Oracle® Secure Backup

Readme

Release 10.2

E05411-06

November 2009

Purpose of this Readme

This Readme document applies only to Oracle Secure Backup release 10.2.0.5. 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.

The most current Oracle Secure Backup documentation can be found at `http://www.oracle.com/technology/products/secure-backup/index.html`. The documentation is updated periodically, and Oracle recommends that you check this site for the current documentation and information on how to best use Oracle Secure Backup.

Contents

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.

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/

Release Components

The only product in this release is Oracle Secure Backup.

Licensing Information

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

Upgrading Oracle Secure Backup Releases 10.1 and 10.2 to Release 10.2.0.5

If you are upgrading an existing Oracle Secure Backup release 10.1 installation to release 10.2.0.5, then you must upgrade every host in the Oracle Secure Backup administrative domain. Oracle Secure Backup release 10.2 is incompatible with Oracle Secure Backup release 10.1.

If you are upgrading an existing Oracle Secure Backup release 10.2.0.1, 10.2.0.2, or 10.2.0.3 installation to Oracle Secure Backup release 10.2.0.5, then you must upgrade the administrative server and media server hosts in the Oracle Secure Backup administrative domain. Oracle recommends that you also update your clients in the domain to Oracle Secure Backup release 10.2.0.5. But hosts acting as clients only can remain at Oracle Secure Backup release 10.2.0.1, 10.2.0.2, or 10.2.0.3 and participate as part of an Oracle Secure Backup release 10.2.0.5 domain.

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: Oracle recommends backing up the administrative server before upgrading.

Before upgrading an existing administrative domain to Oracle Secure Backup release 10.2.0.5, you must shut down drivers and background processes related to Oracle Secure Backup 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.

Preparing Oracle Secure Backup Administrative Domain Hosts for Upgrade to Oracle Secure Backup Release 10.2.0.5

Before performing an upgrade installation, you must stop the daemons and services related to Oracle Secure Backup on all hosts in your administrative domain. The preferred methods for stopping the Oracle Secure Backup daemons are as follows.

On Linux:

```
# /etc/init.d/observiced stop
```

On Solaris:

```
#/etc/init.d/OracleSecureBackup stop
```

On both Linux and Solaris administrative servers, it is also necessary to stop the Oracle Secure Backup Web tool processes. Use the `ps` command to identify the Oracle Secure Backup httpd 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:

1. Open the Services applet.
2. Right-click the **Oracle Secure Backup Services** service, and select **Stop**.

Upgrade Installation of Oracle Secure Backup Release 10.2.0.5 on Windows 32-Bit

You can upgrade your Windows 32-bit administrative server, media servers, and clients from Oracle Secure Backup release 10.2.0.1, 10.2.0.2, or 10.2.0.3 to Oracle Secure Backup release 10.2.0.5 simply by running the Oracle Secure Backup release 10.2.0.5 installer. This is called an *upgrade installation*. The installer detects the existing installation of Oracle Secure Backup and runs the uninstaller for the previous version automatically before beginning the new installation.

When you upgrade your administrative server from Oracle Secure Backup release 10.2.0.1, 10.2.0.2, or 10.2.0.3 to Oracle Secure Backup release 10.2.0.5, the uninstaller will display 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.
```

You *must* choose the **Keep** option for the admin directory files. Selecting the **Delete** option will cause the installation to be incomplete, and then you must uninstall and reinstall Oracle Secure Backup to complete the installation. If you do not want to save the existing admin directory files, then you must exit the installation, uninstall Oracle Secure Backup release 10.2.0.1, 10.2.0.2, or 10.2.0.3, and select the **Delete** option. After you have uninstalled Oracle Secure Backup release 10.2.0.1, 10.2.0.2, or 10.2.0.3, you can install Oracle Secure Backup release 10.2.0.5 by running the Oracle Secure Backup release 10.2.0.5 installer.

You can upgrade your Windows 32-bit administrative server and clients from Oracle Secure Backup release 10.1 to Oracle Secure Backup 10.2.0.5 with an upgrade installation, so long as the administrative server is not also a media server.

When you upgrade your administrative server from Oracle Secure Backup release 10.1 to Oracle Secure Backup release 10.2.0.5, you should select the **Keep** option to keep the existing configuration of your administrative domain. If you select the **Delete** option, then the Oracle Secure Backup release 10.2.0.5 installation will succeed, but you will have to re-enter all of your Oracle Secure Backup configuration settings.

An upgrade installation will not successfully upgrade a media server or an administrative server that is also a media server from Oracle Secure Backup release 10.1 to Oracle Secure Backup release 10.2.0.5. In this special case, you can use the following procedure:

1. Uninstall the existing Oracle Secure Backup software.

   You can uninstall the existing Oracle Secure Backup software by selecting **Start > Programs > Oracle Secure Backup > Uninstall Oracle Secure Backup**.

2. Select the **Keep** option if you are upgrading an administrative server that is also a media server.

3. Restart the host.

4. Run the Oracle Secure Backup release 10.2.0.5 installer.

Upgrade Installation of Oracle Secure Backup Release 10.2.0.5 on Windows x64

Different upgrade installation procedures must be used for Windows x64 than those described in "Upgrade Installation of Oracle Secure Backup Release 10.2.0.5 on Windows 32-Bit" on page 3. You can use the following procedure to upgrade a Windows x64 administrative server or client, so long as the administrative server is not also a media server:

1. Uninstall the existing Oracle Secure Backup software, selecting the **Keep** option if you are upgrading an administrative server.

   > **See Also:** "Upgrade Installation of Oracle Secure Backup Release 10.2.0.5 on Windows 32-Bit" on page 3 for more information on uninstalling Oracle Secure Backup software and the **Keep** option

2. Run the Oracle Secure Backup release 10.2.0.5 installer.

You can use the following procedure to upgrade a Windows x64 media server or administrative server that is also a media server:

1. Uninstall the existing Oracle Secure Backup software, selecting the **Keep** option if you are upgrading an administrative server that is also a media server.

2. Restart the host.

3. Run the Oracle Secure Backup release 10.2.0.5 installer.

Upgrade Installation of Oracle Secure Backup Release 10.2.0.5 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 and Configuration 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.

Upgrade Installation of Oracle Secure Backup Release 10.2.0.5 on AIX

Oracle Secure Backup release 10.2.0.5 supports the administrative server, media server, and client roles on AIX platforms. The previous version of Oracle Secure Backup must be uninstalled before installing Oracle Secure Backup 10.2.0.5.

> **Note:** *Oracle Secure Backup Installation and Configuration Guide* states that AIX support is limited to the client role. This statement is no longer correct.

During Oracle Secure Backup installation, the Oracle Secure Backup `admin` user is mapped by default to UNIX user `root` and UNIX group `root`. In this configuration, Oracle Secure Backup requires that the user `root` be a member of the group `root` to back up the file system successfully. AIX does not define a group `root` by default. If the group `root` does not exist on your AIX system, then you must create it and make user `root` a member of it.

> **Note:** This mapping of the Oracle Secure Backup `admin` user can be changed post-installation.

AIX Device Identification

In order to access SCSI or Fibre Channel tape devices, Oracle Secure Backup requires the following identifying information about how the devices are attached to their hosts:

- SCSI bus name
- Target ID
- Logical Unit Number (LUN)

This information might not be readily available for all attached devices using standard operating system commands. To assist with gathering device information in AIX environments, Oracle Secure Backup includes the standalone tool `obscan`. The `obscan` executable is in the cdtools directory of the Oracle Secure Backup CD or CD image.

> **Note:** The information obtained from `obscan` is required when running the Oracle Secure Backup `makedev` command. See "Creating Device Special Files with makedev" in the *Oracle Secure Backup Installation and Configuration Guide* for more information.

You must have operating system privilege to access devices, which is often root access, to run `obscan`. The syntax for `obscan` is as follows, where *`device_filename`* is the device file name of the SCSI bus or Fibre Channel fabric to scan:

```
obscan device_filename
```

Run `obscan` for each SCSI and Fibre Channel adapter with tape devices to be used by Oracle Secure Backup. In the following example, `obscan` gathers information about the tape devices connected to the SCSI bus identified by the device file /dev/scsi2:

```
obscan /dev/scsi2

obscan version 10.2.0.3 (AIX)
Copyright (c) 2008, Oracle. All rights reserved.

DEVICE information for /dev/scsi2

 Target-id : 0, Lun : 0
    Vendor : ADIC  Product : FastStor 2

 Target-id : 5, Lun : 0
    Vendor : HP    Product : Ultrium 2-SCSI

 Total count of Media Changers and/or Tape devices found : 2
```

In this second example, `obscan` gathers information about the tape devices connected to the Fibre Channel fabric identified by /dev/fssci0:

```
obscan /dev/fscsi0

DEVICE information for /dev/fscsi0

 Target-id : 6423827, Lun : 0
    Vendor : ADIC  Product : Scalar 24    World Wide Name : 2001006045175222

 Target-id : 6423827, Lun : 1
    Vendor : IBM   Product : ULTRIUM-TD2  World Wide Name : 2001006045175222

 Target-id : 6423827, Lun : 2
    Vendor : IBM   Product : ULTRIUM-TD2  World Wide Name : 2001006045175222

 Target-id : 6491411, Lun : 0
    Vendor : ADIC  Product : Scalar i500  World Wide Name : 2400005084800672

 Target-id : 6491411, Lun : 1
    Vendor : IBM   Product : ULTRIUM-TD3  World Wide Name : 2400005084800672

 Target-id : 6491411, Lun : 2
    Vendor : IBM   Product : ULTRIUM-TD3  World Wide Name : 2400005084800672

 Target-id : 6491411, Lun : 3
    Vendor : IBM   Product : ULTRIUM-TD3  World Wide Name : 2400005084800672

 Target-id : 6491411, Lun : 4
    Vendor : IBM   Product : ULTRIUM-TD3  World Wide Name : 2400005084800672

 Total count of Media Changers and/or Tape devices found : 8
```

Using the information from the `obscan` tool, you can create attach points used within Oracle Secure Backup to identify devices for backup and restore operations. In the following example the attach point /dev/obl8 is created for the ADIC FastStor 2 library attached to scsi2 having the target id 0 and lun 0:

```
makedev
Enter logical unit number 0-31 [0]: 8
Enter 'd' if this device is a tape drive or 'l' if a SCSI-2 addressable
```

```
    tape library [d]: 1
Enter SCSI bus name: scsi2
Enter SCSI target id 0-16777215: 0
Enter SCSI logica l unit number (lun) 0-7 [0]: 0
/dev/obt8 created
```

In this second example the attach point /dev/obl9 is created for the ADIC Scalar 24 library attached to fsci0 having the target id 6423827 and lun 0:

```
makedev
Enter logical unit number 0-31 [0]: 9
Enter 'd' if this device is a tape drive or 'l' if a SCSI-2 addressable
    tape library [d]: 1
Enter SCSI bus name: fscsi0
Enter SCSI target id 0-16777215: 6423827
Enter SCSI logical unit number (lun) 0-7 [0]: 0
/dev/obl9 created
```

Note: The obscan tool is not included as part of the Oracle Secure Backup installation. It is provided as an optional tool for device identification in AIX environments.

Supported Tape Devices and Platforms

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

http://support.oracle.com/

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

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

Outstanding Bugs and Known Issues

This section discusses Oracle Secure Backup release 10.2.0.5 outstanding bugs and known issues.

Creating Attach Points for Solaris 10 Fibre Channel Devices

Oracle Secure Backup supports the use of Fibre Channel-attached tape devices on media servers running Solaris 10. The Oracle Secure Backup install script and makedev utility cannot be used to create the needed links in the /dev directory to the device special files for such devices.

The Solaris sgen driver must be disabled before installing Oracle Secure Backup. If it is not disabled, then it might attach to your media changer or tape devices and prevent Oracle Secure Backup from attaching to them.

To disable the Solaris sgen driver:

1. Comment out all entries in /kernel/drv/sgen.conf.
2. Check the /etc/driver_aliases file for any sgen entries and remove them using the update_drv command. Suppose, for example, that /etc/driver_aliases contains the following entries:

    ```
    sgen "scsa,08.bfcp"
    ```

```
sgen "scsc,08.bvhci"
```

To remove these entries you would run the following commands:

```
/usr/sbin/update_drv -d -i '"scsa,08.bfcp'" sgen
/usr/sbin/update_drv -d -i '"scsa,08.bvhci'" sgen
```

3. Restart your system to release the tape devices.

During installation, the Oracle Secure Backup driver automatically identifies Fibre Channel-attached devices by their World Wide Names. After installing the driver, you must determine the World Wide Name for each device, and then manually create symbolic links in the `/dev` directory that point to the actual attach points for the devices.

To create device special files for Solaris 10 tape devices:

1. Run the Oracle Secure Backup install script on your media server.

   When the Oracle Secure Backup driver is installed, the install script prompts:

   ```
   NOTE: The Oracle Secure Backup device driver has been successfully installed.
   Would you like to configure (or reconfigure) any Oracle Secure Backup
   devices that are attached to dlsun1976 [no]?
   ```

   Enter `no`.

2. After install completes, run the `dmesg` command and examine the output.

   The Oracle Secure Backup driver adds messages to the log that contain the World Wide Names for the Fibre Channel-attached tape devices. The attach points for tape drives contain the string `sgen`. The attach points for tape libraries contain the string `st`.

   For example, the following output contains the World Wide Names and corresponding attach points for a tape drive and a tape library:

   ```
   Dec 12 17:12:53 storabck22 scsi: [ID 799468 kern.info] ob30 at fp0: name
   w500308c162680e24,1, bus address 6119e8
   Dec 12 17:12:53 storabck22 genunix: [ID 936769 kern.info] ob30 is
   /pci@1f,4000/fibre-channel@2/fp@0,0/sgen@w500308c162680e24,1
   Dec 12 17:12:53 storabck22 scsi: [ID 799468 kern.info] ob31 at fp0: name
   w500308c162680e24,0, bus address 6119e8
   Dec 12 17:12:53 storabck22 genunix: [ID 936769 kern.info] ob31 is
   /pci@1f,4000/fibre-channel@2/fp@0,0/st@w500308c162680e24,0
   ```

3. For each device listed in the `dmesg` output, assign an Oracle Secure Backup logical unit number.

4. Create symbolic links in the `/dev` directory that reference the attach points.

   The name for the symbolic link should be `/dev/obt`*n* for tape drives and `/dev/obl`*n* for tape libraries, where *n* is the Oracle Secure Backup logical unit number you assigned to the device in step 3.

   For example, assume that you assign the devices listed in the output of step 2 the Oracle Secure Backup logical unit number 0. The resulting device names are `/dev/obl0` for the tape library, and `/dev/obt0` for the tape drive. The following commands create the required symbolic links in `/dev`:

   ```
   ln -s /devices/pci@1f,4000/fibre-channel@2/fp@0,0/sgen@w500308c162680e24,1:fp0
   /dev/obl0
   ln -s /devices/pci@1f,4000/fibre-channel@2/fp@0,0/st@w500308c162680e24,0:fp0
   ```

```
/dev/obt0
```

5. Use the mkdev command in obtool or the Oracle Secure Backup Web tool to add these devices to your administrative domain.

Avoid Importing Volumes with Identical Volume IDs Between Alternate Oracle Secure Backup Domains

Volumes created within one Oracle Secure Backup domain can be imported into an alternate Oracle Secure Backup domain. Best practice recommendation is to use a different Volume ID naming scheme for each domain to avoid duplicate Volume IDs when volumes are imported into an alternate Oracle Secure Backup domain (catalog). With the same Volume ID naming scheme in multiple domains, importing volume metadata between domains could potentially be problematic, allowing multiple volumes with the same Volume ID maintained within one domain.

Associated with Bug 6631412.

Upgrade Does Not Preserve NDMP Media Server User Name and Password

You must restore the NDMP media server user name and password after upgrading to Oracle Secure Backup release 10.2.0.5. You can use the obtool chhost command:

```
# chhost -ndmppass <ndmp-password> --ndmpuser <ndmp-username> <host-name>
```

Associated with Bug 6893306.

Oracle Secure Backup Web Tool Does Not Display the Correct Encryption Algorithm for a Host

The encryption algorithm displayed in the Oracle Secure Backup Web tool Configure: Hosts page is incorrect. You must use the obtool lsh command to display the correct setting:

```
# lsh -l <host-name>
```

Associated with Bug 6894525.

Cannot Change Host Encryption Algorithm with Oracle Secure Backup Web Tool

You cannot change the encryption algorithm for a host on the Oracle Secure Backup Web tool Configure: Hosts page. You must use the obtool chhost command:

```
# chhost -algorithm <algorithm-type>  <host-name>
```

Associated with Bug 6894525.

Oracle Secure Backup Web Tool Does Not Display Default TCP/IP Setting for a Host

The TCP/IP buffer size displayed on the Oracle Secure Backup Web tool Configure: Hosts page is blank when the buffer size is set to the default. You must use the obtool lsh command:

```
# lsh -l <host-name>
```

Associated with Bug 6911984.

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).

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

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

Also, in Oracle Enterprise Manager Grid Control releases 10.2.0.1 and 10.2.0.2 and Oracle Enterprise Manager Database Control release 10.2.0.2, the Oracle Secure Backup section of the Maintenance page is not displayed by default.

Follow the steps in "Enabling Oracle Secure Backup Links in Oracle Enterprise Manager" in Chapter 4 of *Oracle Secure Backup Installation and Configuration Guide* to configure Oracle Enterprise Manager to include the Oracle Secure Backup section in the Maintenance page.

> **Note:** The Oracle Secure Backup section of the Maintenance page might not appear in Oracle Database Control, even after enabling display of Enterprise Manager links using the procedure described in *Oracle Secure Backup Installation and Configuration Guide*. The resolution for this problem is described in Metalink note 399826.1.

Windows x64 Upgrade from Oracle Secure Backup Release 10.1.0.2 Is Unable to Complete Installation

Oracle Secure Backup release 10.2.0.5 for Windows x64 installation cannot upgrade an existing Oracle Secure Backup release 10.1.0.2 installation. The upgrade will fail and cause the Install Wizard to be interrupted. The failure will not modify the current Oracle Secure Backup installation. You must first uninstall the current Oracle Secure Backup installation before installing Oracle Secure Backup release 10.2.0.5.

> **See Also:** "Upgrade Installation of Oracle Secure Backup Release 10.2.0.5 on Windows x64" on page 4

Catalog Recovery Procedure Change for Windows Platforms

Steps 4 and 5 of the Catalog Recovery Procedure in the *Oracle Secure Backup Administrator's Guide* are different for the Windows platform. All other steps in the recovery procedure should be followed.

- Step 4 for Windows is the following:

  Load your `OSB-CATALOG-MF` backup volume into the drive and verify the volume and file number by indexing the tape using the `obtar -tf drive_name -F file_number` command as shown in the following example:

  ```
  C:\>obtar -tf t4_d1 -F 1 > outt

  C:\>more outt
  C:\osb\backup\admin
  ...
  C:\osb\backup\db
  ...
  ```

- Step 5 for Windows is the following:

  Extract the backup directory to an alternate location using the `obtar -xf drive_name -F file_number -s,P,R,` (Replace prefix P with string R) command.

  Note, the path substitution syntax for `obtar` is "`-s,P,R,` (Replace prefix P with string R)."

  You absolutely must restore the catalog backup to an alternate directory. Restoring the catalog backup to its original location leaves Oracle Secure Backup configuration in an inconsistent state.

  ```
  C:\>obtar -xf t4_d1 -F 1 -s,C:/osb/backup,C:/osb/backup-restored,

  C:\osb\backup-restored>dir *.
  <DIR> admin
  <DIR> db
  ```

Bugs Fixed in Oracle Secure Backup Release 10.2.0.5

This section lists bugs that have been fixed in Oracle Secure Backup release 10.2.0.5.

Table 1 Oracle Secure Backup Bugs

Bug Number	Subject
7044337	OBTOOL LSD -L SHOWS INCORRECT CAPSIZE
7044342	OBTOOL CHD -C TO CHANGE CAPID FOR A CAP DOESN'T WORK
7387404	WILDCARDS IN DATASET INCLUDE PATH RESULTS IN INCLUDE PATH PER FILE
7423327	CRASH IN OBACSLIBD IN LARGE ACSLS SYSTEMS
7454723	UNSORTED AIF PERFORMANCE PROBLEM WITH NDMP BACKUPS
7454992	CATALOG RECORDS ARE EXPANDED ONE BLOCK AT A TIME
7533861	ENHANCE INVENTORY OPERATION ON ACSLS TO PARSE/UPDATE CLEANING TAPE INFORMATION
7583295	LSVOL SHOWS EJECTED TAPES IN ACSLS LIBRARY
7609777	INVENTORY OF ACSLS LIBRARY WILL SHOW RESTRICTED TAPE DRIVES
7665919	WARNING: FINI: NODE RECORD WITH INODE (36E6FC) HAS NO MATCHING DIR REC (376D07)

Table 1 (Cont.) Oracle Secure Backup Bugs

Bug Number	Subject
7672297	CATALOG CLEANUP IS VERY SLOW
7683563	INTERNAL CONSISTENCY CHECK MISMATCH WHEN TRYING TO UPDATE, QUERY OR RM A PIECE
7704605	VOLUME IDS CONSIDERED STALE
7827410	ERROR: CAN'T CONNECT TO NDMP SERVER ... TIMEOUT WAITING FOR CONNECTION STATUS
8206760	LOST INDICES.CUR AFTER SHUT DOWN OF OBIXD
8267216	ACSLS BASED INVENTORY TAGGING VOLUMES AS UNLABELED 10.3 AND 10.2.0.4
8283529	ACSLS Export/Inject inventory causes volumes to be unlabelled
8345949	BACKUP JOB HANGS WHEN VOLUME SWAP IS NEEDED
8331225	RMAN BACKUPS TO TAPE VIA OSB ARE VERY SLOW TO LOAD A TAPE AT START OF BACKUP
8373174	OS COMMAND INJECTION VIA MULTIPLE VARIABLES TO PROPERTY_BOX.PHP
8373151	AUTHENTICATION BYPASS BY USING ANGLE BRACKETS IN USERNAME FIELD OF LOGIN.PHP
8451264	BUFFER OVERFLOW WHEN RESOLVED DNS NAME FOR CLIENT IS OVER 112 CHARACTERS LONG
8849663	ARG NOT BEING ESCAPED ON WINDOWS

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. 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.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at `http://www.fcc.gov/cgb/consumerfacts/trs.html`, and a list of phone numbers is available at `http://www.fcc.gov/cgb/dro/trsphonebk.html`.

Oracle Secure Backup Readme, Release 10.2
E05411-06