Symantec™ Disaster Recovery Advisor Release Notes

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

6.3

Symantec

Symantec Disaster Recovery Advisor Release Notes

Product version: 6.3

Document version: 6.3 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

New user role/privilege management, supporting:

- Privileges – The privilege level can now be set for various functions of the product to a great level of granularity.
- Scope – A new concept that replaces and expands on the functionality of Roles in previous releases. This allows defining a collection of Business Entities, Labels and Areas to define a scope for a user profile.
- Role – This defines a collection of privileges.
- Profile – This is a combination of a Role and a Scope that can be assigned to a user, or to an Active Directory Group.
- User Roles defined in previous releases are automatically converted to the new standards.

Improved and simplified Active Directory (AD) integration

- Auto discovery of AD Domains. Manual configuration is also supported.
- Integration with new user role/privilege management.
- If you are already using AD integration configured in an earlier release of DRA - see “Important Notes” below.

Configuration wizard enhancements

- In the SymCLI Probe configuration, in addition to the already supported "Manual" or "All" selection options, users can restrict scanning to Local storage arrays only.
- New columns added to the Host, Storage and Database table views to track scanning errors, time of last scan and time of last successful scan.

Comparison module enhancements

- New default worksheet is now automatically created upon fresh installation or upgrade.
- In additional to the already existing “monitor” option for individual differences, users can now select entire Sections for monitoring.

Software SLA

- A new “Software SLA” tab is added to the SLA Policy.
- User can specify mandatory software products and their minimal version.
- Out-of-the-box support for selection of major backup tools as mandatory software products.

Standby Host configuration improvement

- User can show/hide hosts/clusters that have standbys already defined.

Enhanced scan troubleshooting page

- User can filter by Business Entity
- User can add notes

Framework/backend

- Automatic upgrade of Tomcat and Java to version 7

New platforms support

- EMC Isilon(NAS)
- EMC DataDomain (NAS)

Gaps

- New gap signatures

Fixed issues

This DRA release fixes the following issues:

Users with access to specific Business Entities can run certain reports on the entire environment

Certain reports will run on the entire environment even for users with a limited business entities scope. [4700]

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

DRA may generate false tickets about 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.

DRA may generate false tickets about an EMC Symmetrix device

DRA may generate false tickets about EMC Symmetrix device ID 000. [4440]

Workaround: Suppress the tickets.

After an Oracle failover, DRA may generate false tickets

When an Oracle failover occurs, DRA may generate false tickets about image storage replication errors. [6342]

Workaround: Suppress the tickets.

If the collector's time is not synchronized, DRA may generate false tickets

When cluster nodes are scanned using different collectors, DRA may generate false tickets if the collector's time is not synchronized. [6141]

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. [6655]

Topology view issues

The Topology search for relationships may take too long to complete

When DRA searches for *stored on* between a physical volume and a Symmetrix device, the results may not appear for 15 minutes. [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 Symmetrix 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 a full 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. [5819]

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

Some user interface functions might not work correctly in IE 10

Some user interface functions might not work correctly using Internet Explorer 10. [6735]

Workaround: Use Internet Explorer 10 Compatibility View.

Assigning host to site does not work from the Edit Host page

Assigning or changing the site associated with each host does not work from the edit host page. [7355]

Workaround: Assign sites from the Site Definition page in the configuration wizard.

The Web UI may return an HTTP Error 400 unexpectedly

While working with the web UI, the user may unexpectedly get an HTTP Error 400. [7308]

Workaround: Clear the cookies for the domain in the Internet Explorer and refresh the page.

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: Ignore or remove 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 and 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]

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]

The collector configuration file is not updated

When you update 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.

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 role Backup.
- The upgrade process starts the Tomcat 7 installation wizard. Tomcat 7 should be installed in the same drive letter in which Tomcat 6 is installed.
- You should configure the “Maximum memory pool” in Tomcat 7 -> Configure Tomcat -> Java to be the same as it was in Tomcat 6.
- If Tomcat 6 was configured with HTTPS, you should apply the same configuration for Tomcat 7.
- It is recommended to uninstall Java 6 from the DRA server when the upgrade is finished.
- The upgrade installs Java 7 on the DRA server – but not on already configured Collectors. To upgrade the collectors to Java 7 you need to manually reinstall them. You can download a new Collector after the upgrade is complete, and use the jre-7u45-windows-x64.exe file provided by Symantec in the Collector zip file to install Java.
- Requirements for using the new Active Directory (AD) integration option
  a. If upgrading from a previous release with AD already configured:
     i. DRA now supports only full Domain names (e.g. domain.company.corp). If you are currently using pre-Windows 2000 / short Domain names – make sure you replace them with full ones before the upgrade.
     ii. After the upgrade, all the AD users are unusable until a credential is associated with the currently used Domain. Note that DRA 6.3 now supports using more than one Domain.
  b. If you experience issues in DRA automatic discovery of certain AD Domains, please validate that the following requirements are met:
     i. Each AD Domain name must be included to the “DNS Suffix Search List” on the DRA server (can be validated using “ipconfig /all” from the command line).

ii. The AD Domain name must be DNS-resolvable from the DRA server (can be validated using nslookup [Domain name] from the command line).

c. For each domain configured in the product, an existing Active Directory user credentials should be configured. This user must have sufficient permissions for reading the LDAP tree of the domain

New privileged commands

The scanning in this release requires the following new privileged commands:

Table 3-1 New privileged commands

Command	Mandatory	Requires 'sudo'	Required for
/usr/symcli/bin/symmaskdb list	Yes	Yes	EMC Symmetrix

Limitations

Assigning a DRA profile to an AD group

- When assigning a DRA profile to an AD Universal Group, the DRA master server must have access to the Global Catalog of the AD Forest.
- When assigning a DRA profile to an AD Local Domain Group, DRA cannot assign the profile to AD Users from a different domain – even though such configuration is valid within AD. This means 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 to which the AD user belongs.

Oracle database discovery

To discover Oracle databases, start the Oracle process or make sure 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 Hitachi Data System (HDS).
- RPO/SLA for NetAPP works only for direct replication from primary devices.

- RPO/SLA for CLARiiON works only for direct replication from primary devices.
- RPO/SLA is not calculated for EMC CLARiiON MirrorView/S.
- RPO/SLA is not calculated for IBM DS and XIV.

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.

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.

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.
