



CHAPTER 11

Configuring Database Applications

Database applications are typically high-value assets, and as such, they are common targets for attacks. Database applications provide MARS with user activity, such as successful and failed login attempts, session durations, and activities indicative of privilege escalation.

This chapter explains how to bootstrap and add the following database applications to MARS:

- [Oracle Database Server Generic, page 11-1](#)

Oracle Database Server Generic

To configure CS-MARS to collect information from the Oracle database server, you must perform three tasks:

- configure the Oracle database server to generate an audit trail and record those events in the database.
- represent the device in the web interface
- configure the interval at which CS-MARS should pull the logs from the Oracle database server.

Configuring the pull interval is a one-time operation that applies to all of the Oracle database servers monitored by the MARS Appliance.

This section contains the following topics:

- [Configure the Oracle Database Server to Generate Audit Logs, page 11-1](#)
- [Add the Oracle Database Server to MARS, page 11-2](#)
- [Configure Interval for Pulling Oracle Event Logs, page 11-3](#)

Configure the Oracle Database Server to Generate Audit Logs

You must configure the Oracle database server to write audit logs to the database. You may need your DBA support to perform most of these configurations. Once configured, MARS can retrieve the audit logs from your Oracle database server. The following examples are for an Oracle instance running on a UNIX/Linux application host.

To configure an Oracle database server to write audit logs, follow these steps:

Step 1 As sysdba execute `cataudit.sql` to create audit trail views:

```
[oracle@server]$ sqlplus /nolog
```

```
SQL> conn / as sysdba;
SQL> @$ORACLE_HOME/rdbms/admin/cataudit.sql
```

- Step 2** Enable auditing to the database by adding the following entry to the Oracle instance initialization file, usually named `init<SID>.ora`

```
AUDIT_TRAIL=DB
```

This file is usually located in `$ORACLE_BASE/admin/<SID>/pfile`, where `<SID>` is the name of the Oracle instance.

If a binary initialization file is used for this instance, make sure you update it first. This file is usually located in `$ORACLE_HOME/dbs` and named `spfile<SID>.ora`. Ask your DBA about the location of these files as well as the policies applied for this server.

- Step 3** Restart the database to activate the change made to the initialization file.

```
[oracle@server]$ sqlplus /nolog

SQL> conn / as sysdba;
SQL> shutdown immediate;
SQL> startup;
```

- Step 4** Turn on all the logs that you want to audit. The following example is turning on the “audit session”.

```
SQL> audit session;
Audit succeeded.
```

- Step 5** Repeat the previous step for all the logs that you want to audit.

- Step 6** Create a user account on this server and grant select privilege for the view `dba_audit_trail`. Our example assumes the user has login name “pnuser”.

```
SQL> grant select on dba_audit_trail to pnuser
```

You’ll use “pnuser” as the value for “User Name” in the MARS setup.

- Step 7** To test that everything was properly configured, audit logs are written to the database and “pnuser” has read access to them, execute the following commands:

```
[oracle@server]$ sqlplus pnuser/<password>@<oracle_server>

SQL> select count(*) from dba_audit_trail;

COUNT(*)
-----
          3
```

If the above count is anything but zero, congratulations, you have successfully configured the Oracle Server! You will have to repeat the above procedure for every Oracle server that you want to report audit logs to MARS.

Add the Oracle Database Server to MARS

To represent the Oracle database server in the web interface, follow these steps:

- Step 1** Click **Admin > Security and Monitor Devices > Add**.

- Step 2** From the **Device Type** list, select **Add SW Security apps on a new host** or **Add SW security apps on existing host**.
- Step 3** Enter the **Device Name** and **IP addresses** if adding a new host.
- Step 4** Click **Apply**.
- Step 5** From the **Select Application** list, select **Oracle Database Server Generic**.
- Step 6** Click **Add**.

The screenshot shows a configuration form for the Oracle Database Server Generic application. The form is set against a light green background and contains the following fields and controls:

- User Name:** An empty text input field.
- Password:** An empty text input field.
- Protocol:** A dropdown menu with "TCP" selected.
- Port:** A text input field containing "1521" with "(Default:1521)" displayed to its right.
- Oracle Service Name:** An empty text input field.
- Audit View:** A text input field containing "DBA_AUDIT_TRAIL".

Below the form, there are three buttons: "Test Connectivity", "Cancel", and "Submit". A small vertical number "143265" is visible to the right of the "Submit" button.

- Step 7** Enter the **User Name, Password and Oracle Service Name**
- **User Name** – the Oracle Database User Name
 - **Password** – the Oracle Database User password
 - **Oracle Service Name** – the Oracle Service Name

The Oracle Service Name is the GLOBAL_DBNAME=username.server which can be found inside a file called listener.ora.

- Step 8** Click **Test Connectivity** to verify the configuration.
- Step 9** Click **Submit**.

Configure Interval for Pulling Oracle Event Logs

To specify the interval at which MARS should pull the event logs from all Oracle database servers on your network, follow these steps:

- Step 1** Click **Admin > System Parameters > Oracle Event Log Pulling Time Interval**.

Oracle Event Log Pulling Time Interval

Oracle Event Log Pulling Time Interval: (secs)

143252

Step 2 Enter the new time interval in seconds. The default value is 300 (five minutes).

Step 3 Click **Submit**.
