Veritas™ Disaster Recovery Advisor Release Notes

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

6.0

Symantec

Veritas Disaster Recovery Advisor Release Notes

Legal Notice

Product version: 6.0

Document version: 6.0.3

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 maintenance 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 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 Maintenance Programs, you can visit our Web site at the following URL:

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 maintenance agreement may access Technical Support information at the following URL:

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:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

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 maintenance 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 Web site.

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

Veritas Disaster Recovery Advisor Release Notes

Introduction

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

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.
- Auditing and compliance documentation, including a map of your production environment, disaster recovery configuration, and dependencies.
- Identify differences between production, standby, and DR hosts.

System requirements and software limitations

Upgrading the DRA database to Oracle 11g is mandatory.

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

New features

This DRA release introduces new features in the following categories:

Application	Distributed collection Expansion packages Host Configuration Comparison module Ticket labels External tickets systems integration Allow read-only access into the DRA configuration management database DRA configuration API (Web service)
Data collection	IBM SAN Volume Controller (SVC) IBM Virtual I/O (VIO) IBM PowerHA NetApp Zapi
Gaps	New gap signatures

Fixed issues

Ticketing and reporting issues

Items may expire when EMC ControlCenter (ECC) is scanned

If ECC is not being scanned properly, DRA may close and reopen tickets. This causes items to expire when ECC is scanned. [4278]

Workaround: This is only relevant in environments where DRA completes data from the ECC storage scope (non-default configuration). Schedule the scan when ECC is most idle.

Cycle issues

Queries may fail when DRA scans a suspended database

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

DRA does not collect device vendors in all environments

On Red Hat Linux Advanced Server 2.1, DRA does not collect device vendors. [4199]

Creation time of CLARiiON SnapView session may be incorrect

When DRA scans CLARiiON Flare 6.19-6.23, the creation time displayed for CLARiiON SnapView sessions may be incorrect. [5376]

Scanning issues

When an Oracle instance name differs from its database name, DRA detects the database as an instance and adds it to the system

This error usually occurs in a Real Application Cluster (RAC) environment. If the database is changed or removed, DRA creates a new database and does not remove the old or changed database. [4813]

The instance is added to the system only if the instance is running.

Workaround: Ignore the redundant database in the system.

Scanning DB2 on a host scanned using a proxy is not possible

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

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

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

Generating a Ticket Details report with the Topology option checked may take too long

Depending on the options you check, when a large amount of tickets match the filter criteria, generating a Ticket Details report with the Topology option may take a prohibitively long time. [3690]

Workaround: Schedule the report to be sent as an email.

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.

In CLARiiON Flare V6.19, the state property is not displayed

In the Topology view, when you view the properties of a CLARiiON SnapView Snapshot, the state property is not displayed. [5255]

The HBA Summary report might show used host bus adapters (HBAs) as unused for Windows hosts

The HBA Summary report might show unused HBAs for Windows hosts even though they are used. [5321]

DRA may generate false tickets when the Oracle DataGuard standby server is scanned

When both the primary and standby Oracle DataGuard servers are scanned, DRA may generate false tickets about the standby database server. [5930]

Cycle issues

Cannot edit some full cycles

You cannot edit full cycles that have the + character in the name field.

Workaround: Install DRA Hot Fix 3.

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 was changed to be the target and the target was changed to be the source. [4410]

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.

Installation issues

The DRA installer continues installation, even when the Java Runtime Environment (JRE) installation fails

If the JRE installation fails, DRA does not detect it and continues the installation. After such an installation, DRA does not work properly. [4148]

Workaround: Run the installation again, and make sure that the JRE installs properly.

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.

Scanning issues

Full scanning resumes when the system restarts

If a full scan is running and the system stops during the scan, the scan resumes when the system restarts.

Workaround: Install DRA Hot Fix 3.

Error scanning Enterprise Core Component (ECC) 6

Scanning ECC 6 with Secure Sockets Layer (SSL) fails on connection error.

Workaround: Install DRA Hot Fix 2.

NetApp scans may fail

If NetApp does not support Z-Kit Application Program Interface (ZAPI) API version 1.12 or later, NetApp scans fail.

Workaround: Install DRA Hot Fix 2.

UNIX proxy may not work

The UNIX proxy (scanning a host using a jump server) does not work if the proxy and the scanned hosts have different operating system types.

Workaround: Install DRA Hot Fix 1.

Analytics may start before the scan finishes

When scanning storage arrays or hosts takes a long time, the analytics may start before the scan is finished.

Workaround: Install DRA Hot Fix 1.

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.

DRA may alert you about Hitachi/IBM physical volumes that do not have storage volumes

DRA may open a scanning issue about Hitachi/IBM DAS volumes that do not have storage volumes. [5494]

Workaround: Ignore this scanning error.

HBAs are not collected for Linux and HP-UX hosts

DRA does not collect HBA data for Linux and HP-UX hosts. [5506]

IBM DS Global Mirror replication might not be presented correctly

DRA may fail to present IBM DS Global Mirror replication. [5512]

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. [5525]

The collector configuration file is not updated

When you update the DRA server configuration file, the change might not populate to all the collectors. [5972]

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

Other issues

View Storage Arrays page has limited searchability

You cannot search by the Source column on the View Storage Arrays page.

Workaround: Install DRA Hot Fix 3.

DRA does not show Oracle Automatic Storage Management (ASM) disks with the ORCL prefix

DRA does not show Oracle ASM disks with the `ORCL` prefix.

Workaround: Install DRA Hot Fix 2.

Directory structure comparison may fail

When you use the Host Comparison section of the Expansion Packages to compare directories, some differences may not be displayed.

Workaround: Install DRA Hot Fix 2.

Limitations

Oracle database discovery

To discover Oracle databases, start the Oracle process or the /etc/oratab or /var/opt/oracle/oratab file should be present.

Recovery point objective (RPO)/service level agreement

DRA also has the following RPO/SLA limitations:

- RPO/SLA is not supported in 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

Automatic update

The automatic update feature is no longer supported.

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.
