Veritas™ Resiliency Platform 1.2: Release Notes

April 2016

VERITAS™

Veritas Resiliency Platform: Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: 1.2

Document version: 1.2 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. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within the company to answer your questions in a timely fashion.

Our support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about our support offerings, you can visit our website at the following URL:

www.veritas.com/support

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.veritas.com/support

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information

- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Technical Support
  - Recent software configuration changes and network changes

Licensing and registration

If your product requires registration or a license key, access our technical support Web page at the following URL:

www.veritas.com/support

Customer service

Customer service information is available at the following URL:

www.veritas.com/support

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Advice about technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact us regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

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

Contents

Chapter 1

Overview

This chapter includes the following topics:

About Veritas Resiliency Platform

Veritas Resiliency Platform offers a unified approach for visibility and control of IT service continuity for applications, virtual machines, and complex, multi-tier business services across a global landscape.

Resiliency Platform has the following core capabilities:

Recovery	Resiliency Platform provides a disaster recovery (DR) solution using data centers on premises in different geographical locations. The management console simplifies recovery, with single-click rehearsal and recovery operations.
Visibility	The console Dashboard provides visibility into the health of applications, virtual machines, and multi-tier business services.
Orchestration	Resiliency Platform can assist in data center day-to-day workload automation activities. For instance, virtual machines or IT services can be started and stopped for maintenance.

About Resiliency Platform features and components

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

resiliency domain	The logical scope of a Resiliency Platform deployment. It can extend across multiple data centers.
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.
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.
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.

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 also migrate or takeover the entire VBS.

New features and changes in Veritas Resiliency Platform 1.2

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

Support for InfoScale Availability on Solaris and AIX platforms

Veritas Resiliency Platform 1.2 extends support for InfoScale Availability on Solaris and AIX platforms. From Veritas Resiliency Platform 1.2 onwards, you can manage the InfoScale applications on Windows, Linux, Solaris, and AIX platforms that are configured in Veritas InfoScale Operations Manager.

Enhanced replication support

Veritas Resiliency Platform 1.2 extends support for the following replication technologies:

- HPE 3PAR Remote Copy for replication of virtual machines.
- EMC RecoverPoint replication for application data.

What is not supported?

Veritas Resiliency Platform does not support the following features:

- 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
- Static IP customization of Windows guest in VMware environment
- Database user authentication for Oracle applications

Chapter 2

System requirements

This chapter includes the following topics:

Supported hypervisors for 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:

- ESX 5.1, 5.5, 6.0
- vCenter Server 5.1, 5.5, 6.0

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 and Infrastructure Management Server (IMS):

Disk space	60 GB
RAM	16 GB
Virtual CPU	8

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

In addition to the above mentioned resources, 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.

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.
- Veritas Resiliency Platform supports only Internet protocol version (IPV) 4.
- 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 2-1 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	TCP
14176	Used for communication between the Resiliency Manager and Infrastructure Management Server (IMS)	Resiliency Manager and IMS Resiliency Managers of the two data centers	Bi-directional	TCP
7000	Used for database replication	Resiliency Managers of the two data centers	Bi-directional	TCP
7001	Used for database replication	Resiliency Managers of the two data centers	Bi-directional	TCP
22	Used for communication between remote host to the appliance CLISH access	Appliance and the hosts	Bi-directional	TCP
123	Used for NTP synchronization	Appliance and the NTP server	Bi-directional	TCP

Table 2-2 Ports used for 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 Resiliency Managers of the two data centers	Bi-directional	TCP
5634	Used for IMS configuration	IMS and the hosts	Bi-directional	TCP
14161	Used for running the IMS console	Resiliency Manager and IMS	Resiliency Manager to IMS	TCP

Table 2-2 Ports used for IMS *(continued)*

Ports used	Description	For communication between	Direction	Protocol
22	Used for communication between remote host to the appliance CLISH 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

Chapter 3

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)
- IP plumbing required on both sites while configuring DNS for InfoScale resiliency group (3861866)
- Disk utilization risk not resolved after DR operations
- Migrate operation hangs 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 gets updated when production site is down (3863081)
- Rehearsal for applications sometimes may not work as expected (3872688)
- DR operations may fail for applications on RHEL 6 hosts (3867690)
- Rehearsal for Microsoft SQL Server configured in Microsoft Fail Over Cluster environment fails (3872686)
- Enclosure configuration removal operation fails for EMC VNX block enclosures (3874870)

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 turn off and restart the Hyper-V guest machine from Hyper-V manager.

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.

IP plumbing required on both sites while configuring DNS for InfoScale resiliency group (3861866)

While configuring disaster recovery for an InfoScale resiliency group, you need to plumb the IP of the application on both the production and recovery sites. Once the disaster recovery configuration of the resiliency group is complete, you can remove the plumbing of the application IP at recovery site.

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 hangs 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 hangs 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 gets 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.

Rehearsal for applications sometimes may not work as expected (3872688)

Sometimes, rehearse operation for applications may be displayed as successful on Resiliency Platform console even when the application fails to come online on the recovery site host.

DR operations may fail for applications on RHEL 6 hosts (3867690)

When you run DR operations such as rehearsal, cleanup rehearsal, and migrate for application on RHEL 6 hosts for the first time, the DR operation may fail while importing the LVM Volume Group. This may happen if the partitions are not read by the operating system in time.

Workaround:

To resolve the issue, re-run the same DR operation again.

Rehearsal for Microsoft SQL Server configured in Microsoft Fail Over Cluster environment fails (3872686)

In case of Microsoft SQL Server configured in Microsoft Fail Over Cluster environment, the nodes on production site as well as recovery site need to be configured in the same domain. When you perform the rehearse operation for such configuration, the Microsoft SQL Server instance fails to come online on the recovery site as an instance with same name might already be running on the production site within the domain. Still, the rehearsal operations is shown as successful in the Resiliency Manager console.

Enclosure configuration removal operation fails for EMC VNX block enclosures (3874870)

If you try to remove the enclosure configuration from an Infrastructure Management Server (IMS), the operation fails with the following error message:

Failed to make the server call, check the URL or network connection.

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. The new

password must not be a Dictionary word and must be at least six characters long. If the admin user password is lost, Veritas may access the root using the grub access, and reset the admin user password.

On successful completion of the product bootstrap, admin user can only access a limited menu of commands through CLISH. 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 **CLISH**. An option `support > shell` is provided in the **CLISH** 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 14.

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.

Appendix B

Getting help

This appendix includes the following topics:

Getting help

If an issue arises while you use the products, refer to the product documentation and online help. If necessary, report it to Veritas.

For technical assistance, visit

www.veritas.com/support

This site provides access to resources such as TechNotes, product alerts, software downloads, hardware and software compatibility lists, and the customer email notification service. Use the Knowledge Base Search feature to access additional product information, including current and past releases of product documentation.

Using the product documentation

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

Table B-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 and HTML format. Online help portal. The help content is also available from the product console.
https://www.veritas.com/support/en_US/article.000107881	The late breaking news that is related to this release.

Table B-2 Names of Veritas Resiliency Platform guides

Title	Description
Veritas Resiliency Platform Getting Started Guide	An overview of processes of deployment, configuration, and disaster recovery in Resiliency Platform.
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: Deployment Guide *Veritas Resiliency Platform: Solutions for Applications* *Veritas Resiliency Platform: Solutions for Microsoft Hyper-V* *Veritas Resiliency Platform: Solutions for VMware* *Veritas Resiliency Platform: Solutions for Virtual Business Services* *Veritas Resiliency Platform: Application Enablement SDK*	The information about deploying Resiliency Platform and using the solutions.
Veritas Resiliency Platform Third-Party Software License Agreements	The information about the third-party software that is used in Resiliency Platform.