Oracle Maximum
Availability Architecture

Oracle FMW Identity and Access Management（11.1.2.3）のベスト・プラクティス：Oracle Adaptive Access Managerによるエンタープライズ・デプロイメントの拡張

Oracle ホワイト・ペーパー | 2016 年 7 月

ORACLE

目次

はじめに

Oracle Identity and Access Management 11.1.2.3 エンタープライズ・デプロイメント・ガイドでは、Oracle Identity and Access Management のエンタープライズ・デプロイメントのセットアップ方法を説明します。このガイドに書かれているプロセスに沿って作業を進めれば、次の製品のミッション・クリティカルなデプロイメントをセットアップできます。

» Oracle Unified Directory、Oracle Internet Directory、または Active Directory

» Oracle Access Manager

» Oracle Identity Manager

このドキュメントでは、このデプロイメントの活用方法と、これを Oracle Adaptive Access Manager を使ってさらに拡張する方法について説明します。

Oracle Adaptive Access Manager の導入により既存の認証フローが強化され、イベント発生時点でのリスク評価が可能になり、リスクベースの犯罪防止メカニズム（マルチファクタ帯域外認証など）が導入されるため、不正や悪用を防止できます。ポリシーを直感的に管理でき、Oracle Identity and Access Management Suite のコンポーネントとの統合が標準化されている Oracle Adaptive Access Manager は、企業のセキュリティにおけるリスクを軽減するうえで優れた柔軟性と効果を発揮します。また、リアルタイムおよびバッチでのリスク分析により複数のアクセス・チャネルをまたぐ不正や誤用を阻止できるほか、アクセス・イベントやトランザクション・イベントを調査して不正や悪用を検出する作業が自動化されることから、時間と費用の節約も実現します。確かな機能を備え、迅速に投資を回収できる Oracle Adaptive Access Manager は、どの企業も必ず所有すべき製品です。

Oracle Adaptive Access Manager（OAAM）は Java EE を基盤とする複数層デプロイメント・アーキテクチャ上に構築されているため、プラットフォームのプレゼンテーション層、ビジネス・ロジック層およびデータ層が分離されています。層がこのように分離されているため、パフォーマンス要件に合せてすばやく調整できます。このアーキテクチャでは、Java、XML、およびオブジェクト・テクノロジーの組合せという、もっとも柔軟でもっとも採用されているクロス・プラットフォームである Java EE サービスを利用できます。OAAM がスケーラブルでフォルト・トレラントなソリューションであるのは、このアーキテクチャのおかげです。

Oracle Adaptive Access Manager は次の 2 つのコンポーネントで構成されています。

» Oracle Adaptive Access Manager 管理アプリケーション

» Oracle Adaptive Access Manager サーバー・アプリケーション

Oracle Adaptive Access Managerを使用した
エンタープライズ・デプロイメント・トポロジ

このドキュメントに記載されている手順を完了すると、エンタープライズ・デプロイメント・トポロジは次のようになります。

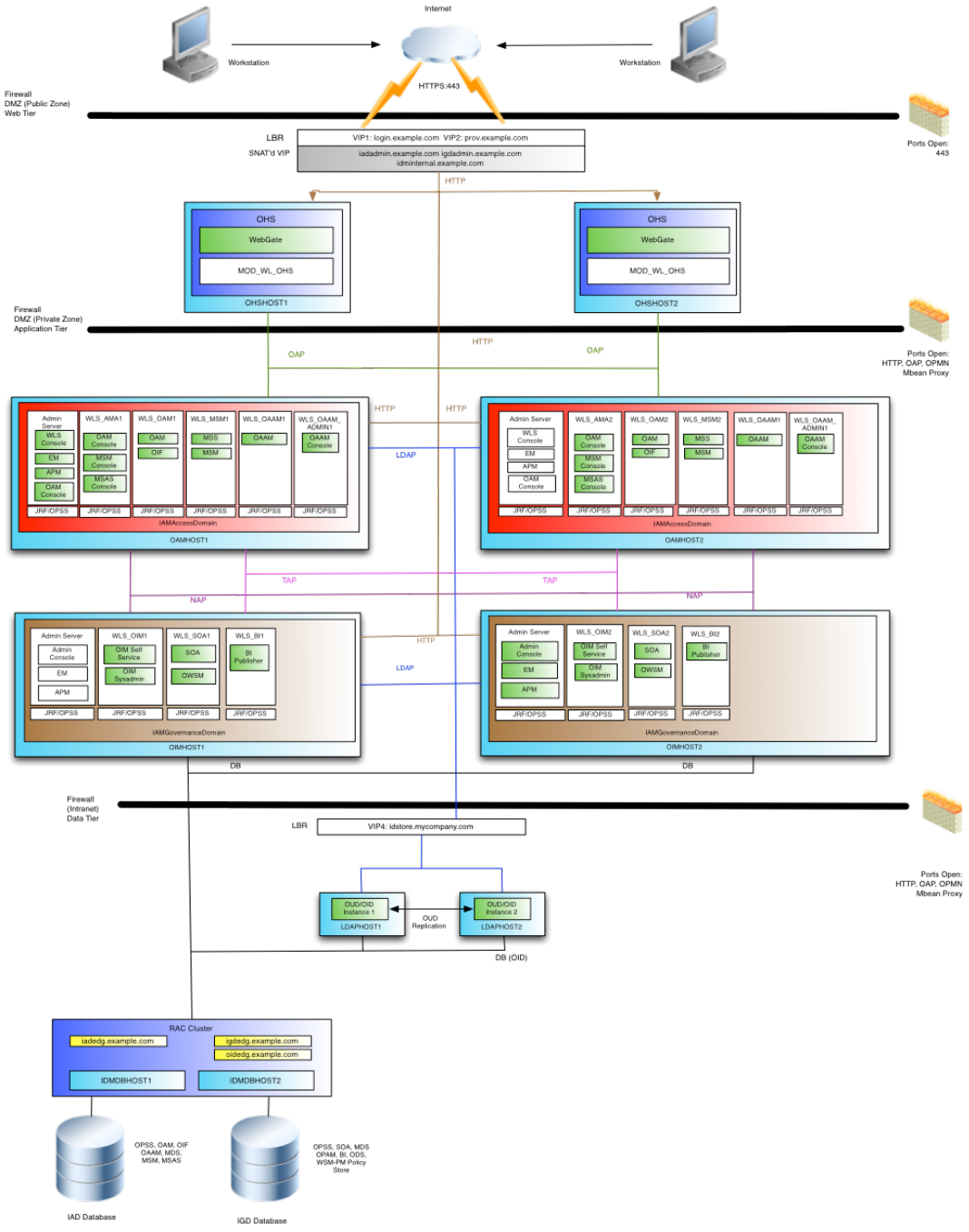

図1：Oracle Identity and Access Managementのトポロジ

Oracle Identity and Access Managementの標準的なエンタープライズ・デプロイメントに必要なメモリ、ファイル記述子、およびプロセス

表 1 は、Oracle SOA Suite の標準的なエンタープライズ・デプロイメントで管理サーバーおよび管理対象サーバーとして使用される各コンピュータに必要なメモリ、ファイル記述子、およびプロセスをまとめたものです。表で示している値は一例に過ぎませんが、これを基にして初期のエンタープライズ・デプロイメントに必要な最小メモリ量を見積もることができます。

表 1 の例は、デプロイメント・トポロジに関する項に掲載した参照トポロジに描かれている OAMHOST1 上で必要な管理対象サーバーおよび他のサービスを構成する場合の最小要件を表しています。

マシンを調達する際は、「最大メモリ概算量」の列に書かれている値を参考にして、各ホスト・コンピュータの使用可能な物理メモリ量がどのくらい必要なのかを判断してください。

ホスト・コンピュータ・ハードウェアを調達してオペレーティング・システム要件を検証したら、ソフトウェア構成を調査し、「ファイル記述子」の列に書かれているオープン・ファイルの数と「オペレーティング・システムのプロセスとタスク」の列に書かれているプロセスの数に対応できるようにオペレーティング・システムの設定が構成されていることを確認します。

表1：各エンタープライズ・デプロイメント・ホストに必要な標準的なメモリ、ファイル記述子、およびプロセス

管理対象サーバー、ユーティリティ、またはサービス	最大メモリ概算量	ファイル記述子の数	オペレーティング・システムのプロセスとタスク
WLS_OAAM_ADMIN	2GB	800	100
WLS_OAAM	1.5 GB	750	100

エンタープライズ・デプロイメント・ワークブックの使用

このガイドには、Oracle Fusion Middleware エンタープライズ・デプロイメント・ワークブックが付属しています。これは、アーキテクト、システム・エンジニア、データベース管理者などがインストール環境の詳細（サーバー名、URL、ポート数、インストール・パス、および他のリソースなど）を計画したり記録したりすることに使用できるスプレッドシートです。エンタープライズ・デプロイメント・ワークブックについて詳しくは、『Oracle Identity and Access Management 11.1.2.3 エンタープライズ・デプロイメント ガイド』を参照してください。

Oracle Identity and Access Management エンタープライズ・デプロイメント・ワークブックは、Oracle Fusion Middleware のドキュメント・ライブラリから Microsoft Excel スプレッドシートとして入手できます。ライブラリのインストール、パッチ、およびアップグレード・ページのリンクから入手できます。

Oracle Adaptive Access Managerの詳細

Oracle Identity and Access Management のデプロイのために作成したエンタープライズ・デプロイメント・ワークシートのブックのほかに、このワークシートを使用して OAAM 固有の追加情報を記録します。

表2：Oracle Adaptive Access Managerの詳細

説明	ドキュメント内での変数	ドキュメント内での値	実際の値
OAAM 管理対象サーバーの名前		WLS_OAAM1 WLS_OAAM2	
OAAM 管理対象サーバーのポート	OAAM_PORT	14300	
OAAM 管理対象サーバーの SSL ポート	OAAM_SSL_PORT	14301	
OAAM 管理の管理対象サーバーの名前		WLS_OAAM_ADMIN1 WLS_OAAM_ADMIN2	
OAAM 管理の管理対象ポート	OAAM_ADMIN_PORT	14200	
OAAM 管理の管理対象 SSL ポート	OAAM_ADMIN_SSL_PORT	14201	
ID ストア・ホスト	LDAPHOST	LDAPHOST1.EXAMPLE.COM	
ID ストア・ポート	LDAP_PORT	1389	
ID ストアのバインド DN	LDAP_ADMIN_USER	cn=oudadmin	
ID ストア管理者ポート	LDAP_ADMIN_PORT	4444	
ID ストア・グループ検索ベース	LDAP_GROUP	cn=Groups,dc=example,dc=com	

OAAM 管理ユーザー	OAAMADMINUSER	oaamadmin	
Access Manager ホスト 1	OAMHOST1	OAMHOST1	
Access Manager ホスト 2	OAMHOST2	OAMHOST2	

OAAMを追加するためのドメイン拡張の概要

Oracle Adaptive Access Manager は次の 2 つのコンポーネントで構成されています。

» Oracle Adaptive Access Manager 管理アプリケーション

» Oracle Adaptive Access Manager サーバー・アプリケーション

前提条件

ドメインを拡張して Oracle Adaptive Access Manager（OAAM）を追加する前に、次の前提条件を満たしておく必要があります。

高可用性データベースの作成

IADDB を使用していない場合は、OAAM のデータを保持するための可用性の高いデータベースを作成します。リポジトリ作成ユーティリティを使用して、このデータベースに OAAM のデータ・オブジェクトを事前にシードします。このドキュメントでは、OAAM スキーマに Access Database Service を使用することを前提とします。

LDAPでのOAAMユーザーとグループの作成

次の要領でOAAMユーザーとグループを作成します。

次の内容の構成ファイルを作成します。

Common

IDSTORE_HOST:LDAPHOST1.example.com IDSTORE_PORT:1389

IDSTORE_ADMIN_PORT:4444

IDSTORE_BINDDN: cn=oudadmin

IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com

IDSTORE_SEARCHBASE: dc=example,dc=com

IDSTORE_USERNAMEATTRIBUTE: cn

IDSTORE_LOGINATTRIBUTE: uid

IDSTORE_USERSEARCHBASE: cn=Users, dc=example,dc=com

IDSTORE_OAAMADMINUSER: oaamadmin

コマンド説明：

» IDSTORE_HOST（LDAP_HOST）と IDSTORE_PORT（LDAP_PORT）はそれぞれ、ID ストア・ディレクトリのホストとポートです。次に例を示します。

» OUD:LDAPHOST1 および 1389

» IDSTORE_ADMIN_PORT（LDAP_ADMIN_PORT）は、Oracle Unified Directory インスタンスの管理ポートです。

» IDSTORE_BINDDN（LDAP_ADMIN_USER）は、ID ストア・ディレクトリ内の管理ユーザーです。

» IDSTORE_GROUPSEARCHBASE は、グループが保存されているディレクトリの場所です。例：cn=Groups,dc=example,dc=com

» IDSTORE_SEARCHBASE は、ユーザーとグループが保存されているディレクトリの場所です。例：cn=Users,dc=example,dc=com

» IDSTORE_USERNAMEATTRIBUTE は、ユーザーの名前を含むディレクトリ属性の名前です。例：cn。なお、これはログイン名とは異なります。

» IDSTORE_LOGINATTRIBUTE は、ユーザーのログイン名が含まれる LDAP 属性です。例：uid

» IDSTORE_USERSEARCHBASE は、ユーザーが保存されているディレクトリの場所です。たとえば、dc=example,dc=com です。

» IDSTORE_OAMADMINUSER（OAAMADMINUSER）は、Oracle Adaptive Access Manager の管理者として作成するユーザーの名前です。

idmConfigToolを使用してユーザーを作成します。

Oracle Identity and Access Management のコンポーネントに必要なユーザーとグループを、ID ストアにシードする必要があります。ID ストアにユーザーとグループをシードするには、OAMHOST1 上で次のタスクを実行します。

1. 環境変数を設定します。

   MW_HOME を *IAD_MW_HOME* に設定します。

   ORACLE_HOME を *IAD_ORACLE_HOME* に設定します

   JAVA_HOME を *JAVA_HOME* に設定します。

2. コマンド idmConfigTool を使用して、ID ストアを構成します。

   このコマンドは *IAD_ORACLE_HOME*/idmtools/bin にあります。

   Linux でのコマンドの構文は、次のとおりです。

   ```
   idmConfigTool.sh -prepareIDStore mode=OAAM input_file=configfile
   ```

   configfile は、この項の最初で作成した構成ファイルの名前です。

3. コマンドを実行すると、ID ストアに接続しているアカウントのパスワードの入力を求められます。

コマンドの実行中に、作成しているアカウントのパスワードの入力を求められます。すべてに共通のパスワードを使用する場合は、使い勝手をよくするために *COMMON_IDM_PASSWORD* を入力することをお勧めします。

コマンドを実行するたびに、ログ・ファイルでエラーや警告を確認して修正します。ツールの実行元のディレクトリに、automation.log という名前のファイルが作成されます。

Oracle Adaptive Access Managerでのドメイン拡張

OAMHOST1 で次のコマンドを実行して構成ウィザードを起動します。

IAD_MW_HOME/oracle_common/common/bin/config.sh

続いて、次の手順を実行します。

1. Welcome 画面で、「**Extend an Existing WebLogic Domain**」を選択します。「**Next**」をクリックします。

2. Select a WebLogic Domain 画面で、ナビゲータを使用して管理サーバーのドメイン・ホームを選択します。例：*IAD_ASERVER_HOME*

   「**Next**」をクリックします。

3. Select Extension Source 画面で、次の製品を選択します。

   - Oracle Adaptive Access Manager - Server
   - Oracle Adaptive Access Manager - Admin Server

   「**Next**」をクリックします。

4. Configure JDBC Component Schema 画面で次のとおりに実行します。

   次を選択します。

   - OAAM Admin Schema
   - OAAM Server Schema
   - OAAM Admin MDS Schema

   各コンポーネントのスキーマ用の Oracle RAC 構成の場合は、「**Convert to GridLink**」を選択します。「**Next**」をクリックします。

5. Gridlink RAC Component Schema 画面が表示されます。この画面で次のフィールドの値を入力して、RCU でシードされた Oracle RAC データベースの接続情報を指定します。Exadata SDP Connections に以下の TCP パラメータを入力します。後でこれを SDP Connect String に変換する必要があります。

» **Driver**：「Oracle's driver (Thin) for GridLink Connections,Versions:10」以降を選択します。

» 「**Enable FAN**」を選択します。

» 次のいずれかの手順を実行します。

- ONS 通知の暗号化用に SSL が構成されていない場合は、「SSL」を選択解除します。
- 「SSL」を選択して、適切なウォレットとウォレット・パスワードを入力します。
- **Service Listener**：使用中の Oracle RAC データベースの SCAN アドレスとポートを入力します。このアドレスは、次のようにデータベースでパラメータ remote_listener の問合せを実行すると特定できます。

```
SQL>show parameter remote_listener;

NAME              TYPE     VALUE
------------------------------------------------------------
remote_listener   string   iamdbscan.example.com:1521
```

注：

Oracle Database 11g Release 1（11.1）の場合は、各データベース・インスタンス・リスナーの仮想 IP とポートを使用します。たとえば、DBHOST1-VIP.example.com（ポート 1521）と DBHOST2-VIP.example.com（ポート 1521）を使用します。なお、1521 は DB_LSNR_PORT です。

- **ONS Host**：Oracle RAC データベースの SCAN アドレスと、次のコマンドを実行してデータベースから返される ONS リモート・ポートを入力します。

```
srvctl config nodeapps -s

ONS exists:Local port 6100, remote port 6200, EM port 2016
```

注：

Oracle Database 11g Release 1（11.1）の場合、各データベースの ONS のホスト名とポートを使用します。たとえば、次のとおりです。

`DBHOST1.example.com`（ポート `6200`）

および

`DBHOST2.example.com`（ポート `6200`）

次の RAC コンポーネント・スキーマ情報を入力します。

表3：Oracle RACコンポーネント・スキーマの情報

スキーマ名	サービス名	スキーマ所有者	パスワード
OAAM Admin Schema	EDGIAD.example.com	EDGIAD_OAAM	Password
OAAM Admin MDS Schema	EDGIAD.example.com	EDGIAD_MDS	Password
OAAM Server Schema	EDGIAD.example.com	EDGIAD_OAAM	Password

6. Test Component Schema 画面では、構成ウィザードによってデータソースの検証が試行されます。データソースの検証が成功したら、「**Next**」をクリックします。

   失敗した場合、「**Previous**」をクリックして問題を修正し、再試行します。

7. Select Optional Configuration 画面で「**Managed Server Clusters and Machines**」を選択します。「**Next**」をクリックします。

8. 初めて Configure Managed Servers 画面を開くと、Access Manager などの構成済みコンポーネントのエントリが表示されます。さらに、2 つの新しい OAAM 用の管理対象サーバーが作成されます。

注：

この画面を初めて開いたときには、デフォルトの管理対象サーバーがすでに作成されています。

次の詳細に合わせて、デフォルトの管理対象サーバーの詳細を変更します。すなわち、**1 つのエントリを変更してエントリを 1 つ追加します**。

以前のアプリケーション・デプロイメントの一部としてすでに構成済みの管理対象サーバーの構成は変更しないでください。

表4：OAAM管理対象サーバーの詳細

デフォルト名	名前	リスニング・アドレス	リスニング・ポート	SSL リスニング・ポート	SSL 有効化
OAAM_SERVER_SERVER1	WLS_OAAM1	OAMHOST1	14300（OAAM_ADMIN_PORT）	14301（OAAM_ADMIN_SSL_PORT）	選択する
	WLS_OAAM2	OAMHOST2	14300（OAAM_ADMIN_PORT）	14301（OAAM_ADMIN_SSL_PORT）	選択する
OAM_ADMIN_SERVER1	WLS_OAAM_ADMIN1	OAMHOST1	14200（OAAM_PORT）	14201（OAAM_SSL_PORT）	選択する
	WLS_OAAM_ADMIN2	OAMHOST2	14200（OAAM_PORT）	14201（OAAM_SSL_PORT）	選択する

注：自動パッチ適用を行うには、表 4 に記載されている名前を使用する必要があります。

他のフィールドはすべてデフォルト設定のままにして、「**Next**」をクリックします。

9. Configure Clusters 画面で、「Add」をクリックしてクラスタを作成し、次の表に示されている oaam_cluster の値を入力します。さらに、「Add」をクリックして 2 つ目のクラスタを作成し、表の oaam_admin_cluster の値を入力します。

表5：クラスタの詳細

名前	クラスタ・メッセージング・モード	マルチキャスト・アドレス	マルチキャスト・ポート	クラスタ・アドレス
OAAM_CLUSTER	Unicast	N/A	N/A	空のままにします。
OAAM_ADMIN_CLUSTER	Unicast	N/A	N/A	空のままにします。

他のフィールドはすべてデフォルト設定のままにして、「Next」をクリックします。

10. Assign Servers to Clusters 画面で、管理対象サーバーとクラスタを関連付けます。右ペインのクラスタ名をクリックします。Servers の下に表示されている管理対象サーバーをクリックしてから矢印をクリックして、管理対象サーバーをクラスタに割り当てます。

次のように、サーバーをクラスタに割り当てます。

表6：クラスタへのサーバーの割当て

クラスタ	サーバー
OAAM_CLUSTER	WLS_OAAM1、WLS_OAAM2
OAAM_ADMIN_CLUSTER	WLS_OAAM_ADMIN1、WLS_OAAM_ADMIN2

注：以前のアプリケーション・デプロイメントの一部としてすでに構成済みのクラスタの構成は変更しないでください。

「**Next**」をクリックします。

11. Configure Machines 画面で「Next」をクリックします。注：デプロイメントを実行するとマシンが作成されます。

12. Assign Servers to Machines 画面で、次のようにサーバーをマシンに割り当てます。

    - OAMHOST1：wls_oaam1、wls_oaam_admin1
    - OAMHOST2：wls_oaam2、wls_oaam_admin2

    「**Next**」をクリックして続行します。

13. Configuration Summary 画面で「**Extend**」をクリックしてドメインを拡張します。

    注：次のような警告が表示されることがあります。

    CFGFWK:Server listen ports in your domain configuration conflict with ports in use by active processes on this host

    その場合は「**OK**」をクリックします。

    この警告は、管理対象サーバーが以前のインストールの一部として定義されている場合に表示されるものであるため、無視してかまいません。

OAMHOST1上での管理サーバーの再起動

OAMHOST1 上で WebLogic 管理サーバーを再起動します。

ローカル・ストレージへの管理対象サーバーの構成の展開

構成が完了したら、OAMHOST1 および OAMHOST2 の管理対象サーバーのディレクトリに Oracle Adaptive Access Manager の構成を伝播する必要があります。

Oracle Adaptive Access Manager を伝播するには、最初に共有ストレージの場所からドメイン IAMAccessDomain を圧縮し、ローカル・ストレージの管理対象サーバーのディレクトリに解凍します。

これを行うには、ドメインの圧縮と解凍を実行します。最初に OAMHOST1 の IAMAccessDomain でドメインを圧縮し、次に OAMHOST1 および OAMHOST2 でそれを解凍します。

次の手順を実行して、管理対象サーバーのドメイン・ディレクトリにドメインを伝播します。

14. OAMHOST1 の ORACLE_COMMON_HOME/common/bin/から pack ユーティリティを起動します。

```
./pack.sh -domain=IAD_ASERVER_HOME -template=iam_domain.jar -template_name="IAM Domain" -managed=true
```

15. OAMHOST1 と OAMHOST2 で unpack ユーティリティを起動します。このユーティリティもディレクトリ ORACLE_COMMON_HOME/common/bin/にあります。

```
./unpack.sh -domain=IAD_MSERVER_HOME -template=iam_domain.jar -overwrite_domain=true -
app_dir=IAD_MSERVER_HOME/applications
```

次のようなメッセージが表示された場合は無視してもかまいません。

```
-------------------------------------------------------
```

>> Server listen ports in your domain configuration conflict with ports in use by active processes on this host.

Port 14100 on wls_oam2

起動および停止スクリプトへのOAAMサーバーの追加

デプロイメントを実行すると、ドメインに定義した管理対象サーバーを起動および停止するスクリプト群が作成されます。ドメインで新しい管理対象サーバーを作成した場合は必ずドメイン構成を更新し、新しく作成した管理対象サーバーもこれらの起動および停止スクリプトで起動できるようにする必要があります。この作業はこの時点では各 OAAM 管理対象サーバーに対して行う必要があります。

ドメイン構成を更新するには、serverInstancesCustom.txt ファイルを編集します。このファイルは *SHARED_CONFIG_DIR*/scripts ディレクトリにあります。

新しいマシンでノード・マネージャを起動する場合は、次のようなエントリを追加します。

```
newmachine.example.com NM nodemanager_pathname nodemanager_port
```

次に例を示します。

```
OAMHOST3.example.com NM /u01/oracle/config/nodemanager/oamhost3.example.com 5556
```

表 4：OAAM 管理対象サーバーの詳細に記載されている各 OAAM 管理対象サーバーで、次のようなエントリを追加します。

```
newmachine.example.com OAAM ManagedServerName
```

次に例を示します。

```
OAMHOST1 OAAM wls_oaam1 IADADMINVHN 7001

OAMHOST1 OAAM wls_oaam_admin1 IADADMINVHN 7001

OAMHOST2 OAAM wls_oaam2 IADADMINVHN 7001

OAMHOST2 OAAM wls_oaam_admin2 IADADMINVHN 7001
```

ファイルを保存します。

OAMHOST1上でのOAAMの起動と検証

OAMHOST1上でのOracle Adaptive Access Managerの起動

IAMAccessDomain の WebLogic 管理コンソールを起動します。

ドメイン構造メニューから「**Environment**」→「**Servers**」の順に選択し、「**Control**」タブをクリックします。

サーバー**wls_oaam_admin1** と **wls_oaam1** を選択して「**Start**」をクリックします。

OAMHOST1上でのOAAMの検証

http://OAMHOST1.example.com:14200/oaam_admin にある OAAM 管理サーバーに接続して、実装を検証します。OAAM 管理コンソールのログイン・ページが表示され、「LDAP での OAAM ユーザーとグループの作成」の項で作成した oaamadmin アカウントを使用してログインできれば、正しく実装されています。

次の場所にある OAAM サーバーに接続して、実装を検証します。
http://oamhost1.example.com:14300/oaam_server

OAAM サーバーのログイン・ページが表示されれば正しく実装されています。

OAMHOST2上でのOAAMの起動と検証

この項では、Oracle Adaptive Access Manager を OAMHOST2 で構成する方法を説明します。

OAMHOST2上でのOracle Adaptive Access Managerの起動

IAMAccessDomain 用、WebLogic 管理対象サーバーwls_oaam2 および wls_oaam_admin2 用の WebLogic 管理コンソールを使用して、OAMHOST2 上で Oracle Adaptive Access Manager を起動します。

OAMHOST2上でのOAAMの検証

http://OAMHOST2.example.com:14200/oaam_admin にある OAAM 管理サーバーに接続して、実装を検証します。OAAM 管理コンソールのログイン・ページが表示され、「LDAP での OAAM ユーザーとグループの作成」の項で作成した oaamadmin アカウントを使用してログインできれば、正しく実装されています。

http://OAMHOST2.example.com:14300/oaam_server にある OAAM サーバーに接続して、実装を検証します。OAAM サーバーのログイン・ページが表示されれば正しく実装されています。

Web層と連携するためのOAAMの構成

この項では、Oracle Adaptive Access Manager を構成して Oracle HTTP Server と連携する方法を説明します。

Oracle HTTP Serverからのアクセスの構成

WEBHOST1 および WEBHOST2 上の次のファイルを更新して、OAAM を Web 層構成に追加する必要があります。

IADADMIN.example.comの更新

次の内容を *OHS_ORACLE_INSTANCE/config/OHS/component_name/moduleconf/iadadmin_vh.conf* に追加します。

```
#####################################################
## Oracle Adaptive Access Manager に必要なエントリ
#####################################################

# OAAM コンソール
<Location /oaam_admin>
  SetHandler weblogic-handler
  WebLogicCluster OAMHOST1.example.com:14200,OAMHOST2.example.com:14200
</Location>
```

login.example.comの更新

次の内容を OHS_ORACLE_INSTANCE/config/OHS/component_name/moduleconf/login_vh.conf に追加します。

```
#####################################################
## Oracle Adaptive Access Manager に必要なエントリ
#####################################################

<Location /oaam_server>
  SetHandler weblogic-handler
  WebLogicCluster OAMHOST1.example.com:14300,OAMHOST2.example.com:14300
  WLProxySSL ON
  WLProxySSLPassThrough ON
</Location>
```

Oracle HTTP ServerおよびOAAM管理対象サーバーの再起動

WEBHOST1 および WEBHOST2 上の Oracle HTTP Server を再起動します。

管理対象サーバーwls_oaam1、wls_oaam2、wls_oaam_admin1、wls_oaam_admin2 を再起動します。

WebLogicにおけるホスト・アサーションの変更

Oracle HTTP Server は WebLogic のプロキシとして機能するため、デフォルトでは特定の CGI 環境変数は WebLogic に渡されません。これらの環境変数には、ホストやポートも含まれます。WebLogic で仮想サイト名およびポートを使用しているため、内部 URL を適切に生成できることを、WebLogic に対して通知する必要があります。

これを実行するために、IAMAccessDomain の WebLogic 管理コンソールにログインします。

以下の手順を実行します。

1. ホーム・ページから「Clusters」を選択するか、Domain 構造メニューから「**Environment**」→「**Clusters**」を選択します。
2. Change Center ウィンドウで「**Lock and Edit**」をクリックして、編集を有効にします。
3. クラスタ名（oaam_cluster）をクリックします。
4. 「HTTP」を選択して次の値を入力します。
   - Frontend Host：login.example.com（IAM_LOGIN_URI）
   - Frontend HTTP Port：80（HTTP_PORT）
   - Frontend HTTPS Port：443（HTTP_SSL_PORT）

   このように設定すると、WebLogic 内で作成された HTTPS URL はすべて、ロードバランサのポート 443 に転送されるようになります。

5. 「**Save**」をクリックします。
6. ホーム・ページから「Clusters」を選択するか、Domain 構造メニューから「**Environment**」→「**Clusters**」の順に選択します。
7. クラスタ名（oaam_admin_cluster）をクリックします。
8. 「**HTTP**」を選択して次の値を入力します。

» **Frontend Host**：IADADMIN.example.com（IAD_DOMAIN_ADMIN_LBRVHN）

» **Frontend HTTP Port**：80（HTTP_PORT）

9. 「**Save**」をクリックします。
10. Change Center ウィンドウで「**Activate Changes**」をクリックして、編集を有効にします。

Oracle Adaptive Access Managerの検証

oaamadmin アカウントを使用して Oracle Adaptive Access Management 管理コンソールにログインします。

次の URL にアクセスできることを確認します。

https://login.example.com:443/oaam_server/oamLoginPage.jsp

Oracle Adaptive Access Managerシード・データのロード

この項では、シード・データを Oracle Adaptive Access Manager にロードする方法を説明します。

注：OAMHOST1 から(ブラウザを実行している)ローカル・マシンにファイルをコピーするか、OAMHOST1 で起動したブラウザから次の手順を実行します。

1. Oracle Adaptive Access Management 管理コンソールにログインします。
   oaamadmin アカウントを使用して接続します。
2. 「Navigation」→「**Environment**」メニューにある「**System Snapshots**」をクリックします。
   「**Open**」をクリックします。
3. 「**Load From File**」をクリックします。
4. 以下の情報を入力します。

   Name：Default Snapshot

   Notes：Default Snapshot

   「**Backup Current System Now**」を選択します。

   「**Continue**」をクリックします。
5. 「**OK**」をクリックしてバックアップの作成を了承します。
6. 「**Browse**」をクリックします。
7. 次の場所にあるファイル oaam_base_snapshot.zip を選択します。

   IAD_ORACLE_HOME/oaam/init

   「**open**」をクリックします。
8. 「**Load**」をクリックします。
9. スナップショット・ファイルが正常にロードされたことを通知するメッセージが表示されます。「**OK**」をクリックしてこのメッセージを了承します。
10. 右上付近にある「**Restore**」をクリックします。
11. ロードが完了するとメッセージが表示されます。「**OK**」をクリックします。

Oracle Adaptive Access Managerと Oracle Access Management Access Managerの統合

この項では、OAAM を Access Manager および Oracle Identity Manager と統合する方法を説明します。OAAM を Access Manager と統合すると、標準の Access Manager ログインではなく OAAM を使用してリソースへのアクセスを検証できます。OAAM でも認証が実行されていますが、それは Access Manager の中のユーザーに対する認証です。

OAAM を Oracle Identity Manager と統合すると、Oracle Identity Manager がユーザー名やパスワードを忘れたユーザーの役に立ちます。

簡易モード用グローバル・パスフレーズの取得

Access Manager のインストール時に、簡易モード通信用のランダムなグローバル・パスフレーズが生成されます。このパスフレーズを取得する方法は次の手順のとおりです。パスフレーズはこの章の後のほうで必要になります。

簡易モード通信用のランダムなグローバル・パスフレーズを取得するには、OAMHOST1 で IAM_ORACLE_HOME/common/bin にある WebLogic Scripting Tool を起動します。wlst シェルに入ったら、次のコマンドを入力して接続します。

```
./wlst.sh

wls:/offline> connect()
```

プロンプトに対して次のように応答します。

```
Please enter your username [weblogic] : weblogic

Please enter your password [weblogic] :COMMON_IDM_PASSWORD

Please enter your server URL [t3://localhost:7001] : t3://IADADMINVHN:7001

wls:/IAMAccessDomain/serverConfig>
```

次のコマンドを入力して、場所を読取り専用の domainRuntime ツリーに変更します。ヘルプを表示するには help(domainRuntime)を使用します。

```
wls:/IAMAccessDomain/domainRuntime>domainRuntime()
```

次のコマンドを入力してグローバル・パスフレーズを表示します。

```
wls:/IAMAccessDomain/domainRuntime> displaySimpleModeGlobalPassphrase()
```

このパスフレーズをメモし、exit コマンドで wlst を終了します。

```
wls:/IAMAccessDomain/domainRuntime> exit()
```

サード・パーティ・アプリケーションとしてのOAAMの登録

簡易セキュリティ・トランスポート・プロトコルを使用するように Access Manager を構成した場合は、OAAM をサード・パーティ・アプリケーションとして登録する必要があります。

OAAM をサード・パーティ・アプリケーションとして登録するには、次の手順を実行します。

1. OAAM キーストアを保持するディレクトリを作成します。このディレクトリを IAD_ASERVER_HOME に配置すると、すべての OAAM ホストでこれを使用できるようになります。

   ```
   mkdir -p SHARED_CONFIG_DIR/keystores
   ```

2. OAMHOST1 で、IAD_ORACLE_HOME/common/bin ディレクトリから WLST シェルを起動します。たとえば、Linux では次のように入力します。

   ```
   ./wlst.sh
   ```

3. 次の wlst の connect コマンドを使用して、WebLogic 管理サーバーに接続します。

   ```
   connect('AdminUser',"AdminUserPassword",t3://hostname:port')
   ```

   次に例を示します。

   ```
   connect("weblogic","admin_password","t3://IADADMINVHN.example.com:7001")
   ```

4. 次に示す registerThirdPartyTAPPartner コマンドを実行します。

   ```
   registerThirdPartyTAPPartner(partnerName = "partnerName", keystoreLocation= "path to
   keystore" , password="keystore password", tapTokenVersion="v2.0",
   tapScheme="TAPScheme", tapRedirectUrl="OAAM loginURL")
   ```

   次に例を示します。

   ```
   registerThirdPartyTAPPartner(partnerName = "OAAMTAPPartner", keystoreLocation=
   "SHARED_CONFIG_DIR/keystores/oaam_keystore.jks" , password="password",
   tapTokenVersion="v2.0", tapScheme="TAPScheme",
   tapRedirectUrl="https://login.example.com/oaam_server/oamLoginPage.jsp")
   ```

   コマンド説明：

   - partnerName は一意の名前です。Access Manager にパートナーが存在する場合は構成が上書きされます。
   - keystoreLocation は、既存のキー・ストアの場所です。指定したディレクトリ・パスが存在しない場合はエラーが発生します。
   - password は、キー・ストアを暗号化するために指定するパスワードです。これは後で必要になるため、覚えておいてください。
   - tapTokenVersion は常に v2.0 です。
   - tapScheme は更新される認証スキームです。
   - tapRedirectUrl はアクセス可能な URL です。アクセスできない場合は登録が失敗し、

Error!Hyperlink reference not valid というメッセージが表示されます。

tapRedirectUrl は次のとおりです。

https://login.example.com/oaam_server/oamLoginPage.jsp

5. WLST を終了します。

   exit()

6. Access Management 管理コンソールにログインします。

7. Access Manager セクションの「**Authentication Schemes**」をクリックします。

   Search Authentication Schemes ページが表示されます。

   Search Name ボックスに TAPScheme と入力して「**Search**」をクリックします。

8. 「**TAPScheme**」をクリックします。

9. Challenge URL が次のように設定されていることを確認します。

   ```
   /oaam_server/oamLoginPage.jsp
   ```

   パラメータ TAPPartnerId=OAAMTAPPartner と SERVER_HOST_ALIAS=OAMSERVER は、チャレンジ・パラメータとしてすでにリストされているはずです。次のチャレンジ・パラメータを追加します。

   ```
   MatchLDAPAttribute=uid
   TAPOverrideResource=https://login.example.com:443/oamTAPAuthenticate
   ```

   注：パラメータ MatchLDAPAttribute の値は、ID ストアで指定した username 属性に設定する必要があります。

10. 「**Apply**」をクリックします。

11. wls_oaam1 と wls_oaam2 を再起動します。

IAMSuiteAgentプロファイルへのエージェント・パスワードの追加

Access Manager をインストールすると、IAMSuiteAgent（WebLogic のセキュリティ・プロバイダ、および対応する Access Manager の 10g WebGate プロファイル）が作成されます。デフォルトではパスワードが設定されていません。OAAM と Access Manager を TAP で統合すると、OAAM から Access Manager に接続するときに IAMSuiteAgent プロファイル(OAAM CLI を使用して OAAM で TAP の統合を設定するときに構成したもの)が使用されますが、この接続にはエージェント・パスワードが必要です。

IAMSuiteAgent プロファイルのエージェント・パスワードを Access Manager で設定する必要があります。このパスワードは複数の場所で使用されるため、これは Access Manager と Oracle Adaptive Access Manager の統合に必要な手順です。パスワードを設定するには、次の手順を実行します。

1. 次の Oracle Access Management コンソールにログインします。
   http://iadadmin.example.com:*IAD_HTTP_PORT*/oamconsole
2. Oracle Access Management コンソールで、ウィンドウの上部にある「**Application Security**」をクリックします。
3. **Application Security** コンソールで、Agents セクションの「**Agents**」をクリックします。WebGates タブがアクティブになっている Search SSO Agents ページが開きます。
4. 表示された Search SSO Agents ページで、検索するエージェント名として IAMSuiteAgent を入力します。
5. 「**Search**」ボタンをクリックして検索を開始します。
6. Search Results 表で **IAMSuiteAgent** を選択し、「**Edit**」をクリックします。
7. IAMSuiteAgent Webgate ページで Access Client Password フィールドにパスワードを指定し、「**Apply**」をクリックして変更を保存します。

検証

OAM Access Tester ツールを使用して、この統合が正常に完了したことを確認します。統合が正常に完了したことを確認するには、次の手順を実行します。

1. 環境で JAVA_HOME が設定されていることを確認します。
2. JAVA_HOME/bin を PATH に追加します。たとえば、次のコマンドを実行します。

   export PATH=$JAVA_HOME/bin:$PATH
3. ディレクトリを次のように変更します。

   IAD_ORACLE_HOME/oam/server/tester

   次のコマンドを使用して、ターミナル・ウィンドウでテスト・ツールを起動します。java -jar oamtest.jar
4. 次の値を使用して接続します。
   - **Primary OAM Host**：OAMHOST1
   - **Port**：5575（*OAM_PROXY_PORT*）
   - **Agent ID**：IAMSuiteAgent
   - **Agent Password**：IAMSuiteAgent プロファイルに割り当てたパスワード
   - **Mode**：AIX プラットフォームの場合は「Open」を選択します。それ以外の場合は「Simple」を選択します。
   - **Global Passphrase**：簡易モードを選択した場合は、「簡易モード用グローバル・パスフレーズの取得」の項で取得した Access Manager のグローバル・パスフレーズを入力します。

「**Connect**」をクリックします。

5. Protected Resource URI セクションは次のように指定します。

   - **Scheme**：http
   - **Host**：IAMSuiteAgent
   - **Port**：空白のままにします。
   - **Resource**：/oamTAPAuthenticate

   「**Validate**」をクリックします。

6. ユーザーID oamadmin と oamadmin のパスワードを指定します。

   「**Authenticate**」をクリックします。認証に成功すれば、統合は正常に完了しています。

OAMHOST2 で同じ検証を実行します。

Access ManagerのOAAMプロパティの設定

oaam_cli.properties ファイルを編集して、Access Manager の OAAM プロパティを設定します。OAMHOST1 上で OAAM プロパティを設定するには、次の手順を実行します。

1. *IAD_ORACLE_HOME*/oaam/cli を一時的な場所にコピーします。次に例を示します。

   cp -r *IAD_ORACLE_HOME*/oaam/cli /u01/oracle/config/oaam

2. ファイル oaam_cli.properties を編集します。このファイルは次のディレクトリにあります。

   /u01/oracle/config/oaam/conf/bharosa_properties

   ファイル内の次のプロパティ値を設定します。

表7：OAAMプロパティ

パラメータ	値
oaam.adminserver.hostname	IADADMINVHN.example.com
oaam.adminserver.port	7001
oaam.adminserver.username	weblogic
oaam.adminserver.password	WebLogic ユーザーのパスワード
oaam.db.url	OAAM データベースの DBC URL。形式： jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCP)(HOST=IAMDBSCAN) (PORT=1521))(CONNECT_DATA=(SERVICE_NAME=oaamedg.example.com)))

oaam.uio.oam.tap.keystoreFile	「サード・パーティ・アプリケーションとしての OAAM の登録」の項で作成したキーストアの場所。次に例を示します。 IAD_ASERVER_HOME/keystores/oaam_keystore.jks
oaam.uio.oam.tap.partnername	OAAMTAPPartner
oaam.uio.oam.host	OAMHOST1
oaam.uio.oam.port	Access Manager サーバー・プロキシ・ポート、OAM_PROXY_PORT。次に例を示します。5575.
oaam.uio.oam.webgate_id	IAMSuiteAgent
oaam.uio.oam.secondary.host	OAMHOST2
oaam.uio.oam.secondary.host.port	2 つ目の Access Manager サーバーの Access Manager サーバー・プロキシ・ポート、OAM_PROXY_PORT。次に例を示します。5575.
oaam.uio.oam.security.mode	これは、Access Manager で使用しているトランスポート・セキュリティ・モードにより異なります。これが AIX ビルドの場合、値は 1（Open）になり、それ以外の場合は 2（Simple）になります。
oam.uio.oam.rootcertificate.keystore.filepath	ルート証明書用に生成されたキーストア・ファイルの場所。IAD_ASERVER_HOME/output/webgate-ssl/oamclient-truststore.jks これが必要なのは、セキュリティ・モードが 2（Simple）および 3（Cert）の場合のみです。
oam.uio.oam.privatekeycertificate.keystore.filepath	秘密鍵用に生成されたキーストア・ファイルの場所。IAD_ASERVER_HOME/output/webgate-ssl/oamclient-keystore.jks これが必要なのは、セキュリティ・モードが 2（Simple）および 3（Cert）の場合です。

ファイルを保存します。

3. コマンド setupOAMTapIntegration.sh を発行して OAAM CLI ツールを実行します。このコマンドは次のディレクトリにあります。

   /u01/oracle/config/oaam 次のように設定します。

   ORACLE_MW_HOME を IAD_MW_HOME に設定します。

   JAVA_HOME を JAVA_HOME に設定します。

   WLS_HOME を IAD_MW_HOME/wlserver_10.3 に設定します。

   APP_SERVER_TYPE を weblogic に設定します。

   次のコマンドを実行します。

   ```
   chmod +x /u01/oracle/config/oaam/setupOAMTapIntegration.sh

   /u01/oracle/config/oaam/setupOAMTapIntegration.sh \

   /u01/oracle/config/oaam/conf/bharosa_properties/oaam_cli.properties
   ```

   コマンドを実行すると、次の情報の入力を求められます。

- » OAAM 管理サーバーのユーザー名：weblogic_idm
- » OAAM 管理サーバーのパスワード：weblogic_idm アカウントのパスワード
- » OAAM DB のユーザー名：EDG_OAAM

» OAAM DB のパスワード：OAAM データベース・ユーザーのパスワード。

» CSF に格納する OAM Web ゲートの資格証明：WebGate のパスワード（COMMON_IDM_PASSWORD）を入力します。

» OAM TAP キー・ストア・ファイルのパスワード：「サード・パーティ・アプリケーションとしての OAAM の登録」の項で、サード・パーティ・アプリケーションとして OAAM を登録したときに割り当てたパスワード（COMMON_IDM_PASSWORD）。

» OAM 秘密鍵証明書キー・ストア・ファイルのパスワード：「簡易モード用グローバル・パスフレーズの取得」の項で取得した Access Manager のグローバル・パスフレーズ。

» OAM グローバル・パスフレーズ：OAAM 簡易セキュリティ・モデルを使用している場合は、「簡易モード用グローバル・パスフレーズの取得」の項で取得した値。

テスト・リソースの作成

この検証を実行するには、まずテスト・リソースを作成します。

注：Oracle Traffic Director を使用している場合は、静的な HTML ページを作成する手順を省略してもかまいません。Oracle HTTP Server とは異なり、静的な HTML ページを表示するのは困難な場合がありますが、OAAM をテストするためにこのリソースを作成します。

WEBHOST1 と WEBHOST2 で、テスト・ページ oaam_sso.html を作成します。もっとも簡単な方法は、WEB_ORACLE_INSTANCE/config/OHS/component/htdocs ディレクトリで、次の内容の oaam_sso.html ファイルを作成する方法です。

```
<html>
<body>
<center>
<p>
<h2>
OAAM によって保護されるリソース
</h2>
</p>
</center>
</body>
</html>
```

Oracle Adaptive Acces s Managerポリシーの作成

IAMSuite アプリケーション・ドメインに、OAAM によって保護されるリソース用のグループを作成します。

1. 以前に作成した oamadmin アカウントを使用して Access Management コンソールにログインします。
2. 「**Application Domains**」をクリックします。
3. 「**Search**」をクリックします。
4. 「**IAM Suite**」をクリックします。IAM Suite Domain ページが表示されます。
5. 「**Authentication Policies**」タブをクリックします。
6. 「**Create Authentication Policy**」をクリックして次の情報を入力します。

   Name：OAAM Protected Resources

   Description：Resources protected by OAAM

   Authentication Scheme：TAPScheme

   「**Apply**」をクリックします。
7. 手順 1 から 7 を繰り返します。ただし、「Create Authentication Policy」をクリックした後は次の値を入力します。

   Name：LDAP Protected Resource

   Description：Resources protected by LDAPScheme

   Authentication Scheme：LDAPScheme

Access Managerでのリソースの作成

現在は保護すべきものがあるため、Access Manager でリソースを作成して、先ほど作成したポリシー・グループのいずれかに割り当てる必要があります。

1. Access Management コンソールにログインします。
2. 「**Application Domains**」をクリックします。
3. 「**Search**」をクリックします。
4. 「**IAM Suite**」をクリックします。
5. 「**Resources**」タブをクリックします。

6. 「**Create**」をクリックして次の情報を入力します。

   Type：http

   Description：OAAM Test Page

   Host Identifier：IAMSuiteAgent

   Resource URL：/oaam_sso.html

   Protection Level：Protected

   Authentication Policy：OAAM Protected Resources

   Authorization Policy：Protected Resource Policy

   「**Apply**」をクリックします。

Oracle Adaptive Access Managerの検証

URL: https://login.example.com:443/oaam_sso.html を使用して、保護されているリソースにアクセスします。登録およびチャレンジのために OAAM にリダイレクトされます。Access Manager のログイン・ページの代わりに OAAM のログイン・ページが表示されます。

oamadmin などの認可された Access Manager ユーザーを使用してログインします。ログインすると、oaam で保護されているリソースが表示されます。

注：

Oracle Traffic Director を使用している場合は、OAAM 認証を使用すると、"page not found"というエラーが表示されます。認証テスト用のポリシーを作成しただけで、oaam_sso.html ページは作成していないため、このようになります。

Oracle HTTP Server があれば、単純な HTML ページは簡単に作成できます。これは Oracle Traffic Director でも可能ですが、手間がかかります。リソースにアクセスしようとしたときに OAAM チャレンジが表示され、この検証をパスすれば、OAAM の検証としてはそれで十分です。簡単な HTML ページが最後に表示されるかどうかは重要ではなく、それでテストが無効になるわけでもありません。

TAPリソースのLDAPポリシーへの移動

1. 以前に作成した oamadmin アカウントを使用して Access Management コンソールにログインします。
2. Access Manager セクションの「**Application Domains**」をクリックします。
3. **Application Domains** Search 画面が表示されます。
4. 「**Search**」をクリックします。
5. 「**IAM Suite**」をクリックして IAM Suite Domain ページを開きます。
6. 「**Authentication Policies**」サブタブをクリックします。

7. 「**Protected Higher Level Policy**」をクリックします。
8. 「**Resources**」サブタブをクリックします。
9. Resources ウィンドウで「**/oamTAPAuthenticate**」をクリックします。
10. 「**Delete**」をクリックします。
11. 「**Apply**」をクリックします。
12. Access Manager セクションの「**Application Domains**」をクリックします。
13. Application Domains Search 画面が表示されます。

    「**Search**」をクリックします。
14. 「**IAM Suite**」をクリックして IAM Suite Domain ページを開きます。「Authentication Policies」サブタブをクリックします。
15. 「LDAP Protected Resources」をクリックします。

    Browse タブの下のツールバーで「**Open**」をクリックします。
16. Resources ウィンドウで「**Add**」をクリックします。

    Search ボックスが表示されたら次のように入力します。

    Resource URL：/oamTAPAuthenticate

    「**Search**」をクリックします。
17. 検索結果から「/oamTAPAuthenticate」をクリックします。
18. 「**Add Selected**」をクリックします。
19. リソース「/oamTAPAuthenticate」を選択します。
20. 「**Apply**」をクリックします。

Oracle Adaptive Access ManagerとOracle Identity Managerの統合

OAAM には広範なチャレンジ質問が用意されています。これには次のような機能があります。

» 必要に応じて認証の前後に一連の質問でユーザーの身元を確認する。

» 質問をイメージとして提示し、多様な入力装置からの回答を求める。

» 次々に質問する（正しい答えが入力された場合のみ後続の質問を表示する）。

Oracle Identity Manager にも基本的なチャレンジ質問機能があります。これによりユーザーは、パスワードを忘れた場合に、一連の構成可能な質問に答え、パスワードを再設定できます。OAAM とは異なり、Oracle Identity Manager には豊富なパスワード検証機能も用意されており、これにより、簡単な属性に加えて、所有するアカウントに基づいてポリシーを設定できます。

Identity and Access Management のデプロイメントでは、チャレンジ質問を 1 セットのみ登録し、1 セットのパスワード・ポリシーを使用することをお薦めします。OAAM を Oracle Identity Manager と統合することにより、OAAM ではチャレンジ質問を処理し、Oracle Identity Manager ではパスワードの検証、保管および伝播を処理することが可能となります。これにより、OAAM の不正防止機能と Oracle Identity Manager によるパスワード検証を同時に使用することができます。OAAM を Oracle Identity Manager と統合すると、Oracle Identity Manager がユーザー名やパスワードを忘れたユーザーの役に立ちます。

CSFでのOracle Identity Manager暗号化鍵の構成

1. ドメイン IAMAccessDomain 用の Oracle Enterprise Manager Fusion Middleware Control に移動します。
2. WebLogic 管理者アカウント（weblogic_idm など）を使用してログインします。左側ペインのナビゲーション・ツリーで「WebLogic Domain」アイコンを展開します。
3. 「**IAMAccessDomain**」を選択し、右クリックしてメニュー・オプション「**Security**」を選択して、サブメニューにあるオプション「**Credentials**」を選択します。
4. 「**oaam**」をクリックしてマップを選択し、「**Create Key**」をクリックします。

   ポップアップ・ウィンドウで、Select Map が **oaam** になっていることを確認します。

   次のように入力します。

   Key Name：oim.credentials

   Type：Password

   UserName：xelsysadm

   Password：xelsysadm アカウントのパスワード、COMMON_IDM_PASSWORD

   「**OK**」をクリックして秘密鍵を資格証明ストア・フレームワークに保存します。

Oracle Identity ManagerとOracle Adaptive Access Manager間のクロス・ドメインの信頼の構成

Oracle Adaptive Access Manager をデプロイする際に、Oracle Identity Manager と Oracle Adaptive Access Manager が別々のドメインにある場合は、クロス・ドメインの信頼を構成する必要があります。

次の手順に従って、ドメイン IAMAccessDomain でクロス・ドメインの信頼を構成します。

1. IAMAccessDomain の WebLogic 管理コンソールにログインします。
2. 「**Lock and Edit**」をクリックします。
3. Domain Structure で「**IAMAccessDomain**」をクリックし、「**Security**」タブを選択します。
4. 「**Advanced**」セクションを展開します。

5. 「**Cross domain security enabled**」を選択します。
6. クロス・ドメインの信頼の確認に使用するパスワードを選択し、**Credential** フィールドと **Confirm Credential** フィールドに入力します。
7. 「**Save**」をクリックします。
8. 「**Activate Changes**」をクリックします。

次の手順に従って、ドメイン IAMGovernanceDomain でクロス・ドメインの信頼を構成します。

1. IAMGovernanceDomain の WebLogic 管理コンソールにログインします。
2. 「**Lock and Edit**」をクリックします。
3. Domain Structure で「**IAMGovernanceDomain**」をクリックし、「Security」タブを選択します。
4. 「**Advanced**」セクションを展開します。
5. 「**Cross domain security enabled**」を選択します。
6. IAMAccessDomain の Credential フィールドに入力したパスワードを **Credential** フィールドと **Confirm Credential** フィールドに入力します。
7. 「**Save**」をクリックします。
8. 「**Activate Changes**」をクリックします。

Oracle Identity Manager用のOracle Adaptive Access Managerプロパティの設定

OAAM 管理コンソールに移動します。

「LDAP での OAAM ユーザーとグループの作成」の項で作成した oaamadmin アカウントを使用してログインします。以下の手順を実行します。

1. ナビゲーション・ツリーで、Environment 見出しの下の「**Properties**」をクリックし、「**Open**」をクリックします。Properties search ページが表示されます。
2. プロパティ値を設定するために、**Name** フィールドに名前を入力して「**Search**」をクリックします。検索結果ウィンドウに現在の値が表示されます。
3. エントリをクリックします。Value フィールドが表示されます。新しい値を入力して「**Save**」をクリックします。

4. 次のプロパティを設定して、Oracle Adaptive Access Manager を Oracle Identity Manager に統合できるようにします。

   - **bharosa.uio.default.user.management.provider.classname**：com.bharosa.vcrypt.services.OAAMUserMgmtOIM
   - **bharosa.uio.default.signon.links.enum.selfregistration.url**：https://login.example.com:443/identity/faces/register?&backUrl=https://login.example.com:443/identity
   - **bharosa.uio.default.signon.links.enum.trackregistration.enabled**：true
   - **bharosa.uio.default.signon.links.enum.selfregistration.enabled**：true
   - **bharosa.uio.default.signon.links.enum.trackregistration.url**：

     https://login.example.com:443/identity/faces/trackregistration?&backUrl=https://login.example.com:443/identity
   - **oaam.oim.url**：t3://oimhost1vhn.example.com:14000,oimhost2vhn.example.com:14000

OAAM用のOracle Identity Managerプロパティの設定

1. Oracle Identity Manager システム管理コンソールにログインします。
2. System Configuration 見出しの下の「Configuration Properties」をクリックします。Configuration Properties ウィンドウが開きます。
3. Search System Properties で「Search」をクリックします。
4. 表示されたプロパティをそれぞれクリックして、「Edit」を選択します。次に示すとおりに各プロパティの値を設定し、「Save」をクリックして値を保存します。

   注：

   プロパティ名は keyword 列に表示されます。

   - **OIM.DisableChallengeQuestions**：TRUE
   - **OIM.ChangePasswordURL**：https://login.example.com:443/oaam_server/oimChangePassword.jsp
   - **OIM.ChallengeQuestionModificationURL**：https://login.example.com:443/oaam_server/oimResetChallengeQuestions.jsp

IAMAccessDomainおよびIAMGovernanceDomainの再起動

次の管理サーバーと管理対象サーバーを再起動します。

» WebLogic 管理サーバー

» wls_oam1 および wls_oam2

» wls_oim1 および wls_oim2

» wls_oaam1 および wls_oaam2

Oracle Adaptive Access Managerによる保護を受けるためのドメイン変更

あるリソースを OAAM で保護する必要がある場合は、「Access Manager でのリソースの作成」の項で作成したによって保護されるリソースの認証ポリシーを追加すると可能になります。

次の手順を実行すると、あらゆるものに OAAM 認証を使用できるようになります。

1. Access Management コンソールにログインします。
2. 「**Application Domains**」をクリックします。
3. 「**Search**」をクリックします。
4. 「**IAM Suite**」をクリックします。
5. 「**Authentication Policies**」タブをクリックします。
6. ポリシー**Protected HigherLevel Policy** をクリックします。
7. **Authentication Scheme** の値を TAPScheme に変更します。
8. 「**Apply**」をクリックします。

OAAMとOracle Identity Managerの統合の検証

前の説明で作成したテスト・ページ（例：https://login.example.com/oaam_sso.html）にアクセスします。OAAM のログイン・ページが表示されます。リンク「Registration」または「Track Registration」をクリックします。正しく統合されている場合は OIM に転送されます。

注：バグがあるため、OAAM サーバーを両方とも実行している場合は、OAAM 認証イメージが正しくレンダリングされません。この問題を回避するには、1 つの OAAM 管理対象サーバーのみを実行する必要があります。この問題が発生するのは、管理対象サーバーで MW_HOME が共有されている場合のみです。

Oracle Identity ManagerとOAAMの統合の検証

Oracle Identity Manager が OAAM と統合されていることを検証するには、次の手順を実行します。

Oracle Identity Manager のセルフサービス・コンソールに xelsysadm ユーザーでログインします。

チャレンジ質問と OAAM 固有のセキュリティ画像の設定を求めるプロンプトが表示されます。

アプリケーション層の構成のバックアップ

結論

以上の手順に沿って構成すれば、一般的な企業での使用に適した ID 管理アプリケーションを構築できます。

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

海外からのお問い合わせ窓口
電話：+1.650.506.7000
ファクシミリ：+1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services

ホワイト・ペーパーOracle Adaptive Access Manager による Oracle Identity and Access Management エンタープライズ・デプロイメントの拡張 2016 年 7 月
著者：Michael Rhys
共著者：Firdaus Fraz