LAB 2: Configuring Oracle Database Firewall

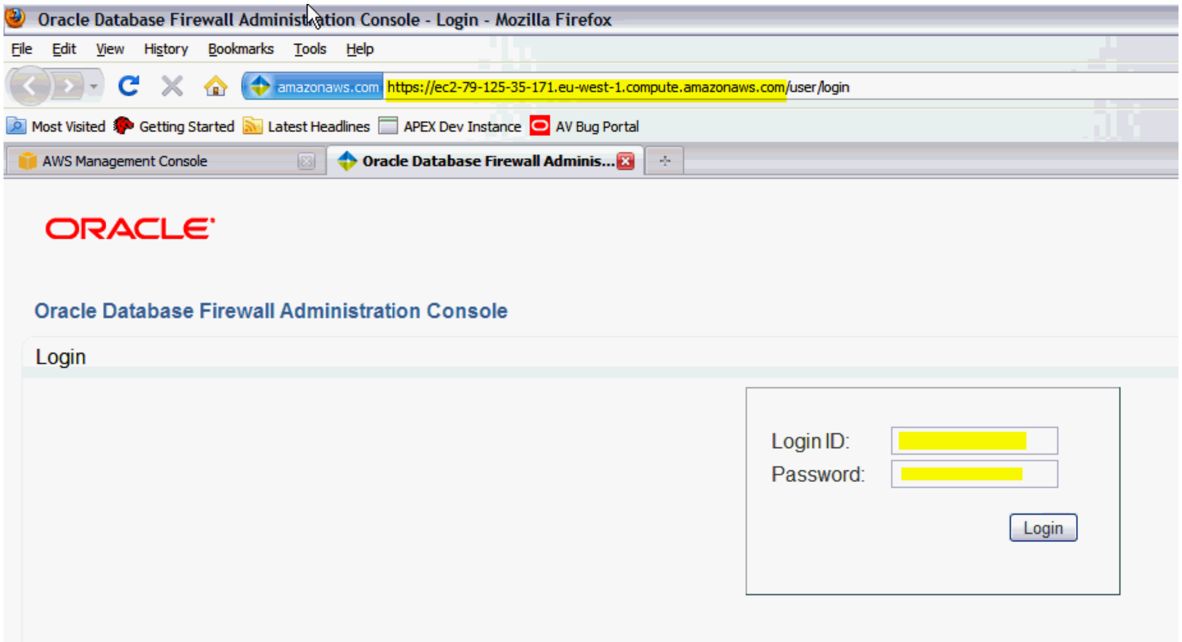
1. System Setting

For full details on the System settings, see Chapter 2 : Configuring the Database Firewall System in the Deployment and Administration Guide.

2. Configuring your Oracle Database Firewall

To access your Oracle Database Firewall, use your WinClient virtual machine enter the IP Address into your browser using https:

https://<your Oracle Database Firewall IP Address>



Oracle Database Firewall Administration Console - Login - Mozilla Firefox

https://ec2-79-125-35-171.eu-west-1.compute.amazonaws.com/user/login

Oracle Database Firewall Administration Console

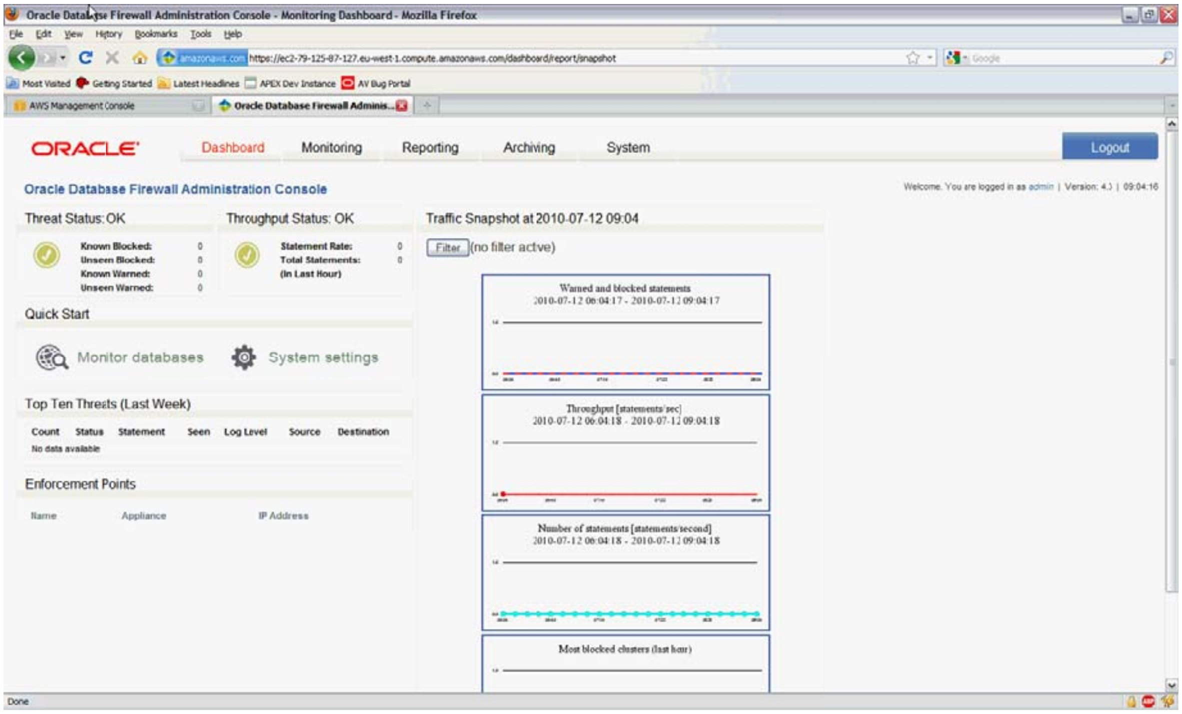
Login

Login ID:

Password:

Login using the ID: admin and password: oracle (or the password you changed it to)

A. Create Yourself!



Oracle Database Firewall Administration Console - Monitoring Dashboard - Mozilla Firefox

https://ec2-79-125-87-127.eu-west-1.compute.amazonaws.com/dashboard/report/snapshot

Oracle Database Firewall Administration Console

Welcome. You are logged in as admin | Version: 4.3 | 09:04:16

Threat Status: OK

Known Blocked: 0
Unseen Blocked: 0
Known Warned: 0
Unseen Warned: 0

Throughput Status: OK

Statement Rate: 0
Total Statements: 0
(In Last Hour)

Traffic Snapshot at 2010-07-12 09:04

Filter (no filter active)

Quick Start

Monitor databases System settings

Top Ten Threats (Last Week)

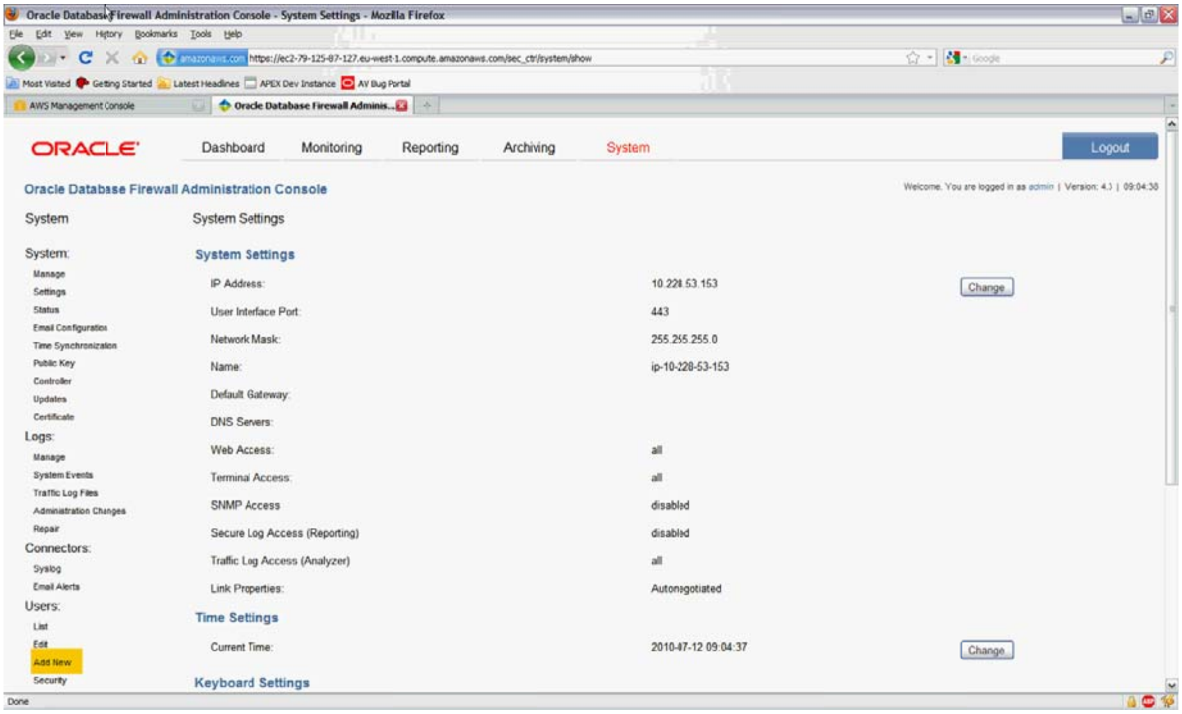
Count	Status	Statement	Seen	Log Level	Source	Destination
No data available						

Enforcement Points

Name	Appliance	IP Address

Warned and blocked statements
2010-07-12 06:04:17 - 2010-07-12 09:04:17
Throughput [statements/sec]
2010-07-12 06:04:18 - 2010-07-12 09:04:18
Number of statements [statements/second]
2010-07-12 06:04:18 - 2010-07-12 09:04:18
Most blocked clusters (last hour)

1. Click on System Tab, on left hand side under ‘Users’, click on ADD NEW



Oracle Database Firewall Administration Console - System Settings - Mozilla Firefox

https://ec2-79-125-87-127.eu-west-1.compute.amazonaws.com/sec_ctr/system/show

Oracle Database Firewall Administration Console

Welcome. You are logged in as admin | Version: 4.3 | 09:04:38

System Settings

System Settings

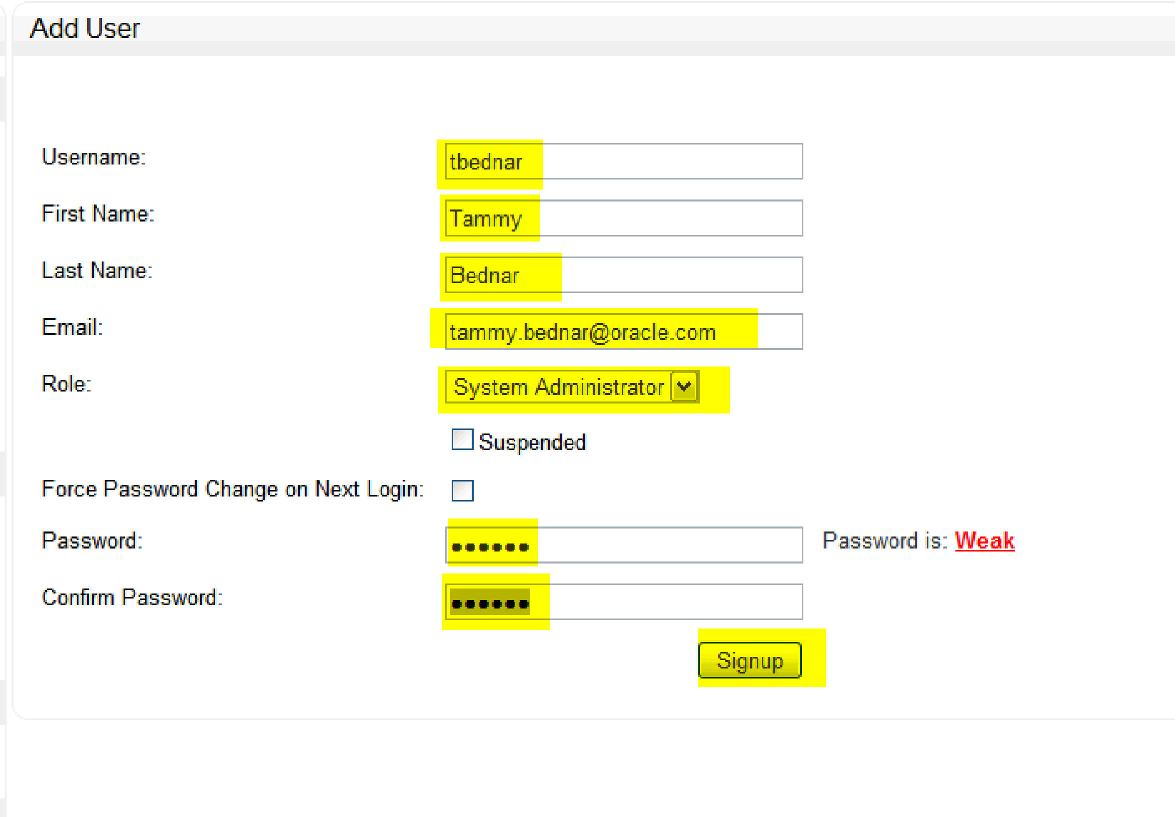
IP Address: 10.228.53.153
User Interface Port: 443
Network Mask: 255.255.255.0
Name: ip-10-228-53-153
Default Gateway:
DNS Servers:
Web Access: all
Terminal Access: all
SNMP Access: disabled
Secure Log Access (Reporting): disabled
Traffic Log Access (Analyzer): all
Link Properties: Autonegotiated

Time Settings

Current Time: 2010-07-12 09:04:37

Keyboard Settings

2. Substitute **YOUR** information in the example below and press Signup.



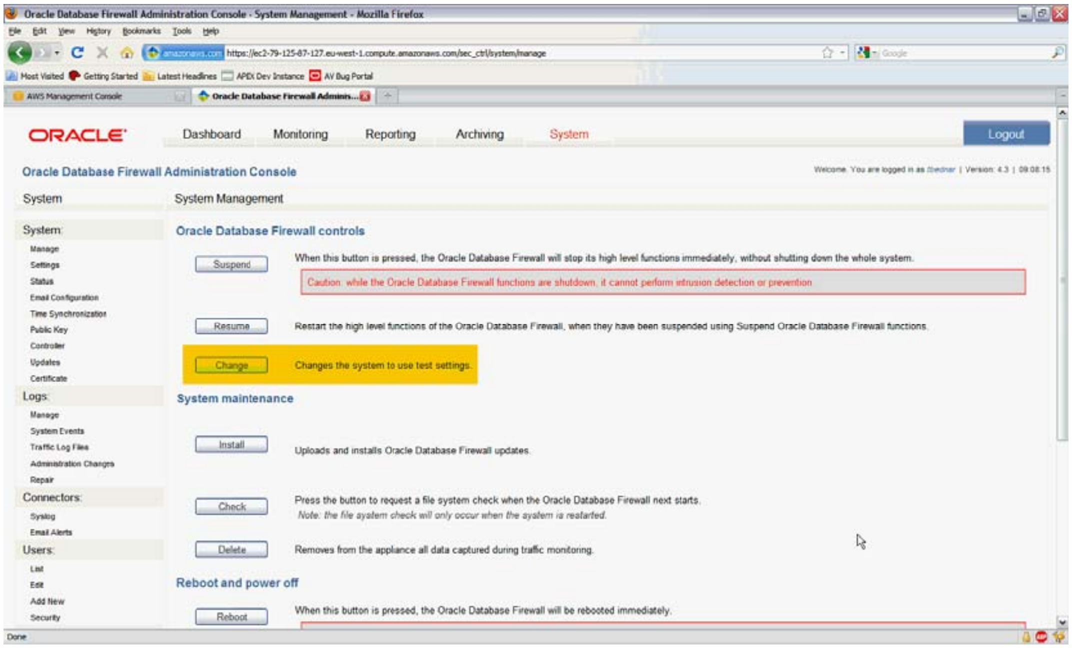
Add User

Username:	tbednar
First Name:	Tammy
Last Name:	Bednar
Email:	tammy.bednar@oracle.com
Role:	System Administrator
	□ Suspended
Force Password Change on Next Login:	□
Password:	•••••• Password is: Weak
Confirm Password:	••••••

3. Logout and log back in with your credentials.

B. Set Test Mode on

1. Click on System tab, then on Manage on the left under System



Oracle Database Firewall Administration Console

Welcome. You are logged in as tbednar | Version: 4.3 | 09:08:15

System Management

Oracle Database Firewall controls

When this button is pressed, the Oracle Database Firewall will stop its high level functions immediately, without shutting down the whole system.

Caution: while the Oracle Database Firewall functions are shutdown, it cannot perform intrusion detection or prevention

Restart the high level functions of the Oracle Database Firewall, when they have been suspended using Suspend Oracle Database Firewall functions.

Changes the system to use test settings.

System maintenance

Uploads and installs Oracle Database Firewall updates.

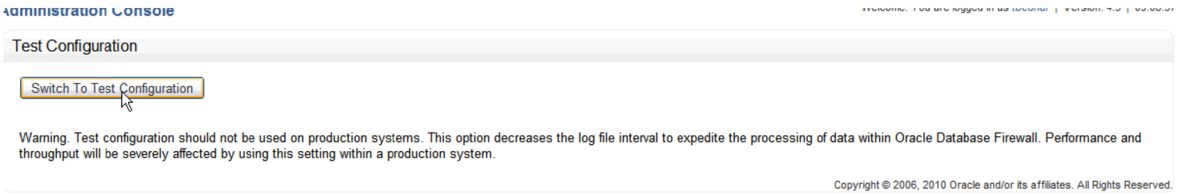
Press the button to request a file system check when the Oracle Database Firewall next starts.
Note: the file system check will only occur when the system is restarted.

Removes from the appliance all data captured during traffic monitoring.

Reboot and power off

When this button is pressed, the Oracle Database Firewall will be rebooted immediately.

Click on Switch to Test Configuration



Administration Console

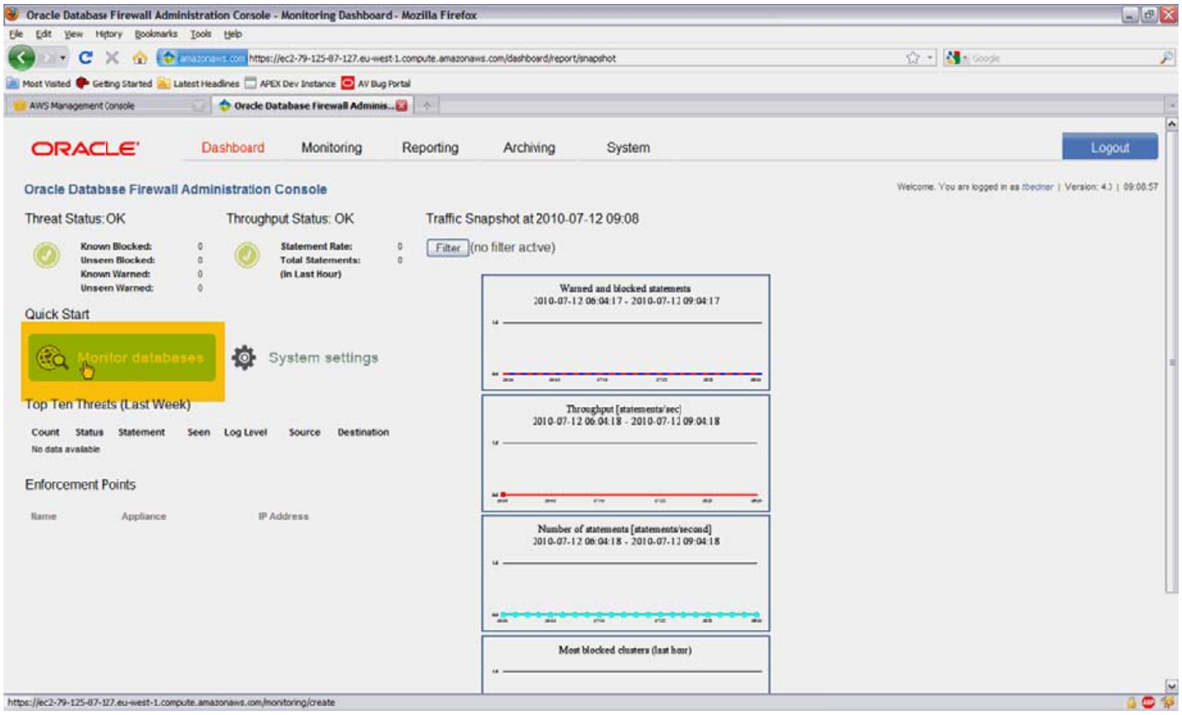
Test Configuration

Warning. Test configuration should not be used on production systems. This option decreases the log file interval to expedite the processing of data within Oracle Database Firewall. Performance and throughput will be severely affected by using this setting within a production system.

Copyright © 2006, 2010 Oracle and/or its affiliates. All Rights Reserved.

C. Configure an Enforcement Point

1. Click on Dashboard tab, Monitor Databases


Oracle Database Firewall Administration Console - Monitoring Dashboard - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://ec2-79-125-87-127.eu-west-1.compute.amazonaws.com/dashboard/report/snapshot
Most Visited Getting Started Latest Headlines APEX Dev Instance AV Bug Portal
AWS Management Console
Oracle Database Firewall Adminis...
ORACLE
Dashboard
Monitoring
Reporting
Archiving
System
Logout
Monitor databases
System settings
Filter
Warned and blocked statements
2010-07-12 06:04:17 - 2010-07-12 09:04:17
Throughput [statements/sec]
2010-07-12 06:04:18 - 2010-07-12 09:04:18
Number of statements [statements/second]
2010-07-12 06:04:18 - 2010-07-12 09:04:18
Most blocked clusters (last hour)
https://ec2-79-125-87-127.eu-west-1.compute.amazonaws.com/monitoring/create

Oracle Database Firewall Administration Console

Welcome. You are logged in as tbednar | Version: 4.3 | 09:08:57

Threat Status: OK

Known Blocked:	0
Unseen Blocked:	0
Known Warned:	0
Unseen Warned:	0

Throughput Status: OK

Statement Rate:	0
Total Statements: (In Last Hour)	0

Traffic Snapshot at 2010-07-12 09:08

(no filter actve)

Quick Start

Top Ten Threats (Last Week)

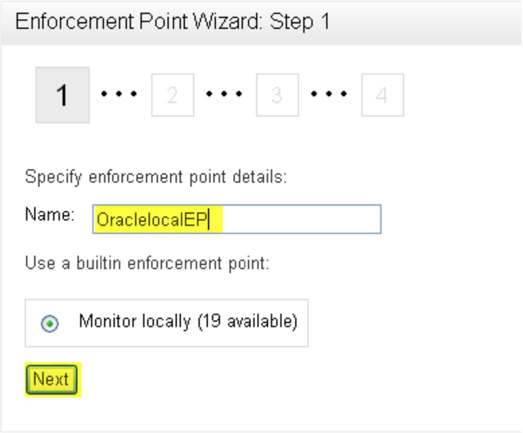
Count	Status	Statement	Seen	Log Level	Source	Destination
No data available						

Enforcement Points

Name	Appliance	IP Address

2. Enter the name of the Enforcement Point.

   Name: DbsecEP



Enforcement Point Wizard: Step 1

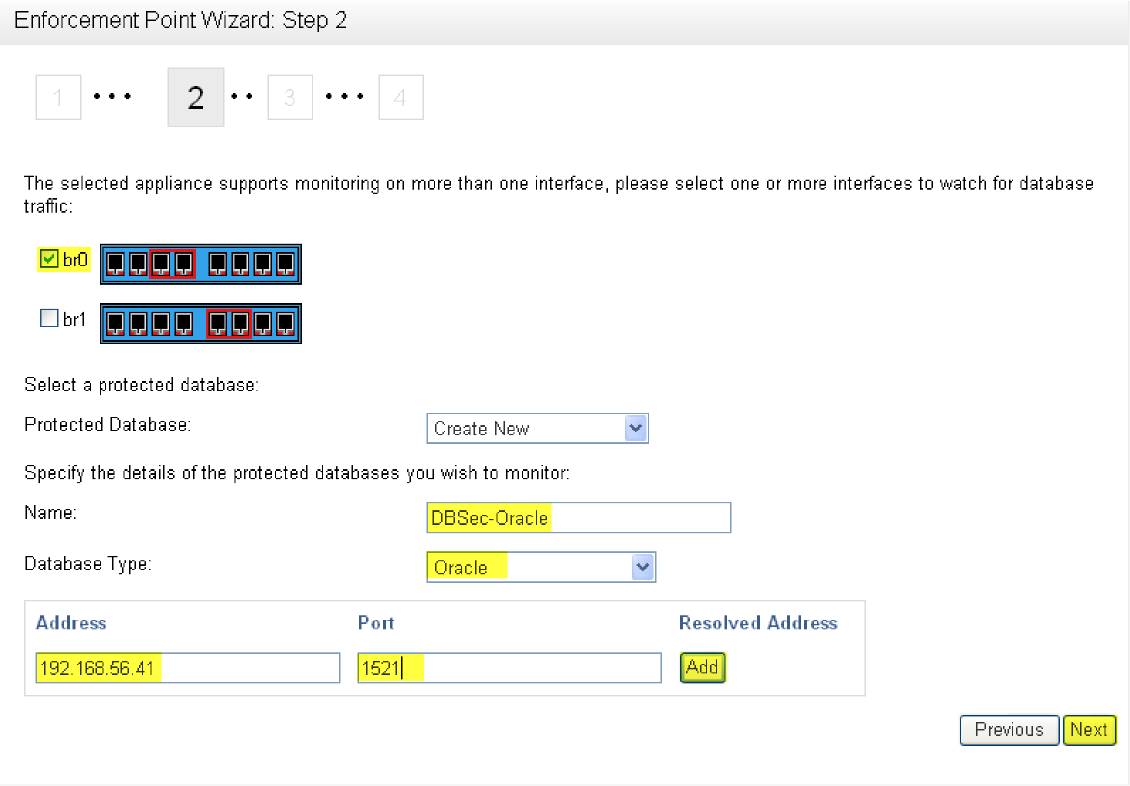
Specify enforcement point details:

Name: OraclelocalEP

Use a builtin enforcement point:

● Monitor locally (19 available)

3. Select br0 as the traffic source. Enter a name for the database that will be protected, select the database type. Enter the IP address the Oracle database security image and port 1521. Click ‘Add’, then Next.



Enforcement Point Wizard: Step 2

The selected appliance supports monitoring on more than one interface, please select one or more interfaces to watch for database traffic:

☑ br0

□ br1

Select a protected database:

Protected Database: Create New

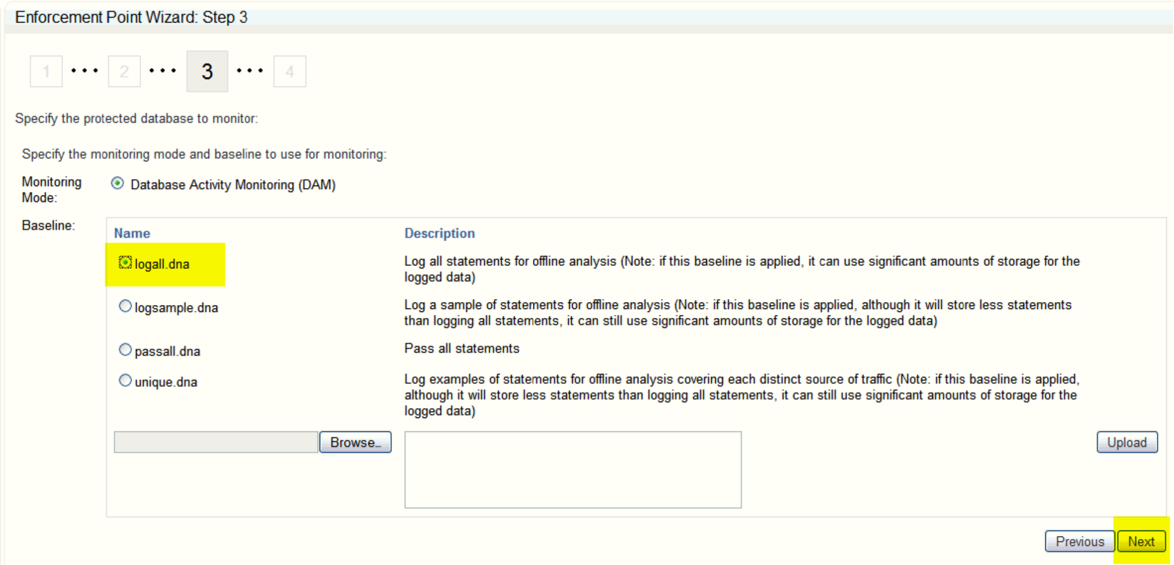
Specify the details of the protected databases you wish to monitor:

Name: DBSec-Oracle

Database Type: Oracle

Address	Port	Resolved Address
192.168.56.41	1521	Add

4. Select the log all policy and click on Next.



Enforcement Point Wizard: Step 3

Specify the protected database to monitor:

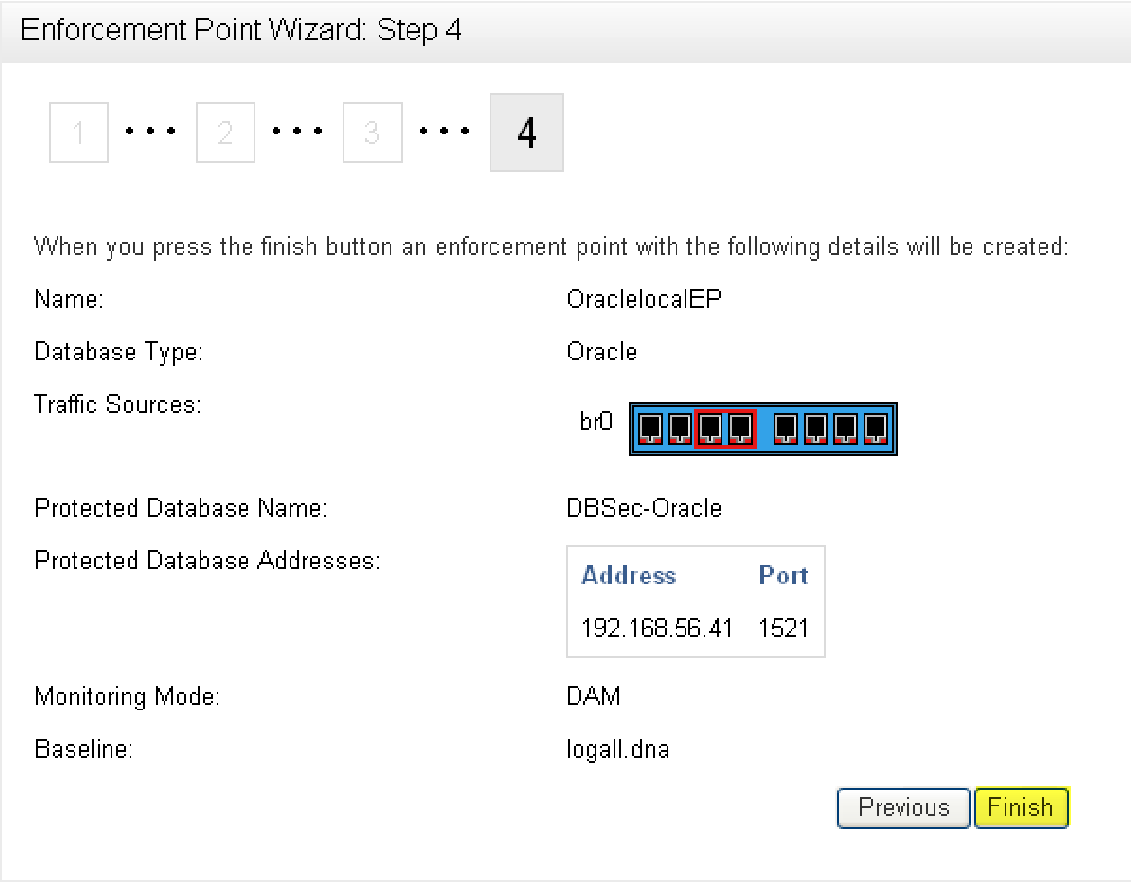
Specify the monitoring mode and baseline to use for monitoring:

Monitoring Mode: ● Database Activity Monitoring (DAM)

Baseline:

Name	Description
● logall.dna	Log all statements for offline analysis (Note: if this baseline is applied, it can use significant amounts of storage for the logged data)
○ logsample.dna	Log a sample of statements for offline analysis (Note: if this baseline is applied, although it will store less statements than logging all statements, it can still use significant amounts of storage for the logged data)
○ passall.dna	Pass all statements
○ unique.dna	Log examples of statements for offline analysis covering each distinct source of traffic (Note: if this baseline is applied, although it will store less statements than logging all statements, it can still use significant amounts of storage for the logged data)

5. Check the details are correct and click on Finish.



Enforcement Point Wizard: Step 4

When you press the finish button an enforcement point with the following details will be created:

Name: OraclelocalEP

Database Type: Oracle

Traffic Sources: br0

Protected Database Name: DBSec-Oracle

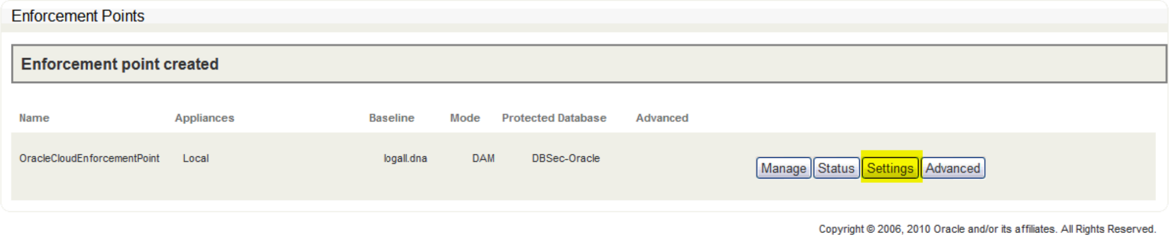
Protected Database Addresses:

Address	Port
192.168.56.41	1521

Monitoring Mode: DAM

Baseline: logall.dna

6. On the Enforcement Point you have just created, click on Settings to set additional options.



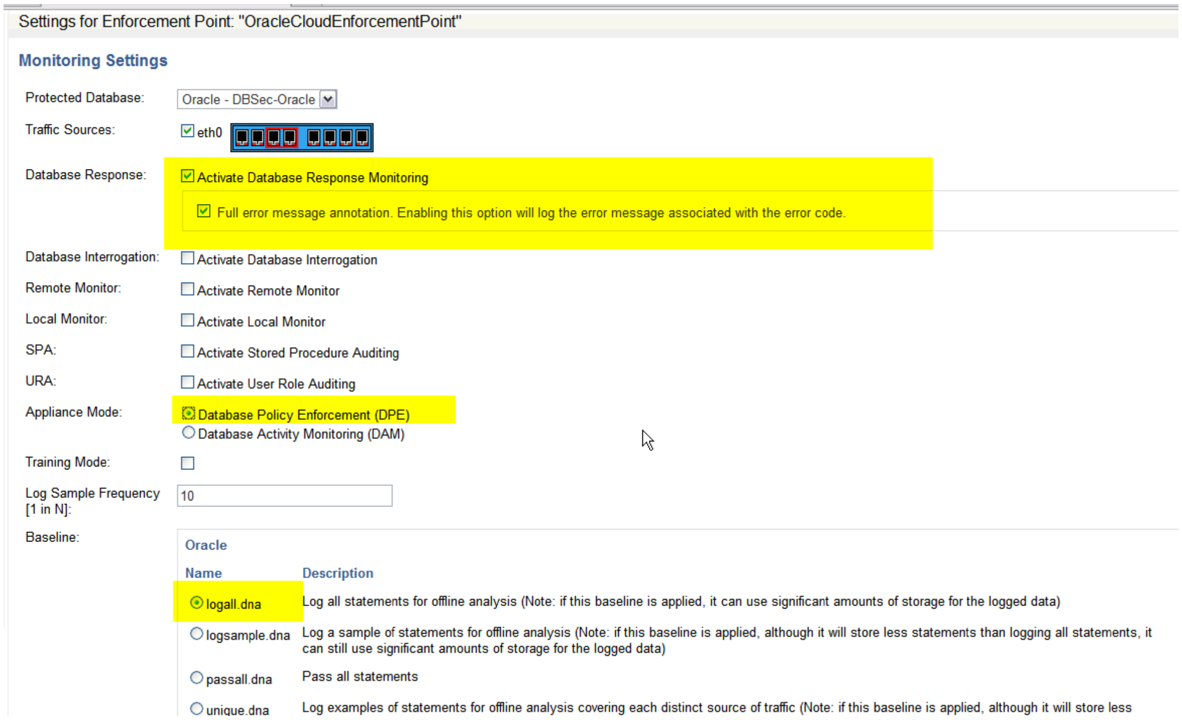
Enforcement Points

Enforcement point created

Name	Appliances	Baseline	Mode	Protected Database	Advanced
OracleCloudEnforcementPoint	Local	logall.dna	DAM	DBSec-Oracle	Manage Status Settings Advanced

Copyright © 2006, 2010 Oracle and/or its affiliates. All Rights Reserved.

7. Select Activate Database Response Monitoring and Full error message annotation. Switch the Enforcement Point into blocking mode by selecting DPE.



Settings for Enforcement Point: "OracleCloudEnforcementPoint"

Monitoring Settings

Protected Database: Oracle - DBSec-Oracle

Traffic Sources: ☑ eth0

Database Response: ☑ Activate Database Response Monitoring

☑ Full error message annotation. Enabling this option will log the error message associated with the error code.

Database Interrogation: □ Activate Database Interrogation

Remote Monitor: □ Activate Remote Monitor

Local Monitor: □ Activate Local Monitor

SPA: □ Activate Stored Procedure Auditing

URA: □ Activate User Role Auditing

Appliance Mode: ● Database Policy Enforcement (DPE)
○ Database Activity Monitoring (DAM)

Training Mode: □

Log Sample Frequency [1 in N]: 10

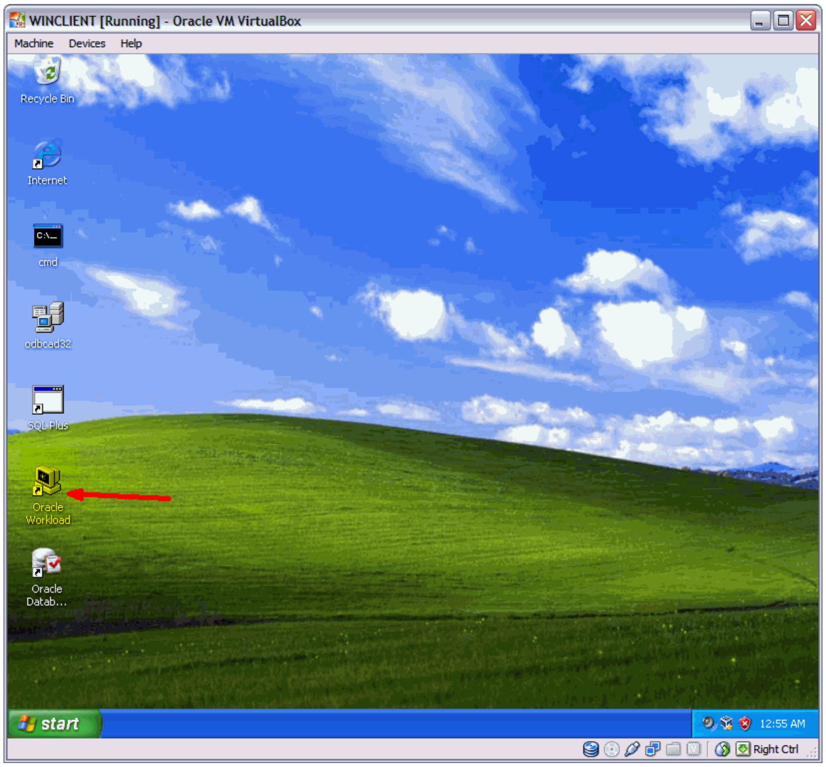
Baseline:

Oracle

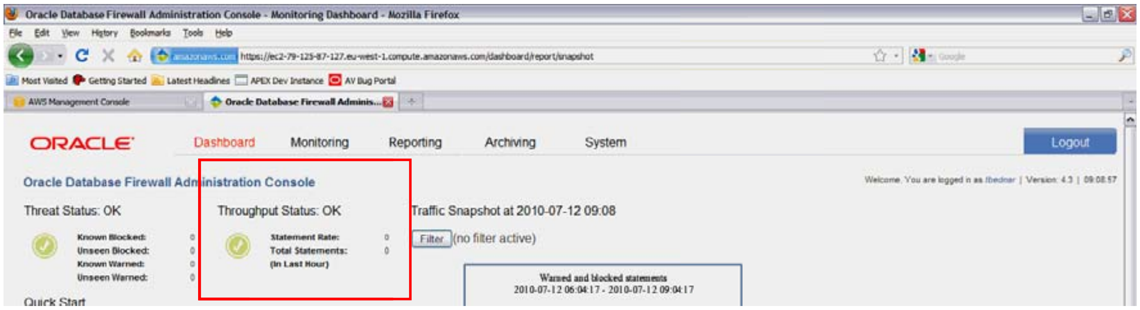
Name	Description
● logall.dna	Log all statements for offline analysis (Note: if this baseline is applied, it can use significant amounts of storage for the logged data)
○ logsample.dna	Log a sample of statements for offline analysis (Note: if this baseline is applied, although it will store less statements than logging all statements, it can still use significant amounts of storage for the logged data)
○ passall.dna	Pass all statements
○ unique.dna	Log examples of statements for offline analysis covering each distinct source of traffic (Note: if this baseline is applied, although it will store less

Click on Save.

8. In the WindowsClient, Run Oracle Workload.



9. Go to Database Firewall Dashboard to see if any statements have been collected.



Oracle Database Firewall Administration Console - Monitoring Dashboard - Mozilla Firefox
File Edit View History Bookmarks Tools Help
amazonaws.com https://ec2-79-125-87-127.eu-west-1.compute.amazonaws.com/dashboard/report/snapshot
Google
Most Visited Getting Started Latest Headlines APEX Dev Instance AV Bug Portal
AWS Management Console
Oracle Database Firewall Adminis...
ORACLE
Dashboard
Monitoring
Reporting
Archiving
System
Logout
Filter

Oracle Database Firewall Administration Console

Welcome. You are logged in as lbednar | Version: 4.3 | 09:08:57

Threat Status: OK

Known Blocked:	0
Unseen Blocked:	0
Known Warned:	0
Unseen Warned:	0

Throughput Status: OK

Statement Rate:	0
Total Statements: (In Last Hour)	0

Traffic Snapshot at 2010-07-12 09:08

(no filter active)

Warned and blocked statements
2010-07-12 06:04:17 - 2010-07-12 09:04:17

Quick Start