

Virtual machine name limited to 35 characters

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

Appendix A

Virtual appliance security features

This appendix includes the following topics:

Operating system security

Veritas Resiliency Platform appliance operating system is hardened against potential security exploitation by removing the operating system packages that are not used by the Resiliency Platform. All the default yum repository files that are shipped with the operating system are removed.

The Control + Alt + Delete key combination has been disabled to avoid any accidental reboot of the virtual appliance. Exec-shied is enabled to protect the virtual appliance from stack, heap, and integer overflows.

Management Security

Only two users are available on the appliance: admin user and support user. These two user accounts are used to access the appliance based on the requirement.

Only admin login is available for the appliance. The password policy of admin login is modified to prompt the user to change the password on the first login.

If the admin user password is lost, you need to contact Veritas support for resetting the admin user password.

On successful completion of the product bootstrap, admin user can only access a limited menu of commands through klish. Besides admin user, support user is also supported in the appliance but remote login of support user is disabled. To access the support user, one need to login as an admin and go through **klish**. An option `support > shell` is provided in the **klish** menu to switch the user to support and access the bash shell of support. After selecting this option, the support user is given superuser privileges. Using this option is not recommended and it should be used only with the assistance of technical support.

Timeout of the bash shells of all users is set to 900 seconds.

Network security

The TCP timestamp responses are disabled in Resiliency Platform virtual appliance. Another network security feature of the appliance is that during the product bootstrap process, only those ports that are used by the product for communication and data transfer, are opened through the firewall and all the other communications are blocked.

Uncommon network protocols such as DCCP, SCTP, RDC, TIPC have been disabled so that any process cannot load them dynamically.

See “Network and firewall requirements” on page 17.

Access control security

Resiliency Platform virtual appliance implements certain access control measures. The umask is set to 0700 across the appliance. The access permissions of some of the files such as home folder of root, the log directory etc. is restricted. All the security and the authorization messages are logged into the appliance.

Physical security

In the Resiliency Platform virtual appliance, the USB storage access is disabled.