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 Privileged Account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

免責事項

以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することをコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。オラクルの製品に関して記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。

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 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 Privileged Account Manager を使ってさらに拡張する方法について説明します。

Oracle Privileged Account Manager（OPAM）は、Linux/Unix の'root'や Oracle データベースの'sys'などの特権アカウントのパスワードへのアクセス権の生成、プロビジョニングおよび管理のために設計されたセキュアなパスワード管理ソリューションです。これにより、通常は特権アカウントの資格証明を共有するユーザーに対する監査が可能になり、アカウンタビリティが確立されます。OPAM が Oracle Identity Manager および Oracle Identity Analytics とともに形成する完全な Oracle Identity Governance プラットフォームでは、一般ユーザーおよび特権ユーザーを対象とする一元化されたガバナンス、完全な監査、ユーザーの一般アカウントおよび共有アカウントのレポートおよびサーティフィケーション、そしてリクエスト、承認から認定および使用追跡にいたるライフサイクル管理が提供されます。Oracle Privileged Account Manager は、セキュリティを強化し、コンプライアンスを大幅に向上させます。このドキュメントでは、すでにプロビジョニングされている Identity and Access Management ソリューションを Oracle Privileged Account Manager を使って拡張する方法を説明します。既存のデプロイメントの拡張は、エンタープライズ・デプロイメント・ガイドのベスト・プラクティスに沿って実施します。

このドキュメントは、必ずエンタープライズ・デプロイメント・ガイドの手順を完了してから使用してください。このガイドでは、従来の実装と Exalogic の実装の両方に関する手順を説明します。

注：パッチ・マネージャを使用して OPAM にパッチを適用することはできなくなります。

OPAM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。

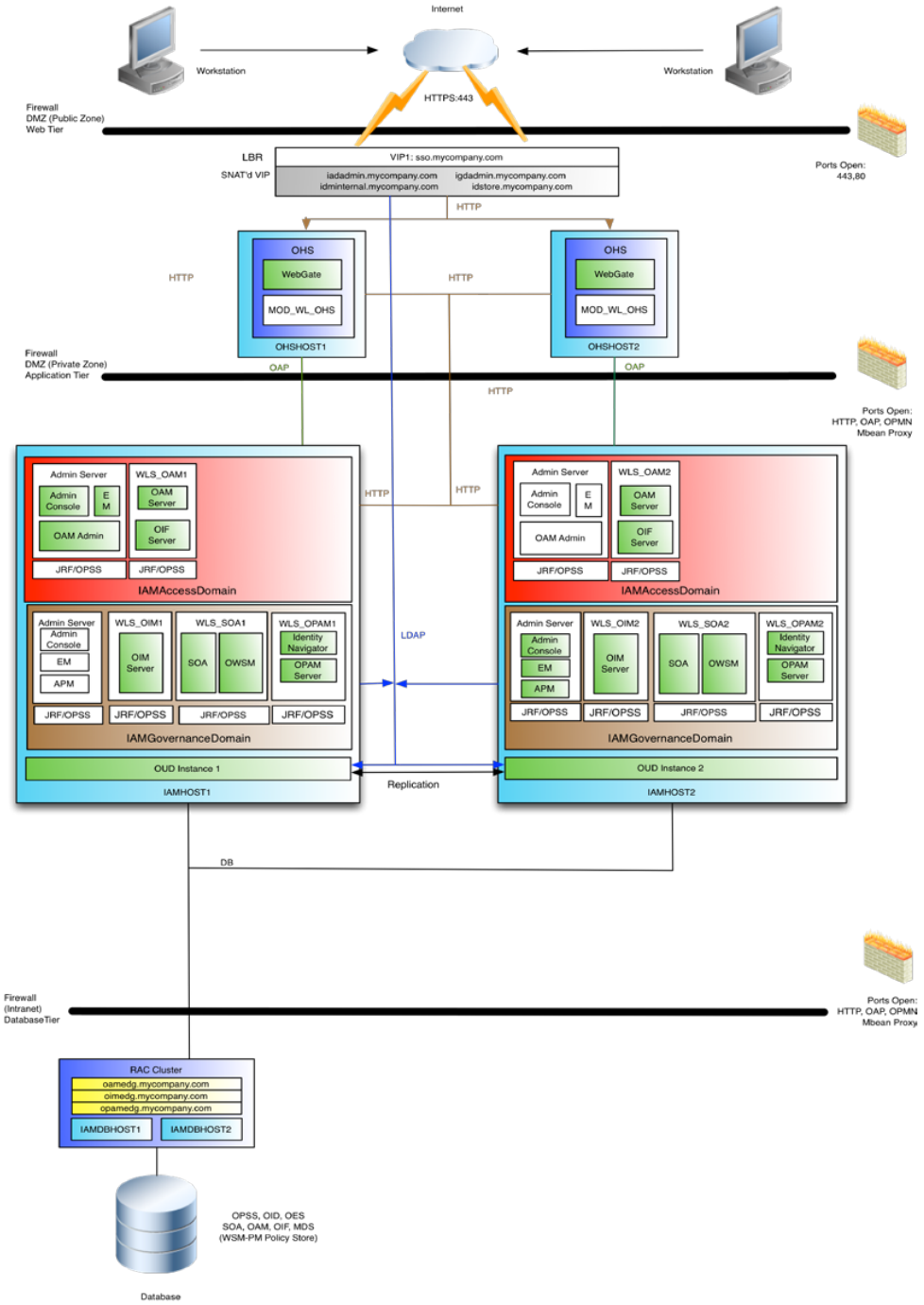

図1：OPAMのデプロイメント・トポロジ

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 IAMHOST1 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
アクセス管理サーバー	3GB	1300	180
ガバナンス管理サーバー	3GB	2100	100
WLS_SOA	2GB	1400	210
WLS_OIM	2GB	1400	190
WLS_BI	2GB	900	100
WLS_OAM	1GB	900	170
WLS_AMA	2GB	1200	160
WLS_MSM	2GB	900	120
ノード・マネージャ	268MB	300	20

概要

このプロセスは次の手順で構成されています。

» 必要な前提条件に適合していることの確認

» LDAP での OPAM 管理ユーザーとグループの作成

» OPAM による IAMGovernanceDomain の拡張

» OPAM スキーマの暗号化

» OPAM の構成

» OPAM SSL の無効化

» JDK 信頼ストアへのロードバランサ証明書の追加

» 起動および停止スクリプトへの OPAM システムの追加

» OPAM と Web 層の統合

» OPAM クラスタを使用するために必要な Oracle Identity Navigator の構成

» ターゲットを管理するために必要な OPAM の構成

» OPAM と OIM の統合

前提条件

ドメインを拡張して Oracle Privileged Account Manager（OPAM）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

IAMDB を使用していない場合は、OPAM のデータを保持するために必要な可用性の高いデータベースを作成します。『Oracle Fusion Middleware Repository Creation Utility』の説明に従って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 OPAM のデータ・オブジェクトを事前にシードします。スキーマは Oracle Privileged Account Manager を選択します。

このドキュメントでは、OPAM スキーマ名を"*igdedg_opam*"とし、データベース・サービス名は IAMGovernanceDomain 用に作成したサービスと同じ'*IGDEDG.EXAMPLE.COM*'とします。

なお、データベースでは透過的データ暗号化を有効にすることを強くお勧めします。このドキュメントでは、透過的データ暗号化が有効化されているものとします。

データベースでのOPAMスキーマの暗号化

Oracle Privileged Account Manager を使用するには、OPAM スキーマ内の情報を暗号化する必要があります。そのためには、『Oracle Advanced Security 管理者ガイド』の説明に従って、データベースで透過的暗号化（TDE）が使用されるように構成する必要があります。

http://www.oracle.com/pls/topic/lookup?ctx=idm111220&id=ASOAG9522

TDE を有効にしたら、OPAM スキーマを暗号化する必要があります。そのために、ディレクトリ *IAM_ORACLE_HOME*/opam/sql にある SQL スクリプト opamxencrypt.sql を実行します。

次に例を示します。

sqlplus EDGIGD_OPAM/*password*@opamxencrypt.sql コマンド説明：

EDGIGD_OPAM は OPAM スキーマのユーザー名です。

注：このコマンドは sqlplus がインストールされているホストで実行する必要がありますが、通常はデータベース・ホスト自体が該当します。この使用例では、コマンドを実行する前にデータベース・マシンにファイルをコピーします。

LDAPでのOPAMユーザーとグループの作成

次の要領で OPAM ユーザーとグループを作成します。

構成ファイルの作成

次の内容の構成ファイルを作成します。

```
# Common
IDSTORE_HOST: idstore.example.com IDSTORE_PORT: 1389
IDSTORE_ADMIN_PORT: 4444
IDSTORE_BINDDN: cn=oudadmin
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_APMUSER: opamadmin
```

コマンド説明：

なお、イタリック体の値は『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』に定義されているドキュメント変数です。

» IDSTORE_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。これは、ディレクトリ・インスタンスのロードバランサ・エントリ・ポイントを指している必要があります。例：idstore.example.com と 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 は、ID ストア・ディレクトリ内の管理ユーザーです。例：cn=oudadmin

» 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。これは、定義済みの *REALM_DN* と同じです。例：cn=Users,dc=example,dc=com

» 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。これは cn=Groups と *REALM_DN* を組み合わせたものです。例：cn=Groups,dc=example,dc=com

» 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。これは cn=Users と定義済みの REALM_DN を組み合わせたものです。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_OPAMUSER は、Oracle Privileged Account Manager の管理者として作成するユーザーの名前です。

idmConfigToolによるユーザーおよびグループの作成

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 ストアをシードするには、OIMHOST1 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 *IGD_MW_HOME* に設定します。

ORACLE_HOME を *IGD_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 IGD_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=APM input_file=configfile
```

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

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。

OPAMでのドメイン拡張

OIMHOST1 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。

```
IGD_MW_HOME/oracle_common/common/bin/config.sh
```

注：次の手順を実行する前にドメインを停止する必要があります。

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：*IGD_ASERVER_HOME*（IAMGovernanceDomain）

   「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 Privileged Account Manager

   「**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。

   OPAM Schema

   「**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、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。

   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。

   または

   - 「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 DB-SCAN.EXAMPLE.COM:1521
```

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。

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。例：DBHOST1 - VIP.example.com（ポート 1521）と DBHOST2 - VIP.example.com（ポート 1521）（1521 は *DB_LSNR_PORT* です）

```
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 Oracle Notification Service 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。

Schema Name：OPAM Schema

Service Name：igdedg.us.oracle.com

Schema Owner：EDGIGD_OPAM

Password：上記アカウントのパスワード

「**Next**」をクリックします。

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、構成済みコンポーネントのエントリとして Identity Manager などが表示されます。さらに、2 つの新しい OPAM 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（opam_server1）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、新しい管理対象サーバーを追加します。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。

» 下の表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ます。

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
opam_server	wls_opam1	OIMHOST1	18101	18102	有効化
	wls_opam2	OIMHOST2	18101	18102	有効化

「**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 opam_cluster の値を入力します。

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
Opam_cluster	unicast	N/A	N/A	N/A

他のフィールドはすべてデフォルト設定のままにします。

「**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。

クラスタ	サーバー
opam_server	wls_opam1
	wls_opam2

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。

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。

    OIMHOST1：wls_opam1

    OIMHOST2：wls_opam2、

    「**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：

    » デプロイメントを実行するとマシンが作成されます。

    » 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

    「**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。

    OIMHOST1 上での管理サーバーの再起動

    OIMHOST1 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、OIMHOST1 および OIMHOST2 の管理対象サーバーのディレクトリに構成を伝播する必要があります。

    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 OIMHOST1 の IAMGovernanceDomain でドメインを圧縮し、次に OIMHOST1 および OIMHOST2 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。1.pack ユーティリティを OIMHOST1 の *ORACLE_COMMON_HOME*/common/bin/ から起動します。

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

    これにより、iam_domain.jar という名前のファイルが作成されます。このファイルを OIMHOST2 にコピーします。

    OIMHOST1 と OIMHOST2 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。

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.

ノード・マネージャのSSLに合わせた管理対象サーバーの構成

標準のエンタープライズ・デプロイメントのノード・マネージャは、SSL を使用して管理対象サーバーと通信するように構成されています。OPAM の新しい管理対象サーバーが 2 つあるため、これらも SSL を有効にする必要があります。キーストアは自動ツールによって作成されるため、管理対象サーバーのみ更新する必要があります。この操作を行うには、次の手順を実行します。

1. URL http://igdadmin.us.oracle.com/console を使用して、weblogic_idm ユーザーで WebLogic 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. 「Environment」→「Servers」の順にナビゲートして、WebLogic server の Summary ページを表示します。
4. 新たに作成した OPAM サーバーの 1 つ（例：wls_opam1）をクリックします。
5. 「Configuration」→「Keystores」を選択します。
6. Keystores フィールドの横にある「**change**」をクリックし、秘密鍵/デジタル証明書のペアと信頼できる CA ストアを保存および管理するための「**Custom Identity and Custom Trust**」メソッドを選択します。「**Save**」をクリックします。
7. Identity セクションで、ID キーストアの属性を定義します。
   - **Custom Identity Keystore**：ID キーストアの完全修飾パス：*`SHARED_CONFIG_DIR`*`/keystores/appIdentityKeyStore.jks`
   - **Custom Identity Keystore Type**：空白のままにします。デフォルトで JKS に設定されます。
   - **Custom Identity Keystore Passphrase/Confirmation**：キーストアのパスワード。これは、プロビジョニング・プロセスの一部として提供される COMMON_IAM_PASSWORD です。
8. Trust セクションで、信頼キーストアのプロパティを定義します。
   - **Custom Trust Keystore：信頼キーストアの完全修飾パス**：*SHARED_CONFIG_DIR*/keystores/appTrustKeyStore-oimhost1.example.com.jks

     注：ホスト名 oimhost1 は、使用している環境に該当する値です。
   - **Custom Trust Keystore Type**：空白のままにします。デフォルトで JKS に設定されます。
   - **Custom Trust Keystore Passphrase**：キーストアのパスワード。これは、プロビジョニング・プロセスの一部として提供される *COMMON_IAM_PASSWORD* です。
9. 「**Save**」をクリックします。

10. 「Configuration」→「SSL」を選択します。
11. **Private Key Alias** フィールドに、管理対象サーバーがリスニングするホスト名で使用したエイリアスを入力します。たとえば、次のとおりです。
    - WLS_OPAM1 には appIdentity-oimhost1.example.com を使用します。
    - WLS_OPAM2 には、appIdentity-oimhost2.example.com を使用します。

    使用している環境のホストおよびドメインに置き換えてください。
12. **Private Key Passphrase** フィールドと **Confirm Private Key Passphrase** フィールドに、プロビジョニング・プロセスの一部として提供される *COMMON_IAM_PASSWORD* を入力します。
13. 「**Save**」をクリックします。
14. ページの「**Advanced**」セクションを開きます。
15. host name verification を **Bea Hostname Verifier** に設定します。
16. 「**Save**」をクリックします。
17. 管理コンソールの Change Center で「**Activate Changes**」をクリックして、変更を有効にします。

注：テスト用証明書を使用していて、証明書のホストがサイト名と一致しない場合は、手順 15 で host name verification を none に設定します。

OPAMの構成

OPAM 管理対象サーバーを起動する前に、OPAM の初期構成をいくつか実行する必要があります。構成といっても、ディレクトリ IAM_ORACLE_HOME/opam/bin にあるスクリプト opam-config.sh を実行するだけです。

このコマンドを実行するには、次のコマンドを実行します。

set ORACLE_HOME to IAM_ORACLE_HOME

set ANT_HOME to IGD_MW_HOME/modules/org.apache.ant_1.7.1

set JAVA_HOME to JAVA_HOME

set ANT_OPTS to '-Xmx512M -XX:MaxPermSize=512m'

```
cd IAM_ORACLE_HOME/opam/bin
./opam-config.sh
```

プロンプトが表示されたら、次の値を入力します。

Oracle Weblogic の管理ユーザー名：weblogic

Oracle WebLogic の管理パスワード：*IAM_COMMON_PASSWORD*

Oracle WebLogic 管理サーバーの URL：t3://igdadminvhn.example.com:7101

Oracle WebLogic のドメイン名：IAMGovernanceDomain

Oracle Middleware のホーム：IGD_MW_HOME

WebLogic 管理サーバーを再起動します。

SSLの無効化

デフォルトでは、Oracle Privileged Account Manager と Web サーバーの通信に SSL が使用されます。エンタープライズ・デプロイメントでは、SSL はロードバランサにオフロードされるため、Oracle HTTP Server と OPAM 管理対象サーバーの通信には SSL 以外（http）を使用する必要があります。ロードバランサとクライアントとの間のトラフィックはロードバランサで処理されるため、この部分は引き続き SSL が有効になります。

OPAM の SSL を無効にするには、次の手順を実行します。

1. opam という名前のディレクトリを共有ストレージ上に作成します。次に例を示します。

```
mkdir SHARED_CONFIG_DIR/opam
```

2. 次のコンテンツを使用して、このディレクトリに plan.xml というファイルを作成します。

```
<?xml version='1.0' encoding='UTF-8'?>
<deployment-plan xmlns="http://xmlns.oracle.com/weblogic/deployment-plan"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://xmlns.oracle.com/weblogic/deployment-plan
        http://xmlns.oracle.com/weblogic/deployment-plan/1.0/deployment-
        plan.xsd" global- variables="false">
  <application-name>opam</application-name>
  <variable-definition>
    <variable>
      <name>TransportGuarantee_type</name>
      <value>NONE</value>
    </variable>
  </variable-definition>

  <module-override>
    <module-name>opam.war</module-name>
    <module-type>war</module-type>
    <module-descriptor external="false">
      <root-element>web-app</root-element>
      <uri>WEB-INF/web.xml</uri>
      <variable-assignment>
         <name>TransportGuarantee_type</name>
         <xpath>/web-app/security-constraint/user-data-
         constraint/transport-guarantee</xpath>
      </variable-assignment>
    </module-descriptor>
  </module-override>

  <config-root>/u01/oracle/config/opam</config-root>
</deployment-plan>
```

ファイルを保存します。

3. 次の URL を使用して IAMGovernanceDomain の Weblogic コンソールにログインします。

   http://igdadmin.us.oracle.com/console

4. Domain Structure メニューの「**Deployments**」をクリックします。デプロイメントの一覧が表示されます。
5. デプロイメントの一覧から OPAM（バージョン）を選択します（名前をクリックするのではなく、隣にあるチェック・ボックスをチェックします）。
6. 「Lock & Edit」をクリックします。
7. 「**Update**」をクリックします。
8. Deployment Plan Path の隣にある「**Change Path**」をクリックします。
9. パスを、前に作成したデプロイメント・ファイルに設定します。次に例を示します。SHARED_CONFIG_DIR/opam/plan.xml
10. 「**Next**」をクリックします。
11. 「Redeploy this application using the following deployment files」を選択します。
12. 「**Next**」をクリックします。
13. 「**Finish**」をクリックします。
14. 「Activate Changes」をクリックします。
15. 管理サーバーおよび実行中のすべての OPAM 管理対象サーバーを再起動します。

信頼ストアへのロードバランサ証明書の追加

Oracle Privileged Account Manager を使用するには、ロードバランサで使用される SSL 証明書を、OPAM で使用される JDK の信頼できる証明書に追加する必要があります。この操作を行うには、次の手順を実行します。

ロードバランサからの証明書の取得

証明書を取得するもっとも簡単な方法は、インターネット　ブラウザから保存するやり方です。Firefox を使用する場合の手順を次に示します。Oracle Privileged Account Manager サーバーの CA 証明書を取得するには、次の手順を実行します。

Oracle Privileged Account Manager サーバーの Web サービスにブラウザから接続します。
https://sso.example.com

Firefox ブラウザを使用する場合の例を示します。

1. ブラウザのアドレス・バーにあるロック・アイコンをクリックします。
2. 情報ダイアログが表示されたら、「**詳細を表示**」をクリックします。
3. ページ情報ダイアログで「**証明書を表示**」をクリックします。
4. 証明書ビューア・ダイアログで、「詳細」タブを選択して証明書の階層を表示します。

5. 証明書の階層リストの最初（root）にある証明書を選択して、「**エクスポート**」をクリックします。
6. 証明書をファイルに保存ダイアログが表示されたら、ファイルを保存するディレクトリにナビゲートします。例：`/tmp/opam.pem`。
7. 「ファイルの種類」メニューから「**X.509 証明書 (PEM)**」を選択し、ファイル名として **`sso.pem`** を入力して「**保存**」をクリックします。
8. ブラウザを使用して Web サイトにアクセスするのが初めての場合は、代わりに次の手順を使用できます。
9. cert exception が表示されたら、「**例外を追加**」をクリックします。
10. 「証明書を取得」をクリックします。
11. 「セキュリティ例外を承認」をクリックします。
12. Firefox で「オプション」→「詳細」→「証明書」→「証明書を表示」にナビゲートします。
13. 「サーバー証明書」をクリックします。
14. 先ほど追加した証明書（例：MyCompany - sso.example.com）を探します。
15. 証明書をクリックします。
16. 「**エクスポート**」をクリックします。
17. 名前（sso.pem）と証明書のエクスポート先を選択します。
18. 証明書を oimhost1 にコピーします。

JDKおよびノード・マネージャの信頼ストアへの証明書のロード

次のコマンドを実行して CA 証明書ファイル（sso.pem）を次の信頼ストアにインポートします。

IGD_MW_HOME Java 信頼ストア

ノード・マネージャの信頼ストア

Oracle Identity Manager が稼働しているサーバー上でこの操作を実行するには、次のコマンドを実行します。

set JAVA_HOME to *IGD_MW_HOME*/jdk6

set PATH to include JAVA_HOME/bin

```
keytool -importcert -file Path_to_cert/sso.pem -trustcacerts -keystore
$JAVA_HOME/jre/lib/security/cacerts

keytool -importcert -file Path_to_cert/sso.pem -trustcacerts -keystore
SHARED_CONFIG_DIR/keystores/appTrustKeyStore-oimhost1vhn.example.com.jks

keytool -importcert -file Path_to_cert/sso.pem -trustcacerts -keystore
SHARED_CONFIG_DIR/keystores/appTrustKeyStore-oimhost2vhn.example.com.jks

keytool -importcert -file Path_to_cert/sso.pem -trustcacerts -keystore
SHARED_CONFIG_DIR/keystores/appTrustKeyStore-oimhost1.example.com.jks
```

JAVA_HOME は *IGD_MW_HOME*/jdk6 に設定します。

入力を求めるプロンプトが表示されるので、キーストアのパスワード、JDK のデフォルト・パスワード（changeit）およびノード・マネージャのキーストアの *COMMON_IAM_PASSWORD* を入力します。証明書が有効であることも確認します。

注：OIM サーバーに割り当てた仮想ホストの名前は oimhost1vhn と oimhost2vhn になり、OPAM サーバーが稼働しているホストの名前は oimhost1 と oimhost2 になります。

起動および停止スクリプトへのOPAM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。ドメインに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各 OPAM 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。

例：

```
OIMHOST1 OAAM wls_opam1 IGDADMINVHN 7101
OIMHOST2 OAAM wls_opam2 IGDADMINVHN 7101
```

注：OPAM というタイプはありませんが、代わりに OAAM というサーバー・タイプを使用できます。

ファイルを保存します。

OPAMの起動と検証

OIMHOST1でのOPAMの起動

次の URL を使用して IAMGovernanceDomain 管理サーバーにログインして、OPAM 管理対象サーバーを起動します。

http://igdadmin.example.comconsole

「Servers」→「Control」を選択します。

サーバーwls_opam_admin1 を選択して「**Start**」をクリックします。

OIMHOST1の検証

次の場所にある OPAM 管理サーバー

http://OIMHOST1.example.com:18101/oinav/opam

および、次の場所にある OPAM サーバーに接続して、実装を検証します。

http://OIMHOST1.example.com:18101/opam

なお、内部ネットワークにアクセス中であるため、これらを確認するには Exalogic マシン内でブラウザを起動する必要があります。

OPAM サーバーのログイン・ページが表示され、「LDAP での OPAM ユーザーとグループの作成」で作成した opamadmin 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。

OIMHOST2でのOPAMの起動

「Starting and Stopping Components」に記載されている起動手順を WebLogic 管理対象サーバー wls_opam2 に対して実行し、OIMHOST2 上の Oracle Privileged Account Manager を起動します。

OIMHOST2の検証

http://OIMHOST2.example.com:18101/oinav/opam にある OPAM 管理コンソールに接続して、実装を検証します。

OPAM 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 opamadmin 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://OIMHOST2.example.com:18101/opam にある OPAM サーバーに接続して、実装を検証します。OPAM 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OPAMの構成

この項では、Oracle Adaptive Access Manager を構成して Oracle Web Tier と連携する方法を説明します。なお、Oracle Web Tier は Oracle Traffic Director または Oracle HTTP Server とします。

Oracle Traffic Directorからのアクセスの構成

Oracle Traffic Director にサーバー・プールを作成し、各仮想ホスト用に作成されたルートを変更する必要があります。

OPAM用のOTDサーバー・プールの作成

1. 次の URL を使用して、管理コンソールにログインします。

   https://OTDADMINVHN:8989

2. ページの左上隅にある「**Configurations**」ボタンをクリックします。選択できる構成の一覧が表示されます。

3. サーバー・プールを作成する構成を選択します。

4. Common Tasks ペインで「**New Server Pool**」をクリックします。

5. New Origin-Server Pool ウィザードが起動します。

   Server Pool Information 画面で次の情報を入力します。

   Name：サーバー・プールの名前。例：opam-pool。

   Origin Server Type：プールで処理するリクエストの種類。例：HTTP。

   「**Next**」をクリックします。

6. Origin Server Information 画面で次の情報を入力します。

   Origin Server Host：OIMMHOST1.example.com

   Port：18101

   「**Add Server**」をクリックします。

7. 他のすべてのサーバーの情報を入力します。次に例を示します。

   Origin Server Host：OIMHOST2.example.com

   Port：18101

   「**Next**」をクリックします。

OTDルートの作成

次の OTD ルートを作成する必要があります。

仮想ホスト	ルート	元のサーバー・プール	条件
Igdadmin.example.com	Opam-admin-route	Opam-pool	$uri =~ '/oinav'
sso.example.com	Opam-route	Opam-pool	$uri =~ '/opam'

ルート opam-route に対して、「Enabling SSO PassThorough for sso.mycompany.com」の説明に従って SSO パススルーを有効にします。

管理コンソールによる構成のデプロ

管理コンソールを使用して構成をデプロイするには、次の手順を実行します。

1. 次の URL を使用して管理コンソールにログインします。

   https://OTDADMINVHN:8989

2. ページの左上隅にある「Configurations」ボタンをクリックします。

   選択できる構成の一覧が表示されます。

   「IAM」構成を選択します。

   「**Deploy**」をクリックします。

   更新された構成が正しくデプロイされたことを示すメッセージが表示されます。

3. 「Close」をクリックします。

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、OPAM を Oracle HTTP 構成に追加する必要があります。

IGDADMIN.example.comの更新

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

```
## Entries Required by Oracle Privileged Manager
############################################################
# OPAM Console
<Location /oinav>
      SetHandler weblogic-handler
      WebLogicCluster OIMHOST1.example.com:18101,OIMHOST2.example.com:18101
</Location>
```

prov.example.comの更新

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

```
#########################################################
## Entries Required by Oracle Privileged Acct Manager
#########################################################

   <Location /opam>
        SetHandler weblogic-handler
        WebLogicCluster
        OIMHOST1.example.com:18101,OIMHOST2.example.com:18101 WLProxySSL ON
        WLProxySSLPassThrough ON
   </Location>
```

Oracle HTTP ServerおよびOPAM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_opam1、wls_opam2 を再起動します。

Web層の検証

Web 層が正しくセットアップされていることを検証します。次の URL を使用して OPAM へのアクセスを試行します。

https://prov.example.com/opam - OPAM ユーザーのユーザー名とパスワードの入力を求められます。「LDAP での OPAM ユーザーとグループの作成」で作成した opamadmin ユーザーを使用します。

http://igdadmin.example.com/oinav/opam - OAM のログイン・ページが表示されたら、上記で作成した opamadmin ユーザーを使用してログインします。

OPAM用のOAMポリシーの作成

OPAM の URL に送信されるリクエストが WebGate によってインターセプトされないようにするために、OAM にポリシーを作成する必要があります。この操作を行うには、次の手順を実行します。

1. 次の URL を使用して OAM のコンソールにログインします。

   http://iadadmin.example.com/oamconsole

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. 「**New Resource**」をクリックして次の情報を入力します。
   - Type：http
   - Description：Opam
   - Host Identifier：IAMSuiteAgent
   - Protection Level：Excluded
   - Authentication Policy：n/a
   - Authorization Policy：n/a
7. 「Apply」をクリックします。

OPAMクラスタの使用に必要なOPAMコンソールの構成

1. 次の URL を使用して OPAM のコンソールにログインします。

   http://igdadmin.example.com/oinav/opam
2. OAM のログイン・ページが表示されたら、上記で作成した opamadmin ユーザーを使用してログインします。
3. 「Server Configuration」をクリックします。
4. 以下の情報を入力します。

   Host：prov.example.com

   SSL Port：389

   「**Test**」をクリックします。

   テストが成功したら「**Apply**」をクリックします。成功しなかった場合は管理対象サーバーwls_opamx のログ・ファイルをチェックし、問題を特定して解決します。
5. 「Session Manager Configuration」をクリックします。

   Oracle Privileged Account Manager の URL で「**Ad**」をクリックします。

   OPAM サーバーの URL に https://prov.example.com/opam と入力します。

   他の URL（管理対象サーバーの 1 つを指すデフォルトの URL など）はすべて削除します。

   「**Apply**」をクリックします。
6. 管理対象サーバーwls_opam1 と wls_opam2 を再起動します。

ターゲットを管理するために必要なOPAMの構成

システムを管理する OPAM の構成について詳しくは、OPAM の管理者ガイドを参照してください。OPAM が正常に動作するように構成できるよう、以下に手順を掲載します。

手順には UNIX ホストの構成が含まれます。

ホスト・オペレーティング・システム上でのサービス・アカウントの作成

OPAM を使用するには、通常のユーザーには使用されないアカウントをターゲット・システム上にセットアップする必要があります。たとえば、システム上のアカウントを検索して詳細を表示する、チェックアウト中のアカウントを特定するといった操作をターゲット・システムで実行するときに、このアカウントが OPAM によって使用されます。ターゲット上でアカウント・パスワードを変更するときなどにもこれが使用されます。

opam_service という名前のアカウントをターゲット・システム上に作成するには、root としてログインして次のコマンドを発行します。

```
useradd -d /home/opam_service -m -g root -G bin,daemon,sys,adm,disk,wheel -o -u 0 opam_service
```

次のコマンドを使用してアカウントのパスワードを設定します。

```
passwd opam_service
```

ターゲットとしてのホストのOPAMへの追加

アカウントを作成したら、これをターゲットとして OPAM に追加する必要があります。この操作を行うには、次の手順を実行します。

1. URL http://igdadmin.us.oracle.com/oinav/opam を使用して、opamadmin アカウントとして OPAM のコンソールにログインします。
2. 「**Targets**」をクリックします。
3. 「**Add**」をクリックして次の情報を入力します。

   Target Type：unix

   Target Name：ターゲットを識別する名前（例：idmhost1）。

   Description：ターゲットの説明。

   Domain：ターゲット・サーバーが存在するドメイン（例：example.com）。

   Password Policy：デフォルトのパスワード・ポリシーのままにします。

   Host：ターゲット・サーバーのホスト名（例：oimhost1.example.com）。

   Port：使用する SSH ポートを入力します（例：22）。

   Login User：ホスト上のサービス・ユーザー名を入力します（例：opam_service）。

   Login Password：サービス・アカウントのパスワードを入力します。
4. 「**Test**」をクリックして接続をテストします。

テストが成功したら「Save」をクリックします。

OPAMで管理する特権アカウントの割当て

検証用として、OPAM で管理するダミー・アカウントをターゲット・システム上に作成します。このアカウントには opam_test という名前を付けます。

Unix ホスト上で root として次のコマンドを発行して、アカウント opam_test を作成します。

```
useradd opam test
```

次のコマンドを使用してアカウントにパスワードを割り当てます。

```
passwd opam test
```

1. URL http://igdadmin.example.com/oinav/opam を使用して、opamadmin アカウントとして OPAM のコンソールにログインします。
2. 「**Accounts**」をクリックします。
3. 「**Add**」をクリックします。
4. Target Name の横にある虫メガネ・アイコンをクリックすると検索ウィンドウが表示されます。
5. 「**Search**」をクリックして検索ウィンドウを表示します。
6. Target Name に%を入力して「**Search**」をクリックします。検索結果ウィンドウが表示されます。
7. ターゲット oimhost1.example.com を選択して「**Set**」をクリックします。
8. Account Name フィールドに opam_test と適切な説明を入力します。
9. 「**Test**」をクリックします。
10. テストが成功したら「**OK**」をクリックして「**Save**」をクリックします。

アカウントへのユーザー・アクセス権の付与

» 「**Accounts**」をクリックします。

» 「**Search**」をクリックすると、新たに割り当てられたアカウント opam_test が表示されます。

» このアカウントをクリックして Account ウィンドウを表示します。

» 「**Grants**」をクリックします。

» 「**Add**」をクリックして Add users ダイアログを表示します。

» ユーザー名 opamadmin を入力して「**search**」をクリックします。

» 返された opamadmin アカウントをクリックして「**add**」をクリックします。

» 「**Close**」をクリックして検索ウィンドウを閉じます。

» 「**Apply**」をクリックします。

OPAMの検証

OPAM で管理できるアカウントの準備ができたので、アカウントをチェックアウトしてターゲット・マシンにログインすることで、OPAM が正しく動作するかチェックできます。この操作を行うには、次の手順を実行します。

» URL http://igdadmin.example.com/oinav/opam を使用して、opamadmin アカウントとして OPAM のコンソールにログインします。

» 「**My Accounts**」をクリックします。

» 「**Search**」をクリックします。

» アカウント opam_test が返されます。

» アカウントをクリックして「**Password Check Out**」をクリックします。

» チェックアウトの理由を入力して「**check out**」をクリックします。

» アカウントがチェックアウトされ、パスワードが使用できるようになります。これを確認するために、「**Show password**」をクリックします。

» アカウント opam_test と、手順 7 で取得したパスワードを使用して、ターゲット・マシン（例：oimhost1）にログインします。

» 終了したら「**My Checkouts**」をクリックします。

» アカウント opam_test をクリックして「**Check In**」をクリックします。

» 確認ウィンドウが表示されたら「**Check In**」をクリックします。

OPAMとOracle Identity Managerの統合

OPAM が正しく動作していることを確認できたので、OPAM と Oracle Identity Manager を統合できます。

この操作を行うには、次の手順を実行する必要があります。

Generic LDAP コネクタのインストール

Oracle Identity Manager はすでに OUD ディレクトリとリンクされていますが、Generic LDAP コネクタを構成して同じディレクトリにアクセスできるようにする必要があります。これにより、OPAM を OIM カタログに表示できるようになります。

Generic LDAP コネクタをインストールするには、次の手順を実行する必要があります。

次の URL から最新の Oracle Internet Directory コネクタを入手します。

http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html

バージョン番号が 11.1.2.2 ではなくても心配ありません。また、Oracle Internet Directory と呼ばれるものでも心配ありません。これが Generic LDAP コネクタです。

ファイル oid-version.zip をディレクトリ *IGD_ORACLE_HOME*/server/ConnectorDefaultDirectory に解凍します。

» 次の URL を使用して Oracle Identity Manager のシステム管理コンソールにログインします。

http://igdadmin.us.oracle.com/sysadmin

ログイン・ユーザーは xelsysadm を使用します。

» System Management の下の「**Manage Connector**」をクリックします。Manage connector 画面が表示されます。

» 「**Install**」をクリックします。

» Connector リストから ODSEE/OUD/LDAPV3 コネクタ・バージョンを選択して「**Load**」をクリックします。

» 「Continue」をクリックしてコネクタをインストールします。これには少し時間がかかることがあります（画面が真っ白になっても、しばらく待機してください）。

» コネクタのインストールが完了すると、正しくインストールされたことを示す Summary ページが表示されます。「**Exit**」をクリックします。

ITリソースの構成

コネクタをインストールしたときに、DSEE Server と呼ばれる IT リソースが作成されます。この IT リソースは、OUD サーバーの詳しい接続情報を使用して更新する必要があります。この操作を行うには、次の手順を実行します。

» 次の URL を使用して Oracle Identity Manager のシステム管理コンソールにログインします。

http://igdadmin.us.oracle.com/sysadmin

ログイン・ユーザーは xelsysadm を使用します。

» Provisioning Configuration の下の「**IT Resource**」をクリックします。検索結果ウィンドウが表示されます。

» IT Resource Name に DSEE Server と入力して「**Search**」をクリックします。

» 検索結果ウィンドウに DSEE Server が返されたら「**Edit**」をクリックします。

» 以下の情報を入力します。

Configuration Lookup：Lookup.LDAP.OUD.Configuration

Connector Server Name：空白のままにします。

baseContexts：“dc=example,dc=com”

Principal：cn=oimLDAP,cn=systemids,dc=example,dc=com

Credentials：上記アカウントのパスワード。これは COMMON_IAM_PASSWORD になります。

Host：idstore.example.com

Port：LDAP_LBR_PORT でロードバランサがリスニングするポート（例：1389）

ssl：false

» 「**Update**」をクリックします。

» ウィンドウを閉じます。

ID管理サンドボックスの作成

Identity Manager カタログにエントリを追加できるようにするには、Oracle Identity Manager をサンドボックス・モードにする必要があります。この操作を行うには、次の手順を実行します。

» 次の URL を使用して Oracle Identity Manager のシステム管理コンソールにログインします。

http://igdadmin.example.com/sysadmin

ログイン・ユーザーは xelsysadm を使用します。

» 画面の右上隅にある「**Sandbox**」をクリックします。

» 「**Create Sandbox**」をクリックします。

» 以下の情報を入力します。

Sandbox Name：OPAM

Sandbox Description：OPAM

「Activate Sandbox」を選択します。

「**save and close**」をクリックします。

» 確認メッセージが表示されたら「**OK**」をクリックします。

新しいITリソース用のUIフォームの作成

» 次の URL を使用して Oracle Identity Manager のシステム管理コンソールにログインします。

http://igdadmin.example.com/sysadmin

ログイン・ユーザーは xelsysadm を使用します。

» Provisioning Configuration の下の「**Form Designer**」をクリックします。検索結果ウィンドウが表示されます。

» 「**Create**」をクリックして次の情報を入力します。

Resource Type：LDAP User

Form Name：OUDUser

その他はすべてデフォルトのままにして「**Create**」をクリックします。

OIMでのOPAM用アプリケーションの作成

» 次の URL を使用して Oracle Identity Manager のシステム管理コンソールにログインします。

http://igdadmin.example.com/sysadmin

ログイン・ユーザーは xelsysadm を使用します。

» Provisioning Configuration の下の「**Application Instances**」をクリックします。検索ウィンドウが表示されます。

» 「**Create**」をクリックします。Create Application Instance ウィンドウが表示されるので、次の情報を入力します。

Name：OPAM

Display Name：Oracle Privileged Account Manager

Description：Oracle Privileged Account Manager

Resource Object：LDAP User

IT Resource Instance：DSEE Server

Form：OUDUser

「**Save**」をクリックします。

サンドボックスの公開

新しいプロビジョニング・フォームとアプリケーション・インスタンスを公開するには、次の手順を実行します。

» 次の URL を使用して Oracle Identity Manager のシステム管理コンソールにログインします。

http://igdadmin.example.com/sysadmin

ログイン・ユーザーは xelsysadm を使用します。

» 画面の右上隅にある「**Sandbox**」をクリックします。

» サンドボックス「**OPAM**」をクリックします。

» 「Publish Sandbox」をクリックします。

» 確認を求められたら「**Yes**」をクリックします。

opamSetup.shによるOPAMとOIMの統合

IT リソースとアプリケーションの作成が完了したので、OPAM と OIM を関連付けることができます。この操作を実行するには、スクリプト opamSetup.sh を実行します。このスクリプトは、iamhost1 の *IGD_ORACLE_HOME*/server/bin ディレクトリにあります。

コマンド・セットを実行する前に、次の環境変数を設定します。

APP_SERVER を weblogic に設定します。

OIM_ORACLE_HOME を *IGD_ORACLE_HOME* に設定します。

JAVA_HOME を *JAVA_HOME* に設定します。

MW_HOME を *IGD_MW_HOME* に設定します。

WL_HOME を *IGD_MW_HOME*/wlserver_10.3 に設定します。

DOMAIN_HOME を *IGD_ASERVER_HOME* に設定します。

コマンドは次のとおりです。

```
opamSetup.sh
```

プロンプトが表示されたら次の情報を入力します。

» OIM URL：いずれかの OIM 管理対象サーバーの t3 URL アドレス（例：t3://oimhost1vhn1.example.com:14000）

» OIM username：Oracle Identity Manager のログイン・ユーザー名（例：xelsysadm）

» OIM User Password：OIM username アカウントのパスワード

» OPAM IT resource name：Oracle Privileged Account Manager の IT リソース名。これは、OPAM 用に作成されるリソースの名前です。

» OPAM server name：OPAM サーバーの名前（例：sso.example.com）

» OPAM server port：Oracle Privileged Account Manager サーバーのポート（例：443）

» OPAM user：Oracle Privileged Account Manager のログイン・ユーザー名（例：opamadmin）

» OPAM user password：Oracle Privileged Account Manager のログイン・パスワード

» ID Store IT resource name：ID ストアの IT リソースの名前（例：DSEE サーバー）

» Context：これは weblogic.jndi.WLInitialContextFactory にする必要があります。

コマンドが完了したら、成功したことを示すメッセージが表示されます。

opamSetup スクリプトで実行されるタスクは次のとおりです。

» セットアップ・スクリプトの各パラメータ（opamServer、opamPort、opamUser、および opamPassword）を使用して Oracle Privileged Account Manager の IT リソースを作成する。

» OPAM_TAGS という名前の UDF 列を Oracle Identity Manager カタログに作成する。

» 次の内容で Oracle Privileged Account Manager の同期スケジュール・ジョブを作成する。

» Name：Oracle Privileged Account Manager Catalog Synchronization Job。この名前のジョブがすでに存在する場合は、ジョブ名に-1、-2 などと順に付加されます。

» Schedule type：Periodic、15 分間隔で実行します。

» OPAMServerIdStoreItResource：セットアップ・スクリプトの idStoreItResource パラメータ。

» OpamServerItResource：セットアップ・スクリプトの opamItResource パラメータ。

» OIM.OPAM.Integration システム・プロパティを作成（存在しない場合）して true に設定する。

どのタスクが失敗しても、スクリプトにより自動的に次のタスクが実行されます。

OPAM_TAGSというUDFの作成

Oracle Privileged Account Manager と Oracle Identity Manager の統合環境をセットアップしたら、ユーザー定義フィールド（UDF）の `OPAM_TAGS` と `OPAM_CERT_TAGS` を手動で Oracle Identity Manager カタログに作成する必要があります。`OPAM_TAGS` と `OPAM_CERT_TAGS` という UDF は、Oracle Privileged Account Manager による Oracle Identity Manager カタログの検索を可能にします。

OPAM_TAGS と `OPAM_CERT_TAGS` という UDF を手動で作成するには、次の手順を実行します。

ID管理サンドボックスの作成

Identity Manager カタログにエントリを追加できるようにするには、Oracle Identity Manager をサンドボックス・モードにする必要があります。この操作を行うには、次の手順を実行します。

» 次の URL を使用して Oracle Identity Manager のシステム管理コンソールにログインします。

http://igdadmin.example.com/sysadmin

ログイン・ユーザーは xelsysadm を使用します。

» 画面の右上隅にある「**Sandbox**」をクリックします。

» 「Create Sandbox」をクリックします。

» 以下の情報を入力します。

Sandbox Name：OPAM_TAG

Sandbox Description：OPAM TAG

» 「save and close」をクリックします。

» 確認メッセージが表示されたら「**OK**」をクリックします。

» ツールバーで「**Activate Sandbox**」をクリックします。

カスタム・フィールドの作成

» 次の URL を使用して Oracle Identity Manager のシステム管理コンソールにログインします。

http://igdadmin.example.com/sysadmin ログイン・ユーザーは xelsysadm を使用します。

» 左側のペインで、**System Entities** の下の「**Catalog**」をクリックして manage Catalog ページを開きます。

» 「Create a custom field」アイコンをクリックします。

» 「Select Field Type」ダイアログ・ボックスが表示されたら、「**Text**」フィールド・タイプを選択してテキスト・フィールドを作成します。「**OK**」をクリックします。

» カスタム・フィールドを作成するためのページが表示されたら、次の情報を入力します。

Appearance セクション：

Display Label：OPAM_TAGS

Display Width：256

Name セクション：

Name：OPAM_TAGS

Description：OPAM メタデータ・タグ

Constraints セクション：

Searchable：Select

その他はすべてデフォルトのままにします。

» 「**Save and Close**」をクリックして、ユーザー定義フィールドがカスタム・フィールド表に表示されることを確認します。

» UDF である OPAM_CERT_TAGS を作成するには、次の部分を変更して上の手順を繰り返します。

» **Appearance セクション**の **Display Label** フィールドの値"OPAM_TAGS"を"OPAM CERT TAGS"に置き換えます。

» **Name セクション**の **Name** フィールドの値"OPAM_TAGS"を"OPAM_CERT_TAGS"に置き換えます。

サンドボックスの公開

Identity Manager カタログにエントリを追加できるようにするには、Oracle Identity Manager をサンドボックス・モードにする必要があります。この操作を行うには、次の手順を実行します。

» 次の URL を使用して Oracle Identity Manager のシステム管理コンソールにログインします。

http://igdadmin.example.com/sysadmin

ログイン・ユーザーは xelsysadm を使用します。

» 画面の右上隅にある「**Sandbox**」をクリックします。

» サンドボックス「OPAM_TAG」をクリックします。

» 「Publish Sandbox」をクリックします。

» 確認を求められたら「**Yes**」をクリックします。

OPAMメタデータによるカタログ・エントリのタグ付け

`opamSetup` スクリプトで作成された Oracle Privileged Account Manager のカタログ同期ジョブによって、Oracle Privileged Account Manager メタデータを使用してカタログ・エントリにタグが付けられます。このジョブは 15 分間隔で自動的に実行されます。

ジョブをすぐに実行する必要がある場合は、次のサイクルが始まるのを待つ代わりに、Oracle Identity Manager の管理コンソールから次の手順を手動で実行できます。

» 次の URL を使用して Oracle Identity Manager のシステム管理コンソールにログインします。

http://igdadmin.example.com/sysadmin

ログイン・ユーザーは xelsysadm を使用します。

» System Configuration で「Scheduler」をクリックします。

» Search Scheduled jobs 画面が表示されたら、検索フィールドに LDAP Connector Group Lookup Reconciliation と入力して「**Search**」をクリックします。

» Search Results ウィンドウに表示されたジョブをクリックします。

» 「**Run Now**」をクリックします。

» ジョブが終了したら「**Refresh**」をクリックします。

» ジョブが正常に実行されたことを確認し、**Job History** ビューをチェックします。

» ジョブ **OPAM Catalog Synchronization** について手順 1～7 を繰り返します。

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 Privileged Account 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