Oracle® Enterprise Manager

System Monitoring Plug-in User's Guide for Audit Vault and Database Firewall

13c Release 4

F23677-03

August 2020

Oracle Enterprise Manager System Monitoring Plug-in User's Guide for Audit Vault and Database Firewall, 13c Release 4

F23677-03

Contents

4 Managing Oracle AVDF in Cloud Control

5 Administering the AVDF Plug-in

Preface

This document provides the installation, configuration, and management instructions for the Oracle Audit Vault and Database Firewall plug-in through Enterprise Manager Cloud Control 13*c*.

Audience

This document is intended for administrators and users of Oracle Audit Vault and Database Appliance.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information about Oracle Audit Vault and Database Firewall or Oracle Enterprise Manager Cloud Control, see the following documentation:

- Oracle Audit Vault and Database Firewall documentation:
  - *Oracle Audit Vault and Database Firewall Administrator's Guide*
  - *Oracle Audit Vault and Database Firewall Auditor's Guide*
  - *Oracle Audit Vault and Database Firewall Release Notes*
  - *Oracle Audit Vault and Database Firewall Concepts Guide*
  - *Oracle Audit Vault and Database Firewall Installation Guide*
  - *Oracle Audit Vault and Database Firewall Developer's Guide*
  - *Oracle Audit Vault and Database Firewall Licensing Information*
  - Oracle Audit Vault and Database Firewall product page:

    https://www.oracle.com/database/technologies/security/audit-vault-firewall.html

    Visit the Oracle Audit Vault and Database Firewall documentation library:

Oracle Audit Vault and Database Firewall 20.1 Library

- Oracle Enterprise Manager Cloud Control documentation:
  - *Oracle Enterprise Manager Cloud Control Administrator's Guide*

  Visit the Oracle Enterprise Manager Cloud Control documentation library:

  `Enterprise Manager Cloud Control Library`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Introduction to the Oracle AVDF Plug-in

The Oracle Audit Vault and Database Firewall (AVDF) plug-in provides an interface within Enterprise Manager Cloud Control for administrators to manage and monitor Audit Vault and Database Firewall components.

The following topics are discussed:

Versions Supported

The Oracle AVDF plug-in supports the following versions of products:

Table 1-1 lists supported versions of Oracle Enterprise Manager and Oracle Audit Vault Database Firewall.

Table 1-1 Support Matrix

Oracle Enterprise Manager Version	AVDF Release/Version
12.x	12.1.0.5
13.1.x	12.1.1
13.2 - 13.3	12.2.x
13.4	20.1

> **Note:**
>
> Oracle Audit Vault and Database Firewall (AVDF) plug-in is supported only with the above mentioned EM releases.

Prerequisites

The following prerequisites must be met before you can deploy the Management Agent:

- A user (such as, `AVAdmin`) on the Audit Vault (AV) Server that has Super Admin privileges (refer to the *Oracle Audit Vault and Database Firewall Administrator's Guide*).
- The password for the `root` user on the AV Server.
- The fully qualified names and IP addresses for each AVDF server.

- The password for the `support` user on the AVDF servers.
- There is no need for physical access to the servers. You will log in as the `support` user and run the `su` command to become the `root` user (and then later to become `oracle` user).
- Information about your Oracle Enterprise Manager Cloud Control instance:
  - OMS host name.
  - OMS port.

  This information can be obtained with the following command:

  ```
  emctl status oms -details -sysman_pwd <password>
  ```

Known Issues

While the AVDF plug-in automates many of the installation steps, the AVDF plug-in for the Windows environment has a known issue where installation of the AV agent must be completed manually.

2

Installing the Enterprise Manager Management Agent

This chapter provides the instructions for installing the Enterprise Manager (EM) Management Agent onto the Audit Vault Server and Database Firewall Appliance.

Follow the steps below to install the EM Management Agent:

- Manually Installing the Enterprise Manager Management Agent

Prerequisites to Installing Enterprise Manager Agent

There are multiple prerequisites that need to be done in the Audit Vault console before installing the Enterprise Manager agent.

Topics:

- Allow SSH Access to User `oracle`
- Configure User `oracle`
- Unlock `dbsnmp` and `asmsnmp` Accounts

Allow SSH Access to User `oracle`

- Audit Vault Server must use a fully qualified domain name. (E.g. test01.example.com). This is done through the network configuration screen.
- Enable all SSH connectivity. This is done through the services configuration screen.

1. Open a terminal window and edit the file: `/etc/ssh/sshd_config` to allow SSH access to user `oracle`.

   ```
   $ vi /etc/ssh/sshd_config
   ```

2. Append `oracle` to the AllowUsers line.

   ```
   AllowUsers support oracle
   ```

3. Restart sshd.

   ```
   $ service sshd restart
   ```

Configure User `oracle`

1. Create the agent home directory:

   ```
   $ mkdir $ORACLE_BASE/agent13c
   ```

2. Edit the `oraenv` command inside `.bashrc`:

   a. `$ vi $HOME/.bashrc`

b. Add a -s to `oraenv`.
```
./usr/local/bin/oraenv -s
```

Unlock `dbsnmp` and `asmsnmp` Accounts

1. Change user to `dvaccountmgr`:
```
$ su dvaccountmgr
```
2. Run the following command:
```
sqlplus /
alter user dbsnmp identified by <password> account unlock;
```
3. Change user to `grid`:
```
$ su grid
```
4. Run the following command:
```
orapwd file=/var/lib/oracle/grid/dbs/orapw+ASM password=<password>
sqlplus / as sysasm
alter user asmsnmp identified by <password> account unlock;
grant sysdba to asmsnmp;
```
Oracle recommends creating a Oracle Database user `asmsnmp` with `sysdba` privileges.

Installing the Enterprise Manager Agent With UI

Installing the Oracle Enterprise Manager Cloud Control 13c agent is done via a push method from the OEM console.

1. From the **Setup** dropdown select **Add Target**, then click **Add Target Manually**.
2. Click **Install Agent on Host**.
3. Click the **+ Add** button, fill in the **Host Name** and **Platform**.
4. Click **Next**.
5. Fill in the **Installation Base Directory** as `/var/lib/oracle/agent13c`.
6. Create a **Named Credential** for user `oracle`.
7. Leave the `root` credential blank.
8. Click **Deploy Agent**.

> **Note:**
>
> During the installation phase, you will get an error about sudo not being setup with visible password. Click **Continue All Hosts**.

9. Open a terminal window in the Audit Vault Server as `root` and run the following command:

```
$ ./var/lib/oracle/agent13c/<agent_version>/root.sh
```

Manually Installing the Enterprise Manager Management Agent

Follow the steps below to install the Enterprise Manager (EM) Management Agent manually:

1. Manually Installing the EM Management Agent on the Audit Vault Server
2. Manually Installing the EM Management Agent on the Database Firewall Appliance

Once installed, you will then install or configure the EM Management Agent on each server where an AVDF agent resides.

Manually Installing the EM Management Agent on the Audit Vault Server

Follow the steps below to set the host name, configure the DNS, and to download and install the EM Management Agent on the Audit Vault Server:

1. Log in to the Audit Vault Server console as a user with the `AV_ADMIN` role.
2. Set the hostname to a fully qualified hostname (for example, `location.mycompany.com`). On the Audit Vault server console, click **Settings**, then **Network** under the Systems group header. On the Network page, change the host name.
3. Configure the DNS on each appliance, which are to be monitored, to be the same as that on the OMS server. Click **Settings**, then **Services** under the System group header. On the Services page, configure the DNS, and change the host name.

   By default, SSH access into Audit Vault Server and Database Firewall is disabled. For the following steps, SSH is required. Therefore, on the same Services page, replace **disabled** inside the SSH box either with the **IP address** of the machine from which you will connect or with **all** to allow SSH connections from all machines on the network.
4. Log in to the operating system of the Audit Vault Server as the `root` user.
5. Unblock the network port through which the EM Management Agent and the Enterprise Manager server communicate:

> **Note:**
>
> Changes made here to the `template-iptables` file might be rolled back by a subsequent Oracle Audit Vault and Database Firewall patch or upgrade. If you notice after applying the next patch or upgrade that Enterprise Manager is no longer collecting information about AV Server correctly, then repeat steps 2a and 2b below.

a. Edit the file `/usr/local/dbfw/templates/template-iptables` file with the following entry:

> **Note:**
>
> By default, the permissions for this file is **read-only**. You must change the permissions to allow editing, edit the file, and then change the permissions back to **read-only**:
>
> i. As `root`, change the permissions of the `template-iptables` file:
>
> ```
> # chmod 644 template-iptables
> ```
>
> ii. Edit the line as described below.
>
> iii. Change the permissions of the `template-iptables` file back to read-only:
>
> ```
> # chmod 444 template-iptables
> ```

```
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW --dport 3872 -j ACCEPT
```

There may be similar entries already for database listener ports. Make your entry below them.

> **WARNING:**
>
> Take extreme care when modifying the `template-iptables` file. Any mistakes here could make the system inoperable.
>
> Only make this change and no other.

b. Run the following command as `root`:

```
# /usr/local/dbfw/bin/priv/configure-networking
```

c. Test your change. If port 3872 is used (this port is officially registered with IANA by Oracle for `oem-agent`), use:

```
iptables -L | grep oem
```

If another port was used, use:

```
iptables -L -n | grep <port number>
```

You will see that there is now an `ACCEPT` rule for the Management Agent.

6. While logged in as the `root` user on the Audit Vault Server, run the following command to become the `oracle` user:

```
# su - oracle
```

7. Download the `AgentPull.sh` script as follows:

```
$ cd /tmp
$ curl "https://<OMS_HOST>:<OMS_PORT>/em/install/getAgentImage" -k -o
AgentPull.sh
```

8. Give execute permission to the `AgentPull.sh` script:

   ```
   $ chmod +x AgentPull.sh
   ```

9. Create a response `agent.rsp` file:

   ```
   LOGIN_USER=sysman
   PLATFORM="Linux x86-64"
   ```

10. Run the `AgentPull.sh` script to download and install the Management Agent:

    ```
    $ ./AgentPull.sh RSPFILE_LOC=/tmp/agent.rsp AGENT_BASE_DIR=/var/lib/oracle/
    emagent ORACLE_HOSTNAME=location.mycompany.com AGENT_PORT=3872
    ```

    Where `ORACLE_HOSTNAME` is the fully qualified hostname of the Audit Vault Server where the EM Management Agent is being installed.

    > **Note:**
    >
    > You will be prompted for two passwords immediately upon executing this command.

    The installation of the EM Management Agent starts automatically as soon as the download has finished. At the end of the installation, you will be prompted to run a script as `root`.

    After running that script, continue with Discovering the Oracle AVDF Target .

Manually Installing the EM Management Agent on the Database Firewall Appliance

Follow the steps below to set the host name, configure the DNS, and to download and install the EM Management Agent on the Database Firewall appliance:

1. Log in to Database Firewall appliance console as a user with Firewall Admin privileges.
2. Set the hostname to a fully qualified hostname (for example, `location.mycompany.com`). On the Database Firewall console, click **Network** under the **System** header, and then click the **Change** button on the lower right-hand corner of the page.
3. Configure the DNS to be the same as that on the OMS server. Click **System** and then **Services**. On the Services page, configure the DNS.

   By default, SSH access into Database Firewall is disabled. For the following steps, SSH is required. Therefore, on the same Services page, replace **disabled** inside the SSH box either with the **IP address** of the machine from which you will connect or with **all** to allow SSH connections from all machines on the network.
4. Log in to the operating system of the Database Firewall appliance as the `root` user.
5. Unblock the network port through which the EM Management Agent and the Enterprise Manager server communicate:

> **Note:**
>
> Changes made here to the `template-iptables` file might be rolled back by a subsequent Oracle Audit Vault and Database Firewall patch or upgrade. If you notice after applying the next patch or upgrade that Enterprise Manager is no longer collecting information about Database Firewall correctly, then repeat steps 2a and 2b below.

a. Edit the file `/usr/local/dbfw/templates/template-iptables` file with the following entry:

> **Note:**
>
> By default, the permissions for this file is **read-only**. You must change the permissions to allow editing, edit the file, and then change the permissions back to **read-only**:
>
> i. As `root`, change the permissions of the `template-iptables` file:
>
> ```
> # chmod 640 template-iptables
> ```
>
> ii. Edit the line as described below.
>
> iii. Change the permissions of the `template-iptables` file back to read-only:
>
> ```
> # chmod 440 template-iptables
> ```

```
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW --dport 3872 -j ACCEPT
```

There may be similar entries already for database listener ports. Make your entry below them.

> **WARNING:**
>
> Take extreme care when modifying the `template-iptables` file. Any mistakes here could make the system inoperable.
>
> Only make this change and no other.

b. Run the following command:

```
# /usr/local/dbfw/bin/priv/configure-networking
```

c. Test your change. If port 3872 is used (this port is officially registered with IANA by Oracle for `oem-agent`), use:

```
iptables -L | grep oem
```

If another port was used, use:

```
iptables -L -n | grep <port number>
```

You will see that there is now an `ACCEPT` rule for the Management Agent.

6. While logged in as the `root` user on the Audit Vault Server, run the following command to become the `oracle` user:

   ```
   # su - oracle
   ```

7. Download the `AgentPull.sh` script as follows:

   ```
   $ cd /tmp
   $ curl "https://<OMS_HOST>:<OMS_PORT>/em/install/getAgentImage" -k -o
   AgentPull.sh
   ```

8. Give execute permission to the `AgentPull.sh` script:

   ```
   $ chmod +x AgentPull.sh
   ```

9. Create a response `agent.rsp` file:

   ```
   LOGIN_USER=sysman
   PLATFORM="Linux x86-64"
   ```

10. Run the `AgentPull.sh` script to download and install the Management Agent:

    ```
    $ ./AgentPull.sh RSPFILE_LOC=/tmp/agent.rsp AGENT_BASE_DIR=/var/lib/oracle/
    emagent ORACLE_HOSTNAME=location.mycompany.com AGENT_PORT=3872
    ```

    Where `ORACLE_HOSTNAME` is the fully qualified hostname of the Database Firewall where the EM Management Agent is being installed.

    > **Note:**
    >
    > You will be prompted for two passwords immediately upon executing this command.

    The installation of the EM Management Agent starts automatically as soon as the download has finished. At the end of the installation, you will be prompted to run a script as `root`.

    After running that script, continue with Discovering the Oracle AVDF Target .

3
Discovering the Oracle AVDF Target

Before you can begin monitoring Oracle Audit Vault and Database Firewall, it must first be *discovered* by Oracle Enterprise Manager Cloud Control. This chapter describes the necessary steps for discovering the Oracle AVDF target:

1. Deploy the Oracle AVDF Plug-in
2. Discover Targets
    a. Discover Audit Vault Server Target
    b. Discover Database Firewall Target
    c. Discover Audit Vault Agent Target

Deploy the Oracle AVDF Plug-in

You can deploy plug-ins to an OMS instance using the Enterprise Manager Cloud Control interface or the EM Command Line Interface (EMCLI). While the graphical interface mode enables you to deploy one plug-in at a time, the command line interface mode enables you to deploy multiple plug-ins at a time, thus saving plug-in deployment time and downtime, if applicable.

The *Managing Plug-ins* chapter in the *Oracle Enterprise Manager Cloud Control Administrators Guide* provides instructions for deploying the plug-in.

Complete the following sections to deploy the AVDF plug-in on:

- Your Management Server (performed within Enterprise Manager Cloud Control). See the “Deploying Plug-Ins to Oracle Management Service” section for details:
- Your Management Agent (AV Server, performed within Enterprise Manager Cloud Control). See the “Deploying Plug-ins to Oracle Management Agent” section for details.

Once completed, return and continue with the instructions outlined in Discover Targets.

Discover Targets

After successfully installing the Management Agent and deploying the plug-in, follow the steps below to add the following targets to Enterprise Manager Cloud Control for central monitoring and management:

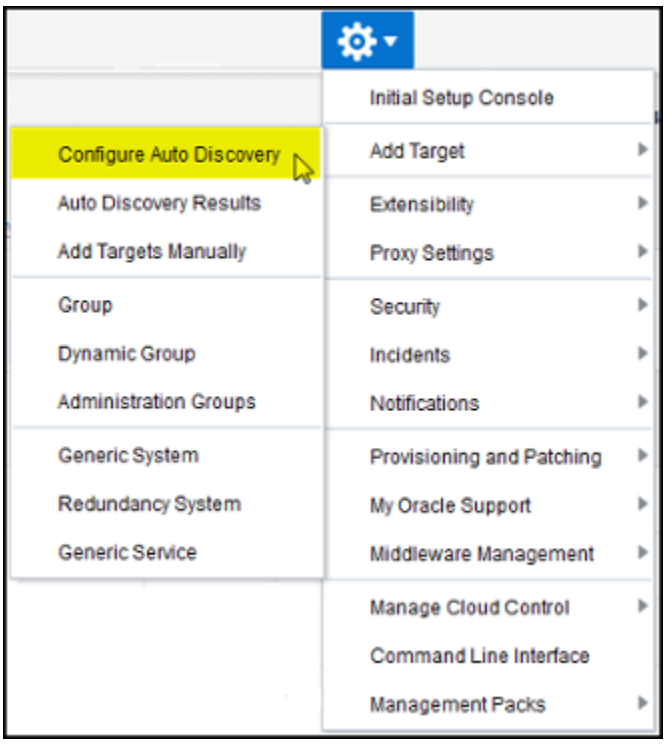
- Discover Audit Vault Server Target
- Discover Database Firewall Target
- Discover Audit Vault Agent Target

Discover Audit Vault Server Target

Follow the steps below to add the Oracle Audit Vault Server target:

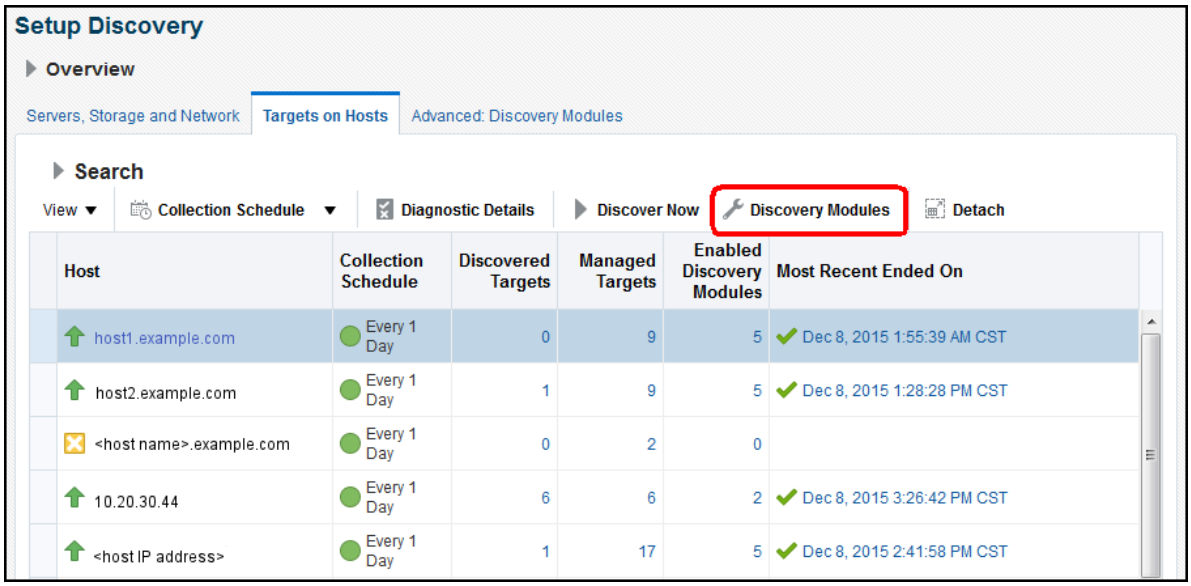
1. Log in to Enterprise Manager Cloud Control.
2. Click **Setup**, then **Add Target**, and finally **Configure Auto Discovery**, as shown in Figure 3-1:

Figure 3-1 Configure Auto Discovery Menu



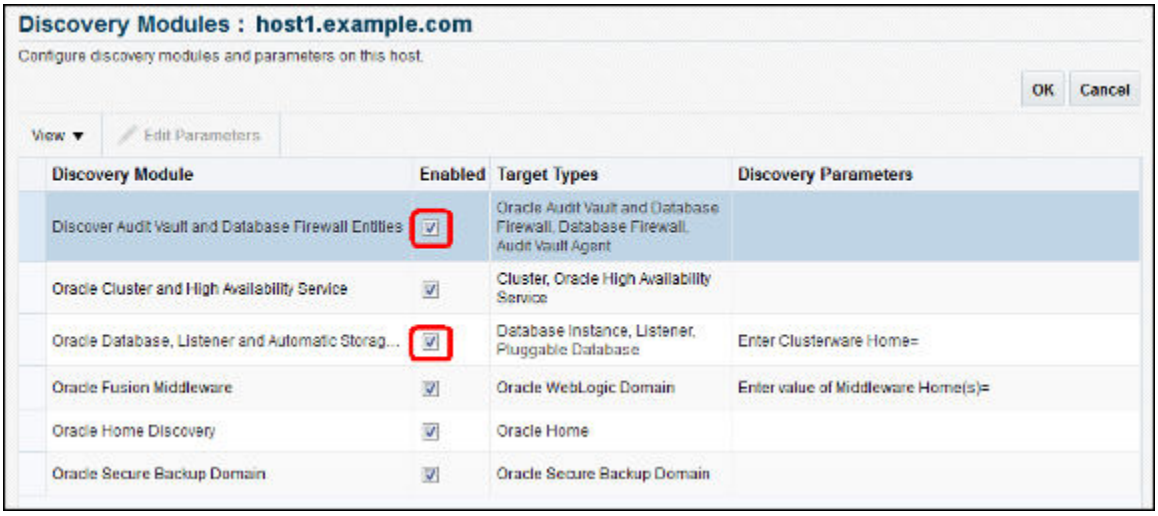
3. On the Setup Discovery page, select a host on the Targets on Hosts tab and click **Discovery Modules**, as shown in Figure 3-2:

Figure 3-2 Setup Discovery



4. On the Discovery Modules page, confirm that **Discover Audit Vault and Database Firewall Entities** and the **Oracle Database, Listener and Automatic Storage Management** options are enabled, as shown in Figure 3-3:

Figure 3-3 Discovery Modules



Click **OK**.

5. Returning to the previous page, highlight the hostname of the Oracle Audit Vault Server and click **Discover Now**. A pop-up window will appear while the discovery is in progress.
6. Rename the Audit Vault Server and Database Firewall instances:
   a. Click **Setup**, then **Add Target**, and finally **Auto Discovery Results**.
   b. Click the **Targets on Hosts** tab.
   c. In the Target Type column, look for *Oracle Audit Vault and Database Firewall*, this is your Audit Vault Server. Highlight the row and click **Rename** to rename it to any meaningful name, such as `AVServer_Legal_and_HR`.
   d. Next, highlight the row with Database Instance as a target type. Click **Rename** to rename it to any meaningful name, such as `AVS_Repository`.
7. Promote the Audit Vault Server (AV Server):
   a. Highlight the row of the Audit Vault Server and click **Promote**.
   b. On the next page, provide user name and password of the AV Server user with `AV_ADMIN` privilege. The Preferred Connect String should be populated already. However, if it is not, go to the AV Server Web administration console and log in as a user with the `AV_ADMIN` privilege. Click **Settings**, then **Status**, and copy the preferred connect string from there. The `ORACLE_HOME` is:

      ```
      /var/lib/oracle/dbfw
      ```

   c. Click **Promote**.
8. Promote AV Repository Database instance:
   a. Highlight the row with the `AVS_Repository` database instance. Click on **Promote**.

b. On the next page, check `AVS_Repository` and click **Configure**.

c. Enter the Monitor password (user is `dbsnmp`, unlock the account in the AVS repository database), change the port from 1522 to **1521**, and change the Listener Machine Name to the **fully qualified hostname** of your AV Server.

d. Click **Test Connection**; when successful, click **Save**.

9. Back on the previous page, click **Next**. On the following page, click **Save**.

10. To navigate to your new AV Server home page in Enterprise Manager Cloud Control:

a. From the Targets menu, select **All Targets**.

b. Expand the **Others** list item.

c. Select **Oracle Audit Vault and Database Firewall**. The AV repository database is listed under **Targets**, **Databases**.

Discover Database Firewall Target

Follow the steps below to add the Oracle Database Firewall target:

1. Log in to Enterprise Manager Cloud Control.

2. Click **Setup**, then select **Add Target**, and finally **Configure Auto Discovery**.

3. On the Setup Discovery page, select a host on the Targets on Hosts tab and click **Discovery Modules**, as shown in Figure 3-2.

4. On the Discovery Modules page, confirm that **Discover Audit Vault and Database Firewall Entities** and the **Oracle Database, Listener and Automatic Storage Management** options are enabled.

5. On the Discovery Modules page, confirm that **Discover Audit Vault and Database Firewall Entities** and the **Oracle Database, Listener and Automatic Storage Management** options are enabled.

   Click **OK**.

6. Returning to the previous page, highlight the hostname of the Oracle Database Firewall Server and click **Discover Now**. A pop-up window will appear while the discovery is in progress.

7. Rename the Audit Vault Server and Database Firewall instances:

a. Click **Setup**, then **Add Target**, and finally **Auto Discovery Results**.

b. In the Target Type column, look for *Database Firewall*, this is your Database Firewall Server. Highlight the row and click **Rename** to rename it to any meaningful name, such as `DBFW_Legal_and_HR`.

c. Next, highlight the row with Database Instance as a target type. Click **Rename** to rename it to any meaningful name, such as `DBFW_Repository`.

8. Promote the Database Firewall Server (DBFW Server):

a. Highlight the row of the DBFW Server and click **Promote**.

b. On the next page, provide user name and password of the AV Server user with `AV_ADMIN` privilege. The Preferred Connect String should be populated already. However, if it is not, go to the AV Server Web administration console and log in as a user with the `AV_ADMIN` privilege. Click **Settings**, then **Status**,

and copy the preferred connect string from there. Replace the IP address with the hostname of the AV Server; confirm ports are set to **1521**.

> **Note:**
>
> The DBFW Server is managed through the AV Server. When promoting the DBFW Server, you will still provide all the credentials for the AV Server.

c. Click **Promote**. After clicking Promote, the console will ask for credentials again. Use the `av_admin` privilege credential of the AVDF Server.

> **Note:**
>
> There is no need to promote the Database Firewall Repository instance.

9. Back on the previous page, click **Next**. On the following page, click **Save**.
10. To navigate to your new AV Server home page in Enterprise Manager Cloud Control:
    a. From the Targets menu, select **All Targets**.
    b. Expand the **Others** list item.
    c. Select **Database Firewall**. The DBFW repository database is listed under **Targets**, **Databases**.

Discover Audit Vault Agent Target

Discovery of the Audit Vault (AV) Agent also can be done using automated discovery. Similar to other AVDF targets, you can run discovery on the host where the AV Agent is installed. The discovery script identifies the AV Agent and includes it with the discovered targets, which could be promoted by providing the Oracle home of the AV Agent and AVDF server `AV_Admin` credential.

> **Note:**
>
> In order to manage an Audit Vault agent with Enterprise Manager Cloud Control, a Management Agent needs to be present on the machine where the Audit Vault agent is about to be deployed.

Follow the steps below to add the Oracle Audit Vault agent target:

1. Log in to Enterprise Manager Cloud Control.
2. Click **Setup**, then **Add Target**, and finally **Add Targets Manually**.
3. Select **Add Targets Declaratively by Specifying Target Monitoring Properties**.

4. From the Target type drop-down select the **Audit Vault Agent** target type. Then, for the Monitoring Agent, select the Enterprise Manager agent installed on the host on which the AV Agent is installed.

   For example, if the AV Agent is installed on `host1.mycompany.com`, then you would need to search for the Enterprise Manager Agent (Monitoring Agent) on `host1.mycompany.com`. To search for the Monitoring Agent, click on the search icon to open a pop-up window with all the Enterprise Manager agents associated with this instance of Enterprise Manager.

5. Click **Add Manually**.

6. Follow the prompts for the Add Targets wizard to complete the process, including the following property settings:

   - AV Agent Name - The host agent name as it appears in AVDF console.
   - AV Agent Home - The location where the AV Agent is installed.
   - AVDF Monitor UserName - The user with the Super Administrator role on the AVDF repository.
   - AVDF Monitor Password.
   - AVDF Server Connect String.
     - For a single AVDF server setup, it should look like this:

       ```
       (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<host IP>)(PORT=1521))
       (CONNECT_DATA=(SERVICE_NAME=DBFWDB.DBFWDB)))
       ```

     - For a High Availability configuration of AVDF servers, the AVDF Connect string should look like this:

       ```
       (DESCRIPTION=(ENABLE=BROKEN)(FAILOVER=on)(RETRY_COUNT=3)
       (ADDRESS_LIST=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCP)(HOST=<primary
       host ip>)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=DBFWDB.DBFWDB))
       (ADDRESS_LIST=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCP)
       (HOST=<secondary host ip>)(PORT=1521)))
       (CONNECT_DATA=(SERVICE_NAME=DBFWDB.DBFWDB)))
       ```

   - Associated Oracle AVDF Target - Optional. Name of the Enterprise Manager target of the corresponding AVDF.

4

Managing Oracle AVDF in Cloud Control

This chapter describes the various regions displayed on the Audit Vault and Database Firewall (AVDF) plug-in home page and includes the monitoring capabilities. The following topics are provided:

Install and Monitor the AV Agent

As part of the set up of Enterprise Manager Cloud Control 12*c*, most hosts and targets are already discovered by Enterprise Manager. As part of Enterprise Manager, you can use this setup to install Audit Vault Agents and Sources:

To install an Audit Vault Agent:

1. On the Audit Vault listing page, click **Install**.

   A new page will display which has a hosts table and an Add/Remove button. Initially, the host table is blank.

2. Click **Add** to bring up a pop-up window to search and add hosts for which the installation should happen. The pop-up window should only show those hosts where the AVDF plug-in is installed ***and*** where the host does not yet have the AV Agent installed.

3. Enterprise Manager will auto compute the AV Agent installation directory based on the Enterprise Manager Agent installation directory. You will have an option to change the directory.

4. Select the hosts you want to install the AV Agent. For those hosts you select, Enterprise Manager will show:
   - Host name, operating system, and platform details.
   - Agent installation directory.
   - A text box for the credential name. Click on the button next to the text box to view a pop-up window which displays all the credentials stored in Enterprise Manager. Select the credential name which is applicable for the host. If none of those credentials are for the particular host, then click on the new credential and provide the new credential information. This information will be saved for future reference.

     You can either chose credentials for each host individually or click the default host credential and provide one credential applicable on all hosts.

     > **Note:**
     >
     > If you choose the default host credential and still provide a credential for some other host in the host details table, then the credential provided in the column will override the default credential.

5. Click Submit to initiate the job (one per host) for the AV Agent setup.

   After the job is submitted, the AV listing page is displayed.

6. To monitor the progress, click the refresh button to see the new AV Agents added to the system.

   For any jobs that fail, use the EM Jobs page to diagnose the failure. As part of the job execution, Enterprise Manager will log any relevant information to aid the AV Administrator for diagnosing the issue.

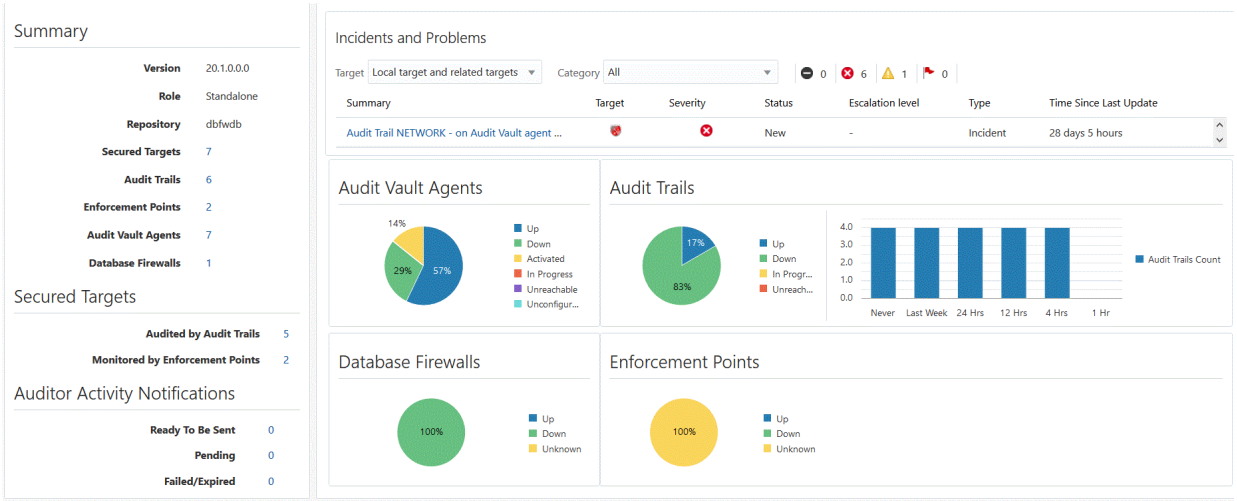
Once you have successfully installed an Audit Vault Agent on a host, Oracle recommends refreshing the latest configuration before adding a Target belonging to that host. To refresh the configuration page, follow these steps:

1. From the Oracle Audit Vault and Database Firewall main menu, select **Configuration**, then click **Latest**.
2. In the latest configuration page, click **Refresh**.

The AVDF Plug-in Home Page

Once installed and configured, you can monitor Oracle Audit Vault and Database Firewall from Enterprise Manager Cloud Control, as shown in Figure 4-1. Each section and region of this page is described in Primary AVDF Plug-in Monitoring Overview.

Figure 4-1 Oracle AVDF Plug-in Home Page in Cloud Control



> **Note:**
>
> AVDF Plug-in pages require metrics to be enabled in order to work correctly.

Primary AVDF Plug-in Monitoring Overview

The regions described below provide high-level information about the status or performance of the Audit Vault Server and Database Firewall Appliance.

From the Oracle Audit Vault and Database Firewall plug-in home page, you can monitor the following information:

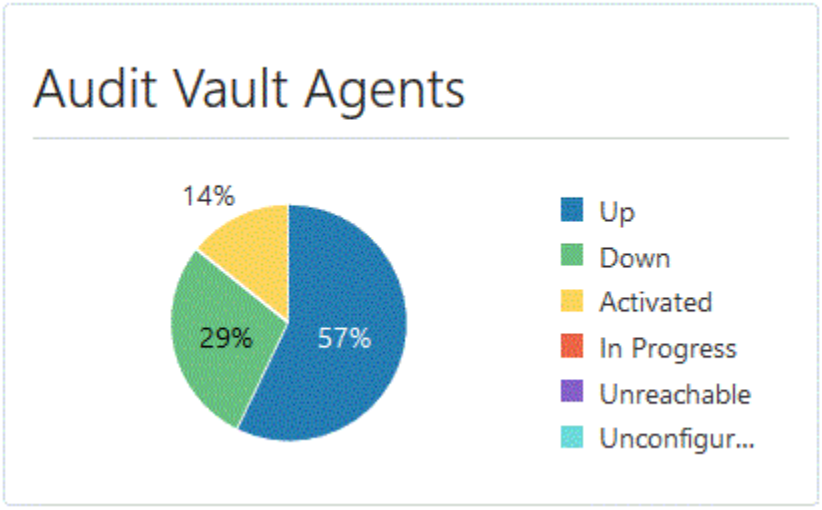
- Audit Vault Agents
- Audit Trails
- Database Firewalls
- Monitoring Points
- Targets

Audit Vault Agents

This region shows the status information and configuration issues of all Audit Vault Agents monitored by Audit Vault and Database Firewall, not only monitored by Enterprise Manager as an Enterprise Manager target. It also shows the information about the Audit Vault Agents not monitored by Enterprise Manager as an Enterprise Manager target.

A graph shows if the agent is down, in progress, unreachable, or up. (See Figure 4-2.)

Figure 4-2 Audit Vault Agents Region



For a detailed report (Audit Vault Agents List), select **Audit Vault Agents** from the Oracle Audit Vault and Database Firewall menu or click the **Audit Vault Agents** title found in the Summary region on the AVDF Oracle Home Page.

Audit Vault Agents List

This page lists all of the Audit Vault Agents monitored by Audit Vault and Database Firewall. The following information is available:

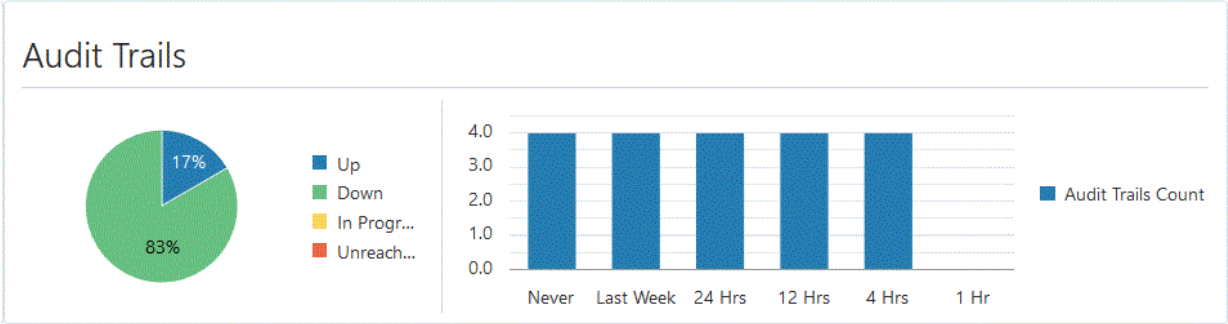
- Host Name: The host on which the Audit Vault Agent is installed.
- Version: The version of the Audit Vault Agent.
- Generation Time: Time at which the Audit Vault Agent was added into the Audit Vault server.
- Status: Identifies if the agent is Up, Down, Unreachable, Not Activated, etc.
- Audit Vault Agent Location: The path on the host where the Audit Vault Agent is installed.
- Activation Time: Time at which the Audit Vault Agent was activated in the Audit Vault server.
- Audit Trails: A separate summary count of Audit Trail status shown like how many Audit Trails are in UP status and DOWN status.
- Incidents: The number of incidents logged against a particular agent (it may or may not be monitored by Enterprise Manager Cloud Control) and all the audit trails managed by it. Incidents have a state of Fatal, Critical, Warning, and Escalated.

You can **Install, Activate, Deactivate, Start, Stop,** or **Delete** any of the Audit Vault Agents listed in this page by selecting the agent and clicking on the required button.

Audit Trails

Like Audit Vault Agents region, the Audit Trails region (Figure 4-3) shows status information for all the audit trails in the Audit Vault and Database Firewall system. It shows since how long the data upload issues exist.

Figure 4-3 Audit Trails Region



For a detailed report (Audit Trails List), select **Audit Trails** from the Oracle Audit Vault and Database Firewall menu or select the **Audit Trails** title found under Summary region from the Oracle AVDF Home Page.

Audit Trails List

This page lists all of the audit trails monitored by the Audit Vault and Database Firewall plug-in. The following information is available:

- Location
- Secured Target
- Status: identifies if the secured target is Up, Down, Idle, Unreachable, Not Activated, etc.
- Audit Vault Agent: lists the host name of the Audit Vault Agent. Click the link to display that agent's home page summary.
- Type
- Time Since Last Upload: The elapsed time since the last upload. This represents the time since when the audit trails has not uploaded any audit data into Audit Vault and Database Firewall repository.
- Throughput: shows the number of queries audited per second.
- Incidents: Identifies the number of incidents logged against an audit trail. Incidents have a state of Critical, Warning, and Escalated.

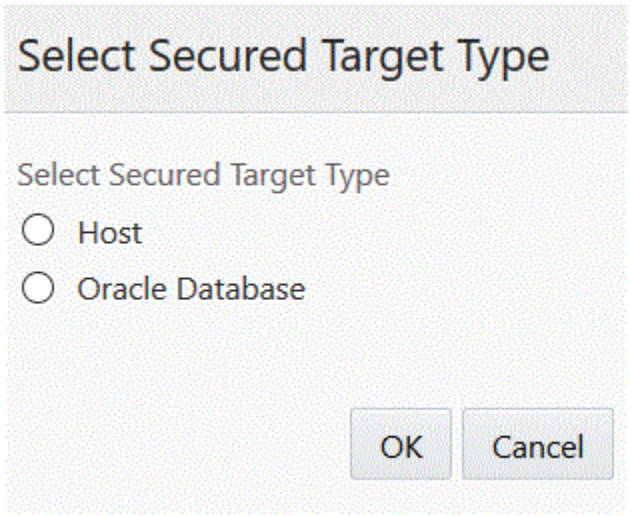
You can **Add, Stop, Start,** or **Delete** any of the audit trails listed in this page by selecting the trail and clicking on the required button.

Adding an Audit Trial

Follow the steps below to add an audit trail.

1. From the Oracle Audit Vault and Database Firewall home page, click the home page menu and select **Audit Trails**.
2. On the Audit Trails page, click **Add**.
3. On the pop-up window, select either **Host Operating System** or **Oracle Database.**

Figure 4-4 Select Secured Target Type



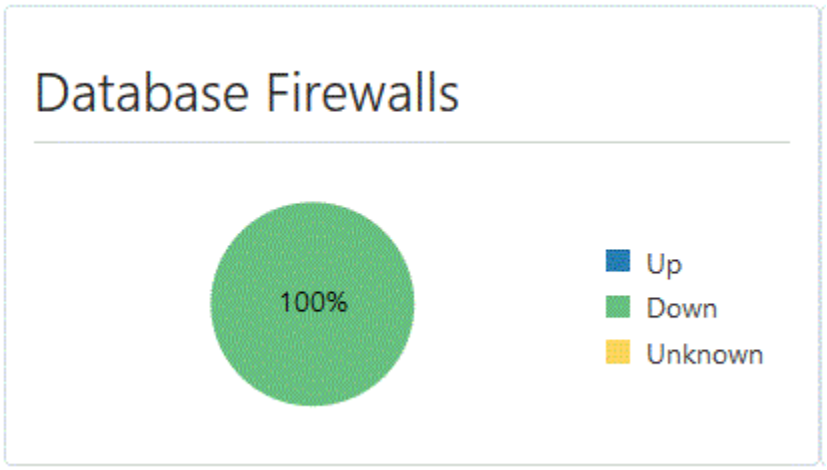
Click **OK**.

4. On the Search and Select Secured Targets page, select the target(s) and click **OK**.
5. For Oracle Database Secured Target, click the Configure Trail icon and select the trail types that you want to enable the trail for, else enter the trail location for the host secured target.
6. Click **Submit.**
7. Enter the credentials in the Credentials pop-up window and click **OK.**

Database Firewalls

Like the Audit Vault Agents region, the Database Firewalls region (Figure 4-5) shows all of the firewalls in the Audit Vault and Database Firewall system, not only the one monitored by Enterprise Manager as an Enterprise Manager target. This section also shows the count of Database Firewalls not monitored by Enterprise Manager as an Enterprise Manager target.

Figure 4-5 Database Firewalls Region



For a detailed report (Database Firewalls List), select **Database Firewalls** from the Oracle Audit Vault and Database Firewall menu or click on the **Database Firewalls** title found under Summary region from the Oracle Audit Vault Home Page.

Database Firewalls List

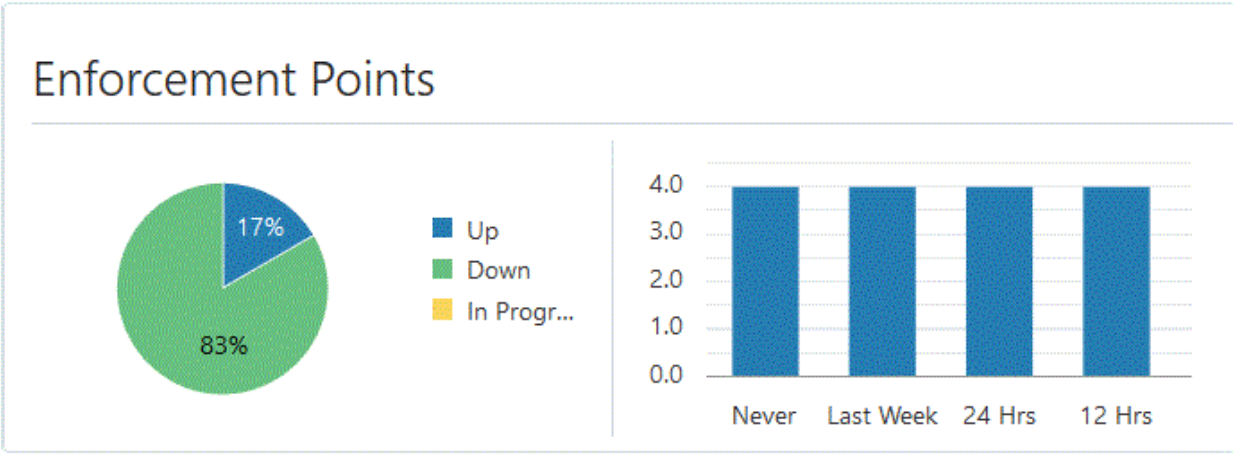
This page lists all of the Database Firewalls monitored by the Audit Vault and Database Firewall plug-in. The following information is available:

- Firewall: The Database Firewall name for all Database Firewalls in the Audit Vault and Database Firewall system - whether they are monitored by Enterprise Manager or not. Click the link for a detailed #unique_53 for the selected Database Firewall.
- Status: Identifies if the firewall is Up, Down, Idle, Unreachable, Not Activated, etc.
- Firewall Host: Depending on the information available, this field displays:
  - The host name when available. The IP address of the Database Firewall host is shown as a tooltip of the host name.
  - The IP address of the Database Firewall host.
- Role: This field shows whether the firewall has **primary** or **secondary** role in a High Availability (HA) configuration. If the Database Firewall is not HA configured, then this would be standalone.
- High Availability Pair: This field shows the name of the other firewall which is paired and its role in High Availability configuration.
- Enforcement Points: It shows the status count summary of Enforcement points including UP, DOWN, and UNREACHABLE state.
- Incidents: Identifies the number of incidents logged against a particular Database Firewall, whether monitored by Enterprise Manager Cloud Control or not. Incidents have a state of Critical, Warning, and Escalated.

Monitoring Points

This region (Figure 4-6) shows a high-level status of the monitoring points in the Audit Vault and Database Firewall system data. A timestamp shows since how long enforcement points have not scanned any queries (from the last hour to the last week).

Figure 4-6 Monitoring Points Region



For a detailed report (Monitoring Points List), select **Monitoring Points** from the Oracle Audit Vault and Database Firewall menu.

Monitoring Points List

This page lists all of the monitoring points monitored by the Audit Vault and Database Firewall plug-in. The following information is available:

- Monitoring Point: the name of the monitoring point for a particular Database Firewall. Click the link for a detailed #unique_55 of the monitoring point.
- Status: identifies if the monitoring point is Up, Down, Idle, Unreachable, Not Activated, etc.
- Monitoring Mode:
  - Database Activity Monitoring (DAM): monitors the activity of the database.
  - Database Policy Monitoring Mode (DPM): blocks activity if a policy violation occurs.
- Firewalls: lists the Database Firewalls associated with a particular monitoring point.
- Target: identifies the name of the target. Click the link for a pop-up window with a detail summary.
- Time Since Last scan: The time since the monitoring point last scanned any query.
- Throughput: shows the number of queries audited per second.
- Incidents: Identifies the number of incidents logged against an monitoring point. Incidents have a state of Critical, Warning, and Escalated

Targets

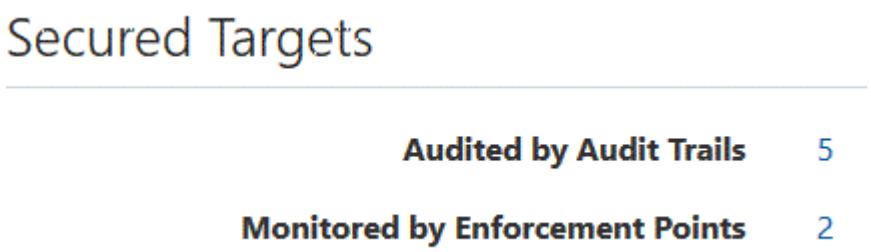
Targets can be supported databases or operating systems that Audit Vault and Database Firewall monitors. You must register all targets in Oracle Audit Vault and Database Firewall. From this page you can perform the following tasks:

- Add a Database Target
- Add Host Target
- Delete a Database Target or a Host Target
- Targets Page Information

This region (see Figure 4-7) shows number of Targets:

- Contained in the Audit Vault and Database Firewall system.
- Monitored by the Audit Trails in Audit Vault and Database Firewall system.
- Protected by the monitoring points in the Audit Vault and Database Firewall system.

Figure 4-7 Secured Targets Region

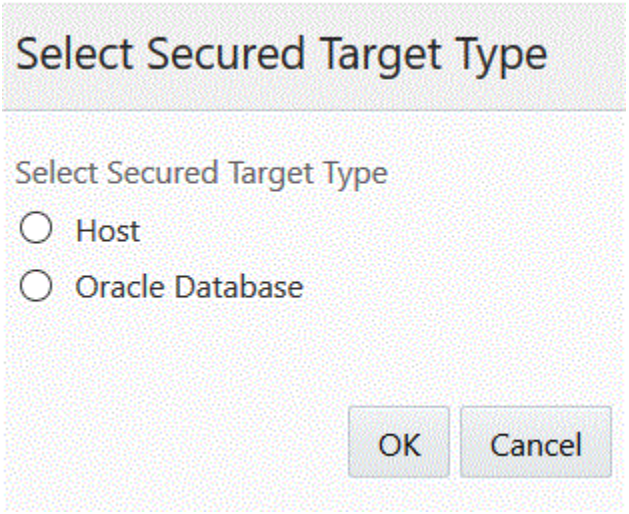


For a detailed report, select **Targets** from the Oracle Audit Vault and Database Firewall menu or click the **Targets** title on the Oracle AVDF home page.

Add a Database Target

1. From the Targets page, click **Add**.
2. On the pop-up, select **Oracle Database**, as shown in Figure 4-8:

Figure 4-8 Add Oracle Database Target Type



Click **OK**.

3. Another pop-up displays, which shows all available Oracle Database targets. Select an Oracle Database target. Click **OK** to return to the Targets page.
4. *Optional:* On the Targets page, you can modify the Database target name. Click the DB name and then enter a new target name.
5. Select the host credentials:
   - Under Target Details, select **Default Target Host Credential** and select the default host credentials for all Database hosts (applicable for all targets).

     Or

   - In the Credentials pop-up, set the host credentials for each Database host, overriding the default.
6. Enter the Sys password:
   - Under Host Details, select **Default Sys User Password** and enter the default sys password for all Databases (applicable for all targets).

     Or

   - In the DB Sys Password field, enter the **sys password** for each Database, overriding the default.
7. Select the AVDF user credentials:
   - Under Host Details, select **Default AVDF User Credential** and enter the default `avdf` user credential - a credential for a user to be created and configured on the target Oracle Database and applicable for all targets.

     Or

   - In the AVDF User Account column, click **New Credential** and enter the `avdf` user credentials for each Database target, overriding the default.
8. Click **Submit**.

Add Host Target

1. From the Targets page, click **Add**.
2. On the pop-up, select **Host Operating System**. Click **OK**.
3. Another pop-up displays, which shows all available Host Targets. Select a host target from the list. Click **OK** to return to the Targets page.
4. *Optional:* On the Targets page, you can modify the Host target name. Click the Host name and then enter a new target name.
5. Click **Submit**.
6. On the credential pop-up, enter the Oracle user credential for the AV Server host. Click **OK**.

Delete a Database Target or a Host Target

To delete a database target or a host target, follow these steps:

1. From the Targets page, select a target from the list that you want to delete.
2. Click **Delete**.
3. In the pop-up, specify the credential for the user who owns the Oracle Home of Audit Vault Agent(s).
4. Click **OK** to close the Credentials window. The deletion request is submitted as a job to Cloud Control.

Targets Page Information

On the Targets list page, the following information is available:

- **Target:** name of the target
- **Type:** the type of the supported database or operating system (such as, Oracle Database or Microsoft SQL Server)
- **Status:** shows whether the database is **Up** or **Down**
- **Audit Trails:** Number of audit trails associated with a Secure Target.
- **Monitoring Points:** the number of monitoring points associated with a Target.
- **Connection String:**
- **Monitored by:** identifies the Audit Vault Agent and Audit Trails that are monitoring this Target
- **Protected by:** identifies the Database Firewall and enforcement points that are protecting this Target

Other AVDF Plug-in Monitoring

The regions described below may provide links for additional information about the target. For example, the links in the Summary Region takes you to the corresponding component listing page which has the summary of all the components of that type. Other link and chart sections are also clickable, which will take you to the corresponding component listing page after applying the appropriate filter.

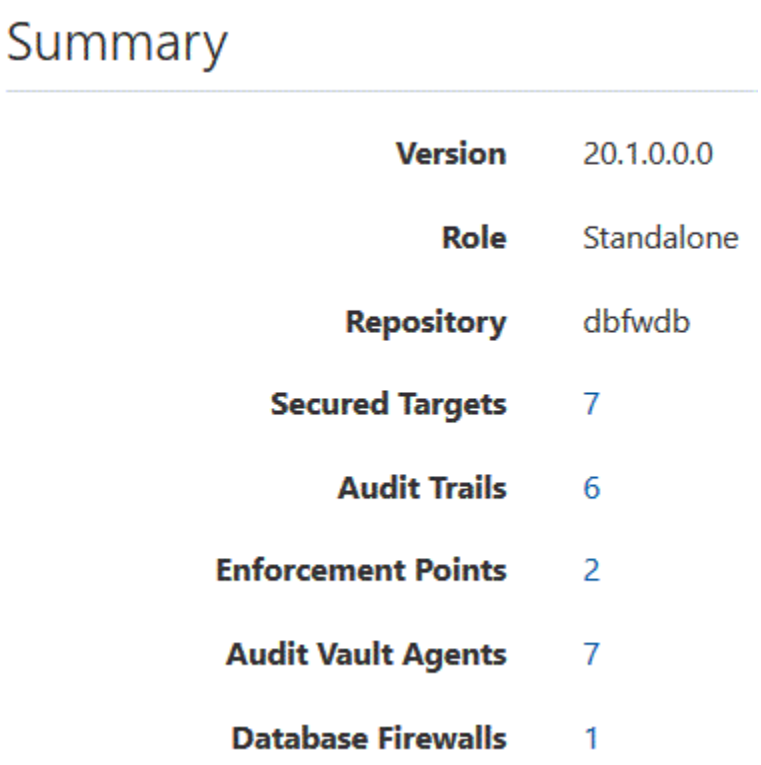
From the Oracle Audit Vault and Database Firewall plug-in home page, you can monitor the following information:

- Summary Region
- Auditor Activity Notifications
- Incidents and Problems

Summary Region

This region shows high-level information including the Oracle Audit Vault Server version and the number and type of components monitored by the plug-in (as shown in Figure 4-9).

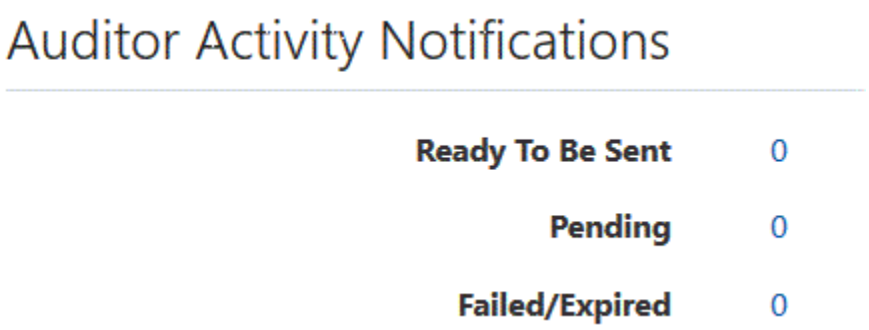
Figure 4-9 Summary Region



Auditor Activity Notifications

This region (Figure 4-10) shows the number of Auditor Activity Notifications. A notification can be **Ready to be Sent**, **Pending**, or **Failed/Expired**. These notifications are generated by Audit Trails in the Audit Vault and Database system.

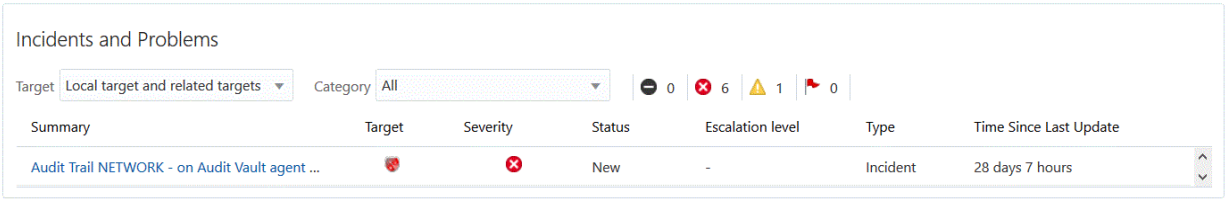
Figure 4-10 Auditor Activity Notifications Region



Incidents and Problems

This region (Figure 4-11) provides a summary of any incident or problem for the components monitored by the plug-in. If there is an incident or problem listed, click the link in the Message column to show details in the Incident Manager feature of Enterprise Manager Cloud Control.

Figure 4-11 Incidents and Problems Region



5

Administering the AVDF Plug-in

Learn more about how to upgrade and undeploy the AVDF plug-in.

Upgrade

The Self Update feature allows you to expand Enterprise Manager's capabilities by updating Enterprise Manager components whenever new or updated features become available. Updated plug-ins are made available via the Enterprise Manager Store, an external site that is periodically checked by Enterprise Manager Cloud Control to obtain information about updates ready for download. See the *Updating Cloud Control* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to update the plug-in.

Undeploy

See the *Managing Plug-ins* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to undeploy the plug-in.

Index