ORACLE®

SECURE DATA AT THE SOURCE
SAVE TIME AND MONEY

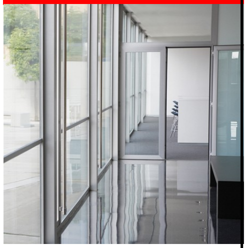
Security Inside Out

Oracle Database Security

ORACLE®

Oracle Database Firewall 5.1 & Audit Vault 10.3 Update

Program Agenda



- Audit Vault 10.3
  - New Features
  - Customer Update
- Database Firewall 5.1
  - New Features
  - PoC Guide Updates
- Summary
- Q&A

Audit Vault 10.3 New Features

- Update Database Repository to use Oracle Database 11.2.0.3
  - Simplified installation process
- New Installer for the Audit Vault Server with options to install software only for setting up Data Guard or move Server to a new host
- Added Database Certification
  - Sybase ASE 15.5 & 15.7, DB2 9.7
- Secure by default for HTTP for Audit Vault Console
- In-place Upgrade from Audit Vault 10.2.3.2.6 to 10.3
- Can be installed on Exadata and Oracle Database Appliance

Audit Vault 10.3 New Features

- Linux 64 available now
- Additional Server and Agents will be available end of Jan 2012
  - Server Platforms
    - AIX, HP-UX Itanium, Solaris SPARC
  - Agent Platforms
    - AIX, HP-UX Itanium, HP-UX PA-RISC, Windows 64 (2008, 2008 R2), Solaris SPARC

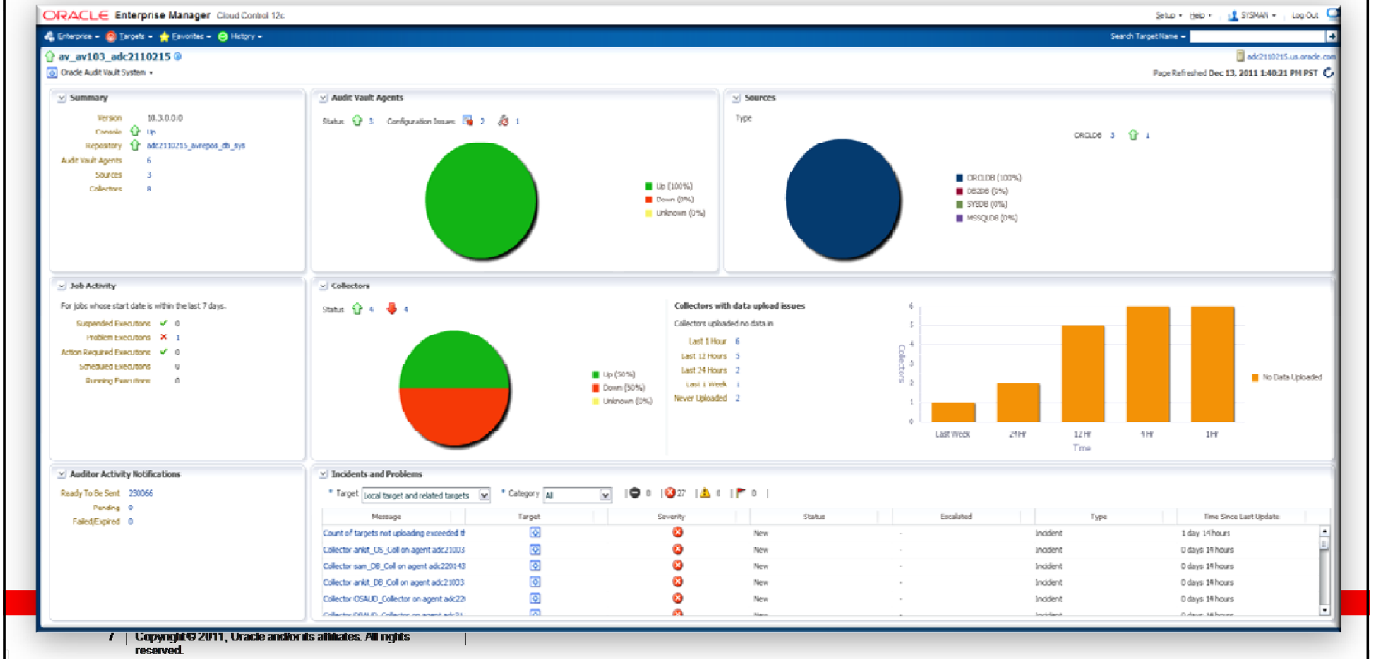
ORACLE

Audit Vault EM Plug-In – Target Jan 2012

- Added Audit Vault target types to Enterprise Manager
  - Audit Vault Server, Audit Vault Agent
- Monitor and manage the health of your environment
  - Startup / Shutdown
  - Up / Down Status
  - Alert when metrics are out of policy
  - Number of audit records collected
- View Audit Vault enterprise topology
- Must use Audit Vault 10.3 and EM 12.1 Cloud Control

ORACLE

Audit Vault Plug-in Dashboard



av_av103_adc2110215

Oracle Audit Vault System ▾

adc2110215.us.oracle.com

Page Refreshed Dec 13, 2011 1:40:31 PM PST

Summary

Version	10.3.0.0.0
Console	Up
Repository	adc2110215_avrepos_db_sys
Audit Vault Agents	6
Sources	3
Collectors	8

Audit Vault Agents

Status 5 Configuration Issues: 2 1

Sources

Type

ORACLE 3 1

Job Activity

For jobs whose start date is within the last 7 days.

Suspended Executions	✓	0
Problem Executions	✗	1
Action Required Executions	✓	0
Scheduled Executions		0
Running Executions		0

Collectors

Status 4 4

Collectors with data upload issues

Collectors uploaded no data in

Last 1 Hour	6
Last 12 Hours	5
Last 24 Hours	2
Last 1 Week	1
Never Uploaded	2

Auditor Activity Notifications

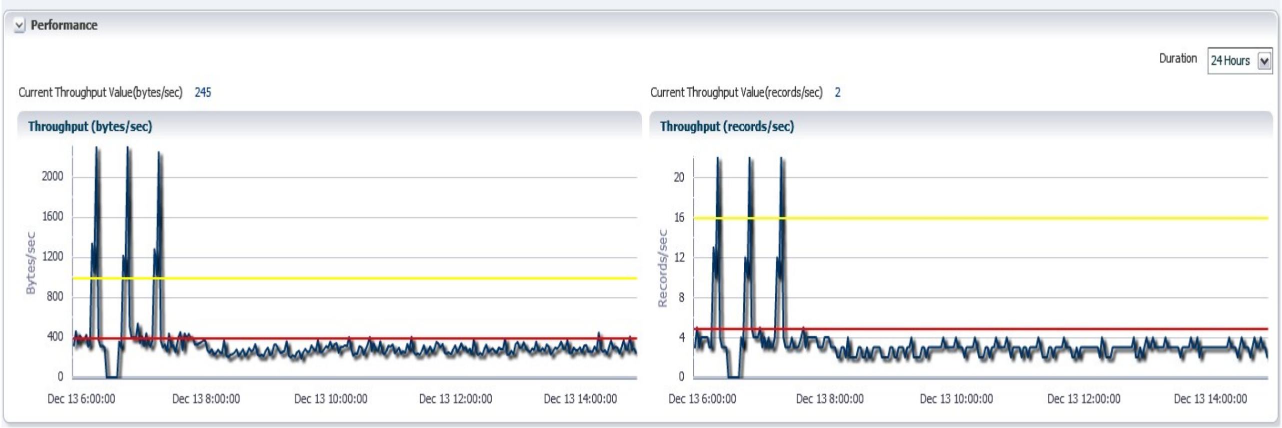
Ready To Be Sent	230066
Pending	0
Failed/Expired	0

Incidents and Problems

* Target Local target and related targets * Category All | 0 | 27 | 0 | 0 |

Message	Target	Severity	Status	Escalated	Type	Time Since Last Update
Count of targets not uploading exceeded th		✗	New	-	Incident	1 day 14 hours
Collector ankit_US_Coll on agent adc21003		✗	New	-	Incident	0 days 14 hours
Collector sam_DB_Coll on agent adc220143		✗	New	-	Incident	0 days 14 hours
Collector ankit_DB_Coll on agent adc21003		✗	New	-	Incident	0 days 14 hours
Collector OSAUD_Collector on agent adc22		✗	New	-	Incident	0 days 14 hours

Audit Vault Plug-in
Collector State and Performance



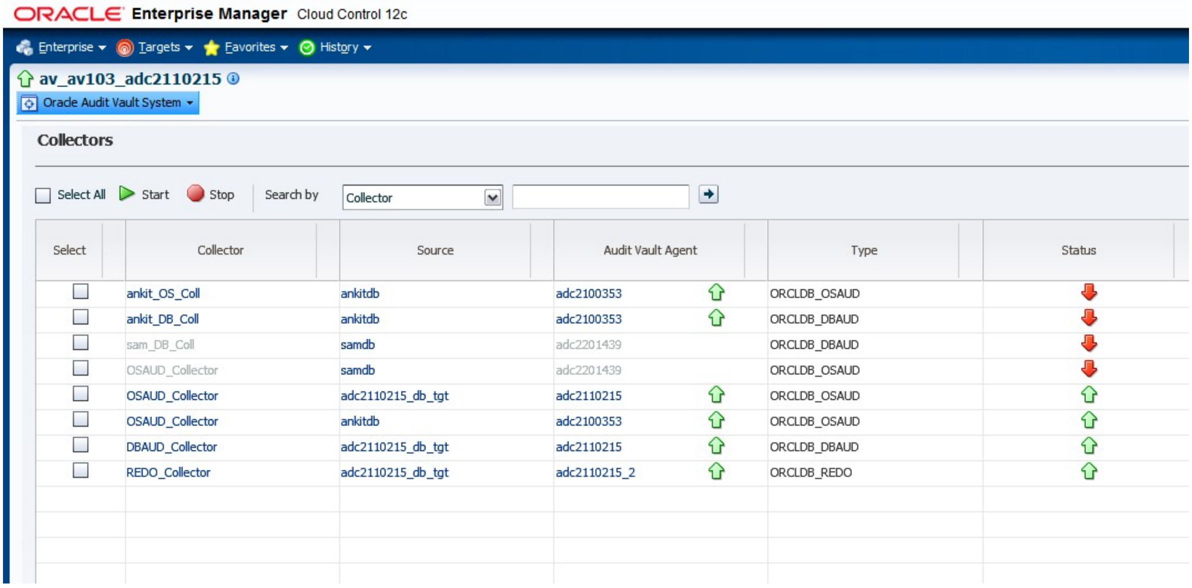
Performance

Duration 24 Hours

Current Throughput Value(bytes/sec) 245

Current Throughput Value(records/sec) 2

Audit Vault Plug-in Start / Stop Multiple



ORACLE Enterprise Manager Cloud Control 12c

Enterprise ▾ Targets ▾ Favorites ▾ History ▾

↑ av_av103_adc2110215

Oracle Audit Vault System ▾

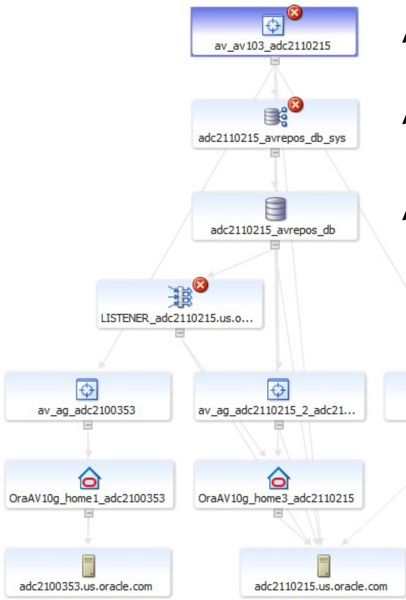
Collectors

□ Select All ▶ Start ● Stop Search by Collector

Select	Collector	Source	Audit Vault Agent		Type	Status
□	ankit_OS_Coll	ankitdb	adc2100353	↑	ORCLDB_OSAUD	↓
□	ankit_DB_Coll	ankitdb	adc2100353	↑	ORCLDB_DBAUD	↓
□	sam_DB_Coll	samdb	adc2201439		ORCLDB_DBAUD	↓
□	OSAUD_Collector	samdb	adc2201439		ORCLDB_OSAUD	↓
□	OSAUD_Collector	adc2110215_db_tgt	adc2110215	↑	ORCLDB_OSAUD	↑
□	OSAUD_Collector	ankitdb	adc2100353	↑	ORCLDB_OSAUD	↑
□	DBAUD_Collector	adc2110215_db_tgt	adc2110215	↑	ORCLDB_DBAUD	↑
□	REDO_Collector	adc2110215_db_tgt	adc2110215_2	↑	ORCLDB_REDO	↑

Audit Vault Plug-in Configuration Topology

- View your Audit Vault system from a single view
- Drill down to each target type to obtain a snapshot of the status
- Go directly to problem areas
- See dependencies and interactions directly


av_av103_adc2110215
adc2110215_avrepos_db_sys
adc2110215_avrepos_db
LISTENER_adc2110215.us.o...
av_ag_adc2100353
av_ag_adc2110215_2_adc21...
av_ag_adc2110215
OraAV10g_home1_adc2100353
OraAV10g_home3_adc2110215
adc2100353.us.oracle.com
adc2110215.us.oracle.com

AV System

AV Server

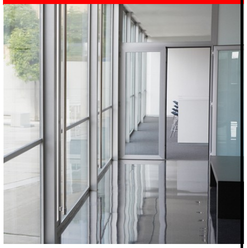
AV Database

Agents

Agent Home

Agent Host

Program Agenda



- Audit Vault 10.3
  - Customer Update
  - New Features
- Database Firewall 5.1
  - New Features
  - PoC Guide Updates
- Summary
- Q&A

Database Firewall 5.1 New Features

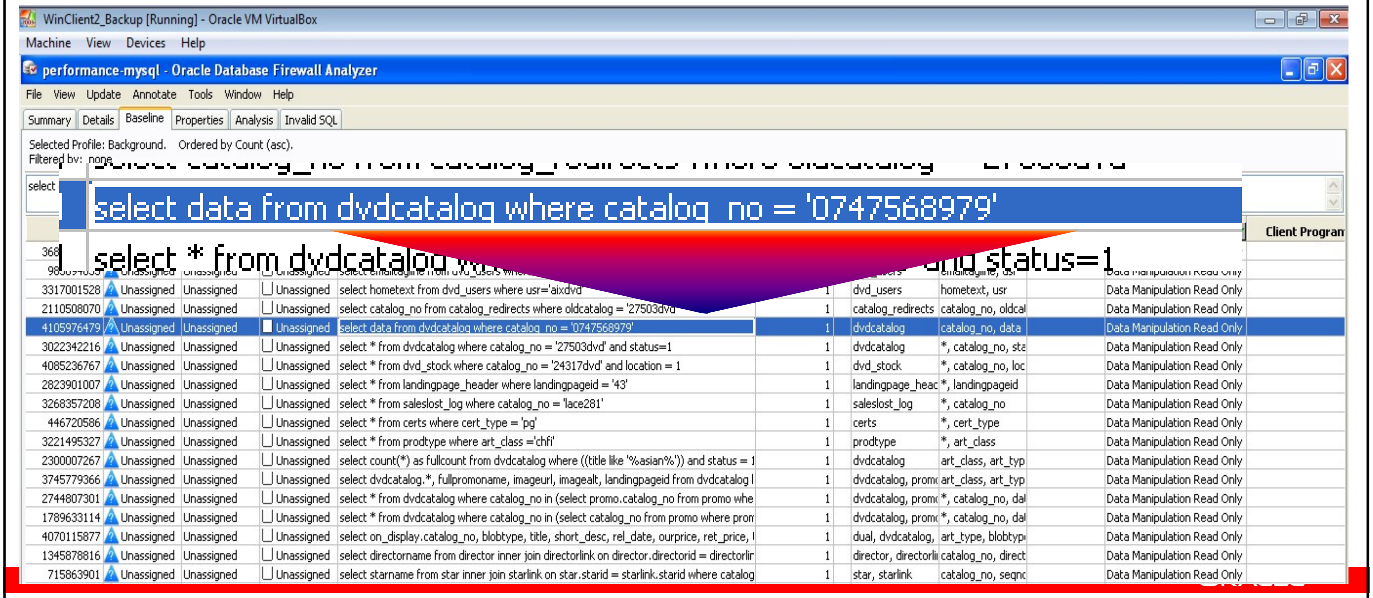
- Expanded Heterogeneous Support
- Proxy Mode Deployment
- Network Encryption
- Enhanced Policy Management
- Enhanced Reporting
- Performance with Multi-Core Support
- Installation

MySQL Functionality

Supported Versions 5.0, 5.1, 5.5

- ✓ Database Response Monitoring
- ✓ SQL Language Monitoring
- ✓ Automated Rule Generation of clusters in the Analyzer
- ✓ Blocking
- ✓ Statement Substitution
- ✓ User Role Auditing
- ✓ Stored Procedure Audit
- ✓ Remote Monitor (Linux only)

MySQL And Database Firewall Analyzer


WinClient2_Backup [Running] - Oracle VM VirtualBox
Machine View Devices Help
performance-mysql - Oracle Database Firewall Analyzer
File View Update Annotate Tools Window Help
Summary Details Baseline Properties Analysis Invalid SQL
Client Program

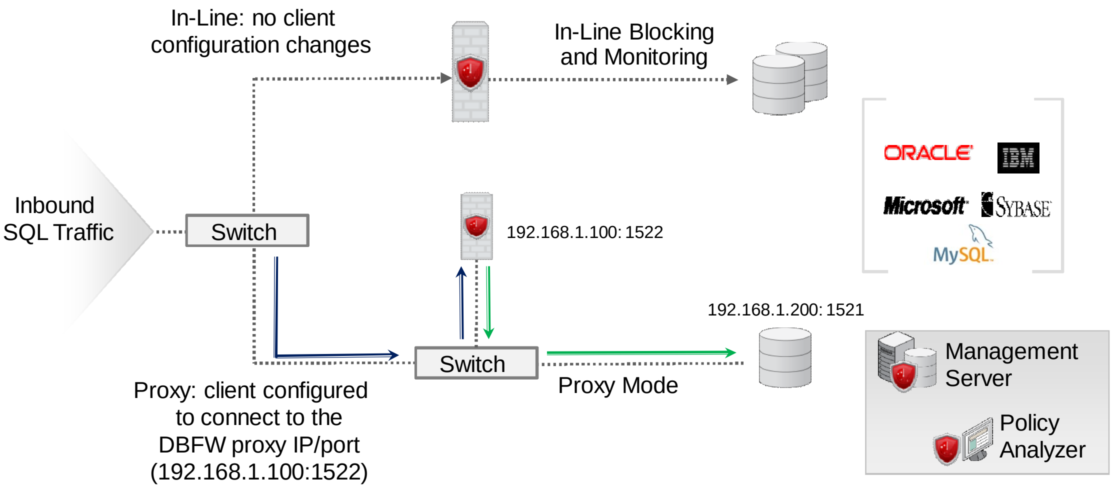
Selected Profile: Background. Ordered by Count (asc).
Filtered by: none

select data from dvdcatalog where catalog_no = '0747568979'

select * from dvdcatalog ... and status=1

3317001528	Unassigned	Unassigned	☐ Unassigned	select hometext from dvd_users where usr='aixdvd'	1	dvd_users	hometext, usr	Data Manipulation Read Only
2110508070	Unassigned	Unassigned	☐ Unassigned	select catalog_no from catalog_redirects where oldcatalog = '27503dvd	1	catalog_redirects	catalog_no, oldcat	Data Manipulation Read Only
4105976479	Unassigned	Unassigned	☐ Unassigned	select data from dvdcatalog where catalog_no = '0747568979'	1	dvdcatalog	catalog_no, data	Data Manipulation Read Only
3022342216	Unassigned	Unassigned	☐ Unassigned	select * from dvdcatalog where catalog_no = '27503dvd' and status=1	1	dvdcatalog	*, catalog_no, sta	Data Manipulation Read Only
4085236767	Unassigned	Unassigned	☐ Unassigned	select * from dvd_stock where catalog_no = '24317dvd' and location = 1	1	dvd_stock	*, catalog_no, loc	Data Manipulation Read Only
2823901007	Unassigned	Unassigned	☐ Unassigned	select * from landingpage_header where landingpageid = '43'	1	landingpage_heac	*, landingpageid	Data Manipulation Read Only
3268357208	Unassigned	Unassigned	☐ Unassigned	select * from saleslost_log where catalog_no = 'lace281'	1	saleslost_log	*, catalog_no	Data Manipulation Read Only
446720586	Unassigned	Unassigned	☐ Unassigned	select * from certs where cert_type = 'pg'	1	certs	*, cert_type	Data Manipulation Read Only
3221495327	Unassigned	Unassigned	☐ Unassigned	select * from prodtype where art_class ='chfi'	1	prodtype	*, art_class	Data Manipulation Read Only
2300007267	Unassigned	Unassigned	☐ Unassigned	select count(*) as fullcount from dvdcatalog where ((title like '%asian%')) and status = 1	1	dvdcatalog	art_class, art_typ	Data Manipulation Read Only
3745779366	Unassigned	Unassigned	☐ Unassigned	select dvdcatalog.*, fullpromoname, imageurl, imagealt, landingpageid from dvdcatalog l	1	dvdcatalog, promo	art_class, art_typ	Data Manipulation Read Only
2744807301	Unassigned	Unassigned	☐ Unassigned	select * from dvdcatalog where catalog_no in (select promo.catalog_no from promo whe	1	dvdcatalog, promo	*, catalog_no, dal	Data Manipulation Read Only
1789633114	Unassigned	Unassigned	☐ Unassigned	select * from dvdcatalog where catalog_no in (select catalog_no from promo where prom	1	dvdcatalog, promo	*, catalog_no, dal	Data Manipulation Read Only
4070115877	Unassigned	Unassigned	☐ Unassigned	select on_display.catalog_no, blobtype, title, short_desc, rel_date, ourprice, ret_price, l	1	dual, dvdcatalog,	art_type, blobtyp	Data Manipulation Read Only
1345878816	Unassigned	Unassigned	☐ Unassigned	select directorname from director inner join directorlink on director.directorid = directorlir	1	director, directorli	catalog_no, direct	Data Manipulation Read Only
715863901	Unassigned	Unassigned	☐ Unassigned	select starname from star inner join starlink on star.starid = starlink.starid where catalog	1	star, starlink	catalog_no, seqnc	Data Manipulation Read Only

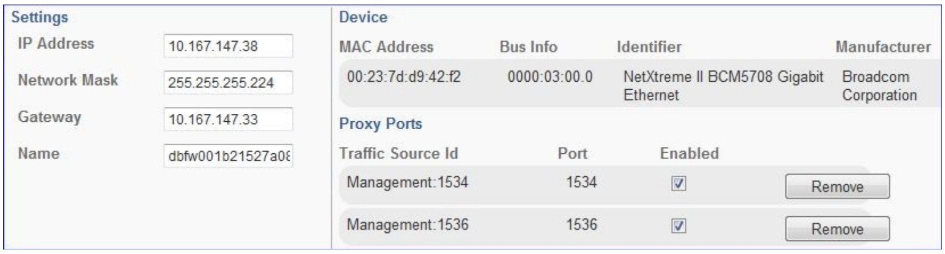
Proxy Deployment



Proxy: client configured to connect to the DBFW proxy IP/port (192.168.1.100:1522)

Proxy Mode Deployment

- Add a Proxy port to the Management Server
  - Any port can be identified as long as it not in use
- Each Proxy supports an Enforcement Point



Settings

IP Address	10.167.147.38
Network Mask	255.255.255.224
Gateway	10.167.147.33
Name	dbfw001b21527a08

Device

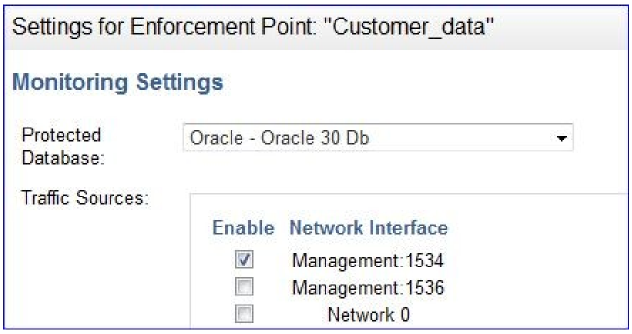
MAC Address	Bus Info	Identifier	Manufacturer
00:23:7d:d9:42:f2	0000:03:00.0	NetXtreme II BCM5708 Gigabit Ethernet	Broadcom Corporation

Proxy Ports

Traffic Source Id	Port	Enabled	
Management:1534	1534	☑	Remove
Management:1536	1536	☑	Remove

Proxy Mode Deployment

- Configure Enforcement Point and select the Proxy Port that will be accepting traffic for that Protected Database



Settings for Enforcement Point: "Customer_data"

Monitoring Settings

Protected Database: Oracle - Oracle 30 Db

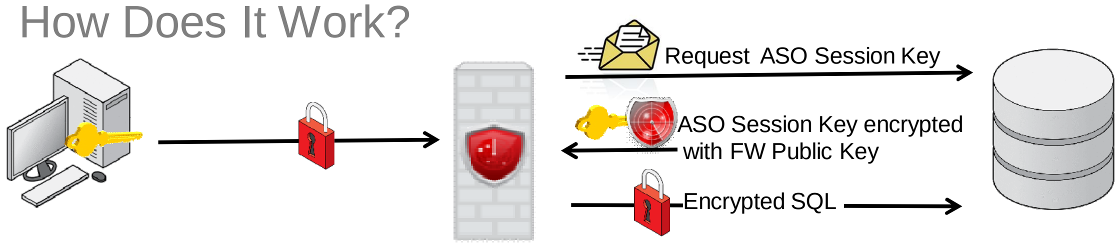
Traffic Sources:

Enable	Network Interface
☑	Management:1534
□	Management:1536
□	Network 0

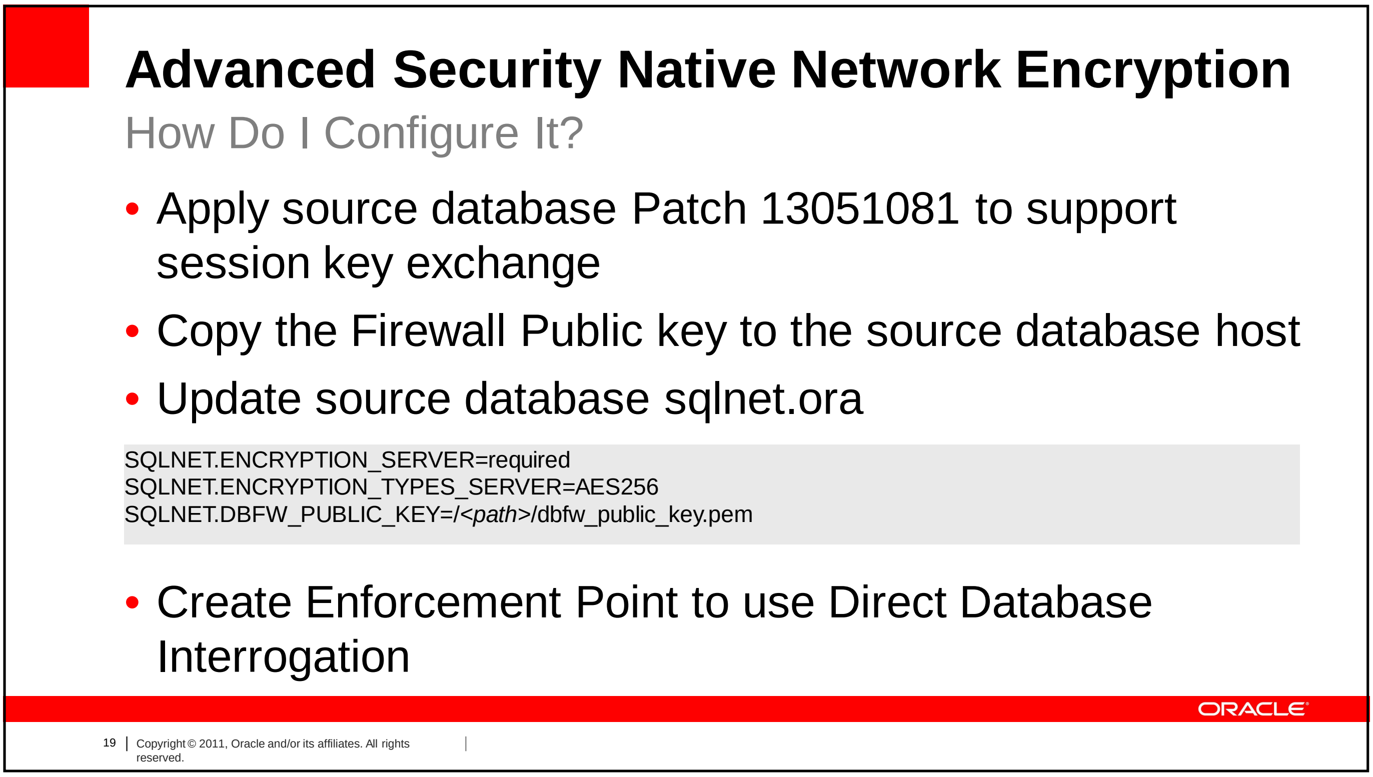
e.g. SQL Client configured to connect to Database Firewall and Port 1534

Advanced Security Native Network Encryption

How Does It Work?



1. Client established a connection to database using ASO encryption
2. Firewall recognizes encrypted traffic and request ASO session key from database
3. Database returns ASO session key encrypted with the Firewall's public key
4. Firewall retrieves ASO session key and uses it to decrypt SQL traffic from client
5. Firewall applies policy on the decrypted traffic
6. Firewall sends original encrypted SQL or new encrypted SQL with SQL substitution to database



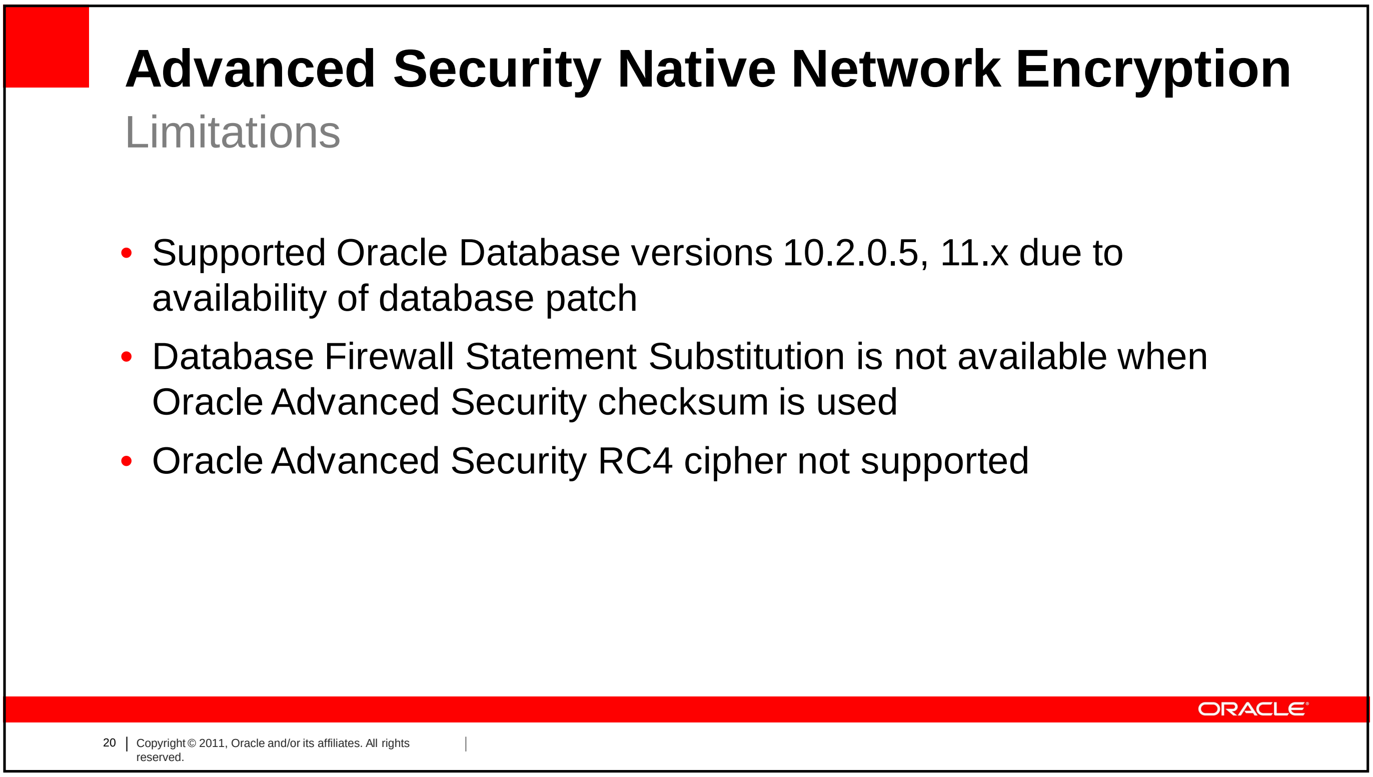
Advanced Security Native Network Encryption

How Do I Configure It?

- Apply source database Patch 13051081 to support session key exchange
- Copy the Firewall Public key to the source database host
- Update source database sqlnet.ora

```
SQLNET.ENCRYPTION_SERVER=required
SQLNET.ENCRYPTION_TYPES_SERVER=AES256
SQLNET.DBFW_PUBLIC_KEY=/<path>/dbfw_public_key.pem
```

- Create Enforcement Point to use Direct Database Interrogation



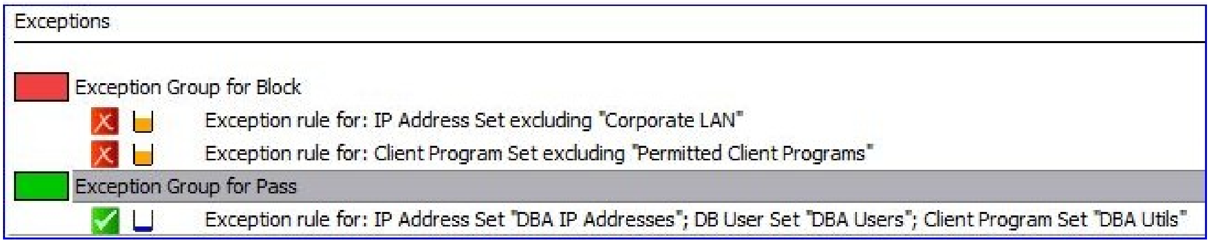
Advanced Security Native Network Encryption

Limitations

- Supported Oracle Database versions 10.2.0.5, 11.x due to availability of database patch
- Database Firewall Statement Substitution is not available when Oracle Advanced Security checksum is used
- Oracle Advanced Security RC4 cipher not supported

Policy Setting Enhancements

- Dual actions for exceptions:
  - Session-based block list
  - Privileged user policy bypass (e.g. Block external IPs and Out-of-policy applications, Log all DBA activity)



Exceptions

🟥 Exception Group for Block

☒ Exception rule for: IP Address Set excluding "Corporate LAN"

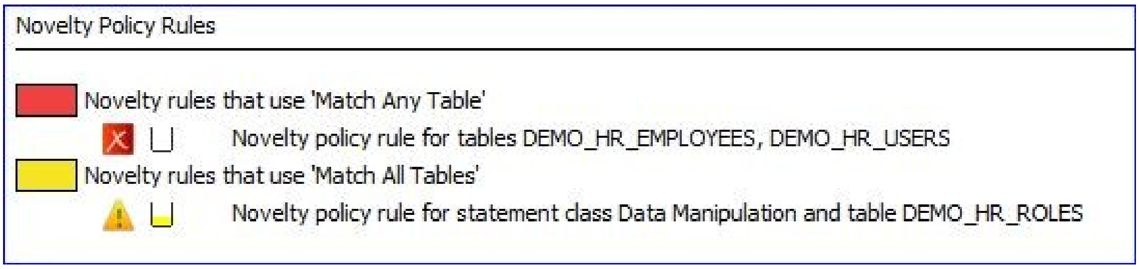
☒ Exception rule for: Client Program Set excluding "Permitted Client Programs"

🟩 Exception Group for Pass

✓ Exception rule for: IP Address Set "DBA IP Addresses"; DB User Set "DBA Users"; Client Program Set "DBA Utils"

Policy Setting Enhancements

- Enhanced Novelty Policies
  - Rules that match 'any' tables in the policy (for auditing)
  - Rules that match 'all' tables in the policy (for security)



Novelty Policy Rules

🟥 Novelty rules that use 'Match Any Table'

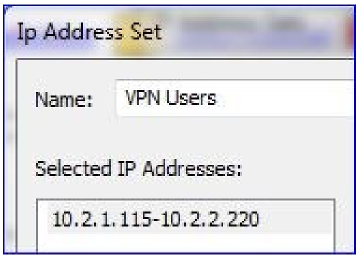
☒ Novelty policy rule for tables DEMO_HR_EMPLOYEES, DEMO_HR_USERS

🟨 Novelty rules that use 'Match All Tables'

⚠ Novelty policy rule for statement class Data Manipulation and table DEMO_HR_ROLES

Policy Setting Enhancements

- IP ranges
  - Define client by IP range
    (note that user names already support wild cards)



Ip Address Set

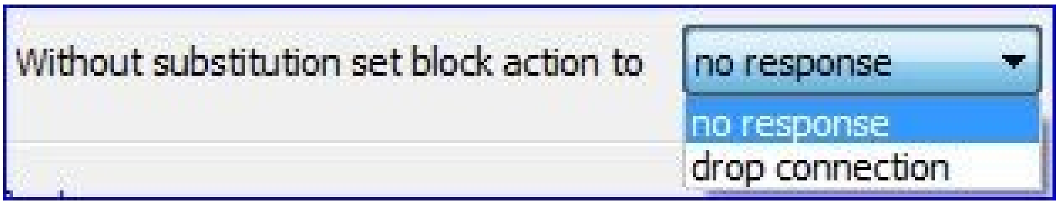
Name: VPN Users

Selected IP Addresses:

10.2.1.115-10.2.2.220

Policy Setting Enhancements

- Blocking options
  - Option to use TCP reset when Statement Substitution not used

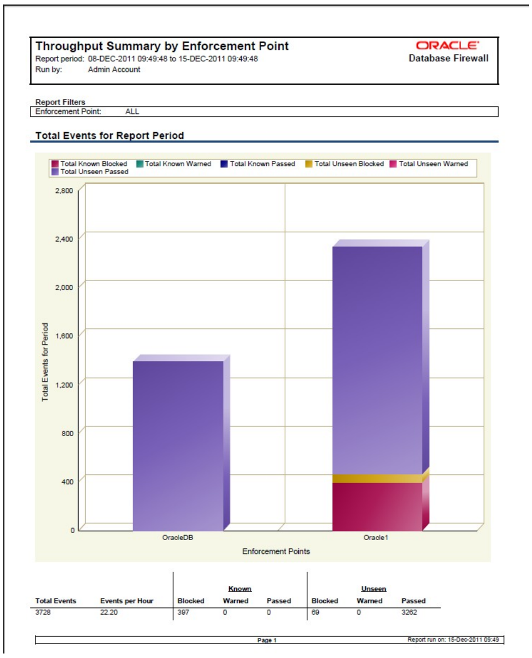


Without substitution set block action to: no response

Report Enhancements

BI Publisher Run-Time Integration

- Crystal was replaced with BI Publisher runtime
- Use BI Publisher to easily create and load new reports via the Report UI
- Audit reports allow you to select search results to use for report output



Throughput Summary by Enforcement Point
Report period: 08-DEC-2011 09:49:48 to 15-DEC-2011 09:49:48
Run by: Admin Account

ORACLE Database Firewall

Report Filters
Enforcement Point: ALL

Total Events for Report Period

		Known			Unseen		
Total Events	Events per Hour	Blocked	Warned	Passed	Blocked	Warned	Passed
3728	22.20	397	0	0	69	0	3262

Page 1 Report run on: 15-Dec-2011 09:49

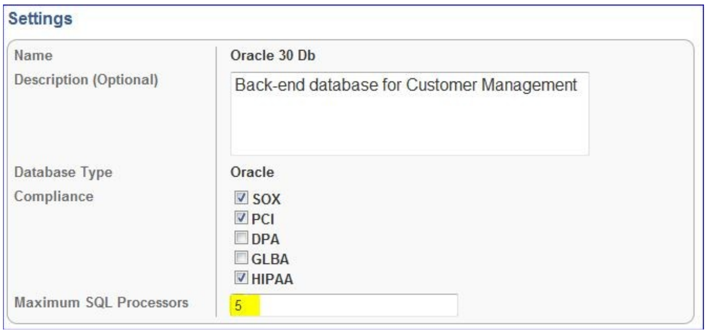
Added Reports

- New Summary reports to provide extended overview of database activity.
  - Throughput Summary by Enforcement Point
  - Statement Count by Session Summary
  - Count of Clusters Grouped by DML Keyword
- New Session Factor reports designed to facilitate developing session-based profiles for more effective policy enforcement and monitoring.
  - Session Summary ordered by IP Address
  - Session Summary ordered by IP Address
  - OS Users List
  - Client Application Name List
  - Summary of Client IP Address ordered by Protected Database
  - Summary of Database Users ordered by Protected Database

Enhanced Vertical Scalability

Multi-Core Support

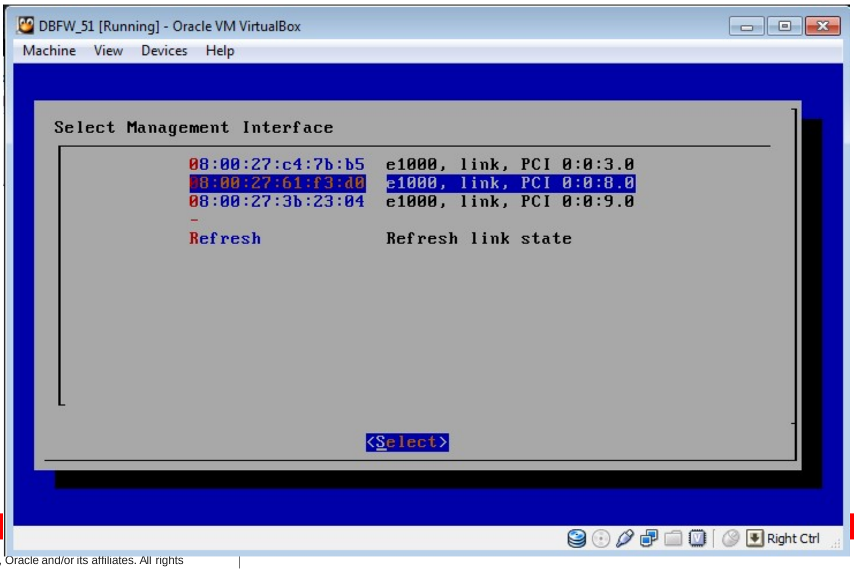
- Improves support for high-throughput systems
- Allocate dedicated cores per protected database per database firewall
- Works for all database platforms



Settings

Name	Oracle 30 Db
Description (Optional)	Back-end database for Customer Management
Database Type	Oracle
Compliance	☑ SOX ☑ PCI □ DPA □ GLBA ☑ HIPAA
Maximum SQL Processors	5

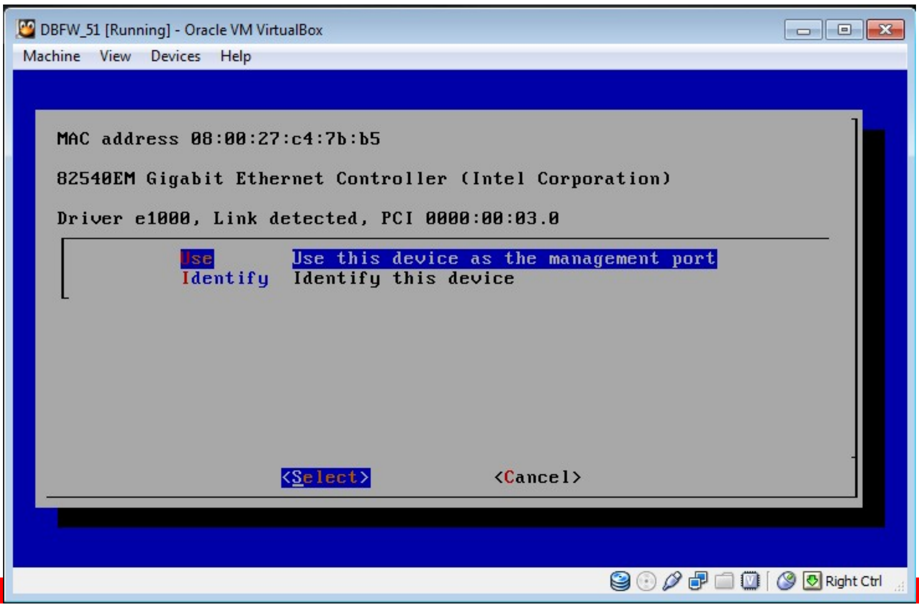
Install Changes
Only Select Management Interface



DBFW_51 [Running] - Oracle VM VirtualBox
Machine View Devices Help
Right Ctrl

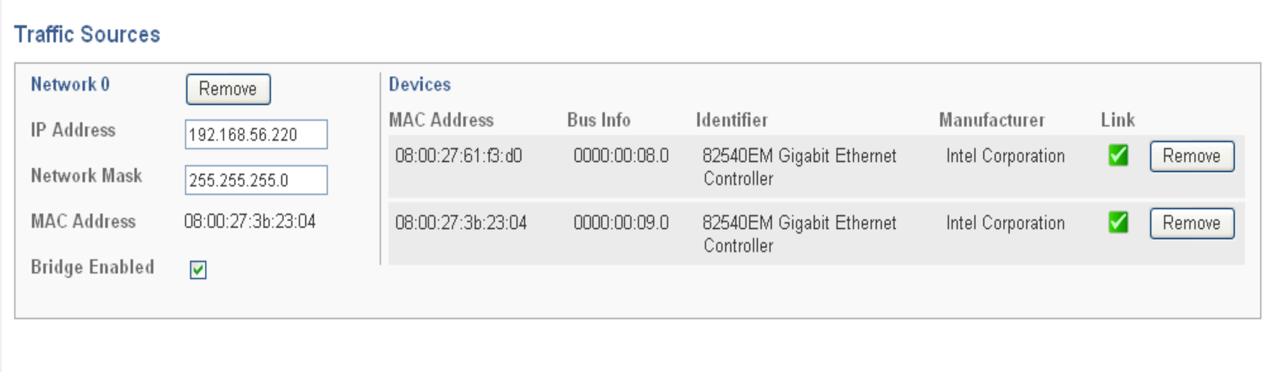
```
Select Management Interface

     08:00:27:c4:7b:b5   e1000, link, PCI 0:0:3.0
     08:00:27:61:f3:d0   e1000, link, PCI 0:0:8.0
     08:00:27:3b:23:04   e1000, link, PCI 0:0:9.0
     -
     Refresh             Refresh link state

                    <Select>
```

Provides Additional Information of NIC


DBFW_51 [Running] - Oracle VM VirtualBox
Machine View Devices Help
Right Ctrl

```
MAC address 08:00:27:c4:7b:b5

82540EM Gigabit Ethernet Controller (Intel Corporation)

Driver e1000, Link detected, PCI 0000:00:03.0

         Use        Use this device as the management port
         Identify   Identify this device

            <Select>              <Cancel>
```

Manage the Addition / Removal of NICs



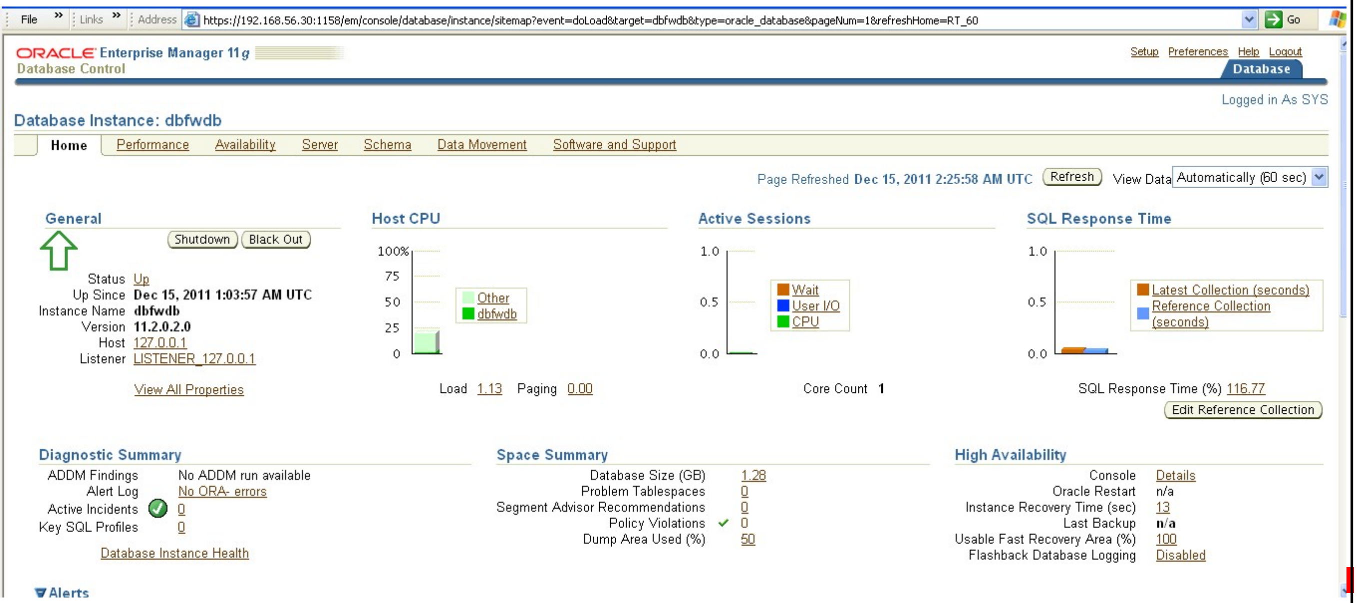
Traffic Sources

Network 0	Remove
IP Address	192.168.56.220
Network Mask	255.255.255.0
MAC Address	08:00:27:3b:23:04
Bridge Enabled	☑

Devices

MAC Address	Bus Info	Identifier	Manufacturer	Link	
08:00:27:61:f3:d0	0000:00:08.0	82540EM Gigabit Ethernet Controller	Intel Corporation	✓	Remove
08:00:27:3b:23:04	0000:00:09.0	82540EM Gigabit Ethernet Controller	Intel Corporation	✓	Remove

Manage the Oracle Embedded Database



File
Links
Address
https://192.168.56.30:1158/em/console/database/instance/sitemap?event=doLoad&target=dbfwdb&type=oracle_database&pageNum=1&refreshHome=RT_60
Go
ORACLE Enterprise Manager 11g
Database Control
Setup Preferences Help Logout
Database

Logged in As SYS

Database Instance: dbfwdb

Home | Performance | Availability | Server | Schema | Data Movement | Software and Support

Page Refreshed Dec 15, 2011 2:25:58 AM UTC Refresh View Data Automatically (60 sec)

General

Shutdown Black Out

Status	Up
Up Since	Dec 15, 2011 1:03:57 AM UTC
Instance Name	dbfwdb
Version	11.2.0.2.0
Host	127.0.0.1
Listener	LISTENER_127.0.0.1

View All Properties

Host CPU

Load 1.13 Paging 0.00

Active Sessions

Core Count 1

SQL Response Time

SQL Response Time (%) 116.77

Edit Reference Collection

Diagnostic Summary

ADDM Findings	No ADDM run available
Alert Log	No ORA- errors
Active Incidents	✓ 0
Key SQL Profiles	0

Database Instance Health

Space Summary

Database Size (GB)	1.28
Problem Tablespaces	0
Segment Advisor Recommendations	0
Policy Violations	✓ 0
Dump Area Used (%)	50

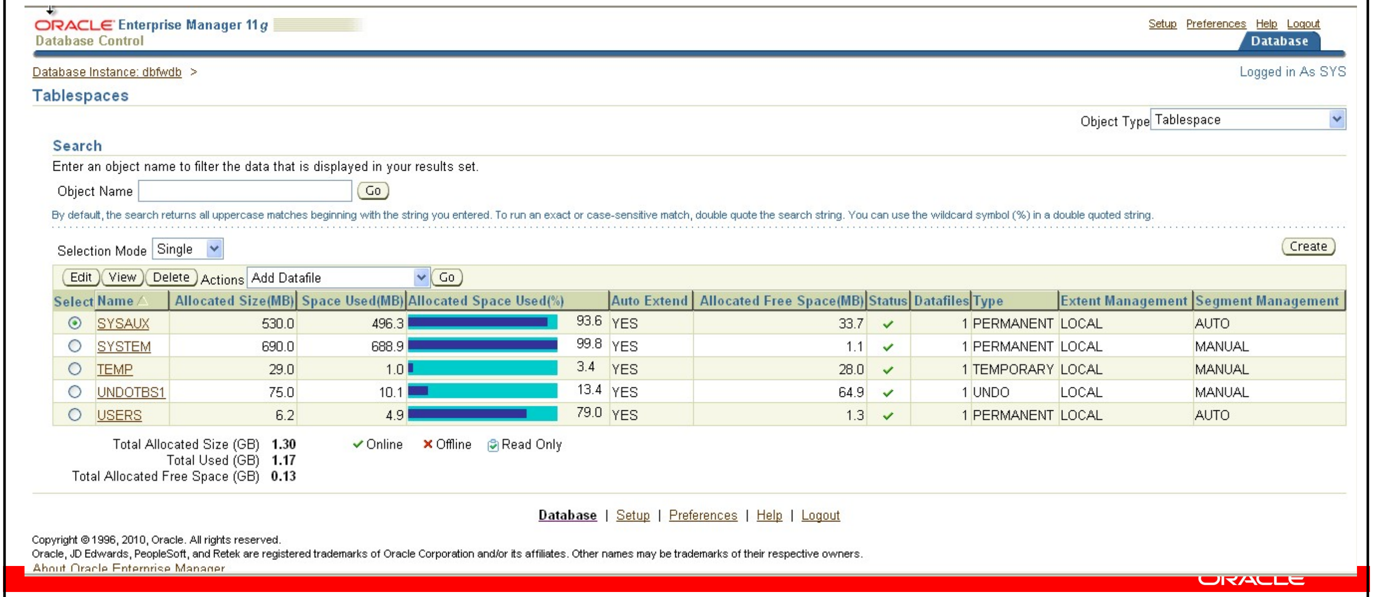
High Availability

Console	Details
Oracle Restart	n/a
Instance Recovery Time (sec)	13
Last Backup	n/a
Usable Fast Recovery Area (%)	100
Flashback Database Logging	Disabled

▼Alerts

31 |

View & Manage Tablespaces



Database Instance: dbfwdb >

Logged in As SYS

Tablespaces

Object Type Tablespace

Search

Enter an object name to filter the data that is displayed in your results set.

Object Name [ ] Go

By default, the search returns all uppercase matches beginning with the string you entered. To run an exact or case-sensitive match, double quote the search string. You can use the wildcard symbol (%) in a double quoted string.

Selection Mode Single Create

Edit View Delete Actions Add Datafile Go

Select	Name	Allocated Size(MB)	Space Used(MB)	Allocated Space Used(%)	Auto Extend	Allocated Free Space(MB)	Status	Datafiles	Type	Extent Management	Segment Management
●	SYSAUX	530.0	496.3	93.6	YES	33.7	✓	1	PERMANENT	LOCAL	AUTO
○	SYSTEM	690.0	688.9	99.8	YES	1.1	✓	1	PERMANENT	LOCAL	MANUAL
○	TEMP	29.0	1.0	3.4	YES	28.0	✓	1	TEMPORARY	LOCAL	MANUAL
○	UNDOTBS1	75.0	10.1	13.4	YES	64.9	✓	1	UNDO	LOCAL	MANUAL
○	USERS	6.2	4.9	79.0	YES	1.3	✓	1	PERMANENT	LOCAL	AUTO

Total Allocated Size (GB)	1.30
Total Used (GB)	1.17
Total Allocated Free Space (GB)	0.13

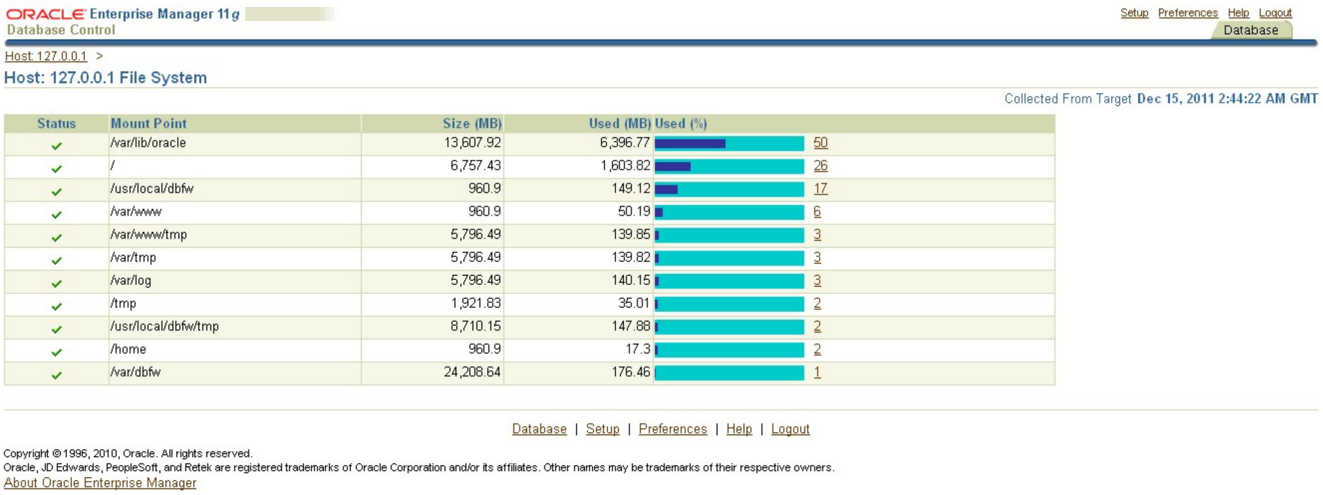
✓ Online ✗ Offline Read Only

Database | Setup | Preferences | Help | Logout

About Oracle Enterprise Manager

32 |

View File System Storage



ORACLE Enterprise Manager 11*g*
Database Control

Setup Preferences Help Logout

Database

Host: 127.0.0.1 >

Host: 127.0.0.1 File System

Collected From Target **Dec 15, 2011 2:44:22 AM GMT**

Status	Mount Point	Size (MB)	Used (MB)	Used (%)
✓	/var/lib/oracle	13,607.92	6,396.77	50
✓	/	6,757.43	1,603.82	26
✓	/usr/local/dbfw	960.9	149.12	17
✓	/var/www	960.9	50.19	6
✓	/var/www/tmp	5,796.49	139.85	3
✓	/var/tmp	5,796.49	139.82	3
✓	/var/log	5,796.49	140.15	3
✓	/tmp	1,921.83	35.01	2
✓	/usr/local/dbfw/tmp	8,710.15	147.88	2
✓	/home	960.9	17.3	2
✓	/var/dbfw	24,208.64	176.46	1

Database | Setup | Preferences | Help | Logout

About Oracle Enterprise Manager

Q&A

ORACLE®