

Oracle® Database Firewall

Release Notes

Release 5.1 for Oracle Linux

E22689-03

December 2011

These *Release Notes* contain important information about the Oracle Database Firewall Release 5.1. They apply to Oracle Database Firewall on all platforms.

This document contains the following sections:

- [Downloading the Latest Version of This Document](#)
- [Installing Oracle Database Firewall 5.1](#)
- [Upgrading to Oracle Database Firewall 5.1](#)
- [Known Issues](#)
- [Documentation Accessibility](#)

1 Downloading the Latest Version of This Document

You can download the most current version of this document from the following Web site:

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

2 Installing Oracle Database Firewall 5.1

Refer to the *Oracle Database Firewall Installation Guide* for installation instructions.

3 Upgrading to Oracle Database Firewall 5.1

You can upgrade from Oracle Database Firewall release 5.0 to 5.1.

3.1 Pre-requisite

If you have not already done so, you must apply the Oracle Database Firewall Bundle Patch 5 (Patch 13077854) before upgrading from release 5.0 to 5.1.

3.2 Overview of the Upgrade Procedure

The upgrade procedure is done in the three stages detailed in the following sections. If you have a Management Server, perform all three of these stages on the Management Server first, then on the Database Firewall:

- [Upgrading the Base Platform](#)
- [Upgrading the Oracle Database Firewall or Management Server](#)
- [Upgrading the Embedded Oracle Database](#)

Caution: Be sure that your configuration and data backups are up-to-date before performing the upgrade procedure.

3.3 Upgrading the Base Platform

To upgrade the base platform:

1. Log in to the Database Firewall or Management Server as `root`.
2. Insert Oracle Database Firewall 5.1 installation disk 1, and mount using the command:

```
mount /dev/cdrom /mnt
```

3. Create a `/tmp/disk1.repo` file, and insert the following in this file:

```
[DBFW-disk1]
name=DBFW Platform update
baseurl=file:///mnt/secerno/updates
enabled=1
gpgcheck=0
```

4. Execute the command:

```
yum -y update -c /tmp/disk1.repo
--disablerepo=secerno-updates
```

Inspect the output for errors.

5. Unmount Disk 1 using the command:

```
umount /mnt
```

6. Remove the disk from the drive.

3.4 Upgrading the Oracle Database Firewall or Management Server

Note: If you have managed Database Firewalls, first upgrade the Management Server, then the Database Firewalls.

To upgrade the Oracle Database Firewall or Management Server:

1. Insert Oracle Database Firewall 5.1 installation Disk 2, and mount using the command:

```
mount /dev/cdrom /mnt
```

2. Copy the RPM file that matches your platform from Disk 2 to the Database Firewall or Management Server.

The RPM file is in the `root` directory on Disk 2.

3. Apply the RPM by running the command:


```
rpm --freshen --repackage RPM_File
```
4. Unmount Disk 2 using the command:


```
umount /mnt
```
5. Reboot the Database Firewall or Management Server.

Note: Check console 9 for additional booting messages.
6. To verify this procedure:
 - a. Log in to the Database Firewall or Management Server Administration Console, and check that it displays version 5.1.
 - b. Run one of the following commands and verify that version 5.1 is displayed.

For a Database Firewall, run: `rpm -q dbfw-multi`

For a Management Server, run: `rpm -q dbfw-mgmtsvr`
 - c. Run the command:


```
uname -r
```

The output should be: 2.6.18-274.3.1.0.1.e15PAE or later.

3.5 Upgrading the Embedded Oracle Database

To upgrade the embedded Oracle Database:

1. Insert Oracle Database Firewall 5.1 installation Disk 3.
2. As user `root`, mount using the command:


```
mount /dev/cdrom /mnt
```
3. Shutdown the following Database Firewall or Management Server system services:


```
/etc/init.d/monitor stop
/etc/init.d/dbfw stop
/etc/init.d/controller stop
/etc/init.d/stund stop
/etc/init.d/dbfwlistener stop
/etc/init.d/dbfwdb stop
```
4. Switch to user `oracle`:


```
su - oracle
```
5. Run the command:


```
. /var/lib/oracle/dbfw/bin/oraenv
```

Specify `dbfwdb` when prompted.
6. Install the `opatch` utility update:


```
cd $ORACLE_HOME
unzip /mnt/updates/opatch/p6880880_112000_LINUX.zip
```

If prompted, select to replace all files in this directory.

7. Check that the opatch utility was successfully installed by running the command:

```
/var/lib/oracle/dbfw/OPatch/patch version
```

Version 11.2.0.1.6 should be displayed.
8. Unzip the PSU zip file:

```
unzip /mnt/updates/psu/p12419331_112020_LINUX.zip -d /tmp
```
9. Change directory:

```
cd /tmp/12419331
```
10. In the /tmp/12419331 apply the patch using the command:

```
/var/lib/oracle/dbfw/OPatch/patch apply
```

If there are errors, see the patch documentation.
11. Exit, and start the Oracle database as user root:

```
/etc/init.d/dbfwdb start  
/etc/init.d/dbfwlistener start
```
12. Switch to user oracle:

```
su - oracle
```
13. Run the command:

```
./var/lib/oracle/dbfw/bin/oraenv
```

Specify dbfwdb when prompted.
14. Upgrade existing databases:

```
sqlplus /nolog  
SQL> CONNECT / AS SYSDBA  
SQL> @/var/lib/oracle/dbfw/rdbms/admin/catbundle.sql psu apply  
SQL> QUIT
```
15. In the directory \$ORACLE_BASE/cfgtoollogs/catbundle, check the following files for errors. The *timestamp* is the actual time:

```
catbundle_PSU_database_SID_APPLY_timestamp.log  
catbundle_PSU_database_SID_GENERATE_timestamp.log
```
16. Reboot the system.
Note: Check console 9 for additional booting messages.
17. Verify that the Oracle database was upgraded correctly:
 - a. Log in as user Oracle, and run the command:

```
./var/lib/oracle/dbfw/bin/oraenv
```

Specify dbfwdb when prompted.
 - b. Log in to the database:

```
sqlplus sys as sysdba
```
 - c. Check the dba_registry_history table:

```
select * from dba_registry_history
```

Verify that patch set update 11.2.0.2.3 is mentioned.

4 Known Issues

The system has the following known issues:

- [Enabling or Disabling Local Monitor in DPE Mode Terminates Database Sessions](#)
- [Booting Message Is Not Displayed During Upgrade](#)
- [Update from Disc 1 Fails if Run a Second Time During Upgrade](#)

4.1 Enabling or Disabling Local Monitor in DPE Mode Terminates Database Sessions

If you enable or disable Local Monitor from a protected database being monitored in DPE mode, any existing database sessions terminate.

This issue is tracked with Oracle bug 11859598.

4.2 Booting Message Is Not Displayed During Upgrade

After the first stage of the upgrade procedure (upgrading the base platform), the booting Database Firewall message is not displayed. To see the complete booting messages, check console 9.

This issue is tracked with Oracle bug 13461821.

4.3 Update from Disc 1 Fails if Run a Second Time During Upgrade

During stage one of the upgrade (upgrading the base platform), once you execute the command in Step 4 (`yum -update . . .`), if you then run this command another time, for example if you use a different Disc 1, the update fails.

The workaround is to run the following command before you run the `yum -update . . .` command again:

```
yum clean all -c /tmp/disk1.repo --disablerepo=secerno-updates
```

This issue is tracked with Oracle bug 13452515.

5 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are

hearing impaired.

Oracle Database Firewall Release Notes, Release 5.1 for Oracle Linux
E22689-03

Copyright © 2003, 2011, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. 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, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.