

Oracle® Secure Backup

Readme

Release 10.1

B25050-01

April 2006

Purpose of this Readme

This Readme file is relevant only to Oracle Secure Backup Release 10.1. This Readme documents supported platforms and devices as well as known issues.

Documentation

For documentation, use your Web browser to access the Oracle Secure Backup documentation library. The library home page is named `index.htm` and is located in the `doc` directory of your CD-ROM image. You can also access the library online at the following URL:

<http://www.oracle.com/technology/documentation/>

Contents

[Section 1, "CD-ROM Image Contents"](#)

[Section 2, "Release Components"](#)

[Section 3, "Licensing Information"](#)

[Section 4, "Bugs and Known Issues"](#)

[Section 5, "Supported Tape Devices and Platforms"](#)

[Section 6, "Documentation Accessibility"](#)

1 CD-ROM Image Contents

The CD-ROM image contains all necessary tools, documentation, and software to install and operate Oracle Secure Backup on the supported platforms. You can access the image from a physical CD-ROM or through a TAR file downloaded from the following product site:

<http://www.oracle.com/technology/products/secure-backup/>

The images in the CD-ROM and TAR file are identical.

2 Release Components

The only product in this release is Oracle Secure Backup.

3 Licensing Information

Refer to *Oracle Secure Backup Licensing Information* for licensing terms.

4 Bugs and Known Issues

The following sections describe bugs and known issues with Oracle Secure Backup.

4.1 Including Oracle Secure Backup in Enterprise Manager Maintenance Page

The Maintenance page in the Enterprise Manager console does not include the Oracle Secure Backup section.

In releases 10.2.0.1 and 10.2.0.2 of Enterprise Manager Grid Control and release 10.2.0.2 of Enterprise Manager Database Control, you must apply a patch to make the Oracle Secure Backup links active. Follow the steps in the section "Using Enterprise Manager" in the "Getting Started" chapter of *Oracle Secure Backup Administrator's Guide*.

4.2 Time Synchronization and "failed to validate certificate" Errors

The clocks on the administrative server, the clients and the media servers must be synchronized to within 60 minutes of each other. If the time skew among hosts in the administrative domain is more than 60 minutes, then you may encounter problems when attempting to issue the `mkhost` command to configure new hosts. The error that appears in the `observed` log file on the client or media server is "failed to validate certificate".

The solution is to synchronize the clock on all hosts in the administrative domain to match the clock on the administrative server, and then retry the failed operation.

4.3 Cannot Edit RMAN-DEFAULT Media Family in Enterprise Manager

You cannot edit the `RMAN-DEFAULT` media family when using Enterprise Manager 10.2.0.2 or earlier.

Use the Oracle Secure Backup Web tool or `obtool` to edit the `RMAN-DEFAULT` media family.

4.4 Tape Device Debug Logging Can Cause Backup Failures

Tape device-related debug logging should only be enabled under the direction of Oracle Support. Enabling tape device-related debug logging outside the instructions of a support representative can cause backup failures.

4.5 Installing SCSI Generic Driver on Linux

Configuring a Linux host for the Oracle Secure Backup media server role requires that the SCSI Generic driver be installed on that host. The host must also be configured to automatically reload the driver after a reboot.

Kernel modules are usually loaded directly by the facility that requires them, if the correct settings are present in the `/etc/modprobe.conf` file. However, it is sometimes necessary to explicitly force the loading of a module at boot time.

For example, on RedHat Enterprise Linux, the module for the SCSI Generic driver is named `sg`. Red Hat Enterprise Linux checks for the existence of the

`/etc/rc.modules` file at boot time, which contains various commands to load modules.

Note: The `rc.modules` should be used, and not `rc.local`, because `rc.modules` is executed earlier in the boot process.

The following commands can be used to add the `sg` module to the list of modules configured to load as `root` at boot time:

```
# echo modprobe sg >> /etc/rc.modules
# chmod +x /etc/rc.modules
```

4.6 Securecomms Security Policy and `obtool` on Windows

On Windows platforms, when the `securecomms` security policy is enabled (the default setting), you must be logged in as Administrator (or your logged-in account must belong to the Administrators group) in order to run the Oracle Secure Backup `obtool` command line tool.

4.7 Restart Windows Media Servers and Clients When Changing Policy Parameters

Oracle Secure Backup clients and media servers running on Windows platforms are not automatically updated when changes are made to certain policy parameters.

The parameters affected are:

- `rmanresourcewaittime`
- `rmanrestorestartdelay`
- `securecomms`

After making changes to any of these parameters, you must stop and restart the `observed` service on each Windows client and media server in Services. (To access Services, click **Start**, and then select **Programs, Administrative Tools, Services**.)

4.8 Oracle Secure Backup Driver CPU Usage (Win2K)

When there are no media devices attached to a Windows 2000 host, do not configure that host for the media server role.

If you configure the media server role on a Windows 2000 host with no attached media devices, then the operating system will continuously try to load the Oracle Secure Backup driver. Continuously trying to load the driver uses most of the available CPU cycles on that system, and renders the system unusable.

4.9 Restriction on Number of Hosts and Tape Drives with Windows Administrative Servers

When using a Windows host as an Oracle Secure Backup administrative server, there is a resource limitation that determines the maximum number of hosts and

tape drives that can be included in the administrative domain. The limitation is as follows:

$$H + (4 * T) < 40$$

where:

- H is the number of hosts in your administrative domain
- T is the number of tape drives (standalone or in tape libraries)

If you configure an Oracle Secure Backup administrative domain on Windows that exceeds this limit, and run multiple simultaneous backup or restore jobs, then in some cases jobs may hang waiting for resources. When this condition arises, you will see the following error message in the `observed` log file:

```
reached maximum Windows event limit (FSP event manager)
```

To resolve the problem, kill the hung backup or restore jobs, and let the others run to completion. Then restart the hung jobs and allow them to run.

4.10 Interaction of Windows Firewall with Oracle Secure Backup (Windows XP)

The default configuration of the Windows Firewall in Windows XP can block ports used by Windows hosts running Oracle Secure Backup. This can prevent Windows hosts from connecting to other hosts in the administrative domain.

Instructions for configuring the Windows Firewall to not interfere with Oracle Secure Backup are contained in the *Oracle Secure Backup Installation Guide*.

4.11 Use Only Lower-Case Letters in Host Names on Windows Administrative Servers

When using a Windows host as an Oracle Secure Backup administrative server, host names cannot contain upper-case characters. An `invalid name` error results when upper-case letters are used in host names with Windows as the administrative server. This limitation does not apply with Linux or Solaris as the administrative server.

4.12 Specifying Oracle User and Password for migrate2osb Migration Tool

The `migrate2osb.exe` tool on Windows and the `migrate2osb.pl` Perl script on Linux and Solaris, used to migrate backups created with Legato into Oracle Secure Backup, require the username and password of an Oracle user with SYSDBA privileges for use during the migration process.

You can use the `--user` (abbreviated as `-u`) command line option to specify the user, and the `--password` (abbreviated as `-p`) command line option to specify the password, respectively. For example:

```
migrate2osb
--user myuser --password passwd1
--restore date --fromdate '10/mar/06' --todate '26/apr/06'
--mmparms 'SBT_LIBRARY=/opt/nsr/libnwora.so'
--directory /tmp --size 10G
--backup --osbparms 'SBT_LIBRARY=/usr/local/oracle/backup/lib/libobk.so'
```

-
-
- Note:** ■ The use of the `-u` or `--user` and `-p` or `--password` arguments is optional. If you do not provide these arguments, then `migrate2osb` prompts for a username and password during its execution.
- On Linux and Unix operating systems, the `ps` command can be used to view the command line arguments used to start a process. Therefore, using the command line arguments to specify the username and password for `migrate2osb` on Linux and Unix can expose your password to someone who runs the `ps` command. If you are concerned about security during the migration process, consider allowing `migrate2osb` to prompt for the username and password instead of using command line arguments to specify them.
-
-

4.13 Documentation Example Error: SBT Backup With ENV Parameter

In the *Oracle Secure Backup Reference*, Example E-2, "SBT Backup with ENV Parameter", is incorrect. The RMAN commands in the example should read as follows:

```
RUN
{
  ALLOCATE CHANNEL c1 DEVICE TYPE sbt
  PARMS 'ENV=(OB_DEVICE=tape2)';
  BACKUP TABLESPACE users;
}
```

4.14 Documentation Error: Supported Platforms List in Installation Guide Not Accurate

In the *Oracle Secure Backup Installation Guide*, the section "Platforms and Operating Systems Supported by Oracle Secure Backup" contains incorrect information.

The only official list of supported platforms for Oracle Secure Backup is available on Certify on Metalink, at the following URL:

<http://metalink.oracle.com/>

5 Supported Tape Devices and Platforms

Supported platforms, web browsers and NAS are listed on Certify on Metalink, at the following URL:

<http://metalink.oracle.com/>

Tape device matrixes are available at the following URL:

<http://www.oracle.com/technology/products/secure-backup/>

6 Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at <http://www.oracle.com/accessibility/>.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Oracle Secure Backup Readme, Release 10.1
B25050-01

Copyright © 2006, Oracle. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software—Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs. Oracle, JD Edwards, and PeopleSoft are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.