Symantec™ Disaster Recovery Advisor Release Notes

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

6.4

Symantec

Symantec Disaster Recovery Advisor Release Notes

Product version: 6.4

Document version: 6.4 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

Introduction 9
DRA features 9
System requirements and software limitations 10
New features 11
New privileged commands 12
Additional changes and enhancements 12
Fixed issues 12
Known issues 14
Limitations 24
Installation Notes for This Release 27
Upgrade for This Release 27
Getting help 28

Symantec Disaster Recovery Advisor Release Notes

- Introduction
- DRA features
- System requirements and software limitations
- New features
- Fixed issues
- Fixed issues
- Getting help

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

For more information about system requirements and software limitations, refer to the *Symantec Disaster Recovery Advisor Support Requirements* document.

New features

This DRA release introduces new features in the following categories:

New Platform Support

- HP 3PAR StoreServ Storage
- EMC VPLEX (for VMware and EMC CLARiiON/VNX environments)
- IBM V7000 Storage
- Oracle GoldenGate
  For more information on new platform support, refer to the *DRA 6.4 Support Requirements* and DRA 6.4 *Deployment Guide*.

Newly designed Storage Scan Configuration screen

- The Storage Scan Configuration User Interface was redesigned in order to simplify the management of storage array scanning and provide more visibility onto the scan scope and status.
- The new design presents the scanned storage systems in the main view, as opposed to storage proxies in past releases.
  For more information on new Storage Scan Configuration UI, refer to the *DRA 6.4 User Guide*.

Oracle RAC support for the DRA database

- The support has been added for running the Oracle database used by the DRA Software on an Oracle RAC system

Gaps

- New gap signatures

New privileged commands

No new privileged commands are required for host scanning as part of this new release.

Additional changes and enhancements

Following are the additional changes and enhancements done in this release of Symantec Disaster Recovery Advisor.

DRA uses TNSNAMES.ORA for internal database connection

In new installations of DRA, the connection to the internal DRA Oracle database relies on the database TNS entry in the Oracle TNSNAMES.ORA file on the DRA server. The existing installations remain unchanged.

Ability to define exclusion list for comparison of kernel parameters and users

System Properties were added under the “Reports” category to allow user-defined filtration of certain kernel parameters and users from the comparison tab and host configuration differences report, based on regular expressions.

DRA data collection for VMware Virtual Network

The vCenter scan by DRA collects information regarding VMware Virtual networks (virtual switches, port groups and more).

More granular scheduling of reports

The Report Scheduling screen enables scheduling reports in intervals of one minute (as opposed to five in past releases).

Fixed issues

This DRA release fixes the following issues:

Running the DRA database on Oracle RAC is not supported

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

Unclear scan status for certain storage proxies

When an EMC Symmetrix array is inaccessible, the error reported is “Could not establish connection to proxy”. [P7091]

When SVC discovery command fails, an incorrect message may be listed regarding the connection/credentials. [P6767]

When adding an additional XIV array in Step 2 and its verification fails - it marks the Connectivity Status for all the array as failed. [P6912]

Unclear “Connectivity Verified” message when discovering an EMC Symmetrix/VMAX array. [P5646]

The "Verified" status column of a proxy does not differentiate between authentication and connection error. [P5372]

Non-impactful differences may be reported for dynamic, case-insensitive, and site-dependent parameters

In certain cases, DRA may report differences related to options that are dynamically changing or depending on the location and thus non-impactful (DNS.StealthMasters, RecoverPoint.CopyName, RecoverPoint.RPAAddr, RecoverPoint.VCSBookMark, ip_conntrack_count, ESX syslog options, ESX Misc.SIOCControlFlag2). [P7305, P7301, G63, G1223]

Incorrect ticket regarding OS version mismatch is opened

In specific circumstances, Availability may incorrectly report on an OS version mismatch between cluster hosts. [G355]

SVC storage systems missing from the dashboard and scan status report

Successfully scanned IBM SVC systems do not appear in the dashboard and in the scan status report. [P7764]

False ticket regarding insufficient number of Netapp hot spares

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

User Guide does not include information regarding the Software SLA tab

The Software tab of the SLA policy is not documented in the DRA User Guide. [P7719]

The Storage Scan pie chart in the dashboard shows incorrect number of arrays

In certain cases, the storage scan pie chart of the dashboard presents incorrect number of arrays. [P7724]

Error when defining an AD group that has the slash (/) sign in the group name

AD Integration fails when the user defines an AD group that has the slash (/) sign in the group name. [P7750]

Incorrect details in specific sections of the License Usage report

In certain cases, the “Virtual Infrastructure” section of the License Usage report presents incorrect information. [P7752]

Incorrect details in specific sections of the Scan Status report

In certain cases, the storage systems and database sections of the Scan Status report presents incorrect information. [P7765]

WebLogic data collection may fail in certain conditions

The data collection of WebLogic configuration may fail in specific cases such as when registry file is the only discovery source (and not domain registry) or when there is a large number of application files to verify. [P7757]

Occasionally a non-impactful scan error message are presented

A scan error for the sympd command with "return code: 1" message is opened when sympd finds no devices. [P7285]

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 [P3314]

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

Workaround: Suppress the tickets.

False tickets for an EMC Symmetrix device [P4439]

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

Workaround: Suppress the tickets.

False tickets may be generated after an Oracle RAC failover [P6175]

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

Workaround: Suppress the tickets.

False tickets may be generated if collectors' times are not synchronized [P5975]

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

Workaround: Suppress the tickets.

The dependency between Path (PV) to HBA is not always available [P7638, P7612]

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

When comparing Hardware, Comparison tab may not show all the cluster nodes [P7611]

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

Host HBA Comparison report is occasionally not readable in a standard PDF/RTF report size [A14]

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.

Workaround: Export the report to excel.

False tickets regarding missing mount point directories [P7349]

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

Workaround: Contact Support for assistance.

Non-impactful ticket regarding mixed storage may be opened when ASM mirroring is used [P7607]

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

Workaround: Suppress the tickets.

False tickets of Gap 01003WSMANR - Windows Services not running [P7333]

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

Workaround: Suppress the tickets or the Gap type.

Duplicate gap suppression messages in the Ticket History tab [A19]

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

Incorrect tickets are opened for MSCS when resource names end with white space [P6724]

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

Workaround: Suppress the ticket.

Incorrect ticket regarding the MSCS cluster group when SRDF/CE is used [P5919]

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

Workaround: suppress the ticket.

Incorrect ticket regarding mount resources in Solaris Zone environment [G378]

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

Workaround: Suppress the ticket.

False ticket regarding masking configuration inconsistency [G364]

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).

Workaround: Suppress the ticket.

NFS share is mistakenly recognized as CIFS share [G360]

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

Simple recovery mode tickets are opened for Snapshot databases [G351]

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

Workaround: Suppress the tickets.

Incorrect ticket regarding shred storage not collected to cluster nodes [G340]

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

Workaround: Suppress the tickets.

Invalid ticket for missing file systems on a standby host [G335]

Gap 00243SBMPNE may generate tickets which reference invalid / non-existent filesystems.

Workaround: Suppress the tickets.

Incorrect ticket regarding EMC CLARiiON/VNX - number of hot spares [G1011]

In certain conditions, DRA may report incorrect tickets regarding suboptimal number of hot spares for EMC CLARiiON or VNX array.

Workaround: Suppress the tickets.

Incorrect ticket regarding missing VCS LV resources [G1173, G1185]

In specific circumstances, DRA may incorrectly open tickets regarding missing VCS LV resources.

Workaround: Suppress the tickets.

Incorrect ticket regarding suboptimal SAN I/O policy [G1177]

DRA may incorrectly open suboptimal SAN I/O policy when the selected policy is PRNX_PSP_RR.

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 [P6484]

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.

Topology view issues

The Topology search for relationships may take too long to complete [P2757]

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

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 [P4172]

Adding a business entity partially updates the SLA module.

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

Configuration issues

Setting an SLA in the Edit Business Entity wizard might fail in the Internet Explorer (IE) 6 [P5654]

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

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 [A254]

Some user interface functions might not work correctly using Internet Explorer 10 or Internet Explorer 11.

Workaround: Use Internet Explorer 10/11 Compatibility View.

Errors presented regarding Active Directory connection are not informative [A69]

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

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

Configuration tab - user selection is dismissed due to table data refresh [A247]

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

The collector configuration file is not updated [A11]

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

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

Manually adding Host URLs reduces the size of the list box [A10]

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

Deleted AD domains may still appear in the Add User dialogue [A21]

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

Users may manage scheduled reporting tasks created by other users [A55]

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

Scanning issues

When DRA scans a suspended DB2 database, queries may fail [P4438]

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

DB2 discovery fails on a host scanned using a proxy [5049]

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

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

DRA may identify unsupported devices incorrectly [P4310]

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

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 [P4312]

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

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 [P5934]

DRA does not collect NICs which are unplumbed.

IBM DS GlobalMirror replication might not be presented correctly [P6481]

DRA may fail to present IBM DS GlobalMirror replication.

Workaround: Contact Support for assistance.

IBM DS/XIV LUN discovery might be incorrect for Solaris/HPUX hosts [P6480]

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

Workaround: Contact Support for assistance.

Failure when scanning a vCenter with no managed ESX/ESXi hosts [P7659]

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

Server incorrectly classified as partially scanned [P7610]

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

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

Incorrect collection of XIV cluster name [P7339]

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

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. [P7307]

Scan errors for EMC VNX clone/mirror command may appear when these features are disabled. [P7240]

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

Inactive disk groups and logical volumes are not always collected [P7250, P7041]

Information regarding inactive disk groups and unmounted logical volumes is not always collected.

Scan of IBM UDB V10.x may fail [P7207]

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

HBA driver info is not always available for Linux systems [P7196]

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

HMC scan may fail in an IBM FLEX environment [P7667]

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

Workaround: Contact support for assistance.

If the security level on the Naviseccli server is set to MEDIUM, EMC VNX scan hangs. [P6964]

Workaround: Reduce the security level to allow scanning.

When the password contains special chars, EMC VNX arrays scan fails [P6962]

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

Discovery may report UDB instances as down [P6949]

In rare cases, DRA may report online UDB instances as down.

Workaround: Contact Support for assistance.

Free space information is not available for Windows 2003 Servers [P6053]

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

Scan status report does not include Management Consoles [P7678, A25]

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

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

Nodes with the same cluster name and ID are incorrectly merged to a single VCS [P7773]

In certain cases when multiple clusters with the same name, DRA may incorrectly merge these clusters to a single VCS.

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 [P3690]

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

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

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, and LV mirroring. Also it does not include the 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 [5455]

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 [A87, A109, A105]

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

Non-impactful differences may be reported for dynamic or site-dependent parameters [P7219]

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

Workaround: Suppress these differences.

SSH key supports only keys with less than 4000 characters [P6645]

When NTLMv2 is used, authentication may fail [P7206]

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

Workaround: Contact support for assistance.

DRA may fail without notice when no space left on its disk drives [A41]

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

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 [P6835]

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

CSV Import of Business Entities does not create new sites [A15]

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.

Workaround: Use step 3 of the Configuration Wizard to define any missing sites (manually or through CSV import).

Installation Notes for This Release

Read the Installation Procedure chapter of the User Guide for guidance about installing DRA V6.4. 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 6.4 is available from the 6.3.2 release. If your system is currently installed with an earlier release, an upgrade to version 6.3.2 is mandatory before upgrading to version 6.4.

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 6.3.2 to version 6.4:

1. Login as a local administrator to the master DRA Server.
2. Run the **DRA_6_4.exe** as an administrator.
3. Click **Next** in the Welcome screen.
4. Select **"Yes, upgrade DRA 6.3.2.X to 6.4.0"**.

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 maintenance 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.
