



## 第 11 章 データベース アプリケーションの設定

データベース アプリケーションは一般に高価値な資産であるため、攻撃のターゲットになることが頻繁にあります。データベース アプリケーションは、ログイン試行の成功や失敗、セッション期間などのユーザ アクティビティ、および権限エスカレーションを示すアクティビティに関する情報を MARS に提供します。

この章では、次のデータベース アプリケーションをブートストラップして、MARS に追加する方法を説明します。

- ・ Oracle データベース サーバ一般

### Oracle データベース サーバ一般

Oracle データベース サーバから情報を収集するように CS-MARS を設定するには、次の 3 つのタスクを実行する必要があります。

- ・ 監査追跡を生成し、データベースにこれらのイベントを記録するように、Oracle データベース サーバを設定します。
- ・ HTML インターフェイスでデバイスを指定します。
- ・ CS-MARS が Oracle データベース サーバからログをプルするインターバルを設定します。

プル インターバルは、1 回設定すると、MARS アプライアンスがモニタするすべての Oracle データベース サーバに適用されます。

ここで説明する内容は、次のとおりです。

- ・ 「監査ログを生成するための Oracle データベース サーバの設定」
- ・ 「MARS への Oracle データベース サーバの追加」
- ・ 「Oracle イベント ログのプル インターバルの設定」

### 監査ログを生成するための Oracle データベース サーバの設定

監査ログをデータベースに書き込むように Oracle データベースを設定する必要があります。このように設定するには、通常、DBA のサポートが必要です。設定が完了したら、MARS は Oracle データベース サーバから監査ログを取得できます。次に、UNIX/Linux アプリケーション ホストで稼働している Oracle インスタンスの例を示します。

監査ログを書き込むように Oracle データベースを設定する手順は、次のとおりです。

**ステップ 1** sysdba として cataudit.sql を実行して、監査証跡ビューを作成します。

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

```
SQL> conn / as sysdba;
```

```
SQL> @$ORACLE_HOME/rdbms/admin/cataudit.sql
```

**ステップ 2** Oracle インスタンス初期化ファイル(通常は init<SID>.ora)に次のエントリを追加して、データベースに対する監査をイネーブルにします。

```
AUDIT_TRAIL=DB
```

このファイルは通常、\$ORACLE\_BASE/admin/<SID>/pfile に格納されています。<SID> は Oracle インスタンスの名前です。

このインスタンスにバイナリ初期化ファイルが使用されている場合は、最初にこのファイルを更新する必要があります。このファイルは通常、spfile<SID>.ora という名前で \$ORACLE\_HOME/dbs に格納されています。これらのファイルの場所、およびこのサーバに適用されるポリシーは、DBA に確認してください。

**ステップ 3** データベースを再起動して、初期化ファイルに対する変更を有効にします。

```
[oracle@server]$ sqlplus /nolog
SQL> conn / as sysdba;
SQL> shutdown immediate;
SQL> startup;
```

**ステップ 4** 監査するログをすべてオンにします。次に「監査セッション」をオンにする例を示します。

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

**ステップ 5** 監査するすべてのログについて上記の手順を繰り返します。

**ステップ 6** このサーバのユーザ アカウントを作成し、ビュー dba\_audit\_trail の選択権限を付与します。例では、ユーザ ログイン名に「pnuser」を使用します。

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

MARS を設定する場合、「User Name」の値には「pnuser」を使用します。

**ステップ 7** すべてが適切に設定されている (監査ログがデータベースに書き込まれるように設定され、「pnuser」にこのデータベースの読み取りアクセス権がある) ことをテストするには、次のコマンドを実行します。

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

```
SQL> select count(*) from dba_audit_trail;
```

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

上記のカウントがゼロでない場合は、Oracle サーバは正しく設定されています。監査ログを MARS に報告するすべての Oracle サーバに対して、上記手順を繰り返す必要があります。

## MARS への Oracle データベース サーバの追加

HTML インターフェイスで Oracle データベース サーバを指定する手順は、次のとおりです。

**ステップ 1** Admin > Security and Monitor Devices > Add の順にクリックします。

**ステップ 2** Device Type リストで、Add SW Security apps on a new host または Add SW security apps on existing host をクリックします。

**ステップ 3** 新しいホストを追加する場合は、Device Name にデバイス名、IP addresses に IP アドレスを入力します。

**ステップ 4** Apply をクリックします。

**ステップ 5** Select Application リストから、Oracle Database Server Generic を選択します。

**ステップ 6** Add をクリックします。

User Name:   
 Password:   
 Protocol:    
 Port:  (Default:1521)  
 Oracle Service Name:   
 Audit View:

**ステップ 7** User Name、Password、および Oracle Service Name を入力します。

- ・ **User Name** — Oracle データベースのユーザ名
- ・ **Password** — Oracle データベースのユーザ パスワード
- ・ **Oracle Service Name** — Oracle サービスの名前

Oracle Service Name は、ファイル listener.ora に定義されている GLOBAL\_DBNAME=username.server になります。

**ステップ 8** Test Connectivity をクリックして、設定を確認します。

**ステップ 9** Submit をクリックします。

## Oracle イベント ログのプル インターバルの設定

MARS がネットワーク上のすべての Oracle データベース サーバからイベント ログをプルするインターバルを指定する手順は、次のとおりです。

**ステップ 1** Admin > System Parameters > Oracle Event Log Pulling Time Interval の順にクリックします。

Oracle Event Log Pulling Time Interval

Oracle Event Log Pulling Time Interval:  (secs)

**ステップ 2** 新しいインターバルを秒単位で入力します。デフォルト値は 300 秒 (5 分間) です。

**ステップ 3** Submit をクリックします。

