

Veritas™ Disaster Recovery Advisor Support Requirements

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

6.0

Veritas Disaster Recovery Advisor Support Requirements

Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

Product version: 6.0

Document version: 6.0.0

Symantec, the Symantec Logo, Veritas and Veritas Storage Foundation are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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

Chapter 1	Disaster Recovery Advisor support requirements	
Host requirements	9
Hardware	9
Software	10
Scanned entities	11
Servers	11
Storage arrays	11
Hosts discovery	12
Databases	13
Multipath programs	13
Logical volume managers	13
Clusters	14

Disaster Recovery Advisor support requirements

This document includes the following topics:

- [“Host requirements”](#) on page 9
- [“Scanned entities”](#) on page 11

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 11g Standard Edition installed with full database administrator rights
Server	Apache Tomcat 6.0 (this is the only supported version); product is automatically installed if not already on your system
Web client access	<ul style="list-style-type: none">■ 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 Celleria is not supported.	SRDF, BCV, Clone, Snap	Using SymCLI Note: You must install SymCLI on at least one host.
Hitachi HDS (all series)	TrueCopy, UniversalReplicator, 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, MetroMirror, GlobalCopy, GlobalMirror	Using DSCLI
IBM XIV	Snapshot, RemoteMirror	Using XCLI
IBM SAN Volume Controller (SVC)	FlashCopy, MetroMirror, GlobalMirror	

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
Hardware Management Console (HMC) (by IBM)	7 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

DRA supports the following multipath programs:

- EMC PowerPath
- Veritas Dynamic Multi-Pathing (DMP)
- Hitachi Dynamic Link Manager (HDLM)
- IBM Subsystem Device Driver (SDD)
- HP-UX PVLlinks
- Linux MPIO
- AIX MPIO
- NetApp DSM

Note: Unless explicitly noted, 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
- IBM PowerHA

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.