Veritas™ Risk Advisor Release Notes

AIX, ESX, HP-UX, Linux, Solaris, Windows Server

7.0

VERITAS

Veritas Risk Advisor Release Notes

Product version: 7.0

Document version: 7.0 Rev 1

Legal Notice

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 maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp

Contacting Technical Support

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

http://www.symantec.com/business/support/assistance_care.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/techsupp

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp

Customer Service is available to assist with 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 maintenance 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

Documentation feedback

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions to storage_management_docs@symantec.com.

Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting.

Maintenance agreement resources

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

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

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Veritas Risk Advisor Release Notes

This chapter includes the following topics:

Introduction

This document provides important information about Veritas Risk Advisor (VRA).

For important updates regarding this release and for more information about Veritas Risk Advisor (VRA), review this entire document and see the Late-Breaking News TechNote on the Symantec Technical Support Web site:

www.symantec.com/docs/TECH68401

VRA (formerly DRA) features

VRA is a risk detection and management solution that lets organizations diagnose High Availability (HA) and disaster recovery (DR) vulnerabilities (also called gaps) and optimize data protection.

VRA enables enterprises to effectively manage business continuity implementations, to ensure that their critical business data is protected at all times.

VRA is an agentless enterprise discovery and monitoring tool that automatically scans your enterprise infrastructure and detects gaps and infrastructure vulnerabilities in your HA/DR implementation.

VRA automatically detects and alerts you to any potential gaps, best practice violations, or service level agreement (SLA) breaches.

VRA gathers information about your environment and does the following:

- Provides automated insight into your data replication environment to create an online, detailed, and up-to-date HA/DR topology
- Automatically detects and analyzes gaps and unprotected production areas using a signature knowledge base of over 5,000 signatures
- Discovers the current data protection status of your critical applications and compares it to the state needed to comply with HA/DR SLAs

VRA uses this information to provide the following:

- Detailed recommendations on how you can improve your environment, based on best practices and recovery objectives.
- Detailed lists and information about current data protection and HA/DR risks and the prioritized actions for fixing them. VRA also provides a variety of tools that let you drill down and analyze your environment using detailed tables and topology maps. You can use this information to fix the problems that VRA detects.
- Identify differences between production, standby, and DR hosts.
- Auditing and compliance documentation, including a map of your production environment, disaster recovery configuration, and dependencies.

System requirements and software limitations

For more information about system requirements and software limitations, refer to the *Veritas Risk Advisor Support Requirements* document.

New features

This VRA release introduces new features in the following categories:

Product re-branding

- **Disaster Recovery Advisor (DRA)** is re-branded as **Veritas Risk Advisor (VRA)**. The product name, installation path, URL and user interface were changed accordingly.

Veritas Risk Advisor/ SAN

- Veritas Risk Advisor (VRA) has a new separately licensed option that enables you to scan **SAN Switches** and detect risks.

VRA framework upgrade

- The **Java** and **Apache Tomcat** versions used by VRA have been upgraded to version 8.

New platform support

- SAN Switches: Brocade, Cisco MDS, HP VirtualConnect
- NetApp Clustered Data ONTAP 8.3.

Enhanced storage data collection options

- VRA can collect EMC Symmetrix and VNX storage configuration information by connecting to a **Windows Storage Management/CLI server** (in addition to the previously supported UNIX/Linux Storage Management/CLI servers

Gaps

- New gap signatures

New privileged commands

No new privileged commands are required for host scanning as part of this new release.

For more information on privileged command requirements, refer to the *VRA 7.0 Deployment guide*.

Additional changes and enhancements

Following are the additional changes and enhancements done in Veritas Risk Advisor.

VRA data folder moved to a new path

The VRA Data folder has been moved from *[INSTALLATION_DRIVE]:\Program Files\Symantec\Disaster Recovery Advisor\Data* to *[INSTALLATION_DRIVE]:\VRA*. The existing content of the folder is copied to the new path as part of the upgrade process.

Note: Update any monitoring, backup or other tools accessing VRA log files accordingly.

VRA Application URL change

The application URL has changed to reflect the new product name. The updated address is http://<VRA_server>:8080/VRA (or https://<VRA_server>:8443/VRA when https is used).

Note: Update end users and clients accessing VRA using Web Services with the new URL.

Email alerts for system maintenance issues risking VRA system availability

Alerts have been added to notify the application administrator regarding maintenance issues that may lead to the system being unavailable or unable to scan/analyze risks. Alerts are received through email and presented in the dashboard. VRA will perform the system checks before a scan task, analysis task or full cycle and upon tomcat restart. In addition, the user may configure a weekly schedule for the system checks using the A**dvanced - System Issues detector schedule, day of week/time of day** system properties.

To receive email alerts, configure the **System Alerts - List of admin e-mail addresses** system property.

The **Minimum free disk space for running scheduled tasks, in MB** can be used to set the threshold for reporting a disk space issue on the VRA server.

Risk analysis duration improvements

Several improvements have been implemented to shorten the run time of the risk analysis process.

Support for EMC VPLEX using HDS storage arrays

Support has been added for HDS storage systems managed by EMC VPLEX.

Support for EMC VPLEX accessed by UNIX/Linux hosts

Support has been added for EMC VPLEX systems used by Unix and Linux hosts.

Oracle GoldenGate as part of the user-defined SLA policy

End users may configure the required RPO for GoldenGate replication as part of the SLA policy and receive tickets regarding policy violations as they occur.

Compared hosts are presented with relevant meta-data

The comparison output has been improved to include information such as whether the host is a primary or standby server, cluster membership and business entity.

Cluster node information added to several VCS risk signatures

Tickets of Gap IDs 509, 539 and 554 were enhanced to include a node list and present the nodes in the ticket topology [G-1302]

Link HB Status added to ticket of Gap ID 534 ("Cluster in jeopardy")

Tickets of Gap ID 534 was enhanced to show the status of network interfaces through the "Link HB Status" column [G-377]

Performance improvement for internal validation and correction processes

The time required for deleting invalid VRA DB objects missing mandatory key connections was shorted. [A-417]

New functionality added to resolve VM configuration issues following migration

New functionality was added to allow users to transfer the configuration of a previously scanned virtual machine to its new virtual machine object and vCenter system. In the **View Hosts** screen, the **Migrate Virtual Machine** button was added. The dialogue opened by this button presents virtual machines previously scanned which their current vCenter and ESXi host are unknown. For each VM, the system presents the estimated current vCenter and VM or a selection link. When approved by the user, the system will copy the configuration of the previously scanned VM to the new VM object in the new vCenter, and retain information such as Business Entity and SLA. Take care to scan the target vCenter prior to using the "Migrate Virtual Machine" functionality.

Performance improvement when saving high volumes of data

In cases where the system writes high volumes of data to the internal database, the risk analysis process may suffer from severe slowdown. [A-402, A-407]

Support for Active Directory authentication using Cyber-Ark

When assigning credentials to automatic Active Directory domain discovery, the system now supports Credentials of type "Cyber-Ark" in additional to the previously supported “User/Password” type. [A-388]

New system properties

The following system properties were added:

- "Collection - Use sudo for the cat command
- "Collection - Use sudo for the ls command
  For additional information, see "Incorrect tickets opened due to insufficient permissions to test a directory" under Fixed Issues.
- "System Alerts - Advanced - System Issues detector schedule, day of week
- "System Alerts - Advanced - System Issues detector schedule, time of day
- "System Alerts - List of admin e-mail addresses" system property.

- "System Alerts - The Minimum free disk space for running scheduled tasks, in MB
  For more information, see "Email alerts" under "Additional Changes and Enhancements".

Important Notes

DO NOT choose to uninstall previous Java versions when installing or upgrading to version 7.0.

When presented with the "Uninstall out of date versions" upon the completion of the Java 8 installation, take particular care to select "Remind me later" and not "Uninstall". Choosing "Uninstall" will result in removal of the Java 8 just installed, and will lead to overall VRA installation or upgrade failure.

Scanning NetApp storage systems using SSL

If an error is experienced when connecting to NetApp storage systems using SSL, the following changes can be performed to resolve the connection error:

- "Enable TLS on the target NetApp storage system using the "option tls.enable on" command; or
- "Comment the following line in the java.security file of the Java installation used by the master/collector servers:

  jdk.tls.disabledAlgorithms=SSLv3
  The default path for the file is
  C:\Program Files\Java\jre1.8.0_40\lib\security.
  This option was uncommented on Java v8.31

VRA Application URL change

The application URL has changed to reflect the new product name. The updated address is **http://<VRA_server>:8080/VRA** (or **https://<VRA_server>:8443/VRA** when https is used).

Java and Tomcat versions

VRA V7.0 supports Java version 8 build 40 and above, and Apache Tomcat 8 version 8.0.21 and above. Java and Apache Tomcat version 7 are no longer supported.

Using the Backup Host Role

To avoid false tickets regarding storage access or SAN I/O configuration inconsistency that involves backup servers, configure the backup servers inside a business entity and assign the 'Backup' role.

Fixed Issues

The dependency between Path (PV) to HBA is not always available

Tickets and Topology involving I/O paths may not show the connection between an I/O path and its HBA port. [P-7638, P-7612]

Incorrect ticket regarding mount resources in Solaris Zone environment

Gap ID 00500VCSONNOMOUNT may generate false tickets regarding the path of mount resources. [G-378]

Incorrect ticket regarding shared storage not connected to cluster nodes

In rare cases Gap ID 00571GCSGNM may generate incorrect tickets regarding cluster node not connected to the shared storage devices. [G-340]

Incorrect ticket regarding suboptimal SAN I/O policy

VRA may incorrectly open suboptimal SAN I/O policy tickets when the selected policy is PRNX_PSP_RR. [G-1177]

A ticket may not be opened regarding insufficient number of Netapp hot spares

In certain conditions, the system may not open a ticket regarding an issue of insufficient number of NetApp hot spare disks. [G-1240, G-1181]

Gap ID 448 (VLAN ID Inconsistency) may open incorrect or unclear tickets

Occasionally tickets of gap ID 448 are opened that do not show any VLAN ID inconsistency [G-1234]

The data presented in the table under the ticket description is not highlighted and does not mark the abnormal VLAN id. [G-1239]

Scan of IBM UDB V10.x may fail

The scan of IBM UDB version 10 and above may fail. [P-7207]

Gap ID 456 (VM Port Group inconsistency) may open incorrect tickets

When the VMs are pinned through affinity rules to hosts with proper port group configuration, non-impactful tickets may be opened by gap ID 456. [G-1342]

Scanned virtual machine that is moved to a new vcenter appears as a physical server

When a scanned virtual machine is migrated to a new vcenter, it may appear in VRA as a physical server. [A-344]

Oracle ASM disk group not connected to physical volume on Linux hosts

In certain cases, Oracle ASM disk groups are not always correctly associated with physical volumes on Linux hosts. [P-7890]

WebLogic domain info partially collected

In rare cases, the domain information of a WebLogic Application server is not collected. [P-7883]

WebLogic server not connected to its host

In rare cases, topology does not show the connection between a WebLogic server and its host. [P-7874]

Gap signatures may fail to run successfully

Execution of Gap signatures may fail to complete successfully, reporting an error in the log file (Gap IDs 380, 405, 456, 419, 239, 494, 1600, 417, 418). [G-1366, G-1357, G-1419, G-1305, G-1393, G-1423, G-1346, G-1358, G-1435]

Solaris zones partially collected

In rare cases, specific solaris zones may not be collected and documented. [P-7882]

WebSphere deployments info partially collected

In rare cases, the deployments information of a WebSphere Application server is not collected. [P-7878]

Tomcat application information is partially collected

When Tomcat uses a non-default directory, tomcat configuration is not collected. [P-7855]

Scan fails for hosts assigned with "Rotating Password" Credentials

Host scan may fail when a “Rotating Password” Credentials Type is used and password change is due. [P-7854]

Oracle ASM disk groups are not always collected when scanning OEM

Oracle ASM disk groups may not be collected when scanning through OEM. [P-7851]

Non-actionable scan issue generated for EMC VNX/CLARiiON

In case SnapView is not being used, a non-actionable scan issue regarding SnapView query command failure is presented. [P-7850]

Sybase database scan may fail

Sybase database scan may fail occasionally. [P-7811]

Data collection of VMware Distributed Virtual Uplinks Port Group List may fail

The system may fail to collect information regarding VMware Distributed Virtual Uplinks Port Group Lists. [P-7800]

The “/” char appears as “%2f” in an ESXi cluster name

The “/” character appears as “%2f” in an ESXi cluster name. [P-7776]

Incorrect tickets opened due to insufficient permissions to test a directory

In case the scan user is missing permissions to read a mount point or other directory, incorrect tickets may be opened regarding missing directories. [P-7349]

Note: Users who have encountered this issue should verify that the read-only cat and ls commands are authorized for the scan user by the privilege management solution used by the organization (generally referred to as “sudo”), and enable the following two system properties in order to resolve it:

- Collection - Use sudo for the cat command
- Collection - Use sudo for the ls command

Incorrect ticket regarding MS-SQL files

In rare cases, incorrect tickets are opened regarding MS-SQL files that do not exist. [P-7727]

Virtual Machines templates are presented as actual virtual machines

In specific cases, VM templates are presented in the standard list of virtual machines. [P-6999]

Incorrect tickets opened by gap ID 494 (NTP best practices) when an ESXi host is not selected for scan

When a host is returned by a scanned vCenter but the host itself is not enabled for scanning, an incorrect ticket is opened by Gap ID 494 for the host. [G-1438]

Incorrect tickets may be reported when LVM mirroring is used

Incorrect tickets may be reported when LVM mirroring is used and the mirror sets within the volume groups are inconsistent in terms of storage configuration. [G-1397]

Invalid file system name collected

In rare cases, the system collected an invalid file system name. As a side effect, RPO SLA gaps could go un-detected. [G-1387]

Gap ID 420 (vMotion misconfiguration) May open non-impactful tickets if DRS mode is set to manual

When VMware DRS mode is set to Manual, non-impactful tickets may be opened by gap ID 420. [G-1344]

Gap ID 463 (vCenter VM and DRS best practice) may open incorrect tickets

Gap ID 463 may open incorrect tickets when affinity rules are configured to pin the VM to host/s. [G-1343]

Tickets of Gap ID 2410 (SRM Protection Group consistency) are unclear

The risk and information included in tickets of Gap ID 2410 are unclear [G-852]

Prolonged deletion of symptoms as part of the risk analysis

In rare conditions when an exceptionally high number of symptoms must be deleted, the system may require a long period of time for completing the deletion, thus leading to prolonged risk analysis [A-435]

Gap ID 310 (LVM Mirroring) may open incorrect tickets

Incorrect tickets are reported when LV mirror ID is not consistent on the PV and/or array [G-1321]

Import hosts from a CSV file may fail

When importing hosts from a CSV file that includes business entity hierarchy, import may fail. [A-426]

Obsolete scan issues are not removed after storage proxy replacement

When a user replaces the proxy used to scan a storage system, scan issues regarding last scan through the previous proxy remain in the Scan Troubleshooting page and report. [A-418]

Gap ID 419 (Admission Control) may open incorrect tickets

Tickets of gap ID 419 are opened for un-scanned ESXi clusters. [G-1334]

Topology display function may not show all entities

The “Display all connected entities” topology operation does not show bi-directional connections. [A-412, A387]

Agent scan of a Windows host using its IP address fails

Scanning a Windows host installed with an agent through its IP address fails. [A-408]

Connection to VRA agent may fail

Occasionally the connection between the master or collector server to the VRA agent may fail, thus leading to scan failure. [A-406]

Application Server Enrichment error

In certain conditions an enrichment rule processing WebLogic deployment information may fail. [A-405]

Disabled arrays are scanned

During a cycle the system scans an array through a storage proxy even if the array was disabled by the user for the proxy. As a result, arrays accessible to multiple proxies are scanned multiple times. [A-393]

In certain conditions SLA gap signatures may fail to load policy details

In certain conditions SLA gap signatures may fail to load policy details and SLA violation risk detection may not work as expected. [A-390]

In rare conditions RPO SLA violation may go un-detected

RPO SLA violations based on user-defined policies may go un-detected under rare circumstances. [G-1364]

“Show all hosts” requires a long period of time to present the list

In very large environments, the "show all hosts" operation may require a long period of time to complete. [A-365]

Business Continuity Risks report does not correctly count suppressed tickets

Tickets of suppressed gap types are not correctly counted in the statistics presented by the Business Continuity Risks report. [A-311]

Local IBM ServerRAID controllers are identified as IBM DS arrays

Local IBM ServerRAID controllers are incorrectly identified as IBM DS arrays. [P-7902]

Note: Following an upgrade to V7.0 and full scan, delete any "IBM.Serv" storage systems listed under step 2 of the configuration wizard.

Incorrect HDS arrays are identified on hosts accessing VNX and HDS

Incorrect HDS arrays are identified on hosts accessing VNX and HDS. [P-7901]

Note: Following an upgrade to V7.0 and full scan, delete any HDS systems listed under step 2 which are not identified as actual HDS system by the storage administration team.

---

vCenter scan fails with an exception

When the target vCenter returns no information for license query, the scan of the target vCenter will fail. [P-7897]

Invalid objects remain the VRA database following a Delete Host operation

Invalid objects remain the VRA database following a Delete Host operation. This issue may lead to prolonged run time of internal validation and correction processes running on startup and as part of the risk analysis. [A-440]

Login is not allowed until internal validation process is completed

User Login is not allowed until the completion of an internal data validation and correction process which is executed on startup. [A-444]

Known issues

This VRA release has the following known issues planned to be fixed in future releases.

If you contact Symantec Technical Support about one of these issues, refer to the incident number in brackets.

Ticketing and reporting issues

False tickets for database files stored on a mixture of RAID types [P3314]

When you separate rollback segments and data files, VRA may generate false tickets about database files stored on a mixture of RAID types.

Workaround: Suppress the tickets.

False tickets for an EMC Symmetrix device [P4439]

VRA may generate false tickets about EMC Symmetrix device ID 000.

Workaround: Suppress the tickets.

False tickets may be generated after an Oracle RAC failover [P6175]

When an Oracle RAC failover occurs, VRA may generate false tickets about image storage replication errors.

Workaround: Suppress the tickets.

False tickets may be generated if collectors' times are not synchronized [P5975]

When cluster nodes are scanned using different collectors, VRA may generate false tickets if the collectors' times are not synchronized.

Workaround: Suppress the tickets.

Host HBA Comparison report is occasionally not readable in a standard PDF/RTF report size [A14]

Due to a large number of HBA properties, the Host HBA Comparison report may not be readable when executed for Linux and exported as a PDF or RTF file.

Workaround: Export the report to Excel.

Non-impactful ticket regarding mixed storage may be opened when ASM mirroring is used [P7607]

When you use Automatic Storage Mirroring (ASM) and each mirror resides on a different array, VRA may open an incorrect ticket regarding mixed storage.

Workaround: Suppress the tickets.

False tickets of Gap 01003WSMANR - Windows Services not running [P7333]

When you configure VRA with 'Automatic Trigger Start', VRA may still report these services should be running.

Workaround: Suppress the tickets or the Gap type.

Duplicate gap suppression messages in the Ticket History tab [A19]

After you suppress a gap and perform multiple ticket searches, the **Ticket History** tab of a ticket of the suppressed gap may show multiple suppression records.

Incorrect tickets are opened for MSCS when resource names end with white space [P6724]

When resource names end with white space, VRA may report incorrect tickets for Microsoft Cluster.

Workaround: Suppress the ticket.

False ticket regarding masking configuration inconsistency [G364]

Gap 00322SANMIC may generate incorrect ticket when the host name is defined using a capital letter on the storage and using lower case letters on the host (or vice versa).

Workaround: Suppress the ticket.

NFS share is mistakenly recognized as CIFS share [G360, P7817]

Gap 00360NFSIA may generate tickets that incorrectly classify NFS as CIFS.

Simple recovery mode tickets are opened for Snapshot databases [G351]

Gap 01074MSSQLRMS generates a non-impactful ticket regarding Simple Recovery mode for snapshot databases.

Workaround: Suppress the tickets.

Incorrect ticket regarding EMC CLARiiON/VNX - number of hot spares [G1011]

In certain conditions, VRA may report incorrect tickets regarding suboptimal number of hot spares for EMC CLARiiON or VNX arrays.

Workaround: Suppress the tickets.

Incorrect ticket regarding missing VCS LV resources [G1173, G1185]

In specific circumstances, VRA may incorrectly open tickets regarding missing VCS LV resources.

Workaround: Suppress the tickets.

In specific scenarios, when a replication source becomes the target and the target becomes the source, VRA does not calculate the data age for the replication [P6484]

This error may occur when, between two scans, the source is changed to be the target and the target is changed to be the source.

Incorrect ticket regarding EMC CLARiiON/VNX hot spares [P7861]

VRA may incorrectly open EMC CLARiiON/VNX hot spare best practice violation tickets (Gap ID 255). [P-7861]

Workaround: Suppress the tickets.

Several Gap signatures may fail [G1426, G1420, G1391]

Execution of Gap IDs 456, 380 and 313 may fail to complete successfully, reporting an error in the log file.

Gap ID 00238GKRORB may incorrectly open a ticket [G1367]

Gap ID 238 may incorrectly open a ticket regarding using the LB policy for a gatekeeper device when only one path is configured.

Workaround: Suppress the tickets.

Topology view issues

The Topology search for relationships may take too long to complete [P2757]

The search for relationships which contain many records may take several minutes to complete.

Workaround: Symantec recommends to use the Topology module, browse to the selected host, and review the associations between the host's physical volumes and SAN devices. This process is more focused, efficient, and significantly shorter.

Service Level Agreement (SLA) issues

In certain circumstances, the SLA module is only partially updated [P4172]

Adding a business entity partially updates the SLA module.

Workaround: After you add a business entity, run the analysis cycle so that the changes take effect.

Application issues

Setting an SLA in the Edit Business Entity wizard might fail in the Internet Explorer (IE) 6 [P5654]

JavaScript errors may pop up when setting an SLA in the Edit Business Entity wizard using the Internet Explorer 6.

Workaround: Try again or use the **Edit Role & SLA Definition** button.

Some user interface functions might not work correctly in IE 10 and IE 11 [A254]

Some user interface functions might not work correctly using IE 10 or IE 11.

Workaround: Use Internet Explorer 10/11 Compatibility View.

Errors presented regarding Active Directory connection are not informative [A69]

In some cases, a detailed error message regarding the Active Directory (AD) connection error is not presented.

Workaround: Review the rg.0.log file for additional information or contact Support.

Configuration tab - user selection is dismissed due to table data refresh [A247]

In specific screens of the **Configuration** tab, user selection of records gets unselected after a short period of time (refresh interval).

The collector configuration file is not updated [A11]

When you update the VRA server configuration file, the change might not populate to all the collectors.

Workaround: Restart the VRA server and then restart all the collectors.

Manually adding Host URLs reduces the size of the list box [A10]

When you add Host URL in the Active Directory Configuration screen, the size of the list box is decreased with each host URL added.

Deleted AD domains may still appear in the Add User dialogue [A21]

Deleted Domains are presented in the domain field of the Add User dialogue.

Users may manage scheduled reporting tasks created by other users [A55]

You may be able to see and edit scheduled reports tasks that were created by other users, potentially for entities external to their own user scope.

Excel export of database list contains object IDs instead of names [P7835]

When exporting information presented in the "View Databases" dialogue to Excel, some of the columns in the output file contain object ID instead of name.

Excel export of storage array list contains object IDs instead of names [A438]

When exporting information presented in the step 2 of the Configuration Wizard to Excel, some of the columns in the output file contain object ID instead of name.

HTTP Error 404 when accessing the VRA GUI [A448]

In rare conditions, users may experience an HTTP 404 Page not Found error when accessing the VRA user interface.

Workaround: Delete the cookies from IE, open a new browser window and login.

Deletion of invalid OS/Host object requires a long period of time [A439]

Upon startup and as part of the risk analysis, the system runs an internal validation and correction process for hosts. If a large number of invalid hosts found, the system may require a long period of time in order to delete them, up to several hours. [A-439]

Creation of SAPI_STORAGE_MASKING DB view may require a long period of time [A431]

In exceptionally large VRA environments, the creation of the SAPO_STORAGE_MASKING database view may require a long period of time, up to several hours.

Unsupported Credentials type can be selected for Active Directory authentication [A348]

The system enables users to selected credentials type which are unsupported for Active Directory authentication, such as “Rotating Password” and “SSH Public Key”.

Dashboard may present inactive collectors as “Down” [A377]

The dashboard may present inactive collectors as collectors which are down.

Login is not allowed during the risk analysis task [A368]

User Login are not allowed to login during a risk analysis task, even when the “allow login during full cycle” is marked.

AD Domain names are case sensitive in VRA [A395]

Duplicate domain records can be configured within DRA with the same name but different letter case.

Verify Configuration for Database Views does not check privileges granted through roles [P7845]

The Verify Configuration operation available for Database Views does not check the privileges granted for the user through user roles.

Scanning issues

When VRA scans a suspended DB2 database, queries may fail [P4438]

If VRA scans a database when the database is suspended, most queries may fail.

DB2 discovery fails on a host scanned using a proxy [P5049]

VRA cannot discover DB2 on a UNIX host that is scanned through a proxy.

Workaround: Scan the host directly and not through the proxy.

VRA may identify unsupported devices incorrectly [P4310]

VRA shows unsupported storage array devices as direct-attached storage (DAS) devices, which may open false tickets.

Workaround: Suppress the tickets or avoid scanning hosts that use storage that VRA does not support.

Only active Network Interface Cards (NICs) are collected on Solaris [P5934]

VRA does not collect NICs which are “unplumb”.

IBM DS GlobalMirror replication might not be presented correctly [P6481]

VRA may fail to present IBM DS GlobalMirror replication.

Workaround: Contact Symantec Technical Support for assistance.

IBM DS/XIV LUN discovery might be incorrect for Solaris/HP-UX hosts [P6480]

VRA may fail to discover the correct LUN for UNIX hosts accessing IBM DS or XIV storage.

Workaround: Contact Symantec Technical Support for assistance.

Failure when scanning a vCenter with no managed ESX/ESXi hosts [P7659]

When executing a scan of a vCenter with no hosts, the scan fails.

Server incorrectly classified as partially scanned [P7610]

In rare circumstances, an incorrect scan error is reported regarding a `/dev/unknown` PV that leads to a partial scan status.

Workaround: Suppress the scan issue and consider the scan as successful.

Incorrect collection of XIV cluster name [P7339]

When the cluster name includes multiple words separated by white space, only the first word is collected.

Occasionally a non-impactful scan error message is presented

A scan error with the `No MPIO disks are present` message is occasionally opened for Windows servers. [P7307]

Scan errors for EMC VNX clone/mirror command may appear when these features are disabled. [P7240]

Workaround: Ignore or suppress the scan issue under the Scan Troubleshooting screen

Inactive disk groups and logical volumes are not always collected [P7250, P7041]

Information regarding inactive disk groups and unmounted logical volumes is not always collected.

HBA driver information is not always available for Linux systems [P7196]

In rare cases, HBA model, driver, and firmware information is not available for Linux systems.

HMC scan may fail in an IBM FLEX environment [P7667]

When HMC is scanned in an IBM Flex environment, the scan may fail.

Workaround: Contact Symantec Technical Support for assistance.

If the security level on the Naviseccli server is set to MEDIUM, EMC VNX scan hangs. [P6964]

Workaround: Reduce the security level to allow scanning.

When the password contains special characters, EMC VNX arrays scan fails [P6962]

Workaround: Change the password such that no special characters are included.

Discovery may report UDB instances as down [P6949]

In rare cases, VRA may report online UDB instances as down.

Workaround: Contact Symantec Technical Support for assistance.

Free space information is not available for Windows 2003 Servers [P6053]

Free space information is not available for Logical volumes on Windows 2003 Servers.

Scan status report does not include Management Consoles [A25]

The Scan Status report does not include information regarding scan of management consoles.

Workaround: Review the status of the consoles in the **Configuration** tab or in the System Log report.

Nodes with the same cluster name and ID are incorrectly merged to a single VCS [P7773]

In certain cases when multiple clusters with the same name, VRA may incorrectly merge these clusters to a single VCS.

Oracle ASM disk groups are not always collected [P7797]

In certain cases where the target name is not consistently defined between OEM tables, ASK disk group information may not be collected.

Agent scan failure on Windows servers with only .NET 4 installed [A319]

When the target Windows system is only installed with .NET 4, the VRA agent fails to run VB data collection scripts on it.

Error connecting ASM Disk groups to SunOS/AIX physical volumes [P7892, 7891]

In specific cases, the system may fail to identify on which SunOS/AIX physical volumes the Oracle ASM diskgroups are stored.

Incorrect scope issue regarding storage array not being scanned [P7889]

The system may incorrectly report a "Source/Target replication not scanned" message in the Scan Troubleshooting page for storage arrays that are in fact scanned.

Workaround: Ensure that both the storage systems are scanned as part of the same cycle.

Non-actionable scan issues reported for EMC Symmetrix arrays [P7841]

When no RDF groups are defined on the array, the system may incorrectly open a scan issue reporting the failure of the "symcfg list -rdfg" command.

Workaround: Suppress the scan issues.

Incorrect mapping of NFS mount to CIFS export [P7817]

In specific cases, the system may incorrectly associate an NFS mount to a CIFS export.

Command error not presented as a scan issue [A413]

The system does not always present command errors as scan issues in the Scan troubleshooting GUI. Examples: the NetApp license-v2-list-info, IBM get_local_nodename commands.

Command timeout scan issue does not present script name [A353]

In rare cases, the "Command with high importance timed out" scan issue may fail to include the name of the script.

Scan Troubleshooting page may not report on un-scanned Brocade switches [P7869]

The Scan Troubleshooting page under the Configuration tab may fail to report on discovered but un-scanned Brocade switches.

Limitations

Assigning a profile to an Active Directory group

- When assigning a profile to an AD Universal Group, the VRA master server must have access to the Global Catalog of the AD Forest
- When assigning a profile to an AD Local Domain Group, VRA will not be able to assign the Profile to AD Users from a different Domain - even though such configuration is valid within AD. In other words - an AD user can log in to VRA (with all the correct profiles assigned) only if each AD Local Domain Group it belongs to is part of the same AD Domain the AD user belongs to

Oracle database discovery

To discover Oracle databases, start the Oracle process or ensure that the `/etc/oratab` or `/var/opt/oracle/oratab` file is present.

Recovery point objective (RPO)/service level agreement (SLA)

VRA also has the following RPO/SLA limitations:

- RPO/SLA is not supported in HDS
- RPO/SLA for NetAPP only works for direct replication from primary devices
- RPO/SLA for CLARiiON only works for direct replication from primary devices

- RPO/SLA for HP 3PAR only works for direct replication from primary devices.
- RPO/SLA is not calculated for EMC CLARiiON MirrorView/S
- RPO/SLA is not calculated for IBM DS

Incorrect time logged in system log files when DLS is not automatically updated

VRA log files may log incorrect timestamp when the VRA server is not configured with automatic Day Light Saving adjustment.

VRA Database Views include a subset of the information collected from target systems

VRA Database Views do not include information regarding VMware Virtual Networking, Database Tablespaces, Installed Software and Kernel Parameters, RecoverPoint consistency groups, LV mirroring, and Application Servers. Also, it does not include the historical data.

In specific cases scan error messages are not sufficiently informative

The Scan Troubleshooting screen occasionally presents scan error messages that include the error code but no additional details.

Workaround: Run the erroneous command or script manually to see the full scan error message. If further assistance required, contact Symantec Technical Support.

Incorrect tickets may open when target systems are not scanned successfully

When certain target systems are not scanned successfully, VRA may open incorrect tickets as a result.

Workaround: Search for the symbol specifying whether scan issues exist in the ticket summary, and review any scan issues reported in the ticket or in the Scan Troubleshooting prior to reviewing the risk details.

Large amount of memory is consumed when generating an extremely large report [P5455]

When generating reports with over 500 pages, large amount of memory may be consumed

Workaround: Limit the scope of the report or divide it to multiple reports.

When importing objects into VRA, special characters are converted [A87, A109, A105]

When importing names and properties of objects from CSV/CMDB/API, special characters such as the ampersand (&), nonbreaking space ( ) and certain UTF8 characters are converted to alphanumeric characters.

Minor differences may be reported for dynamic or site-dependent parameters [P7219]

In certain cases, VRA may report differences related to options that are dynamically changing or depending on the location and thus non-impactful.

Workaround: Suppress these differences.

SSH key supports only keys with less than 4000 characters [P6645]

SSH key only supports the keys with less than 4000 characters.

When NTLMv2 is used, authentication may fail [P7206]

Scanning systems in an environment where only NTLMv2 is allowed may fail without additional configuration.

Workaround: Contact Symantec Technical Support for assistance.

VRA may fail without notice when no space left on its disk drives [A41]

When nearly no space is left on the disk drives storing the VRA software, the system may fail without a notice.

Workaround: Take particular care to ensure sufficient free disk space is available on the master server.

HMC is required in order to scan IBM VIO environments [P6835]

If HMC is not available and you use IVM, contact Technical Support for assistance.

CSV Import of Business Entities does not create new sites [A15]

The Import process uses the site field to correctly match hosts specified in the CSV file to existing hosts, but does not create the sites if they do not exist in the system.

Workaround: Use step 3 of the Configuration Wizard to define any missing sites (manually or through CSV import).

Incorrect replication mode and state collected for an array included in the symavoid file

When a scanned Symmetrix array is included in the symavoid file on a SYMCLI server, it will not correctly report the status and mode of replications for the array.

Workaround: Take care to use SYMCLI servers which can effectively report on the replication mode and status - both for the source and target arrays.

Scan of large vCenter system may require a long period of time

When scanning exceptionally large vCenter systems, scan may require a long period of time to complete. [P-7894]

Workaround: use collectors that are located within the same site as the target vCenter, and ensure latency is minimal (<10ms). Increase data collection timeout values through the VRA System Properties dialogue as needed.

Installation notes for this release

Read the Installation Procedure chapter of the User Guide for guidance about installing VRA V7.0. In addition, review the Deployment Guide for information on the VRA infrastructure requirements and the prerequisites for scanning your data centers.

Upgrade for this release

An upgrade path to the VRA version 7.0 is available from the DRA 6.4.1 release. If your system is currently installed with an earlier release, an upgrade to version 6.4.1 is mandatory before upgrading to version 7.0.

Important Notes:

- The upgrade requires the complete stop of VRA operations, including data collections and data analysis. While it is a fully automatic process, the length of the upgrade process may require several hours to complete in large environments. During this time, it is important not to restart the VRA server or terminate the upgrade task. In addition, it is essential that the Oracle database used by VRA will be available throughout the upgrade process.
- Before you upgrade, read the release notes in full, and make any necessary changes to the VRA infrastructure and/or to user account permissions as required, and make sure you have sufficient free disk space on the master server.
- Verify that you have an up-to-date backup of the VRA server disk drives using your standard backup tools, and an up-to-date VRA database export. You can generate a database export using the EXPDP or EXP Oracle command.
- When the master VRA server is updated and the Tomcat service starts, VRA automatically checks and upgrades the VRA collectors. There is no manual collector upgrade process. For gradual collector upgrade, disable the collectors before initiating the upgrade on the master server, and gradually enable the collectors you wish to upgrade following the completion of the software upgrade on the master server.

To upgrade from version 6.4.1 to version 7.0:

1. **Disable collectors**. If collectors are used - either stop all VRA services on the Collector servers or disable the collectors from the **Collectors** user interface by double-clicking a collector and un-checking the **Enabled** box.
2. On the master VRA server, login as a local administrator.

3. Run the **VRA_7_0.exe** as an administrator.
4. On the **Welcome** screen, click **Next**.
5. The Java 8 update 45 64-Bit installation wizard will start if not already installed. Ensure that Java is installed correctly and do **not** select removal of outdated Java versions.
6. Select **"Yes, upgrade DRA 6.4.1 to VRA 7.0"**.
7. Accept the License Agreement and click **Next**.
8. Accept the GNU License Agreement and click **Next**.
9. Select whether to perform a database export prior to upgrading and whether to start Tomcat 8 after the upgrade completes, and click **Next**. It is recommended to keep the default settings.
10. Click **Install** to begin the Software Upgrade process.
11. Click **Finish**.

Getting help

If you have a current maintenance agreement, you may access Symantec Technical Support information here:

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

Customer service information is available here:

www.symantec.com/support/assistance_care.jsp

Note: If you forget or lose the VRA administrator password, contact Symantec Technical Support.
