Veritas™ Disaster Recovery Advisor Support Requirements

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

5.4

Symantec

Veritas Disaster Recovery Advisor Support Requirements

Legal Notice

Product version: 5.4

Document version: 5.4.0

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 automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp

Contacting Technical Support

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

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

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp

Customer Service is available to assist with 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

Documentation feedback

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions to storage_management_docs@symantec.com.

Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting.

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance 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

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Chapter 1

Disaster Recovery Advisor support requirements

This document includes the following topics:

Host requirements

This section describes the system requirements for hosts that are installing Disaster Recovery Advisor (DRA).

Hardware

CPU/core	2 Intel/AMD (4 recommended)
RAM	8 GB
Free disk space	100 GB

Software

Operating system	Windows Server 2008 R2[1] Standard Edition 64-bit[2]
Database	Oracle 10g Standard Edition installed with full database administrator rights and patch 4 (10.2.0.5.0) applied
Server	Apache Tomcat 6.0 (this is the only supported version); product is automatically installed if not already on your system
Web client access	■ Internet Explorer 6 or later, with Java client 1.6 or later ■ HTTP access from clients to the DRA server through port 8080 (configurable)

1: If your organization does not plan to use Windows Remote Management (WinRM) to collect data from Windows servers, you can also use Windows Server 2003/2008 64-bit.

2: Although a 32-bit operating system is not recommended, you can use one if you have a small to midsize environment. If you install a 32-bit operating system, you need at least 4 GB of RAM.

DRA requires administrator rights on the DRA application server.

Scanned entities

This section describes the various servers, storage arrays, and databases that DRA can scan, as well other DRA support requirements.

Servers

Table 1-1 describes the servers that DRA can scan.

Table 1-1 Servers DRA can scan

Server	Operating system version	Processor architecture
AIX	4 and later	Power3 series and later
HP-UX	11 and later	PA8700/8800/8900, IA64, IA64 Dual Core Montecito
Linux Red Hat/SUSE	RedHat Advanced Server, SUSE	Intel EM64T, AMD Opteron
Solaris	8 and later	UltraSPARC II/III/IV/T1/T2/T2+, SPARC64-V/VI /VII series
Solaris x64	8 and later	Intel EM64T, AMD Opteron
Windows	Windows XP/2000/ 2003/2008/2008 R2	Intel EM64T, AMD Opteron
ESX, ESXi	3.5 and later	

Storage arrays

Table 1-2 describes the storage arrays that DRA can scan.

Table 1-2 Storage arrays that DRA can scan

Storage array	Supported replications	Comments
EMC Symmetrix (all series) Note: EMC Cellera is not supported.	SRDF, BCV, Clone, Snap	Using SymCLI **Note:** You must install SymCLI on at least one host.
Hitachi HDS (all series)	TrueCopy, Universal Replicator, ShadowImage, QuickShadow	Using HiCommand 4 and later

Table 1-2 Storage arrays that DRA can scan (Continued)

Storage array	Supported replications	Comments
NetApp Filer	SnapMirror, SnapVault	Using Ontap 6 and later
CLARiiON Note: CLARiiON devices connected to hosts via iSCSI are not supported.	SnapView, MirrorView, SAN Copy	NaviSecCLI 6.24 and later
IBM DS (6000, 8000)	FlashCopy, Metro Mirror, Global Copy, Global Mirror	Using DSCLI
IBM XIV	Snapshot, Remote Mirror	Using XCLI

Hosts discovery

Table 1-3 describes the console applications used to discover hosts in your environment.

Table 1-3 Console applications used to discover hosts

Application	Version
ECC (by EMC)	5 and later
HiCommand (by Hitachi Data Systems)	4 and later
vCenter (by VMware)	3.5 and later

Databases

Table 1-4 describes the databases that DRA can scan.

Table 1-4 Databases that DRA can scan

Database	Version	Comments
Oracle	8 and later	Including RAC and ASM
Microsoft SQL Server	2000 and later	
Sybase	12.5 and later	
IBM UDB	8 and later	

Multipath programs

Table 1-5 describes the multipath programs that DRA supports.

Table 1-5 Multipath programs that DRA can scan

Software	Comments
EMC PowerPath	
Veritas DMP	
Hitachi Dynamic Link Manager (HDLM)	
IBM Subsystem Device Driver (SDD)	
HP-UX PVLinks	
Linux MPIO	
AIX MPIO	

Note: Unless explicitly noted in Table 1-5, all versions of the multipath software are supported.

Logical volume managers

DRA can scan the following logical volume managers (LVMs):

- Symantec Veritas VxVM
- HP-UX-native LVM
- AIX-native LVM
- Solaris ZFS
- Linux LVM2
- Oracle ASM

Clusters

DRA supports the following clusters:

- Veritas Cluster Server 5.0 and later
- MS Cluster

Basic cluster support does not include vendor-specific gap signatures, but does include heuristics for cluster identification and vulnerability detection. These heuristics are based on storage sharing and significant capacities for node host configuration.