# Oracle Audit Vault and Database Firewall: Install & Configure

**Activity Guide**

D86587GC10

Edition 1.0

August 2014

## Authors

Donna K. Keesling, James L. Spiller

## Technical Contributors and Reviewers

Paul Betteridge, Andrey Brozhko, Melody S. Liu, Pedro Lopes, Dinesh Rajasekharan

**This book was published using: Oracle Tutor**

# Table of Contents

# Practices for Lesson 1: Introduction to Oracle Audit Vault and Database Firewall

**Chapter 1**

# Practices for Lesson 1

## Practices Overview

In these practices, you will identify Audit Vault and Database Firewall components. You will indicate which features are supported for various secured targets. You will also distinguish between tasks typically performed by AVDF administrators and auditors.

# Practice 1-1: Identifying Audit Vault and Database Firewall Components

## Overview

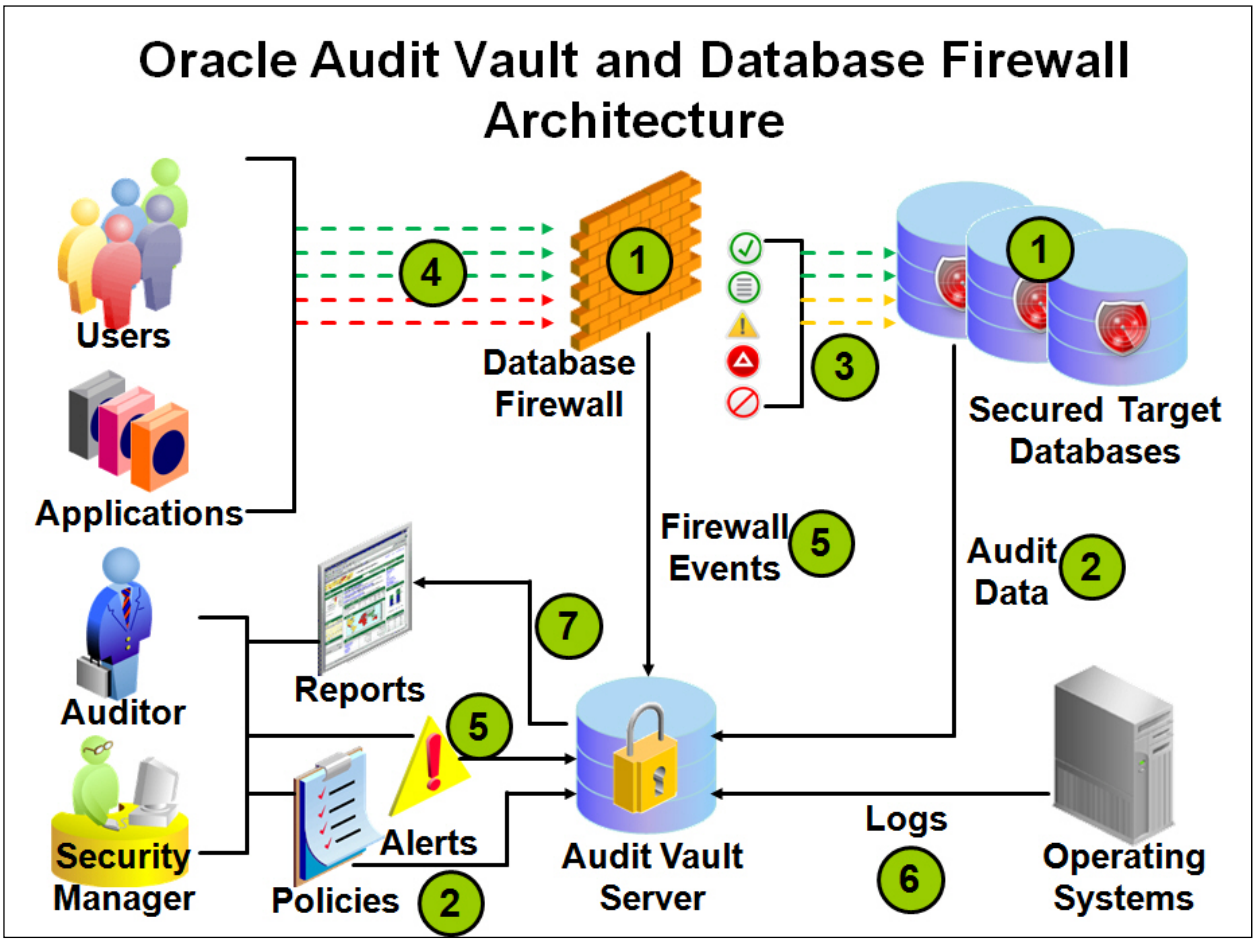
In this pen-and-paper practice, you identify Audit Vault and Database Firewall components, and explain the Oracle Audit Vault and Database Firewall (Oracle AVDF) architecture.

## Tasks

1. Fill in the blank with the Oracle AVDF component.
   a. The _____ is the component that manages the retrieval of audit trail data from a secured target database.
   b. The _____ is the central repository that stores consolidated audit data and event logs.
   c. The _____ is the network monitoring component that monitors inbound SQL traffic.

   *Answers:*

   *a. Audit Vault Agent*
   *b. Audit Vault Server*
   *c. Database Firewall*
2. For each item listed, identify which number it corresponds to in the Oracle AVDF architecture diagram:



a. The Database Firewall can be configured to monitor and raise alerts only, or to block SQL traffic and optionally substitute statements according to the defined policy.
b. If you deploy the Audit Vault Agent, it manages the retrieval of audit data from the secured target and sends the data to the Audit Vault Server.
c. After audit data is stored in the data warehouse, an auditor can generate reports.
d. For each secured target, you can deploy the Audit Vault Agent and/or place the Database Firewall in the network to protect the target.
e. If you have deployed a Database Firewall to protect the target, a firewall policy is applied.
f. The Audit Vault Server includes an internal database warehouse, which is used to store Oracle AVDF configuration data and collected audit data.
g. The Database Firewall monitors SQL traffic for secured targets and sends data to the Audit Vault Server based on the policies that have been configured.

*Answers:*

*a. 5*
*b. 2*
*c. 7*
*d. 1*
*e. 3*
*f. 6*
*g. 4*

# Practice 1-2: Identifying Supported Secured Targets

## Overview

In this pen-and-paper practice, you identify supported secured targets and determine whether out-of-the-box plug-ins can be used to support a given target.

## Tasks

1. Refer to Appendix B in the *Oracle Audit Vault and Database Firewall Administrator's Guide* to determine whether each feature is supported for the listed secured targets. You can also find the latest supported platform information in Article 1536380.1 on the My Oracle Support web site.

| Secured Target | Audit Trail Collection | Entitlement Auditing | Stored Procedure Auditing | Database Firewall | Host Monitor | Database Interrogation |
|---|---|---|---|---|---|---|
| IBM DB2 for LUW | | | | | | |
| Microsoft SQL Server 2008 | | | | | | |
| Microsoft SQL Server 2012 | | | | | | |
| MySQL 5.5 and 5.6 | | | | | | |
| Oracle Database 10*g*, 11*g*, and 12*c* | | | | | | |
| Sybase ASE 12.5.4 to 15.7 | | | | | | |

## Practice 1-3: Identifying Third-Party Product Integration

### Overview

In this pen-and-paper practice, you identify which third-party products Oracle AVDF is integrated with.

### Tasks

1. List reasons you might want to integrate Oracle AVDF with third-party products:
   a. _____
   b. _____
   c. _____

# Practice 1-4: Distinguishing Typical Tasks of Oracle AVDF Administrators and Auditors

## Overview

In this pen-and-paper practice, you distinguish between the typical tasks of an Oracle AVDF administrator and auditor.

## Tasks

1. An Oracle AVDF administrator typically performs which of the following tasks?
   a. Creating secured targets in the Audit Vault Server for each monitored database or operating system
   b. Deploying and activating the Audit Vault Agent on the secured target host computers
   c. Designing a firewall policy based on analyzed SQL statements from a secured target
   d. Creating enforcement points for secured targets
   e. Creating simple alerts for secured targets
   f. Scheduling and generating a variety of audit and firewall reports

   *Answer: a, b, and d*
2. An Oracle AVDF auditor typically performs which of the following tasks?
   a. Specifying audit and/or firewall policies for a secured target
   b. Configuring connections to host computers
   c. Designing and provisioning audit policies
   d. Specifying alert notifications by using email templates
   e. Configuring audit trails for secured targets
   f. Creating administrator users and managing access

   *Answer: a, c, and d*

# Practices for Lesson 2: Planning the Oracle Audit Vault and Database Firewall Implementation

**Chapter 2**

# Practices for Lesson 2

## Practices Overview

In these practices, you will review a list of requirements and determine the appropriate implementation of Oracle Audit Vault and Database Firewall (Oracle AVDF).

# Practice 2-1: Implementing Oracle AVDF

## Overview

In this pen-and-paper practice, you describe the appropriate Oracle AVDF implementation given a set of requirements.

## Assumptions

Your site has several small to medium databases that you want to protect with Oracle AVDF. Some of the database must have blocking. Others only require monitoring and alerts. These databases are scattered across several subnets and buildings on your campus. The maximum number of transactions per second for all databases combined is 4,000 transactions per second. All the databases are inside a corporate firewall and all clients must access the databases from outside the firewall.

## Tasks

1. How many CPUs are required and why?
2. What configurations meet the requirements of both blocking and monitoring?
3. Which configuration would require the fewest number of DBFW appliances?
4. Is the Audit Vault Server appliance required?
5. How many network cards would be required to implement the configuration in step 3? How many would be recommended?
6. Sketch a possible placement of the DBFW and AVSVR appliances.

# Practice 2-2: Configuring Oracle AVDF and Deploying the Audit Vault Agent

## Overview

In this pen-and-paper practice, you answer questions about the configuration of Oracle AVDF and deployment of the Audit Vault Agent.

## Assumptions

There are three databases that require auditing. The operating system for the database machines is Linux. The audit trails and syslogs must be stored for at least 6 months on-line and 7 years offline. The audit trails must be reasonably protected from tampering by any users with access to the database machines.

## Tasks

1. What is the role of the Audit Vault Server in this scenario?
   *Answer: The Audit Vault Servers serves as the repository for audit trails and syslog records.*
2. How would you handle the long term storage requirements?
   *Answer: Use the archive retention policies to move long term records to file storage.*
3. Where will the Audit Vault Agent be deployed?
   *Answer: The agent will be deployed to each database with a TABLE type audit trail to capture the database audit trail and a SYSLOG type audit trail to capture the system logs*.

# Practice 2-3: Configuring Oracle AVDF and Deploying the Database Firewall

## Overview

In this pen-and-paper practice, you answer questions about the configuration of Oracle AVDF and deployment of the Database Firewall.

## Assumptions

A large database with peak throughput of 10,000 tps must be protected with SQL blocking for unapproved SQL statements. Failing statements must generate alerts and be audited. The database firewall system must be audited for system level changes.

## Tasks

1. How would you configure the Oracle database to protect the database?
   *Answer: Inline*
2. How many CPUs would be required for the database firewall?
   *Answer: Three. One for the management and two for transaction processing*
3. How many network interface cards are required?
   *Answer: Three. One for the management interface and two for network interfaces*
4. How will the Database Firewall be configured (in general terms)?
   *Answer: The Database Firewall policies would be set to alert and block on failure. Alerts could be sent via email. System logs could be forwarded to a remote machine and the remote machine would have an Audit Vault Agent installed to capture the system logs.*

# Practices for Lesson 3: Installing the Audit Vault Server

**Chapter 3**

# Practices for Lesson 3

## Practices Overview

In these practices, you will complete the Audit Vault Server installation process by performing the post-installation tasks.

# Practice 3-1: Performing Audit Vault Server Post-Installation Tasks

## Overview

In this practice, you perform post-installation tasks for Audit Vault Server.

## Assumptions

Oracle Audit Vault Server has been installed.

In the Oracle University classroom, the IP address for the Audit Vault Server appliance is 192.0.2.191.

## Tasks

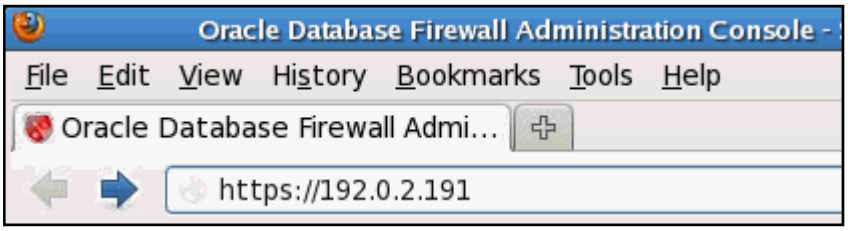
1. Access the Audit Vault Console by using the em12c VM. This simulates accessing the console from a management node.
   a. Open a terminal window.
   b. Connect to the em12c Virtual Machine (VM) with ssh and port forwarding. The login to em12c is: OS username of `oracle` with password of `oracle`.

```
$ ssh -X oracle@em12c
oracle@em12c's password:
Last login: Fri Apr 25 16:45:06 2014 from dom0.example.com
```

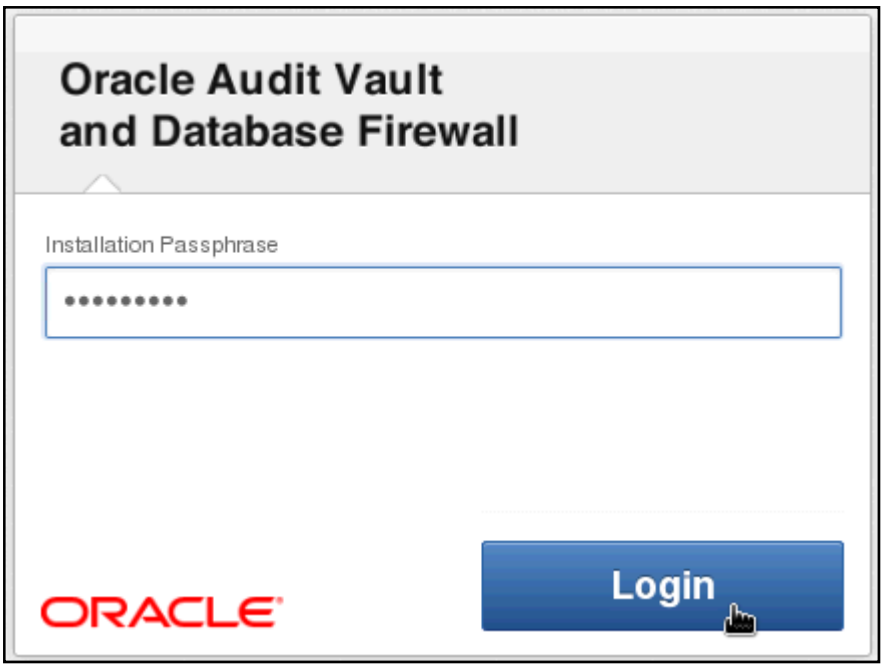
   c. Open the Firefox browser.

```
[oracle@em12c ~]$ firefox
```

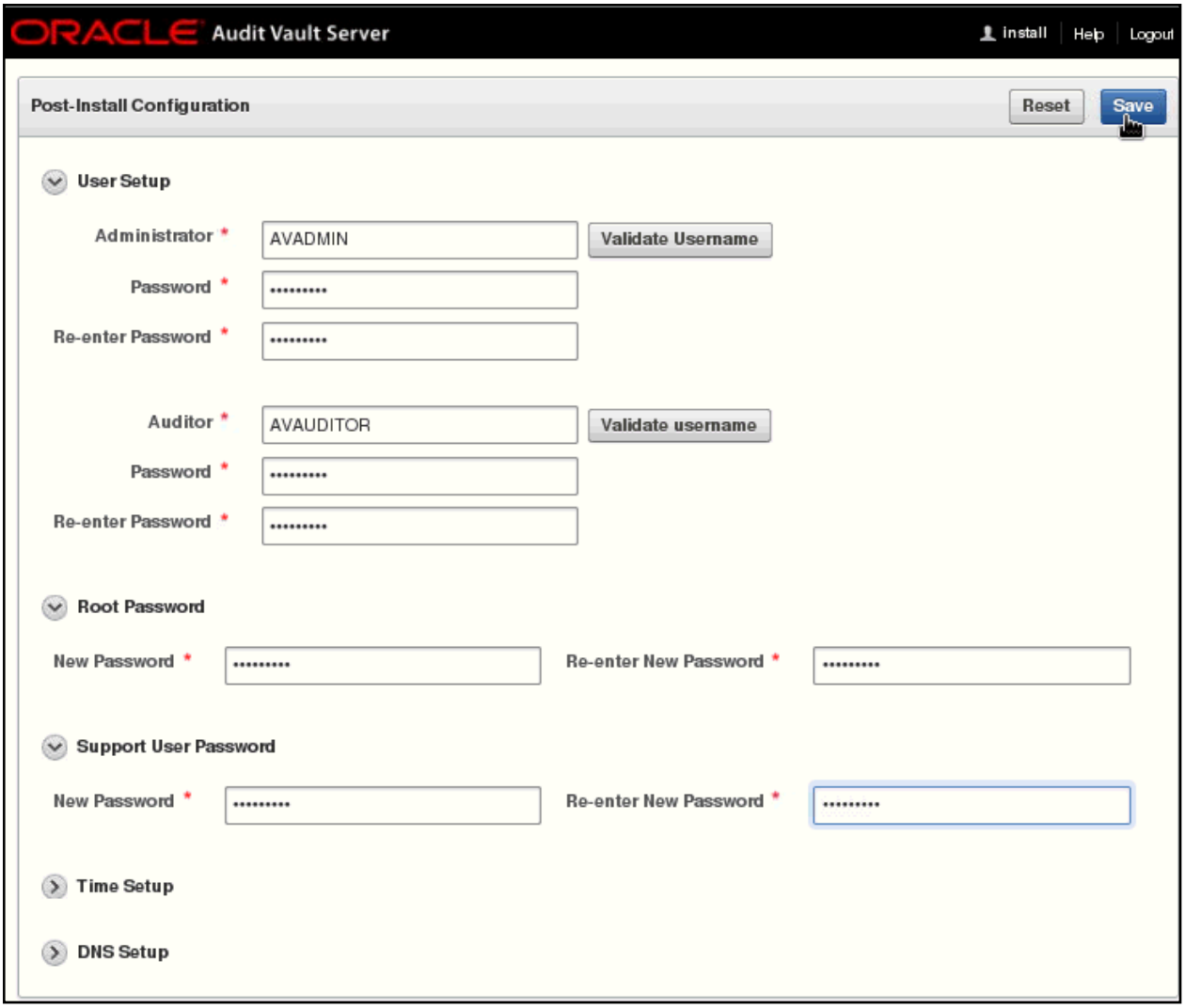
   d. Launch the Audit Vault Console by entering the following URL: https://192.0.2.191.



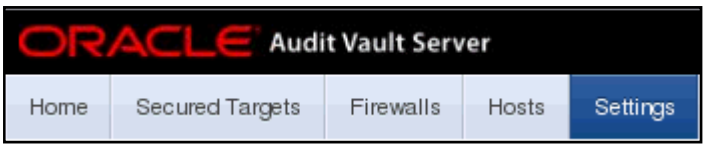

   e. On first access, you will see a dialog box stating “This Connection is Untrusted.” Click “**I Understand the Risks**” and then click **Add Exception**.
   f. In the Add Security Exception box, click **Confirm Security Exception**.
   g. On the Audit Vault and Database Vault Login page, enter the installation passphrase of **`oracle_4U`** and click **Login**.



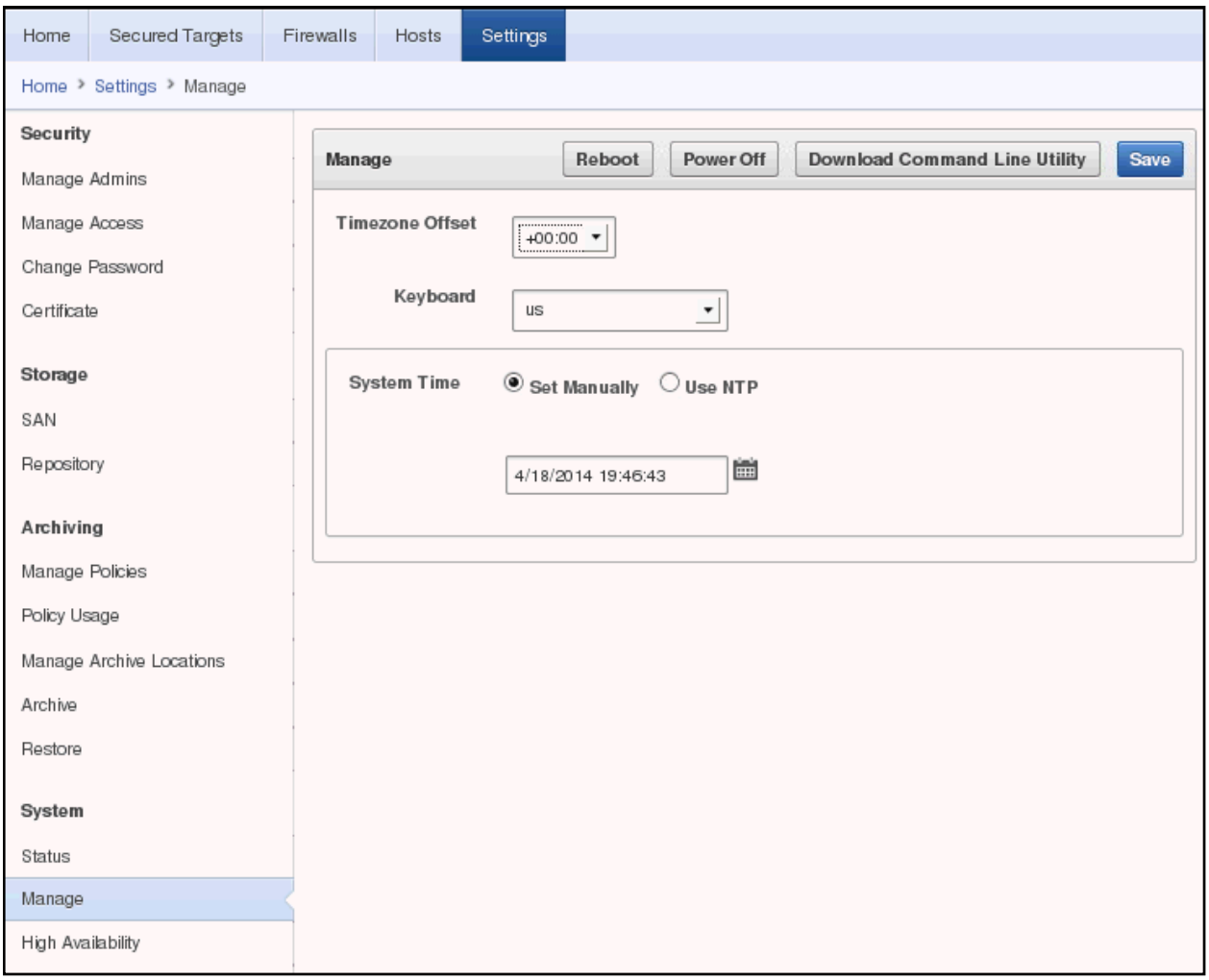

2. On the Post-Install Configuration page, perform the following tasks to set up the users:
   a. Set the Administrator field to **AVADMIN** with a password of **oracle_4U**.
   b. Set the Auditor field to **AVAUDITOR** with a password of **oracle_4U**.
   c. Set Root password to **oracle_4U**.
   d. Set Support User password to **oracle_4U**.
   e. Click **Save**.



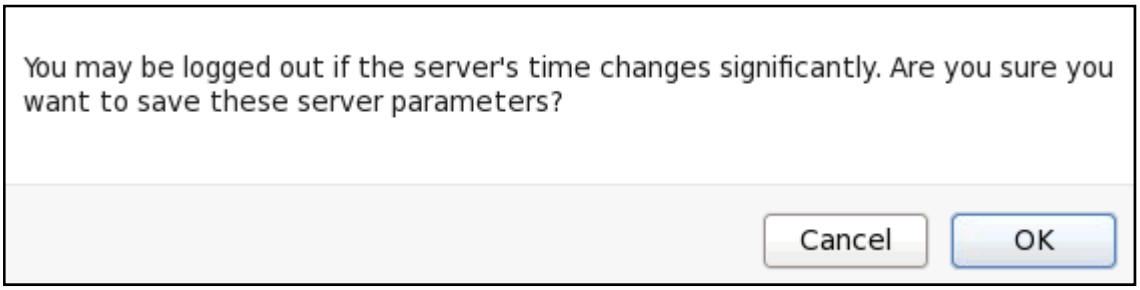

3. On the Oracle Audit Vault and Database Vault Login page, enter **`AVADMIN`** in the user name field and **`oracle_4U`** in the password field. Click **Login**.
4. Set the time. Specify the IP addresses for up to three time (NTP) servers.
   a. Navigate to the Settings page by clicking **Settings** in the menu at the top of the page.




   b. Click **Manage** in the **System** menu on the left side of the page.

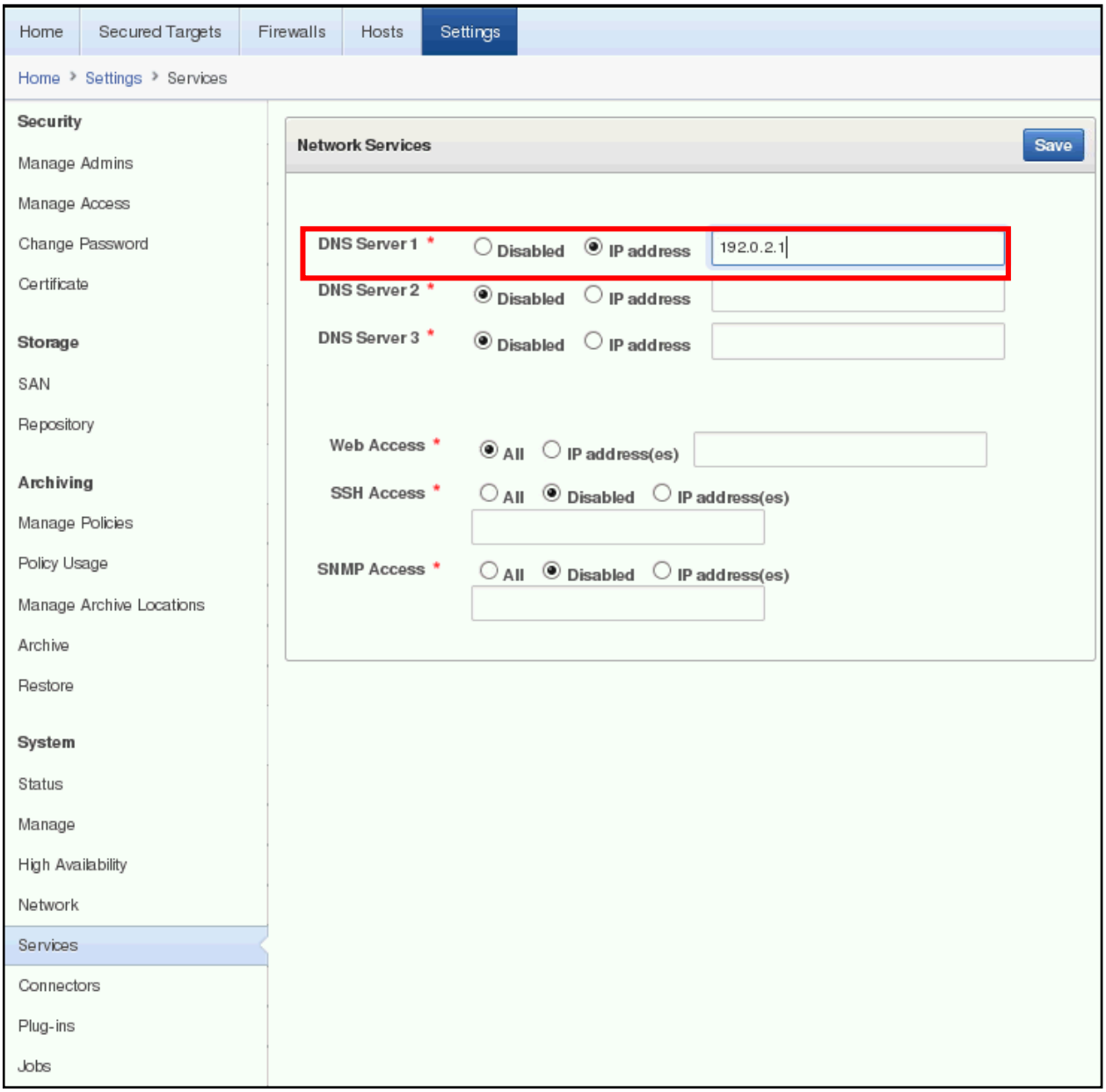



c. Verify that the keyboard setting is `us`.
d. Set the System Time to "**Use NTP**." The page refreshes.
e. When the page refreshes, select **Synchronize Periodically**.
f. Specify NTP Server 1 address as **192.0.2.1**. Click **Test Server**.
g. Click **Apply Server**.
h. Click **Save**.
i. A warning message box appears. Click **OK**.




5. Set DNS servers. Specify the IP addresses for up to three DNS servers.
   a. Click **Services** in the **System** menu on the left side.
   b. For DNS Server1, click the **IP Address** radio button and enter the IP address of **192.0.2.1**.

c. Click **Save**.




6. Log out of the Audit Vault Server console by clicking **Logout** at the top right of the window.

# Practices for Lesson 4: Configuring the Audit Vault Server

**Chapter 4**

# Practices for Lesson 4

## Practices Overview

In these practices, you will perform the tasks required to configure the Audit Vault Server.

# Practice 4-1: Creating Audit Vault Server Administrative Users

## Overview

In this practice, you create the Audit Vault Server administrative accounts.

As a best practice, you should use the installed Audit Vault and Database Firewall user accounts only as back-up accounts. Add new user accounts, with unique usernames and passwords, for the users who are responsible for the day-to-day Oracle AVDF operations.

Audit Vault Server super administrators can create both super administrator and administrator user accounts.

## Assumptions

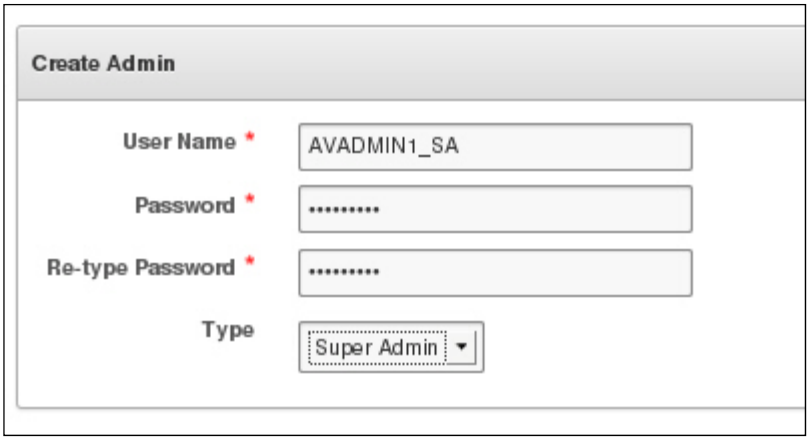
A Firefox browser window is open and the Oracle Audit Vault and Database Firewall Login page is displayed.

## Tasks

Perform the following steps to create administrative accounts in the Audit Vault Server:

1. Log in to the Audit Vault Server as a super administrator. On the login page, enter the following:
   - Username: **`AVADMIN`**
   - Password **`oracle_4U`**

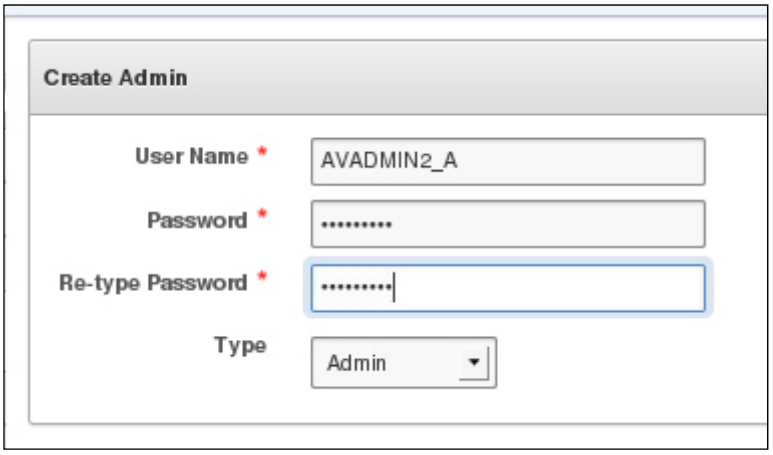
   Click **Login**.
2. Click the **Settings** tab.
3. In the **Security** menu, click **Manage Admins**.
4. On the Manage Admins page, click **Create**.
5. Enter the following values in the User Name and Password fields:
   - User name: **`AVADMIN1_SA`**
   - Password: **`oracle_4U`**
6. In the **Type** drop-down list, select **Super Admin**.



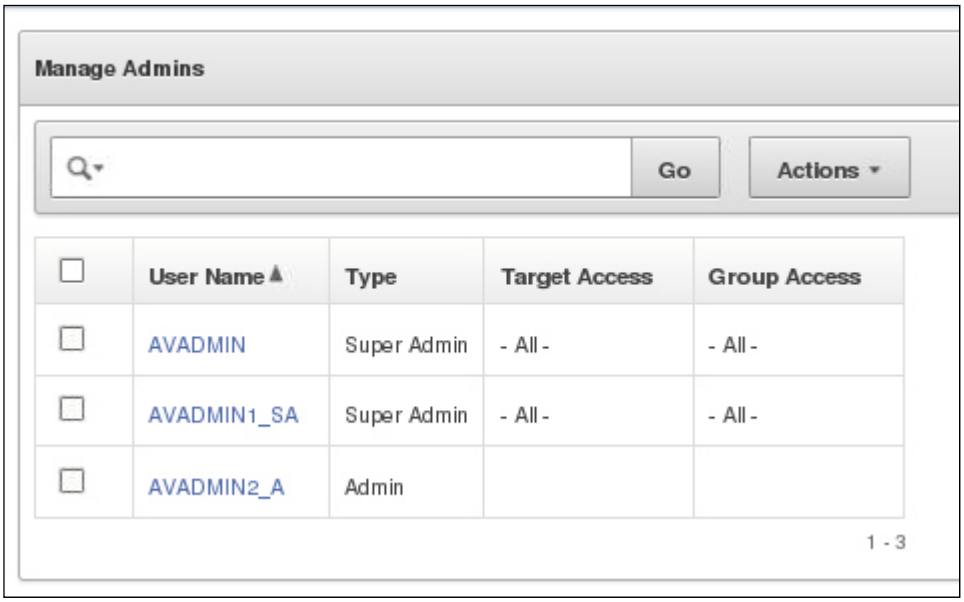

7. Click **Save**.
8. On the Manage Admins page, click **Create**.
9. Enter the following values in the User Name and Password fields:
   - User name: **`AVADMIN2_A`**

- Password: `oracle_4U`

10. In the **Type** drop-down list, select **Admin**.




11. Click **Save**.
12. The Manage Admins page includes the two new user accounts.




13. Log out of the Audit Vault Server console.

# Practice 4-2: Verifying the Server Date and Time Settings

## Overview

In this practice, you verify the settings for the server date and time.

Audit Vault Server stores all data in UTC. If a user is accessing data interactively (for example, using the Audit Vault Server UI or AVCLI command line), all time stamps are in the user's time zone. The time zone is derived from either the user's browser time zone, or if using AVCLI, from the "shell" time zone. If a user is accessing data non-interactively (for example, looking at a PDF report or email generated by the system), time stamps displayed reflect the Time Zone Offset set in the Audit Vault Server Manage page.

## Assumptions

A Firefox browser window is open, and the Oracle Audit Vault and Database Firewall Login page is displayed.

## Tasks

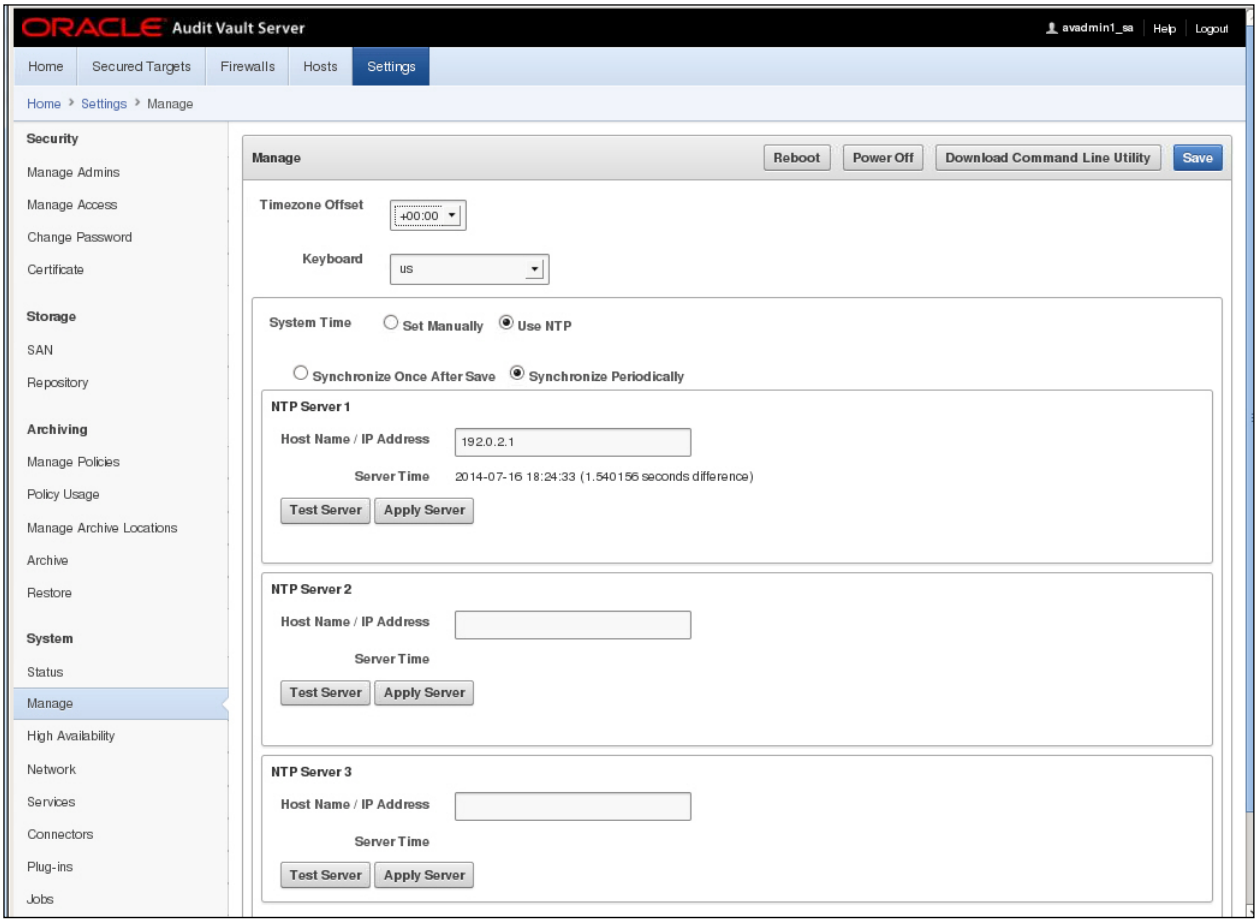
Verify the server date and time by performing the following steps:

1. Log in to the Audit Vault Server console as a super administrator by entering the following values:
   - User: **`AVADMIN1_SA`**
   - Password: **`oracle_4U`**

   Click **Login**.
2. Click the **Settings** tab.
3. In the **System** menu on the left, click **Manage**.
4. From the **Timezone Offset** drop-down list, select (or verify) your local time in relation to Coordinated Universal Time (UTC).

   **Note:** Machines in the Oracle University classroom are set to UTC.
5. In the **System Time** field, select (or verify) **Use NTP**.
6. If you selected Use NTP, select **Synchronize Periodically** in order to start using the NTP Server time. Select **Synchronize Periodically** if you want the time to continue to be synchronized when you click Save.
7. In the NTP Server 1 section, enter (or verify) **192.0.2.1** in the Host Name/IP Address field.

   **Note:** In the Oracle University practice environment, this is the only time server available.
8. If you made changes:
   a. Click **Test Server**.
   b. Click **Apply Server** to update the Audit Vault Server time from this NTP server. The update will not take effect until you click Save.




c. Click **Save**.

d. You will see a Warning message box that states “You may be logged out if the server’s time changes significantly. ….”. Click **Ok**.

9. Log out of the Audit Vault Server or continue to the next practice.

# Practice 4-3: Verifying the Audit Vault Server Network Configuration

## Overview

In this practice, you verify the Audit Vault Server network configuration.

The Oracle AVDF installer configures initial network settings for the Audit Vault Server during installation. You can change the network settings after installation.

## Tasks

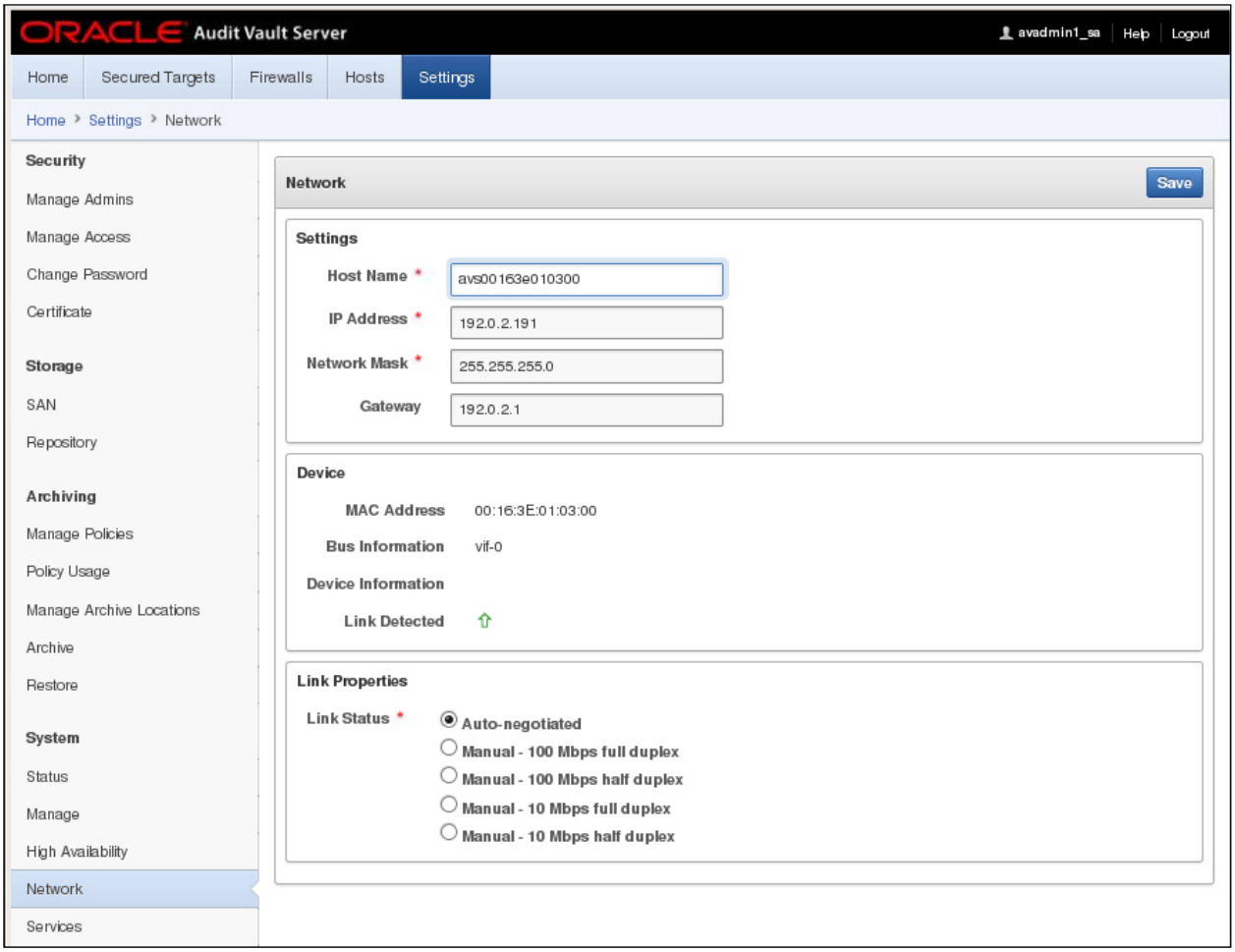
Verify the Audit Vault Server network configuration by performing the following steps:

1. Log in to the Audit Vault Server console as a super administrator by entering the following values:
   - User: **`AVADMIN1_SA`**
   - Password: **`oracle_4U`**
2. Click the **Settings** tab.
3. In the System menu on the left, click **Network**.
4. Review the values on the Network page.

   In a large network environment, it is a good practice to give the Audit Vault Server host a unique name such as provided by default.

   How does the Audit Vault Server create the default host name?

   *The host name is comprised of "avs" and the MAC address from the network card.*




**Warning:** If you make changes to the IP address, you will lose the connection to the appliance. You will have to reconnect using the new IP address.

5. Log out of the Audit Vault Server console or continue to the next practice.

# Practice 4-4: Verifying the Audit Vault Server Services

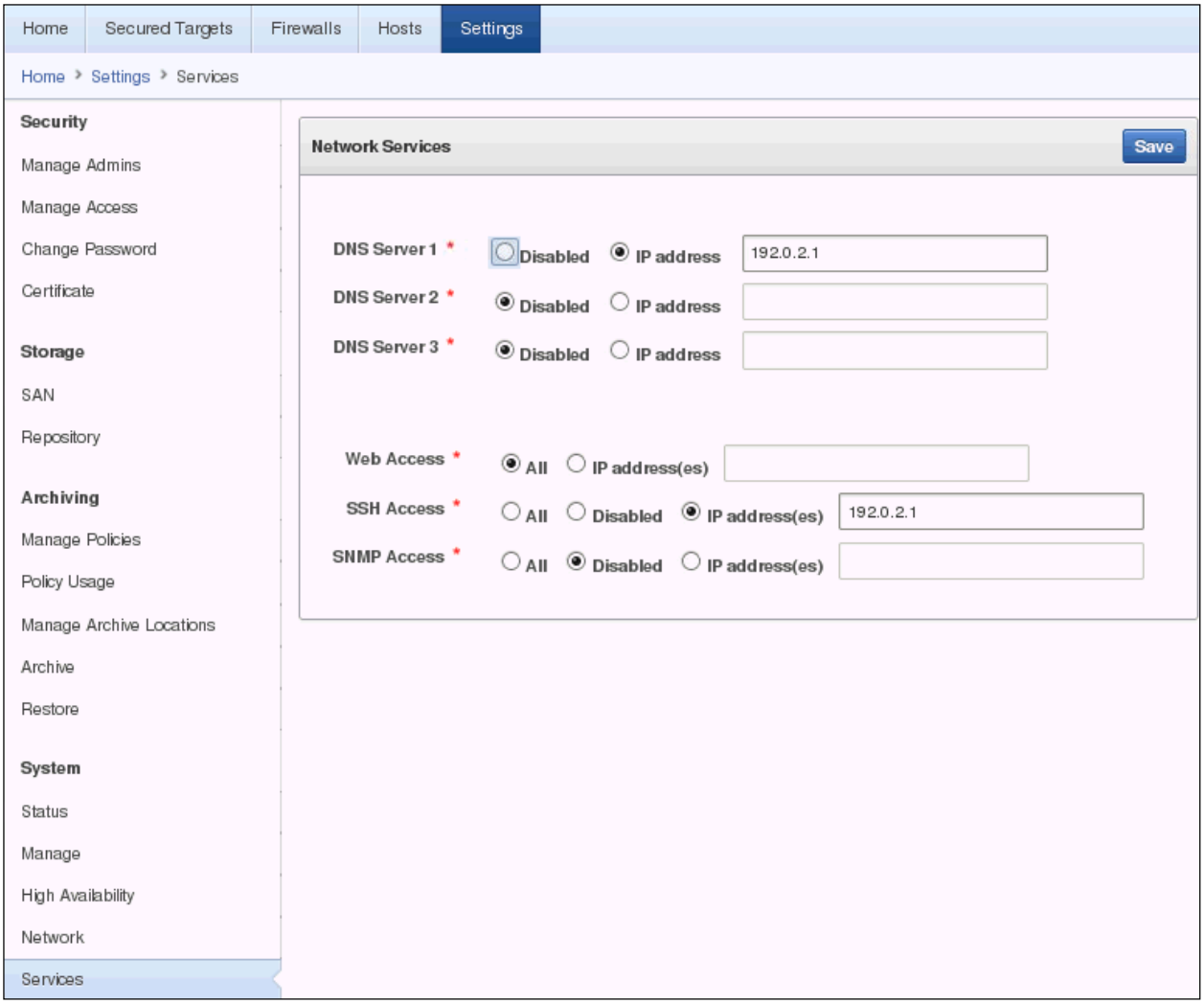
## Overview

In this practice, you verify that the Audit Vault Server services are configured appropriately for your needs.

## Tasks

1. Log in to the Audit Vault Server console as a super administrator by entering the following values:
   - User: **`AVADMIN1_SA`**
   - Password: **`oracle_4U`**
2. Click the **Settings** tab.
3. In the System menu, click **Services**.
4. Complete the following fields as necessary:
   - DNS Server 1: Select **IP address** and verify or enter the value of **192.0.2.1** (**Note:** In the Oracle University practice environment, this is the only DNS server available.)
   - Web Access: Verify that **All** is selected.
   - SSH Access: Select **IP address(es)** and enter the value of **192.0.2.1**.

   **Note:** ssh access to the Audit Vault Server appliance is NOT required for normal activity. It is required for trouble shooting in subsequent practices in this course.
   - SNMP Access: Verify that **Disabled** is selected.




5. Click **Save**.
6. Log out of the Audit Vault Server.

# Practice 4-5: Configuring `syslog` Messages

## Overview

In this practice, you configure syslog messages that will be sent from the Audit Vault Server.

You can configure the following types of syslog messages to be sent from the Audit Vault Server: Alert, debug, info, and system.

## Assumptions

Syslog has been configured on a remote machine to receive syslog messages from a remote machine.

In the Oracle University practice environment, the `em12c` virtual machine (VM) with IP address of 192.0.2.115 is configured to receive syslog messages on port 601 using TCP.

Test for proper configuration as follows:

a. Open a terminal window.

b. Connect to the avsvr VM as the **`support`** user with a password of **`oracle_4U`**.

```
$ ssh support@avsvr
support@avsvr's password:
Last login: Tue May 20 12:37:02 2014 from 192.0.2.1
```

c. Issue the following command:

```
nc –v –w0 192.0.2.115 601 <<< 'testing from avsvr'
```

```
[support@avs00163e010300 ~]$ nc -v -w0 192.0.2.115 601 <<<
'testing from avsvr'
Connection to 192.0.2.115 601 port [tcp/syslog-conn] succeeded!
```

d. Exit the connection to the avsvr VM.

```
[support@avs00163e010300 ~]$ exit
```

e. Connect to the `em12c` VM as the **`root`** user with a password of **`oracle`**.

```
$ ssh root@em12c
The authenticity of host 'em12c (192.0.2.115)' can't be
established.
RSA key fingerprint is
21:bf:3e:55:21:54:a6:5e:04:15:7c:ef:9e:d9:47:7d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'em12c,192.0.2.115' (RSA) to the list
of known hosts.
root@em12c's password:
Last login: Fri Apr 25 15:54:14 2014 from dom0.example.com
```

f. On the `em12c` VM, issue the following command as the `root` user:

```
grep testing /var/log/messages
```

```
[root@em12c ~]# grep testing /var/log/messages
May 20 12:28:57 testing from avsvr
[root@em12c ~]#
```

g. Exit the connection to the em12c VM and close the terminal window.

```
[root@em12c ~]# exit
```

## Tasks

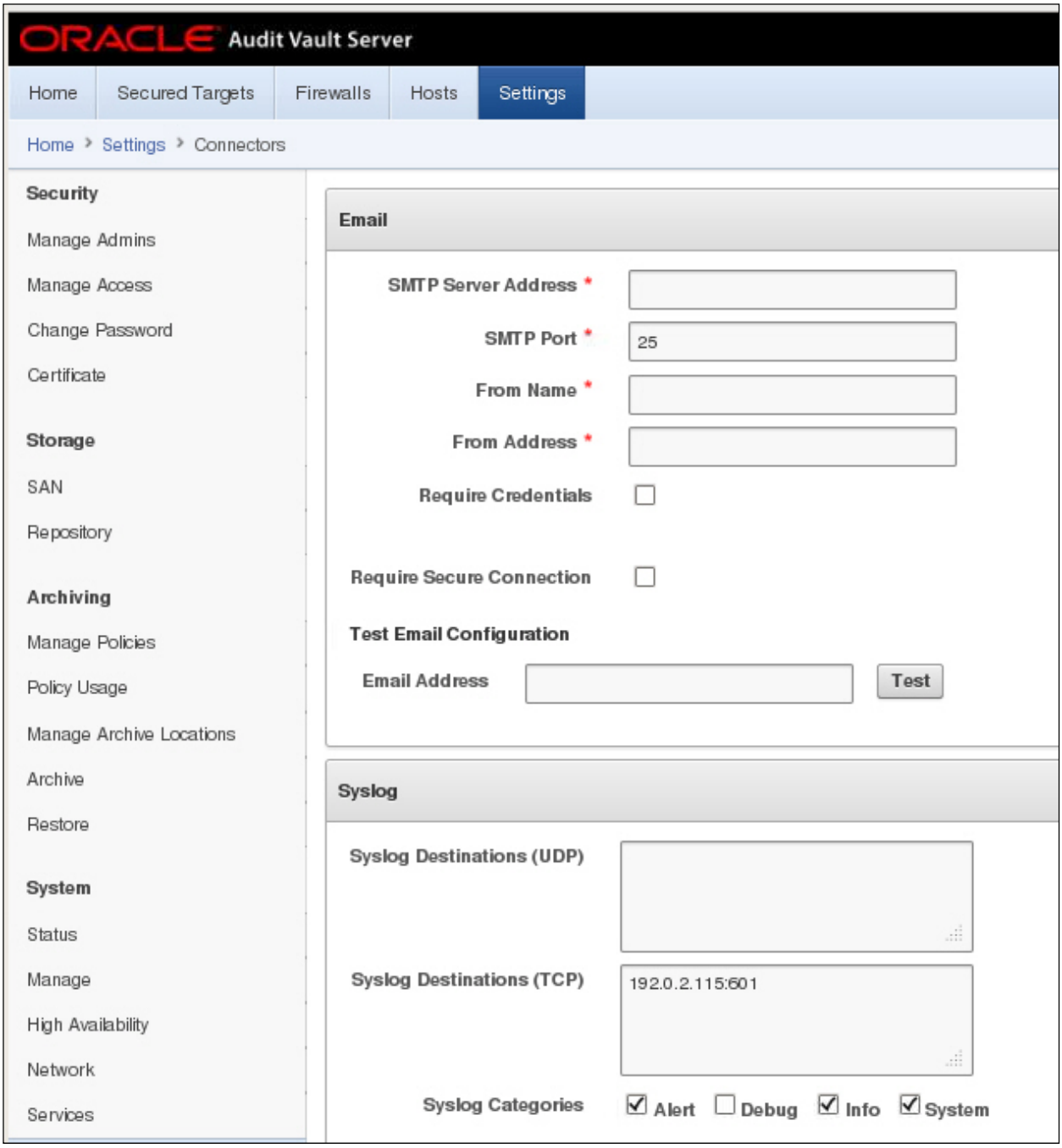
Perform the following steps to configure syslog messages:

1. Log in to the Audit Vault Server console as a super administrator by entering the following values:

   User: **AVADMIN1_SA**

   Password: **oracle_4U**

   Click **Login**.
2. Click the **Settings** tab.
3. In the System menu, click **Connectors**.
4. Scroll down to the **Syslog** section.
5. Complete the following fields:
   - Syslog Destinations (TCP): Enter **192.0.2.115:601**
   - Syslog Categories: Select **Alert, Info, System**




6. Click **Save**.
7. Log out of the Audit Vault Server console.

# Practice 4-6: Defining an Archiving Location

## Overview

In this practice, you define a location for archiving.

You can archive data files in Oracle AVDF as part of your information life cycle strategy. To do so, you must create archiving (or retention) policies, and configure archive locations to which data will be transferred according to the policies.

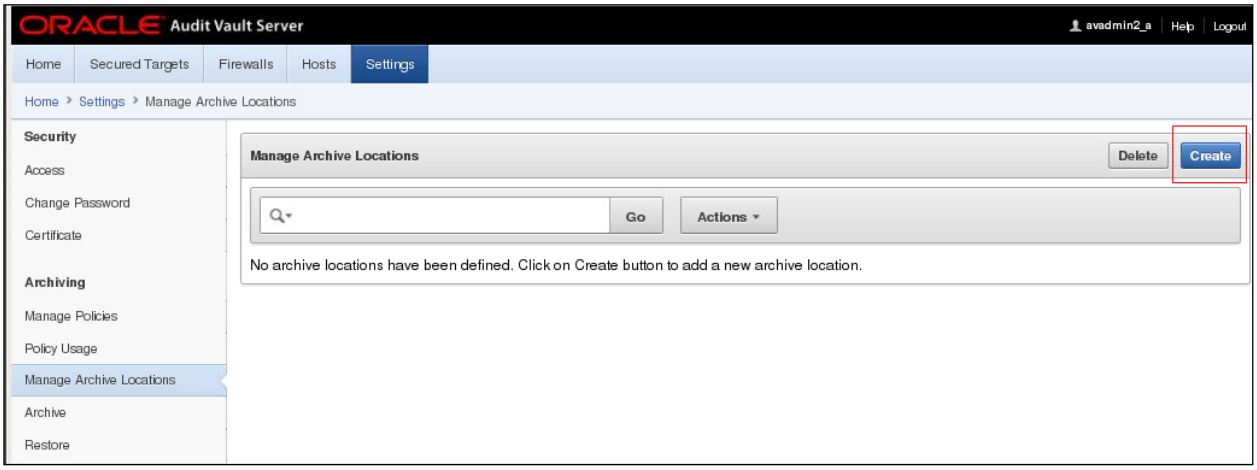
## Assumptions

The `em12c` (192.0.2.115) VM has been configured as an archiving location with a directory named `/u02/archive` dedicated to archiving.

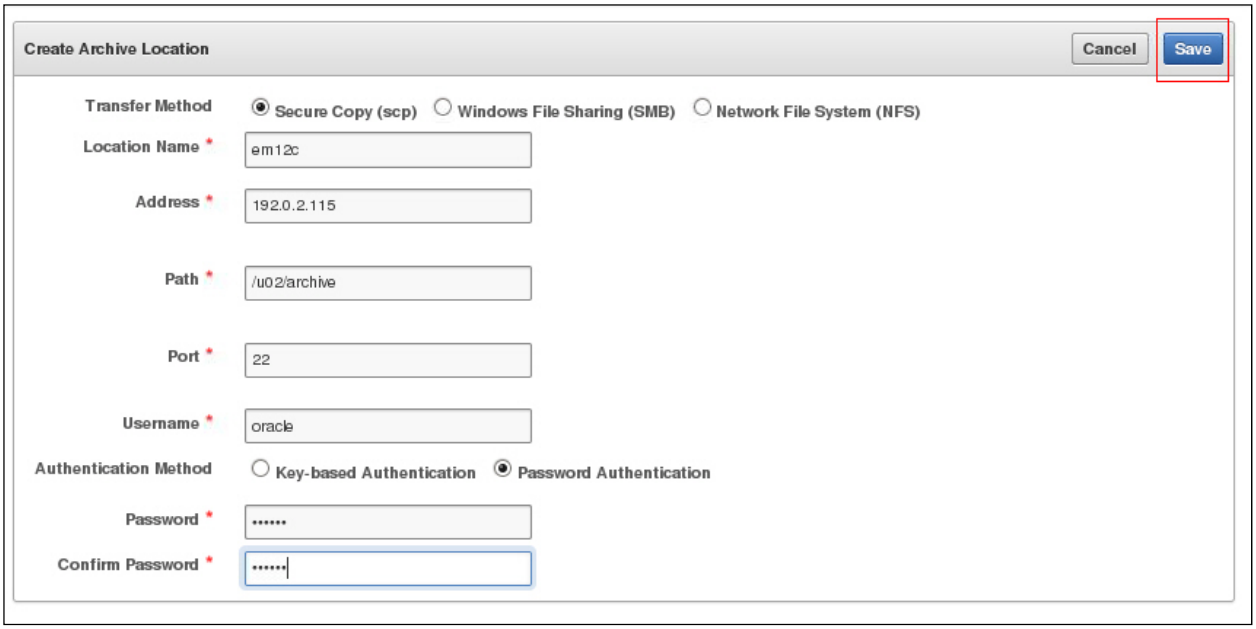
## Tasks

Perform the following steps to define an archive location:

1. Log in to the Audit Vault Server console as an administrator.
   User: **`AVADMIN2_A`**
   Password: **`oracle_4U`**
2. Click the **Settings** tab.
3. Under Archiving, click **Manage Archive Locations**.
4. Click **Create**.




5. Select or enter the following values in the fields on the Create Archive Location page:
   - Transfer Method: **SecureCopy(scp)**
   - Location Name: **em12c**
   - Address: <em12c_IP> **192.0.2.115**
   - Path: **/u02/archive**
   - Port: **22**
   - Username**: oracle**
   - Select **Password Authentication**
   - Password: **oracle**




6. Click **Save**. A message appears confirming the archive destination has been successfully created. The Manage Archive Locations page lists the new location.


7. Log out of the Audit Vault Server console.

# Practice 4-7: Creating Archive Policies

## Overview

In this practice, you define the archiving policy.

You can archive data files in Oracle AVDF as part of your information life cycle strategy. To do so, you must create archiving (or retention) policies, and configure archive locations to which data will be transferred according to the policies.

After you create a retention policy, an Oracle AVDF auditor can apply it to secured targets.

## Assumptions

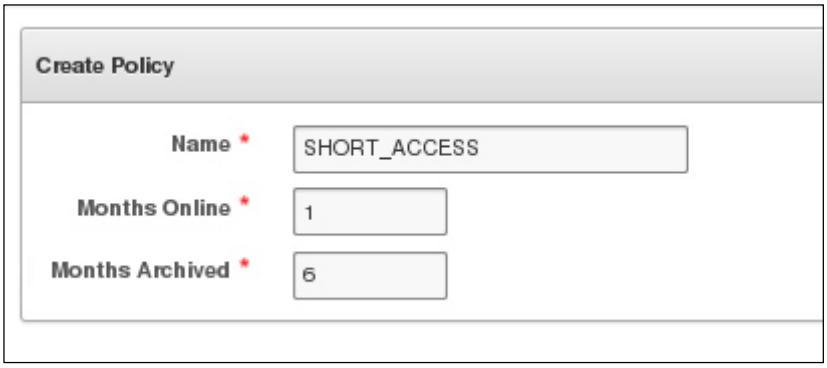
The Archive location has been created.

## Tasks

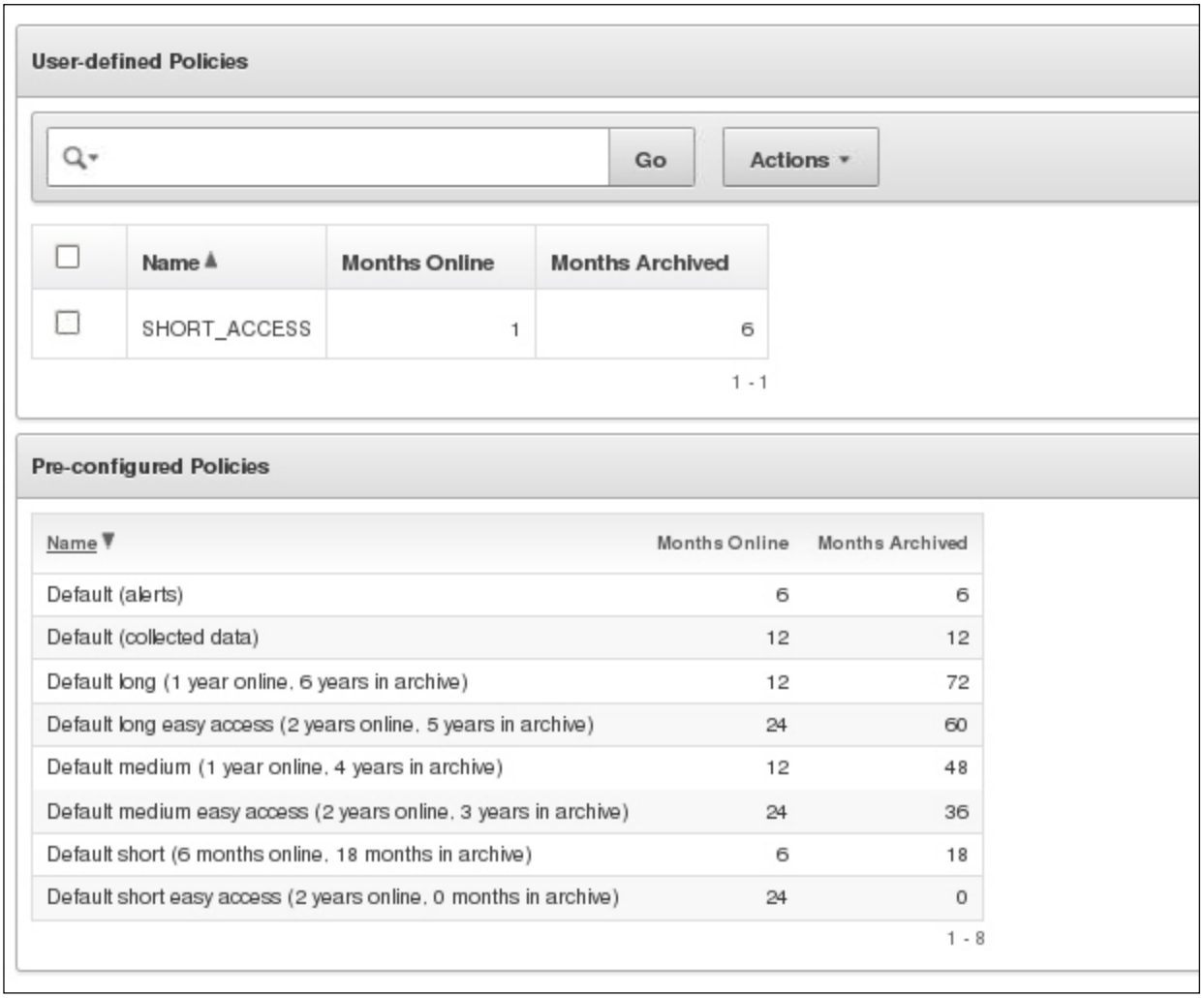
Perform the following steps to create an archiving (retention) policy:

1. Log in to the Audit Vault Server console as a super administrator.
   User: **`AVADMIN1_SA`**
   Password: **`oracle_4U`**
   Click **Login**.
2. Click the **Settings** tab.
3. Under Archiving, select **Manage Policies**.


4. Click the **Create** button.
   **Note:** The **Create** button is not available for an administrator, only for a super administrator.
5. Enter a Name for this policy: **`SHORT_ACCESS`**
6. In the **Months Online** field, enter the number of months to retain audit data in the Audit Vault Server before it is marked for archiving. Enter **1** in the **Months Online** field.
7. In the **Months Archived** field, enter the number of months to retain audit data in the archive location. Enter **6** in the **Months Archived** field.




8. Click **Save**. The new policy is listed in the User-Defined Policies section.




9. Log out of the Audit Vault Server console.

# Practices for Lesson 5: Configuring Oracle AVDF and Deploying the Audit Vault Agent

**Chapter 5**

# Practices for Lesson 5

## Practices Overview

In these practices, you will register the host and deploy the Audit Vault Agent.

# Practice 5-1: Registering the Host

## Overview

In this practice, you register the secured target host machine with the Audit Vault Server.

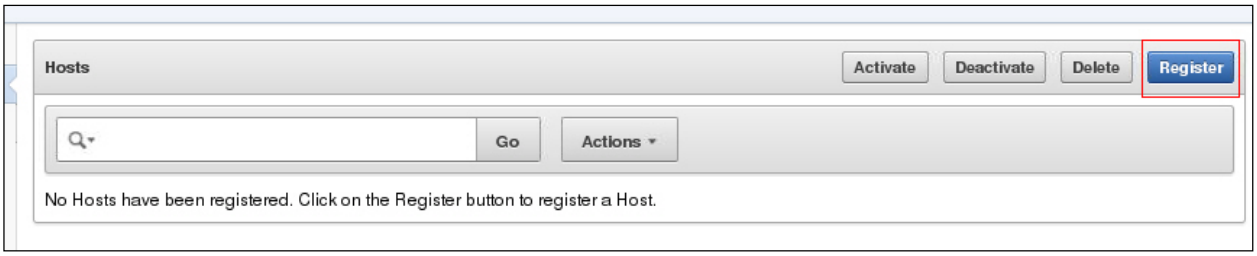
If you want to collect audit data from a secured target, you must configure a connection between the Audit Vault Server and the host machine where the Audit Vault Agent resides for that secured target (usually the same computer as the secured target).

## Tasks

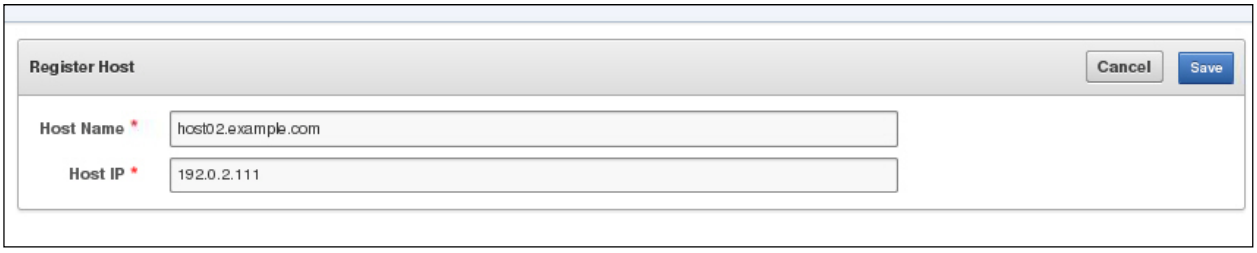
Perform the following steps to register a host machine in the Audit Vault Server:

1. Log in to the Audit Vault Server console as an administrator.
   - Username: **`AVADMIN2_A`**
   - Password: **`oracle_4U`**

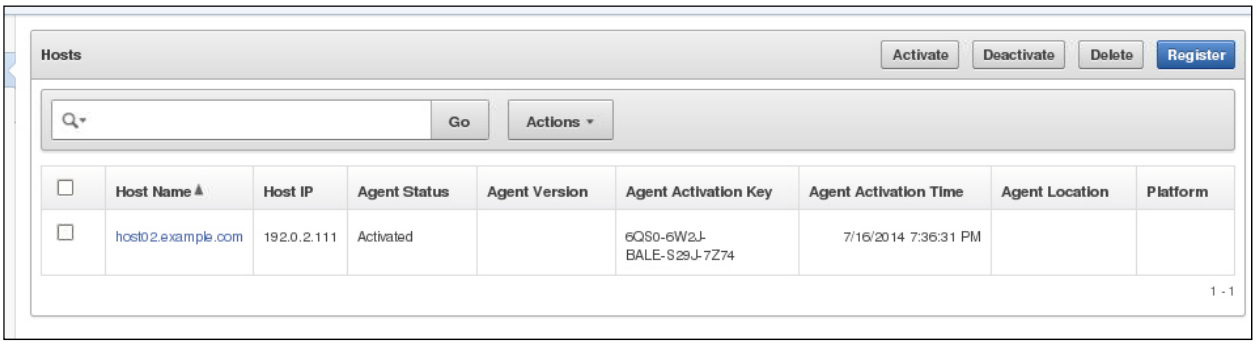
   Click **Login**.
2. Click the **Hosts** tab.
3. Click **Register**.




4. Enter the **Host Name** and **Host IP address** as follows:
   - Host name: **`host02.example.com`**
   - IP address: **`192.0.2.111`**




5. Click **Save**. A confirmation message appears stating “Host registered successfully.” The Hosts page lists the newly registered host.




6. Log out of the Audit Vault Server console.

# Practice 5-2: Deploying the Audit Vault Agent on the Host

## Overview

In this practice, you deploy the Audit Vault agent on the host machine.

To collect audit trails from secured targets, you must deploy the Audit Vault Agent on a host computer, usually the same computer where the secured target resides. The Audit Vault Agent includes plug-ins for each secured target type, as well as host monitoring functionality.

You must use an OS user account to deploy the Audit Vault Agent. In this step, you copy the `agent.jar` file from the Audit Vault Server and deploy this file on the target machine.

Up to this point the browser could have been invoked from anywhere. For this practice, the browser must be started on the host02 VM, so that the agent will download from the avsvr to the host02 (target) machine.

## Tasks

Perform the following steps to copy the `agent.jar` file and deploy the Audit Vault Agent to the host machine:

1. Close the browser if it is open.
2. Open a terminal window.
3. At the `bash` operating system prompt, enter the following command:

   **`ssh -X oracle@host02`**

   The password for the `oracle` user is **`oracle`**.

   **Note:** The `-X` option enables port forwarding to allow the X-based graphics to display on the desktop where the `ssh` process was started.

```
$ ssh -X oracle@host02
The authenticity of host 'host02 (192.0.2.111)' can't be
established.
RSA key fingerprint is
b6:f7:35:01:50:43:8b:97:73:73:c6:cc:c6:ee:d5:2d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'host02' (RSA) to the list of known
hosts.
oracle@host02's password:
Last login: Thu May 15 20:44:49 2014 from 192.0.2.1
[oracle@host02 ~]$
```

4. Start Firefox.

```
[oracle@host02 ~]$ firefox
```

5. Log in to the Audit Vault Server console as an administrator.
   a. Enter the following URL: https://192.0.2.191
   b. In the Untrusted Connection dialog, click **I Understand the Risks** and then click **Add Exception**.
   c. In the Add Security Exception dialog, click **Confirm Security Exception**.
   d. In the Browser menu, click **Edit > Preferences**.
   e. In the Firefox Preferences Dialog, click the **General** tab and then select **Always ask me where to save files**.

f. **Close** the Preferences dialog.

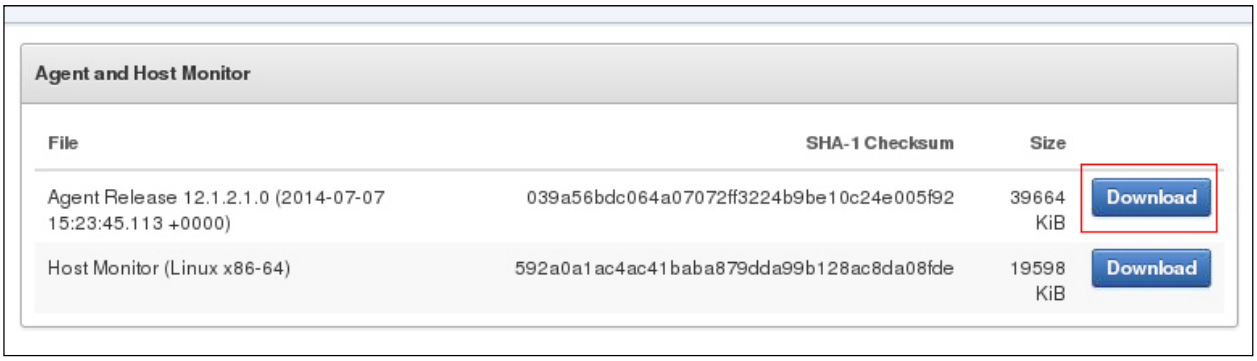
g. Log in to the Audit Vault Server console as an administrator by entering the following values:

- User Name: **`AVADMIN2_A`**
- Password: **`oracle_4U`**

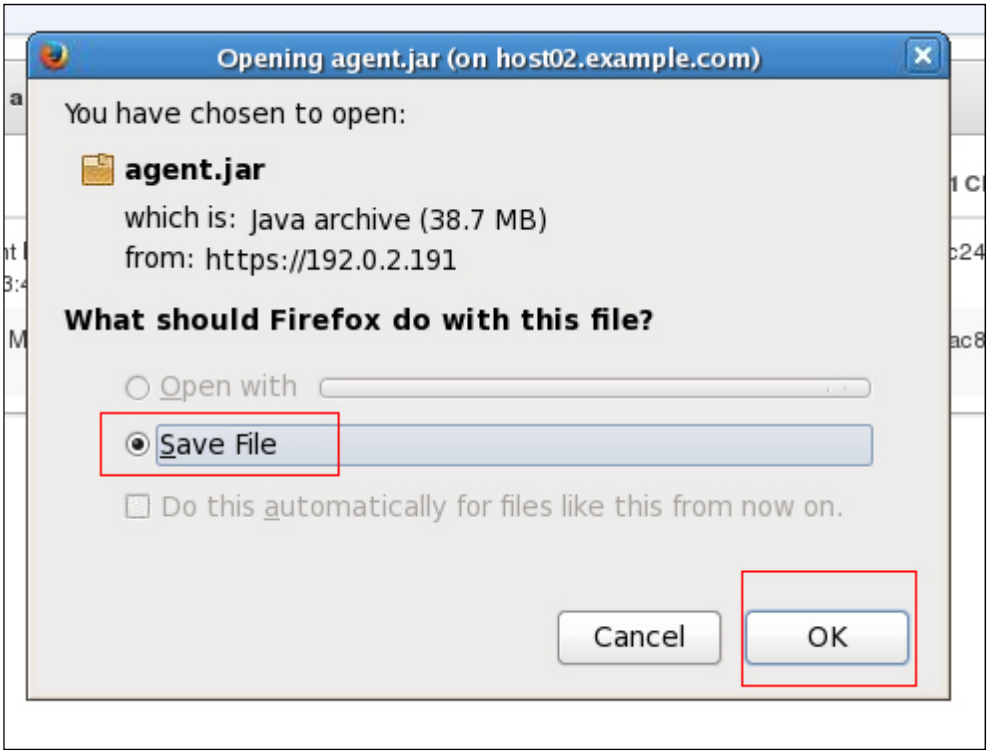
Click **Login**.

6. Click the **Hosts** tab.
7. In the Hosts menu on the left, click **Agent**.
8. Click the **Download** button next to the Agent file, and then save the **`agent.jar`** file to the following location: **/home/oracle**.

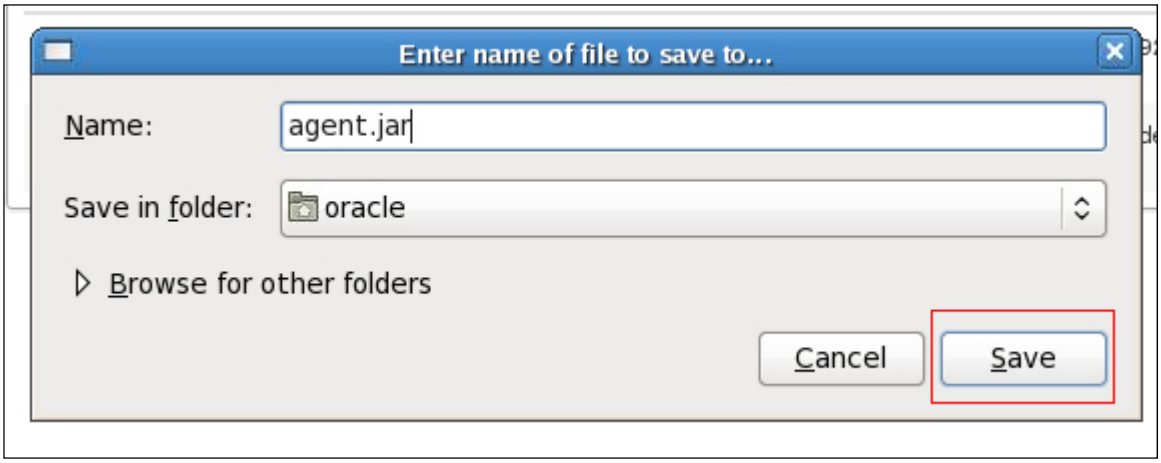
a. Click the **Download** button.




b. In the Opening … dialog, select **Save File** and click **OK**.




c. In the Enter name of file … dialog, enter **agent.jar** in the Name field. Enter **oracle** in the "Save in folder" field. Then click **Save**.




9. When the download is complete, log out of the Audit Vault Server console and close the Firefox browser.
10. In the terminal window on the **host02** machine, set **JAVA_HOME** to the installation directory of the `jdk1.6` (or higher version), and make sure the Java executable corresponds to this `JAVA_HOME` setting.
    a. In the terminal window as the `oracle` user on `host02`, determine the Java version by using the following command: **java -version**

```
[oracle@host02 ~]$ java -version
java version "1.7.0_51"
OpenJDK Runtime Environment (rhel-2.4.4.1.0.1.el6_5-x86_64 u51-b02)
OpenJDK 64-Bit Server VM (build 24.45-b08, mixed mode)
```

    b. Determine the installation directory by using the following command: **which java**

```
[oracle@host02 ~]$ which java
/usr/bin/java
```

    c. Set the **JAVA_HOME** environment variable as shown in the code box.

```
[oracle@host02 ~]$ export JAVA_HOME=/usr
```

11. In the directory where you placed the `agent.jar` file, extract it by executing the following command: **java -jar agent.jar -d Agent_Home**
    a. Change directory to the directory where you placed the `agent.jar` file.

```
[oracle@host02 ~]$ cd /home/oracle
[oracle@host02 ~]$ ls
afiedt.buf  Desktop    Downloads  oradiag_oracle  Public
Videos
agent.jar   Documents  Music      Pictures        Templates
```

    b. Extract the agent.

```
[oracle@host02 ~]$ java -jar agent.jar -d Agent_Home
Checking for updates...
Agent is updating. This operation may take a few minutes. Please wait...
Agent updated successfully.
```

```
Agent installed successfully.
If deploying hostmonitor please refer to product documentation
for additional installation steps.
```

c. **If the extract of the agent worked correctly, proceed to Practice 5-3.** If you encountered a corrupt file when executing the `java` command, proceed to the next step in this practice.

12. **Perform this step only if you encountered a problem with the `java` command in step 11b.** If the `java` command indicated the file is corrupt, perform the following steps to use transfer the file and extract the file.

a. In a terminal window, execute the command shown in the code box to transfer the `agent.jar` file. The support user's password is `oracle_4U` and the Oracle user's password is `oracle`.

```
$ scp support@avsvr:/var/lib/oracle/dbfw/av/jlib/agent.jar
oracle@host02:/home/oracle/agent.jar
support@avsvr's password:
The authenticity of host 'host02 (192.0.2.111)' can't be
established.
RSA key fingerprint is
b6:f7:35:01:50:43:8b:97:73:73:c6:cc:c6:ee:d5:2d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'host02,192.0.2.111' (RSA) to the
list of known hosts.
oracle@host02's password:
agent.jar                     100%   39MB  12.9MB/s   00:03
Connection to avsvr closed.
```

b. Extract the agent.

```
[oracle@host02 ~]$ java -jar agent.jar -d Agent_Home
Checking for updates...
Agent is updating. This operation may take a few minutes. Please
wait...
Agent updated successfully.
Agent installed successfully.
If deploying hostmonitor please refer to product documentation
for additional installation steps.
```

c. Log in to the Audit Vault Server console as the **`AVADMIN1_SA`** user to activate the Host. In the host window, select the **host.02.example.com** row and click **Activate**.

d. Click OK in the 'Are you sure…' dialog.

e. Log out of the Audit Vault Server console.

# Practice 5-3: Activating the Audit Vault Agent

## Overview

In this practice, you activate the Audit Vault Agent with the Agent Activation Key and start the Agent.

## Assumptions

Practice 5-1 or host registration must be completed before this practice.

## Tasks

Perform the following steps to activate the Audit Vault Agent and start the Agent:

1. In the em12c VM window, start Firefox.

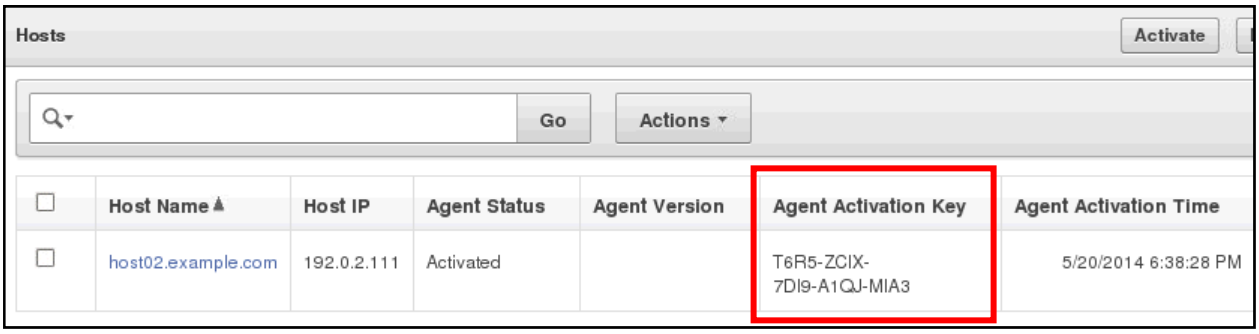
```
[oracle@em12c ~]$ firefox
```

2. Enter the URL for the Audit Vault Console: https://192.0.2.191
3. Log in to the Audit Vault Server console as an administrator.
   - User Name: **AVADMIN2_A**
   - Password: **oracle_4U**

   Click **Login**.
4. Click the **Hosts** tab.
5. Make a note of the **Agent Activation Key** for this host. You can use the browser copy (Edit > Copy) to copy the value.

   Agent Activation Key: _____

   **Note:** The Agent activation Key is unique for each host.




6. In a terminal window on the **host02** machine, change directory to the **/home/oracle/Agent_Home/bin** directory as shown in the code box.

```
[oracle@host02 ~]$ cd ~/Agent_Home/bin
```

7. Execute the following command and provide the Agent Activation Key when prompted: `agentctl start -k`

   **Note:** Enter the Activation Key as it is shown, including dashes and capitalization. You can use the window paste feature (Edit > Paste). Note that the Activation Key is NOT echoed.

```
[oracle@host02 bin]$ ./agentctl start -k
Enter Activation Key:
Agent started successfully.
[oracle@host02 bin]$
```

# Practice 5-4: Creating User Accounts on the Secured Target

## Overview

In this practice, you create a user account for Oracle Audit Vault and Database Firewall (Oracle AVDF) in the Oracle Database 12*c* database.

You must set up a user account with appropriate privileges on each secured target for Oracle AVDF to use in performing functions related to monitoring and collecting audit data. Oracle AVDF includes setup scripts for database secured targets.

## Tasks

Perform the following steps to set up Oracle AVDF user privileges on the Oracle Database 12*c* secured target:

1. In a terminal window on the `host02` machine logged in as the `oracle` user, create a user account for Oracle AVDF in the Oracle Database. You will use this username and password when registering this Oracle Database as a secured target in the Audit Vault Server.
   a. At the operating system prompt, use the **`oraenv`** utility to set the environment to the `orcl` database.

```
[oracle@host02 ~]$ cat /etc/oratab
…
orcl:/u01/app/oracle/product/12.1.0/dbhome_140115:N
[oracle@host02 ~]$ . oraenv
ORACLE_SID = [oracle] ? orcl
The Oracle base has been set to /u01/app/oracle
-bash: [: /u01/app/oracle: integer expression expected
```

   b. Change directory to `/home/oracle/Agent_Home/av/plugins/co.oracle.av.plugins.oracle/config`.

```
[oracle@host02 ~]$ cd
/home/oracle/Agent_Home/av/plugins/com.oracle.av.plugin.oracle/config
```

   c. Log in to SQL*Plus as the **`SYSTEM`** user with a password of **`oracle_4U`**.

```
[oracle@host02 ~]$ sqlplus system/oracle_4U

SQL*Plus: Release 12.1.0.1.0 Production on Mon Apr 28 17:40:38
2014

Copyright (c) 1982, 2014, Oracle.  All rights reserved.


Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.1.0 -
64bit Beta
With the Partitioning, OLAP, Advanced Analytics and Real
Application Testing options
```

d. Execute the **CREATE USER** command to create a new user as follows: **CREATE USER avdfuser IDENTIFIED BY avdfpass**

```
SQL> CREATE USER avdfuser IDENTIFIED BY avdfpass;

User created.
```

2. Connect as the SYS user with the SYSDBA privilege by executing the following command: **CONNECT / AS SYSDBA**

```
SQL> CONNECT / AS SYSDBA
Connected.
```

3. Execute the setup script as follows: **@oracle_user_setup.sql avdfuser SETUP**

```
SQL> @oracle_user_setup.sql avdfuser SETUP
Granting privileges to AVDFUSER ... Done.
Disconnected from Oracle Database 12c Enterprise Edition Release
12.1.0.1.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real
Application Testing options
[oracle@host02 ~]$
```

# Practice 5-5: Registering the Secured Target

## Overview

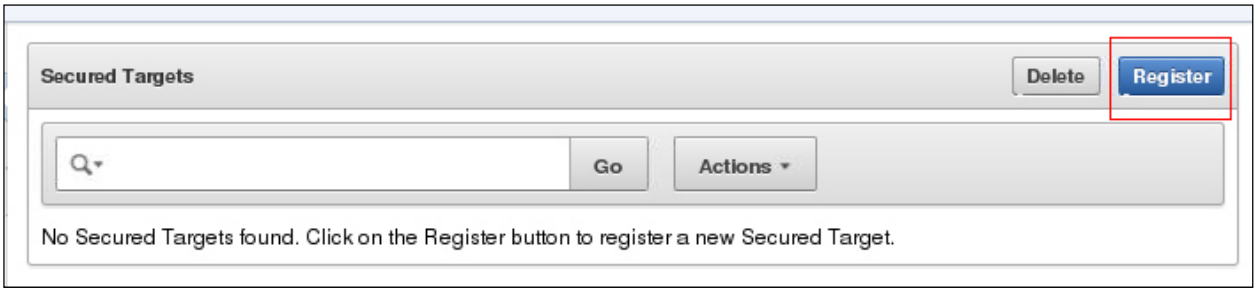
In this practice, you register the Oracle Database 12*c* secured target with the Audit Vault Server.

Secured targets can be supported databases or operating systems that Audit Vault and Database Firewall monitors. You must register all secured targets in the Audit Vault Server, regardless of whether you are deploying the Audit Vault Agent, the Database Firewall, or both.

## Tasks

Perform the following steps to register the Oracle Database 12*c* database with the Audit Vault Server.

1. Log in to the Audit Vault Server console as the administrator user **`AVADMIN2_A`**.
2. Click the **Secured Targets** tab.
3. Click **Register**.

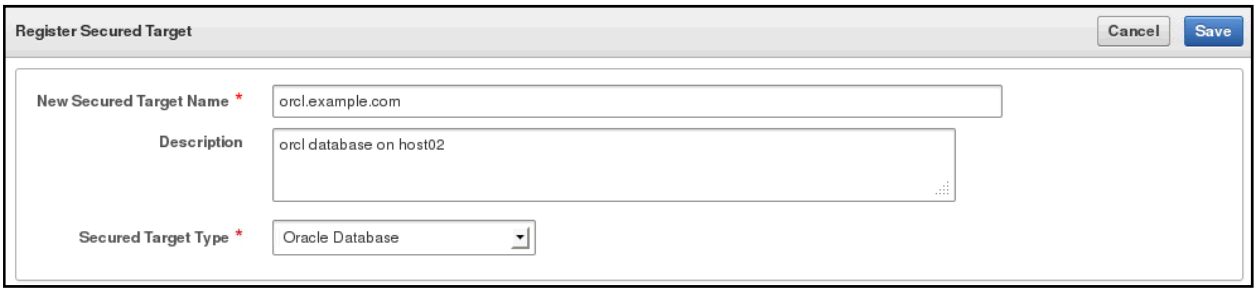



4. On the Register Secured Target page, enter a new secured target name and optional description for the new target as follows:

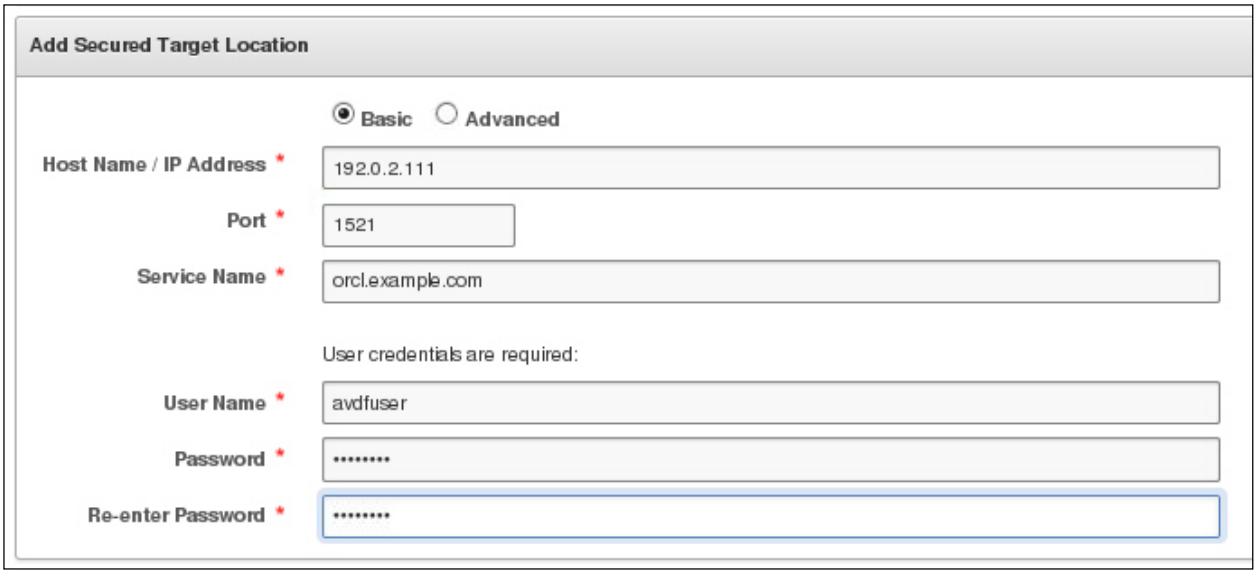
   New Secured Target Name: **`orcl.example.com`**

   Description: **`orcl database instance on host02`**

5. In the Secured Target Type menu, select the secured target type of **Oracle Database**.

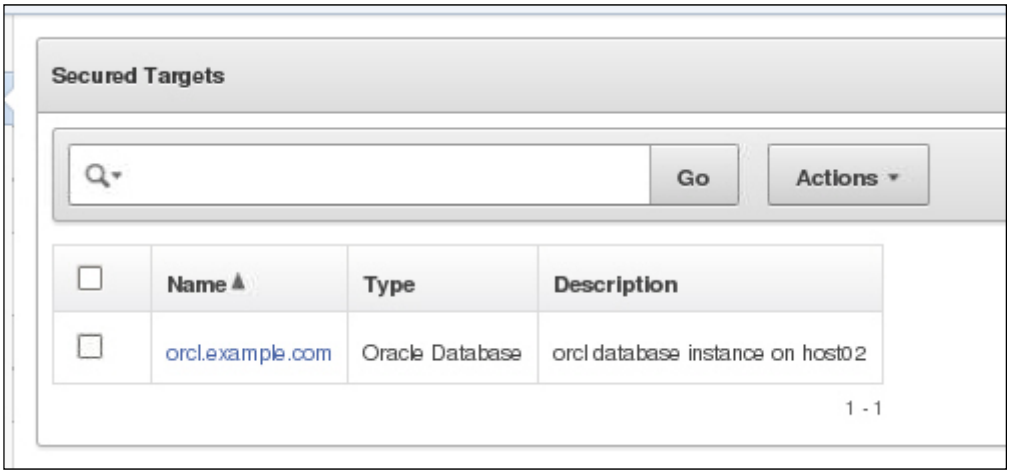



6. In the **Add Secured Target Location** section, enter the IP address, port, and the service name.
   - IP Address: **192.0.2.111**
   - Port: **1521**
   - Service Name: **`orcl.example.com`**
7. Enter the credentials for the secured target user account you created for Oracle AVDF.
   - User Name: **`avdfuser`**
   - Password: **`avdfpass`**




8. In the Add Secured Target Addresses section, enter the IP address, port number, and service name. Click **Add**.


9. Click **Save**. A confirmation appears briefly. The Secured Targets page lists the new secured target.




10. Log out of the Audit Vault Server console or continue to the next practice.

# Practice 5-6: Configuring an Audit Trail for the Secured Target

## Overview

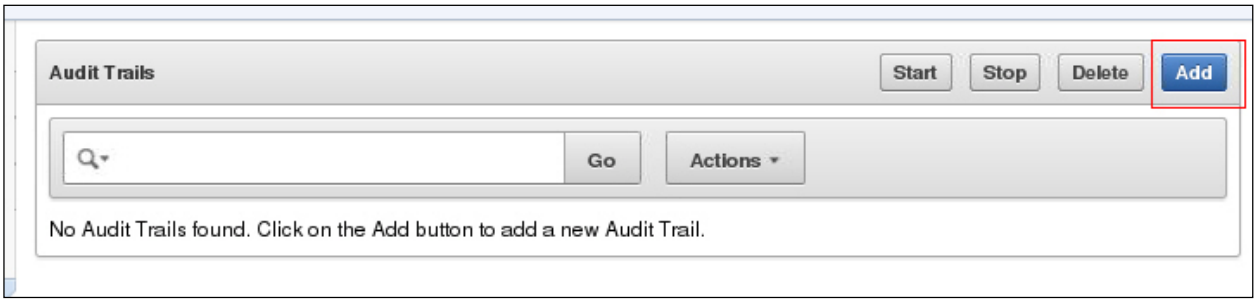
In this practice, you configure an audit trail for the Oracle Database 12*c* secured target.

To start collecting audit data, you must configure an audit trail for each secured target in the Audit Vault Server, and then start the audit trail collection manually.

## Tasks

Perform the following steps to configure an audit trail for the Oracle Database 12*c* secured target in the Audit Vault Server.

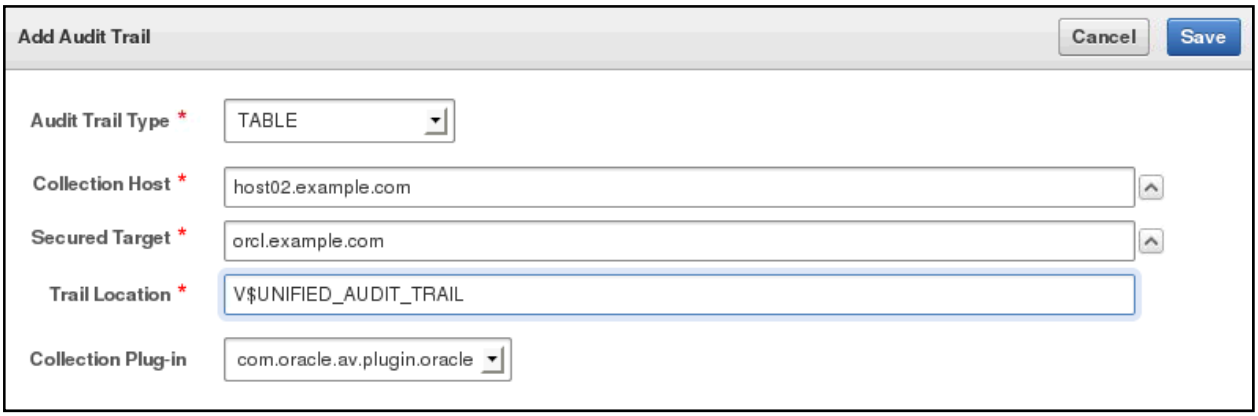
1. Log in to the Audit Vault Server console as the administrator user **`AVADMIN2_A`**.
2. Click the **Secured Targets** tab.
3. Under Monitoring, click **Audit Trails**.
4. On the Audit Trails page, click **Add**.



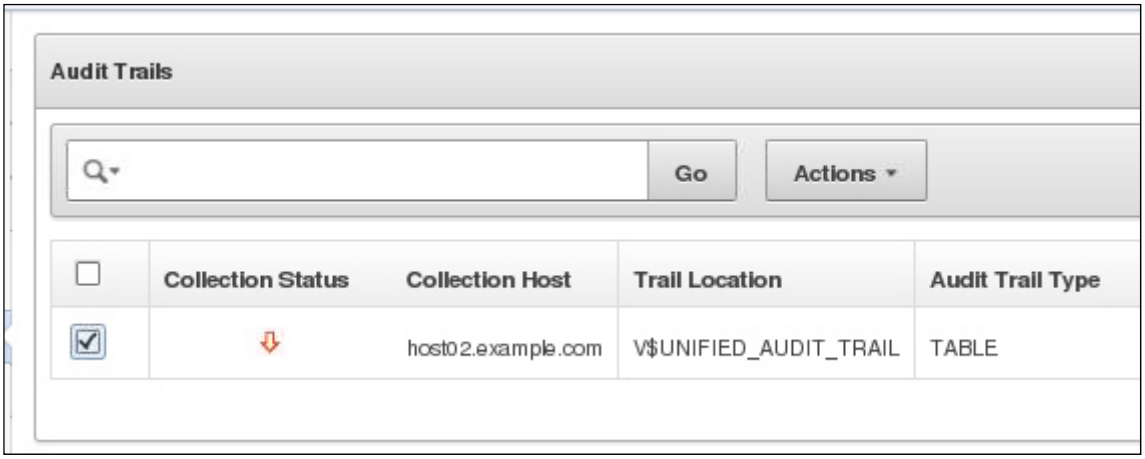

5. In the Audit Trail Type drop-down list, select **TABLE**.
6. In the Collection Host field, click the up-arrow icon to display a search box. Select the host computer where the Audit Vault Agent is deployed.


7. In the Secured Target field, click the up-arrow icon to display a search box. Select the secured target.


8. In the Trail Location field, enter the location of the audit trail on the secured target computer: **`V$UNIFIED_AUDIT_TRAIL`**




9. Click **Save**. A confirmation message appears. Although the Collection Status indicates the audit trail is not yet started, it will start automatically after a short period of time.




10. Log out of the Audit Vault Server console.

# Practice 5-7: Configuring Stored Procedure Auditing

## Overview

In this practice, you configure stored procedure auditing for the Oracle Database 12*c* database secured target.

Stored procedure auditing (SPA) enables Oracle AVDF auditors to audit changes to stored procedures on secured target databases. Oracle AVDF connects to the database server at scheduled intervals and discovers any changes or additions that have been made to stored procedures. SPA is supported for all database secured targets supported by Oracle AVDF.

To enable SPA, you configure the user account privileges necessary for Oracle AVDF to perform stored procedure auditing on a secured target. Oracle AVDF includes scripts for setting up these privileges.

## Assumptions

The `AVDFUSER` user was created in Practice 5-4.

## Tasks

Perform the following steps to configure stored procedure auditing for the Oracle Database 12*c* database secured target.

1. In a terminal window on `host02` as the `oracle` user, change directory to **`Agent_Home/av/plugins/com.oracle.av.plugin.oracle/config/`** as shown.

```
[oracle@host02 ~]$ cd
~/Agent_Home/av/plugins/com.oracle.av.plugin.oracle/config/
[oracle@host02 config]$
```

2. Invoke SQL*Plus and log in as the **`SYS`** user with the **`SYSDBA`** privilege.

```
[oracle@host02 config]$ sqlplus / as sysdba
…
Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.1.0 -
64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real
Application Testing options
```

3. Execute the setup script as follows:

**`@oracle_user_setup.sql avdfuser SPA`**

```
SQL> @oracle_user_setup.sql avdfuser SPA
Granting privileges to AVDFUSER ... Done.
Disconnected from Oracle Database 12c Enterprise Edition Release
12.1.0.1.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real
Application Testing options
[oracle@host02 config]$
```

# Practices for Lesson 6: Networking and Oracle AVDF

**Chapter 6**

# Practices for Lesson 6

## Practices Overview

In these practices, you will review requirements for a Database Firewall configuration. You will use various diagnostics tools.

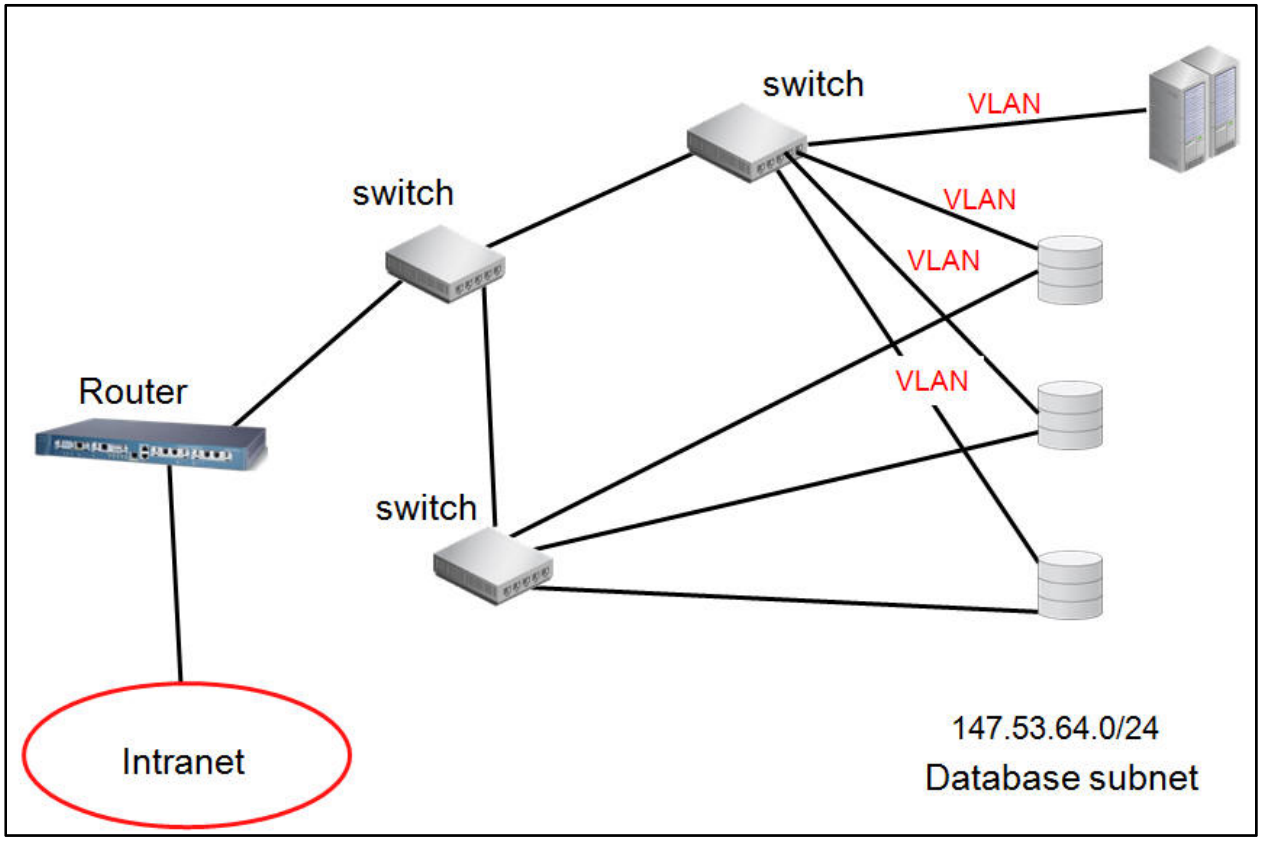
# Practice 6-1: Configuring Database Firewall

## Overview

In this pen-and-paper practice, you describe the appropriate Oracle Database Firewall configuration given a set of requirements.

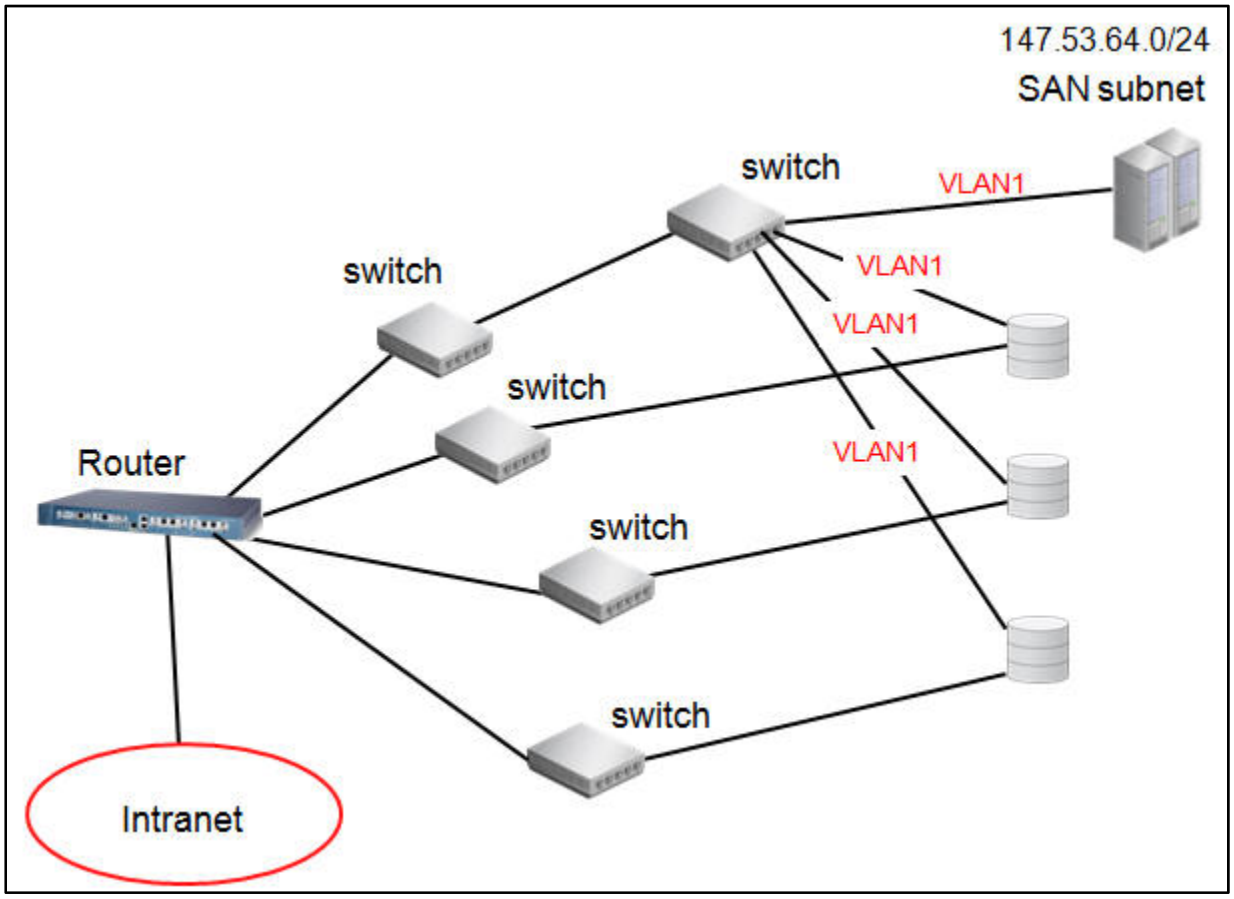
## Tasks

1. Review the diagram below and the notes:
   a. There are three databases all in the same subnet 147.53.64.xxx. Each database is behind a separate switch that includes VLANS for a SAN network for storage array for all three databases.
   b. The concern is that disgruntled employees, and third parties with internal access could introduce database exploits accessing the databases through the application servers and ad-hoc tools.
   c. No access to the database servers is allowed through remote terminals. DBA access is allowed only though a local login, a console attached to the server.
   d. The database machines are in a secure room.




2. Draw in the positioning of the database firewall. How many DBFW appliances will you use?
3. What mode will you use for the Database Firewall?
4. Review the following diagram and the notes:
   a. There are multiple databases on different subnets. Each database is behind a separate switch that includes VLANS for a SAN network for storage array for all three databases.

b. The goal is to certify compliance to government regulations that SQL accessing a set of tables containing sensitive information is logged and alerted.
c. No access to the database servers is allowed through remote terminals. DBA access is allowed only through a local login, a console attached to the server.
d. The database machines are in a secure room.




5. Draw in the positioning of the database firewall. How many DBFW appliances will you use?
6. What mode will you use for the Database Firewall?

# Practice 6-2: Using Network Diagnostic Tools

## Overview

In this practice, you use basic networking troubleshooting tools such as `ping`, `tnsping`, `tcpdump`, `netcat(nc)`, and `nslookup`. Each tool is used to discover configuration information about each OSI layer.

## Tasks

1. From a terminal session on the em12c VM, use `ping` to verify connectivity and host resolution.
   a. Use `ping` to send four packets to `192.0.2.101`. Record the average time_____.

```
$ ping 192.0.2.101 -c 4
PING 192.0.2.101 (192.0.2.101) 56(84) bytes of data.
64 bytes from 192.0.2.101: icmp_seq=1 ttl=64 time=0.161 ms
64 bytes from 192.0.2.101: icmp_seq=2 ttl=64 time=0.128 ms
64 bytes from 192.0.2.101: icmp_seq=3 ttl=64 time=0.176 ms
64 bytes from 192.0.2.101: icmp_seq=4 ttl=64 time=0.186 ms

--- 192.0.2.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.128/0.162/0.186/0.026 ms
```

   b. Use `ping` to send four packets to `dbfw`. Record the average time_____.

```
$ ping -c 4 dbfw
PING dbfw.example.com (192.0.2.101) 56(84) bytes of data.
64 bytes from dbfw.example.com (192.0.2.101): icmp_seq=1 ttl=64
time=0.159 ms
64 bytes from dbfw.example.com (192.0.2.101): icmp_seq=2 ttl=64
time=0.196 ms
64 bytes from dbfw.example.com (192.0.2.101): icmp_seq=3 ttl=64
time=0.187 ms
64 bytes from dbfw.example.com (192.0.2.101): icmp_seq=4 ttl=64
time=0.178 ms

--- dbfw.example.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.159/0.180/0.196/0.013 ms
```

   c. Why is the average time different? *The extra time taken could be due to host resolution*.
   d. Use `ping` to send four packets to `192.0.2.111`. Record the average time_____.

```
# ping 192.0.2.111 -c 4
PING 192.0.2.111 (192.0.2.111) 56(84) bytes of data.
```

```
64 bytes from 192.0.2.111: icmp_seq=1 ttl=64 time=0.159 ms
64 bytes from 192.0.2.111: icmp_seq=2 ttl=64 time=0.206 ms
64 bytes from 192.0.2.111: icmp_seq=3 ttl=64 time=0.238 ms
64 bytes from 192.0.2.111: icmp_seq=4 ttl=64 time=0.276 ms

--- 192.0.2.111 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.159/0.219/0.276/0.046 ms
```

e. Use `ping` to send four packets to `host02`. Record the average time_____.

```
$ ping host02 -c 4
PING host02.example.com (192.0.2.111) 56(84) bytes of data.
64 bytes from host02.example.com (192.0.2.111): icmp_seq=1
ttl=64 time=0.173 ms
64 bytes from host02.example.com (192.0.2.111): icmp_seq=2
ttl=64 time=0.196 ms
64 bytes from host02.example.com (192.0.2.111): icmp_seq=3
ttl=64 time=0.179 ms
64 bytes from host02.example.com (192.0.2.111): icmp_seq=4
ttl=64 time=0.202 ms

--- host02.example.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.173/0.187/0.202/0.018 ms
```

f. Use `ping` to send four packets to `192.0.2.191`. Record the average time_____.

```
$ ping -c 4 192.0.2.191
PING 192.0.2.191 (192.0.2.191) 56(84) bytes of data.
64 bytes from 192.0.2.191: icmp_seq=1 ttl=64 time=0.158 ms
64 bytes from 192.0.2.191: icmp_seq=2 ttl=64 time=0.204 ms
64 bytes from 192.0.2.191: icmp_seq=3 ttl=64 time=0.181 ms
64 bytes from 192.0.2.191: icmp_seq=4 ttl=64 time=0.189 ms

--- 192.0.2.191 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.158/0.183/0.204/0.016 ms
```

g. Use `ping` to send four packets to `avsvr`. Record the average time_____.

```
$ ping -c 4 avsvr
PING avsvr.example.com (192.0.2.191) 56(84) bytes of data.
64 bytes from avsvr.example.com (192.0.2.191): icmp_seq=1 ttl=64
time=0.410 ms
64 bytes from avsvr.example.com (192.0.2.191): icmp_seq=2 ttl=64
time=0.160 ms
```

```
64 bytes from avsvr.example.com (192.0.2.191): icmp_seq=3 ttl=64
time=0.195 ms
64 bytes from avsvr.example.com (192.0.2.191): icmp_seq=4 ttl=64
time=0.166 ms

--- avsvr.example.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.160/0.232/0.410/0.104 ms
```

2. Use `nslookup` to verify host resolution for each of `host02`, `dbfw`, `avsvr`, and `em12c`.
   a. Verify host resolution for `host02`.

```
$ nslookup host02
Server:         192.0.2.1
Address:        192.0.2.1#53

Name:   host02
Address: 192.0.2.111
```

   b. Verify host resolution for `dbfw`.

```
$ nslookup dbfw
Server:         192.0.2.1
Address:        192.0.2.1#53

Name:   dbfw
Address: 192.0.2.101
```

   c. Verify host resolution for `avsvr`.

```
$ nslookup avsvr
Server:         192.0.2.1
Address:        192.0.2.1#53

Name:   avsvr
Address: 192.0.2.191
```

   d. Verify host resolution for `em12c`.

```
$ nslookup em12c
Server:         192.0.2.1
Address:        192.0.2.1#53
```

```
Name:   em12c
Address: 192.0.2.115
```

e. Stop the host resolution services for the em12c machine. Use the following command:
`sudo mv /etc/resolv.conf /etc/resolv.conf.org`

```
$ sudo mv /etc/resolv.conf /etc/resolv.conf.org
```

f. Verify host resolution for `host02`.

```
$ nslookup host02
;; connection timed out; no servers could be reached
```

g. Use `ping` to verify host resolution for `host02`.

```
$ ping host02 -c4
PING host02.example.com (192.0.2.111) 56(84) bytes of data.
64 bytes from host02.example.com (192.0.2.111): icmp_seq=1
ttl=64 time=0.191 ms
64 bytes from host02.example.com (192.0.2.111): icmp_seq=2
ttl=64 time=0.170 ms
64 bytes from host02.example.com (192.0.2.111): icmp_seq=3
ttl=64 time=0.178 ms
64 bytes from host02.example.com (192.0.2.111): icmp_seq=4
ttl=64 time=0.196 ms

--- host02.example.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.170/0.183/0.196/0.019 ms
```

h. Restore host resolution services.

```
$ sudo mv /etc/resolv.conf.org /etc/resolv.conf
```

i. Verify host resolution for `host02`.

```
$ nslookup host02
Server:         192.0.2.1
Address:        192.0.2.1#53

Name:   host02
Address: 192.0.2.111
```

3. Use `tnsping` to verify Oracle Net connectivity.

**Note:** `tnsping` sends a TNS payload to the listener, and receives an acknowledgement. A successful `tnsping` says the listener is available but not necessarily the database service. `tnsping` is only available on machines with the Oracle Database Client installed.

a. Set the Oracle environment for `em12rep` with:
`. oraenv`

```
$ . oraenv
```

```
ORACLE_SID = [oracle] ? em12rep
The Oracle base for
ORACLE_HOME=/u01/app/oracle/product/11.2.0/dbhome_1 is
/home/oracle
```

b. Send a `tnsping` to the `orcl.example.com` service on `host02` at listener port `1521`.

```
$ tnsping host02:1521/orcl.example.com

TNS Ping Utility for Linux: Version 11.2.0.3.0 - Production on
20-JUN-2014 20:00:54

Copyright (c) 1997, 2011, Oracle.  All rights reserved.

Used parameter files:

Used HOSTNAME adapter to resolve the alias
Attempting to contact
(DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=orcl.example.com))(ADDR
ESS=(PROTOCOL=TCP)(HOST=192.0.2.111)(PORT=1521)))
OK (20 msec)
```

c. If the listener was on a port other than 1521, how would the output appear? Test by using a different port number.

```
$ tnsping host02:1523/orcl.example.com

TNS Ping Utility for Linux: Version 11.2.0.3.0 - Production on
20-JUN-2014 20:03:08

Copyright (c) 1997, 2011, Oracle.  All rights reserved.

Used parameter files:

Used HOSTNAME adapter to resolve the alias
Attempting to contact
(DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=orcl.example.com))(ADDR
ESS=(PROTOCOL=TCP)(HOST=192.0.2.111)(PORT=1523)))
TNS-12541: TNS:no listener
```

d. If the service did not exist, how would the output appear? Test by using a different service name.

```
$ tnsping host02:1521/test.example.com

TNS Ping Utility for Linux: Version 11.2.0.3.0 - Production on
20-JUN-2014 20:05:14

Copyright (c) 1997, 2011, Oracle.  All rights reserved.
```

```
Used parameter files:


Used HOSTNAME adapter to resolve the alias
Attempting to contact
(DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=test.example.com))(ADDR
ESS=(PROTOCOL=TCP)(HOST=192.0.2.111)(PORT=1521)))
OK (0 msec)
```

**Note:** The service name is not considered in `tnsping`. If contact is made with the listener action is successful.

e. If the hostname was wrong, how would the output appear? Test by using a different hostname.

```
$ tnsping host99:1521/orcl.example.com

TNS Ping Utility for Linux: Version 11.2.0.3.0 - Production on
20-JUN-2014 20:08:08

Copyright (c) 1997, 2011, Oracle.  All rights reserved.

Used parameter files:

TNS-03505: Failed to resolve name
```

**Note:** When the hostname is not resolvable

f. If the machine was not responding (assume the machine is powered down), how would the output appear? **DO NOT TEST!** The following is what the output would be if the machine was powered down.

```
$ tnsping host02:1521/orcl.example.com

TNS Ping Utility for Linux: Version 11.2.0.3.0 - Production on
20-JUN-2014 20:57:00

Copyright (c) 1997, 2011, Oracle.  All rights reserved.

Used parameter files:

Used HOSTNAME adapter to resolve the alias
Attempting to contact
(DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=orcl.example.com))(ADDR
ESS=(PROTOCOL=TCP)(HOST=192.0.2.111)(PORT=1521)))
TNS-12543: TNS:destination host unreachable
```

4. Use `tcpdump` to view traffic while connected to the em12c terminal.

   a. Use the `tcpdump` command to begin capturing packets to a file named `eth0_packets`, on interface eth0, and the full packet for 10-20 seconds. Then end the packet collection with a `[ctrl]-C` command.

   ```
   tcpdump -i eth0 –s 65535 –w eth0_packets
   ```

```
$ sudo tcpdump -i eth0 -s 65535 -w eth0_packets
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture
size 65535 bytes

^C27 packets captured
27 packets received by filter
0 packets dropped by kernel
```

b. In a terminal session on your desktop, issue the following command:

`ping em12c –c 4`

```
$ ping em12c -c 4
PING em12c.example.com (192.0.2.115) 56(84) bytes of data.
64 bytes from em12c.example.com (192.0.2.115): icmp_seq=1 ttl=64
time=0.089 ms
64 bytes from em12c.example.com (192.0.2.115): icmp_seq=2 ttl=64
time=0.099 ms
64 bytes from em12c.example.com (192.0.2.115): icmp_seq=3 ttl=64
time=0.101 ms
64 bytes from em12c.example.com (192.0.2.115): icmp_seq=4 ttl=64
time=0.109 ms

--- em12c.example.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.089/0.099/0.109/0.012 ms
```

c. In the original terminal session where you started `tcpdump`, end the packet collection with a `[ctrl]-C`. The number of packets captured will vary.

```
 ^C21 packets captured
22 packets received by filter
0 packets dropped by kernel
```

d. Find the ping packets that were captured using the `tcpdump` read and filter options:

`tcpdump icmp –r eth0_packets`

```
$ sudo tcpdump icmp –r eth0_packets
reading from file eth0_packets, link-type EN10MB (Ethernet)
10:38:44.635045 IP ntp.example.com > em12c.example.com: ICMP
echo request, id 11783, seq 1, length 64
10:38:44.635066 IP em12c.example.com > ntp.example.com: ICMP
echo reply, id 11783, seq 1, length 64
10:38:45.631452 IP ntp.example.com > em12c.example.com: ICMP
echo request, id 11783, seq 2, length 64
10:38:45.631474 IP em12c.example.com > ntp.example.com: ICMP
echo reply, id 11783, seq 2, length 64
10:38:46.627908 IP ntp.example.com > em12c.example.com: ICMP
echo request, id 11783, seq 3, length 64
10:38:46.627930 IP em12c.example.com > ntp.example.com: ICMP
echo reply, id 11783, seq 3, length 64
```

```
10:38:47.624236 IP ntp.example.com > em12c.example.com: ICMP
echo request, id 11783, seq 4, length 64
10:38:47.624253 IP em12c.example.com > ntp.example.com: ICMP
echo reply, id 11783, seq 4, length 64
```

**Note:** An `icmp` packet includes `ping` packets. `ping` sends an echo request and gets an echo reply in return. `tcpdump` has a large number of options and expressions for filtering the collected packets.

5. Use `nc` (netcat) to send an arbitrary payload to an arbitrary IP address.

   **Note:** In Practice 5, an example of nc was shown in the Assumptions section to test whether rsyslog had been configured on em12c. A string was sent to em12c from avsvr and then the `/var/log/messages` files were searched for that string.

   a. In a terminal window on em12c as the `oracle` user, start an `nc` process to listen on port 63001 by using the following command:

      `nc –l 63001 –v`

      ```
      $ nc -l 63001 -v
      ```

   b. In another terminal on your desktop, start a sending process by using the following command:

      `nc 192.0.2.115 63001`

      ```
      $ nc 192.0.2.115 63001 –v
      ```

      **Note:** Because you are using the `–v` option, you should receive a connection verification message in both terminals immediately.

   c. On the sending terminal, send a message to the listening `nc` process by typing a string and pressing return.

      `All the world is a stage.`

      ```
      $ nc 192.0.2.115 63001 -v
      Connection to 192.0.2.115 63001 port [tcp/*] succeeded!
      All the world is a stage
      ```

   d. In the listening terminal, verify that message was received.

      ```
      nc -l 63001 -v
      Connection from 192.0.2.1 port 63001 [tcp/*] accepted
      All the world is a stage
      ```

   e. In the listening terminal, type a string and press return.

      `A rose by any other name.`

      ```
      $ nc -l 63001 -v
      Connection from 192.0.2.1 port 63001 [tcp/*] accepted
      All the world is a stage
      A rose by any other name
      ```

   f. In the sending terminal, verify that message was received.

      ```
      $ nc 192.0.2.115 63001 -v
      Connection to 192.0.2.115 63001 port [tcp/*] succeeded!
      ```

```
All the world is a stage
A rose by any other name
```

g. Stop the listening process by using the `[ctrl-C]` command.

h. Verify that the sending process has stopped.

# Practices for Lesson 7: Installing a Database Firewall

**Chapter 7**

# Practices for Lesson 7

## Practices Overview

In these practices, you will perform the necessary post-installation tasks for Database Firewall.

# Practice 7-1: Performing Database Firewall Post-Installation Tasks

## Overview

In this practice, you perform post-installation tasks for Database Firewall.

## Assumptions

Oracle Audit Vault and Database Firewall (Database Firewall component) has been installed.

The IP address for the Database Firewall appliance management port `<DBFW_MGT_IP>` is 192.0.2.101.

## Tasks

1. Access the Database Firewall Console.
   a. Open a terminal window and connect to the em12c VM as the **`oracle`** OS user. The password is **`oracle`**.

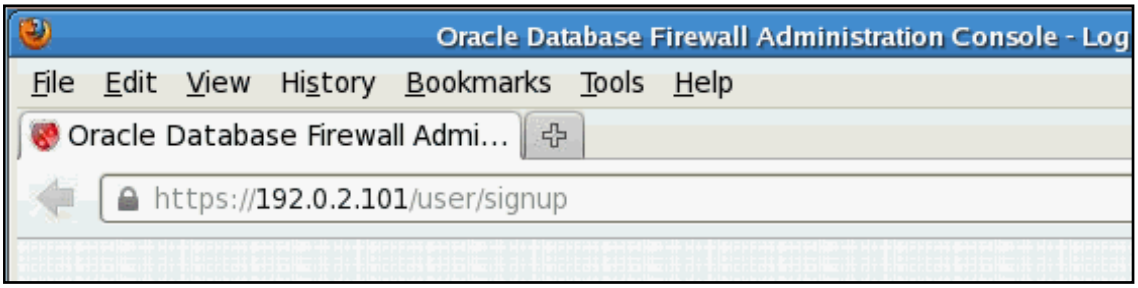
```
$ ssh -X oracle@em12c
oracle@em12c's password:
Last login: Tue May 27 15:19:02 2014 from dom0.example.com
[oracle@em12c ~]$
```

   b. Start Firefox and launch the Database Firewall console by entering the following command at the prompt:

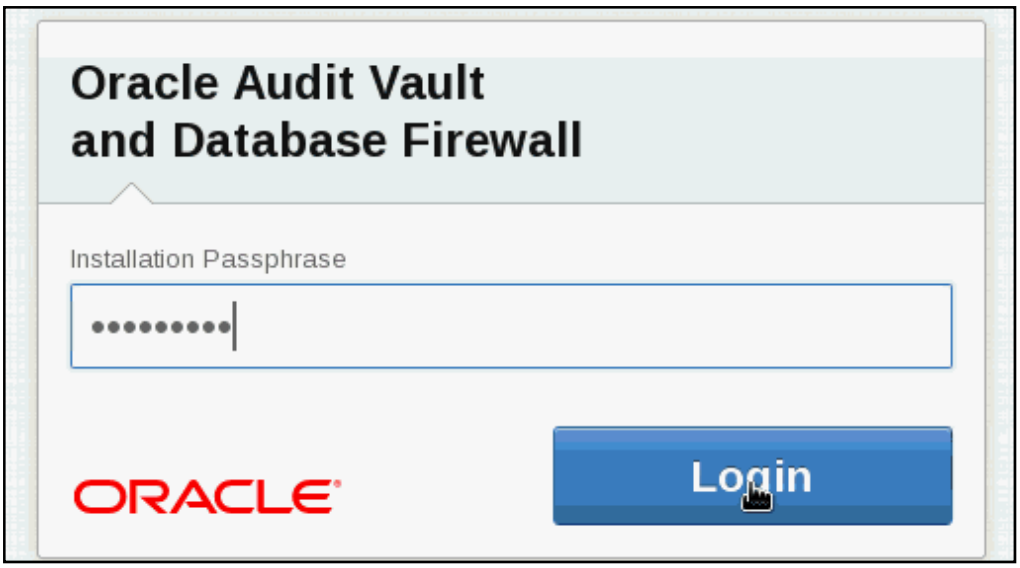
```
firefox https://<DBFW_MGT_IP>
```

```
[oracle@em12c ~]$ firefox https://192.0.2.101
```

**Note:** Because this is the first connection, an “untrusted connection” dialog will display. Continue by confirming a security exception.




   c. Enter the installation passphrase of **`oracle_4U`** and click **Login**.

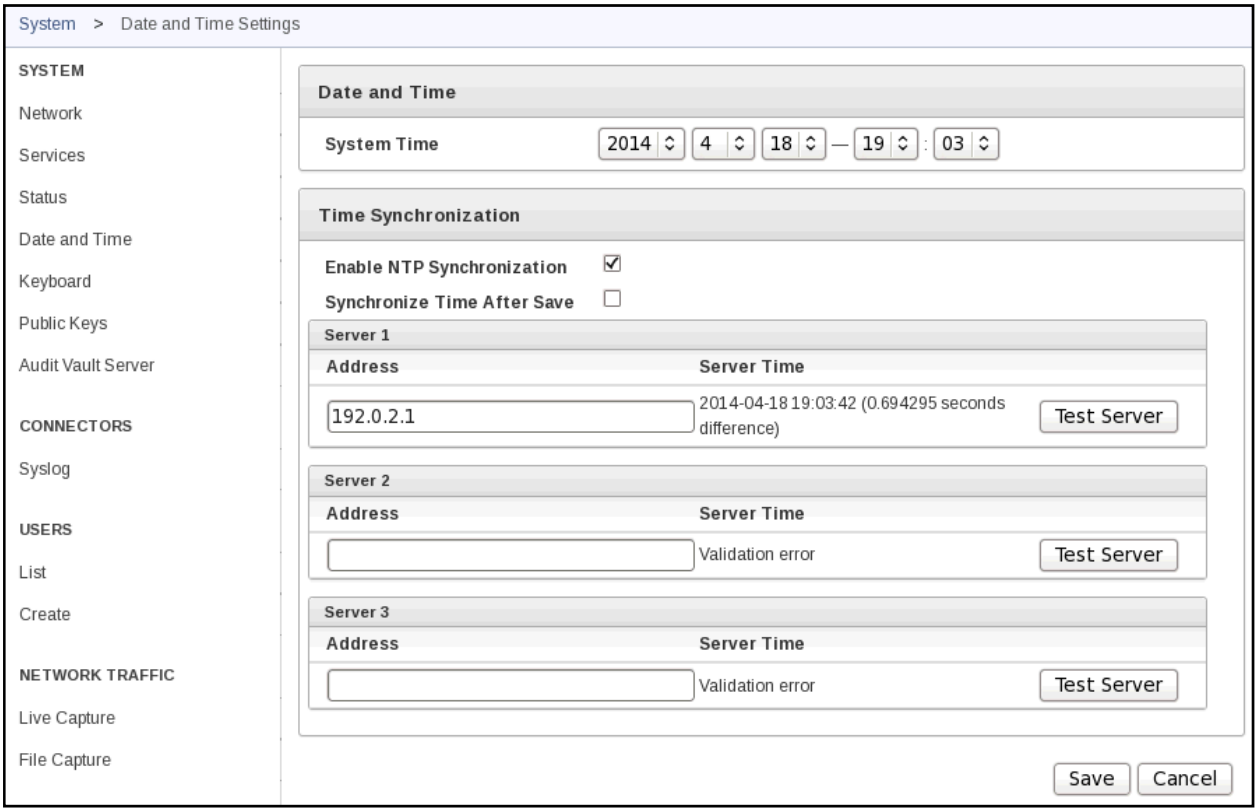



2. On the Post-Install Configuration page, perform the following tasks:
   a. Enter **`fwadmin`** in the User Name field and **`oracle_4U`** in the Password field for the Database Firewall Administrator. Enter the installation passphrase of **`oracle_4U`**.
   b. Enter passwords for the root and support users. Use **`oracle_4U`** for all.
   c. Click **Save**.


3. The login page appears. Enter **`fwadmin`** as the user name with **`oracle_4U`** as the password. Click **Login**. The System Status page appears.
4. Modify keyboard settings as follows:
   a. Navigate to the Keyboard page by clicking **Keyboard** in the menu on the left.
   b. If the Keyboard layout is set to something other than `US`, set the keyboard. Otherwise click **Cancel**.
5. Set the time by performing the following steps:
   a. Navigate to the Date and Time page by clicking **Date and Time** in the menu on the left.
   b. On the Date and Time page, click **Change**.
   c. Select **Enable NTP Synchronization**.
   d. Set the Server 1 Address field to **`192.0.2.1`**.

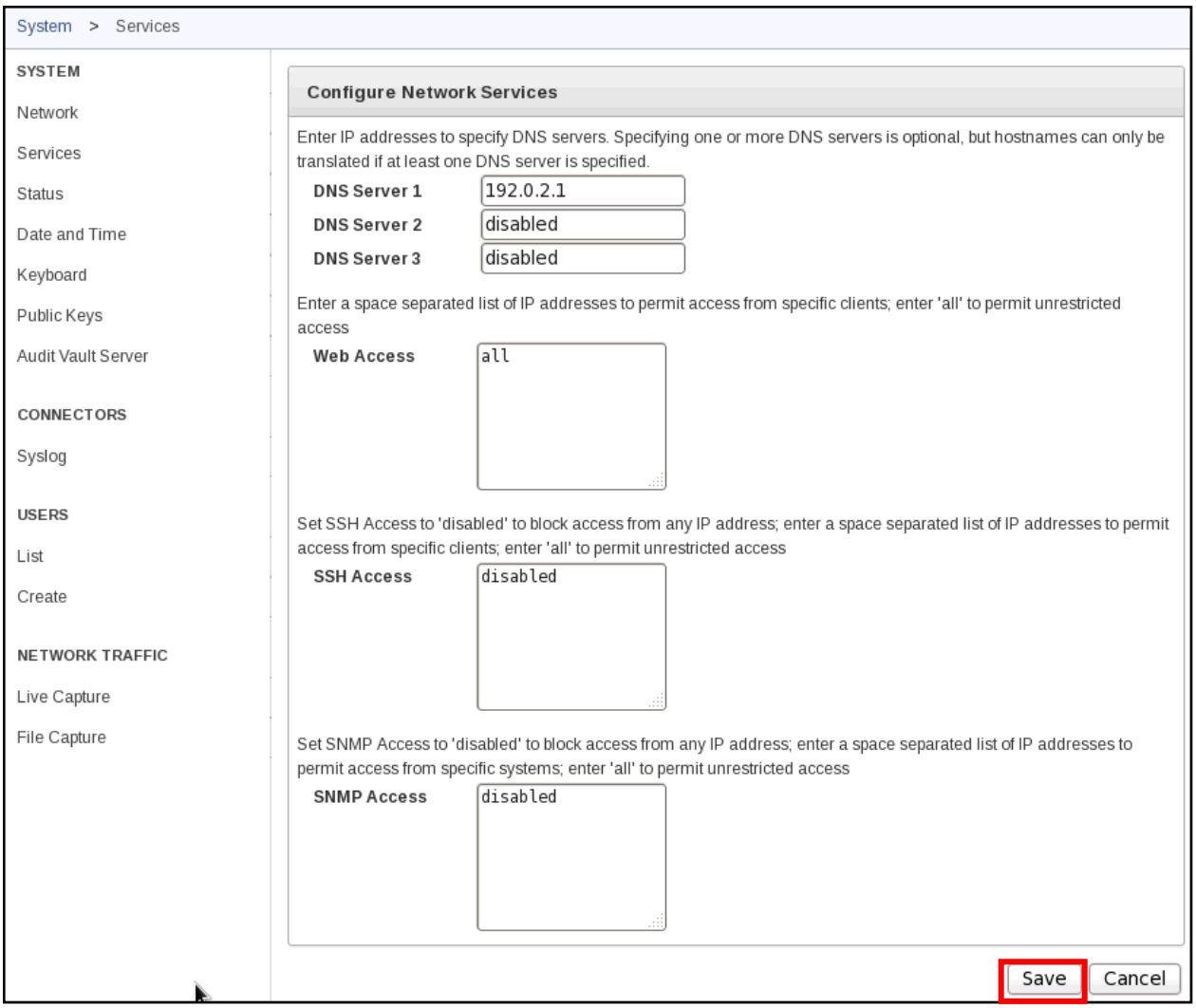
   **Note:** Multiple time servers are recommended, but only one is available in the practice environment.

e. Click **Test Server**.
f. The Server Time column will show the time difference.
g. Click **Save**.




h. On the System Data and Time settings page, click the **Apply** button for Server 1. When the page refreshes, the difference in the Server Time column should become very small.

6. Set DNS servers as follows:
   a. Navigate to the Services page by clicking **Services** in the menu on the left.
   b. On the Configure Network Services page, click **Change**.
   c. Set the DNS Server 1 field to **192.0.2.1**.
   d. Click **Save**.




7. Log out of the Database Firewall console.

# Practices for Lesson 8: Configuring Oracle AVDF and Deploying Database Firewall

**Chapter 8**

# Practices for Lesson 8

## Practices Overview

In these practices, you will verify Database Firewall settings, configure traffic sources, register the Database Firewall, and create enforcement points.

# Practice 8-1: Verifying the Database Firewall's Network Settings

## Overview

In this practice, you verify the network settings for the Database Firewall.

## Assumptions

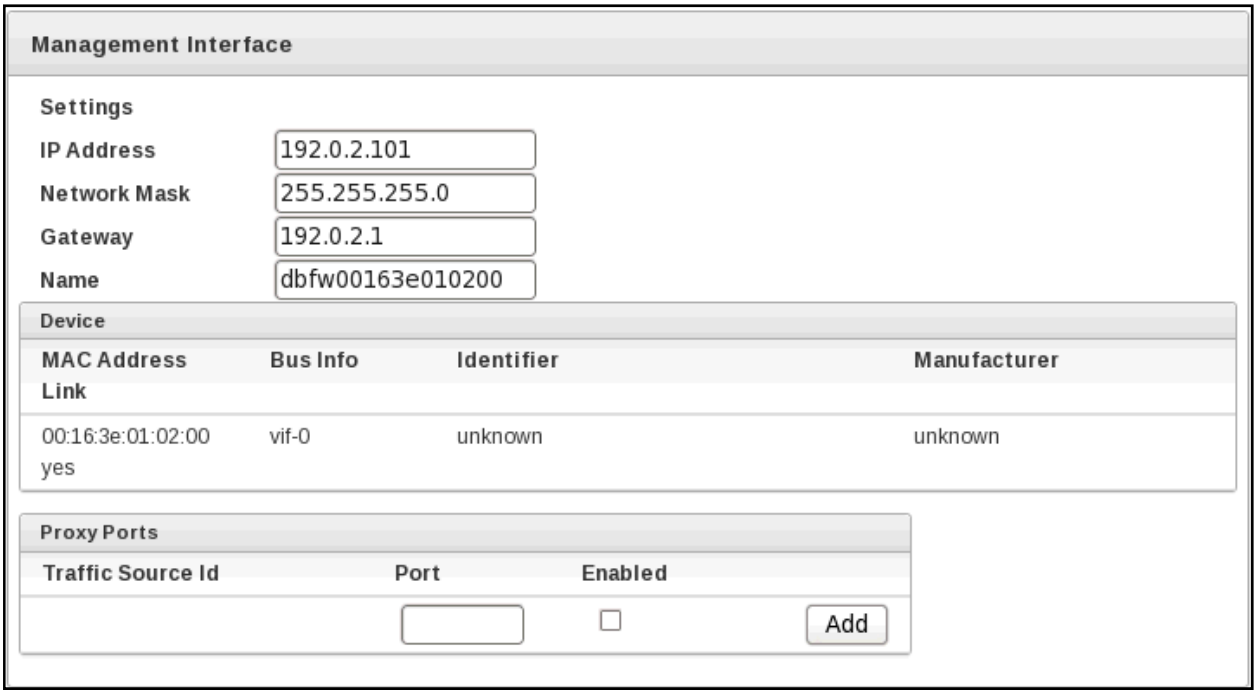
A terminal window is open to the em12c VM. Open a terminal window and enter the following command: `ssh -X oracle@em12c`

## Tasks

The installer configures initial network settings for the Database Firewall during installation. You can change the network settings after installation.

Perform the following steps to verify or change the Database Firewall network settings:

1. Log in to the Database Firewall administration console.
   - URL: https://192.0.2.101
   - User Name: `FWADMIN`
   - Password: `oracle_4U`
2. In the System menu, select **Network**.
3. Scroll to the bottom of the Network Configuration page and click **Change**.
4. Verify the settings in the Management Interface section:
   - IP Address: **`192.0.2.101`**
   - Network Mask: **`255.255.255.0`**
   - Gateway: **`192.0.2.1`**
   - Name: `dbfw` (+MAC address)




5. If you made any changes, click **Save**. Otherwise, click **Cancel**.
6. Log out of the Database Firewall console or continue to the next practice.

# Practice 8-2: Verifying the Database Firewall's Network Services

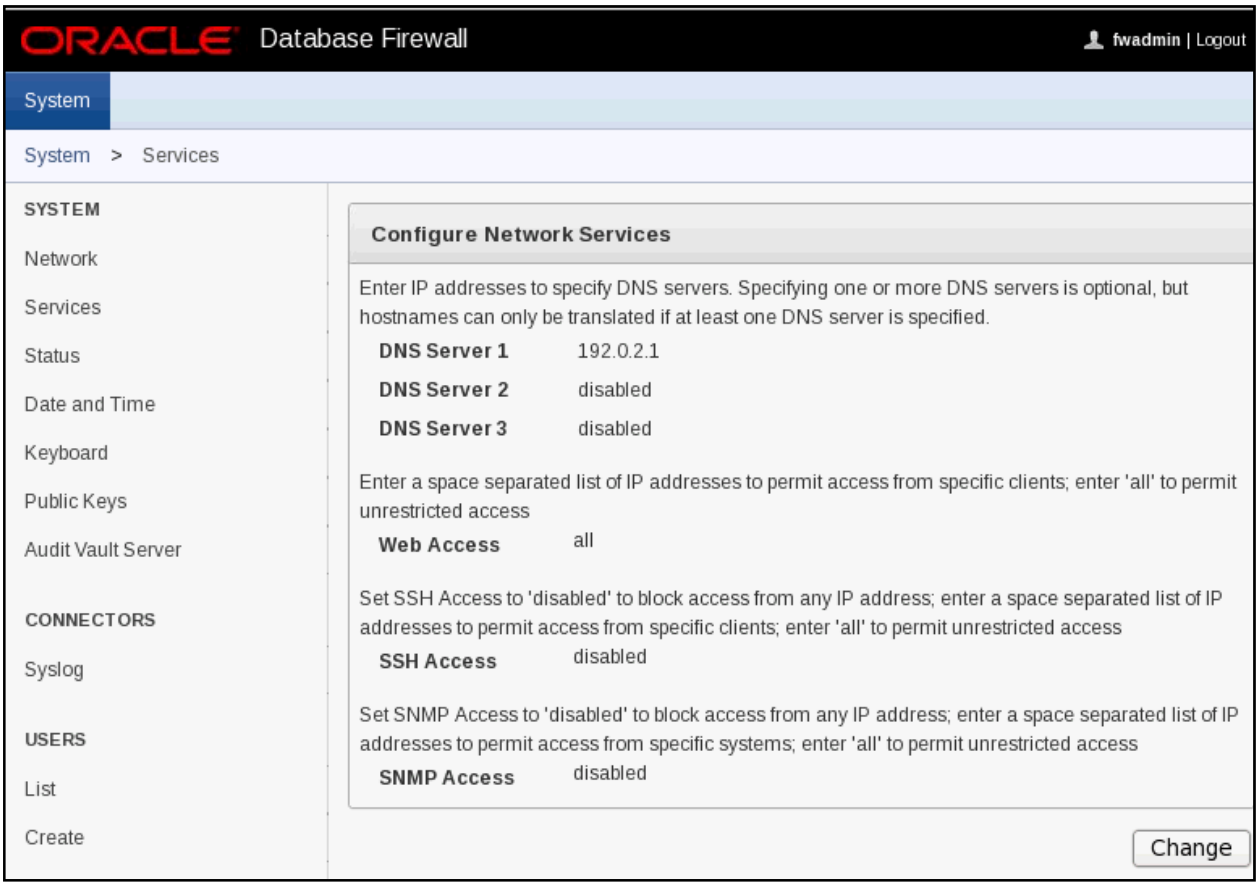
## Overview

In this practice, you verify the configuration of the Database Firewall's network services.

## Tasks

The network services configuration determines how users can access the Database Firewall.
Perform the following steps to verify the Database Firewall's network services configuration:

1. Log in to the Database Firewall administration console.
   - URL: https://192.0.2.101
   - User Name: `FWADMIN`
   - Password: `oracle_4U`
2. In the System menu, select **Services**.
3. On the Configure Network Services page, verify or change the following:
   - DNS Server 1: **192.0.2.1**
   - DNS Server 2: disabled
   - DNS Server 3: disabled
   - Web Access: all
   - SSH Access: disabled
   - SNMP Access: disabled



4. It there are any changes needed, click **Change** and make the changes.
5. If you made any changes, click **Save**.
6. Log out of the Database Firewall console or continue to the next practice.

# Practice 8-3: Verifying the Traffic Source Configuration

## Overview

In this practice, you verify and change the Database Firewall's traffic source configuration. Every Database Firewall requires a network interface for a management interface. A traffic source corresponds to a network interface (NIC). An inline bridge deployment requires additional two NICs. A traffic proxy usually requires one or two NICs in addition to the management interface, but in some cases the traffic proxy could use the same NIC as the management interface. An out-of-band monitor requires only one NIC. We configure both a inline bridge and a traffic proxy in this set of practices. In actual deployment, you would normally deploy a Bridge or a Traffic Proxy in a single firewall appliance, not both. Additional Network Interface Cards (NICs) have been added to the practice environment to allow both configurations.

## Tasks

During your planning of the network configuration, you decide whether to place Database Firewalls inline with traffic to your secured target databases, or out of band (for example, using a spanning or mirror port). You may also decide to use a firewall as a traffic proxy. The network configuration is decided by whether the Database Firewall will operate in DAM (monitoring only) or DPE (blocking) mode, and which network confirmation.

Using the Database Firewall administration console, you configure each firewall's traffic sources, specifying whether the sources are inline with network traffic, and whether the firewall will act as a proxy.

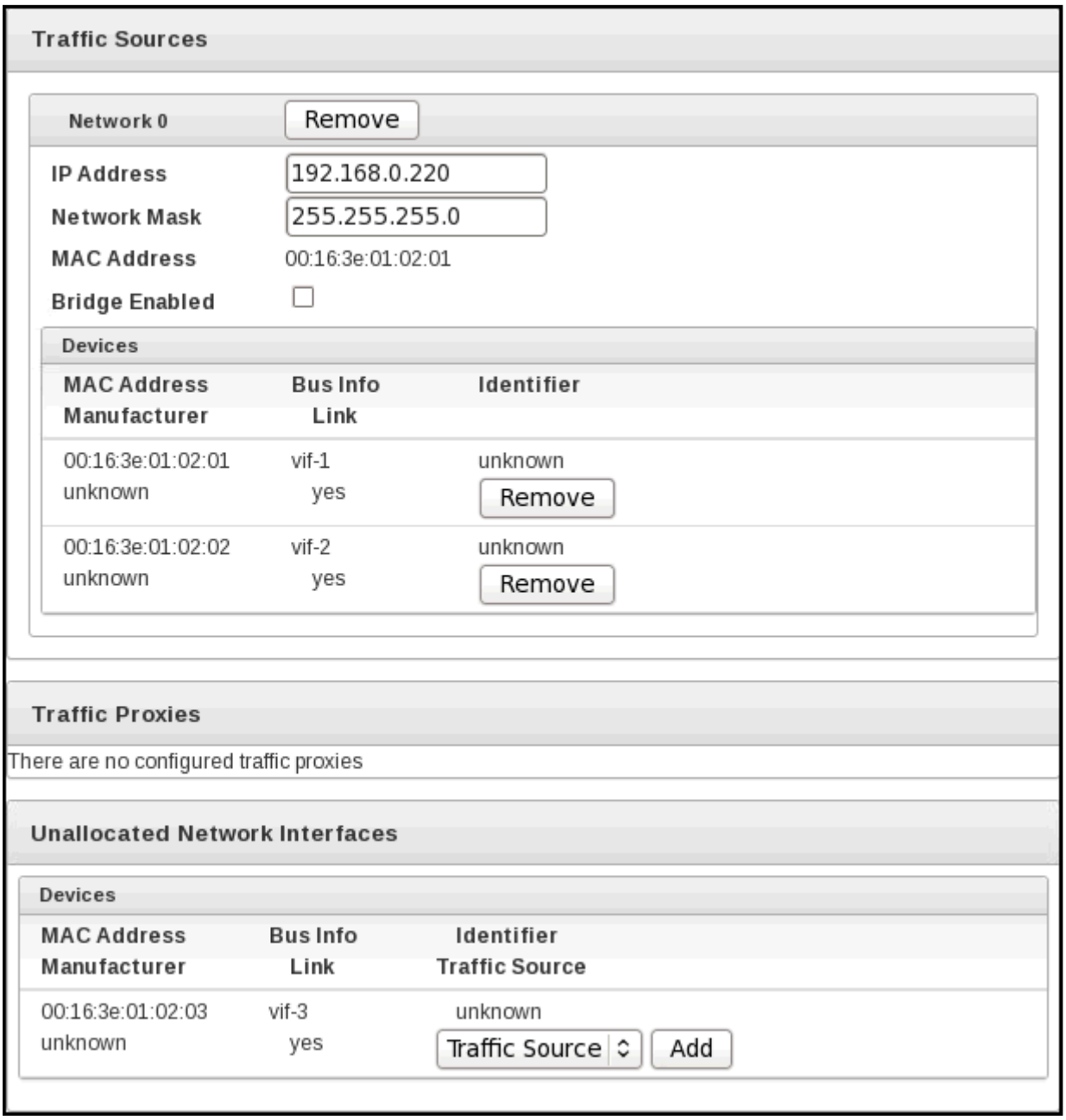
You will use a firewall's traffic and proxy sources to configure enforcement points for each secured target database you are monitoring with that firewall.

**Note:** A traffic proxy can only operate in DPE mode.

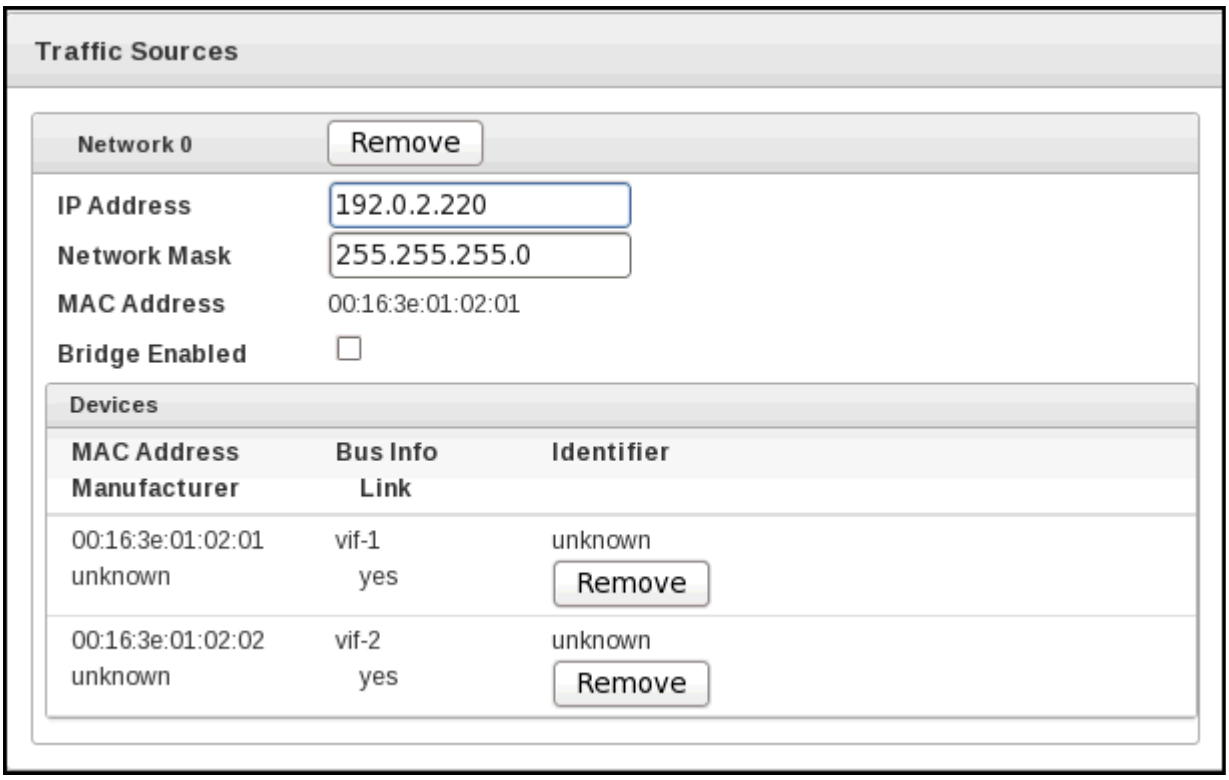
Perform the following steps to verify or change the traffic source configuration:

1. Log in to the Database Firewall administration console as the **`FWADMIN`** user.
2. In the System menu, click **Network**.
3. Scroll to the bottom of the page and click **Change**.

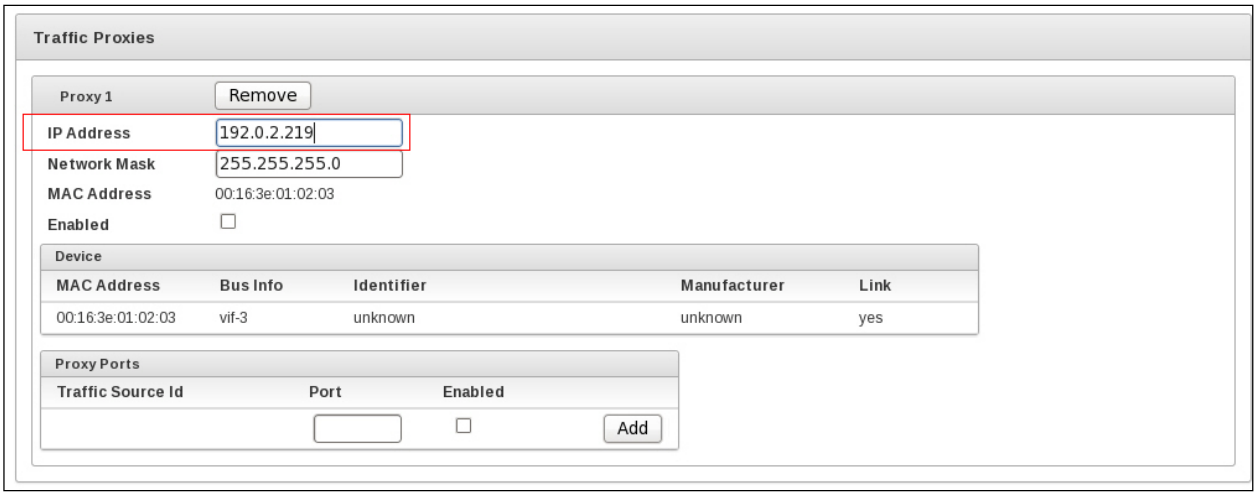
   In the practice environment, two NICs are assigned to Network 0 and one NIC is unallocated as shown in the accompanying screenshot.



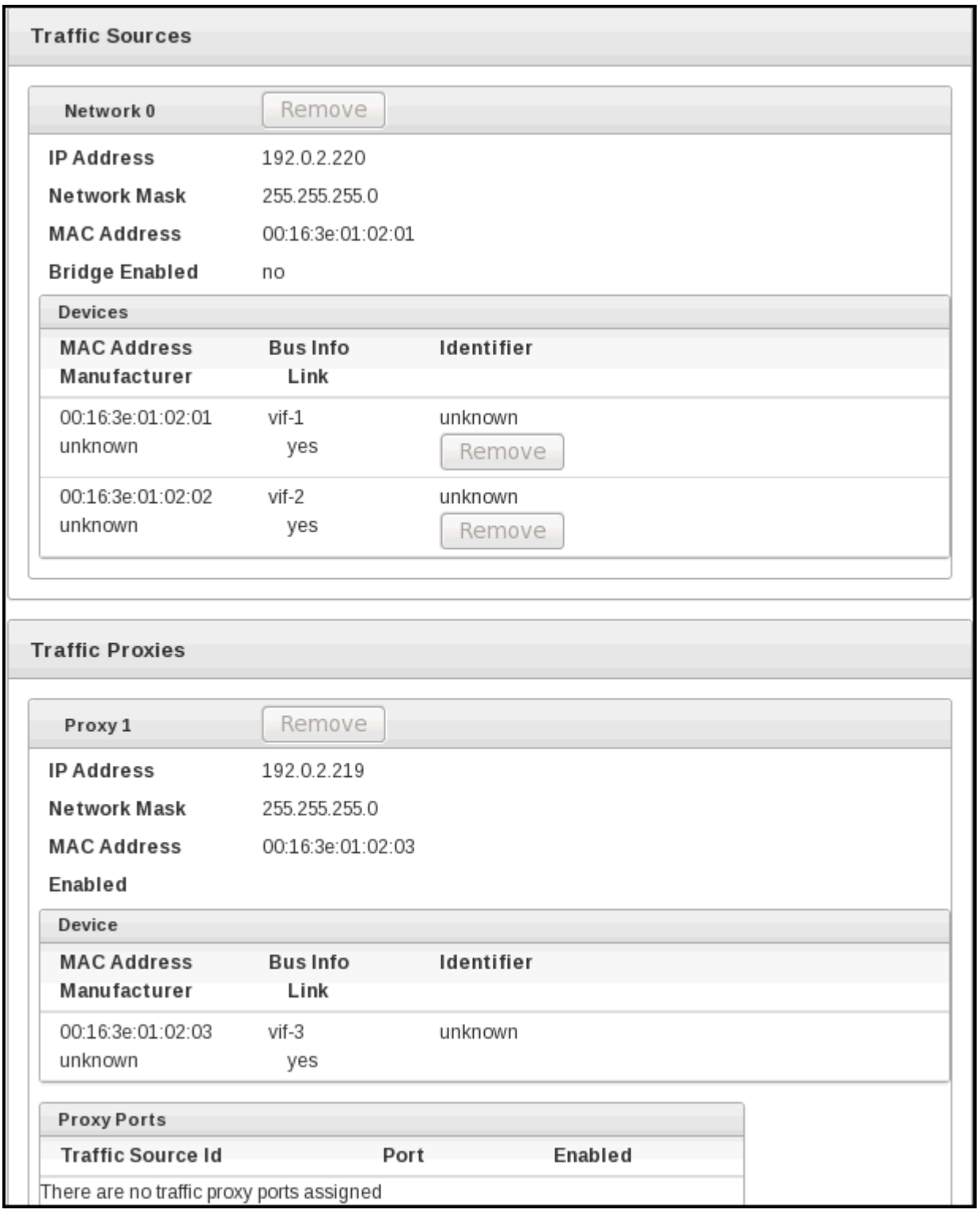

4. Scroll to the Traffic Sources section and verify or change the following:
   - IP Address: **192.0.2.220**
   - Network Mask: **255.255.255.0**
   - Bridge Enabled: **DO NOT SELECT**




5. Add a network interface to the Traffic Proxies.
   a. Scroll to the Unallocated Network Devices section.
   b. In the Traffic Source drop-down list for the vif-3 interface, select **Traffic Proxy**.
   c. Click **Add**.
   d. When the page refreshes, scroll to the Traffic Proxies section and change the IP address of Proxy 1 to **192.0.2.219**.




   e. Click **Save**. The final configuration is shown in the screenshot.




6. Log out of the Database Firewall console or continue to the next practice.

# Practice 8-4: Configuring a Bridge in the Database Firewall

## Overview

In this practice, you configure a traffic source as a bridge.

## Assumptions

Practice 8-3 has been completed. In practice 8-3 you verified the bridge had two interfaces assigned and the bridge IP address was set properly.

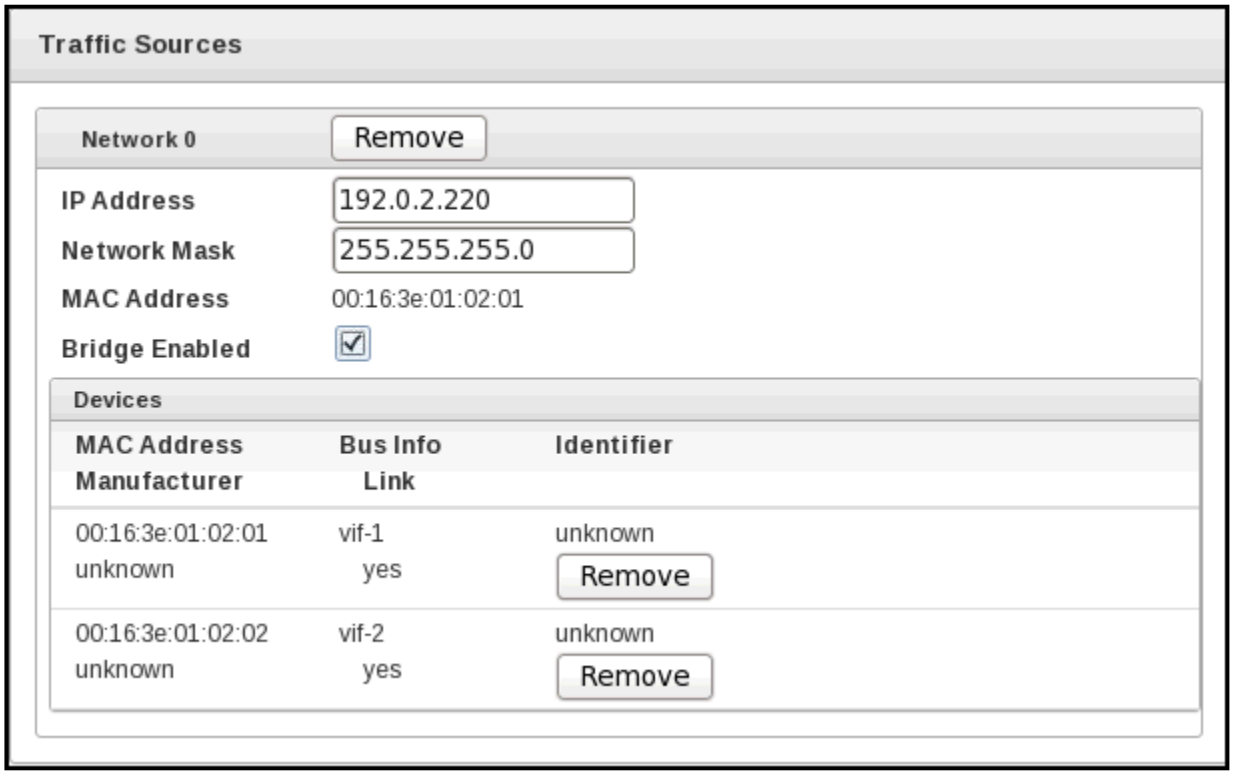
## Tasks

The Database Firewall must be inline with network traffic if used in blocking mode to block potential SQL attacks. To enable the bridge, an IP address that is unique to the database network must be allocated. The bridge IP address is used to redirect traffic within the Database Firewall.

To enable a traffic source as a bridge, that traffic source must have two network interfaces. These network interface devices must connect the Database Firewall inline between the database and its clients (whether Database Policy Enforcement or Database Activity Monitoring mode is used).

Perform the following steps to configure the Database Firewall bridge IP address:

1. Log in to the Database Firewall administration console as the **`FWADMIN`** user.
2. In the System menu, click **Network**.
3. Scroll to the bottom of the page and click **Change**.
4. In the Traffic Sources section, locate the traffic source that you want to configure as a bridge. In our course, the traffic source is Network 0. Select **Bridge Enabled** for this traffic source.



5. Scroll to the bottom of the page and click **Save**. A message stating “Network configuration complete” is displayed.
6. Log out of the Database Firewall console or continue to the next practice.

# Practice 8-5: Configuring a Database Firewall as a Traffic Proxy

## Overview

In this practice, you configure a Database Firewall as a traffic proxy.

## Assumptions

Practice 8-3 is complete and the traffic sources have been configured.

## Tasks

Depending on your network configuration, you may prefer to configure a traffic proxy in the Database Firewall instead of a bridge inline with network traffic. You can then associate the proxy with an enforcement point. You can also specify multiple ports for a proxy and use them for different enforcement points.

Once you set up the Database Firewall as a traffic proxy, your database clients connect to the database by using the Database Firewall proxy IP and port.

Perform the following steps to configure a traffic proxy:

1. Ensure that the IP address of the proxy interface is on the same subnet as the secured target. Use the `nslookup` command with the machine names to find the IP addresses.

   **Note:** Because the network mask is 255.255.255.0 they are on the same subnet if the first three octets are the same. This is the same as saying the subnet is 192.0.2.0/24, which means the first 24 bits of the address are the same.

   a. Open a terminal window and enter the following command: **`ssh -X oracle@em12c`**

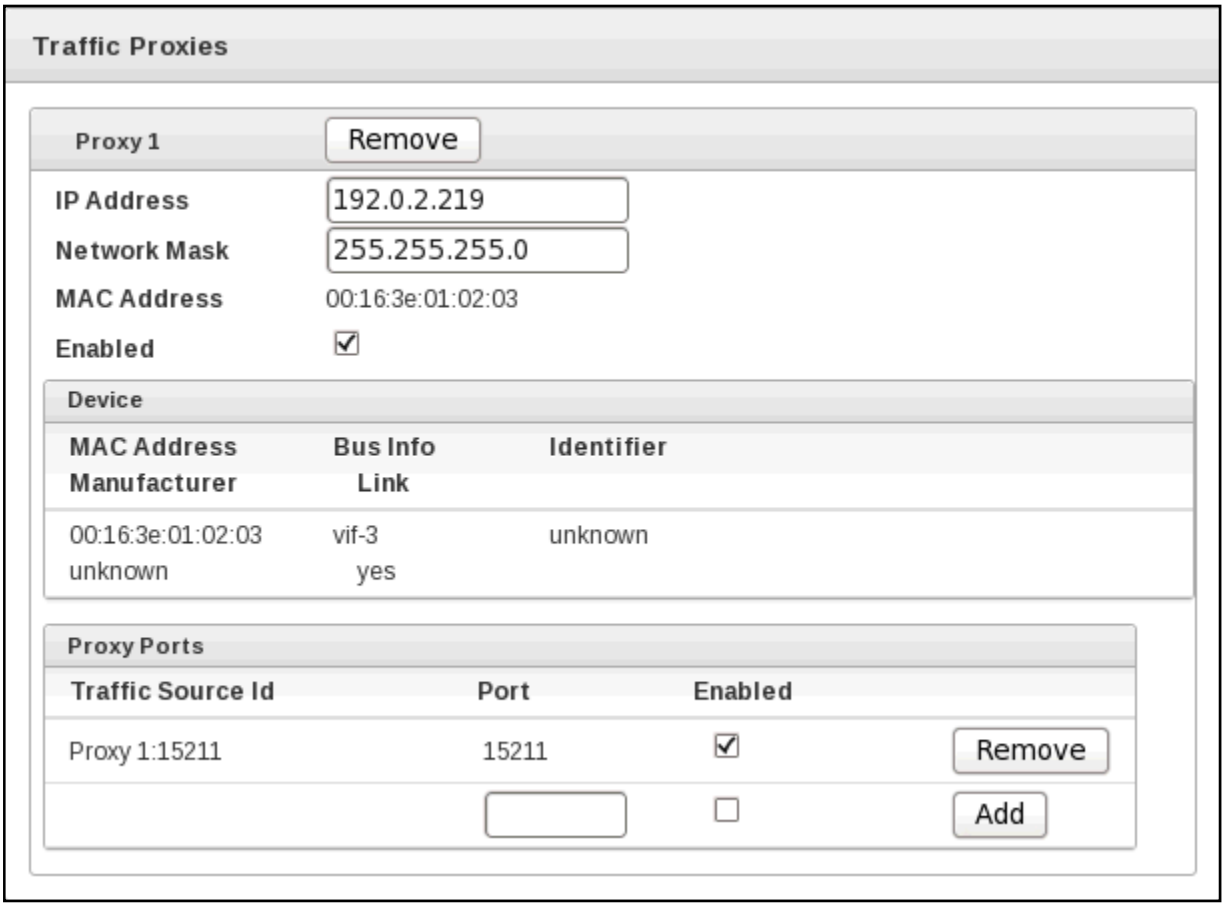
   b. Enter the `nslookup` command as shown in the code box:

```
$ nslookup dbfw
Server:         192.0.2.1
Address:        192.0.2.1#53

Name:   dbfw.example.com
Address: 192.0.2.101

$ nslookup host02
Server:         192.0.2.1
Address:        192.0.2.1#53

Name:   host01.example.com
Address: 192.0.2.111
```

   c. Close the terminal window.

2. Log in to the administration console of the Database Firewall that is acting as a proxy.
   - URL: https://192.0.2.101
   - User Name: `FWADMIN`
   - Password: `oracle_4U`
3. In the System menu, click **Network**.
4. Scroll to the bottom of the page and click **Change**.

5. In the Traffic Proxies section:
   a. Select **Enabled**.
   b. In the Proxy Ports section for the new proxy, enter **15211** or any unused port number.
   c. Select **Enabled** next to the port number.
   d. Click **Add**.




6. Click **Save**. A “Network Configuration complete” message is displayed.
7. Log out of the Database Firewall console or continue to the next practice.

# Practice 8-6: Specifying the Audit Vault Server Certificate and IP Address

## Overview

In this practice, you associate each Database Firewall with an Audit Vault Server by specifying the server's certificate and IP address.

## Tasks

You must associate each Database Firewall with an Audit Vault Server by specifying the server's certificate and IP address, so that the Audit Vault Server can manage the firewall. If you are using a resilient pair of Audit Vault Servers for high availability, you must associate the firewall to both servers.

You must specify the Audit Vault Server certificate and IP address to the Database Firewall before you register the firewall in the Audit Vault Server.

Perform the following steps to specify the Audit Vault Server certificate and IP address:

1. Launch the Audit Vault Server console in the Firefox browser.
   a. In a terminal window, connect to the em12c VM as the **oracle** user with the password **oracle** with X forwarding enabled.

```
$ ssh -X oracle@em12c
oracle@em12c's password:
Last login: Thu Jun  5 11:50:01 2014 from dom0.example.com
```

   b. Start the Firefox browser and launch the Audit Vault Server console.

```
[oracle@em12c ~]$ firefox https://192.0.2.191
```

2. Log in as the Administrator user **AVADMIN2_A**.
3. Click the **Settings** tab.
4. Click **Certificate** in the Security Menu on the left side of the window.
5. Select and copy the entire text that appears in the box labeled Server Certificate including the lines `---BEGIN CERTIFICATE----` and `----END CERTIFICATE----`
   You can use the browser's copy/paste feature for this task.
6. Return to the Database Firewall console (URL https://192.0.2.101).
7. Click **Audit Vault Server** in the System menu on the left side of the window.
8. Paste the certificate into the Certificate box in the window.
9. Enter **192.0.2.191** in the Audit Vault Server IP address field.
10. Click **Apply**. A "Settings saved" message is displayed.
11. Log out of the Database Firewall console or continue to the next practice.

# Practice 8-7: Registering the Database Firewall

## Overview

In this practice, you will register the Database Firewall with the Audit Vault Server.

## Assumptions

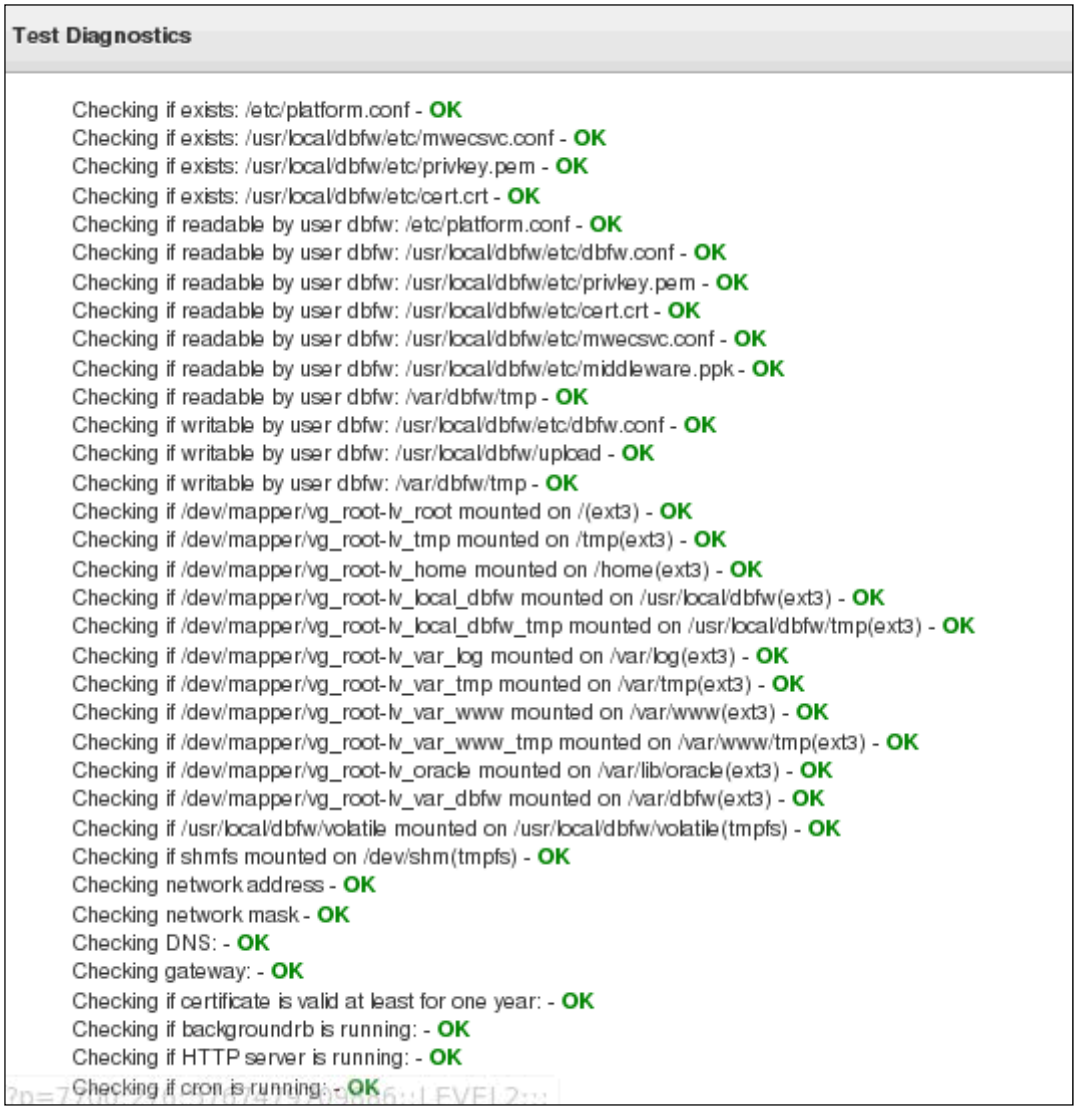
Practice 8-6 has been completed and the Audit Vault Server certificate has been saved.

## Tasks

You must register each Database Firewall in the Audit Vault Server in order to enable communication between the two.

Perform the following steps to register the Database Firewall in the Audit Vault Server:

1. Log in to the Audit Vault Server as the administrator user named **`AVADMIN2_A`**.
2. Click the **Firewalls** tab.
3. Click **Register**.
4. Enter the following information for the Database Firewall:
   - Name: **dbfw.example.com**
   - IP Address: **192.0.2.101**
5. Click **Save**.
6. A confirmation message stating that the firewall was registered appears.
7. Run Test Diagnostics to ensure that everything is running correctly.
   a. Click the **Settings** tab.
   b. Click **Status** in the System section of the menu on the left.
   c. Click **Test Diagnostics**.
   d. The report appears. Every line should have a green **OK** next to it.



**Test Diagnostics**

Checking if exists: /etc/platform.conf - **OK**
Checking if exists: /usr/local/dbfw/etc/mwecsvc.conf - **OK**
Checking if exists: /usr/local/dbfw/etc/privkey.pem - **OK**
Checking if exists: /usr/local/dbfw/etc/cert.crt - **OK**
Checking if readable by user dbfw: /etc/platform.conf - **OK**
Checking if readable by user dbfw: /usr/local/dbfw/etc/dbfw.conf - **OK**
Checking if readable by user dbfw: /usr/local/dbfw/etc/privkey.pem - **OK**
Checking if readable by user dbfw: /usr/local/dbfw/etc/cert.crt - **OK**
Checking if readable by user dbfw: /usr/local/dbfw/etc/mwecsvc.conf - **OK**
Checking if readable by user dbfw: /usr/local/dbfw/etc/middleware.ppk - **OK**
Checking if readable by user dbfw: /var/dbfw/tmp - **OK**
Checking if writable by user dbfw: /usr/local/dbfw/etc/dbfw.conf - **OK**
Checking if writable by user dbfw: /usr/local/dbfw/upload - **OK**
Checking if writable by user dbfw: /var/dbfw/tmp - **OK**
Checking if /dev/mapper/vg_root-lv_root mounted on /(ext3) - **OK**
Checking if /dev/mapper/vg_root-lv_tmp mounted on /tmp(ext3) - **OK**
Checking if /dev/mapper/vg_root-lv_home mounted on /home(ext3) - **OK**
Checking if /dev/mapper/vg_root-lv_local_dbfw mounted on /usr/local/dbfw(ext3) - **OK**
Checking if /dev/mapper/vg_root-lv_local_dbfw_tmp mounted on /usr/local/dbfw/tmp(ext3) - **OK**
Checking if /dev/mapper/vg_root-lv_var_log mounted on /var/log(ext3) - **OK**
Checking if /dev/mapper/vg_root-lv_var_tmp mounted on /var/tmp(ext3) - **OK**
Checking if /dev/mapper/vg_root-lv_var_www mounted on /var/www(ext3) - **OK**
Checking if /dev/mapper/vg_root-lv_var_www_tmp mounted on /var/www/tmp(ext3) - **OK**
Checking if /dev/mapper/vg_root-lv_oracle mounted on /var/lib/oracle(ext3) - **OK**
Checking if /dev/mapper/vg_root-lv_var_dbfw mounted on /var/dbfw(ext3) - **OK**
Checking if /usr/local/dbfw/volatile mounted on /usr/local/dbfw/volatile(tmpfs) - **OK**
Checking if shmfs mounted on /dev/shm(tmpfs) - **OK**
Checking network address - **OK**
Checking network mask - **OK**
Checking DNS: - **OK**
Checking gateway: - **OK**
Checking if certificate is valid at least for one year: - **OK**
Checking if backgroundrb is running: - **OK**
Checking if HTTP server is running: - **OK**
Checking if cron is running: - **OK**

# Practice 8-8: Registering the Secured Targets in the Audit Vault Server (OPTIONAL)

## Overview

In this practice, you register the Oracle Database 12*c* secured target with the Audit Vault Server. **You only need to perform this practice if you did not complete this task in an earlier practice.**

Secured targets can be supported databases or operating systems that Audit Vault and Database Firewall monitors. You must register all secured targets in the Audit Vault Server, regardless of whether you are deploying the Audit Vault Agent, the Database Firewall, or both.

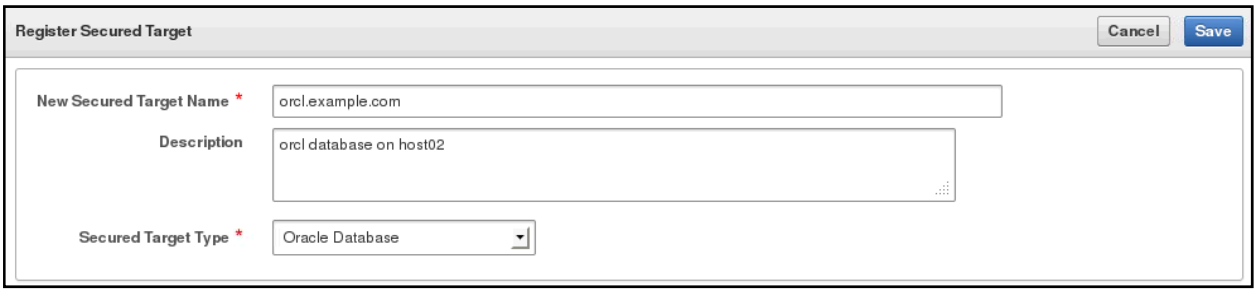
## Tasks

Perform the following steps to register the Oracle Database 12*c* database with the Audit Vault Server.

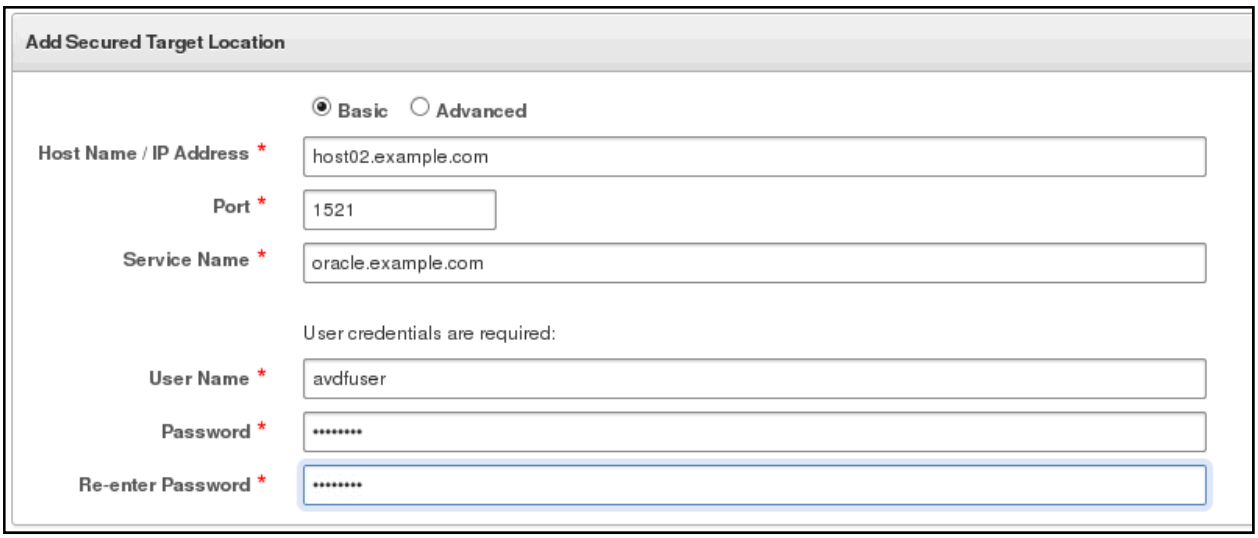
1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Secured Targets** tab.
3. Click **Register**.
4. On the Register Secured Target page, enter a New Secured Target Name and optional Description for the new target as follows:

   Secured Target Name: **`orcl.example.com`**

   Description: **`orcl database instance on host02`**




5. In the Secured Target Type field, select the secured target type of **Oracle Database**.
6. In the **Add Secured Target Location** section, enter the host name or IP Address, port, and the service name or SID. If you know the exact connect string, you can click the Advanced radio button instead and enter the string there.




7. If required by this type of secured target, in the User Name, Password, and Re-enter Password fields, enter the credentials for the secured target user account you created for Oracle Audit Vault and Database Firewall (Oracle AVDF).
8. In the Add Secured Target Addresses section, enter the host name, port number, and service name.


9. Click **Add**.
10. Click **Save**.

# Practice 8-9: Creating and Configuring Enforcement Points

## Overview

In this practice, you configure an enforcement point.

## Assumptions

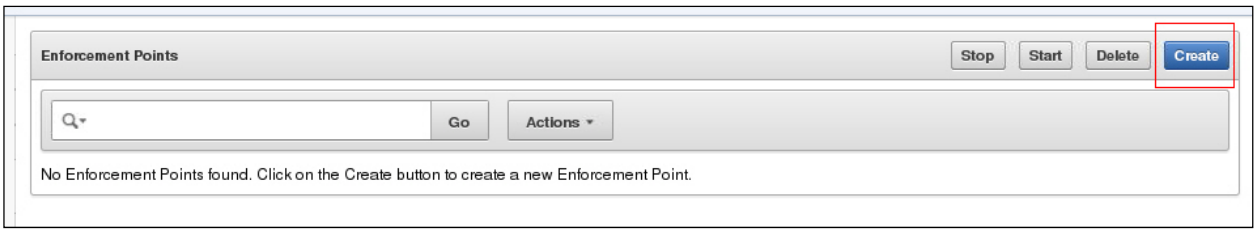
The firewall has been registered. The target host and the secure target have been registered.

## Tasks

If you are monitoring databases with a Database Firewall, you must configure one enforcement point for every secured target database that you want to monitor with the firewall. The enforcement point configuration lets you specify the firewall monitoring mode (DAM or DPE), identify the secured target database being monitored, the network traffic sources to that database, and the Database Firewall used for the enforcement point.

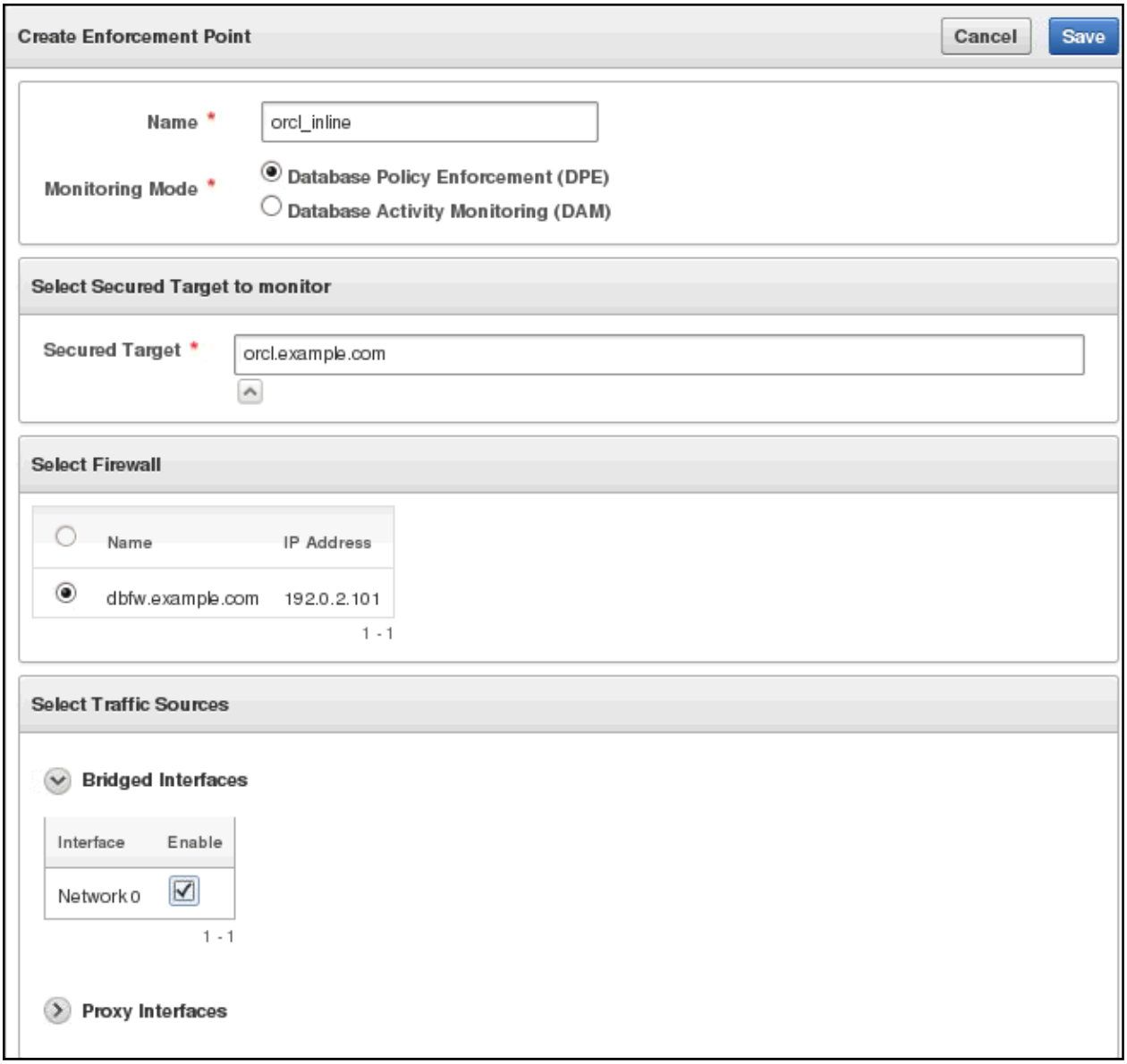
Perform the following steps to configure an enforcement point for an inline deployment:

1. Log in to the Audit Vault Server console as the administrator user **`AVADMIN2_A`**.
2. Click the **Secured Targets** tab.
3. In the Monitoring menu, click **Enforcement Points**.
4. Click **Create**.

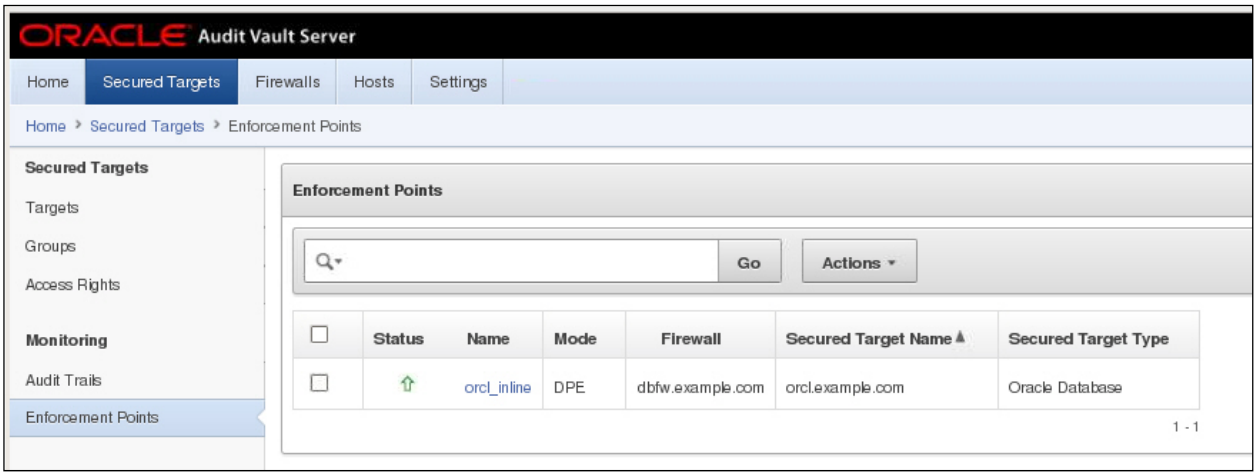



5. Enter a name for this enforcement point: **orcl_inline**
6. Select the Monitoring Mode: **Database Policy Enforcement (DPE)**

   **Note:** DPE mode with a pass-all policy is equivalent to Database Activity Monitoring (DAM) mode.
7. Select the Secured Target to monitor:
   a. Click the **Up** arrow beside the Secured Target field.
   b. In the Select a Secure Target window, click **Select** for **orcl.example.com**.
8. In the Select Firewall section, select **dbfw.example.com**, which is the database firewall that handles this enforcement point.
9. When the page refreshes, select traffic sources in the Bridged Interfaces area:
   a. Expand **Bridged Interfaces**.
   b. Select **Enable** for Network 0.




10. Click **Save**. A confirmation message briefly appears.

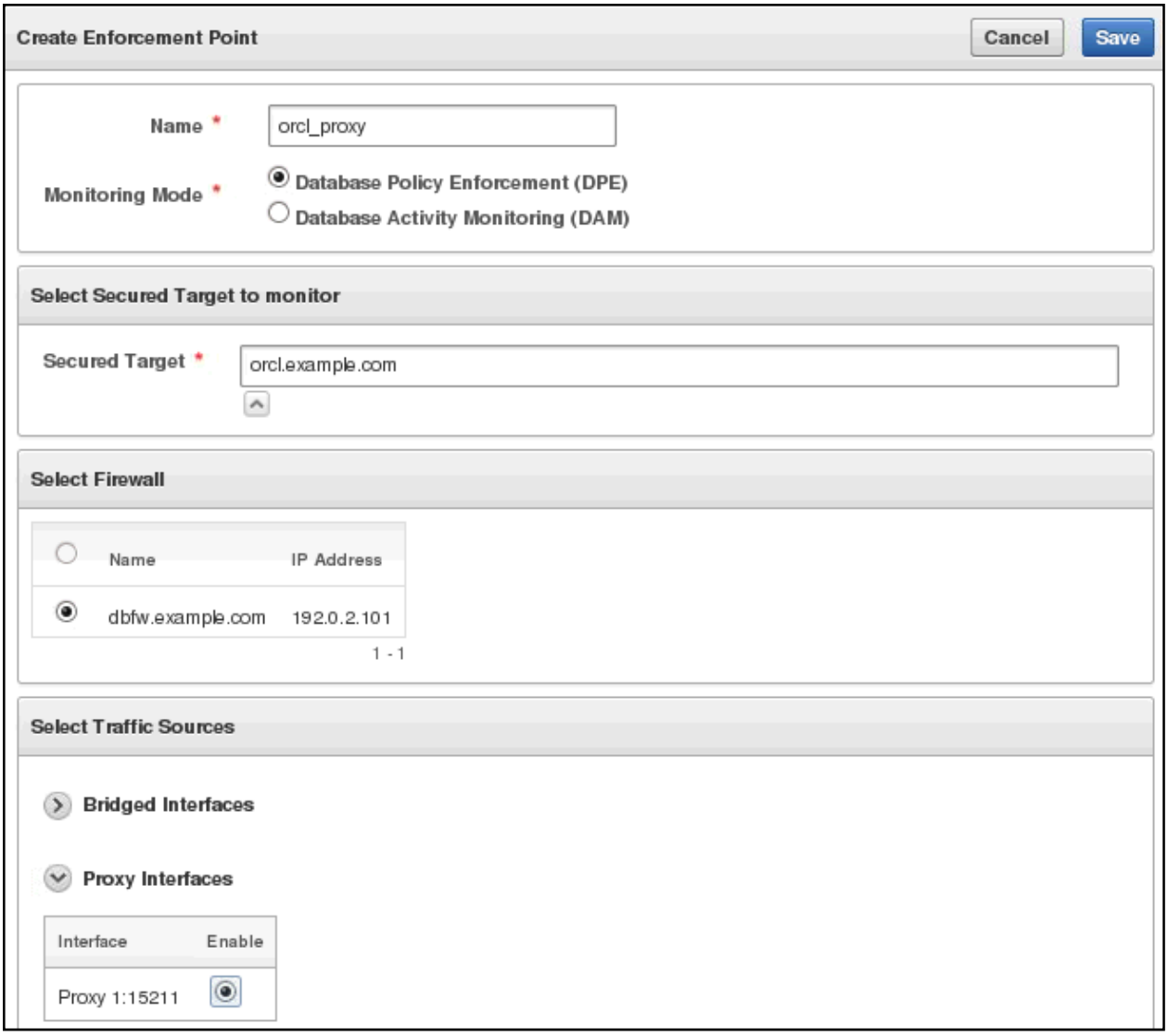


Perform the following steps to configure an enforcement point for a proxy deployment.

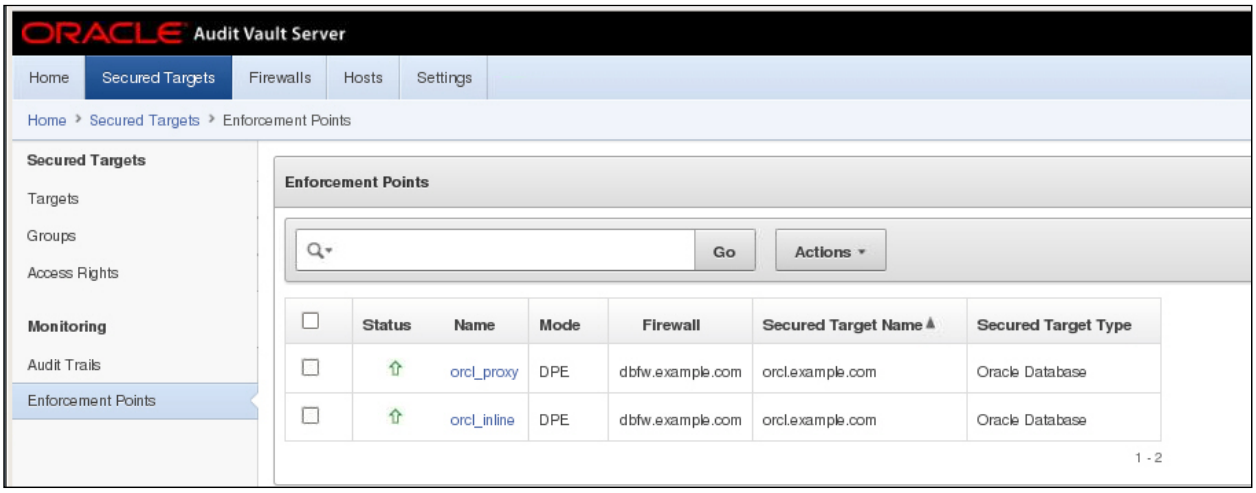
**Note:** The first three steps of the proxy deployment are the same as the inline deployment.

11. On the Enforcement Points page, click **Create**.
12. Enter a name for this enforcement point: **orcl_proxy**
13. Select a Monitoring Mode: **Database Policy Enforcement (DPE)**

    **Note:** DPE mode with a pass-all policy is equivalent to Database Activity Monitoring (DAM) mode.
14. Select the Secured Target to monitor:
    a. Click the **Up** arrow beside the Secured Target field.
    b. In the Select a Secure Target window, click **Select** for **orcl.example.com**.
15. In the Select Firewall section, select **dbfw.example.com**, which is the database firewall that handles this enforcement point.
16. When the page refreshes, select traffic sources in the **Proxy Interfaces** area:
    a. Expand **Proxy Interfaces**.
    b. Select **Enable** next to Proxy 1:15211.

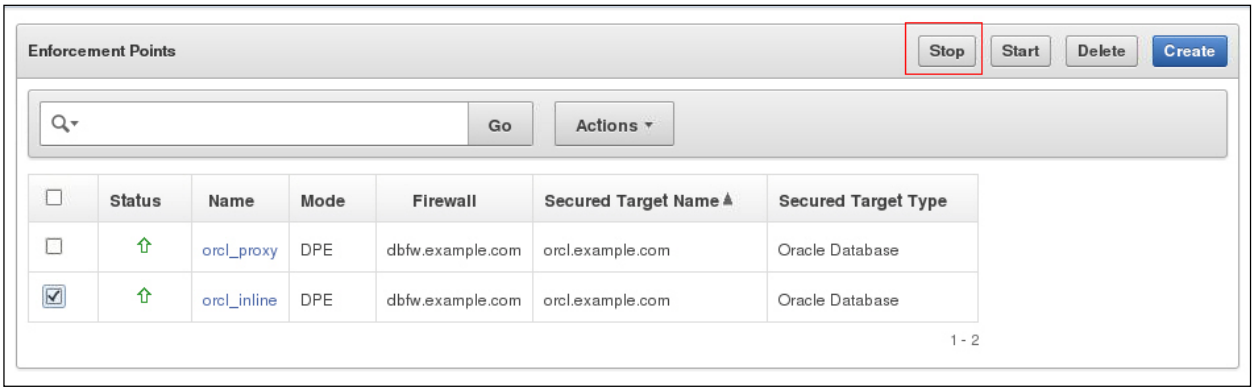



17. Click **Save**. A confirmation message briefly appears.

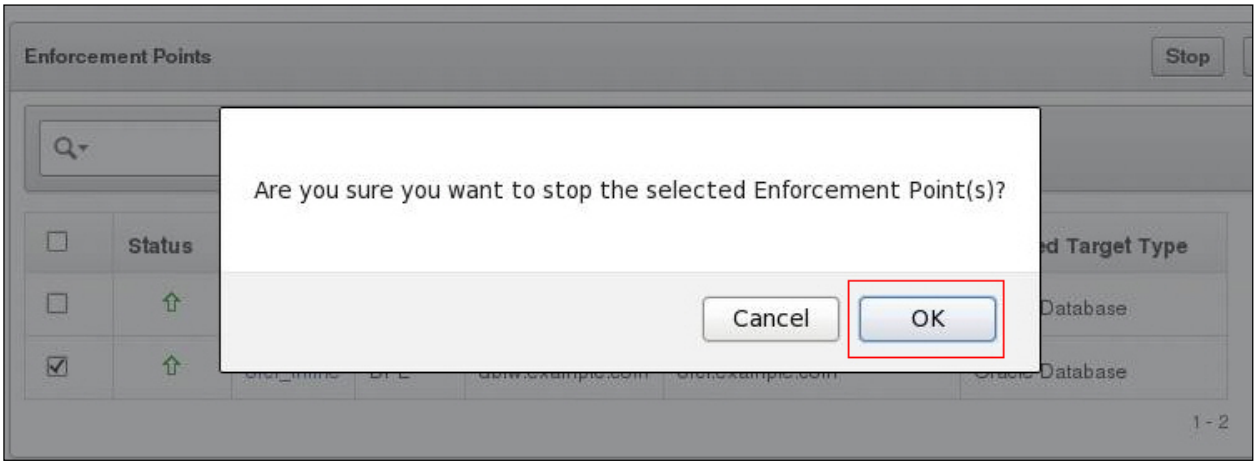


**Note:** You now have two enforcement points for the same database. In our practice environment, the "database side" of the firewall bridge is connected to eth1 on host02. The eth1 device is "down" by default. The traffic proxy is connected to eth0, which is "up" by default. To test the bridged firewall configuration, the eth0 and eth1 devices must be reversed with eth0 down and eth1 up.

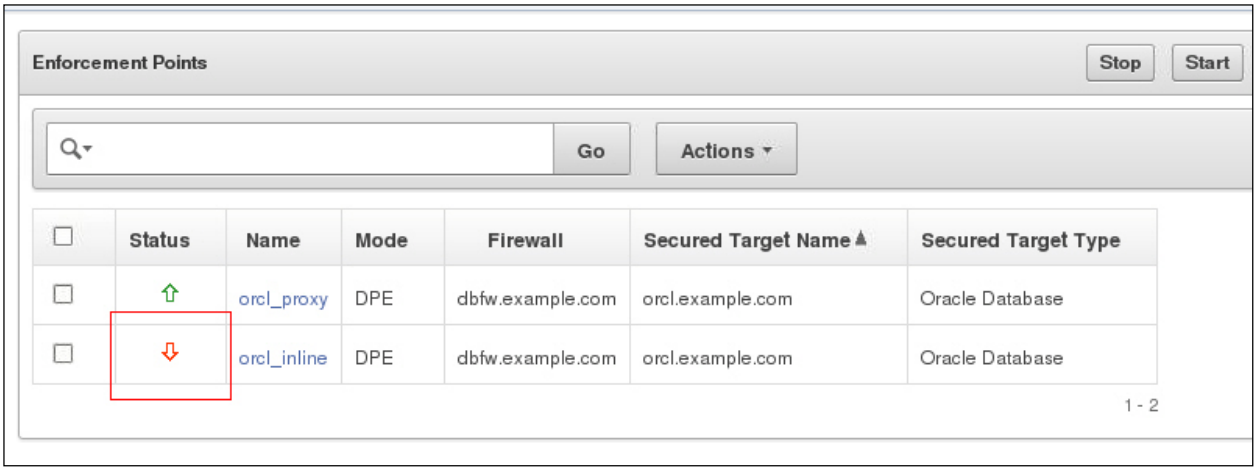
18. For the rest of this course, you will use only the **`orcl_proxy`** enforcement point. Perform the following steps to stop the **`orcl_inline`** enforcement point and disable the bridge.
    a. On the Enforcement Points page in the Audit Vault Server console, select the **`orcl_inline`** enforcement point and click **Stop**.




    b. Confirm that you want to stop the enforcement point by clicking **OK**.




    c. The Enforcement Points page now shows that the **`orcl_inline`** enforcement point is stopped.

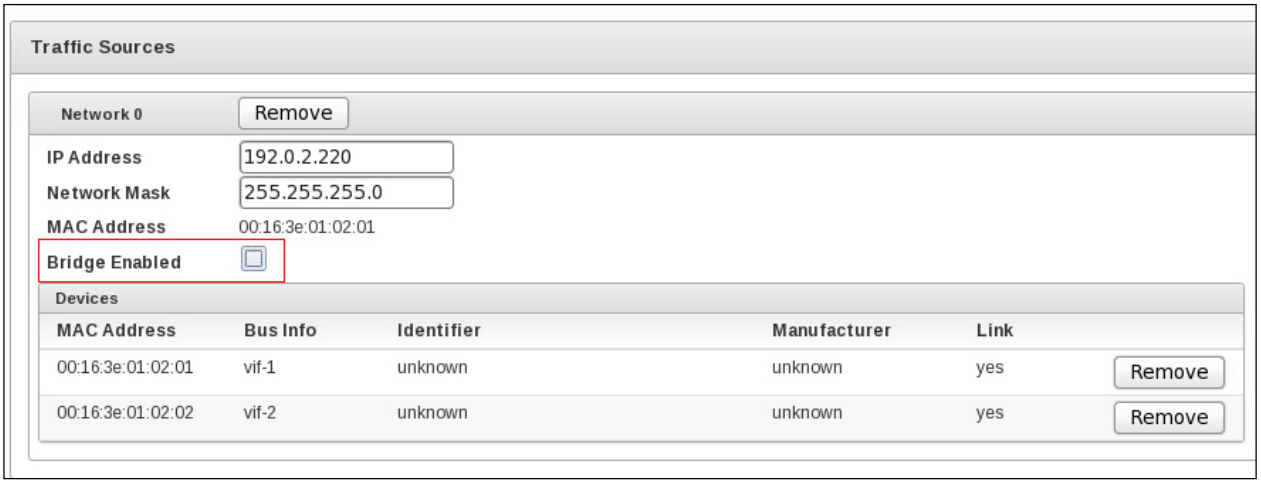



d. Log in to the Database Firewall console as the **`FWADMIN`** user.

e. Click **Network** in the System menu.

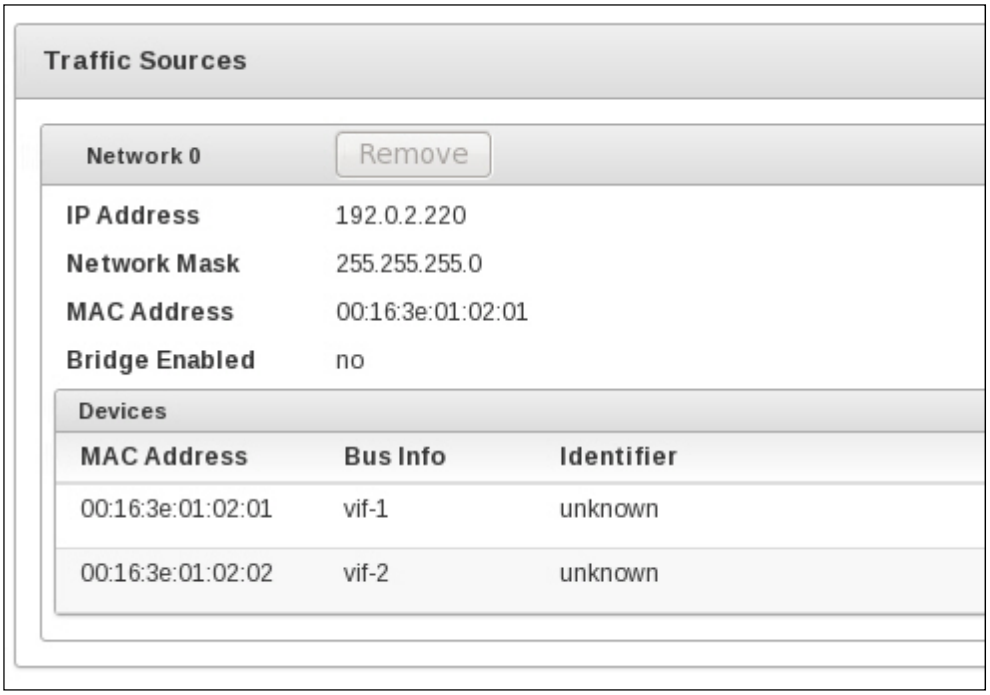
f. Scroll to the bottom of the page and click **Change**.

g. In the Traffic Sources section, deselect **Bridge Enabled**.




h. Scroll to the bottom of the page and click **Save**.

i. The Traffic Sources page now indicates the bridge is no longer enabled.




j. Log out of the Database Firewall console.

19. Log out of the Audit Vault Server console or continue to the next practice.

# Practice 8-10: Configuring Database Response Monitoring

## Overview

In this practice, you enable database response monitoring for a secured target.

## Assumptions

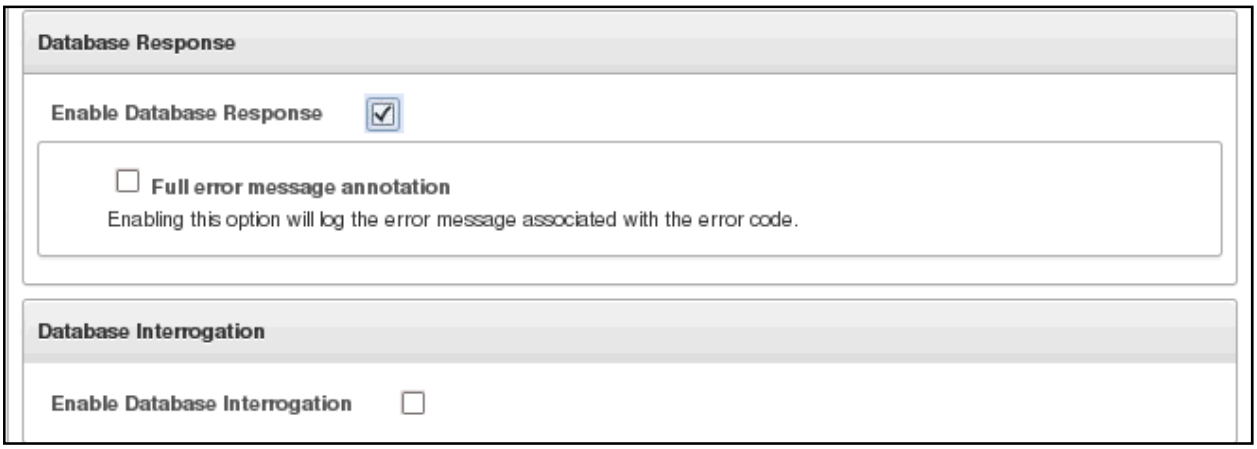
Practice 8-9 is complete and enforcement points have been created. The proxy enforcement point is active.

## Tasks

Enabling the Database Response Monitoring feature allows the Database Firewall to record responses that the secured target database makes to login requests, logout requests and SQL statements sent from database clients. This feature allows you to determine whether the database executed logins, logouts, and statements successfully, and can provide useful information for audit and forensic purposes.

Perform the following steps to enable database response monitoring for a secured target:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Secured Targets** tab.
3. In the Monitoring menu, click **Enforcement Points**.
4. Select the `orcl_proxy` enforcement point by clicking **`orcl_proxy`** in the Name field.
5. In the Database Response section of the Modify Enforcement Point page, select **Enable Database Response**.




6. Click **Save**.
7. Log out of the Audit Vault Server console.

# Practices for Lesson 9: Using Host Monitoring

**Chapter 9**

# Practices for Lesson 9

## Practices Overview

In these practices, you will configure host monitoring.

# Practice 9-1: Reviewing Sample Configurations for Host Monitoring Implementation

## Overview

In this **pen-and-paper** practice, you review sample configurations and determine whether host monitoring is an appropriate choice.

## Tasks

1. You have many small databases in a distributed environment. You want Oracle Audit Vault and Database Firewall (Oracle AVDF) to monitor all of these small databases centrally. Is Host Monitoring the correct solution for this environment?

   *Answer: Yes*

# Practice 9-2: Installing the Host Monitor

## Overview

In this practice, you install the host monitor.

This installation procedure is applicable only for Linux hosts. For Windows hosts, the host monitor is automatically installed when the Audit Vault Agent is deployed.

## Assumptions

The Audit Vault Agent has been deployed.

## Tasks

Perform the following steps to install the Host Monitor:

1. Open a terminal window and enter the following command:

   `ssh -X oracle@host02`

   Enter a password of `oracle` when prompted.

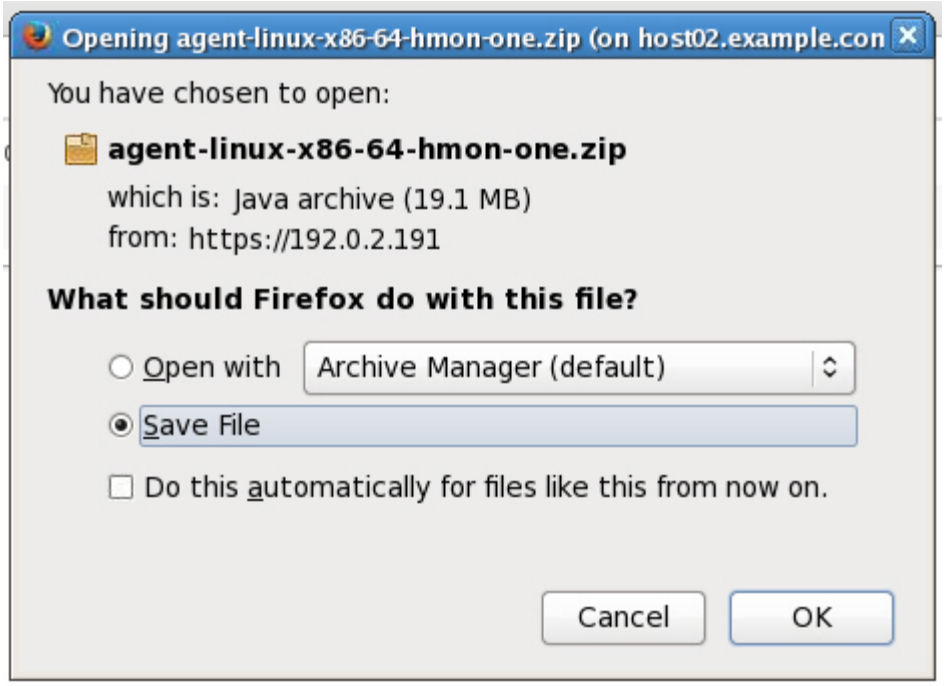
```
$ ssh -X oracle@host02
oracle@host02's password:
Last login: Wed Jun 11 18:37:59 2014 from em12c.example.com
[oracle@host02 ~]$
```

2. Start Firefox and launch the Audit Vault console.

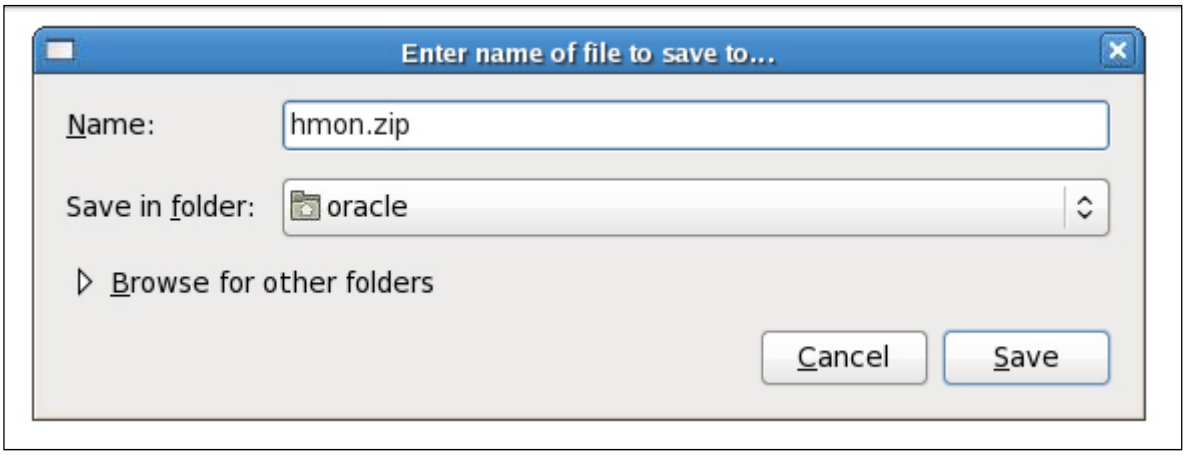
```
[oracle@host02 ~]$ firefox https://192.0.2.191
```

3. Configure Firefox so that you can specify where a file should be saved:
   a. Expand the **Edit** menu and click **Preferences**.
   b. On the General tab, select "**Always ask me where to save files**" and click **Close**.
4. Log in to the **Audit Vault Server console** as the administrator with username of **`AVADMIN2_A`** and password of **`oracle_4U`**.
5. Click the **Hosts** tab.
6. Click **Agent** on the left side.
7. Click the **Download** button next to Host Monitor (Linux x86-64).


8. Select **Save File** and click **OK**.




9. Change the file name to **`hmon.zip`** and select the `oracle` directory. Then click **Save**.




10. Close the Downloads window.
11. Open another terminal window and enter the following command:
    **`ssh -X oracle@host02`**
    Enter a password of **`oracle`** when prompted.

```
$ ssh -X oracle@host02
oracle@host02's password:
Last login: Tue Jun 17 17:28:22 2014 from 192.0.2.1
[oracle@host02 ~]$
```

12. Switch user to the **`root`** user and enter a password of **`oracle`** when prompted.

```
[oracle@host02 ~]$ su -
Password:
```

13. Change directories to the **`/usr/local`** directory.

```
root@host02 ~]# cd /usr/local
[root@host02 local]#
```

14. Copy the **hmon.zip** file from the **/home/oracle** directory.

```
[root@host02 local]# cp /home/oracle/hmon.zip hmon.zip
[root@host02 local]#
```

15. As the **root** user, unzip the host monitor file.

```
[root@host02 local]# unzip hmon.zip
Archive:  hmon.zip
   creating: hm/
  inflating: hm/hostmonsetup
  inflating: hm/HMDeployerMain.o
  inflating: hm/HostMonManagerMain.o
  inflating: hm/HostMonitorMain.o
  inflating: hm/hostmon.mk
  inflating: hm/libhmdeployer11.a
  inflating: hm/libhostmon11.a
   creating: hm/network/
   creating: hm/network/admin/
  inflating: hm/network/admin/sqlnet.ora
  inflating: hm/libapr-1.so.0
  inflating: hm/libclntsh.so.11.1
  inflating: hm/libocci.so.11.1
  inflating: hm/libnnz11.so
  inflating: hm/libociicus.so
  inflating: hm/bootstrap.prop
 extracting: hm/network/admin/avwallet/ewallet.p12
 extracting: hm/network/admin/avwallet/cwallet.sso
[root@host02 local]#
```

**Note:** When you unzip the file the `HM_Home` directory (`hm`) is created.

16. Ensure that the **hostmonsetup** file permissions include execute.

```
[root@host02 local]# ls -l hm/hostmonsetup
-r-x------ 1 root root 35927 Mar 28 03:01 hm/hostmonsetup
```

17. Execute the following command, providing parameter values as described:
    **HM_Home/hostmonsetup install agenthome=Agent_Home agentuser=Agent_Username agentgroup=Agent_Group**
    Parameter values:
    - **HM_Home**: **hm**
    - **Agent_Home** (Audit Vault Agent installation directory): **/home/oracle/Agent_Home**
    - **Agent_Username** (username of the user who installed the Audit Vault Agent): **oracle**
    - **Agent_Group** (group to which the Agent_Username belongs): **oinstall**

```
[root@host02 local]# hm/hostmonsetup install
agenthome=/home/oracle/Agent_Home  agentuser=oracle
agentgroup=oinstall
Setting ownership to root:root for:
        /usr/local/hm/bootstrap.prop
        /usr/local/hm/network/admin/sqlnet.ora
Detected AV Server DB's IP - 192.0.2.191
hostmonitor installed at "/usr/local/hm" directory.
The user:group who owns the agent - oracle:oinstall
#####################################
# Setting permission and ownership #
#####################################
Setting ownership to root:oinstall and permission to -rwxr-x---
for
        /usr/local/hm
Setting ownership to root:oinstall for:
        /usr/local/hm/libclntsh.so*
        /usr/local/hm/libapr-1.so*
        /usr/local/hm/libnnz11.so
        /usr/local/hm/libociicus.so
        /usr/local/hm/libocci.so*
        /usr/local/hm/HostMonitorMain.o
        /usr/local/hm/HostMonManagerMain.o
        /usr/local/hm/libhostmon11.a
        /usr/local/hm/hostmonitor
        /usr/local/hm/hostmonsetup
        /usr/local/hm/hostmon.mk
Setting -r--r----- permission to
        /usr/local/hm/libclntsh.so*
        /usr/local/hm/libapr-1.so*
        /usr/local/hm/libnnz11.so
        /usr/local/hm/libociicus.so
        /usr/local/hm/libocci.so*
        /usr/local/hm/HostMonitorMain.o
        /usr/local/hm/HostMonManagerMain.o
        /usr/local/hm/libhostmon11.a
        /usr/local/hm/hostmon.mk
Setting ownership to root:oinstall and permission to -r-x--x---
for
        /usr/local/hm/hostmonmanager
Converting /usr/local/hm/hostmonitor
        to setuid executable.
```

```
Setting -r-x------ permission to
\n\t/usr/local/hm/hostmonsetup\n
Setting ownership to root:oinstall for:
        /usr/local/hm/HMDeployerMain.o
        /usr/local/hm/libhmdeployer11.a
        /usr/local/hm/hmdeployer
Setting -r--r----- permission to
        /usr/local/hm/HMDeployerMain.o
        /usr/local/hm/libhmdeployer11.a
Converting /usr/local/hm/hmdeployer
        to setuid executable.
Generating the private key for hostmonitor.
Generating RSA private key, 2048 bit long modulus
.....................................................................
.....................................................+++
....+++
unable to write 'random state'
e is 65537 (0x10001)
Generating a certificate request for the hostmonitor.
Generating a Self signed certificate for hostmonitor.
Signature ok
subject=/CN=Hostmonior_Cert_
Getting Private key
unable to write 'random state'
Setting ownership to root:root for:
        /usr/local/hm/hmcert.crt
        /usr/local/hm/hmcsr.csr
        /usr/local/hm/hmprivkey.perm
        /usr/local/hm/network/admin/avwallet/ewallet.p12
        /usr/local/hm/network/admin/avwallet/cwallet.sso
Setting -r-------- permission for:
        /usr/local/hm/hmcert.crt
        /usr/local/hm/hmcsr.csr
        /usr/local/hm/hmprivkey.perm
        /usr/local/hm/network/admin/avwallet/ewallet.p12
        /usr/local/hm/network/admin/avwallet/cwallet.sso
Deleting /home/oracle/Agent_Home/hm if exist.
Creating /home/oracle/Agent_Home/hm symlink to
        /usr/local/hm
Setting ownership to oracle:oinstall for
        /home/oracle/Agent_Home/hm
Note: To enable authentication,
1. Transfer /usr/local/hm/hmcsr.csr file to
```

```
        /usr/local/dbfw/etc directory of AVS Server(using root
credential of AVS Server)
2. At AVS Server, login as root and sign this file by executing
        /usr/local/dbfw/bin/generate_casigned_hmcert.sh
3. Replace /usr/local/hm/hmcert.crt with the above signed
certificate.
4. As root, run -
        a) chown root:root /usr/local/hm/hmcert.crt
        b) chmod 400 /usr/local/hm/hmcert.crt
5. At DBFW, login as root and run the following command:
        cp /usr/local/dbfw/etc/controller.crt
/usr/local/dbfw/etc/fw_ca.crt
        chown dbfw:dbfw /usr/local/dbfw/etc/fw_ca.crt
        chmod 400 /usr/local/dbfw/etc/fw_ca.crt
6. Restart/start hostmonitor
Successfully completed hostmonitor setup.
Host Monitor is now installed.
```

18. Exit from the `root` session and close the terminal window.

# Practice 9-3: Configuring an Audit Trail for Host Monitoring

## Overview

In this practice, you configure an audit trail for host monitoring.

To start collecting audit data, you must configure an audit trail for each secured target in the Audit Vault Server, and then start the audit trail collection manually. For host monitoring, you must configure an audit trail with a type of NETWORK.

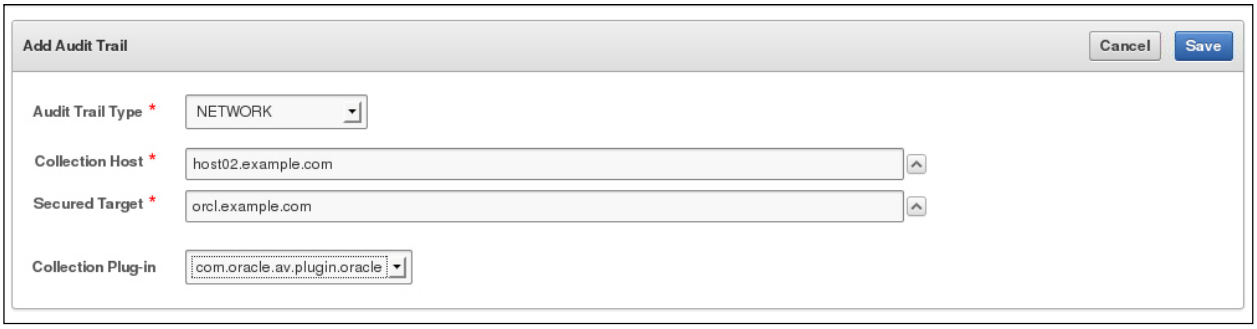
## Assumptions

Practice 5-5: Registering the Secured Target and Practice 8-9: Creating and Configuring Enforcement Points have been successfully completed.

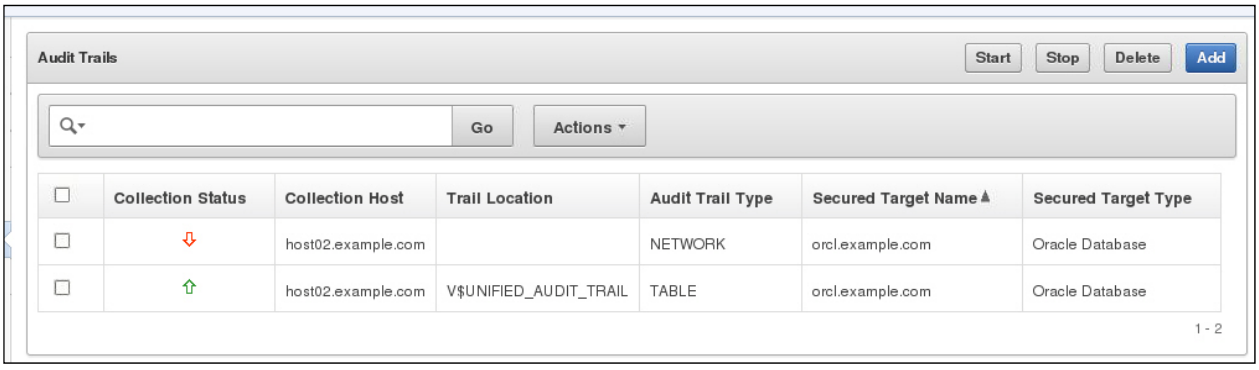
## Tasks

Perform the following steps to configure a NETWORK audit trail for host monitoring.

1. Log in to the Audit Vault Server console as the administrator with a username of **`AVADMIN2_A`** and password of **`oracle_4U`**.
2. Click the **Secured Targets** tab.
3. Under Monitoring, click **Audit Trails**.
4. On the Audit Trails page, click **Add**.
5. In the Audit Trail Type drop-down list, select **NETWORK**.
6. In the Collection Host field, click the up-arrow icon to display a search box. Select the host computer where the Audit Vault Agent is deployed**: host02.example.com**
7. In the Secured Target field, click the up-arrow icon to display a search box. Select the secured target: **orcl.example.com**
8. Click **Save**.




9. The Audit Trails page shows the new audit trail.




10. Log out of the Audit Vault Server console or continue to the next practice.

# Practice 9-4: Starting the Host Monitor

## Overview

In this practice, you start the host monitor. Starting the host monitor consists of starting collection for the NETWORK audit trail on the host you are monitoring.

The audit trail will start automatically after some time. You can start it manually by following the steps in this practice.

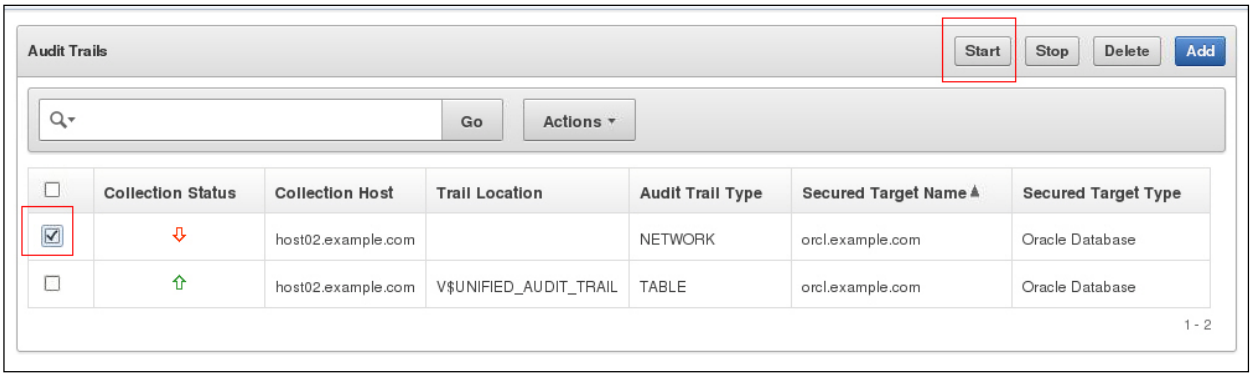
## Assumptions

Practice 9-3: Configuring an Audit Trail for Host Monitoring has been completed.

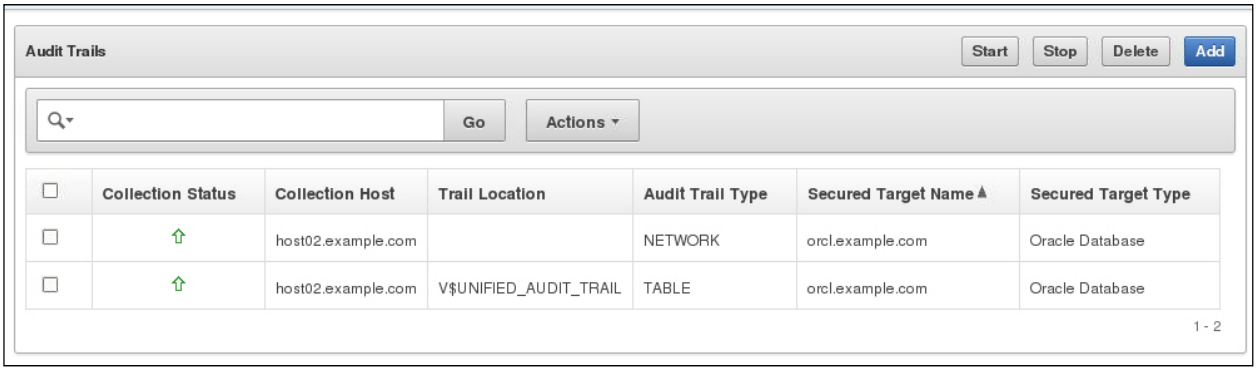
## Tasks

Perform the following steps to manually start the host monitor:

1. Log in to the Audit Vault Server console as an administrator.
2. Click the **Secured Targets** tab.
3. Under Monitoring, click **Audit Trails**.
4. Select the **NETWORK** audit trail and click **Start**.




5. Click **OK** to confirm you want to start the audit trail.
6. The Collection Status changes indicating the audit trail is started.




7. Log out of the Audit Vault Server console.

# Practices for Lesson 10: Configuring High Availability

**Chapter 10**

# Practices for Lesson 10

## Practices Overview

In these practices, you will determine whether resilient pairs are an appropriate configuration given a set of requirements. You will also list the steps required to configure a resilient pair of Audit Vault Servers and Database Firewalls.

# Practice 10-1: Listing the Steps to Configure a Resilient Pair of Audit Vault Servers

## Overview

In this pen-and-paper practice, you list the steps required to configure a resilient pair of Audit Vault Servers.

## Tasks

Place the following tasks required for configuring a resilient pair of Audit Vault Servers in the correct order.

1. Copy the server certificate from the secondary server to the primary server and enter the IP address of the secondary server.
2. Copy the server certificate from the primary server to the secondary server and enter the IP address of the primary server.
3. Start high availability pairing of the Audit Vault Servers at the primary server.

*Answer: 2, 1, 3*

# Practice 10-2: Listing the Steps to Configure a Resilient Pair of Database Firewalls

## Overview

In this pen-and-paper practice, you list the steps required to configure a resilient pair of Database Firewalls.

## Tasks

Place the following tasks required for configuring a resilient pair of Audit Vault Servers in the correct order.

1. Select the primary and secondary firewalls you want to pair on the Resilient Pairs page of the Audit Vault Server console.
2. Disable enforcement points configured on the Database Firewalls.

*Answer: 2, 1*

# Practices for Lesson 11: Creating Custom Collection Plug-ins

**Chapter 11**

# Practices for Lesson 11

## Practices Overview

In these practices, you will identify whether a source is applicable for a custom collection plug-in. You will also identify specific requirements for plug-ins and list the steps for creating a custom collection plug-in.

# Practice 11-1: Identifying the Need for a Custom Collection Plug-in

## Overview

In this **pen-and-paper** practice, you identify whether an out-of-the box collection plug-in exists for a list of source databases.

## Tasks

1. You want to collect audit data from a number of different database sources. For which of the following is an out-of-the box collection plug-in available?
   a. Oracle Database 9*i*
   b. Oracle Database 12*c*
   c. Microsoft SQL Server 2012
   d. MySQL 5.0
   e. MySQL 5.6
   f. Sybase ASE 15.7

   *Answer: b, c, e, f*

# Practice 11-2: Identifying Database Table Collection Plug-in Requirements

## Overview

In this **pen-and-paper** practice, you review a description and determine whether the system meets the requirements for a database table collection plug-in.

Database table collection plug-ins can collect audit data from an audit table, using information from an XML Mapper file you create.

## Tasks

1. You plan to create a database table collection plug-in for a system with the following characteristics:
   a. The system employs a one-step user/password authentication mechanism.
   b. The audit data is stored in a set of hierarchical tables.
   c. The audit data tables are accessible via a JDBC driver.

   Is this system a good candidate for a database table collection plug-in?

   *Answer: No, the audit data must be stored in a 'flat' table.*

# Practice 11-3: Identifying XML File Collection Plug-in Requirements

## Overview

In this **pen-and-paper** practice, you review a description and determine whether the system meets the requirements for an XML file collection plug-in.

XML file collection plug-ins can collect audit data from XML audit files present in a single directory, using information from an XML Mapper file you create.

## Tasks

1. You plan to create an XML file collection plug-in for a system with the following characteristics:
   a. The XML audit log files are stored in a single directory conforming to a *.xml pattern.
   b. An XML audit log file can be reopened by the auditing system.
   c. The XML audit log files are complete XML documents.

   Is this system a good candidate for an XML file collection plug-in?

   *Answer: No, the requirement is that once the XML file has been written to and is complete (closed and a new one opened), it is never reopened by the auditing system.*

# Practice 11-4: Listing the Steps to Create a Custom Collection Plug-in

## Overview

In this **pen-and-paper** practice, you list the steps you need to perform to create and package a custom collection plug-in.

## Tasks

Place the following steps in the correct order to enable the implementation of a custom collection plug-in.

1. Start collections.
2. Create an XML mapper file.
3. Deploy the collection plug-in at the Audit Vault Server.
4. Package the XML mapper file and manifest file.
5. Set secured target collection attributes.
6. Create a `STAGE_DIR_ROOT` with subdirectories.

*Answer: 6, 2, 4, 3, 5, 1*

# Practices for Lesson 12: Managing the Audit Vault Server

**Chapter 12**

# Practices for Lesson 12

## Practices Overview

In these practices, you will verify that an archived location has been set and start an archive job.

# Practice 12-1: Verifying an Archived Location Definition

## Overview

In this practice, you verify that an archived location has been defined.

You must define one or more locations as destinations for archive files before you can start an archive job. An archiving destination specifies the archive storage locations and other settings.

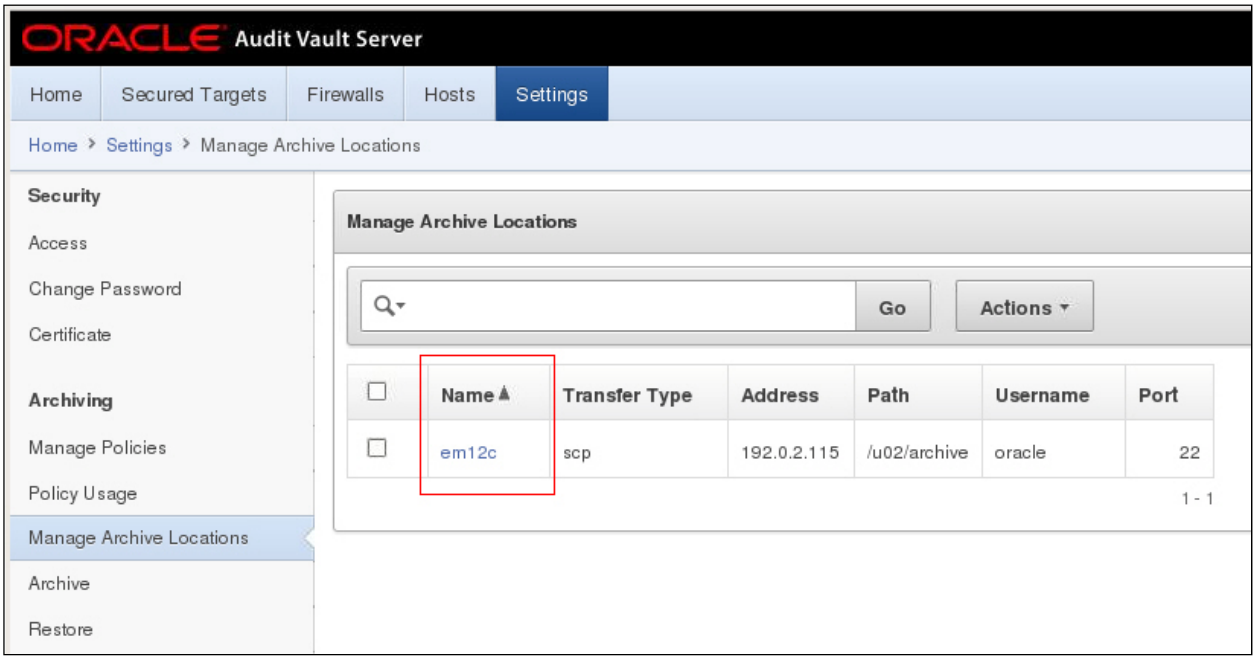
## Assumptions

You completed Practice 4-6, Defining an Archiving Location.

## Tasks

Perform the following steps to verify that an archived location has been defined:

1. Log in to the Audit Vault Server as the administrator **`AVADMIN2_A`** with a password of **`oracle_4U`**.
2. Click the **Settings** tab.
3. Under Archiving, click **Manage Archive Locations**.
4. A list of existing archive locations is displayed. Verify that the location named **em12c** has been defined.




5. Log out of the Audit Vault Server console or continue to the next practice.

# Practice 12-2: Starting an Archive Job

## Overview

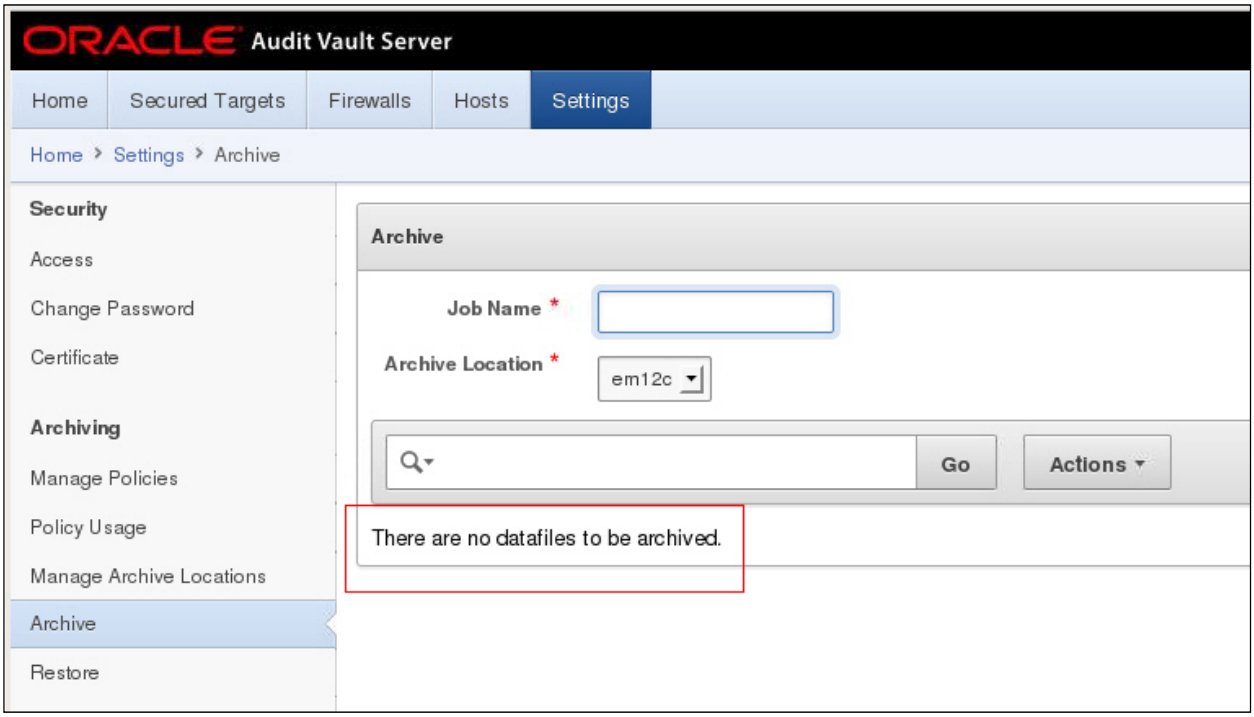
In this practice, you attempt to start an archive job.

When an Oracle Audit Vault and Database Firewall (Oracle AVDF) auditor selects a retention (archiving) policy for a secured target, audit data for that secured targets will be available for archive jobs according to the Months Online specified in the retention policy. After the “months online” period has expired, the data is available for archiving and is no longer visible in reports.

## Tasks

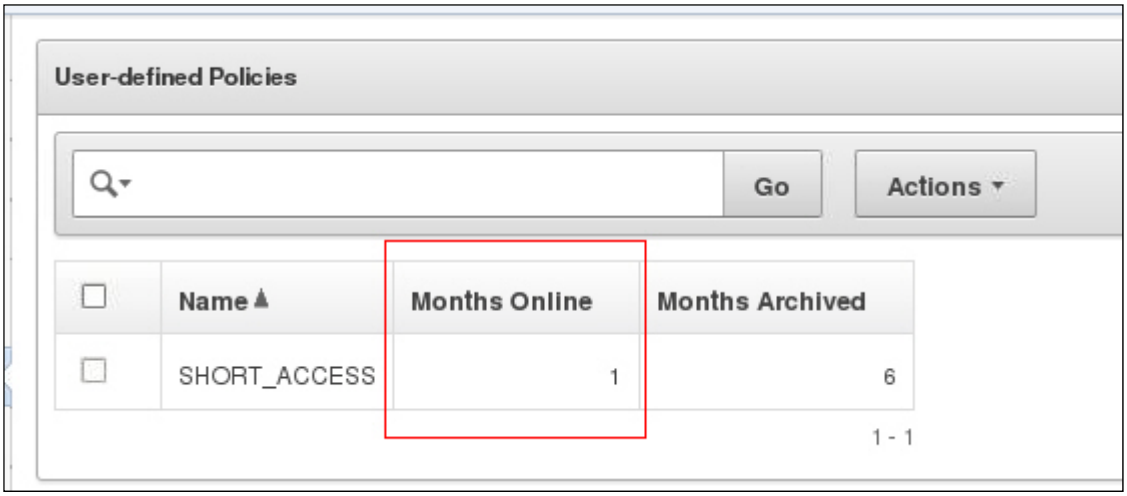
Perform the following steps to start an archive job:

1. Log in to the Audit Vault Server as an administrator.
2. Click the **Settings** tab.
3. In the Archiving menu, click **Archive**.
4. The Archive page is displayed. On this page, you enter a name for the archive job, select the archive location, and select the files to be archived. Why are there no data files listed on this page?




*Answer: The files listed are those for which the Months Online period has expired according to the secured target’s retention policy.*

5. Click **Manage Policies** in the menu to view the retention policy.




6. Log out of the Audit Vault console or continue to the next practice.

# Practice 12-3: Restoring Archived Data Files

## Overview

In this practice, you determine whether archived data files can be restored.

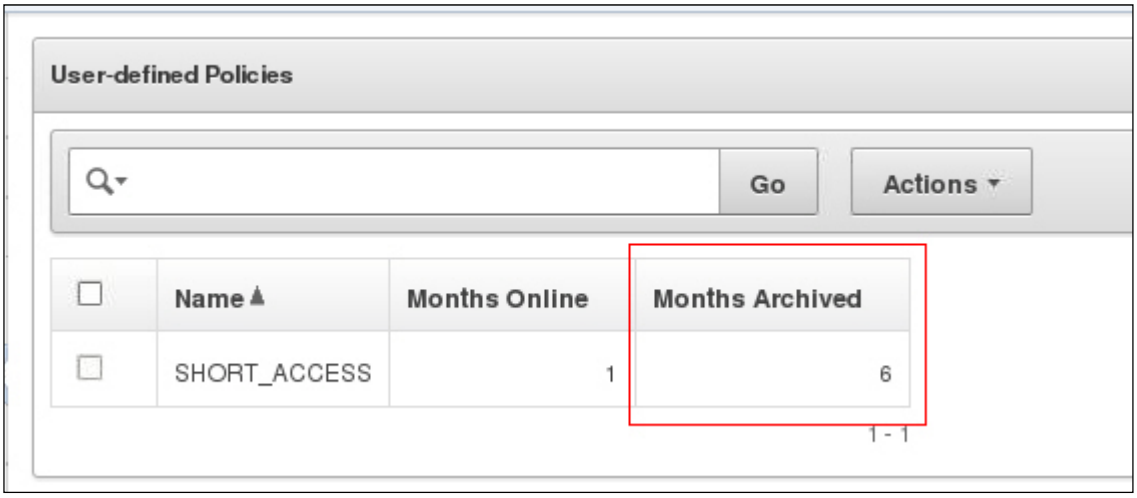
You can restore data files for a specific secured target and time range. The Months Archived value in a secured targets retention (archiving) policy determines how long the secured target's data is available to restore to the Audit Vault Server. When the Months Archived period expires, the data is no longer available to restore; however, it continues to reside in the archive location.

## Tasks

Data is needed for a report that is from 9 months ago. You know the data was archived. Can it be restored?

Perform the following steps to determine whether the archived data files can be restored:

1. Log in to the Audit Vault Server as an administrator.
2. Click the **Settings** tab.
3. In the Archiving menu, click **Manage Policies**.
4. Review the value in Months Archived. Can the requested data files be restored?




*Answer: No, the requested files are older than what is available to be restored.*

# Practices for Lesson 13: Managing the Database Firewall

**Chapter 13**

# Practices for Lesson 13

## Practices Overview

In these practices, you will view network traffic and diagnostic information.

# Practice 13-1: Viewing Live Network Traffic

## Overview

In this practice, you view live network traffic.

You may want to view network traffic for debugging purposes. You can view live network traffic going through a firewall, or capture the traffic to a file (.pcap file type) that you can download and analyze.

## Tasks

Perform the following steps to view live network traffic in a Database Firewall:

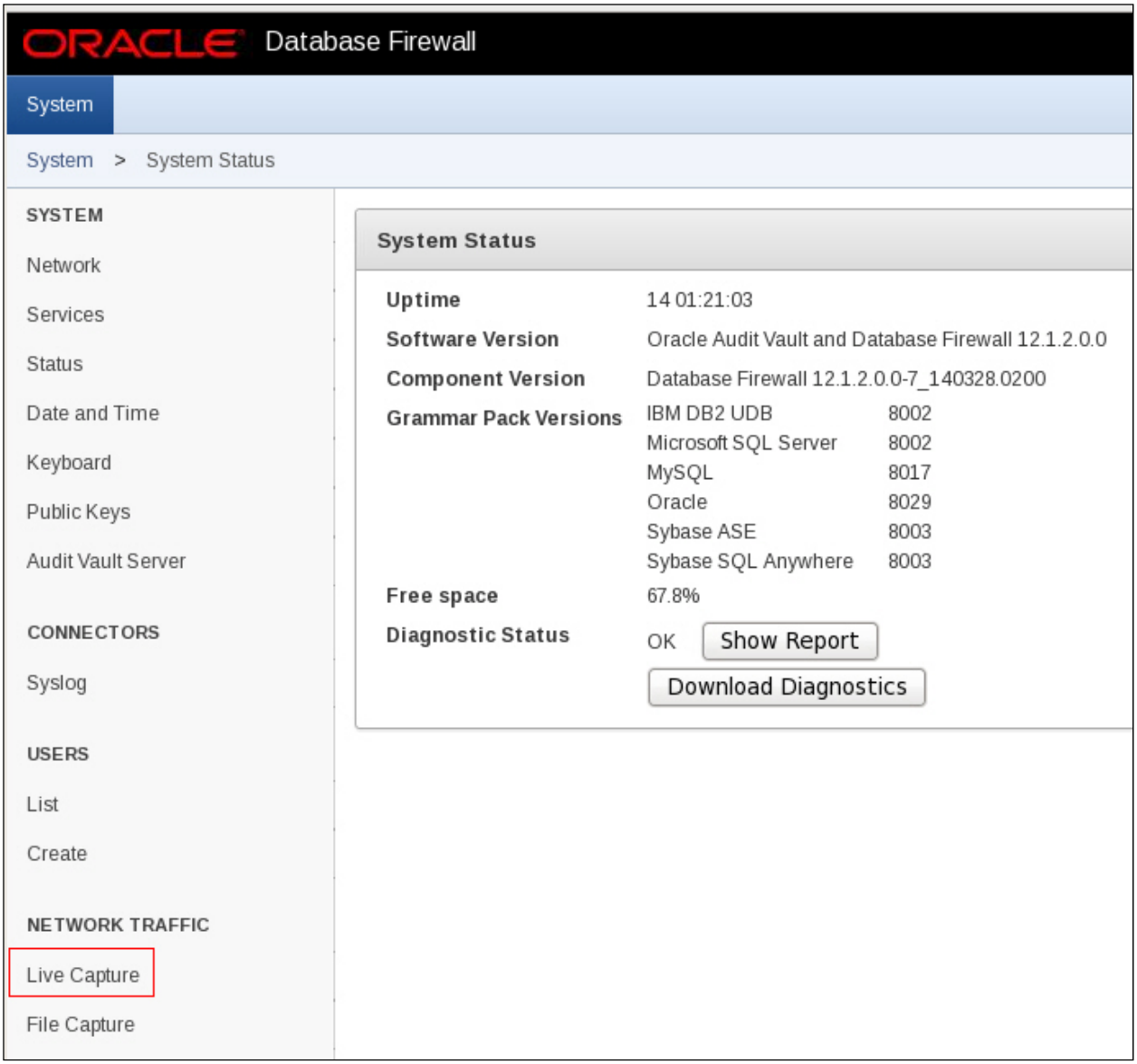
1. Log in to the Database Firewall administration console.
   a. Open a terminal window and connect to the em12c VM as the **oracle** OS user. The password is **oracle**.

```
$ ssh -X oracle@em12c
oracle@em12c's password:
Last login: Fri Jun  6 20:00:30 2014 from dom0.example.com
[oracle@em12c ~]$
```

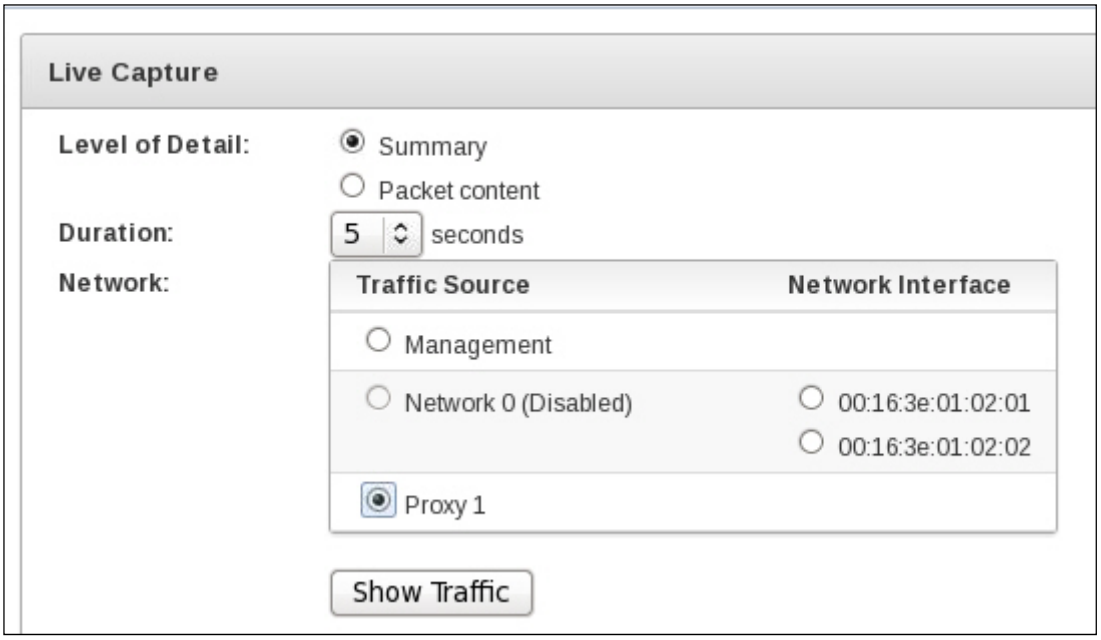
   b. Start Firefox and launch the Database Firewall console.

```
[oracle@em12c ~]$ firefox https://192.0.2.101
```

   c. Enter **fwadmin** as the username with **oracle_4U** as the password. Click **Login**.
2. Under Network Traffic, click **Live Capture**.




3. In the Level of Detail field, select Summary or Packet Content. For this practice, select **Summary**.
4. In the Duration field, select the number of seconds to capture live traffic. For this practice, select **5 seconds**.
5. In the Network field, select the network traffic source for which to capture traffic. For this practice, select **Proxy 1**.
6. Click the **Show Traffic** button.




The live traffic is displayed for the selected duration.

7. Log out of the Database Firewall console or continue to the next practice.

# Practice 13-2: Capturing Network Traffic

## Overview

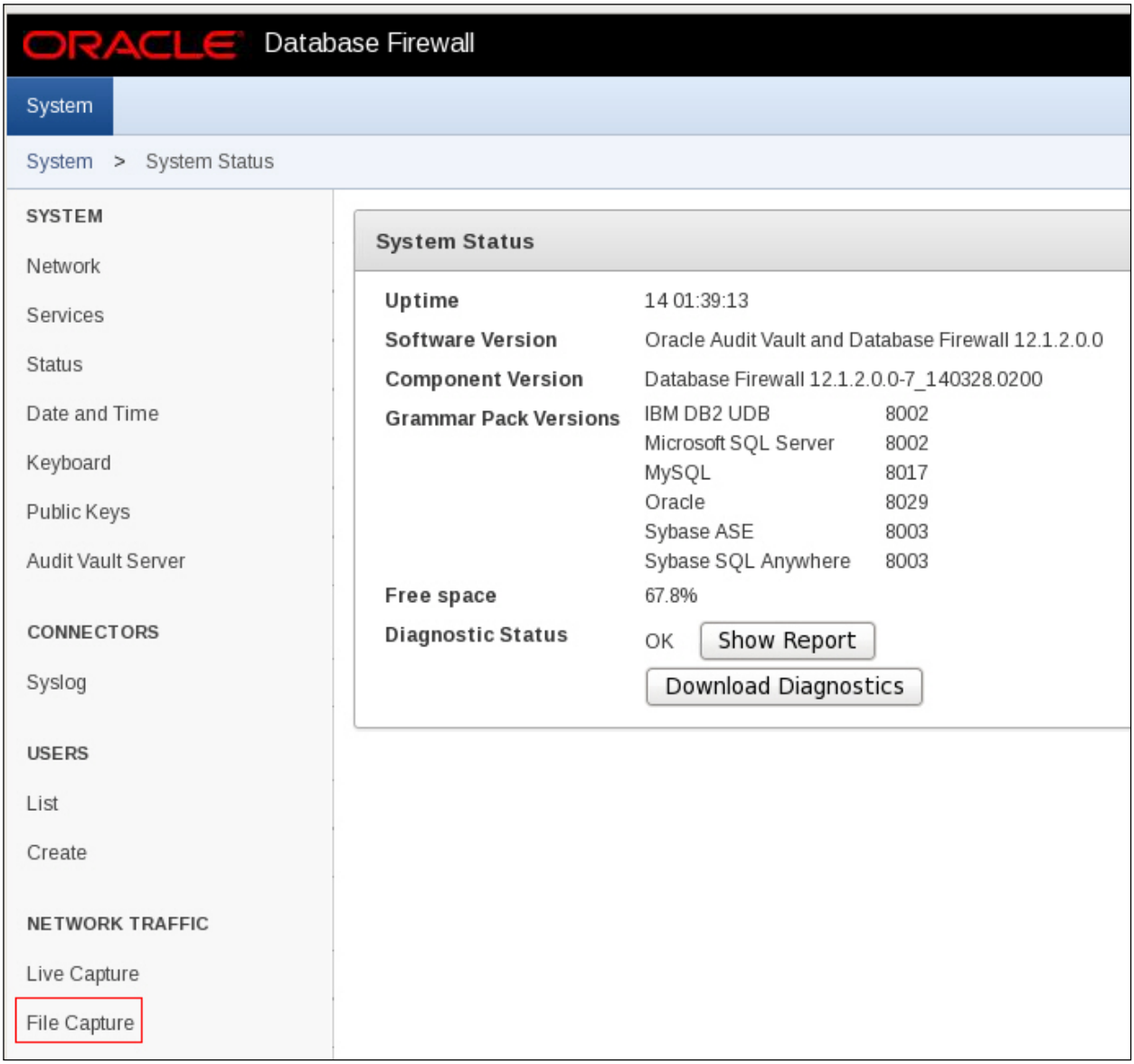
In this practice, you capture network traffic to a file.

You may wish to view network traffic for debugging purposes. You can view live network traffic going through a firewall, or capture the traffic to a file (`.pcap` file type) that you can download and analyze.

## Tasks

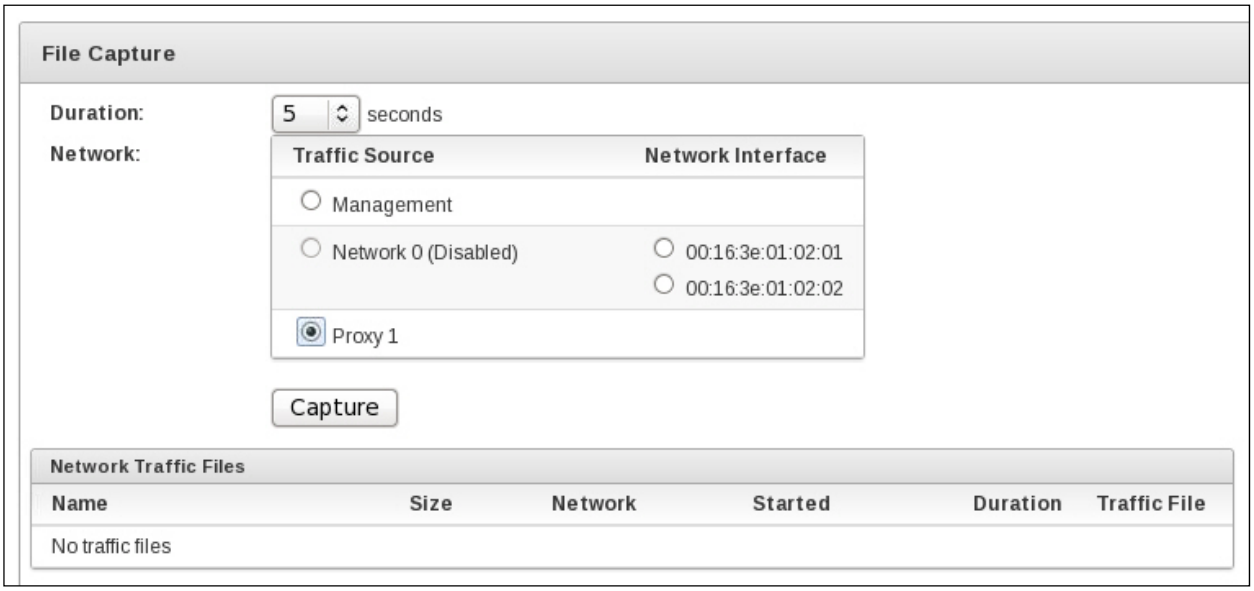
Perform the following steps to capture network traffic to a file:

1. Log in to the Database Firewall administration console as the **`fwadmin`** user with a password of **`oracle_4U`**.
2. Under Network Traffic, click **File Capture**.

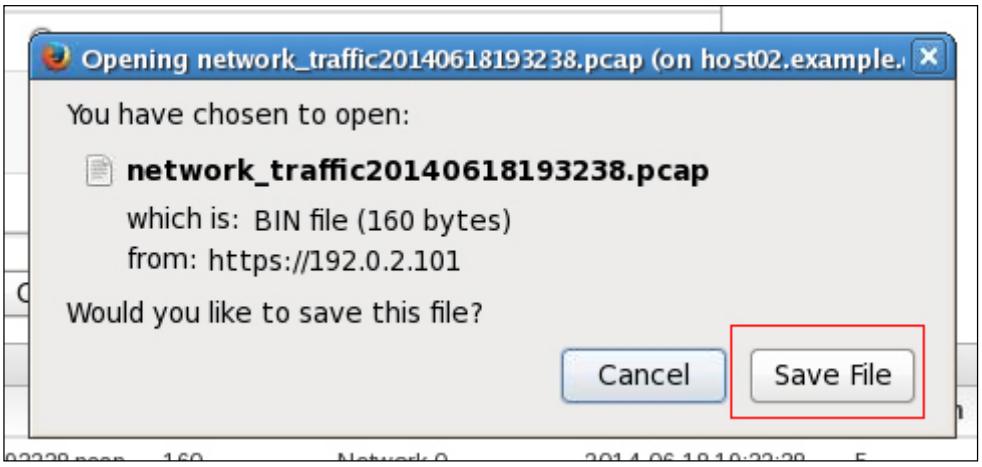



3. In the Duration field, select the number of seconds to capture traffic. For this practice, select **5 seconds**.

4. In the Network field, select the network traffic source for which to capture traffic. For this practice, select **Proxy 1**.
5. Click **Capture**.




6. The traffic file (`.pcap` format) is displayed in the Network Traffic Files list. Click **Download** for the file you want to download.
7. Save the file.
   a. Click **Save File**.




   b. Click **Save**.
8. Open a terminal window and log in to the em12c VM as the Oracle user.

```
$ ssh -X oracle@em12c
oracle@em12c's password:
Last login: Tue Jun 17 17:35:03 2014 from 192.0.2.1
```

9. Verify that the file you downloaded is in the `/home/oracle` directory.

```
[oracle@em12c ~]$ ls
afiedt.buf    Documents  Music
Templates
```

```
Agent_Home     Downloads  network_traffic20140618193238.pcap
Videos
agent.jar      hmon.zip   oradiag_oracle
demoapps.dmp   hr         Pictures
Desktop        hr.zip     Public
[oracle@host02 ~]$
```

10. View the pcap file by using the **tcpdump -r** command. **Note:** The contents of your file may vary from what is shown in the code box.

```
[oracle@em12c ~]$ tcpdump -r network_traffic20140618193238.pcap
reading from file network_traffic20140715163214.pcap, link-type
EN10MB (Ethernet)
16:32:15.259241 STP 802.1d, Config, Flags [none], bridge-id
8000.fe:ff:ff:ff:ff:ff.8009, length 35
16:32:17.256100 STP 802.1d, Config, Flags [none], bridge-id
8000.fe:ff:ff:ff:ff:ff.8009, length 35
16:32:19.254286 STP 802.1d, Config, Flags [none], bridge-id
8000.fe:ff:ff:ff:ff:ff.8009, length 35
```

11. Close the terminal window.
12. Log out of the Database Firewall console or continue to the next practice.

# Practice 13-3: Viewing the Database Firewall Status Report

## Overview

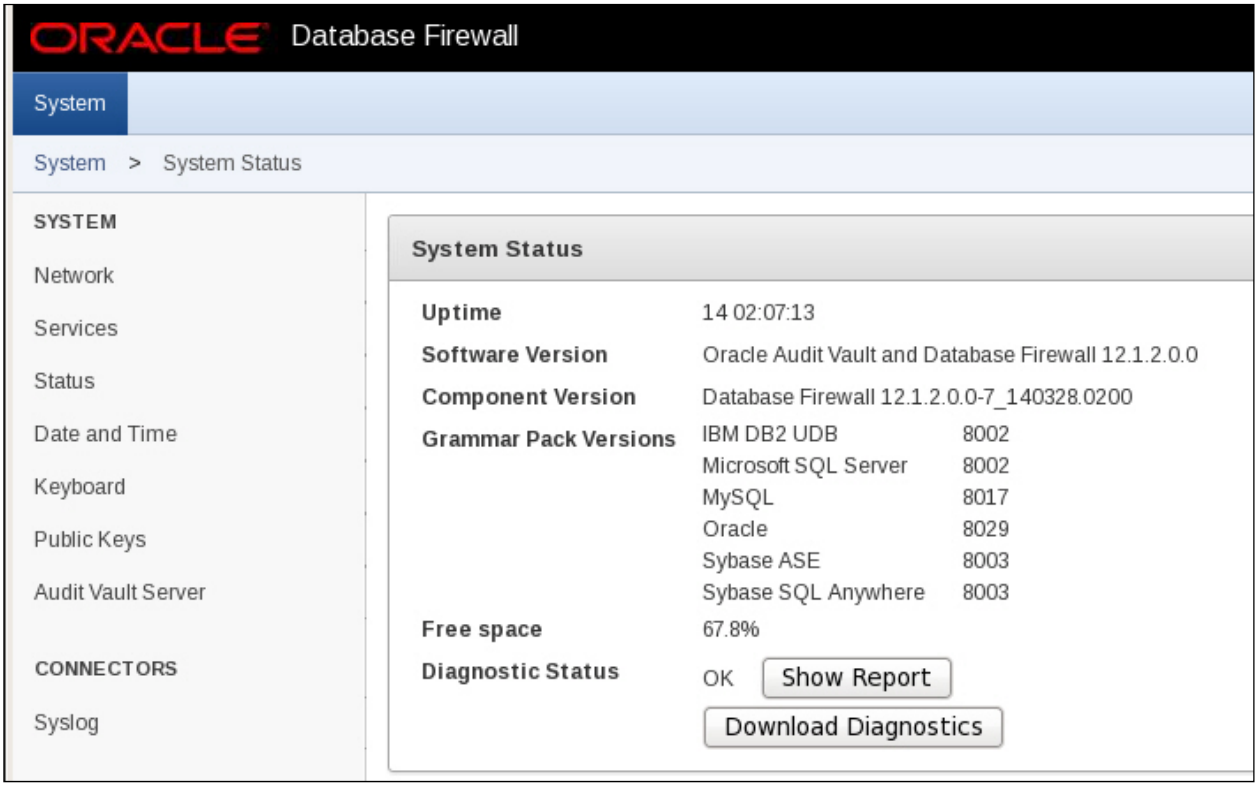
In this practice, you view the Database Firewall status report.

The Status page displays system status, component versions, and diagnostic status.

## Tasks

Perform the following steps to view the status report for a Database Firewall:

1. Log in to the Database Firewall administration console as the **`fwadmin`** user with a password of **`oracle_4U`**.
2. The Status page is displayed by default. You can also click Status in the System menu to access the System Status page.




3. Log out of the Database Firewall console or continue to the next practice.

# Practice 13-4: Viewing a Database Firewall Diagnostic Report

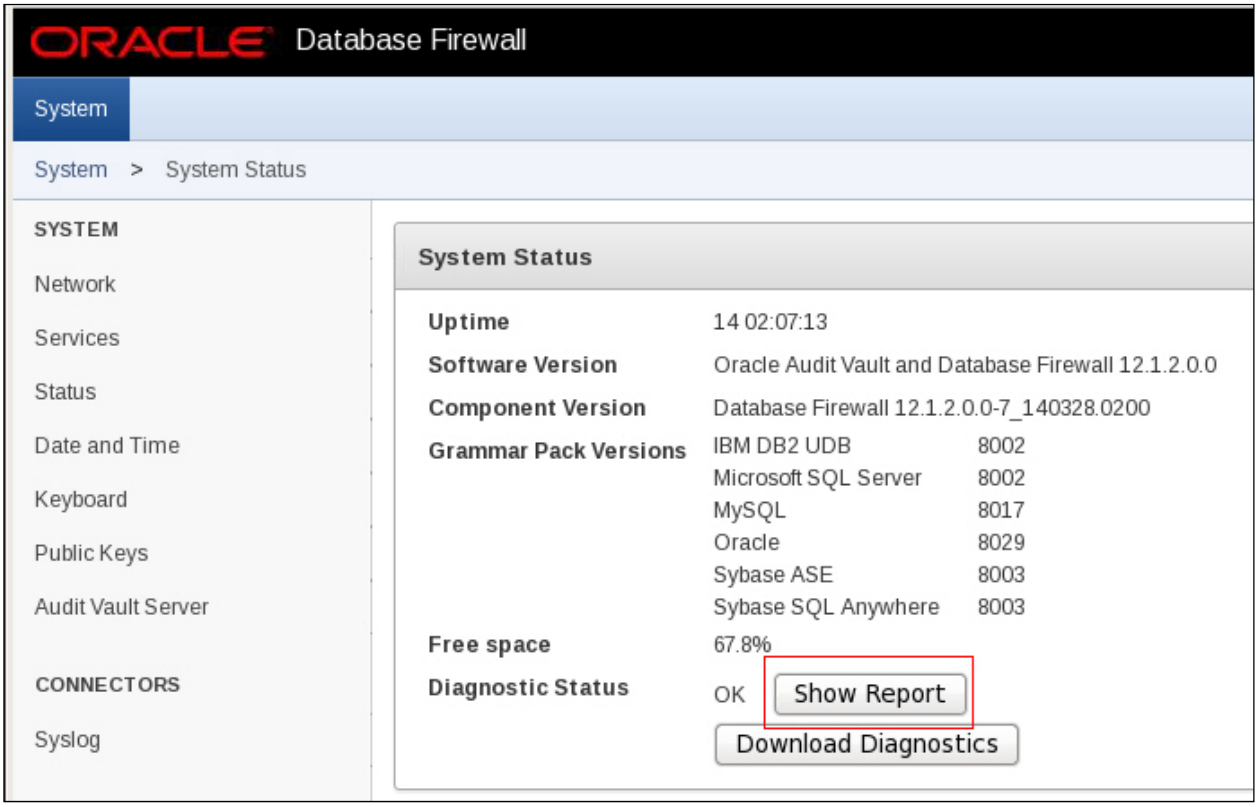
## Overview

In this practice, you view a Database Firewall diagnostic report.

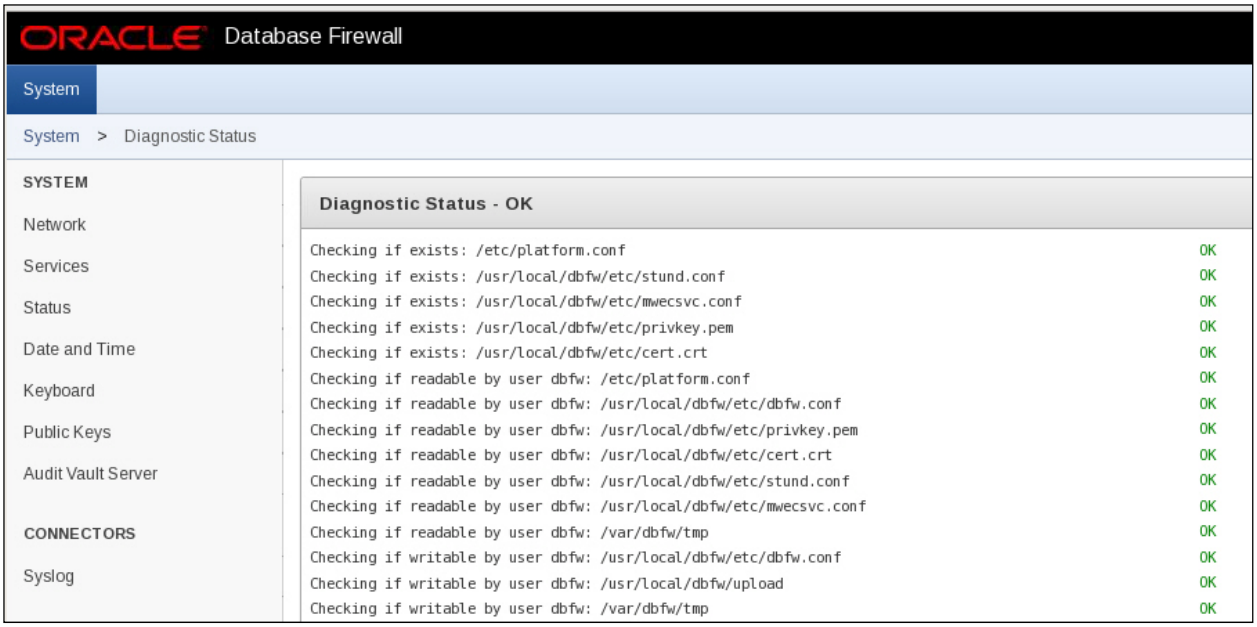
## Tasks

Perform the following steps to view the diagnostic report for a Database Firewall:

1. Log in to the Database Firewall administration console as the **`fwadmin`** user with a password of **`oracle_4U`**.
2. The Status page is displayed by default. You can also click Status in the System menu to access the System Status page.
3. To view a diagnostics report, click **Show Report** next to the Diagnostic Status field.




4. The diagnostics status report shows the status of various components. Scroll through the report to verify that the status of all components is OK.




5. Log out of the Database Firewall console.

# Practices for Lesson 14: Overview of the Auditing and Reporting Features

**Chapter 14**

# Practices for Lesson 14

## Practices Overview

In these practices, you will review the steps to create an audit policy and review built-in reports.

# Practice 14-1: Identifying Steps to Create an Audit Policy

## Overview

In this pen-and-paper practice, you identify steps to create an audit policy.

## Tasks

Identify the correct order of the following steps to enable you to create an audit policy for Oracle Database.

a. Provision the audit policy to the secured target database.
b. Define audit policy settings.
c. Retrieve current audit policy settings from the secured target Oracle database.
d. Specify which of the current settings are needed.

*Answer: c, d, b, a*

# Practice 14-2: Viewing the Auditor's Dashboard

## Overview

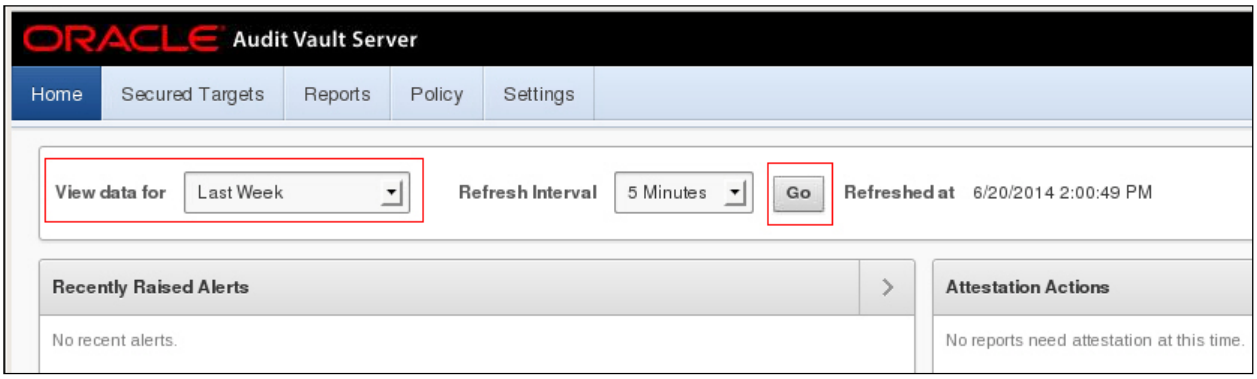
In this practice, you log in to the Audit Vault Server console as the auditor and view the auditor's dashboard.

When you log into Audit Vault Server console as an auditor or super auditor, you see the auditor's dashboard on the Home page, and the functions available for the auditor roles.

## Tasks

Perform the following steps to view the auditor's dashboard:

1. Log in to the Audit Vault Server console as an auditor:
   - Username: **`avauditor`**
   - Password: **`oracle_4U`**
2. Select a date range for viewing event data and then click **Go**.




3. View the graphical summaries (pie charts and bar graphs) of alert activity and event activity over the specified time period. Why is there no data?

   *Answer: In this course you have not configured any policies or alerts.*

# Practice 14-3: Determining Whether Built-in Reports Satisfy Requirements

## Overview

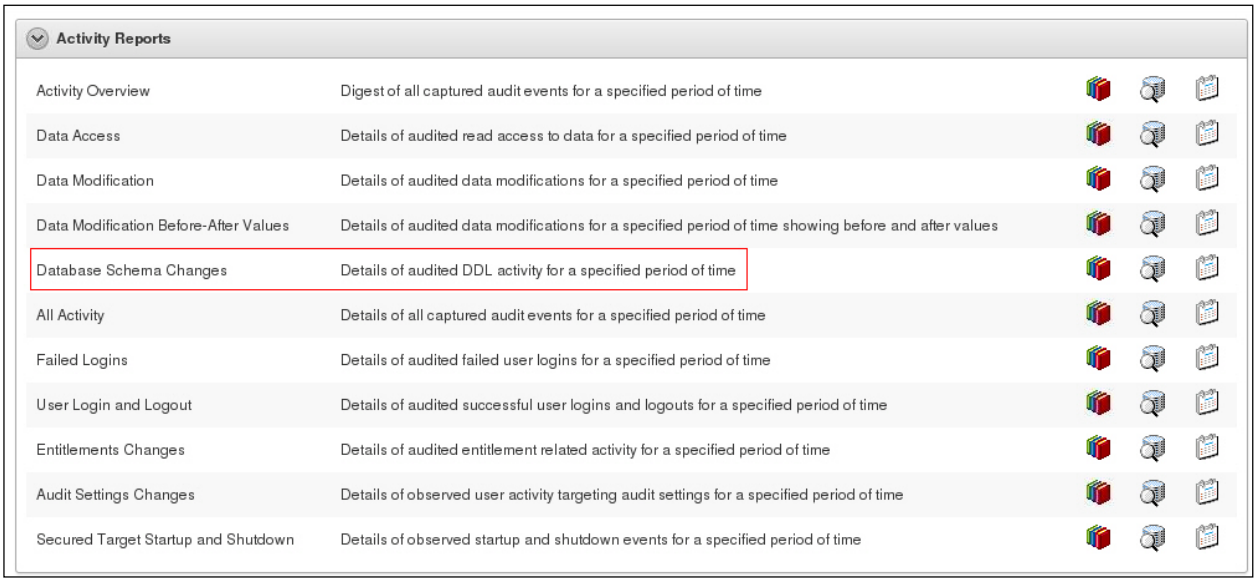
In this practice, you review a list of requirements and determine whether built-in reports are available to satisfy the requirements.

From the Built-in Reports section of the Reports tab, you can browse report data online, schedule reports, and link to previously scheduled and generated reports.

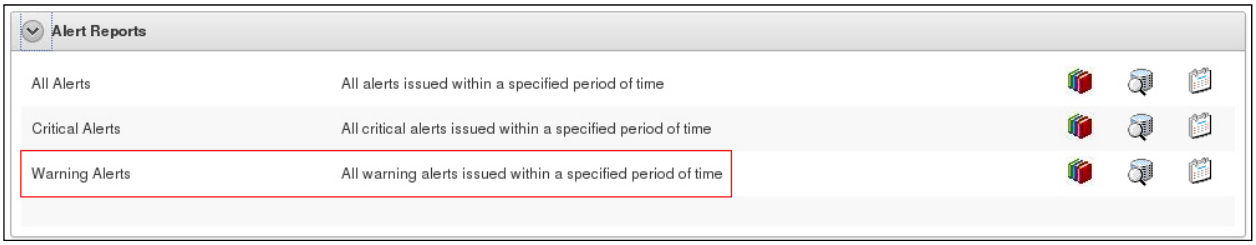
## Tasks

Review each of the following requirements and determine whether there is a built-in report that can be used to provide the needed information:

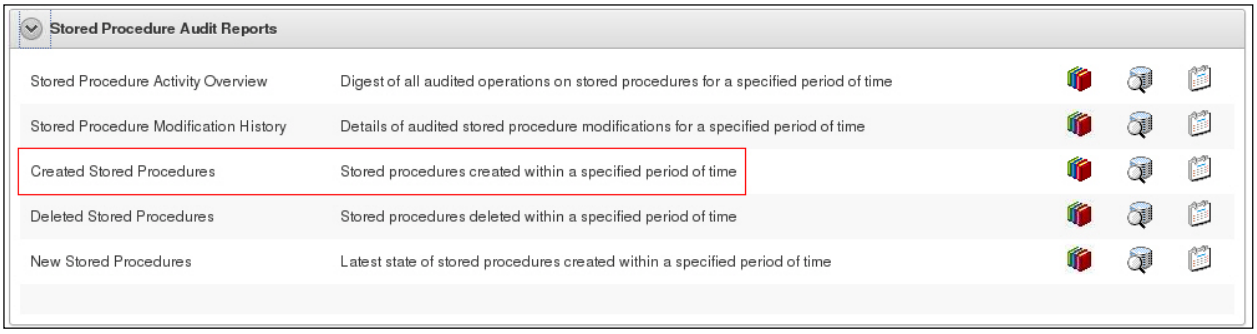
1. Audited DDL activity for the last week



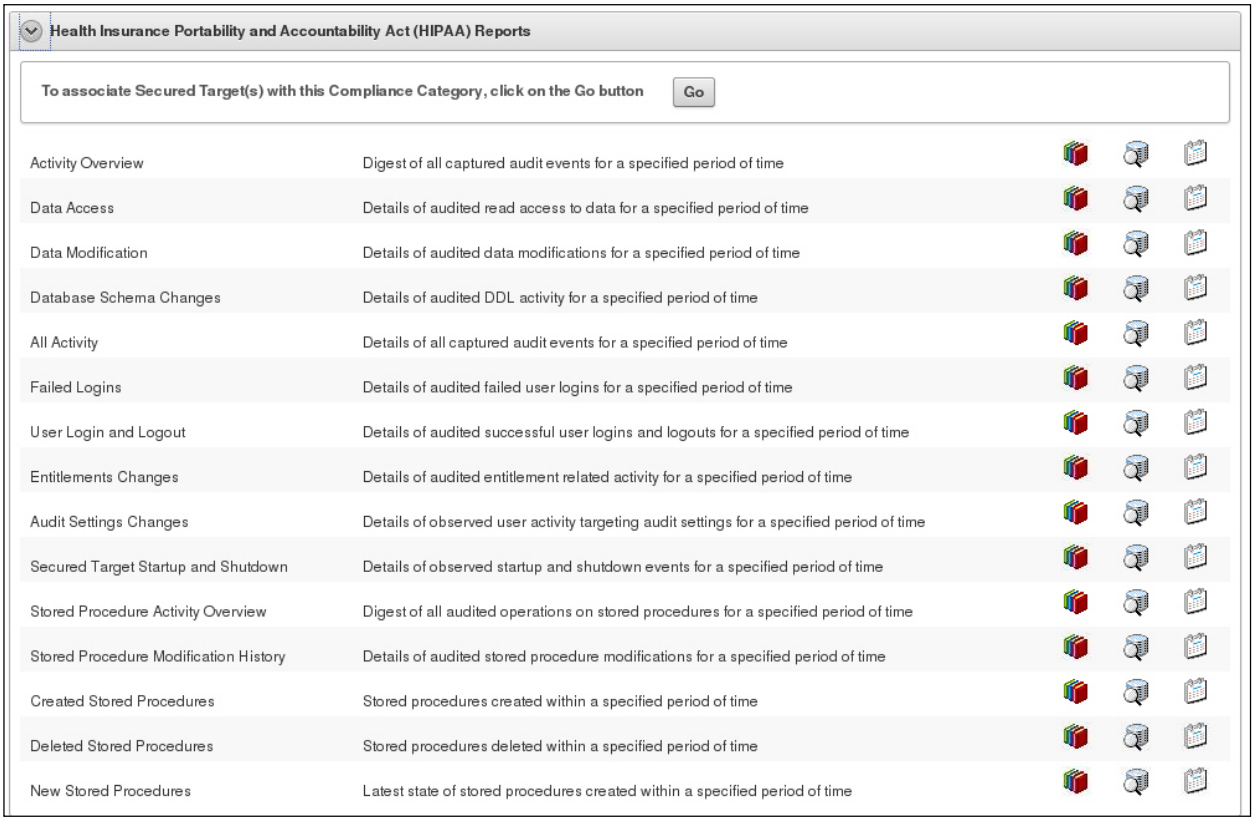

2. Warning alerts that have been issued within the last 24 hours




3. List of stored procedures that have been created within the last week




4. Reports that provide information needed comply with regulations related to health care data




5. Traffic for a specific IP address