Veritas™ Resiliency Platform 1.0: Release Notes

VERITAS™

July 2015

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: 1.0

Document version: 1.0

Legal Notice

This Symantec product may contain third party software for which Symantec 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. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

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. SYMANTEC CORPORATION 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 Symantec 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.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec 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 Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's 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 Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/index.jsp

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.symantec.com/business/support/contact_techsupp_static.jsp

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 Symantec
  - Recent software configuration changes and network changes

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/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
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

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

Asia-Pacific and Japan	customercare_apj@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec's enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

http://www.symantec.com/connect/storage-management

Documentation

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation

Contents

Chapter 1

Overview

This chapter includes the following topics:

- About Veritas Resiliency Platform
- About Resiliency Platform features and components

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 Resiliency Platform 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.

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 the IMS for discovery and monitoring.

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/takeover the entire VBS.

Chapter 2

System requirements

This chapter includes the following topics:

- Supported hypervisors for Resiliency Platform virtual appliance
- System resource requirements for Resiliency Platform
- Virtual appliance security requirements
- Network and firewall requirements

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 5.5
- vCenter Server 5.5

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.

Virtual appliance security requirements

Veritas Resiliency Platform virtual appliance implements a number of features to ensure the security of the product.

See "About virtual appliance security" on page 28.

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

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

Ports used	Description	For communication between	Direction	Protocol
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
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:

- Creating a resiliency group for applications fails if Veritas Resiliency Platform Applications Enablement add-on is not correctly installed (3721298)
- In the Hyper-V guest environment, the writable disk is shown in the Read-Only state (3785911)
- The configure DR operation may fail if the operation is launched immediately after create resiliency group operation (3774674)
- There is an authorization error if the Resiliency Manager console is left inactive for sometime (3766645)
- Long SRDF device group names are not discovered (3786827)
- Configure disaster recovery operation fails while you perform the Protect Virtual Machine or Protect Application operation (3790551)
- Multiple repository paths on the same host are not allowed for the repository server (3734149)
- The data center column may be empty in the configure DR wizard (3797315)
- The remove host operation displays a time out error (3796565)
- Both the data centers appear active even when the host in the production data center is down (3798853)
- File System Full alert is not triggered on a Windows host (3753620)
- The workflow task continues to run although the Resiliency Manager is turned off (3787995)
- Special characters or spaces are not allowed in the path for the Add custom application wizard (3798907)
- Unknown state displayed for the Resiliency groups of dark sites that are part of VBS (3794650)
- A repository assigned from CLISH is not reflected in the console in cases of a single appliance for Resiliency Manager and IMS (3802310)
- An Oracle custom application is not discovered if the instance names do not match (3796579)
- A custom application may show inputs pending if the start program file goes missing (3802979)
- Tool tip displays stale data for exception and issue in modifying exceptions (3799843)

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

The carousel view for VBS configuration may be blank

While you create or modify a Virtual Business Service (VBS), if you remove a tier or remove a resiliency group from a tier, the carousel view for VBS configuration may be blank.

Disaster recovery (DR) configuration for resiliency group fails if Microsoft Hyper-V Replica is configured after you add a virtual machine in Resiliency Platform (3703679)

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 (3703674)

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 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.

The Resiliency Platform console shows incorrect information about the resiliency group state, replication state, and replication type

Sometimes the data discovered from the Infrastructure Management server (IMS) may not be updated properly in the Resiliency Manager database. This situation may result in displaying incorrect information about the resiliency group state, replication state, and replication type.

Workaround:

Refresh the appropriate IMS in both the data centers.

The configure DR operation may sometimes fail

Sometimes the data discovered from the Infrastructure Management server (IMS) may not be updated properly in the Resiliency Manager database. Due to this incorrect data, the configure DR operation fails with errors.

Workaround:

- Check the exact error and see if the configuration is done accordingly.
- Refresh the IMS in both the data centers and perform the operation again.
- If the operation still fails, log in to the IMS and refresh the appropriate hosts, virtualization servers, and enclosures.

The hypervisor should not be added as a host in certain environments

If the applications are installed inside virtual machines running on Microsoft Hyper V technology and the applications are having data that is replicated using EMC SRDF, and these applications are to be configured for DR, then you should not add the hypervisor itself as a host to the IMS.

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.

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

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 at least 12 hours.

Validation of inputs provided for partially discovered applications takes time (3764836)

For partially discovered applications, after you provide the inputs for the related questions, the validation of answers take time.

Creating a resiliency group for applications fails if Veritas Resiliency Platform Applications Enablement add-on is not correctly installed (3721298)

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.

Workaround:

Reinstall the add-on on the managed host and create the resiliency group for applications.

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.

The configure DR operation may fail if the operation is launched immediately after create resiliency group operation (3774674)

If you launch the configure DR operation immediately after performing the create resiliency group operation, the configure DR operation may fail. This happens because the attributes required for the configure DR operation take some time to be written in the database after the create resilience group operation.

Workaround:

You need to wait for some time and then perform the configure DR operation again.

There is an authorization error if the Resiliency Manager console is left inactive for sometime (3766645)

If you leave the Resiliency Manager web console idle for a long time and then try to perform an operation in the console, you may get an error message saying that you are not authorized to perform operations.

Workaround:

You need to log out from the Resiliency Manager console, and log in again.

Long SRDF device group names are not discovered (3786827)

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

Configure disaster recovery operation fails while you perform the Protect Virtual Machine or Protect Application operation (3790551)

While you perform the Protect Virtual Machine or Protect Application operation, the configure disaster recovery (DR) task fails. This happens because the create resiliency group task which is a part of the operation is still in progress. You need to re-configure DR after the resiliency group is successfully created.

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.

The data center column may be empty in the configure DR wizard (3797315)

In the configure DR wizard, if you expand the virtual machine selections pane, at times the data center column might appear empty, and the VM State might appear incorrect.

This issue is only related to the view and does not affect any functionality.

The remove host operation displays a time out error (3796565)

If you try to remove a host from Infrastructure Management Server (IMS), a timeout error message may be displayed. This error message does not impact the functionality. The host is removed from the IMS despite the error message.

Both the data centers appear active even when the host in the production data center is down (3798853)

After the physical servers belonging to the production data center go down and the takeover operation to the recovery data center is successful, the web console shows the resiliency group active in both the data centers.

This does not impact any functionality, and the resiliency group state returns to normal after the physical servers in the production data center comes back online.

File System Full alert is not triggered on a Windows host (3753620)

On a Windows host which is not under the control of Storage Foundation, the File System Full alert is not triggered.

The workflow task continues to run although the Resiliency Manager is turned off (3787995)

When a resiliency plan is executed and the Resiliency Manager is turned off, some of the tasks continue to be in the **Running** state.

Special characters or spaces are not allowed in the path for the Add custom application wizard (3798907)

For the Add custom App wizard, if the path to an application on a Linux host contains special characters or spaces, operations such as create resiliency group or migrate may not work. Special characters or spaces are not allowed in the path on a Linux host.

Workaround:

Create a symbolic link to the path having special characters and use these symbolic links in the Add Custom App wizard on Linux hosts.

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.

A repository assigned from CLISH is not reflected in the console in cases of a single appliance for Resiliency Manager and IMS (3802310)

If you assign a repository server to a server that has both the Resiliency Manager and the Infrastructure Manager (IMS) configured on a single appliance, this change is not reflected in the web console.

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.

A custom application may show inputs pending if the start program file goes missing (3802979)

A successfully added custom application may be in the inputs pending state if the location of the start program file goes missing. This may remove some of the previously added custom applications. It may also affect custom applications which are added in the future.

Workaround:

Remove the custom applications which are in the pending inputs state and add them again.

Tool tip displays stale data for exception and issue in modifying exceptions (3799843)

Tool tip on a resiliency group might display stale data about exceptions since the exceptions that are set on that resiliency group in the tier did not get cleared. You need to move such a resiliency group to list and then move it back to the tier to solve this issue.

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.

Chapter 4

What is not supported?

This chapter includes the following topics:

What is not supported?

Resiliency Platform does not support the following features:

- Disaster recovery readiness operations (rehearse and rehearse cleanup) for applications
- VMware fault tolerant virtual machines

Appendix A

Virtual appliance security features

This appendix includes the following topics:

- About virtual appliance security

About virtual appliance security

This chapter covers the following:

See “Operating system security” on page 28.

See “Management Security” on page 28.

See “Network security” on page 29.

See “Access control security” on page 29.

See “Physical security” on page 29.

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.

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, Symantec may access the root using the grub access, and reset the admin user password.

On successful completion of the Resiliency Platform 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.

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 authorization messages are logged into the appliance.

Physical security

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

Getting help

This appendix includes the following topics:

- Getting help
- Using the product documentation

Getting help

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

For technical assistance, visit

www.symantec.com/enterprise/support/index.jsp

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

Table B-1 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 B-1 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: 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*	The information about deploying Veritas 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.
Veritas Resiliency Platform Getting Started Guide	An overview of processes of deployment, configuration, and disaster recovery in Resiliency Platform.

Table B-2 URLs for Veritas Resiliency Platform documentation

URL	Description
https://sort.symantec.com/documents	The latest version of the product documentation.
http://www.symantec.com/docs/TECH231301	The late breaking news that is related to this release.

Veritas Resiliency Platform help content is hosted on the web and is accessed when you launch the product help. The help content can be updated independently of product release.