



Veritas™ Risk Advisor Release Notes

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

7.2.4

Legal Notice

Copyright © 2018 Veritas Technologies LLC. All rights reserved.

Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third party software for which Veritas 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. Refer to the third party legal notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

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. VERITAS TECHNOLOGIES LLC 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 Veritas 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.

Veritas Technologies LLC

500 E Middlefield Road

Mountain View, CA 94043

<http://www.veritas.com>

Veritas Risk Advisor

Release Notes

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) 7.2.4. Review this entire document before you install and use VRA 7.2.4.

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.000037525
- 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 always protected. 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 and highlights

This VRA release introduces new features and significant enhancements in the following areas:

Area	New feature
Oracle VM for SPARC support	Support has been added for Oracle VM for SPARC (formerly Solaris LDOM). VRA now collects all the needed information about Oracle VM for SPARC while scanning the physical Solaris host, identifies all relevant domains and analyzes them for potential risks
NetApp SolidFire support for VMware	Support has been added for NetApp SolidFire LUNs accessed by VMware ESXi hosts. VRA now collects the relevant information from vCenter and analyses it for potential risks.
VRA server ported to Tomcat 8.5	As part of Continuity Software's continuous effort to improve product security, VRA server runs now under Tomcat 8.5 .
Improved Topology functionality	Refer to "Application enhancements" for additional information.
Improved Host Comparison functionality	Refer to "Application enhancements" and "New/Modified system properties" for additional information.
Improved Database Views functionality	Refer to "Application enhancements" and "Application and user interface issues" for additional information.

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

This version introduces no new privileged commands.

Additional changes and enhancements

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

New/Modified system properties

The following system properties are added or modified:

Category	Property	Description
Cloakware Configuration	Cloakware Client Classpath	Default value is none (empty)
General	Include database quantitative statistics in the Server report log	Default value is "No"
Host Comparison	Windows registry entries to ignore in Host Configuration Differences report	Default value is HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Hostname, HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\NV Hostname
Host Comparison	Acceptable hardware difference percentage in Host Configuration Differences report	Default value is 80
Host Comparison	Maximum number of differences to show in Host Configuration Differences report	Default value is 400
Host Comparison	Product name filter regexp in Host Configuration Differences report	Default value is .*\.msg\..*\.man\..*
Host Comparison	Kernel Params filter regexp in Host Configuration Differences report	Default value is none (empty)

Veritas Risk Advisor

Release Notes

Category	Property	Description
Host Comparison	Regexp of ratio-based comparison kernel parameters in Host Configuration Differences report	Default value is .*mem.* .Memory.* .msgmax.*
Host Comparison	Ratio-based comparison kernel parameters ratio in Host Configuration Differences report	Default value is 98
Host Comparison	Users filter regexp in Host Configuration Differences report	Default value is none (empty)
Host Comparison	ESX options to ignore in Host Configuration Differences report	Default value changed to Misc.CosCorefile,ScratchConfig.ConfiguredScratchLocation, ScratchConfig.CurrentScratchLocation, Syslog.Local.DatastorePath, Mem.HostLocalSwapDir,Vpx.Vpxa.config.vpxa.hostIp, Vpx.Vpxa.config.vpxa.hostKey,Migrate.Vmknics, Misc.SIOControlFlag, Misc.SIOControlFlag1,Misc.SIOControlFlag2, UserVars.VshieldEndpointSolutionsConfiguration, UserVars.VshieldVsmConnectionInfo, Syslog.loggers.vpxa.rotate, Syslog.global.logDir

Veritas Risk Advisor

Release Notes

Category	Property	Description
Host Comparison	VMware VM options to ignore in Host Configuration Differences report	Default value changed to evcCompatibilityMode,sched.swap.derivedName, nvram,migrate.migrationId,migrate.hostlog, migrate.hostLogState,vm.genid,vm.genidX,scsi0.sasWWID, vmotion.checkpointSVGASize,vmotion.checkpointFBSize, vmware.tools.requiredversion,tools.remindInstall, tools.guest.desktop.autolock,vmware.tools.internalversion, toolsInstallManager.updateCounter, guestinfo.vf.tc.clientLicenseState,debugStub.linuxOffsets, unity.customColor,unity.wasCapable,softPowerOff, replay.supported,usb:0.deviceType,. *pciSlotNumber, . *.present,. *CPUID. *, guest.commands.sharedSecretLogin.com.vmware.vin, kernel.sched_domain. *, *.sasWWID,machine.id,
Maintenance	Split the deletion process of expired entities to small deletion groups (per items)	Default value is 0
Maintenance	Enable extended history entities cleanup (items, connections, properties) during the scanning validation enrichment	Default value is "No"
Reports	Acceptable hardware difference percentage in Host Configuration Differences report	Moved to Host Comparison category, values kept
Reports	Maximum number of differences to show in Host Configuration Differences report	Moved to Host Comparison category, values kept
Reports	Product name filter regexp in Host Configuration Differences report	Moved to Host Comparison category, values kept

Veritas Risk Advisor

Release Notes

Category	Property	Description
Reports	Kernel Params filter regexp in Host Configuration Differences report	Moved to Host Comparison category, values kept
Reports	Users filter regexp in Host Configuration Differences report	Moved to Host Comparison category, values kept
Reports	ESX options to ignore in Host Configuration Differences report	Moved to Host Comparison category, values kept
Reports	VMware VM options to ignore in Host Configuration Differences report	Moved to Host Comparison category, values kept
Rule Engine	Gap platform process jvm parameters	Default value changed to – Xmx3200M
SLA	Regexp filtration for Replication SLA calculation	Default value is . .*quorum.*,rootdg,.*rootvg,.*temp.*,.*swap.*,/mnt,MSDTC
SLA	Regexp filtration for Retention SLA calculation	Default value is . .*quorum.*,.*temp.*,.*swap.*,/mnt,MSDTC
SLA	Regexp filtration for LVM/Storage Mirroring SLA calculation	Default value is . .*quorum.*,rootdg,.*rootvg,.*temp.*,.*swap.*,/mnt,MSDTC
System Alerts	Enable database memory issue detector	Default value is “No”
SLA	Ignore volume groups, logical volumes and file systems that match regular expression for host level calculation	Replaced with “Regexp filtration for Replication SLA calculation”, values kept
Tickets Module	Display the filter tree	Default value is “Yes”
Topology Module	Undo stack depth	Default value is 10
Topology Module	Maximum number of compound property instances to show in Item tab	Default value is 10

Category	Property	Description
Web Service API	Parallel task queue	Default value is "No"
Web Service API	Parallel task queue depth	Default value is 10

Data collection enhancements

The following enhancements are included:

ID	Description
[N-1504]	Solaris LDOMs – add modelling vCPUs in addition to physical CPUs
[N-1494]	Add "isThinEnabled" boolean property for VNX LUN
[N-1167]	Add "Type" Property needed for LV item
[N-1598]	Add Quorum type property for Microsoft Cluster (MSCS)
[N-1529]	Add a property for a file system managed by cluster and configured in OS
[P-8368]	Add support for Infinidat Replication Lag (RPO)

Risk detection enhancements

The following risk detection enhancements are included:

ID	Description
[G-2156]	Gap 00529VCSVGLV severity changed to "Error"
[G-1492]	Gap 00390SANIOInconsistency performance (runtime) optimization
[G-1967]	Gap 00700HSLARPO logics enhanced to reduce number of tickets for ESX clusters
[N-927]	Gap 00390SANIOIP logics enhanced to reduce number of tickets
[G-2108]	Gap 00243SBMPTS logics enhanced to avoid false tickets
[A-1133]	Add support for EMC Isilon for SLA breaches detection
[A-1145]	Add "LUN Name" to SLA tickets
[A-1146]	Allow more granular control on Ignore Volumes/File systems list for SLA calculations

Application enhancements

The following application enhancements are included:

ID	Description
[N-1591]	Enable installing and running VRA Server on Windows 2016
[A-1013]	Improve deletion of RGDB expired objects
[A-1153]	Topology module: Add "Undo" button

Veritas Risk Advisor

Release Notes

ID	Description
[N-1655]	Topology module: Enhance performance by collapsing properties with many values
[A-1108]	Tickets Module: Add "Match all / Match any" option when filtering tickets by label
[N-1572]	Tickets Module: Remove ability to delete default label from ticket
[A-1112]	Tickets Module, TicketDetails report: Add option to filter temporarily suppressed tickets only
[A-1140]	TicketDetails report: Add additional sorting options
[P-8397]	Host Comparison: Improve User/Groups comparison to avoid duplicate findings
[A-1064]	Host Comparison: Define threshold for reporting meaningful differences
[A-841]	Host Comparison: Add comparison for additional Windows hosts configurations
[A-1050]	Host Comparison: Report on Patches and Services in separate categories
[P-7074]	Host Comparison: Add Refresh button to the DEFAULT worksheet
[A-1066]	Database Views: Add MaskingConfiguration.name to SAPI_STORAGE_MASKING table
[A-1048]	Database Views: Add SYSTEM_EVENT table
[A-764]	Database Views: Add external ticket ID to SAPI_TICKETS table
[A-43]	Database Views: add Area, Labels, Rating to SAPI_TICKETS table
[A-1136]	Database Views: add Scan Group Status to SAPI_SCAN_GROUP
[A-1040]	System Event Log: add events for summarizing total run time of various tasks
[A-1039]	System Event Log: add event for rating or adding a note to a ticket
[A-1113]	Enable scheduling of application restart
[A-1120]	Enhanced configuration for external ticketing integration over e-mail
[N-1520]	Changing gap.platform.jvm.parameters system property should not require application restart
[A-1065]	Add more granular permissions for changing tickets status
[A-87]	Allow using '&' (ampersand) in Business Entities names
[P-8527]	Indicate number of selected rows in UI tables that allow multiselection
[G-2159]	Improve layout of ticket tables
[N-1627]	Transport Layer Protection TLSv1.2

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.

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 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 Runtime Environment (JRE) 8. The latest tested version is 1.8.0.161.
- 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.

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 `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. As of version 7.2.1, VRA provides also an alternative method of scanning Windows servers using WMI which requires PowerShell version 5.1 or higher.

Recommended display size and resolution

VRA's web user interface is best displayed and operated with Full HD resolution (1080p) on minimum 21" screens with aspect ratio of 16:9. Using smaller screens and/or coarser resolution might cause some screens to be partially displayed – in these cases browser's zoom-out function might be used to entirely display the specific screen.

Fixed issues

This VRA release includes the following fixed issues.

Scan and data collection issues

The following issues are resolved:

ID	Description
[G-2169]	False SLA tickets
[G-2167]	OracleASMDiskGroup failure
[P-8536]	Wrong 3PARs arrays detection due to wrong DEC to HEX conversion
[P-8534]	PVtoSV connection issues EMC vPlex to VMware
[P-8535]	MSFLAddHDSDiskIDFromNAA failure
[P-8522]	Error in DCP - hierarchy list list for Unity should contain the member CLARiiON
[P-8521]	OEM response loading failure
[P-8499]	Property types are not correct for InfiniBox RemoteCopy replication
[N-1557]	Missing cmd_prefix for /usr/bin/systool
[G-2154]	Problem connecting ESXi PVs to ESXi FCOE HBAs
[N-1541]	Linux cluster resources not collected (EL6)
[A-1128]	Problem mapping Linux PVs to EMC XtremIO storage volumes
[P-8506]	No connection between IBM SVC and XIV
[A-1306]	vMotion NICs collection issue

Scan management and troubleshooting issues

The following issues are resolved:

ID	Description
[P-8508]	Missing scan issue on insufficient permissions in vcs_directories.sh
[N-1429]	Incorrect PV2SV scan issue reported for Solaris

Risk detection issues

The following issues are resolved:

ID	Description
[G-2139]	Gap 00242PRIMARY logics enhanced to correctly consider NetAppVserver
[G-2166]	Gap 00242PRIMARY logics enhanced to correctly consider SVC
[G-2162]	SLA number of SAN I/O paths violation description problem
[G-2160]	00409IEVCM logics enhanced to consider additional CPU architectures
[P-8526]	Exception in Gap01921VMAntiAffinityRuleRedundancy
[N-1547]	Gap 00473CVNA logics enhanced to avoid false tickets

Application and user interface issues

The following issues are resolved:

ID	Description
[A-1160]	BladeServerSystem enrichment failure
[N-1638]	Typo in VMware Datastore item info
[G-2164]	Ignore list of SLA detector doesn't work as expected
[P-8478]	Report fails to generate due to incorrect XML formatting
[N-1615]	The email alert regarding "insufficient memory for Oracle database" is sent twice
[A-877], [A-438]	Issues with exporting to excel in Configuration Wizard - step 2
[A-474]	Issues with exporting to excel in Configuration Wizard - step 5
[A-1038]	SAPI_TICKETS, FIRST_DETECTION_DATE represents the LAST detection date
[A-23]	SAPI does not contain RecoverPointRemoteCopy in SAPI_CONSISTENCY_GROUP
[P-8524]	SAPI Grant List - customized values delete after upgrade
[P-8516]	OEM scan failure
[A-863]	Unable to delete comparison worksheets of retired AD users
[A-862]	Deleting a user that created Comparison worksheets results in problems loading worksheets
[A-1086]	UI performance issues when opening or filtering for objects
[A-971]	Cloakware plugin "stop" logs
[A-431]	Creation of SAPI_STORAGE_MASKING requires 9 hours in large DB

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 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-1634]	Gap Id 225 (Mixture of database files) may open tickets that include no details under the description section.	Suppress the ticket.
[G-1716]	Gap Id 306 (Inconsistent Database Replication) may fail reporting an exception in the log file.	-

Veritas Risk Advisor

Release Notes

ID	Description	Workaround
[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.	-
[G-1791]	Gap Id 500 (VCS Online mount resource failure) may open inaccurate tickets reporting incorrect file systems and block devices mismatches.	-
[P-8161]	Gap Id 420 (vMotion not configured) may open non-impactful tickets when vMotion is enabled on distributed virtual switches.	-
[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.	-

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-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-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-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.	-

Veritas Risk Advisor

Release Notes

ID	Description	Workaround
[A-532]	Changing policy for EMC CLARiiON/VNX array with no associated proxy may fail.	-
[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.	-
[A-579]	Installer starts the Tomcat service even when the checkbox is unchecked	-
[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 arrays 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 fails, 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.	-
[A-696]	Change CLI path under the Scan Troubleshooting page is occasionally disabled.	-

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.	-
[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.

Veritas Risk Advisor

Release Notes

ID	Description	Workaround
[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.
[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.	-
[A-688]	Killed scan tasks appears as "Timed out".	-
[P-8443], [P-8421]	Unable to scan Oracle DB due to VIP not found on host	
[P-8440]	SCVMM Hyper-V replicas with same name as primary cannot be scanned	

ID	Description	Workaround
[P-8438]	Exception on vCenter scanning within Full Cycle when parallel scan of vCenters is enabled	
[P-8389]	VG not connected to PV on HP-UX hosts with DMP	
[P-8379], [P-8365]	Cisco DCNM zone collection issues	
[P-8337]	Invalid Windows HDS HDLM string format	
[P-8408]	Solaris zones discovery incorrectly assumes uniqueness of zone names	
[P-8491]	Some properties of Oracle DB are not collected when DBs are scanned via OEM	

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, A105]

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.

Firefox does not support Java applets in its new versions

Starting from version 53 (released April 2017), Firefox does no longer support Java plugins and thus the Topology widget might not work properly (in version 52 the Java plugin support is disabled by default but can be turned on). In order to continue running VRA on Firefox, consider using the Firefox 52 ESR (Extended Support Release) 32-bit version.

Topology module might refresh when scrolling other pages on Firefox

Topology module might refresh (flicker) when scrolling other pages (for example – ticket info) on Firefox – this is due to a known Firefox issue published by Mozilla.

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 7.2.4 only from version 7.2.3. If a system has an earlier version of the product installed, you must upgrade to version 7.2.3 before upgrading to version 7.2.4.

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.

- **Important:** Upgrading VRA from version 7.2.3 to version 7.2.4 includes also upgrading Tomcat from version 8.0 to version 8.5
 - New “tomcatuser” will be created automatically by the installation wizard with a new random password
 - Tomcat8 service is disabled, the old tomcatuser is removed
 - Tomcat settings are migrated to the new Tomcat service automatically, including Java memory settings. If additional Tomcat settings were modified manually in Tomcat configuration files (tomcat-users.xml, server.xml, web.xml, etc), they should be set in the new Tomcat service manually as well.
- **Important:** Tomcat 8.5 supports TLS1.2 encryption. Users that configured HTTPS access to VRA server should re-configure it according to instructions – please consult the support team.

To upgrade from version 7.2.3 to version 7.2.4

1. Login as a local administrator to the master VRA server.
2. Run the `VRA_7_2_4.exe` file as an administrator.
3. On the Welcome screen, click **Next**.
4. When prompted, select **Yes, upgrade VRA 7.2.3 to 7.2.4**.
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 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.