VERITAS

Veritas™ Risk Advisor Release Notes

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

7.3.1

Document version: 7.3.1 Rev 0

Last updated: 2018-12-11

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) 7.3.1. Review this entire document before you install and use VRA 7.3.1.

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 and highlights

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

Area	New feature
F5 Load Balancer	Support has been added for F5 Load Balancer devices. VRA now collects the needed information through F5 BIG-IP management console and automatically discovers LB Pools, which can be used for Host Comparison, SLA assignments etc.
HP OneView	VRA now collects the information about HP Blade Server Systems through HP OneView management console, which enables more comprehensive risk analysis.
IBM A9000	Support has been added for IBM A9000 storage platform. VRA now collects the relevant information about IBM A9000 storage arrays and analyzes them for risks.
Hitachi Content Platform (HCP)	Initial support has been added for Hitachi Content Platform (HCP) object storage.
Enhanced Customization Capabilities	Multiple enhancements have been added to Expansion Packages module which allows more flexible and powerful customization of VRA in order to enable efficient development of complex custom checks
Performance Boost	Data Analysis cycle time has been slashed by up to 30% with special optimization for large-scale environments
Historical Host Comparison	A new report has been added to present differences between selected hosts at present and at a given point of time in the past, based on the historical data collected by VRA
Google Chrome support	VRA can run now in Google Chrome browser

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:

Additional changes and enhancements

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

New privileged commands

The following new read-only privileged commands are required:

Command	Required for scanning
adminaccess ssh option show	EMC DataDomain
adminaccess web option show	EMC DataDomain
user password aging show	EMC DataDomain
user show list	EMC DataDomain

New/Modified system properties

The following system properties are added or modified:

Category	Property	Description
Additional Collection - Admin	Enable additional collection for NetApp Expansion Package	Default value is No
Distributed Collection	Encrypt the connection between the server and remote collectors	Default value is No
Distributed Collection	Number of connection attempts for encrypted connection between the server and remote collectors	Default value is 0
Collection - Admin	Enable aggregating UNIX scripts to run as “here-document”	Default value is No. Set this property to Yes in order run UNIX scripts as a single aggregated script – and this is in order to avoid requesting elevated privileges per individual script/command
Collection - Admin	Maximal aggregated script size in bytes to create on AIX	Default value is 40000. This property is effective only when aggregating scripts is enabled.
Collection - Admin	Maximal aggregated script size in bytes to create on HPUX	Default value is 120000 This property is effective only when aggregating scripts is enabled.

Category	Property	Description
Collection - Admin	Maximal aggregated script size in bytes to create on Linux	Default value is 120000 This property is effective only when aggregating scripts is enabled.
Collection - Admin	Maximal aggregated script size in bytes to create on Solaris	Default value is 120000 This property is effective only when aggregating scripts is enabled.
Collection - Admin	The number of BIG-IP probes the system can run in parallel	Default value is 2
Collection - Admin	The number of OneView probes the system can run in parallel	Default value is 2
Collection - Admin	The number of HCP probes the system can run in parallel	Default value is 2
Collection - Admin	The number of NetAppExpansionPackage probes the system can run in parallel	Default value is 5
Collection - Admin	NetApp Expansion Package support - create NetApp storages from DFM	Default value is No
Collection - Admin	NetApp Expansion Package support - create NetAppExpansionPackage probe	Default value is No
Collection Timeouts	Timeout for scanning all NetAppExpansionPackages, in minutes	Default value is 180
Collection Timeouts	Timeout for scanning all HCP in minutes	Default value is 180
Collection Timeouts	Timeout for scanning all BIG-IP in minutes	Default value is 180
Collection Timeouts	Timeout for scanning all OneView in minutes	Default value is 180
Collection Timeouts	Timeout for a single NetAppExpansionPackage scan, in minutes	Default value is 30
Collection Timeouts	Timeout for a single HCP scan, in minutes	Default value is 60

Category	Property	Description
Collection Timeouts	Timeout for a single BIG-IP scan, in minutes	Default value is 60
Collection Timeouts	Timeout for a single OneView scan, in minutes	Default value is 60
Collection	HCP port	Default value is 9090
Collection	BIG-IP port	Default value is 443
Collection	OneView port	Default value is 443
Rule Engine - Admin	Ignore ESXi hosts in maintenance mode for Risk Analysis	Default value is No. When set to Yes, ESXi hosts in maintenance mode will not be considered for Risk Analysis, which means that no new tickets will be created, existing tickets will be closed – and reopened upon the end of maintenance
Gap Rules	Resource names to ignore in VCS GCO resource comparison in all resources	Default value is none (empty). The allowed value can be either a comma-delimited list of strings or regexp. The change take effect upon the next full cycle.
Reports	Transpose table rows and columns when exporting to excel	Default value is No. This property affects Host Comparison report only. When set to Yes, hosts appear as rows and parameters as columns in the excel report.
Reports	Maximum number of rows for excel transposition	Default value is 50 This property affects Host Comparison report only and effective only when “Transpose table rows and columns when exporting to excel” property is set to Yes.
Reports	Percentage threshold for marking differing values in excel	Default value is 66 This property affects Host Comparison report only. If the percentage of identical values for a given host is above this threshold, the non-identical values will be colored in red in the excel report

Category	Property	Description
Housekeeping	Enable Database Exporter	Default value is No. Set this property to Yes to enable an alternative way of exporting database as part of the support package, which is expected to be significantly more compact.
Housekeeping	Database Exporter - Remove history	Default value is No. This property is effective only if Database Exporter is enabled.
Housekeeping	Database Exporter - Tables to ignore	Default value is “INDIRECT_CONNECTION, REQUEST, RESPONSE”. Do not change this property without consulting support.

Data collection enhancements

The following enhancements are included:

ID	Description
P-8606	Collect vCenter Server Settings
P-8607	Collect ESXi / Volume SchedNumReqOutstanding + IOPS options
G-1954	Collect VMware Tools (tools.conf) file
P-8574	Support for VMware SRM - vSphere Replication RPO
N-2046	VMware APD / PDL options in ESX 6+
N-1951	vCenter response loading performance optimization
P-8577	Brocade scan with fewer permissions
P-8561	Minimize the number of requests to PowerBroker
P-8546, N-2070	Responses should be disqualified upon PowerBroker failure
A-1204	Supporting 4096 bit keys for public ssh authentication
N-1893	Additional collection for MS SQL Always On

Risk detection enhancements

The following risk detection enhancements are included:

ID	Description
N-1866	Generalize existing UCS Blade Servers risk signatures to cover also HP Blade System Servers
N-1971	Generalize existing VMware risk signature with vSphere versions 6.5 and 6.7
G-2137, N-2042, N-1534	Enable excluding ESX hosts under maintenance from data analysis and indicate hosts under maintenance in tickets if not excluded
G-2184	Use Regex to filter Resources Attributes in specific VCS gap signatures

Application enhancements

The following application enhancements are included:

ID	Description
N-1974	Improve Host Comparison Differences Excel Report
N-1909, A-1152	Added filtering capabilities for table views across UI
N-2092	Enable WS API authentication with LDAP
A-1274	Add WS API functions for hosts and tickets retrieval
A-1248	Ability to create & save custom ticket filter
A-1	Additional options for ticket filters
A-155	Add notes to databases and storage arrays
N-1896	Database Views ERD (Entity-Relation Diagram)
N-1992	Database Views Expansion Packages
A-1231	Expansion Packages – Reporting – Add ability to link queries
N-2002	Expansion Packages – Gap Analysis – Debug Capabilities
A-1235	Expansion Packages – Ability to deactivate configuration items
N-2020	Expansion Packages Export – add Select All option
N-2006	Expansion Packages – Add ability to clone packages and gap signatures
N-2017	Gap Analysis Expansion Package – Data Collection Signature – ability to add more than one source
N-1898	Database Views – Add system property: List of views/tables to avoid from creating
N-1895	Database Views for Standby Pairs
N-2044	Custom Reports – Add SUM and AVG options for specific columns in table
A-1207	Custom Reports: add verbose design capabilities

ID	Description
N-2045	Database Views – Add “IS_IN_SCOPE” column
N-2047	Database Views – additional fields needed
A-1241	Add Clone option to Report scheduling
N-2000	Custom Reports – Support Charts
N-1549	New scan issues for property values
N-2108	Comparison – add BE column to clusters/hosts selectors
A-224	Comparison – add Notes columns to hosts selector
A-1224	Encrypt the connection between the master and collectors
A-1221	VMware SRM - vSphere Replication - Data Protection Status report and SLA improvements
N-2086	Add ability to view business entity topology
A-1205	Rules for automatic association - by naming conventions
A-237	Show application time and timezone in the Info dialog
A-1288	Enhanced Cross Site Scripting (XSS) protection

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.

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. 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
A-1246	SymmetrixSVCorrection enrichment fails
P-8537	3PAR PV to SV: fail to connect rootvg not managed by multipath software to SVs
N-1349	"No possible replica pair for SRDF" log message
P-8587	Duplicate DNS name servers collected for ESXi hosts, incorrect DNS reports
N-2110	linux_nicport.sh script issues
P-8572	Incorrect / misleading scan issue reported for hosts ("not scanned")
N-1965	Missing PV to SV connection between Linux hosts to Infinidat storage
N-2110	Linux nicport collection script issues

Data Analysis issues

The following issues are resolved:

ID	Description
G-1954	Gap 00443APPQSC – use additional source of information
G-2203	Gap 00430VMWCOI – adjust severity and category
G-2142	Gaps 00459NRR and 00471PGSAA are merged, logic enhanced
N-1910	Wrong lag calculation for MS SQL Server Always On
G-2192	02402SRMOD – non-impact ticket
G-2037, G-2031	Gap 00430VMWCOI – non-impact tickets
G-2151	Gap 00580CHBAC – non-impact ticket
G-2138	Gap 00471PGSAA – ticket contains incorrect information

ID	Description
N-2122, G-2143	Gap 00471PGSAA – ticket topology issues
G-2204	Gap 00322SANMIC – logic enhanced
N-1460	Gap 00234UMGVIS – non-impact ticket
P-8458	Gap 00350VRTSUDIDMIS – non-impact ticket
G-1962	Gap 00442OHV – adjust severity and category
P-8582	Gap 01025MSCS failure
A-8562	Gap 00529VCSVGLV – non-impact ticket
G-2196	Gap 00243SBMPNE – logic enhanced
A-965	Gap 00420NAHCWVM – non-impact ticket
G-2219	Gap 00500VCSOFFDIRMISS – non-impact ticket
G-2134	Gap 00305AVLRELLUNINC – non-impact ticket
G-2199	Gap 00443APPQSC – adjust severity and category
G-2210	Gap 00360NFSIA – non-impact ticket
G-2141	Gap 00243SBMPNE – non-impact ticket
G-2195	Gap 00558VCSHB – non-impactful ticket
G-2214	Gap 00556VCSGCOCS – non-impactful ticket

Application and user interface issues

The following issues are resolved:

ID	Description
A-1245	Tomcat configuration should be set to use the default jvm.dll
A-289	Misleading label in Standby Definition screen
N-2100	Velocity.log size is uncontrolled
A-1249	Host Comparison: non-impact differences reported in Windows Registry
A-1251	Error “page 400” in dashboard
A-1134	Ticket details report: heading style is lost after first table when exported to RTF
P-8584	Step 2 – Storage Discovery cannot display the arrays on “View All Storage Arrays”
N-1981	SAPI Database Views – remote database – cannot create procedures
N-2004	Custom Reports – File name is “Custom Report” instead of the report name itself
A-1021	UI takes too long to load – comparison default worksheet

ID	Description
A-1203	User Scope limited Top Level Business Entities and doesn't bring the nested BEs
G-2187	Host comparison: differences should not be reported for parameters that contain host name and/or unique identifiers
A-1202	Custom report scheduling: No prompt when report is deleted + wrong report used in the scheduling
N-1994	Topology: connections and labels visualization issues
A-1166	UI – Step 4 takes too long to load and sometimes hangs
N-1890	Issues with automatic onboarding and removal of hosts using CLI
A-1206	Cannot edit text in custom reports
G-2190	Host Comparison: non-impact differences reported
A-1038	SAPI_TICKETS,FIRST_DETECTION_DATE represents the LAST detection date
A-1272	Security issue – password appear in clear text in agent logs
A-1223	Cannot see NetApp / NFS / CIFS replication in the Data Protection Status report
A-1287	Setting a note for multiple hosts does not update the UI properly
A-1227	Host search in Topology module should be case insensitive

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.	-

ID	Description	Workaround
[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.	-
[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.	-

ID	Description	Workaround
[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.	-

ID	Description	Workaround
[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.	-
[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.

ID	Description	Workaround
[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.

ID	Description	Workaround
[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.
[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.

ID	Description	Workaround
[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	
[P-8438]	Exception on vCenter scanning within Full Cycle when parallel scan of vCenters is enabled	
[P-8389]	VG not connected to PV on HPUX 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.

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 7.3.1 only from version 7.3. If a system has an earlier version of the product installed, you must upgrade to version 7.3 before upgrading to version 7.3.1.

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.

To upgrade from version 7.3 to version 7.3.1

1. Login as a local administrator to the master VRA server.
2. Run the `VRA_7_3_1.exe` file as an administrator.
3. On the Welcome screen, click **Next**.
4. When prompted, select **Yes, upgrade VRA 7.3 to 7.3.1**.
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 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.