Veritas™ Risk Advisor Release Notes

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

7.2

Document version: 7.2 Rev 0

Last updated: 2016-12-04

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043
http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

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

https://sort.veritas.com/documents

Documentation feedback

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

doc.feedback@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

About this document

This document provides important information about Veritas Risk Advisor (VRA) 7.2. Review this entire document before you install and use VRA 7.2.

Getting more information or help

- For the latest information about updates, patches, and software issues regarding this release, see the following Late Breaking News (LBN):
  https://www.veritas.com/support/en_US/article.TECH68401
- For more information about system requirements and software limitations, see the following documents:
  - Veritas Risk Advisor Support Requirements
  - Veritas Risk Advisor Deployment Requirements
- If you forget or lose the VRA administrator password, contact Veritas Technical Support.

Overview of Veritas Risk Advisor

VRA is a risk detection and management solution that enables organizations to diagnose high availability (HA) and disaster recovery (DR) vulnerabilities (gaps) and optimize data protection. It empowers enterprises to effectively manage business continuity implementations to ensure that critical business data is protected at all times.

VRA is an agentless discovery and monitoring tool that automatically scans your enterprise infrastructure to detect vulnerabilities in the HA/DR configurations. It alerts you to any potential gaps, best practice violations, and service level agreement (SLA) breaches.

The information and insight provided by VRA includes:

- Detailed information about the current data protection and HA/DR risks and the prioritized actions that you can take to fix them
- Recommendations for improving HA/DR performance based on best practices and recovery objectives
- Differences that it identifies between the production, standby, and DR systems
- Auditing and compliance documentation, including a topology map of your production environment, DR configuration, and dependencies

Changes introduced in this release

The following changes have been introduced in this release.

New features

This VRA release introduces new features in the following areas:

Area	New feature
Hitachi Virtual Storage Platform G1000 Support	Support has been added for collecting Hitachi Virtual Storage Platform G1000 information and analyzing it for potential risks. Refer to the *Veritas Risk Advisor Deployment Guide* for information regarding the scan requirements.
RedHat Cluster Support	Support has been added for collecting RedHat Cluster information and analyzing it for potential risks. The support is currently limited to RedHat Cluster Suite version 6.x. Refer to the *Veritas Risk Advisor Deployment Guide* for information regarding the scan requirements.
Automated HealthCheck Report	New HealthCheck Executive Summary Report has been added. This report clearly and briefly presents the scope of scan, main findings and conclusions. Also, numerous gap signatures were redesigned for the sake of improved clarity and accuracy of tickets.
Internet Explorer 11 Support	VRA can now run in Internet Explorer 11 without the need to set the Compatibility View. Older versions of Internet Explorer are no longer supported.
Gaps	New gap signatures have been added.
Enhancements and resolved issues	A number of known issues have been addressed, as well as requested enhancements, which have been implemented.

Documentation packaging change

Beginning with release 7.2, VRA documentation will not be included in the tar ball with the VRA software. You can access the VRA docs at the following location:

https://sort.veritas.com/documents

Note: You need to select Risk Advisor in the Product list.

New privileged commands

The following new read-only privileged commands are required:

Command	Mandatory?	Required for scanning
`ccs --getconf`	Yes	RedHat Cluster
`ccs –cehckconf`	Yes	RedHat Cluster
`clustat`	Yes	RedHat Cluster

Refer to the *Veritas Risk Advisor Deployment Guide* for information regarding privileged command requirements.

Additional changes and enhancements

The following additional changes and enhancements have been introduced in this release.

New system properties

The following system properties that pertain to the **System Timeouts** category are added:

Property	Description
Timeout for scanning all DCNM in minutes	This property defines the period in minutes after which the scan of all DCNM systems will be aborted. The default value is 180 minutes.
Timeout for scanning all Brocades in minutes	This property defines the period in minutes after which the scan of all Brocade switches will be aborted. The default value is 180 minutes.
Timeout for scanning all HPVirtualConnect in minutes	This property defines the period in minutes after which the scan of all HPVirtualConnect systems will be aborted. The default value is 180 minutes.
Timeout for scanning all Cisco in minutes	This property defines the period in minutes after which the scan of all Cisco switches will be aborted. The default value is 180 minutes.
Timeout for scanning all BNA in minutes	This property defines the period in minutes after which the scan of all BNA systems will be aborted. The default value is 180 minutes.
Timeout for scanning all Infinidat in minutes	This property defines the period in minutes after which the scan of all Infinidat systems will be aborted. The default value is 180 minutes.
Timeout for a single DCNM scan, in minutes	This property defines the period in minutes after which the scan of a single DCNM system will be aborted. The default value is 90 minutes.

Property	Description
Timeout for a single Brocade scan, in minutes	This property defines the period in minutes after which the scan of a single Brocade switch will be aborted. The default value is 90 minutes.
Timeout for scanning all vCenters, in minutes	This property defines the period in minutes after which the scan of all vCenters will be aborted. The default value is changed to 300 minutes.
Timeout for a single vCenter scan, in minutes	This property defines the period in minutes after which the scan of a single vCenter will be aborted. The default value is 180 minutes.

Data collection enhancements

The following enhancements are included:

ID	Description
[N-380]	When scanning Windows servers using WMI protocol, VRA tries to connect both directly and using the collector local host as a proxy in case the direct connection fails. In the latter case, the target user should be added to collector's local administrator group.
[N-339]	Added indirect connection between Datastore to its Virtual Machines in the Topology view
[N-249]	Improved FCPATH modeling and collection for VMware's Native Multipathing (NMP) and PowerPath across all supported Operating Systems.
[N-134]	Add Affinity Rules presentation to the Topology view
[N-299]	Connect Windows Physical volumes to NetApp volumes using Serial Number
[N-288]	A scan issue is added when a VM was scanned but the corresponding ESX cluster is not (disabled)
[N-72]	IBM SVC/V7000 storage masking configuration information is now collected
[N-356]	ZFS Mirroring modeling has been improved
[N-234], [N-302]	SAN, WRM and WMI timeouts are now exposed in the UI for the admin user
[N-403]	Default vCenter timeout scan values have been enlarged
[P-7206]	Scanning systems in an environment where only NTLMv2 is allowed

Application enhancements

The following application enhancements are included:

ID	Description
[N-311]	Cross Site Scripting (XSS) vulnerability resolved
[N-234]	Housekeeping Cleanup actions have been improved
[N-217]	A new system property allows to limit the maximal number of objects to be displayed in the Topology view and in Ticket Details report
[N-213]	Installer prompts with detailed information regarding available vs. required disk space during the upgrade

Improved risk categorization and ticket clarity

The following gap signatures have been revised (logics enhancements and/or additional data to tickets):

ID	Description
[N-177]	Gap 489 - Inconsistent ID for shared ESX cluster LUNs
[N-107]	Gap 300 - Storage group inconsistency
[N-106]	Gap 554 VCS Service Group with no critical resources
[N-105]	Gap 300 - Storage volume physical split
[N-104]	Gap 700 - Number of I/O paths SLA violation
[N-103]	Gap 443 - VMs not configured with UUID
[N-102]	Gap 421 - RDM volumes not configured on all ESX cluster nodes
[N-100]	Gap 397 - Suboptimal HBA configuration
[N-99]	Gap 245 - Devices with dead SAN I/O paths
[N-98]	Gap 447 - Suboptimal NFS Max Queue Depth setting
[N-97]	Gap 304 - Partial replica sets
[N-96]	Gap 446 - Transparent Page Sharing (TPS) is enabled
[N-95]	Gap 490 - ESX inconsistent LUN number
[N-94]	Gap 494 - Incorrect timekeeping configuration on ESX nodes
[N-93]	Gap 451 - Datastores not configured on all cluster nodes
[N-92]	Gap 318 - Inconsistent SAN I/O Access

ID	Description
[N-292]	Gap 255 - Hot Spare best practice violation
[N-70]	Gap 2410 – Inconsistency between SRM protection groups and storage
[N-340]	Gap 441 – Invalid CBT configuration

Important Notes

Review the following important notes about the various VRA configurations.

Oracle database locale requirement

The oracle instance used as the backend database for VRA must be configured with the English Locale. This requirement is complementary to other requirements identified in the Deployment guide and/or other documents.

Internet Explorer requirement

Internet Explorer (IE) Enhanced Security must be disabled on the VRA server. Accessing the VRA application using IE on the VRA server when IE Enhanced Security is enabled can lead to configuration errors. This requirement is complementary to other requirements identified in the Deployment guide and/or other documents. **Important**: VRA 7.2 requires Internet Explorer 11, without the need to set the Compatibility View. The minimum recommended version of Internet Explorer is 11.00.33. Older versions of Internet Explorer are no longer supported.

Scanning HP 3PAR using InForm CLI proxy

When using InForm CLI proxy to scan HP 3PAR arrays, it is mandatory to use encrypted passwords.

Scanning Hitachi G1000

Scanning of Hitachi G1000 systems requires HiCommand API version 8 or higher – which is different from the default version considered by VRA. Please make sure that the system property HiCommand API major version, which can be found under the Collection system properties, is set to 8.

Scanning NetApp storage systems using SSL

If an error is experienced when connecting to NetApp storage systems using SSL, perform one of the following changes to resolve the connection error:

- Enable TLS on the target NetApp storage system using the `option tls.enable on` command.
- 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.

Java Requirements for Viewing Topology

- Every Windows system requiring access to the VRA Web User Interface must be installed with Java Run Time Environment (JRE) 8. Java must be enabled for Internet Explorer.
- On 64-bit Windows versions, it is generally recommended to install both 32-bit and 64-bit versions of JRE to avoid compatibility issues relating to 64-bit vs. 32-bit computing.
- If Internet Explorer 64-bit is used, ensure JRE 64-bit is installed. Alternatively, if Internet Explorer 32-bit is used, ensure JRE 32-bit is installed.
- Important notes:
  - The default Internet Explorer 8 is 32-bit.
  - Internet Explorer 10 is 64-bit - however it uses 32-bit iexplore.exe processes to run the IE tabs. Thus, Java 32-bit is also required.

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.

Enabling data collection from vSphere Infrastructure Navigator (VIN)

In order to enable remote data collection from VIN, the following steps must be performed on the VIN appliance:

- Edit the `/opt/vadm-engine/webapps/jolokia/WEB-INF/classes/jolokia-access.xml` configuration file and specify the IP Address of the VRA collector that will connect VIN.
- Run the `/opt/vadm-engine/bin/disable_security.sh` script in order to enable remote connection (disables some of the local security configurations such as firewalls).
- Restart the VIN discovery engine by running `/etc/init.d/vadm-engine restart`.
- Check connection by browsing to the `http://[VIN IP]:8080/jolokia` URL.

Scan of Storage and Replication Management servers

It is recommended to scan all production/DR storage management servers as hosts in step 4 of the configuration wizard – also in the case they are already scanned through step 2. Scanning the servers as hosts ensures all replication group information is collected and analyzed.

Scan of Windows hosts through WMI

Scanning of Windows hosts updated with KB3139940 might fail with Access Is Denied message. To overcome this failure, please make sure that the user configured to authenticate to this server is a member of the Local Administrator group on the VRA server.

Fixed issues

This VRA release includes the following fixed issues.

Scan and data collection issues

The following issues are resolved:

ID	Description
[N-341]	Several ESX PVs are not connected to their NetApp SAN SVs
[N-386]	XIV Storage Masking collection issue
[N-239]	Inconsistent Hitachi Array ID returned by different sources
[N-320]	Exception in DBFileToOSObject
[N-219]	Failure to identify PV on Solaris host
[N-174]	HDLM Paths not collected in certain cases on Windows
[N-77]	HDS Collection: inqraid command fails with segmentation fault
[N-173]	XIV volume serial number does not uniquely identify a volume
[N-294]	Wrong Item ID for Oracle RAC
[N-295]	Multiple multipath tools manage the same storage volume
[N-283]	MSCS node not connected to required devices
[N-326]	Unable to scan vCenter with newer VI API with error: Requested array size exceeds VM limit
[N-319]	Exception in OracleASMDiskGroup
[N-290]	Unable to scan BNA
[N-378]	Praxair POC - Incorrect path type on Windows with HDLM
[N-375]	Exception when scanning BNA: ERROR preloading set fcswitches
[N-201]	Can't connect to WMI server through proxy
[N-129]	3PAR replication doesn't connect well with VC

ID	Description
[N-243]	Incorrect serial number collection from HDS machines
[N-390]	VPLEXVirtualVolume is filtered when saving VPLEX XML response
[N-366]	AIX+VxDMP Parsing Issues - Partial Replication Tickets
[N-410]	CLARiiON LUN to FED-Port connection added
[N-400]	DB2 files are filtered out
[N-439]	Windows registry query for HBA parameters added
[N-308]	Rule PV-to-SV has failed

Scan management and troubleshooting issues

The following issues are resolved:

ID	Description
[N-346]	Manual setting of cli.exe path does not work when 3PAR proxy server runs on Windows
[N-354]	Issues with XML parsing when scanning WebLogic servers
[N-387]	Incorrect scan issue reported for VCS HAHB
[N-355]	Incorrect scan issue reported for IBM CCD
[N-384]	Redundant scan issue on FCINFO on Windows VM
[N-74]	WebLogic script collects unnecessary additional data
[N-246]	Sudo misconfiguration generates errors in the raw data but no scan issues

Risk detection issues

The following issues are resolved:

ID	Description
[N-391]	Exception in Gap 304
[N-347]	Exception in Gap 512
[N-350]	Exception in Gap 280
[N-296]	Exception in Gap 242
[N-337]	Exception in Gap 318
[N-352]	Exception in Gap 250
[N-338]	Exception in Gap 705
[N-321]	Exception in Gap 2200

ID	Description
[N-441]	Exception in Gap 1805
[N-309]	Exception in Gap 494
[N-353]	Gap 487 - Description table is missing
[N-172]	Gap 505 – Wrong ticket opened when share resource missing mount resource
[N-171]	Gap 554 – Wrong ticket opened when VCS service group is of type "parallel"
[N-247]	Gap 419 – wrong ticket opened for clusters with "Host Monitoring" disabled
[N-293]	Gap 300 – Wrong ticket opened for Non-Active VG
[N-301]	Gap 580 – Wrong ticket opened with HBA Speed 0
[N-344]	Gap 300 – Wrong ticket opened due to missing ASM Group mirroring data collection

Application and user interface issues

The following issues are resolved:

ID	Description
[N-395]	DiskSet Enrichment fails with Exception
[N-318]	Exception in pseudoPV
[N-291]	Exception in log when browsing configuration tab
[N-212]	"Activity report" fails with exception
[N-165]	There is no error message in the UI when we fail to delete a proxy definition that used by a policy
[N-215]	Incorrect Licensing expiration message is presented at the Login screen
[N-256]	Hosts that are part of a comparison worksheet and are deleted - cause an error
[N-289]	Unable to see entities assigned to Business Entity
[N-214]	Formatting Issues with Tickets Exported to PDF
[N-300]	Error in Column "HBA Supported Speed" in "Report SAN SUBOPTIMAL SPEED"
[N-69]	Host HBA Comparison Report causes a NullPointerException
[N-351]	False ticket opened due to unexpired properties
[N-164]	Notes always has a 3 dots suffix [...] and a tooltip, even if they are empty
[N-137]	CLARiiON: Add Storage Array: Adding a port value larger than 5 characters crashes the window
[N-421]	User is able to login without password
[N-333]	Exception when an user wants to associate few hosts with a policy

Known issues

This VRA release has the following known issues planned to be fixed in future releases.
If you contact Technical Support about one of these issues, please refer to the incident number in brackets.

Ticket and report issues

The following ticket and report issues exist:

ID	Description	Workaround
[A-14]	Due to a large number of HBA properties, the Host HBA Comparison report may not be readable when executed for Linux and exported as PDF/RTF.	Export the report to excel.
[A-19]	After suppressing a gap and performing multiple ticket searches, the history tab of a ticket of the suppressed gap may show multiple suppression records.	-
[A-510]	Report: What-If Impact Analysis: Report generation fails failed under certain circumstances.	-
[A-551]	VMware Summary report contains incorrect set of ESXi hosts; some hosts are potentially not marked for the scan while other scanned hosts may fail to be included.	-
[A-578]	Gap Id 1601 (Snapshots enabled for Zerto Virtual Manager - ZVM) - when ticket is exported, impact contains ">".	-
[G-1504	Gap Id 360 (NFS options inconsistency) may generate large tickets or non-impactful tickets.	Suppress the ticket.
[G-1580]	Gap Id 700 (SLA) may fail reporting an exception in the log file.	-
[G-1591]	Gap Id 80459 (Network redundancy and resiliency) may open incorrect tickets for iSCSI environments.	Suppress the ticket.
[G-1602]	Gap Id 700 (SLA) may fail when replication target set is defined as “Any Site”.	-
[G-1634]	Gap Id 225 (Mixture of database files) may open tickets that include no details under the description section.	Suppress the ticket.

ID	Description	Workaround
[G-1716]	Gap Id 306 (Inconsistent Database Replication) may fail reporting an exception in the log file.	-
[G-1734]	Gap Id 335 (SAN switch single point of failure) may open incorrect tickets for logical ISL between logical Brocade switches.	Suppress the ticket.
[P-3314]	When rollback segments and data files are separated, VRA may generate false tickets about database files stored on a mixture of RAID types.	Suppress the ticket.
[P-5975]	When cluster nodes are scanned using different collectors, VRA may generate false tickets if the collectors' times are not synced.	Suppress the ticket.
[P-6484]	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. 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.	-
[P-7333]	Gap Id 1003 (Windows services not running): when configured with 'Automatic Trigger Start', VRA may still report these services as such that should be running.	Suppress the tickets or the Gap type.
[P-8080]	When OEM data is outdated for certain databases, consequently VRA may open tickets with outdated / incorrect information.	Suppress the ticket.
[G-1828]	Gap Id 242 (Host Accessing Remote Devices) may fail.	-
[G-1791]	Gap Id 500 (VCS Online mount resource failure) may open inaccurate tickets reporting incorrect file systems and block devices mismatches.	-
[P-8205]	Gap Id 234 (Wrong visibility) may open incorrect tickets regarding EMC meta devices.	-
[P-8201]	Certain Gap signatures may open tickets for Powered-off virtual machines.	Suppress the ticket.
[P-8161]	Gap Id 420 (vMotion not configured) may open non-impactful tickets when vMotion is enabled on distributed virtual switches.	-

ID	Description	Workaround
[P-8118]	Gap Ids 213 and 250 may open tickets with no textual description.	-
[G-1829]	VRA does not take Affinity and VM to host rules into consideration in certain Gap signatures and non-impactful tickets may be opened.	-
[G-1826]	Non-impactful partial replication tickets may be opened when Oracle redo log multiplexing is used and only some one of the redo log members of each group is replicated.	-
[N-508]	Veritas logo doesn't appear in the ticket report	-
[N-521]	Export to excel does not work from Ticket Details tab when table contains a hyperlink	-

Topology view issues

The following topology view issues exist:

ID	Description	Workaround
[A-534]	Incorrect Topology connection between 3PAR Vol and Masking Configuration.	-
[P-8095]	NetApp vServers are not presented in the topology as storage arrays.	-

Application issues

The following application issues exist:

ID	Description	Workaround
[A-10]	When adding Host URL in the Active Directory Configuration screen, the size of the list box is decreased with each host URL added.	-
[A-11]	When updating the VRA server configuration file, the change might not populate to all the collectors.	Restart the VRA server and then restart all the collectors.

ID	Description	Workaround
[A-21]	Deleted Domains will be presented in the domain field of the Add User dialogue.	-
[A-377]	The dashboard may present inactive collectors as collectors that are down.	-
[A-384]	The system enables users to select credentials type which are unsupported for Active Directory authentication, such as “Rotating Password” and “SSH Public Key”.	-
[A-431]	In exceptionally large VRA environments, the creation of the SAPO_STORAGE_MASKING database view may require a long period, up to several hours.	-
[A-438]	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.	-
[A-448]	In rare conditions, users may experience an HTTP 404 Page not Found error when accessing the VRA user interface.	Delete the cookies from IE, open a new browser window and login.
[A-495]	Collector that failed to upgrade is marked as enabled/healthy.	-
	Check upgrade, collector and server health log files.	-
[A-511]	Error when adding SYMCLI proxy with no description.	Add a description when adding a SYMCLI proxy.
[A-512, P-8104]	Windows host/storage proxy cannot be scanned using credential sets defined with domain suffix (e.g. user@domain).	Redefine the credential with domain prefix (e.g. domain\user).
[A-521, A 520, A 523]	In certain conditions, Gap Tuning page fails to un-suppress tickets or suppresses tickets that should not be suppressed.	-
[A-532]	Changing policy for EMC CLARiiON/VNX array with no associated proxy may fail.	-
[A-543]	In rare cases, clicking the “save” button does not actually save the worksheets in Host Comparison tab.	-
[A-55]	Users may see and edit scheduled reports tasks that were created by other users, potentially for entities external to their own user scope.	-

ID	Description	Workaround
[A-563]	Unable to create a group-based scan/cycle task using IE8/9.	Use IE10/11, and ensure compatibility mode is enabled
[A-575]	Failure to define custom gap using "Not Empty Result Set" Condition.	-
[A-579]	Installer starts the Tomcat8 service even when the checkbox is unchecked	-
[A-580]	The system does not accept the suppression date requested by the user if the chosen day of week is the same as the current.	Select the next or previous day.
[A-69]	In some cases, a detailed error message regarding the AD connection error is not presented.	Review the rg.0.log file for additional information or contact Support.
[G-1717]	The Business Continuity Risk Report may present incorrect number of Storage scanned under certain conditions.	-
[P-7835]	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.	-
[P-8067]	Duplicate system events logged when SAN switches are scanned.	-
[P-8202]	When testing SMTP configuration and authentication fail, an incorrect message is presented regarding successfully completing the test.	Check your email to ensure a test email was in fact received.
[A-633, P-8195]	When entering an invalid character or white space in the IP field of a target management or storage proxy, scan may fail and the scan symbol will continue to spin.	-
[A-635]	Agent cannot be deleted from the Agents page if it was already uninstalled on the server	First delete the agent in the GUI and only then perform the uninstall operation.
[A-683]	When send ticket by email fails, no notification is presented to the user.	-

ID	Description	Workaround
[A-696]	Change CLI path under the Scan Troubleshooting page is occasionally disabled.	-
[N-535]	Redundant scroll bars appear in the Topology view after the browser window is maximized and then restored to its normal size	-

Scanning issues

The following scanning issues exist:

ID	Description	Workaround
[A-25]	The Scan Status report does not include information regarding scan of management consoles.	Review the status of the consoles in the Configuration tab or in the System Log report.
[A-353]	In rare cases, the “Command with high importance timed out” scan issue may fail to include the name of the script.	-
[A-505]		-
	SRM may fail with the following message: “Unsupported version URI urn:srm0/2.0”.	Contact support.
[P-4310]	VRA shows unsupported storage array devices as direct-attached storage (DAS) devices, which may open false tickets.	Suppress the tickets or avoid scanning hosts that use storage that VRA does not support.
[P-4438]	If VRA scans a database when the database is suspended, most queries may fail.	-
[P-5049]	VRA cannot discover DB2 on a UNIX host that is scanned through a proxy.	Scan the host directly and not through the proxy.
[P-5934]	VRA ignores NICs that are configured as “unplumb” on Solaris hosts.	-
[P-6053]		-
	Free space information is not available for Logical volumes on Windows 2003 Servers.	-

ID	Description	Workaround
[P-6480]	VRA may fail to discover the correct LUN for UNIX hosts accessing IBM DS or XIV storage.	Contact Support for assistance.
[P-6481]	VRA may fail to present IBM DS GlobalMirror replication.	Contact Support for assistance.
[P-6962]	When the password contains special characters, EMC VNX arrays scan fails.	Change the password such that no special chars are included.
[P-6964]	If the security level on a “Naviseccli” server is set to MEDIUM, EMC VNX scan hangs.	Reduce the security level on the Naviseccli server to allow scanning.
[P-7041]	Information regarding inactive disk groups is not always collected.	-
[P-7196]	In rare cases, HBA model, driver and firmware info is not available for Linux systems.	-
[P-7659]	When executing a scan of a vCenter with no hosts, the scan fails.	-
[P-7667]	When HMC is scanned in an IBM Flex environment, the scan may fail.	Contact support for assistance.
[P-7773]	In certain cases when multiple VCS clusters with the same name exist, VRA may incorrectly merge these clusters to a single one.	-
[P-7978]	LUN Map info is not collected for IBM V7000, Storwize and SVC.	-
[P-8007, P-8006]	Brocade and HP Virtual Connect switches scan may fail and a scan issue will not be reported.	-
[P-8020]	Unnecessary scan issue for 3PAR showr* commands when remote copy is not licensed.	Suppress the scan issue.
[P-8035]	NaviCLI and InformCLI scan may wait on user prompt and fail with timeout. Certain storage proxies may enter user-interactive mode upon executing the first command by a user, and ask to approve certain initial settings.	Such settings should be completed prior to scanning with VRA, as interactive mode will cause the scan to hang.

ID	Description	Workaround
[P-8039]	Unnecessary scan issue reported for symcfg command when no RDF replications are configured.	Suppress the scan issue.
[P-8061]	Unnecessary scan issue for Microsoft MPIO when the mpclaim.exe command returns a “No MPIO disks are present” message.	Suppress the scan issue.
[P-8177]	HBA data collection may fail on certain Windows 2003 servers.	-
[P-8163]	"Last Successful Scan" is not always updated after a successful scan.	-
[A-688]	Killed scan tasks appears as “Timed out”.	-
[F-77]	Windows 2008 R2 clusters defined with the same name at remote sites might be incorrectly identified as the same cluster	-

Limitations

You may encounter the following limitations when working with VRA.

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 for active HDS asynchronous HUR replication.
- 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, Application Servers and does not include 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 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.

Incorrect tickets may open when file read permission is not granted

When VRA cannot read or list a file or a directory, incorrect tickets may open.
Workaround: Take particular care to grant the required privileges for the user configured for the scan, as described in the VRA deployment guide [A-619].

When importing objects into VRA, special characters are converted

When importing names and properties of objects from CSV/CMDB/API, special characters such as “&”,‘no-break-space’ and certain UTF8 chars are converted to alphanumeric chars. [A87, A109, A105]

Non-impactful differences may be reported for dynamic or site-dependent parameters

In certain cases, VRA may report differences relating to options that are dynamically changing or depending on the location and thus non-impactful. [P7219]
Workaround: Suppress these differences.

SSH key supports only keys with less than 4000 characters

The SSH key supports only those keys that contain less than 4000 characters. [P6645]

HMC is required in order to scan IBM VIO environments

If HMC is not available and IVM is used, contact Support for assistance. [P6835]

CSV Import of Business Entities does not create new sites

The Import process will use the site field to correctly match hosts specified in the CSV file to existing hosts, but will not create the sites if they do not exist in the system. [A-15]
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 that can effectively report on the replication mode and status – both for the source and target arrays.

SAN switches installed with unsupported versions should not be scanned

Refrain from scanning a Fabric if it includes switches that are installed with an unsupported version. For information regarding supported versions, refer to the VRA Support Requirements document. [P-7971]

JDBC-SSL is not supported for database scanning

It is not possible to connect and scan databases using JDBC SSL. [P-7964]

Linux Software RAID devices managed by mdadm are unsupported

As a result, VRA may report a non-actionable scan issue regarding unknown mdadm host physical volumes not connected to storage volumes. [A-618]

SAN switches are not automatically removed when no longer discovered by their proxy

SAN switches are not automatically deleted when their proxy no longer discovers them. [A-522]

Modal dialogs cannot be moved on the screen

Modal dialogs (pop-up windows) cannot be moved on the screen – use mouse wheel to scroll when needed.

Upgrading to this release

For information about installing VRA, see the *Veritas Risk Advisor User's Guide*. In addition, review the *Veritas Risk Advisor Deployment Guide* for guidance about the VRA infrastructure requirements and the preparations needed for scanning your datacenters.

You can upgrade to VRA 7.2 only from version 7.1.1. If a system has an earlier version of the product installed, you must upgrade to version 7.1.1 before upgrading to version 7.2.

Consider the following before you begin the upgrade process:

- Carefully read the release notes in full, and make any necessary changes to the VRA infrastructure and/or to user account permissions as required, and ensure sufficient free disk space is available 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. A database export can be generated using the EXPDP or EXP Oracle commands.
- Once the upgrade on the master VRA server is completed 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.
- The upgrade requires that you completely stop all VRA operations, including data collections and data analysis. While it is fully automatic, 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 be available throughout the upgrade process.

- During the upgrade to version 7.2, a few symptoms might be deleted. This might result in reopening of some tickets of gaps 421 and 451 in case these tickets were closed by suppressing these specific symptoms. In this case, you need to suppress these symptoms again as a one-time action.
- **Important**: VRA 7.2 requires Internet Explorer 11, without the need to set the Compatibility View. The recommended minimum version of Internet Explorer is 11.00.33. Older versions of Internet Explorer are no longer supported. Make sure you have IE11 installed on all clients.

To upgrade from version 7.1.1 to version 7.2

1. Login as a local administrator to the master VRA server.
2. Run the `VRA_7.2.exe` file as an administrator.
3. On the Welcome screen, click **Next**.
4. When prompted, select **Yes, upgrade VRA 7.1.1 to 7.2**.
5. Accept the License Agreement and click **Next**.
6. Accept the GNU License Agreement and click **Next**.
7. Specify whether to perform a database export prior to upgrading and whether to start Tomcat 8 after the upgrade completes, and click **Next**. Veritas recommends that you keep the default settings.
8. Click **Install** to begin the software upgrade process. This process may require up to several hours to complete, depending on the size of the scanned environment.
9. Click **Finish** to close the installer.