Oracle® Secure Backup

Readme

Release 10.1.0.2

B32120-02

November 2006

Purpose of this Readme

This Readme document applies only to Oracle Secure Backup Release 10.1.0.2. This Readme documents licensing, supported platforms and devices as well as known and fixed 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

1 CD-ROM Image Contents

The CD-ROM image for each platform contains all necessary tools, documentation, and software to install and operate Oracle Secure Backup on the selected platform.

> **Note:** Each supported platform requires its own separate CD-ROM or installation Zip file. For example, if you are running an administrative domain using both Windows and Linux clients, you require separate installation media (CD-ROM or downloaded Zip file) for Windows and for Linux.

You can access the installation files from a physical CD-ROM or through a Zip file downloaded from the following product site:

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

The contents of the CD-ROM and Zip file for a given platform 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 Upgrading Existing Oracle Secure Backup Installations to 10.1.0.2

In an upgrade installation, the Oracle Secure Backup catalogs (contained in the `admin` directory) are preserved retaining configuration information and backup metadata for your administrative domain. This state information for your administrative domain, such as the backup catalog, host, user and device configuration information, and any scheduled backup jobs, is stored in the `admin` directory under the Oracle Secure Backup home on your administrative server.

Note: As with any upgrade, we recommend backing up the Administrative Server prior to upgrading.

Before upgrading an existing Oracle Secure Backup administrative domain to 10.1.0.2, you must shut down Oracle Secure Backup-related drivers and background processes on all hosts. Upgrade the administrative server, host first, and then the other hosts in the domain.

Brief instructions on each step are described in the following sections.

4.1 Preparing Administrative Domain Hosts for Upgrade Installation of Oracle Secure Backup

Before performing an upgrade installation, you must stop the Oracle Secure Backup-related daemons and services on all hosts in your administrative domain.

On Linux or Unix, use the `ps` command to identify the Oracle Secure Backup daemon processes:

```
# /bin/ps -ef | grep ob
```

Use the `kill -9` command to stop each process.

On Windows hosts, you must stop the Oracle Secure Backup Services service, and, on media servers, disable the Oracle Secure Backup device driver.

To disable the driver, in Device Manger, under Tape Drives, right-click **Oracle Secure Backup Device Driver**, and select **Disable**. Then reboot the system.

To stop the Oracle Secure Backup Services service, open the Services applet, right-click the **Oracle Secure Backup Services** service, and select **Stop**.

4.2 Upgrade Installation of Oracle Secure Backup on Windows

To upgrade a Windows installation of Oracle Secure Backup, follow the Windows installation process described in ***Oracle Secure Backup Installation Guide***.

Before the new version of Oracle Secure Backup can be installed, the previous version must be uninstalled. When the installer detects the existing install of Oracle Secure Backup, it runs the uninstaller program for the previous version automatically, before beginning the new installation.

Note: On a Windows administrative server, the uninstallation program displays the following prompt:

```
This system was configured as an Oracle Secure Backup
Administrative Server.

Oracle Secure Backup creates files specific to this administrative
domain in the "admin" directory. Would you like to keep these files
in case you reinstall Oracle Secure Backup?

If you choose "Delete" all files related to Oracle Secure Backup
will be removed from this system. If you choose "Keep" the files
specific to this administrative domain will be retained.
```

Click **Keep** to retain the files in the `admin` directory. The new installation of Oracle Secure Backup uses these files to keep the configuration of your administrative domain.

Complete the rest of the installation process as described in ***Oracle Secure Backup Installation Guide***.

Note: Specify the same host roles for each host as were used in the previous installation.

4.3 Upgrade Installation of Oracle Secure Backup on Linux or Unix

To upgrade a Linux or Unix installation of Oracle Secure Backup, follow the setup and installation process described in ***Oracle Secure Backup Installation Guide***.

During the upgrade process, the installer displays the following prompt:

```
Oracle Secure Backup is already installed on this machine (myhostname-sun2).
Would you like to re-install it preserving current configuration data[no]?
```

Enter `yes` to perform the upgrade installation, retaining your previous configuration.

5 Outstanding Bugs and Known Issues

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

5.1 Manually Start Oracle Secure Backup Services After Installation (Windows)

On Windows Server 2003 and Windows 2000, on hosts that are only configured for the media server or client roles, the Oracle Secure Backup Services service is not started automatically after installation. You must start it manually.

Note:

- This issue does not apply to Windows XP.
- This issue does not apply to hosts configured for the administrative server role.
- This issue only occurs immediately after the installation. The service is started automatically whenever Windows is rebooted.

To start the Oracle Secure Backup Services service, open the Services applet, right-click the **Oracle Secure Backup Services** service, and select **Start**.

5.2 Using Upper-Case Letters in the Job Summary Title Prevents E-Mail Notification (Windows)

On Windows administrative servers, if the title for a backup job contains upper case characters, email notification of the backup job summary fails.

5.3 Setting Permissions for Generic SCSI Device Files (SUSE)

On SUSE Linux, permissions for the Generic SCSI device files `/dev/sg0 -/dev/sg31` and `/dev/sga - /dev/sgp` must be changed from 640 to 666 for Oracle Secure Backup to operate properly.

5.4 Bidirectional PNI Support

The Preferred Network Interface (PNI) capability supports bidirectional specification of communication between hosts. The PNI behavior is described below.

In cases where hosts have more than one network interface, you can specify which interface is used to transmit data to be backed up or restored between hosts by configuring Preferred Network Interface (PNI) settings for each host.

Configuring host A to specify a Preferred Network Interface on host B identifies the network interface on host B to use when host A and host B communicate.

When host A attempts to establish a connection with host B, the PNI settings on host A and host B are applied in the following manner:

- Host A queries the administrative server for the PNI settings configured for host B, to see if a specific interface on host B should be used for transfers

from host A. If an interface at host B is specified for communications with host A, then it is used for the transfer.

- Host A also queries the administrative server for the PNI settings configured for host A, to see if a specific interface is preferred for transfers to host B. If an interface at host A is specified for communications with host B, then it is used for the transfer.

For example, suppose the host storabck10 has the following PNI setting configured:

```
ob> lspni
storabck10:
    PNI 1:
      interface:        storabck10-rac
      clients:          stacx53
```

When the host stacx53 connects to storabck10, it consults the configured PNI settings and determines that it must connect over the interface on storabck10 named storabck10-rac.

Now suppose that storabck10, acting as a client, wants to connect to a device connected to stacx53 (that is, stacx53 is now acting as a media server). storabck10 also references the PNI settings for both hosts, and discovers that it should use the local interface storabck10-rac in order to establish the connection with stacx53.

The `obtar` command reports which interfaces are in use for a connection between `obtar` and a remote backup device. To display this information in the `obtar` transcript, use the `-J` option on the `obtar` command line, or as part of the `backupoptions` policy. In the example above, the connection would be shown as:

```
09:38:38 A_0: sock 8 connects (local) storabck10.rac to (remote) stacx53
```

5.5 Globalization Restrictions Within Oracle Secure Backup

The following globalization restrictions apply to Oracle Secure Backup:

- The Oracle Secure Backup Web Tool and command line interface are English-only, and are not globalized. Localizations or multi-byte character set data are not supported. All messages and documentation are in English.
- Oracle Secure Backup does not support filenames or RMAN Backup names that are encoded in character sets that do not support null termination, such as Universal Character Set (UCS).

5.6 Visibility of Oracle Secure Backup Links on the Enterprise Manager Maintenance Page

On a Linux host running Enterprise Manager Database Control or Enterprise Manager Grid Control, support for managing Oracle Secure Backup is not included until you apply the first Oracle Database 10g Release 2 patch set.

Also, 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, the Oracle Secure Backup section of the Maintenance page is not displayed by default.

Follow the steps in the section "Using Enterprise Manager" in the "Getting Started" chapter of *Oracle Secure Backup Administrator's Guide* to configure Enterprise Manager to include the Oracle Secure Backup section in the Maintenance page.

5.7 Time Synchronization and "failed to validate certificate" Errors

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

5.8 Cannot Edit RMAN-DEFAULT Media Family in Enterprise Manager

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

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

5.9 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
```

5.10 Securecomms Security Policy and obtool (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.

5.11 Oracle Secure Backup Driver CPU Usage (Windows 2000)

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.

Microsoft has provided a hotfix which should be applied to any Windows 2000 host configured for the media server role. For a description of the Windows 2000 issue that causes this problem and the hotfix that resolves it, refer to the following URL:

`http://support.microsoft.com/default.aspx?kbid=841382`

To avoid this issue, when there are no media devices attached to a Windows 2000 host, do not configure that host for the media server role.

5.12 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***.

5.13 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.

5.14 Upgrading Release 10.1.0.1 to 10.1.0.2 on Windows

When uninstalling Oracle Secure Backup on a Windows administrative server, the uninstaller allows you to click **Keep**, to keep files containing the record of your administrative domain and backups for use by a future installation of Oracle Secure Backup, or **Delete**, to delete these files and create a new administrative domain in a future installation.

However, the release 10.1.0.1 uninstaller does not correctly preserve these files. Running the installer from release 10.1.0.1 deletes the administrative domain configuration, even if you choose **Keep**.

To upgrade an installation of release 10.1.0.1 and preserve the configuration of the administrative domain, run the installation program for release 10.1.0.2. Do not uninstall release 10.1.0.1 first. The installer for 10.1.0.2 upgrades an existing installation of release 10.1.0.1 transparently, and preserves the administrative domain configuration.

5.15 Release 10.1.0.2 on Windows Does Not Support Modify or Repair Installation Options

If you run the installer for Oracle Secure Backup release 10.1.0.2 on Windows on a system with release 10.1.0.2 already installed, the installer displays the Modify, Repair and Remove options. Only the Remove option is correctly supported in release 10.1.0.2. Do not use the Modify or Repair options in the installer when installing in place over an existing 10.1.0.2 installation.

5.16 Manually Delete orasbt32.dll when Upgrading Windows 64-Bit Systems

When upgrading an existing Windows 64-bit installation of Oracle Secure Backup release 10.1.0.0.0 to release 10.1.0.2, you must uninstall release 10.1.0.0.0 before you can run the installer for release 10.1.0.2.

However, the Microsoft Installer reports an internal error, if the file `%WINDIR%\system32\orasbt.dll` is present when you run the Windows installer for Oracle Secure Backup release 10.1.0.2. Therefore, delete this file manually before running the installer for Oracle Secure Backup release 10.1.0.2.

6 Bugs Fixed in Release 10.1.0.2

The following bugs have been addressed in Oracle Secure Backup Release 10.1.0.2:

Table 1

Bug Number	Description
4878473	**Very Long Volume IDs Became Corrupted** When a volume ID of 25 or more characters is used, the last six characters are required to be numeric. Previous versions of Oracle Secure Backup did not correctly enforce this requirement and generated Volume IDs that did not end with numeric characters. Oracle Secure Backup now replaces the last six characters of long volume IDs with numeric characters.
5228264	**"Device Already Opened By This Process" Error** When testing whether a locally attached tape device was already in use, Oracle Secure Backup compared the SCSI channel, SCSI ID and SCSI LUN but did not compare the addresses of the SCSI adapters. This meant that a process could not simultaneously open two tape devices whose addresses differed only on adapter address. As a result, backups or other operations failed with a "Device already opened by this process" error if two media devices on different SCSI adapters had the same SCSI channel, SCSI ID and SCSI LUN values.
5389348	**Windows 2000 Client Host Database Backup Fails with Repeated Warning "unsupported message 0.0 received"** A database backup from a Windows 2000 client could fail with repeated error messages sent to RMAN. The communication between RMAN and the Windows 2000 client was handled incorrectly, and caused repeated zero-length messages to be sent. In this case, the `obproxyd.log` file contained repeated `unsupported message 0.0 received` messages, for each of the zero-length messages sent. This behavior caused the backup to fail. RMAN database backups no longer fail in this manner.
5370286	**"Page Not Found" Errors in Web Tool After Login** Selecting a user password that was a multiple of eight characters long would make the Web tool inaccessible.
5221340	**Can Only Use Lower-Case Letters in Host Names on Windows Administrative Servers** Windows administrative servers now support upper-case letters in host names.
5211979	**Tape Device Debug Logging Can Cause Backup Failures** Restriction on enabling tape device-related debug logging has been removed.
5207935	**RMAN Backup Failed with RMAN-00600 Error** An RMAN database backup could fail when a file system backup job was started by the scheduler during a long-running backup job. This failure no longer occurs.
4398115	**Restriction on Number of Hosts and Tape Drives with Windows Administrative Servers** The previous limitation on the maximum number of hosts and tape drives supported when using a Windows host as administrative server has been removed.

Table 1 (Cont.)

Bug Number	Description
5149059	**Restart Windows Media Servers and Clients When Changing Policy Parameters** It is no longer necessary to restart Windows media servers when changing policy parameters.
5040299	**Database Backup Jobs Fail If Tape Device Becomes Temporarily Unavailable During Backup** If the device becomes available again within the user-configured RMAN resource wait time, then the database backup job will now continue when the tape device becomes available again.
5016065	**Backup of Oracle Sparse Files Fails if Exclude Oracle Files Option is Specified** The backup of a database sparse file of size greater than 2GB now succeeds on Linux when the backup excludes database temporary files.
4924506	**Device Restrictions Cannot Be Removed Via Web Browser** Web tool can now remove device restrictions
4736477	**Obtool LSBU Command Not Handling '\' in Path** Obtool now supports the backslash character \ in path names.
5353546	**Administrative Server Role Not Supported on Non-English Windows Installations** Oracle Secure Backup can now be successfully configured as an administrative server on supported non-English versions of Windows. Previous limitations have been removed.

7 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 drive and library matrixes are available at the following URL:

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

8 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 10.1.0.2
B32120-02