VERITAS

Veritas™ Risk Advisor Release Notes

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

7.2.1

Last updated: 2017-02-17

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) 7.2.1. Review this entire document before you install and use VRA 7.2.1.

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
Oracle Exadata Support	Added support for collecting Oracle Exadata Storage Server information and analyzing it for potential risks. **Note**: Exadata support requires Oracle Enterprise Manager (OEM) version 12 or higher. For information on the scan requirements, see the *Veritas Risk Advisor Deployment Guide*.
Dell EMC XtremIO	Added support for collecting Dell EMC XtremIO information and analyzing it for potential risks. For information on the scan requirements, see the *Veritas Risk Advisor Deployment Guide*.
Hitachi Virtual Storage Platform G Series	Added support for collecting information from additional models of Hitachi VSP G series (G200, G400, G600, G800). This furthers the support for Hitachi G1000 platform that was added in version 7.2. For information on the scan requirements, see the *Veritas Risk Advisor Deployment Guide*.
CA Privileged Access (Cloakware) support	Integration with CA Privileged Access (formerly Cloakware) has been added to assure safe access to credentials. For information on settings and integration, see the *Veritas Risk Advisor Deployment Guide*.
Mozilla Firefox Support	Added support for running Veritas Risk Advisor in the Mozilla Firefox browser. The recommended version of Firefox is 50 or higher.
Global Labels	Added support for adding a global label to all the tickets of a specific gap—existing and future—as opposed to an individual ticket. For more details, see the *Veritas Risk Advisor User Guide*.

Area	New feature
Gaps	New gap signatures have been added.
Enhancements and resolved issues	A number of known issues have been addressed and some requested enhancements 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

No additional privileges are required for this version.

For information on privileged command requirements, see the *Veritas Risk Advisor Deployment Guide*.

New OEM queries

VRA uses read-only JDBC queries to collect additional data from Oracle Enterprise Manager (OEM). Queries on the following views were added.

Note: Some of these views are available on OEM 12 only:

OEM View	OEM 12 only
MGMT$AVAILABILITY_CURRENT	
MGMT$APPLIED_PATCHES	
MGMT$AGENTS_MONITORING_TARGETS	Yes
MGMT$MANAGEABLE_ENTITIES	Yes
MGMT$DB_FEATUREUSAGE	Yes

Additional changes and enhancements

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

New system properties

The following system properties are added:

Category	Property	Description
Cloakware Configuration	Default Alias	This property will be used by default if the account alias is not provided in Cloakware credentials. The default is none (empty).
Cloakware Configuration	Bypass Cache	This property determines whether the local credential cache will be bypassed. The default is true.
Collection – Admin	Number of threads during probe scan	This property defines the number targets of the same type can be scanned in parallel. The default value is 1 which keeps the pre-7.2.1 behavior. **Note**: Setting this value to higher value is expected to result in a faster scanning cycle, however setting it too high might result in instability of the server and the network. Please consult support before changing it.
Collection – Admin	Login scanner WMI use PowerShell	This property controls the new method of WMI scanner using PowerShell which allows scanning Windows target servers directly with no proxy. The default value is false which keeps the pre-7.2.1 behavior. **Note**: PowerShell version 5.1 or higher is required on the VRA server
Collection – Admin	Scan Microsoft Windows Cluster using VBscript instead of PowerShell	This property controls new method of Windows Cluster scanning using PowerShell. Applicable for MS Windows Cluster 2012 or higher. If set to “yes” or if the version of MS Cluster is lower than 2012 then the scanning will require cluster.exe to be installed on the scanned server – pre-7.2.1 behavior. **Note**: the new method requires PowerShell version 3.0 or higher on the scanned server.

Category	Property	Description
Collection	Validity period (in days) of Oracle instance information retrieved from OEM	Information retrieved from OEM has timestamp older than this value will not be used for data analysis of Oracle instances. The default is 120 days.
Collection	Retry after command timeout	This property defines whether there will be made another attempt to invoke a command which failed on timeout. The default is true.
Database Views	Database Views scheduler	This property controls the optional scheduler of database views generation. The default is false.
Database Views	Database Views scheduler, day(s) of the week	This property defines on which days of week the optional scheduler of database views generation will run – if enabled. The default value is Sunday
Database Views	Database Views scheduler, time of the day	This property defines the time of the day the optional scheduler of database views generation will run – if enabled. The default value is 00:00
Maintenance	Database analyzer degree	This property determines the degree of parallelism for Oracle statistics gathering - used in the database analyzer. The default is 4.
Maintenance	Database analyzer estimate percentage table	This property determines the sampling percentage for Oracle statistics gathering - used in the database analyzer. The default is 40.
Rule Engine	Enable escalate exception for Data Analysis	This property determines whether to stop the data analysis if an execution of enrichment rule has failed. The default value is false.
Gap Rules	Should partially state be filtered	This property controls whether tickets should be created when resource is “Partially Online” or “Offline” for gap type “VCS Service group in bad state”. The default value is false.

The following system properties are changed:

Category	Property	Description
Collection	HiCommand API major version	This property specifies the HiCommand API major version to use when connecting to HiCommand. The default value cleared to allow the system to detect the most appropriate version automatically. Setting a non-empty value for this property will override the value automatically detected by the system.
Collection	HiCommand API minor version	This property specifies the HiCommand API minor version to use when connecting to HiCommand. The default value cleared to allow the system to detect the most appropriate version automatically. Setting a non-empty value to this property will override the value automatically detected by the system.
Collection	Use sudo for the ls command	This property defines whether to use sudo for the ls command. Default value changed from true to false.
Collection	Use sudo for the cat command	This property defines whether to use sudo for the cat command. Default value changed from true to false.

Data collection enhancements

The following enhancements are included:

ID	Description
[N-463]	WMI - Windows target servers can be scanned directly **Note**: PowerShell version 5.1 or higher is required on the VRA server.
[N-465]	Auto-detect clusters on Windows Server 2012 **Note**: PowerShell version 3.0 or higher is required on the scanned server.
[N-461]	Windows 2008 R2 clusters with the same name at different sites are detected as separate clusters
[N-394]	Multiple scan targets of the same type can be scanned in parallel
[N-762]	HDS scan - when scanning HiCommand, the system detects the most appropriate API version
[N-704]	Added scan issue when scanning private Solaris zone without global zone
[N-493]	Added system property to control number of retries after command/process timeout
[N-486]	Scan should not fail when using recommended sudo with out of the box system property configuration

ID	Description
[N-502]	Added Support for storage access by Hyper-V Host
[N-589]	Added collection of QueueDepth information from hosts
[N-485]	Added collection of AIX_MPIO information
[N-470]	Added collection of TransparentHugePages property on Linux servers
[N-720]	Added collection of HCC information
[N-697]	Improved collection of HBA Ports information

Application enhancements

The following application enhancements are included:

ID	Description
[N-310]	Security enhancements
[N-646]	Do not proceed with data analysis upon failure of an enrichment rule
[N-645]	View Hosts - added cluster and BE columns
[N-641]	Database analyzer degree for multithreading - default value changed
[N-640]	Added maintenance.database.analyzer.estimate.percent to configuration.xml
[N-639]	Storage Allocation Optimization Report - added ability to filter by site
[N-636]	Tomcat service when stopped should also stop the platform process
[N-605]	Granular scheduling of DB Views Update
[N-518]	Remove hosts by API/CLI

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 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:

1. 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.
2. 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).

3. Restart the VIN discovery engine by running `/etc/init.d/vadm-engine restart`.
4. Check connection by browsing to the `http://[VIN IP]:8080/jolokia` URL.

Scanning 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.

Scanning 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. Version 7.2.1 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
[N-735]	Solaris private zones are not discovered following Global zone scan
[N-701]	FP - [01009MSCSRS] MSCS resource does not have required owners
[N-571]	FP - VCS GCO communication state

ID	Description
[N-495]	00706SHSLA - SLA violation False-Positive when RACs are used
[N-490]	DB2 scan is timing out instead of failing due to SQLCODE=-551 ()

Scan management and troubleshooting issues

The following issues are resolved:

ID	Description
[N-643]	No scan issue on LPAR configured as physical
[N-575]	OEM Collection Timestamp is outdated (causes FPs)

Risk detection issues

The following issues are resolved:

ID	Description
[N-703]	Gap 451: false ticket was open in a specific scenario
[N-702]	Gap 445: false ticket was open in a specific scenario
[N-649]	Gap 555: false ticket was open in a specific scenario
[N-396]	Gap 280: false ticket was open in a specific scenario
[N-556]	Gap 322: false ticket was open in a specific scenario
[N-569]	Gap 300: false ticket was open in a specific scenario
[N-537], [N-538], [N-539]	Gap 554: false tickets were open in several specific scenarios
[N-491]	Gap 304: false ticket was open in a specific scenario
[N-712]	Gap 441: do not open tickets for powered off VMs
[N-487]	Gap 501: exception fixed
[N-444]	Gap 595: exception fixed
[N-597]	Gap 1309: exception fixed
[N-596]	Gap 300: exception fixed

Application and user interface issues

The following issues are resolved:

ID	Description
[N-768]	Unable to suppress a symptom
[N-737]	Several typos
[N-684]	aggregation when there is a list in a cell comes out wrong
[N-667]	Gap summary format issue
[N-626]	ScanningValidation Enrichment does not complete in a reasonable time (hours)
[N-623]	exceptionMarkMethod does not work with links (ticket detail report)
[N-576]	Host comparison tab -missing scroll bar to see and monitor created expansion packages.
[N-572]	Automatic Import for CMDB integration doesn't work when MSSQL is used
[N-520]	Remove label from ticket throws exception
[N-289]	Unable to see entities assigned to BE

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.	-

ID	Description	Workaround
[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.
[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.	-
[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.	-

ID	Description	Workaround
[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”.	-

ID	Description	Workaround
[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.	-
[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.

ID	Description	Workaround
[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 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.

ID	Description	Workaround
[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.
[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.

ID	Description	Workaround
[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”.	-

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.

Topology module might refresh when srolling 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 on installing VRA, see the *Veritas Risk Advisor User's Guide*. For guidance on the VRA infrastructure requirements and the preparations needed for scanning your datacenters, see the *Veritas Risk Advisor Deployment Guide*.

You can upgrade to VRA 7.2.1 only from version 7.2. If a system has an earlier version of the product installed, you must upgrade to version 7.2 before upgrading to version 7.2.1.

Consider the following before you begin the upgrade process:

- Carefully read the *Veritas Risk Advisor Release Notes* in full, and make any necessary changes to the VRA infrastructure and/or to user account permissions as required, and ensure that sufficient 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.

To upgrade from version 7.2 to version 7.2.1

1. Login as a local administrator to the master VRA server.
2. Run the `VRA_7_2_1.exe` file as an administrator.
3. On the Welcome screen, click **Next**.
4. When prompted, select **Yes, upgrade VRA 7.2 to 7.2.1**.
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.