ORACLE

# Oracle Cloud Infrastructure

## Oracle Cloud Infrastructure（OCI）への Oracle Identity and Access Managementの移行

2021年5月 | バージョン1.2

公開

## 本書の目的

このドキュメントには、Oracle Identity and Access Management（Oracle IDM）を既存のデプロイメントからOracle Cloud Infrastructure（OCI）に移行するための説明、要件の要約、セットアップ手順が記載されています。このホワイト・ペーパーの対象読者は、Oracle Identity and Access Management、Oracle WebLogic、Oracle Databaseの管理の知識、および基本的なオペレーティング・システムの知識を持つ技術者です。

## 免責事項

本文書には、ソフトウェアや印刷物など、いかなる形式のものも含め、オラクルの独占的な所有物である占有情報が含まれます。この文書へのアクセスと使用は、締結および遵守に同意したOracle Software License and Service Agreementの諸条件に従うものとします。本文書は、ライセンス契約の一部ではありません。また、オラクル、オラクルの子会社または関連会社との契約に組み込むことはできません。
本書は情報提供のみを目的としており、実装および記載されている製品機能の計画を支援することのみを意図しています。マテリアルやコード、機能の提供をコミットメント（確約）するものではなく、購買を決定する際の判断材料になさらないでください。本書に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。

## 改訂履歴

この技術概要には下記の改訂が行われてきました。

| 日付 | 改訂 | コメント |
|---|---|---|
| 2021年2月 | 1.0 | 初期リリース |
| 2021年3月 | 1.1 | フィードバックの反映 |
| 2021年5月 | 1.2 | フィードバックの反映 |
| | | |
| | | |
| | | |

# 目次

## はじめに

多くのお客様が、既存のOracle Fusion MiddlewareデプロイメントからOracle Cloud Infrastructure（OCI）への移行に関心を持っています。これを実行するには多数のアプローチがあり、演習の一環としてコンポーネントをアップグレードする機会は頻繁にあります。この技術概要では、OCIへの既存のデプロイメントのコピーに関してのみ扱います。本文書の目的は、既存の環境をOCIへクローニングするために必要な最小限の再構成のためのアプローチを示すことです。ソース環境は、オンプレミス・ハードウェアまたは他のクラウド・プラットフォームでも構いません。

この技術概要では、Oracle Identity and Access ManagementをOracle Cloud Infrastructure（OCI）に移行するための準備、インストール、および構成手順のソリューション、ならびに運用上のベスト・プラクティスについて説明します。ソース・システムとOCIで、元の構成は同じバージョンになります。

このソリューションには、データベースとOracle Identity and Access Managementインストール環境の両方のクローニングが含まれます。少ないリスクで新しいバージョンへのアップグレードを実行したい場合は、本文書の手順を使用して環境のクローンを作成することができます。そののち、適切なアップグレード・ガイドを使用して、目的のリリースに環境をアップグレードできます。

このアプローチは、実際に実行する前に練習する必要があります。稼働中のシステムにアプローチが与える影響は最小限にとどまるため、自信をもってプロセスを実行できるようになるまで必要なだけ繰り返すことができます。

本文書で示すプロセスはOracle Identity and Access Managementを対象にしていますが、概念と手順はOracle Fusion Middlewareデプロイメントのあらゆるタイプに適用できます。

本文書では、OCIオブジェクトの作成および管理、Oracle Fusion Middleware（Oracle FMW）のインストール、構成、および管理、Oracle Databaseの管理など、複数の異なるトピックを取り扱います。ソリューションには、既存のシステムからOCIへのクローニングが含まれます。

クローニング・プロセス中に、環境の一貫性バックアップを取得するために短時間の停止が必要になる場合がありますが、これは実行されるバックアップのタイプによって異なります。オラクルでは、WebLogicドメインのバックアップを取得する際はWebLogic Serverドメインを完全にシャットダウンすることを推奨しています。停止時間は、デプロイメントのサイズやドメインの再起動時間などの複数の要素に依存します。ソース・データベースとWebLogic Serverドメインを並行してクローニングできる場合、メンテナンスの停止時間は短縮される場合があります。

本文書のアプローチはホスト名の等価性に依存しており、そのようなアプローチにはスタンドアロン環境と統合環境の両方で使用でき、段階的なアプローチを提供するために使用できます。本文書で示すアプローチは、シングル・インスタンス/シングル・ホスト・デプロイメントおよび可用性の高いマルチホスト・デプロイメントで使用できます。

本文書で示すソリューションは、ポイント・イン・タイム・クローンであることに注意してください。クローンがデプロイされると、既存のシステムに行われた変更はクローニングされたシステムにレプリケートされません。この要件を満たすように特定のプロシージャを適用できますが、それは本文書の範囲外です。

## 前提条件

本文書では、以下の環境構成を取り扱います。また、Oracle Identity and Access ManagementからOCIへの移行を計画している管理者の大半が同様の構成を使用していることを前提とします。

この移行を簡素化するために、OCIではソース・システムと同じホスト名が維持されることに注意してください。本文書で提供するクローニング操作を実行する前に、ハードコーディングされたIPアドレスを使用する構成を確認して、ホスト名またはFQDNを使用できるようにソース環境で更新する必要があります。『エンタープライズ・デプロイメント・ガイド』の推奨事項に従った場合は仮想ホスト名を使用することになりますが、このアプローチに従わなかった場合は本文書に詳述するプロセスに従うことができます。

クローニングされた環境は、ソース環境とまったく同一なコピーになります。ソース環境が10ホスト/VMである場合、OCI環境は10ホスト/VMとなります。

### Oracle Internet Directory

Oracle Internet Directoryは、エンタープライズ・デプロイメントまたは高可用性（HA）デプロイメントの一部として構成されます。エンタープライズ・デプロイメントには、主にスケーリングまたは高可用性の目的で複数のノード経由で構成された複数のインスタンスがあります。ただし、ユーザーはすべてのアプリケーションを単一のサーバー構成にデプロイする可能性があります。

### Oracle Unified Directory

Oracle Unified Directoryは、エンタープライズ・デプロイメントまたは高可用性（HA）デプロイメントの一部として構成されます。エンタープライズ・デプロイメントには、主にスケーリングまたは高可用性の目的で複数のノード経由で構成された複数のインスタンスがあります。ただし、ユーザーはすべてのアプリケーションを単一のサーバー構成にデプロイする可能性があります。

### Oracle Access Manager

Oracle Access Managerは、エンタープライズ・デプロイメントまたは高可用性（HA）デプロイメントの一部として構成されます。エンタープライズ・デプロイメントには、主にスケーリングまたは高可用性の目的で複数のノード経由で構成された複数のインスタンスがあります。ただし、ユーザーはすべてのアプリケーションを単一のサーバー構成にデプロイする可能性があります。

### Oracle Identity Governance（旧Oracle Identity Manager）

Oracle Identity Governanceは、エンタープライズ・デプロイメントまたは高可用性（HA）デプロイメントの一部として構成されます。エンタープライズ・デプロイメントには、主にスケーリングまたは高可用性の目的で複数のノード経由で構成された複数のインスタンスがあります。ただし、ユーザーはすべてのアプリケーションを単一のサーバー構成にデプロイする可能性があります。カスタマイゼーションについて、本文書では明示的に取り上げていません。手順ではクローニングされたアプローチを使用しているため、カスタマイゼーションはクローニングされた環境でも動作するはずです。

### Oracle Database

Oracle Internet DirectoryやOracle Access Managerと同様に、Oracle DatabaseもHAデプロイメントの一部として設定されます。Oracle Databaseの場合、HAはOracle Grid InfrastructureおよびOracle Real Application Cluster（Oracle RAC）と共に実行されます。ただし、単一ノード構成にデプロイしたデータベースも存在します。

### Oracle Cloud Infrastructure

ユーザーは、Oracle Cloud Infrastructureの認定ライセンス同意書とOCI管理の基礎知識を備えている必要があります。詳しくは、Oracle Cloud Infrastructureのドキュメントを参照してください。

本書は、既存のOracle Identity and Access Managementデプロイメントを1セットのハードウェアから別のハードウェアへコピーするプロセスに関するものです。本書では、Oracle Cloud Infrastructure（OCI）への移行について説明します。必要に応じて、OCIに関する情報が含まれます。本書では、OCIへのアプリケーションのデプロイに関連するベスト・プラクティスのすべてを取り上げるものではありません。たとえば、インターネットへのアクセスのブロック/許可の方法やコンピュート・インスタンス/サービスへのアクセスのロックダウン方法を決定するセキュリティ・ルールなどに関する説明はありません。

Oracle Cloud Infrastructureのドキュメント、およびOCIへのアプリケーション導入に関連するベスト・プラクティスについてのOracle技術概要を参照してください。

## 環境変数

Oracle Identity and Access Managementの管理者は、各ホストまたはFMW製品をホストするOCIコンピュート・インスタンス上で構成する必要のあるさまざまな環境変数に精通している必要があります。これらの変数は、Oracleドキュメントを参照する際に必要とされ、タスクの実行を大幅に簡素化します。以下は、リフト・アンド・シフト構成に必要な環境変数のリストです。

**ORACLE_HOME：**11g Oracle Identityインストールのベースの場所。
次に例を示します。
/u01/oracle/products/identity

**JAVA_HOME：**Javaインストールのベースの場所。
たとえば次のとおりです。
/u01/oracle/products/jdk

**ASERVER_HOME：**WebLogicドメイン構成のベースの場所。
たとえば次のとおりです。
/u01/oracle/config/domains/IAMGovernanceDomain

**MSERVER_HOME**：管理対象サーバーが起動するWebLogicドメイン構成の場所。たとえば次のとおりです。
/u02/private/oracle/config/domains/IAMGovernanceDomain

*注：『エンタープライズ・デプロイメント・ガイド』では、ドメイン・ディレクトリを2つ設定することを推奨しています。シングル・インスタンスのデプロイメント、または『エンタープライズ・デプロイメント・ガイド』に記載のプラクティスに従わなかったデプロイメントがある場合は、DOMAIN_HOMEディレクトリが1つしかない場合があります。*

**APPLICATION_HOME**：ドメインのアプリケーション・ファイルの場所
。たとえば次のとおりです。
/u01/oracle/config/applications/IAMGovernanceDomain

## クローニング戦略

以下に、Oracle Identity and Access Managementをオンプレミスの実装からOCIへクローニングするために必要なタスクの概要を示します。この手順はバージョンに依存しません。

### リファレンス・アーキテクチャ

ソース・ドメイン、およびデータベースのトポロジとスケーリングは、Oracle Identity and Access ManagementのOracleエンタープライズ・リファレンス・アーキテクチャとは異なる場合があります。

### Oracle Internet Directory

図1：以下の「Oracle Internet Directoryトポロジの移行の概要」は、アーキテクチャの一例です。スケーリングは、ユーザーの実装とは異なる場合があります。

*注：エクスポートおよびインポートは、オンプレミス環境の1つのOracle Internet Directoryインスタンスから OCI環境の1つのインスタンスにのみ構成する必要があります。OCI環境の他のインスタンスはすべて、クラスタにサービスを提供するデータベースからのデータを同期させます。*

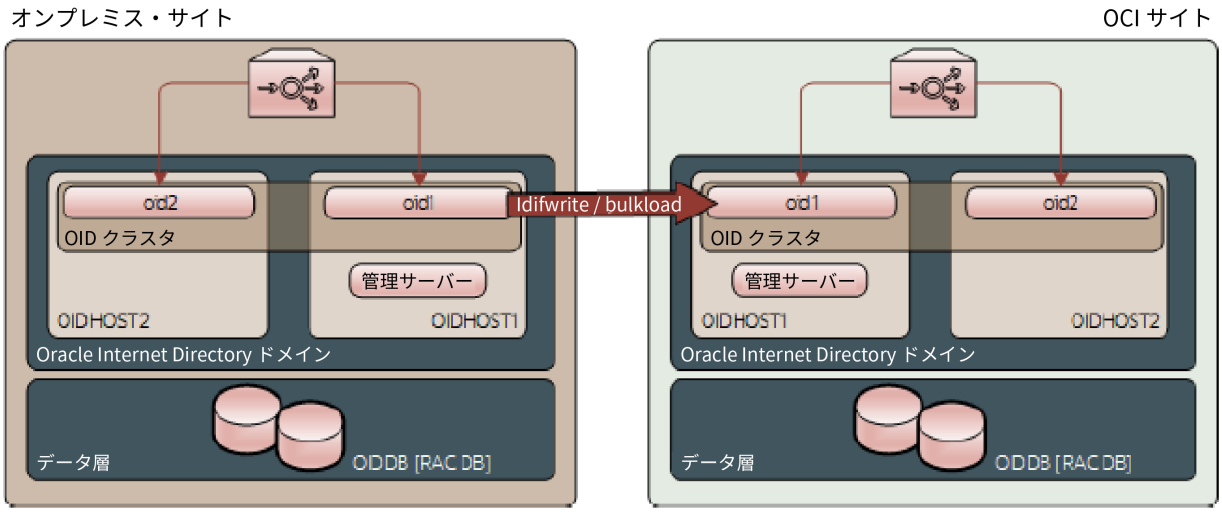



図1：Oracle Internet Directoryトポロジの概要

### Oracle Unified Directory

図2：以下の「Oracle Unified Directoryトポロジの移行の概要」は、アーキテクチャの一例です。スケーリングは、ユーザーの実装とは異なる場合があります。

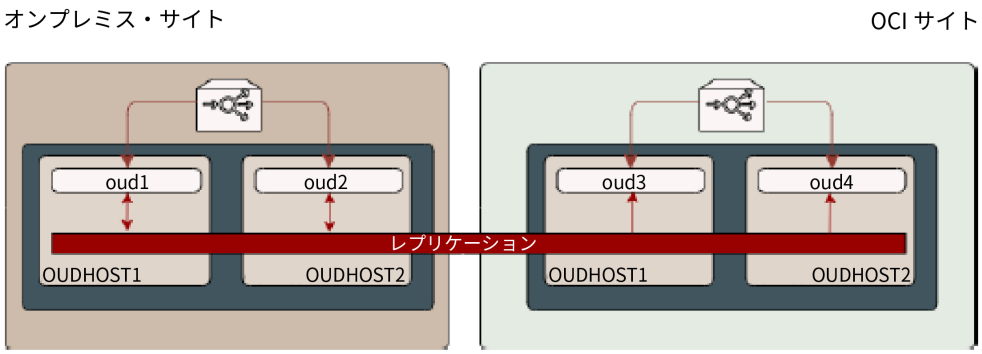



図2：Oracle Unified Directoryトポロジの概要

## Oracle Access Manager

図3：「Oracle Access Mangerトポロジの概要」は、アーキテクチャの一例です。スケーリングは、ユーザーの実装とは異なる場合があります。

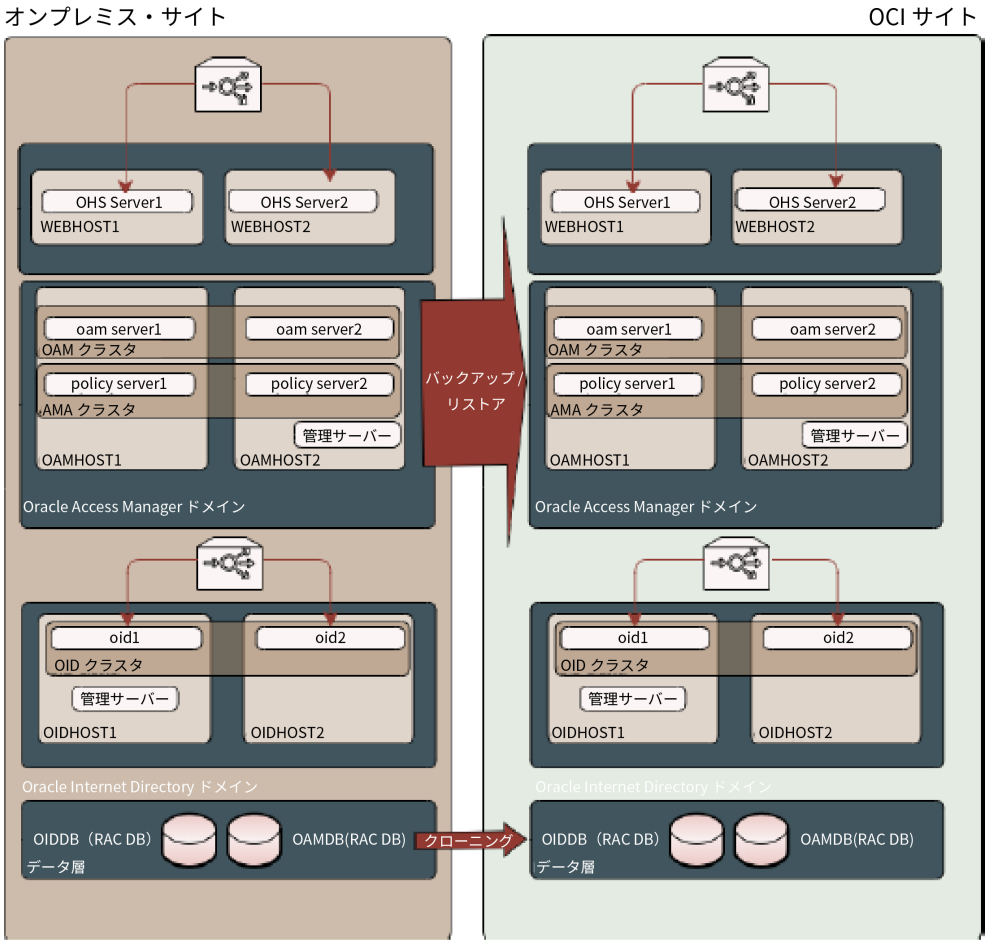



図3：Oracle Access Managerトポロジの概要

## Oracle Identity Governance

図4：「Oracle Identity Governanceトポロジの概要」は、アーキテクチャの一例です。スケーリングは、ユーザーの実装とは異なる場合があります。

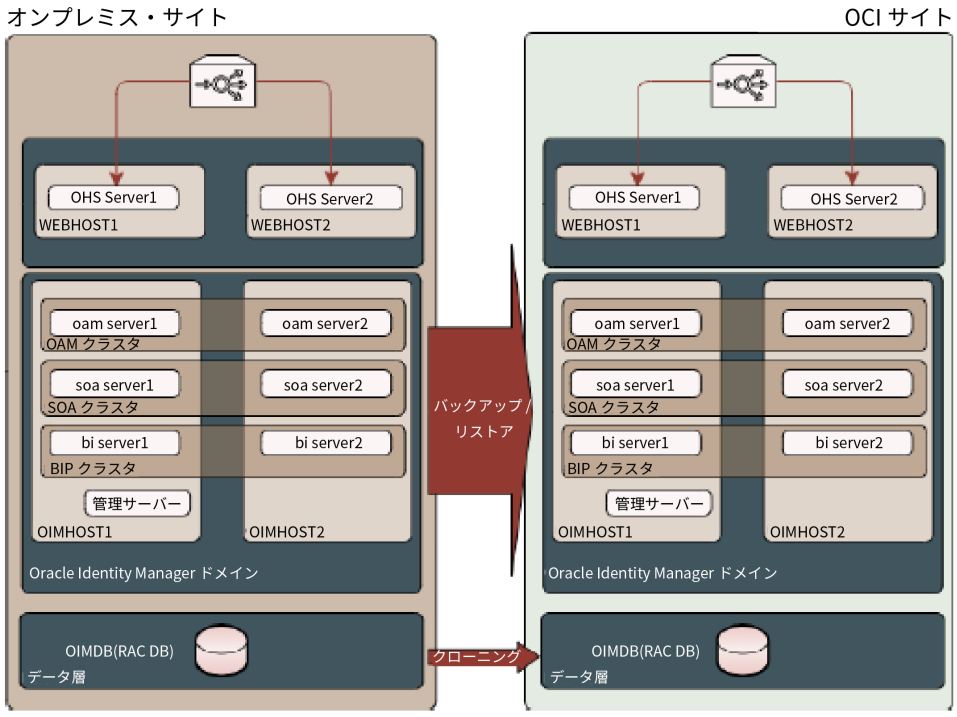



図4：Oracle Identity Governanceトポロジの概要

# クローニングのアプローチ

## Oracle Internet Directory

Oracle Internet directoryで考慮対象となるアプローチは複数あります。アプローチ1 – バックアップとリストア

- 既存のOracle Databaseオブジェクトをバックアップして OCIにリストア
- Oracle Internetバイナリを OCIインスタンスにバックアップしてリストア
- Oracle Internet Directoryインスタンス/ドメインを OCIインスタンスにバックアップしてリストア
- データベースと OCI上のインスタンスを起動

アプローチ2 – Dataguard

- ソース・データベースのDataguardのコピーを作成して OCIにリストア
- ソース・システムから OCIへのデータベース・レプリケーションを実現
- Oracle Internetバイナリを OCIインスタンスにバックアップしてリストア
- Oracle Internet Directoryインスタンス/ドメインを OCIインスタンスにバックアップしてリストア
- OCI上のデータベースへスイッチオーバー
- OCIでOracle Internet Directoryインスタンスを起動

アプローチ3 – OIDのレプリケーション

- ターゲット・システムにOracle Internet Directoryをインストール
- ソース・システムとターゲット・システム間でOracle Internet Directoryのレプリケーションを設定

アプローチ1の利点は、OCIシステムがターゲット・システムの正確なコピーであるため、そのシステムとのすべての相互作用が同じままであることです。欠点は、プライマリ・システムへの変更がOCIシステムにレプリケートされないことです。そのため、OCI上のバージョンはポイント・イン・タイム・レプリカです。

アプローチ2および3では、ソース・システムに適用された変更をターゲット・システムにも適用し続けることができます。これは、アプローチ2ではデータベース経由で、アプローチ3ではOIDのレプリケーション・メカニズム経由で実行されます。

アプローチ2ではソース・システムの正確なコピーができるため、そのシステムとのすべての相互作用が同じままになります。欠点は、データベース全体がDataguard構成の一部となるため、そのデータベースのすべてのデータがレプリケートされることです。

アプローチ3ではOIDデータのみをレプリケートでき、レプリケーションは競合解消を回避するための方法の1つとなります。アプローチ3の欠点は、その両方のOIDインストールから異なる変更ログが生成されることです。Oracle Identity Governanceは、リコンシリエーションをこれらの変更ログに依存しています。このアプローチを適用することにし、Oracle Identity Governanceも使用している場合は、カットオーバー時に新しいディレクトリに対してリコンシリエーションを完全に実行する必要があります。

## Oracle Unified Directory

Oracle Unified Directoryは、疎結合のレプリケーション・メカニズムとクッキーベースの変更ログを維持します。これは、他のシステムへの移行に理想的です。Oracle Unified Directoryのクローニングのアプローチは、以下のとおりです。

- Oracle Unified Directoryバイナリをターゲット OCIシステムにインストール
- ターゲットOCIシステムに新しいOUDインスタンスを作成
- ソース・システムとOCI間にレプリケーションを実現
- ターゲットOCIインスタンスに追加の索引またはアクセス権を作成

ソース・システム上に作成されたデータは、ターゲットOCIシステムに自動的にレプリケートされます。
カットオーバーでは、ソース・インスタンスではなくOCI OUDインスタンスを使用し、レプリケーション構成からソース・システムを削除するだけです。

## Oracle Access Manager

Oracle Access Managerで使用できるアプローチは2つあります。

アプローチ1 – バックアップとリストア

- 既存のOracle Databaseオブジェクトをバックアップして OCIにリストア
- Oracle Identity and Access Managementのバイナリを OCIインスタンスにバックアップしてリストア
- Oracle Access ManagementドメインをOCIコンテナにバックアップしてリストア
- データベースとOCI上のドメインを起動

Approach 2 – マルチ・データセンター

- Oracle Identity and Access Managementのバイナリを OCIインスタンスにバックアップしてリストア
- OCIのデータベースにAccess Managementスキーマを作成
- OCIにAccess Managerドメインを作成
- ソース・サイトとOCI間にマルチ・データセンターを設定

アプローチ1は、ある時点でのOracle Access Managerの同一のコピーを保証します。進行中の変更はOCIシステムに伝播されません。

アプローチ2は、両方ともアクティブ/アクティブで稼働する2つの同一のシステムを作成します。プライマリ・システムで行われた変更は、カットオーバーまでターゲット・システムにレプリケートされます。カットオーバーでは、OCI OAMデプロイメントをOAMソース・システムにし、そこにリクエストを送信します。

本書では、アプローチ2には言及しません。アプローチ2を使用する場合は、Oracle Access Managerのマルチ・データセンターの設定に関するOracleドキュメントを参照してください。

### Oracle Identity Governance

Oracle Identity Governanceで考慮できるアプローチは、以下の1つのみです。

アプローチ1 – バックアップとリストア

- 既存のOracle Databaseオブジェクトをバックアップして OCIにリストア
- Oracle Identity and Access Managementのバイナリを OCIインスタンスにバックアップしてリストア
- Oracle Identity GovernanceドメインをOCIインスタンスにバックアップしてリストア
- データベースとOCI上のドメインを起動

## ソース環境の検証

### ホスト名の使用の確認

本文書のクローニング・ソリューションは、すべての構成プロパティにおいて、IPアドレスではなくホスト名の使用に依存しています。ソース環境のドメインおよびアプリケーションのさまざまな構成パラメータを検証して、直接構成されるIPアドレスがないようにしてください。IPアドレスが使用中であることが分かった場合は、クローニング・プロセスの開始前にソース環境を更新する必要があります。

#### WebLogic Serverドメイン構成の監査

ドメインが、さまざまなリスナー、ノード・マネージャ、データソースのhost/SCAN/ONSパラメータなどのIPアドレスを用いて構成されていないことを検証します。カスタマ構成は範囲が異なり、確認すべきパラメータの数は特に多いため、ここでは基本的な監査プロセスのみを紹介します。既知の各ホスト名について、またはドメイン名、IPアドレス・リストやネットワーク範囲ごとにドメイン構成ファイルを簡単に検索することで、すばやくレポートを作成できます。

以下のホスト・ファイルの例から、ソース環境に含まれるホスト・レコードは次のようになります。

```
# オンプレミスのホスト・エントリ
10.99.5.42    srchost27.example.com srcHost27        webhost1
10.99.5.43    srchost28.example.com srcHost28        webhost2
10.99.5.44    srchost20.example.com srcHost20        ldaphost1
10.99.5.45    srchost21.example.com srcHost21        ldaphost2
10.99.5.46    srchost23.example.com srcHost23        oamhost1
10.99.5.47    srchost24.example.com srcHost24        oamhost2
10.99.5.48    srchost25.example.com srcHost25        oimhost1
10.99.5.49    srchost26.example.com srcHost26        oimhost2

# 管理サーバーのフローティングVIP用のVNICセカンダリIPを計算
10.99.5.61    srcVIPiad.example.com srcVIPiad
10.99.5.62    srcVIPigd.example.com srcVIPigd

# オンプレミスのオーバーライド・エイリアスが設定されたデータベース・システム
10.99.5.20    src-DB-SCAN.example.com src-DB-SCAN
```

```
# ロードバランサIP
        10.99.5.6       prov.example.com        login.example.com       idstore.example.com     iadadmin.example.com
                        igdadmin.example.com    iadinternal.example.com igdinternal.example.com
```

確認対象の値は、簡単なコマンドラインを使ってファイルに書き込むことができます。関連する可能性のある企業のホスト・ネーミング規則から企業のネットワーク範囲、部分ドメイン名、および部分文字列を含めてから、DOMAIN_HOME/configフォルダからすべてのXML構成ファイルの検索を実行します。

```
cat << EOF > /tmp/domainHostNameSearchList.txt
10.99.
.example.com
srcHost
webhohst
ldaphost
oamhost
oimhost
EOF

cd /u01/oracle/config/domains/domain_name/config
find .-name "*.xml" -exec grep -H -f /tmp/domainHostNameSearchList.txt {}¥;
```

これにより、構成ファイルのパス/名前のリスト、およびテキストがある行が表示されます。生成されたリストには、マシンおよびリスニング・アドレス・エントリ、JDBC URL、ONSノード・リスト・エントリ（Gridlink JDBCドライバを使用している場合）などが含まれます。

```
./config.xml:       <machine>OIMHOST1</machine>
./config.xml:       <listen-address>OIMHOST1</listen-address>
./config.xml:       <arguments>-Dtangosol.coherence.wka1=OIMHOST1 –
Dtangosol.coherence.wka2=OIMHOST2 –Dtangosol.coherence.localhost=OIMHOST1 -
Dtangosol.coherence.wka1.port=8089 -Dtangosol.coherence.wka2.port=8089 –
Dtangosol.coherence.localport=8089</arguments>
./config.xml:       <machine>OIMHOST1</machine>
./config.xml:       <listen-address>10.99.5.48</listen-address>
./config.xml:       <machine>OIMHOST1</machine>
./config.xml:       <listen-address>OIMHOST1</listen-address>
./config.xml:       <name>OIMHOST2</name>
./config.xml:       <name>OIMHOST2</name>
./config.xml:       <listen-address>srcHost26</listen-address>
./jdbc/mds-soa-jdbc.xml:
<url>jdbc:oracle:thin:@(DESCRIPTION=(ENABLE=BROKEN)(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(
                    HOST=
src-DB-SCAN.example.com)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=igdupgdb.example)))</url>
./jdbc/mds-soa-jdbc.xml: <ons-node-list>src-DB-SCAN.example.com:6200</ons-node-list>
```

すべてのエントリに、短いホスト名または完全修飾ホスト名のいずれかが使用されていることを確認します。これらは、OCIホスト・ファイルで確認する必要がある値です。
*注：IPアドレスを指定する構成はいずれも、クローニングの前にソース・システムで修正する必要があります。*

**メタデータ・サービス（MDS）に保存されたアプリケーション構成データの監査**

Oracle Identity and Access Managementは構成の詳細をOracle Fusion Middlewareメタデータ・ストア（MDS）データベース・スキーマに保存します。これらの構成の詳細にはエンドポイントURIおよびJDBC接続文字列が含まれ、環境をクローニングする前にそれらを確認して検証する必要があります。このようなURIおよび接続文字列で参照されるホストは、IPアドレスではなく、ホスト名または完全修飾ドメイン名（FQDN）として構成する必要があります。IPアドレスが使用されている場合、ターゲットのOCI環境ではそれらを上書きできないため、クローニング・プロセスの間に変更する必要があります。

これらのパラメータは、Enterprise Manager System MBeanブラウザで1つずつ確認するか、またはまとめてエクスポートしてコマンドラインからWLST経由で迅速に検索することができます。

クローニングのメンテナンスの前に、ソース環境を修正して、ハードコーディングされたIPアドレスをすべて適切なホスト名に置き換えることを推奨します。以下は、Oracle Identity Governance向けの例です。

OIGのために保存されたメタデータ構成をWLST経由で監査するには、以下を実行します。

1. ソース環境のOIMホストに、ORACLE_HOMEディレクトリへの権限を持つOSユーザーとしてログインします。
2. 一時的な作業ディレクトリを作成します。
   mkdir -p /tmp/mds/oig/
3. WLST経由で管理サーバーに接続します。
   $ ORACLE_HOME/common/bin/wlst.sh
   wls:/offline> connect()
   Please enter your username :weblogic_idm
   Please enter your password :
   Please enter your server URL [t3://localhost:7001] :t3://igdadminvhn:7001
   Connecting to t3://igdadminvhn:7001 with userid weblogic_idm ...
   Successfully connected to Admin Server 'AdminServer' that belongs to domain 'IAMGovernanceDomain'.
   wls:/IAMGovernanceDomain/serverConfig>

4. FMWメタデータ・ストアからOIM構成のXMLデータをエクスポートし、WLSTを終了します。
   - Application='OIMMetadata'
   - server='WLS_OIM1' (your server name may vary)
   - toLocation='/tmp/mds/oim'
   - docs= '/db/oim-config.xml'

   たとえば次のとおりで。

   wls:/IAMGovernanceDomain/serverConfig> exportMetadata(application='OIMMetadata', server='WLS_OIM1', toLocation='/tmp/mds/oim', docs='/db/oim-config.xml')

   Executing operation: exportMetadata.

   Operation "exportMetadata" completed.Summary of "exportMetadata" operation is:
   1 documents successfully transferred.
   List of documents successfully transferred:

   /db/oim-config.xml

   wls:/IAMGovernanceDomain/serverConfig> exit()

5. OIM構成から関連データをフィルタリングするために使用する検索語のファイルを作成します。
   エクスポートされたXMLファイルには、多数の構成要素があります。フィルタリングに使用するための短いリストを作成します。
   注：例の中の"<"の文字は誤植ではありません。

   たとえば次のとおりです。

   $ cat << EOF > /tmp/mds/oig/grepHostValidationTerms.txt
   <directDBConfigParams
   biPublisherURL
   oimFrontEndURL
   oimExternalFrontEndURL
   oimJNDIURL
   backOfficeURL
   accessServerHost
   tapEndpointUrl
   soapurl

rmiurl
host
serviceURL
EOF

6. 検索語を使ってOIM構成データを検索します。

   たとえば次のとおりです。
   $ grep -f /tmp/mds/oig/grepHostValidationTerms.txt  /tmp/mds/oig/db/oim-config.xml

   <directDBConfigParams checkoutTimeout="1200"
   connectionFactoryClassName="oracle.jdbc.pool.OracleDataSource"
   connectionPoolName="OIM_JDBC_UCP" driver="oracle.jdbc.OracleDriver" idleTimeout="360"
   maxCheckout="1000" maxConnections="5" minConnections="2" passwordKey="OIMSchemaPassword"
   sslEnabled="false" url="jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=src-DB-SCAN.example.com )(PORT=1521)) (CONNECT_DATA= (SERVICE_NAME=igdupgdb.example)))"
   username="IGDUPG_OIM" validateConnectionOnBorrow="true">
   <bIPublisherURL>http://OIMHOST2:9704,OIMHOST1:9704</bIPublisherURL>
   <oimFrontEndURL>http://igdinternal.example.com</oimFrontEndURL>
   <oimExternalFrontEndURL>https://prov.example.com:443</oimExternalFrontEndURL>
   <oimJNDIURL>@oimJNDIURL</oimJNDIURL>
   <backOfficeURL/>
   <accessServerHost>srcHost23</accessServerHost>
   <tapEndpointUrl>https://login.example.com:443/oam/server/dap/cred_submit</tapEndpointUrl>
   <soapurl>http://OIMHOST2:8001</soapurl>
   <rmiurl>cluster:t3://cluster_soa</rmiurl>
   <host>@oaacghost</host>
   <serviceURL>@oaacgserviceurl</serviceURL>

7. 検索結果を確認し、すべての構成プロパティで適切なホスト名または完全修飾ドメイン名が使用されていることを確認します。
   注：一部のプロパティにプレースホルダ値が含まれる場合があります（@oaacghostや@oaacgserviceurlなど）。それらは現状のままで問題ありません。
   注：通常、指定された<rmiurl>URIは、WLSサーバー名またはクラスタ名へアドレス指定されたWLS t3プロトコルURIで、ホスト名を使用しません。これも現状のままで問題ありません。

## OCIオブジェクトの準備

ソフトウェアのインストールと構成を始める前に、OCIテナンシーでオブジェクトを作成する必要があります。テナンシーの取得、ユーザーの作成、および仮想ネットワーキングの構成は、本書の範囲外です。詳しくは、Oracle Cloud Infrastructureのドキュメントを参照してください。

### コンピュート・インスタンスおよびデータベース・インスタンスの作成

OCIでは、サーバー・ホストはコンピュート・インスタンスと呼ばれます。おのおののコンピュート・インスタンスを作成するために、インスタンスのイメージおよびシェイプにいくつかのオプションがあります。イメージはコンピュート・インスタンスにインストールされるオペレーティング・システムで、シェイプはコンピュート・インスタンス・タイプです。つまり、仮想マシンまたはベア・メタル、およびコンピュート・インスタンス上に構成されるリソース、CPU、メモリなどです。ユーザーのオンプレミス環境で構成された各Oracle Identity Governanceホストに対し、数が一致するコンピュート・インスタンスをOCIサイトに作成する必要があります。オペレーティング・システムの選択肢は維持されます。
ただし、オペレーティング・システムのバージョンは、Oracle Fusion Middleware Supported System Configurationsマトリクスに従ってアップグレードできます。インスタンスの選択と作成については、お客様それぞれのニーズが異なるため、本文書の範囲外です。

同様に、ソース環境で構成された各データベース・ノードは、OCIで作成された、数が一致するデータベース・インスタンスを含む必要があります。コンピュート・インスタンスと同様、インスタンス・タイプには選択肢があります。仮想マシン、ベア・メタル・マシン、およびExadataマシンの選択肢です。インスタンスの選択と作成については、お客様それぞれのニーズが異なるため、本文書の範囲外です。

作成されるおのおののコンピュート・インスタンスは、そのコンピュート・インスタンスのために作成される同等のストレージを必要とします。使用されるストレージ・タイプの選択、およびストレージのサイジングはユーザーによって異なるため、本文書の範囲外です。詳しくは、「クラウド・ストレージ」を参照してください。ストレージのマウント・ポイントは、WebLogic Serverドメインの現状の直接コピーを可能にするために、オンプレミス環境のホストのマウント・ポイントと一致する必要があります。

## オペレーティング・システムの構成

OCIコンピュート・インスタンスおよびデータベース・インスタンスのインストールおよび構成の特定の要素を実行するには、オペレーティング・システム要件をいくつか構成する必要があります。以下に、それぞれの詳細を示します。

*プラガブル認証モジュール（PAM）を有効にするための構成*

1. すべてのホストのSSHデーモンでPAMが有効になるようにします。
2. インスタンスにログインします。
3. 任意のエディタを使用して、/etc/ssh/sshd_configを開きます。UsePAMパラメータを含む行を検索します。
4. コメントがある場合は、行の最初からコメントを削除します。
5. UsePAMパラメータの値がYesになっていることを確認します。Noに設定されている場合は、値を変更します。
6. ファイルを保存します。
   注：SSHDの再起動は、次のセクションで実行されます。

### ソース・ホストとターゲット・ホスト間のOSパッケージの整合性

デプロイされたOSパッケージを比較してギャップや差異を特定し、必要に応じて修正します。

### Fusion Middleware操作に必要とされるLinuxオペレーティング・システムの設定

以下の構成がFusion Middleware 12cの要件です。

1. /etc/sysctl.confファイルを編集して、以下を追加します。
   kernel.sem 256 32000 100 142
   kernel.shmmax = 4294967295（最小要件）
2. /sbin/sysctl -pを実行して変更を有効にします。
3. OSバージョンに応じて、/etc/security/limits.conf または/etc/security/limits.d/20-nproc.confファイルを編集します。これらのパラメータを確認し、必要に応じて以下の値以上に設定します。
   * soft nofile 32767
   * hard nofile 327679
   * soft nproc 2047
   * hard nproc 16384

### Linuxコンピュート・インスタンスのインスタンス・ファイアウォール・ルール

デフォルトでは、SELINUXはすべてのLinuxコンピュート・インスタンスで有効化されているため、インスタンスの外部からアクセスする必要がある各ポートでは、ファイアウォール・ルールをコンピュート・インスタンス上に作成する必要があります。ルールを構成する手順は次のとおりです。

1. 以下のコマンドを使用して、ソースOIGドメイン内のすべてのホスト上のサービス・リスナー・ポートの完全なセットをrootとして確認します。
   netstat -tulpn | grep LISTEN | grep java | sort -n

   *WebLogic Server、Oracle Identity Governance、SOA、およびBIPのデフォルトのポートは、以下のとおりです。*
   *5556、7001、7010、8001、8089、8090、9704、14000、46067*

2. アクセスする必要があるすべてのポートについて、以下を実行します。
   sudo firewall-cmd --permanent --add-port=ポート番号/tcp
   たとえば次のとおりです。
   sudo firewall-cmd --permanent --add-port==7001/tcp

3. 以下を実行して、すべてのポートが構成されてからファイアウォール・サービスを再起動します。
   sudo systemctl restart firewalld

4. 以下を実行して、ファイアウォール構成を確認します。
   sudo firewall-cmd --list-ports

**Linuxコンピュート・インスタンスのユーザーとグループ**

必ずしもOCIインスタンスにオンプレミス・インストールと同じユーザーとグループを構成する必要はありませんが、11gインストールがクローニングされるため、作業が簡素化する可能性があります。このため、OCIインスタンスに同じアカウント所有者とグループを作成することを推奨します。ソース環境で一致するUID/GIDを用いてoinstallグループとoracleユーザーを作成するには、以下のプロシージャを使用できます。

```
sudo groupadd -g 1002 oinstall
sudo adduser -u 1001 -g oinstall -G oinstall oracle
```

## ロードバランサの作成

高可用性構成の場合、Oracle Identity and Access Managementは、Oracle Identity and Access Management WebLogicコンポーネントにリクエストをルーティングするために使用されるOracle HTTPサーバーの内側に存在します。Oracle HTTPサーバーへのアクセスは、ロードバランサ経由で行われます。ロードバランサがOCI内にある場合もあれば、オンプレミスの既存のロードバランサを使用して、カットオーバー時に新しいOCIデプロイメントにリクエストを送信する場合もあります。

Oracle Identity and Access Managementでロードバランサを使用することについて詳しくは、『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。

## セカンダリIPアドレスの作成によるサービス移行のサポート

ソース・インストールでWebLogic管理サーバーに仮想IPアドレスを使用する場合、または『エンタープライズ・デプロイメント・ガイド』で説明されている他のサービスを使用する場合は、同様のセカンダリIPアドレスを適切なコンピュート・インスタンスに合わせてプライマリVNIC上のOCIに作成する必要があります。

これを行うには、次の手順を実行します。

1. OCIコンソールから、次のように進みます。「**Compute**」→「**Instances**」→-「**Instance Details**」→「**Attached VNICS**」→「**VNIC Details**」→「**IP Addresses**」（ドメインの管理サーバーを実行するコンピュート・インスタンスの1つ（OIMHOST1など））
2. 「Assign Private IP address」をクリックします。
3. ホスト名を、IGDADMINVHNまたは使用中の何らかの名前に設定します。他はすべてデフォルトのままにできます。
4. 「assign」をクリックして、新しいIPアドレスが割り当てられたことを確認します。
5. コンピュート・インスタンスにログインします。
6. IPアドレスをアクティブVNICに割り当てます（ip addrを使用して確認）。
   たとえば、メインVNICが**ens3**の場合は、以下のコマンドを使用して新しいセカンダリIPアドレスをそのインタフェースに割り当てることができます。

   ```
   sudo ip addr add 10.0.2.21 dev ens3 label ens3:0
   ```

7. 以下のコマンドを使用して割当てを確認します。

   ```
   ip addr
   ```

8. 新しいIPアドレス、OCIホスト名、およびドメイン構成で使用されるソース環境の完全修飾ホスト名について、すべてのホスト上で一貫して/etc/hostsファイルにエントリを作成します。詳しくは、以下の「OCIホスト・ファイル」セクションを参照してください。

   ```
   10.0.2.21 igdadminvhn.idm.tenant.oraclevcn.com igdadminvhn srcVIPigd.example.com srcVIPigd
   ```

### OCIオブジェクトのサマリー

デプロイメント内のOCIオブジェクトのトポロジと配置は、選択した地域のOracle Cloud Infrastructureデータセンターで使用できる可用性ドメインの現在の数によって異なります。ここで示す例には、複数の可用性ドメインが提供されている場合のトポロジ、および単一の可用性ドメインのみが提供されている場合の障害ドメインの使用が含まれます。クロスリージョンの高可用性は本書の範囲外です。

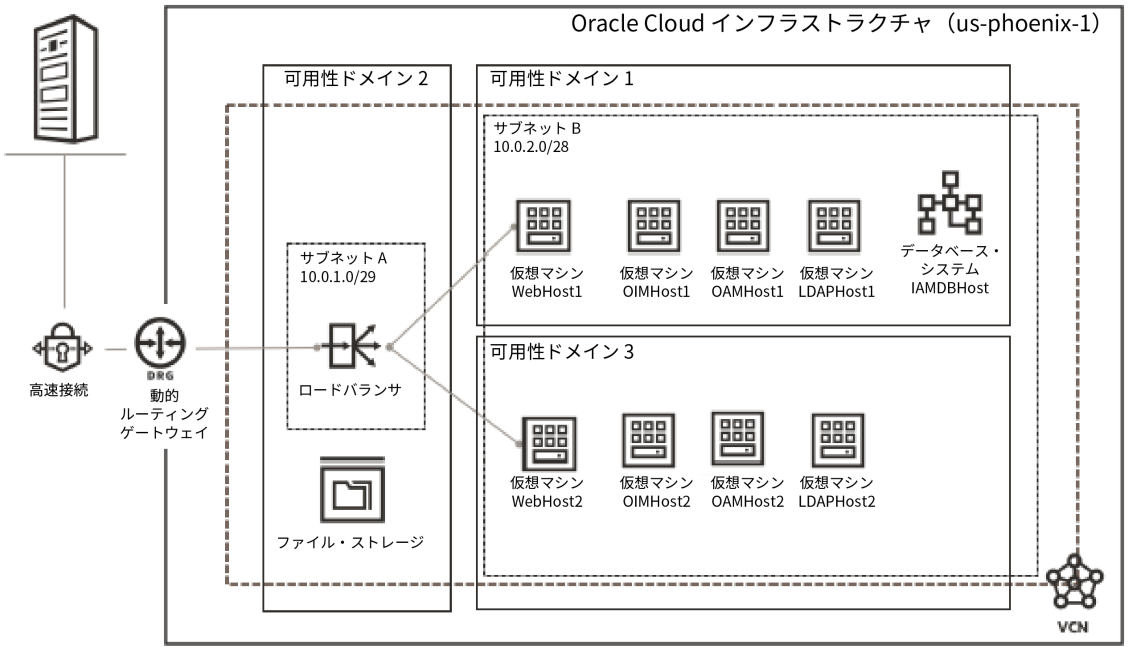



図1 - 複数の可用性ドメインを備えたOCIトポロジ

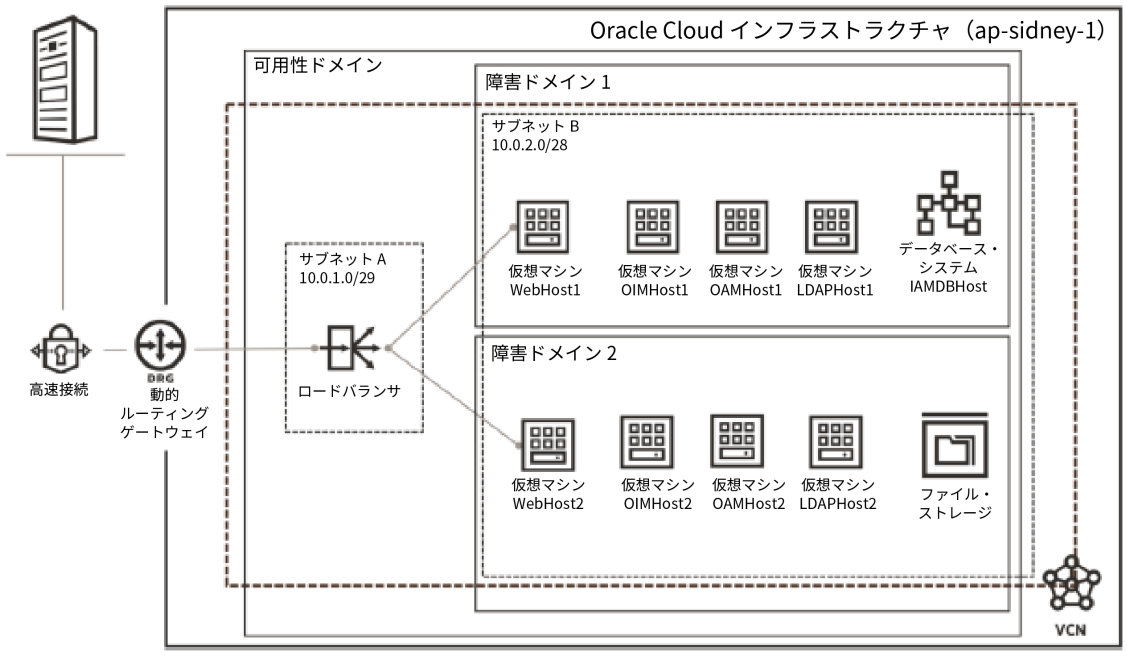



図2 - 単一の可用性ドメインを備えたOCIトポロジ

## OCIホスト・ファイル

クローン環境の状況では、OCIで参照されるホスト名がソース・システムのホスト名と同じであることが不可欠です。これが、クローニング戦略の鍵となります。『エンタープライズ・デプロイメント・ガイド』の推奨事項に従い、すべての構成に仮想ホスト名を使用した場合は、これは単にこれらのエントリを実際のOCIホスト名へ別名設定する問題に過ぎません。たとえば次のとおりです。

```
10.0.2.17       oimhost1.idm.tenant.oraclevcn.com       oimhost1
```

ソースのWebLogic構成で物理ホスト名を使用している場合は、これらの名前を実際のOCIホスト名に別名設定する必要があります。たとえば次のとおりです。

```
10.0.2.17       oimhost1.idm.tenant.oraclevcn.com       oimhost1            srchost25.example.com srcHost25
```

さらに、ソース環境に管理サーバーのマシン・リスニング・アドレスおよびノード・マネージャのホストの宣言のための追加のフローティングVIPおよびFQDNが含まれる場合は、適切なOCIコンピュート・インスタンスに合わせてOCIのセカンダリIPアドレスをVNIC上で構成し、ホスト・ファイルに追加する必要があります。これらのセカンダリIPアドレス・エントリには、管理サーバーに接続した際にDNSをオーバーライドするためのソース環境のFQDNおよびホスト名も含まれる必要があります。

```
10.0.2.21       igdadminvhn.idm.tenant.oraclevcn.com igdadminvhn srcVIPigd.example.com srcVIPigd
```

以下は、/etc/hostsファイルの1例です。

```
127.0.0.1       localhost localhost.localdomain localhost4 localhost4.localdomain4
::1             localhost localhost.localdomain localhost6 localhost6.localdomain6

# オンプレミスのオーバーライド・エイリアスによる計算
10.0.2.11       webhost1.idm.tenant.oraclevcn.com       webhost1        srchost27.example.com srcHost27
10.0.2.12       webhost2.idm.tenant.oraclevcn.com       webhost2        srchost28.example.com srcHost28
10.0.2.13       ldaphost1.idm.tenant.oraclevcn.com      ldaphost1       srchost20.example.com srcHost20
10.0.2.14       ldaphost2.idm.tenant.oraclevcn.com      ldaphost2       srchost21.example.com srcHost21
10.0.2.15       oamhost1.idm.tenant.oraclevcn.com       oamhost1        srchost23.example.com srcHost23
10.0.2.16       oamhost2.idm.tenant.oraclevcn.com       oamhost2        srchost24.example.com srcHost24
10.0.2.17       oimhost1.idm.tenant.oraclevcn.com       oimhost1        srchost25.example.com srcHost25
10.0.2.18       oimhost2.idm.tenant.oraclevcn.com       oimhost2        srchost26.example.com srcHost26

# 管理サーバーのフローティングVIP用のVNICセカンダリIPを計算
10.0.2.20       iadadminvhn.idm.tenant.oraclevcn.com    iadadminvhn     srcVIPiad.example.com srcVIPiad
10.0.2.21       igdadminvhn.idm.tenant.oraclevcn.com    igdadminvhn     srcVIPigd.example.com srcVIPigd

# オンプレミスのオーバーライド・エイリアスが設定されたデータベース・システム
10.0.2.19       iamdbhost.idm.tenancy.oraclevcn.com     iamdbhost       src-DB-SCAN.example.com
                src-DB-SCAN

# ロードバランサIP
10.0.1.10       prov.example.com login.example.com      idstore.example.com     iadadmin.example.com
igdadmin.example.com        iadinternal.example.com     igdinternal.example.com
```

*注：おのおののOCIコンピュート・インスタンスおよびDBホスト/SCANアドレスのエントリが、トポロジのすべてのホストのホスト・ファイルに存在することを確認してください。*

# ソース環境のクローニング

## データベースからOCIへのクローニング

Oracle Internet Directory、Oracle Access Manager、およびOracle Identity Governanceのクローニングには、ソース・データベースからOCIへのクローニングが必要です。

これには複数の方法があり、それぞれに異なるメリットがあります。使用される可能性があるオプションのリストを以下に示します。オプション1 – データベースのエクスポート/インポート

- 小規模なデータベースに最適
- バージョン間の移動が可能（例：12.1.0.3から19c）
- アプリケーション単位 / PDB単位でのコンテナ・データベース / プライベート・データベースへの移動が可能
- 完全なコピー。演習をやり直すには、そのたびにデータをターゲットから削除する必要あり
- 継続的な同期はなし
- カットオーバー中は更新のためにソース・システムを凍結する必要あり
- データベースのエクスポート中はWLSドメインのシャットダウンが推奨される

オプション2 – RMANの使用によるデータベースの複製

- あらゆるサイズのデータベースに最適
- データベース全体のバックアップを取得
- データベースのアップグレードを独立したタスクとして実行することが必要
- リストア後にCDB/PDBの移行が必要
- 継続的な同期はなし
- カットオーバー中は更新のためにソース・システムを凍結する必要あり

オプション3 – Dataguardデータベース

- あらゆるサイズのデータベースに最適
- データベース全体のバックアップを取得
- データベースのアップグレードを独立したタスクとして実行することが必要
- CDP/PDBの移行を独立した演習として実行することが必要
- 継続的な同期。データベースをオープンしてアップグレードをテストし、再びクローズしてデータとオンプレミス・ソースとの同期の維持が可能

この技術概要では、エクスポート/インポートを使って説明していきます。他のソリューションについては、以下を参照してください。

Oracle Database Backup and Recovery Users Guide
Oracle Data Guard Concepts and Administration

## エクスポート/インポートを使用したデータベースのクローニング

**ソース環境では次のとおりです。**

1. ソースDBホスト上でエクスポート・プロセスのディレクトリの詳細情報を作成して設定します。
    a. ソースDBホスト上で十分な領域のある場所にディレクトリを作成します。
    mkdir -p /u01/installers/database
    b. ソース・データベースとターゲット・データベースでこの場所を参照するデータベース・ディレクトリ・オブジェクトを作成します。
    SQL> CREATE DIRECTORY orcl_full AS '/u01/installers/database';

2. WebLogic Server管理対象サーバーまたはクラスタをシャットダウンします。
   注：ドメインのバックアップと同時に実行する場合は、管理サーバーとノード・マネージャを含むドメイン全体のシャットダウンを調整してください。

3. Oracle Identity Governanceを使用している場合は、ソース・データベースのSOA DBMS Queuesを停止します。

   a. ユーザー・キューのSOAINFRAスキーマ・ユーザーおよびクエリーとして接続します。

```
$ sqlplus <PREFIX>_SOAINFRA@<sourceDB>
SQL> COLUMN name FORMAT A32
SQL> SELECT name,enqueue_enabled,dequeue_enabled
FROM USER_QUEUES where queue_type = 'NORMAL_QUEUE' order by name;

NAME                                               ENQUEUE  DEQUEUE
-------------------------------------------------- -------- --------
B2B_BAM_QUEUE                                      YES      YES

EDN_EVENT_QUEUE                                    YES      YES
EDN_OAOO_QUEUE                                     YES      YES
IP_IN_QUEUE                                        YES      YES
IP_OUT_QUEUE                                       YES      YES
TASK_NOTIFICATION_Q                                YES      YES

6 rows selected.
```

   b. 各キューを停止します。

```
SQL> BEGIN

DBMS_AQADM.STOP_QUEUE ('B2B_BAM_QUEUE');

DBMS_AQADM.STOP_QUEUE ('EDN_OAOO_QUEUE');

DBMS_AQADM.STOP_QUEUE ('EDN_EVENT_QUEUE');

DBMS_AQADM.STOP_QUEUE ('IP_IN_QUEUE');

DBMS_AQADM.STOP_QUEUE ('IP_OUT_QUEUE');

DBMS_AQADM.STOP_QUEUE ('TASK_NOTIFICATION_Q');

END;

/
exit
```

4. OIMスキーマ・ユーザーとして、ソース・データベースで実行中のOIG DBMS_SCHEDULERジョブに対するクエリーを実行して停止します。

```
$ sqlplus <PREFIX>_OIM@<sourceDB>

SQL> SELECT job_name,session_id,running_instance,elapsed_time
FROM user_scheduler_running_jobs ORDER BY job_name;

no rows selected
```

   注：ジョブを実行中の場合は、完了まで待機するか、または以下を使用してジョブを‘正しく’停止してください。

```
SQL> BEGIN

DBMS_SCHEDULER.stop_job('REBUILD_OPTIMIZE_CAT_TAGS');

END;

/

SQL> exit
```

5. システム・ポリシーを付与して、Data Pumpジョブのエクスポート中のエラーを回避してください。

```
$ sqlplus SYS as SYSDBA
SQL> GRANT EXEMPT ACCESS POLICY TO SYSTEM;
SQL> exit
```

6. システムおよびスキーマ・ダンプをソース・データベースからエクスポートし、ディレクトリ・プロパティを適切に設定します。

   a. system.schema_version_registryの表およびビューをエクスポートします。

```
$ expdp ¥"sys/<password>@<sourcedb> as sysdba¥" ¥
DIRECTORY=orcl_full ¥
DUMPFILE=idm_system.dmp ¥
LOGFILE=idm_system_exp.log ¥
SCHEMAS=SYSTEM ¥
INCLUDE= VIEW:"IN('SCHEMA_VERSION_REGISTRY')"  TABLE:"IN('SCHEMA_VERSION_REGISTRY$')"¥
JOB_NAME=MigrationExportSys
```

   b. ソースWebLogicServerドメインのデータソースで使用される**すべての**スキーマをエクスポートします。

OIGの例

```
$ expdp ¥"sys/<password>@<sourcedb> as sysdba¥" ¥
      DIRECTORY=orcl_full ¥
      DUMPFILE=idm.dmp ¥
      LOGFILE=idm_exp.log ¥
      SCHEMAS=IGD_OIM,IGD_SOAINFRA,IGD_BIPLATFORM, ¥
      IGD_MDS,IGD_ORASDPM,IGD_OPSS,IGDJMS,IGDTLOGS ¥
      JOB_NAME=MigrationExport ¥
      EXCLUDE=STATISTICS
```

OAMの例

```
expdp ¥"sys/password@IADUPGDB1 as sysdba¥" ¥
      DIRECTORY=orcl_full ¥
      DUMPFILE=idm.dmp ¥
      LOGFILE=idm_exp.log ¥
      SCHEMAS=IAD_OAM,IAD_MDS,IAD_OPSS,IAD_OMSM,IAD_IAU_VIEWER,¥
      IAD_IAU_APPEND,IAD_IAU¥
      EXCLUDE=STATISTICS
```

インストールのスキーマの完全なリストを取得するには、次のSQLスクリプトを実行します。

```
Select username
From all_users
Where username like ‘RCU_PREFIX%’;
```

7. 表領域、スキーマ・ユーザー、および付与のソース・データベースDDLを抽出します。

この手順により、ターゲット・データベース上に正しい表領域を効率的に作成でき、スキーマ・ユーザーのパスワードを保持できるため、この点においてはドメインの再構成は必要ありません。エクスポートされたスキーマ外部のオブジェクトへのシステムおよびオブジェクトの付与も考慮され、無効なオブジェクトのリスクや再コンパイルの難しさが軽減されます。完全なSQL DDL出力をすべて一度に作成するためのスクリプトの例を示します。この例は、CDB/PDBを使用していない場合には修正する必要があります。

a. SQLPLUSでは、SQLスクリプトの例を実行して、Data Pumpがダンプをエクスポートしたのと同じディレクトリのddl.sqlファイルにDDLを抽出します。ソース環境のRCU接頭辞とターゲットPDBを入力します。スクリーンおよびddl.sqlと名付けられたファイルの両方に出力がコピーされます。

```
$ cd /u01/installers/database
$ sqlplus SYS as SYSDBA
SQL> @extract_ddl.sql
Enter RCU Prefix:RCUPREFIX
Enter PDB: targetPDB
```

b. 出力ddl.sqlのシステムQT*_BUFFERビューのオブジェクト付与をすべて削除します。
バッファ・ビューはターゲット・データベースに存在せず、エラーがスローされます。

```
$ sed -i.bak -e '/QT.*_BUFFER/d' /u01/installers/database/ddl.sql
```

**スクリプト例：**

*注：赤字の行は、ターゲット・データベースがPDBの場合のみ適用できます。*
*このSQLは、すべてのオブジェクトがRCU接頭辞を使用して作成されていることを前提としています。接頭辞を使用せずにオブジェクトを作成した場合は（JMSの表領域/ユーザーまたはTLogsなど）、これらを手動で追加する必要があります。*

```
$ cat << EOF > extract_ddl.sql
set pages 0
set feedback off
set heading off
set long 5000
set longchunksize 5000
set lines 200
set verify off
exec dbms_metadata.set_transform_param (dbms_metadata.session_transform, 'SQLTERMINATOR',
true);
exec dbms_metadata.set_transform_param (dbms_metadata.session_transform, 'PRETTY', true);
accept PREFIX char prompt 'Enter RCU Prefix:'
accept PDBNAME char prompt 'Enter PDB:'

spool ddl.sql

select 'alter session set container=&&PDBNAME;'
from dual
/
SELECT DBMS_METADATA.GET_DDL('TABLESPACE',Tablespace_name)
from dba_tablespaces
where tablespace_name like '&&PREFIX%'
/
set lines 600
SELECT DBMS_METADATA.GET_DDL('USER',USERNAME)
from DBA_USERS
where USERNAME like '&&PREFIX%'
```

```
set lines 200
SELECT DBMS_METADATA.GET_GRANTED_DDL ('SYSTEM_GRANT',USERNAME)
from DBA_USERS
where USERNAME like '&&PREFIX%'
and USERNAME NOT LIKE '%_IAU_APPEND'
and USERNAME NOT LIKE '%_IAU_VIEWER'
/

SELECT DBMS_METADATA.GET_GRANTED_DDL ('OBJECT_GRANT',USERNAME)
from DBA_USERS
where USERNAME like '&&PREFIX%'
and USERNAME NOT LIKE '%TLOGS'
and USERNAME NOT LIKE '%JMS'
/

spool off
EOF
```

8. Oracle Identity Governanceをクローニングする場合は、SOA DBMS Queuesを再起動してください。SOAINFRAスキーマ・ユーザーとして接続し、先に停止した各キューを再起動します。

```
$ sqlplus PREFIX_SOAINFRA@sourceDB
SQL> BEGIN

        DBMS_AQADM.START_QUEUE ('B2B_BAM_QUEUE');

        DBMS_AQADM.START_QUEUE ('EDN_OAOO_QUEUE');

        DBMS_AQADM.START_QUEUE ('EDN_EVENT_QUEUE');

        DBMS_AQADM.START_QUEUE ('IP_IN_QUEUE');

        DBMS_AQADM.START_QUEUE ('IP_OUT_QUEUE');

        DBMS_AQADM.START_QUEUE
        ('TASK_NOTIFICATION_Q');

END;

/
SQL> COLUMN name FORMAT A32
SQL> SELECT name,enqueue_enabled,dequeue_enabled
FROM USER_QUEUES where queue_type = 'NORMAL_QUEUE' order by name;

NAME                             ENQUEUE    DEQUEUE
-------------------------------- ---------- ----------
B2B_BAM_QUEUE                    YES        YES
EDN_EVENT_QUEUE                  YES        YES
EDN_OAOO_QUEUE                   YES        YES
IP_IN_QUEUE                      YES        YES
IP_OUT_QUEUE                     YES        YES
TASK_NOTIFICATION_Q              YES        YES

6 rows selected.
SQL> exit
```

9. OIM、SOA、およびBIPのWebLogic Server管理対象サーバーまたはクラスタを再起動します。

10. DDL SQLおよびData Pumpダンプ・ファイルをターゲット・データベースのホストにレプリケートします。
    - oim.dmp
    - oim_system.dmp
    - ddl.sql

**ターゲットOCI環境では次のとおりです。**

1. FMW要件に従ってターゲット・データベースを十分にインストール/構成します。
   使用するバージョンのOracle DatabaseをOCIにインストールします。このデータベースには、シングル・インスタンス・データベース、Oracle Real Applications Cluster（Oracle RAC）データベースがあります。これには、標準データベース、あるいはコンテナ・データベースと独立したプラガブル・データベース（PDB）のOIGなどがあります。

2. ターゲット・データベースが、『Oracle Identity and Access Management Installation Guide』に定義されているOracle Access Managerの基準すべてに合致するように構成されていることを確認します。

3. 必要に応じて、OCIのプラガブル・データベースのTNSエントリを作成します。たとえば、次のとおりです。

```
IGDPDB =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)
                 (HOST = iamdbhost.idm.tenancy.oraclevcn.com)
                 (PORT = 1521)
      )
      (CONNECT_DATA =
          (SERVER = DEDICATED)
          (SERVICE_NAME = igdpdb.idm.tenancy.oraclevcn.com)
      )
    )
```

4. ソースDBホスト上でエクスポート・プロセスのディレクトリの詳細情報を作成して設定します。
   a. OCI DBホスト上で十分な領域のある場所にディレクトリを作成します。
      $ mkdir -p /u01/installers/database
   b. ソース・データベースとターゲット・データベースでこの場所を参照するデータベース・ディレクトリ・オブジェクトを作成します。
      SQL> CREATE DIRECTORY orcl_full AS '/u01/installers/database';

5. トランザクションをロールバックする必要がある場合は、データベース・リストア・ポイントを作成します。

6. ソース環境と同じサービス名を使用して、新しいデータベースのデータベース・サービスを作成して起動します。
   たとえば次のとおりです。
   $ srvctl add service -db iamcdb_phx1g8 -pdb igdpdb -service *onpremservice* -rlbgoal SERVICE_TIME -clbgoal SHORT
   $ srvctl start service -db iamcdb_phx1g8 -service *onpremservice*
   $ srvctl status service -db iamcdb_phx1g8 -service *onpremservice*

7. エクスポートしたData Pumpダンプ・ファイルとSQLファイルがターゲット・データベース・ホスト上の正しいディレクトリで使用でき、データベースのDBAディレクトリ名とパスが一致していることを確認します。

```
$ ls -al /u01/installers/database
$ sqlplus / as sysdba
SQL> ALTER SESSION SET CONTAINER = igdpdb;
SQL> CREATE DIRECTORY orcl_full AS '/u01/installers/database';
```

確認するには、以下を実行します。

```
$ sqlplus / as sysdba
SQL> ALTER SESSION SET CONTAINER = igdpdb;
```

```
SQL> COLUMN directory_name FORMAT A32
SQL> COLUMN directory_path FORMAT A64
SQL> set linesize 128
SQL> SELECT directory_name,directory_path  FROM dba_directories ORDER BY directory_name;
```

8. 必要とされるDBMS_SHARED_POOLおよびXATRANSデータベース・オブジェクトが存在することを確認し、もし存在しない場合は作成します。スキーマ・エクスポート・ダンプがリストアされるターゲット・データベースで、以下の各SQLの数が2であることを確認します。

```
SQL> SELECT COUNT(*) FROM dba_objects
WHERE owner = 'SYS' AND object_name = 'DBMS_SHARED_POOL'
AND object_type IN ('PACKAGE','PACKAGE BODY');

  COUNT(*)
------------
         2

SQL> SELECT COUNT(*) FROM dba_objects
WHERE owner = 'SYS' AND object_name like '%XATRANS%';

  COUNT(*)
------------
         0
```

   c. DBMS_SHARED_POOLの数が2未満の場合、適切なSQLを実行して再構成します。

```
SQL> @/u01/app/oracle/product/19.0.0.0/dbhome_1/rdbms/admin/dbmspool.sql
SQL> @/u01/app/oracle/product/19.0.0.0/dbhome_1/rdbms/admin/prvtpool.plb
```

   d. XATRANSの数が2未満の場合、適切なSQLを実行して再構成します。

```
SQL> @/u01/app/oracle/product/19.0.0.0/dbhome_1/rdbms/admin/xaview.sql
```

9. 正しいフォルダからソース・データベースのシステム・ダンプをインポートして、schema_version_registry表およびビューを作成してから、必要なパブリック・シノニムをSQL経由で手動で作成します。

```
$ cd /u01/installers/database
$ impdp ¥"SYS/<password>@<targetdb> AS SYSDBA¥" ¥
      PARALLEL=4
      DIRECTORY=orcl_full ¥
      DUMPFILE=idm_system.dmp ¥
      LOGFILE=idm_system_imp.log ¥
      FULL=YES;

      $ sqlplus / as sysdba

      SQL> alter session set container=igdpdb;


      SQL> CREATE PUBLIC SYNONYM schema_version_registry FOR system.schema_version_registry;
      SQL> exit
```

10. schema_version_registry表データがソース環境と一致することを確認します。
    以下のクエリーがデプロイメントとの一貫性がある行を返すことを確認することが重要です。この表は、上記の手順の一部としてインポートされている必要があります。これに失敗した場合は、ソース・システムの値を用いて表を移入する必要があります。

    ```
    $ sqlplus / as sysdba
    SQL> alter session set container=igdpdb;
    SQL> set linesize 100
    SQL> col comp_id for a10
    SQL> col comp_name for a50
    SQL> col version for a10
    SQL> select comp_id, comp_name, version, status, upgraded
    from system.schema_version_registry;
    ```

    出力は次のようになります。

    | COMP_ID | COMP_NAME | VERSION | STATUS | U |
    |---|---|---|---|---|
    | IAU | Audit Service | 12.2.1.2.0 | VALID | N |
    | IAU_APPEND | Audit Service Append | 12.2.1.2.0 | VALID | N |
    | IAU_VIEWER | Audit Service Viewer | 12.2.1.2.0 | VALID | N |
    | MDS | Metadata Services | 12.2.1.3.0 | VALID | N |
    | OAM | Oracle Access Manager | 12.2.1.3.0 | VALID | N |
    | OPSS | Oracle Platform Security Services | 12.2.1.0.0 | VALID | N |
    | STB | Service Table | 12.2.1.3.0 | VALID | N |
    | WLS | WebLogic Services | 12.2.1.0.0 | VALID | N |

11. ソース・データベースからDDL SQLを実行して、同じパスワード、システム付与、およびオブジェクト付与を用いて、必要な表領域、スキーマ・ユーザーを作成します。PDBを使用している場合は、コンテナを正しく設定するようにしてください。

    ```
    $ sqlplus / as sysdba
    SQL> alter session set container=igdpdb;
    SQL> @'/u01/installers/database/ddl.sql'
    SQL> exit
    ```

12. FMWアプリケーションのスキーマ・ダンプをインポートします。
    注：ユーザーを事前作成したため、ORA-31684エラーが生じます。以下のタイプのエラーは無視します。
    - プロシージャ/パッケージ/関数/トリガー・コンパイル警告
    - DBMS_AQエラー
    - ORA-31684:Object type USER:"" already exists

    たとえば次のとおりです。

    ```
    $ cd /u01/installers/database
    $ impdp ¥"SYS/<password>@<targetdb> AS SYSDBA¥" ¥
        PARALLEL=4 ¥
        DIRECTORY=orcl_full ¥
        DUMPFILE=idm.dmp ¥
        LOGFILE=oim_imp.log
        FULL=YES;
    ```

13. インポートされたスキーマの無効なオブジェクトを問い合わせて、無効なオブジェクトを含む各スキーマの再コンパイルを実行します。

たとえば次のとおりです。

```
$ sqlplus / as sysdba
SQL> alter session set container=igdpdb;
SQL> COLUMN owner FORMAT A24
SQL> COLUMN object_type FORMAT A12
SQL> COLUMN object_name FORMAT A32
SQL> SET LINESIZE 128
SQL> SET PAGESIZE 50

SQL> SELECT owner,object_type,object_name, status
FROM dba_objects
WHERE status = 'INVALID'
AND owner like '<RCUPREFIX>%
ORDER BY owner, object_type, object_name;

OWNER                          OBJECT_TYPE      OBJECT_NAME                              STATUS
------------------------------ ---------------- ---------------------------------------- -------------
IGDUPG_OIM                     SYNONYM          ALTERNATE_ADF_LOOKUPS                    INVALID
IGDUPG_OIM                     SYNONYM          ALTERNATE_ADF_LOOKUP_TYPES               INVALID
IGDUPG_OIM                     SYNONYM          FND_LOOKUPS                              INVALID
IGDUPG_OIM                     SYNONYM          FND_STANDARD_LOOKUP_TYPES                INVALID


SQL> EXECUTE UTL_RECOMP.RECOMP_SERIAL('IGDUPG_OIM');

SQL> SELECT owner,object_type,object_name, status
FROM dba_objects
WHERE status = 'INVALID'
AND owner like '<RCUPREFIX>%
ORDER BY owner, object_type, object_name;

no rows selected
```

14. Oracle Identity Governanceをクローニングする場合は、SOA DBMS Queuesを起動します。
    e. ユーザー・キューのSOAINFRAスキーマ・ユーザーおよびクエリーとして接続します。

```
$ sqlplus <PREFIX>_SOAINFRA@<sourceDB>
SQL> COLUMN name FORMAT A32
SQL> SELECT name,enqueue_enabled,dequeue_enabled FROM USER_QUEUES where queue_type =
'NORMAL_QUEUE' order by name;

NAME                             ENQUEUE    DEQUEUE
-------------------------------- ---------- ----------
B2B_BAM_QUEUE                    YES        YES
EDN_EVENT_QUEUE                  YES        YES
EDN_OAOO_QUEUE                   YES        YES
IP_IN_QUEUE                      YES        YES
IP_OUT_QUEUE                     YES        YES
TASK_NOTIFICATION_Q              YES        YES

6 rows selected.
```

    f. 各キューを起動します。

```
SQL> BEGIN

DBMS_AQADM.START_QUEUE ('B2B_BAM_QUEUE');

DBMS_AQADM.START_QUEUE ('EDN_OAOO_QUEUE');
```

```
DBMS_AQADM.START_QUEUE ('EDN_EVENT_QUEUE');

DBMS_AQADM.START_QUEUE ('IP_IN_QUEUE');

DBMS_AQADM.START_QUEUE ('IP_OUT_QUEUE');

DBMS_AQADM.START_QUEUE ('TASK_NOTIFICATION_Q');

END;


/ exit
```

## ソース・バイナリのクローニング

ソース・システムとターゲット・システムが使用するOracleバイナリは、同一であることが必要です。これをもっとも簡単に実現する方法は、好みのバックアップ・ツールを使用してバックアップおよびリストア操作を実行することです。以下の例では、tarを使用します。

好みのバックアップ・ツールを使用して、ソース・サイトのOIMHOST1から以下の場所のバックアップを作成します。

- oraInventory
- MW_HOME

次に例を示します。

```
tar cvzPpsf oim_binaries.tar.gz ¥
    /u01/oracle/oraInventory ¥
    /u01/oracle/products/identity

tar cvzPpsf oam_binaries.tar.gz ¥
    /u01/oracle/oraInventory ¥
    /u01/oracle/products/access

tar cvzPpsf ldap_binaries.tar.gz ¥
    /u01/oracle/oraInventory ¥
    /u01/oracle/products/dir
```

## WebLogicドメインのクローニング

ソースWebLogic Serverドメインをクローニングする際は、プロセスのバックアップ部分の期間中にドメインを完全にシャットダウンすることを推奨します。WebLogic Serverおよびノード・マネージャのプロセスの実行時には、クローニングされた環境の起動に干渉する可能性のある多数のロック・ファイルが作成され、完全に静止しないと処理中のランタイム・トランザクションに一貫性がなくなる場合があります。

## ホスト・ファイルによるOCIでのソース・ホスト名およびFQDNのオーバーライドの確認

クローニングされたドメイン構成のホスト名およびSCANアドレスが、OCI IPアドレスに正しく解決されることを確認します。

1. 以前列挙したソース・ホスト/ソースFQDNが、/etc/hostsファイルのOCI IPアドレスの一覧に表示されていることを確認します。例については、前述の「OCIホスト・ファイル」のセクションを参照してください。

2. OCIホストからソースFQDNにpingを実行し、pingが正しいIPアドレスで応答することを確認します。

## ドメインの完全なシャットダウン

すべてのホストでバックアップ・プロセスが完了するまで、すべての管理対象サーバー、管理サーバー、およびノード・マネージャ・プロセスを停止します。

### ソース・ドメイン構成のバックアップの作成

1. 好みのバックアップ・ツールを使用して、ソース・サイトのOIMHOST1から以下の場所のバックアップを作成します。
   - ASERVER_HOME
   - MSERVER_HOME
   - キーストア
   - ノード・マネージャ構成ファイル

   *注：『エンタープライズ・デプロイメント・ガイド』に記載されているような分離されたDOMAIN_HOMEではなく、組み合わされたDOMAIN_HOMEを使用している場合は、ASERVER_HOMEやMSERVER_HOMEではなく、DOMAIN_HOMEを含めてください。*

   *注：tarを使用する場合は、必ず権限とルート・パスを保持してください。*

   たとえば、一般的なエンタープライズ・デプロイメントの場合、バックアップ・コマンドは以下のようになります。

   Oracle Identity Governanceの場合

   ```
   tar cvzPpsf oimhost1_config.tar.gz ¥

       /u01/oracle/config/nodemanager/OIMHOST1 ¥
       /u01/oracle/config/nodemanager/OIMHOST2 ¥
       /u01/oracle/config/nodemanager/IGDADMINVHN ¥
       /u01/oracle/config/keystores ¥
       /u01/oracle/runtime/domains/IAMGovernanceDomain ¥
       /u01/oracle/config/domains/IAMGovernanceDomain ¥
       /u02/private/oracle/config/domains/IAMGovernanceDomain
   ```

   Oracle Access Managerの場合

   ```
   tar cvzPpsf oamhost1_config.tar.gz ¥

       /u01/oracle/config/nodemanager/OAMHOST1 ¥
       /u01/oracle/config/nodemanager/OAMHOST2 ¥
       /u01/oracle/config/nodemanager/IADADMINVHN ¥
       /u01/oracle/config/keystores ¥
       /u01/oracle/config/domains/IAMAccessDomain ¥
       /u02/private/oracle/config/domains/IAMAccessDomain
   ```

   Oracle Internet Directory 12cの場合

   ```
   tar cvzPpsf oamhost1_config.tar.gz ¥

       /u01/oracle/config/nodemanager/LDAPHOST1 ¥
       /u01/oracle/config/nodemanager/LDAPHOST2 ¥
   ```

/u01/oracle/config/domains/OIDDomain ¥
/u02/private/oracle/config/domains/OIDDomain

2. 追加のすべてのノードについて繰り返します。たとえば、OIMHOST2に対するコマンドは以下のようになります。
   tar cvzPpsf OIMHOST2.tar.gz /u02/private/oracle/config/domains/IAMGovernanceDomain

## ドメインの起動

すべてのノード・マネージャ・プロセス、管理サーバー、およびすべての管理対象サーバーを起動します。

## バックアップ・ファイルのターゲット環境へのレプリケート

生成されたバックアップ・ファイルを適切なOCIホストへコピーします。

## OCIインスタンスのバックアップのリストア

### 構成バックアップのリストア

好みの抽出ツールを使用して、バイナリ・バックアップをOCIノードへ抽出します。共有ストレージを使用している場合、これを実行する必要があるのは共有ごとに1度だけです。

注：tarを使用する場合は、必ず権限とルート・パスを保持してください。

OIMHOST1の場合

```
tar xvzPpsf oig_binaries.tar.gz
```

OAMHOST1の場合

```
tar xvzPpsf oam_binaries.tar.gz
```

LDAPHOST1の場合

```
tar xvzPpsf ldap_binaries.tar.gz
```

### 構成バックアップのリストア

好みの抽出ツールを使用して、バックアップをOCIノードへ抽出します。

注：tarを使用する場合は、必ず権限とルート・パスを保持してください。

たとえば次のとおりです。

OIMHOST1の場合

```
tar xvzPpsf oimhost1_config.tar.gz
```

OIMHOST2の場合

```
tar xvzPpsf oimhost2_config.tar.gz
```

OAMHOST1の場合

```
tar xvzPpsf oamhost1_config.tar.gz
```

OAMHOST2の場合

```
tar xvzPpsf oamhost2_config.tar.gz
```

LDAPHOST1の場合

```
tar xvzPpsf ldaphost1_config.tar.gz
```

LDAPHOST2の場合

```
tar xvzPpsf ldaphost2_config.tar.gz
```

### ソース環境からコピーされたロック・ファイルおよびログ・ファイルのクリーンアップ

ドメインのオンラインバックアップを試みた場合は、実行中のドメインからコピーされたすべてのロック・ファイルを削除します。また、必要に応じて、ソース環境から古いログ・ファイルをクリーンアップします。

たとえば次のとおりです。

OIMHOST1の場合

```
# ロック・ファイルのクリーンアップ：

find /u01/oracle/config/nodemanager  -type f -name "*.lck" -exec rm -f {} ¥;

find /u01/oracle/config/domains/IAMGovernanceDomain ¥
    -type f ¥( -name "*.lck" -or -name "*.lok" ¥) -print -exec rm -f {} ¥;

find /u02/private/oracle/config/domains/IAMGovernanceDomain ¥
    -type f ¥( -name "*.lck" -or -name "*.lok" ¥) -print -exec rm -f {} ¥;

# Log File Cleanup:

find /u01/oracle/config/nodemanager/OIMHOST1 ¥
    -type f ¥( -name '*.log' -or -name '*.out' ¥) -print -exec rm -f {} ¥;

find /u01/oracle/config/nodemanager/OIMHOST2 ¥
    -type f ¥( -name '*.log' -or -name '*.out' ¥) -print -exec rm -f {} ¥;

find /u01/oracle/config/nodemanager/IGDADMINVHN ¥
    -type f ¥( -name '*.log' -or -name '*.out' ¥) -print -exec rm -f {} ¥;

find ${ASERVER_HOME}/servers/AdminServer/logs ¥
    -type f ! -size 0c -print -exec rm -f {} ¥+

find ${MSERVER_HOME}/servers/*/logs ¥
    -type f ! -size 0c -print -exec rm -f {} ¥+
```

OIMHOST2の場合

```
# ロック・ファイルのクリーンアップ：

find /u02/private/oracle/config/domains/IAMGovernanceDomain ¥
    -type f ¥( -name "*.lck" -or -name "*.lok" ¥) -print -exec rm -f {} ¥;

# Log File Cleanup:

find ${MSERVER_HOME}/servers/*/logs ¥
    -type f ! -size 0c -print -exec rm -f {} ¥+
```

### OCIにクローニングされたドメインの起動

OCIインスタンスへのバックアップのリストアが完了したら、OCIでドメインを起動します。

- ASERVER_HOMEのノード・マネージャを起動
- すべてのノードでMSERVER_HOMEのノード・マネージャを起動
- 管理サーバーを起動してログを確認
- OAM管理対象サーバー/クラスタを起動（OAM）
- ポリシー管理対象サーバー/クラスタを起動（OAM）
- SOA管理対象サーバー/クラスタを起動してログを確認（OIG）
- ビジネス・インテリジェンス・プラットフォーム管理対象サーバー/クラスタを起動してロゴを確認（OIG）
- OIM管理対象サーバー/クラスタを起動してログを確認（OIG）

## Oracle Internet Directoryインスタンスのクローニング

Oracle Internet Directory 12cをクローニングし、それをWeblogicドメインにデプロイした場合は、Weblogicドメインのクローニングに関する前述の手順に従う必要があります。

Oracle Internet Directory 11gからクローニングを実行する場合は、インスタンス・ディレクトリをOCIにクローニングする必要があります。たとえば次のとおりです。

### ソース・インスタンス構成のバックアップの作成

好みのバックアップ・ツールを使用して、ソース・サイトのOIMHOST1から以下の場所のバックアップを作成します。

- INSTANCE_HOME

*注：tarを使用する場合は、必ず権限とルート・パスを保持してください。*

たとえば、バックアップ・コマンドは以下のようになります。

```
tar cvzPpsf ldaphost1_config.tar.gz ¥
    /u02/private/oracle/config/instances/oid1
```

LDAPHOSTごとに、上記の手順を繰り返します。

### バックアップ・ファイルのターゲット環境へのレプリケート

生成されたバックアップ・ファイルを適切なOCIホストへコピーします。

### OCIインスタンスのバックアップのリストア

好みの抽出ツールを使用して、バックアップをOCIノードへ抽出します。

注：tarを使用する場合は、必ず権限とルート・パスを保持してください。

たとえば次のとおりです。

LDAPHOST1の場合

```
tar xvzPpsf ldaphost1_config.tar.gz
```

### OIDインスタンスの起動

以下のコマンドを使用してOIDインスタンスを起動できるようになりました。

*INSTANCE_HOME*/bin/opmnctl startall

## Oracle Unified Directoryのクローニング

Oracle Unified Directoryのクローニングは、追加のOracle Unified Directoryレプリカを既存のデプロイメントに加えるプロセスですが、新しいレプリカはOCI内に存在します。

詳しくは、『Oracle Unified Directoryインストール・ガイド』を参照してください。

### OCIでのOUDレプリカの作成

必要な手順を次に示します。

1. 環境変数JAVA_HOMEをJAVA_HOMEに設定します。
2. ディレクトリをDIR_ORACLE_HOME/oudに変更します。
3. 環境変数INSTANCE_NAMEを../../admin/oud2に設定します。

   たとえば次のとおりです。

   export INSTANCE_NAME=../../../../u02/private/oracle/config/instances/oud2
4. 次のコマンドを実行して、Oracle Unified Directory構成アシスタントを起動します。

   ./oud-setup
5. 次の点を除いて、『エンタープライズ・デプロイメント・ガイド』に記載されているように設定画面を完了します。
   a. トポロジ・オプション画面で、「This server will be part of a replication topology」を選択していることを確認してください。ソース環境がレプリケーション用に設定されていない場合でも、このオプションを選択してください。
   b. トポロジ・オプション画面で、「There is already a server in the topology」を選択し、ソース・ホストの1つとその資格証明を入力します。
   c. ここで初めてレプリケーションを設定する場合は、グローバル管理者IDを作成するように求められます。
6. インスタンスを作成したら、ソース・システムのすべてのデータがOCIインスタンスにレプリケートされます。

## OUDの変更ログへのアクセス権の付与

インスタンスが作成されたため、変更ログにアクセス権を付与する必要があります。これは、以下のコマンドを使用して実行できます。これらのコマンドは、新しいインスタンスに対してのみ実行されます。

1. OUD管理パスワードを含むパスワード・ファイルを作成します。この例では、passwordfileという名前を使用します。

2. 以下のコマンドを実行して、既存の変更ログの権限を削除します。

```
OUD_ORACLE_INSTANCE/OUD/bin/dsconfig set-access-control-handler-prop ¥
--remove ¥
global-aci:"(target=¥"ldap:///cn=changelog¥")(targetattr=¥"*¥")(version  3.0; acl
¥"External changelog access¥"; deny (all) userdn=¥"ldap:///anyone¥";)" ¥
        --hostname OUD Host ¥
        --port OUD Admin Port ¥
        --trustAll ¥
        --bindDN cn=oudadmin ¥
         -bindPasswordFile passwordfile ¥
        --no-prompt
```

3. 以下のコマンドを使用して、新しいOCIを追加します。

```
OUD_ORACLE_INSTANCE/OUD/bin/dsconfig  set-access-control-handler-prop  ¥
--add ¥

global-aci:"(target=¥"ldap:///cn=changelog¥")(targetattr=¥"*¥")(version  3.0; acl ¥"External changelog
access¥"; allow (read,search,compare,add,write,delete,export)
groupdn=¥"ldap:///cn=OIMAdministrators,cn=groups,dc=example,dc=com¥";)" ¥
        --hostname OUD Host ¥
        --port OUD Admin Port ¥
        --trustAll ¥
        --bindDN cn=oudadmin ¥
        --bindPasswordFile passwordfile ¥
        --no-prompt
```

OIMAdministratorsは、OIMを管理するためにLDAPにあるグループです。詳しくは、『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。

## OUD索引の作成

新しく作成したインスタンスにOUDのローカル索引を作成します。そのために、次のコマンドを実行します。

```
OUD_ORACLE_INSTANCE/OUD/bin/ldapmodify -h LDAPHOST2.example.com -Z -X -p 4444 -a -D
"cn=oudadmin" -j passwordfile -c ¥-f IAD_ORACLE_HOME/idm/oam/server/oim-
intg/ldif/ojd/schema/ojd_user_index_generic.ldif

OUD_ORACLE_INSTANCE/OUD/bin/ldapmodify -h LDAPHOST2.example.com -Z -X -p 4444 -a -D
"cn=oudadmin" -j passwordfile -c ¥-f
IAD_ORACLE_HOME/idm/idmtools/templates/oud/oud_indexes_extn.ldif
```

索引を作成したら、以下のコマンドを使用して索引を強制的に再構築する必要があります。

1. 次のコマンドを使用してOUDインスタンスをシャットダウンします。

```
OUD_ORACLE_INSTANCE/OUD/bin/stop-ds
```

2. 次のコマンドを実行します。

   OUD_ORACLE_INSTANCE/OUD/bin/rebuild-index --rebuildAll -b "dc=example,dc=com"

3. 次のコマンドを使用して、OUDインスタンスを再起動します。

   OUD_ORACLE_INSTANCE/OUD/bin/start-ds

## クローン環境へのアクセスの検証

Oracle HTTPサーバー経由でOracle Identity and Access Managementのインストールを実行する場合は、このドメインのクローンを検証する前に、それらを最初にOCIに移行しておく必要があります。

環境には、直接またはロードバランサ経由でアクセスでき、この構成はカットオーバー時まで変更しないでください。ただし、ローカル・ホスト・ファイルの環境のホスト名を優先させることにより、構成を引き続き検証できます。

たとえば、Oracle Identity Managerインストールでは、以下のようなエントリ・ポイントを使用してアプリケーションにアクセスします。

- http://igdadmin.example.com/console
- http://igdadmin.example.com/identity
- https://login.example.com

これらのURLのホスト名は、企業DNSによって、リクエストをルーティングするロードバランサのIPアドレスに解決されます。ソース環境のIPアドレスへのデフォルトの名前解決をオーバーライドするには、これらのホスト名が、トラフィックをOCIホストに送信する別のロードバランサ、または内部のOCIロードバランサ（構成済みの場合）を参照するようにします。

クローン環境の起動前に検証を行う目的で、クライアント・システムのローカル・ホスト・ファイルを使用して、環境の本稼働の前に、必要に応じてオンプレミス・ホストのIPアドレスをOCIコンピュート・インスタンスのIPアドレスにオーバーライドします。これは、ブラウザで使用されるクライアント・ワークステーションでのみ、OCIコンピュート・インスタンスで使用されるのと同じ構成です。

1. ワークステーションの/etc/hostsファイル・エントリを更新して検証します。
2. クライアントOS DNSキャッシュを消去します。
3. ブラウザ・キャッシュを消去します。
4. ロードバランサおよび管理対象サーバー（アクセス可能な場合）のソース環境のFQDN、および必要に応じてデータベース・アドレス（またはSCAN）にpingを実行します。OCI IPアドレスからレスポンスがあることを確認します。
   - igdadmin.example.com
   - login.example.com
   - oimhost1.example.com
   - oimhost2.example.com
   - ldaphost1.example.com
   - ldaphost2.example.com
   - src-DB-SCAN.example.com
5. ソース環境のFQDNを使用してOIM URLエンドポイントを参照します。
   注：webgateおよびOAMがまだ完全にデプロイされていない、または機能していない場合は、この検証の間httpd.confのwebgateを無効化してください。
   - https://igdadmin.example.com/console
   - https://igdadmin.example.com/identity
6. クライアント・トラフィックがOCI WEBHOST1/2 OHSアクセス・ログに記録されていることを確認します。
7. リクエストがWebLogic Serverログに記録されていることを確認します。

参照するとログイン・ページにリダイレクトされ、ログイン資格証明を入力すると、Oracle WebLogic Consoleが表示されます。このやり取りを経てアクセス・ログにリクエストが表示されると、クローンへのログインが成功したことになります。

必要に応じて、他のテストを実行します。

## クローニング後のタスク

### OIM LDAPの統合された完全なリコンシリエーション・ジョブの実行

Oracle Internet Directoryのレプリケーションを使用してOracle Internet Directoryのクローニングを行った場合、変更番号は同期されなくなります。ドメインを同期状態に戻すには、Oracle Identity Governanceの完全なリコンシリエーション・ジョブを再実行する必要があります。

ドメインをクローニングした後は、完全なリコンシリエーション・ジョブを実行する必要があります。詳しくは、『Oracle Fusion Middleware Oracle Identity Manager管理者ガイド』を参照してください。

1. https://igdadmin.example.com/sysadminを参照し、xelsysadmとして認証します。
2. 左ペインのSystem Configurationで「Scheduler」をクリックします。ポップアップ・ウィンドウが表示されます。
3. IDシステム管理ポップアップ・ウィンドウで、スケジュールされたジョブLDAP Consolidated Full Reconciliationを検索します。

   Oracle Identity Governance 12cをクローニングしていて、コネクタ・ベースの同期に移行した場合は、次のジョブを実行する必要があります。

   - SSO Connector Integration Group Full Reconciliation
   - SSO Connector Integration User Reconciliation
   - SSO Connector Integration Group Membership Full Reconciliation
   - SSO Connector Integration Group Hierarchy Sync Full Reconciliation

4. 検索結果の「LDAP Consolidated Full Reconciliation」エントリをクリックして、ジョブの詳細を表示します。
5. 「Run Now」ボタンをクリックしてジョブを実行し、確認メッセージ"Job is running"を確認します。
6. 定期的に「Refresh」ボタンをクリックして、ジョブ・ステータスを確認します。
7. ジョブ・ステータスに"Stopped"が表示された場合は、"Success"の実行ステータスを検証します。ログをチェックし、必要に応じてトラブルシューティングを実行します。

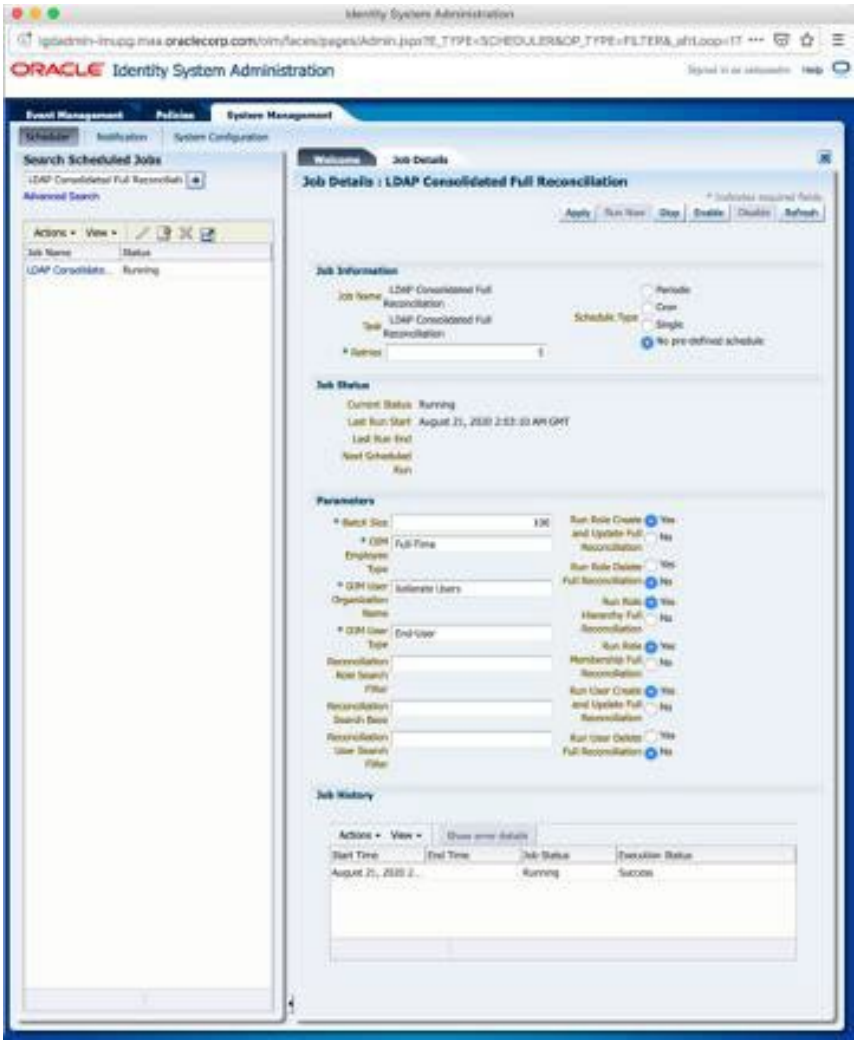
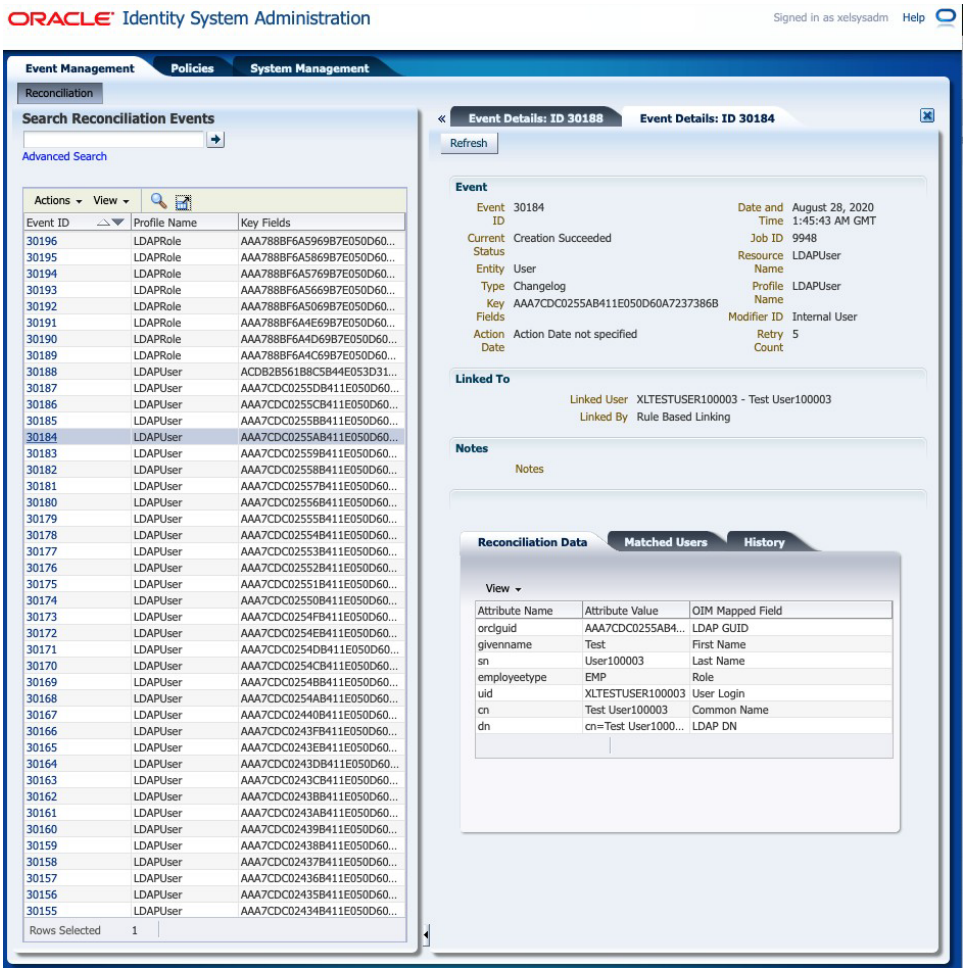



図3 - IDシステム管理 - スケジュールされたジョブの詳細 - LDAP Consolidated Full Reconciliation

8. タブを"Event Management"に切り替えて、最近のすべてのリコンシリエーション・イベントに対して空の検索を実行します。
9. イベントにスポットチェックを実行し、現在のステータスが"Creation Succeeded"またはUpdate Succeeded"であることを確認します。




## ユニキャストへのOIMオブジェクト・キャッシュの移行

オンプレミス環境からOracle Identity Managerを移行している場合に、OIMキャッシュでマルチキャスト通信を使用しているユーザーもいるかもしれませんが、OCIを含め多くのクラウド環境ではマルチキャストを利用できません。マルチキャストを使用している場合は、以下の資料の手順に従ってユニキャストに変換する必要があります。

How To Deploy OIM Cluster With Unicast Configuration For Cachine（Doc ID 2387392.1）

## OCIへのカットオーバー

OCIデプロイメントにスイッチオーバーする準備ができたら、既存のリソースが新しいOCIデプロイメントを参照するようにする必要があります。

### ロードバランサのカットオーバー

Oracle IdentityおよびAccessのデプロイメントにロードバランサ経由でアクセスする場合は、2つのオプションを使用できます。つまり、新しいアプリケーションにアクセスするために構成するOCI内部のロードバランサを使用するように切り替えるか、または新しいOCI OIMデプロイメントを参照するように既存のオンプレミス・ロードバランサを再構成します。

### OCIロードバランサ

新しいOCIロードバランサを構成した場合は、必ずSSL証明書を既存のオンプレミス・ロードバランサから新しいOCIロードバランサへロードしてください。

アプリケーションの完全修飾ホスト名（igdadmin.example.comなど）がOCIロードバランサ内の仮想ホストを参照するように、DNSを更新します。

### オンプレミス・ロードバランサ

デプロイメントで引き続き使用したいオンプレミス・ロードバランサがある場合は、新しいOAM OCIホストを既存のロードバランサ・プールに追加して、既存のエントリを削除する必要があります。

## 参考資料

- Oracle Cloud Infrastructureのドキュメント
- Oracle Cloud Infrastructureで安全にグラフィカル・アプリケーションを実行
- Oracle Fusion Middleware Supported System Configurations
- Oracle Identity and Access Managementエンタープライズ・デプロイメント・ガイド（11.1.2.3.0）
- Oracle Identity and Access Management Enterprise Deployment Guide（12.2.1.4.0）
- Upgrading Oracle Identity Governance 12.2.1.3
- Upgrading Oracle Identity Governance 12.2.1.4

## CONNECT WITH US

+1.800.ORACLE1までご連絡いただくか、oracle.comをご覧ください。
北米以外の地域では、oracle.com/contactで最寄りの営業所をご確認いただけます。

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


オンプレミスからOracle Cloud InfrastructureへのOracle Internet Directoryの移行
2021年5月
著者：Michael Rhys、寄稿者：Frank Rizzo