Oracle® Database Firewall

Release Notes

Release 5.0 for Oracle Linux

E18694-04

September 2011

These *Release Notes* contain important information that was not included in the Oracle Database Firewall Release 5.0 documentation. They apply to Oracle Database Firewall on all platforms.

This document contains the following sections:

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 Known Issues

This section contains:

2.1 Oracle Database Firewall Management Server Operation

Certain long running operations, such as deleting large amounts of traffic log data, may interfere with the Management Server Administration Console. Wait until these operations are complete before performing administration tasks.

Performing a Configuration Restore job will delete any Archive Jobs that have been made previously.

2.2 JavaScript Disabled in High Availability Environment

In a High Availability environment where a user's browser has JavaScript disabled, the user must manually refresh the Appliances List page to obtain the status of the appliances.

2.3 Paired Oracle Database Firewalls on High Availability Environment Must Run on Identical Hardware Specifications

When you configure a High Availability environment, ensure that the specifications of the hardware used for paired Database Firewalls are identical.

2.4 Must Turn Off IP Spoofing Detection for Database Firewall System in DPE Mode with Firewall Between It and the Network

When you use a Database Firewall system in DPE mode, with a Database Firewall between it and the rest of the network, you must turn off any IP spoofing detection rules in the Database Firewall.

2.5 Database Firewall May Route Responses Out of Wrong Interface

Where the Database Firewall Management Server and the Bridge are connected to physically separate networks which are on the same subnet, Database Firewall may route responses out of the wrong interface. If physically separate networks are required, use different subnets.

2.6 Must Reboot if Upgrading an Installation with a Patch

When you upgrade an existing installation using a patch, you must restart the upgraded system after you install the patch. This ensures that all services can restart.

2.7 Archive Traffic Logs to Avoid Loss when Restoring a Configuration

The system overwrites the existing configuration when you restore a configuration. This can lead to traffic logs being removed. If you merge an old configuration with current traffic logs, archive the data, restore the configuration, and then restore the data.

2.8 Restoring Previously Archived Traffic Log Data

When you restore previously archived traffic log data to a system using the Restore functionality, determine whether or not these log files must be associated with a monitoring point. You can do this from the Repair Menu option in the System menu.

2.9 Avoid Creating More than One Protected Database Using Same Database Details

Do not create two or more protected databases containing the same database details (IP address and port number). This can cause problems with report generation.

2.10 Enabling or Disabling Local Monitor in Database in DPE Terminates Existing Database Sessions

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

2.11 syslog Does Not Log More than 1000 Messages Per Minute for Protected Databases

If a protected database being monitored receives more than 1000 alerts in one minute, subsequent alerts are not shown in the syslog messages. In this event, the following message is written to the syslog,:

```
WARN - More than 1000 alerts in the last minute. Subsequent alerts will not be
processed.
```

2.12 Database Firewall Time Configurations must be Correct for the Analyzer to use Correct Time Ranges

When you configure Database Firewall, ensure that the System Time and Time Offset are set correctly so that Database Firewall Analyzer uses the correct time ranges when training on log data.

2.13 Log Search Result Show Percentage Complete Based on Total Logged Statements

When you generate log search results, the percentage complete figure shown is based on the total number of statements that have been logged rather than the maximum results value specified when defining the Log Search Result.

2.14 If DNS Configuration Is Broken, It Can Prevent Local Monitor Forward and Reverse DNS Lookup

Local Monitor does both a forward and reverse DNS lookup to determine if a session is from the local machine. If a DNS configuration is broken and prevents the server from doing the lookup successfully, then the Local Monitor cannot record console events. To ensure that Local Monitor records all local sessions, check that your DNS configuration is correct.

2.15 Link Light

Database Firewall may not show a link light when connected to certain switches, for example, Cisco 2900. To ensure connectivity, in the **System Settings** menu on the **System** tab, set the link properties to use a manual setting rather than the **Autonegotiated** setting.

2.16 Ensure that tempdb Database is Large Enough

For Sybase ASE stored procedure auditing, the `tempdb` database must be large enough to accommodate the generated temp files. To check this, perform the following steps:

1. Run the `sp_helpdb` system stored procedure.
2. Compare the `db_size` columns for the `sybsystemproc` and `tempdb` databases.

   The `tempdb` database should be larger than `sybsystemproc`, at least by a couple of MBs.

2.17 When Setting Database Firewall to DPE all Connections to the Database Must Reconnect

When you set a Database Firewall to DPE mode (through Enforcement Point Settings or by restarting a Database Firewall with network passthrough), ensure that all connections to the database are forced to reconnect. In addition, in DPE mode, if you change Enforcement Point Settings, you must also force all database connections to reconnect.

2.18 Certain Novelty Policies Not Enabled for Oracle Database Firewall Release 5.0

Novelty policies in Oracle Database Firewall Release 5.0 do not allow the action warn or escalations. If baseline policies are loaded from Oracle Database Firewall Release 4.3 or earlier, with these options enabled, the Analyzer will update the policy. Ensure that the changes to your Novelty Policies are correct.

2.19 Need Uppercase for Novelty Policies and Sensitive Field Masking in Oracle Database Firewall Prior to Release 5.0

For any baselines created with Oracle Database Firewall prior to Release 5.0, you must manually update the following to ensure that all names are uppercase:

- Sensitive field masking
- Novelty policies based on table, column, or procedure names

2.20 Error in syslog after Update

The following error may appear in the `syslog` after an update:

```
WARN - Failed to connect to database:ORA-12541: TNS:no listener
```

If this error appears, then run the following commands as the `root` user:

```
. oraenvs
lsnrctl start
```

2.21 Traffic Log Mode Performance Issue on High Throughput Systems

Do not use Traffic log diagnostic mode on high throughput systems. (To find this mode, in either the Management Server or the standalone Database Firewall Administration Console, select the **Reporting** tab, and then from the **Traffic Log** menu, select **View**.) Doing so decreases the performance of the Oracle Database Firewall system.

3 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 5.0 for Oracle Linux
E18694-04