Symantec™ Disaster Recovery Advisor Release Notes

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

6.3.2

Symantec

Symantec Disaster Recovery Advisor Release Notes

Product version: 6.3.2

Document version: 6.3.2 Rev 1

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

http://www.symantec.com/business/support/index.jsp

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

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

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

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level

- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support web page at the following URL:

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

Customer service

Customer service information is available at the following URL:

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

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

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

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

Documentation

Product guides are available on the media in PDF format. Make sure that you are

using the current version of the documentation. The document version appears on page 2 of each guide. The latest product documentation is available on the Symantec website.

https://sort.symantec.com/documents

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

Contents

Symantec Disaster Recovery Advisor Release Notes

Introduction

This document provides important information about Symantec Disaster Recovery Advisor (DRA).

Before you install DRA, review this entire document and read the Late Breaking News TechNote for the latest information on updates, patches, and software issues for this release:

www.symantec.com/docs/TECH68401

DRA features

DRA is a data protection risk assessment solution that lets you diagnose high availability (HA) and disaster recovery (DR) problems (also called gaps) and

optimize data protection. DRA enables enterprises to effectively manage business continuity implementations, to ensure that their critical business data is protected. DRA automatically detects and alerts you to any potential gaps, best practice violations, or service level agreement (SLA) breaches.

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

DRA gathers information about your environment and does the following:

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

DRA uses this information to provide the following:

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

System requirements and software limitations

Upgrading the DRA database to Oracle 11g is mandatory.

For more information about system requirements and software limitations, see *Symantec Disaster Recovery Advisor Support Requirements*.

New features

This DRA release introduces new features in the following categories:

Application

- Gap Tuning– In addition to the previous capability to suppress a gap type (risk signature) entirely, new options have been added to allow users to suppress a gap type for a specific scope of entities, define gap type suppression expiration date and document the suppression reason. The **Suppress Gap** button in the **Tickets** tab has been renamed to **Gap Tuning**. To learn more about **Gap Tuning**, review the User Guide.
- Advanced Configuration - Database Views – A new screen has been added in order to allow users to control advanced settings of the DRA Database Views (formerly System API)

Scan Configuration

- The ability to selectively scan Hitachi storage arrays has been added. After configuring a HiCommand Storage Proxy and performing Storage Array Discovery, users may click Edit Storage Scope to select which of the arrays managed by the HiCommand will be scanned. The default setting is “All storage arrays”.

Integration and Reporting

- System API (SAPI) has been renamed to **DRA Database Views**.
- In addition to the previous capability of automatic creation and management of the Oracle schema for the **Database Views** by DRA, a new method has been added to allow users to manually configure fixed Oracle schema's. To learn more details about the methods available for creating the **Database Views**, review the **User Guide** and the **Advanced Configuration - Database Views** screen.
- Users may control whether the creation of Database Views is performed as part of the data analysis and define a timeout for the views creation process.

Gaps

- New gap signatures

New privileged commands

For UNIX hosts and storage proxies scanned with non-privileged credentials, the following new privileged commands are required:

Table 3-1 New privileged commands

Command	Mandatory?	Requires 'sudo' or equivalent?	Required for scanning
/usr/symcli/bin/symaccess list	Yes	Yes	EMC VMAX
/usr/sbin/vradmin printvol	Yes	Yes	Symantec VVR
/usr/sbin/vradmin printrvg	Yes	Yes	Symantec VVR

For scanning NetApp Filers and NetApp DFM, the following new capabilities (rights) must be granted to the user account:

Table 3-2 New capabilities

Capability	Mandatory?	Required for scanning
api-cifs-share-list-iter-end	Yes	NetApp Filers / DFM
api-snapvault-primary-relationship-status-list-iter-end	Yes	NetApp Filers / DFM

For more information, refer to *DRA 6.3.2 Deployment Guide*.

Additional changes and enhancements

Scan Troubleshooting improvements

The Scan Troubleshooting report can now be exported to an Excel file, in addition to the PDF/Word options. In addition, the scan error messages for SYMCLI command errors have been improved.

Business Continuity Risks report improvements

An option has been added to show a more detailed version of the report.

RPO calculation enhancement for EMC SRDF

Data age (RPO) is calculated for EMC SRDF replicas in the Suspended state.

System events for the creation of DRA Database Views (formerly System API)

New events are logged in the system event log to reflect the start and end times of the DRA Database Views creation.

Important change to Virtual Machine removal process

In past releases, a Virtual Machine discovered through vCenter is automatically removed from the DRA system in certain circumstances such as when permissions to access the vCenter components were changed or when the VM moved to a new vCenter system (regardless of whether the VM is included in a scan group or not). To avoid scenarios when Virtual Machines are deleted and omitted without notice from the scan and analysis, this behavior has changed in V6.3.2. Virtual Machines included in scan groups are not removed unless the user selects to remove them through the **View Hosts** screen in the **Configuration** tab.

Added an option to skip the DRA database export step of the Installation/Upgrade

When installing or upgrading in Production environment, it is advised not to skip this phase.

A number of security enhancements

Various system aspects were enhanced to provide improved protection against attacks.

Support for EMC CLARiiON / VNX storage pools

DRA collects the storage pool information, RAID type and LUN association.

Update to the hardware requirements for a DRA collector server

The minimal memory size supported for a Collector server is now 8GB.

Added an option to manually define WebSphere home directory

An option has been added to manually configure the path to the home directory of WebSphere Application Servers. In the **Configuration** tab, navigate to the **Scan Troubleshooting** screen and to the **Installed Applications** tab, select the relevant host, select the WebSphere application at the bottom A**pplication Path and Binary Files Used for scanning** pane and click **Edit Paths** to change the directory.

Better distinction between suppressed open and suppressed closed tickets

The existing status icon for suppressed tickets has been replaced by two new icons, to better distinguish between open and closed suppressed tickets:

'Suppressed open' tickets are represented by the icon

'Suppressed closed' tickets are represented by the icon

A tooltip appears when hovering over the new icons with a text representing their meaning

It is now also possible to search tickets more granularly using the two new status types

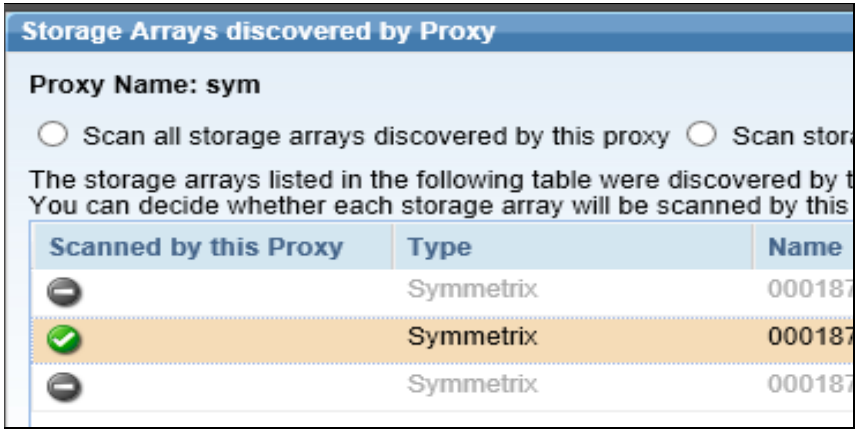
- 'Suppressed open' tickets are represented by the  icon
- 'Suppressed closed' tickets are represented by the  icon
- A tooltip appears when hovering over the new icons with a text representing their meaning
- It is now also possible to search tickets more granularly using the two new status types

Comparison module enhancements

In previous versions, when comparing a specific host group, the user had the ability to choose which categories to use for comparison (for example, “hardware”, “software”, “operating system”, and so on). There was no way perform similar choice when using the “Compare all Groups in Worksheet” () button. This behavior is now changed, and once “Compare all Groups in Worksheet” is clicked, a set of check boxes appear (with all options checked by default) to allow more control over comparison.

Improved icons in the “edit proxy scope” page

When editing a proxy scope (in step 2 of the configuration wizard), the column “Scanned by this proxy” in the array table now better reflects whether each arrays is enabled for scanning ( )or disabled ( ), as illustrated in the figure below:



Fixed issues

This DRA release fixes the following issues:

The Web UI might unexpectedly return an HTTP Error 400

While working with the web UI, the user might unexpectedly get an HTTP Error 400. [7132]

Active Directory integration may fail when LDAPS is used

When LDAP SSL is used, integration with Active Directory for user management may fail. [7673]

OEM scan may fail when the connection string used is long

When the connection string to the OEM is longer than 128 characters, connection to OEM is unsuccessful. [7649]

In certain circumstances, scan requests suffer from delayed execution

When a large number of systems are manually selected in step 4 of the Configuration Wizard and scan is initiated, occasionally the scan would only start after a certain period of time. [7373]

Certain VVR read-only commands fail with a Permission Denied error

The commands have been added to the Privileged Commands requirements. For additional details, refer to the “New Privileged Commands” section and the *Deployment Guide*. [7371]

EMC storage masking data collection error

Collection of storage masking configuration does not work for EMC VMAX and/or remote arrays. [7359]

In certain circumstances, the refresh of DRA Database Views hangs

The refresh of the DRA Database Views hangs in a specific case. [7319]

The Virtual Machines pie chart is missing in the Last Cycle Scan Coverage Dashboard section

In certain configurations, the dashboard includes a Last Cycle Scan Coverage section. The section was missing a pie chart for Virtual Machines. [7310]

Occasionally incorrect state reported for AIX lpars

Occasionally DRA reports the down state for AIX lpars that are online. [7304]

Gap 00430VMWCOI does not perform case insensitive analysis for certain parameters

As a result, non-impactful inconsistencies are reported. [7302].

Scan troubleshooting message reported for HITACHI directly attached drives

An incorrect scan error message reported for servers using certain model of HITACHI DAS drives regarding inability to detect the SAN storage volume. [7294].

In specific circumstances, vCenter data is not analyzed correctly

As a result, DRA may show incorrect connections between datastores and storage devices. [7291].

Remote Symmetrix arrays are presented as local

In the Edit Storage Proxy screen, remote Symmetrix arrays are presented as local in specific circumstances. [7287].

Physical volumes data collection issue for AIX lpar in a VIO environment

In specific circumstances, certain physical volume information is omitted for AIX lpars in a VIO environment. [7282].

Active Directory configuration - failure to add a large number of Host URLs

When the length of the host URLs exceeds 256 chars, an error message is presented when attempting to save [7282].

Occasionally incorrect state reported for Oracle RAC resource

In specific cases, a RAC resource may be incorrectly reported with an offline state instead of online state. [7274]

Scan error messages for removed databases

When scanning OEM, Scan Troubleshooting report may include messages for databases removed from scope. [7270].

Multiple labels in the topology

Occasionally connections in the topology may have duplicate labels. [7257].

Comparison tab reports incorrect differences

In certain rare circumstances, identical values for kernel parameters may be reported as different. [6816].

Gap 00243SBRV does not present RDM devices

The ticket generated by Gap 00243SBRV does not present RDM devices in the description. [6726].

Non default application server installation directories are not discovered automatically

DRA searched for application servers (WebLogic and WebSphere) only in the default installation directories. Path discovery from installed packages and running processes is not used.

Ticket editing may fail and generate an internal error message

Editing a ticket (rating, suppressing or adding a note) may fail with a "snapshot too old" error.

The impact for the MultiplePseudoPVs gap is unavailable

There is an error when viewing the impact of the MultiplePseudoPVs ticket. The impact text is unavailable.

Oracle RAC state incorrect ticket

A false positive ticket might open regarding a bad Oracle RAC state when one of the RAC commands fails.

Incorrect description for the RAC resource state gap

The description of the Oracle RAC resource state gap may contain irrelevant data about other RAC clusters.

Inactive processors on AIX are not ignored

Defined processors on AIX are not filtered out and considered as active.

Incorrect comparison between EMC INQ and Syminq outputs

In some scenarios, the comparison between EMC INQ and Syminq outputs is incorrect because one of the commands returns only the pseudo PVs and the other returns all the paths.

Local FileSystem inconsistency gap might generate a wrong ticket if the FileSystem if not mounted

A false positive ticket might open regarding inconsistency in local FileSystem size between cluster nodes. This happens when the FileSystem is not mounted on one node and its size is considered 0. [7346]

PowerHA cluster state gap might open in inaccurate ticket

An inaccurate ticket about a bad PowerHA cluster state might open even though the cluster is functioning correctly.

Incorrect CyberArk domain user identification

A CyberArk user is considered a domain user only if the policyId attribute starts with “windomain”. The “windowsdomain” prefix is not checked.

Known issues

This DRA release has the following known issues. They should be fixed in future releases.

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

Ticketing and reporting issues

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

When rollback segments and data files are separated, DRA may generate false tickets about database files stored on a mixture of RAID types. [3314]

Workaround: Suppress the tickets.

False tickets for an EMC Symmetrix device

DRA may generate false tickets about EMC Symmetrix device ID 000. [4439]

Workaround: Suppress the tickets.

False tickets may be generated after an Oracle RAC failover

When an oracle RAC failover occurs, DRA may generate false tickets about image storage replication errors. [6175]

Workaround: Suppress the tickets.

False tickets may be generated if collectors' times are not synced

When cluster nodes are scanned using different collectors, DRA may generate false tickets if the collectors' times are not synced. [5975]

Workaround: Suppress the tickets.

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

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

Non-impactful tickets regarding SCSI3 inconsistency are occasionally opened.

DRA may open a ticket regarding SCSI3 setting inconsistency at the array level without taking the host HBA settings into account. [7624]

Workaround: Suppress the tickets or the gap type.

When comparing Hardware, Comparison tab may not show all the cluster nodes

Occasionally when comparing Hardware configuration between servers using the Comparison tab, not all servers are presented, [7611]

Host HBA Comparison report is occasionally not readable in a standard PDF/RTF report size.

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. [7360]

Workaround: Export the report to excel.

False tickets regarding missing mount point directories

In specific cases, false tickets of Gap 00518VCSORARES may be reported due to permission issues. [7349]

Workaround: contact Support for assistance.

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

When ASM mirroring is used and each mirror resides on a different array, an incorrect ticket regarding mixed storage may be opened. [7607]

Workaround: Suppress the tickets.

False tickets of Gap 01003WSMANR - Windows Services not running

When configured with 'Automatic Trigger Start', DRA may still report these services as such that should be running. [7333]

Workaround: Suppress the tickets or the Gap type.

Duplicate gap suppression messages in the Ticket History tab

After suppressing a gap and performing multiple ticket searches, the history tab of a ticket of the suppressed gap may show multiple suppression records. [7344]

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

Incorrect tickets may be reported for Microsoft Cluster when resource names end with white space. [6724]

Workaround: Suppress the ticket.

Incorrect ticket regarding the MSCS cluster group when SRDF/CE is used

DRA may open a false ticket regarding EMC resources in the cluster group when SRDF/CE is used. [5919]

Workaround: suppress the ticket.

Incorrect ticket regarding mount resources in Solaris Zone environment

Gap 00500VCSONNOMOUNT may generate false tickets regarding the path of mount resources. [G378]

Workaround: Suppress the ticket.

False ticket regarding masking configuration inconsistency

Gap 00322SANMIC may generate incorrect ticket when the host name is defined using capital letter on the storage and using lower case letters on the host (or vice versa). [G364]

Workaround: Suppress the ticket.

NFS share is mistakenly recognized as CIFS share

Gap 00360NFSIA may generate tickets that incorrectly classify NFS as CIFS. [G360]

Simple recovery mode tickets are opened for Snapshot databases

Gap 01074MSSQLRMS generates a non-impactful ticket regarding Simple Recovery mode for snapshot databases. [G351]

Workaround: Suppress the tickets.

Incorrect ticket regarding shred storage not collected to cluster nodes

In rare cases Gap 00571GCSGNM may generate incorrect tickets regarding cluster node not connected to the shared storage devices. [G340]

Workaround: Suppress the tickets.

False ticket regarding insufficient number of Netapp hot spares

Gap 00251HSNA may open incorrect tickets regarding insufficient number of spares. [G333]

Workaround: Suppress the tickets.

Invalid ticket for missing file systems on a standby host

Gap 00243SBMPNE may generate tickets which reference invalid / non-existent file systems. [G335]

Workaround: Suppress the tickets.

Cycle issues

In specific scenarios, when a replication source becomes the target and the target becomes the source, DRA 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 was changed to be the source. [6484]

Topology view issues

The Topology search for relationships may take too long to complete

The search for relationships which contain many records may take several minutes to complete. [2757]

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

Service Level Agreement (SLA) issues

In certain circumstances, the SLA module is only partially updated

Adding a business entity partially updates the SLA module. [4172]

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

Configuration issues

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

JavaScript errors may pop up when setting an SLA in the Edit Business Entity wizard using Internet Explorer 6. [5654]

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

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

Some user interface functions might not work correctly using Internet Explorer 10 Internet Explorer 11. [6563]

Workaround: Use Internet Explorer 10/11 Compatibility View.

Errors presented regarding Active Directory connection are not informative

In some cases, a detailed error message regarding the AD connection error is not presented. [7651]

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

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

In specific screens of the Configuration tab, user selection of records gets unselected after a short period of time (refresh interval). [7617]

The collector configuration file is not updated

When updating the DRA server configuration file, the change might not populate to all the collectors. [6650]

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

Manually adding Host URLs reduces the size of the list box

When adding Host URL in the Active Directory Configuration screen, the size of the list box is decreased with each host URL added [7281]

Deleted AD domains may still appear in the Add User dialogue

Deleted Domains will be presented in the domain field of the Add User dialogue. [7673]

Users may manage scheduled reporting tasks created by other users

Users may see and edit scheduled reports tasks that were created by other users, potentially for entities external to their own user scope. [7030]

Scanning issues

When DRA scans a suspended DB2 database, queries may fail

If DRA scans a database when the database is suspended, most queries may fail. [4439]

DB2 discovery fails on a host scanned using a proxy

DRA cannot discover DB2 on a UNIX host that is scanned through a proxy. [5201]

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

DRA may identify unsupported devices incorrectly

DRA shows unsupported storage array devices as direct-attached storage (DAS) devices, which may open false tickets. [4310]

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

While a scan operation is running, users are not blocked from certain operations

While a scan operation (connectivity verification, discovery, or scan) is running, a user can edit or delete a host or database. [4312]

Workaround: While you run a scan, do not delete or edit the host or database.

Only active network interface cards (NICs) are collected on Solaris

DRA does not collect NICs which are unplumbed. [6100]

IBM DS GlobalMirror replication might not be presented correctly

DRA may fail to present IBM DS GlobalMirror replication. [6652]

Workaround: Contact Support for assistance.

IBM DS/XIV LUN discovery might be incorrect for UNIX hosts

DRA may fail to discover the correct LUN for UNIX hosts accessing IBM DS or XIV storage. [6651]

Workaround: Contact Support for assistance.

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

When executing a scan of a vCenter with no hosts, the scan fails. [7659]

Server incorrectly classified as partially scanned

In rare circumstances, an incorrect scan error is reported regarding a "/dev/unknown" PV that leads to a partial scan status. [7610]

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

Successfully scanned SVC Storage proxy does not appear on the Dashboard

SVC storage proxies are missing from the dashboard and scan status report [7367]

Incorrect collection of XIV cluster name

When the cluster name includes multiple words separated by white space, only the first word is collected. [7339]

Occasionally a non-impactful scan error message are presented

A scan error with the 'No MPIO disks are present' message is occasionally opened for Windows servers. [7307]

A scan error for the sympd command with "return code: 1" message is opened when sympd finds no devices. [7285]

Scan errors for EMC VNX clone/mirror command may appear when these features are disabled. [7240]

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

Inactive disk groups and logical volumes are not always collected.

Information regarding inactive disk groups and unmounted logical volumes is not always collected. [7250, 7041]

Scan of IBM UDB V10.x may fail

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

HBA driver info is not always available for Linux systems

In rare cases, HBA model, driver and firmware info is not available for Linux systems [7196]

Unclear scan status for certain storage proxies

When an EMC Symmetrix array is inaccessible, the error reported is “Could not establish connection to proxy”. [7091]

When SVC discovery command fails, an incorrect message may be listed regarding the connection/credentials. [6767]

When adding an additional XIV array in Step 2 and its verification fails - it marks the Connectivity Status for all the array as failed. [6912]

HMC scan may fail in an IBM FLEX environment

When HMC is scanned in an IBM Flex environment, the scan may fail. [7667]

Workaround: Contact support for assistance.

If the security level on the Naviseccli server is set to MEDIUM, EMC VNX scan hangs. [6964]

Workaround: Reduce the security level to allow scanning

When the password contains special chars, EMC VNX arrays scan fails [6962]

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

Discovery may report UDB instances as down

In rare cases, DRA may report online UDB instances as down [6949]

Workaround: Contact Support for assistance.

Free space information is not available for Windows 2003 Servers

Free space information is not available for Logical volumes on Windows 2003 Servers. [6053]

Scan status report does not include Management Consoles

The Scan Status report does not include information regarding scan of management consoles. [7678]

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

Important Notes

- To avoid false positive tickets about storage access or storage area network (SAN) I/O configuration inconsistency that involves backup servers, configure the backup servers inside a business entity and assign the 'Backup' role.

Limitations

Assigning a profile to an Active Directory group

- When assigning a profile to an AD Universal Group, the DRA master server must have access to the Global Catalog of the AD Forest
- When assigning a profile to an AD Local Domain Group, DRA 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 DRA (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)

DRA also has the following RPO/SLA limitations:

RPO/SLA is not supported in HDS

RPO/SLA for NetAPP only works for direct replication from primary devices

RPO/SLA for CLARiiON only works for direct replication from primary devices

RPO/SLA is not calculated for EMC CLARiiON MirrorView/S

RPO/SLA is not calculated for IBM DS

No topology images in Ticket Details report

Ticket Details report might be generated without topology images if many tickets are included. [3690]

Workaround: Run the report on selective tickets or increase the "Ticket details report topology number of tickets limitation" system property.

Running the DRA database on Oracle RAC is not supported

Configuring DRA to use an Oracle RAC as its database is not supported.

Workaround: If only Oracle RAC is available, use a specific RAC node as the database server.

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

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

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

DRA Database Views do not include information regarding VMware Virtual Networking, Database Tablespaces, Installed Software and Kernel Parameters, RecoverPoint consistency groups, LV mirroring 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, DRA may open incorrect tickets as a result.

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

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

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

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

When importing objects into DRA, special characters are converted

When importing names and properties of objects from CSV/CMDB/API, special characters such as "&" are converted to alphanumeric chars. [7345]

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

In certain cases, DRA may report differences relating to options that are dynamically changing or depending on the location and thus non-impactful. [7305, 7301, 7219]

Workaround: Suppress these differences.

SSH key supports only keys with less than 4000 characters [6645]

When NTLMv2 is used, authentication may fail

Scanning systems in an environment where only NTLMv2 is allowed may fail without additional configuration. [7206]

Workaround: Contact support for assistance.

DRA may fail without notice when no space left on its disk drives

When nearly no space is left on the disk drives storing the DRA software, the system may fail without a notice. [6884]

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

HMC is required in order to scan IBM VIO environments.

If HMC is not available and IVM is used, contact Support for assistance. [6835]

Installation Notes for This Release

Read the Installation Procedure chapter of the User Guide for guidance about installing DRA V6.3.2. In addition, review the Deployment Guide for guidance about the DRA infrastructure requirements and the preparations needed for scanning your data centers.

Upgrade for This Release

An upgrade path to version 6.3.2 is available from the 6.3.1 release. If your system is currently installed with an earlier release, an upgrade to version 6.3.1 is mandatory before upgrading to version 6.3.2.

Important Notes:

- Prior to upgrading, take care to read the release notes in full, and make any necessary changes to the DRA infrastructure and/or to user account permissions as required, and ensure sufficient free disk space is available on the master server.
- Prior to upgrading, verify you have an up-to-date backup of the DRA server disk drives using your standard backup tools, and an up-to-date DRA database export. A database export can be generated using the EXPDP or EXP Oracle command.
- Once the upgrade on the master DRA server is completed and the Tomcat service starts, DRA will automatically check and upgrade the DRA 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 will require the complete stop of DRA operations, including data collections and data analysis. While it is a fully automatic process, the length of the upgrade process may require several hours to complete in large environments. During this time it is important not to restart the DRA server or terminate the upgrade task. In addition, it is essential that the Oracle database used by DRA will be available throughout the upgrade process.

To upgrade from version 6.3.1.X to version 6.3.2:

1. Login as a local administrator to the master DRA Server.
2. Run the **DRA_6_3_2.exe** as an administrator.
3. Click **Next** in the Welcome screen.
4. Select **"Yes, upgrade DRA 6.3.1.X to 6.3.2.0"**.

5 Accept the License Agreement and click **Next**.

6 Accept the GNU License Agreement and click **Next**.

7 Select whether to perform a database export prior to upgrading and whether to start Tomcat 7 after the upgrade completes, and click **Next**. It is recommended to keep the default settings.

8 Click **Install** to begin the Software Upgrade process.

9 Click **Finish**.

Getting help

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

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

Customer service information is available here:

www.symantec.com/support/assistance_care.jsp

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