Oracle® Access Manager

インストレーション・ガイド

10*g*（10.1.4.0.1）

部品番号 : B31475-01

2006 年 11 月

このガイドには、Oracle Access Manager を使用環境に正常にインストールするために必要なあらゆる事項が記載されています。

ORACLE®

Oracle Access Manager インストレーション・ガイド , 10*g*（10.1.4.0.1）

部品番号 : B31475-01

原本名 : Oracle Access Manager Installation Guide, 10*g* (10.1.4.0.1)

原本部品番号 : B25353-01

原本著者 : Gail Tiberi

原本協力者 : Nina Wishbow, Norman Bock, Paresh Borkar, Pradnyesh Rane, Ramakrishna Narla, Chetan Barhate, Steven Frehe.

目次

5 WebPass のインストール

6 ID システムの設定

第 III 部　アクセス・システムのインストールおよび設定

7　Policy Manager のインストール

8　Access Server のインストール

9　WebGate のインストール

第 IV 部　オプションのコンポーネントのインストール

10　Oracle Virtual Directory を使用した Oracle Access Manager の設定

17 Oracle Access Manager のための Apache v2、IHS および OHS Web サーバーの構成

18 WebGates のための Lotus Domino Web サーバーの設定

第 VII 部 製品の削除、ヒント、トラブルシューティング

19 重要な注意事項

20 Oracle Access Manager の削除

第 VIII 部 付録

A Active Directory に対する Oracle Access Manager のインストール

B ADAM に対する Oracle Access Manager のインストール

C Oracle Access Manager インストール後のディレクトリ証明書の追加

D ディレクトリ・サーバー・ホストの変更

E インストールの問題のトラブルシューティング

索引

はじめに

このインストレーション・ガイドでは、サポートされているプラットフォーム上での Oracle Access Manager コンポーネントの基本的なインストールと設定の情報について説明します。能率的に作業するための考慮点、前提条件、準備ワークシート、および正常に操作するための手順についての説明も含まれます。

> **注意：** Oracle Access Manager の旧称は Oblix NetPoint および Oracle COREid です。

ここでは、次の項目について説明します。

対象読者

このマニュアルは、Oracle Access Manager コンポーネントをインストールする管理者を対象としています。

次の概念について理解していることを前提としています。

- オペレーティング・システムおよびファイル・システム（Windows ベースまたは UNIX ベース）
- インターネットに接続したサイトおよびネットワーキング・プロトコル
- ネットワーク・セキュリティ : ファイアウォールの構築、認証システムの配備など
- ホスト・セキュリティ : パスワード、UID、ファイル権限、ファイル・システム整合性など
- ネットワーク・セキュリティ : ファイアウォールの構築、認証システムの配備など
- Web サーバー、Web ブラウザおよび構成詳細
- データベース管理および使用する LDAP ディレクトリ

ドキュメントのアクセシビリティについて

オラクル社は、障害のあるお客様にもオラクル社の製品、サービスおよびサポート・ドキュメントを簡単にご利用いただけることを目標としています。オラクル社のドキュメントには、ユーザーが障害支援技術を使用して情報を利用できる機能が組み込まれています。HTML 形式のドキュメントで用意されており、障害のあるお客様が簡単にアクセスできるようにマークアップされています。標準規格は改善されつつあります。オラクル社はドキュメントをすべてのお客様がご利用できるように、市場をリードする他の技術ベンダーと積極的に連携して技術的な問題に対応しています。オラクル社のアクセシビリティについての詳細情報は、Oracle Accessibility Program の Web サイト `http://www.oracle.com/accessibility/` を参照してください。

ドキュメント内のサンプル・コードのアクセシビリティについて

スクリーン・リーダーは、ドキュメント内のサンプル・コードを正確に読めない場合があります。コード表記規則では閉じ括弧だけを行に記述する必要があります。しかし JAWS は括弧だけの行を読まない場合があります。

外部 Web サイトのドキュメントのアクセシビリティについて

このドキュメントにはオラクル社およびその関連会社が所有または管理しない Web サイトへのリンクが含まれている場合があります。オラクル社およびその関連会社は、それらの Web サイトのアクセシビリティに関しての評価や言及は行っておりません。

Oracle サポート・サービスへの TTY アクセス

アメリカ国内では、Oracle サポート・サービスへ 24 時間年中無休でテキスト電話（TTY）アクセスが提供されています。TTY サポートについては、(800)446-2398 にお電話ください。

関連ドキュメント

詳細は、Oracle Access Manager リリース 10*g*（10.1.4.0.1）ドキュメント・セット内の次のドキュメントを参照してください。

- 『Oracle Access Manager 概要』: Oracle Access Manager の概要、Oracle Access Manager のマニュアルへのロードマップ、および用語集を提供します。
- Oracle Application Server のリリース・ノート: 最新の Oracle Access Manager アップデートについて参照してください。リリース・ノートはプラットフォーム固有のマニュアルで入手できます。リリース・ノートの最新バージョンは、Oracle Technology Network のサイト `http://www.oracle.com/technology/documentation` で入手できます。
- 『Oracle Access Manager インストレーション・ガイド』: コンポーネントをインストールおよび構成する方法について説明します。
- 『Oracle Access Manager アップグレード・ガイド』: 以前のバージョンを最新バージョンにアップグレードする方法について説明します。
- 『Oracle Access Manager ID および共通管理ガイド』: ID システムのアプリケーションを構成してユーザー、グループおよび組織についての情報を表示する方法、および ID システムのアプリケーションに表示されるデータを表示および変更する権限をユーザーに割り当てる方法について説明します。またユーザーに関する基本情報の追加、ユーザーに関する追加情報の提供、および新規ユーザー・エントリの承認などの Identity アプリケーションの機能と結合するワークフローを、一連の自動実行の手順に構成する方法についても説明します。このマニュアルでは、ディレクトリ・プロファイル構成、パスワード・ポリシー構成、ロギングおよび監査などの、ID システムおよびアクセス・システムに共通の管理機能についても説明します。
- 『Oracle Access Manager アクセス管理ガイド』: ポリシー・ドメイン、認証スキームおよび認可スキームを定義してリソースを保護する方法、シングル・ドメインおよび複数ドメインでのシングル・サインオンを構成して 1 つのログインで複数のリソースにアクセスできるようにする方法、およびカスタム・ログイン・フォームを設計する方法について説明します。アクセス・システムを設定および管理する方法についても説明します。
- 『Oracle Access Manager デプロイメント・ガイド』: Oracle Access Manager を実行する環境の計画および管理の担当者向けの情報について説明します。容量計画、システム・チューニング、フェイルオーバー、ロード・バランシング、キャッシングおよび移行計画についても説明します。
- 『Oracle Access Manager カスタマイズ・ガイド』: Oracle Access Manager アプリケーションの表示形式を変更する方法や、オペレーティング・システム、Web サーバー、ディレクトリ・サーバー、ディレクトリの内容を変更したり、CGI ファイルまたは JavaScript を Oracle Access Manager 画面に接続することによって Oracle Access Manager を制御する方法について説明します。Access Manager API と、認可および認証プラグイン API についても説明します。
- 『Oracle Access Manager 開発者ガイド』: IdentityXML および WSDL を介してプログラムによって ID システム機能にアクセスする方法、カスタム WebGate（AccessGate）を作成する方法、およびプラグインを開発する方法について説明します。Oracle Access Manager 用の CGI ファイルまたは JavaScript をいつ作成するかを認識するための情報についても説明します。
- 『Oracle Access Manager 統合ガイド』: Oracle Access Manager を設定して、BEA WebLogic、Plumtree Portal および IBM WebSphere などのサード・パーティの製品とともに実行する方法について説明します。
- 『Oracle Access Manager スキーマ詳細』: Oracle Access Manager スキーマの詳細を説明します。

表記規則

このマニュアルでは次の表記規則を使用します。

規則	意味
太字	太字は、注意する必要のある見出しおよび情報を示します。また、太字は、操作に関連する Graphical User Interface 要素を示す場合もあります。
イタリック	イタリックは、ユーザーが特定の値を指定するプレースホルダ変数を示します。
固定幅フォント	固定幅フォントは、段落内のコマンド、URL、サンプル内のコード、画面に表示されるテキスト、または入力するテキストを示します。

サポートおよびサービス

次の各項に、各サービスに接続するための URL を記載します。

Oracle サポート・サービス

オラクル製品サポートの購入方法、および Oracle サポート・サービスへの連絡方法の詳細は、次の URL を参照してください。

```
http://www.oracle.co.jp/support/
```

製品マニュアル

製品のマニュアルは、次の URL にあります。

```
http://otn.oracle.co.jp/document/
```

研修およびトレーニング

研修に関する情報とスケジュールは、次の URL で入手できます。

```
http://www.oracle.co.jp/education/
```

その他の情報

オラクル製品やサービスに関するその他の情報については、次の URL から参照してください。

```
http://www.oracle.co.jp
http://otn.oracle.co.jp
```

注意： ドキュメント内に記載されている URL や参照ドキュメントには、Oracle Corporation が提供する英語の情報も含まれています。日本語版の情報については、前述の URL を参照してください。

Oracle Access Manager の新機能

この項では、Oracle Access Manager 10*g*（10.1.4.0.1）の新機能について説明し、このマニュアルの追加情報の指針を示しています。現行リリースへ移行中のユーザーのために、以前のリリースからの情報も記載しています。

次の項では、このマニュアルで扱っている Oracle Access Manager の新機能について説明します。

- 製品名およびコンポーネント名の変更
- Oracle Access Manager 10g（10.1.4.0.1）の新機能
- 各章の更新内容

> **注意：** Oracle Access Manager 10*g*（10.1.4.0.1）の新機能の包括的なリストおよびその説明箇所は、『Oracle Access Manager 概要』の「Oracle Access Manager の新機能」の章を参照してください。

製品名およびコンポーネント名の変更

元の製品名 Oblix NetPoint は、Oracle Access Manager に変更になりました。大部分のコンポーネント名の変更はありません。ただし、次の表に示すいくつかの重要な変更には留意する必要があります。

項目	以前	現在
製品名	Oblix NetPoint Oracle COREid	Oracle Access Manager
製品名	Oblix SHAREid NetPoint SAML Services	Oracle Identity Federation
製品名	OctetString Virtual Directory Engine（VDE）	Oracle Virtual Directory
製品リリース	Oracle COREid 7.0.4	Oracle Application Server 10*g* Release 2（10.1.2）の一部としても提供
ディレクトリ名	COREid Data Anywhere	Data Anywhere
コンポーネント名	COREid Server	Identity Server
コンポーネント名	Access Manager	Policy Manager
コンソール名	COREid システム・コンソール	ID システム・コンソール
ID システム・トランスポート・セキュリティ・プロトコル	NetPoint ID プロトコル	Oracle ID プロトコル
アクセス・システム・トランスポート・プロトコル	NetPoint Access プロトコル	Oracle Access プロトコル
管理者	NetPoint 管理者 COREid 管理者	マスター管理者
ディレクトリ・ツリー	Oblix ツリー	構成ツリー
データ	Oblix データ	構成データ
Software Developer Kit	Access Server SDK ASDK	Access Manager SDK
API	Access Server API Access API	Access Manager API
API	アクセス管理 API Access Manager API	Policy Manager API
デフォルト・ポリシー・ドメイン	NetPoint ID ドメイン COREid ID ドメイン	ID ドメイン
デフォルト・ポリシー・ドメイン	NetPoint Access Manager COREid Access Manager	Access ドメイン
デフォルト認証スキーム	NetPoint の認証なし COREid の認証なし	匿名
デフォルト認証スキーム	NetPoint Basic Over LDAP COREid Basic Over LDAP	Oracle Access and Identity Basic Over LDAP

項目	以前	現在
デフォルト認証スキーム	AD Forest 用の NetPoint Basic Over LDAP AD Forest 用の COREid Basic Over LDAP	AD Forest 用の Oracle Access and Identity Basic Over LDAP
アクセス・システム・サービス	AM サービスのステータス	Policy Manager API サポート・モード

製品またはドキュメント内で使用されている従来の名称は、新しい名前を意味しています。

Oracle Access Manager 10*g*（10.1.4.0.1）の新機能

このマニュアルでは、次の機能について説明します。

- グローバリゼーション

  このマニュアルでは、Oracle Access Manager 10*g*（10.1.4.0.1）のインストールに重点が置かれ、英語（AMERICAN）以外のオペレーティング・システムのマシン上にインストールする場合に必要な情報、およびオラクル社提供の言語パックのインストールに関する詳細が含まれています。

  関連項目： 第 3 章「マルチ言語環境の概要」

  インストールの章にある各コンポーネントの前提条件

- このリリースでは、Oracle HTTP Server（OHS）サポートは、WebPass コンポーネント、Access Manager コンポーネントおよび WebGate コンポーネントに対して提供されています。

  関連項目： 第 16 章「Apache v1.3 Web サーバーおよび Oracle HTTP Server Web サーバーの構成」

- このリリースでは、Oracle Internet Directory サポートは一般使用に含まれています。

  関連項目： 第 2 章「インストールの準備」、第 4 章「Identity Server のインストール」および 第 15 章「コンポーネントのレプリケート」

各章の更新内容

xx ページの「製品名およびコンポーネント名の変更」で説明しているように、一般的な製品および名前の変更がこのマニュアル全体で行われています。プラットフォームのサポートの詳細はこのマニュアルから削除され、現在は、`https://metalink.oracle.com` の「Certify」タブの下に移動されています。それぞれの章の更新内容および変更内容は、次のとおりです。

- 第 1 章「インストール・タスク、オプションおよびメソッドの概要」は整理されました。
- 第 2 章「インストールの準備」には、新しいコンポーネントをインストールする場合の考慮点が加えられました。インストールの考慮点は、以前はコンポーネントのインストールの章にありましたが、冗長性を排除して関連した内容をまとめるため、この準備の章に統合されました。マルチ言語環境の詳細は、別の章に移動しました。
- 第 3 章「マルチ言語環境の概要」には、マルチ言語環境でのインストール準備に関する新しい情報、およびオラクル社提供の言語パックのインストールに関する更新の詳細が含まれています。
- 第 4 章「Identity Server のインストール」は更新され、インストールの考慮点は第 2 章「インストールの準備」に移動しました。
- 第 5 章「WebPass のインストール」のインストールの考慮点は、第 2 章「インストールの準備」に移動しました。
- 第 7 章「Policy Manager のインストール」は更新され、インストールの考慮点は第 2 章「インストールの準備」に移動しました。
- 第 8 章「Access Server のインストール」は更新され、インストールの考慮点は第 2 章「インストールの準備」に移動しました。
- 第 9 章「WebGate のインストール」は更新され、インストールの考慮点は第 2 章「インストールの準備」に移動しました。
- 第 10 章「Oracle Virtual Directory を使用した Oracle Access Manager の設定」は、『Oracle Access Manager 統合ガイド』から移動し、説明のマイナー・チェンジ、グラフィックを説明する新しい情報、および DN 変換ツールの更新表が追加されています（OctetString 社はオラクル社に買収されました）。
- 第 13 章「データベースの監査コンポーネントのインストール概要」では、この機能の概要について説明しています。詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。
- 第 14 章「Software Developer Kit の概要」は、Software Developer Kit（SDK）の個別インストールについて簡単な概要を説明するために追加されました。詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。
- 第 15 章「コンポーネントのレプリケート」は更新され、新しい構文およびコマンドが追加されています。
- 第 16 章「Apache v1.3 Web サーバーおよび Oracle HTTP Server Web サーバーの構成」は更新され、OHS に関する詳細および WebGate パフォーマンスに関する新しい情報が追加されています。
- 第 17 章「Oracle Access Manager のための Apache v2、IHS および OHS Web サーバーの構成」は更新され、OHS に関する情報および Apache ベースの Web サーバーに関する新しい情報が追加されています。
- 第 19 章「重要な注意事項」は、これまで importantnotes.txt というファイルに含まれていた詳細を記載するために追加されました。
- 第 20 章「Oracle Access Manager の削除」は新しい章で、言語パックなどのコンポーネントのアンインストールと、スキーマ・オブジェクトおよび Web サーバー構成詳細の削除に関する詳細を説明しています。
- 付録 B「ADAM に対する Oracle Access Manager のインストール」は更新され、スキーマ手動更新の要件が反映されています。
- 付録 E「インストールの問題のトラブルシューティング」は新しい情報で更新され、1 つの付録にまとめられました。

第 I 部

インストールの計画と前提条件

ここでは、Oracle Access Manager のインストールの概要、要件および前提条件について説明します。

第 I 部は、次の章で構成されます。

- 第 1 章「インストール・タスク、オプションおよびメソッドの概要」
- 第 2 章「インストールの準備」
- 第 3 章「マルチ言語環境の概要」

1

インストール・タスク、オプションおよびメソッドの概要

この章では、Oracle Access Manager 10*g*（10.1.4.0.1）をインストールする概要について説明します。次の項目について説明します。

- インストール・タスクの概要
- インストール・オプション
- インストール・メソッド

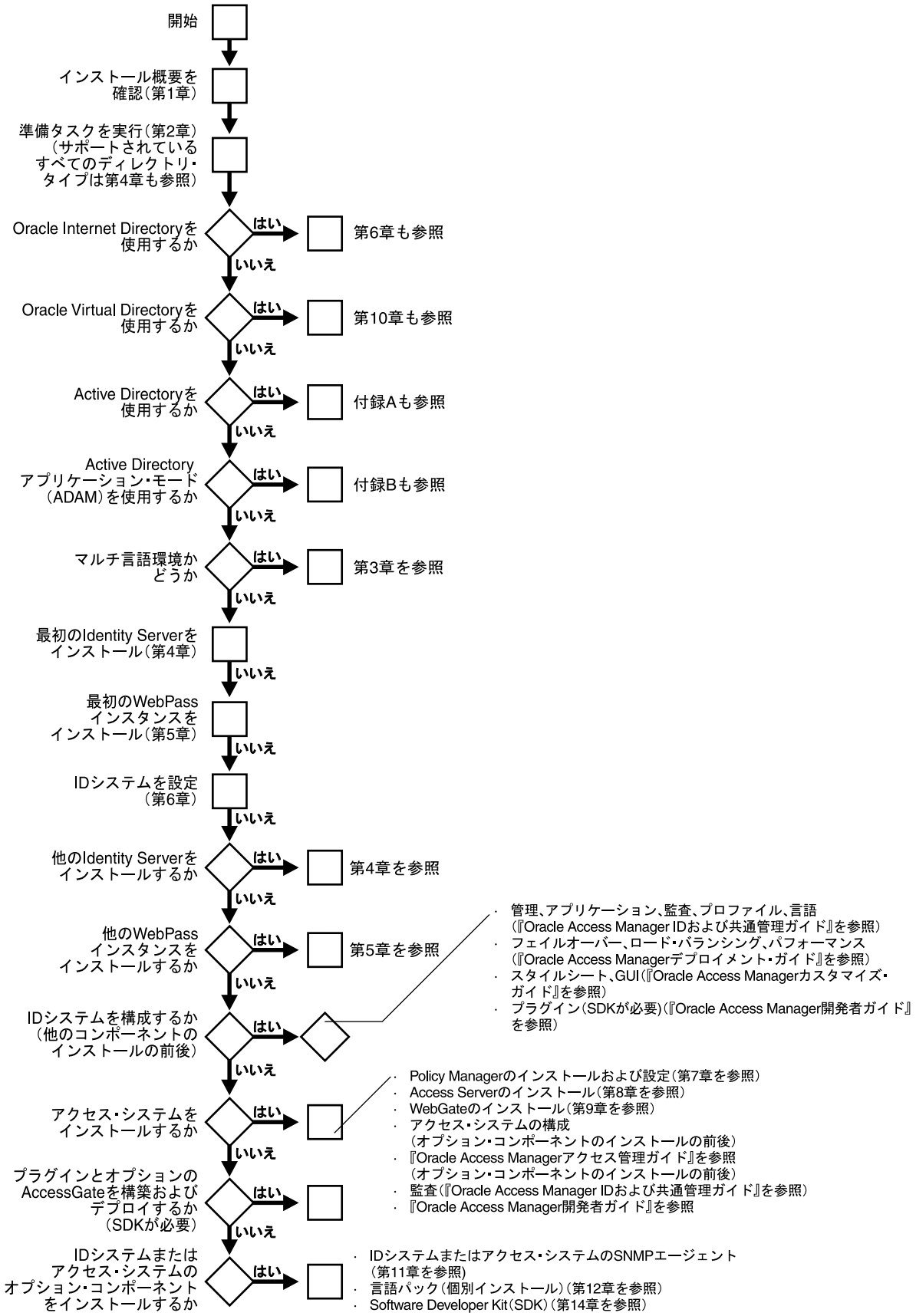
このガイドにあるアクティビティを開始する前に、『Oracle Access Manager 概要』を必ずお読みください。以前のバージョンのインストールを 10*g*（10.1.4.0.1）にアップグレードする方法は、『Oracle Access Manager アップグレード・ガイド』で説明されています。

インストール・タスクの概要

ID システムはすべてのインストールで必要です。アクセス・システムはオプションです。簡易インストールの概観および各システムが動作する仕組みの概要を含めた、ID システムおよびアクセス・システムの両方の概要については、『Oracle Access Manager 概要』を参照してください。

Oracle Access Manager コンポーネントをインストールして設定するために完了する必要のある一連のタスクは、図 1-1 および後続のタスクの概要で説明しています。

図 1-1 インストール・タスクの概要



タスクの概要 : Oracle Access Manager のインストール

1. 1-6 ページの「インストール・オプション」にあるとおりインストールのオプション、および 1-10 ページの「インストール・メソッド」にあるとおりメソッドを確認して選択します。
2. 第 2 章「インストールの準備」の前提条件すべてを満たし、必要に応じてユーザーの環境で次の情報を確認します。
   - このインストールで Oracle Internet Directory を使用している場合は、次も参照してください。
     - 4-15 ページの「Oracle Internet Directory のチューニング」
     - 6-3 ページの「タスクの概要 : Oracle Access Manager と Oracle Internet Directory 間の完全な相互作用の実現」
   - このインストールで Oracle Virtual Directory を使用している場合は、第 10 章「Oracle Virtual Directory を使用した Oracle Access Manager の設定」も参照し、ID システムを設定する前に、すべての前提条件のタスクを完了してください。
   - このインストールで Active Directory を使用している場合は、付録 A「Active Directory に対する Oracle Access Manager のインストール」も参照してください。
   - このインストールに Active Directory アプリケーション・モード（ADAM）を含めている場合は、付録 B「ADAM に対する Oracle Access Manager のインストール」も参照してください。
3. マルチ言語環境の場合は、第 3 章「マルチ言語環境の概要」でマルチ言語環境に関する情報を確認します。
4. 第 4 章「Identity Server のインストール」で説明されているように、最初の Identity Server をインストールします。
5. 第 5 章「WebPass のインストール」で説明されているように、最初の WebPass をインストールします。
6. 第 6 章「ID システムの設定」で説明されているように、オブジェクト・クラスおよび属性がディレクトリ・サーバーに表示され、Identity Server が正常に WebPass と連動するよう ID システムを設定して、システム全体にアクセスできるマスター管理者を割り当てます。
7. 第 4 章「Identity Server のインストール」で説明されているように、他の Identity Server がこの環境に必要であれば、これをインストールします。
8. 第 5 章「WebPass のインストール」で説明されているように、他の WebPass インスタンスがこの環境に必要であれば、これをインストールします。

   注意 : コンポーネントの複数のインスタンスをインストールする場合、最初のインスタンスをインストールして設定した後に、インスタンスのインストールを自動的に実行できます。自動インストールおよびコンポーネントのクローニングおよび同期化の詳細は、第 15 章「コンポーネントのレプリケート」を参照してください。

9. ここで（または、オプションのコンポーネントのインストール後）、ID システムの構成およびカスタマイズを開始します。たとえば、次のようにします。
   - 『Oracle Access Manager ID および共通管理ガイド』で説明されているように、管理者を定義し、ワークフロー、監査およびプロファイルを構成し、アプリケーション（User Manager、Group Manager、Organization Manager）を使用してインストールされた言語を使用するようシステムを構成します。
   - 『Oracle Access Manager デプロイメント・ガイド』で説明されているように、フェイルオーバー、ロード・バランシングおよびキャッシングを構成し、ID システムのパフォーマンスをチューニングして、本番環境の移行計画を確認します。
   - 『Oracle Access Manager カスタマイズ・ガイド』で説明されているように、ID システムのカスタマイズを開始して、アプリケーションの表示形式を変更し、オペレーティ

ング・システム、Web サーバー、ディレクトリ・サーバーおよびディレクトリの内容を変更したり、CGI ファイルまたは JavaScript を Oracle Access Manager 画面に接続したりすることによって、Oracle Access Manager を制御します。

- 『Oracle Access Manager 開発者ガイド』で説明されているように、Software Developer Kit（SDK）および API を使用して ID イベント・プラグインを構築してデプロイする方法や、IdentityXML および WSDL を使用してプログラムによって ID システム機能にアクセスする方法を参照してください。

注意： Oracle Access Manager の Software Developer Kit（SDK）および API のインストールは、第 14 章「Software Developer Kit の概要」で説明しています。詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。

---

10. オプションのアクセス・システムをインストールして設定します。次のようにします。
    - 第 7 章「Policy Manager のインストール」で説明されているように、Policy Manager をインストールして設定します。
    - 第 8 章「Access Server のインストール」で説明されているように、Access Server をインストールします。このインストールでは、Access Server インスタンスをアクセス・システム・コンソールに追加します。
    - 第 9 章「WebGate のインストール」で説明されているように、WebGate をインストールします。このインストールでは、WebGate インスタンスをアクセス・システム・コンソールに追加し、インストール前に WebGate を Access Server に関連付けます。
11. ここで（または、先に他のオプションのコンポーネントをインストールした後）、次のようにアクセス・システムの構成を開始します。
    - 『Oracle Access Manager アクセス管理ガイド』で説明されているように、ポリシー・ドメイン、認証スキームおよび認可スキームを定義し、シングル・ドメインおよび複数ドメインのシングル・サインオンを構成してユーザーが 1 つのログインで複数のリソースにアクセスできるようにし、カスタム・ログイン・フォームを設計します。
    - 『Oracle Access Manager ID および共通管理ガイド』で説明されているように、監査のアクセス・システムを構成します。
    - 『Oracle Access Manager 開発者ガイド』で説明されているように、カスタム WebGate（AccessGate）を作成し、Software Developer Kit および API を使用して、カスタム認証および認可プラグインを開発します。

注意： Oracle Access Manager の Software Developer Kit（SDK）および API のインストールは、第 14 章「Software Developer Kit の概要」で説明しています。詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。

---

12. 必要に応じて、次のようなオプションの Oracle Access Manager コンポーネントをインストールします。
    - 第 11 章「SNMP エージェントのインストール」で説明している SNMP の監視。
    - 第 12 章「言語パックの個別インストール」で説明されているオラクル社提供の言語パック。コンポーネントのインストール後に個別インストールできます。
    - 第 14 章「Software Developer Kit の概要」で説明している Oracle Access Manager の Software Developer Kit および API。詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。

インストール・オプション

ここでは、インストール中に使用可能なオプション、およびその詳細の参照先について説明します。

タスクの概要 : インストール・オプションの選択

1. 1-10 ページの「インストール・メソッド」で説明されているように、インストールを実行する前に、コンポーネントのインストールに GUI メソッドを使用するか、コマンドライン・メソッドを使用するかを決定します。
2. 1-6 ページの「スキーマおよび属性の自動更新と手動更新」で説明されているように、インストール中に、システムが提供するデフォルトを使用してスキーマの自動更新を有効化するか、ID システムおよび Policy Manager の設定中に属性に任意の値を入力するかを選択できます。
3. 1-9 ページの「インストールされた Oracle Access Manager コンポーネントのレプリケート」で説明されているように、コンポーネントの最初のインスタンスをインストールした後、コンポーネントの複数のインスタンスを手動でインストールするか、複数インスタンスの自動インストール・メソッドを使用するかを選択できます。
4. 指定したインストール・ディレクトリに以前のコンポーネント・ファイルがある場合、それ以降のリリースにアップグレードするかどうかの指定を求められます。詳細は、1-9 ページの「Oracle Access Manager の以前のリリースからのアップグレード」を参照してください。

スキーマおよび属性の自動更新と手動更新

ID サーバーおよび Policy Manager のインストール中に、構成データ・ブランチを持つスキーマを自動的に更新するかどうかの指定を求められます。スキーマ更新は、設定プロセスを開始する前に実行される必要があります。

注意 : インストール中にスキーマを自動的に更新して、製品固有のオブジェクト・クラスおよび属性を取得することをお薦めします。インストール時に自動更新を選択しないと、ID システムおよび Policy Manager の設定プロセスの開始時に、スキーマの変更ページが表示されます。ADAM ディレクトリのスキーマの自動更新は、サポートされていません。

Identity Server のインストールによりスキーマが変更されるため、インストール後にカスタム・スキーマに変更を加える必要があります。ID システムおよび Policy Manager の設定中、様々なオブジェクト・クラスを構成するよう求められます。たとえば、ID システムでは、Person オブジェクト・クラスおよび Group オブジェクト・クラスの「フルネーム」、「ログイン」および「パスワード」のセマンティク型への属性の割当てが必要です。時間を節約してエラーを回避するため、設定中に「自動構成」オプションを使用して、属性を自動的に構成することをお薦めします。必要に応じて、後で属性を再構成することもできます。

表 1-1 で示されているように、属性の自動構成は、インストールおよび設定プロセスの 1 つの手順です。付録 B「ADAM に対する Oracle Access Manager のインストール」で説明されているように、ADAM ディレクトリでは、Oracle Access Manager コンポーネントのインストール後に、スキーマおよびデータを手動で更新する必要があります。

表 1-1 スキーマの自動構成（ADAM ディレクトリを除く）

コンポーネント	スキーマの自動構成（ADAM を除く）
Identity Server のインストール	最初の Identity Server のインストール中に「はい」を選択して、スキーマを自動的に更新する。 2 番目以降の Identity Server には、「いいえ」を選択する。
WebPass のインストール	スキーマのオプションなし。
ID システムの設定	オプションがある場合は、「自動構成」を選択する。 設定後、必要に応じて属性を再構成する。
Policy Manager のインストールおよび設定	オプションがある場合は、「自動構成」を選択する。 設定後、必要に応じて属性を再構成する。
Access Server のインストール	スキーマ更新のオプションなし。
WebGate のインストール	スキーマのオプションなし。

属性を手動で構成する場合は、インストール後の設定プロセス中に構成する必要があります。属性の手動構成には、次の場所に 1 つ以上の LDIF ファイルが必要です。

IdentityServer_install_dir¥identity¥oblix¥data.ldap¥common

PolicyManager_install_dir¥access¥oblix¥data.ldap¥common

表 1-2 に示されているように、各 LDIF ファイルには、固有のディレクトリ・サーバー・タイプが先頭に付いています。ほとんどの場合、ldapmodify ツールを使用して更新を実行します。次に例を示します。

```
ldapmodify -h DS_hostname -p DS_port_number -D bind_dn -w password -a -c -f
DS_type_oblix_schema_add.ldif
```

表 1-2 では、各ディレクトリ・サーバー・タイプに必要なスキーマ更新ファイルに関する詳細を示しています。これには構成データまたはユーザー・データに必要な索引ファイルも含まれています。

ディレクトリ要件の詳細は、2-18 ページの「ディレクトリ・サーバーの要件の実現」を参照してください。

表 1-2 スキーマの手動更新ファイル

ディレクトリ・サーバー・タイプ	スキーマの手動更新ファイル
Active Directory	ADSchema.ldif（Windows 2000 のみ） ADdotNetSchema_add.ldif（Windows 2003 のみ） ADAuxSchema.ldif（Windows 2003、静的にリンクされた補助クラス） ADUserSchema.ldif **注意：** Active Directory スキーマは、Ldifde.exe を使用して拡張可能です。詳細は、付録 A「Active Directory に対する Oracle Access Manager のインストール」を参照してください。

表 1-2 スキーマの手動更新ファイル（続き）

ディレクトリ・サーバー・タイプ	スキーマの手動更新ファイル
ADAM	ADAM_oblix_schema_add.ldif ADAM_user_schema_add.ldif ADAMAuxSchema.ldif（静的にリンクされた補助クラス） **注意：** Oracle Access Manager のインストール時に、ADAM スキーマを手動で更新する必要があります。 ADAM スキーマは、Ldifde.exe を使用して拡張可能です。詳細は、付録 B「ADAM に対する Oracle Access Manager のインストール」を参照してください。
Data Anywhere（Oracle Virtual Directory）	VDE_user_schema_add.ldif 次の詳細は、第 10 章「Oracle Virtual Directory を使用した Oracle Access Manager の設定」を参照してください。 ■ Oracle Access Manager の Oracle Virtual Directory Server（VDS）との統合 ■ 前提条件および VDS への Oracle Access Manager のインストール ■ schema.oblix.xml ■ アダプタおよびマッピングのスクリプト・テンプレート ■ 既存の Oracle Access Manager インストールで VDS 用に使用する構成ツリー内のユーザー DN およびグループ DN にパッチを適用する、DN 変換プログラムおよび構成ファイル
IBM Directory Server	V3.oblix.ibm_at.ldif V3.oblix.ibm_oc.ldif V3.user.ibm_at.ldif V3.user.ibm_oc.ldif
Oracle Internet Directory	OID_oblix_schema_add.ldif OID_oblix_schema_delete.ldif OID_oblix_schema_index_add.ldif OID_user_index_add.ldif OID_user_schema_add.ldif OID_user_schema_delete.ldif
Novell Directory Server	NDS_oblix_index_add.ldif NDS_oblix_schema_add.ldif NDS_user_index_add.ldif NDS_user_schema_add.ldif
Sun Directory Server	iPlanet_oblix_schema_add.ldif. iPlanet_user_schema_add.ldif iPlanet5_oblix_index_add.ldif iPlanet5_user_index_add.ldif

インストールされた Oracle Access Manager コンポーネントのレプリケート

コンポーネントの各インスタンスを手動でインストールするのではなく、特定のコンポーネントの最初のインスタンスをインストールして設定した後、そのインスタンスの構成を別のインスタンスにレプリケートできます。

次の 3 つのメソッドから選択できます。

- インストール・パラメータを含むファイルによる、インストール・プロセスを自動化（サイレント・モードのインストール）
- 構成のクローニング
- 2 つのコンポーネントまたは 2 つのコンポーネントの一部を同期化

サイレント・モード

サイレント・モードではユーザーが介入せずにインストールを行うことができます。Oracle Access Manager インストール・スクリプトでは、サイレント・モードのオプション・ファイルからオプションおよび構成情報を取得します。

重要：サイレント・モードは、新規インストールのみを対象としています。

サイレント・モードの詳細は、第 15 章「コンポーネントのレプリケート」を参照してください。

インストール済コンポーネントのクローニングと同期化

インストールしたコンポーネントをクローニングしてレプリケートしたり、2 つのコンポーネントまたは 2 つのコンポーネントの一部を同期化できます。

詳細は、15-30 ページの「インストール済コンポーネントのクローニングと同期化」を参照してください。

Oracle Access Manager の以前のリリースからのアップグレード

Oracle Access Manager コンポーネントのインストールを開始し、以前のバージョンが含まれるターゲットのインストール・ディレクトリを指定すると、コンポーネントが検出され、そのコンポーネントを 10*g*（10.1.4.0.1）にアップグレードするかどうかの指定を求められます。

- アップグレードを回避するには、新規のインストール・ディレクトリ・パスを指定する必要があります。
- アップグレードを受け入れて続行するには、『Oracle Access Manager アップグレード・ガイド』を参照してください。

インストール・メソッド

Oracle Access Manager コンポーネントのインストールには、グラフィカル・ユーザー・インタフェース（GUI メソッド）またはコマンドライン・コンソール（コンソール・メソッド）のいずれかを選択できます。選択するメソッドに関係なく、プロセスは類似しています。このマニュアルで詳述されている順序およびプロンプトは、GUI メソッドを使用しています。相違点は発生時に特定されます。詳細は、次を参照してください。

- GUI メソッド
- コンソール・メソッド

GUI メソッド

使用中のプラットフォームおよび Web サーバーに応じて、Oracle Access Manager コンポーネントの異なるインストール・パッケージが使用可能です。インストールの開始時に選択するメソッドに関係なく、イベントおよびメッセージの順序は同じです。

Oracle Access Manager インストール・メディアをオラクル社から取得します。インストール・パッケージを選択する際、Windows システムでは GUI メソッドがデフォルトになります。次に例を示します。

Oracle_Access_Manager10_1_4_0_1_win32_Identity_Server

サード・パーティの Installshield の ISMP フレームワークとの既知の問題のため、インストール中に入力される文字に「$」が含まれる場合、インストーラは予測がつかない解釈をする場合があります。たとえば、最初の Identity Server のスキーマ更新中に入力されたバインド・パスワードが「Admin$$」の場合、ISMP はこれを「Admin$」と解釈し、スキーマ更新ツールを起動しますが、更新は失敗して「不正な資格証明エラー（49）」と表示されます。特定のツールの起動中にこの問題が発生した場合、そのツールをコマンドラインから実行してください。

注意： 同じパスワードを使用するすべての Oracle Access Manager インストーラが、同様の資格証明の問題によって失敗することがあります。

コンソール・メソッド

UNIX プラットフォーム上に Oracle Access Manager コンポーネントをインストールする場合、コマンドライン・コンソール・メソッドを使用できます。コンソール・メソッドは、UNIX システムのデフォルトです。次に例を示します。

/ Oracle_Access_Manager10_1_4_0_1_sparc-s2_Identity_Server

注意： コンポーネントのインストールにコンソール・メソッドを使用する場合、次のように指示されます。

次へ進むには、[1] を押します。[Enter] キーを押して次へ進む場合と同じです。

取り消すには、[3] を押します。

情報を再度表示するには、[4] を押します。

オプション番号を指定するよう求められた場合は、ゼロ（[0]）を入力して選択を確定します。

2

インストールの準備

この章では、Oracle Access Manager コンポーネントのインストール・プロセスを開始する前に、環境を準備するために必要な重要情報について説明します。次の項目について説明します。

> **注意：** すべての前提条件を満たさない場合、10*g*（10.1.4.0.1）のインストールに悪影響を及ぼすことがあります。

- インストールの前提条件の概要
- セキュアなパスワードと権限の設定
- システム・クロックの同期化
- Oracle Access Manager の要件の実現
- Web サーバーの要件の実現
- ディレクトリ・サーバーの要件の実現
- プラットフォームの要件の確認
- インストーラ用の一時ディレクトリの準備
- Oracle Access Manager コンポーネントのアンインストール
- インストール準備のチェックリスト

Oracle Access Manager のコンポーネント、特徴、機能、対象者およびマニュアルの概要は、『Oracle Access Manager 概要』を参照してください。10*g*（10.1.4.0.1）にアップグレードする方法は、『Oracle Access Manager アップグレード・ガイド』で説明されています。

インストールの前提条件の概要

Oracle Access Manager をインストールする前に次の前提条件を満たすと、インストールを正常に実行できます。

タスクの概要 : Oracle Access Manager のインストールの準備

1. 第 1 章「インストール・タスク、オプションおよびメソッドの概要」を確認し、環境に最も適したインストール・オプションを判断します。
2. 2-2 ページの「セキュアなパスワードと権限の設定」で説明されているように、セキュリティに関するいくつかのベスト・プラクティスを実行します。
3. 複数のマシンにインストールする場合は、2-3 ページの「システム・クロックの同期化」で説明されているように、ホスト・クロックを同期化します。
4. 2-4 ページの「Oracle Access Manager の要件の実現」全体を確認し、アクティビティを完了します。
5. Web サーバー・インスタンスを作成し、2-15 ページの「Web サーバーの要件の実現」を参照します。
6. サポートされているディレクトリ・サーバー・インスタンスを作成し、ディレクトリ・サーバーに管理者レベルのユーザーを少なくとも 1 名定義し（ベンダーのドキュメントを参照）、2-18 ページの「ディレクトリ・サーバーの要件の実現」に記載されているすべてのトピックを確認します。
7. 2-28 ページの「プラットフォームの要件の確認」で説明されているように、環境がプラットフォームおよびサポートの要件を満たしていることを確認します。
8. ソフトウェアをオラクル社提供のインストール・メディアから取得し、2-28 ページの「インストーラ用の一時ディレクトリの準備」で説明されているように、一時ディレクトリを準備します。
9. 2-29 ページの「インストール準備のチェックリスト」で説明されているように、インストール・プロセス中に指定する環境に関する情報を収集および文書化します。
10. オラクル社提供の言語パックを一緒にインストールする場合、または英語（アメリカ）以外の言語または地域のオペレーティング・システムを実行しているマシンにインストールする場合は、第 3 章「マルチ言語環境の概要」を参照し、必要なアクティビティをすべて完了します。

セキュアなパスワードと権限の設定

セキュアなインストールを行うためのベスト・プラクティスは次のとおりです。

- すべてのプラットフォーム上で、インストール中に一時的な LDAP 管理者パスワードを作成し、すべてのコンポーネントのインストール後にそのパスワードをリセットします。
- UNIX 上では、信頼されないユーザーまたはグループへのアクセスがインストール・コンピュータで許可されている場合、信頼できるユーザー・アカウントにのみアクセスできるユーザーおよびグループを使用してインストールを実行します。

  必要に応じて、新しいユーザーおよびグループを作成します。
- Windows 上では、信頼されないユーザーへのアクセスがインストール・コンピュータで許可されている場合、信頼できるユーザーへのアクセスのみを許可するようにすべてのファイル・セキュリティ権限を構成します。

システム・クロックの同期化

Oracle Access Manager コンポーネントを複数のマシンにインストールする場合は、すべてのシステム・クロックが同期化されていることを確認します。これは、ソフトウェアを証明書モードまたはシンプル・モードで実行する場合に特に重要です。

警告 : 各セキュア・リクエストにはタイムスタンプが含まれています。システム・クロックが同期化されていないと、Identity Server へのすべてのリクエストが拒否される場合があります。

たとえば、WebPass の Web サーバーのシステム・クロックが Identity Server のシステム・クロックより進んで設定されている場合、Web サーバー上の WebPass プラグインから送信されるログイン・リクエストには、Identity Server ではまだ発生していない時刻が含まれます。これは、アクセス・システムの場合も同様です。Web サーバーのクロックが Access Server のクロックより進んでいる場合、Policy Manager から Access Server に送信されるリクエストには、Access Server ではまだ発生していない時刻が含まれます。

正常に操作するには、次のようにします。

- すべてのマシンのクロックが同期化されていることを確認してください。時間のずれは許容されません。たとえば、WebGate のクロックが Access Server のクロックよりわずかでも進んでいる場合、WebGate で生成される Cookie は将来のものとなり、Access Server で問題の原因になります。
- WebGate を実行している各マシンのクロックが、それが関連付けられている Access Server より進んでいないことを確認してください。Access Server が WebGate のクロックよりも進んでいる場合、そのずれは 60 秒以内である必要があります。
- WebPass を実行している各マシンのクロックが、それが関連付けられている Identity Server および Policy Manager より進んでいないことを確認してください。

Network Time Protocol の概要

地理的に異なるタイムゾーンにある 10*g*（10.1.4.0.1）コンポーネントを同期化するには、Network Time Protocol（NTP）を使用できます。NTP では、複数のマシンの時刻を数ミリ秒以内に同期化できます。時刻の同期化の詳細は、次の Web サイトにアクセスしてください。

```
http://www.ntp.org/
```

また、comp.protocols.time.ntp ニュース・グループを参照してください。

ntp.conf ファイルには、少なくとも次の内容が含まれています。

```
server <some NTP server name>.com

driftfile /etc/ntp.drift
```

ntp.conf ファイルを作成する方法は、次のサイトで確認できます。

- `http://www.sun.com/products-n-solutions/hardware/docs/html/816-3626-10/after.html`
- `http://inetsd01.boulder.ibm.com/pseries/fr_FR/files/aixfiles/ntp.conf.htm`
- `http://www.developer.ibm.com/tech/faq/individual/0,,2:14789,00.html`

UNIX マシンでは、UTC（GMT とも呼ばれる）を内部で使用し、表示で必要なローカル時間に変換します。Windows マシンではクロックをローカル時間で維持しますが、NTP 同期化プログラムを使用すると、Windows 上での正確な時刻が保証されます。

UNIX システムの場合

すべての UNIX オペレーティング・システムには、いずれかのバージョンの NTP が含まれています。Solaris 上で NTP を構成するには、ntp.conf ファイルを作成します。Solaris に付属の NTP デーモンを使用する ntp.conf ファイルの名前は、/etc/inet/ntp.conf です。このファイルの作成後は、オペレーティング・システムの起動時に、xntp が自動的に起動されます。

- **HP-UX 上 :** sam を使用して NTP を起動します。
- **AIX 上 :** /etc/ntp.conf ファイルを作成し、起動スクリプトを有効化または作成します。
- **すべての UNIX プラットフォーム上 :** 最新（および、よりセキュアな）バージョンの NTP デーモンを `http://www.ntp.org/` から入手します。

Windows システムの場合

Windows マシンでは、いずれかのバージョンの NTP を使用して、マシンの時刻をそのドメイン・コントローラと自動的に同期化します。ドメイン・コントローラは、時刻ソースと同期化されるように構成する必要があります。

ネットワーク全体を同期化するための公式な時刻を取得できるように、多数の ISP からカスタマ向けの時刻サービスが提供されています。

- NTP: このプロトコルには、`http://www.ntp.org` から入手できるオープンな stratum-1 サーバーのリストがあります。

  ただし、このサイトは、最もセキュアな選択肢ではない場合があります。時間ベースの攻撃の例としては、時刻を実際の時刻より進めて見せかけることで Cookie を有効に保つことがあります。

- GPS ベースのクロック : このクロックでは、衛星テクノロジを使用して、非常に正確な時刻を提供します。

  これらのクロックを使用して、ネットワーク全体を同じ時刻に設定できます。GPS テクノロジでは、非常に正確な時刻を必要とします。各衛星には 3 つの原子時計が組み込まれていて、これらの時計の時刻は、相対論的効果を補正するために地上から送信される値によって絶えず修正されます。つまり、現在時刻の正確な推定値は、GPS 受信機の位置を検出することの副次的な効果として得られます。

Oracle Access Manager の要件の実現

次の情報を参考にしてください。

- 一般的なガイドライン
- Linux ホスト・マシンの準備
- ID システムのガイドライン
- アクセス・システムのガイドライン
- ディスク領域の要件の評価
- インストール・ディレクトリの選択

一般的なガイドライン

各コンポーネントに対し、サポートされているホスト・マシンが必要です。これについては、2-28 ページの「プラットフォームの要件の確認」で説明されています。さらに、次の要件があります。

- **管理権限 :** コンポーネントをインストールするアカウントには、管理権限が必要です。Identity Server と Access Server の両方のサーバーは、サービスとして実行されます。Identity Server および Access Server のサービスを実行するために使用するユーザー・アカウントには、サービスとしてログオンするための権限が必要です。この権限は、「管理ツール」→「ローカル セキュリティ ポリシー」→「ローカル ポリシー」→「ユーザー権利の割り当て」→「サービスとしてログオン」で設定できます。
  - **Microsoft Windows 上 :** Identity Server のサービスを実行するために使用するユーザー・アカウントには、サービスとしてログオンするための権限が必要です。これは、「管理ツール」で設定できます。たとえば、次のようにします。

    「管理ツール」→「ローカル セキュリティ ポリシー」→「ローカル ポリシー」→

    「ユーザー権利の割り当て」→「サービスとしてログオン」
  - **UNIX プラットフォーム上 :** Identity Server で使用するユーザー名とグループを指定するよう求められます。通常、デフォルトは nobody です。HP-UX の場合、デフォルトは WWW（ユーザー名）および others（グループ）です。正しいコマンドがインストールされていることを確認し、Web サーバーの実行に使用するユーザー名を確認します。たとえば、次のようにします。

    a. 次のコマンドを検索し（通常は、/usr/bin、/usr/sbin または /usr/csb 内）、その場所が検索パスに含まれていることを確認します。

    ```
    sed、tar、cp、ls、mkdir、rmdir
    ```

    b. Web サーバーの実行には、nobody、root またはその他のユーザー名（Web など）を使用できます。これは、Web サーバーの構成ファイルを確認することで、または Web サーバーの管理コンソールを実行して「View Server Settings」を確認することで特定できます。
- **オンラインのマシン :** インストールの前に、各コンポーネントが実行されるマシンに ping を実行できる必要があります。また、インストール中に、Identity Server と Access Server のインストール・マシンの DNS ホスト名を指定するよう求められます。
- **Linux ライブラリ :** コンポーネントを Linux マシンにインストールする前に、GCC 3.3.2 と互換性のある追加の GCC ランタイム・ライブラリ（libgcc_s.so.1 および libstdc++.so.5）をインストールする必要があります。2-6 ページの「Linux ホスト・マシンの準備」を参照してください。
- **コンポーネントのセキュリティ :** インストール中に、Oracle Access Manager コンポーネント間の通信のトランスポート・セキュリティ・モードを指定する必要があります。詳細は、2-12 ページの「Oracle Access Manager コンポーネントの通信の保護」を参照してください。
- **ディレクトリのセキュリティ :** インストール中（Identity Server、Policy Manager および Access Server）に、コンポーネントが通信するディレクトリ・サーバーのホスト名、DN およびトランスポート・セキュリティ・モードを指定する必要があります。この情報およびその他の重要な情報は、2-18 ページの「ディレクトリ・サーバーの要件の実現」を参照してください。
- **既存の Identity Server 名 :** 既存の Identity Server 名を再利用する場合は、20-6 ページの「Identity Server インスタンス名のリサイクル」を参照してください。
- **インストールの取消し :** インストールの取消しまたはインストールしたコンポーネントの削除が必要な場合は、2-29 ページの「Oracle Access Manager コンポーネントのアンインストール」を参照してください。

- **マルチ言語環境 :**
  - 英語（アメリカ）以外の言語またはロケールのオペレーティング・システムを使用しているマシンへのインストールでは、LANG 環境変数、または任意の NLS_LANG あるいは COREID_NLS_LANG 環境変数を設定できます。
  - Identity Server をオラクル社提供の 1 つ以上の言語パックとともにインストールする場合は、WebPass も同じ言語パックとともにインストールする必要があります（対応するアクセス・システムの言語パックとすべてのアクセス・システム・コンポーネントもインストールする必要があります）。
  - コンポーネントを 1 つの言語パックとともに UNIX システムにインストールする場合は、メイン・インストーラを起動する前に、言語パックのインストーラがコンポーネントと同じディレクトリに存在し、言語パックのインストーラに実行権限があることを確認してください。たとえば、次のようにします。

    ```
    chmod +x "Oracle_Access_Manager10_1_4_0_1_FR_sparc-s2_LP_Identity_System"
    chmod +x "Oracle_Access_Manager10_1_4_0_1_FR_sparc-s2_LP_Access_System"
    ```

    詳細は、第 3 章「マルチ言語環境の概要」を参照してください。

Linux ホスト・マシンの準備

Oracle Access Manager コンポーネントを Linux マシンにインストールしている間に、GCC 3.3.2 と互換性のある追加の GCC ランタイム・ライブラリ（libgcc_s.so.1 および libstdc++.so.5）の場所を指定するよう求められます。これらのライブラリは、製品には付属していません。また、オラクル社の Web サイトでもダウンロード用に提供していません。これらのライブラリが必要な場合は、プラットフォームのベンダーにお問い合せください。

Linux ホストへの libgcc_s.so.1 および libstdc++.so.5 のインストールの手順

1. libgcc_s.so.1 および libstdc++.so.5 ライブラリをプラットフォームのベンダーから入手します。
2. 1 つ以上の Oracle Access Manager コンポーネントをインストールするローカル Linux マシンに次のファイルを格納します。

   libgcc_s.so.1

   libstdc++.so.5
3. Oracle Access Manager のインストール中に、ローカル・マシン上のライブラリの場所を指定し、インストールを続行します。

ID システムのガイドライン

Identity Server は、他の Oracle Access Manager コンポーネントやアプリケーションと同じホスト・システム上に存在する必要はありません。Identity Server と Access Server は異なるマシンにインストールすることをお薦めします。さらに、Identity Server は、他の Oracle Access Manager コンポーネントやアプリケーションと同じホスト・システム上に存在する必要はありません。1 つ以上の Identity Server をインストールする方法の詳細は、第 4 章「Identity Server のインストール」を参照してください。

Identity Server と通信する各 Web サーバー・インスタンスには、WebPass を構成する必要があります。1 つの WebPass は、複数の Identity Server と通信できます。複数の WebPass が同一の Identity Server と通信できます。ロード・バランシングでは、この方法をお薦めします。2-3 ページの「システム・クロックの同期化」も参照してください。

インストール中に指定する WebPass インスタンスの ID は、一意である必要があります。WebPass インスタンスの ID は、インストール後に Web サーバーが起動するまで検証されません。

WebPass は、各 Policy Manager でも同じディレクトリ・レベルで、同じ Web サーバー・インスタンス上にインストールする必要があります。

1 つ以上の WebPass インスタンスをインストールする方法の詳細は、第 5 章「WebPass のインストール」を参照してください。

ID システムの設定中に、すべての Oracle Access Manager 機能へのアクセス権が付与されるユーザーを定義する必要があります。これは、マスター管理者です。詳細は、第 6 章「ID システムの設定」を参照してください。

アクセス・システムのガイドライン

次の各項目は、アクセス・システムの要件とガイドラインの概要について説明します。

- Policy Manager のガイドライン
- Access Server のガイドライン
- WebGate のガイドライン

Policy Manager のガイドライン

Policy Manager は、WebPass と同じディレクトリ・レベルで、WebPass と同じ Web サーバー・インスタンス上にインストールする必要があります。2-3 ページの「システム・クロックの同期化」も参照してください。

Policy Manager とディレクトリ・サーバー間には、ファイアウォールを設定しないことをお薦めします。これは、ヘルス・チェックが実行されないためです。非アクティブ期間の後に、ファイアウォールは警告なしに Policy Manager 接続を削除する場合があります。このような問題を回避するために、Policy Manager とディレクトリ・サーバーがファイアウォールの同じ側に存在するようにするか、可能な場合は、Policy Manager とディレクトリ・サーバー間のファイアウォール接続のタイムアウトを無効化します。ただし、一部のファイアウォールではこれをサポートしていません。

NETWORK アカウントには、ボリューム・ルートでの変更権限が必要です。

Policy Manager で使用するディレクトリ・サーバーに応じて、次の点を検討してください。

- Policy Manager のインストール中に Windows Server 2003 上の Active Directory をディレクトリ・サーバーとして指定すると、動的補助クラスをサポートするかどうかを尋ねる新しいページが表示されます。ADSI を使用している場合は、Policy Manager のインストール後および設定前に、IIS Web サーバーの匿名ユーザー・ログイン・アカウントをドメイン・ユーザーに設定する必要があります。
- Policy Manager が Sun（以前の Netscape）の Web サーバーを使用する Solaris 上にインストールされた場合、Oracle Access Manager はディレクトリ・サーバーと Policy Manager 間の SSL 対応通信をサポートしません。

Policy Manager のインストールに使用している Web サーバーに応じて、次のような考慮点があります。

- **Apache:** Oracle Access Manager は、SSL 対応または非対応の Apache をサポートしています。SSL 対応通信では、Oracle Access Manager は、Apache-SSL ではなく、mod_ssl 付きの Apache のみをサポートしています。mod_ssl は、Apache-SSL から導出され、Apache-SSL にかわるモジュールです。httpd.conf で、Web サーバーの実行ユーザーおよびグループを構成します。
- **IIS:** Policy Manager のインストーラでは、複数の Web サーバー・インスタンスは更新できません。複数の IIS Web サーバー・インスタンスがインストールされている場合は、各 Web サーバー・インスタンスに個別の Policy Manager をインストールしてください。

  IIS を実行している Windows 2000 に Policy Manager をインストールする場合は、Everyone という名前のグループに ¥temp ディレクトリおよび ¥temp ディレクトリが属するドライブ（C や D など）への完全なアクセス権があることを確認してください。

  TEMP 変数は、システム全体または IIS ユーザーに対して、有効なディレクトリを指すように設定する必要があります。TEMP 変数はシステム全体に対して設定することをお薦めします。

1 つ以上の Policy Manager をインストールする方法の詳細は、第 7 章「Policy Manager のインストール」を参照してください。

Access Server のガイドライン

Identity Server と Access Server は異なるマシンにインストールすることをお薦めします。Identity Server は、他の Oracle Access Manager コンポーネントやアプリケーションと同じホスト・システム上に存在する必要はありません。

Policy Manager と同じディレクトリに Access Server をインストールしないでください。同一のディレクトリに複数の Access Server をインストールしないでください。

フェイルオーバーおよびロード・バランシング : フェイルオーバーおよびロード・バランシングのために、複数の Access Server をインストールすることをお薦めします。

ファイアウォール : Access Server をインストールするマシンをファイアウォールで保護することをお薦めします。

以前の WebGate を含んでいるアップグレードされた環境に 10*g*（10.1.4.0.1）Access Server をインストールする場合は、Access Server の globalparams.xml ファイルの `"IsBackwardCompatible" Value="true"` を手動で変更する必要があります。アップグレードされた Access Server は、自動的に以前の WebGate との下位互換性を備えます。詳細は、『Oracle Access Manager アップグレード・ガイド』を参照してください。

1 つ以上の Access Server をインストールする方法の詳細は、第 8 章「Access Server のインストール」を参照してください。

WebGate のガイドライン

WebGate は、Web サーバーをホストするマシンにインストールする必要があります。WebGate は、Web サーバーがアクセス可能な任意のディレクトリにインストールできます。

WebGate は、Policy Manager がインストールされている Web サーバーなど、アクセス・システムで保護するすべての Web サーバーにインストールしてください。Policy Manager および WebPass を保護するために WebGate をインストールする場合、WebGate は Policy Manager および WebPass と同じディレクトリにインストールする必要があります。たとえば、WebPass と Policy Manager が ¥COREid¥WebComponent にインストールされている場合、WebGate もこのディレクトリにインストールします。

WebGate は、ルート・レベルまたはサイト・レベルでインストールできます。WebGate を複数の仮想サイトにインストールしても、生成される WebGate のインスタンスは 1 つのみです。Web サーバー・プロセスを root 以外のユーザーとして実行する場合、root 以外のユーザーを使用して WebGate をインストールすることもできます。

WebGate は、マシン・レベルまたは仮想 Web サーバー・レベルで実行するように構成できます。ただし、マシン・レベルと仮想 Web サーバー・レベルの両方にはインストールしないでください。2-3 ページの「システム・クロックの同期化」も参照してください。

以前の WebGate は、10*g*（10.1.4.0.1）Access Server と共存できます。この場合、次の要件があります。

- リリース 5.x と 10*g*（10.1.4.0.1）WebGate が同じシステムに共存する場合は、RC4 を暗号化スキームとして使用します。
- リリース 6.x と 10*g*（10.1.4.0.1）WebGate が同じシステムに共存する場合は、RC6 を暗号化スキームとして使用します。
- リリース 7.0 または 10*g*（10.1.4.0.1）WebGate が同じシステムに共存する場合は、AES 暗号化スキームを使用します。

また、Access Server と以前の WebGate との下位互換性の詳細は、『Oracle Access Manager アップグレード・ガイド』を参照してください。1 つ以上の WebGate をインストールする方法の詳細は、第 9 章「WebGate のインストール」を参照してください。

Web サーバーおよびオペレーティング・システムのタイプは、WebGate と Access Server 間の通信では考慮されません。ただし、各種環境において、WebGate には次のような考慮点があります。

- **UNIX WebGate:** WebGate をインストールするには、ルートとしてログインします。Web サーバー・プロセスを root 以外のユーザーとして実行する場合は、root 以外のユーザーを使用して WebGate をインストールできます。
- **Apache Web サーバー :** Oracle Access Manager は、SSL 対応または非対応の Apache をサポートしています。SSL 対応通信では、Oracle Access Manager は、Apache-SSL ではなく、mod_ssl 付きの Apache のみをサポートしています。mod_ssl は、Apache-SSL から導出され、Apache-SSL にかわるモジュールです。
- **IHS v2 Web サーバー :** Oracle Access Manager は、SSL 対応または非対応の IHS v2 および IHS v2 リバース・プロキシ・サーバーをサポートしています。詳細は、16-9 ページの「Oracle Access Manager Web コンポーネントのための Web サーバー構成の更新」を参照してください。
- **Domino Web サーバー :** Domino Web サーバーに WebGate をインストールする前に、Domino Enterprise Server R5 を正しくインストールおよび設定する必要があります。詳細は、18-1 ページの「WebGates のための Lotus Domino Web サーバーの設定」を参照してください。
- **IIS Web サーバー :** WebGate をインストールする前に、IIS Web サーバーがロックダウン・モードでないことを確認してください。ロックダウン・モードの場合、サーバーが再起動されてメタベースが再初期化されるまで、つまり、ロックダウン後に発生したアクティビティを IIS が無視するまで、処理が進行しているように表示されます。

  クライアント証明書認証を使用する場合は、WebGate のクライアント証明書を有効化する前に WebGate をホストする IIS Web サーバー上の SSL を有効化する必要があります。

  NTFS をサポートするファイル・システムにインストールする場合にのみ、IIS WebGate では、/access ディレクトリに対する様々な権限の設定が必要です。たとえば、FAT32 ファイル・システムを実行している Windows 2000 マシンに、シンプル・モードまたは証明書モードで ISAPI WebGate をインストールするとします。最後のインストール・パネルには、FAT32 ファイル・システム上で設定できない様々な権限を手動で設定するための指示が表示されます。この場合、この指示は無視してください。

  各 IIS 仮想 Web サーバーには、独自の WebGate.dll ファイルを仮想レベルでインストールするか、全サイトに影響を与える 1 つの WebGate をサイト・レベルでインストールできます。WebGate.dll をサイト・レベルでインストールしてすべての仮想ホストを制御するか、1 つまたはすべての仮想ホスト用に WebGate.dll をインストールします。

  postgate.dll ファイルをマシン・レベルでインストールする必要がある場合もあります。postgate.dll は、9-11 ページの「IIS Web Server 上における postgate.dll のインストール」で説明されているように、¥*WebGate_install_dir* にあります。インストールを複数回実行すると、このファイルの複数のバージョンが作成され、異常な Oracle Access Manager の動作が発生する場合があります。この場合は、webgate.dll および postgate.dll がそれぞれ 1 つずつ存在することを確認してください。

  > **注意 :** postgate.dll は、常にサイト・レベルでインストールされます。なんらかの理由で WebGate を再インストールすると、postgate.dll も再インストールされます。この場合は、postgate.dll のコピーがサイト・レベルで 1 つのみ存在することを確認してください。

  WebGate および関連フィルタを IIS から完全に削除するには、フィルタを IIS のリストから削除するだけでなく、他の手順も必要になります。IIS は、その設定をすべてメタベース・ファイルに保持します。Windows 2000 以降では、これは手動で変更できる XML ファイルです。また、メタベースの編集に利用できるツール（MetaEdit）もあります。MetaEdit は Regedit に類似しており、一貫性チェックとブラウザ / エディタの機能があります。WebGate を IIS から完全に削除するには、MetaEdit を使用してメタベースを編集します。

- **ISA プロキシ・サーバー :** ISA プロキシ・サーバーでは、すべての ISAPI フィルタを ISA のインストール・ディレクトリ内にインストールする必要があります。ISA のインストール・ディレクトリ構造内では、任意の場所にインストールできます。

  1. WebGate を ISA プロキシ・サーバーにインストールする前に、次の手順を実行します。
     - ISA 命令を含む一般 ISAPI フィルタを次の場所でチェックします。

       http://msdn.microsoft.com/library/default.asp?url=/library/en-us/isa/isaisapi_5cq8.asp
     - 内部および外部通信レイヤーが正しく構成されて動作していることを確認します。
  2. インストール中に、これが ISA のインストールかどうかの指定を求められます。次の点に注意してください。
     - 質問に対し、これが ISA プロキシ・サーバーのインストールであることを示します。
     - ISA のインストール・ディレクトリのパスを WebGate のインストール・パスとして指定します。
     - 自動 Web サーバー更新機能を使用して、WebGate のインストール中に ISA プロキシ・サーバーを更新します。
  3. WebGate のインストール後、ファイル configureISA4webgate.bat を検索します。このファイルにより、プログラム的に追加する必要がある ISA サーバー・フィルタを構成する多数の vbscript およびプロセスがコールされます。

ディスク領域の要件の評価

表 2-1 に、各コンポーネントに必要な空きディスク領域の推定値を参考として示します。

表 2-1 ディスク領域の要件

	Windows	UNIX
Identity Server	128MB	90MB
WebPass	93MB	200MB
Policy Manager	122MB	130MB
Access Server	95MB	200MB
WebGate	76MB	150MB
SNMP エージェント	50MB	75MB

インストール・ディレクトリの選択

コンポーネントは、デフォルトのディレクトリまたは任意のディレクトリにインストールできます。パス名を変更する際は、オペレーティング・システムで許容されている任意の文字を含めることができます。たとえば、Windows システムでは空白を含めることができますが、UNIX システムではできません。

すべてのファイルおよびパス名は英語の文字のみで指定してください。ファイルおよびパス名に、国際文字は使用できません。

いずれの場合も、プラットフォームに関係なく、一貫した方法で名前を設定することをお薦めします。たとえば、Windows プラットフォームでは、名前に空白ではなくアンダースコアを使用します。通常、Oracle Access Manager のデフォルトのインストール・ディレクトリは次のとおりです。

Windows プラットフォーム : ¥Program Files¥COREid¥

UNIX プラットフォーム : /opt/coreid/（すべて小文字）

表 2-2 に示すように、インストールするコンポーネントによって、パスは若干異なります。次に例を示します。

- すべての Identity コンポーネントのパス名には、¥identity が自動的に追加されます。
- すべての Access コンポーネントのパス名には、¥access が自動的に追加されます。
- WebPass、Policy Manager および WebGate のインストールでは、デフォルトのパス名に ¥WebComponent が（¥identity または ¥access とともに）自動的に追加されます。

表 2-2 インストール・ディレクトリのパス名

コンポーネント	インストール・ディレクトリ
Identity Server	Windows: ¥Program Files¥OracleAccessManager¥identity
	UNIX: /opt/oracleaccessmanager/identity
	このガイド内 : ¥*IdentityServer_install_dir*¥identity
WebPass	Windows: ¥Program Files¥OracleAccessManager¥WebComponent¥identity
	UNIX: /opt/oracleaccessmanager/WebComponent/identity
	このガイド内 : ¥*WebPass_install_dir*¥identity
Access Server	Windows: ¥Program Files¥OracleAccessManager¥access
	UNIX: /opt/oracleaccessmanager/access
	このガイド内 : ¥*AccessServer_install_dir*¥access
Policy Manager	Windows: ¥Program Files¥OracleAccessManager¥WebComponent¥access
	UNIX: /opt/oracleaccessmanager/WebComponent/access
	このガイド内 : ¥*PolicyManager_install_dir*¥access
WebGate	Windows: ¥Program Files¥OracleAccessManager¥WebComponent¥access
	UNIX: /opt/oracleaccessmanager/WebComponent/access
	このガイド内 : ¥*WebGate_install_dir*¥access

このマニュアルでは、各 Oracle Access Manager コンポーネントのインストール・ディレクトリのパスは、表 2-2 に示すように、¥*Component_install_dir* に続いて、このパスに自動的に設定される接尾辞が追加されて表されます。一般的な形式を使用する場合、*Component_install_dir*/identity|access のように、*Component_install_dir* の後に、一般的な接尾辞である identity|access が続きます。

Oracle Access Manager のインストールを UNIX システムで開始する場合、-is:tempdir パス・パラメータを使用して、十分な領域のあるディレクトリをインストール先として指定できます。

UNIX システムでの一時ディレクトリの指定の手順

1. -is:tempdir パラメータを次のコマンドで使用します。次に例を示します。

   ```
   ./ Oracle_Access_Manager10_1_4_0_1_sparc-s2_Identity_Server
   -is:tempdir /export/home/oblix/temp
   ```

   パスは、相対パスではなく、絶対パスである必要があります。

2. パス /export/home/oblix/temp を、十分な領域があるファイル・システムに変更します。

Oracle Access Manager コンポーネントの通信の保護

インストール前に、コンポーネント間で使用するトランスポート・セキュリティのタイプを決定する必要があります。Oracle Access Manager では、コンポーネント間で発生する通信に対して 3 種類のトランスポート・セキュリティをサポートしています。

- オープン : 暗号化されていない通信を許可。2-12 ページの「オープン・モード」を参照。
- シンプル : Oracle による暗号化をサポート。2-13 ページの「シンプル・モード」を参照。
- 証明書 : サード・パーティの証明書が必要。2-13 ページの「証明書モード」を参照。

トランスポート・セキュリティのガイドライン

ここでは、インストール中に Oracle Access Manager コンポーネント間にトランスポート・セキュリティを計画および実装する際に従う必要のあるガイドラインについて説明します。特に、次の点に注意してください。

- すべての ID システムのコンポーネント（Identity Server インスタンスおよび WebPass インスタンス）間のトランスポート・セキュリティは一致している必要があります（すべてオープン、シンプルまたは証明書モード）。
- すべてのアクセス・システム・コンポーネント（Policy Manager、Access Server および関連 WebGate）間のトランスポート・セキュリティは一致している必要があります（すべてオープン、シンプルまたは証明書モード）。

通告

アクセス・キャッシュ・フラッシュが Identity Server で有効化されている場合、Identity Server は Access Server と通信します。この場合、次の 5 つの全コンポーネント間のトランスポート・セキュリティ・モードが同じである必要があります。

- Identity Server および WebPass インスタンス
- Policy Manager、Access Server および関連付けられている WebGate

オープン・モード

トランスポート・セキュリティが環境内で問題ない場合は、オープン・モードを使用します。オープン・モードでは、AccessGate と Access Server 間で認証や暗号化は行われません。AccessGate は Access Server の ID の証明を要求せず、Access Server はすべての AccessGate からの接続を受け入れます。同様に、Identity Server は WebPass からの ID の証明を要求しません。

シンプル・モード

ある程度のセキュリティを確保する場合は、シンプル・モードを使用します。たとえば、独自の認証局（CA）は管理しないけれども、パスワードをプレーン・テキストで送信することは避ける場合などです。

シンプル・モードでは、Web クライアント間（WebPass と Identity Server 間、Policy Manager と WebPass 間、および Access Server と WebGate 間）の通信は、TLS v1 を使用して暗号化されます。シンプル・モードと証明書モードの両方では、Oracle Access Manager コンポーネントは X.509 デジタル証明書のみを使用します。この機能では、標準 cert-decode プラグインが証明書をデコードし、証明書情報を標準 credential_mapping 認証プラグインに渡す証明書認証が WebGate と Access Server 間で行われます。

Oracle Access Manager では、すべての AccessGate および Access Server コンポーネントにインストールされる独自の秘密鍵を持つ CA が用意されています。Oracle Access Manager では、追加のパスワード・チェックを行い、他のカスタマが同じ CA を使用することを防止します。

各公開鍵には、対応する秘密鍵があり、この秘密鍵は Oracle Access Manager によって aaa_key.pem ファイル（Oracle Access Manager の場合は ois_key.pem）に格納されます。¥tools サブディレクトリにある openSSL という名前のプログラムにより、秘密鍵が生成されます。openSSL プログラムは、各 AccessGate および Access Server のインストール中に自動的にコールされます。証明書モードとは異なり、Oracle Access Manager によって秘密鍵はすでに生成されています。この鍵は、インストール中に自動的に提供されます。

シンプル・モードでは、証明書モードと同様に、各コンポーネントのインストール中に指定する Privacy Enhanced Mail（PEM）パスフレーズを使用して秘密鍵を保護します。インストール中に、PEM パスフレーズはグローバル・アクセス・プロトコル・パスフレーズとして参照される場合もあります。このマニュアルでは、パスフレーズという総称を一般に使用します。

注意： AccessGate または Access Server は、秘密鍵を使用する前に、正しいパスフレーズを必要とします。パスフレーズは、名目上暗号化されている password.lst というファイルに格納されます。シンプル・モードでは、PEM パスフレーズは各 WebGate および Access Server インスタンスで同一のものです。

Access Server のインストール中にパスワードをファイルに格納しない場合、次のようになります。

- Windows では、Access Server を起動するたびにパスフレーズを求められます。
- UNIX では、start_access_server スクリプトを起動するたびに、-P オプションを使用してパスワードを渡す必要があります。

証明書モード

サーバー証明書を処理する認証局（CA）が内部にある場合は、証明書（SSL）モードを使用します。証明書モードでは、WebGate と Access Server 間、および Identity Server と WebPass 間の通信は、Transport Layer Security、RFC 2246（TLS v1）を使用して暗号化されます。シンプル・モードと証明書モードの両方では、Oracle Access Manager コンポーネントは X.509 デジタル証明書のみを使用します。この機能では、標準 cert-decode プラグインが証明書をデコードし、証明書情報を標準 credential_mapping 認証プラグインに渡す証明書認証が WebGate と Access Server 間で行われます。

各公開鍵には、対応する秘密鍵があり、この秘密鍵は Oracle Access Manager によって Access Server の場合は aaa_key.pem ファイル（Identity Server の場合は ois_key.pem）に格納されます。

¥tools サブディレクトリにある openSSL という名前のプログラムにより、秘密鍵が生成されます。このプログラムは、各 AccessGate および Access Server のインストール中に自動的にコールされます。インストール中に、CA から取得した証明書を提示します。

秘密鍵は、各コンポーネントのインストール時に指定する Privacy Enhanced Mail（PEM）パスフレーズを使用して保護します。このマニュアルでは、パスフレーズという用語を使用します。

注意： WebGate または Access Server は、秘密鍵を使用する前に、正しい PEM パスフレーズを必要とします。PEM パスフレーズは、WebGate パスフレーズおよびトランスポート・パスワードとしても参照されます。このパスフレーズは、名目上暗号化されている password.lst というファイル（Oracle Access Manager の場合は password.xml）に格納できます。これは、各 WebGate および Access Server で異なるパスフレーズにすることができます。

Oracle Access Manager のインストール中に、証明書をまだ取得していない場合はこれをリクエストできます。この場合、ステータスが証明書保留中でも、インストールを完了できます。ただし、証明書が発行されて適切なディレクトリにコピーされるまで、コンポーネントまたはシステムは設定できません。

証明書リクエストを生成する場合は、次の点に注意してください。

- リクエストが保留中の場合、インストールは通常どおり完了できますが、設定は実行できません。
- リクエストは、コンポーネントのインストール・ディレクトリに配置する必要があります。次に例を示します。

  IdentityServer_install_dir¥identity¥oblix¥config¥ois_req.pem

  通常、.pem ファイルには、リクエストを表す暗号化された文字列の他に、余分なデータも含まれています。
- 選択した CA から次の情報を「証明書リクエスト」フィールドにコピーし、リクエストを CA に送信する必要があります（Oracle ではこれを行いません）。

```
*-----------Begin request---------------
A97C7u54Sd0000lotsofrandomstuff864Ouwst
89111mmmIyoSSTKHS9670sd
*-----------End request-----------------
```

- CA から証明書が返されたら、証明書ファイルを適切なコンポーネントのインストール・ディレクトリにコピーし、コンポーネント・サーバーまたはサービスを再起動できます。次に例を示します。

  ¥*IdentityServer_install_dir*¥identity¥oblix¥config

  詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

Access Server のインストール中にパスフレーズまたはパスワードをファイルに格納しない場合、次のようになります。

- **Windows 上 :** Access Server を起動するたびにパスフレーズを求められます。
- **UNIX 上 :** start_access_server スクリプトを起動するたびに、-P オプションを使用してパスワードを渡す必要があります。

トランスポート・セキュリティ・モードの詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

Web サーバーの要件の実現

WebPass、Policy Manager および WebGate コンポーネントをホストする Web サーバーが 1 つ以上必要です。Identity Server および Access Server では、Web サーバー・インスタンスは不要です。

WebPass と Identity Server を同じ Web サーバーにインストールする場合、WebPass のインストール先を Identity Server と同じにすることはできません。

Policy Manager と WebPass を同じ Web サーバーにインストールする場合は、この 2 つを同じディレクトリ・レベルに配置する必要があります。たとえば、WebPass のインストール・ディレクトリとして C:¥COREid¥WebComponent を指定すると、2 つのコンポーネントが同じマシン上に存在する場合、これを Policy Manager のインストール・ディレクトリとしても指定する必要があります。WebPass のインストール・ディレクトリには ¥identity が追加され、Policy Manager のインストール・ディレクトリには ¥access が追加されます。

インストールを開始する前に、Web サーバーがすべての要件を満たすことを確認してください。2-3 ページの「システム・クロックの同期化」も参照してください。

タスクの概要 : Web サーバーの準備

1. Web サーバーのバージョンが、サポートされているプラットフォーム（Policy Manager、WebPass の Web サーバーおよび WebGate の Web サーバー）のリストに記載されていることを確認します。このリストは、`https://metalink.oracle.com` の「Certify」タブにあります。
   - 指示に従って MetaLink にログインします。
   - 「Certify」タブをクリックします。
   - 「View Certifications by Product」をクリックします。
   - 「Application Server」オプションを選択し、「Submit」をクリックします。
   - 「Oracle Application Server」を選択し、「Submit」をクリックします。
2. データに基づいて実行される Web サーバーの新しいインスタンスを作成し、他のアプリケーションのサービスを停止せずに変更を容易に行えるようにします。詳細は、Web サーバーのドキュメントを参照してください。
3. Web サーバーのインストール先を計画し、詳細を 2-29 ページの「インストール準備のチェックリスト」に記録します。

詳細は、次を参照してください。

- Web サーバー固有のインストール・パッケージ
- Web サーバーに関する一般的な考慮点

Web サーバー固有のインストール・パッケージ

WebPass、Policy Manager および WebGate コンポーネントには、個別の Web サーバー固有のインストール・パッケージが提供されています。必ず使用している Web サーバーおよびプラットフォームに適したインストール・パッケージを選択してください。

- **ISAPI:** Microsoft Internet Information Server と通信する Web サーバー・コンポーネント（Windows 環境の場合は IIS Web サーバー）の識別に Oracle Access Manager で使用するインターネット Web サーバー拡張機能。
- **NSAPI:** Windows または Solaris 上で実行されている Sun（以前の Netscape/iPlanet）の Web サーバーと通信する Web コンポーネントの識別に Oracle Access Manager で使用するインターネット Web サーバー拡張機能。
- **Apache:** Windows、Solaris、Linux などの各種プラットフォーム上で実行されている Apache Web サーバーと通信する Web コンポーネントの識別に Oracle Access Manager で使用するインターネット Web サーバー拡張機能。詳細は、2-28 ページの「プラットフォームの要件の確認」を参照してください。

注意： Oracle Access Manager は、SSL 対応または非対応の Apache をサポートしています。SSL 対応通信では、Apache-SSL ではなく、mod_ssl 付きの Apache がサポートされています。mod_ssl は、Apache-SSL から導出され、Apache-SSL にかわるモジュールです。

Oracle Access Manager 10*g*（10.1.4.0.1）では、SSL 対応または非対応の Apache をサポートするコンポーネント用の単一パッケージが用意されています。次に例を示します。

- APACHE_WebGate は、第 16 章「Apache v1.3 Web サーバーおよび Oracle HTTP Server Web サーバーの構成」で説明されているように、SSL 対応または非対応の v1.3.x をサポートしています。
- APACHE2_WebGate は、SSL 対応または非対応（および Solaris と Linux 上で有効化されているリバース・プロキシ対応または非対応）の v2 をサポートしています。第 17 章「Oracle Access Manager のための Apache v2、IHS および OHS Web サーバーの構成」も参照してください。

- **IHS:** 各種プラットフォーム上で実行されている IBM HTTP（IHS）Web サーバー（powered by Apache）と通信する Oracle Access Manager Web コンポーネントを識別するインターネット Web サーバー拡張機能。次に例を示します。
  - Solaris、Linux および Windows 上の IHS_WebGate powered by Apache v.1.3.x。
  - IBM-AIX 上の IHS2_WebGate powered by Apache v2。第 17 章「Oracle Access Manager のための Apache v2、IHS および OHS Web サーバーの構成」を参照してください。
- **OHS:** Oracle HTTP Server（OHS）と通信する Oracle Access Manager Web コンポーネントを識別するインターネット Web サーバー拡張機能。オラクル社は、オープン・ソース Apache v1.3（OHS_... という名前）および v2（OHS2_... という名前）に基づく OHS Web コンポーネントを提供しています。10*g*（10.1.4.0.1）では、Linux および Windows プラットフォーム上のスタンドアロン Oracle HTTP Server にインストールできる WebPass、Policy Manager および WebGate コンポーネントを用意しています。
  - 『Oracle Access Manager アクセス管理ガイド』で説明されているように、Oracle Single Sign-On との統合を可能にするには、OHS または OHS2 WebGate を Oracle Application Server にインストールする必要があります。
  - OHS または OHS2 WebPass および Access Manager（元の名前は Policy Manager の Web コンポーネントを表す）は、Oracle Application Server とともに使用できます。ただし、Apache WebPass および Access Manager（Policy Manager）の Web コンポーネントもこのアプリケーションに対してサポートされています。

詳細は、第 16 章「Apache v1.3 Web サーバーおよび Oracle HTTP Server Web サーバーの構成」および第 17 章「Oracle Access Manager のための Apache v2、IHS および OHS Web サーバーの構成」を参照してください。バージョンのサポートは、`https://metalink.oracle.com` の「Certify」タブを参照してください。

- **Domino:** 各種プラットフォーム上で実行されている Lotus Domino Web サーバーと通信する Web コンポーネントの識別に Oracle Access Manager で使用するインターネット Web サーバー拡張機能。

  詳細は、第 18 章「WebGates のための Lotus Domino Web サーバーの設定」を参照してください。バージョンのサポートは、`https://metalink.oracle.com` の「Certify」タブを参照してください。

Web サーバーに関する一般的な考慮点

Oracle Access Manager のインストールに含まれる Web サーバーに関しては、次の一般的な考慮点を理解しておくことをお薦めします。

- Identity Server の各インスタンスは、Web サーバーのホスト上にインストールされている WebPass プラグインを介して Web サーバーと通信します。

  Policy Manager と WebPass を同じ Web サーバーにインストールする場合は、この 2 つを同じディレクトリ・レベルに配置する必要があります。たとえば、WebPass のインストール・ディレクトリとして C:¥COREid¥WebComponent を指定すると、2 つのコンポーネントが同じマシン上に存在する場合、これを Policy Manager のインストール・ディレクトリとしても指定する必要があります。WebPass のインストール・ディレクトリには ¥identity が追加され、Policy Manager のインストール・ディレクトリには ¥access が追加されます。

- WebPass、Policy Manager および WebGate のインストール中は、Oracle Access Manager と連動するように Web サーバーを構成する必要があります。この Web サーバー構成の更新を自動または手動で実行するように指定できます。

  注意： Web サーバーの更新プロセスを簡素化してエラーを回避するために、自動構成オプションを使用することをお薦めします。

- ID システムまたは Policy Manager にアクセスする場合は、対象の ID システムまたは Policy Manager に接続されている WebPass インスタンスの Web サーバーのホスト名と WebPass の Web サーバー・インスタンスの HTTP ポートを指定する必要があります。
- WebGate の Web サーバーに関する追加のガイドラインは、2-8 ページの「WebGate のガイドライン」で説明されています。
- UNIX システムでは、WebPass、Policy Manager および WebGate のインストール中に、Web サーバーで使用するユーザー名とグループを指定する必要があります。通常、デフォルトは nobody です。HP-UX では、デフォルトは WWW（ユーザー名）および others（グループ）です。
- Linux システムでは、Apache および OHS を使用する Oracle Access Manager Web コンポーネントをインストールする場合、Web サーバーを実行しているのと同じユーザーとしてインストールするよう求められます。この情報は、User および Group ディレクティブ・エントリの httpd.conf ファイルにあります。

ディレクトリ・サーバーの要件の実現

インストールには、1 つ以上のディレクトリ・サーバーが必要です。インストールを開始する前に、ディレクトリ・サーバーが Oracle Access Manager の要件を満たし、適切に準備されていることを確認してください。

注意： 必要に応じて、付録 A「Active Directory に対する Oracle Access Manager のインストール」および付録 B「ADAM に対する Oracle Access Manager のインストール」も参照してください。

タスクの概要：ディレクトリ・サーバーの準備

1. `https://metalink.oracle.com` の「Certify」タブで説明されているように、ディレクトリ・サーバーがサポートされているプラットフォームのリストに記載されていることを確認します。
   - 指示に従って MetaLink にログインします。
   - 「Certify」タブをクリックします。
   - 「View Certifications by Product」をクリックします。
   - 「Application Server」オプションを選択し、「Submit」をクリックします。
   - 「Oracle Application Server」を選択し、「Submit」をクリックします。

   注意： Siemens DirX ディレクトリは、10*g*（10.1.4.0.1）ではサポートされていません。ただし、インストール画面では、可能なオプションとして DirX が表示される場合があります。

   ---

2. 2-19 ページの「バインド DN の割当て」で説明されているように、インストールおよび設定を完了するマスター管理者として使用される担当者をディレクトリで 1 名以上特定します。
3. 2-19 ページの「ディレクトリ・サーバーの領域の評価」で説明されているように、ディレクトリ・サーバーの領域を推定し、十分な領域があることを確認します。
4. 2-20 ページの「ディレクトリ・サーバーの通信の保護」で説明されているように、ディレクトリ・サーバーと Oracle Access Manager コンポーネントとの通信を保護する方法を決定します。
5. 1 つ以上のディレクトリ・サーバー・インスタンスが Oracle Access Manager のインストールに使用可能であることを確認し、2-22 ページの「データ記憶域の要件」で説明されているように、ユーザー・データを構成およびポリシー・データとは別に格納するかどうかを決定します。
6. 次の項で説明されているように、データの検索ベース、構成 DN およびポリシー・ベースを確立します。
   - ユーザー・データおよび検索ベース
   - 構成データおよび構成 DN
   - ポリシー・データおよびポリシー・ベース
7. 2-27 ページの「Person オブジェクト・クラスおよび Group オブジェクト・クラスの概要」で説明されているように、Person および Group オブジェクト・クラスを記録します。
8. 2-29 ページの「インストール準備のチェックリスト」で説明されているように、次のようなディレクトリ・サーバーの詳細を記録します。
   a. 各ディレクトリ・サーバーのホスト名、IP アドレス、ネットワーク・ポートおよびルート DN。
   b. ディレクトリ・サーバーのユーザー・ログオン ID およびパスワード。

9. 1-6 ページの「スキーマおよび属性の自動更新と手動更新」で説明されているように、スキーマの更新方法（自動または手動）を決定します。

10. スキーマ・データを Oracle Access Manager で使用可能にする方法の詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

    すべてのオブジェクトの継承は、スーパー・クラスが構造化オブジェクト・クラスと補助クラスの両方に共通するという仮定に基づきます。この仮定以外では、オブジェクト・クラスの拡張は不可能です。

バインド DN の割当て

Identity Server と Policy Manager のインストールおよび設定中に、バインド DN（Oracle Access Manager ではルート DN とも呼ばれる）を指定するよう求められます。Oracle Access Manager のバインド先のディレクトリ・アカウントには、読取り、書込み、追加、削除、検索、比較および自己書込み権限が必要です。これらの権限を持つユーザーの作成方法は、ディレクトリ・ベンダーによって異なります。詳細は、ディレクトリのドキュメントを参照してください。

ネイティブ・ディレクトリのアクセス制御命令（ACI）およびアクセス制御リスト（ACL）によって Oracle Access Manager のバインド DN アカウントのアクセスがユーザーおよび構成ブランチに制限されないようにしてください。制限されると、Oracle Access Manager のバインド DN は、パスワード・ポリシーなどのネイティブ・ディレクトリ・サーバーの制約によって影響を受ける場合があります。

また、バインド DN として作成するユーザーは、Oracle Access Manager ソフトウェアのアップグレードの実行時にスキーマにアクセスできる必要があります。これはスキーマがアップグレード中に変更される場合があるためです。スキーマがバインド DN にアクセスできない場合、アップグレードは失敗し、アップグレードの完了には手動の操作が必要になります。これには、ACL でディレクトリ・スキーマ・エントリを変更することが含まれます。

次のガイドラインを考慮してください。

Oracle Internet Directory: Oracle Internet Directory を使用する Identity Server をインストールする場合、完全修飾された DN（cn=orcladmin,cn=users,dc=us,dc=mycompany,dc=com）ではなく、ルート DN をスーパーユーザー cn=orcladmin として指定する必要があります。

Sun（以前の iPlanet）: バインド DN ユーザーをディレクトリ・マネージャ以外にすることをお薦めします。かわりに、別のユーザーをバインド DN として作成します。ディレクトリ・マネージャ・アカウントは、ディレクトリ・サーバーのサイズとタイムアウトの制限を無視します。このため、大規模な検索によってディレクトリ・サーバーの動作が妨げられる場合があります。

詳細は、「ユーザー・データおよび検索ベース」も参照してください。

ディレクトリ・サーバーの領域の評価

ディレクトリ・サーバーでは、各ユーザー・オブジェクトに対して少なくとも 1KB の RAM が必要です。各 Oracle オブジェクトには、少なくとも 16KB の RAM が必要です。

次の情報を参照し、インストールに必要な領域を計算してください。

- 250,000 のユーザー・オブジェクトが含まれるディレクトリ・サーバーでは、最大で 250MB の RAM が必要です。
- このサイズのディレクトリでは、5,000 の Oracle オブジェクト（250,000 のユーザー・エントリに対する高い見積り）を含むことができ、これによって追加の 80MB が必要になります。
- このデータ量に対する索引には、Oracle オブジェクトの約 2 倍の領域（約 160MB）が必要です。

ディレクトリ・サーバーの通信の保護

Identity Server、Policy Manager および Access Server は、ディレクトリ・サーバーと通信します。Oracle Access Manager のインストールおよび設定中に、ディレクトリ・サーバーと通信するコンポーネント用のデフォルトのディレクトリ・プロファイルが作成されます。各ディレクトリ・プロファイルには、ディレクトリ・サーバーの通信方法などが示されているデータベース（DB）インスタンス・プロファイルが含まれています。Oracle Access Manager とディレクトリ・サーバー間では、非セキュアとセキュアの 2 つの通信方法を使用できます。Oracle Access Manager とディレクトリ・サーバー間のセキュア通信は、SSL 対応通信とも呼ばれます。非セキュア通信は、オープン通信とも呼ばれます。

Oracle Access Manager は、base64 形式の CA 証明書をサポートしています。SSL 対応通信では、サード・パーティの認証局から提供される base64 形式の署名者の証明書（ルート CA 証明書）を必要とします。たとえば、Identity Server とディレクトリ・サーバー間で SSL を使用する場合、Identity Server のインストール中に、SSL 対応通信を確立するための証明書へのパスを指定するよう求められます。この場合、ディレクトリ・サーバーの指示に従い、証明書がディレクトリ・サーバーにインストールされる必要があります。ディレクトリ・サーバーがクライアント認証を要求しないようにしてください（この方法は、ディレクトリ・サーバーのドキュメントを参照してください）。

ディレクトリ・サーバーに SSL を構成する場合、Oracle Access Manager ではサーバー認証のみをサポートしていることに注意してください。クライアント認証はサポートされていません。Oracle Access Manager では、製品の設定中にインポートされたルート CA 証明書に対してサーバー証明書を検証します。

ガイドライン

Oracle Access Manager とディレクトリ・サーバー間の通信を計画および構成する際は、次のガイドラインが適用されます。

- Identity Server とディレクトリ・サーバー間の通信は同じである必要はありません。
- Access Server とディレクトリ・サーバー間の通信は同じである必要はありません。
- すべての Policy Manager とディレクトリ・サーバー間の通信は一環している必要があります（すべて SSL 対応またはすべてオープン）。

注意： ユーザー・データを構成およびポリシー・データとは異なるディレクトリ・サーバー・タイプに格納する場合、複数のルート CA 証明書がサポートされます。ユーザー・データ、構成データおよびポリシー・データをディレクトリ・サーバー・タイプに格納すると、それぞれが個別のルート CA を使用できます。詳細は、2-22 ページの「データ記憶域の要件」を参照してください。

通告

Policy Manager が Sun（以前の Netscape）Web サーバーを使用する Solaris 上にインストールされた場合、ディレクトリ・サーバーとの SSL 対応通信はサポートされません。Solaris 上に Policy Manager がある異機種間環境では、ディレクトリ・サーバーとインストールするすべての Policy Manager との間にオープン通信を指定してください。

Oracle Access Manager コンポーネントは、ディレクトリ・サーバーとの通信に同じモードを使用するようにインストールされていなくても、DB プロファイルを共有できます。たとえば、Identity Server と Access Server がオープン・モードでインストールされており、Policy Manager が SSL 対応でインストールされているとします。この場合、ディレクトリ・サーバーと通信する各 Oracle Access Manager コンポーネントに対して cert8.db および key3.db ファイルが存在する必要があり、これらのファイルが Oracle Access Manager の *Component_install_dir*¥identity | access¥oblix¥config ディレクトリに置かれている必要があります。これらのファイルは、他の Oracle Access Manager コンポーネント・ディレクトリからコピーするか、genCert（Policy Manager）またはその他のユーティリティを実行して生成できます。

注意： Oracle Access Manager 10*g*（10.1.4.0.1）は、cert7.db（アップグレードされた環境）と cert8.db（新規インストール）の両方の証明書ストアと連動します。アップグレードされた環境の詳細は、『Oracle Access Manager アップグレード・ガイド』を参照してください。

すべてのディレクトリ・サーバー：ディレクトリ・サーバーに SSL を構成する場合、Oracle Access Manager ではサーバー認証のみをサポートしていることに注意してください。クライアント認証はサポートされていません。Oracle Access Manager では、製品の設定中にインポートされたルート CA 証明書に対してサーバー証明書を検証します。

タスクの概要：ディレクトリ・サーバーの通信のセキュリティの定義

1. Oracle Access Manager をインストールする前に、この項および 2-18 ページの「ディレクトリ・サーバーの要件の実現」で説明されているように、10*g*（10.1.4.0.1）に対するすべてのディレクトリ・サーバーの要件を確認してください。
2. Oracle Access Manager のインストールの前に、ディレクトリ・サーバーのベンダーおよび証明書のドキュメントに従い、必要に応じて SSL をディレクトリ・サーバーで有効化します。たとえば、次のようにします。
   a. ディレクトリ・サーバー・インスタンスがない場合は、これを作成します。
   b. そのインスタンスの証明書を CA に申請します。
   c. 証明書をインストールしてディレクトリ・サーバー・インスタンスを暗号化し、ディレクトリ・サーバーを再起動します。

   注意： ユーザー・データを構成およびポリシー・データとは異なるディレクトリ・サーバー・タイプに格納する場合、複数のルート CA 証明書がサポートされます。
3. 2-20 ページの「ディレクトリ・サーバーの通信の保護」で説明されているように、Identity Server のインストール中に、ディレクトリ・サーバーと Identity Server 間に適切な通信を選択します。
4. この項および第 6 章「ID システムの設定」で説明されているように、ID システムの設定中に、ディレクトリ・サーバーと ID システム間に適切な通信を選択します。

   注意： 下位 CA によって生成された証明書を使用している場合、ルート CA の証明書は下位 CA 証明書とともに、xxx_chain.pem に存在する必要があります。検証を適切に行い、ID システムを正常に設定するためには、両方の証明書が存在する必要があります。
5. 2-20 ページの「ディレクトリ・サーバーの通信の保護」で説明されているように、Policy Manager のインストールおよび設定中に、ディレクトリ・サーバーと Policy Manager 間に適切な通信を選択します。
6. 2-20 ページの「ディレクトリ・サーバーの通信の保護」で説明されているように、Access Server のインストール中に、ディレクトリ・サーバーと Access Server 間に適切な通信を選択します。
7. 『Oracle Access Manager ID および共通管理ガイド』で説明されているように、インストール後に、Oracle Access Manager とディレクトリ・サーバー間の通信モードを変更できます。

データ記憶域の要件

ここでは、データ記憶域のオプションと要件の詳細を説明します。この情報は、Identity Server、Policy Manager および Access Server に関係があります。

すべてのディレクトリ・サーバー・タイプ : Oracle Access Manager は、単一のディレクトリ・サーバーへのユーザー・データ、Oracle Access Manager 構成データおよびポリシー・データの格納をサポートしています。

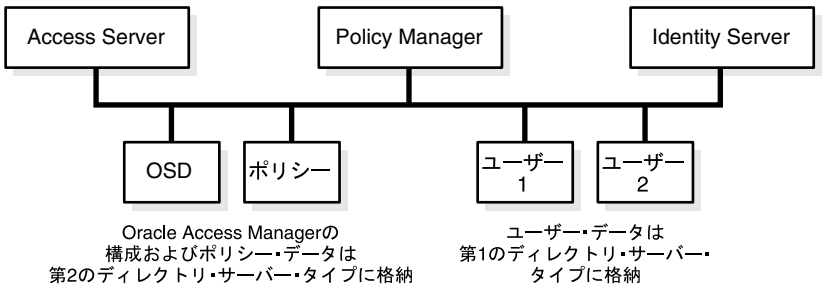
また、ユーザー・データをあるディレクトリ・サーバー・タイプに格納し、Oracle Access Manager の構成およびポリシー・データを別のタイプのディレクトリ・サーバーに格納することもできます。たとえば、ユーザー・データを Active Directory に格納し、Oracle Access Manager の構成およびポリシー・データを ADAM（または Oracle Internet Directory）に格納できます。

ユーザー・データを構成およびポリシー・データとは別のディレクトリ・サーバーのタイプに格納する場合、次のようになります。

- すべてのユーザー・データは、同じディレクトリ・サーバー・タイプに格納する必要があります。
- 構成データとポリシー・データは、同じディレクトリ・サーバー・タイプに格納する必要があります。
- SSL では、個別のルート CA がサポートされます。

図 2-1 は、ユーザー・データを構成およびポリシー・データとは別のディレクトリ・サーバー・タイプに格納した場合を示しています。

図 2-1 別のディレクトリ・サーバー・タイプに格納されたユーザー・データ



データを異なるディレクトリのタイプに格納する場合、ユーザー・データの検索ベース、構成 DN およびポリシー・ベースは一意である必要があります。

Oracle Access Manager のインストールおよび設定中に、環境に適したユーザーおよび構成ディレクトリ・サーバー・タイプを選択する必要があります。

構成およびポリシー・データの両方をユーザー・データとは異なるディレクトリ・サーバー・タイプに格納した場合、次のファイルが機能します。

IdentityServer_install_dir¥identity¥oblix¥data¥common¥ldaposdreferentialintegrityparams.xml

これは、構成およびポリシー・データがユーザー・データとは異なるディレクトリ・サーバー・タイプに格納される場合、ldapreferentialintegrityparams.xml ファイル内の `"referential_integrity_using" Value="oblix"` が適用されないためです。

また、この場合は、サーバーを DB プロファイルにマップするために、元の exclude_attrs ファイルではなく、次のファイルが ID システムとアクセス・システムによって使用されます。

IdentityServer_install_dir¥identity¥oblix¥data¥common¥

exclude_user_attrs.xml

exclude_oblix_attrs.xml

PolicyManager_install_dir¥access¥oblix¥data¥common¥

AccessServer_install_dir¥access¥oblix¥data¥common¥

exclude_oblix_attrs.lst

ユーザー・データのディレクトリ・サーバーのすべてのパラメータは、DB プロファイルを使用して読み取られます。構成データのディレクトリ・サーバーでは、DB サブタイプは次の場所から読み取られます。

Component_install_dir¥identity | access¥oblix¥config¥ldap¥*DB.xml

Data Anywhere: このディレクトリ・サーバー・オプションは、ユーザー・データのディレクトリ・サーバーでのみ使用でき、Oracle Virtual Directory での実装は第 10 章「Oracle Virtual Directory を使用した Oracle Access Manager の設定」で説明されています。Data Anywhere は、ユーザー・データを複数のソース（RDBMS および LDAP ディレクトリなど）から、ID システムで管理できる仮想 LDAP ツリーに集約および統合するデータ管理レイヤーであり、アクセス・システムを使用した認証および認可のサポートに使用されます。

Oracle Access Manager の構成およびポリシー・データを含んでいる LDAP ディレクトリ・ブランチは、VDS またはユーザー・データをホストするディレクトリ・サーバー以外の 1 つ以上のディレクトリ・サーバーに存在する必要があります。Oracle Access Manager アプリケーションは、VDS 仮想ディレクトリ外に存在する構成およびポリシー情報のみを認識します。

警告： Data Anywhere とともに使用する Oracle Access Manager をインストールする前に、第 10 章「Oracle Virtual Directory を使用した Oracle Access Manager の設定」を読み、指定されているアクティビティを完了してください。

IBM Directory Server（以前の SecureWay）: すべてのディレクトリ・サーバー・タイプについての前述の詳細を参照してください。

Oracle Internet Directory および Sun: Oracle Access Manager では、Oracle Internet Directory（複数レルム）および Sun ディレクトリ・サーバーを使用して、構成およびポリシー・データとは別にユーザー・データを格納できます。これらのディレクトリ・サーバーを使用すると、データを同じディレクトリ・サーバーに格納するか、同じタイプの別のディレクトリ・サーバーに格納できます。次に例を示します。

- ユーザー・データは、構成データとは別に、または一緒に格納できます。
- 構成データは、ユーザー・データとは別に、または一緒に格納できます。
- ポリシー・データは、ユーザー・データとは別に、または一緒に格納できます。

データを異なるディレクトリに格納する場合、ユーザー・データの検索ベース、構成 DN およびポリシー・ベースは結合されていない必要があります。つまり、ポリシーおよび構成データを異なる Sun ディレクトリ、または複数の Oracle Internet Directory レルムに格納する場合、これらの DN は一意である必要があります。

注意： Oracle Internet Directory では、構成 DN の値は、ID 管理レルムのコンテキスト（cn=OracleContext）から移入されます。また、デフォルトでは、検索ベースは構成 DN と同じです。

複数のユーザー・データ・ディレクトリおよび検索ベースを使用する場合、インストールおよび設定中にメインのユーザー・データ・ディレクトリと検索ベースを指定してください。

Active Directory、ADAM および Novell eDirectory に関する通告

Novell 社の eDirectory、Active Directory および Active Directory アプリケーション・モード（ADAM）による参照整合性の厳格な保持のため、Oracle Access Manager の構成データおよびポリシー・データは、共通のディレクトリ環境に格納する必要があります。Novell eDirectory、Active Directory および ADAM は、LDAP の実装ではより厳格であり、参照整合性を強化します。これらのディレクトリ・サーバーでは、相互参照（DN 参照など）を使用してデータを 2 つの個別のツリー / フォレストに格納することはできません。

Oracle Access Manager では、ユーザー・データを製品の構成データおよびポリシー・データとは別のディレクトリを用意すると、同じ Novell ディレクトリ・サーバー・ツリーまたは Active Directory フォレストに意図せず存在する複数の異なるサーバー上で個別の LDAP（非結合）ツリーを使用できます。Oracle Access Manager の構成データおよびポリシー・データは、ディレクトリ環境全体の個別の部分に格納でき、このため、Oracle Access Manager 固有の情報をユーザー・データから分離できます。

Active Directory 上 : Active Directory 環境では、Oracle Access Manager の構成データをある特定のドメイン・コントローラに格納し、ポリシー・データを別のコントローラに格納できます。ポリシー・データと構成データのドメイン・コントローラは、同じフォレスト内に存在する必要があります。ユーザー・データは、同じフォレスト内に存在する必要はありません。レプリケーションについては、これを回避するか、十分に理解することが重要です。詳細は、付録 A「Active Directory に対する Oracle Access Manager のインストール」を参照してください。

ユーザー・データを構成およびポリシー・データとは別のディレクトリ・サーバー・タイプに格納する場合、補助クラスのサポートが一致する必要があります。Oracle Access Manager では、動的補助に対する混合モードはサポートしていません。ユーザー・データのディレクトリ・サーバーと構成データのディレクトリ・サーバーが別々のフォレストに存在する場合は、ADSI を使用していずれかのディレクトリ・サーバーに接続できます。ADSI では、両方のフォレストに対して同時にバインドを実行することはできません。ADSI が有効化されている場合、次のようになります。

- **ユーザー・データのディレクトリ・サーバー :** Identity Server および Policy Manager の設定中に、ADSI がユーザー・データのディレクトリ・サーバー・タイプに選択された場合、構成のディレクトリ・サーバー・タイプの詳細を選択する際に「ADSI」チェック・ボックスは使用できません。
- **構成データのサーバー :** このディレクトリ・タイプで ADSI が有効化されている場合、次のようになります。
  - Identity Server の globalparams.xml ファイルで、パラメータ "IsADSIEnabled" および値 "true" が表示されます。
  - Policy Manager の globalparams.lst ファイルで、パラメータ "adsiEnabled"=true が表示されます。

    Active Directory の dbSubType "adsiEnabled" フラグは、DB プロファイルを使用して読み取られます。ADSI がユーザー・データのディレクトリ・サーバーに対して有効化されている場合、この値は ADSI です。ActiveDirectory および ADAM フラグは globalparams.xml ファイルから削除されます。

    詳細は、付録 A「Active Directory に対する Oracle Access Manager のインストール」を参照してください。

ユーザー・データのディレクトリ・サーバー・タイプが Active Directory の場合、exclude_attrs-ad.xml のコンテンツは次の場所にコピーされます。

IdentityServer_install_dir¥identity¥oblix¥data¥common¥exclude_user_attrs.xml

構成およびポリシー・データのディレクトリ・タイプが Active Directory の場合、exclude_attrs-ad.xml .lst のコンテンツは次の場所にコピーされます。

IdentityServer_install_dir¥identity¥oblix¥data¥common¥exclude_oblix_attrs.xml

PolicyManager_install_dir ¥access¥oblix¥data¥common¥exclude_oblix_attrs.lst

AccessServer_install_dir¥access¥oblix¥data¥common¥exclude_oblix_attrs.lst

注意： ActiveDirectory フラグは globalparams.xml で表示されなくなります。

ADAM の場合：データは次のように格納できます。

- ユーザー・データは、構成およびポリシー・データとは異なるパーティションに格納できます。
- ユーザー・データは、構成およびポリシー・データとは別のディレクトリ・サーバー・タイプに格納できます。
- Oracle Access Manager では、構成およびポリシー DN に対して、オブジェクト・クラス属性の値が organizationalUnit（ou）のノードを必要とします。
- 構成およびポリシー・データは、同じ ADAM インスタンスを共有するか、異なる ADAM インスタンスに格納できます。

詳細は、付録 B「ADAM に対する Oracle Access Manager のインストール」を参照してください。

Novell eDirectory: GroupOfUniqueNames に関する問題を回避するために、LDAP グループ・オブジェクトの Groups に対するクラス・マッピングを変更し、groupOfNames（デフォルト）ではなく GroupOfUniqueNames を参照するようにします。変更しない場合、いずれかの属性を保存するたびに、スキーマ違反が発生する可能性があり、グループが正しく機能しないことがあります。たとえば、NDS の場合、groupOfUniqueNames LDAP グループ・オブジェクトは、groupOfNames オブジェクトより前に一覧表示される必要があります。

NDS Console1 による順序変更の手順

1. NDS ツリーを開きます。
2. 左側のペインの NDS ノードに対し、右側のペインで「LDAP Group」オブジェクトを右クリックし、「Properties」→「Class Map」タブを選択します。
3. 2 つのグループ・オブジェクトが表示される順序を変更します。

   このマッピングを追加する方法の詳細は、Novell eDirectory のドキュメントを参照してください。

ユーザー・データおよび検索ベース

ユーザー・データは、ID システムで管理されるユーザー・ディレクトリのエントリで構成されます。このデータには、ID システムで管理されるユーザー、グループ、場所およびその他の汎用オブジェクトに関する情報が含まれます。

Oracle Access Manager のインストール時は、メイン・ディレクトリ・サーバーのプロファイルを設定するために、次の情報を指定する必要があります。

- ユーザー・データを格納するディレクトリ・サーバーのタイプ
- DNS ホスト名、ポート、ユーザー名（バインド DN）、パスワードなどのバインド情報
- 検索ベース（このデータが格納されるディレクトリ情報ツリー、すなわち DIT 内のノードと、すべてのユーザー・データ検索に使用可能な最上位のベースを識別する）

  注意： 複数のユーザー・データ・ディレクトリおよび検索ベースを使用する場合、インストールおよび設定中にメインのユーザー・データ・ディレクトリと検索ベースを指定してください。設定後、1 つ以上のデータベース・プロファイルを手動で追加して非結合ネームスペースを追加する必要があります。

- マスター管理者（1 名以上）

構成情報を含む Oracle Access Manager スキーマ・クラスをロードするために、設定中にディレクトリを自動的に更新することをお薦めします。

次のガイドラインに従ってください。

Oracle Internet Directory: Oracle Internet Directory を使用する Identity Server をインストールする場合、完全修飾された DN（cn=orcladmin,cn=users,dc=us,dc=mycompany,dc=com）ではなく、ルート DN をスーパーユーザー cn=orcladmin として指定する必要があります。

Sun（以前の iPlanet）: バインド DN ユーザーをディレクトリ・マネージャ以外にすることをお薦めします。かわりに、別のユーザーをバインド DN として作成します。ディレクトリ・マネージャ・アカウントは、ディレクトリ・サーバーのサイズとタイムアウトの制限を無視します。このため、大規模な検索によってディレクトリ・サーバーの動作が妨げられる場合があります。

詳細は、2-22 ページの「データ記憶域の要件」を参照してください。

構成データおよび構成 DN

構成データ（Oracle Access Manager の構成の詳細）は、ディレクトリに格納されます。このデータには、ID システムおよびアクセス・システムの表示形式と機能を決定するワークフローおよび構成情報が含まれます。構成データは、ID システムで管理されます。

Oracle Access Manager のインストール時は、構成データを格納するディレクトリ・サーバーの詳細を指定する必要があります。構成データとユーザー・データを一緒に格納する場合、この情報は同じになります。次の通告が適用されます。

- 構成データのバインド DN は、ベース接尾辞以外の任意の場所にすることができます。
- 構成データのバインド DN（構成 DN とも呼ばれる）は、ユーザー・データの検索ベースと類似しており、ID システムおよびアクセス・システムの Oracle Access Manager スキーマとすべての構成データが格納される DIT 内のノードを識別するために指定する必要があります。
- 2-22 ページの「データ記憶域の要件」で説明されているように、追加の通告が適用される場合もあります。

注意： Oracle Internet Directory では、構成 DN の値は、ID 管理レルムのコンテキスト（cn=OracleContext）から移入されます。また、デフォルトでは、検索ベースは構成 DN と同じです。

前述のように、構成情報を含む Oracle Access Manager スキーマ・クラスをロードするために、設定中にディレクトリを自動的に更新することをお薦めします。

Oracle Internet Directory: Oracle Internet Directory では、構成 DN の値は、ID 管理レルムのコンテキスト（cn=OracleContext）から移入されます。また、デフォルトでは、検索ベースは構成 DN と同じです。複数レルム・インストールの場合、ID システムのインストールおよび設定後に非結合検索ベースを設定する方法の詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

ポリシー・データおよびポリシー・ベース

ポリシー・データは、リソースへのアクセスを決定するポリシー定義およびルールで構成されます。このデータは、Policy Manager によってディレクトリ・サーバーで管理されます。

Oracle Access Manager のインストール時は、ポリシー・データをインストールするディレクトリ・サーバーの詳細を指定する必要があります。ポリシー・データをユーザー・データとは別に格納する場合、ディレクトリ・サーバーの詳細は、ユーザーまたは構成データに指定する詳細とは異なります。詳細は、2-22 ページの「データ記憶域の要件」を参照してください。

Policy Manager の設定中は、Oracle Access Manager のすべてのポリシー・データが格納される DIT 内の場所と、すべてのポリシー検索に使用可能な最上位のベースを識別するために、ポリシー・ベースも指定する必要があります。Policy Manager の設定時にデフォルトの "/" をポリシー・ドメインとして受け入れると、Web サーバー全体が保護されます。

Person オブジェクト・クラスおよび Group オブジェクト・クラスの概要

Oracle Access Manager では、User と Group を標準の Person および Group オブジェクト・クラスとしてそれぞれサポートしています。また、Oracle Access Manager では、User と Group をサポートしています。

Person オブジェクト・クラスは、ユーザーのプロファイル情報を定義します。使用する特定のオブジェクト・クラスがない場合、Oracle Access Manager では一般的な Person オブジェクト・クラス定義を自動的に構成できます。

Person オブジェクト・クラス

- **User:** Active Directory
- **InetOrgPerson:** ADAM、Data Anywhere（Oracle Virtual Directory）、IBM、Oracle Internet Directory および Sun ディレクトリ・サーバー
- **organizationalPerson:** NDS

Group オブジェクト・クラスは、グループの属性を定義します。使用する特定のオブジェクト・クラスがない場合、Oracle Access Manager では一般的な Group オブジェクト・クラス定義を次のように自動的に構成できます。

Group オブジェクト・クラス

- **Group:** Active Directory
- **GroupofUniqueNames:** ADAM、Data Anywhere、IBM、NDS、Oracle Internet Directory および Sun ディレクトリ・サーバー

プラットフォームの要件の確認

Oracle Access Manager 10*g*（10.1.4.0.1）では、様々なオペレーティング・システム、ディレクトリ・サーバー、Web サーバー、コンパイラおよびブラウザをサポートしており、多数のアプリケーション・サーバー、ポータル・サーバー、システム管理製品およびアプリケーション・パッケージとの統合もサポートしています。

最新のサポート情報は、次のサイトの「Certify」タブを参照してください。

```
http://metalink.oracle.com
```

MetaLink の使用手順

1. `http://metalink.oracle.com` に移動します。
2. 指示に従って MetaLink にログインします。
3. 「Certify」タブをクリックします。
4. 「View Certifications by Product」をクリックします。
5. 「Application Server」オプションを選択し、「Submit」をクリックします。
6. 「Oracle Application Server」を選択し、「Submit」をクリックします。

無料のリリース・ノート、ホワイトペーパーまたはその他の資料をダウンロードするには、Oracle Technology Network（OTN）にアクセスしてください。OTN を使用するには、オンライン登録が必要です。登録は無料であり、次のサイトで行うことができます。

```
http://www.oracle.com/technology/membership/
```

OTN のユーザー名とパスワードがすでにある場合は、OTN の Web サイトの次のドキュメント・セクションに直接アクセスできます。

```
http://www.oracle.com/technology/documentation/
```

インストーラ用の一時ディレクトリの準備

Oracle Access Manager のインストール・メディアには、言語パックなど、Oracle Access Manager コンポーネントのインストールに必要なすべての製品パッケージが用意されています。これらのパッケージは、Oracle Access Manager コンポーネントをインストールするディレクトリとは別の一時インストール・ディレクトリにコピーすることをお薦めします。Oracle Access Manager のコンポーネントを 1 つ以上の言語パックとともにインストールする場合は、必要な言語パッケージをコンポーネント・インストーラと同じ一時ディレクトリにコピーする必要があります。別のディレクトリにコピーすると、コンポーネント・インストーラは言語パックを検出できず、インストール時に言語パックを提供できません。言語パックをインストールしない場合は、目的の Oracle Access Manager コンポーネントをインストール・メディアから直接インストールできます。

インストール用の Oracle Access Manager インストーラの格納の手順

1. Oracle Access Manager コンポーネント・インストーラ（ID システムおよびアクセス・システムに必要なすべての言語パック・インストーラを含む）を格納する一時ディレクトリを作成します。
2. インストール・メディアから、コンポーネントと言語パックを同時にインストールできる一時ディレクトリに、Oracle Access Manager パッケージをコピーします。
3. コンポーネントのインストール中 : このマニュアルの該当する章で説明されているように、インストーラを一時ディレクトリから実行します。

Oracle Access Manager コンポーネントのアンインストール

Oracle Access Manager コンポーネントのインストール時には、特定の操作を行った後に情報が保存されます。情報が保存されるまでは、前に戻って、詳細を指定しなおすことができます。ただし、コンポーネントがインストール中であると通知された後は、ファイル・システムに Oracle Access Manager ファイルが追加されています。

注意： コンポーネントをインストール中であることを示すメッセージの通知後、およびすべての手順の完了前にインストール・プロセスを取り消す場合は、Oracle Access Manager 関連の情報を削除してシステムをその前の状態にリストアする必要があります。

Oracle Access Manager に加えられた変更の一部は、自動的には処理されず、アンインストーラ・プログラムの終了時に手動で削除する必要があります。Oracle Access Manager コンポーネントを削除する方法の詳細は、第 20 章「Oracle Access Manager の削除」を参照してください。

状況によっては、既存の Identity Server 名を再利用する場合があります。システム・コンソールで元の Identity Server 名を削除しないと、新しいインスタンスの設定の後でログインしたときに、「アプリケーションが設定されていません」というメッセージが表示されることがあります。Identity Server 名をリサイクルするときは、アプリケーションを設定してログインするために特別な手順を実行する必要があります。詳細は、20-6 ページの「Identity Server インスタンス名のリサイクル」を参照してください。

インストール準備のチェックリスト

Oracle Access Manager をインストールするには、多少の計画が必要です。このためチェックリストが用意されています。たとえば、表 2-3 のチェックリストは次のように使用できます。

- 実際の環境を計画し、記録できるスペースがあります。
- Oracle Access Manager のインストールおよび設定中に表示されるプロンプトに応答するための準備に役立ちます。
- 1-2 ページの「インストール・タスクの概要」に記載のコンポーネントの推奨されるインストール順序と、各コンポーネントのインストール・プロセスに従って編成されています。
- このマニュアル内の特定のページ番号への参照があり、追加情報を検索できます。

表 2-3 インストール準備のチェックリスト

タスク	サブタスク	チェックリスト：Oracle Access Manager のインストールおよび設定の準備	参照
1 ～ 3		ID システムのインストールおよび設定の準備	
1		**Identity Server のインストールの準備**	
	1.1	デフォルト・ロケール（管理者の言語） 言語 言語パック	第 3 章「マルチ言語環境の概要」を参照
	1.2	Identity Server と WebPass 間のトランスポート・セキュリティ・モード： ■ オープン ■ シンプル ■ 証明書	2-12 ページの「Oracle Access Manager コンポーネントの通信の保護」を参照

表 2-3 インストール準備のチェックリスト（続き）

タスク	サブタスク	チェックリスト : Oracle Access Manager のインストールおよび設定の準備	参照
	1.3	この Identity Server インスタンスを識別するために Oracle Access Manager 内で使用される一意の Identity Server ID: Identity Server がインストールされるマシンのホスト名 : Identity Server/WebPass 通信用のポート番号 : これがこのディレクトリ・サーバーにインストールされる最初の Identity Server かどうか ■ ○ ■ ×	
	1.4	ディレクトリ・サーバーと Identity Server 間のセキュリティ・モード : ■ SSL ■ オープン SSL の場合、ルート CA 証明書へのパス : シンプル・モードのみ グローバル・アクセス・プロトコル・パスフレーズ 証明書モードのみ 証明書 PEM パスフレーズ : 証明書リクエスト・ファイルのパス（証明書リクエストのみ）: 証明書ファイルのパス（証明書モードのみ）: キー・ファイルのパス（証明書モードのみ）: 連鎖ファイルのパス（証明書モードのみ）:	
	1.5	ディレクトリ・サーバー詳細の準備 ディレクトリ・サーバー内の構成データの場所 : ■ ユーザー・データ・ディレクトリ・サーバー ■ 個別のディレクトリ・サーバー ■ 手動インストール ディレクトリ・サーバー・タイプ : ■ Sun Directory Server 5.x ■ NDS ■ Active Directory ■ Windows サーバー 2003 上の Active Directory ■ Active Directory アプリケーション・モード ■ IBM Directory Server ■ Data Anywhere **注意 :** Data Anywhere（Oracle Virtual Directory Server）は、ユーザー・データのディレクトリ・サーバーでのみ使用できます。構成およびポリシー・データは、ネイティブ・ディレクトリに格納する必要があります。 ディレクトリ・サーバーのホスト・マシンの名前または IP アドレス : ディレクトリ・サーバーのポート番号 : ディレクトリ・サーバーのバインド DN:	Data Anywhere を使用する Oracle Access Manager をインストールする前に、第 10 章「Oracle Virtual Directory を使用した Oracle Access Manager の設定」を参照

表 2-3 インストール準備のチェックリスト（続き）

タスク	サブタスク	チェックリスト : Oracle Access Manager のインストールおよび設定の準備	参照
		ディレクトリ・サーバーの管理パスワード :	
	1.6	（**Windows のみ**）Identity Server の複数インスタンスをインストールする場合は、このインスタンスを「サービス」ウィンドウで識別する一意の Identity Server サービス名 :	
2		**WebPass をインストールする準備** 次を決定する :	
	2.1	デフォルト・ロケール（管理者の言語）	
		言語	
		言語パック	
		Identity Server と同じ言語パック	
		Web サーバーのユーザー名（UNIX のみ）:	
		Web サーバーのグループ（UNIX のみ）:	
		WebPass のインストール・ディレクトリ。Identity Server と同じマシンにインストールする場合、Identity Server と同一のインストール・ディレクトリは使用不可。	
	2.2	Identity Server と WebPass 間のトランスポート・セキュリティ・モード :	この表のタスク 1 を参照 2-12 ページの「Oracle Access Manager コンポーネントの通信の保護」を参照
		WebPass インスタンスの識別に Oracle Access Manager で使用される WebPass ID:	
	2.3	WebPass のホスト名 :	
		Identity Server/WebPass 通信用のポート番号 :	この表のタスク 1 を参照
		シンプル・モードのみ	この表のタスク 1 を参照
		グローバル・アクセス・プロトコル・パスフレーズ	
		証明書モードのみ	
		証明書 PEM フレーズ :	
		証明書リクエスト・ファイルのパス（証明書リクエストのみ）:	
		証明書ファイルのパス（証明書モードのみ）:	
		キー・ファイルのパス（証明書モードのみ）:	
		連鎖ファイルのパス（証明書モードのみ）:	
	2.4	Web サーバーを WebPass の情報に基づいて自動的に更新するかどうか ■ ○ ■ ×	
		更新する場合、obj.conf ファイル（Apache の場合は httpd.conf ファイル）を含んでいる Web サーバーの構成ディレクトリの絶対パス :	

表 2-3 インストール準備のチェックリスト（続き）

タスク	サブタスク	チェックリスト : Oracle Access Manager のインストールおよび設定の準備	参照
3		**ID システムの設定の準備**	
		次を決定する :	
	3.1	ディレクトリ・サーバー・タイプ :	この表のタスク 1 を参照
		ディレクトリ・サーバーのホスト・マシンの名前または IP アドレス :	この表のタスク 1 を参照
		ディレクトリ・サーバーのポート番号 :	この表のタスク 1 を参照
		ディレクトリ・サーバーのバインド DN:	この表のタスク 1 を参照
		ディレクトリ・サーバーの管理パスワード :	この表のタスク 1 を参照
		ディレクトリ・サーバーと Identity Server 間のセキュリティ・モード :	この表のタスク 1 を参照
		構成データがユーザー・データのディレクトリ・サーバーに格納されるかどうか	この表のタスク 1 を参照
		構成 DN:	
		ユーザー・データを格納するディレクトリ検索ベース :	
	3.2	Person オブジェクト・クラス :	
		Person オブジェクト・クラスを自動構成するかどうか ■ ○ ■ ×	
		Group オブジェクト・クラス :	
		Group オブジェクト・クラスを自動構成するかどうか ■ ○ ■ ×	
		Person オブジェクト・クラスの構成（手動プロセスはオプション）	
		Person オブジェクト・クラスを自動構成しないと選択した場合は、次の属性を構成する :	
		ユーザーのフルネーム属性 :	
		ユーザーのログイン ID 属性 :	
		パスワード属性 :	
	3.3	Group オブジェクト・クラスの構成（手動プロセスはオプション）	
		Group オブジェクト・クラスを自動構成しないと選択した場合は、次の属性を構成する :	
		グループ名属性 :	
	3.4	マスター管理者を定義する準備	
		マスター管理者（1 名または複数）:	

表 2-3 インストール準備のチェックリスト（続き）

タスク	サブタスク	チェックリスト : Oracle Access Manager のインストールおよび設定の準備	参照
4 ～ 8		**アクセス・システムのインストールおよび設定の準備**	
4		**Policy Manager をインストールする準備** 次を決定する :	
	4.1	第 5 章「WebPass のインストール」で説明されているように、この Policy Manager の WebPass をインストールして、次を実行する。 ■ Policy Manager をインストールするのと同じ Web サーバー・インスタンス、同じディレクトリ・レベルに WebPass がインストールされていることを確認する。 ■ WebPass が特定の Identity Server と連動するように構成されていることを確認する。	
	4.2	デフォルト・ロケール（管理者の言語） 言語 言語パック ID システムと同じ言語パック	この表のタスク 1 を参照
		Web サーバーのユーザー名（UNIX のみ）:	この表のタスク 2 を参照
		Web サーバーのグループ（UNIX のみ）:	この表のタスク 2 を参照
		WebPass のインストール・ディレクトリ :	この表のタスク 2 を参照
	4.3	ディレクトリ・サーバー・タイプ : ■ Sun Directory Server 5.x ■ NDS ■ Active Directory ■ Windows サーバー 2003 上の Active Directory ■ Active Directory アプリケーション・モード ■ IBM Directory Server **注意 :** Data Anywhere（Oracle Virtual Directory Server）は、ユーザー・データのディレクトリ・サーバーでのみ使用でき、Policy Manager と Access Server では使用できません。 ポリシー・データをユーザー・データのディレクトリ・サーバーとは別に格納するかどうか ■ ○ ■ ×	構成およびポリシー・データは、第 10 章「Oracle Virtual Directory を使用した Oracle Access Manager の設定」で説明されているように、ネイティブ・ディレクトリへの格納が必要
	4.4	Policy Manager と Access Server 間のトランスポート・セキュリティ・モード : ■ オープン ■ シンプル ■ 証明書 シンプル・モードのみ グローバル・アクセス・プロトコル・パスフレーズ : 証明書モードのみ 証明書 PEM パスフレーズ : 証明書リクエスト・ファイルのパス（証明書モードのみ）:	2-12 ページの「Oracle Access Manager コンポーネントの通信の保護」を参照。

表 2-3 インストール準備のチェックリスト（続き）

タスク	サブタスク	チェックリスト : Oracle Access Manager のインストールおよび設定の準備	参照
		証明書ファイルのパス（証明書モードのみ）:	
		キー・ファイルのパス（証明書モードのみ）:	
		連鎖ファイルのパス（証明書モードのみ）:	
	4.5	Web サーバーの構成ファイルをアクセス・システムの情報に基づいて自動的に更新するかどうか	
		- ○	
		- ×	
		更新する場合、obj.conf ファイル（Apache の場合は httpd.conf ファイル）を含んでいる Web サーバーの構成ディレクトリの絶対パス :	タスク 2 を参照
5		**Policy Manager を設定する準備**	
		この Policy Manager のインストールに基づいて次を記入 :	
	5.1	ディレクトリ・サーバー・タイプ :	タスク 4 を参照
		ディレクトリ・サーバーのホスト・マシンの名前または IP アドレス :	タスク 4 を参照
		ディレクトリ・サーバーのポート番号 :	タスク 4 を参照
		ディレクトリ・サーバーのバインド DN:	タスク 4 を参照
		ディレクトリ・サーバーの管理パスワード :	タスク 4 を参照
		ディレクトリ・サーバーと Policy Manager 間のセキュリティ・モード :	
		- オープン	
		- SSL	
		SSL の場合、SSL 証明書へのパス :	
		ディレクトリ・サーバー内の構成データの場所 :	
		- ユーザー・データ・ディレクトリ・サーバー	
		- 個別のディレクトリ・サーバー	
		個別のディレクトリ・サーバー上の場合、ディレクトリ・サーバーのホスト・マシンの名前または IP アドレス :	
		個別のディレクトリ・サーバー上の場合、ディレクトリ・サーバーのポート番号 :	
		個別のディレクトリ・サーバー上の場合、ディレクトリ・サーバーのバインド DN:	
		個別のディレクトリ・サーバー上の場合、ディレクトリ・サーバーの管理パスワード :	
		個別のディレクトリ・サーバー上の場合、ディレクトリ・サーバーと Policy Manager 間のセキュリティ・モード :	
		- オープン	
		- SSL	
		SSL の場合、SSL 証明書へのパス :	

表 2-3 インストール準備のチェックリスト（続き）

タスク	サブタスク	チェックリスト : Oracle Access Manager のインストールおよび設定の準備	参照
		ディレクトリ・サーバー内のポリシー・データの場所 :	
		- ユーザー・データ・ディレクトリ・サーバー	
		- 構成データ・ディレクトリ・サーバー	
		- 個別のディレクトリ・サーバー	
		個別のディレクトリ・サーバー上の場合、ディレクトリ・サーバーのホスト・マシン :	
		個別のディレクトリ・サーバー上の場合、ディレクトリ・サーバーのポート番号 :	
		個別のディレクトリ・サーバー上の場合、ディレクトリ・サーバーのバインド DN:	
		個別のディレクトリ・サーバー上の場合、ディレクトリ・サーバーの管理パスワード :	
		個別のディレクトリ・サーバー上の場合、ディレクトリ・サーバーと Policy Manager 間のセキュリティ・モード :	
		- オープン	
		- SSL	
		SSL の場合、SSL 証明書へのパス :	
		ユーザー・データを格納するディレクトリ検索ベース :	タスク 3 を参照
		構成 DN:	タスク 3 を参照
		ポリシー・ベース :	
		Person オブジェクト・クラス名 :	タスク 3 を参照
		Policy Manager のポリシー・ドメイン・ルート :	
5.2		認証スキームを構成するかどうか	
		- ○	
		- ×	
		構成する場合、1 つ以上の認証スキームを選択 :	
		Oracle Access Manager 関連の認証スキームおよびポリシー・ドメインの構成	
		認証スキーム	
		- Basic Over LDAP	
		- クライアント証明書	
		- 匿名	
		- Oracle Access and Identity	
		- Oracle Access and Identity	
		（AD Forest 用）	
		ポリシー・ドメイン	
		- Identity ドメイン	
		- Access ドメイン	

表 2-3 インストール準備のチェックリスト（続き）

タスク	サブタスク	チェックリスト : Oracle Access Manager のインストールおよび設定の準備	参照
		Oracle Access Manager 関連の URL を保護するポリシーを構成するかどうか	
		- ○	
		- ×	
6		**アクセス・システム・コンソールで Access Server インスタンスを作成する準備**	
		続行する前に次を決定する :	
	6.1	Access Server 名（スペースは使用不可）:	
		Access Server のホスト名 :	
		Access Server がリスニングするポート番号 :	
		Access Server と WebGate 間のトランスポート・セキュリティ・モード :	2-12 ページの「Oracle Access Manager コンポーネントの通信の保護」を参照
		- オープン	
		- シンプル	
		- 証明書	
	6.2	アクセス・システム・コンソールでの Access Server インスタンスの作成	8-5 ページの「システム・コンソールでの Access Server インスタンスの作成」を参照
7		**Access Server をインストールする準備**	
	7.1	デフォルト・ロケール（管理者の言語）	
		言語	
		言語パック	
		Policy Manager と同じ言語パック	
		Web サーバーのユーザー名（UNIX のみ）:	
		Web サーバーのグループ（UNIX のみ）:	
		Access Server のインストール・ディレクトリ :	
	7.2	Access Server と WebGate/AccessGate 間のトランスポート・セキュリティ・モード :	タスク 6 を参照
	7.3	構成データ・ディレクトリ・サーバーと Access Server 間のセキュリティ・モード :	
		- オープン	
		- SSL	
		- 構成データ・ディレクトリ・サーバーのホスト・マシン :	
		Policy Manager の DS と同じかどうか	
		-- ○	
		-- ×	
		構成データ・ディレクトリ・サーバーのポート番号 :	
		Policy Manager の DS と同じかどうか	
		-- ○	
		-- ×	

表 2-3 インストール準備のチェックリスト（続き）

タスク	サブタスク	チェックリスト : Oracle Access Manager のインストールおよび設定の準備	参照
		構成データ・ディレクトリ・サーバーのバインド DN:	
		Policy Manager の DS と同じかどうか	
		-- ○	
		-- ×	
		構成データ・ディレクトリ・サーバーの管理パスワード :	
		Policy Manager の DS と同じかどうか	
		-- ○	
		-- ×	
		構成データ・ディレクトリ・サーバーのタイプ :	
		- Sun Directory Server 5.x	
		- NDS	
		- Active Directory	
		- Active Directory アプリケーション・モード	
		- IBM Directory Server	
		注意 : Access Server のインストールが Windows プラットフォーム上で行われるたびに、ADSI を使用する Active Directory について指定を求められます。	
		どのディレクトリ・サーバーで構成データを格納するか	タスク 1 を参照
		どのディレクトリ・サーバーでポリシー・データを格納するか	タスク 1 を参照
		Access Server 名 :	タスク 6 を参照
		構成 DN:	タスク 3 を参照
		ポリシー・ベース :	タスク 4 を参照
		シンプル・モードのみ	タスク 4 を参照
		グローバル・アクセス・プロトコル・パスフレーズ :	
		証明書モードのみ	
		証明書 PEM フレーズ :	
		PEM フレーズをパスワード・ファイルに保存するかどうか（シンプルおよび証明書モードのみ）:	
		- ○	
		- ×	
		証明書リクエスト・ファイルのパス（証明書モードのみ）:	
		証明書ファイルのパス（証明書モードのみ）:	
		キー・ファイルのパス（証明書モードのみ）:	
		連鎖ファイルのパス（証明書モードのみ）:	
8		**アクセス・システム・コンソールで WebGate インスタンスを作成する準備** 続行する前に次を決定する :	
	8.1	WebGate 名（スペースは使用不可）:	
		WebGate のホスト名 :	

表 2-3 インストール準備のチェックリスト（続き）

タスク	サブタスク	チェックリスト : Oracle Access Manager のインストールおよび設定の準備	参照
		Web サーバーのポート番号 :	
		WebGate のパスワード / パスワードの確認 :	
		Access Server と WebGate 間のトランスポート・セキュリティ・モード :	タスク 6 を参照
	8.2	アクセス・システム・コンソールでの WebGate インスタンスの定義	9-3 ページの「WebGate インスタンスの作成」を参照
	8.3	WebGate と Access Server の関連付け	9-4 ページの「WebGate および Access Server の関連付け」を参照
9		**WebGate をインストールする準備** 続行する前に次を決定する :	
	9.1	デフォルト・ロケール（管理者の言語）	
		言語	
		言語パック	
		Policy Manager および Access Server と同じ言語パック	
		Web サーバーのユーザー名（UNIX のみ）:	
		Web サーバーのグループ（UNIX のみ）:	
		WebGate のインストール・ディレクトリ（WebPass と同じインストール・ディレクトリを使用可能）:	
	9.2	Access Server と WebGate 間のトランスポート・セキュリティ・モード :	タスク 6 を参照
	9.3	WebGate の ID:	タスク 8 を参照
		WebGate のパスワード :	タスク 8 を参照
		Access Server ID:	タスク 6 を参照
		Access Server のホスト名 :	タスク 6 を参照
		Access Server のポート番号 :	タスク 6 を参照
		シンプル・モードのみ	タスク 6 を参照
		グローバル・アクセス・プロトコル・パスフレーズ :	
		証明書モードのみ	
		証明書 PEM フレーズ :	
		証明書リクエスト・ファイルのパス（証明書モードのみ）:	
		証明書ファイルのパス（証明書モードのみ）:	
		キー・ファイルのパス（証明書モードのみ）:	
		連鎖ファイルのパス（証明書モードのみ）:	
	9.5	Web サーバーの構成ファイルを自動的に更新するかどうか	
		- ○	
		- ×	
		更新する場合、obj.conf ファイル（Apache の場合は httpd.conf ファイル）を含んでいる Web サーバーの構成ディレクトリの絶対パス :	

表 2-3 インストール準備のチェックリスト（続き）

タスク	サブタスク	チェックリスト : Oracle Access Manager のインストールおよび設定の準備	参照
10 ～ 14		**使用するオプション・コンポーネント**	
	10	Oracle Virtual Directory Server（Data Anywhere コンポーネント） - ○ - ×	第 10 章「Oracle Virtual Directory を使用した Oracle Access Manager の設定」を参照
	11	SNMP エージェント（オプション） - ○ - ×	第 11 章「SNMP エージェントのインストール」を参照
	12	データベースの監査コンポーネント - ○ - ×	第 13 章「データベースの監査コンポーネントのインストール概要」を参照
	13	言語パック、個別インストール（オプション） - ○ - ×	第 12 章「言語パックの個別インストール」を参照
	14	ソフトウェア開発キット（SDK）はオプションかどうか - ○ - ×	『Oracle Access Manager 開発者ガイド』を参照

3

マルチ言語環境の概要

この章では、マルチ言語環境で 10*g*（10.1.4.0.1）をインストールする場合に、Oracle Access Manager ホスト・マシンを設定する方法について説明します。次の項目について説明します。

- マルチ言語環境でのインストールの概要
- コマンドライン・ツールの環境変数の設定（オプション）
- 言語パックを使用したインストール
- ディレクトリ構造
- 言語パックの削除

注意： Oracle Access Manager 10*g*（10.1.4.0.1）の動作は、英語のみのインストールでもマルチ言語を含むインストールでも同じです。動作の概要は、『Oracle Access Manager 概要』を参照してください。

マルチ言語環境でのインストールの概要

言語パックを使用せずに Oracle Access Manager をインストールする場合、管理者およびエンド・ユーザー向け製品メッセージの表示に使用される言語は英語のみです。オラクル社提供の言語パックを使用してインストールすると、管理アクティビティのデフォルトとして使用される管理者用の言語を選択できます。管理者のデフォルトに選択する言語（ロケール）およびインストールするその他の言語パックに関係なく、英語は常にインストールされます。

注意： 3-5 ページの「言語パックを使用したインストール」で説明しているように、コンポーネントのインストール中にオラクル社提供の言語パックを 1 つ以上含めることができます。また、第 12 章「言語パックの個別インストール」で説明しているように、コンポーネントをインストールした後で言語パックをインストールすることもできます。

管理情報は、インストールした管理者用の言語のみで表示されます。管理ページが管理者用にサポートされていない言語でリクエストされた場合（ブラウザの設定に基づいて）、そのページの表示には、製品のインストール中に管理者用のデフォルト言語として選択された言語が使用されます。言語の詳細は、『Oracle Access Manager 概要』を参照してください。

静的製品ページ（/identity/oblix/index.html および /access/oblix/index.html）では、Identity Server および Access Server のインストール時にこの場所で選択した管理者用のデフォルト言語が常に使用されます。

エンド・ユーザーに対しては、Oracle Access Manager 10*g*（10.1.4.0.1）は、エラー・メッセージや、タブ、パネルおよび属性の表示名などの静的アプリケーション・データを、インストールされたエンド・ユーザーの言語で表示することが可能です。言語パックをインストールした後、使用するすべての言語を有効にしてから、属性、タブおよびパネルの表示名を入力して、インストールした言語を使用する Oracle Access Manager を構成する必要があります。言語を有効にする詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

英語（AMERICAN）のオペレーティング・システムを実行しているマシンに Oracle Access Manager をインストールする場合、インストールおよび設定のメッセージは英語で表示されます。英語（AMERICAN）以外の対応言語のオペレーティング・システムを実行しているマシンにインストールする場合は、インストール・メッセージはオペレーティング・システムのロケールで表示され、設定メッセージはコンポーネントのインストール中に管理機能のデフォルト・ロケールに選択した言語で表示されます（オラクル社提供の言語パックをインストールしている場合）。

注意： インストール中のマシンが、英語（AMERICAN）以外の言語、アメリカ以外の地域、および ASCII 以外のキャラクタ・セットを指定するオペレーティング・システムで実行している場合は、次に「コマンドライン・ツールの環境変数の設定（オプション）」を確認してください。

コマンドライン・ツールの環境変数の設定（オプション）

デフォルトでは、各マシンのコンソールはオペレーティング・システムのロケールおよびキャラクタ・セットをサポートしています。また、UTF-8 などの他の文字コードをサポートしている場合もあります。

Oracle Access Manager 10*g*（10.1.4.0.1）コンソール・ベースのコマンドライン・ツールでは、英語以外の言語およびアメリカ以外のロケールによるデータ（国際化されたデータ）を処理する場合に使用する言語を決定する様々な環境変数を自動的に検出して使用します。

注意： 言語およびキャラクタ・セットを指定する環境変数が設定されていない場合、Oracle Access Manager コマンドライン・ツールでは、言語に英語（AMERICAN）、地域にアメリカ（AMERICA）およびキャラクタ・セットに ASCII（US7ASCII）を使用します。この場合、Oracle Access Manager コマンドライン・ツールでは、英語以外の言語およびアメリカ以外のロケールによるコマンドライン入力は、適切に処理されない場合があります。

次の環境変数を設定すると、自動検出機能を無効化して、優先する言語を指定できます。

- LANG: サーバーのネイティブ言語、ローカル・カスタム、コード化キャラクタ・セット（サーバーが使用する言語およびキャラクタ・セットで、ロケールとも呼ばれる）の設定に使用できる UNIX システムの環境変数です。LANG を設定すると、Oracle Access Manager コンソール・ベースのコマンドライン・ツールでは、この変数で指定した言語およびキャラクタ・セットが使用されます。
- NLS_LANG: この変数を設定すると、Oracle Access Manager コマンドライン・ツールの自動検出機能が無効化され、Oracle アプリケーション（Oracle Access Manager を含むがこれに限定されない）によって入力および表示されるデータに優先する言語およびキャラクタ・セットが指定されます。
- COREID_NLS_LANG: この変数を設定すると、自動検出機能が無効化され、Oracle Access Manager およびそのコマンドライン・コンソールのみによって入力および表示されるデータに使用する言語および地域が設定されます。

目的のホスト・マシンが、AMERICAN 以外の言語、AMERICA 以外の地域および US7ASCII 以外のキャラクタ・セットを指定するサポート対象のオペレーティング・システムを実行している場合、自動検出機能は Oracle Access Manager コマンドライン・ツールのサーバーのロケールを確認して使用します。ただし、設定時、NLS_LANG は LANG に優先し、COREID_NLS_LANG は NLS_LANG に優先します。

つまり、NLS_LANG および COREID_NLS_LANG は、サーバーのロケールの Oracle Access Manager 自動検出を無効にし、コマンドライン引数として渡されたデータおよびコンソールのキャラクタ・セット・エンコーディングからの同等のデータを、Oracle Access Manager 内で使用される UTF-8 エンコーディングに変換します。これによって、Oracle Database Server などに NLS_LANG を設定でき、また、COREID_NLS_LANG を設定して、同一マシン上でこれらの製品が実行している場合に Oracle Access Manager コマンドライン・インタフェースの適切な操作を有効化できます。

NLS_LANG または COREID_NLS_LANG が指定するキャラクタ・セットは、クライアント・アプリケーションの設定に反映されている必要があります。Oracle Access Manager の場合、クライアント・アプリケーションとはコンソールおよびコマンドライン・ツールで、Oracle Access Manager の構成、ポリシーおよびユーザー・データでディレクトリ・サーバー・スキーマを更新したり、Web サーバーの構成を変更したり、Windows プラットフォーム上の Identity Server および Access Server のサービスを作成したり、Policy Manager に Access Server を登録する操作やその他の操作を実行するためにインストール中に起動されます。管理者はいつでも起動できます。

NLS_LANG および COREID_NLS_LANG は、次の書式（記号を含む）で指定されている 3 つのコンポーネントで構成されています。

```
NLS_LANG = language_territory.charset
COREID_NLS_LANG = language_territory.charset
```

例：

```
NLS_LANG = FRENCH_CANADA.WE8ISO8859P1
COREID_NLS_LANG = JAPANESE_JAPAN.JA16EUC
```

NLS_LANG および COREID_NLS_LANG の各コンポーネントは、グローバリゼーション・サポート機能およびローカライゼーション・サポート機能のサブセットの操作を制御します。

- **language** は、Oracle メッセージ、ソート、曜日名および月名に使用する言語などの表記規則を指定します。対応言語にはそれぞれ、AMERICAN、FRENCH、GERMAN などのように一意の名前が付けられています。言語の引数は、地域およびキャラクタ・セットの引数のデフォルト値を指定します。言語が指定されていない場合は、デフォルト値は AMERICAN になります。
- **_territory** は、日付、通貨、数値などのデフォルトの書式の表記規則を指定します。サポート対象の地域にはそれぞれ、AMERICA、FRANCE、CANADA などのように一意の名前が付けられています。地域が指定されていない場合は、地域の値は言語の値に基づきます。
- **.charset** は、クライアント・アプリケーションが使用するキャラクタ・セット（通常は、ユーザーの端末のキャラクタ・セットまたはオペレーティング・システムのキャラクタ・セットに対応する Oracle のキャラクタ・セット）を指定します。サポート対象のキャラクタ・セットにはそれぞれ、US7ASCII や JA16EUC などのように一意の頭字語が付けられています。各言語には、言語に関連付けられたデフォルトのキャラクタ・セットがあります。

たとえば、データベースのキャラクタ・セットが AL32UTF8、クライアントが Windows オペレーティング・システム上で実行している場合、クライアントのキャラクタ・セットに AL32UTF8 を設定しないでください。NLS_LANG または COREID_NLS_LANG は、クライアントのコード・ページを反映する必要があります。たとえば、英語の Windows クライアント上でコード・ページは 1252 で、適切な設定は、AMERICAN_AMERICA.WE8MSWIN1252 です。

UNIX および Windows のプラットフォーム上では、NLS_LANG および COREID_NLS_LANG は、ローカル環境変数として設定される必要があります。

NLS_LANG の詳細は、『Oracle Database グローバリゼーション・サポート・ガイド』を参照してください。

Windows システム上での NLS_LANG および COREID_NLS_LANG の設定

Windows システムでは、コード体系（キャラクタ・セット）はコード・ページで指定されます。コード・ページは、共通記述システムを共有する特定の言語または言語グループをサポートするために定義されます。オラクル社では、コード・ページとキャラクタ・セットという用語は同義であるとみなします。中国語、日本語、韓国語以外の環境では、Windows の GUI および DOS のコマンド・プロンプトは同じコード・ページを使用しません。

注意： NLS_LANG の詳細は、『Oracle Database グローバリゼーション・サポート・ガイド』を参照してください。

NLS_LANG および COREID_NLS_LANG の設定の手順

1. 「スタート」メニューから、「ファイル名を指定して実行」を選択します。
2. コマンド・ウィンドウで、cmd を入力してから「OK」をクリックします。
3. コマンド・プロンプトで、使用中のシステムに適した環境変数を入力します。次に例を示します。

   ```
   C:¥>set COREID_NLS_LANG = JAPANESE_JAPAN.JA16EUC
   ```

4. 必要に応じて、名前 NLS_LANG を持つエントリを検索して編集します。

UNIX システム上での NLS_LANG および COREID_NLS_LANG の設定

先述のように、Oracle Access Manager 10*g*（10.1.4.0.1）コンソール・ベースのコマンドライン・ツールでは、英語以外の言語およびアメリカ以外のロケールによるデータ（国際化されたデータ）を処理する場合、サーバーのロケールを自動的に検出して使用します。UNIX の LANG 環境変数を設定したり（UNIX ドキュメントを参照）、Oracle の NLS_LANG 環境変数および COREID_NLS_LANG 環境変数を設定すると（この章を参照）、自動検出機能を無効化して、優先する言語を指定できます。

UNIX システムでは、他の環境変数を設定する場合と同じように設定します。メソッドは、bash、csh、sh などのシェルによって異なります。

注意： NLS_LANG の詳細は、『Oracle Database グローバリゼーション・サポート・ガイド』を参照してください。

言語パックを使用したインストール

オラクル社提供の言語パックを使用せずに Oracle Access Manager をインストールすると、エンド・ユーザーおよび管理者用の情報の言語は英語に設定されます。オラクル社提供の言語パックを 1 つ以上使用して Oracle Access Manager をインストールすると、Oracle Access Manager アプリケーションをローカライズし、エラー・メッセージや、タブ、パネルおよび属性の表示名などの静的データを、エンド・ユーザーの言語でエンド・ユーザーに表示できます。

注意： Oracle Access Manager では、中国語や日本語などのマルチバイト言語の UTF-8 エンコーディングをサポートし、また、双方向言語もサポートしています。ユーザーおよび管理者用の情報で使用可能な言語の完全なリストは、『Oracle Access Manager 概要』を参照してください。特定の言語パックに関する情報は、オラクル社にお問い合せください。

言語パックのインストーラは、Oracle Access Manager インストール・メディアで入手できます。オラクル社がサポートする（言語パックを必要としない英語以外の）各言語には、ID システム用に 1 つの言語パック・インストーラ、アクセス・システム用に 1 つの言語パック・インストーラが用意されています。たとえば、Identity Server 上に言語パックをインストールする場合、WebPass 上にも言語パックをインストールする必要があります。アクセス・システムがある場合は、アクセス・システムのインストーラを使用して言語パックをインストールする必要があります。

コンポーネントのインストーラは、サイレント・モードで言語パックのインストーラを呼び出し、同時に言語パックのインストールを実行します。インストールする各コンポーネントには、適切な言語パックを実行する必要があります。たとえば、Identity Server および WebPass インスタンスのインストール時には ID システムの言語パック・インストーラを使用し、Access Server、WebGate および Policy Manager のコンポーネントにはアクセス・システムの言語パック・インストーラを使用します。

後述の概要では、Oracle Access Manager コンポーネントをインストールする場合に言語パックのインストールが必要な手順について説明しています。第 12 章「言語パックの個別インストール」で説明されているように、Oracle Access Manager のインストールおよび設定後に個別に言語パックをインストールすることも選択できます。どちらの場合でも、後述のタスクを完了している必要があります。

Oracle Access Manager とともに言語パックをインストールする準備の手順

1. インストール前に、目的の言語パックのインストーラを、コンポーネントのインストーラと同じ一時ディレクトリに移動します。たとえば、次のようにします。

   Oracle_Access_Manager10_1_4_0_1_FR_Win32_LP_Identity_System.exe
   Oracle_Access_Manager10_1_4_0_1_JA_Win32_LP_Identity_System.exe
   Oracle_Access_Manager10_1_4_0_1_DE_Win32_LP_Identity_System.exe

2. **UNIX:** 各言語パックに実行権限があることを確認した後でメイン・インストーラを起動します。たとえば、次のようにします。

```
chmod +x " Oracle_Access_Manager10_1_4_0_1_FR_sparc-s2_LP_Identity_System"
chmod +x " Oracle_Access_Manager10_1_4_0_1_JA_sparc-s2_LP_Identity_System"
chmod +x " Oracle_Access_Manager10_1_4_0_1_DE_sparc-s2_LP_Identity_System"

chmod +x " Oracle_Access_Manager10_1_4_0_1_FR_sparc-s2_LP_Access_System"
chmod +x " Oracle_Access_Manager10_1_4_0_1_JA_sparc-s2_LP_Access_System"
chmod +x " Oracle_Access_Manager10_1_4_0_1_DE_sparc-s2_LP_Access_System"
```

3. コンポーネントのインストール中、管理者用の言語のデフォルト・ロケールおよびその他のロケールを選択します（検出された言語パックのインストーラに基づいて一覧表示されます）。

4. インストール後、使用するすべての言語を有効にしてから、（属性、タブおよびパネルの表示名をオブジェクト・クラス・レベルで）入力して、インストールした言語を使用する Oracle Access Manager 製品アプリケーションを構成する必要があります。詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

インストール中、次のプロセスが自動的に実行されます。

- 3-7 ページの「言語のディレクトリ」で説明されているように、/langTag フォルダが、インストールされた各言語の Component_install_dir/oblix/lang ディレクトリ内に作成されます。
- インストールされた各言語の言語エントリが、`obid=langTag and configDN` のように、LDAP ディレクトリの構成ノードの下に含まれます（ここで `configDN` はディレクトリの構成 DN です）。
- ¥*Component_install_dir*¥identity | access¥oblix¥config にある obnls.xml 構成ファイルが、インストールされた各言語に対して（次に示すように）更新されます。ドイツ語（de-de）および日本語（js-jp）の言語パックがインストールされています。

```
 <?xml version="1.0" encoding="UTF-8" ?>
- <ParamsCtlg xmlns="http://www.oblix.com" CtlgName="obnls.xml">
- <CompoundList xmlns="http://www.oblix.com" ListName="">
- <SimpleList>
  <NameValPair ParamName="default" Value="en-us" />
  </SimpleList>
- <ValList xmlns="http://www.oblix.com"
ListName="languages">  <ValListMember Value="en-us" />
  <ValListMember Value="de-de" />
  <ValListMember Value="ja-jp" />
  </ValList>
...    </CompoundList>
  </ParamsCtlg>
```

注意： 言語パックを削除する詳細は、2-29 ページの「Oracle Access Manager コンポーネントのアンインストール」を参照してください。言語の問題をトラブルシューティングを行う必要がある場合は、E-17 ページの「言語の問題」を参照してください。

ディレクトリ構造

リリース 6.5 のリリースから、静的情報をユーザーのネイティブ言語でユーザーに表示できる言語パックの追加に対応するため、新しいディレクトリ構造が導入されました。Oracle Access Manager では、Oracle National Language Support Library の自動インストール中、各コンポーネントに ¥oblix¥oracle¥nlstrl という名前の新しいディレクトリが作成されます。

OracleAccessManager¥access

OracleAccessManager¥identity

OracleAccessManager¥webcomponent

Oracle Access Manager が内部的に使用するグローバリゼーション・ファイルは、¥oblix¥Oracle の下の Identity Server のインストール・ディレクトリに格納されます。

注意： OracleAccessManager は、最上位のディレクトリに割り当てられたデフォルト名です。ただし、これはインストール・プロセス時に任意の名前に変更できます。このマニュアルでは、¥OracleAccessManager を含むパス名、および *Component_install_dir*¥ への参照が使用されています。

言語のディレクトリ

Oracle Access Manager のインストールには、¥lang という名前のディレクトリが含まれ、このディレクトリには、インストールされた各言語の名前付きサブディレクトリが含まれます。たとえば、¥lang¥ en-us には、すべてのインストール時に含まれる英語固有のディレクトリおよびファイルが含まれています。

インストールされた各言語パックには、*¥langtag* ディレクトリが作成され、対応する言語タグで名前が付けられます。次の例では、ドイツ語および日本語の言語パックがインストールされ、適切な名前付きディレクトリが自動的に作成されています。

Component_install_dir¥identity¥oblix¥lang¥en-us（常に存在）

Component_install_dir¥identity¥oblix¥lang¥de-de

Component_install_dir¥identity¥oblix¥lang¥ja-jp

など

前述の例では、*Component_install_dir* はメイン・コンポーネントがインストールされているディレクトリを表し、identity|access はインストール時にパスに追加された適切な接尾辞を表します。

注意： オラクル社提供の言語パックがインストールされている場合を除いて、インストールは英語のみです。

各 *¥langTag* ディレクトリには、様々なアプリケーションの .xml メッセージ・カタログ・ファイルが含まれています。他の .html ファイルと同様に、.xml メッセージ・カタログ・ファイルはカスタマイズできます。詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

言語パックの削除

インストールした各言語パックは、コンポーネントのアンインストール・ディレクトリにある適切なファイルを使用して、個別に削除（アンインストール）する必要があります。インストール時に選択されたデフォルトの管理者言語に関連付けられている言語パックは削除（アンインストール）しないでください。

詳細は、第 20 章「Oracle Access Manager の削除」を参照してください。

第 II 部

ID システムのインストールおよび設定

ここでは、ID システムを正常にインストールおよび設定するために必要なすべての情報について説明します。

第 II 部は、次の章で構成されます。

- 第 4 章「Identity Server のインストール」
- 第 5 章「WebPass のインストール」
- 第 6 章「ID システムの設定」

4

Identity Server のインストール

アクセス・システムをインストールする前に、ID システムをインストールする必要があります。Identity Server は、最初にインストールする必要がある Oracle Access Manager コンポーネントです。ここでは、次の項目について説明します。

- Identity Server およびインストールの概要
- Identity Server の前提条件チェックリスト
- Identity Server のインストール
- Oracle Internet Directory のチューニング

以前のリリースを 10*g*（10.1.4.0.1）にアップグレードする方法は、『Oracle Access Manager アップグレード・ガイド』を参照してください。

Identity Server およびインストールの概要

Identity Server は、最初にインストールする必要がある Oracle Access Manager コンポーネントです。Identity Server は、Web ベースのインタフェースによるアプリケーションを提供し、ユーザー、グループおよび組織の識別に関連するすべてのリクエストを処理します。

Identity Server の各インスタンスは、Web サーバーのホスト上にインストールされた WebPass プラグインからのリクエストを受信します。Identity Server の各インスタンスは、ネットワーク接続を介して、LDAP ディレクトリ・サーバーでの読取りおよび書込みを実行します。詳細は、『Oracle Access Manager 概要』を参照してください。

個別のプラットフォーム固有の Identity Server インストール・パッケージが、¥win32 および ¥solaris のサブディレクトリに提供されています。プラットフォームによる相違点は、必要に応じて手順で示されます。次に例を示します。

Windows: ¥Software¥Win32¥OracleAccessManager¥...

Solaris: /Software/Solaris/OracleAccessManager/...

注意： Identity Server のインスタンス名を再利用する場合は、20-6 ページの「Identity Server インスタンス名のリサイクル」を参照してください。

オペレーティング・システムや、GUI モードまたはコンソール・モードのどちらを選択するかに関係なく、インストール・プロセスは同じ順序に従います。

インストール中、選択するトランスポート・セキュリティ・モードは、後の手順で指定する通信詳細の有効範囲に影響を与えます。また、これがディレクトリ・サーバーにインストールされる最初の Identity Server かどうかも指定を求められます。この指定によって、後の手順でのアクティビティの有効範囲が決定されます。通告はすべて確認されますが、使用中の環境に該当しない場合はスキップされることがあります。次に例を示します。

インストール中、情報は様々な時点で保存されます。指定した情報にエラーが検出されると、情報を再指定するか、再度手順を完了するかを選択できます。情報が保存された後は、戻って情報を再指定することはできません。

- **シンプル :** 手順 4 を完了します。
- **証明書 :** 手順 5 に進みます。

ディレクトリ・サーバー詳細を指定すると、2 つの手順が示されます。

- 1 つの手順では、ディレクトリ・サーバーに対して最初の Identity Server をインストールできます。
- もう 1 つの手順では、Windows システム上に追加でインストールされた Identity Server の詳細を指定できます。UNIX システム上に複数の Identity Server をインストールする場合は、追加のディレクトリ・サーバー詳細は必要ありません。

指定する情報に基づいて、Identity Server のデフォルトのディレクトリ・プロファイルが作成されます。第 6 章「ID システムの設定」で説明されているように、このプロファイルは、ID システムを設定した後に使用可能です。

すべての手順を完了する前や、Identity Server をインストール中であると通知された後にインストールを取り消す場合は、2-29 ページの「Oracle Access Manager コンポーネントのアンインストール」で説明されているように、その Identity Server をアンインストールする必要があります。

詳細は、次を参照してください。

- Identity Server および Software Developer Kit
- 複数の Identity Server のインストールの概要
- アップグレードした環境への新規 Identity Server の追加

Identity Server および Software Developer Kit

ID システムの一部の機能では Oracle Access Manager Software Developer Kit（SDK）が必要です。デフォルトでは、SDK は ¥*IdentityServer_install_dir*¥identity の下のサブディレクトリにインストールされます。『Oracle Access Manager ID および共通管理ガイド』で説明されているように、ID システムの設定に続き、ID システム用に手動で SDK を構成して目的の機能を有効化する必要があります。

サポートしている各開発プラットフォーム用の簡単な AccessGate のサーブレットまたはアプリケーションを作成する SDK のインストールの詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。

複数の Identity Server のインストールの概要

複数の Identity Server をインストールし、すべて同じディレクトリ・サーバーに関連付ける場合があります。

タスクの概要 : Identity Server の追加インストール

1. 最初の Identity Server をインストールします。詳細は、この章を参照してください。
2. 第 5 章「WebPass のインストール」で説明されているように、WebPass をインストールします。
3. 第 6 章「ID システムの設定」で説明されているように、最初の Identity Server を ID システムで設定します。
4. 『Oracle Access Manager ID および共通管理ガイド』で説明されているように、新しい Identity Server インスタンスを ID システム・コンソールに追加します。
5. 『Oracle Access Manager ID および共通管理ガイド』で説明されているように、新しい Identity Server インスタンスを WebPass に関連付け、優先順位を「プライマリ」に指定します。
6. 『Oracle Access Manager ID および共通管理ガイド』で説明されているように、WebPass インスタンスを変更し、すべてのプライマリ Identity Server と通信するよう最大接続数を適切な数値に設定します。

   WebPass 構成ファイルの webpass.xml が新規インスタンス情報で確実に更新されるよう、手順 7 に進む前に 1 分以上待機してください。1 分以上待機しない場合、WebPass インスタンスは新しい情報を受信できないことがあり、新規 Identity Server インスタンスに接続できません。
7. インストールされたすべての Identity Server が停止するまで、1 分以上待機してください。
8. 新規 Identity Server をインストールして、このディレクトリ・サーバーに対する最初の Identity Server ではないことを示します。

   スキーマを再更新する必要はありません。
9. 6-13 ページの「他の Identity Server インスタンスの設定」で説明されているように、新規 Identity Server を設定します。
10. 『Oracle Access Manager デプロイメント・ガイド』で説明されているように、Identity Server をフェイルオーバー・サーバーとして構成します。

アップグレードした環境への新規 Identity Server の追加

10*g*（10.1.4.0.1）から、Identity Server は UTF-8 エンコーディングを使用し、プラグイン・データには UTF-8 データが含まれます。以前のプラグインは、Latin-1 エンコーディングでデータを送受信します。

以前の Identity Server を 10*g*（10.1.4.0.1）にアップグレードする場合、アップグレードされた Identity Server と以前の ID イベント・プラグインの間の下位互換性は自動です。この場合、以前のプラグインとの下位互換性を確保するため、新規フラグ（encoding）が oblixpppcatalog.lst ファイルに自動的に追加されます。下位互換性のある Identity Server は、以前のプラグインに Latin-1 エンコーディングでのデータの送信を継続します。この書式は、次のとおりです。

```
actionName;exectype;netpointparam1,...;path;execparam,...;apiVersion;encoding;
```

アップグレードした環境に新規 10*g*（10.1.4.0.1）Identity Server を追加する場合は、Identity Server の oblixpppcatalog.lst で encoding フラグを手動で設定して、Latin-1 データに対して下位互換性を必要とする以前のプラグインおよびインタフェースとの通信を有効化する必要があります。Latin-1 データとの下位互換性には、Latin-1 にエンコーディング・フラグを設定する必要があります。前述のように、このフラグは、イベント・ハンドラで使用するイベント API のバージョンを指定する ApiVersion フラグの次にくる必要があります。ApiVersion パラメータが preNP60 に設定されると、Latin-1 エンコーディングがデフォルトであると想定されます。ApiVersion フラグを設定しない場合は、ApiVersion には値がないことを示すために、Latin-1 フラグの前にセミコロンを追加する必要があります。次の手順の例を参照して、実行内容を確認してください。

アップグレードした環境への新規 Identity Server の追加の手順

1. 『Oracle Access Manager アップグレード・ガイド』で説明されているように、環境をアップグレードします。
2. 4-3 ページの「複数の Identity Server のインストールの概要」のアクティビティを実行します。
3. *IdentityServer_install_dir*¥identity¥oblix¥apps¥common¥bin¥oblixpppcatalog.lst. にある新規 Identity Server の oblixpppcatalog.lst ファイルを検索して開きます。
4. ApiVersion フラグ（存在する場合）の後でエンコーディングを Latin-1 に設定して、Latin-1 データに対する下位互換性を確立します。たとえば、次のようにします。

   設定前 :

   ```
   userservcenter_view_pre;lib;;..¥..¥..¥unsupported¥ppp¥ppp_dll¥
   ppp_dll.dll;Publisher_USC_PreProcessingTest_PPP_Automation;
   ```

   設定後 :

   ```
   userservcenter_view_pre;lib;;..¥..¥..¥unsupported¥ppp¥ppp_dll¥
   ppp_dll.dll;Publisher_USC_PreProcessingTest_PPP_Automation;;Latin-1
   ```

5. 必要に応じて、このファイルのエントリに対して同じ処理を繰り返します。
6. ファイルを保存します。
7. Identity Server サービスを再起動します。
8. 下位互換性が必要であるかぎり、アップグレードした環境で新規 Identity Server ごとに繰り返します。

注意 : すべてのプラグインおよびカスタマイズが正常にアップグレードされ、下位互換性が不要になった場合、すべての Identity Server の oblixpppcatalog.lst ファイルで encoding フラグを手動でリセットすることをお薦めします。

Identity Server の前提条件チェックリスト

Identity Server のインストールを開始する前に、表 4-1 のタスクをタスクを完了していることを確認してください。前提条件が満たされていないと、Oracle Access Manager のインストールに悪影響が生じる場合があります。

表 4-1 Identity Server インストールの前提条件チェックリスト

チェックリスト	Identity Server インストールの前提条件
	第 I 部「インストールの計画と前提条件」で説明されている、ユーザーの環境に適用される前提条件および要件がすべて満たされていることを確認する。

Identity Server のインストール

Identity Server をインストールする際、記入済のインストール準備ワークシートを参照します。インストール・タスクは、次の手順にわかれています。

タスクの概要 : Identity Server のインストール

1. 4-5 ページの「インストールの開始」で説明されているように、インストールを開始します。
2. 4-6 ページの「Identity Server のインストール」に進みます。
3. 4-7 ページの「トランスポート・セキュリティ・モードの指定」に進みます。
4. 4-8 ページの「Identity Server の構成詳細の指定」で説明されているように、Identity Server を識別します。
5. 4-9 ページの「通信詳細の定義」で説明されているように、通信詳細を定義します。
6. 4-10 ページの「ディレクトリ・サーバー詳細の定義」で説明されているように、ディレクトリ・サーバー詳細を定義します。
7. 4-14 ページの「Identity Server インストールの終了」を実行して終了します。

インストールの開始

インストーラは、GUI モードまたはコンソール・モードで起動できます。詳細は、次を参照してください。

- GUI モードでのインストールの開始の手順
- コンソール・モードでのインストールの開始の手順

ユーザーのプラットフォームに関係なく手順は類似しているため、プログラムの起動後に一連の手順が提供されます。

注意 : 実行するインストールに該当しない詳細はスキップしてください。Microsoft Active Directory にインストールする場合は、続行する前に、A-1 ページの付録 A「Active Directory に対する Oracle Access Manager のインストール」を参照してください。

GUI モードでのインストールの開始の手順

1. 管理者権限を持つユーザーとしてログインします。
2. インストール・メディアから、Oracle Access Manager パッケージを一時ディレクトリにコピーし、そこからコンポーネントと言語パックを同時にインストールできます。
3. Identity Server インストーラ（インストールする ID システム言語パックを含む）を検索して起動します。

   例 :

   Windows の GUI メソッド :
   Oracle_Access_Manager10_1_4_0_1_Win32_Identity_Server.exe

   「ようこそ」画面が表示されます。
4. 「次へ」をクリックして、「ようこそ」画面を閉じてから、4-6 ページの「Identity Server のインストール」で説明されているように続行します。

警告 : InstallShield に関連する問題のため、$ または他の特殊な文字列を含むパスワードは、正しく解釈されない場合があります。詳細は、1-10 ページの「GUI メソッド」を参照してください。

コンソール・モードでのインストールの開始の手順

1. 管理者権限を持つユーザーとしてログインします。
2. インストール・メディアから、Oracle Access Manager パッケージ一時ディレクトリにコピーし、そこからコンポーネントと言語パックをインストールできます。
3. Identity Server インストーラ（インストールする ID システム言語パックを含む）を検索して起動します。

   例 :

   Solaris のコンソール・メソッド :
   ./ Oracle_Access_Manager10_1_4_0_1_sparc-s2_Identity_Server

   「ようこそ」画面が表示されます。
4. 「次へ」をクリックして、「ようこそ」画面を閉じてから、「Identity Server のインストール」で説明されているように次に進みます。

Identity Server のインストール

ここでは、Identity Server のインストール・ディレクトリを指定する必要があります。Identity Server インストール・パッケージと同じディレクトリに言語パックがある場合、言語を選択するよう求められます。

Identity Server のインストールの手順

1. プラットフォームに基づいて管理者権限に関する質問に応答します。たとえば、次のようにします。

   - **Windows:** 管理者権限でログインしている場合は、「次へ」をクリックします（管理者権限でログインしていない場合は、「取消」をクリックして、管理者権限を持つユーザーとしてログインしてからインストールを再開します）。
   - **UNIX:** Identity Server が使用するユーザー名およびグループを指定してから、「次へ」をクリックします。通常、デフォルトは nobody です。

     HP-UX では、デフォルトは WWW（ユーザー名）および others（グループ）です。

   Identity Server のインストール・ディレクトリを指定するよう求められます。ディレクトリを指定して「次へ」をクリックすると、インストールが開始され、戻って名前を再指定することはできません。

2. 「次へ」をクリックしてデフォルトのディレクトリを受け入れます（またはインストール先を変更してから「次へ」をクリックします）。たとえば、次のようにします。

   ¥OracleAccessManager

   インストールするロケール（ベース言語）および他のロケール（言語）を選択するには、手順 3 を完了します。それ以外の場合は、手順 4 にスキップします。

3. **言語パック :** インストールする管理者の言語および他のロケールに使用するデフォルト・ロケールを選択してから、「次へ」をクリックします。次に例を示します。

   英語
   フランス語
   アラビア語

   サマリーでは、インストール・ディレクトリおよび必要なディスク領域を識別し、後で参照できるように情報をメモするようユーザーに指示します。

4. まだメモしていない場合、準備ワークシートにインストール・ディレクトリ名を記入してから、「次へ」をクリックして続行します。

   Identity Server がインストールされたという通知があります。通知には数秒かかる場合があります。Windows システムの場合、Microsoft 管理インタフェースが構成されています。

   注意 : Oracle Access Manager コンポーネントまたはファイルの以前のバージョンが検出された場合は、新しいインストール・ディレクトリのパスを指定するか、既存のバージョンをアンインストールする必要があります。

   ここで、トランスポート・セキュリティ・モードを指定するよう求められます。この時点では、戻ってこれまでの詳細を再指定することはできません。

トランスポート・セキュリティ・モードの指定

すべての ID システムのコンポーネント（Identity Server インスタンスおよび WebPass インスタンス）間のトランスポート・セキュリティは一致している必要があります（すべてオープン、シンプルまたは証明書モード）。詳細は、2-12 ページの「Oracle Access Manager コンポーネントの通信の保護」を参照してください。

トランスポート・セキュリティ・モードの指定の手順

1. Identity Server とそのクライアントの間で使用するモードを、「オープン」、「シンプル」または「証明書」から選択します。

   「シンプル」または「証明書」のいずれかを選択した場合、後で詳細を指定します。

2. 「次へ」をクリックします。

   ここで、Identity Server の構成詳細を指定します。

Identity Server の構成詳細の指定

ID システム・コンソールに表示される一意の名前を入力して、Identity Server を識別するよう求められます。指定する名前は、使用中の LDAP ディレクトリ・サーバーの同一インスタンスにアクセスするその他の Identity Server とは別の名前にする必要があります。また、指定する名前に空白を含めることはできません。この名前は、Identity Server の Windows サービス名として使用できます。

また、Identity Server がインストールされる DNS のホスト名、およびこの Identity Server が WebPass（および拡大解釈では Web サーバー）と通信するポート番号を識別するよう求められます。

Identity Server について指定した後、これがディレクトリ・サーバーにインストールされる最初の Identity Server かどうかの指定を求められます。この回答によって、現時点および WebPass インストール後の設定プロセス中のアクティビティの有効範囲が決定します。「はい」を選択した場合、これが最初の Identity Server であることを示し、ディレクトリ・サーバー通信、スキーマ更新およびディレクトリ・サーバー構成詳細について指定を求められます。

- 「はい」を選択した場合、これが最初の Identity Server であることを示します。ユーザーは、ディレクトリ・サーバー通信、スキーマ更新およびディレクトリ・サーバー構成詳細について指定を求められます。
- 「いいえ」を選択した場合、このディレクトリ・サーバーにはすでに Identity Server が設定されていることを示します。ユーザーは、ディレクトリ・サーバー通信についてのみ指定を求められます。
- Windows システムの場合、Active Directory 詳細についても指定を求められます。

この Identity Server の識別の手順

1. 前述のガイドラインに従い、この Identity Server の一意の名前を入力します。たとえば、次のようにします。

   IdentityServer_1014_6025

2. Identity Server がインストールされる DNS のホスト名を入力します。たとえば、次のようにします。

   DNS_hostname.domain.com

3. この Identity Server がクライアントと通信するポート番号を入力してから、「次へ」をクリックします。たとえば、次のようにします。

   6025

4. これがディレクトリ・サーバーに対してインストールされる最初の Identity Server かどうかについて指定を求められた場合は回答し、その後「次へ」をクリックします。

   たとえば、最初の Identity Server のみをインストールしている場合は、次を選択します。

   はい

最初の Identity Server かどうかについての質問に対する回答に関係なく、ここで、ディレクトリ・サーバーおよび以前に選択したトランスポート・セキュリティ・モードの通信詳細を指定するよう求められます。

通信詳細の定義

ここでは、Identity Server とディレクトリ・サーバー間の通信の保護について指定を求められます。『Oracle Access Manager ID および共通管理ガイド』で説明されているように、このインストール中に「いいえ」と回答して、後でディレクトリへの SSL 接続を設定できます。また、以前に指定した情報に基づいて、Oracle Access Manager トランスポート・セキュリティ詳細を指定するよう求められます。

UNIX システム : Identity Server の「オープン」トランスポート・セキュリティまたは「シンプル」トランスポート・セキュリティのいずれかを使用して UNIX システム上にインストールし、これが最初の Identity Server ではない場合、セキュリティ・オプションはほとんどなく、ディレクトリ・サーバー詳細は必要ありません。この場合は、必要に応じて次の手順を完了してから、4-14 ページの「Identity Server インストールの終了」にスキップします。

通信詳細の定義の手順

1. 証明書があり、Identity Server とディレクトリ・サーバー間の SSL を有効化する場合は、適切なオプションの横のボックスを選択してから、「次へ」をクリックします。次に例を示します。

   ディレクトリ・サーバー ... ユーザー・データは SSL 内に存在

   ディレクトリ・サーバー ... 構成データは SSL 内に存在

   注意 : 証明書があり、オプションの SSL を有効化する場合は、各オプションの横にチェック・マークが付いていることを確認してください。

2. **SSL:** ルート CA 証明書へのパスを指定し、「次へ」をクリックします。

   Active Directory Forest 上にインストールしている場合は、取得した CA 証明書のディレクトリおよびファイル名を入力します。詳細は、付録 A「Active Directory に対する Oracle Access Manager のインストール」を参照してください。

3. 以前に選択したモードに従って、「トランスポート・セキュリティ」ダイアログを完了します。たとえば、次のようにします。

   - **オープン :** UNIX システム上にインストールしており、これが最初の Identity Server ではない場合を除いて、4-10 ページの「ディレクトリ・サーバー詳細の定義」にスキップします。UNIX システム上にインストールしており、これが最初の Identity Server ではない場合は、4-14 ページの「Identity Server インストールの終了」にスキップします。
   - **シンプル :** 手順 4 を完了します。
   - **証明書 :** 手順 5 に進みます。

4. **シンプル :** 「パスフレーズ」を入力して確認し、Identity Server と WebPass 間を認証してから、「次へ」をクリックして次のように進みます。

   - これが最初の Identity Server の場合、または Windows システム上に Identity Server を追加インストールしている場合は、4-10 ページの「ディレクトリ・サーバー詳細の定義」にスキップします。
   - UNIX システム上に Identity Server をインストールしており、これが最初の Identity Server ではない場合、4-14 ページの「Identity Server インストールの終了」にスキップします。

5. **証明書 :** 証明書をリクエストまたはインストールしていることを示してから、「次へ」をクリックして続行します。

6. **証明書 :** 「パスフレーズ」を入力して確認し、Identity Server と WebPass 間を認証してから、「次へ」をクリックします。

   - 証明書をインストールする場合は、手順 10 にスキップします。
   - 証明書をリクエストする場合は、手順 7 にスキップします。

7. **証明書のリクエスト :** リクエストされた情報を入力してから、「次へ」をクリックし、CA へ証明書のリクエストを発行します。次に例を示します。
8. **証明書のリクエスト :** 証明書ファイルの場所が表示されている場合は記録します。
9. **証明書のリクエスト :** 証明書が使用可能な場合は、「はい」をクリックして手順 10 に進みます（証明書が使用不可の場合は、「いいえ」をクリックして 4-10 ページの「ディレクトリ・サーバー詳細の定義」にスキップします）。

   「いいえ」を選択した場合は、指示が与えられます。

   注意 : インストールの完了のために、証明書が手元にある必要はありません。ただし、証明書が ¥*IdentityServer_install_dir*¥identity¥oblix¥config にコピーされ、Identity Server が再起動されるまで、Identity Server は設定されません。詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

10. **証明書のインストール :** 次の 3 つのファイルへのフルパスを指定してから、「次へ」をクリックします。

    IdentityServer_install_dir¥identity¥oblix¥config

    - 証明書ファイル（ois_cert.pem）。
    - キー・ファイル（ois_key.pem）。このファイルの場所を、インストーラが認識している場合があります。
    - 連鎖ファイル（ois_chain.pem）。

    注意 : 下位 CA によって生成された証明書を使用している場合、ルート CA の証明書は下位 CA 証明書とともに、xxx_chain.pem に存在する必要があります。検証を適切に行い、ID システムを正常に設定するためには、両方の証明書が存在する必要があります。

    提供した情報は保存され、スキーマを更新するかどうかの指定を求められます。戻って詳細を再指定することはできません。
11. 次に、「ディレクトリ・サーバー詳細の定義」に進みます。

ディレクトリ・サーバー詳細の定義

ここで確認および実行する内容は、これがディレクトリ・サーバーにインストールされる最初の Identity Server かどうかの指定を求められたときの回答にある程度依存します。次の項目を参照し、このインストールに対していずれかを選択します。

- 最初の Identity Server のインストール
- Windows 上での Identity Server の追加インストール

注意 : UNIX システム上に Identity Server をインストールしており、これが最初の Identity Server ではない場合、4-14 ページの「Identity Server インストールの終了」にスキップします。

最初の Identity Server のインストール

これがディレクトリ・サーバーにインストールされている最初の Identity Server であることを示した場合、Oracle Access Manager スキーマでディレクトリ・サーバーを更新するかどうかの指定を求められます。スキーマには、Oracle Access Manager 固有のワークフロー定義、属性ポリシー、タブおよびパネルの構成、構成属性などが含まれます。

スキーマ拡張 : 最初の Idetity Server のインストール中にスキーマを自動的に拡張することをお薦めします。スキーマは 1 回のみ更新します。「はい」を選択すると、ディレクトリ・サーバー・タイプおよび仕様について質問されます。

Windows システム上で「いいえ」を選択すると、Active Directory について質問されます。UNIX システム上で「いいえ」を選択すると、インストールが完了します。

個別のデータ記憶域 : 構成データとは別にユーザー・データを格納する場合、詳細は、2-22 ページの「データ記憶域の要件」を参照してください。

デフォルトでは、構成データおよびユーザー・データは同一のディレクトリ・サーバー上にあるとみなされます。Sun ディレクトリ・サーバーなどの特定のディレクトリ・サーバーでは、データは、同一のディレクトリ・サーバー上に一緒に格納される場合も、同じタイプの異なるディレクトリ・サーバー上に格納される場合もあります。

注意 : Siemens DirX ディレクトリは、10*g*（10.1.4.0.1）ではサポートされていません。ただし、インストール画面では、可能なオプションとして DirX が表示される場合があります。

最初の Identity Server のディレクトリ・サーバー詳細の定義の手順

1. ユーザーの環境を説明するオプションを選択します。たとえば、次のようにします。

   構成データはユーザー・データ・ディレクトリ内に存在

2. ユーザーの環境の適切なスキーマ更新オプションを選択してから、「次へ」をクリックします。たとえば、次のようにします。

   はい

   - 「はい」の場合、手順 3 に進みます。
   - 「いいえ」の場合で、Windows システム上にインストールしている場合は、4-13 ページの「Windows 上での Identity Server の追加インストール」にスキップします。
   - 「いいえ」の場合で、UNIX システム上にインストールしている場合は、4-14 ページの「Identity Server インストールの終了」にスキップします。

3. 自動構成に対してディレクトリ・サーバー・タイプを選択し、「次へ」をクリックします。たとえば、次のようにします。

   Sun

   ここで、ディレクトリ・サーバー構成詳細の指定を求められます。Windows2003 の Active Directory を選択した場合は、動的補助クラスのサポートについて指定を求められます。

4. ディレクトリ・サーバー構成詳細を指定してから、「次へ」をクリックします。たとえば、次のようにします。

   - **ホスト名 :** ディレクトリ・サーバー・マシンの DNS のホスト名
   - **ポート番号 :** ディレクトリ・サーバーがリスニングするポート番号（SSL 接続の場合、暗号化ポートを指定）
   - **バインド DN:** ユーザー・データのディレクトリ・サーバーに対して指定

注意 : バインド DN として入力する識別名には、ユーザーおよびディレクトリ情報ツリー（DIT）の構成ブランチに対する完全な権限がある必要があります。Oracle Access Manager は、このアカウントでディレクトリ・サーバーにアクセスします。例は、表 4-2 を参照してください。ディレクトリ・サーバーの構成は異なる場合があります。

表 4-2 様々なディレクトリ・サーバーのバインド DN

ディレクトリ・サーバー	バインド DN
Active Directory または Windows サーバー 2003 上の Active Directory	cn=administrator,cn=users,<domain DN> **注意 :** この情報は、暗黙的バインドで ADSI を使用している場合でも必要です。詳細は、付録 A「Active Directory に対する Oracle Access Manager のインストール」および『Oracle Access Manager ID および共通管理ガイド』を参照してください。
ADAM	cn=*administrator,o=domain.com* 次を示す値 : Windows セキュリティ・プリンシパル・ユーザー名 ADAM がインストールされているマシンのドメイン名 **注意 :** マスター管理者は、Windows セキュリティ・プリンシパルではなく、管理者権限を持つ ADAM ユーザーである必要があります。詳細は、付録 B「ADAM に対する Oracle Access Manager のインストール」を参照してください。
Data Anywhere（Oracle Virtual Directory）	cn=*admin*
IBM Directory Server	cn=*root*
NDS	cn=*admin*,o=nds
Oracle Internet Directory	cn=*orcladmin* **注意 :** ID システムの設定中に Person オブジェクト・クラスを変更する場合を除いて、これがデフォルトです。
Sun Directory Server	cn=*administrator* **注意 :** cn=Directory Manager を使用しないようにしてください。詳細は、2-18 ページの「ディレクトリ・サーバーの要件の実現」を参照してください。

- パスワード : ユーザー・データのディレクトリ・サーバーのバインド DN のパスワード

5. 「次へ」をクリックして、次のように進みます。

   - Active Directory 2003 の場合 :（ユーザー・データの）ADSI について指定を求められます。
   - 構成データが個別の場合 : 手順 4 を繰り返して、構成データ・ディレクトリの詳細を指定します。必要に応じて、SSL 手順がこのディレクトリに対して繰り返されます。

   スキーマが更新されなかった場合、再度手順を実行して、情報を再指定するオプションが提供されます。このオプションを利用しない場合は、LDAP SDK に同梱されている ldapmodify ユーティリティ、または次のファイルを使用して、スキーマを手動で更新する必要があります。

   ¥*IdentityServer_install_dir*¥identity¥oblix¥tools¥ldap_tools¥ds_conf_update.exe

注意： -h オプションを使用すると、すべての ldapmodify オプションが表示されます。--help オプションを使用すると、すべての ds_conf_update オプションが表示されます。どちらのユーティリティも、Identity Server および Policy Manager のインストールで使用できます。

ldapmodify コマンドの例は、1-6 ページの「スキーマおよび属性の自動更新と手動更新」を参照してください。ds_conf_update を使用して、Oracle Access Manager 構成データを持つスキーマを更新する選択をする場合のコマンドは次のとおりです。

```
ds_conf_update -h DS_hostname -p 389 -D cn=administrator,o=my-company -w passwd
 -i C:¥np¥ois¥identity -d 8 -e C:¥errFile.txt -n 3
```

-d オプションおよびディレクトリ・サーバー・タイプの入力の詳細は、15-6 ページの「サイレント・モード・パラメータ」を参照してください。

6. 4-14 ページの「Identity Server インストールの終了」に進みます。

Windows 上での Identity Server の追加インストール

ここでは、Active Directory に関連する情報を指定するよう求められます。この手順は、次の場合にのみ発生します。

- インストール中にこれが最初の Identity Server ではないことを示した場合
- Windows システム上で自動スキーマ更新を選択しなかった場合

注意： 指定に応じて、この手順の有効範囲が決定します。手順が終了した後で、4-14 ページの「Identity Server インストールの終了」にスキップします。

Windows システム上での Active Directory 詳細の指定の手順

1. スキーマを更新するかどうかの指定を求められた場合、「いいえ」をクリックしてから「次へ」をクリックします。
2. ADSI で Active Directory を使用している場合は「はい」（使用していない場合は「いいえ」）をクリックしてから、「次へ」をクリックします。たとえば、次のようにします。

   はい

   「はい」の場合、手順 3 に進みます。「いいえ」の場合は、4-14 ページの「Identity Server インストールの終了」にスキップします。
3. Identity Server をインストールしているマシンが Oracle Access Manager データとは別の Active Directory ドメインにある場合は「はい」（同じドメインの場合は「いいえ」）をクリックしてから、「次へ」をクリックします。たとえば、次のようにします。

   いいえ

   「いいえ」の場合、手順 4 に進みます。「はい」の場合は、4-14 ページの「Identity Server インストールの終了」にスキップします。
4. ディレクトリ・サーバーで暗黙的バインドを使用する場合は「はい」をクリック（使用しない場合は「いいえ」をクリック）してから、「次へ」をクリックします。たとえば、次のようにします。

   はい

Identity Server インストールの終了

Microsoft Windows 上にインストールしている場合のみ、最初の手順を終了します。それ以外の場合は、手順 2 にスキップします。

インストールの終了の手順

1. **Windows:** Windows の「サービス」ウィンドウに Identity Server を識別する一意のサービス名を指定してから、「次へ」をクリックします。

   指定した名前がこのホスト上ですでに Windows サービス名として登録されている場合は、再試行するかどうかの指定を求めれられます。この場合、「はい」を選択してここで一意の名前を指定するか、「いいえ」を選択して *¥IdentityServer_install_dir*¥identity¥oblix¥apps¥common¥bin¥config_ois.exe を使用して手動で名前を指定できます。

   README の情報が表示されます。

2. README の情報をスクロールします。

3. 「次へ」をクリックして、インストール・サマリーを表示します。

   インストール・サマリーは、このインストール中にユーザーが指定した詳細を表示し、インストールの終了時に Identity Server を起動するようユーザーに指示します。

4. 必要に応じて、このインストールの詳細をメモしてから、「次へ」をクリックします。

5. 「終了」をクリックして、手順を完了します。

6. 次のように Identity Server サービスを起動し、Identity Server がインストールされ、適切に動作していることを確認します。

   - **Windows:** 「サービス」ウィンドウを開いてから、Identity Server サービスを検索して起動します。

     デフォルトでは、Identity Server（Oracle Identity Server（OIS））は手動で起動しますが、起動タイプを「自動」に設定できます。詳細は、Microsoft Windows のヘルプを参照してください。

   - **UNIX:** 次のコマンドを実行します。

     /IdentityServer_install_dir/identity/oblix/apps/common/bin/start_ois_server

7. ユーザーの環境に応じて次に進みます。

   - Oracle Internet Directory に Identity Server をインストールした場合は、次に「Oracle Internet Directory のチューニング」のアクティビティを完了します。
   - それ以外の場合は、第 5 章「WebPass のインストール」で説明されているように、最初の WebPass をインストールします。

Oracle Internet Directory のチューニング

Oracle Internet Directory に Oracle Access Manager をインストールした場合は、次の `ldapmodify` コマンドを実行して、Oracle Internet Directory が適切にチューニングされていることを確認する必要があります。

Oracle Access Manager の Oracle Internet Directory のチューニングの手順

1. 次の ldap コマンドを実行します。

```
ldapmodify -D cn=orcladmin -w <adminPsswd> -h <OID_host> -p <OID_port> << eof
dn: cn=dsaconfig, cn=configsets, cn=oracle internet directory
changetype: modify
add:  orclinmemfiltprocess
orclinmemfiltprocess:
(|(obuseraccountcontrol=activated)(!(obuseraccountcontrol=*)))
(|(!(obuseraccountcontrol=*))(obuseraccountcontrol=activated))
eof
```

2. 第 6 章「ID システムの設定」で説明されているように、Oracle Internet Directory に Oracle Access Manager をインストールする場合、ID システムの設定中に追加手順が必要になります。

5

WebPass のインストール

WebPass は、2 番目にインストールする Oracle Access Manager コンポーネントです。この章では、WebPass のインストール方法および Web サーバーを構成して WebPass と連動させる方法について説明します。詳細は、次を参照してください。

- WebPass およびインストールの概要
- WebPass の前提条件チェックリスト
- WebPass のインストール
- Web サーバーの手動構成
- IIS 上の WebPass の権限の検証
- Identity Server との通信の確立
- WebPass のインストールの確認

以前のバージョンを 10*g*（10.1.4.0.1）にアップグレードする方法は、『Oracle Access Manager アップグレード・ガイド』で説明しています。

WebPass およびインストールの概要

『Oracle Access Manager 概要』で説明されているように、WebPass は Web サーバーのプラグインで、Web サーバーと Identity Server 間で情報を受送信します。（2-6 ページの「ID システムのガイドライン」で説明されているように、WebPass は、各 Policy Manager にもインストールする必要があります。）

WebPass のインストールは、Identity Server のインストールと類似した手順であり、いくつかの同じ手順が含まれます。ただし、WebPass はディレクトリ・サーバーと通信しません。そのため、ディレクトリ・サーバー詳細は必要ありません。

WebPass は Web サーバーと通信しません。2-28 ページの「プラットフォームの要件の確認」で説明されているように、必ず使用している Web サーバーおよびプラットフォームに適したパッケージを選択してください。Web サーバー構成は、WebPass のインストール中に自動的に、またはインストール後に手動で更新する必要があります。

重要： WebPass は、Identity Server（Policy Manager）と同じディレクトリに存在することはできません。たとえば、Identity Server が C:¥OracleAccessManager¥ にインストールされている場合、WebPass を C:¥OracleAccessManager¥WebComponent にインストールすることを検討してください。

タスクの概要 : WebPass のインストール

1. 5-3 ページの「WebPass のインストール」で説明されているように、WebPass をインストールし、WebPass の一意の ID（Identity Server の ID とは異なる）を指定します。
2. インストールの該当する手順を完了します。次に例を示します。
   - Web サーバーの手動構成（インストール時に自動的に構成されなかった場合）
   - IIS 上の WebPass の権限の検証
   - WebPass のインストールの確認

選択するインストール方法および使用中のオペレーティング・システムに関係なく、インストール・プロセスは類似しています。特定のオペレーティング・システムおよび Web サーバーの違いは、適宜インストール手順内で通知されます。また、通告はすべて確認されますが、使用中の環境に該当しない場合はスキップされることがあります。

Windows システム上での WebPass のインストール時、Windows サービス名を指定することは求められません。WebPass サービスを開始および停止するのではなく、WebPass の Web サーバーを開始および停止します。

複数の WebPass インスタンスのインストールの概要

複数の WebPass インスタンスをインストールする場合、次の項目に十分注意してください。

- Oracle Access Manager は、各 Web サーバーのインスタンスに対して 1 つの WebPass をサポートします。つまり、各 WebPass インスタンスには、独自の Web サーバーのインスタンスを指定する必要があります。
- すべての WebPass インスタンスは、接続先の Identity Server と同じトランスポート・セキュリティ・モードでインストールする必要があります。
- 第 6 章「ID システムの設定」で説明されているように、Identity Server の設定を実行する前に、1 つ以上の WebPass インスタンスをインストールする必要があります。
- 最初の Identity Sever の設定後に、任意の数の WebPass インスタンスをインストールできます。追加の各 WebPass に対して、ID システム・コンソールで新規インスタンスの情報を追加する必要があります。詳細および指示は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

WebPass の前提条件チェックリスト

WebPass のインストールを開始する前に、表のタスクを完了していることを確認してください。前提条件が満たされていないと、Oracle Access Manager のインストールに悪影響が生じる場合があります。

表 5-1 WebPass のインストールの前提条件チェックリスト

チェックリスト	WebPass のインストールの前提条件
	第 I 部「インストールの計画と前提条件」で説明されている、ユーザーの環境に適用される前提条件および要件がすべて満たされていることを確認する。
	第 4 章「Identity Server のインストール」のアクティビティをすべて完了する。

WebPass のインストール

WebPass をインストールしながら、記入済のインストール準備ワークシートを参照します。ここでの手順は、GUI メソッドおよびコンソール・メソッドで使用できます。手順は類似しているため、プログラムの起動に続いて、1 セットの手順が提供されます。

WebPass をインストールするには、次の手順を完了する必要があります。

タスクの概要 : WebPass のインストール

1. 5-3 ページの「インストールの開始」で説明されているように、インストール・メソッドを選択してプロセスを開始します。
2. 5-4 ページの「トランスポート・セキュリティ・モードの指定」で説明されているように、WebPass のトランスポート・セキュリティ・オプションを選択します。
3. 5-4 ページの「WebPass 構成詳細の指定」で説明されているように、WebPass 構成詳細を特定します。
4. 5-6 ページの「WebPass の Web サーバー構成の更新」で説明されているように、自動 Web サーバー構成の更新を実行します。
5. 5-7 ページの「WebPass のインストールの終了」で説明されているように、プロセスを完了します。

インストールの開始

必ず使用している Web サーバーおよびプラットフォームに適したパッケージを選択してください。

WebPass のインストールの開始の手順

1. 管理者権限を持つユーザーとしてログインします。
2. 作成した一時ディレクトリで WebPass インストーラ（インストールする ID システム言語パックを含む）を検索します。
3. 選択したプラットフォーム、インストール・メソッド、および Web サーバーの WebPass インストーラを起動します。次に例を示します。
   - **GUI メソッド**

     Windows: Oracle_Access_Manager10_1_4_0_1_Win32_*API*_WebPass.exe
   - **コンソール・メソッド**

     Solaris: ./ Oracle_Access_Manager10_1_4_0_1_sparc-s2_*API*_WebPass

     「ようこそ」画面が表示されます。
4. 「次へ」をクリックして、「ようこそ」画面を閉じます。
5. プラットフォームに基づいて管理者権限に関する質問に応答します。次に例を示します。

6. インストール先を選択してから、「次へ」をクリックします。次に例を示します。

   ¥OracleAccessManager¥Webcomponent

7. **言語パック：**インストールする管理者の言語および他のロケールに使用するデフォルト・ロケールを選択してから、「次へ」をクリックします。

   サマリーでは、インストール・ディレクトリおよび必要なディスク領域を識別し、後で参照できるように情報をメモするようユーザーに指示します。

8. 必要に応じてインストール・ディレクトリ名を記録して、「次へ」をクリックして続行します。

   WebPass がインストールされたという通知があり、プロセスのステータスについて引き続き通知されます。通知には数秒かかる場合があります。Windows システムの場合、Microsoft 管理インタフェースも構成されています。

   トランスポート・セキュリティ・モードを指定して WebPass と Identity Server の間で使用するよう求められます。この時点で、戻ってインストール・ディレクトリを再指定することはできません。

トランスポート・セキュリティ・モードの指定

すべての ID システムのコンポーネント（Identity Server インスタンスおよび WebPass インスタンス）間のトランスポート・セキュリティは一致している必要があります（すべてオープン、シンプルまたは証明書モード）。詳細は、2-12 ページの「Oracle Access Manager コンポーネントの通信の保護」を参照してください。

トランスポート・セキュリティ・モードの指定の手順

1. Identity Server に選択したものと同じトランスポート・セキュリティ・モードを WebPass に対して選択します。
2. 「次へ」をクリックします。

   「シンプル」または「証明書」を指定した場合、後で詳細の指定を求められます。ここで、WebPass 構成詳細の指定を求められます。

WebPass 構成詳細の指定

ここで、この WebPass に使用する一意の名前を入力するよう求められます。これは設定後に ID システム・コンソールに表示されます。

各 WebPass には、それぞれを識別する一意の名前を指定する必要があります。指定する WebPass 名に空白を含めることはできません。また WebPass 名は、ID システム・コンソールおよび LDAP ディレクトリ内でこの WebPass を一意に識別できる必要があります。

また、この WebPass が通信する Identity Server の DNS ホスト名およびポート番号を識別するよう求められます。加えて、シンプルまたは証明書モードのいずれかのみを選択した場合に、選択したトランスポート・セキュリティ・モードについての追加情報を求められることがあります。

WebPass 構成詳細の指定の手順

1. 前述のガイドラインに従い、この WebPass の固有の名前を入力します。次に例を示します。

   WebPass_1014_1_72

2. この WebPass が通信する Identity Server の DNS のホスト名を入力します。次に例を示します。

   Identity_DNS_hostname

3. この WebPass が通信する Identity Server のポート番号を入力し、「次へ」をクリックします。次に例を示します。

   Identity_port

4. 以前に選択したトランスポート・セキュリティ・モードに従って、次の操作を実行します。

   - **オープン :** 5-6 ページの「WebPass の Web サーバー構成の更新」にスキップします。
   - **シンプル :**「パスフレーズ」を指定して確認し、Identity Server と WebPass 間を認証してから、「次へ」をクリックして 5-6 ページの「WebPass の Web サーバー構成の更新」に進みます。
   - **証明書 :** 手順 5 に進みます。

5. **証明書 :** 証明書をリクエストまたはインストールしていることを示してから、「次へ」をクリックして続行します。

   - 証明書をリクエストする場合、組織についての情報を入力して「次へ」をクリックし、リクエストを CA に発行して手順 6 に進みます。
   - 証明書をインストールする場合は、手順 8 にスキップします。

6. **証明書のリクエスト :** 表示されている場合、秘密鍵ファイルおよび証明書リクエスト・ファイルの場所を記録し、「次へ」をクリックします。

7. **証明書のリクエスト :** 証明書が使用可能な場合は「はい」（証明書が使用不可の場合は「いいえ」）をクリックして「次へ」をクリックし、手順 8 に進みます。

   証明書が準備されていない場合、インストールを完了します。証明書を受信する場合、これらを ¥*WebPass_install_dir*¥*identity*¥oblix¥config ディレクトリにコピーして、WebPass の Web サーバーを再起動します。

   注意 : IIS Web サーバーの場合、WebPass のインストール後に `net stop iisadmin` および `net start w3svc` を使用して IIS を停止および開始することを検討してください。これは、メタベースが破損しないようにすることに適した方法です。

   ---

8. **証明書のインストール :** リクエスト済ファイルへのフルパスを指定してから、「次へ」をクリックして 5-6 ページの「WebPass の Web サーバー構成の更新」に進みます。

数秒間、WebPass を構成中というで通知があります。情報はすでに保存されており、前の画面に戻って詳細を再指定する必要はありません。

ここで、WebPass の Web サーバー構成を更新するよう求められます。

WebPass の Web サーバー構成の更新

WebPass コンポーネントを使用するには、製品関連の構成情報により WebPass の Web サーバーを構成する必要があります。この更新は自動または手動で実行できます。Web サーバー構成は次のように更新されます。

- Sun Web サーバーの場合、構成の更新には obj.conf および magnus.conf ファイルの更新が含まれます。
- IIS Web サーバーの場合、構成の更新には、ISAPI フィルタの追加および Oracle Access Manager で必要な拡張機能の作成による Web サーバーの直接の更新が含まれます。
- Apache Web サーバーの場合、構成の更新には httpd.conf ファイルの更新が含まれます。

自動的に Web サーバー構成を更新することをお薦めします。ただし、手動による構成指示も含まれています。

Web サーバー構成の自動更新の手順

1. Web サーバーを自動的に更新するには「はい」をクリックしてから、「次へ」をクリックします。たとえば、次のようにします。
   - **ほとんどの Web サーバー :** Web サーバー構成ファイルを含むディレクトリの絶対パスを指定します。
   - **IIS Web サーバー :** プロセスが即時に開始され、プロセスには 1 分以上かかることがあります。

   Web サーバー構成が更新された場合に画面が表示されます。
2. **Sun Web サーバー :** 続行する前に、Web サーバー管理コンソールで変更を適用します。
3. WebPass の Web サーバー・インスタンスを停止し、Identity Server サービスを停止します。
4. Identity Server サービスを開始し、WebPass の Web サーバー・インスタンスを開始します。

   注意 : IIS を使用する場合、WebPass のインストール後に `net stop iisadmin` および `net start w3svc` を使用して Web サーバーを停止および開始するのは、メタベースが破損しないようにすることに適した方法です。
5. 「次へ」をクリックして通知を閉じ、5-7 ページの「WebPass のインストールの終了」に進みます。

   README の情報が表示されます。

Web サーバー構成の手動更新の手順

1. 自動更新を続行するかどうかの指定を求められた場合、「いいえ」をクリックしてから「次へ」をクリックします。

   新規画面とともに README の情報が表示され、Oracle Access Manager の Web サーバーを手動で設定できます。
2. WebPass のインストール画面に戻り、「次へ」をクリックしてインストールを終了します。
3. 5-7 ページの「Web サーバーの手動構成」を完了してください。

WebPass のインストールの終了

README の情報には、ドキュメントおよびオラクル社に関する詳細が記載されています。

WebPass のインストールの終了の手順

1. README の情報を確認します。
2. 「次へ」をクリックしてインストールを完了します。
3. 必要に応じて、次の手順に進みます。
   - Web サーバーの手動構成（WebPass のインストール時に自動的に構成されなかった場合）
   - IIS 上の WebPass の権限の検証
   - Identity Server との通信の確立
   - WebPass のインストールの確認
   - 第 6 章「ID システムの設定」

Web サーバーの手動構成

WebPass のインストール中にインストール・ウィザードで Web サーバー構成を更新しない場合、Identity Server の設定前に手動で更新する必要があります。

注意： 必要な場合にかぎり、手順 1 を完了してオンラインの指示を表示します。

WebPass の Web サーバーの構成の手順

1. Web ブラウザを起動し、必要に応じて次のファイルを開きます。次に例を示します。

   ¥*WebPass_install_dir*¥identity¥oblix¥lang¥langTag¥docs¥config.htm

   ここで、¥*WebPass_install_dir* は、WebPass をインストールしたディレクトリであり、langTag は en-us などの言語です。
2. 画面の表から該当する Web サーバー・インタフェース構成プロトコルを選択します。
3. Web サーバーのタイプに固有の指示にすべて従い、次を実行します。
   - Web サーバーの設定中に変更する必要があるファイルのバックアップ・コピーを作成します。これは、再度 Web サーバーを設定する必要がある場合に使用できます。
   - 設定によっては、新しいブラウザ・ウィンドウが起動されます。または、情報を入力するためにコマンド・ウィンドウを起動する必要があります。このため、元の設定指示に戻ってすべてを実行し、該当する Oracle Access Manager ファイルを Web サーバーが認識できるようにします。

     注意： 誤ってウィンドウを閉じた場合、ブラウザ・ウィンドウで ¥*WebPass_install_dir*¥identity¥oblix¥apps¥common¥docs¥config.htm ファイルを開き、該当するリンクを再度クリックできます。

     ---
4. Web サーバーの更新が終了した場合、環境に該当するタスクを続行します。次に例を示します。
   - IIS 上の WebPass の権限の検証
   - WebPass のインストールの確認

IIS 上の WebPass の権限の検証

WebPass をインストールして Web サーバー構成を更新した場合、WebPass のインストール・ディレクトリに正常に実行するための適切な権限があることを確認する必要があります。

WebPass の IIS Web サーバー構成の検証の手順

1. 次のディレクトリを検索します。

   ¥*WebPass_install_dir*¥identity¥oblix¥apps¥webpass¥bin

2. ¥bin ディレクトリを右クリックして、「プロパティ」を選択します。
3. 「セキュリティ」タブを選択して、読取りおよび書込み権限の許可がユーザー "SERVICE" に付与されていることを確認します。

「シンプル」または「証明書」モードで WebPass が設定された場合の検証の手順

1. 次のディレクトリを検索します。
   ¥*WebPass_install_dir*¥identity¥oblix¥config¥password.xml.
2. password.xml を右クリックして、「プロパティ」を選択します。
3. 「セキュリティ」タブを選択して、読取り権限の許可がユーザーに付与されていることを確認します。

   "IUSR_<machine_name>"

   "IWAM_<machine_name>"

   "NETWORK SERVICE"

   "IIS_WPG"（IIS 6.0 のみ）

Identity Server との通信の確立

インストール後、Web サーバーが次の手順を使用して再起動される場合に、WebPass と Identity System 間の通信を確立する必要があります。

WebPass と Identity Server 間の通信の確立の手順

1. WebPass の Web サーバー・インスタンスを停止します。
2. Identity Server サービスを停止して再起動します。
3. WebPass の Web サーバー・インスタンスを開始します。

WebPass のインストールの確認

次の手順を完了して、WebPass が正しくインストールされていることを確認します。

WebPass のインストールの確認の手順

1. Identity Server および WebPass の Web サーバーが実行されていることを確認します。
2. 次の URL を指定して、ブラウザから ID システム・コンソールに移動します。次に例を示します。

   ```
   http://hostname:port/identity/oblix
   ```

   ここで、*hostname* は Web サーバーをホストするマシン、*port* は WebPass の Web サーバー・インスタンスの HTTP ポート番号をそれぞれ指し、/identity/oblix は ID システム・コンソールに接続します。

   ID システムのランディング・ページが表示されます。

注意： システムが設定されていないため、ID システムのランディング・ページではいずれのリンクも選択しないでください。第 6 章「ID システムの設定」を参照してください。

6

ID システムの設定

Identity Server および WebPass をインストールした後で、ユーザーの環境内で動作するように ID システムを設定および構成する必要があります。

この章では、ID システムを設定して必須属性を構成する方法について説明します。次の項目を参照してください。

- ID システムの設定の概要
- ID システムの設定の考慮点
- ID システムの設定の前提条件チェックリスト
- ID システムの設定
- 属性の手動構成
- 他の Identity Server インスタンスの設定

注意： 設定中は、「次へ」ボタンをクリックするたびに仕様が保存されます。設定を中止して後で設定を再開すると、同じ場所に戻ります。

ID システムの設定の概要

最初の Identity Server および WebPass をインストールした後で、関連付けを完了してシステムを機能させるよう ID システムを設定する必要があります。このプロセスは、Web ブラウザを使用して完了します。

設定プロセス中に、ディレクトリ・サーバーに関する情報を入力し、Oracle Access Manager 固有の情報を使用して、必要な LDAP Person オブジェクト・クラスおよび Group オブジェクト・クラスを構成します。これによって、Identity Server は WebPass と関連付けられ、製品ブランチおよび属性が含まれるようにディレクトリ・サーバー・スキーマが拡張されます。たとえば、ID システムでは、Person オブジェクト・クラスおよび Group オブジェクト・クラスの「フルネーム」、「ログイン」および「パスワード」のセマンティク型への属性の割当てが必要です。詳細は、6-7 ページの「Oracle Access Manager のオブジェクト・クラスの概要」を参照してください。

ID システムのアプリケーションを使用する前に、設定プロセス全体を完了する必要があります。設定中、入力した情報は次のページへ進むときに保存されます。設定プロセスは、いつでも中止および再開できます。この場合は、最後の入力の次の質問から続行します。

一部の情報は、更新されたスキーマに基づいて、設定ページに自動的に表示される場合があります。Identity Server のインストール中にスキーマを自動的に更新しなかった場合は、設定を開始すると、一連のスキーマ変更ページが表示されます。これらのページは見ればわかるので、ここでは説明しません。

ID システムの設定の考慮点

この章で説明する設定プロセスは、特定のディレクトリ・サーバーに接続される最初の Identity Server インスタンスの作成にのみ適用されます。すべて同じディレクトリ・サーバーに関連付けられる、複数の Identity Server をインストールする場合があります。2 番目以降の Identity Server インスタンスの設定プロセスについては、4-3 ページの「複数の Identity Server のインストールの概要」で説明されています。

注意： ID システムの設定を開始する前に、次の重要な考慮点を必ず確認してください。

次に示すのは、ID システムを設定する前に注意する必要がある重要な考慮点です。

下位 CA によって生成された証明書 : ルート CA の証明書は下位 CA 証明書とともに、ois_chain.pem に存在する必要があります。検証を適切に行い、ID システムを正常に設定するためには、両方の証明書が存在する必要があります。

複数のユーザー・データ・ディレクトリ : 複数のユーザー・データ・ディレクトリおよび検索ベースを使用する場合、ID システムの設定中にメインのユーザー・データ・ディレクトリおよび検索ベースを指定します。『Oracle Access Manager ID および共通管理ガイド』で説明されているように、設定の完了後に、非結合ネームスペース用のデータベース・プロファイルを 1 つ以上追加します。

Active Directory: 続行する前に、A-8 ページの「Active Directory に対するインストールと設定の考慮事項」をお読みください。Microsoft Active Directory フォレスト内に Oracle Access Manager をインストールする場合、設定中に次の追加手順が必要です。

- 「動的補助オブジェクト・クラス」機能について指定を求められた場合は、横のボックスを選択して、この機能を有効化します。
- セマンティク型「ログイン」が 1 つの属性に割り当てられており、マスター管理者として選択した人すべてがログイン属性の値を持っていることを確認します。詳細は、6-9 ページの「マスター管理者の構成」および『Oracle Access Manager ID および共通管理ガイド』を参照してください。

ADSI とともに Active Directory を使用している場合は、次のことが必要です。

- A-17 ページの「ADSI の設定（オプション）」で説明されているように、ID システムの設定の前に ADSI の設定手順を完了します。
- 設定中、ディレクトリ・サーバー・タイプを指定するときに「ADSI を有効化」オプションをオンにして、Active Directory とのネイティブ統合を有効化し、暗黙的フェイルオーバーおよびネイティブ・パスワード変更を可能にします。

  これによって、デフォルトのディレクトリ・プロファイルおよび関連付けられたデータベース・エージェントが作成されます。この構成により、デフォルトの ID- マシン名表記規則を使用した名前が、ディレクトリ・プロファイル（データベース・エージェント）に自動的に割り当てられます。この名前を、それぞれのドメイン名を反映するように変更して、ユーザー認証を容易にする必要があります。結果のディレクトリ・プロファイルによって、関連付けられた Identity Server は、暗黙的バインドを使用して Active Directory ツリー内のプライマリ・ドメイン・コントローラですべての操作を実行できます。

Active Directory アプリケーション・モード : 続行する前に、付録 B「ADAM に対する Oracle Access Manager のインストール」をお読みください。

Data Anywhere（Oracle Virtual Directory Server）: Data Anywhere とともに使用するために ID システムを設定する前に、第 10 章「Oracle Virtual Directory を使用した Oracle Access Manager の設定」を読み、指定されているアクティビティを完了してください。

Oracle Internet Directory: 複数のレルムのインストールおよび複数のディレクトリ検索の操作については、『Oracle Access Manager ID および共通管理ガイド』でインストール後の詳細を参照してください。Oracle Access Manager と Oracle Internet Directory 間の完全な相互作用の実現に関する詳細は、この後のタスクの概要を参照してください。

注意 : 4-15 ページの「Oracle Internet Directory のチューニング」で説明されている Oracle Internet Directory のチューニング手順を必ず完了してください。

タスクの概要 : Oracle Access Manager と Oracle Internet Directory 間の完全な相互作用の実現

1. ID システムの設定中に、Oracle Internet Directory によって使用されるユーザー・オブジェクト・クラスおよびグループ・オブジェクト・クラスの指定を求められた場合は、これらのオブジェクト・クラスを指定します。
2. ID システムの設定中に、orclUserV2 オブジェクト・クラスを構成し、この補助オブジェクト・クラスを User Manager の「従業員」タブに関連付けます。これによって、Oracle Internet Directory ユーザー・エントリ内の orclUserV2 属性を、ID システム・コンソールを使用して管理できます。

   次の手順は、ID システムの設定中か、または後で ID システム・コンソールを使用して Oracle Internet Directory 検索ベースを追加することによって、完了できます。
3. ユーザーまたはオブジェクトを作成したアプリケーション（Oracle Access Manager または Oracle Internet Directory）に関係なく、Oracle Access Manager と Oracle Internet Directory の両方が特定の Oracle Internet Directory インスタンス内のすべての新規ユーザーまたはグループを認識できるようにするために、Oracle Internet Directory が使用するユーザーとグループ両方の検索ベースを使用するように ID システムを構成します。
4. Oracle Internet Directory によって管理されるグループ・オブジェクト : 次のように、orclGroup 補助クラスを Oracle Access Manager によって作成されたグループ・オブジェクトにアタッチします。
   - ID システムの設定後、ID システム・コンソールを使用して補助クラス（orclGroup）を手動で構成します。
   - Oracle Access Manager Group Manager インタフェースを使用して、この補助オブジェクト・クラスの新規グループ・タイプを構成します。グループ・タイプの構成の詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

- orclGroup から少なくとも 1 つの属性を、ID システムによってグループ・オブジェクトの作成のために定義されたワークフローに含めます。これにより、Group Manager によって作成されたグループは orclGroup オブジェクト・クラスに属し、Oracle Internet Directory Oracle Delegated Administration Services によって管理できます。

5. Oracle Internet Directory で、以前に Oracle Access Manager によって「検索可能」とマークされたすべての属性を索引付けします。これにより、LDAP フィルタで使用されるすべての属性を、Oracle Internet Directory によって検索できます。

   次のアクティビティを完了して、User Manager、Group Manager および Org. Manager に対して検索可能としてマークされた属性を判別します。

   - ID システム・コンソールで、適切なアプリケーションの構成タブ（「User Manager 構成」など）をクリックします。
   - アプリケーションの構成ページで、「タブ」をクリックし、「既存のタブ」リスト内の名前（「従業員」など）をクリックします。
   - 「タブの表示」ページで、「検索属性の表示」ボタンをクリックします。
   - 前述の手順をすべてのアプリケーション（User Manager、Group Manager および Org. Manager）およびアプリケーション内の既存の各タブについて繰り返します。

6. Oracle Directory Manager または Oracle Internet Directory セルフサービス・コンソールを使用して、EMailAdminsGroup が UMAdminsGroup のメンバーではないことを確認します。これにより、Access Server の失敗の原因になる可能性がある、際限なく繰り返される検索を防ぎながら、ネストされたグループの検索が可能になります。

注意： Oracle Access Manager を Oracle Internet Directory とともに使用する場合、LDAP 参照および継続参照はサポートされません。

ID システムの設定の前提条件チェックリスト

WebGate のインストールを開始する前に、表 6-1 のタスクを完了していることを確認してください。すべての前提条件を満たさない場合、インストールに悪影響を及ぼすことがあります。

表 6-1 ID システムの設定の前提条件チェックリスト

チェックリスト	ID システムの設定の前提条件
	第 I 部「インストールの計画と前提条件」で説明されている、ユーザーの環境に適用される前提条件および要件がすべて満たされていることを確認する。
	第 4 章「Identity Server のインストール」のアクティビティをすべて完了する。
	第 5 章「WebPass のインストール」のアクティビティをすべて完了する。

ID システムの設定

Identity Server の設定を完了する際、記入済のインストール準備ワークシートを参照します。設定プロセスは、わかりやすいように次の手順に分割されています。

タスクの概要 : ID システムの設定

1. 6-5 ページの「設定プロセスの開始」で説明されているように、プロセスを開始します。
2. 6-6 ページの「ディレクトリ・サーバー詳細およびデータの場所の詳細の指定」で説明されているように、ディレクトリ・サーバーおよびデータの場所を指定します。
3. 6-7 ページの「オブジェクト・クラス詳細の指定」で説明されているように、Person オブジェクト・クラスおよび Group オブジェクト・クラスの詳細を定義します。
4. 6-9 ページの「オブジェクト・クラス変更の確認」で説明されているように、オブジェクト・クラスの変更を検証します。
5. 6-9 ページの「マスター管理者の構成」で説明されているように、システム全体を管理する人を指定します。
6. 6-10 ページの「ID システムの設定の完了」で説明されているように、設定を終了します。

設定プロセスの開始

この手順を完了して、ID システムの設定を開始します。

注意 : WebPass のインストールを確認した直後で、「ID システム・コンソール」設定ページが使用可能になっている場合は、手順 2 にスキップします。

設定の開始の手順

1. ユーザーの環境に応じて次の URL を指定して、ブラウザから ID システム・コンソールに移動します。たとえば、次のようにします。

   ```
   http://hostname:port/identity/oblix
   ```

   ここで、*hostname* は WebPass の Web サーバーをホストするマシン、port は WebPass の Web サーバー・インスタンスの HTTP ポート番号をそれぞれ指し、/identity/oblix は ID システム・コンソールに接続します。

2. 「ID システム・コンソール」リンクをクリックします。

   「システム・コンソール」設定ページが表示されます。

3. 「セットアップ」ボタンをクリックします。

   - Identity Server のインストール中にスキーマを更新した場合 : 6-6 ページの「ディレクトリ・サーバー詳細およびデータの場所の詳細の指定」にスキップします。
   - Identity Server のインストール中にスキーマを更新しなかった場合 : スキーマの変更ページが表示され、手順 5 を完了します。詳細情報は、1-6 ページの「スキーマおよび属性の自動更新と手動更新」を参照してください。

4. **スキーマの変更 :** スキーマの変更ページが表示された場合、そこで説明されているアクティビティを完了し、続行します。
5. 次に説明する手順を完了します。詳細は、第 19 章「重要な注意事項」を参照してください。

ディレクトリ・サーバー詳細およびデータの場所の詳細の指定

ユーザー・データおよび構成データが格納されるディレクトリ・サーバーの詳細を指定する必要があります。

注意： Data Anywhere ディレクトリ・サーバー・オプションは、ユーザー・データのディレクトリ・サーバー、および Oracle Virtual Directory Server（VDS）との統合についてのみ使用可能です。Data Anywhere とともに使用する最初の Identity Server を設定する前に、第 10 章「Oracle Virtual Directory を使用した Oracle Access Manager の設定」を読み、指定されているアクティビティを完了してください。

通常、ユーザー・データの詳細が最初に要求され、次に構成データの詳細が要求されます。スキーマ更新中に入力した情報は、通常は設定ページに表示されます。

ユーザー・データと構成データを別々に格納する場合は、ディレクトリ・サーバーの詳細を指定する手順を繰り返します。

ディレクトリ・サーバー詳細の指定の手順

1. ユーザー・データのディレクトリ・サーバーのタイプを指定します。次に例を示します。

   Sun

   次に、ユーザー・データのディレクトリ・サーバーの場所の指定を求められます。インストール中にスキーマを更新した場合、ほとんどの詳細はすでに入力されています。

2. インストールに従ってユーザー・データのディレクトリ・サーバー詳細を指定してから、「次へ」をクリックします。次に例を示します。

   - **ホスト :** ユーザー・データのディレクトリ・サーバーの DNS ホスト名
   - **ポート番号 :** ユーザー・データのディレクトリ・サーバーのポート番号
   - **ルート DN:** ユーザー・データのディレクトリ・サーバーのバインド DN
   - **ルート・パスワード :** バインド DN パスワード
   - **ディレクトリ・サーバー・セキュリティ・モード :** ユーザー・データのディレクトリ・サーバーと Identity Server の間で「非保護」または「SSL 有効」
   - **Oracle データもこのディレクトリに格納しますか :** 「はい」（デフォルト）または「いいえ」

   注意： ユーザー・データが構成データとは別に格納されている場合、同様のページが表示されます。そこで構成データ・ディレクトリの情報を入力します。ただし、その手順についてはここでは省略します。

   新しいページで、ユーザー・データおよび構成データの場所の指定が求められます。

3. 使用する構成バインド DN およびユーザー・データ検索ベースを入力します。

   たとえば、データを同じディレクトリに格納する場合は次のとおりです。

   - **構成 DN:** o=my-company,c=us
   - **検索ベース :** o=my-company,c=us

   注意： ユーザー・データと構成データを別々に格納する場合、構成 DN および検索ベースは一意である必要があります。また、各ディレクトリの詳細は、各フィールドの右側に表示されます。

   ---

4. 「次へ」をクリックして、「オブジェクト・クラス詳細の指定」に進みます。

オブジェクト・クラス詳細の指定

ID システムの設定プロセスの次の手順では、Person オブジェクト・クラスおよび Group オブジェクト・クラスの詳細を求められます。ここでは、次の項目に分けて説明します。

- 「Oracle Access Manager のオブジェクト・クラスの概要」では、概要について説明します。これらの概念をすでに理解している場合は、スキップできます。
- 「Person オブジェクト・クラスおよび Group オブジェクト・クラスの指定」では、このタスクを実行する手順について説明します。

注意： Oracle Internet Directory とともに動作する ID システムの設定の詳細は、6-3 ページの「タスクの概要 : Oracle Access Manager と Oracle Internet Directory 間の完全な相互作用の実現」を参照してください。

Oracle Access Manager のオブジェクト・クラスの概要

ディレクトリ・サーバーで、データは Oracle Access Manager によってオブジェクトとして格納されます。各オブジェクトは、ID システムの各アプリケーションのプロファイル・ページに表示される属性とその値で構成されます。すべてのオブジェクトは、オブジェクト・クラスに関連付けられます。

ID システムには独自のオブジェクト・クラスがあり、ディレクトリ・サーバー・スキーマに追加する必要があります。これらのオブジェクト・クラスは接頭辞 ob で始まり、ID システムの機能情報が含まれています。ID システムの設定後に、追加のオブジェクト・クラスを構成できます。

Oracle Access Manager には、少なくとも 1 つの Person オブジェクト・クラスと Group オブジェクト・クラスが必要です。ID システムのアプリケーションにログインする前に、これらを設定する必要があります。詳細は、2-27 ページの「Person オブジェクト・クラスおよび Group オブジェクト・クラスの概要」を参照してください。

注意： 時間を節約しエラーをなくすために、ID システムの設定中に Person オブジェクト・クラスと Group オブジェクト・クラスの両方を自動的に構成することをお薦めします。

自動構成によって、Person オブジェクト・クラスおよび Group オブジェクト・クラスに属性が追加されます。特に、デフォルトの表示名、セマンティク型および表示タイプの属性が追加されます。ID システムのアプリケーションにログインする前に、「フルネーム」、「ログイン」および「パスワード」のセマンティク型に属性を割り当てる必要があります。

設定後に、必要に応じて属性を再構成して、独自のオブジェクト・クラスおよび属性を定義し、エンタープライズに固有の要件を組み込むことができます。

Person オブジェクト・クラスおよび Group オブジェクト・クラスの指定

次の手順を完了して、Person オブジェクト・クラスおよび Group オブジェクト・クラスの詳細を指定します。推奨の「自動構成」オプションを使用しない場合は、6-11 ページの「属性の手動構成」で説明されているように、手動で行う必要があります。ここでは一部のページのみを示して、完了した設定ページを説明します。

Person オブジェクトクラスおよび Group オブジェクト・クラスの詳細の指定の手順

1. User Manager の Person オブジェクト・クラスを入力します。次に例を示します。

   Person オブジェクト・クラス : `InetOrgPerson`

   前述のとおり、設定プロセスを効率化するために、「自動構成オブジェクト・クラス」機能がデフォルトで有効化されています。この設定プロセスの後半で、自動構成を検証して確定または変更できます。オブジェクト・クラスを手動で構成する場合は、この機能を無効化できます。

   ここでの指示は、Person オブジェクト・クラスと Group オブジェクト・クラス両方の自動構成に基づいています。

2. 「次へ」をクリックして、Person オブジェクト・クラスの構成を完了します（または、「自動構成オブジェクト・クラス」を無効化して、「次へ」をクリックします）。

   「Group オブジェクト・クラス」ページが表示されます。

3. Group Manager の Group オブジェクト・クラスを入力し、「次へ」をクリックして、Group オブジェクト・クラスの構成を完了します。たとえば、次のようにします。

   Group オブジェクト・クラス : `GroupofUniqueNames`

   次に表示されるページで、ID システムの再起動を求められます。Identity Server によるオブジェクト・クラスの自動構成にかかる時間が、Web ブラウザのタイムアウトを超える場合があります。Identity Server を待機しているときにブラウザがタイムアウトした場合は、1、2 分待ってからブラウザの「更新」ボタンをクリックして続行します。

4. WebPass の Web サーバー・インスタンスを停止します。
5. Identity Server サービスを停止して再起動します。
6. WebPass の Web サーバー・インスタンスを開始します。
7. ID システムの設定ウィンドウに戻り、「次へ」をクリックします。

ID システムの再起動後に行う作業は、設定であらかじめ選択した更新メソッドによって異なります。次に例を示します。

- Person オブジェクト・クラスまたは Group オブジェクト・クラスを自動的に構成することを選択した場合は、6-9 ページの「オブジェクト・クラス変更の確認」に進みます。
- Person オブジェクト・クラスまたは Group オブジェクト・クラスの自動構成を無効化した場合は、6-11 ページの「属性の手動構成」に進みます。

オブジェクト・クラス変更の確認

この設定中、自動的に行われたオブジェクト・クラスの変更内容が表示されます。指定されたオブジェクト・クラスの変更内容を確認し、「はい」をクリックして確定します。「いいえ」をクリックすると、「属性の構成」機能を起動して修正を行うことができます。

次の手順は、Person オブジェクト・クラスと Group オブジェクト・クラス両方の自動構成を有効化したことを前提としています。

オブジェクト・クラス変更の確認の手順

1. Person オブジェクト・クラス属性リストを確認します。
2. 「はい」をクリックして、変更を確定します（または、「いいえ」をクリックして「属性の構成」機能を起動します）。
   - 「はい」の場合、手順 3 に進みます。
   - 「いいえ」の場合、6-11 ページの「属性の手動構成」に進みます。
3. Group オブジェクト・クラス属性リストを確認し、「はい」をクリックして変更を確定し（または、「いいえ」をクリックして変更を拒否し）、次のように進みます。
   - 「はい」の場合、6-9 ページの「マスター管理者の構成」に進みます。
   - 「いいえ」の場合、6-11 ページの「属性の手動構成」に進みます。

マスター管理者の構成

オブジェクト・クラスおよび属性を構成した後で、インストールおよびシステム全体のマスター管理者として 1 名以上を指定することを求められます。

注意： マスター管理者として適切な Person オブジェクト・クラスを持つ人を選択してください。

マスター管理者は、すべての構成機能および管理機能にアクセスできます。これには、他の管理者を割り当て、他の管理者が実行できるすべてのタスクを実行する権限も含まれます。たとえば、設定プロセスの後で、マスター管理者は次の管理者を 1 名以上割り当てることができます。

- マスター ID 管理者。ID システムを構成し、個人を委任 ID 管理者に割り当てる権限を持ちます。
- マスター・アクセス管理者。WebGate、Access Server、認証パラメータ、ポリシー・ドメインの初期セットなどのアクセス・システムを構成する権限を持ちます。これには、個人を委任アクセス管理者のロールに割り当てる権限も含まれます。

  詳細は、『Oracle Access Manager ID および共通管理ガイド』および『Oracle Access Manager アクセス管理ガイド』を参照してください。

マスター管理者の割当ての手順

1. 「管理者の構成」設定ページで、「管理者」の横の「ユーザーの選択」ボタンをクリックします。

   「セレクタ」ページが表示され、2 つの検索基準リスト、検索する最低 3 文字を入力する空のフィールドおよび結果を表示するためのボタンが示されます。

2. 左上にある 2 つのドロップダウン・リストから検索基準を選択し（「フルネーム」と「次を含む」など）、空のフィールドに最低 3 文字を入力し、「実行」ボタンをクリックして、必要な人を検索します。

   検索結果が、基準の下に表示されます。デフォルトでは、（「実行」ボタンの横のフィールドに示されているように）8 個の結果が表示されます。「前へ」および「次へ」ボタンを使用して、必要に応じて結果内を移動できます。

   左側の制御ボタンにより、リスト内のすべての人を追加（「すべて追加」）または、個人を追加（必要な名前の横の「追加」ボタンを選択）できます。いずれかのボタンを選択すると、追加する名前がウィンドウ右側の「選択」の下に表示されます。

3. マスター管理者として割り当てる人の名前の横の「追加」ボタンをクリックします。

4. 追加した名前が、ウィンドウ右側の「選択」の下、および左側の両方に表示されていることを確認します。

   手順 3 で行った名前の追加を続行できます。また、名前の横の削除ボタンまたは「すべて削除」ボタンを使用して、「選択」リストから名前を削除できます。

5. 「完了」をクリックして元の「管理者の構成」ページに戻り、追加する人が「管理者」の横に表示されていることを確認します。

6. 「次へ」をクリックします。

   データ・ディレクトリの保護ページが表示され、ID システムの設定の後で実行する内容が示されます。

ID システムの設定の完了

データ・ディレクトリの保護ページには、ID システムのセキュリティの維持のために保護する必要がある Oracle Access Manager のディレクトリが表示されます。また、次の両方の点からも保護する必要があります。

- ブラウザからのアクセスおよびファイル・システムを介してディレクトリにアクセスするネットワーク・ユーザーからのアクセスを制限します。ディレクトリを保護する方法に関する指示が必要な場合は、使用中の Web サーバーおよびオペレーティング・システムのドキュメントを参照してください。
- Oracle Access Manager ポリシー・ドメイン内の ID システムを保護します。詳細は、『Oracle Access Manager アクセス管理ガイド』を参照してください。

ID システムの設定の完了の手順

1. 「完了」をクリックして、ID システムの設定を完了します。

   ID システムのログイン・ページが表示されます。ID システムの設定および最小限の構成が完了しました。

   この Identity Server のデフォルトのディレクトリ・プロファイルが、ID システム・コンソールで使用可能です。

2. 次のタスクを任意で実行します。

   a. 6-13 ページの「他の Identity Server インスタンスの設定」で説明されているように、複数の Identity Server インスタンスを設定します。

   b. 7-3 ページの「Policy Manager のインストール」で説明されているように、最初のアクセス・システム・コンポーネントのインストールを開始します。

c. マスター管理者として ID システムにログインし、『Oracle Access Manager ID および共通管理ガイド』で説明されているように、次のタスクを任意で完了します。

例 :

- 「ID システム・コンソール」→「システム構成」→「ディレクトリ・プロファイル」→ *link_to_this_profile* を選択して、この Identity Server のディレクトリ・サーバー・プロファイルを表示します。
- User Manager、Group Manager、Organization Manager で、パネルを設定します。
- User Manager でオブジェクトベースの検索ベースを設定します。
- User Manager、Group Manager または Organization Manager で、アクセス制御を設定します。
- ワークフロー定義を作成します。
- メール・サーバーやセッション設定などのオプションを構成します。

属性の手動構成

属性構成機能は、ID システムが機能するために必要な最小限の構成を手動で完了する場合や、設定中に自動的に構成された属性を微調整する場合に役立ちます。ここでの手順を使用して、設定後にいつでも属性を変更できます。

「属性の構成」ページは次の状況で表示されます。

- ID システムの設定中に「自動構成オブジェクト・クラス」を無効化して、Identity Server および Web サーバーを再起動した場合。
- ID システムの設定中に「自動構成オブジェクト・クラス」を有効化して、Identity Server および Web サーバーを再起動し、構成が正しいかどうかの指定を求められたら「いいえ」をクリックした場合。
- 設定後に、「ID システム・コンソール」を選択し、「共通構成」を選択し、「オブジェクト・クラス」を選択して、次に *object_class_link* を選択し、「属性の変更」を選択して、「属性の変更」ページに移動した場合。

Novell Directory Server の考慮点

Novell Directory Server（NDS）は、属性およびオブジェクト・クラス名を、ネイティブ・ディレクトリ・サーバーから NDS の LDAP レイヤーにマップします。一部の属性またはオブジェクト・クラスは、LDAP レイヤー内に複数のマッピング（別名）を持ちます。たとえば、ネイティブ NDS オブジェクト・クラスは Group ですが、NDS の LDAP レイヤーは GroupofNames および GroupofUniqueNames という 2 つの別名をマップします。

Oracle Access Manager および NDS の正しい機能の確認の手順

1. 構成中に指定したオブジェクト・クラスまたは属性名が、同じオブジェクト・クラスまたは属性の他のマッピングよりも前にあることを確認します。
2. consoleOne によって、マッピングの順序を確認します。

属性の構成または調整

次の手順を使用して、Person オブジェクト・クラスおよび Group オブジェクト・クラスを手動で設定します。

最小限の Person オブジェクト・クラス属性セットの定義の手順

1. 「属性の構成」ページの属性リストで、次の Person オブジェクト・クラス属性の詳細を選択または入力します。
   a. **属性 :** Person オブジェクト・クラスのクラス属性。多くの場合、cn です。
   b. **表示名 :**「名前」または「フルネーム」。
   c. **セマンティク型 :**「DN 接頭辞」および「フルネーム」。
   d. **表示タイプ :**「単一行テキスト」。
   e. **属性値 :**「単一」。
2. 「保存」をクリックしてから、「OK」をクリックして確認メッセージを閉じます。
3. 属性リストで、次の詳細を選択または入力して、ログイン ID 属性を定義します。
   - **属性 :** ユーザーのログイン ID を定義する属性。多くの場合、uid 属性です。
   - **表示名 :** ログイン ID など。
   - **セマンティク型 :**「ログイン」。
   - **表示タイプ :**「単一行テキスト」。
   - **属性値 :**「単一」。
4. 「保存」をクリックしてから、「OK」をクリックして確認メッセージを閉じます。
5. 属性リストで、次の詳細を選択または入力して、姓属性を定義します。
   - **属性 :** ユーザーの姓を定義する属性。多くの場合、sn です。
   - **表示名 :**（姓など）。
   - **表示タイプ :**「単一行テキスト」。
   - **属性値 :**「単一」。
   - 「セマンティク型」は指定しません。
6. 「保存」をクリックしてから、「OK」をクリックして確認メッセージを閉じます。
7. 属性リストで、次の詳細を選択または入力して、ユーザー・パスワード属性を定義します。
   - **属性 :** ユーザー・パスワードを定義する属性。多くの場合、password または userPassword 属性です。
   - **表示名 :** パスワードなど。
   - **表示タイプ :**「パスワード」。
   - **属性値 :**「パスワード」。
   - **属性値 :**「単一」。
8. 「保存」をクリックしてから、「OK」をクリックして確認メッセージを閉じます。
9. 「次へ」をクリックして、Group オブジェクト・クラスを構成するページに進みます。

Group オブジェクト・クラス属性の最小限のセットの指定の手順

1. 属性リストで、次の詳細を選択または入力します。
   - **属性 :** グループ名を定義する属性。多くの場合、cn 属性です。
   - **表示名 :** グループ名など。
   - **セマンティク型 :** 「DN 接頭辞」および「フルネーム」。
   - **表示タイプ :** 「単一行テキスト」。
   - **属性値 :** 「単一」。
2. 「保存」をクリックしてから、「OK」をクリックします。
3. 必要に応じて、次の手順に進みます。
   - 「他の Identity Server インスタンスの設定」、次に
   - 第 7 章「Policy Manager のインストール」で説明されている「Policy Manager のインストール」
   - 『Oracle Access Manager ID および共通管理ガイド』で説明されている ID システム用の Access Server SDK の構成

     ID システムの一部の機能では、Access Server SDK が必要です。デフォルトでは、Access Server SDK は、¥*IdentityServer_install_dir*¥identity の下のサブディレクトリにインストールされます。ID システムの設定後、ID システムでこれらの機能を有効化するには、Access Server SDK を手動で構成する必要があります。

他の Identity Server インスタンスの設定

表 6-2 に、追加の Identity Server インスタンスを設定する前に完了する必要があるタスクを示します。

表 6-2 追加の Identity Server の設定準備

チェックリスト	追加の Identity Server の設定の前提条件
	第 I 部「インストールの計画と前提条件」で説明されている、ユーザーの環境に適用される前提条件および要件がすべて満たされていることを確認する。
	4-5 ページの第 II 部「ID システムのインストールおよび設定」で説明されているように、Identity Server をインストールする。
	6-5 ページの「ID システムの設定」のアクティビティをすべて完了する。
	4-5 ページの「Identity Server のインストール」で説明されているように、追加の Identity Server をインストールする。
	まだ行っていない場合は、すべての Identity Server サービスを停止する。
	新規 Identity Server サービスのみ、6-14 ページの手順「Identity Server の設定および WebPass との関連付けの手順」で起動する。

追加の Identity Server の設定には、元の設定プロセスのサブセットのみが含まれます。

Identity Server の設定および WebPass との関連付けの手順

1. 通常どおり、ID システム・コンソールに移動します。

   ```
   http://hostname:port/identity/oblix/
   ```

   WebPass は、元の Identity Server に接続しようとします。接続できない場合、WebPass は新規 Identity Server に接続し、設定ページを起動します。

2. 「セットアップ」をクリックし、指示に従って Identity Server を設定します。
   詳細は、6-5 ページの「ID システムの設定」を参照してください。

3. 設定中に指示された場合は、新規 Identity Server サービスを再起動します。

4. 他の Identity Server サービスを再起動します。

5. 必要に応じて、追加の Identity Server ごとに繰り返します。

第 III 部

アクセス・システムのインストールおよび設定

ここでは、アクセス・システムを正常にインストールおよび設定するために必要なすべての情報について説明します。

第Ⅲ部は、次の章で構成されます。

7

Policy Manager のインストール

ID システムのインストール後、アクセス・システムのインストールを開始できます。アクセス・システムには、Policy Manager、Access Server、および WebGate の 3 つのコンポーネントが含まれています。この章の項目で説明するように、Policy Manager は最初にインストールする必要のあるコンポーネントです。

- Policy Manager のインストールおよび設定の概要
- Policy Manager の前提条件チェックリスト
- Policy Manager のインストール
- Web サーバーの手動構成
- IIS 上の Policy Manager の権限の検証
- Policy Manager の設定
- Policy Manager の設定の確認

10*g*（10.1.4.0.1）にアップグレードする方法は、『Oracle Access Manager アップグレード・ガイド』で説明されています。

Policy Manager のインストールおよび設定の概要

Policy Manager は、アクセス・システムのログイン・インタフェースを提供し、ディレクトリ・サーバーと通信してポリシー・データを書き込み、Oracle Access プロトコルにより Access Server と通信して、一定のポリシーを変更した場合に Access Server を更新します。マスター・アクセス管理者および委任アクセス管理者は、Policy Manager を使用して保護するリソースを定義し、リソースをポリシー・ドメインにグループ化します。概要は、『Oracle Access Manager 概要』で説明されています。

Policy Manager のインストールには、アクセス・システム・コンソールが含まれます。Policy Manager のインストールにより、Identity Server および WebPass のインストール両方の要素が結合されます。たとえば、Policy manager のインストール時に Oracle Access Manager ポリシー・データの格納場所を識別する必要があります。デフォルトの Policy Manager のディレクトリ・プロファイルが作成され、設定後に使用可能になります。また、WebPass に対して実行したように、Policy Manager の Web サーバー構成を更新する必要があります。Policy Manager のサービスを開始および停止するのではなく、Policy Manager の Web サーバーを開始および停止します。

また、プラットフォーム固有のディレクトリ内の Policy Manager に対して、個別の Web サーバー固有のインストール・パッケージが提供されています。選択するインストール方法および使用中のオペレーティング・システムに関係なく、インストール・プロセスは類似しています。情報は、インストール中の特定の時点で保存されます。Policy Manager がインストールされていることが通知された後でインストールを取り消す場合は、1-9 ページの「Oracle Access Manager の以前のリリースからのアップグレード」で説明されているように、コンポーネントをアンインストールする必要があります。

インストール後、その他のアクセス・システムのコンポーネントをインストールする前に、Policy Manager の設定プロセスを完了する必要があります。ID システムの設定と同様に、設定中に 1 つのページから次へ進む際に情報が保存されます。いつでも前のページに戻ることができ、設定プロセスは、いつでも中止および再開できます。設定プロセスを再開する場合、最後に保存した入力の次の質問から続行します。

インストールの考慮点は、2-7 ページの「Policy Manager のガイドライン」を参照してください。

複数の Policy Manager のインストールの概要

フォルト・トレランスに備えて、複数の Policy Manager をインストールすることをお薦めします。複数の Policy Manager をインストールするには、各新規の Policy Manager インスタンスに対してこの章で説明するインストールおよび設定を実行します。

IIS Web サーバーにインストールされた Policy Manager は、レジストリに依存して ¥*PolicyManager_install_dir* を取得します。1 台のマシン上に 2 つの Policy Manager（1 つは IIS Web サーバーとともに、もう 1 つは Sun Web サーバーとともに）をインストールする場合のレジストリ内の競合を回避するため、次の手順で説明しているように Policy Manager をインストールする必要があります。

IIS および Sun の Web サーバーのインスタンスの競合の回避の手順

1. Sun Web サーバーの Policy Manager を最初にインストールします。
2. 次に、IIS Web サーバーの Policy Manager をインストールします。

Policy Manager の前提条件チェックリスト

WebGate のインストールを開始する前に、表 7-1 のタスクを完了していることを確認してください。すべての前提条件を満たさない場合、Oracle Access Manager のインストールに悪影響を及ぼすことがあります。

表 7-1 Policy Manager の前提条件チェックリスト

チェックリスト	Policy Manager の前提条件
	第 I 部「インストールの計画と前提条件」で説明されている、ユーザーの環境に適用される前提条件および要件がすべて満たされていることを確認する。
	第 II 部「ID システムのインストールおよび設定」のアクティビティをすべて完了する。
	第 5 章「WebPass のインストール」で説明されているように、この Policy Manager の WebPass をインストールして、次を実行する。 ■ Policy Manager をインストールするのと同じ Web サーバー・インスタンス、同じディレクトリ・レベルに WebPass がインストールされていることを確認する。 ■ WebPass が特定の Identity Server と連動するように構成されていることを確認する。

Policy Manager のインストール

Policy Manager は、WebPass と同じディレクトリにインストールする必要があります。WebPass が含まれていないディレクトリを指定する場合、WebPass をインストールするか、別のディレクトリを指定するかの指定を求められます。WebPass のインストールを選択する場合、自動的に起動します。

Policy Manager をインストールしながら、記入済のインストール準備ワークシートを参照します。インストール・タスクは、次の手順にわかれています。

タスクの概要 : Policy Manager のインストール

1. 7-4 ページの「インストールの開始」で説明されているように、インストール・メソッドを選択して、プロセスを開始します。
2. 7-5 ページの「ディレクトリ・サーバー・タイプおよびポリシー・データの場所の定義」で説明されているように、ディレクトリ・サーバーおよびデータの場所を特定します。
3. 7-7 ページの「トランスポート・セキュリティ・モードの指定」で説明されているように、トランスポート・セキュリティ・モードを特定します。
4. 7-8 ページの「Policy Manager の Web サーバー構成の更新」で説明されているように、Web サーバー構成を更新します。
5. 7-9 ページの「Policy Manager のインストールの終了」で説明されているように、インストールを完了します。

インストールの開始

必ず使用している Web サーバーに適したインストール・パッケージを選択してください。

Policy Manager のインストールの開始の手順

1. 管理者権限を持つユーザーとしてログインします。
2. 作成した一時ディレクトリで Policy Manager インストーラ（インストールするアクセス・システム言語パックを含む）を検索します。
3. 選択したプラットフォーム、インストール・メソッド、および Web サーバーの Policy Manager インストーラを起動します。

   例 :

   - **GUI メソッド**

     Oracle_Access_Manager10_1_4_0_1_Win32_*API*_Policy_Manager.exe

   - **コンソール・メソッド**

     ./ Oracle_Access_Manager10_1_4_0_1_sparc-s2_*API*_Policy_Manager

   「ようこそ」画面が表示されます。
4. 「次へ」をクリックして、「ようこそ」画面を閉じます。
5. プラットフォームに基づいて管理者権限に関する質問に応答します。次に例を示します。

   Policy Manager のインストール・ディレクトリを指定するよう求められます。
6. インストール先を選択してから、「次へ」をクリックします。

   例 :

   ¥OracleAccessManager¥WebComponent
7. **言語パック :** この画面が表示される場合、インストールするデフォルト・ロケールおよびその他のロケールを選択してから、「次へ」をクリックします。

   サマリーでは、インストール・ディレクトリおよび必要なディスク領域を識別し、後で参照できるように情報をメモするようユーザーに指示します。
8. 必要に応じてインストール・ディレクトリ名を記録して、「次へ」をクリックします。

数秒間、Policy Manager をインストール中という通知があります。Windows システムの場合、Microsoft 管理インタフェースが構成中であることが通知されます。情報は保存されており、前の画面に戻って情報を再指定することはできません。

インストール・プロセスはまだ完了していません。Oracle Access Manager ポリシー・データの場所の指定を求められます。

ディレクトリ・サーバー・タイプおよびポリシー・データの場所の定義

Oracle Access Manager ポリシー・データには、リソースへのアクセスを管理するルールが含まれています。ポリシー・データの格納場所および Oracle Access Manager スキーマをここで追加するか、後で追加するかの指定を求められます。ポリシー・データが格納されている場所に応じて、次のように実行します。

- **同じディレクトリ・サーバー :**「いいえ」と応答します。Oracle Access Manager ポリシー・データが構成データまたはユーザー・データと同じディレクトリ・サーバーに格納される場合、Identity Server のインストール中にスキーマが追加されているため、更新は必要ありません。
- **個別のディレクトリ・サーバー :** Oracle Access Manager ポリシー・データが構成データまたはユーザー・データとは別のディレクトリに格納される場合、Oracle Access Manager スキーマを追加する必要があります。この追加は次のいずれかで実行できます。
  - **自動 :**「はい」と応答して、ここでスキーマを自動的に更新します。
  - **手動 :**「いいえ」と応答して、後でスキーマを手動で更新します。詳細は、1-6 ページの「スキーマおよび属性の自動更新と手動更新」を参照してください。

ポリシー・データの場所の識別の手順

1. ディレクトリ・サーバー・タイプを選択して、「次へ」をクリックします。

   例 :

   Sun

2. ポリシー・データの格納場所についての質問に応答します。
   - **いいえ :** ポリシー・データがユーザー・データおよび構成データと一緒に格納される場合、または後でスキーマを手動で更新する場合、「いいえ」と応答します。
   - **はい :** ポリシー・データが個別に格納される場合、またはここでスキーマを自動的に更新する場合、「はい」と応答します。

   この情報は保存され、戻って情報を再指定することはできません。
3. 「次へ」をクリックして、環境に該当する手順にスキップします。
   - スキーマを更新しない Solaris の続行
   - スキーマを更新しない Windows の続行
   - ポリシー・データの個別の格納およびスキーマの更新

スキーマを更新しない Solaris の続行

Solaris システムでのインストール中、ポリシー・データが他の Oracle Access Manager データと一緒に格納される場合、既存のディレクトリ・サーバーの通信方法について指定を求められます。

ディレクトリ・サーバー通信の詳細の指定の手順

1. SSL でディレクトリ・サーバー通信の保護についての質問に応答し、「次へ」をクリックします。

   注意 : Sun Web サーバーとともに Solaris にインストールされている Policy Manager では、SSL はサポートされていません。

2. **SSL:** 証明書へのパスを指定し、「次へ」をクリックします。
3. 7-7 ページの「トランスポート・セキュリティ・モードの指定」に進みます。

スキーマを更新しない Windows の続行

Windows システムでのインストール中、ポリシー・データが他の Oracle Access Manager データと一緒に格納される場合、ディレクトリ・サーバーとの通信について指定を求められます。

注意： この手順が終了したら、トランスポート・セキュリティ詳細の指定を求められます。この場合、7-7 ページの「トランスポート・セキュリティ・モードの指定」にスキップします。

既存のディレクトリ・サーバー詳細の指定の手順

1. ADSI で Active Directory を使用している場合は「はい」（使用していない場合は「いいえ」）をクリックしてから、「次へ」をクリックします。たとえば、次のようにします。

   いいえ

   次に、ユーザー・データ、構成データ、およびポリシー・データの 3 タイプそれぞれに対するディレクトリ・サーバーと Policy Manager 間の通信について指定を求められます。

2. ディレクトリ・サーバーで SSL 通信が必要な各データのタイプの横のボックスを選択してから、「次へ」をクリックします。次に例を示します。

   ディレクトリ・サーバー ... ユーザー・データは SSL 内に存在

   ディレクトリ・サーバー ... 構成データは SSL 内に存在

   ディレクトリ・サーバー ... ポリシー・データは SSL 内に存在

3. **SSL:** 各証明書へのパスを指定してから、「次へ」をクリックします。

4. 7-7 ページの「トランスポート・セキュリティ・モードの指定」に進みます。

ポリシー・データの個別の格納およびスキーマの更新

ポリシー・データが個別に格納されている場合、ディレクトリ・サーバーのタイプおよびその他の関連する詳細を識別する必要があります。詳細は、2-22 ページの「データ記憶域の要件」を参照してください。

ディレクトリ・サーバー・タイプおよび構成詳細の指定の手順

1. 個別に格納されたポリシー・データのディレクトリ・サーバー・タイプを指定してから、「次へ」をクリックします。たとえば、次のようにします。

   Sun

2. 次のディレクトリ・サーバー構成情報を指定してから、「次へ」をクリックします。次に例を示します。

   - **ホスト名：** ポリシー・データのディレクトリ・サーバー・マシンの DNS ホスト名
   - **ポート番号：** ポリシー・データのディレクトリ・サーバーがリスニングするポート番号（SSL 接続の場合、暗号化ポートを指定）
   - **バインド DN:** ポリシー・データのディレクトリ・サーバーの DN

注意： バインド DN として入力する識別名には、ディレクトリ情報ツリー（DIT）のポリシー・データ・ブランチに対する完全な権限がある必要があります。Oracle Access Manager は、このアカウントでディレクトリ・サーバーにアクセスします。例は、表 7-2 を参照してください。ユーザーの構成は異なる場合があります。

表 7-2 サポートされているディレクトリ・サーバーのバインド DN の例

ディレクトリ・サーバー	バインド DN
Sun Directory Server 5.x	*cn=administrator* **注意 :** cn=Directory Manager を使用しないことをお薦めします。詳細は、2-18 ページの「ディレクトリ・サーバーの要件の実現」を参照してください。

- **パスワード :** ユーザー・データのディレクトリ・サーバーのバインド DN のパスワード
- **SSL 接続を使用して更新しますか。**（「はい」または「いいえ」）: Sun Web サーバーとともに Solaris にインストールする場合、SSL はサポートされていないため、通信は「オープン」にする必要があります。

SSL を示した場合は手順 3 を完了します。

3. **SSL のみ :** 証明書パスを指定し、「次へ」をクリックします。

   指定した情報内にエラーが存在する場合、スキーマを更新できません。インストール中に構成情報を変更したり、ファイル : ¥*PolicyManager_install_dir*¥access¥oblix¥tools¥ldap_tools¥ds_conf_update を使用して後でスキーマを手動更新できます。1-6 ページの「スキーマおよび属性の自動更新と手動更新」も参照してください。

   次に、トランスポート・セキュリティについて指定を求められます。

トランスポート・セキュリティ・モードの指定

Policy Manager および WebPass のトランスポート・セキュリティ・モードを指定する必要があります。すべてのアクセス・システム・コンポーネント（Policy Manager、Access Server および関連 WebGate）間のトランスポート・セキュリティは一致している必要があります（すべてオープン、シンプルまたは証明書モード）

トランスポート・セキュリティ・モードの指定の手順

1. 残りのアクセス・システムと通信するためにこの Policy Manager が使用するトランスポート・セキュリティ・モードを指定します。
2. 「次へ」をクリックして、選択したトランスポート・セキュリティ・モードに従って、次の操作を実行します。次に例を示します。
   - **オープン :** 7-8 ページの「Policy Manager の Web サーバー構成の更新」にスキップします。
   - **シンプル :** アクセス・システム・パスフレーズを指定および確認してから、「次へ」をクリックして 7-8 ページの「Policy Manager の Web サーバー構成の更新」に進みます。
   - **証明書 :** 証明書パスワード（PEM 句）を指定および確認し、「次へ」をクリックして手順 3 に進みます。
3. **証明書 :** 証明書をリクエストまたはインストールしていることを示してから、手順を完了して、「次へ」をクリックして 7-8 ページの「Policy Manager の Web サーバー構成の更新」に進みます。

   注意 : 証明書が ¥*PolicyManager_install_dir*¥access¥oblix¥config ディレクトリにコピーされ、Policy Manager Web サーバーが再起動されるまで Policy Manager は設定できません。詳細は、『Oracle Access Manager アクセス管理ガイド』を参照してください。

   Policy Manager の Web サーバー構成を更新できます。

Policy Manager の Web サーバー構成の更新

Web サーバーは、Policy Manager と連動するように構成する必要があります。この Web サーバー構成の更新を自動または手動で実行するように指定できます。

注意： 自動的に Web サーバー構成を更新することをお薦めします。ただし、手動による構成指示も含まれています。

Web サーバー構成の自動更新の手順

1. Web サーバーを自動的に更新するには「はい」をクリックしてから、「次へ」をクリックします。

   - **ほとんどの Web サーバー：** Web サーバー構成ファイルを含むディレクトリの絶対パスを指定して、「次へ」をクリックします。
   - **IIS Web サーバー：** プロセスが即時に開始され、プロセスには 1 分以上かかることがあります。

   Web サーバー構成が更新されたことを通知する画面が表示されます。

2. **Sun Web サーバー：** 続行する前に、Web サーバー管理コンソールで変更を適用します。
3. Policy Manager の Web サーバー・インスタンスを停止し、Identity Server サービスを停止および再起動して、Policy Manager の Web サーバー・インスタンスを開始します。

注意： IIS Web サーバーの場合、特に Policy Manager のインストール後に `net stop iisadmin` および `net start w3svc` を使用して Web サーバーを停止および開始すると効率的です。net コマンドは、インストールに伴いメタベースが破損しないようにするために役立ちます。

---

4. 「次へ」をクリックして通知を閉じ、7-9 ページの「Policy Manager のインストールの終了」に進みます。

   README の情報が表示されます。

Web サーバー構成の手動更新の手順

1. 自動更新を続行するかどうかの指定を求められた場合、「いいえ」をクリックしてから「次へ」をクリックします。

   新規のウィンドウが表示され、Oracle Access Manager の Web サーバーの手動設定が可能になります。

2. Policy Manager のインストール画面に戻り、「次へ」をクリックします。
3. インストールを終了した後、および Policy Manager を設定する前に 7-9 ページの「Web サーバーの手動構成」を参照してください。

Policy Manager のインストールの終了

README の情報には、ドキュメントおよびオラクル社の連絡先に関する詳細が記載されています。

Policy Manager のインストールの終了の手順

1. README の情報を確認してから、「次へ」をクリックします。

   Policy Manager が正常にインストールされたことが通知されます。

2. 「終了」をクリックして、ウィザードを閉じます。

3. 必要に応じて、次の手順に進みます。

   - Web サーバーの手動構成（インストール時に自動的に構成されなかった場合）
   - IIS 上の Policy Manager の権限の検証
   - Policy Manager の設定

Web サーバーの手動構成

Policy Manager のインストール中に、Web サーバーのインストールを自動で更新するかどうかの指定を求められます。「いいえ」を選択した場合、Policy Manager を設定する前にこれを手動で実行する必要があります。

注意： Policy Manager のインストール中に手動構成プロセスを起動した場合、手順 1 をスキップできます。

Policy Manager の Web サーバーの手動構成の手順

1. Web ブラウザを起動し、必要に応じて次のファイルを開きます。

   ¥*PolicyManager_install_dir*¥access¥oblix¥lang¥langTag¥docs¥config.htm

   ここで、¥*PolicyManager_install_dir* は、Policy Manager をインストールしたディレクトリです。

2. 画面の表から該当するサポート対象の Web サーバー・インタフェース構成プロトコルを選択します。

3. 表示される各 Web サーバーのタイプに固有の指示にすべて従い、次の点に注意します。

   - Web サーバーの設定中に変更する必要があるファイルのバックアップ・コピーを作成します。これは、再度 Web サーバーを設定する必要がある場合に使用できます。
   - 設定によっては、新しいブラウザ・ウィンドウが起動されます。または、情報を入力するためにコマンド・ウィンドウを起動する必要があります。このため、元の設定指示に戻ってすべてを実行し、該当する Oracle Access Manager ファイルを Web サーバーが認識できるようにします。

   注意： 誤ってウィンドウを閉じた場合、手順 1 に戻り、該当するリンクを再度クリックできます。

   ---

4. 次の手順に進みます。

   - IIS 上の Policy Manager の権限の検証（必要な場合）
   - Policy Manager の設定

IIS 上の Policy Manager の権限の検証

構成を Policy Manager のインストール中に自動的に更新する場合、または手動で更新する場合のいずれも、ディレクトリ権限が Oracle Access Manager に対して正しく設定されていることを容易に検証できます。

Policy Manager の IIS Web サーバー構成の検証の手順

1. Web ブラウザを起動し、必要に応じて次のファイルを開きます。たとえば、次のようにします。

   ¥*PolicyManager_install_dir*¥access¥oblix¥lang¥langTag¥docs¥config.htm

2. 7-9 ページの「Web サーバーの手動構成」でも示しているように、画面の表から該当する Web サーバー・インタフェース構成プロトコルを選択します。
3. ディレクトリ権限を確認して、Policy Manager の Web サーバーに設定されたディレクトリ権限と比較します。

Policy Manager の設定

作成する新規ポリシーを書き込むために、Policy Manager はディレクトリ・サーバーと通信する必要があります。次の手順は、この通信に必要な接続を確立する場合のガイドです。

設定中は、「次へ」ボタンをクリックするたびに仕様が保存されます。設定を中止して後で設定を再開すると、同じ場所に戻ります。

タスクの概要 : Policy Manager の設定

1. 7-10 ページの「設定プロセスの開始」で説明されているように、プロセスを開始します。
2. 7-11 ページの「ディレクトリ・サーバー詳細およびデータの場所の指定」で説明されているように、ディレクトリ詳細を定義します。
3. 7-14 ページの「認証スキームの構成」で説明されているように、認証スキームを設定します。
4. 7-15 ページの「Policy Manager の設定の完了」で説明されているように、設定プロセスを終了します。

設定プロセスの開始

ポリシー情報の格納に使用するディレクトリ・サーバーが Oracle Access Manager スキーマにロードされていない場合、Policy Manager の設定は完了できません。

次の条件のいずれにも該当する場合、設定プロセスを開始する前に、ポリシー・データのディレクトリ・サーバーのスキーマを手動で更新する必要があります。

- 個別のディレクトリ・サーバーにポリシー・データを格納する場合
- ID システムの設定中にこのディレクトリ・サーバーのスキーマを更新しなかった場合

これを実行する必要がある場合、次のファイルの指示を使用してください。

¥*PolicyManager_install_dir*¥access¥oblix¥lang¥*langTag*

¥ldap_schema_changes_directory_server.html

ここで、パス名の *directory_server* は、特定のディレクトリ・サーバー・タイプを表し、¥*langTag* は、使用中の言語（たとえば ¥en-us など）を表します。

Policy Manager の設定の開始の手順

1. Web サーバーが実行されていることを確認します。
2. Policy Manager に接続する WebPass インスタンスの URL を指定して、ブラウザからアクセス・システム・コンソールに移動します。次に例を示します。

   `http://hostname:port/access/oblix`

   ここで、*hostname* は Web サーバーをホストするマシン、*port* は WebPass の Web サーバー・インスタンスの HTTP ポート番号をそれぞれ指し、`/access/oblix` はアクセス・システム・コンソールに接続します。

   アクセス・システムのメイン・ページが表示されます。
3. 「アクセス・システム・コンソール」リンクをクリックします。

   アプリケーションがまだ設定されていないことが通知されます。
4. 「セットアップ」ボタンをクリックします。

   次のページでディレクトリ・サーバー・タイプについて指定します。
5. 7-11 ページの「ディレクトリ・サーバー詳細およびデータの場所の指定」に進み、詳細は第 19 章「重要な注意事項」を参照してください。

ディレクトリ・サーバー詳細およびデータの場所の指定

ユーザー・データ、構成データ、およびポリシー・データが格納されるディレクトリ・サーバーの詳細を指定する必要があります。各タイプのデータに対してディレクトリ・サーバーの情報を指定するよう求められます。

- ユーザー・データ
- 構成データ
- ポリシー・データ

ディレクトリ・サーバー・タイプは、アクティビティの範囲に影響を与えます。Sun ディレクトリ・サーバーでは、ポリシー・データを構成データやユーザー・データとは異なるディレクトリ・サーバーに格納できます。すべてのポリシー・データは、同じディレクトリ・サーバーに格納する必要があります。

Active Directory では、純粋な ADSI 構成が作成され、ADSI オプションを選択する場合、ディレクトリ・サーバーへの通信は ADSI を介して構成されます。「動的補助オブジェクト・クラス (Windows 2003 のみ)」を有効化する場合、A-4 ページの「動的リンク補助クラスについて」を参照してください。

設定中に表示される情報は、環境により異なります。この例では、ユーザー・データ、構成データ、およびポリシー・データは同じディレクトリ・サーバーに格納されています。ユーザーの環境とは異なる場合があります。

Policy Manager の設定中のディレクトリ・サーバー詳細の指定の手順

1. ユーザー・データのディレクトリ・サーバー・タイプを選択してから、「次へ」をクリックします。次に例を示します。

   Sun

   ここで、ユーザー・データのディレクトリ・サーバー詳細を指定して、Policy Manager がディレクトリ・サーバーを検索して、このディレクトリ・サーバーに情報をコピーできるようにします。

2. インストールに従ってユーザー・データのディレクトリ・サーバー詳細を指定してから、「次へ」をクリックします。次に例を示します。

   - **マシン :** ユーザー・データのディレクトリ・サーバーの DNS ホスト名
   - **ポート番号 :** ユーザー・データのディレクトリ・サーバーのポート番号
   - **ルート DN:** ユーザー・データのディレクトリ・サーバーのバインド DN
   - **ルート・パスワード :** バインド DN パスワード

   注意 : Active Directory の場合、「ドメイン名」フィールドは、入力に含まれます。ADSI の場合、「ユーザー・プリンシパル名」フィールドは、ルート DN の UserPrincipleName を入力する場所（admin@mycompany.com など）に含まれます。

   ユーザー・データおよび構成データの格納場所について指定を求められます。

3. 構成データのディレクトリ・サーバー・タイプを選択してから、「次へ」をクリックします。次に例を示します。

   Sun

   次に、ユーザー・データおよび構成データを同じディレクトリまたは個別のディレクトリに格納できることが通知され、デプロイの構成を選択するよう求められます。

4. ユーザー・データおよび構成データが（一緒または個別に）格納される場所を記述する項目を選択してから、「次へ」をクリックします。

   - データが一緒に格納される場合、ポリシー・データの格納場所の指定を求められます。この場合は、手順 5 に進みます。
   - データが個別に格納される場合、作業を続行する前に、構成データのディレクトリ・サーバー詳細を指定するよう求められます。

5. ポリシー・データおよび構成データが（一緒または個別に）格納される場所を記述する項目を選択して、「次へ」をクリックします。

   - データが一緒に格納される場合、手順 6 に進みます。
   - データが個別に格納される場合、作業を続行する前に、ポリシー・データのディレクトリ・サーバー詳細を指定するよう求められます。

   次のページで「セットアップ・ヘルプ」ボタンが表示されます。このボタンを選択して、設定プロセス中の追加情報を取得できます。ここで、構成 DN、検索ベース、およびポリシー・ベースの場所を指定するよう求められます。

   注意 : 構成 DN、検索ベース、およびポリシー・ベースは、ディレクトリ・ツリーと同じレベルにある場合も異なるレベルにある場合もあります。ただし、検索ベースおよびポリシー・ベースが個別のディレクトリにある場合、これらには固有の DN を指定する必要があります。つまり、これらが個別のディレクトリに入っている場合、検索ベースは o=oblix,< ポリシー・ベース > または ou=oblix,< ポリシー・ベース > にできません。同様に、ポリシー・ベースおよび構成 DN が個別のディレクトリに入っている場合、同じにはできません。

6. インストールに該当する情報を指定して、「次へ」をクリックします。次に例を示します。

   - **検索ベース :** o=my-company,c=us

     これは、ID システム構成中に指定した検索ベースと同じである必要があります。

   - **構成 DN:** o=my-company,c=us

     これは、ID システム構成中に指定した構成 DN と同じである必要があります。

   - **ポリシー・ベース :** o=my-company,c=us

     このノードは、ポリシー・ディレクトリ・サーバー内に存在します。このノードが存在していない場合、手動で作成します。

   ここで、Person オブジェクト・クラスを指定するよう求められます。これは、ID システムの設定中に指定したものと一致する必要があります。詳細は、準備ワークシートおよび6-8 ページの「Person オブジェクトクラスおよび Group オブジェクト・クラスの詳細の指定の手順」を参照してください。

7. Person オブジェクト・クラス名を入力して、「次へ」をクリックします。

   例 :

   Person オブジェクト・クラス : `gensiteOrgPerson`

   この時点で、Web サーバーの再起動を求めるプロンプトが表示されます。

   注意 : IIS を使用している場合、画面上の追加の指示に従います。`net stop iisadmin` および `net start w3svc` を使用して IIS を停止および開始することを検討してください。net コマンドは、メタベースが破損しないようにするために役立ちます。

   ---

8. 通常どおり WebPass/Policy Manager の Web サーバー・インスタンスおよび関連する Identity Server のインスタンスを停止および再起動し、「次へ」をクリックして続行します。

   ここで、Oracle Access Manager ポリシー・ドメインのルート・ディレクトリを指定するよう求められます。

   ポリシー・ドメインを定義および保護するマスター管理者の機能を制限しない場合は、デフォルト値 "/" を受け入れることをお薦めします。詳細は、『Oracle Access Manager アクセス管理ガイド』を参照してください。

9. ポリシー・ドメインのデフォルトのルート・ディレクトリを受け入れ（または新規ルート・ディレクトリを指定して）、「次へ」をクリックします。次に例を示します。

   Policy Domain Root /

   次のページで認証スキームの構成の情報を指定します。

認証スキームの構成

Policy Manager の設定中に、次の 2 つの認証スキームが自動的に構成されます。

- **Oracle Access and Identity:** Oracle Access Manager 関連リソース（URL）および Active Directory の Oracle Access Manager 関連リソース（URL）の保護に使用します。
- **匿名 :** 特定の Oracle Access Manager URL の保護解除に使用します。

  匿名認証方式は、匿名ユーザーに提供されるため特に有用です。ユーザーは、自己登録およびロスト・パスワード管理などのアクセス・システムにより保護されない Oracle Access Manager 固有の URL にアクセスできます。

また、ユーザー・ディレクトリの構成情報に基づき、基本およびクライアント証明書認証スキームを自動的に構成できます。

- **Basic Over LDAP:** この組込み Web サーバー・チャレンジ・メカニズムでは、ユーザーはログイン ID およびパスワードを入力する必要があります。指定された資格証明は、LDAP ディレクトリ・サーバーでユーザー・プロファイルと比較されます。
- **クライアント証明書 :** これは、証明書ベースのユーザー識別方式です。この方式を使用するには、証明書がブラウザにインストールされており、Web サーバーで SSL が有効化されている必要があります。

各スキームの設定ページ上のフィールドには、設定する Oracle Access Manager 環境と一貫性のある情報を入力する必要があります。ほとんどの場合、該当するデフォルトが設定ページに表示されます。これらのパラメータは、アクセス・システム・コンソールを使用して後で変更できます。

また、ポリシーを設定するかどうかの指定を求められます。このオプションを受け入れる場合、次の 2 つのポリシー・ドメインが自動的に作成されます。

- Access ドメイン
- Identity ドメイン

自動構成を拒否し、後で Basic Over LDAP およびクライアント証明書認証スキームをアクセス・システム・コンソールで設定することも可能です。認証スキームおよびポリシー・ドメインの詳細は、『Oracle Access Manager アクセス管理ガイド』を参照してください。

認証スキームの完了の手順

1. 自動構成の手順を開始するには「はい」を選択し、すべての認証スキームを手動で設定するには「いいえ」を選択してから、「次へ」をクリックします。
   - 「はい」の場合、手順 2 に進みます。
   - それ以外の場合は、手順 5 にスキップします。
2. 自動的に構成する認証スキームを選択してから、「次へ」をクリックします。
   - Basic Over LDAP を選択する場合、定義が指定されたページが表示されます。この定義はここで変更することも、後で変更することもできます。この場合は、手順 3 に進みます。
   - クライアント証明書のみを選択している場合、手順 4 にスキップします。
3. 必要に応じて Basic Over LDAP のパラメータを確認および変更してから、「次へ」をクリックします。
4. 必要に応じてクライアント証明書のパラメータを確認および変更してから、「次へ」をクリックします。

   次に、ポリシーを構成して Oracle Access Manager 関連（URL）を保護するかどうかの指定を求められます。デフォルトは、「いいえ」です。

5. ポリシーを構成するには「はい」、または「いいえ」を選択して、「次へ」をクリックします。次に例を示します。

   ポリシー・ドメインを使用する前に、WebGate および Access Server を関連付けてインストールする必要があります。ポリシー・ドメインの詳細は、『Oracle Access Manager アクセス管理ガイド』を参照してください。

   次のページで、Policy Manager の設定を完了するための指示が表示されます。

Policy Manager の設定の完了

データ・ディレクトリの保護ページには、ID システムのセキュリティを維持するために保護する必要がある Oracle Access Manager のディレクトリが表示されます。

- ブラウザからのアクセス、およびファイル・システムによってディレクトリにアクセスするネットワーク・ユーザーからのアクセスを制限する必要があります。ディレクトリを保護する方法に関する指示が必要な場合は、使用中の Web サーバーおよびオペレーティング・システムのドキュメントを参照してください。
- ポリシー・ドメイン内のアクセス・システムも保護できます。詳細は、『Oracle Access Manager アクセス管理ガイド』を参照してください。

画面上のページの後半部には、Oracle Access Manager ポリシー・ドメインの構成についての追加情報が表示されます。

Policy Manager の設定の完了の手順

1. 続行する前にページ上のすべての情報を読んでください。

   注意： Active Directory を使用する場合、続行する前に追加情報についてA-20 ページの「アクセス・システムのインストールと設定」を参照してください。

2. 次の順序で、Web サーバーおよび Identity Server のサービスを再起動します。
   a. Policy Manager と同じ WebPass の Web サーバー・インスタンスを停止します。
   b. WebPass の Identity Server サービスを停止して再起動します。
   c. WebPass/Policy Manager の Web サーバー・インスタンスを再起動します。
3. Web サーバーの再起動の後、「完了」をクリックします。

   Policy Manager のホームページが表示されます。
4. 次の情報を確認します。次の手順のいずれも実行できます。
   a. 7-16 ページの Policy Manager の設定の確認。
   b. 第 8 章「Access Server のインストール」。
   c. 『Oracle Access Manager アクセス管理ガイド』で説明されているように、設定中ディレクトリの保護ページに示されるディレクトリを保護します。

Policy Manager の設定の確認

ログインして、設定プロセス中に自動的に構成された認証スキームを確認することによって、Policy Manager の設定を容易に確認できます。また、『Oracle Access Manager アクセス管理ガイド』で説明されているように、アクセス・システム・コンソールの使用を開始して、Access Server インスタンスを設定し、その他の管理者を定義することもできます。

注意： Policy Manager のホームページが画面上に表示されている場合、手順 2 をスキップできます。

Policy Manager の設定の確認の手順

1. ブラウザからアクセス・システム・コンソールに移動します。次に例を示します。

   ```
   http://hostname:port/access/oblix
   ```

   ここで、*hostname* は Web サーバーをホストするマシン、*port* は WebPass の Web サーバー・インスタンスの HTTP ポート番号をそれぞれ指し、/access/oblix はアクセス・システム・コンソールに接続します。

2. 「アクセス・システム・コンソール」リンクを選択します。

3. マスター管理者権限を持つユーザーとしてログインします。

   アクセス・システム・コンソールが表示されます。

   トップ・ナビゲーション・バーのタブをクリックして、オプションのリストを表示できます。これは、画面上のページの左側に表示されます。たとえば、手順 4 を完了して、現在構成されている認証スキーマのリストを表示します。

4. 「アクセス・システム構成」タブを選択して、左列に表示される「認証管理」をクリックします。

   現在構成されている認証スキーマのリストが新規ページの本体に表示されます。スキーマの自動構成を選択しなかった場合、何もリストされません。

   この時点で、次を実行できます。

   - スキームに対応するリンクをクリックして認証スキームの構成詳細を表示すること。
   - サイド・ナビゲーション・バーの「Access Server 構成」を選択して Access Server インスタンスを追加すること（これは Access Server のインストールの前提条件です）。

     詳細は、8-6 ページの「Access Server のインストール」を参照してください。
   - アクセス・システム・コンソールおよび Policy Manager の内容表示を続行すること。

     たとえば、『Oracle Access Manager アクセス管理ガイド』で説明されているように、ポリシー・ドメインを定義または変更できます。Access Server または WebGate をインストールしていない場合でも、これらを定義する機能に影響はありません。これらのコンポーネントをインストールした後は、ポリシー・ドメインに影響を与えます。
   - サイド・ナビゲーション・バーの「ログアウト」を選択してログアウトすること。

     詳細は、『Oracle Access Manager アクセス管理ガイド』を参照してください。
   - Access Server のインストール。

     詳細は、第 8 章「Access Server のインストール」を参照してください。

8

Access Server のインストール

この章では、Access Server をインストールする方法について説明します。Access Server は、2 番目にインストールする必要があるアクセス・システム・コンポーネントです。次の項目を参照してください。

- Access Server およびインストールの概要
- Access Server の前提条件チェックリスト
- システム・コンソールでの Access Server インスタンスの作成
- Access Server のインストール

以前のバージョンを 10*g*（10.1.4.0.1）にアップグレードする方法は、『Oracle Access Manager アップグレード・ガイド』で説明しています。Oracle Access Manager コンポーネントの概要は、『Oracle Access Manager 概要』の概要の項を参照してください。

Access Server およびインストールの概要

Access Server は、Web ベースと Web 以外の両方のリソースおよびアプリケーションに動的なポリシー評価サービスを提供するスタンドアロン・コンポーネントです。Access Server は、アクセス・クライアント（WebGate またはカスタム AccessGate）からリクエストを受信し、LDAP ディレクトリに認証、認可および監査ルールを問い合せ、資格証明の検証、ユーザーの認可および Oracle Access Manager のユーザー・セッションの管理を行います。詳細は、『Oracle Access Manager 概要』を参照してください。

Access Server をインストールする前に、アクセス・システム・コンソールで Access Server 用のインスタンスを作成する必要があります。

タスクの概要 : インスタンスの追加および Access Server のインストール

1. 8-5 ページの「システム・コンソールでの Access Server インスタンスの作成」で説明されているように、アクセス・システム・コンソールで Access Server インスタンスを作成します。
2. 8-6 ページの「Access Server のインストール」で説明されているように、Access Server をインストールします。
3. 必要に応じて、8-3 ページの「複数の Access Server のインストールの概要」で説明されているように、追加の Access Server をインストールします。
4. 8-3 ページの「アップグレードした環境への新規 Access Server の追加」で説明されているように、アップグレードした環境に新規 Access Server を追加し、globalparams.xml ファイルに適切なパラメータを手動で設定して、以前のプラグインとの下位互換性を確認します。

Access Server のインストールは、Identity Server のインストールと類似しています。このインストール中に、ディレクトリ・サーバー詳細を指定します。デフォルトのディレクトリ・プロファイルが、この Access Server について作成されます。デフォルトのプロファイルは、Access Server インスタンスの作成後に使用可能になります。完了したプロファイルは、インストール後に使用可能になります。Access Server のインストールに Web サーバーは関係しません。

Access Server には、次の 2 つのインストール・パッケージが用意されています。

Windows: Oracle_Access_Manager10_1_4_0_1_win32_Access_Server

UNIX: Oracle_Access_Manager10_1_4_0_1_sparc-s2_Access_Server

また、プラットフォーム固有のパッケージが使用可能であり、選択したプラットフォームまたはインストール・モードに関係なく、インストールは類似しています。情報は特定の時点で保存されます。Access Server がインストールされていることが通知された後でインストールを取り消す場合は、1-9 ページの「Oracle Access Manager の以前のリリースからのアップグレード」で説明されているように、コンポーネントをアンインストールする必要があります。通告はすべて確認されますが、使用中の環境に該当しない場合はスキップされることがあります。

詳細は、2-8 ページの「Access Server のガイドライン」を参照してください。

複数の Access Server のインストールの概要

フェイルオーバーおよびロード・バランシングに備えて、複数の Access Server をインストールすることをお薦めします。これを実行する手順は、1 つの Access Server をインストールする手順と類似しています。

タスクの概要 : 複数の Access Server のインストール

1. 8-5 ページの「システム・コンソールでの Access Server インスタンスの作成」で説明されているように、アクセス・システム・コンソールで各 Access Server インスタンスを作成します。

   注意 : 同一のディレクトリに複数の Access Server をインストールしないでください。

2. 8-6 ページの「Access Server のインストール」で説明されているように、Access Server をインストールし、Access Server ごとに異なるインストール・ディレクトリを指定します。

   第 15 章「コンポーネントのレプリケート」で説明されているように、オプション・ファイルを使用して既存のインストールをレプリケートできます。

3. 第 9 章「WebGate のインストール」で説明されているように、1 つ以上の AccessGate/WebGate をインストールし、それらに Access Server をプライマリ Access Server またはセカンダリ Access Server として割り当てます。

これらの機能を有効化する方法の詳細な指示は、『Oracle Access Manager アクセス管理ガイド』を参照してください。

アップグレードした環境への新規 Access Server の追加

10*g*（10.1.4.0.1）から、Access Server は UTF-8 エンコーディングを使用し、プラグイン・データには UTF-8 データが含まれます。以前のプラグインは、Latin-1 エンコーディングでデータを送受信します。

10*g*（10.1.4.0.1）よりも前のリリースでは、Cookie の暗号化および復号化は WebGate/AccessGate によって処理されました。ただし、現在は Cookie の暗号化および復号化は Access Server によって処理されます。

以前の Access Server を 10*g*（10.1.4.0.1）にアップグレードすると、新規パラメータ `"IsBackwardCompatible" Value="true"` が Access Server の globalparams.xml ファイルに自動的に設定されます。これによって下位互換性が提供され、Access Server は以前のカスタム認証および認可プラグインへの Latin-1 エンコーディングでのデータの送信（および受信）を継続できます（以前のカスタム・プラグインは、Latin-1 エンコーディングでデータを設定します）。また、Access Server は、Cookie の暗号化および復号化を継続する、以前の WebGate およびカスタム AccessGate との下位互換性を維持します。

ただし、アップグレードした環境に新規 10*g*（10.1.4.0.1）Access Server を追加する場合は、`"IsBackwardCompatible" Value="true"` を新規 Access Server の globalparams.xml ファイルに手動で設定して、以前のプラグインおよびインタフェース、以前の WebGate およびカスタム AccessGate との通信を有効にする必要があります。

アップグレードした環境への新規 Access Server の追加の手順

1. 『Oracle Access Manager アップグレード・ガイド』で説明されているように、環境をアップグレードします。
2. 8-3 ページの「複数の Access Server のインストールの概要」で詳細を確認します。
3. 8-5 ページの「システム・コンソールでの Access Server インスタンスの作成」のアクティビティを実行します。
4. 8-6 ページの「Access Server のインストール」で説明されているように、新規 Access Server を追加します。
5. *AccessServer_install_dir*¥access¥oblix¥apps¥common¥bin¥globalparams.xml にある新規 Access Server の globalparams.xml ファイルを検索して開きます。
6. `"IsBackwardCompatible" Value="true"` を設定します。たとえば、次のようにします。

```
<SimpleList>
     <NameValPair
           ParamName="IsBackwardCompatible"
            Value="true">
     </NameValPair>
</SimpleList>
```

7. ファイルを保存します。
8. Access Server サービスを再起動します。
9. 以前のプラグインおよび WebGate に下位互換性が必要であるかぎり、アップグレードした環境に追加する新規 Access Server ごとに繰り返します。

注意： すべてのプラグインおよび WebGate が正常にアップグレードされ、下位互換性が不要になった場合、すべての Access Server の globalparams.xml ファイルで `"IsBackwardCompatible" Value="false"` を手動で設定することをお薦めします。

詳細は、『Oracle Access Manager アップグレード・ガイド』の Access Server および下位互換性に関する項を参照してください。

Access Server の前提条件チェックリスト

Access Server のインストールを開始する前に、表 8-1 のタスクを完了していることを確認してください。すべての前提条件を満たさない場合、Oracle Access Manager のインストールに悪影響を及ぼすことがあります。

表 8-1 Access Server の前提条件チェックリスト

チェックリスト	Access Server の前提条件
	第 I 部「インストールの計画と前提条件」で説明されている、ユーザーの環境に適用される前提条件および要件がすべて満たされていることを確認する。
	第 II 部「ID システムのインストールおよび設定」のアクティビティをすべて完了する。
	第 7 章「Policy Manager のインストール」で説明されているように、Policy Manager をインストールおよび設定し、Policy Manager が動作していることを確認する。

システム・コンソールでの Access Server インスタンスの作成

Access Server をインストールする前に、Policy Manager およびアクセス・システム・コンソールで Access Server 用のインスタンスを作成する必要があります。これは、マスター管理者、または定義されている場合はマスター・アクセス管理者が実行できます。

インスタンスを作成するときに指定する Access Server ID は一意である必要があり、スペース、コロン（:）、番号記号（#）または英語以外のキーボードの文字は使用できません。Windows システムでは、この Access Server ID は NetPoint AAA Server を接頭辞として持つ Windows サービス名として使用されます。

Access Server インスタンスの作成の手順

1. アクセス・システム・コンソールにログインします。たとえば、次のようにします。

   `http://`*`hostname`*`:`*`port`*`/access/oblix`

   ここで、*hostname* は Web サーバーをホストするマシン、*port* は WebPass の Web サーバー・インスタンスの HTTP ポート番号をそれぞれ指し、/access/oblix はアクセス・システム・コンソールに接続します。

   アクセス・システムのメイン・ページが表示されます。

2. 「アクセス・システム・コンソール」リンクをクリックしてから、マスター管理者でログインします。

   アクセス・システム・コンソールのメイン・ページには、3 つのタブが上部にあり、機能の説明が中央にあります。

3. 「アクセス・システム構成」タブをクリックし、サイド・ナビゲーション・バーが表示されたら「Access Server 構成」をクリックします。

   これが最初の Access Server の場合、ディレクトリ・サーバー内に Access Server が検索されなかったことがメイン・ページから通知されます。それ以外の場合は、すでに追加されている Access Server が表示されます。

4. 「追加」ボタンをクリックすると、「新規 Access Server の追加」ページがいくつかのデフォルトとともに表示されます。

   インスタンスを作成するには、基本情報の入力のみが必要です。インストール後に、『Oracle Access Manager アクセス管理ガイド』で説明されているように、追加の構成を完了できます。オンライン・ヘルプも提供されます。

5. インストールする Access Server について、次のパラメータを指定します。たとえば、次のようにします。

   - **名前 :** このディレクトリ・サーバーですでに使用されている他の Access Server とは異なる Access Server を説明する名前。名前に、スペース、コロン（:）または番号記号（#）を使用しないでください。
   - **ホスト名 :** Access Server がインストールされるマシンの名前。Access Server には Web サーバー・インスタンスは必要ありません。
   - **ポート :** Access Server がリスニングするポート。
   - **トランスポート・セキュリティ :** すべての Access Server および関連 WebGate 間のトランスポート・セキュリティは一致している必要があります（すべてオープン、シンプルまたは証明書モード）。

6. 「保存」をクリックします。

   すべての Access Server のリスト・ページが、このインスタンスへのリンクとともに表示されます。

7. Access Server インスタンスへのリンクをクリックし、後で参照するために「詳細」ページを印刷して、ページの最下部にある「戻る」ボタンをクリックします。

8. インストールする追加の Access Server インスタンスごとに、手順 3 から手順 7 を繰り返します。

9. 「ログアウト」をクリックし、ブラウザ・ウィンドウを閉じて、「Access Server のインストール」に進みます。

Access Server のインストール

Access Server をインストールしながら、記入済のインストール準備ワークシートを参照します。Access Server ごとに、次の手順を完了する必要があります。

タスクの概要 : Access Server のインストールに含まれる手順

1. 8-6 ページの「インストールの開始」で説明されているように、インストール・メソッドを選択してプロセスを開始します。
2. 8-7 ページの「トランスポート・セキュリティ・モードの指定」で説明されているように、トランスポート・セキュリティ・モードを定義します。
3. 8-7 ページの「ディレクトリ・サーバー詳細および通信詳細の指定」で説明されているように、ディレクトリ・サーバー詳細を識別します。
4. 8-9 ページの「Access Server のインストールの終了」で説明されているように、プロセスを完了します。

インストールの開始

Access Server のインストール手順は、他の Oracle Access Manager コンポーネントで実行したインストール手順と類似しています。

注意 : Policy Manager と同じディレクトリに Access Server をインストールしないでください。同一のディレクトリに複数の Access Server をインストールしないでください。

Access Server のインストールの開始の手順

1. 管理者権限を持つユーザーとしてログインします。
2. Access Server インストーラ（インストールするアクセス・システム言語パックを含む）を検索します。
3. 選択したプラットフォームおよびインストール・メソッドの Access Server インストーラを起動します。

   例 :

   - **GUI メソッド**

     Windows: Oracle_Access_Manager10_1_4_0_1_Win32_Access_Server.exe

   - **コンソール・メソッド**

     Solaris: ./ Oracle_Access_Manager10_1_4_0_1_sparc-s2_Access_Server
4. 「次へ」をクリックして、「ようこそ」画面を閉じます。
5. プラットフォームに基づいて管理者権限に関する質問に応答します。次に例を示します。
6. インストール・ディレクトリを指定してから、「次へ」をクリックします。

   例 :

   ¥OracleAccessManager
7. **言語パック :** インストールするデフォルト・ロケールおよび他のロケールを選択してから、「次へ」をクリックします。

8. インストール・ディレクトリ名を記録してから、「次へ」をクリックします。

   数秒後、Access Server がインストールされます。Windows システムの場合、Microsoft 管理インタフェースが構成されるという通知が表示されます。

   トランスポート・セキュリティ・モードを指定するよう求められます。

トランスポート・セキュリティ・モードの指定

すべてのアクセス・システム・コンポーネント（Policy Manager、Access Server および関連 WebGate）間のトランスポート・セキュリティは一致している必要があります（すべてオープン、シンプルまたは証明書モード）。

トランスポート・セキュリティ・モードの指定の手順

1. トランスポート・セキュリティ・モード（「オープン」、「シンプル」または「証明書」）を選択します。
2. 「次へ」をクリックします。

   トランスポート・セキュリティの選択に関係なく、次にディレクトリ・サーバー詳細を指定するよう求められます。

ディレクトリ・サーバー詳細および通信詳細の指定

ここでは、ユーザーの環境、Oracle Access Manager の構成およびポリシー・データのディレクトリ・サーバーの詳細を指定するよう求められます。Oracle Access Manager は、ディレクトリ・サーバーに構成エントリを追加します。

ディレクトリ・サーバー詳細の指定の手順

1. 構成データのディレクトリ・サーバーについてリクエストされた情報を指定し、「次へ」をクリックします。
   - 「オープン」または「SSL」。
   - **ホスト・マシン :** 構成データのディレクトリ・サーバーの DNS ホスト名。
   - **ポート番号 :** 構成データのディレクトリ・サーバーがリスニングするポート（SSL 接続の場合、暗号化ポートを指定）。
   - **ルート DN:** 構成データのディレクトリ・サーバーのバインド DN。
   - **ルート・パスワード :** 構成データのディレクトリ・サーバーのバインド DN パスワード。
   - **構成ディレクトリ :** Oracle Access Manager 構成データのディレクトリ・サーバーのタイプ。たとえば、次のようにします。

     Sun
2. **SSL のみ :** SSL 証明書のパスを入力します。

   Oracle Access Manager ポリシー・データの格納場所を指定する必要があります。Oracle Access Manager 構成データと一緒に格納するか、個別のディレクトリ・サーバーに格納します。詳細は、2-22 ページの「データ記憶域の要件」を参照してください。

3. Oracle Access Manager のポリシー・データの格納場所を指定します。たとえば、次のようにします。

   構成ディレクトリ

   > **注意 :** ポリシー・データを個別に格納する場合、ポリシー・データのディレクトリ・サーバーの情報を指定する必要があります。構成 DN およびポリシー・ベースは一意である必要があります。詳細は、2-22 ページの「データ記憶域の要件」を参照してください。

   ここで、アクセス・システム・コンソールで指定した Access Server インスタンス ID と、構成 DN およびポリシー・ベースを指定するよう求められます。

4. リクエストされた詳細を入力してから、「次へ」をクリックします。たとえば、次のようにします。

   Access Server ID: *Access_Server_1014_A*

   構成 DN: o=*my-company*,c=us

   ポリシー・ベース : o=*my-company*,c=us

5. 以前に選択したトランスポート・セキュリティ・モードに従って、次の操作を実行します。

   - **オープン :** 8-9 ページの「Access Server のインストールの終了」にスキップします。
   - **シンプル :** 手順 6 に進みます。
   - **証明書 :** 証明書をリクエストするかインストールするかを指定し、「次へ」をクリックしてから、手順 6 に進みます。

6. 「パスフレーズ」を指定および確認し、パスワードをファイルに格納するよう求められたら「はい」（または「いいえ」）をクリックして、「次へ」をクリックします。

   > **注意 :** Windows で「いいえ」を選択した場合、Access Server を起動するたびに PEM 句を求められます。UNIX で「いいえ」を選択した場合、start_access_server スクリプトを起動するたびに、-P オプションを使用してパスワードを渡す必要があります。

7. **シンプル :** 8-9 ページの「Access Server のインストールの終了」にスキップします。

8. **証明書 :** 証明書リクエストおよびインストール手順を完了し、8-9 ページの「Access Server のインストールの終了」に進みます。

   > **注意 :** 証明書をリクエストして、このインストール中に準備されなかった場合は、証明書を ¥*AccessServer_install_dir*¥access¥oblix¥config ディレクトリにコピーして Access Server を再起動するまでは、Access Server を使用できません。

   Access Server が構成中であることが通知され、次に README の情報が表示されます。

Access Server のインストールの終了

README の情報には、ドキュメントおよびオラクル社の連絡先に関する詳細が記載されています。

Access Server のインストールの終了の手順

1. README の情報を確認してから、「次へ」をクリックして終了します。

   インストールが完了し、Access Server を起動する必要があることが通知されます。

2. 「終了」をクリックして、ウィザードを閉じます。

   Access Server を起動する必要があります。これによって、Access Server のインストールが成功したことが確認され、WebGate のインストールが準備されます。

3. Access Server を起動して、正常にインストールされて稼働していることを確認します。

   - **Windows:** アクセス・システム・コンソールで指定した Access Server ID が、サービス名（Oracle Access Manager 接頭辞を含む）として使用されます。
   - **UNIX:** /*AccessServer_install_dir*/access/oblix/apps/common/bin ディレクトリに移動し、./start_access_server を実行します。

   注意： パスワード・ファイルを使用しないインストールの場合、Access Server をローカルで起動する必要があります。これを（NetMeeting などの端末エミュレータや Windows 2000 のリモート・サービス再起動によって）リモートで行おうとすると、失敗します。

次の作業は、ユーザーの環境によって異なります。

- この章で説明されているように、Access Server を追加します。
- A-17 ページの「ADSI の設定（オプション）」で説明されているように、ADSI を設定します。
- 第 9 章「WebGate のインストール」で説明されているように、WebGate をインストールします。

9

WebGate のインストール

この章では、WebGate のインストール方法および WebGate を構成して Web サーバーと連動させる方法について説明します。ここでは、次の項目について説明します。

- WebGate のインストールの概要
- WebGate の前提条件チェックリスト
- WebGate インスタンスの作成
- WebGate および Access Server の関連付け
- WebGate のインストール
- Web サーバーの手動構成
- IIS WebGate のインストールの完了
- httpd.conf 更新の完了
- WebGate のインストールの確認

10*g*（10.1.4.0.1）にアップグレードする方法は、『Oracle Access Manager アップグレード・ガイド』で説明されています。Oracle Access Manager コンポーネントの概要は、『Oracle Access Manager 概要』の概要の項を参照してください。

WebGate のインストールの概要

WebGate は、Oracle Access Manager に同梱された、すぐに使用可能な Web サーバー・プラグインです。WebGate は、Web リソースのユーザーからの HTTP リクエストを捕捉して、これらを認証および認可するための Access Server に転送します。AccessGate は、Web リソースおよび Web 以外のリソースのリクエストを処理する Oracle Access Manager アクセス・クライアントであり、Software Developer Kit を使用して開発されています。AccessGate および WebGate という用語は、同じ意味で使用されることがあります。WebGate をインストールする前に、WebGate を Access Server に関連付ける必要があります。

タスクの概要 : インスタンスの追加および WebGate のインストール

1. 9-3 ページの「WebGate インスタンスの作成」で説明されているように、インスタンスを作成します。
2. 9-4 ページの「WebGate および Access Server の関連付け」で説明されているように、インスタンスを関連付けます。
3. 9-5 ページの「WebGate のインストール」で説明されているように、WebGate をインストールします。
4. 必要に応じて、次の手順を完了します。
   - Web サーバーの手動構成（インストール時に自動的に構成されなかった場合）
   - IIS WebGate のインストールの完了（必要な場合）
   - httpd.conf 更新の完了（必要な場合）
5. 9-15 ページの「WebGate のインストールの確認」により終了します。これは適切な方法です。

WebGate のインストールは、WebPass のインストールと類似しています。指定するディレクトリ・サーバー詳細はなく、WebGate の Web サーバー構成を更新する必要があります。

様々なプラットフォーム上の WebGate に対して、個別の Web サーバー固有のインストール・パッケージが提供されています。必ず環境にあわせたパッケージを選択してください。

正常なインストールのためには、すべての手順を完了する必要があります。情報は、インストール・プロセス中の特定の時点で保存されます。WebGate がインストールされていることが通知された後でインストールを取り消す場合は、1-9 ページの「Oracle Access Manager の以前のリリースからのアップグレード」で説明されているように、コンポーネントをアンインストールする必要があります。通告はすべて確認されますが、使用中の環境に該当しない場合はスキップされることがあります。

詳細は、2-8 ページの「WebGate のガイドライン」を参照してください。

複数の WebGate のインストールの概要

フェイルオーバーおよびロード・バランシングに備えて、複数の WebGate をインストールすることをお薦めします。第 15 章「コンポーネントのレプリケート」で説明されているように、クローニング機能を使用して複数システム上のインストールを容易にすることをお薦めします。

複数の WebGate のインストールは、この章で説明されている手順と同じ手順に従います。

WebGate の前提条件チェックリスト

WebGate のインストールを開始する前に、表 9-1 のタスクを完了していることを確認してください。すべての前提条件を満たさない場合、Oracle Access Manager のインストールに悪影響を及ぼすことがあります。

表 9-1 WebGate の前提条件チェックリスト

チェックリスト	WebGate の前提条件
	第 I 部「インストールの計画と前提条件」で説明されている、ユーザーの環境に適用される前提条件および要件がすべて満たされていることを確認する。
	第 II 部「ID システムのインストールおよび設定」のアクティビティをすべて完了する。
	第 7 章「Policy Manager のインストール」で説明されているように、Policy Manager をインストールおよび設定し、Policy Manager が動作していることを確認する。
	第 8 章「Access Server のインストール」で説明されているように、Access Server をインストールおよび設定し、Access Server が動作していることを確認する。

WebGate インスタンスの作成

AccessGate または WebGate をインストールする前に、アクセス・システム・コンソールを使用して新規の WebGate インスタンスを定義する必要があります。アクセス・システム・コンソールで指定する WebGate ID は、一意である必要があり、スペース、コロン（:）、番号記号（#）または英語以外のキーボードの文字は使用できません。

アクセス・システム・コンソールでの WebGate インスタンスの定義の手順

1. アクセス・システム・コンソールに移動します。次に例を示します。

   ```
   http://hostname:port/access/oblix
   ```

   ここで、*hostname* は Web サーバーをホストするマシン、port は WebPass の Web サーバー・インスタンスの HTTP ポート番号をそれぞれ指し、/access/oblix はアクセス・システム・コンソールに接続します。

   アクセス・システムのメイン・ページが表示されます。

2. 「アクセス・システム・コンソール」リンクをクリックしてから、マスター管理者でログインします。

   アクセス・システム・コンソールのメイン・ページが表示されます。

3. 「アクセス・システム構成」をクリックしてから、「新規 Access Gate の追加」を選択します。

4. WebGate（AccessGate）に次のパラメータを指定して、「保存」をクリックします。

   - **AccessGate 名 :** この WebGate/AccessGate を説明する一意の名前。名前にスペースを使用しないでください。
   - **説明 :** オプション。後で追加できます。大 / 小文字は区別されません。このフィールド内の情報の大文字使用を変更する場合、新しい情報を含めないかぎり受け入れられません。
   - **ホスト名 :** WebGate/AccessGate がインストールされるマシンの名前。
   - **ポート :** WebGate の Web サーバーがリスニングするポート。詳細は、9-3 ページの「WebGate の前提条件チェックリスト」を参照してください。
   - **「Access Gate のパスワード」および「Access Gate のパスワードを再入力」:** トランスポート・セキュリティ・モードに関係なくコンポーネントを検証および識別するオプ

ションの一意のパスワード。各 WebGate インスタンスに対して異なるものを使用する必要があります。

- **トランスポート・セキュリティ :** Access Server および関連する WebGate の間のトランスポート・セキュリティのレベル。デフォルト値は、「オープン」です。詳細は、2-12 ページの「Oracle Access Manager コンポーネントの通信の保護」を参照してください。『Oracle Access Manager ID および共通管理ガイド』で説明されているように、後でモードを変更できます。
- **優先 HTTP ホスト :** ここで、このパラメータは、WebGate のインストールの前に必要です。保護された Web サーバーにユーザーがアクセスを試行した場合にホスト名がすべての HTTP リクエストに表示される方法を定義します。HTTP リクエストのホスト名は、ユーザーの HTTP リクエストで定義された方法に関係なく、このフィールドに入力した値に翻訳されます。

  優先ホスト機能により、ホスト識別子が「ホスト識別子」リストに含まれていない場合に誤って作成される可能性があるセキュリティ・ホールが回避されます。ただし、仮想 Web ホスティングでは使用できません。仮想ホスティングの場合、ホスト識別子機能を使用する必要があります。詳細は、『Oracle Access Manager アクセス管理ガイド』を参照してください。

WebGate の詳細が表示され、Access Server または Access Server クラスタを AccessGate（WebGate）に関連付けるように求められます。このページの下部のボタンを使用して、仕様を変更すること、Access Server を一覧表示すること、または前のページに戻ることができます。

5. このページを印刷してから、「戻る」ボタンをクリックします。
6. 9-4 ページの「WebGate および Access Server の関連付け」に進みます。

WebGate および Access Server の関連付け

各 Access Server は、WebGate/AccessGate との関連付けで、プライマリ・サーバーまたはセカンダリ・サーバーとして機能します。このサーバーがこの WebGate に関連付けている唯一の Access Server である場合、このサーバーはプライマリ・サーバーになります。複数のプライマリ・サーバーは、リクエストの到達時に着信リクエストを共有します。セカンダリ・サーバーは、プライマリ・サーバーが停止中にのみアクティブになります。複数の Access Server がある場合、この WebGate に対して 1 つ以上のプライマリ Access Server を定義し、その他の Access Server をプライマリ・サーバーまたはセカンダリ・サーバーとして定義します。

接続数は、この WebGate が接続できる Access Server の数、および WebGate を介したリクエストに対する Access Server の相対的優先度を識別します。たとえば、2 つのプライマリ Access Server があり、最初のサーバーに 2 接続を、2 番目のサーバーに 1 接続を指定する場合、最初のサーバーは 2 番目のサーバーが 1 リクエストを受信するたびに 2 リクエストを受信します。デフォルトは 1 です。WebGate が 1 回に受信するリクエストの数は、「AccessGate 構成」ページの最大接続数パラメータにより制御されます。

注意 : 上の手順 5 から続けている場合、手順 1 をスキップできます。

WebGate への Access Server の割当ての手順

1. 「AccessGate の詳細」ページに移動します。必要に応じて、「アクセス・システム・コンソール」→「アクセス・システム構成」→「AccessGate 構成」→ *WebGate_Link* に移動します。

   この WebGate を個々の Access Server または Access Server のクラスタに関連付けることができます。クラスタの詳細は、『Oracle Access Manager アクセス管理ガイド』を参照してください。

2. 「AccessGate の詳細」ページで、ページ下部の「Access Server をリスト」（または「クラスタをリスト」）ボタンをクリックします。

   ページが表示され、現在この WebGate にはプライマリまたはセカンダリの Access Server が構成されていないことが示されます。

3. 「追加」ボタンをクリックして、「新規 Access Server の追加」ページに進みます。

4. 「サーバーの選択」リストから Access Server を選択して、優先度を指定し、この WebGate が接続できる Access Server（接続）の数を定義します。

   たとえば、次のようにします。

   サーバーの選択 : Your_Choice
   優先順位の選択 : Primary Server
   接続数 : 1

   必要な Access Server が一覧表示されていない場合、これを構成する必要がある場合があります。詳細は、8-5 ページの「システム・コンソールでの Access Server インスタンスの作成」を参照してください。

5. 「追加」ボタンをクリックして、関連付けを完了します。

   ページが表示され、この WebGate に関連付けられた Access Server がリストされます。

6. リンクをクリックしてサマリーを表示し、後で使用するためにこのページを印刷します。

7. 必要に応じて、手順 3 から手順 6 を繰り返して、別の WebGate および Access Server を関連付けます。

8. ログアウトして、9-5 ページの「WebGate のインストール」に進みます。

WebGate のインストール

WebGate インスタンスを作成し、これを Access Server に関連付けた後、WebGate をインストールできます。次の手順を完了しながら、記入済のインストール準備ワークシートを参照します。

タスクの概要 : WebGate のインストールに含まれる手順

1. 9-6 ページの「インストールの開始」
2. 9-7 ページの「トランスポート・セキュリティ・モードの指定」
3. 9-7 ページの「WebGate 構成詳細の指定」
4. 9-8 ページの「WebGate の Web サーバー構成の更新」
5. 9-9 ページの「WebGate のインストールの終了」

インストールの開始

WebGate のインストール手順は、他の Oracle Access Manager コンポーネントで実行したインストール手順と類似しています。

インストールの開始の手順

1. 管理者権限を持つユーザーとしてログインします。
2. 作成した一時ディレクトリで WebGate インストーラ（インストールするアクセス・システム言語パックを含む）を検索します。
3. 選択したプラットフォーム、インストール・モード、および Web サーバーの WebGate インストーラを起動します。たとえば、次のようにします。

   GUI メソッド

   Windows: Oracle_Access_Manager10_1_4_0_1_Win32_*API*_WebGate.exe

   コンソール・メソッド

   Solaris: ./ Oracle_Access_Manager10_1_4_0_1_sparc-s2_*API*_WebGate

   Linux: ./ Oracle_Access_Manager10_1_4_0_1_linux_*API*_WebGate

   ここで、*API* は、Web サーバーが使用する API を指します。たとえば、IIS Web サーバーの ISAPI などです。

   HP-UX および AIX システムの場合、-is:tempdir パス・パラメータを使用して、十分な領域のあるディレクトリにインストールを送ることができます。パスは、十分な領域のあるファイル・システムへの絶対パスにしてください。
4. 「次へ」をクリックして、「ようこそ」画面を閉じます。
5. プラットフォームに基づいて管理者権限に関する質問に応答します。次に例を示します。
6. WebGate のインストール・ディレクトリを指定します。次に例を示します。

   ¥OracleAccessManager¥WebComponent¥
7. **言語パック :** インストールするデフォルト・ロケールおよびその他のロケールを選択してから、「次へ」をクリックします。次に例を示します。
8. まだ記録していない場合、準備ワークシートにインストール・ディレクトリ名を記入してから、「次へ」をクリックして続行します。

   数秒後、WebGate がインストールされます。Windows システムの場合、Microsoft 管理インタフェースが構成されるという通知が表示されます。

   インストール・プロセスはまだ完了していません。トランスポート・セキュリティ・モードを指定するよう求められます。この時点で、戻って情報を再指定することはできません。

トランスポート・セキュリティ・モードの指定

すべてのアクセス・システム・コンポーネント（Policy Manager、Access Server および関連 WebGate）間のトランスポート・セキュリティは一致している必要があります（すべてオープン、シンプルまたは証明書モード）。

トランスポート・セキュリティ・モードの指定の手順

1. WebGate に対して、「オープン」、「シンプル」または「証明書」を選択します。
2. 「次へ」をクリックします。

   ここで、WebGate 構成詳細を指定するよう求められます。

WebGate 構成詳細の指定

次の手順を完了して、アクセス・システム・コンソールから印刷したページを参照することをお薦めします。この手順の間、WebGate および関連する Access Server の詳細を指定するよう求められます。

WebGate 構成詳細の指定の手順

1. アクセス・システム・コンソールで指定したように WebGate についてリクエストされた情報を指定します。
   - **WebGate ID:** アクセス・システム・コンソールで指定した一意の ID
   - **WebGate パスワード :** アクセス・システム・コンソールで定義したパスワード（パスワードを入力しなかった場合、フィールドを空白にします。）
   - **Access Server ID:** この WebGate に関連付けられた Access Server ID
   - **DNS ホスト名 :** この WebGate に関連付けられた Access Server 用
   - **ポート番号 :** この WebGate をリスニングする Access Server のポート番号

   注意 :「シンプル」トランスポート・セキュリティ・モードを指定した場合、グローバル・ネットワーク・プロトコルのパスフレーズの指定も求められます。「証明書」モードを指定した場合、パスワード・フレーズを求められます。
2. 「次へ」をクリックして続行します。
3. 以前に選択したトランスポート・セキュリティ・モードに従って、次の操作を実行します。
   - **「オープン」または「シンプル」:** 9-8 ページの「WebGate の Web サーバー構成の更新」にスキップします。
   - **証明書 :** 証明書の手順を完了し、9-8 ページの「WebGate の Web サーバー構成の更新」に進みます。

   証明書をリクエストし、このインストール中にまだ準備ができていない場合、¥*WebGate_install_dir*¥access¥oblix¥config ディレクトリに証明書をコピーして、これらの到達時に WebGate を再起動してください。

   警告 : WebGate の証明書リクエストにより、証明書リクエスト・ファイル aaa_req.pem が作成されます。この WebGate の証明書リクエストを、AAA server により信頼されたルート CA に送信する必要があります。ルート CA は、WebGate 証明書を返します。これは、WebGate のインストール中またはインストール後にインストールできます。

WebGate の Web サーバー構成の更新

Web サーバーは、WebGate と連動するように構成する必要があります。インストール中に、自動的に Web サーバー構成を更新することをお薦めします。ただし、自動および手動の更新の手順があります。

Web サーバー構成の自動更新の手順

1. Web サーバーを自動的に更新するには「はい」をクリックしてから、「次へ」をクリックします。
   - **ほとんどの Web サーバー :** Web サーバー構成ファイルを含むディレクトリの絶対パスを指定します。
   - **IIS Web サーバー :** プロセスが即時に開始され、プロセスには 1 分以上かかることがあります。

   Web サーバー構成が更新されたことを通知する画面が表示されます。
2. **Sun Web サーバー :** 続行する前に、Web サーバー管理コンソールで変更を適用します。
3. **IIS Web サーバー :** 続行する前に、実行する必要のある特別な指示を受信することがあります。

   注意 : NTFS をサポートするファイル・システムにインストールする場合にのみ、IIS WebGate では、/access ディレクトリに対する様々な権限の設定が必要です。最後のインストール・パネルには、FAT32 ファイル・システム上で設定できない様々な権限を手動で設定するための指示が表示されます。この場合、この指示は無視してください。

   ---

4. Web サーバーを停止および再起動して、構成の更新を有効化します。

   注意 : IIS Web サーバーを使用する場合、メタベースが破損しないように、WebGate のインストール後、`net stop iisadmin` および `net start w3svc` を使用することを検討してください。

   ---

5. 「次へ」をクリックして、9-9 ページの「WebGate のインストールの終了」に進みます。

Web サーバー構成の手動更新の手順

1. 自動更新を続行するかどうかの指定を求められた場合、「いいえ」をクリックしてから「次へ」をクリックします。

   新規画面とともに README の情報が表示され、WebGate の Web サーバーを手動で設定できます。
2. WebGate のインストール画面に戻り、「次へ」をクリックします。
3. 9-9 ページの「Web サーバーの手動構成」に進みます。

WebGate のインストールの終了

README の情報には、ドキュメントおよびオラクル社に関する詳細が記載されています。

WebGate のインストールの終了の手順

1. README の情報を確認してから、「次へ」をクリックして終了します。
2. 「終了」をクリックして、インストールを終了します。
3. Web サーバーをすぐに再起動するか、後で再起動します。

   IIS Web サーバーを使用する場合、メタベースが破損しないように、WebGate のインストール後、`net stop iisadmin` および `net start w3svc` を使用することを検討してください。
4. 必要に応じて、該当する手順に進みます。たとえば、次のようにします。
   - Web サーバーの手動構成（インストール時に自動的に構成されなかった場合）
   - IIS Web Server 上における postgate.dll のインストール
   - httpd.conf 更新の完了
5. 9-15 ページの「WebGate のインストールの確認」により終了します。

Web サーバーの手動構成

WebGate のインストール中に、Web サーバーのインストールを自動で更新するかどうかの指定を求められます。「いいえ」を選択した場合、これを手動で実行する必要があります。

注意： WebGate のインストール中に手動構成プロセスを起動した場合、次の手順の手順 1 をスキップできます。

WebGate の Web サーバーの手動構成の手順

1. Web ブラウザを起動し、必要に応じて次のファイルを開きます。次に例を示します。

   ¥*WebGate_install_dir*¥access¥oblix¥lang¥*langTag*¥docs¥config.htm

   ここで、¥*WebGate_install_dir* は、WebGate をインストールしたディレクトリです。
2. 次のサポートされている Web サーバーから選択します。
3. 表示される、各 Web サーバーのタイプに固有の指示にすべて従い、次を実行します。
   - Web Gate の設定中に変更する必要があるファイルのバックアップ・コピーを作成します。これは、再度 Web サーバーを設定する必要がある場合に使用できます。
   - 設定によっては、新しいブラウザ・ウィンドウが起動されます。または、情報を入力するためにコマンド・ウィンドウを起動する必要があります。このため、元の設定指示に戻ってすべてを実行し、該当する Oracle Access Manager ファイルを Web サーバーが認識できるようにします。

   注意： 誤ってウィンドウを閉じた場合、手順 1 に戻り、該当するリンクを再度クリックできます。

   ---
4. 必要に応じて、次の手順のいずれかに進みます。
   - IIS WebGate のインストールの完了
   - httpd.conf 更新の完了

IIS WebGate のインストールの完了

IIS 上で、クライアント証明書認証を使用する場合、WebGate のクライアント証明書を有効化する前に WebGate をホストする IIS Web サーバー上の SSL を有効化する必要があります。また、様々なフィルタが特定の順序でインストールされていることを確認する必要があります。さらに、postgate.dll を ISAPI フィルタとしてインストールする必要がある場合があります。

タスクの概要 : IIS WebGate のインストールの完了に含まれる手順

1. 9-10 ページの「IIS Web サーバー上の SSL の有効化」
2. 9-11 ページの「ISAPI フィルタの順序」
3. 9-11 ページの「IIS Web Server 上における postgate.dll のインストール」
4. 9-13 ページの「デフォルト・サイトが設定されていない場合の Web サイトの保護」

IIS Web サーバー上の SSL の有効化

次の手順をガイドとして使用します。これは IIS v5 用の手順です。

IIS Web サーバー上の SSL の有効化の手順

1. 必要に応じて、インターネット・インフォメーション・サービス・コンソールを開始します。「スタート」→「プログラム」→「管理ツール」→「インターネット・インフォメーション・サービス」をクリックします。
2. ローカル・コンピュータを開き、Web サイトを表示します。
3. デフォルトの Web サイトまたは該当する Web サイトを開いてから、¥access¥oblix¥apps¥webgate¥bin を開きます。
4. cert_authn.dll を右クリックして、「プロパティ」を選択します。
5. 「プロパティ」パネルの「ファイル セキュリティ」タブを選択します。
6. 「セキュアな通信」サブパネルで、「編集」をクリックします。
7. 「クライアント証明書認証」サブパネルで、「証明書の承認」を選択して「OK」をクリックします。
8. cert_authn.dll の「プロパティ」パネルで「OK」をクリックします。

設定中にクライアント証明書認証を選択する場合、ISAPI フィルタの 1 つとして cert_authn.dll も追加する必要があります。

ISAPI フィルタとしての cert_authn.dll の追加の手順

1. 必要に応じて、インターネット・インフォメーション・サービス・コンソールを開始します。「スタート」→「プログラム」→「管理ツール」→「インターネット・インフォメーション・サービス」をクリックします。
2. ローカル・コンピュータを開き、Web サイトを表示します。
3. 該当する Web サイトを右クリックして、「プロパティ」パネルを表示します。
4. 「ISAPI フィルタ」タブをクリックし、「追加」ボタンをクリックして「フィルタのプロパティ」パネルを表示します。
5. フィルタ名 cert_authn を入力します。
6. 「参照する」ボタンをクリックして、次のディレクトリに移動します。

   ¥*WebGate_install_dir*¥access¥oblix¥apps¥webgate¥bin
7. cert_authn.dll を実行可能ファイルとして選択します。
8. 「フィルタのプロパティ」パネルで「OK」をクリックします。
9. 「ISAPI フィルタ」パネルで「適用」をクリックします。

10. 「OK」をクリックします。
11. フィルタが正しい順序で一覧表示されていることを確認します。

ISAPI フィルタの順序

WebGate ISAPI フィルタが正しい順序で含まれていることを確認する必要があります。

WebGate ISAPI フィルタの順序付けの手順

1. 必要に応じて、インターネット・インフォメーション・サービス・コンソールを開始します。「スタート」→「プログラム」→「管理ツール」→「インターネット・インフォメーション・サービス」をクリックします。
2. ローカル・コンピュータを開き、Web サイトを表示します。
3. Web サイトを右クリックして、「プロパティ」を選択します。
4. 「プロパティ」をクリックして、ISAPI フィルタを選択します。
5. 次の .dll ファイルが表示されることを確認します。

   例 :

   cert_authn.dll
   webgate.dll
   oblixlock.dll
   transfilter.dll

6. 必要に応じて欠落したフィルタを追加し、フィルタ名を選択して、手順 5 で示すように上矢印および下矢印を使用してフィルタの順序を調整します。

警告 : 1 つの webgate.dll および 1 つの postgate.dll フィルタのみがあることを確認してください。

IIS Web Server 上における postgate.dll のインストール

WebGate のインストールに従い、postgate.dll を手動でインストールする必要がある場合があります。WebGate の拡張メソッド（WebGate がフォームのアクションの場合）の使用時、IIS Web サーバー上のフォーム・ログイン中のパススルーのために POST データが必要です。つまり、IIS Web サーバー上のフォーム認証スキームはパススルー・オプションにより構成され、ログイン・フォームのターゲットは、フォームによりポストされたデータを必要とし、WebGate 拡張メソッド（WebGate DLL がフォームのアクションの場合）は使用できません。そのかわり、WebGate のフィルタ・メソッド（フォームのアクションが WebGate DLL でない保護された URL の場合）を使用する必要があり、postdate DLL をインストールおよび有効化する必要があります。

POST データは、AzMan 許可プラグインのルール・パラメータを含む許可決定で使用されます。この場合、postgate.dll をインストールする必要があります。

次の手順は、IIS Web サーバーのコマンドを理解していることを前提としています。2 つの手順が用意されています。

- IIS Web サーバーの分離モードの設定
- ポストゲート ISAPI フィルタのインストール

IIS Web サーバーの分離モードの設定

IIS 6 Web サーバーの場合のみ、WWW サービスを IIS 5.0 分離モードで実行する必要があります。これは、ISAPI ポストゲート・フィルタで必要となります。

IIS 5.0 分離の IIS6 Web サーバーでの設定の手順

1. 必要に応じて、インターネット・インフォメーション・サービス・コンソールを開始します。「スタート」→「プログラム」→「管理ツール」→「インターネット・インフォメーション・サービス」をクリックします。
2. ローカル・コンピュータを開き、Web サイトを表示します。
3. Web サイトを右クリックして、「プロパティ」を選択します。
4. 「Web サイトのプロパティ」ウィンドウの「サービス」タブを選択します。
5. 「Run WWW service in IIS 5.0 Isolation Mode」の横のボックスを選択します。
6. 「OK」をクリックします。

ポストゲート ISAPI フィルタのインストール

1 台のマシン上で複数の WebGate のインストールを実行する場合、複数のバージョンの postgate.dll ファイルが作成され、異常な Oracle Access Manager の動作が発生する場合があります。

マシンの（上位の）Web サイト・レベルで構成できるのは、1 つの postgate.dll のみです。上位レベルの Web サイトとは異なるレベルで複数の webgate.dll を構成できます。ただし、これらは同一の postgate.dll を共有します。次の順序でフィルタをインストールしてください。

- ISAPI Webgate フィルタは、sspifitt フィルタの後、およびその他のフィルタの前にインストールする必要があります。
- 必要な場合にのみ、ポストゲート・フィルタは WebGate フィルタの前にインストールする必要があります。
- その他すべての Oracle Access Manager フィルタは最後にインストールできます。

注意： インストール前（またはアンインストール後）にフィルタを手動で削除する必要があります。複数のコピーのフィルタがインストールされている場合、このことは、新規フィルタのインストール前にこれらが手動で削除されなかったことを意味します。

次の手順は、ポストゲート ISAPI フィルタをインストールおよび配置する場合のガイドです。

ポストゲート ISAPI フィルタのインストールの手順

1. 必要に応じて、インターネット・インフォメーション・サービス・コンソールを開始します。「スタート」→「プログラム」→「管理ツール」→「インターネット・インフォメーション・サービス」をクリックします。
2. ローカル・コンピュータを開き、Web サイトを表示します。
3. Web サイトを右クリックして、「プロパティ」を選択します。
4. 「Web サイトのプロパティ」ウィンドウの「ISAPI フィルタ」タブを選択します。
5. 「追加」ボタンをクリックして、「フィルタのプロパティ」パネルを表示します。
6. フィルタ名 postgate を入力します。
7. 「参照する」ボタンをクリックして、次のディレクトリに移動します。

   ¥*WebGate_install_dir*¥access¥oblix¥apps¥webgate¥bin
8. postgate.dll を実行可能ファイルとして選択します。

9. 「フィルタのプロパティ」パネルで「OK」をクリックします。
10. 「ISAPI フィルタ」パネルで「適用」をクリックします。

IIS の再起動およびポストゲート ISAPI フィルタの位置の変更の手順

1. 必要に応じて、インターネット・インフォメーション・サービス・コンソールを開始します。
2. ローカル・コンピュータを右クリックして、「すべてのタスク」を選択し、「IIS を再起動」を選択します。
3. 「プロパティ」パネルの「ISAPI フィルタ」タブを選択します。
4. ポストゲート・フィルタを選択し、上矢印を使用して WebGate の上に移動します。

   例 :

   postgate.dll
   webgate.dll
   oblixlock.dll
5. IIS を再起動するか、次の「デフォルト・サイトが設定されていない場合の Web サイトの保護」に進みます。

注意 : メタベースが破損しないように、`net stop iisadmin` および `net start w3svc` を使用することを検討してください。

デフォルト・サイトが設定されていない場合の Web サイトの保護

「デフォルトの Web サイト」が構成されていない IIS Web サーバー上に WebGate をインストールする場合、インストーラは「仮想ディレクトリ→アクセス」を作成しません。これは、次の手順を使用して手動で実行する必要があります。

Web サイト（デフォルト・サイトではない）の保護の手順

1. 必要に応じて、インターネット・インフォメーション・サービス・コンソールを開始します。
2. 保護する Web サイトの名前を選択します。
3. 保護する Web サイトの名前を右クリックして、メニューの「新規」→「仮想ディレクトリ」を選択します。
4. 「次へ」をクリックします。
5. 「別名」access を選択して、「次へ」をクリックします。
6. ディレクトリ : /access ディレクトリへの完全パスを入力してから、「次へ」をクリックします。
7. 「読み取り」、「スクリプトの実行」、および「実行」を選択してから、「次へ」をクリックします。
8. 「終了」をクリックします。
9. IIS を再起動します。たとえば、次のようにします。

   「スタート」を選択して「実行」を選択します。
   `net start w3svc` と入力します。
   「OK」をクリックします。

httpd.conf 更新の完了

WebGate のインストールの終了および自動 Web サーバー更新の完了後に、次の手順を完了して、Apache httpd.conf ファイルを更新する必要があります。

httpd.conf の WebGate セクションの更新の手順

1. 更新された httpd.conf ファイルを WebGate のホスト・マシンで探します。
2. httpd.conf ファイルの WebGate をロードするセクションが次のように表示されることを確認してください（ユーザーの環境により、例とは異なることがあります）。次に例を示します。

```
#*** BEGIN WEBGATE SPECIFIC ****
# The path to this library may need to be changed to suit your installation
LoadFile
"/home/usr/sparc-s2/obdevsun1_wp_apache/identity/oblix/lib/libgcc_s.so.1"
LoadFile
"/home/usr/sparc-s2/obdevsun1_wp_apache/identity/oblix/lib/libstdc++.so.5"
<IfModule mod_ssl.c>
ObWebGateInstalldir
"/home/usr/sparc-s2/obdevsun1_wp_apache/identity"
ObWebGateMode PEER
Obwebgateload obWebgateModule
"/home/usr/sparc-s2/obdevsun1_wp_apache/identity/oblix/apps/webgate/bin/webgatessl.
so"
</IfModule>
<IfModule !mod_ssl.c>
ObWebGateInstalldir
"/home/usr/sparc-s2/obdevsun1_wp_apache/identity"
ObWebGateMode PEER
Obwebgateload obWebgateModule
"/home/usr/sparc-s2/obdevsun1_wp_apache/identity/oblix/apps/webgate/bin/webgate.so"
</IfModule>
<Location /access/oblix/apps/webgate/bin/webgate.cgi>
SetHandler obwebgateerr
</Location>
<Location "/oberr.cgi">
SetHandler obwebgateerr
</Location>
<LocationMatch "/*">
AuthType Oblix
require valid-user
</LocationMatch>
#*** END Oblix NetPoint Specific ****
```

3. chmod -r username:groupname ディレクトリ / ファイルを使用して、ディレクトリまたはファイルのユーザー名およびグループ名を変更します。

   このとき、httpd.conf ファイルの User パラメータと Group パラメータも同様に変更する必要があります。

詳細は、次を参照してください。

- 第 16 章「Apache v1.3 Web サーバーおよび Oracle HTTP Server Web サーバーの構成」
- 第 17 章「Oracle Access Manager のための Apache v2、IHS および OHS Web サーバーの構成」

WebGate のインストールの確認

WebGate のインストールおよび Web サーバーの更新の後、WebGate の診断を有効化して WebGate が正しく実行されていることを確認できます。

WebGate の診断の有効化の手順

1. Identity Server、WebPass の Web サーバー、および Access Server が実行されていることを確認します。
2. WebGate の診断用に次の URL を指定します。次に例を示します。

   ほとんどの Web サーバー : http(s)://*hostname*:*port*/access/oblix/apps/webgate/bin/webgate.cgi?progid=1

   IIS Web サーバー : http(s)://*hostname*:*port*/access/oblix/apps/webgate/bin/webgate.dll?progid=1

   ここで、*hostname* は、WebGate をホストするマシンの名前を、*port* は、Web サーバーのインスタンスのポート番号を表します。

WebGate の診断ページが表示されます。このページが開かない場合、WebGate は正しく機能していないため、アンインストールおよび再インストールする必要があります。

この時点で、次を実行できます。

- 『Oracle Access Manager ID および共通管理ガイド』および『Oracle Access Manager アクセス管理ガイド』で説明されている Oracle Access Manager の構成
- 『Oracle Access Manager カスタマイズ・ガイド』で説明されている Oracle Access Manager のカスタマイズ
- 『Oracle Access Manager 統合ガイド』で説明されているサード・パーティ製品の統合

第 IV 部

オプションのコンポーネントのインストール

ここでは、その他のオプションのコンポーネントを正常にインストールするために必要なすべての情報について説明します。

第 V 部は、次の章で構成されます。

- 第 10 章「Oracle Virtual Directory を使用した Oracle Access Manager の設定」
- 第 11 章「SNMP エージェントのインストール」
- 第 12 章「言語パックの個別インストール」
- 第 13 章「データベースの監査コンポーネントのインストール概要」
- 第 14 章「Software Developer Kit の概要」

10

Oracle Virtual Directory を使用した Oracle Access Manager の設定

この章では、Oracle Virtual Directory を使用して Oracle Access Manager を実装し、Data Anywhere を有効化する方法に焦点を当てます。ここでは、次の項目について説明します。

Oracle Access Manager と Oracle Virtual Directory の実装では、Oracle Virtual Directory の機能のサブセットのみが使用されます。このため、この章で説明する Oracle Access Manager 固有の構成に、Oracle Virtual Directory のドキュメントに記載されているすべての情報が適用されるわけではありません。

この章は、次のマニュアルとともに使用する必要があります。

- 『Oracle Virtual Directory and Virtual Directory Manager Installation Guide』
- 『Oracle Virtual Directory 製品マニュアル』

Oracle Virtual Directory を使用した Oracle Access Manager 実装の概要

Oracle Virtual Directory は、複数のデータ・ソースのユーザー・データを結合し、集約された仮想ディレクトリを作成します。

Oracle Access Manager アプリケーションからは、仮想ディレクトリはその他の LDAP ディレクトリと同じように動作しているように見えます。また、通常、Oracle Access Manager ユーザーには、Oracle Access Manager によって取得されたデータが異機種間ソースのものであると明白に示されることはありません。

ターゲット・データ・ストアの所有者から見ると、Oracle Virtual Directory の影響はほとんどありません。つまり、データ・ストアの所有者がデータの所有権を放棄することもなく、Oracle Virtual Directory がネイティブ・データ構造の形式を変更したり、元のデータのコピーを永続的に保持することもありません。

Oracle Access Manager の特定の機能を有効化するには、ターゲット LDAP ディレクトリのスキーマを拡張するか、仮想ディレクトリに含まれるプライマリ・データベース表に、Oracle Access Manager の補助ユーザー属性をシミュレートする列を追加する必要があります。詳細は、10-15 ページの「スキーマ拡張の概要」を参照してください。

注意： Oracle Virtual Directory を使用した Oracle Access Manager 実装は、ユーザー・プロファイルおよびグループ・リポジトリとともに使用することを目的としています。ただし、この実装は、ポリシー・ルールやワークフローなどの Oracle Access Manager のメタデータはサポートしていません。このメタデータは、公認の LDAPv3 ディレクトリ（Oracle Internet Directory、Sun または Microsoft Active Directory など）に格納する必要があります。

主な用語と機能

Oracle Access Manager と Oracle Virtual Directory の実装に関わる論点を正確に説明するために、このドキュメントでは、次の用語を非常に特殊な意味で使用します。

用語

仮想ディレクトリ : 複数のソースから取り出されたユーザー・データを表す論理的な集約ディレクトリで、これらすべてのデータが、顧客が定義したスキーマが一律に適用されている標準 LDAP ディレクトリから発生したかのように見えます。Oracle Access Manager 実装の趣旨上、Oracle Virtual Directory ではネイティブ・データ・ソースの範囲外でユーザー・プロファイルの永続的なコピーは作成されません。むしろ、Oracle Virtual Directory は、各ユーザー・プロファイルを Oracle Access Manager アプリケーションがリクエストしたとおりに取得および変換します。

仮想ディレクトリは、1 つの連続した検索ベースとして、または複数の非結合検索ベースとして構成できます。詳細は、10-5 ページの「検索ベースのオプションの概要」を参照してください。

スーパー・ディレクトリ : ネームスペース・マッピングを容易にするための特別なタイプの仮想ディレクトリです。このディレクトリには、フェデレートされた LDAP ディレクトリ、RDBMS データベースおよび埋込み仮想データ・ソースの組合せを含めることができます。埋込み仮想データ・ソースは、分割プロファイル、ネイティブ RDBMS 結合およびネイティブ RDBMS ビューになります。複数のデータ・ストアから集約される 1 つの連続した検索ベースを作成するためにサポートされている唯一の方法であるスーパー・ディレクトリは、Oracle Virtual Directory ローカル・ストア・アダプタを使用して Oracle Access Manager に接続します。

フェデレーション : Oracle Access Manager から Oracle Virtual Directory を介して参照する仮想ディレクトリのデータ・ソースを認識できるようにする方法です。特定のユーザー・プロファイルに関するデータはすべて、LDAP ディレクトリ、単一表データベースまたは埋込み仮想データ・ソースなどの 1 つのデータ・ストアから作成されます。

様々なユーザー・プロファイルが様々なフェデレーテッド・データ・ストアから作成されますが、これらのデータ・ストアには、次のタイプのデータ・ソースが組み合されています。

- 複数の異機種間 LDAP ディレクトリ
- すべてのユーザー・データを単一表に格納する複数のリレーショナル・データベース
- 次の 3 つのカテゴリに分けられる埋込み仮想データ・ソース
- ディレクトリとデータベースの組合せが含まれる分割プロファイル
- 複数のデータベース表が含まれるネイティブ RDBMS ビュー
- 複数のデータベース表が含まれるネイティブ RDBMS 結合

詳細は、10-4 ページの「フェデレーテッド・データ・ストア」を参照してください。

埋込み仮想データ・ソース : Oracle Virtual Directory がターゲット・データ・ストアとして認識する仮想オブジェクトであり、Oracle Access Manager から参照したり、仮想ディレクトリでフェデレートした後 Oracle Access Manager から参照できます。各埋込み仮想データ・ストアは、2 つ以上のターゲット・データ・ストアを集約します。埋込み仮想データ・ストアには、次の 3 つのタイプがあります。

- 分割プロファイル
- ネイティブ RDBMS 結合
- ネイティブ RDBMS ビュー

通常、埋込み仮想データ・ストアは認証および認可アクティビティのみに適しています。これは、これらのアクティビティにセカンダリ・データ・ソースが必ず含まれているためです。セカンダリ・データ・ソースは、一連の ID 管理アクティビティでは使用できない場合があります。

分割プロファイル : 複数のデータ・ソースから作成された特別なタイプの埋込み仮想データ・ソースです。分割プロファイルには、LDAP ディレクトリや複数のデータベース表を含む複数のソースから各ユーザーのユーザー・プロファイル属性が取り出されます。

各データ・ストアは、Oracle Virtual Directory 仮想ディレクトリにマップされるユーザー・プロファイル属性のセットを完成するために必要な属性の一部を提供します。これらの属性は、LDAP ディレクトリまたはデータベース表から取得できます。Oracle Access Manager のすべての操作をセカンダリ・ストア内の属性で実行できるとはかぎらないため、Oracle Access Manager のユーザー属性はすべて、プライマリ・データ・ストアに存在する必要があります。Oracle Access Manager は、Oracle Virtual Directory を介して分割プロファイルを標準 LDAP ディレクトリとして認識します。また、分割プロファイルは、仮想ディレクトリの一部としてフェデレートすることもできます。

詳細は、10-7 ページの「分割プロファイル」および 10-12 ページの図 10-8「Oracle Virtual Directory の実装レイヤー」を参照してください。

単一表データベース : 単一表データベースは、必ずしも 1 つの表のみを含むデータベースを指すのではなく、最上位の仮想ディレクトリにマップされるすべてのユーザー・プロファイル属性を 1 つの表のみに格納するデータベースを指します。

複数表データベース : 仮想ディレクトリにマップされるユーザー・プロファイル属性を 1 つ以上の表に格納するデータベースです。

仮想ディレクトリ・スキーマ : Oracle Access Manager が Oracle Virtual Directory を介して参照する最上位ディレクトリで使用するために顧客が開発するスキーマです。このスキーマは、Oracle Access Manager の属性を使用して拡張する必要があります。詳細は、10-17 ページの「仮想ディレクトリ・スキーマ」を参照してください。

必要に応じて、ターゲット・データ・ソースから取り出された顧客属性を使用して仮想ディレクトリ・スキーマをさらに拡張することもできます。詳細は、10-18 ページの「顧客スキーマ」を参照してください。

機能

仮想ディレクトリのテクノロジにより、次の 4 つの主要な機能について Oracle Access Manager の機能が拡張されます。

- フェデレーテッド・データ・ストア : 前述の 10-4 ページの「フェデレーテッド・データ・ストア」を参照してください。
- 分割プロファイル : 前述の 10-7 ページの「分割プロファイル」を参照してください。
- 集約ネームスペース : ターゲット・データ・ストアと埋込み仮想データ・ソースをスーパー・ディレクトリのノードにマップします。スーパー・ディレクトリを作成するには、ローカル・ストア・アダプタをインストールする必要があります。詳細は、10-8 ページの「集約ネームスペース」を参照してください。
- スキーマ・マッピング : 最上位の仮想ディレクトリの顧客が定義したスキーマに応じてすべてのターゲット・データ・ストアからデータを変換します。詳細は、10-9 ページの「集約スキーマ・マッピング」を参照してください。

仮想ディレクトリの一般的な利点に関する背景的な詳細は、『Oracle Virtual Directory 製品マニュアル』を参照してください。

フェデレーテッド・データ・ストア

Oracle Virtual Directory を使用すると、Oracle Access Manager ユーザーは、ユーザー・アカウントが一律に体系化された 1 つのデータ・ソースのものであるかのように、複数の異なるソースのユーザー・データにアクセスして操作できるようになります。ホスト・ディレクトリ・サーバーの各ベンダーが異なり、様々なスキーマが採用されていても、Oracle Virtual Directory は複数の LDAP ディレクトリからユーザー・データを取り込むことができます。図 10-1 は、Oracle Access Manager が複数の LDAP ディレクトリに接続する方法を示します。

図 10-1 フェデレーテッド LDAP ディレクトリがある Oracle Virtual Directory 実装

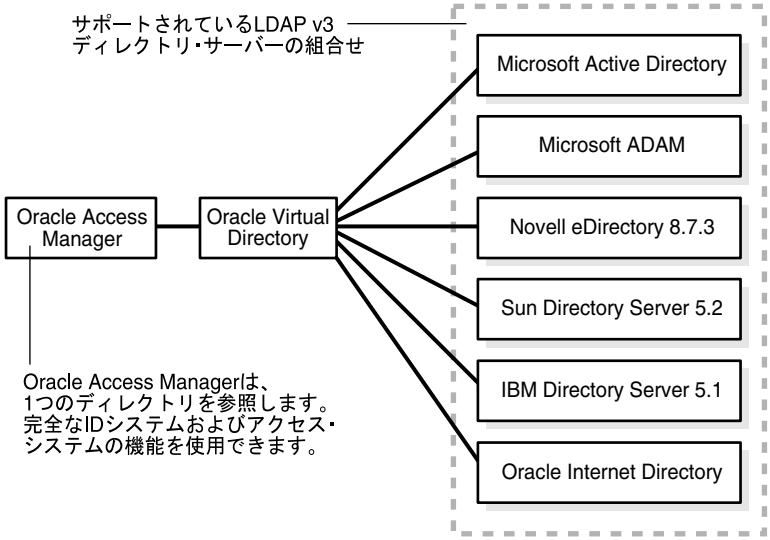


図 10-1 は、1 つのディレクトリ（Oracle Virtual Directory）を参照することにより、サポートされている LDAP v3 ディレクトリ・サーバー（Microsoft、Novell、Sun、Oracle Internet Directory および IBM）の組合せにアクセスしている Oracle Access Manager を示しています。

また、Oracle Virtual Directory 仮想ディレクトリには、すべてのユーザー・データを単一表に格納する RDBMS データベースを組み込むこともできます。複数の表にまたがるユーザー・データの統合の詳細は、10-22 ページの「分割プロファイル」を参照してください。

図 10-2 は、Oracle Access Manager が複数のリレーショナル・データベースに接続する方法を示しています。10-84 ページの「データベースの接続性に関するヒント」も参照してください。

図 10-2 フェデレーテッド RDBMS アプリケーションが含まれる Oracle Virtual Directory 実装

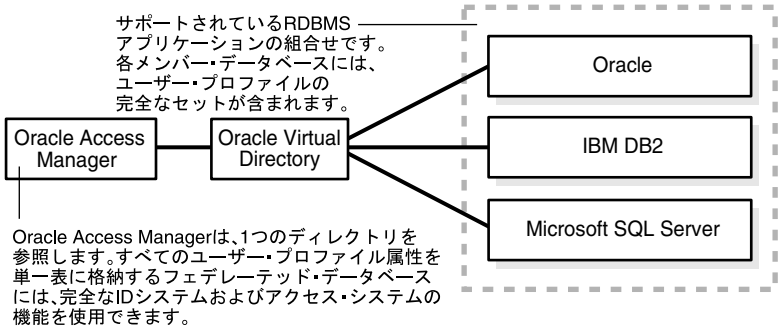


図 10-2 は、Oracle Virtual Directory ディレクトリを参照することにより、Oracle、IBM DB2 および Microsoft SQL Server RDBMS アプリケーションにアクセスしている Oracle Access Manager を示しています。すべてのユーザー・プロファイル属性を単一表に格納するフェデレーテッド・データベースには、完全な ID システムおよびアクセス・システムの機能を使用できます。各メンバー・データベースには、ユーザー・プロファイルの完全なセットが含まれます。

検索ベースのオプションの概要

Oracle Access Manager は、Oracle Virtual Directory を介してターゲット・データ・ストアをフェデレートするために 2 つのオプションをサポートしています。

- Oracle Virtual Directory の非結合検索ベース
- 統合検索ベース

非結合検索ベース : Oracle Access Manager が仮想ディレクトリ内の別個の非結合検索ベースとして各データ・ストアを参照できるように、Oracle Virtual Directory 実装を構成できます。このような構成の場合、ネームスペースは集約できません。また、各ターゲット・データ・ストアは異なる最上位のマッピング・アダプタの背後にあるため、すべてのデータ・ソースを対象としたグローバルなディレクトリ検索は実行できません。

図 10-3 は、非結合検索ベース用として構成された仮想ディレクトリを示しています。

図 10-3 非結合検索ベースが含まれる仮想ディレクトリ

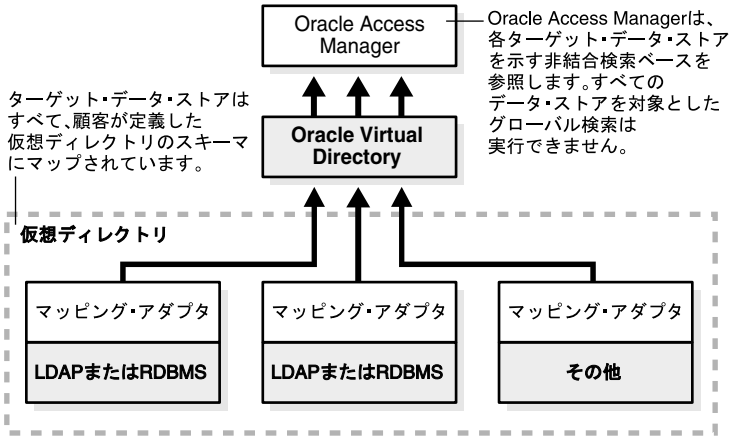


図 10-3 は、Oracle Virtual Directory 仮想ディレクトリにアクセスする Oracle Access Manager を示しています。仮想ディレクトリは、それぞれがマッピング・アダプタとその LDAP または RDBMS である一連のターゲット・データ・ストアで構成されています。ターゲット・データ・ストアはすべて、顧客が定義した仮想ディレクトリのスキーマにマップされています。Oracle Access Manager は、各ターゲット・データ・ストアを表す非結合検索ベースを参照します。すべてのデータ・ストアを対象としたグローバル検索は実行できません。

統合検索ベース : ローカル・ストア・アダプタを最上位にインストールし、ターゲット・データ・ストアをマップするノードを作成することにより、スーパー・ディレクトリを作成できます。このオプションにより、グローバルなディレクトリ検索と強力なネームスペース集約の両方が可能になります。

図 10-4 は、連続した統合検索ベースが含まれるスーパー・ディレクトリを示しています。

図 10-4 連続した統合検索ベースが含まれるスーパー・ディレクトリ

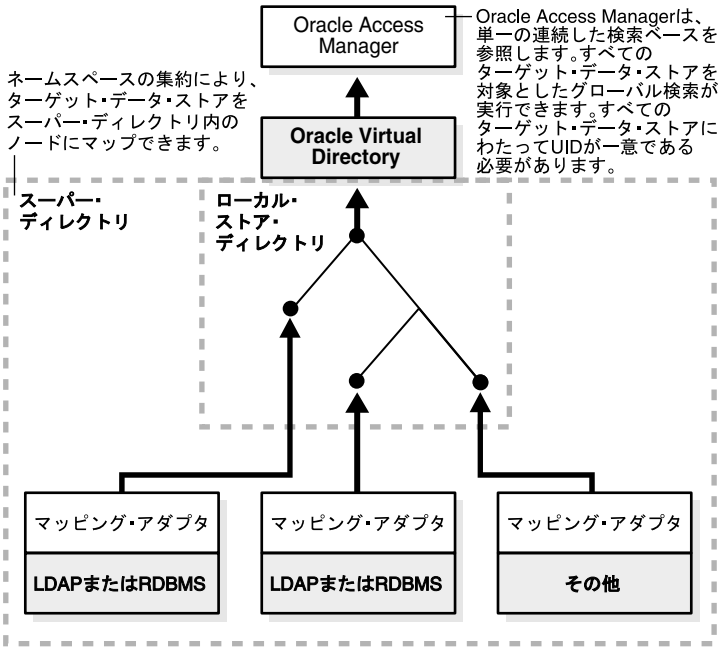


図 10-4 は、最上位にローカル・ストア・アダプタがあるスーパー・ディレクトリにアクセスする Oracle Access Manager を示しています。スーパー・ディレクトリの各ノードには、マッピング・アダプタと LDAP または RDBMS が含まれます。これらは、ローカル・ストア・アダプタを介して Oracle Virtual Directory にアクセスします。Oracle Access Manager は、すべてのターゲット・データ・ストアを対象としてグローバル検索を実行する単一の連続した検索ベースを参照します。この場合、すべてのターゲット・データ・ストアにわたって UID が一意である必要があります。

分割プロファイル

Oracle Virtual Directory を使用すると、Oracle Access Manager ユーザーはフェデレーテッド・データ・ストアにアクセスできるだけでなく、LDAP ディレクトリやリレーショナル・データベース表などの複数のデータ・ソースからユーザー・プロファイル属性が取り出された仮想分割プロファイル・データ・ソースにもアクセスできるようになります。

たとえば、情報技術によって保守される Active Directory アカウントにはユーザーのログイン・パスワードや会社電話番号などの属性を格納するとともに、人事管理によって保守されるリレーショナル・データベース・アカウントには自宅の電話番号や保健プランの加入情報などのその他の属性を格納することが可能です。

このように複数のデータ・ソースに属性を分散するとセカンダリ・データ・ストアで特定の ID 管理機能を実行できなくなるため、分割プロファイル構成は主に、認証および認可（アクセス・システム）操作に適しています。

図 10-5 は、分割プロファイルを含む単純な実装を示しています。

図 10-5 単純な分割プロファイルを対象とした Oracle Access Manager と Oracle Virtual Directory の実装

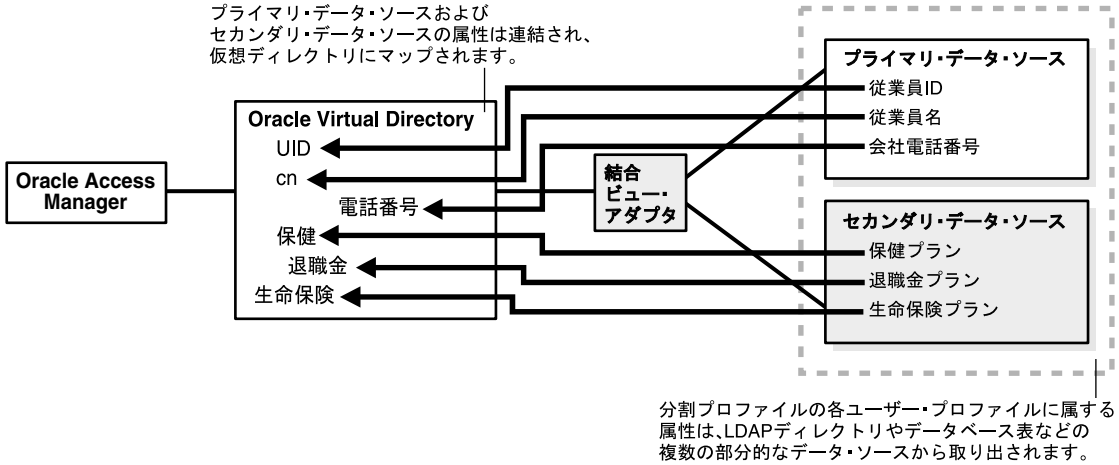


図 10-5 は、単純な分割プロファイルを示しています。Oracle Access Manager は Oracle Virtual Directory にアクセスし、Oracle Virtual Directory は結合ビュー・アダプタを使用してプライマリ・データ・ソースとセカンダリ・データ・ソースにアクセスしています。この例では、プライマリ・データ・ソースは従業員 ID、従業員名および会社電話番号を提供し、セカンダリ・データ・ソースは保健プラン、退職金プランおよび生命保険プランに関するデータを提供しています。これらの 6 つの属性が連結され、仮想ディレクトリにマップされています。

プライマリ・データ・ソースには Oracle Access Manager ユーザー・ブランチ・スキーマ属性が含まれ、セカンダリ・データ・ソースには通常、顧客属性が含まれます。

アクセス・システムおよび ID システム操作はすべて、プライマリ・データ・ソースの属性に対して実行できます。また、アクセス・システム操作はすべてセカンダリ・ソースのデータに対しても実行できますが、特定の ID システム操作はセカンダリ・データ・ストア内の属性に対して実行できません。

詳細は、10-10 ページの「実装の制限」を参照してください。

集約ネームスペース

スーパー・ディレクトリを作成する場合、ID 管理とポリシー管理上のニーズに最適のネームスペース階層を指定できます。この新しい階層は、仮想ディレクトリの構成データ・ストアによって使用されるネイティブ・ネームスペース階層とは異なる場合があります。

図 10-6 に示すように、属性を再編成して新しいレベルに割り当てることができます。

図 10-6 単純なスーパー・ディレクトリを対象としたネームスペースの集約

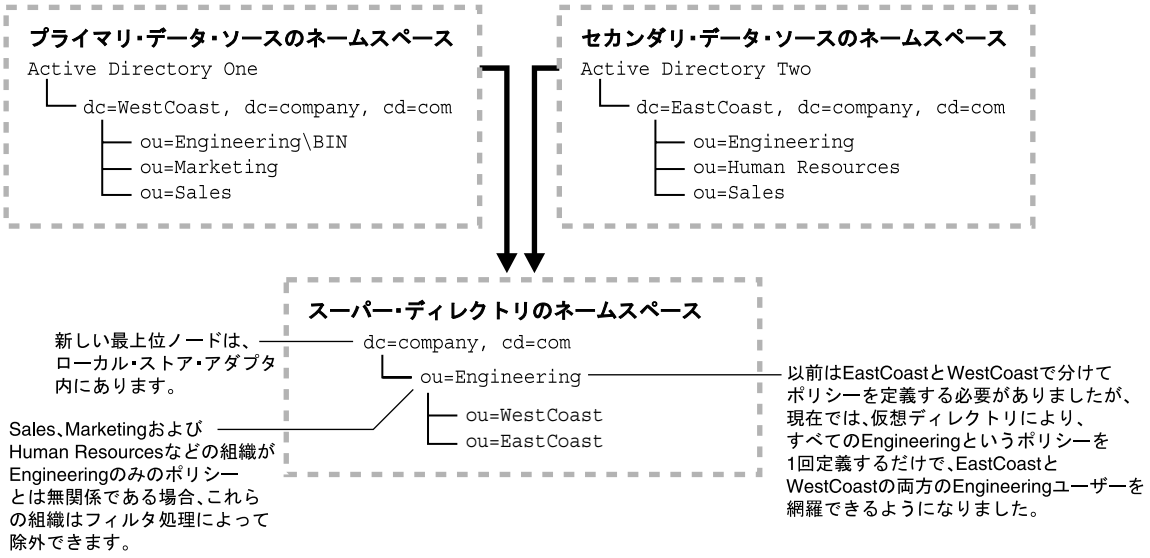


図 10-6 は、プライマリ・データ・ソースのネームスペースとセカンダリ・データ・ソースのネームスペースのデータにアクセスするスーパー・ディレクトリ・ネームスペースを示しています。この例では、プライマリ・データ・ソースのネームスペースには、WestCoast ノードの下に Engineering、Marketing および Sales 属性がある Active Directory One が含まれています。同様に、セカンダリ・データ・ソースのネームスペースには、EastCoast ノードの下に Engineering、Marketing および Sales 属性がある Active Directory Two が含まれています。スーパー・ディレクトリ・ネームスペースでは、company、Engineering、WestCoast または EastCoast の属性の順に属性が再編成されて割り当てられています。

この例では、Sales、Marketing および Human Resources などの組織が Engineering のみのポリシーとは無関係である場合、これらの組織はフィルタ処理によって除外できます。以前は、EastCoast または WestCoast で分けてポリシーを定義する必要がありました。しかし現在では、仮想ディレクトリにより、すべての Engineering というポリシーを 1 回定義するだけで、EastCoast または WestCoast の Engineering ユーザーを網羅できるようになりました。

集約スキーマ・マッピング

Oracle Virtual Directory 仮想ディレクトリを作成する場合、構成データ・ストアによって使用されるネイティブ・スキーマを、仮想ディレクトリによって使用されるスキーマにマップします。図 10-7 は、単純な Oracle Virtual Directory システムにおけるこのマッピングを示しています。

図 10-7 単純な仮想ディレクトリを対象とした集約スキーマ・マッピング

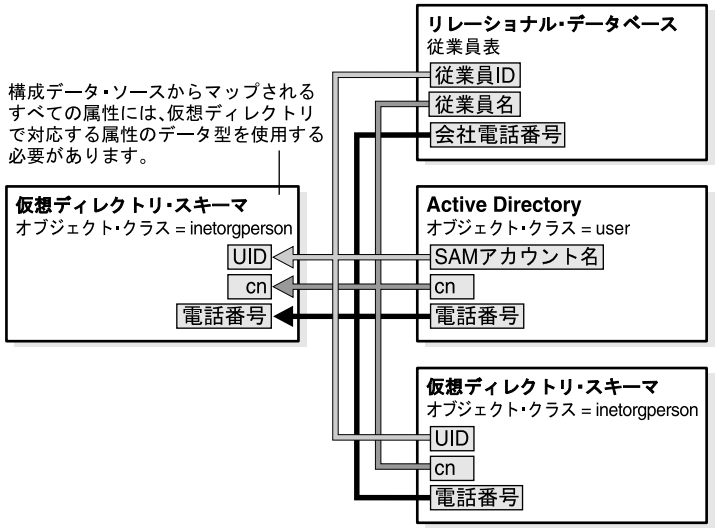


図 10-7 は、次のデータ・ソースに対する仮想ディレクトリ・スキーマ・マッピングを示しています。

- **リレーショナル・データベース :** 従業員 ID、従業員名および従業員の会社電話番号の各行がある従業員表です。
- **Active Directory:** SAM アカウント名、cn および電話番号の属性がある、user と呼ばれるオブジェクト・クラスです。
- **SunOne Directory Server:** UID（ユーザー ID）、cn および電話番号の属性がある、inetorgperson と呼ばれるオブジェクト・クラスです。

構成データ・ソースのすべての属性には、仮想ディレクトリで対応する属性のデータ型を使用する必要があります。たとえば、仮想ディレクトリ・スキーマの電話番号属性は、リレーショナル・データベースの従業員表の会社電話番号、Active Directory の user オブジェクト・クラスの電話番号、および SunOne Directory Server の inetorgperson オブジェクト・クラスの電話番号にマップされます。

実装の制限

Oracle Virtual Directory により、Oracle Access Manager の機能は複数の異機種間ディレクトリおよびデータベースに拡張されますが、これにはいくつかの制限があります。Oracle Virtual Directory を使用して Oracle Access Manager をデプロイする場合、このドキュメントに記載されている制限事項に注意する必要があります。表 10-1 は、制限の対象となる仮想ディレクトリ構成をまとめたもので、これらの問題に関する詳細な説明を示しています。

表 10-1 仮想ディレクトリ構成における Oracle Access Manager の機能の可用性

データ・ソース		Oracle Access Manager の機能の可用性
	アクセス・システム	ID システム
フェデレーテッド LDAP ディレクトリ	完全	完全
フェデレーテッド単一表データベース	完全	完全
フェデレーテッド複数表データベース（ネイティブ RDBMS 結合機能を使用）	完全	プライマリ・データ・ストアに対しては完全な機能を使用できる。ネイティブ RDBMS 結合機能がサポートしている場合、セカンダリ・データ・ストアに対して追加、変更および削除機能を使用することもできる。
フェデレーテッド複数表データベース（ネイティブ RDBMS ビュー機能を使用）	完全	プライマリ・データ・ストアに対しては完全な機能を使用できるが、セカンダリ・データ・ストアに対して追加および削除機能は使用できない。（セカンダリ・データ・ストアに対して変更機能は使用できる。）
分割プロファイル・ディレクトリ（Oracle Virtual Directory の結合ビュー・アダプタを使用）	完全	プライマリ・データ・ストアに対しては完全な機能を使用できるが、セカンダリ・データ・ストアに対して追加、変更および削除機能は使用できない。

詳細は、次を参照してください。

- 多値属性の制限の概要
- 埋込み仮想データ・ソースの制限の概要
- データベースの接続性に関するヒント

多値属性の制限の概要

標準 LDAP ディレクトリに格納されている個々の属性には、複数の値を使用できます。たとえば、各ユーザーのパスワード履歴を記録したり、LDAP ディレクトリに格納されているユーザー・アカウントに複数のサブスクリプションを割り当てることが可能です。

それに対して、SQL 準拠の RDBMS アプリケーションで正しく正規化されたデータ表では、1 つの表内の同じユーザー属性に複数の値は格納できません。このため、データベース表が含まれる Oracle Access Manager と Oracle Virtual Directory の実装では、多値属性に関する機能のサポートは制限されています。詳細は、オラクル社カスタマ・ケアにお問い合せください。

注意： 仮想ディレクトリに LDAP ディレクトリのみが組み込まれている場合、多値属性に関する制限は適用されません。

仮想ディレクトリに組み込むすべてのデータベース表に単一値属性のみが含まれるかぎり、多くの場合、既存の RDBMS データベースにすでに格納されているユーザー・プロファイルが完全に単一値属性を使用して実装されているため、制限は適用されません。

まれなケースとして、正規化されていない RDBMS データ・ストアで多値属性を使用してユーザー・アカウントが実装されている場合、User Manager および Group Manager 操作に関する次の制限に注意すれば、多値属性が含まれるサポート対象外の表を仮想ディレクトリに組み込むことができます。

- パスワード履歴機能はサポートされません。
- グループごとに複数の管理者は構成できません。
- グループごとに複数のサブスクリプションは構成できません。
- グループのサブスクリプション通知と登録解除通知のどちらかをアクティブにできますが、両方を同時にアクティブにはできません。
- グループごとに複数の動的フィルタは構成できません。
- グループごとに複数のグループ・タイプは構成できません。
- グループごとに複数のサブスクリプション・タイプは構成できません（使用可能なタイプ：「オープン」、「閉じる」、「フィルタでオープン」および「ワークフロー経由で制御」）。
- 仮想ディレクトリのデータベース表には複数の多値属性を含めることはできません。
- 仮想ディレクトリ用として新しいデータ・ストアを作成する場合、可能であれば必ず LDAP ディレクトリを使用することをお薦めします。これは、リレーショナル・データベースが多値属性を処理する能力が制限されているため、ID 管理アプリケーションで使用可能な機能が制限されるためです。リレーショナル・データベースに格納されている既存のユーザー・データを処理する場合は、仮想ディレクトリ内での多値属性の処理に関する制限を十分に把握しておいてください。

埋込み仮想データ・ソースの制限の概要

表 10-2 は、複数のデータベース表が含まれる埋込み仮想データ・ソースの制限を示しています。

表 10-2 複数表構成での ID 管理機能の可用性

ID 管理機能	表の集約方式		
	結合ビュー・アダプタ（分割プロファイル）	ネイティブ RDBMS 結合機能	ネイティブ RDBMS ビュー機能
変更	×	○（ネイティブ RDBMS 結合機能によってサポートされている場合）	○
追加	×	○（ネイティブ RDBMS 結合機能によってサポートされている場合）	×
削除	×	○（ネイティブ RDBMS 結合機能によってサポートされている場合）	×

実装アーキテクチャ

Oracle Access Manager と Oracle Virtual Directory の実装は、図 10-8 に示すように、3 つのレイヤーで構成されています。

図 10-8 Oracle Virtual Directory の実装レイヤー

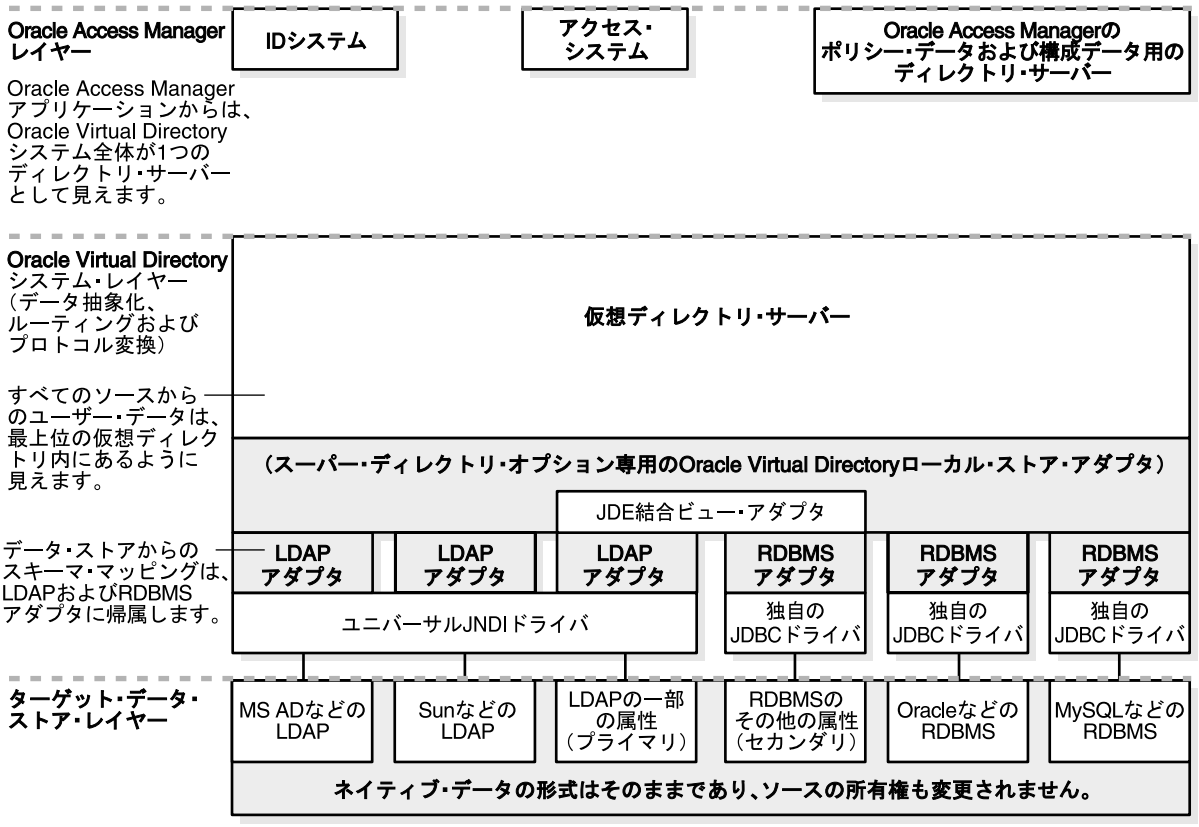


図 10-8 は、Oracle Virtual Directory の 3 つの統合レイヤーを示しています。

- **Oracle Access Manager レイヤー:** このレイヤーには、ID システム、アクセス・システム、および Oracle Access Manager のポリシーおよび構成データ用のディレクトリ・サーバーが含まれます。このレイヤーでは、Oracle Access Manager アプリケーションからは、Oracle Virtual Directory システム全体が 1 つのディレクトリ・サーバーとして見えます。
- **Oracle Virtual Directory システム・レイヤー:** このレイヤーには、スーパー・ディレクトリ・オプション用の Oracle Virtual Directory ローカル・ストア・アダプタの仮想ディレクトリ・サーバーが含まれます。仮想ディレクトリ・サーバーは、LDAP アダプタおよび RDBMS アダプタにアクセスするために、Oracle Virtual Directory 結合ビュー・アダプタを使用します。第 3 レイヤー（ターゲット・データ・ストア・レイヤー）の対応するターゲット・データ・ストアに接続するために、LDAP アダプタは JNDI ドライバを使用し、各 RDBMS アダプタは独自の JDBC ドライバを使用します。データ・ストアからのスキーマ・マッピングは、LDAP および RDBMS アダプタに帰属します。
- **ターゲット・データ・ストア・レイヤー:** このレイヤーには、Oracle Virtual Directory システム・レイヤーの対応する LDAP および RDBMS アダプタにマップされる LDAP および RDBMS データ・ソースが含まれます。このレイヤーでは、ネイティブ・データの形式はそのままであり、そのソースの所有権も変更されません。

Oracle Access Manager レイヤーのユーザーとアプリケーションには、Oracle Virtual Directory システムは、標準スキーマと拡張された Oracle Access Manager の属性が含まれる 1 つの LDAP ディレクトリのように見えます。

仮想ディレクトリ・レイヤー内では、Oracle Virtual Directory は、Oracle Access Manager アプリケーションによるユーザー・データに対するリクエストを受け入れ、リクエストされたデータを構成データ・ストアから取得し、Oracle Access Manager スキーマに合うようにこのデータを変換し、リクエストした Oracle Access Manager アプリケーションに処理データを戻します。図 10-9 は、このプロセスの手順を示しています。

図 10-9 単純な Oracle Access Manager と Oracle Virtual Directory の実装におけるデータ・リクエストの処理

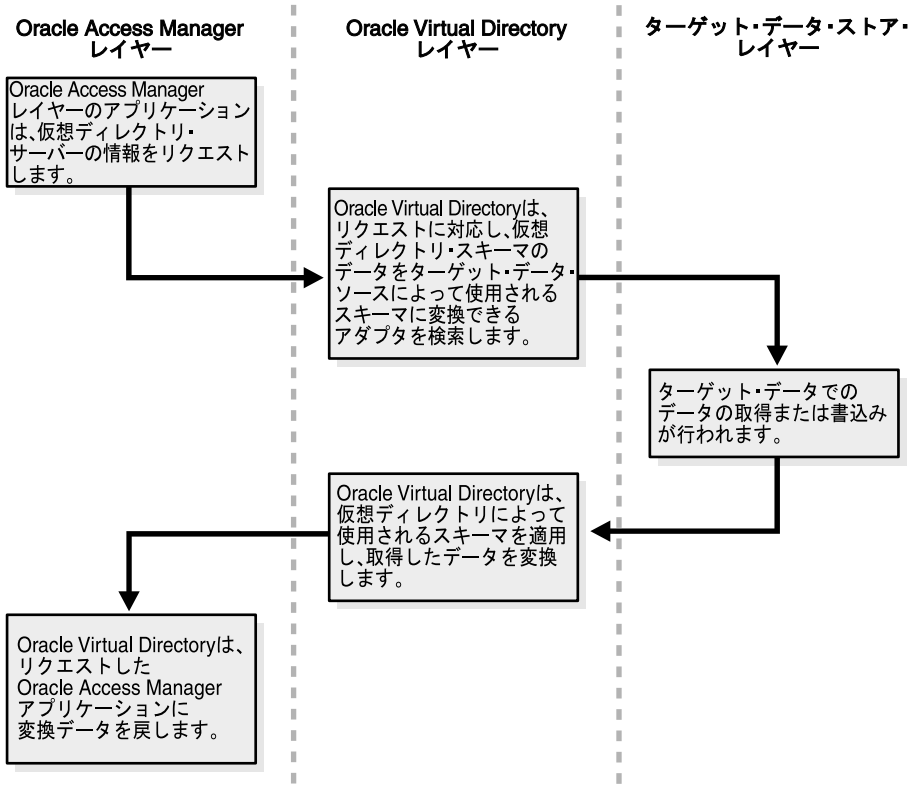


図 10-9 は、次のようなデータ・リクエストの処理手順を示しています。

プロセスの概要 : リクエストの処理

1. Oracle Access Manager レイヤーで、アプリケーションは、仮想ディレクトリ・サーバーの情報をリクエストします。
2. 仮想ディレクトリ・レイヤーで、Oracle Virtual Directory は、リクエストに対応し、仮想ディレクトリ・スキーマのデータをターゲット・データ・ソースによって使用されるスキーマに変換できるアダプタを検索します。
3. ターゲット・データ・ストア・レイヤーで、ターゲット・データ・ストアでのデータの取得または書込みが行われます。
4. 仮想ディレクトリ・レイヤーで、Oracle Virtual Directory は、仮想ディレクトリによって使用されるスキーマを適用し、取得したデータを変換します。
5. Oracle Access Manager レイヤーで、Oracle Virtual Directory は、リクエストした Oracle Access Manager アプリケーションに変換データを戻します。

Oracle Access Manager と Oracle Virtual Directory の実装では、ディレクトリまたはデータベースのネイティブ・ネームスペースまたはデータ構造を永続的に変更する必要がないため、ターゲット・データ・ストア・レイヤーのディレクトリおよびデータベースの管理者には、この実装の影響はほとんどないように見えます。

注意： 使用する機能によっては、ターゲット・データベース表の列として特定の Oracle Access Manager の補助属性を追加する必要がある場合があります。また、Oracle Access Manager スキーマのユーザー・ブランチを使用してターゲット LDAP スキーマを拡張する必要もあります。詳細は、「スキーマ拡張の概要」を参照してください。

また、仮想ディレクトリでは、元のデータ所有者の制御が及ばない場所にデータを永続的にコピーする必要はありません。最後に、個々のデータ・ストア以外に個々のユーザー・プロファイルへのアクセスも ID システムの属性アクセス制御を介して制御できるため、データ・セキュリティは保持されるにとどまらずいっそう強化されます。

Oracle Virtual Directory のドライバとアダプタの概要

Oracle Virtual Directory は、特別なドライバとアダプタを使用して、仮想ディレクトリに組み込むデータ・ソースに接続します。

JNDI ドライバ：JNDI ドライバは、Oracle Virtual Directory インストール・パッケージの一部として同梱されています。JNDI ドライバは Oracle Virtual Directory を LDAP ディレクトリに接続し、JDBC ドライバは Oracle Virtual Directory を RDBMS ソースに接続します。これらのドライバは、Oracle Virtual Directory をホストするマシンにインストールします。

JDBC ドライバ：使用する RDBMS アプリケーションごとに適切なバージョンの JDBC ドライバをインストールする必要があります。詳細は、『Oracle Virtual Directory 製品マニュアル』と『Oracle Virtual Directory and Virtual Directory Manager Installation Guide』を参照してください。Oracle Virtual Directory データベース・アダプタは、JDBC ドライバを備えたデータベースをサポートしています。

アダプタ：仮想ディレクトリのデータ・ソースごとに適切なドライバをインストールするだけでなく、Oracle Virtual Directory に接続するディレクトリまたはリレーショナル・データベースごとに LDAP または RDBMS アダプタを構成する必要があります。これらのアダプタには、Oracle Virtual Directory が仮想ディレクトリ・スキーマを使用してネイティブ・データ・ストアのユーザー・プロファイル情報を変換するために使用するマッピング情報が含まれます。詳細は、10-44 ページの「データ・ストア・アダプタの作成」を参照してください。

Oracle Access Manager 固有のデータの概要

Oracle Access Manager のユーザー・データ、ポリシー・データおよび構成データは、それぞれが LDAP ディレクトリ情報ツリー（DIT）のブランチを占有します。Oracle Virtual Directory 実装では、各ブランチが特定の場所にある必要があります。表 10-3 は、これらの要件を示しています。

表 10-3 Oracle Access Manager ディレクトリのブランチに必要な場所

ブランチ	場所
ポリシー 構成	これらのブランチは、Oracle Access Manager レイヤー内の 1 つ以上のディレクトリ・サーバー上にあることが必要。ホスト・ディレクトリは、Oracle Access Manager のネイティブ・ディレクトリ。
ユーザー・データ	すべてのユーザー・データ・ストアは、Oracle Virtual Directory レイヤー内の Oracle Virtual Directory をホストするマシン上にある最上位ディレクトリの一部であるように見える。

図 10-10 は、Oracle Virtual Directory 実装でのポリシー・ブランチおよび構成ブランチの場所を示しています。

図 10-10 Oracle Virtual Directory 実装でのポリシー・ブランチおよび構成ブランチの場所

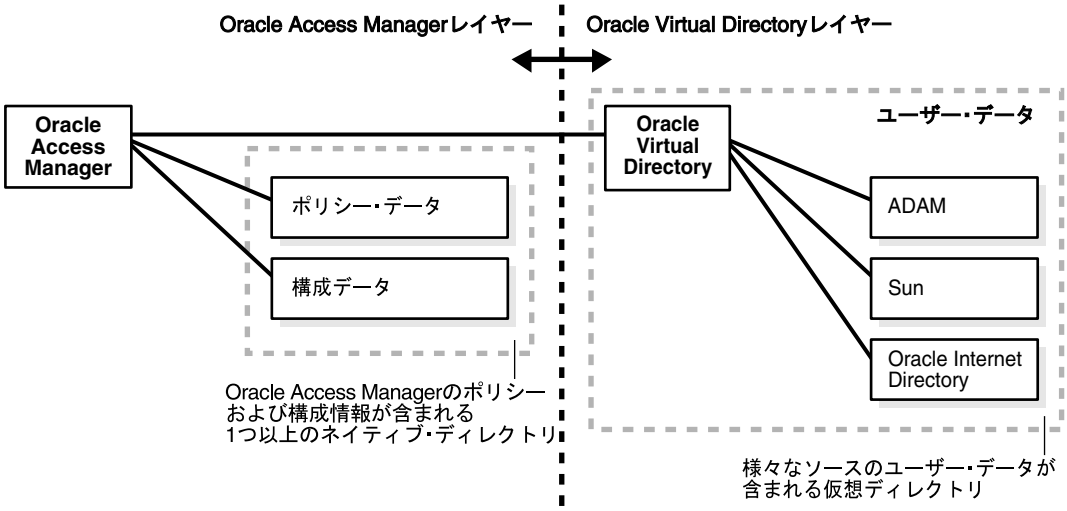


表 10-3 は、この図の内容を示しています。

スキーマ拡張の概要

Oracle Access Manager が正常に機能するには、スキーマに対して userid や userpassword などの特定の属性を拡張する必要があります。

仮想ディレクトリでデータ・ストアによって使用されるネイティブ・スキーマまたは表構造とは関係なく、Oracle Access Manager は、Oracle Virtual Directory 仮想ディレクトリによって使用されるスキーマのみを参照します。これは、Oracle Virtual Directory が、様々なデータ・ストアによって使用されるネイティブ・オブジェクト・クラスまたは属性を、仮想ディレクトリによって使用される対応する論理オブジェクト・クラスまたは属性に自動的にマップするためです。

Oracle Virtual Directory には、業界標準の LDAP ディレクトリ・スキーマと非常に類似したデフォルトの仮想ディレクトリ・スキーマが用意されています。企業のニーズに最適な仮想ディレクトリ・スキーマを開発する場合、このスキーマをベースとして使用できます。

スキーマ拡張に必要なファイルは、次の場所にあります。

IdentityServer_install_dir¥identity¥oblix¥tools¥DNConversionToolkit¥oblix¥tools¥DataAnyWhere¥OblixUserSchema¥*.ldif

図 10-11 は、Oracle Access Manager と Oracle Virtual Directory の実装に関わる必須のスキーマ拡張タスクとオプションのスキーマ拡張タスクの両方を示しています。

図 10-11 実装のスキーマ拡張タスク

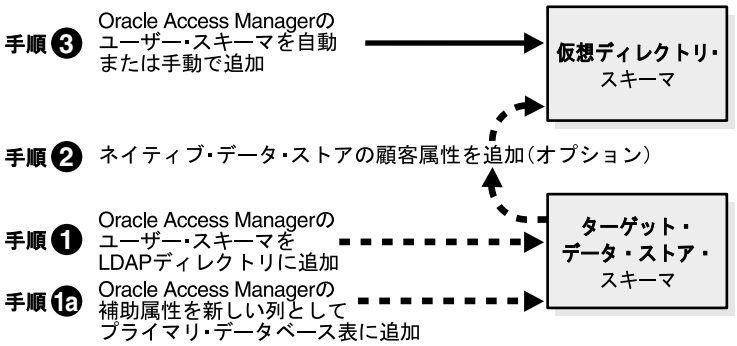


図 10-11 は、次の手順を示しています。

- 手順 1a: ターゲット・データ・ストア・スキーマに対する Oracle Access Manager の補助属性を新しい列としてプライマリ・データベース表に追加します。
- 手順 1: Oracle Access Manager のユーザー・スキーマをターゲット・データ・ストア・スキーマの LDAP ディレクトリに追加します。
- 手順 2: ネイティブ・データ・ストアの顧客属性を追加します（オプション）。
- 手順 3: Oracle Access Manager のユーザー・スキーマを仮想ディレクトリ・スキーマに自動または手動で追加します。

表 10-4 は、仮想ディレクトリの様々なコンポーネントのスキーマ要件を示しています。

表 10-4 この実装のコンポーネントのスキーマ要件

コンポーネント	スキーマ要件
仮想ディレクトリ	Oracle Access Manager のユーザー・スキーマを使用した拡張が必要。 また、顧客属性を使用した拡張も必要。
フェデレーテッド・データ・ソースとして Oracle Virtual Directory に接続された LDAP ディレクトリ	Oracle Access Manager のユーザー・スキーマを使用した拡張が必要。
フェデレーテッド・データ・ソースとして Oracle Virtual Directory に接続されたデータベース	プライマリ・データ・ストアとして機能するデータベース表に対する、表の列の追加が必要。各列は、使用する機能を有効化する Oracle Access Manager の補助属性を示す。ユーザー・ブランチ・スキーマの各属性によって有効になる特定の Oracle Access Manager の機能の詳細は、10-67 ページの「Oracle Access Manager の補助属性」を参照。
分割プロファイル	プライマリ・データ・ストアのスキーマには、Oracle Access Manager のユーザー・スキーマを使用した拡張が必要。プライマリ・データ・ストアがデータベース表である場合、使用する Oracle Access Manager の機能を有効化する補助属性ごとに列の追加が必要。Oracle Access Manager のユーザー・ブランチ・スキーマの各属性によって有効になる特定の機能の詳細は、10-67 ページの「Oracle Access Manager の補助属性」を参照。

詳細は、次を参照してください。

- 仮想ディレクトリ・スキーマ
- ターゲット・ディレクトリ・スキーマ
- ターゲット・データベース表への属性の追加の概要
- 顧客スキーマ

仮想ディレクトリ・スキーマ

仮想ディレクトリが Oracle Access Manager のすべての機能に接続して使用できるようにするには、適切な属性を使用して仮想ディレクトリを拡張する必要があります。たとえば、Oracle Access Manager では、Person オブジェクト・クラスおよび Group オブジェクト・クラスの「フルネーム」、「ログイン」および「パスワード」のセマンティク型に割り当てられた属性が必要です。このユーザー・データとその他の不可欠なユーザー・データが Oracle Access Manager 対応の各ユーザー・ディレクトリのブランチを占有します。詳細は、ID システムの設定に関する章でオブジェクト・クラスに関する項を参照してください。

Oracle Access Manager スキーマの詳細なリストは、『Oracle Access Manager スキーマ詳細』を参照してください。Oracle Access Manager のユーザー属性を使用して Oracle Virtual Directory スキーマを更新する場合、次の 2 つの方法を使用できます。

- **自動 :** 前述の説明のとおり、ID システムの設定時に「自動構成オブジェクト・クラス」チェック・ボックスを選択すると自動的に更新されます。
- **手動 :** 詳細は、6-11 ページの「属性の手動構成」に記載されている属性の手動構成に関する項を参照してください。

ターゲット・ディレクトリ・スキーマ

親仮想ディレクトリのスキーマを拡張するように、仮想ディレクトリに含まれる LDAP ディレクトリによって使用されるネイティブ・スキーマも拡張する必要があります。これを行うには、ldapmodify.exe ユーティリティを使用します。詳細は、10-41 ページの「ディレクトリ・スキーマの拡張」を参照してください。

注意 : 仮想ディレクトリに含まれる分割プロファイルのプライマリ・データ・ストアに Oracle Access Manager の属性を追加することも必要です。詳細は、10-16 ページの表 10-4「この実装のコンポーネントのスキーマ要件」を参照してください。

ターゲット・データベース表への属性の追加の概要

仮想ディレクトリに含まれるデータベースについて、使用する Oracle Access Manager の機能を有効化する補助属性をシミュレートする表の列を追加する必要があります。これが該当するのは、プライマリ・データ・ストアとして使用されるデータベース表のみです。たとえば、「外出中インジケータ」列を追加し、Oracle Access Manager ワークフローのサロゲート機能を有効にします。

注意 : SQL 準拠のデータベースの場合、LDAP オブジェクト・クラスを直接実装する方法はありません。ただし、たとえば、プライマリ・データベース表のすべての行（ユーザー・アカウント）を、仮想ディレクトリによって使用される Person オブジェクト・クラスにマップすることにより、オブジェクト・クラスをシミュレートできます。

特定の機能を有効化する Oracle Access Manager の補助属性のリストは、次を参照してください。

- 表 10-7「User Manager 機能に必要な拡張属性」
- 表 10-8「Group Manager 機能に必要な拡張属性」

顧客スキーマ

必要に応じて、ネイティブ・データ・ストアの顧客属性を追加することにより、デフォルトの Oracle Virtual Directory スキーマをさらに拡張することもできます。たとえば、デフォルトの Oracle Virtual Directory の Person オブジェクト・クラスは UID ですが、Oracle Access Manager の設定時に、InetOrgPerson を追加してから InetOrgPerson を Person オブジェクト・クラスとして指定できます。

Oracle Virtual Directory Manager（VDM、旧称は DME）インタフェースを使用してデフォルトの Oracle Virtual Directory スキーマを変更する方法の詳細は、『Oracle Virtual Directory 製品マニュアル』の構成と設定に関する章のスキーマ構成に関する項を参照してください。

Person オブジェクト・クラスの指定の詳細は、6-7 ページの「Person オブジェクト・クラスおよび Group オブジェクト・クラスの指定」のオブジェクト・クラスに関する項を参照してください。

注意： 顧客属性が 1 つのターゲット・データ・ストアに存在するが、他のデータ・ストアには存在しない場合、Oracle Virtual Directory は、この補助属性を NULL に設定してこれらのその他のデータ・ストアからユーザー・プロファイルを返します。図 10-12 は、この状況を示しています。

図 10-12 単純な仮想ディレクトリに対する補助属性のマッピング

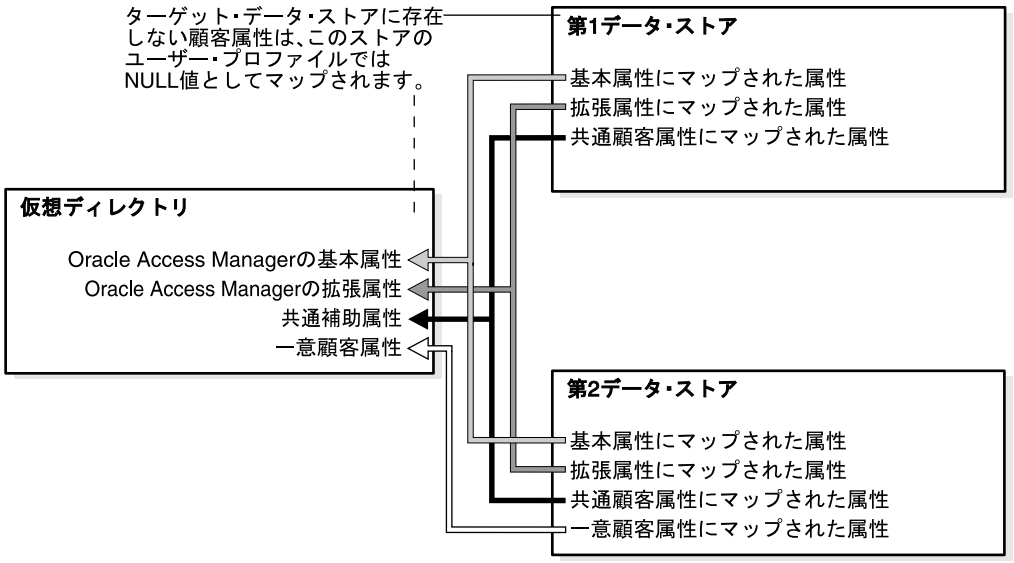


図 10-12 は、単純な仮想ディレクトリにマップされた次の補助属性を示しています。

- 第 1 データ・ストア : 基本属性、拡張属性および共通顧客属性にマップされた属性が含まれます。
- 第 2 データ・ストア : 第 1 データ・ストアと同じ属性が含まれますが、一意顧客属性にマップされた属性も含まれます。

したがって、仮想ディレクトリには、次の属性が含まれます。

- 第 1 データ・ストアと第 2 データ・ストアの両方にマップされた Oracle Access Manager の基本属性
- 第 1 データ・ストアと第 2 データ・ストアの両方にマップされた Oracle Access Manager の拡張属性
- 第 1 データ・ストアと第 2 データ・ストアの両方にマップされた共通補助属性
- 第 1 データ・ストアにはないタイプの属性であるために第 2 データ・ストアのみにマップされた一意顧客属性

実装のシナリオと制限

ここでは、Oracle Virtual Directory を使用して Oracle Access Manager を実装するときにサポートされる 3 つのシナリオについて説明します。また、次の各項では、各シナリオにおける制限についても説明します。

- 異機種間 LDAP ディレクトリ
- 複数の RDBMS データベース
- 分割プロファイル

異機種間 LDAP ディレクトリ

Oracle Access Manager と Oracle Virtual Directory の実装では、1 つ以上のベンダーから複数の LDAP v3 ディレクトリに接続できます。各ディレクトリには、異なるスキーマ（属性およびオブジェクト・クラス）を使用できます。Oracle Virtual Directory が実行時にデータを変換するため、Oracle Access Manager は、Oracle Access Manager スキーマが一律に適用された 1 つのディレクトリとして集約ディレクトリを認識します。

LDAP ディレクトリのみが含まれる（RDBMS データ・ストアは含まれない）Oracle Virtual Directory システムに Oracle Access Manager が接続されている場合、アクセス・システムおよび ID システムの機能はすべて使用可能です。ただし、ディレクトリを結合する場合、いくつかの制限に注意する必要があります。

制限

- Oracle Access Manager は、各ユーザー・プロファイルに関連付けられた 1 つの Person オブジェクト・クラスと 1 つの Group オブジェクト・クラスのみをサポートしています。このため、ネイティブ・ディレクトリの様々な（および場合によっては複数の）Person オブジェクト・クラスと Group オブジェクト・クラスを、仮想ディレクトリの 1 つの Person オブジェクト・クラスと 1 つの Group オブジェクト・クラスにマップする必要があります。
- 構成ディレクトリのネイティブ・ネームスペースは同じでもかまいませんが、これらのネームスペースは仮想ディレクトリ内の異なるネームスペースにマップする必要があります。
- 仮想ディレクトリによってサポートされるユーザーのログイン ID はすべて、含まれるすべてのディレクトリにわたって一意である必要があります。図 10-13 は、この状況を示しています。

図 10-13 単純なスーパー・ディレクトリに対する同一ネームスペースのマッピング

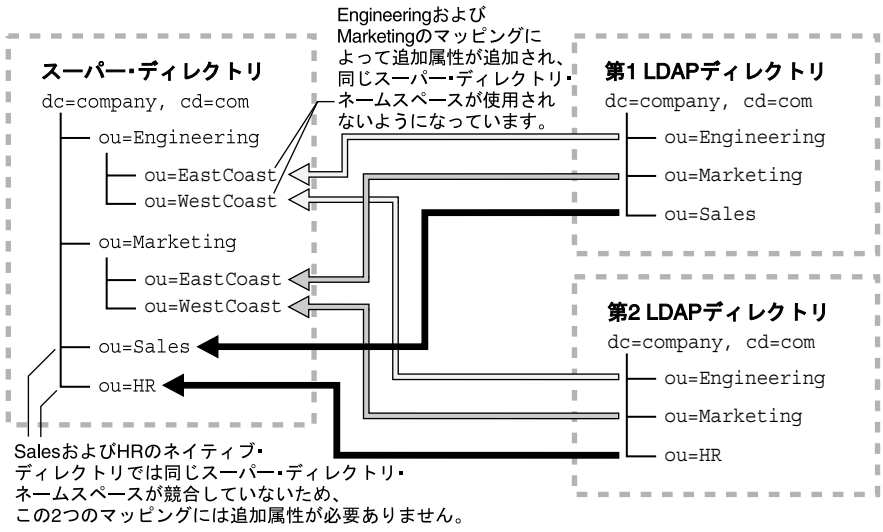


図 10-13 は、スーパー・ディレクトリに対する 2 つの同じ LDAP ディレクトリ・ネームスペースのマッピングを示しています。第 1 LDAP ディレクトリには、Engineering、Marketing および Sales 属性が含まれます。第 2 LDAP ディレクトリには、Engineering、Marketing および HR のマッピングが含まれます。

スーパー・ディレクトリは、Engineering、Marketing、Sales および HR 属性にマップされています。この Engineering と Marketing のマッピングによって追加属性（EastCoast および WestCoast 用）が追加され、同じスーパー・ディレクトリ・ネームスペースが使用されないようになっています。また、このスーパー・ディレクトリには Sales および HR のマッピングもありますが、この 2 つのネイティブ・ディレクトリでは同じスーパー・ディレクトリ・ネームスペースが競合していないため、これらのマッピングには追加属性は必要ありません。

- 構成ディレクトリから仮想ディレクトリの特定の属性にマップされるすべての属性には、共通データ型を使用する必要があります。たとえば、ObOutOfOfficeIndicator 属性は、あるデータ・ソースではバイナリ値には設定できませんが、別のデータ・ソースでは日付（ユーザーが戻る日）に設定できます。
- ネイティブ・ディレクトリに参照整合性制約がある場合、マネージャやグループ・メンバーなどによる参照は同じネイティブ・ディレクトリからのみ可能です。ネイティブ・ディレクトリに参照整合性制約がなく、このネイティブ・ディレクトリが外部参照もサポートしている場合、別のディレクトリからの参照も可能です。
- RDN（相対識別名）はサポートされていません。

複数の RDBMS データベース

Oracle Virtual Directory によってマップされるすべてのユーザー・プロファイル属性を提供する単一表が含まれるデータベースは、仮想ディレクトリにフェデレートして、Oracle Access Manager から参照することが可能です。複数のデータ表が特定のユーザー・プロファイルに属性を提供している場合、これらの表を結合し、ユーザー属性の完全セットが含まれる仮想データ・ソースを作成するために、4 つのオプションが用意されています。

これらのオプションおよびそれぞれの制限の詳細は、10-20 ページの「埋込み仮想データ・ソースでのデータベース表の結合の概要」を参照してください。10-84 ページの「データベースの接続性に関するヒント」も参照してください。

埋込み仮想データ・ソースでのデータベース表の結合の概要

複数のデータ表が特定のユーザー・プロファイルに属性を提供している場合、これらの表を結合し、ユーザー属性の完全セットが含まれる仮想データ・ソースを作成するために、次の 4 つのオプションが用意されています。

- ネイティブ RDBMS 結合機能
- ネイティブ RDBMS ビュー機能
- Oracle Virtual Directory の結合ビュー・アダプタ（分割プロファイル）
- プリファレンスに基づくカスタム・ジョイナ

図 10-14 は、サポートされている 3 つのタイプのうち 1 つの埋込み仮想データ・ソース内で複数のデータベース表を結合する 4 つの方式を示しています。

図 10-14 仮想ディレクトリ内の表を結合する方式

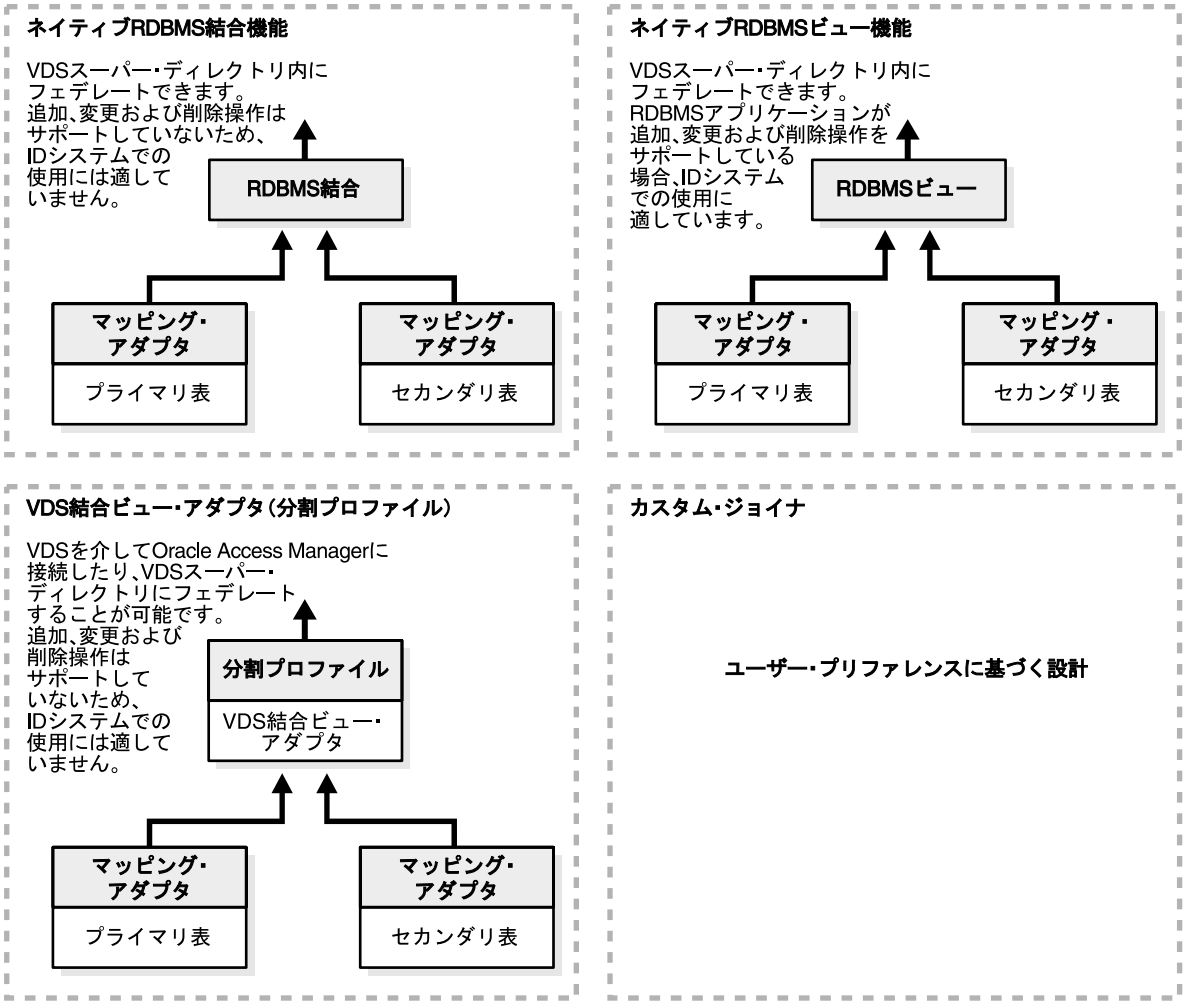


図 10-14 の 4 つの方式に関する詳細情報は、次のとおりです。

- ネイティブ RDBMS 結合機能 : この方式は、それぞれ独自のマッピング・アダプタを持つプライマリ表およびセカンダリ表によって作成される RDBMS 結合を示しています。Oracle Virtual Directory のスーパー・ディレクトリ内にはフェデレートできません。追加、変更および削除操作はサポートしていないため、ID システムでの使用には適していません。
- ネイティブ RDBMS ビュー機能 : この方式は、それぞれ独自のマッピング・アダプタを持つプライマリ表とセカンダリ表によって作成される RDBMS ビューを示しています。Oracle Virtual Directory のスーパー・ディレクトリ内にフェデレートできます。RDBMS アプリケーションが追加、変更および削除操作をサポートしている場合、ID システムでの使用に適しています。
- Oracle Virtual Directory の結合ビュー・アダプタ（分割プロファイル）: この方式は、それぞれ独自のマッピング・アダプタを持つプライマリ表およびセカンダリ表によって作成される Oracle Virtual Directory の結合ビュー・アダプタがある分割プロファイルを示しています。Oracle Virtual Directory を介して Oracle Access Manager に接続することや、Oracle Virtual Directory スーパー・ディレクトリにフェデレートすることは不可能です。追加、変更または削除操作はサポートしていないため、ID システムでの使用には適していません。

- カスタム・ジョイナ : この設計はユーザー・プリファレンスに基づいています。

表 10-5 は、各方式に関する特定の制限を示しています。

表 10-5 仮想ディレクトリ内のデータベース表を結合する方式

方式	適性と制限
ホスト RDBMS アプリケーションのネイティブ結合機能 生成された結合は、仮想ディレクトリの一部としてフェデレートされる。	■ Oracle Access Manager の読取り操作と検索操作の両方がサポートされているため、アクセス・システムでの使用に適している。 ■ Oracle Access Manager の追加、変更および削除操作はサポートされていないため、ID システムでの使用には適していない。
ホスト RDBMS アプリケーションのネイティブ・ビュー機能 生成されたビューは、仮想ディレクトリの一部としてフェデレートされる。	■ Oracle Access Manager の追加操作と検索操作がサポートされているため、アクセス・システムでの使用に適している。 ■ RDBMS アプリケーションのネイティブ・ビュー機能が追加、変更および削除操作をサポートしている場合のみ、ID システムでの使用に適している。
Oracle Virtual Directory の結合ビュー・アダプタ方式 ■ 各データ・ソースは、RDBMS アダプタを介して結合ビュー・アダプタに接続する。 ■ 結果として分割プロファイルが生成される。この分割プロファイルは、Oracle Virtual Directory を介して Oracle Access Manager に接続したり、仮想ディレクトリの一部としてフェデレートしてから Oracle Access Manager に接続することが可能。	■ Oracle Access Manager の追加操作と検索操作がサポートされているため、アクセス・システムでの使用に適している。 ■ ID システムでの使用に適しているが、サブタイプ検索、追加および削除操作はプライマリ表でのみ実行可能。 ■ 結合ビュー・アダプタを使用して結合された LDAP ディレクトリに関する制限はすべて、結合ビュー・アダプタを使用して結合されたデータベースにも適用される。詳細は、10-23 ページの「結合ビュー・アダプタの要件と制限」を参照。
カスタム・ジョイナ方式	RDBMS アプリケーションのネイティブ結合機能およびビュー機能、または標準の結合ビュー・アダプタによって課される制限を克服するためのカスタム・ジョイナを作成できる。 これにはカスタム・プログラミングが必要。詳細は、『Oracle Virtual Directory 製品マニュアル』のジョイナに関する項を参照。

分割プロファイル

各ユーザー・プロファイルの属性を複数のデータ・ソースから取り出す仮想ディレクトリは、分割プロファイルと呼ばれます。これらのデータ・ソースには、LDAP ディレクトリとリレーショナル・データベースの任意の組合せを含めることができます。

1 つのデータ・ストアがプライマリ・データ・ソースとして機能します。このデータ・ストアのスキーマは、Oracle Access Manager 固有のユーザー・データを使用して拡張する必要があります。詳細は、10-15 ページの「スキーマ拡張の概要」を参照してください。

その他のデータ・ストアはすべてセカンダリ・データ・ソースです。これらのセカンダリ・データ・ストアに対して、ID システム機能の一部はサポートされていません。詳細は、10-23 ページの「結合ビュー・アダプタの要件と制限」を参照してください。セカンダリ・データ・ストアに対して Oracle Access Manager のユーザー・スキーマを拡張する必要はありません。

分割プロファイルのデータ・ソースは、Oracle Virtual Directory の標準の結合ビュー・ツール（推奨方式）またはカスタム・ジョイナを使用して結合できます。カスタム・ジョイナの作成の詳細は、『Oracle Virtual Directory 製品マニュアル』を参照してください。

結合ビュー・アダプタの要件と制限

結合ビュー・アダプタは、プライマリ・データ・ストアまたはセカンダリ・データ・ストア内の属性に対するすべてのアクセス・システム操作をサポートしています。これには、認証、認可、監査およびシングル・サインオンが含まれます。

注意： ID システム操作もサポートされていますが、次の制限があります。

制限

- 分割ディレクトリのユーザーのログイン ID 属性は、プライマリ・データ・ストア内にある必要があります。また、ユーザーのログイン・パスワードおよびユーザーのフルネーム属性も、プライマリ・データ・ストア内にある必要があります。
- Oracle Access Manager のユーザー・スキーマは、プライマリ・データ・ストア内にある必要があります。
- ベース・レベル検索は、プライマリ・データ・ストアおよびセカンダリ・データ・ストアの両方に対してサポートされます。
- サブツリー検索は、プライマリ・データ・ストアに対してのみサポートされます。暗黙的に、次の制限が適用されます。
- セカンダリ・データ・ストア内の属性は、検索可能として構成できません。
- セカンダリ・データ・ストア内の属性は、サブツリー検索が関わるフィルタ操作の対象として構成できません。これには次が含まれます。
- ドメイン・フィルタ。
- 動的グループ・フィルタ。
- グループ・サブスクリプション・フィルタ。
- クエリー・ビルダー・フィルタ。
- 属性が存在する特定のデータ・ストアとは関係なく、すべての属性に対して変更操作がサポートされています。
- ユーザー、グループおよびその他のオブジェクトは、プライマリ・データ・ストア内でのみ作成できます。
- プライマリ・データ・ストア内のユーザー、グループおよびその他のオブジェクトのみ削除できます。（Oracle Access Manager アプリケーションは、セカンダリ・データ・ストア内のオブジェクトは削除できません。これは、ターゲット RDBMS アプリケーションまたは LDAP ディレクトリを使用してのみ実行できますが、リアルタイム環境では同期問題が発生する可能性があります。）
- 特定の属性は、1 つのデータ・ストアからのみ構成できます。結合値はサポートされていません。

実装要件

Oracle Access Manager は、仮想ディレクトリに対して他の LDAP ディレクトリの場合と同様にアクセスします。このため、サポートされているほとんどの Oracle Access Manager 構成は Oracle Virtual Directory と円滑に統合できます。次の各項では、Oracle Access Manager と Oracle Virtual Directory の実装の様々な側面におけるサポートおよび要件の詳細を説明します。

Oracle Access Manager: Oracle Access Manager の構成およびポリシー・データが含まれる LDAP ディレクトリのブランチは、Oracle Access Manager の 1 つ以上のネイティブ・ディレクトリ・サーバー上に存在する必要があります。つまり、構成およびポリシー・ブランチは、Oracle Access Manager から参照可能なすべてのユーザー・データが含まれる仮想ディレクトリに存在することはできません。

前述の説明のとおり、構成、ポリシーおよびユーザー・データの場所は、Identity Server、Policy Manager および Access Server のインストールおよび設定時に指定します。

Oracle Virtual Directory: Oracle Virtual Directory をインストールするホスト・マシンの操作に関する最新のサポートの詳細は、次のサイトにある Oracle *MetaLink* または Oracle Technology Network（OTN）を参照してください。

`https://www.metalink.oracle.com/`

`http://www.oracle.com/technology/deploy/security/index.html`

オペレーティング・システム : Oracle Virtual Directory は、10*g*（10.1.4.0.1）をサポートしているオペレーティング・システムが動作するホスト・マシン上にインストールされた Oracle Access Manager コンポーネントを使用して実装できます。

仮想ディレクトリによってサポートされている LDAP ディレクトリおよび RDBMS データベースは、Oracle Virtual Directory によってサポートされているホスト・プラットフォームにインストールできます。

Java ランタイム環境 : Oracle Virtual Directory をインストールするホスト・マシンには、Java ランタイム環境がインストールされている必要があります。

Oracle Access Manager と Oracle Virtual Directory の実装は、JRE v1.4 を使用してテストされています。

JNDI ドライバ : サポートされている Oracle Virtual Directory インストール・パッケージに同梱されている JNDI ドライバを使用します。

JDBC ドライバ : Oracle Virtual Directory をホストするマシン上で、仮想ディレクトリに接続する RDBMS アプリケーションに適したバージョンの JDBC ドライバをインストールする必要があります。適切なドライバは RDBMS アプリケーションのベンダーから入手できます。Oracle Virtual Directory データベース・アダプタは、JDBC ドライバを備えたデータベースをサポートしています。

仮想ディレクトリに複数のベンダーのデータベースが含まれる場合、使用されているベンダーごとに JDBC ドライバをインストールする必要があります。詳細は、『Oracle Virtual Directory 製品マニュアル』を参照してください。

データセット : Oracle Access Manager と Oracle Virtual Directory の実装には、UTF-8 キャラクタ・セットが使用されます。Oracle Virtual Directory はローカライゼーションに対応していますが、明示的にサポートされているのは英語のみです。

リレーショナル・データベース : 通常、Oracle Access Manager は、Oracle Virtual Directory によってサポートされている RDBMS データベースが含まれる任意の仮想ディレクトリに接続できます。詳細は、Oracle Access Manager と Oracle Virtual Directory の実装についてサポートされている RDBMS アプリケーションを示す 10-5 ページの図 10-2「フェデレーテッド RDBMS アプリケーションが含まれる Oracle Virtual Directory 実装」を参照してください。10-84 ページの「データベースの接続性に関するヒント」も参照してください。

ディレクトリ・サーバー : 通常、Oracle Access Manager は、Oracle Virtual Directory によってサポートされている LDAP ディレクトリ・サーバーに接続できます。10-4 ページの図 10-1「フェデレーテッド LDAP ディレクトリがある Oracle Virtual Directory 実装」は、Oracle Access Manager と Oracle Virtual Directory の実装用としてサポートされている LDAP ディレクトリ・サーバーを示しています。

キャッシング : Oracle Virtual Directory は、キャッシングは明示的にはサポートしていません。

Oracle Access Manager と Oracle Virtual Directory の実装の要件およびサポートの詳細は、次を参照してください。

- セキュリティ接続のサポート
- 認証のサポート
- アクセス制御のサポート
- フェイルオーバーのサポート

セキュリティ接続のサポート

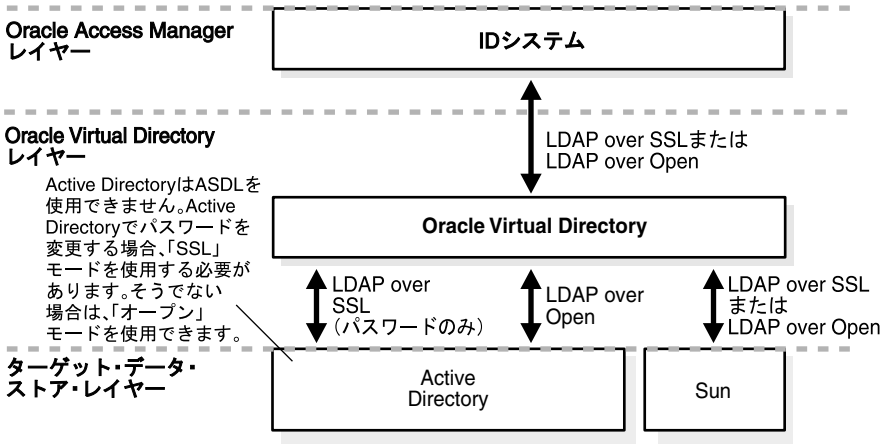
オープン接続または SSL 接続は、Oracle Access Manager と Oracle Virtual Directory 間、および Oracle Virtual Directory とネイティブ・データ・ストア間でサポートされています。

Active Directory の場合、ADSI はサポートされていません。Active Directory 内でパスワードを変更する場合、「SSL」を使用する必要があります。そうでない場合は、「オープン」モードを使用できます。

> **注意 :** Active Directory を Oracle Virtual Directory に接続する場合、最良のパフォーマンスを実現するには、セキュリティ接続モードとして「Password Only SSL」を指定します。このシナリオの場合、Oracle Virtual Directory と Active Directory の間にオープン接続を確立する必要もあります。

図 10-15 は、Oracle Access Manager と Oracle Virtual Directory の実装内で接続に使用されるプロトコルを示しています。

図 10-15 単純な Oracle Access Manager と Oracle Virtual Directory の実装におけるプロトコルのサポート



この図は、図 10-8 で詳細に説明した 3 つのレイヤーにおけるプロトコルのサポートを示しています。各レイヤーの説明は、次のとおりです。

- **Oracle Access Manager レイヤー :** ID システムを示しています。
- **VDS レイヤー :** Oracle Access Manager レイヤーの ID システムにアクセスする Oracle Virtual Directory レイヤーを示しています。また、ターゲット・データ・ストア・レイヤーの Active Directory および Sun にもアクセスしています。
- **ターゲット・データ・ストア・レイヤー :** Active Directory および Sun を示しています。Active Directory は、LDAP over SSL（パスワードのみ）および LDAP over Open を介して Oracle Virtual Directory レイヤーにアクセスしています。Sun は、LDAP over SSL または LDAP over Open を介して Oracle Virtual Directory にアクセスしています。Active

Directory は ASDL を使用できません。Active Directory でパスワードを変更する場合、「SSL」モードを使用する必要があります。そうでない場合は、「オープン」モードを使用できます。

認証のサポート

Oracle Virtual Directory は、次の認証方式をサポートしています。

- 資格証明の受渡し認証
- 単純プロキシ

資格証明の受渡し認証の概要

Oracle Access Manager と Oracle Virtual Directory の実装に資格証明の受渡し認証を使用する場合、「Pass Credentials」を「Always」（または「Bind Only」）に設定し、Oracle Access Manager によって提供されているユーザーの識別名とパスワードを Oracle Virtual Directory がプロキシ設定対象 LDAP ディレクトリに渡すようにします。

背景的な詳細は、『Oracle Virtual Directory 製品マニュアル』の構成と設定に関する章のディレクトリ・ネームスペースと属性マッピングに関する項を参照してください。

アクセス制御のサポート

Oracle Access Manager と Oracle Virtual Directory の両方のアクセス制御がオンになっており、Oracle Access Manager と Oracle Virtual Directory 間の接続についてデフォルト設定が有効化されていることを確認します。背景的な詳細は、『Oracle Virtual Directory 製品マニュアル』のセキュリティとアクセス制御に関する章を参照してください。

Oracle Virtual Directory とターゲット・データ・ストア間の接続については、サポートされているターゲット・データ・ストアごとにアクセス制御をオンにします。（Oracle Virtual Directory は、LDAP クライアントであるため、ターゲット・ディレクトリ・サーバーごとに固有のアクセス制御実装を使用する必要があります。）詳細は、『Oracle Virtual Directory 製品マニュアル』の構成と設定に関する章のアクセス制御と LDAP アダプタに関する項を参照してください。

フェイルオーバーのサポート

Oracle Access Manager と Oracle Virtual Directory の実装では、Oracle Access Manager、Oracle Virtual Directory、ディレクトリ・サーバーおよび RDBMS アプリケーションの既存のフェイルオーバー機能を使用してフェイルオーバーのサポートが実装されます。フェイルオーバーは、次の 3 つのレベルで実装できます。

- Oracle Access Manager のフェイルオーバー
- Oracle Virtual Directory のターゲット・ソースのフェイルオーバー
- ターゲット・データ・ストアのフェイルオーバー

Oracle Access Manager のフェイルオーバー : Identity Server または Access Server は、1 つ以上のプライマリ仮想ディレクトリ・インスタンス、および 1 つ以上のセカンダリ Oracle Virtual Directory インスタンスにアクセスできます。

- 『Oracle Access Manager ID および共通管理ガイド』の ID システムの管理と構成に関する章の LDAP サーバー・プロファイルへのデータベース・インスタンスの追加に関する項を参照してください。
- Oracle Access Manager でのフェイルオーバーの構成の詳細は、『Oracle Access Manager デプロイメント・ガイド』を参照してください。
- 『Oracle Virtual Directory 製品マニュアル』の仮想ディレクトリの計画に関する章のフォルト・トレラントのデプロイに関する項を参照してください。

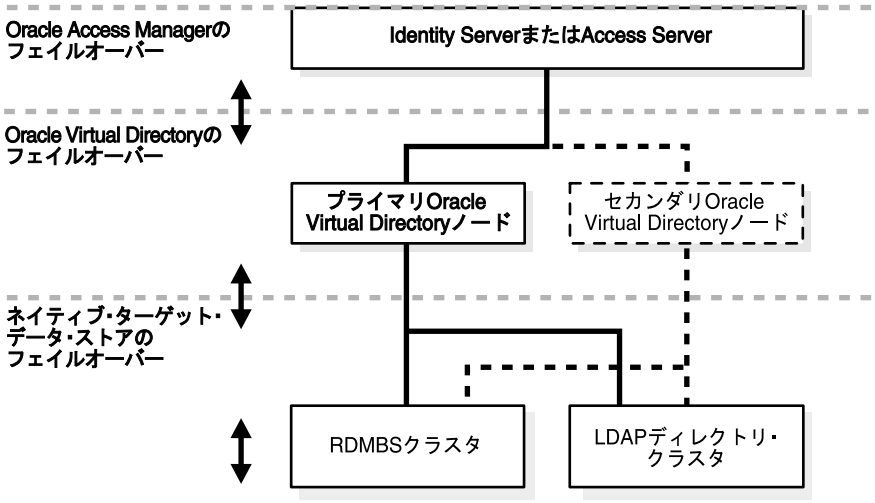
Oracle Virtual Directory のターゲット・ソースのフェイルオーバー : Oracle Virtual Directory では、仮想ディレクトリとターゲット・データ・ストア間でフェイルオーバー保護を実装できます。詳細は、『Oracle Virtual Directory 製品マニュアル』の仮想ディレクトリの計画に関する章のフォルト・トレラントのデプロイに関する項を参照してください。

ターゲット・データ・ストアのフェイルオーバー : 多くの場合、RDBMS アプリケーションおよび LDAP ディレクトリ・サーバーは、ターゲット・データ・ストア・レベルでのクラスタリングという形式でフェイルオーバーをサポートしています。通常、この機能を実装するメカニズムは自動的に動作し、Oracle Virtual Directory や Oracle Access Manager からは認識できません。詳細は、RDBMS アプリケーションまたは LDAP ディレクトリ・サーバーに関するドキュメントを参照してください。

注意 : この章では、環境に応じてフェイルオーバーを構成するための特定の手順は示しません。フェイルオーバーは、製品のドキュメントに従って通常どおりに設定できます。

図 10-16 は、Oracle Access Manager と Oracle Virtual Directory の実装内で潜在的に使用可能なフェイルオーバーのタイプを示しています。

図 10-16 Oracle Access Manager と Oracle Virtual Directory の実装におけるフェイルオーバーのオプション



実装プロセスの概要

次の項目では、2 つの異なる状況について説明します。必ず環境に応じた項目を選択してください。

- Oracle Access Manager がインストールされていない場合 :「Oracle Access Manager のインストール時の Oracle Virtual Directory の実装」を参照してください。
- Oracle Access Manager がインストールされている場合 :「既存の Oracle Access Manager インストールとの Oracle Virtual Directory の実装」を参照してください。

Oracle Access Manager のインストール時の Oracle Virtual Directory の実装

Oracle Access Manager をまだインストールしていない場合、Oracle Virtual Directory との実装を完了するために説明されている作業を行う必要があります。

タスクの概要 : Oracle Access Manager のインストール時の Oracle Virtual Directory の実装

1. 10-30 ページの「環境の準備」
2. 10-34 ページの「Oracle Virtual Directory と Virtual Directory Manager のインストールおよび構成」
3. 10-39 ページの「最初の Identity Server のインストール」
4. 10-41 ページの「ディレクトリ・スキーマの拡張」
5. 10-43 ページの「アダプタのマッピング・ファイルの作成」
6. 10-44 ページの「データ・ストア・アダプタの作成」
7. 10-52 ページの「アダプタおよびマッピング・ファイルのカスタマイズ」
8. 10-66 ページの「ID システムのインストールおよび設定の実行」
9. 10-67 ページの「実装のテスト」

既存の Oracle Access Manager インストールとの Oracle Virtual Directory の実装

ネイティブ・ディレクトリまたは RDBMS を持つ Oracle Access Manager インストール（バージョン 5.2.x 以上）が動作している場合、Oracle Virtual Directory を統合することにより、最初からインストールされていたネイティブ・ディレクトリ・サーバーと追加のユーザー・ディレクトリおよびデータベースにアクセスできるようになります。

この場合、次のタスクの作業を実行し、以前の Oracle Access Manager インストールを 10*g*（10.1.4.0.1）にアップグレードして Oracle Virtual Directory を準備してから、ディレクトリ・スキーマを拡張し、Oracle Access Manager を再構成して「Data Anywhere」オプションをユーザー・データ・ディレクトリ・サーバーとして使用できるようにします。

注意 : DN 変換ツールキットは、Identity Server インストールの一部として自動的にインストールされます。*IdentityServer_install_dir*¥identity¥oblix¥tools¥DNConversionToolkit¥oblix¥ を参照してください。

タスクの概要 : 既存の Oracle Access Manager インストールとの Oracle Virtual Directory の実装

1. 既存の Oracle Access Manager インストールで、ユーザー・データと構成データが別のディレクトリ・サーバーに格納されていることを確認します。
2. 次のディレクトリにある DN 変換ツールキットを検索します。

   IdentityServer_install_dir¥identity¥oblix¥tools¥DNConversionToolkit¥oblix¥

3. 次のディレクトリにある README ファイルで、ビルドおよびランタイム要件と、キットに用意されているファイルおよびディレクトリのリストを確認します。

   IdentityServer_install_dir¥identity¥oblix¥tools¥DNConversionToolkit¥oblix¥tools¥DataAnyWhere¥README

4. 『Oracle Access Manager アップグレード・ガイド』の指示に従って、ネイティブ・ディレクトリがある既存の Oracle Access Manager インストールを 10*g*（10.1.4.0.1）にアップグレードします。
5. 次の説明に従って、Oracle Virtual Directory と統合する追加のディレクトリおよびデータベースを準備します。
   - 環境の準備
   - ディレクトリ・スキーマの拡張
6. 『Oracle Virtual Directory and Virtual Directory Manager Installation Guide』および 10-34 ページの「Oracle Virtual Directory と Virtual Directory Manager のインストールおよび構成」で説明されているように、Oracle Virtual Directory/Virtual Directory Manager をインストールおよび構成します。
7. オラクル社提供の DN 変換ツールを使用して、ネイティブ・ディレクトリにある既存の Oracle Access Manager の構成およびポリシー・データを次のようにクリーン・アップします。

   a. 次のディレクトリにある変換ツールを検索し、Data AnyWhere ディレクトリにある README ファイルを確認します。

      README: *IdentityServer_install_dir*¥identity¥oblix¥tools¥DNConversionToolkit¥tools¥DataAnyWhere/README

      Conversion tool: *IdentityServer_install_dir*¥identity¥oblix¥tools¥DNConversionToolkit¥tools¥DataAnyWhere¥conversion_tools¥obmigrateDN.exe

   b. **オブジェクト・クラスが同じ場合 :** 新しい Oracle Virtual Directory 仮想ディレクトリのオブジェクト・クラスが、元の Oracle Access Manager インストールによって使用されていたオブジェクト・クラスと同じままであり、唯一の変更内容がネームスペース階層のみである場合、構成ブランチ（Oracle Access Manager の構成データ）には、obmigrateDN.exe ツールを使用してパッチを適用できます。このツールを使用すると、元の構成が保存され、既存の Oracle Access Manager インストールによって使用されていたネイティブ DN が、Oracle Virtual Directory 仮想ディレクトリによって使用される新しい仮想（論理）DN に変換されます。ポリシーの UID、Oracle Access Manager のマスター管理者、マスター ID 管理者、マスター・アクセス管理者、およびディレクトリ・サーバー管理者などの DN 参照は、古いネイティブ DN から新しい仮想 DN に変換する必要があります。

      注意 : DN 変換ツール（obmigratedn）の実行時に指定した引数に応じて、実行時に config.lst ファイルが生成されます。これと同じファイルがデータ移行ツール（obmigratedata）の実行時にも生成されます。

   c. **オブジェクト・クラスが異なる場合 :** Oracle Virtual Directory を介して Oracle Access Manager から参照する仮想オブジェクト・クラスが、元の（Oracle Virtual Directory 以前の）インストールによって使用されていた仮想オブジェクト・クラスとは異なる場合、Oracle Access Manager インストール全体を再構成する必要がある場合がありま

す。この場合は通常、LDAP DIT の全体的な構成およびポリシー・ブランチを削除します。

後で新しい ID システムの設定手順を手動で実行するために手順 7 を実行すると、構成されていたすべてのポリシーおよびその他同種の設定が失われることに注意してください。

8. **すべての環境が対象 :** 必要に応じて、次の仕様を使用して Oracle Access Manager の設定を手動で再実行します。

   a. **User Data Directory Server:** ディレクトリ・タイプとして Data Anywhere を選択します。

   b. **User Data -Host:** Oracle Virtual Directory をホストしているマシンを指定します。

   c. **User Data -Port:** Oracle Virtual Directory の LDAP ライセンス・ポートを指定します。

   d. **Searchbase:** 仮想ツリーの任意の場所にある Oracle Virtual Directory の仮想 DN を指定します。

   e. **Oracle Data Directory Server:** Oracle Access Manager に関するかぎり、Oracle Access Manager の構成およびポリシー・データはユーザー・データのみが含まれる Oracle Virtual Directory 仮想ディレクトリの外部に格納する必要があるため、通常どおりネイティブ・ディレクトリを選択します。

   f. **Automatically Update Schema:** 「Yes」を選択し、Oracle Access Manager の補助属性を使用して Oracle Virtual Directory スキーマを自動的に更新します。

   g. **Automatically Configure Person and Group Object Classes:** 「Yes」または「No」を選択し、通常どおり Oracle Virtual Directory スキーマを構成します。

注意 : Person オブジェクト・クラスおよび Group オブジェクト・クラスの手動構成の詳細は、6-7 ページの「Person オブジェクト・クラスおよび Group オブジェクト・クラスの指定」を参照してください。

環境の準備

Oracle Virtual Directory（Data Anywhere）を使用して Oracle Access Manager を実装するための環境の準備には、次の作業が含まれます。

タスクの概要 : 環境の準備

1. インストール・メディアからの 10*g*（10.1.4.0.1）インストール・パッケージの取得時における DN 変換ツールキットの取得
2. 10-31 ページの「実装の設計要素の識別」
3. 10-33 ページの「実装用のディレクトリ・サーバーの準備」
4. 10-33 ページの「実装用のリレーショナル・データベースの準備」

実装の設計要素の識別

実装を開始する前に、情報を収集し、Oracle Access Manager と Oracle Virtual Directory の実装の設計方針を決定します。

必要に応じて、背景的な調査を実行し、次の各質問について検討して回答します。

この実装の要素の識別の手順

1. Oracle Virtual Directory を介してアクセスするデータ・ストアを確認します。

   仮想ディレクトリ内では LDAP ディレクトリおよび RDBMS データベースをフェデレートできます。また、分割プロファイル、ネイティブ RDBMS 結合およびネイティブ RDBMS ビューなどの埋込み仮想データ・ソースも作成およびフェデレートできます。

   ターゲット・データ・ソースとしての LDAP ディレクトリの選定 : Oracle Access Manager には、Oracle Access Manager が Oracle Virtual Directory の実装用としてサポートしている LDAP ディレクトリ・サーバーごとにアダプタ・テンプレートおよびスキーマ・マッピング・テンプレートの両方が用意されているため、LDAP ディレクトリの組込みは比較的簡単です。詳細は、10-70 ページの「DN 変換ツールキットの概要」を参照してください。

   唯一の重要な制限は、スーパー・ディレクトリでは 2 つのディレクトリが同じネームスペースを占有できないことです。ただし、ネイティブ・ディレクトリによって使用されるネームスペースをスーパー・ディレクトリ内の一意のネームスペースにマップすることにより、このような競合を回避できます。詳細は、10-8 ページの「集約ネームスペース」を参照してください。

   ターゲット・データ・ソースとしての RDBMS データベースの選定 : RDBMS データベースの場合、Oracle Access Manager が動作するために不可欠なすべての情報が単一表内に存在するかどうかを最初に確認する必要があります。これには、次の属性にマップされるデータベース列が含まれます。

   - UID（ユーザー・ログイン ID）。
   - ユーザー・パスワード。
   - フルネーム。
   - Person オブジェクト・クラス。これは通常、重要なフィールドがある表の名前によって暗黙的に示されます。たとえば、データベースの従業員表のユーザー・アカウントはすべて、仮想ディレクトリの inetorgperson Person オブジェクト・クラスにマップできます。コンサルタントなどの別の表がある場合、そのユーザー・アカウントもすべて inetorgperson にマップしてから、ネイティブ RDBMS 結合またはビュー機能を使用してこれらのユーザー・アカウントを連結できます。守るべき重要な原則は、仮想ディレクトリによって指定される 1 つの Person オブジェクト・クラスにすべてのユーザー・アカウントを関連付ける必要があるということです。
   - 使用する特定の機能を有効化するために必要な Oracle Access Manager のユーザー・ブランチ属性。たとえば、OOO（Out of Office: 外出中）というラベルの列を従業員表に追加することにより、仮想ディレクトリについてワークフローを実行できるようになります。
   - 重要な情報がすべて単一表内にある場合、データベースを仮想ディレクトリの一部としてフェデレートできます。一部の重要情報がデータベース内にない場合、またはこの情報が複数の表に分散している場合、このデータベースは仮想ディレクトリに含めることに適していない場合があります。または、使用可能な 3 つの方式の 1 つを使用し、データベースを埋込み仮想データ・ソースに変換してから仮想ディレクトリ内にフェデレートする必要がある場合があります。

   Oracle Virtual Directory RDBMS アプリケーション ネイティブ LDAP ディレクトリ・サーバー

2. Oracle Access Manager から参照可能な仮想ディレクトリ情報の項目を確認します。

   Oracle Access Manager が仮想ディレクトリと対話できることを確認するには、手順 1 に記載されている重要項目が Oracle Access Manager から参照できるようにする必要があります。また、Oracle Access Manager から参照可能な顧客属性も確認する必要があります。た

とえば、従業員の携帯電話番号または誕生日を仮想ディレクトリに追加することにより、これらの属性を参照可能にできます。

3. オブジェクト・クラスと属性をマップするために最適な方式を確認します。

   これは、ターゲット・データ・ストアによって使用されるネイティブ・スキーマによって異なります。Oracle Virtual Directory を介して Oracle Access Manager から参照する仮想スキーマは自由に作成できますが、次の点に注意する必要があります。

   - 2 つの異なるターゲット・データ・ストアの情報がスーパー・ディレクトリ内の同じネームスペースを占有することはできません。
   - 仮想ディレクトリに埋込み仮想データ・ストアが含まれる場合は通常、セカンダリ・データ・ストアの情報を変更できないため、ユーザー・アカウントを作成、削除または変更するワークフローは使用しないようにする必要があります。
   - 埋込み仮想ディレクトリ（分割プロファイル、RDBMS 結合および RDBMS ビュー）のセカンダリ・データ・ストアをフィルタまたはサブ検索に含めることはできません。つまり、分割プロファイル、RDBMS 結合および RDBMS ビューなどの埋込み仮想データ・ストアは、アクセス・システム操作（認証および認可）には適していますが、多くの場合、セカンダリ・データ・ストアのデータに対しては追加、削除および変更などの主要機能を使用できないため、通常、これらのデータ・ストアは ID 管理操作には適していません。
   - Oracle Access Manager と Oracle Virtual Directory の実装では、複数の値を持つ属性と、ターゲット・データ・ストアとして使用されるデータベースを同時にはサポートできません。仮想ディレクトリに LDAP ディレクトリのみが含まれる場合は、多値属性を使用できます。

   注意： データベースとともに多値属性を使用する必要がある場合は、10-74 ページの「Oracle Access Manager と Oracle Virtual Directory の実装のテンプレート」および E-12 ページの「複数値属性の問題」を参照してください。

   ---

4. 仮想ディレクトリの情報ごとに Oracle Access Manager が実行する操作を確認します。

   Oracle Access Manager の特定の機能（ワークフローでのサロゲートなど）を使用する場合、埋込み仮想データ・ストアのプライマリ・データベース表に列を追加する必要があります。特定の User Manager および Group Manager 機能と、ターゲット・データ・ストアとして機能するデータベースのプライマリ表に追加する必要がある Oracle Access Manager の補助ユーザー属性の相関関係を示すリストは、10-17 ページの「ターゲット・データベース表への属性の追加の概要」および 10-67 ページの「Oracle Access Manager の補助属性」を参照してください。

5. ポリシー管理と ID 管理の観点から、仮想ディレクトリに最適な DIT 階層を確認します。

   非結合検索ベースと統合検索ベースのどちらかを選択できます。詳細は、10-5 ページの「検索ベースのオプションの概要」を参照してください。

   スーパー・ディレクトリ・オプションを選択した場合、組織のニーズにあわせてネームスペース集約とスキーマ・マッピングを最適化できます。たとえば、企業が合併された場合、2 つの会社のエンジニアリング・ディレクトリを集約できるため、新しい会社のすべてのエンジニアについて構成が必要なアクセス・ポリシーは 1 セットのみです。このようなシナリオを処理したネームスペース・マッピングの簡単な例は、10-8 ページの「集約ネームスペース」を参照してください。

6. コンポーネントをホストするマシンを確認し、次のインストール先を確認します。

   - Oracle Access Manager
   - Oracle Virtual Directory
   - RDBMS アプリケーション
   - ネイティブ LDAP ディレクトリ・サーバー

7. 次の作業に進みます。
   - 実装用のディレクトリ・サーバーの準備
   - 実装用のリレーショナル・データベースの準備

実装用のディレクトリ・サーバーの準備

Oracle Virtual Directory に統合するネイティブ・ディレクトリ・サーバーをインストールおよび構成する必要があります。この作業はここで実行できます。

注意： 後で実行する 2 つ目の要件として、Oracle Access Manager 関連のユーザーおよびグループ情報を使用して各バックエンド・ディレクトリ・サーバーのネイティブ・スキーマを拡張する必要があります。これにより、Oracle Virtual Directory およびネイティブ・スキーマに同じ Oracle Access Manager 属性が含まれます。

各ディレクトリ・サーバーの準備の手順

1. 10-24 ページの「実装要件」を確認します。
2. ベンダーの指示に従ってバックエンド・ディレクトリ・サーバーをインストールします。

   後で、Oracle Access Manager 関連の属性を使用してネイティブ・スキーマを拡張します。
3. 環境に応じて、次の作業を実行します。
   - 実装用のリレーショナル・データベースの準備
   - Oracle Virtual Directory と Virtual Directory Manager のインストールおよび構成

実装用のリレーショナル・データベースの準備

続行する前に、ディレクトリに含める各リレーショナル・データベースの準備を開始する必要があります。この手順は、RDBMS 固有のアダプタを作成するための前提条件です。

実装用の各リレーショナル・データベースの準備の手順

1. ベンダーの指示に従って RDBMS をインストールおよび構成します。
2. 仮想ディレクトリによって使用される Oracle Access Manager スキーマの重要な属性にマップする必要があるフィールドがすべてデータベースの単一表に含まれていることを確認します。これは次のとおりです。
   - UID
   - ユーザー・パスワード
   - フルネーム
3. 次の各項目を考慮してください。
   - データベースに重要なフィールドがすべて含まれていない場合、このデータベースは仮想ディレクトリに含めることに適さない可能性があります。
   - 重要なフィールドがすべて同じ表内にない場合、この表を仮想ディレクトリに含めることはできません（セカンダリ表に存在する重要なフィールドは検索できないためです）。オプションの顧客フィールドはセカンダリ表に格納できます。
   - 重要なフィールドがすべて同じ表内にある場合、次のいずれかの方式を使用して埋込み仮想データ・ストアを作成する必要がある場合があります。
     - 結合ビュー・アダプタ
     - RDBMS アプリケーションのネイティブ・ビュー機能
     - RDBMS アプリケーションの結合機能

注意： 前述の複数表のデータベースを組み込むための 3 つの方式では、特定の ID システム機能が必ず制限されます。

4. RDBMS アプリケーションのベンダーの Web サイトから必要なドライバ・ライブラリをダウンロードします。

   たとえば、Oracle の場合、Oracle JDBC シン・ドライバ（ojdbc14.jar 以上）をダウンロードする必要があります。

5. ベンダーの指示に従ってドライバをインストールします。

6. 10-34 ページの「Oracle Virtual Directory と Virtual Directory Manager のインストールおよび構成」にスキップします。

   後で、Oracle Virtual Directory をホストするマシン上のターゲット・データベースに対して JDBC ドライバをデプロイするよう指示されます。

   10-84 ページのデータベースの接続性に関するヒントも参照してください。

Oracle Virtual Directory と Virtual Directory Manager のインストールおよび構成

実装構成を選択し、データ・ソースを準備した後、実装に必要な Oracle Access Manager と Oracle Virtual Directory ソフトウェアの両方をインストールする必要があります。次のタスクの概要は、実行する必要がある手順を示しています。

タスクの概要 : Oracle Virtual Directory と Virtual Directory Manager のインストールおよび構成

1. 10-35 ページの「Oracle Virtual Directory のインストール」
2. 10-35 ページの「Virtual Directory Manager のインストール」
3. 10-36 ページの「プロジェクト領域およびサーバーの作成」
4. 10-36 ページの「サンプル・アダプタおよびマッピング・テンプレートの取得 / 更新」
5. RDBMS: 37 ページの「RDBMS 用の JDBC ドライバ・ライブラリのデプロイ」
6. 38 ページの「Oracle Virtual Directory の SSL リスナーの構成（オプション）」

Oracle Virtual Directory のインストール

Oracle Virtual Directory を通常どおりインストールします。Oracle Access Manager との実装を容易にするために必要な特定の手段はありません。

Oracle Virtual Directory のインストールの手順

1. 『Oracle Virtual Directory and Virtual Directory Manager Installation Guide』の指示に従って Oracle Virtual Directory をインストールおよび設定します。
2. Oracle Virtual Directory のドキュメントに記載されているデフォルト設定を使用します。
3. 最初の Identity Server をインストールするときに使用する Oracle Virtual Directory インストールに関する情報を記録します。これには次が含まれます。
   - **Host Name:** Oracle Virtual Directory をホストしているマシンの DNS ホスト名。
   - **Port Number:** Oracle Virtual Directory の LDAP ライセンス・ポート。
   - **Bind DN for the user data directory server:** 仮想ツリーの任意の場所にある Oracle Virtual Directory の仮想 DN。
   - **Password:** ユーザー・データのバインド DN のパスワード。
4. Oracle Virtual Directory のドキュメントの説明に従って Oracle Virtual Directory を構成します。

   注意： Oracle Virtual Directory と Oracle Access Manager 間で SSL 接続を構成する場合は、10-38 ページの「Oracle Virtual Directory の SSL リスナーの構成（オプション）」を参照してください。

5. 10-35 ページの「Virtual Directory Manager のインストール」に進みます。

Virtual Directory Manager のインストール

Virtual Directory Manager を通常どおりインストールします。Oracle Access Manager との実装を容易にするために必要な特定の手段はありません。

Virtual Directory Manager のインストールの手順

1. 『Oracle Virtual Directory and Virtual Directory Manager Installation Guide』の指示に従います。
2. Oracle Virtual Directory のドキュメントに記載されているデフォルト設定を使用します。
3. Oracle Virtual Directory のドキュメントに説明に従って Virtual Directory Manager を構成します。
4. 10-36 ページの「プロジェクト領域およびサーバーの作成」に進みます。

プロジェクト領域およびサーバーの作成

Virtual Directory Manager を使用して通常どおりにプロジェクト領域およびサーバーを作成します。ここでは一部のサンプルの手順を示しますが、これらは完全なチュートリアルではありません。

詳細は、Oracle Virtual Directory のドキュメントを参照してください。

プロジェクト領域およびサーバーの作成の手順

1. 「スタート」から「VDM」を選択します。
2. Server Navigator ウィンドウの下にあるメニューから、「Directory Management Project」を選択します。
3. 一意のプロジェクト名を指定します。
4. プロジェクト名を右クリックしてから、「New」→「Server」を選択します。
5. 一意のサーバー名を入力します。
6. 「Finish」をクリックします。
7. 10-36 ページの「サンプル・アダプタおよびマッピング・テンプレートの取得 / 更新」に進みます。

サンプル・アダプタおよびマッピング・テンプレートの取得 / 更新

次の手順を実行し、Oracle Virtual Directory 内のアダプタ・テンプレート・リストでオラクル社提供の適切なサンプル・テンプレートが使用可能であることを確認する必要があります。必要に応じて、独自のテンプレートを最初から作成することもできます。オラクル社では、各データ・ストアに固有のサンプル・テンプレートと、ユーザー定義のスキーマに固有のサンプル・テンプレートの 2 種類のサンプル・テンプレートを提供しています。

サンプル・アダプタ・テンプレート : ネイティブ・データ・ストアを Oracle Virtual Directory に接続する個々のアダプタの基準として使用可能なベンダー固有のアダプタ・ファイルのサンプル・テンプレート。オラクル社提供のサンプル・アダプタ・テンプレート・ファイルは、次の場所に格納されています。

```
IdentityServer_install_dir¥identity¥oblix¥tools¥DNConversionToolkit
¥tools¥DataAnyWhere¥plugins¥OracleAccessManagerOVIDTEmplates
¥adapter_templates
```

サンプル・マッピング・テンプレート : Oracle Virtual Directory が、ネイティブ・データ・ストアによって使用されるスキーマ（またはデータベース・フィールド）を、Oracle Access Manager から参照する集約仮想ディレクトリによって使用される論理スキーマに変換できるようにするためのサンプル・マッピング・ファイル。オラクル社提供のサンプル・マッピング・テンプレートは、次の場所に格納されています。

```
IdentityServer_install_dir¥identity¥oblix¥tools¥DNConversionToolkit
¥tools¥DataAnyWhere¥plugins¥OracleAccessManagerOVIDTEmplates
¥mapping_templates
```

注意 : この時点では、サンプル・テンプレートを取得および更新するのみです。後で、これらのテンプレートを使用して各コネクタを構成し、スキーマとネームスペースのマッピングを行います。詳細は、10-43 ページの「アダプタのマッピング・ファイルの作成」および 10-44 ページの「データ・ストア・アダプタの作成」を参照してください。

Virtual Directory Manager へのサンプル・テンプレートのコピーの手順

1. 環境に適した手順を使用してオラクル社提供のテンプレートを取得および更新します。

   a. **サンプルがまだない場合 :** Virtual Directory Manager で、「Help」→「Software Updates」→「Find」→「Install」をクリックします。

   b. **自動更新、Oracle サンプルがインストールされている場合 :** インストールに適した手順を実行します。

      「Search for updates of currently installed features」を選択します。

      「Search for new features to install」を選択します。

   c. **サンプル・テンプレートの手動更新 :** 配布されている zip ファイル（COREidFeatures_10.1.4.bin.dist.zip など）を Virtual Directory Manager ディレクトリに解凍し、Virtual Directory Manager を再起動します。

      ```
      VDM_install_dir¥
      for example
      C:¥Oracle¥OViD Manager
      ```

2. 環境に応じて、次のいずれかの作業に進みます。

   - RDBMS 用の JDBC ドライバ・ライブラリのデプロイ
   - Oracle Virtual Directory の SSL リスナーの構成（オプション）
   - 最初の Identity Server のインストール

RDBMS 用の JDBC ドライバ・ライブラリのデプロイ

この手順を実行するのは、実装に RDBMS が含まれる場合のみです。

JDBC ドライバ・ライブラリのダウンロードおよびインストールと前述の手順が完了した後、次の手順を実行して各ライブラリをデプロイする必要があります。たとえば、Oracle の場合、Oracle JDBC シン・ドライバ（ojdbc14.jar 以上）をデプロイする必要があります。

また、ここで説明する内容は作業方法の概要を示すものです。詳細は、Oracle Virtual Directory のドキュメントを参照してください。

JDBC ドライバ・ライブラリのデプロイの手順

1. 10-33 ページの「実装用のリレーショナル・データベースの準備」の作業を実行します。
2. 通常どおり Virtual Directory Manager を起動し、Server Navigator ウィンドウに移動します。
3. Oracle Virtual Directory を右クリックし、メニューから「Manage Server Libraries」を選択します。
4. ファイル・メニューを選択します。
5. ファイル・メニューから「New」→「Deploy」を選択します。

   JDBC ドライバ・ファイルは、*JDBC_Driver_install_dir*/lib（C:¥Program Files¥JDBC など）に格納されています。
6. 環境に応じてライブラリを選択します。

   msbase.jar

   mssqlserver.jar

   msutil.jar
7. 通常どおりデプロイします。

Oracle Virtual Directory の SSL リスナーの構成（オプション）

次の手順が必要なのは、Oracle Access Manager と Oracle Virtual Directory 間の SSL 接続を設定する場合のみです。オープン接続を使用する場合は、この項はスキップしてください。

Oracle Virtual Directory の SSL リスナーの構成の手順

1. 次のように、秘密鍵を生成します。
   a. サーバーを右クリックし、「Server-Manager Server keys」を選択します。
   b. 「Generate Key」をクリックします。
   c. 鍵情報を入力します。

      使用する「Common Name」は、後で Oracle Access Manager で使用するホスト名と正確に同じものである必要があります。
2. 次のように、証明書リクエストを生成します。
   a. Key/Certificate ウィンドウで生成した鍵を選択します。
   b. 「Request Certificate」をクリックします。
3. 次のように、証明書リクエストに署名します。
   a. http://machine/certsrv を使用して Microsoft Certificate サービスを起動します。
   b. 「証明書の要求」リンクをクリックします。
   c. 「証明書の要求の詳細設定」リンクをクリックします。
   d. 「Base 64 エンコード CMC または PKCS #10 ファイルを使用して証明書の要求を送信するか ....」リンクをクリックします。
   e. エディタで、手順 2 で生成した証明書リクエスト・ファイルを開きます。
   f. テキストをコピーして証明書サービスの Base64 エンコード・ウィンドウにペーストします。
   g. 「証明書テンプレート」で「Web サーバー」を選択し、「送信」を選択します。
   h. CA 証明書を Base64 エンコード形式でダウンロードします。
4. 次のように、署名した証明書を Oracle Virtual Directory にインポートします。
   a. Virtual Directory Manager の Key/Certificate ウィンドウで、「Import」をクリックします。
   b. 手順 3 で取得した証明書ファイルを選択します。
   c. 手順 1 の鍵に指定されている別名とまったく同じ別名を指定します。
   d. 終了すると、鍵エントリの発行者が CA に対して更新されます。
5. 次のように、SSL を使用して LDAP リスナーを構成します。
   a. Virtual Directory Manager の「Server Navigation」ペインで、「Listeners」をクリックし、「New - Ldap Listener」を選択します。
   b. ポートを指定します。
   c. 「Server Key Alias」で、手順 4 で作成した鍵エントリを選択します。
   d. サーバーに保存します。
6. 次の条件に応じて Oracle Access Manager に証明書をインストールします。
   - **Identity Server がインストールされていない場合 :** Identity Server のインストール時に証明書を自動的にインストールできます。この場合、10-39 ページの「最初の Identity Server のインストール」にスキップしてください。
   - **Identity Server がインストールされている場合 :** 次の手順を実行し、証明書を作成およびインポートします。

7. 必要に応じて、cert8.db を作成します。
   a. *IdentityServer_install_dir*¥identity¥oblix¥tools¥certutil に移動します。
   b. 次のコマンドを発行します。

```
certutil -d IdentityServer_install_dir¥identity¥oblix¥config -N -f
```

8. 次のコマンドを使用してルート CA を Identity Server にインポートします。

```
certutil -d IdentityServer_install_dir¥identity¥oblix¥config -A -n ldap -a -t -C -i
root_ca_file
```

9. 次のように、Identity Server を再構成します。
   a. 「Identity System Console」から、「System Configuration」→「Directory Options」を選択します。
   b. 『Oracle Access Manager ID および共通管理ガイド』で説明されているように、ユーザー・プロファイルおよび DB インスタンスを検索します。
   c. SSL をマークしてから、Oracle Virtual Directory のセキュア・ポートを入力します。
   d. Identity Server を再起動します。
   e. SSL を使用するすべてのインスタンスについてこの作業を繰り返します。
   f. 『Oracle Access Manager ID および共通管理ガイド』で説明されているように、ID システムの設定を手動で再実行します。

最初の Identity Server のインストール

Oracle Virtual Directory を使用した実装を成功させるには、Oracle Access Manager のインストールを段階的に実行する必要があります。1 つ目のフェーズでは、最初の Identity Server のみをインストールします。このインストールには、Oracle Virtual Directory と統合するディレクトリ・サーバーのネイティブ・スキーマを拡張するために必要な ldif ファイルが用意されています。

Oracle Virtual Directory 用の Identity Server のインストール時には、次を指定する必要があります。

- **User Data Directory Server:** ユーザー・データ・ディレクトリ・サーバーを指定するよう求められた場合、Data Anywhere を選択します。
- **Configuration and Policy Data Directory Server:** 構成およびポリシー・データの場所を指定するよう求められた場合、ネイティブ・ディレクトリ・サーバーを指定します。構成およびポリシー・ブランチは、Oracle Virtual Directory インストールと同じホスト・マシン上に存在することはできません。

次の手順が終了すると、Oracle Virtual Directory と統合するネイティブ・ディレクトリ・サーバーのスキーマを拡張できます。

重要： ネイティブ・ディレクトリ・サーバーとともに Identity Server がインストールされている場合、10-28 ページの「既存の Oracle Access Manager インストールとの Oracle Virtual Directory の実装」を参照してから、10-41 ページの「ディレクトリ・スキーマの拡張」にスキップしてください。

最初の Identity Server のインストールの手順

1. 第 I 部「インストールの計画と前提条件」で、インストールの前提条件、要件、オプション、および Identity Server のインストールに関する考慮点を確認します。
2. 第 4 章「Identity Server のインストール」で説明されているように、最初の Identity Server のインストールを開始し、ディレクトリ・サーバーの詳細の定義に進みます。

   Oracle Access Manager の構成データは個別に格納する必要があります。後で、ユーザー・データ・ディレクトリ・サーバーと構成データ・ディレクトリ・サーバーの両方に関する詳細を指定するよう求められます。
3. データの格納先を指定するよう求められた場合、構成データは個別に格納するよう指定します。

   個別に格納する構成データ

   最初の Identity Server のインストール時にスキーマを自動的に格納することをお薦めします。スキーマは 1 回のみ更新します。「Yes」を選択すると、ディレクトリ・サーバー・タイプおよび仕様について質問されます。
4. スキーマの更新について指定を求められた場合、ユーザーおよび構成データの個別格納に対してスキーマ更新オプションの「Automatic」を選択します。
5. ユーザー・データ・ディレクトリ・サーバーの詳細の指定を求められた場合、この実装について次を指定します。

   a. **User Data Directory Server:** Data Anywhere。

   b. ユーザー・データ・ディレクトリ・サーバーの詳細 :

      Host Name: Oracle Virtual Directory をホストしているマシンの DNS ホスト名。

      Port number: ディレクトリ・サーバーがリスニングするポート : Oracle Virtual Directory の LDAP ライセンス・ポートを指定します。

      Bind DN: ユーザー・データ・ディレクトリ・サーバーについて、仮想ツリーの任意の場所にある Oracle Virtual Directory の仮想 DN を指定します。

      Password: ユーザー・データのバインド DN のパスワードを指定します。
6. 構成データ・ディレクトリ・サーバーの詳細の指定を求められた場合、この実装について次を指定します。

   a. **Configuration Data Directory Server:** ネイティブ・ディレクトリ・サーバーのタイプ。

   b. **構成データ・ディレクトリ・サーバーの詳細 :**

      Host name: Oracle Access Manager の構成データを格納するネイティブ・ディレクトリをホストしているマシンの DNS ホスト名。

      Port number: 構成データ・ディレクトリ・サーバーがリスニングするポートを指定します。

      Bind DN: 構成データ・ディレクトリ・サーバーのバインド DN に対して指定します。

      Password: 構成データのバインド DN のパスワード。
7. 通常どおりに最初の Identity Server のインストールを終了します。
8. 次の項目、10-41 ページの「ディレクトリ・スキーマの拡張」に進み、すべての項目を実行します。

重要 : Identity Server のインストールと設定は、この実装の最後の作業です。他のすべての作業を先に完了しないと、Oracle Virtual Directory の実装が失敗する可能性があります。

ディレクトリ・スキーマの拡張

ID システムでは、Person オブジェクト・クラスおよび Group オブジェクト・クラスの「フルネーム」、「ログイン」および「パスワード」のセマンティク型に割り当てられた属性が必要です。

作業を続行する前に、次の手順を実行する必要があります。

- 次の場所にある適切な ldif ファイルを使用して、Oracle Access Manager の属性を使用してバックエンド・ネイティブ・ディレクトリ・スキーマを拡張します。

  IdentityServer_install_dir¥identity¥oblix¥tools¥DNConversionToolkit¥tools¥DataAnyWhere¥OblixUserSchema¥*directory*_user_schema_add.ldif

- 次の場所にある VDE_user_schema_add.ldif ファイルを使用して、Oracle Access Manager の属性を使用して Oracle Virtual Directory スキーマを拡張します。

  IdentityServer_install_dir¥identity¥oblix¥tools¥DNConversionToolkit¥tools¥DataAnyWhere¥OblixUserSchema¥VDE_user_schema_add.ldif

ディレクトリ・スキーマの拡張の手順

1. 仮想ディレクトリに含める準備をするバックエンド・ディレクトリ・サーバーのスキーマを拡張するときに使用する、次のような ldif ファイルを検索します。

   IdentityServer_install_dir¥identity¥oblix¥tools¥DNConversionToolkit¥tools¥DataAnyWhere¥OblixUserSchema/

2. 仮想ディレクトリに含める特定のバックエンド・ディレクトリ・サーバーごとに属性を手動で構成するためのガイドとして、表 10-6 を使用します。

注意： 適切な *.ldif ファイルが *IdentityServer_install_dir*¥identity¥oblix¥tools¥DNConversionToolkit にない場合、*IdentityServer_install_dir*¥identity¥oblix¥data¥common にある対応する *.ldif ファイルを使用できます。

表 10-6 Oracle Access Manager の属性を使用してネイティブ・スキーマを拡張するためのファイルおよびコマンド

ディレクトリ・サーバーおよび ldif ファイル	スキーマの手動更新コマンド
Active Directory ADUserSchema.ldif または ADAuxSchema.ldif （環境に応じて異なる）	ldifde -s host -t port -a bind-dn -w password -c fromDN toDN -i -f ADuserSchema.ldif
ADAM ADAM_user_schema_add.ldif または ADAMAuxSchema.ldif （環境に応じて異なる）	ldifde -s host -t port -a bind-dn -w password -c fromDN toDN -i -f ADAM_user_schema_add.ldif
SunONE ■ iplanet_user_schema_add.ldif	ldapmodify -h host -p port -D bind-dn -w password -a -f iplanet_user_schema_add.ldif
■ iplanet5_user_index_add.ldif	ldapmodify -h host -p port -D bind-dn -w password -a -f iplanet5_user_index_add.ldif

表 10-6 Oracle Access Manager の属性を使用してネイティブ・スキーマを拡張するためのファイルおよびコマンド（続き）

ディレクトリ・サーバーおよび ldif ファイル	スキーマの手動更新コマンド
eDirectory ■ NDS_user_schema_add.ldif	ldapmodify -h host -p port -D bind-dn -w password -a -f NDS_user_schema_add.ldif
■ NDS_user_index_add.ldif	ldapmodify -h host -p port -D bind-dn -w password -a -f NDS_user_index_add.ldif
IBM ■ v3.user.ibm_at.ldif	ldapmodify -h host -p port -D bind-dn -w password -a -f v3.user.ibm_at.ldif
■ v3.user.ibm_oc.ldif	ldapmodify -h host -p port -D bind-dn -w password -a -f v3.user.ibm_oc.ldif

3. インストール内のディレクトリ・サーバーごとにこの手順を繰り返します。

重要： 既存の Oracle Access Manager インストールを使用して作業している場合は、次の手順を使用して Oracle Virtual Directory スキーマを手動で拡張する必要があります。

---

4. 次のように、VDE_user_schema_add.ldif ファイルを使用して、Oracle Access Manager の属性を使用して Oracle Virtual Directory スキーマを手動で拡張します。

```
IdentityServer_install_dir¥identity¥oblix¥tools¥DNConversionToolkit/oblix/tools
/DataAnyWhere/OblixUserSchema/VDE_user_schema_add.ldif
ldapmodify -h host -p port -D bind-dn -w password -a -f
```

5. 次のように、すべてのバックエンド・データ・ソースが示されるように Oracle Virtual Directory スキーマを拡張します。

   - バックエンド・ディレクトリの属性を Oracle Virtual Directory スキーマに追加します。

     Active Directory の例： user または inetOrgPerson オブジェクト・クラスの属性を Oracle Virtual Directory の inetOrgPerson オブジェクト・クラスに対して更新 / 追加します。

     データベースの例： Oracle の従業員表の属性を inetOrgPerson オブジェクト・クラスに追加します。

   - または、ネイティブ・データ・ストアから参照可能なすべての属性を持つ新しいオブジェクト・クラスを作成します。

     Active Directory の例： user または inetOrgPerson オブジェクト・クラスのすべての必須属性を持つ新しいオブジェクト・クラス（MyCompanyPerson）を作成します。

     データベースの例： Oracle の従業員表から参照可能なすべての属性を持つ新しいオブジェクト・クラス（MyCompanyPerson）を inetOrgPerson オブジェクト・クラスに対して作成します。

注意： スキーマの拡張を行うには、VDM のユーザー・インタフェース（「VDM」→「*Your_Project*」→「*Your_Server*」→「Engine」→「Schema」）を使用します。拡張したスキーマが ldif ファイル内にある場合、ldapmodify を使用してこのスキーマを Oracle Virtual Directory インスタンスにロードします。

アダプタのマッピング・ファイルの作成

後で開発するデータ・ストア・アダプタに必要なマッピング・ファイルを作成できます。

- 各マッピング・ファイルにより、バックエンド・スキーマをフロントエンド（Oracle Virtual Directory）スキーマに変換するフィルタが生成されます。
- 各マッピング・ファイルを使用して、データ・ストアのインバウンドおよびアウトバウンド・データをマップし、不適切なデータを削除できます。

独自のマッピング・ファイルを最初から作成することも、複数のプラグインを含むオラクル社提供のサンプル・ファイルを使用することも可能です。詳細は、10-74 ページの「Oracle Access Manager と Oracle Virtual Directory の実装のテンプレート」を参照してください。

次の手順では、オラクル社提供のサンプル・ファイルを使用します。ここでは、これらの手順をガイドとして使用します。この手順は、LDAP マッピング・ファイルと RDBMS マッピング・ファイルのどちらでも同じです。

VDM の使用の詳細は、Oracle Virtual Directory のドキュメントを参照してください。

データ・ストア・アダプタのマッピング・ファイルの作成の手順

1. 10-36 ページの「サンプル・アダプタおよびマッピング・テンプレートの取得 / 更新」の作業を実行し、オラクル社提供のサンプル・マッピング・ファイルを用意します。
2. VDM の Server Navigator ウィンドウで、Oracle Virtual Directory サーバーを選択します。
3. Oracle Virtual Directory から「Engine」を選択し、エンジン・メニューから「Mapping」を選択します。
4. 「Mapping」を右クリックしてから、「New Mapping」を選択します。

   表示される New Mapping ウィンドウの「File」リストには、以前に VDM にコピーしたサンプル・マッピング・テンプレートの名前が含まれています。
5. 要求される情報を指定します。
   - File Name: 変更するバージョンを示す一意の名前を入力します。
   - Server: プロジェクトが含まれるサーバーを指定します。
   - File template: 必要なサンプル・マッピング・テンプレートを選択します。

   後で使用するために保持する必要があるサンプル・テンプレートが変更によって上書きされないように、新しい名前を割り当てる必要があります。
6. 「Name」フィールドで、変更するバージョンを示す一意の名前を入力します。
7. 「Finish」をクリックします。

   名前がウィンドウの左側に表示されます。
8. Virtual Directory Manager の Server Navigator ウィンドウで、作成したファイル名を選択し、ウィンドウの右側に表示します。

   ID システムのインストールおよび設定を終了する前に、マッピング・ファイルをカスタマイズし、データ・ストア・アダプタに追加する必要があります。マッピング・ファイルはここでカスタマイズすることも、後でカスタマイズすることも可能です。
9. 次のように作業を続行します。
   - 通常どおりにマッピング・ファイルをサーバーにデプロイします。
   - 10-44 ページの「データ・ストア・アダプタの作成」に進みます。

   マッピング・スクリプトは、必要に応じてここで変更することも、データ・ストア・アダプタを作成した後に変更することもできます。ファイルをカスタマイズしてアダプタに含める場合、10-52 ページの「アダプタおよびマッピング・ファイルのカスタマイズ」を参照してください。

- オラクル社提供のサンプル・ファイルを使用していない場合、ダミー・ユーザーの作成が必要な場合があります（E-13 ページの「予期しないグループ削除の問題」を参照）。
- オラクル社提供のサンプル・ファイルを使用している場合、これは自動的に行われます。

データ・ストア・アダプタの作成

ここで、接続するデータ・ストアごとにアダプタを作成する必要があります。

- **ディレクトリ :** 10-44 ページの「LDAP ディレクトリのアダプタの作成」で説明されているように、LDAP アダプタを作成します。
- **データベース :** 10-48 ページの「データベース・アダプタの構成」で説明されているように、データベース・アダプタを作成します。
- **分割プロファイル :** データ・ストアごとに個別のアダプタを作成してから、2 つのデータ・ソースを単一のビューに結合するアダプタを作成します。詳細は、10-49 ページの「分割プロファイル・アダプタの作成」を参照してください。
- **複数のディレクトリ :** 10-51 ページの「複数ディレクトリのアダプタの作成」で説明されているように、Oracle Virtual Directory アダプタに各データ・ソースを接続するための個別のアダプタを作成します。

アダプタを最初から作成することもできますが、オラクル社提供のサンプル・テンプレートを使用すると、作業を簡略化できます。オラクル社提供のサンプル・アダプタ・テンプレートを使用する場合、アダプタを作成するために接続および資格証明情報、論理ルート、リモート・ルートなどを入力する必要があります。また、データ・ストアごとに設定を変更および調整する必要もあります。アダプタを作成した後、テンプレートに定義されている情報がこのアダプタに設定されます。

Oracle テンプレートの詳細は、10-74 ページの「Oracle Access Manager と Oracle Virtual Directory の実装のテンプレート」を参照してください。テンプレートの変更の詳細は、10-52 ページの「アダプタおよびマッピング・ファイルのカスタマイズ」を参照してください。

LDAP ディレクトリのアダプタの作成

ホスト・ディレクトリ・サーバーに関係なく、LDAP アダプタの作成の手順は同じです。最初に LDAP アダプタを作成してから、マッピング・ファイルなどのプラグインを追加します。

次に説明するように、ADAM および Active Directory アダプタには、他のアダプタにはない要件があります。

Active Directory および ADAM アダプタについて : Active Directory および ADAM にはそれぞれ 2 つのアダプタが必要です。1 つは最初に作成する必要がある SSL 用のアダプタで、もう 1 つは 2 番目に作成する必要があるオープン接続用のアダプタです。オラクル社は、これらのアダプタごとに個別のサンプル・テンプレートを提供しています。この環境の設定には、次の作業が含まれます。

- SSL 接続用の Active Directory または ADAM アダプタの作成
- オープン接続用の Active Directory または ADAM アダプタの作成

Active Directory および ADAM アダプタには 2 つのプラグインが必要です。オラクル社提供のサンプル・テンプレートを使用する場合、次の 2 つのプラグインがすでに用意されています。ただし、独自のテンプレートを作成する場合、次の 2 つのプラグインを手動で追加する必要があります。

- **Active Directory のパスワード・プラグイン :** Active Directory および ADAM では、セキュア・モードを使用してパスワードを設定または変更する必要があります。

  パフォーマンス上の問題に対応するために、「Password Only SSL」モードがサポートされています。この場合、通常の操作はオープン接続を使用してアダプタを介して行われますが、パスワードの変更 / 設定機能に関する操作は SSL 接続を使用してアダプタにリダイレクトされます。

注意 : オラクル社提供のサンプル・テンプレートを使用しない場合、10-45 ページの「LDAP のアダプタの作成の手順」で説明されているように、Active Directory のパスワード・プラグインとして作成する SSL アダプタを作成対象のオープン接続アダプタに追加する必要があります。

- **Active Directory の範囲属性プラグイン :** Active Directory および ADAM では、Active Directory の範囲属性プラグインを使用してグループ・ページ問題を処理する必要があります。

  このプラグインは、Active Directory/ADAM から返されるすべてのグループ・ページを連結し、この情報を 1 つの結果として Oracle Virtual Directory クライアントに返します。

  注意 : オラクル社提供のサンプル・テンプレートを使用する場合、この値を編集してください。オラクル社提供のサンプル・テンプレートを使用しない場合、Active Directory の範囲属性プラグインを作成し、作成対象のオープン接続アダプタに追加する必要があります。

すべての LDAP ディレクトリを対象として 1 つの汎用手順が用意されています。この例には、ADAM 用の 2 つのアダプタを作成するための手順が含まれています（オラクル社提供の例を使用していない場合）。

注意 : Active Directory または ADAM 用としてオラクル社提供のテンプレートを使用する場合、作成が必要なオープン・コネクタの詳細は、手順 17 を参照してください。SSL コネクタは Oracle テンプレートに含まれています。

LDAP のアダプタの作成の手順

1. 10-52 ページの「アダプタおよびマッピング・ファイルのカスタマイズ」の作業を実行し、オラクル社提供のサンプル・アダプタ・テンプレートを用意します。
2. Virtual Directory Manager で、「Adapters」に移動し、「New」→「LDAP Adapter」をクリックし、「Adapter configuration」画面を表示します。
3. 「Adapter Template」リストから適切なアダプタ・タイプを選択します。

   例 :

   Adapter Template: OblixADAMSSLAdapterUsingMapper
4. 一意のアダプタ名を入力します。

   例 :

   Adapter Name: CustomAdamSSLAdapter
5. 接続する LDAP サーバーのサーバー・アドレス、サーバー・プロキシ・ポートおよびサーバー・プロキシ・バインド DN を入力します。
6. プロキシ・パスワードおよびパススルー資格証明を指定します。

   例 :

   Proxy Password: xxxxxxxx

   Passthrough credentials: Always

   「Always」を指定するとパフォーマンスに影響する可能性がありますが、「Bind Only」または「Never」を使用するとセキュリティが低下します。

   次に、接続オプションを指定します。

注意： オラクル社提供のテンプレートや ADAM または Active Directory を使用しない場合、オープン接続アダプタのプラグインとして含める SSL アダプタを作成します。

7. SSL バージョンの接続オプション（オラクル社提供のテンプレートを使用する場合は必要なし）として、次を選択します。

   Connection Options: Secure SSL/TLS

   この手順により、データ・ストアに接続され、証明書が自動的にダウンロードされます。

8. リモート・ベースについては、省略記号（...）のボタンをクリックします。

   接続する LDAP ディレクトリ・サーバーの検索ベース（ルート DN）を示す画面が表示されます。

   この時点で、物理ネームスペースを論理ネームスペースにマップする必要があります。

9. バックエンド・データ・ストアからリモート物理ネームスペース（検索ベース）を選択します。次に例を示します。

   ```
   ou=company,c=us,dc=intranet,dc=pspl,dc=co,dc=in
   ```

10. 「Mapped Namespace」フィールドで、Oracle Virtual Directory の論理ネームスペースを入力します。

    たとえば、Oracle Virtual Directory のルートの接尾辞が o=MyCompany,c=us である場合、次のようなマップされたネームスペースを使用できます。

    ```
    ou=ADAM,o=MyCompany,c=us
    ```

11. 「Finish」をクリックします。

    新しく作成した LDAP アダプタが Server Navigator ウィンドウの「Adapter」リストの下に表示されます。

12. Server Navigator ウィンドウで新しいアダプタ名をクリックします。

    a. 右側のペインで「Routing」タブをクリックします。

    b. これが Active Directory または ADAM の SSL アダプタである場合、「General Settings」で、可視性が内部に設定されていることを確認します。

       例 :

       General Settings

       Visibility: Internal

    c. 「Finish」をクリックします。

    Oracle Access Manager が正常に機能するには、製品で使用される DN 属性（manger、secretary、uniqueMembers など）が、表示時に論理ビュー形式に変換され、格納時に物理形式に戻される必要があります。

13. Optional: DN Attributes:

    a. 作成したアダプタをダブルクリックします。

    b. 右側のウィンドウで「Config」タブをクリックします。

    c. 「Settings」で、すべてのオブジェクト・クラス / 表について Oracle Virtual Directory 属性のカンマ区切りリストで「DN Attributes」を指定します。

14. Server Navigator ウィンドウでアダプタ名を右クリックし、「Save to Server」を選択します。

    これで第 1 アダプタは完了です。この手順を実装内のデータ・ストアごとに繰り返す必要があります。

    この手順を ADAM の第 2 アダプタに対して繰り返す必要がある場合、そのときはオープン接続を使用します。

    注意 : 次の手順では、前に作成した SSL アダプタと、ADAM および Active Directory に対して作成が必要なオープン接続アダプタの違いのみを示します。他のすべての仕様は同じです。

    ---

15. ADAM/Active Directory のオープン接続アダプタ : 次の異なる仕様を使用して前の手順を繰り返し、必要なオープン接続アダプタを作成します。たとえば、次のようにします。

    Adapter Template: OblixADAMAdapterUsingMapper

    Adapter Name: CustomAdamOpenAdapter

    Port: open_port

    Connection Options: （どちらのボックスも選択なし）

    Searchbase: SSL アダプタと同じ

    Visibility: Yes

16. **Optional:** DN Attributes: オラクル社提供のサンプル・テンプレートを使用せずに作成した Active Directory または ADAM アダプタの場合、前に作成した SSL アダプタで使用したリストと同じにする必要があります。

    a. 作成した Active Directory アダプタをダブルクリックします。

    b. 右側のウィンドウで「Config」タブをクリックします。

    c. 「Settings」で、すべてのオブジェクト・クラス / 表について Oracle Virtual Directory 属性のカンマ区切りリストで「DN Attributes」を指定します。

17. 通常どおり保存およびデプロイします。

18. 次のように作業を続行します。

    - 詳細は、10-64 ページの「マッピング・ファイルを参照するためのアダプタ・プラグインの編集」を参照してください。
    - 10-52 ページの「アダプタおよびマッピング・ファイルのカスタマイズ」も参照してください。
    - 必要に応じてその他の LDAP アダプタを作成するか、次に説明するようにデータベース・アダプタを作成します。

データベース・アダプタの構成

使用環境とは関係ない場合、この手順はスキップできます。

次の手順は一般的な例です。これらは環境によって異なります。

データベース・アダプタの構成の手順

1. 10-37 ページの「RDBMS 用の JDBC ドライバ・ライブラリのデプロイ」の作業を実行します。
2. Virtual Directory Manager で、「Adapters」→「New」→「Database Adapter」を選択し、「Adapter configuration」画面を表示します。
3. 10-82 ページの「データベース・テンプレート : OblixDBAdapterUsingScript」に記載されている OblixDBAdapterUsingScript を選択します。
4. 一意のアダプタ名を入力します。
5. マッピング用の論理ネームスペース DN を入力します。
6. 「use predefined database」を選択します。
7. 接続するデータベースのタイプ（MS SQL Server など）を選択します。
8. データベース・サーバーのホスト、ポート、データベース名、ユーザー名およびパスワードを入力します。
9. 「Validate Connection」をクリックして接続情報が正しいかどうかを確認し、「Next」をクリックします。
10. 環境に応じて次に進みます。
    - **その他のテンプレート :** オラクル社提供のテンプレートを使用していない場合、説明に従って手順 11、12、13 および 14 を実行します。
    - **オラクル社提供のテンプレート :** 手順 11、12、13 および 14 でオラクル社提供の 10-82 ページの「データベース・テンプレート : OblixDBAdapterUsingScript」テンプレートを使用する場合、「Next」をクリックするのみです。
11. 「database adapter mapping Choose table」画面で、次の手順を実行します。
    a. 使用する表を左側のペインから選択します。
    b. 「>」をクリックして右側のペインに移動します。
    c. 「Next」をクリックします。
12. 「database adapter mapping: Build Joins」画面は、「Next」をクリックしてスキップします。
13. 「database adapter mapping: map attributes」画面で、次の手順を実行します。
    a. 前に指定した論理 DN をクリックします。
    b. 「Add」をクリックし、階層を追加します。
    c. ポップアップ・ウィンドウで、次の作業を実行します。

       オブジェクト・クラスで、マップ先の LDAP オブジェクト・クラス（inetorgperson など）を入力します。

       「RDN」フィールドで、RDN 属性名（cn など）を入力します。

       「OK」をクリックします。
14. 「database adapter mapping: map attributes」画面で、次の手順を実行します。
    a. 作成したノード（cn= inetorgperson など）をクリックします。
    b. 「Add」をクリックします。
    c. ポップアップ・ウィンドウで、ldap 属性、表名および表の列を選択します。

LDAP 属性名が（obuseraccountcontrol など）がリストにない場合、入力できます。

d. マップ対象のすべての属性がマップされるまでこの作業を続行します。

注意： Oracle Access Manager が正常に動作するには、少なくとも cn、uid、password および obuseraccountcontrol フィールドをマップする必要があります。obuseraccountcontrol がアクティブであることを確認してください。

---

e. password および obuseraccountcontrol 列が既存の表に含まれていない場合、これらの列を表に追加します。

15. 「Finish」をクリックします。

これで、新しく作成した DB アダプタが Server Navigator ウィンドウの「Adapter」リストの下に表示されます。

16. Server Navigator ウィンドウでアダプタ名を右クリックし、「Save to Server」を選択します。

17. 「Browser」ペインで「Client」ビューを確認し、構成を検証します。

18. **すべての環境が対象：**次のように作業を続行します。

- 10-52 ページの「アダプタおよびマッピング・ファイルのカスタマイズ」も参照してください。
- 10-64 ページの「マッピング・ファイルを参照するためのアダプタ・プラグインの編集」で説明されているように、マッピング・ファイルをこのアダプタに追加します。
- 次に示すように、その他のアダプタを作成します。

分割プロファイル・アダプタの作成

分割プロファイルでは、同じユーザーの様々な属性が異なるディレクトリ・サーバーに格納されています。

プライマリ・データ・ストアには重要な属性が含まれ、セカンダリ・データ・ストアにはオプションの属性が含まれます。たとえば、2 つの異なるディレクトリ・サーバー・タイプおよび RDBMS があるとします。この場合、分割プロファイル・アダプタを作成してこれらのビューを結合する必要があります。

分割プロファイル・アダプタを作成するには、個々のデータ・ストア・アダプタを作成する必要があります。プライマリ・アダプタとセカンダリ・アダプタではそれぞれ「Visibility」を「Internal」に設定し、Oracle Virtual Directory からのみこれらが認識できるようにする必要があります。

分割プロファイル・アダプタを作成する場合、プライマリ・アダプタおよびこのプライマリ・アダプタに対するバインド対象を識別します。分割プロファイル・アダプタを作成した後、プライマリ・アダプタおよび結合対象の第 1 セカンダリ・アダプタを識別する結合ルールを指定します。結合ルールを指定する場合、プライマリ・アダプタを複数のセカンダリ・アダプタに結合するよう指定できます（1 対多）。

注意： オラクル社は、結合ビュー・アダプタ・テンプレートを提供しています。

分割プロファイルの検索ベース（Oracle Virtual Directory はこれをルート・ベースとして参照）は、プライマリ・ディレクトリの検索ベースと同じである必要があります。

分割プロファイル・アダプタの論理ビューがプライマリ・データ・ストアと同じであることを確認する必要があります。分割プロファイル・アダプタは、プライマリ論理ビューの DN 属性値を分割プロファイル論理ビュー（またはこの逆）にマップしません。

後述の手順では、結合ビュー方式を使用して一般的な方法について説明します。詳細は、Oracle Virtual Directory のドキュメントを参照してください。この例では、ADAM がプライマリ・アダプタ、Sun がセカンダリ・アダプタとして使用されています。この場合、ADAM 用として作成したオープン接続アダプタを使用します。これは、このアダプタには、SSL アダプタを含む適切なプラグインが含まれるためです。これらは環境によって異なります。

分割プロファイル・アダプタの作成の手順

1. 10-44 ページの「LDAP ディレクトリのアダプタの作成」で説明されているように、結合するデータ・ストアごとにアダプタを作成します。
2. Virtual Directory Manager の Server Navigator ウィンドウで、Oracle Virtual Directory サーバーを選択し、「Engine」を選択します。
3. 「Adapters」を右クリックし、「New」を選択して「Join View Adapter」を選択します。
4. ダイアログ・ボックスの「Adapter Template」で、デフォルトの結合ビュー・テンプレートを選択します。
5. 「Adapter Name」フィールドで、カスタマイズしたバージョンを示す一意の名前を入力します。

   例 :

   Adapter Name: CustomJoinADAMSun
6. 「Adapter Suffix/Namespace」リストで、プライマリ・アダプタの DN と同じネームスペース（ベース DN）を入力します。

   この例では、プライマリ・アダプタは ADAM です。SSL アダプタがプラグインとして含まれるオープン接続アダプタの名前を指定する必要があります。
7. 「Primary Adapter」フィールドで、プライマリ・アダプタを選択します。

   例 :

   Primary Adapter: CustomAdamAdapter
8. 「Binding Adapter」リストで、同じアダプタを選択します。

   例 :

   Binding Adapter: CustomAdamAdapter
9. 「Finish」をクリックします。

   アダプタ名が左側のペインに表示され、Join View Primary Adapter Configuration ウィンドウが右側に表示されます。
10. Join View Primary Adapter Configuration ウィンドウの「Settings」領域で、プライマリおよびバインディング・アダプタの設定を入力します。

    例 :

    Settings

    Primary Adapter: CustomAdamAdapter

    Binding Adapter: CustomAdamAdapter
11. 「Join Rules」の横にある「New」ボタンをクリックし、「Enter Join Rules」ダイアログを表示します。
12. 「Enter Join Rules」ダイアログで、結合するセカンダリ・アダプタを選択し、環境に応じたタイプ・クラスおよび条件を選択します。

    例 :

    Joined Adapter: CustomSunAdapter

    Type Class: One to Many Joiner

    Conditions: cn=cn

13. 別のアダプタを結合する場合は手順 12 を繰り返し、結合しない場合はこの手順はスキップします。
14. Server Navigator ウィンドウでアダプタ名を右クリックし、「Save to Server」を選択します。
15. Browser ウィンドウで新しい構成、「Client View」を確認します。

複数ディレクトリのアダプタの作成

Oracle Virtual Directory の背後に複数のディレクトリ・サーバーがある場合、次に示すように、Oracle Virtual Directory 内にローカル・データ・ストア・アダプタのエントリを作成し、ID システムの検索ベースとして使用される Oracle Virtual Directory の仮想ルート用のエントリを追加する必要があります。

タスクの概要 : 複数ディレクトリのアダプタの作成

1. 次に示すように、結合するデータ・ストアごとにアダプタを作成します。
   - LDAP ディレクトリのアダプタの作成
   - データベース・アダプタの構成
2. 各ディレクトリ・サーバーによって同じ検索ベースが使用され、複数ディレクトリのアダプタがルートであることを確認します。
3. 10-51 ページの「ローカル・データ・ストア・アダプタの作成」の作業を実行します。
4. 10-52 ページの「仮想ルートの物理ノードの作成」の作業を実行します。

ローカル・データ・ストア・アダプタの作成

Oracle Access Manager でローカル・ストア・アダプタが必要になるのは、複数のアダプタのエントリの親エントリである仮想エントリを作成し、1 つの連続したツリーが存在するように見えるようにする場合のみです。

たとえば、2 つのディレクトリがあり、これらのディレクトリが含まれるディレクトリ・ツリーを作成するとします。

ディレクトリ 1: ou=Marketing,o=Company

ディレクトリ 2: ou=Product,o=Company

このような条件で、o=Company レベルから検索し、ディレクトリ 1 とディレクトリ 2 の両方を網羅する検索を行う場合、ローカル・ストア・アダプタを使用し、1 つのエントリ `o=Company` を唯一のエントリとして作成できます。これにより、次のような完全ツリーが生成されます。

o=Company: Oracle Access Manager はここから検索可能

/ ¥

ou=Marketing ou=Product

ローカル・データ・ストア・アダプタが必要なのは、次の場合のみです。

- 個々のすべてのデータ・ストア・アダプタを対象とした統合検索ベースが必要な場合
- 個々のすべてのデータ・ストア・アダプタのルート検索ベースが同じ場合
- データ・ストアのエントリが重複していない（重複エントリが削除されているか、フィルタを使用して除外されている）場合

次の手順は一般的な手順です。詳細は、Oracle Virtual Directory のドキュメントを参照してください。

Oracle Virtual Directory のアダプタ・エントリの作成の手順

1. Virtual Directory Manager で、「Adapters」に移動します。
2. 「Adapters」を右クリックします。
3. 「New」→「Local Store Adapter」を選択し、「Adapter configuration」画面を表示します。
4. アダプタの接尾辞（すべてのアダプタの共通仮想ルート・ベース）を指定します。
5. 通常どおりサーバーに保存します。
6. 10-52 ページの「仮想ルートの物理ノードの作成」に進みます。

仮想ルートの物理ノードの作成

複数のディレクトリ用のローカル・データ・ストア・アダプタのエントリを作成した後、Oracle Virtual Directory ディレクトリに物理ノードを作成する必要があります。これは、ID システム設定によって構成ノードがグローバル検索ベースとして読み取られるためです。仮想ルートの物理ノードは、通常どおりに ldp ユーティリティを使用して作成します。

Virtual Directory Manager の使用の詳細は、Oracle Virtual Directory のドキュメントを参照してください。

仮想ルートの物理ノードの作成の手順

1. ldp または ldapmodify ユーティリティを検索します。
2. Oracle Virtual Directory の仮想ルートのエントリを追加します。

   たとえば、仮想ルートが `o=Company, c=us` である場合、次のエントリを追加します。

   dn:o=Company,c=us

   Objectclass: organization

   o: Company
3. 各ディレクトリ・サーバーによって同じ検索ベースが使用され、複数ディレクトリのアダプタがルートであることを確認します。
4. 10-52 ページに進みます。

アダプタおよびマッピング・ファイルのカスタマイズ

次の各項目は、Oracle Access Manager の使用方法に関する仕様について説明しています。

カスタマイズの例

前述の説明のとおり、独自のテンプレートを最初から作成することも、オラクル社提供のサンプルをカスタマイズすることもできます。オラクル社提供のサンプルには、次の 2 つのタイプがあります。

サンプル・アダプタ・テンプレート : ネイティブ・データ・ストアを Oracle Virtual Directory に接続する個々のアダプタの基準として使用可能なベンダー固有のアダプタ・ファイルのサンプル・テンプレート。

> **注意 :** オラクル社提供のサンプル・テンプレートは、1 つのデータ・ストアと特定のユーザー定義のスキーマの両方に固有のテンプレートです。これらは環境によって異なります。

サンプル・マッピング・ファイル : Oracle Virtual Directory が、ネイティブ・データ・ストアによって使用されるスキーマ（またはデータベース・フィールド）を、Oracle Access Manager から参照する集約仮想ディレクトリによって使用される論理スキーマに変換できるようにするためのサンプル・マッピング・ファイル。

次の例は、環境に応じて作成可能なオラクル社提供のサンプルに対する変更のタイプを示します。これらの例に含まれる情報および特定の変更内容は、説明のみを目的としています。これらは環境によって異なります。

- Active Directory 用のマッピング・スクリプトのカスタマイズ
- Oracle データベース用のマッピング・スクリプトのカスタマイズ
- Oracle データベース用のアダプタのカスタマイズ

Active Directory 用のマッピング・スクリプトのカスタマイズ

この項の例は、Active Directory ディレクトリ・サーバーのマッピング・ファイルのカスタマイズ・バージョンを示します。この例は、Active Directory ディレクトリ・サーバー用としてオラクル社提供のサンプル・テンプレートと、ここには含まれていない特定のユーザー定義のスキーマから開始します。

> **注意 :** DN 変換ツールキットは、Identity Server インストールの一部として自動的にインストールされます。*IdentityServer_install_dir*¥identity¥oblix¥tools¥DNConversionToolkit¥oblix¥ を参照してください。

Active Directory に対して行われたマッピング・スクリプトの変更タイプの確認の手順

1. Virtual Directory Manager コンソールで、サンプルの OblixADMapping ファイルをベースとして使用してマッピング・ファイルを作成します（10-43 ページの「アダプタのマッピング・ファイルの作成」を参照）。

   IdentityServer_install_dir¥identity¥oblix¥tools¥DNConversionToolkit¥oblix¥¥tools¥DataAnyWhere¥plugins¥OracleAccessmanagerOViDTemplates¥mapping_templates¥OblixADMapping_mpy.xml

2. 環境に応じてマッピング・ファイルを変更し、手順 4 の下に示される Active Directory 用のマッピング・ファイルとこのカスタマイズ・バージョンを比較します。
3. マッピング・スクリプトを通常どおり保存およびデプロイします。
4. マッピング・スクリプトを後で使用するためのテンプレートとして保存します。
   - 新しいマッピング・テンプレート名（MyADMapping など）を右クリックします。
   - 「Save as template」を選択します。

```
<?xml version="1.0" encoding="UTF-8" ?> ...
# Mapping template for: Custom Data sets
#
#   Target DS: AD  : - using static Auxiliary objectclass
#   Target user objectclasses: User and group
#   Target custom schema:
#      AD_custom_schema_add.ldif
#      AD.NET_custom_schema_add.ldif
#
# Functions:
#   a. maps AD user to inetOrgPerson
#   b. maps AD group to groupofuniquenames
#   c. filters out auxiliary class from objectclass in add/modify
#   d. filter out AD system attributes
#   e. set native flag useraccountcontrol when user is activated/deactivated
#   f. set grouptype to 8
#
def inbound():
   #first rename the attributes

renameAttribute({'uniqueMember':'member','owner':'managedby','uid':'samaccountname'
})

renameAttribute({'carlicense':'gencarlicense','departmentnumber':'gendepartmentnumb
er'})

   #temporary.
   removeAttribute('nsaccountlock')

   #map object class names
   revalueAttribute('objectclass','groupofUniqueNames','group')
   revalueAttribute('objectClass','inetOrgPerson','user')

   #If static auxiliary class is used on AD, AD does not like to mention
   #the auxiliary classes in the objectclass attribute. If dynamic auxiliary
   #class is used on AD, comment these out.
   removeAttributeValue('objectclass','person')
   removeAttributeValue('objectclass','organizationalPerson')
   #removeAttributeValue('objectclass','inetOrgPerson')
   removeAttributeValue('objectclass','oblixOrgPerson')
   removeAttributeValue('objectclass','oblixpersonpwdpolicy')
   removeAttributeValue('objectclass','oblixadvancedgroup')
   removeAttributeValue('objectclass','oblixgroup')
   removeAttributeValue('objectclass','oblixAuxLocation')
   #--- Remove custom data auxiliary object classes
   removeAttributeValue('objectclass','genAuxLocation')
   removeAttributeValue('objectclass','genAuxUserEquipment')
   removeAttributeValue('objectclass','genAuxUserNetwork')
   removeAttributeValue('objectclass','genAuxUserPersonal')
   removeAttributeValue('objectclass','genAuxUserSecurity')

   #If static auxiliary class is used in AD, remove the objectclass attribute
   #during modify. AD does not like the mentioning of the auxiliary class.
   if operation == 'modify':
      removeAttribute('objectClass')

   #set the native flag useraccountcontrol based on the value of
obuseraccountcontrol.
   if haveAttribute('obuseraccountcontrol'):
      copyAttribute('obuseraccountcontrol','userAccountControl')
      #during modify, read the user entry first.
      if operation == 'modify':
         currentUser = getByName(name)
```

```
            val = int(`getAttributeValues(currentUser,'userAccountControl')[0]`)
         else:
            val = 546
         #Deactivate - set the 2nd bit
         revalueAttribute('userAccountControl','ObWfPendingActivate',`val | 0x0002`)
         revalueAttribute('userAccountControl','DEACTIVATED',`val | 0x0002`)
         revalueAttribute('userAccountControl','ObWfPendingDeactivate',`val | 0x0002`)
         #Activate - set the 2nd bit
         revalueAttribute('userAccountControl','ACTIVATED',`val & ~0x0002`)

      #when adding a group entry, add the grouptype and samaccountname.
      #groupType is hard coded here. If multiple group types are to be supported,
      #configured grouptype in VDE for user to enter.
      if operation == 'add':
         if haveAttributeValue('objectClass','group'):
            addAttributeValue('groupType','8')
            if not haveAttribute('samaccountname'):
               copyAttribute('cn','samaccountname')
            #remove these attributes as they are not in AD group. It is better not
            #configure them in COREid if not used.
            #removeAttribute ('businessCategory')
            removeAttribute ('seeAlso')
            removeAttribute ('o')

         #if haveAttributeValue('objectClass','user'):
            #removeAttributeValue('objectclass','person')
            #removeAttributeValue('objectclass','organizationalPerson')
            #removeAttributeValue('objectclass','inetOrgPerson')

      if operation == 'modify':
         currentEntry = getByName(name)
         val = getAttributeValues(currentEntry,'objectclass')
         if DirectoryString('group') in val:
            #removeAttribute ('businessCategory')
            removeAttribute ('seeAlso')
            removeAttribute ('o')

      #filter out obgroupcreator otherwise iplanet user cannot create ad group.
      if haveAttribute ('obgroupcreator'):
         removeAttribute ('obgroupcreator')

      return

   def outbound():
      #first rename the attributes

   renameAttribute({'member':'uniqueMember','managedby':'owner','samaccountname':'uid'
   })

   renameAttribute({'gencarlicense':'carlicense','gendepartmentnumber':'departmentnumb
   er'})

      #map object class names
      revalueAttribute('objectClass','group','groupofUniqueNames')
      revalueAttribute('objectClass','user','inetOrgPerson')

      #filter out AD system atrributes
      removeAttribute ('allowedAttributes')
      removeAttribute ('allowedAttributesEffective')
      removeAttribute ('allowedChildClasses')
      removeAttribute ('allowedChildClassesEffective')
      removeAttribute ('assistant')
      removeAttribute ('bridgeheadServerListBL')
```

```
removeAttribute ('canonicalName')
removeAttribute ('createTimeStamp')
removeAttribute ('department')
removeAttribute ('distinguishedName')
removeAttribute ('dSASignature')
removeAttribute ('dSCorePropagationData')
removeAttribute ('extensionName')
removeAttribute ('flags')
removeAttribute ('fromEntry')
removeAttribute ('frsComputerReferenceBL')
removeAttribute ('fRSMemberReferenceBL')
removeAttribute ('fSMORoleOwner')
removeAttribute ('generationQualifier')
removeAttribute ('instanceTyp')
removeAttribute ('isCriticalSystemObject')
removeAttribute ('isDeleted')
removeAttribute ('isPrivilegeHolder')
removeAttribute ('lastKnownParent')
removeAttribute ('managedObjects')
removeAttribute ('modifyTimeStamp')
removeAttribute ('mS-DS-ConsistencyChildCount')
removeAttribute ('mS-DS-ConsistencyGuid')
removeAttribute ('name')
removeAttribute ('netbootSCPBL')
removeAttribute ('nonSecurityMemberBL')
removeAttribute ('nTSecurityDescriptor')
removeAttribute ('objectCategory')
removeAttribute ('objectGUID')
removeAttribute ('objectVersion')
removeAttribute ('partialAttributeDeletionList')
removeAttribute ('partialAttributeSet')
removeAttribute ('possibleInferiors')
removeAttribute ('queryPolicyBL')
removeAttribute ('replPropertyMetaData')
removeAttribute ('replUpToDateVector')
removeAttribute ('revision')
removeAttribute ('sDRightsEffective')
removeAttribute ('serverReferenceBL')
removeAttribute ('showInAdvancedViewOnly')
removeAttribute ('siteObjectBL')
removeAttribute ('subRefs')
removeAttribute ('subSchemaSubEntry')
removeAttribute ('systemFlags')
removeAttribute ('uSNChanged')
removeAttribute ('uSNCreated')
removeAttribute ('uSNDSALastObjRemoved')
removeAttribute ('USNIntersite')
removeAttribute ('uSNLastObjRem')
removeAttribute ('uSNSource')
removeAttribute ('wbemPath')
removeAttribute ('wellKnownObjects')
removeAttribute ('whenChanged')
removeAttribute ('whenCreated')
removeAttribute ('instanceType')
removeAttribute ('ms-sql-olapcube')
removeAttribute ('ms-sql-database')
removeAttribute ('ms-sql-server')
removeAttribute ('ms-sql-sqlpublication')
removeAttribute ('ms-sql-sqldatabase')
removeAttribute ('ms-sql-sqlrepository')
removeAttribute ('ms-sql-sqlserver')
removeAttribute ('acpolity')
removeAttribute ('acsubnet')
```

```
removeAttribute ('msexchconfigurationcontainer')
removeAttribute ('msmqconfiguration')
removeAttribute ('msmqenterprisesettings')
removeAttribute ('msmqmigrateduser')
removeAttribute ('msmqqueue')
removeAttribute ('msmqsettings')
removeAttribute ('msmqsitelink')
removeAttribute ('ntdsconnection')
removeAttribute ('ntdsdsa')
removeAttribute ('ntdsservice')
removeAttribute ('ntdssitesettings')
removeAttribute ('ntfrsmember')
removeAttribute ('ntfrsreplicaset')
removeAttribute ('ntfrssettings')
removeAttribute ('ntfrssubscriber')
removeAttribute ('ntfrssubscriptions')
removeAttribute ('accountExpires')
removeAttribute ('aCSPolicyName')
removeAttribute ('adminCount')
removeAttribute ('badPasswordTime')
removeAttribute ('badPwdCount')
removeAttribute ('codePage')
removeAttribute ('controlAccessRights')
removeAttribute ('dBCSPwd')
removeAttribute ('defaultClassStore')
removeAttribute ('desktopProfile')
removeAttribute ('dynamicLDAPServer')
removeAttribute ('groupMembershipSAM')
removeAttribute ('groupPriority')
removeAttribute ('groupsToIgnore')
removeAttribute ('homeDirectory')
removeAttribute ('homeDrive')
removeAttribute ('lastLogoff')
removeAttribute ('lastLogon')
removeAttribute ('lmPwdHistory')
removeAttribute ('localeID')
removeAttribute ('lockoutTime')
removeAttribute ('logonCount')
removeAttribute ('logonHours')
removeAttribute ('logonWorkstation')
removeAttribute ('mSMQDigests')
removeAttribute ('mSMQDigestsMig')
removeAttribute ('mSMQSignCertificates')
removeAttribute ('mSMQSignCertificatesMig')
removeAttribute ('msNPAllowDialin')
removeAttribute ('msNPCallingStationID')
removeAttribute ('msNPSavedCallingStationID')
removeAttribute ('msRADIUSCallbackNumber')
removeAttribute ('msRADIUSFramedIPAddress')
removeAttribute ('msRADIUSFramedRoute')
removeAttribute ('msRADIUSServiceType')
removeAttribute ('msRASSavedCallbackNumber')
removeAttribute ('msRASSavedFramedIPAddress')
removeAttribute ('msRASSavedFramedRoute')
removeAttribute ('networkAddress')
removeAttribute ('ntPwdHistory')
removeAttribute ('operatorCount')
removeAttribute ('otherLoginWorkstations')
removeAttribute ('preferredOU')
removeAttribute ('primaryGroupID')
removeAttribute ('profilePath')
removeAttribute ('pwdLastSet')
removeAttribute ('scriptPath')
```

```
    removeAttribute ('servicePrincipalName')
    removeAttribute ('userAccountControl')
    removeAttribute ('userParameters')
    removeAttribute ('userSharedFolder')
    removeAttribute ('userSharedFolderOther')
    removeAttribute ('userSMIMECertificate')
    removeAttribute ('userWorkstations')
    removeAttribute ('masteredBy')
    removeAttribute ('maxStorage')
    removeAttribute ('userPrincipalName')
    removeAttribute ('objectSid')
    removeAttribute ('samaccounttype')
    removeAttribute ('badPasswordCount')
    removeAttribute ('sAMAccountControl')
    removeAttribute ('ADsPath')
    removeAttribute ('directReport')

    return
</ldap>
  </adapters>
```

Oracle データベース用のマッピング・スクリプトのカスタマイズ

この項の例は、ユーザー定義のスキーマとともにバック・エンドとして SQL サーバーを使用する Oracle データベース用としてカスタマイズされた後のサンプルの OblixDBMapping ファイルを示します。元のサンプルは次の場所にあります。

IdentityServer_install_dir¥identity¥oblix¥tools¥DNConversionToolkit¥oblix¥tools¥DataAnyWhere¥plugins¥OracleAccessmanagerOViDTemplates¥mapping_templates¥OblixDBMapping_mpy.xml

> **注意：** DN 変換ツールキットは、Identity Server インストールの一部として自動的にインストールされます。*IdentityServer_install_dir*¥identity¥oblix¥tools¥DNConversionToolkit¥oblix¥ を参照してください。ツールキットに同梱されている README ファイルを必ずお読みください。

オラクル社提供の元のサンプルを次のマッピング・ファイルと比較すると、必要な変更のタイプを確認できます。

Oracle データベース用のマッピング・スクリプトの変更の確認の手順

1. Virtual Directory Manager コンソールで、サンプルの OblixDBMapping ファイルをベースとして使用してマッピング・ファイルを作成します（10-43 ページの「アダプタのマッピング・ファイルの作成」を参照）。
2. 環境に応じてマッピング・ファイルを変更し、E-13 ページの「予期しないグループ削除の問題」の例に示されている対策を講じます。
3. マッピング・スクリプトを通常どおり保存およびデプロイします。
4. マッピング・スクリプトを後で使用するためのテンプレートとして保存します。
   - 新しいマッピング・テンプレート名（MyOracleDBMapping など）を右クリックします。
   - 「Save as template」を選択します。

5. 次に、Oracle データベース用のアダプタのカスタマイズも参照してください。

```
<?xml version="1.0" encoding="UTF-8"?>
<variables>
</variables>
<content>
def inbound():
   #These Oblix attributes are not being used. Remove them.
   removeAttribute('obver')
   removeAttribute('nsaccountlock')

   # More custom mapping
   # ....

   # If your user password is stored as character type, for example
   # NVARCHAR, CHAR, VARCHAR, etc, you need to map userPassword attribute
   # from binary syntax.
   mapSyntax('userPassword','IA5String')

   # This is a workaround ... for more information, see "Unexpected Group Deletion
Problem" on page E-13.
   # Need to prevent COREid from writing dummy user to backend database
   if haveAttributeValue('uniqueMember','cn=Dummy User'):
      #removeAttributeValue('uniqueMember','cn=Dummy User')
      if operation != 'modify':
         removeAttributeValue('uniqueMember','cn=Dummy User')
      else:
         change = removeAttribute('uniqueMember')[0]
         change.values.remove(DistinguishedName('cn=Dummy User'))
         addEntryChange(change)

   #Filter out objectclass. Only mention the structure class during add.
   if operation == 'modify':
      removeAttribute('objectClass')
   if operation == 'add':
      newobj = ''
      if haveAttributeValue('objectClass','inetOrgPerson'):
         newobj = 'inetOrgPerson'
      if haveAttributeValue('objectClass','groupOfUniqueNames'):
         newobj = 'groupOfUniqueNames'
         removeAttribute ('businessCategory')
         removeAttribute ('seeAlso')
         removeAttribute ('o')
      if haveAttributeValue('objectClass','oblixlocation'):
         newobj = 'oblixlocation'
      if not newobj == '':
         removeAttribute('objectClass')
         addAttributeValue('objectClass',newobj)

   return

def outbound():
   #code here for handling outbound mapping
   # .....
   # This is a workaround to bug #18865
   if operation=='entry':
      # Add the following workaround for each multiple value DN attribute
      if haveAttribute('uniqueMember') and len(findFilters('uniqueMember')) > 0:
         addAttributeValue('uniqueMember','cn=Dummy User')
   return
</content>
```

Oracle データベース用のアダプタのカスタマイズ

次の例は、Oracle データベース用としてカスタマイズしたサンプル・アダプタを示します。オラクル社提供のサンプル・テンプレートがベースとして使用されています。

```
<?xml version="1.0" encoding="UTF-8"?>
<adapters dirty="" version="0"
  xmlns="http://www.octetstring.com/schemas/Adapters" xmlns:adapters="http://
www.w3.org/2001/XMLSchema-instance">
  <dataBase dirty="" id="DB Adapter Company Employees" version="0">
    <root>ou=Employees,o=MyCompanyDB,c=us</root>
    <active>true</active>
    <routing>
      <critical>true</critical>
      <priority>50</priority>
      <inclusionFilter/>
      <exclusionFilter/>
      <plugin/>
      <retrieve/>
      <store>
        <exclude>carlicense</exclude>
        <exclude>street</exclude>
        <exclude>employeeType</exclude>
      </store>
      <visible>Internal</visible>
      <levels>-1</levels>
      <bind>true</bind>
      <bind-adapters/>
      <views/>
      <dnpattern/>
    </routing>
    <pluginChains xmlns="http://www.octetstring.com/schemas/Plugins">
      <plugins>
        <plugin>
          <name>MyOracleDBMapping</name>
          <class>com.octetstring.VDE.chain.plugins.mapper.Mapper</class>
          <initParams>
            <param name="mapfile" value="MyOracleDBMapping.mpy"/>
          </initParams>
        </plugin>
        <plugin>
          <name>Dump after</name>
          <class>com.octetstring.VDE.chain.plugins.DumpTransactions.DumpTransactions</
class>
          <initParams>
            <param name="loglevel" value="info"/>
          </initParams>
        </plugin>
        <plugin>
          <name>Dump before</name>
          <class>com.octetstring.VDE.chain.plugins.DumpTransactions.DumpTransactions</
class>
          <initParams>
            <param name="loglevel" value="info"/>
          </initParams>
        </plugin>
      </plugins>
      <default>
        <plugin name="Dump before"/>
        <plugin name="MyOracleDBMapping"/>
        <plugin name="Dump after"/>
      </default>
    </pluginChains>
    <driver>oracle.jdbc.driver.OracleDriver</driver>
```

```
    <url>jdbc:oracle:thin:@127.0.0.1:1521:QA2</url>
    <user>CUSTDATA</user>
    <password>oblix</password>
    <ignoreObjectClassOnModify>false</ignoreObjectClassOnModify>
    <includeInheritedObjectClasses>true</includeInheritedObjectClasses>
    <maxConnections>10</maxConnections>
    <mapping>
      <joins/>
      <objectClass name="inetOrgPerson" rdn="cn">
        <attribute field="EMPLOYEE_ID" ldap="uid"
          table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="NAME" ldap="cn" table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="FIRST_NAME" ldap="givenName"
          table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="LAST_NAME" ldap="sn"
          table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="TITLE" ldap="title" table="CUSTDATA.EMPLOYEES"
type="VARCHAR"/>
        <attribute field="USERPASSWORD" ldap="userPassword"
          table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="PREFERREDLANGUAGE"
          ldap="PreferredLanguage" table="CUSTDATA.EMPLOYEES" type="CHAR"/>
        <attribute field="MAIL" ldap="mail" table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="CHALLENGEPHRASE" ldap="ChallengePhrase"
          table="CUSTDATA.EMPLOYEES" type="CHAR"/>
        <attribute field="PHOTO" ldap="Photo"
          table="CUSTDATA.EMPLOYEES" type="BLOB"/>
        <attribute field="DESCRIPTION" ldap="Description"
          table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="OBUSERACCOUNTCONTROL"
          ldap="OBUSERACCOUNTCONTROL" table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="OBLOGINTRYCOUNT" ldap="oblogintrycount"
          table="CUSTDATA.EMPLOYEES" type="NUMERIC"/>
        <attribute field="OBPASSWORDCREATIONDATE"
          ldap="obpasswordcreationdate" table="CUSTDATA.EMPLOYEES" type="VARCHAR"/ >
        <attribute field="OBPASSWORDHISTORY" ldap="obpasswordhistory"
          table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="OBPASSWORDCHANGEFLAG"
          ldap="obpasswordchangeflag" table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="OBPASSWORDEXPMAIL" ldap="obpasswordexpmail"
          table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="OBLOCKOUTTIME" ldap="oblockouttime"
          table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="OBFIRSTLOGIN" ldap="obfirstlogin"
          table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="OBRESPONSETRIES" ldap="obresponsetries"
          table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="OBLASTLOGINATTEMPTDATE"
          ldap="oblastloginattemptdate" table="CUSTDATA.EMPLOYEES" type="VARCHAR"/ >
        <attribute field="OBLASTRESPONSEATTEMPTDATE"
          ldap="oblastresponseattemptdate" table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="OBRESPONSETIMEOUT" ldap="obresponsetimeout"
          table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
        <attribute field="MANAGER_DN" ldap="Manager"
          table="CUSTDATA.EMPLOYEES" type="VARCHAR"/>
      </objectClass>
      <objectClass name="groupOfUniqueNames" rdn="cn">
        <attribute field="GROUP_NAME" ldap="cn"
          table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="OWNER_DN" ldap="owner"
          table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="MEMBER_DN" ldap="uniqueMember"
          table="CUSTDATA.GROUPS" type="VARCHAR"/>
```

```
        <attribute field="MAIL" ldap="mail" table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="OBGROUPCREATOR" ldap="obgroupcreator"
          table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="OBGROUPCREATIONDATE"
          ldap="obgroupcreationdate" table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="OBGROUPTYPE" ldap="obgrouptype"
          table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="OBSUBSCRIPTIONTYPES"
          ldap="obsubscriptiontypes" table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="OBVER" ldap="obver"
          table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="OBGROUPSUBSCRIPTIONTYPE"
          ldap="obgroupsubscriptiontype" table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="OBGROUPEXPANDEDDYNAMIC"
          ldap="obgroupexpandeddynamic" table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="OBGROUPPUREDYNAMIC" ldap="obgrouppuredynamic"
          table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="OBGROUPADMINISTRATOR"
          ldap="obgroupadministrator" table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="OBGROUPSUBSCRIBEMESSAGE"
          ldap="obgroupsubscribemessage" table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="OBGROUPUNSUBSCRIBEMESSAGE"
          ldap="obgroupunsubscribemessage" table="CUSTDATA.GROUPS" type="VARCHAR"/ >
        <attribute field="OBGROUPSUBSCRIPTIONFILTER"
          ldap="obgroupsubscriptionfilter" table="CUSTDATA.GROUPS" type="VARCHAR"/ >
        <attribute field="OBGROUPSUBSCRIBENOTIFICATION"
          ldap="obgroupsubscribenotification"
          table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="OBGROUPDYNAMICFILTER"
          ldap="obgroupdynamicfilter" table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="OBGROUPSIMPLIFIEDACCESSCONTROL"
          ldap="obgroupsimplifiedaccesscontrol "
          table="CUSTDATA.GROUPS" type="VARCHAR"/>
        <attribute field="GROUP_DESC" ldap="description"
          table="CUSTDATA.GROUPS" type="VARCHAR"/>
      </objectClass>
      <objectClass name="oblixlocation" rdn="obid">
        <attribute field="OBID" ldap="obid"
          table="CUSTDATA.OBLIXLOCATION" type="VARCHAR"/>
        <attribute field="OBLOCATIONNAME" ldap="oblocationname"
          table="CUSTDATA.OBLIXLOCATION" type="VARCHAR"/>
        <attribute field="OBLOCATIONTITLE" ldap="oblocationtitle"
          table="CUSTDATA.OBLIXLOCATION" type="VARCHAR"/>
        <attribute field="OBPARENTLOCATIONDN" ldap="obparentlocationdn"
          table="CUSTDATA.OBLIXLOCATION" type="VARCHAR"/>
        <attribute field="OBRECTANGLE" ldap="obrectangle"
          table="CUSTDATA.OBLIXLOCATION" type="VARCHAR"/>
        <attribute field="OBPHOTO" ldap="obphoto"
          table="CUSTDATA.OBLIXLOCATION" type="BLOB"/>
      </objectClass>
    </mapping>
  </dataBase>
</adapters>
```

Oracle Access Manager の一般設定のカスタマイズ

一般的なアダプタ構成および設定情報は、Oracle Virtual Directory/Virtual Directory Manager の製品マニュアルに記載されています。アダプタの作成後、ほとんどの設定でデフォルト値が有効になります。次の重要事項は、Oracle Access Manager に関するものです。

- DN 属性
- 接続情報

DN 属性 :

- DN 属性は、DN 構文に準拠する属性名を使用して設定する必要があります。

  これらの DN 属性は、顧客スキーマに存在する場合や、Oracle Access Manager の補助クラスによって取り入れられる場合があります。これにより、Oracle Virtual Directory は、これらの DN の値を論理フォームではなくネイティブ・フォームで格納します。

- DN 属性は、使用するオブジェクト・クラスと関連しています。
  - **inetorgperson および groupofuniquenames の場合**、次を使用します。

    uniquemember、manager、secretary、owner
  - **user および group の場合**、次を使用します。

    member、memberOf、managedObjects、distinguishedname、objectcategory、manager、secretary、managedby
  - **Oracle Access Manager に取り入れられた補助クラスの場合**、次を使用します。

    obgroupadministrator、obgroupcreator
  - 「Pass-Through Mode」の場合、次を選択します。

    Always

接続情報 : 想定される作業量に基づいて次の接続情報を Oracle Virtual Directory に設定します。

操作のタイムアウト
最大プール接続
最大プール待機
最大プール試行

Oracle Access Manager の一般設定のカスタマイズの手順

1. 前述の情報を確認します。
2. Virtual Directory Manager の Server Navigator ウィンドウで、サーバーを選択し、アダプタ名を検索して選択します。
3. 右側のペインで「Routing」タブをクリックします。
4. 「General Settings」で、可視性が内部に設定されていることを確認します。

   例 :

   General Settings

   Visibility: Internal（分割プロファイルのアダプタ用）
5. この項で説明する設定がアダプタに使用されていることを確認します。
6. 「Finish」をクリックします。
7. Server Navigator ウィンドウでアダプタ名を右クリックし、「Save to Server」を選択します。

ルーティング設定のカスタマイズ

結合ビュー・アダプタによって使用されるアダプタを設定する場合、プライマリおよびセカンダリ・アダプタの可視性は内部に設定し、これらが結合ビュー・アダプタによってのみ起動されるようにする必要があります。

アダプタの動作中は、パフォーマンスを観察するとともにログを診断し、アダプタによって特定の操作が必要以上に繰り返し起動されていないことを確認します。このような兆候がある場合は、次の機能を使用して、このアダプタによる不要な操作をフィルタでブロックします。全体的なパフォーマンスを向上させるために、この手順は非常に重要です。

- 包含用のフィルタ
- 除外用のフィルタ
- DN 照合

ルーティング設定のカスタマイズの手順

1. Server Navigator ウィンドウでアダプタ名を選択します。
2. 右側のペインで「Routing」タブをクリックします。
3. 環境に応じてオプションを選択します。
   - 包含用のフィルタ
   - 除外用のフィルタ
   - DN 照合
4. 通常どおりサーバーに保存します。

マッピング・ファイルを参照するためのアダプタ・プラグインの編集

10-74 ページの「Oracle Access Manager と Oracle Virtual Directory の実装のテンプレート」で説明されているように、オラクル社提供のサンプル・アダプタ・テンプレートには、複数のプラグインがすでに含まれています。プラグインには次の 2 つのタイプがあります。

- **プラグイン :** 構成用としてパラメータ・ベースのユーザー・インタフェースを提供する事前定義のプラグイン。
- **マッピング・プラグイン :** マッピング・スクリプト用のプラグイン。

作業上、次の点に注意してください。

- オラクル社提供のサンプル・テンプレートを使用する場合、プラグインを変更するのみです。
- オラクル社提供のサンプル・テンプレートを使用しない場合、アダプタにプラグインを追加する必要があります。次に例を示します。

前述の説明のとおり、Active Directory および ADAM アダプタには、オラクル社提供のサンプル・テンプレートに含まれる 2 つの特定のプラグインが必要です。

オラクル社提供のサンプル・テンプレートを使用しない場合、Active Directory のパスワード・プラグインとして作成する SSL アダプタを作成対象のオープン接続アダプタに追加するとともに、Active Directory の範囲属性プラグインも追加する必要があります。この場合、SSL アダプタと同じようにマップされたネームスペースを指定するようにしてください。詳細は、10-44 ページの「LDAP ディレクトリのアダプタの作成」を参照してください。

次の手順は例としてのみ示します。Virtual Directory Manager の使用の詳細は、Oracle Virtual Directory のドキュメントを参照してください。

マッピング・ファイルを参照するためのアダプタ・プラグインの編集の手順

1. 次の作業を実行します。
   - アダプタのマッピング・ファイルの作成
   - データ・ストア・アダプタの作成
2. Virtual Directory Manager の Server Navigator ウィンドウで、プロジェクトとサーバーを選択し、プラグインを追加または検証するアダプタ名を検索して選択します。
3. 右側のペインで「Plug-ins」タブをクリックします。
4. 「Adapter Plug-ins」画面で、次の作業を行います。
   a. ADAM または Active Directory の場合、次のプラグインが次の順序で必要です。

      Active Directory の範囲属性 OblixADMapping（前に作成したマッピング・ファイル）

      Active Directory のパスワード

   b. 上下矢印を使用して環境に応じてプラグインを配置します。
   c. 前に作成したマッピング・ファイルが表示されていない場合は、次のようにします。

現在のマッピング（OblixADMapping など）を選択してから、「Edit」ボタンをクリックします。

「Name」フィールドで、名前をマッピング・ファイル名（MyADMapping など）に変更します。

「Name」フィールドで、名前をマッピング・ファイル名（MyADMapping など）に変更します。

   d. Active Directory または ADAM アダプタ用として Oracle 以外のテンプレートを使用する場合、パスワードを処理するために前に作成した SSL アダプタを追加します。

「New Plug-in」ボタンをクリックします。

「Select from Server」をクリックしてから、Active Directory のパスワード・プラグインを選択します。

パラメータの値として SSL アダプタ名（CustomAdamSSLAdapter など）を指定します。

パラメータ行を選択してから、「Edit」をクリックします。

値として ADAM または Active Directory の SSL アダプタ名（CustomAdamSSLAdapter など）を指定します。

5. 通常どおり終了し、保存およびデプロイします。

ID システムのインストールおよび設定の実行

これで、前述した他のすべての重要な作業が完了したため、ID システムのインストールおよび設定を実行できます。

ID システムのインストールおよび設定の実行の手順

1. 前述のタスクをすべて完了します。
2. **WebPass:** 第 5 章「WebPass のインストール」で説明されているように、WebPass をインストールします。
3. **ID システムの設定 :** 次の仕様を使用して ID システムを設定してから、通常どおりに設定を終了します。
   a. **User Data Directory Server:** ディレクトリ・タイプとして Data Anywhere を選択します。
   b. **User Data ... Host:** Oracle Virtual Directory をホストしているマシンを指定します。
   c. **User Data ... Port:** Oracle Virtual Directory の LDAP ライセンス・ポートを指定します。
   d. **Searchbase:** 仮想ツリーの任意の場所にある Oracle Virtual Directory の仮想 DN を指定します。
   e. **Configuration Data Directory Server:** Identity Server のインストール時に指定したネイティブ・ディレクトリを選択します。構成（およびポリシー・データ）は、Oracle Virtual Directory 仮想ディレクトリの外部に格納する必要があります。
   f. **Automatically Update Schema:** 「Yes」を選択し、Oracle Access Manager の補助属性を使用して Oracle Virtual Directory スキーマを自動的に更新します。
   g. **Automatically Configure Person and Group Object Classes:** 「Yes」または「No」を選択し、通常どおり Oracle Virtual Directory スキーマを構成します。

   注意 : Person オブジェクト・クラスおよび Group オブジェクト・クラスの手動構成の詳細は、6-7 ページの「Person オブジェクト・クラスおよび Group オブジェクト・クラスの指定」を参照してください。
4. **Policy Manager:** 7-1 ページで説明されているように、後述の特定の詳細を使用して Policy Manager をインストールおよび設定してから、通常どおりに設定を完了します。
   a. 前述の説明に従って、設定時にユーザー・データ・ディレクトリ・サーバーの詳細を指定します。
   b. Policy Manager の設定時に次を指定します。

      Searchbase: ID システムの設定時に指定した検索ベースと同じである必要があります。

      Configuration DN: ID システムの設定時に指定した構成データ DN と同じである必要があります。

      Policy Base: Access Manager の設定時に指定したポリシー・データ DN と同じである必要があります。
5. **Access Server:** 第 8 章「Access Server のインストール」で説明されているように、Access Server をインストールします。この場合、次のようにします。
   a. 構成データ・ディレクトリ・サーバーに関する情報を指定します。
   b. Oracle Access Manager のポリシー・データの格納場所を指定します。
   c. 求められた場合、次の情報を指定します。

Access Server ID

Configuration DN: 前に指定したものと同じである必要があります。

Policy Base: 前に指定したものと同じである必要があります。

6. **WebGate:** 第 9 章「WebGate のインストール」で説明されているように、WebGate をインストールします。
7. **フェイルオーバー :** 次の説明に従って構成します。
   - フェイルオーバーのサポート
   - 『Oracle Access Manager デプロイメント・ガイド』
   - 製品のドキュメント

実装のテスト

実装をテストする場合、ネイティブ・ディレクトリからのユーザー・データの取得が必要な Oracle Access Manager の機能を実行してください。

この操作が実行されると、実装は成功です。

参照情報

次の各項では、Oracle Access Manager 向けの Oracle Virtual Directory の実装の様々な側面に関する技術上の詳細を説明します。

- Oracle Access Manager の補助属性
- DN 変換ツールキットの概要
- Oracle Access Manager と Oracle Virtual Directory の実装のテンプレート

Oracle Access Manager の補助属性

Oracle Access Manager の特定の機能では、最上位の仮想ディレクトリのスキーマと各ターゲット・データ・ストアのスキーマ（またはデータベースの対応フィールド）の両方に特定の属性が存在する必要があります。

- 仮想ディレクトリ・スキーマは、次のように自動的に拡張できます。
  - ID システムをインストールおよび設定するときに、Data Anywhere をユーザー・データ・ディレクトリ・サーバーとして選択する場合、Oracle Virtual Directory スキーマを自動（または手動）で拡張できます。ID システムのインストールおよび設定の詳細は、第 II 部「ID システムのインストールおよび設定」を参照してください。
  - 以前のインストールを Oracle Access Manager 10*g*（10.1.4.0.1）にアップグレードした後、10-41 ページの「ディレクトリ・スキーマの拡張」で説明されているように、ldapmodify ユーティリティを使用して Oracle Virtual Directory スキーマを手動で拡張する必要があります。
- 10-41 ページの「ディレクトリ・スキーマの拡張」で説明されているように、適切な ldif ファイルを使用して ldapmodify.exe ユーティリティを実行し、ターゲット LDAP ディレクトリを拡張します。
- プライマリ・データベース表内のすべてのユーザー・アカウントを適切なクラスにマップし、仮想ディレクトリのオブジェクト・クラスをシミュレートします。詳細は、10-17 ページの「ターゲット・データベース表への属性の追加の概要」を参照してください。
- プライマリ・データベース表に追加列を作成し、Oracle Access Manager の特別な機能を有効化する補助ユーザー属性をシミュレートします。詳細は、10-17 ページの「ターゲット・データベース表への属性の追加の概要」を参照してください。

アンバウンド・データまたはユーザー・データに対しては長さが 1000 の NVARCHAR、Oracle Access Manager 固有のすべての属性に対しては長さが 240 の VARCHAR を使用します。

表 10-7 は、特定の User Manager 機能に必要な Oracle Access Manager の補助属性を示しています。

> **注意：** Oracle Virtual Directory を使用する場合、ロケーション・オブジェクトはサポートされないため、User Manager アプリケーションではユーザー・ロケーション機能はサポートされません。

表 10-7 User Manager 機能に必要な拡張属性

User Manager 機能	必須属性	推奨される属性のタイプおよび長さ
ユーザーの追加 / アクティブ化 / 非アクティブ化	Obuseraccountcontrol	VARCHAR (240)
ワークフローのサロゲート	oboutofofficeindicator	VARCHAR (240)
リセット時のパスワード変更	obpasswordchangeflag	VARCHAR (240)
パスワードの最大ログイン試行回数	oblogintrycount	VARCHAR (240)
パスワード有効期間	obpasswordcreationdate	VARCHAR (240)
パスワード期限切れ通知期間	obpasswordcreationdate	VARCHAR (240)
パスワードのロックアウト継続時間	oblockouttime	VARCHAR (240)
パスワードのログイン試行のリセット	oblastloginattemptdate	VARCHAR (240)
パスワードの最小期間	obpasswordcreationdate	VARCHAR (240)
パスワード履歴	obpasswordhistory	NVARCHAR (1000)
	オプションのパスワード履歴のサポート	
チャレンジ・レスポンス	チャレンジ・フレーズおよびチャレンジ・レスポンスの顧客属性	NVARCHAR (1000)
チャレンジ・レスポンスのログイン試行のリセット	oblastresponseattemptdate	VARCHAR (240)
チャレンジ・レスポンスのロックアウト継続時間	Obresponsetimeout	VARCHAR (240)
	oblockouttime	VARCHAR (240)
チャレンジ・レスポンスの最大ログイン試行回数	obresponsetries	VARCHAR (240)

表 10-8 は、特定の Group Manager 機能に必要な Oracle Access Manager の補助属性を示しています。

表 10-8 Group Manager 機能に必要な拡張属性

Group Manager 機能	必須属性	推奨される属性のタイプおよび長さ
サブスクリプション・タイプ	obgroupsubscriptiontype	VARCHAR (240)
グループ拡張	obgroupexpandeddynamic	VARCHAR (240)
純動的グループ	obgrouppuredynamic	VARCHAR (240)
グループ管理者	obgroupadministrator 仮想ディレクトリは、グループごとに 1 名のみの管理者をサポートする必要がある。	NPVARCHAR (1000)
サブスクリプション・メッセージ	obgroupsubscribemessage	NPVARCHAR (1000)
登録解除メッセージ	obgroupunsubscribemessage	NPVARCHAR (1000)
サブスクリプション・フィルタ	obgroupsubscriptionfilter	NPVARCHAR (1000)
サブスクリプション通知タイプ	仮想ディレクトリは、グループごとに 1 つのみのサブスクリプションをサポートする必要がある。	NPVARCHAR (1000)
動的フィルタ	obgroupsubscribenotification サブスクリプション通知と登録解除通知のどちらかを実装できるが、両方の機能を同時には実装できない。	NPVARCHAR (1000)
単純アクセス制御	obgroupdynamicfilter 仮想ディレクトリは、グループごとに 1 つのみの動的フィルタをサポートする必要がある。	
グループ・タイプ	obgrouptype 仮想ディレクトリは、グループごとに 1 つのみのグループ・タイプをサポートする必要がある。	
選択可能サブスクリプション・タイプ	obsubscriptiontypes 仮想ディレクトリは、グループごとに 1 つのみのサブスクリプション・タイプをサポートする必要がある。使用可能なサブスクリプション・タイプは、「オープン」、「閉じる」、「フィルタでオープン」および「ワークフロー経由で制御」。	NPVARCHAR (1000)

DN 変換ツールキットの概要

DN 変換ツールキットは、既存の Oracle Access Manager インストールを使用しているときに Oracle Virtual Directory を統合する場合に使用します。DN 変換ツールキットは、構成 / ポリシー・ツリーにあるユーザー・データ関連のすべてのネイティブ DN 接尾辞を論理 DN 接尾辞に変換します。

DN 変換ツールキットは、Identity Server インストールの一部として自動的にインストールされます。表 10-9 は、このツールキットの内容を示しています。

注意： ツールキットに同梱されている README ファイルを必ずお読みください。DN 変換ツールキットに含まれていない *.ldif ファイルは、*IdentityServer_install_dir*¥identity¥oblix¥data¥common にあります。

表 10-9 Oracle Access Manager の DN 変換ツールキットの内容

DNConversionToolkit¥oblix	ファイル・コンポーネント	説明
¥apps¥common¥bin¥	globalparams.xml	特に、検索ベースの検索範囲を制御するファイル。
¥lib	obxmlengine.dll（Windows）	Windows および Solaris 用のライブラリ。
	obxerces-c21.dll（Windows）	
	msvci70.dll（Windows）	
	msvci70d.dll（Windows）	
	msvcr70.dll（Windows）	
	msvcr70d.dll（Windows）	
	libxmlengine.so（Solaris）	
	libstdc++.so.5（Solaris）	
	libgcc_s.so.1（Solaris）	
	Solaris に必要なすべての ldap sdk ライブラリ	
¥tools¥DataAnyWhere	README	内容の概要、ランタイム要件、および DN 変換ツールキットのコンポーネントの簡単な使用例。
¥tools¥DataAnyWhere	obmigrateDN.exe	DN 変換バイナリおよび構成ファイル。
¥conversion_tools	obmigrateDNmsg.lst	Oracle Virtual Directory を既存の Identity Server インストールと統合する場合、obmigrateDN は、Oracle Access Manager の構成ツリー内のユーザーおよびグループ DN を変換する。この場合、obmigrateDN は、Oracle Virtual Directory の DN 固有の操作を処理するために obmigratedata を内部的にコールする。これにより、obmigratedata は、ldapmodify 実行可能ファイルを参照する。
¥tools¥DataAnywhere	feature.xml	
¥features¥		
¥OracleAccessManager OViDFeatures		

表 10-9 Oracle Access Manager の DN 変換ツールキットの内容（続き）

DNConversionToolkit¥oblix	ファイル・コンポーネント	説明
¥tools¥DataAnyWhere ¥OblixUserSchema	ADUserSchema.ldif ADAuxSchema.ldif ADAM_user_schema_add.ldif ADAMAuxSchema.ldif f iPlanet_user_schema_add.ldif iPlanet_user_schema_delete.ldif NDS_user_schema_add.ldif NDS_user_schema_delete.ldif v3.user.ibm_at.ldif v3.user.ibm_oc.ldif schema.oblix.xml VDE_user_schema_add.ldif VDE_user_schema_delete.ldif **注意：**可能であれば、Identity Server インストールに用意されている ldif ファイルを使用してください。	schema.oblix.xml は、Oracle Access Manager のユーザー・スキーマを仮想ディレクトリまで拡張する。 VDE_user_schema_add.ldif は、Oracle Access Manager の属性を使用して Oracle Virtual Directory スキーマを拡張する。 その他のファイルは、Oracle Access Manager のユーザー・スキーマを、Oracle Access Manager と Oracle Virtual Directory の実装によってサポートされているディレクトリ・サーバーまで拡張する。
¥tools¥DataAnywhere ¥plugins ¥OracleAccessmanager OViDTemplates	plugin.xml	
¥tools¥DataAnywhere ¥plugins ¥OracleAccessmanager OViDTemplates ¥adapter_templates	OblixADAdapterUsingMapper_adapter_template.xml OblixADAdapterUsingScript_adapter_template.xml OblixADSSLAdapterUsingMapper_adapter_template.xml OblixADAMAdapterUsingMapper_adapter_template.xml OblixADAMAdapterUsingScript_adapter_template.xml OblixADAMSSLAdapterUsingMapper_adapter_template.xml OblixSunOneAdapterUsingMapper_adapter_template.xml OblixSunOneAdapterUsingScript_adapter_template.xml 詳細は、次を参照。 10-74 ページの「Oracle Access Manager と Oracle Virtual Directory の実装のテンプレート」	テンプレートを必要とするディレクトリ・サーバー用の Oracle Virtual Directory のアダプタ・テンプレート。 これらは、アダプタの作成のベースとして使用できる。 各テンプレートには、基本設定、事前構成データ、プラグインおよびプラグイン・パラメータが含まれる。 10-44 ページの「データ・ストア・アダプタの作成」を参照。

表 10-9 Oracle Access Manager の DN 変換ツールキットの内容（続き）

DNConversionToolkit¥oblix	ファイル・コンポーネント	説明
¥tools¥DataAnywhere ¥plugins ¥OracleAccessmanager OViDTemplates ¥mapping_templates	OblixADAMMapping_mpy.xml OblixADMapping_mpy.xml OblixDBMapping_mpy.xml OblixeDirectoryMapping_mpy.xml OblixSunOneMapping_mpy.xml	マッピング・スクリプト・テンプレート。 これらのサンプル・マッピングにより、アダプタ・テンプレートのオブジェクト・クラス・マッパー・プラグインによって生成された構成と同じ構成が実行される。 マッピング・スクリプトの方が柔軟性があるため、プラグインでは不可能な高度な調整を行うことができる。 10-43 ページのアダプタのマッピング・ファイルの作成を参照。
¥tools ¥ldap_tools	ldapmodify.exe libobnspr4.dll libobplc4.dll libobplds4.dll obnsldap32v50.dll obnsldappr32v50.dll obnsldapssl32v50.dll obnss3.dll obsoftokn3.dll obsoftokn3.dll	DN 変換ツールキットとともに使用する ldapmodify ツール。 Windows 用のライブラリ・ファイル。
¥tools ¥migration_tools ¥obmigratedata	at_DN_Conversion_map_osd_offline.lst oc_DN_Conversion_map_osd_offline.lst at_DN_Conversion_map_osd_online.lst oc_DN_Conversion_map_osd_online.lst obmigratedata.exe obmigratedatamsg.lst	実行時に obmigratedata が必要とするファイル。 これらには、特別な処理を必要とするオブジェクト・クラスと属性の詳細が含まれる。 これは通常のアップグレードと同じだが、DN 変換ツールの場合、オフラインおよびオンライン・モードで特別な処理を必要とする点が異なる（README ファイルを参照）。

DN 変換ツールは、Oracle Access Manager の構成およびポリシー・ツリーの構成およびポリシー・ブランチのネイティブ DN を、仮想ディレクトリが使用可能な論理（仮想）DN に変更します。次のツールを使用します。

IdentityServer_install_dir¥identity¥oblix¥tools¥DNConversionToolkit¥oblix¥tools

¥DataAnyWhere¥conversion_tools ¥obmigrateDN.exe

条件

変換を正常に実行するには、Oracle Access Manager ディレクトリが次の 2 つの条件を満たしている必要があります。

- Oracle Access Manager の構成およびポリシー・データが Oracle Virtual Directory の外部のネイティブ・ディレクトリに存在すること。
- Oracle Access Manager からは、この製品から参照できるすべてのユーザー・データが含まれる、Oracle Virtual Directory 仮想ディレクトリとは別のディレクトリに、この構成およびポリシー・データが属しているように見えること。

要件

- 変換する DN 属性のリストが含まれるファイル
- ネイティブ DN を論理 DN に関連付ける作成対象のマッピング・リスト
- ホスト名、ポート番号、バインド DN、パスワード、ディレクトリ・タイプ、構成 DN、Oblix ノード、インストール・ディレクトリ、ネイティブ DN、論理 DN、モード（オンライン、オフライン、テスト）

詳細

- このツールが変換を行うのは、Oracle Virtual Directory でドメインが異なる場合のみです。次に例を示します。

  Oracle Access Manager の DN が次のとおりだとします。

  ```
  o=company, c=us
  ```

  また、Oracle Virtual Directory 上の iPlanet の DN が次のとおりだとします。

  ```
  o=iPlanet, o=company,c=us
  ```

  このとき、入力時に指定されたマッピング詳細を参照して変換が実行されます。

- 属性自体のみが異なる場合、マッピングは実行されません。次に例を示します。

  ```
  cn=manisha, o=company, c= us
  ```

  この場合、Oracle Virtual Directory にはマップできません。

  ```
  cn=manisha, o=iPlanet, o=company, c=us
  ```

- このツールは、DN 値ごとに少なくとも 1 回は実行する必要があります。

  注意： 構成ブランチがポリシー・ブランチと同じディレクトリ・サーバー上にない場合、DN 値ごとにこのツールを 2 回実行する必要があります。

- このツールは SSL をサポートしていません。
- スキーマの DSML バージョンは自動的にはロードされません。
- 既存の Oracle Access Manager インストールをアップグレードする場合、システム設定を再実行する前に、統合するディレクトリから DBProfile ブランチを手動で削除する必要があります。

  注意： システム設定の前に必ず古い DBProfile を手動で削除してください。設定後は、新しい DBProfile が自動的に作成されます。

- このツールは、ADSI（Active Directory Services Interface）をサポートしていません。セキュアな接続が必要な場合は、かわりに SSL を使用する必要があります。

Oracle Access Manager と Oracle Virtual Directory の実装のテンプレート

オラクル社では、各ディレクトリおよびデータベースを容易に設定できるようにアダプタ・テンプレートおよびスクリプト・テンプレートを提供しています。アダプタを構成する場合、後で説明するテンプレートを選択し、スキーマ・マッピングおよび特別な処理を実行できます。マッピング基準によっては、これらのテンプレートをそのまま使用することも、調整のベースとして使用することもできます。

用意されているテンプレートは、表 10-9「Oracle Access Manager の DN 変換ツールキットの内容」に一覧表示されています。各テンプレートの実行機能を完全に理解するには、次の説明を参照してください。

- Active Directory 用のテンプレート
- ADAM 用のテンプレート
- Sun Directory Server 用のテンプレート
- eDirectory 用のテンプレート
- eDirectory 用のテンプレート
- スキーマ・マッピング・スクリプト・テンプレート

注意： オブジェクト・クラス・マッパー・テンプレートは、パラメータ・ベースのユーザー・インタフェースを持つプラグインです。オブジェクト・クラス・マッパー・テンプレートおよびスクリプト・テンプレートでは、同じ操作が実行され、同じ結果が生成されます。場合によってはスクリプトを使用する方が自由度が高くなりますが、マッパーを使用する方が便利な場合もあります。どちらを使用するかは自由に選択できます。

詳細は、10-44 ページの「データ・ストア・アダプタの作成」および 10-70 ページの「DN 変換ツールキットの概要」を参照してください。

Active Directory 用のテンプレート

Oracle Access Manager には、Active Directory 用として次の 3 つのテンプレートが用意されています。

- Active Directory 用の OblixADAdapterUsingMapper
- Active Directory 用の OblixADAdapterUsingScript
- Active Directory 用の OblixADSSLAdapterUsingMapper

Active Directory 用の OblixADAdapterUsingMapper

このテンプレートは、次が含まれるオブジェクト・マッパー・プラグインを使用して、Active Directory の user および group データを Oracle Virtual Directory の inetorgperson および groupofuniquenames に変換するアダプタを定義します。

1. inetorgperson、groupofuniquenames および Oracle Access Manager のユーザー補助クラスの DN 構文を持つすべての属性を使用して DN 属性を設定し、これらの DN をネイティブ DN 形式で格納するためのメカニズム。
2. Active Directory の範囲属性用のプラグイン。

   Active Directory は、xxx バイトのチャンクとしてエントリを返します。このプラグインは、すべてのチャンクを 1 つの結果エントリとして連結します。
3. 表 10-10 に示すオブジェクト・クラスおよび属性をマップするためのパラメータ・ベースのユーザー・インタフェースを備えるオブジェクト・クラス・マッパー用のプラグインも含まれます。

表 10-10 OblixADAdapterUsingMapper、オブジェクト・クラス・マッパーのプラグイン・パラメータ

パラメータ	値	コメント
`filterObjectClass OnModify`	true	Active Directory が静的補助クラスとして構成されていることが前提。
addAttribute-group	samaccountname=%cn%	オブジェクト・クラスが group である場合、samaccountname 属性を追加し、値を cn と同じ値に設定。これは、Active Directory では、group に対して samaccountname が必要であるため。
addAttribute-group	`groupType=4`	オブジェクト・クラスが group である場合、`groupType` 属性を追加し、デフォルト値を 4 に設定する。この値は、顧客のニーズに応じて変更できる。
`mapAttribute`	uniqueMember= member	Oracle Virtual Directory の `uniqueMember` 属性を Active Directory の member 属性にマップする。
`mapAttribute`	owner=`managedBy`	Oracle Virtual Directory の owner 属性を Active Directory の managedBy 属性にマップする。
`mapAttribute`	uid=samaccountname	Oracle Virtual Directory の uid 属性を Active Directory の `samaccountName` 属性にマップする。
`filterAttribute-group`	次も参照。 `businessCategory`	オブジェクト・クラスが group である場合、これらの属性をフィルタ処理によって除外する。これは、Active Directory の group がこれらの 3 つの属性をサポートしていないため。
`mapObjectClass`	groupofuniquenames= group	Oracle Virtual Directory の `groupOfUniqueNames` オブジェクト・クラスを Active Directory の group オブジェクト・クラスにマップする。
`mapObjectClass`	inetorgperson=user	Oracle Virtual Directory の inetorgperson オブジェクト・クラスを Active Directory の user オブジェクト・クラスにマップする。

表 10-10 OblixADAdapterUsingMapper、オブジェクト・クラス・マッパーのプラグイン・パラメータ（続き）

パラメータ	値	コメント
filterAttribute	（システム属性のリスト）	リスト内のすべての属性をフィルタ処理によって除外する。Active Directory には、Oracle Access Manager からは参照できないようにする必要があるシステム属性の長いリストがある。
directoryType	ActiveDirectory	ディレクトリ・タイプ。
activationAttribute	obuseraccountcontrol	Active Directory アダプタがアクティブ化および非アクティブ化の対象を検索するために使用する Oracle Access Manager の属性名。Active Directory アダプタは、これに基づいてネイティブ・フラグ useraccountcontrol を設定する。
activationValue	ACTIVATED	obuseraccountcontrol のアクティブ化の値。
deactivationValue	DEACTIVATED ObWfPendingActivate ObWfPendingDeactivate	obuseraccountcontrol の非アクティブ化の値。
filterAuxiliaryClass	person organizationalPerson OblixOrgPerson oblixpersonpwdpolicy oblixadvancedgroup oblixgroup oblixAuxLocation	フィルタ処理によって除外する補助クラス。これは、Active Directory が静的補助クラスとして構成されているという前提に基づく。

4. 表 53 のパラメータを使用してユーザーのパスワードを設定または変更するために SSL 接続を使用する必要がある Active Directory のパスワード用のプラグインが含まれます。

注意： 現在のアダプタにオープン接続が使用されている場合、このプラグインは、SSL 接続を使用して構成されているアダプタにパスワードの設定 / 変更をリダイレクトします。

表 10-11 Active Directory のパスワード・プラグインのパラメータおよび値

パラメータ	値	コメント
adapter	AD SSL Adapter	OblixADSSLAdapterUsingMapper テンプレートに定義されているアダプタにリダイレクトする。
mapPassword	（設定なし。デフォルトは true）	パスワード属性を userPassword から unicodePwd にマップする。

Active Directory 用の OblixADAdapterUsingScript

このテンプレート（OblixADAdapterUsingScript）により、前述の説明とまったく同じ結果が得られます。このテンプレートの項目の内容は、10-75 ページの「Active Directory 用の OblixADAdapterUsingMapper」の 1、2 および 4 の内容と同じです。

OblixADAdapterUsingScript を使用する場合の唯一の違いは項目 3 です。この場合、この項目は次のようになります。

3. 表 10-10「OblixADAdapterUsingMapper、オブジェクト・クラス・マッパーのプラグイン・パラメータ」のパラメータがあり、マッピング・スクリプト・テンプレート OblixADMapping に定義されている Python で作成されたプラグイン・スクリプトが、10-75 ページの「Active Directory 用の OblixADAdapterUsingMapper」の項目 3 でオブジェクト・クラス・マッパーについて記載されているすべての機能を実行します。

Active Directory 用の OblixADSSLAdapterUsingMapper

このテンプレートは、SSL を介して Active Directory に接続するアダプタを定義します。これは、前述の項目 4 で説明したリダイレクト先のアダプタ用です。次を参照してください。

- Active Directory 用の OblixADAdapterUsingScript
- Active Directory 用の OblixADAdapterUsingScript

ADAM 用のテンプレート

ADAM 用として次の 3 つのテンプレートが用意されています。

- ADAM 用の OblixADAMAdapterUsingMapper
- ADAM 用の OblixADAMAdapterUsingScript
- ADAM 用の OblixADAMSSLAdapterUsingMapper

ADAM 用の OblixADAMAdapterUsingMapper

このテンプレート（OblixADAMAdapterUsingMapper）は、次が採用されたオブジェクト・マッパー・プラグインを使用して、ADAM の user および group データを Oracle Virtual Directory の inetorgperson および groupofuniquenames に変換するアダプタを定義します。

1. inetorgperson、groupofuniquenames および Oracle Access Manager のユーザー補助クラスの DN 構文を持つすべての属性を使用して DN 属性を設定し、これらの DN をネイティブ DN 形式で格納するためのメカニズム。
2. Active Directory の範囲属性用のプラグイン。

   ADAM は、xxx バイトのチャンクとしてもエントリを返します。このプラグインは、すべてのチャンクを 1 つの結果エントリとして連結します。
3. 表 10-12 に示すオブジェクト・クラスおよび属性をマップするためのパラメータ・ベースのユーザー・インタフェースを備えるオブジェクト・クラス・マッパー用のプラグインも含まれます。

表 10-12 OblixADAMAdapterUsingMapper、オブジェクト・クラス・マッパーのパラメータおよび値

パラメータ	値	コメント
`filterObjectClass OnModify`	（設定なし。デフォルトは false）	動的補助クラスが前提。ADAM が静的補助クラスとして構成されている場合、true に設定。
`addAttribute-group`	`groupType=4`	オブジェクト・クラスが group である場合、groupType 属性を追加し、デフォルト値を 4 に設定。この値は、顧客のニーズに応じて変更できる。
`mapAttribute`	`uniqueMember=member`	Oracle Virtual Directory の uniqueMember 属性を ADAM の member 属性にマップする。

表 10-12 OblixADAMAdapterUsingMapper、オブジェクト・クラス・マッパーのパラメータおよび値（続き）

パラメータ	値	コメント
mapAttribute	owner=managedBy	Oracle Virtual Directory の owner 属性を ADAM の managedBy 属性にマップする。
mapAttribute	uid=samaccountname	Oracle Virtual Directory の uid 属性を ADAM の samaccountName 属性にマップする。
filterAttribute-group	seeAlso,businessCategory,o	オブジェクト・クラスが group である場合、これらの属性をフィルタ処理によって除外する。これは、Active Directory の group がこれらの 3 つの属性をサポートしていないため。
mapObjectClass	groupofuniquenames=group	Oracle Virtual Directory の groupOfUniqueNames オブジェクト・クラスを Active Directory の group オブジェクト・クラスにマップする。
mapObjectClass	inetorgperson=user	Oracle Virtual Directory の inetorgperson オブジェクト・クラスを ADAM の user オブジェクト・クラスにマップする。
filterAttribute	（システム属性のリスト）	リスト内のすべての属性をフィルタ処理によって除外する。ADAM には、Oracle Access Manager からは参照できないようにする必要があるシステム属性の長いリストがある。
directoryType	ADAM	ディレクトリ・タイプ。
activationAttribute	obuseraccountcontrol	ADAM アダプタがアクティブ化および非アクティブ化の対象を検索するために使用する Oracle Access Manager の属性名。ADAM アダプタは、これに基づいてネイティブ・フラグ useraccountcontrol を設定。
activationValue	ACTIVATED	obuseraccountcontrol のアクティブ化の値。
deactivationValue	DEACTIVATED ObWfPendingActivate ObWfPendingDeactivate	obuseraccountcontrol の非アクティブ化の値。
filterAuxiliaryClass	（設定なし）	フィルタ処理によって除外する補助クラス。これは、ADAM が動的補助クラスとして構成されているという前提に基づく。ADAM が静的補助クラスとして構成されている場合、このパラメータに補助クラス名を指定する。

4. Active Directory のパスワード用のプラグインが含まれます（ADAM では、表 55 のパラメータを使用してユーザーのパスワードを設定または変更するために SSL 接続を使用する必要があります）。

> **注意：** 現在のアダプタにオープン接続が使用されている場合、このプラグインは、SSL 接続を使用して構成されているアダプタにパスワードの設定 / 変更をリダイレクトします。

表 10-13 OblixADAMAdapterUsingMapper、Active Directory のパスワードのパラメータ

パラメータ	値	コメント
adapter	ADAM SSL Adapter	`OblixADAMSSLAdapterUsingMapper` テンプレートに定義されているアダプタにリダイレクトする。
mapPassword	false	ADAM では userPassword 属性が使用されるため、パスワード属性をマップしない。

ADAM 用の OblixADAMAdapterUsingScript

このテンプレート（OblixADAMAdapterUsingScript）により、前述の説明とまったく同じ結果が得られます。このテンプレートの項目の内容は、10-77 ページの「ADAM 用の OblixADAMAdapterUsingMapper」の 1、2 および 4 の内容と同じです。

OblixADAMAdapterUsingScript を使用する場合の唯一の違いは項目 3 です。この場合、この項目は次のようになります。

3. 表 10-12「OblixADAMAdapterUsingMapper、オブジェクト・クラス・マッパーのパラメータおよび値」のパラメータがあり、テンプレート OblixADAMMapping に定義されている Python で作成されたプラグイン・スクリプトが、10-79 ページの「ADAM 用の OblixADAMSSLAdapterUsingMapper」の項目 3 でオブジェクト・クラス・マッパーについて記載されているすべての機能を実行します。

ADAM 用の OblixADAMSSLAdapterUsingMapper

このテンプレートは、SSL を介して ADAM ディレクトリに接続するアダプタを定義します。これは、前述の項目 4 で説明したリダイレクト先のアダプタ用です。次を参照してください。

- ADAM 用の OblixADAMAdapterUsingMapper
- ADAM 用の OblixADAMAdapterUsingScript

Sun Directory Server 用のテンプレート

Sun Directory Server 用としては、次の 2 つのテンプレートが用意されています。

- SunOne 用の OblixSunOneAdapterUsingMapper
- SunOne 用の OblixSunOneAdapterUsingScript

SunOne 用の OblixSunOneAdapterUsingMapper

このテンプレートは、次が含まれるオブジェクト・マッパー・プラグインを使用して、Sun Directory Server（旧 SunOne）の inetorgperson および groupofuniquenames を Oracle Virtual Directory の inetorgperson および groupofuniquenames に変換するアダプタを定義します。

1. inetorgperson、groupofuniquenames および Oracle Access Manager のユーザー補助クラスの DN 構文を持つすべての属性を使用して DN 属性を設定するためのメカニズム。これにより、これらの DN をネイティブ DN 形式で格納します。
2. 表 10-14 に示すオブジェクト・クラスおよび属性をマップするためのパラメータ・ベースのユーザー・インタフェースを備えるプラグイン（オブジェクト・クラス・マッパー）も含まれます。

表 10-14 OblixSunOneAdapterUsingMapper、オブジェクト・クラス・マッパーのパラメータ

パラメータ	値	コメント
`directoryType`	SunOne	ディレクトリ・タイプ。
`activationAttribute`	obuseraccountcontrol	SunOne アダプタがアクティブ化および非アクティブ化の対象を検索するために使用する Oracle Access Manager の属性名。SunOne アダプタは、これに基づいてネイティブ・フラグ nsaccountlock を設定。
`activationValue`	ACTIVATED	obuseraccountcontrol のアクティブ化の値。
`deactivationValue`	DEACTIVATED ObWfPendingActivate ObWfPendingDeactivate	obuseraccountcontrol の非アクティブ化の値。

SunOne 用の OblixSunOneAdapterUsingScript

このテンプレート（OblixSunOneAdapterUsingScript）により、前述の説明とまったく同じ結果が得られます。このテンプレートの項目の内容は、10-80 ページの「SunOne 用の OblixSunOneAdapterUsingMapper」の 1 の内容と同じです。

OblixSunOneAdapterUsingScript を使用する場合の唯一の違いは項目 2 です。この場合、この項目は次のようになります。

2. 表 10-14「OblixSunOneAdapterUsingMapper、オブジェクト・クラス・マッパーのパラメータ」のパラメータがあり、テンプレート OblixSunOneMapping に定義されている、Python で作成されたプラグイン・スクリプト。この表により、10-80 ページの「SunOne 用の OblixSunOneAdapterUsingMapper」の項目 2 でオブジェクト・クラス・マッパーについて記載されているすべての機能を実行できます。

eDirectory 用のテンプレート

eDirectory 用として次の 2 つのテンプレートが用意されています。

- eDirectory 用の OblixeDirectoryAdapterUsingMapper
- eDirectory 用の OblixeDirectoryAdapterUsingScript

eDirectory 用の OblixeDirectoryAdapterUsingMapper

このテンプレートは、次が含まれるオブジェクト・マッパー・プラグインを使用して、eDirectory の inetorgperson および groupofuniquenames を Oracle Virtual Directory の inetorgperson および groupofuniquenames に変換するアダプタを定義します。

1. inetorgperson、groupofuniquenames および Oracle Access Manager のユーザー補助クラスの DN 構文を持つすべての属性を使用して DN 属性を設定するためのメカニズム。これにより、これらの DN をネイティブ DN 形式で格納します。
2. 表 10-15 に示すオブジェクト・クラスと属性をマップするためのパラメータ・ベースのユーザー・インタフェースを備えるプラグイン（オブジェクト・クラス・マッパー）。

表 10-15 eDirectory 用の OblixeDirectoryAdapterUsingMapper

パラメータ	値	コメント
`directoryType`	SunOne	ディレクトリ・タイプ。
`activationAttribute`	obuseraccountcontrol	eDirectory アダプタがアクティブ化および非アクティブ化の対象を検索するために使用する Oracle Access Manager の属性名。これにより、eDirectory アダプタはネイティブ・フラグ logindisabled を設定。
`activationValue`	ACTIVATED	obuseraccountcontrol のアクティブ化の値。
`deactivationValue`	DEACTIVATED、ObWfPendingActivate、ObWfPendingDeactivate	obuseraccountcontrol の非アクティブ化の値。

eDirectory 用の OblixeDirectoryAdapterUsingScript

このテンプレート（OblixeDirectoryAdapterUsingScript）により、OblixeDirectoryAdapterUsingMapper を使用して説明した内容とまったく同じ結果が得られます。

OblixeDirectoryAdapterUsingScript を使用する場合の唯一の違いは項目 2 です。この場合、この項目は次のようになります。

2. 10-81 ページの「eDirectory 用の OblixeDirectoryAdapterUsingMapper」の項目 2 でオブジェクト・クラス・マッパーについて記載されているすべての機能を実行できる 10-81 ページの「eDirectory 用の OblixeDirectoryAdapterUsingMapper」のパラメータがあり、OblixeDirectoryMapping テンプレートに定義されている、Python で作成されたスクリプト。

データベース・テンプレート : OblixDBAdapterUsingScript

このテンプレートは、データベース用のアダプタを定義します。このテンプレートには、特定のマッピングは含まれていませんが、OblixDBMapping スクリプトはコールします。OblixDBMapping テンプレートに定義されているこのスクリプトは、Python で作成されており、LDAP の操作時にオブジェクト・クラスに関する不要な記載をフィルタ処理によって除外します。

スキーマ・マッピング・スクリプト・テンプレート

次のマッピング・スクリプト・テンプレートは、前述のアダプタ・テンプレートによって使用されます。これらのサンプル・マッピングにより、アダプタ・テンプレートのオブジェクト・クラス・マッパー・プラグインによって生成された構成と同じ構成が実行されます。マッピング・スクリプトの方が柔軟性があるため、プラグインでは不可能な高度な調整を行うことができます。

これらのマッピング・スクリプト・テンプレートには、スキーマ・マッピングおよび特別な処理を実行するための代替スクリプトが用意されています。

OblixADMapping: このマッピング・テンプレートには、次の機能があります。

- Active Directory の user および group データを inetorgperson および groupofuniquenames にそれぞれ変換します。
- ユーザーがアクティブ化または非アクティブ化されるときにネイティブ・フラグを設定します。
- 静的補助オブジェクト・クラスを処理します。
- grouptype を 4 に設定します。
- useraccountname が cn と同じになるように設定します。

OblixADAMMapping: このマッピング・テンプレートには、次の機能があります。

- Active Directory の user および group データを inetorgperson および groupofuniquenames にそれぞれ変換します。
- ユーザーがアクティブ化または非アクティブ化されるときにネイティブ・フラグを設定します。
- 静的補助オブジェクト・クラスを処理します。
- grouptype を 4 に設定します。

OblixeDirectoryMapping: ユーザーがアクティブ化または非アクティブ化されるときにネイティブ・フラグを設定します。

OblixSunOneMapping: ユーザーがアクティブ化または非アクティブ化されるときにネイティブ・フラグを設定します。

ヒント

次の項では、Oracle Virtual Directory の実装に関するその他の情報について説明します。10-84 ページの「データベースの接続性に関するヒント」も参照してください。

マッピング DN: マップされた DN は、Oracle Virtual Directory の論理 DN です。ただし、マップされた DN には物理ノードがありません。

アプリケーション（ID システムなど）が論理 DN を検索し、DN の存在の有無を確認したりその属性を取得することが必要な場合、たとえば、ldp.exe ユーティリティを使用して、エントリを手動で追加する必要があります。たとえば、マッピング DN が o=virtual company である場合、次のように、ldp.exe を使用して対応するエントリを作成する必要があります。

- obobjectclass: organization
- o: virtual_company

ここで、*organization* は xxx、virtual_company は xxx です。

構成およびポリシー・データの参照 DN: ポリシー・データで使用される UID などの参照 DN は、論理形式になっています。つまり、参照 DN は、ネイティブ・ディレクトリではなく Oracle Virtual Directory の DN として格納されています。このため、Oracle Virtual Directory のネームスペースのマッピングが完了した後、このマッピングは変更できません。ネームスペースのマッピングを変更すると、Oracle Access Manager の構成およびポリシー・データに格納されている参照 DN に影響が及びます。

スキーマ・マッピング : 論理からネイティブに属性をマッピングする場合、属性の構文に注意するとともに、属性が多値と単一値のどちらであるかに注意してください。

- Oracle Virtual Directory からディレクトリにマップする場合、文字列構文の微調整を除いて、同じ構文のままにする必要があります。
- Oracle Virtual Directory からデータベースにマップする場合、表 10-16「Oracle Virtual Directory からデータベースへのマッピング」を参考にしてください。

表 10-16 Oracle Virtual Directory からデータベースへのマッピング

LDAP 属性の構文	MS SQL のデータ型
1.3.6.1.4.1.1466.115.121.1.5 DESC 'Binary'	binary
1.3.6.1.4.1.1466.115.121.1.6 DESC 'Bit String'	binary
1.3.6.1.4.1.1466.115.121.1.7 DESC 'Boolean'	varchar
1.3.6.1.4.1.1466.115.121.1.8 DESC 'Certificate'binary	binary
1.3.6.1.4.1.1466.115.121.1.9 DESC 'Certificate List'	binary
1.3.6.1.4.1.1466.115.121.1.10 DESC 'Certificate Pair'	binary
1.3.6.1.4.1.1466.115.121.1.11 DESC 'Country String'	varchar
1.3.6.1.4.1.1466.115.121.1.12 DESC 'DN'	varchar
1.3.6.1.4.1.1466.115.121.1.15 DESC 'Directory String'	varchar
1.3.6.1.4.1.1466.115.121.1.22 DESC 'Facsimile Telephone Number'	varchar
1.3.6.1.4.1.1466.115.121.1.23 DESC 'Fax'	tvarchar
1.3.6.1.4.1.1466.115.121.1.24 DESC 'Generalized Time'	timestamp
1.3.6.1.4.1.1466.115.121.1.26 DESC 'IA5 String'	binary
1.3.6.1.4.1.1466.115.121.1.27 DESC 'INTEGER'	numeric/int
1.3.6.1.4.1.1466.115.121.1.28 DESC 'JPEG'	binary
1.3.6.1.4.1.1466.115.121.1.33 DESC 'MHS OR Address'	varchar
1.3.6.1.4.1.1466.115.121.1.36 DESC 'Numeric String'	varchar
1.3.6.1.4.1.1466.115.121.1.38 DESC 'OID'	varchar

表 10-16 Oracle Virtual Directory からデータベースへのマッピング（続き）

LDAP 属性の構文	MS SQL のデータ型
1.3.6.1.4.1.1466.115.121.1.39 DESC 'Other Mailbox'	varchar
1.3.6.1.4.1.1466.115.121.1.41 DESC 'Postal Address'	varchar
1.3.6.1.4.1.1466.115.121.1.44 DESC 'Printable String'	varchar
1.3.6.1.4.1.1466.115.121.1.50 DESC 'Telephone Number'	varchar
1.3.6.1.4.1.1466.115.121.1.53 DESC 'UTC Time'	timestamp

データベースの接続性に関するヒント

データベースの接続性に関する考慮点は、次のとおりです。

- エントリ名の構成
- 複数表の書込み
- 多値属性
- 検索
- 書込み
- 連鎖削除

エントリ名の構成 : エントリ名の一部（エントリ名の基本部分は除く）として使用されるデータベース・フィールドはすべて、データベース・アダプタを介して Oracle Virtual Directory にマップされて返される行に含まれる必要があります。

たとえば、ユーザー・オブジェクトの名前に共通名（cn）および組織単位（ou）の両方（cn=Joe User,ou=Marketing）が含まれる階層を作成する場合、cn および ou は両方とも作成対象のエントリの一部である必要があります。

単純 LDAP では、ou 属性は親エントリの一部であるため、この属性は必要ありません。データベースは階層的ではないため、この機能をサポートしながら、階層を定義するために大量の新しいメタデータを作成および管理しなくてすむようにするには、これが唯一の適切な方法です。

複数表の書込み : 1 つのデータベース・アダプタに対して、複数の表を直接書き込むことはできません。これは、Oracle Virtual Directory の設計上の制限ではなく、実際にはデータベース上の制限です。たとえば、データベースのビューが複数の表を示している場合、ほとんどのデータベースのビューは直接更新できません。

Oracle Virtual Directory では、独自の結合ビュー実装を使用してこの制限を回避しています。複数のデータベース・アダプタ（たいていは表ごとに 1 つ）を作成し、これらの関係を定義することにより、複数の表を介して構成されたエントリへの書込みを Oracle Virtual Directory が管理できるようになります。結合ビューの作成の詳細は、『Oracle Virtual Directory 製品マニュアル』を参照してください。

多値属性 : 通常、データベースでは、表の単一行内の 1 つのフィールドに複数の値は使用できません。配列型がサポートされている例外もありますが、これらのデータ型は比較的制限される傾向があります。ユーザーによっては、カンマやパイプ（|）などのデリミタを使用してフィールド内のデータ（アカウント・フラグなど）を区切ることにより、1 行に複数の値を入力する場合があります。

従来のデータベース設計では、複数の値を持つフィールドは追加表に正規化するよう規定されています。データ・ウェアハウスの一部であるデータベースの場合、非正規化された表にすべてのフィールドのすべての順列を配置するという別の方式が使用されることがあります。

通常、Oracle Virtual Directory はどちらのモデルもサポートしています。オラクル社は、非正規化された表に順列を配置する方式を最終的な手段としてのみ使用することをお薦めします。正規化されたセカンダリ表方式の場合、Oracle Access Manager での検索に対して一貫性のある正確な結果が返されない可能性があります。

多値属性の詳細は、次を参照してください。

- Oracle Access Manager と Oracle Virtual Directory の実装のテンプレート
- E-12 ページの複数値属性の問題

検索 : 検索は、正規化された表または非正規化された表に対してサポートされています。この場合、必要に応じてデータベース・レベルの結合を構成する以外、他の作業は必要ありません。

検索に関して注意が必要な考慮点は、最も一般的な使用事例により、データベース・アダプタの現在の設計では、多値属性が検索されるとエントリの一部として検索と一致する値のみが返されるようになっている点です。これにより、大きなグループの検索時のパフォーマンスが向上します。Oracle では、すべての値を返すための 2 次選択をサポートするために、将来のバージョンではこの構成を実現する予定です。それまでには、マッピングで追加検索を実行してすべての属性を取得できるようになります。

書込み : 正規化された表に対する書込みは、データベースの設計に基づいて属性を各表に分割する結合ビューを介して実行する必要があります。データベースの設計に関する一般的なガイドラインは複数存在し、すべての顧客のデータベースは異なるため、このような作業が必要です。

既存の重要な表を使用するほとんどの顧客は、これらの表の更新管理の一環としてストアド・プロシージャも使用します。これらのストアド・プロシージャは API コールと似ており、その構成およびコール方法はデータベースごとに独自の仕様になっていますが、コール自体は顧客独自の仕様になっています。Oracle では、プラグイン・システムを使用してストアド・プロシージャをサポートしています。

Oracle Virtual Directory は、エントリの RDN として使用されるフィールドに関連付けられたエントリで使用される各フィールドの値を持つ非正規化された表に対する直接書込みを管理できます。追加、変更および削除はすべてサポートされます。

変更操作については、変更→置換操作によって既存の属性値が削除され、新しい属性値が追加される点に注意する必要があります。これは、SQL の挿入、更新および削除で構成された一連の操作ではなく、SQL 削除と SQL 挿入を意味します。ここで、正規化された表を持つ顧客には、挿入または削除によってデータベース内でその他のアクションがトリガーされるという潜在的な問題があります。このような場合、変更→置換操作を処理するプラグインを構成する必要があります。

ほとんどの顧客は、変更に対する直接的な SQL アクセスを使用していないか、複数の値を読取り専用として使用しているか、変更→追加および変更→削除のみを直接使用しているかのいずれかのため、このような状況にはなりません。たとえば、大きなグループに関する問題に取り組んでいる顧客の場合、Oracle Virtual Directory を介してグループをデータベースに格納します。グループ・メンバーに関するほとんどの変更内容は、置換ではなく追加と削除です。

連鎖削除 : 書込みに関する項で説明した問題の中で、Oracle Virtual Directory によってデータベースへの直接書込みが処理される既存のデータベースについて最も注意が必要なのは、顧客データベースにおける連鎖削除の使用です。連鎖削除の場合、前の項で説明した変更→置換操作により、直接関係のある表の外部で削除がトリガーされる可能性があります。

ただし、このトリガーが正規化された表に基づいて行われる場合、単一値の正規化された表の変更時には Oracle Virtual Directory において削除→挿入操作ではなく SQL 更新が実行されるため、これは問題ではありません。これにより、前述の問題は解消されます。

連鎖削除に関して潜在的に危険な設定が適用された特定の顧客状況に関して不明な点がある場合は、オラクル社にお問い合せください。また、Oracle Virtual Directory のデバッグ・レベルを上げてテスト・データベースを指定することにより、LDAP 操作の順序について Oracle Virtual Directory によって生成される SQL を確認することもできます。

Oracle Virtual Directory を使用した実装のトラブルシューティング

詳細は、E-11 ページの「Oracle Virtual Directory の実装の問題」を参照してください。

11

SNMP エージェントのインストール

この章では、Simple Network Management Protocol（SNMP）エージェントをインストールする方法について説明します。SNMP エージェントによって、ネットワーク上の様々なコンポーネントのアクティビティを監視できます。次を参照してください。

- SNMP エージェントおよびインストールの概要
- SNMP エージェントのインストールの考慮点
- SNMP のインストールの前提条件チェックリスト
- Oracle Access Manager SNMP エージェントのインストール

インストール後の SNMP エージェントの構成の詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

SNMP エージェントおよびインストールの概要

Oracle Access Manager は SNMP およびネットワーク管理システム（NMS）で使用できるデータを提供し、これにより Identity Server および Access Server のステータスおよびアクティビティを監視できます。

SNMP エージェントはオプションのコンポーネントです。インストールした場合、SNMP エージェントは、エージェントがインストールされたものと同じサーバー・ホスト上の Identity Server または Access Server に関する情報にアクセスします。SNMP エージェントのインストール・プロセスは、他の Oracle Access Manager コンポーネントの場合と類似しています。インストール・ディレクトリは次のとおりです。

Windows のデフォルト : ¥Program Files¥OracleAccessManager_SnmpAgent¥snmp

UNIX のデフォルト : /opt/OracleAccessManager_SnmpAgent¥snmp

このマニュアルの場合 : ¥*SNMP_install_dir*¥snmp

SNMP エージェントのインストールの考慮点

SNMP エージェントは、サービスを実行する Oracle Access Manager サーバー、つまり Identity Server または Access Server と同じマシンにインストールする必要があります。Oracle Access Manager SNMP エージェントは、Identity Server または Access Server と同じユーザーとして実行する必要があります。

ネットワーク管理ステーション（NMS）ホストの SNMP データにはコミュニティ名が必要です。NMS ホストの Oracle Access Manager SNMP トラップに対しても、トラップ先を構成する必要があります。

SNMP エージェントは専用ユーザーが所有する必要があります。UNIX では、root ユーザーまたは専用ユーザーのみがエージェント・サービスを起動できます。ほとんどの場合、サーバーは root または nobody として実行されます。UNIX では、ユーザーが属するグループも入力します。

SNMP のインストールの前提条件チェックリスト

表 11-1 は、Oracle Access Manager で SNMP エージェントをインストールする前に満たす必要がある項目のチェックリストです。

表 11-1 WebGate の前提条件チェックリスト

チェックリスト	SNMP 前提条件
	第 I 部「インストールの計画と前提条件」で説明されている、ユーザーの環境に適用される前提条件および要件がすべて満たされていることを確認する。
	第 II 部「ID システムのインストールおよび設定」のアクティビティをすべて完了する。
	第 III 部「アクセス・システムのインストールおよび設定」のアクティビティをすべて完了する。
	ネットワーク管理ステーション（NMS）ホストの SNMP データにコミュニティ名を作成する。
	NMS ホストに SNMP トラップのトラップ先を構成する。

Oracle Access Manager SNMP エージェントのインストール

SNMP エージェントをインストールする方法を次に説明します。

SNMP エージェントのインストールに含まれる手順

1. 11-3 ページの「インストールの開始」
2. 11-3 ページの「Oracle Access Manager SNMP エージェントのインストール」
3. 11-4 ページの「SNMP エージェントの構成詳細の指定」
4. 11-5 ページの「インストールの終了」

インストールの開始

SNMP エージェントに固有の点を除き、インストールは、他の Oracle Access Manager コンポーネントの場合と類似しています。

SNMP エージェントのインストールの手順

1. 管理者権限を持つユーザーとしてログインします。
2. ソフトウェアのダウンロード時に作成した一時ディレクトリで、コンポーネントのインストーラを検索して起動します。

   例 :

   - **GUI モード**

     Windows: Oracle_Access_Manager10_1_4_0_1_win32_Snmp_Agent.exe

   - **コンソール・モード**

     UNIX: ./ Oracle_Access_Manager10_1_4_0_1_sparc-s2_Snmp_Agent

   「ようこそ」ダイアログが表示されます。
3. 「次へ」をクリックして「ようこそ」画面を閉じます。
4. プラットフォームに基づいて管理者権限に関する質問に応答します。次に例を示します。
5. インストール・ディレクトリを指定してから、「次へ」をクリックします。次に例を示します。

   ¥SnmpAgent

   インストール・ディレクトリのサマリーと必要なディスク領域が表示されます。
6. インストール・ディレクトリを記録して、「次へ」をクリックします。

   数秒後、SNMP エージェントがインストールされます。Windows システムの場合、Microsoft 管理インタフェースが構成されるという通知が表示されます。

   Windows: 次の情報を入力して Windows の「サービス」ウィンドウでこの SNMP エージェントを特定してから、「次へ」をクリックします。次に例を示します。

   - **Windows サービス名 :** この SNMP エージェントに一意の名前。

     たとえば、SNMP1014 という名前を付けた場合、「サービス」ウィンドウに表示される名前は Oracle Access Manager SNMP Agent (SNMP1014) となります。
   - **アカウント名 :** この SNMP エージェントの DomainName¥UserName（デフォルトは LocalSystem です）。
   - **パスワード :** このアカウントのパスワード。

   次に、この SNMP エージェントに固有の詳細を定義するよう求められます。

SNMP エージェントの構成詳細の指定

ここでは、この SNMP エージェントのポート情報およびコミュニティ情報を入力します。

SNMP エージェント詳細の指定の手順

1. Oracle Access Manager で SNMP 統計の公開に使用する SNMP エージェント TCP ポートを入力します。次に例を示します。

   6012

   これは、特定の Identity Server または Access Server で SNMP エージェントを有効化するときに指定するポート番号と同じです。Oracle Access Manager コンポーネントはこのポートと通信してマネージャ・ステーションに統計を公開します。

   次に、SNMP エージェントの問合せに使用するネットワーク管理システムで定義されている UDP ポートおよびコミュニティ名の指定を求められます。これらはネットワーク・マネージャ・ステーションでこの SNMP エージェントを問い合せるときに使用するものと同じである必要があります。

2. SNMP エージェント UDP ポートおよびコミュニティ名を入力してから、「次へ」をクリックします。

   例 :

   - **SNMP エージェント UDP ポート :** 161
   - **コミュニティ名 :** ユーザーのコミュニティ

     ここで、SNMP トラップを送信するときに SNMP エージェントで使用されるネットワーク管理システムから、ネットワーク・モニター・ステーション名およびトラップ・ポートを入力するよう求められます。トラップ・ポートは Oracle Access Manager の SNMP トラップを受信するポートです。

3. 次の情報を入力してから、「次へ」をクリックします。

   例 :

   - **マネージャ・ステーション名 :** ユーザーのステーション名
   - **トラップ・ポート :** 162

   ここで、この SNMP エージェントに他のマネージャ・ステーションを構成するかどうかを指定する必要があります。

4. 他のマネージャ・ステーションを構成することを示す場合は「はい」（構成しない場合は「いいえ」）をクリックしてから、「次へ」をクリックします。

   - 「はい」の場合、新しいステーションに対して手順 3 を繰り返し、他のステーションを構成するかどうかの指定を求められます。
   - 「いいえ」の場合、*SNMP_install_dir*¥snmp¥tools¥setup¥setup_agent のツールを後で使用して他のマネージャ・ステーションを手動で構成することもできます。

   確認ダイアログが表示されます。

インストールの終了

その他のコンポーネントのインストールと同様に、インストールが終了します。

インストールの終了の手順

1. README の情報を確認してから、「次へ」をクリックします。

   サマリー画面が表示されます。

2. このインストールの詳細をまだ準備ワークシートに書き込んでいない場合はここで書き込んでから、「次へ」をクリックしてインストールを終了します。

『Oracle Access Manager ID および共通管理ガイド』で説明されている、SNMP エージェントの構成の準備が整いました。

12

言語パックの個別インストール

この章では、Oracle Access Manager コンポーネントのインストールおよび設定後（または以前のリリースからのアップグレード後）にオプションの言語パックをインストールする方法について説明します。次の項目について説明します。

- 言語パックおよびインストールの概要
- 言語パックのインストールの考慮点
- 言語パックの前提条件チェックリスト
- 言語パックの個別インストール
- インストールされたファイル
- 言語ステータスの確認

言語の概要は、『Oracle Access Manager 概要』および第 3 章「マルチ言語環境の概要」を参照してください。

言語パックおよびインストールの概要

オラクル社は、Oracle Access Manager アプリケーションをローカライズし、エラー・メッセージや、タブ、パネルおよび属性の表示名などの静的データをユーザーのネイティブ言語で表示する機能を提供しています。英語は常に使用可能で、インストールまたは構成は特に必要ありません。さらに、オラクル社提供の言語パックをインストールし、Oracle Access Manager 用の管理者のデフォルト言語を選択できます。

注意： Oracle Access Manager では、Latin1、および中国語や日本語のようなマルチバイト言語を含む UTF-8 のデータなどもサポートされています。特定の言語パックに関する情報は、オラクル社にお問い合せください。

オラクル社がサポートする各言語には、ID システム用に 1 つの言語パック・インストーラ、アクセス・システム用に 1 つの言語パック・インストーラが用意されています。他の章で説明するように、言語パックは Oracle Access Manager コンポーネントとともにインストールできます。ただし、この章で説明するように、Oracle Access Manager のインストールおよび設定後に言語パックを個別にインストールすることも可能です。

第 3 章「マルチ言語環境の概要」で説明しているように、言語パック用に指定するインストール・ディレクトリは、操作対象のコンポーネントのインストール・ディレクトリと一致している必要があります。次に例を示します。

¥*IdentityServer_install_dir*

¥*WebPass_install_dir*

¥*PolicyManager_install_dir*

¥*AccessServer_install_dir*

¥*WebGate_install_dir*

さらに、ID システムのコンポーネントに言語パックをインストールする場合は、アクセス・システムのコンポーネントすべてに同じ言語パックをインストールする必要があります。

インストール中、¥*langTag* ディレクトリがファイル・システム内でメインの Oracle Access Manager コンポーネントのインストール・ディレクトリの下に作成されます。たとえば、*Component_install_dir*¥identity | access¥oblix¥lang¥*langTag* の場合、*langTag* は英語（en-us）またはフランス語（fr-fr）のような特定の言語を表します。例は、12-6 ページの「インストールされたファイル」を参照してください。

インストールされた各言語の言語エントリが、obid=langTag, configDN のように LDAP ディレクトリの Oblix ノードの下に作成されますが、ここで configDN はディレクトリの構成 DN です。

obnls.xml 構成ファイルは各コンポーネントに対して ¥*Component_install_dir*¥identity | access¥oblix¥config¥obnls.xml で更新されます。obnls.xml にインストールされた言語およびエントリは各コンポーネントと一致している必要があります。次のサンプルの obnls.xml ファイルにインストールされた言語には、英語、アラビア語、チェコ語、日本語および簡体字中国語があります。

```
 <?xml version="1.0" encoding="UTF-8" ?>
- <ParamsCtlg xmlns="http://www.oblix.com" CtlgName="obnls.xml">

- <CompoundList xmlns="http://www.oblix.com" ListName="">
- <SimpleList>
  <NameValPair ParamName="default" Value="en-us" />
  </SimpleList>
- <ValList xmlns="http://www.oblix.com" ListName="languages">

  <ValListMember Value="en-us" />
  <ValListMember Value="ar-ar" />
 <ValListMember Value="cs-cs" />
   <ValListMember Value="ja-jp" />
```

```
  <ValListMember Value="zh-CN" />
</ValList>
 - <ValNameList xmlns="http://www.oblix.com" ListName="en-us">
   <NameValPair ParamName="sortRulesFile" />
  <NameValPair ParamName="dirPath" Value="en-us" />
 </ValNameList>
 - <ValNameList xmlns="http://www.oblix.com" ListName="ar-ar">
  <NameValPair ParamName="sortRulesFile" />
  <NameValPair ParamName="dirPath" Value="ar-ar" />
  </ValNameList>
- <ValNameList xmlns="http://www.oblix.com" ListName="cs-cs">
 <NameValPair ParamName="sortRulesFile" />
  <NameValPair ParamName="dirPath" Value="cs-cs" />
  </ValNameList>
- <ValNameList xmlns="http://www.oblix.com" ListName="ja-jp">
  <NameValPair ParamName="sortRulesFile" />
   <NameValPair ParamName="dirPath" Value="ja-jp" />
 </ValNameList>
- <ValNameList xmlns="http://www.oblix.com" ListName="zh-CN">
  <NameValPair ParamName="sortRulesFile" />
 <NameValPair ParamName="dirPath" Value="zh-CN" />
   </ValNameList>
 - <!--  List of locales that require bidi support
  -->
- <ValList xmlns="http://www.oblix.com"
ListName="bidiLanguages">
 <ValListMember Value="he" />
 <ValListMember Value="ar" />
  <ValListMember Value="iw" />
  </ValList>
  </CompoundList>
   </ParamsCtlg>
```

タスクの概要 : 言語パックの個別インストール

1. 12-5 ページの「言語パックの個別インストール」で説明されているように、インストール（またはアップグレード）された Identity Server およびインストールされた WebPass をホストしている各マシンで、ID システム言語パックのインストーラを実行します。
2. 12-6 ページの「言語ステータスの確認」の手順に従って、インストールした言語が有効であることを確認します。
3. 12-5 ページの「言語パックの個別インストール」の手順に従って、インストール（またはアップグレード）された Policy Manager、Access Server および WebGate をホストしている各マシンで、アクセス・システム言語パックのインストーラを実行します。

   Access Server および WebGate のユーザー・インタフェースがない場合でも、他のコンポーネントの場合と同様に、同じ言語パックをインストールする必要があります。
4. 12-6 ページの「言語ステータスの確認」の手順に従って、インストールした言語が有効であることを確認します。

言語パックのインストールの考慮点

各コンポーネントのインストール中またはインストール後に、言語を追加インストールして Oracle Access Manager でマルチ言語機能を有効化できます。

Policy Manager と WebGate を同じディレクトリにインストールしている場合、言語パックを同じディレクトリにインストールすると両方のコンポーネントで使用できます。つまり、Policy Manager 用に言語パックをインストールした後で、同じディレクトリに存在する WebGate に対してこのプロセスを繰り返す必要はありません。

注意： 同じディレクトリに Policy Manager、言語パック、WebGate の順にインストールしないでください。この順番でインストールした場合、WebGate の obnls.xml ファイルに適切な言語エントリが表示されません。

UNIX システムでは、言語パックに実行権限があることを確認した後でインストーラを起動する必要があります。たとえば、次のようにします。

```
chmod +x "Oracle_Access_Manager10_1_4_0_1_FR_sparc-s2_LP_Identity_System"
chmod +x "Oracle_Access_Manager10_1_4_0_1_FR_sparc-s2_LP_Access_System"
```

Oracle Access Manager の各コンポーネントをインストール中に言語パックのサイレント・インストールを実行する場合、言語パックのインストーラはコンポーネントのインストーラと同じ一時ディレクトリに存在している必要があります。詳細は、このマニュアルの第 3 章「マルチ言語環境の概要」、およびインストールに関する個々の章を参照してください。

言語パックの前提条件チェックリスト

言語パックの個別インストールを開始する前に、12-4 ページの「言語パックの前提条件チェックリスト」のタスクをチェックします。これらの前提条件が満たされていることを確認します。前提条件が満たされていないと、Oracle Access Manager のインストールに悪影響が生じる場合があります。

表 12-1 言語パックのインストールの前提条件チェックリスト

チェックリスト	言語パックのインストールの前提条件
	第 I 部「インストールの計画と前提条件」で説明されている、ユーザーの環境に適用される前提条件および要件がすべて満たされていることを確認する。
	第 II 部「ID システムのインストールおよび設定」のアクティビティをすべて完了する。
	第 III 部「アクセス・システムのインストールおよび設定」のアクティビティをすべて完了する。

Oracle Access Manager コンポーネントと同時に言語パックをインストールするには、言語パックのインストール・パッケージをコンポーネントのインストール・パッケージと同じディレクトリに移動し、このマニュアルで該当する章を参照してください。

言語パックの個別インストール

この手順によって、Oracle Access Manager コンポーネントのインストールおよび設定後に言語パックを個別に追加できます。

言語パックの個別インストールの実行の手順

1. 管理者権限を持つユーザーとしてログインします。
2. 目的の言語パックおよびコンポーネントのインストール・パッケージを検索して起動し、インストーラを起動します。

   例 :

   - **Windows の GUI メソッド**

     Oracle_Access_Manager10_1_4_0_1_win32_*langTag*_Identity_System.exe

     または

     Oracle_Access_Manager10_1_4_0_1_win32_*langTag*_Access_System.exe

   - **UNIX のコンソール・メソッド**

     / Oracle_Access_Manager10_1_4_0_1_sparc-s2_*langTag*_Identity_System

     または

     / Oracle_Access_Manager10_1_4_0_1_sparc-s2_*langTag*_Access_System

     ここで *langTag* は FR（フランス語）のような特定の言語タグを指します。

     「ようこそ」画面が表示されます。
3. 「次へ」をクリックして「ようこそ」画面を閉じます。
4. プラットフォームに基づいて管理者権限に関する質問に応答します。
5. インストールするメインのコンポーネントと一致するように宛先ディレクトリを変更してから、「次へ」をクリックします。

   例 :

   ¥*IdentityServer_install_dir*

   数秒間、言語パックをインストール中という通知があります。次に README の情報が表示されます。
6. README の情報を確認してから、「次へ」をクリックして終了します。

   サマリー画面が表示されます。
7. 「終了」をクリックしてこのインストールを完了します。
8. インストールを完了した言語パックのサービスを再起動します。
9. 次のコンポーネントで言語パックのインストールを繰り返します。
   - ID システム言語パックを使用して WebPass の全コンポーネントにインストールします。
   - アクセス・システム言語パックを使用してアクセス・システムの全コンポーネントにインストールします。
     - Policy Manager
     - Access Server
     - WebGate

インストールされたファイル

第 3 章「マルチ言語環境の概要」で説明しているように、¥lang ディレクトリと、¥lang¥en-us および ¥lang¥shared サブディレクトリはすべてのインストールに含まれます。言語を追加インストールする場合、¥lang の下に *¥langTag* サブディレクトリが作成されます。これには ¥en-us と同じタイプのコンテンツが含まれ、ローカライズのみ行われます。

言語ステータスの確認

次の手順を使用して Oracle Access Manager にインストールされ、有効化されている言語を確認します。

有効な言語の確認の手順

1. ID システム・コンソールに移動し、通常どおりログインします。

   ```
   http://hostname:port/identity/oblix/
   ```

   ここで、*hostname* は Web サーバーをホストするマシン、*port* は WebPass の Web サーバー・インスタンスの HTTP ポート番号をそれぞれ指し、/identity/oblix は ID システム・コンソールに接続します。

2. 「ID システム・コンソール」をクリックして「システム構成」を選択してから、「サーバー設定」をクリックします。

3. ページ下部の「マルチ言語」リンクをクリックします。

   「マルチ言語の管理」ページが表示され、現在インストールされている言語および有効な言語が示されます。

4. 有効化する言語の横のボックスをクリックしてから、「有効化」ボタンをクリックします。

5. ブラウザ画面をリフレッシュするか、ブラウザを開きなおします。

   インストール後、使用する言語をすべて有効化する必要があります。その後で ID システム・コンソールを使用して属性、タブおよびパネルの表示名を（オブジェクト・クラスのレベルで）入力することによって、インストールした言語を使用するユーザー、グループまたは Org Manager のアプリケーションを構成する必要があります。

6. 詳細は、次のドキュメントを参照してください。

   - Oracle Access Manager コンポーネントのアンインストール
   - 言語の問題
   - 言語プリファレンスの設定、および Oracle Access Manager の情報のローカライズの詳細は『Oracle Access Manager ID および共通管理ガイド』を参照してください。

13

データベースの監査コンポーネントのインストール概要

Oracle Access Manager の監査機能ではポリシーとプロファイルの設定、システム・イベント、および使用パターンに関連するデータが収集および表示されます。Oracle Access Manager では 2 つのタイプの監査レポートを生成できます。

- **静的 :** これらのレポートは、Oracle Access Manager ディレクトリ・サーバーに格納されたポリシーおよびプロファイルの情報から導出されます。
- **動的 :** これらのレポートはシステム内のサーバーから収集されたアクセス・システムおよび ID システムのイベントから導出されます。

  最も詳細なレベルでは、動的な監査レポートにより、いつ、誰によってシステム・イベントがトリガーされたかがわかります。上位レベルでは、これらのレポートにより、コンポーネントのロード・レベル、リソースのリクエスト・パターン、システム侵入攻撃、および全体的なシステム・パフォーマンスがわかります。

  監査の他に、Oracle Access Manager ではロギング、SNMP 監視、およびその他のレポート機能がサポートされています。

すべての動的な監査レポートと一部の静的な監査レポートを、ディスク・ファイル、リレーショナル・データベース、またはその両方に記録できます。静的なレポートの一部には、グラフィカル・ユーザー・インタフェースを介して制限付きの形式で表示できるものもあります。

監査レポートを画面上に表示したり、監査結果をディスク・ファイルに送信する場合、特別なコンポーネントのインストールは必要ありません。この方法で監査レポートを表示する場合、『Oracle Access Manager ID および共通管理ガイド』の構成指示を完了する必要があります。

データベースの監査は一部の Oracle Access Manager システム構成に制限され、「システム・コンソール」を使用する設定の他に特別なコンポーネントのインストールを必要とします。詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

14

Software Developer Kit の概要

Access Manager Software Developer Kit（SDK）によって、開発者は Oracle Access Manager のアクセス管理機能を拡張できます。Access Manager SDK はライブラリ、構築方法および例から構成され、ユーザー（または Oblix）が Web リソースおよび Web 以外のリソースに対してカスタム AccessGate を作成する際に使用できます。

AccessGate では Access Server を使用して Web サイトへのアクセスの試行を制御します。AccessGate は、Oracle Access Manager で提供される WebGate アクセス・クライアントに類似しています。WebGate クライアントは、個々の Web サーバーと Access Server 間のインタフェースとして機能します。WebGate はユーザーからの Web リソースのリクエストを捕捉して、Access Server を介してそれらを認可します。

AccessGate によって認可および認証ルールを URL 以外の他のリソースにも適用して、ユーザーの Oracle Access Manager 以外のアプリケーションとの対話を制御できます。これにより、Web リソースおよび Web 以外のリソースに適用される、集中管理されたポリシー情報の使用が可能になります。

Access Manager SDK を使用すると、BEA 社の WebLogic、IBM 社の WebSphere、iPlanet 社の Application Server などの市販されているアプリケーション・サーバー、あるいは Access Server にアクセスできるその他のアプリケーションに構築可能なインタフェースを作成できます。Access Manager API は Java および C/C++ アプリケーションと統合できます。

SDK の使用はオプションであり、開発者のみに関連します。したがって、SDK のインストールに関する情報は『Oracle Access Manager 開発者ガイド』にあります。

ID システムの一部の機能では Oracle Access Manager Software Developer Kit（SDK）が必要です。デフォルトでは、SDK は ¥*IdentityServer_install_dir*¥identity の下のサブディレクトリにインストールされます。『Oracle Access Manager ID および共通管理ガイド』で説明されているように、ID システムの設定に続き、ID システム用に手動で SDK を構成して目的の機能を有効化する必要があります。

第 V 部

レプリケーション

ここでは、レプリケーション、サイレント・モード・オプション、およびインストール済コンポーネントのクローニングと同期化について説明します。また、コンポーネントのアンインストールについても説明します。

第 VI 部は、次の章で構成されます。

- 第 15 章「コンポーネントのレプリケート」

15

コンポーネントのレプリケート

コマンドラインまたはインストール GUI を使用して Oracle Access Manager のコンポーネントをインストールするかわりに、インストール済コンポーネントの構成を別のコンポーネントにレプリケートすることでインストール・プロセスを自動化できます。これは、オプション・ファイルからのインストール、またはインストール済コンポーネントのクローニングによって行います。2 つのインストール済コンポーネントを同期化することで、コンポーネントを部分的にレプリケートすることもできます。

この章では、オプション・ファイル、クローニングおよび同期化を使用したインストールについて説明します。内容は次のとおりです。

サイレント・モード・オプション・ファイルについて

GUI またはコンソールから Oracle Access Manager をインストールする他に、インストールのためのパラメータと値を含むファイルを使用して自動インストールを実行できます。これはサイレント・モードのインストールと呼ばれます。サイレント・モードではユーザーが介入せずにインストールを行うことができます。

注意： サイレント・モードは、Oracle Access Manager の新規インストールのみが対象です。移行やアップグレードでは使用できません。ADAM およびサイレント・インストールの詳細は、B-17 ページの「Oracle Access Manager のサイレント・モード・インストールのパラメータ」を参照してください。

サイレント・モード・インストールはオプション・ファイルを使用して実行します。Oracle Access Manager コンポーネントをインストールすると、インストール・プログラムによって install_options.txt という名前のファイルが自動的に作成され、コンポーネントのインストール・ディレクトリに書き込まれます。一般的なパスは次のとおりです。

/*Component_install_dir*/identity|access/oblix/config/install_options.txt

Component_install_dir はこのパスの最上位のディレクトリです。identity|access は各 Oracle Access Manager コンポーネントの接尾辞を表します。次に例を示します。

/OracleAccessManager/identity/oblix/config/install_options.txt

インストール・セッションはインストール・オプション・ファイルに記録されます。このファイルには、インストール時にユーザーに対して表示されるプロンプトと、ユーザーが指定する値の情報が含まれます。将来のインストール時には、パラメータ値を必要に応じて変更し、このファイルをテンプレートとして使用できます。

インストール時にいずれかの値を再入力する場合はファイルを編集する必要があります。インストール・セッション全体がこのファイルに記録されるため、同じオプションに対して複数回データを入力した場合は情報を削除する必要があります。また、新たにインストールするためにパラメータ値を変更するときも、このファイルを編集する必要があります。Identity Server や WebPass の場合や、少なくとも、新しいコンポーネントに一意の ID を指定する必要があります。インストール中に入力されたパスワードは、セキュリティ上の理由から記録されません。

サイレント・モード・オプション・ファイルのその他の利用方法

サイレント・モード・オプション・ファイルは、対話型インストールのデフォルト値を指定するためにも使用できます。これは、Oracle Access Manager コンポーネントの複数のインスタンスをインストールする際にデフォルト値を指定する場合に役立ちます。インストールのデフォルト値を提供するには、この章の説明に従ってください。ただし次の例外があります。

- デフォルトのないパラメータと値（パスワード値など）はオプション・ファイルから削除します。
- この後で説明する -silent オプションなしでインストール・プログラムを起動します。

サイレント・モード・オプション・ファイルの実行

サイレント・モード・オプション・ファイルを実行する手順は次のとおりです。

注意： サイレント・モードは新規インストールのみが対象です。移行やアップグレードでは使用できません。

新しいコンポーネントをサイレント・モードでインストールする手順

1. 元のオプション・ファイルのコピーを作成します（まだ作成していない場合）。
2. 次のオプションを使用してコマンド・プロンプトからインストールを実行します。

   ```
   -options path_to_install_options.txt -silent
   ```

   path_to_install_options.txt はサイレント・モード・オプション・ファイルの場所です。パスにファイル名を含める必要があります。ファイル名は install_options.txt でなくてもかまいません。

注意： インストールのダイアログ・ボックスを表示しない場合は、このコマンドに -is:silent オプションを付けます。

HP-UX および AIX でのインストール・ディレクトリの選択

インストール先として十分な領域のあるディレクトリを指定する場合は、-is:tempdir パス・パラメータを使用できます。パスは、十分な領域のあるファイル・システムの絶対パスとして指定する必要があります。

インストール・パスワードの入力

コマンドラインからパスワードを入力するか、サイレント・モード・オプション・ファイルを編集してパスワードを保存する必要があります。パスワードを指定しないとインストールは失敗します。コマンドラインからパスワードを入力する例を次に示します。

```
installer -is:silent -silent -options path_to_install_options.txt -W
oblixDSinfoBean.dsPassword=Your_Password
```

path_to_install_options.txt は、サイレント・モード・オプション・ファイルの場所です。

サイレント・モード・オプション・ファイルの編集

オプション・ファイルは次の場所にあります。

/*Component_install_dir*/identity|access/oblix/config/install_options.txt

Component_install_dir はこのパスの最上位のディレクトリです。identity|access はコンポーネントのタイプを表します。

このオプション・ファイルをコピーし、環境に合せてコピーを編集する必要があります。次のガイドラインに従ってください。

- パラメータと値は大文字と小文字が区別されます。
- すべての値は引用符で囲みます。

次の例を参照してください。

- サンプル・オプション・ファイル
- Access Server のサンプル・オプション・ファイル

サンプル・オプション・ファイル

Identity Server のオプション・ファイルの例を例 15-5 に示します。

注意： デフォルトでは、サイレント・モード・オプション・ファイルが最初に作成されたとき、パスワード・フィールドはコメント化されており、パスワードは指定されていません。パスワードを入力する場合はパスワード・フィールドを編集します。# を削除して正しいパスワードを入力します。

Access Server のサンプル・オプション・ファイル

次にいくつかの例を示します。

- サンプル : 同じディレクトリ・サーバー
- サンプル : 別のディレクトリ・サーバー
- サンプル : 別のディレクトリ・サーバー（ユーザー・データが SSL 対応）
- サンプル : 別のディレクトリ・サーバー（ポリシーは SSL 対応）

サンプル : 同じディレクトリ・サーバー

Access Server のオプション・ファイルの例を例 15-1 に示します。この例では、構成データとポリシー・データが同じディレクトリ・サーバーに格納されます。

例 15-1 Access Server のオプション・ファイル（同じディレクトリ・サーバー）

```
Log file for this installation is located at C:¥DOC¥AMIT¥LOCAL¥Temp/aaa.log
-P aaa.installLocation="C:¥OracleAccessManager¥oblix¥access"
-W securityModeBean.securityModeChoices="open"
# The following are recommended to be entered as command line arguments.
-W oblixDSInfoBean.dsType="NCSP10"
-W oblixDSInfoBean.dsMode="open"
-W oblixDSInfoBean.dsHostMachine="marinello"
-W oblixDSInfoBean.dsPortNumber="999"
-W oblixDSInfoBean.dsBindDN="cn=administrator"
# The following are recommended to be entered as command line arguments.
-W oblixDSInfoBean.dsPassword="mypassword"
-W policyDataInWhichDSBean.askPolicyDataInWhichDS="OBLIX"
W aaaInfoBean.accessServerID="aaa"
-W aaaInfoBean.policyDataConfigDN="o=company,c=us"
-W aaaInfoBean.policyDSBase="o=company,c=us"
```

サンプル : 別のディレクトリ・サーバー

Access Server オプション・ファイルのこの例では、構成データとポリシー・データが別のディレクトリ・サーバーに格納されます。例 15-2 を参照してください。

例 15-2 Access Server のオプション・ファイル（構成データとポリシー・データが別のディレクトリ）

```
# Log file for this installation is located at C:¥DOC¥AMIT¥LOCAL¥Temp/aaa.log
-P aaa.installLocation="C:¥OracleAccessManager¥oblix¥access"
-W securityModeBean.securityModeChoices="open"
# The following are recommended to be entered as command line arguments.
-W oblixDSInfoBean.dsType="NCSP10"
-W oblixDSInfoBean.dsMode="open"
-W oblixDSInfoBean.dsHostMachine="marinello"
-W oblixDSInfoBean.dsPortNumber="999"
-W oblixDSInfoBean.dsBindDN="cn=administrator"
# The following are recommended to be entered as command line arguments.
-W oblixDSInfoBean.dsPassword="mypassword"
-W policyDataInWhichDSBean.askPolicyDataInWhichDS="POLICY"
-W policyDSInfoBean.dsMode="open"
```

```
-W policyDSInfoBean.dsHostMachine="marinello"
-W policyDSInfoBean.dsPortNumber="999"
-W policyDSInfoBean.dsBindDN="cn=administrator"
# The following are recommended to be entered as command line arguments.
-W policyDSInfoBean.dsPassword="mypassword"
-W aaaInfoBean.accessServerID="aaa"
-W aaaInfoBean.policyDataConfigDN="o=company,c=us"
-W aaaInfoBean.policyDSBase=o=company,c=us"
```

サンプル : 別のディレクトリ・サーバー（ユーザー・データが SSL 対応）

Access Server オプション・ファイルのこの例（例 15-3）では、構成データとポリシー・データが別のディレクトリ・サーバーに格納されます。また、ユーザーのディレクトリ・サーバーは SSL モードで作動しています。

例 15-3 Access Server のオプション・ファイル（別のディレクトリ・サーバー、SSL 対応）

```
# Log file for this installation is located at C:¥DOC¥AMIT¥LOCAL¥Temp/aaa.log
-P aaa.installLocation="C:¥OracleAccessManager¥oblix¥access"
-W securityModeBean.securityModeChoices="open"
# The following are recommended to be entered as command line arguments
-W oblixDSInfoBean.dsType="NCSP10"
-W oblixDSInfoBean.dsMode="open"
-W oblixDSInfoBean.dsHostMachine="marinello"
-W oblixDSInfoBean.dsPortNumber="999"
-W oblixDSInfoBean.dsBindDN="cn=administrator"
# The following are recommended to be entered as command line arguments.
-W oblixDSInfoBean.dsPassword="mypassword"
-W policyDataInWhichDSBean.askPolicyDataInWhichDS="POLICY"
-W policyDSInfoBean.dsMode="open"
-W policyDSInfoBean.dsHostMachine="marinello"
-W oblixDSInfoBean.dsPortNumber="999"
-W policyDSInfoBean.dsBindDN="cn=administrator"
# The following are recommended to be entered as command line arguments.
-W policyDSInfoBean.dsPassword="mypassword"
-W aaaInfoBean.accessServerID="aaa"
-W aaaInfoBean.policyDataConfigDN="o=company,c=us"
-W aaaInfoBean.policyDSBase=o=company,c=us"
-W userDSSSLCertPath.sslCertPath="C:¥Cert¥ca.cert"
```

サンプル : 別のディレクトリ・サーバー（ポリシーは SSL 対応）

Access Server オプション・ファイルのこの例（例 15-4）では、構成データとポリシー・データが別のディレクトリ・サーバーに格納されます。また、ポリシーのディレクトリ・サーバーは SSL モードで作動しています。

例 15-4 Access Server のオプション・ファイル（構成データとポリシー・データが別、SSL 対応）

```
# Log file for this installation is located at C:¥DOC¥AMIT¥LOCAL¥Temp/aaa.log
-P aaa.installLocation="C:¥OracleAccessManager¥oblix¥access"
-W securityModeBean.securityModeChoices="open"
# The following are recommended to be entered as command line arguments
-W oblixDSInfoBean.dsType="NCSP10"
-W oblixDSInfoBean.dsMode="open"
-W oblixDSInfoBean.dsHostMachine="marinello"
-W oblixDSInfoBean.dsPortNumber="999"
-W oblixDSInfoBean.dsBindDN="cn=administrator"
# The following are recommended to be entered as command line arguments.
-W oblixDSInfoBean.dsPassword="mypassword"
-W policyDataInWhichDSBean.askPolicyDataInWhichDS="POLICY"
-W policyDSInfoBean.dsMode="ssl"
-W policyDSInfoBean.dsHostMachine="marinello"
-W policyDSInfoBean.dsPortNumber="333"
-W policyDSInfoBean.dsBindDN="cn=administrator"
```

```
# The following are recommended to be entered as command line arguments.
-W policyDSInfoBean.dsPassword="mypassword"
-W userDSSSLCertPath.sslCertPath="C:¥Cert¥ca.cert"
-W aaaInfoBean.accessServerID="aaa"
-W aaaInfoBean.policyDataConfigDN="o=company,c=us"
-W aaaInfoBean.policyDSBase=o=company,c=us"
```

サンプル : Active Directory を使用する Identity Server のインストール

Identity Server オプション・ファイルのこの例（例 15-5）では、インストールは Active Directory に対して行われます。

例 15-5 Active Directory を使用する Identity Server のインストール・オプション・ファイル

```
# Log file for this installation is located at
C:¥DOCUME~1¥ADMINI~1¥Temp¥OracleAccessManager.log
-P ois.installLocation="D:¥test¥adsi¥ois¥identity"
-W secruityModeBean.securityModeChoices="open"
-WoisInfoBean.hostName="test001"
-W oisInfoBean.serverID="test002"
-W oisInfoBean.portNumber="9002"
-W askFirstIdentityServer.askFirstIdentityServerField="n"
-W askSSLSetup.askSSLSetupField="No"
-W askADSI.isADSI="yes"
-W askUseImplicitBind.useImplicitBind="yes"
-W askNTServiceName.netServiceNameField="testcoreidad"
-W askNTServiceAccount.ntServiceUserAccount=".¥Administrator"
# The following is recommended to be entered as a command line argument
# -W askNTServiceAccount.netServiceUserPassword=<your password>
```

サイレント・モード・パラメータ

次に、コンポーネントごとに、サイレント・インストール・オプション・ファイルで編集できるオプションについて説明します。< と > で囲まれているのはユーザーがパラメータに指定する値です。ファイルでは各パラメータに値を指定する必要があります。すべての値は二重引用符で囲みます。

インストール・プロンプトとそれに対応する値の詳細は、このインストール・ガイドの該当する章を参照してください。たとえば、Identity Server のインストール・プロンプトと値の詳細は、第 4 章「Identity Server のインストール」を参照してください。

この後の項と同じ順序で Oracle Access Manager コンポーネントをインストールすることをお薦めします。パラメータは、インストール GUI に表示されるのと同じ順序で示しています。

注意 : コンポーネントをインストールするときは、すべてのパラメータを指定する必要はありません。指定する必要があるのは、インストールに適用するパラメータの値のみです。

Identity Server のパラメータ

表 15-1 に、Identity Server のサイレント・インストール・パラメータを示します。

表 15-1 Identity Server のサイレント・インストール・パラメータ

Identity Server のパラメータと説明	指定できる値
-P ois.installLocation: インストール・ディレクトリ。デフォルト・ディレクトリは Windows では "C:¥COREid"、UNIX では "/coreid"。	"< インストール・ディレクトリ >"
-W userInfoBean.user: UNIX 専用。製品の実行に使用されるユーザー ID。	"< ユーザー ID>"
-W userInfoBean.group: UNIX 専用。userInfoBean.user に対応するグループ。	"< グループ ID>"
-W localePanel.defaultLang: メイン・インストールに追加の言語をインストールする場合は必須。	"en-us"
-W localePanel.installLanguages: メイン・インストールに追加の言語をインストールする場合は必須。	"en-us;fr-fr"
-W securityModeBean.securityModeChoices: Identity Server のセキュリティ・モード。値 "open" はセキュリティ不使用、値 "simple" は暗号化使用、値 "cert" は独自の CA の実行を意味する。	"open"、"simple"、"cert"
-W oisInfoBean.hostName: Identity Server がインストールされるホスト名。	"<IP アドレス >" または "< ホスト名 >"
-W oisInfoBean.serverID: Identity Server の ID。ユーザーが作成する一意の ID。	"< サーバー ID>"
-W oisInfoBean.portNumber: Identity Server のポート番号。同じマシンの別のインスタンスはこのポート番号を使用できない。	"< ポート番号 >"
-W askFirstIdentityServer.askFirstIdentityServerField: このパラメータは、これが最初にインストールされる Identity Server かどうかを指定する。値 "y"（yes）は最初にインストールされる Identity Server であることを意味し、"n"（no）はそうではないことを意味する。	"y" または "n"
-W askSSLSetup.askSSLSetupField: このパラメータは、Identity Server とディレクトリ・サーバーの間に SSL を設定するかどうかを指定する。	"Yes" または "No"
-W askSSLSetup.askUserSSLSetupField: このパラメータは、Identity Server と、ユーザー・データを含むディレクトリ・サーバーの間に SSL を設定するかどうかを指定する。	"Yes" または "No"
-W askSSLSetup.askOblixSSLSetupField: このパラメータは、Identity Server と、Oracle Access Manager 構成データを含むディレクトリ・サーバーの間に SSL を設定するかどうかを指定する。	"Yes" または "No"
-W askUserSSLCertPath.sslCertPath: SSL 証明書の絶対パス。"askSSLSetup.askUserSSLSetupField" = "Yes" の場合のみ使用。	"< ファイル名を含む絶対パス >"
-W askOblixSSLCertPath.sslCertPath: SSL 証明書の絶対パス。"askSSLSetup.askOblixSSLSetupField" = "Yes" の場合のみ使用。	"< ファイル名を含む絶対パス >"
-W simpleModeBean.passphrase: このパラメータは、シンプル・トランスポート・セキュリティ・モードを使用している場合に使用される。Identity Server が WebPass と通信するためのパスフレーズ。"securityModeBean.securityModeChoices" = "simple" の場合のみ使用。	"< パスフレーズ >"
-W simpleModeBean.passphraseVerify: このパラメータは、シンプル・トランスポート・セキュリティ・モードを使用している場合に使用される。このパラメータは、パスフレーズが simpleModeBean.passphrase のパスフレーズと一致することを確認する。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< パスフレーズ >"

表 15-1 Identity Server のサイレント・インストール・パラメータ（続き）

Identity Server のパラメータと説明	指定できる値
-W certModeBean.passphrase: このパラメータは、証明書トランスポート・セキュリティ・モードを使用している場合に使用される。Identity Server が WebPass と通信するためのパスフレーズ。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< パスフレーズ >"
-W certModeBean.passphraseVerify: このパラメータは、証明書トランスポート・セキュリティ・モードを使用している場合に使用される。このパラメータは、パスフレーズが certModeBean.passphrase のパスフレーズと一致することを確認する。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< パスフレーズ >"
-W installOrRequestCertBean.installOrRequest: ID システムの構成に使用する証明書をインストールするかリクエストするかを決定する。セキュリティ・モードが "cert" に設定されている場合のみ使用。すでに証明書がある場合は "install" を使用する。Oracle Access Manager で証明書をリクエストする場合は "request" を使用する。	"request" または "install"
-W certReqInfoBean.countryName: 国名。DN で有効な 2 文字の国コード。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 国コード >"
-W certReqInfoBean.stateOrProvinceName: 都道府県名。2 文字の都道府県コード。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 都道府県コード >"
-W certReqInfoBean.localityName: 市町村名。市町村名を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 市町村名 >"
-W certReqInfoBean.organizationName: 組織名。通常、組織名を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 組織名 >"
-W certReqInfoBean.organizationalUnitName: 組織単位名。通常、部門名を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 組織単位名 >"
-W certReqInfoBean.commonName: 共通名。通常、人またはエンティティの名前を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 名前 >"
-W certReqInfoBean.emailAddress: 電子メール・アドレス。通常、有効な電子メール・アドレスを指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 電子メール・アドレス >"
-W readyToInstallCertBean.readyToInstallField: Oracle Access Manager で証明書をリクエストするように指定した場合、このパラメータによって、インストールのために証明書の準備ができたことが確認される。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。サイレント・モードでは値 "No" の使用を推奨する。Oracle Access Manager インストール・スクリプトが 1 つの手順から次の手順に進むよりも早く、Oracle Access Manager で生成されたリクエストをユーザーが取得して、証明書を受信することは難しいため。	"Yes" または "No"
-W copyCertificatesInputBean.certFile: 証明書は、証明書ファイル、鍵ファイル、連鎖ファイルの 3 ファイルで構成される。このパラメータは、証明書ファイルのファイル名（ois_cert.pem など）を含む絶対パスを指定する。次の場合に使用。 installOrRequestCertBean.installOrRequest = "install" の場合、または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"

表 15-1 Identity Server のサイレント・インストール・パラメータ（続き）

Identity Server のパラメータと説明	指定できる値
-W copyCertificatesInputBean.keyFile: 証明書は、証明書ファイル、鍵ファイル、連鎖ファイルの 3 ファイルで構成される。このパラメータは、鍵ファイルのファイル名（ois_key.pem など）を含む絶対パスを指定する。次の場合に使用。 installOrRequestCertBean.installOrRequest = "install" の場合、または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"
-W copyCertificatesInputBean.chainFile: 証明書は、証明書ファイル、鍵ファイル、連鎖ファイルの 3 ファイルで構成される。このパラメータは、連鎖ファイルのファイル名（ois_chain.pem など）を含む絶対パスを指定する。次の場合に使用。installOrRequestCertBean.installOrRequest = "install" の場合、または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"
-W updateDSInfo.updateDSInfoChoice: 構成スキーマとユーザー・スキーマを自動的に更新するかどうかを決定する。askFirstIdentityServer.askFirstIdentityServeField= "y" の場合のみ使用。 "YesOneDS" の場合、自動更新が実行される。構成とユーザーのディレクトリ・サーバーは同じ。 "YesTwoDS" の場合、自動更新が実行される。構成とユーザーのディレクトリ・サーバーは異なる。 "No" の場合、自動更新は実行されない。	"YesOneDS"、"YesTwoDS"、"No"
-W AutoUpdateInput.AutoUpdateInputChoice: 構成データがユーザー・データと同じディレクトリに格納されているときに、スキーマを自動的に更新するかどうかを決定する。	"Yes" または "No"
-W OblixDSAutoUpdateInput.AutoUpdateInputChoice: 構成データがユーザー・データとは異なるディレクトリに格納されているときに、スキーマを自動的に更新するかどうかを決定する。	"Yes" または "No"

表 15-1 Identity Server のサイレント・インストール・パラメータ（続き）

Identity Server のパラメータと説明	指定できる値
-W dsTypeInput.dsType: Oracle Access Manager が構成スキーマとユーザー・スキーマを自動的に更新する場合（つまり、updateDSInfo.updateDSInfoChoice が "YesOneDS" または "YesTwoDS" の場合）にこのパラメータを使用。ユーザー・ディレクトリ・サーバーのタイプ： 1: Sun Directory Server 5.x 2: NDS 3: Active Directory 4: ADSI（スキーマは LDAP を使用してアップロードされる） 5: Active Directory（Windows Server 2003） 6: ADSI（Windows Server 2003） 7: Active Directory アプリケーション・モード（Windows 2003 のみ） 8: Siemens DirX（**10*g***（10.1.4.0.1）**ではサポート外）** 9: IBM ディレクトリ・サーバー 10: Data Anywhere 11: Oracle Internet Directory **注意：** Data Anywhere はユーザー・データに対してのみ使用できますが、第 10 章「Oracle Virtual Directory を使用した Oracle Access Manager の設定」の説明に従って Oracle Virtual Directory Server（VDS）と統合する必要があります。構成（およびポリシー）データを含む LDAP ディレクトリ・ブランチは、VDS またはユーザー・データのホストであるディレクトリ・サーバーとは別の 1 つ以上のディレクトリ・サーバーに存在する必要があります。 **その他の注意：** ユーザー・データのディレクトリ・サーバー・タイプと構成データのディレクトリ・サーバー・タイプが異なる場合は、構成データのディレクトリ・サーバー・タイプを指定するために -W dsTypeInput1.dsType=# を使用してください。	"1"、"2"、"3"、"4"、"5"、"6"、"7"、"9"、"10"、"11"
-W dsTypeInput1.dsType: 前の説明の**「その他の注意」**を参照。	
-W dsUserDynAuxClassInput.dynamicAuxiliary: Active Directory で動的補助クラスをサポートする場合はこのパラメータを "y" に設定する。-W dsTypeInput.dsType を "5" または "7" に設定した場合のみ使用。	"y" または "n"
-W dsInfoInput.dsName: ほとんどのディレクトリ・タイプでは、ユーザー・ディレクトリ・サーバーのホスト名。Active Directory では、スキーマ・マスターのホスト名を使用。updateDSInfo.updateDSInfoChoice が "YesOneDS" または "YesTwoDS" の場合のみ使用。	"<IP アドレス >" または "< ホスト名 >"
-W dsInfoInput.dsName: ほとんどのディレクトリ・タイプでは、ユーザー・ディレクトリ・サーバーのホスト名。Active Directory では、スキーマ・マスターのホスト名を使用。updateDSInfo.updateDSInfoChoice が "YesOneDS" または "YesTwoDS" の場合のみ使用。	"<IP アドレス >" または "< ホスト名 >"
-W dsInfoInput.dsPortNumber: ほとんどのディレクトリ・タイプでは、ユーザー・ディレクトリ・サーバーのポート番号。Active Directory では、スキーマ・マスターのポート番号を使用。updateDSInfo.updateDSInfoChoice が "YesOneDS" または "YesTwoDS" の場合のみ使用。	"< ポート番号 >"

表 15-1 Identity Server のサイレント・インストール・パラメータ（続き）

Identity Server のパラメータと説明	指定できる値
-W dsInfoInput.bindDN: ほとんどのディレクトリ・タイプでは、ユーザー・ディレクトリ・サーバーに対する認証に使用される DN。Active Directory では、スキーマ・マスターのバインド DN を使用。updateDSInfo.updateDSInfoChoice が "YesOneDS" または "YesTwoDS" の場合のみ使用。この値は有効な DN 構文を使用して入力する。"cn=User Directory, o=Oblix" など。	"< バインド DN>"
-W dsInfoInput.password: ほとんどのディレクトリ・タイプでは、ユーザー・ディレクトリ・サーバーのパスワード。Active Directory では、スキーマ・マスターのパスワードを使用。updateDSInfo.updateDSInfoChoice が "YesOneDS" または "YesTwoDS" の場合のみ使用。セキュアなパスワード入力の詳細は、15-3 ページの「サイレント・モード・オプション・ファイルの実行」の説明を参照。	"< パスワード >"
-W OblixdsInfoInput.dsName: 構成ディレクトリ・サーバーの名前。構成とユーザーのディレクトリ・サーバーが別で、NDS または Active Directory を使用しない場合のみ使用。具体的には次の場合。 updateDSInfo.updateDSInfoChoice = "YesTwoDS" で、dsTypeInput1.dsType が "2" または "3" でない。	
-W OblixdsInfoInput.dsPortNumber: 構成ディレクトリ・サーバーのポート番号。構成とユーザーのディレクトリ・サーバーが別で、NDS または Active Directory を使用しない場合のみ使用。具体的には次の場合。 updateDSInfo.updateDSInfoChoice = "YesTwoDS" で、dsTypeInput1.dsType が "2" または "3" でない。	"< ポート番号 >"
-W OblixdsInfoInput.bindDN: 構成ディレクトリ・サーバーに対する認証に使用される DN。構成とユーザー・データのディレクトリ・サーバーが別で、NDS または Active Directory を使用しない場合のみ使用。具体的には次の場合。 updateDSInfo.updateDSInfoChoice = "YesTwoDS" で、dsTypeInput1.dsType が "2" または "3" でない。 この値は有効な DN 構文を使用して入力する。"cn=Configuration Directory, o=Oblix" など。	"< バインド DN>"
-W OblixdsInfoInput.password: 構成ディレクトリ・サーバーのパスワード。構成とユーザーのディレクトリ・サーバーが別で、NDS または Active Directory を使用しない場合のみ使用。具体的には次の場合。 updateDSInfo.updateDSInfoChoice = "YesTwoDS" で、dsTypeInput1.dsType が "2" または "3" でない。	"< パスワード >"
-W askNTServiceName.ntServiceNameField: Windows 専用。Identity Server のサービス名。この名前はサービス・コントロール・パネルに表示される。	"< 名前 >"
-W askADSI.isADSI: Active Directory を ADSI と一緒に使用しているかどうかを確認する。	"yes"、"no"
-W askADSISSL.isADSISSL: SSL を使用して Active Directory を ADSI と一緒に実行しているかどうかを確認する。	"yes"、"no"
-W askSeparateADDomain.isSeparateDomain: この Identity Server インスタンスをインストールしているマシンが、ターゲットの Active Directory Forest（Oracle Access Manager が使用するように構成されている）とは異なるフォレストにあるかどうかを指定する。	"yes"、"no"
-W askUseImplicitBind.useImplicitBind: インストール・マシンが同じドメインにある場合に、サービス・アカウント資格証明を使用して Active Directory にアクセスするかどうか。"yes" の場合は、adsi_params.xml ファイルにパラメータ useImplicitBind が設定される。	"yes"、"no"

表 15-1 Identity Server のサイレント・インストール・パラメータ（続き）

Identity Server のパラメータと説明	指定できる値
-W askNTServiceAccount.ntServiceUserAccount: askUseImplicitBind の値を "yes" に設定した場合は、このアカウントでサービスが実行される。".¥Administrator" など。	"< アカウント ID>"
-W askNTServiceAccount.ntServiceUserPassword: askUseImplicitBind の値を "yes" に設定した場合は、サービス・アカウントのパスワード。この値はコマンドラインでの指定を推奨する。	"< パスワード >"

WebPass のパラメータ

表 15-2 に、WebPass のサイレント・インストール・パラメータを示します。

表 15-2 WebPass のサイレント・インストール・パラメータ

WebPass のパラメータと説明	指定できる値
-P webpass.installLocation: インストール・ディレクトリ。デフォルト・ディレクトリは Windows では "C:¥COREid¥WebComponent"、UNIX では "/coreid/webcomponent"。	"< インストール・ディレクトリ >"
-W userInfoBean.user: UNIX 専用。製品の実行に使用されるユーザー ID。	"< ユーザー ID>"
-W userInfoBean.group: UNIX 専用。userInfoBean.user に対応するグループ。	"< グループ ID>"
-W localePanel.defaultLang: メイン・インストールに追加の言語をインストールする場合は必須。	"en-us"
-W localePanel.installLanguages: メイン・インストールに追加の言語をインストールする場合は必須。	"en-us;fr-fr"
-W securityModeBean.securityModeChoices: Identity Server のセキュリティ・モード。値 "open" はセキュリティ不使用、値 "simple" は暗号化使用、値 "cert" は独自の CA の実行を意味する。	"open"、"simple"、"cert"
-W webpassInfoBean.hostName: Identity Server のホスト名。	"<IP アドレス >" または "< ホスト名 >"
-W webpassInfoBean.webpassID: WebPass の ID。インストール時にユーザーが指定する一意の ID。	"<ID>"
-W webpassInfoBean.portNumber: Identity Server のポート番号。	"< ポート番号 >"
-W simpleModeBean.passphrase: Identity Server が WebPass と通信するためのパスフレーズ。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< パスフレーズ >"
-W simpleModeBean.passphraseVerify: Identity Server が WebPass と通信するためのパスフレーズ。このパラメータは、パスフレーズが certModeBean.passphrase のパスフレーズと一致することを確認するために使用される。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< パスフレーズ >"
-W certModeBean.passphrase: Identity Server が WebPass と通信するためのパスフレーズ。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< パスフレーズ >"
-W certModeBean.passphraseVerify: Identity Server が WebPass と通信するためのパスフレーズ。このパラメータは、パスフレーズが certModeBean.passphrase のパスフレーズと一致することを確認する。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< パスフレーズ >"

表 15-2 WebPass のサイレント・インストール・パラメータ（続き）

WebPass のパラメータと説明	指定できる値
-W installOrRequestCertBean.installOrRequest: ID システムの構成に使用する証明書をインストールするかリクエストするかを決定する。セキュリティ・モードが "cert" に設定されている場合のみ使用。すでに証明書をリクエストしている場合は "install" を選択する。CA に提出できる証明書を Oracle Access Manager でリクエストする場合は "request" を選択する。	"install" または "request"
-W certReqInfoBean.countryName: 国名。DN で有効な 2 文字の国コード。証明書をリクエストするために Oracle Access Manager が使用する情報の一部。Oracle Access Manager による証明書のリクエストを選択した場合（つまり、installOrRequestCertBean.installOrRequest = "request" の場合）にこのパラメータを使用。	"< 国コード >"
-W certReqInfoBean.stateOrProvinceName: 都道府県名。DN で有効な 2 文字の都道府県コード。証明書をリクエストするために Oracle Access Manager が使用する情報の一部。Oracle Access Manager による証明書のリクエストを選択した場合（つまり、installOrRequestCertBean.installOrRequest = "request" の場合）に使用。	"< 都道府県コード >"
-W certReqInfoBean.localityName: 市町村名。証明書をリクエストするために Oracle Access Manager が使用する情報の一部。Oracle Access Manager による証明書のリクエストを選択した場合（つまり、installOrRequestCertBean.installOrRequest = "request" の場合）に使用。	"< 市町村名 >"
-W certReqInfoBean.organizationName: 組織名。通常、組織名を指定する。証明書をリクエストするために Oracle Access Manager が使用する情報の一部。Oracle Access Manager による証明書のリクエストを選択した場合（つまり、installOrRequestCertBean.installOrRequest = "request" の場合）に使用。	"< 組織名 >"
-W certReqInfoBean.organizationalUnitName: 組織単位名。通常、部門名を指定する。証明書をリクエストするために Oracle Access Manager が使用する情報の一部。Oracle Access Manager による証明書のリクエストを選択した場合（つまり、installOrRequestCertBean.installOrRequest = "request" の場合）に使用。	"< 組織単位名 >"
-W certReqInfoBean.commonName: 共通名。通常、人またはエンティティの名前を指定する。証明書をリクエストするために Oracle Access Manager が使用する情報の一部。Oracle Access Manager による証明書のリクエストを選択した場合（つまり、installOrRequestCertBean.installOrRequest = "request" の場合）に使用。	"< 名前 >"
-W certReqInfoBean.emailAddress: 電子メール・アドレス。通常、有効な電子メール・アドレスを指定する。証明書をリクエストするために Oracle Access Manager が使用する情報の一部。Oracle Access Manager による証明書のリクエストを選択した場合（つまり、installOrRequestCertBean.installOrRequest = "request" の場合）に使用。	"< 電子メール・アドレス >"
-W readyToInstallCertBean.readyToInstallField: Oracle Access Manager が証明書をリクエストするように指定した場合、このパラメータによって、インストールのために証明書の準備ができたことが確認される。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。サイレント・モードでは "Yes" を使用しないことを推奨する。Oracle Access Manager インストールが 1 つの手順から次の手順に進むよりも早く、Oracle Access Manager で生成されたリクエストをユーザーが取得して、証明書を受信することは難しいため。	"Yes" または "No"

表 15-2 WebPass のサイレント・インストール・パラメータ（続き）

WebPass のパラメータと説明	指定できる値
-W copyCertificatesInputBean.certFile: 証明書は、証明書ファイル、鍵ファイル、連鎖ファイルの 3 ファイルで構成される。このパラメータは、証明書ファイルのファイル名（ois_cert.pem など）を含む絶対パスを指定する。次の場合に使用。installOrRequestCertBean.installOrRequest = "install" の場合、または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"
-W copyCertificatesInputBean.keyFile: 証明書は、証明書ファイル、鍵ファイル、連鎖ファイルの 3 ファイルで構成される。このパラメータは、鍵ファイルのファイル名（ois_key.pem など）を含む絶対パスを指定する。次の場合に使用。installOrRequestCertBean.installOrRequest = "install" の場合、または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"
-W copyCertificatesInputBean.chainFile: 証明書は、証明書ファイル、鍵ファイル、連鎖ファイルの 3 ファイルで構成される。このパラメータは、連鎖ファイルのファイル名（ois_chain.pem など）を含む絶対パスを指定する。次の場合に使用。installOrRequestCertBean.installOrRequest = "install" の場合、または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"
-W askAutoUpdateWSBean.askAutoUpdateWSField: Web サーバーの構成を自動的に更新するかどうかを決定する。	"Yes" または "No"
-W askConfFilePathBean.askConfFilePathField: NSAPI の場合、obj.conf を含む Web サーバーの構成ディレクトリの絶対パス（たとえば、/export/Sun/servers/https-oblix/config）。Apache および Apache SSL の場合は、Web サーバーの構成ディレクトリ内の httpd.conf の絶対パス（たとえば、/export/apache/conf/httpd.conf）。Apache、Apache SSL および NSAPI Web サーバーに対して、askAutoUpdateWSBean.askAutoUpdateWSField = "Yes" の場合のみ使用。	"< 絶対パス（Apache のためのファイル名を含む）>"
-W askLaunchBrowserBean.launchBrowser: ブラウザを起動して、Web サーバー構成の手動更新の手順を表示するかどうかを決定する。UNIX にインストールするときに、askAutoUpdateWSBean.askAutoUpdateWSField = "No" の場合のみ使用。	"Yes" または "No"

Policy Manager のパラメータ

表 15-3 に、Policy Manager のサイレント・インストール・パラメータを示します。

表 15-3 Policy Manager のサイレント・インストール・パラメータ

Policy Manager のパラメータと説明	指定できる値
-P manager.installLocation: インストール・ディレクトリ。デフォルト・ディレクトリは Windows では "C:¥COREid"、UNIX では "/coreid"。	"< インストール・ディレクトリ >"
-W userInfoBean.user: UNIX 専用。製品の実行に使用されるユーザー ID。任意の有効なユーザー ID を指定できる。	"< ユーザー ID>"
-W userInfoBean.group: UNIX 専用。userInfoBean.user に対応するグループ。	"< グループ名 >"
-W localePanel.defaultLang: メイン・インストールに追加の言語をインストールする場合は必須。	"en-us"

表 15-3 Policy Manager のサイレント・インストール・パラメータ（続き）

Policy Manager のパラメータと説明	指定できる値
-W localePanel.installLanguages: メイン・インストールに追加の言語をインストールする場合は必須。	"en-us;fr-fr"
-W updateDSInfo.updateDSInfoChoice: Oracle Access Manager がポリシー・スキーマを自動的に更新するかどうかを決定する。ポリシー・ディレクトリ・サーバーが構成データ・ディレクトリ・サーバーと同じで、ユーザー・ディレクトリ・サーバーとは異なる場合に使用。	"Yes" または "No"
-W dsTypeInput.dsType: ポリシー・ディレクトリ・サーバーが構成サーバーと同じだがユーザー・ディレクトリ・サーバーと異なる（updateDSInfo.updateDSInfoChoice = "Yes"）場合は、ポリシー・ディレクトリ・サーバーのタイプを次のいずれかに指定する必要がある。 1: Sun Directory Server 5.x 2: NDS 3: Active Directory 5: Active Directory（Windows Server 2003） 7: Active Directory アプリケーション・モード（Windows 2003 のみ） 8: Siemens DirX**（10*g*（10.1.4.0.1）ではサポート外）** 9: IBM ディレクトリ・サーバー 10: Oracle Internet Directory	"1"、"2"、"3"、"4"、"5"、"6"、"7"、"9"、"10"
-W dsInfoInput.dsName: ポリシー・ディレクトリ・サーバーの名前。ポリシー・ディレクトリ・サーバーが構成データ・サーバーと同じだが、ユーザー・ディレクトリ・サーバーとは異なり、NDS または Active Directory を使用していない場合に使用。 updateDSInfo.updateDSInfoChoice = "Yes" で、dsTypeInput.dsType が "2" または "3" でない。	"<IP アドレス >" または "< ホスト名 >"
-W dsInfoInput.dsPortNumber: ポリシー・ディレクトリ・サーバーのポート番号。ポリシー・ディレクトリ・サーバーが構成データ・ディレクトリ・サーバーと同じだが、ユーザー・ディレクトリ・サーバーとは異なり、NDS または Active Directory を使用していない場合に使用。 updateDSInfo.updateDSInfoChoice = "Yes" で、dsTypeInput.dsType が "2" または "3" でない。	"< ポート >"
-W dsInfoInput.bindDN: ポリシー・ディレクトリ・サーバーに対する認証に使用される DN。ポリシー・ディレクトリ・サーバーが構成データ・ディレクトリ・サーバーと同じだが、ユーザー・ディレクトリ・サーバーとは異なり、NDS または Active Directory を使用していない場合に使用。 updateDSInfo.updateDSInfoChoice = "Yes" で、dsTypeInput.dsType が "2" または "3" でない。 このエントリには従来の DN 構文を使用する。"cn=Policy Directory, o=Oblix" など。	"< バインド DN>"
-W dsInfoInput.password: ポリシー・ディレクトリ・サーバーのパスワード。ポリシー・ディレクトリ・サーバーが構成データ・ディレクトリ・サーバーと同じだが、ユーザー・ディレクトリ・サーバーとは異なり、NDS または Active Directory を使用していない場合に使用。 updateDSInfo.updateDSInfoChoice = "Yes" で、dsTypeInput.dsType が "2" または "3" でない。	"< パスワード >"

表 15-3 Policy Manager のサイレント・インストール・パラメータ（続き）

Policy Manager のパラメータと説明	指定できる値
-W dsInfoInput.dsSSLConnect: ポリシー・ディレクトリ・サーバーが SSL 接続を使用するかどうかを決定する。ポリシー・ディレクトリ・サーバーが構成データ・ディレクトリ・サーバーと同じだが、ユーザー・ディレクトリ・サーバーとは異なり、NDS または Active Directory を使用していない場合に使用。 updateDSInfo.updateDSInfoChoice = "Yes" で、dsTypeInput.dsType が "2" または "3" でない。	"Yes" または "No"
-W askSSLCertPath.askSSLCertificatePathField: SSL 証明書の絶対パス。ポリシー・ディレクトリ・サーバーが構成データ・ディレクトリ・サーバーと同じだが、ユーザー・ディレクトリ・サーバーとは異なり、NDS または Active Directory を使用していない場合に使用。 updateDSInfo.updateDSInfoChoice = "Yes" で、dsTypeInput.dsType が "2" または "3" ではなく、dsInfoInput.dsSSLConnect = "Yes"。	"< ファイル名を含む絶対パス >"
-W askAutoUpdateWSBean.askAutoUpdateWSField: Web サーバーの構成を自動的に更新するかどうかを決定する。	"Yes" または "No"
-W askConfFilePathBean.askConfFilePathField: NSAPI の場合、obj.conf を含む Web サーバーの config ディレクトリの絶対パス（たとえば、/export/Sun/servers/https-oblix/config）。Apache および Apache SSL の場合は、Web サーバーの構成ディレクトリ内の httpd.conf の絶対パス（たとえば、/export/apache/conf/httpd.conf）。 Apache、Apache SSL および NSAPI Web サーバーに対して、askAutoUpdateWSBean.askAutoUpdateWSField = "Yes" の場合のみ使用。	"< 絶対パス（Apache のためのファイル名を含む）>"
-W askLaunchBrowserBean.launchBrowser: ブラウザを起動して、Web サーバー構成の手動更新の手順を表示するかどうかを決定する。UNIX に対して、askAutoUpdateWSBean.askAutoUpdateWSField = "No" の場合のみ使用。	"Yes" または "No"
-W askADSI.isADSI: Active Directory を ADSI と一緒に実行しているかどうかを確認する。	"yes"、"no"
-W askADSISSL.isADSISSL: SSL を使用して Active Directory を ADSI と一緒に実行しているかどうかを確認する。	"yes"、"no"

Access Server のパラメータ

表 15-4 に、Access Server のサイレント・インストール・パラメータを示します。

表 15-4 Access Server のサイレント・インストール・パラメータ

Access Server のパラメータと説明	指定できる値
-P aaa.installLocation: インストール・ディレクトリ。デフォルト・ディレクトリは Windows では "C:¥COREid"、UNIX では "/coreid"。	"< インストール・ディレクトリ >"
-W userInfoBean.user: UNIX 専用。製品の実行に使用されるユーザー ID。	"< ユーザー ID>"
-W userInfoBean.group: UNIX 専用。userInfoBean.user に対応するグループ。	"< グループ名 >"
-W localePanel.defaultLang: メイン・インストールに追加の言語をインストールする場合は必須。	"en-us"
-W localePanel.installLanguages: メイン・インストールに追加の言語をインストールする場合は必須。	"en-us;fr-fr"

表 15-4 Access Server のサイレント・インストール・パラメータ（続き）

Access Server のパラメータと説明	指定できる値
-W securityModeBean.securityModeChoices: Access Server のセキュリティ・モード。値 "open" はセキュリティ不使用、値 "simple" は暗号化使用、値 "cert" は独自の CA の実行を意味する。	"open"、"simple" または "cert"
- W userDSSSLCerPath.sslCertPath: SSL 証明書の絶対パス。ユーザー・ディレクトリが SSL モードの場合のみ使用。	"< ファイル名を含む絶対パス >"
-W oblixDSInfoBean.dsHostMachine: 構成ディレクトリ・サーバーのホスト・マシン。	"<IP アドレス >" または "< ホスト名 >"
-W oblixDSInfoBean.dsPortNumber: 構成ディレクトリ・サーバーのポート番号。	"< ポート番号 >"
-W oblixDSInfoBean.dsBindDN: 構成ディレクトリ・サーバーに対する認証に使用される DN。	"< バインド DN>"
-W oblixDSInfoBean.dsPassword: 構成ディレクトリ・サーバーのパスワード。	"< パスワード >"
-W oblixDSInfoBean.dsMode: 構成ディレクトリ・サーバーのモード（open または ssl）。	"open" または "ssl"
-W oblixDSInfoBean.dsType: 構成ディレクトリ・サーバーのタイプ。 NS5: Sun Directory Server 5.x NOVELL: NDS MSAD: Microsoft Active Directory MSAD_ADSI: Microsoft Active Directory（ADSI 使用） MSADAM: Active Directory アプリケーション・モード DIRX: Siemens DirX（**10*g***（10.1.4.0.1）**ではサポート外）** IBMSWAY: IBM ディレクトリ・サーバー Oracle Internet Directory	"NS5"、"NOVELL"、"MSAD"、"MSAD_ADSI"、"MSADAM"、"IBMSWAY"、"OID"
-W oblixDSSSLCertPath.sslCertPath: SSL 証明書の絶対パス。oblixDSInfoBean.dsMode = "ssl" の場合のみ使用。	"< ファイル名を含む絶対パス >"
-W policyDataInWhichDSBean.askPolicyDataInWhichDS: ポリシー・ディレクトリ・サーバーがユーザーまたは構成のディレクトリ・サーバーと同じかどうかを決定する。値 "OBLIX" は、ポリシーと構成のディレクトリ・サーバーが同じことを意味する。値 "POLICY" は、ポリシー・ディレクトリ・サーバーがユーザーや構成のディレクトリ・サーバーとは異なることを意味する。	"OBLIX" または "POLICY"
-W policyDSInfoBean.dsHostMachine: ポリシー・ディレクトリ・サーバーのホスト・マシン。ポリシー・ディレクトリ・サーバーが構成サーバーと同じだが、ユーザー・ディレクトリ・サーバーとは異なる場合（policyDataInWhichDSBean.askPolicyDataInWhichDS = "OBLIX"）のみ使用。	"<IP アドレス >" または "< ホスト名 >"
-W policyDSInfoBean.dsPortNumber: ポリシー・ディレクトリ・サーバーのポート番号。ポリシー・ディレクトリ・サーバーが構成サーバーと同じだが、ユーザー・ディレクトリ・サーバーとは異なる場合（policyDataInWhichDSBean.askPolicyDataInWhichDS = "OBLIX"）のみ使用。	"< ポート番号 >"
-W policyDSInfoBean.dsBindDN: ポリシー・ディレクトリ・サーバーに対する認証に使用される DN。ポリシー・ディレクトリ・サーバーがユーザーおよび構成のディレクトリ・サーバーとは異なる場合（policyDataInWhichDSBean.askPolicyDataInWhichDS = "POLICY"）のみ使用。このエントリでは従来の DN 構文を使用する。"cn=Policy Directory, o=Oblix" など。	"< バインド DN>"

表 15-4 Access Server のサイレント・インストール・パラメータ（続き）

Access Server のパラメータと説明	指定できる値
-W policyDSInfoBean.dsPassword: ポリシー・ディレクトリ・サーバーのパスワード。ポリシー・ディレクトリ・サーバーがユーザーおよび構成のディレクトリ・サーバーとは異なる場合（policyDataInWhichDSBean.askPolicyDataInWhichDS = "POLICY"）のみ使用。	"< パスワード >"
-W policyDSInfoBean.dsMode: ポリシー・ディレクトリ・サーバーのモード（open または ssl）。ポリシー・ディレクトリ・サーバーがユーザーおよび構成のディレクトリ・サーバーとは異なる場合（policyDataInWhichDSBean.askPolicyDataInWhichDS = "POLICY"）のみ使用。	"open" または "ssl"
-W policyDSSSLCertPath.sslCertPath: SSL 証明書の絶対パス。ポリシー・ディレクトリ・サーバーが構成サーバーと同じだが、ユーザー・ディレクトリ・サーバーとは異なる場合（policyDataInWhichDSBean.askPolicyDataInWhichDS = "OBLIX"）のみ使用。	"< ファイル名を含む絶対パス >"
-W aaaInfoBean.accessServerID: アクセス・システム・コンソールに登録されている Access Server の ID。この Access Server のアクセス・システム・コンソールに入力した値を指定する。	"< 値 >"
-W aaaInfoBean.policyDataConfigDN: ポリシー・データの構成 DN。このエントリでは従来の DN 構文を使用する。"cn=Policy Data, o=Oblix" など。	"<DN>"
-W aaaInfoBean.policyDSBase: ポリシー・ベース。すなわちポリシー・ディレクトリ内で構成のポリシー関連データが格納されるノード。"cn=Policy Data, o=Oblix" など。	"<DN>"
-W simpleModeInfoBean.passphrase: パスフレーズ。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< パスフレーズ >"
-W simpleModeInfoBean.passphraseVerify: パスフレーズ（確認用）。simpleModeInfoBean.passphrase と同じ値を指定。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< パスフレーズ >"
-W simpleModeInfoBean.storePassPhraseinFile: パスフレーズをファイルに格納するかどうかを決定する。ファイルに格納すると、起動時にユーザーまたはスクリプトによるパスフレーズの指定なしに Access Server を起動可能。	"true" または "false"
-W certModeInfoBean.passphrase: パスフレーズ。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< パスフレーズ >"
-W certModeInfoBean.passphraseVerify: パスフレーズ（確認用）。certModeInfoBean.passphrase と同じ値を指定。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< パスフレーズ >"
-W certModeInfoBean.storePassPhraseinFile: パスワードすなわちパスフレーズをファイルに格納するかどうかを決定する。ファイルに格納すると、起動時にユーザーによるパスフレーズの指定なしに Access Server を起動可能。	"true" または "false"
-W installOrRequestCertBean.installOrRequest: アクセス・システムの構成に使用する証明書をインストールするかリクエストするかを決定する。セキュリティ・モードが "cert" に設定されている場合のみ使用。すでに証明書がある場合は "install" を使用する。Oracle Access Manager で証明書をリクエストする場合は "request" を使用する。	"request" または "install"
-W certReqInfoBean.countryName: 国名。通常、DN で有効な 2 文字の国コード。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 国コード >"

表 15-4 Access Server のサイレント・インストール・パラメータ（続き）

Access Server のパラメータと説明	指定できる値
-W certReqInfoBean.stateOrProvinceName: 都道府県名。通常、DN で有効な 2 文字の都道府県コード。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 都道府県コード >"
-W certReqInfoBean.localityName: 市町村名。市町村名を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 市町村名 >"
-W certReqInfoBean.organizationName: 組織名。通常、組織名を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 組織名 >"
-W certReqInfoBean.organizationalUnitName: 組織単位名。通常、部門名を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 組織名 >"
-W certReqInfoBean.commonName: 共通名。通常、人または別のエンティティの名前を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 名前 >"
-W certReqInfoBean.emailAddress: 電子メール・アドレス。通常、有効な電子メール・アドレスを指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 電子メール・アドレス >"
-W readyToInstallCertBean.readyToInstallField: Oracle Access Manager で証明書をリクエストするように指定した場合、このパラメータによって、インストールのために証明書の準備ができたことが確認される。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。サイレント・モードでは "Yes" を使用しないことを推奨する。Oracle Access Manager インストールが 1 つの手順から次の手順に進むよりも早く、Oracle Access Manager で生成されたリクエストをユーザーが取得して、証明書を受信することは難しいため。	"Yes" または "No"
-W copyCertificatesInputBean.certFile: 証明書ファイルのファイル名（aaa_cert.pem など）を含む絶対パス。次の場合に使用。installOrRequestCertBean.installOrRequest = "install" の場合、または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"
-W copyCertificatesInputBean.keyFile: 鍵ファイルのファイル名（aaa_key.pem など）を含む絶対パス。次の場合に使用。installOrRequestCertBean.installOrRequest = "install" の場合、または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"
-W copyCertificatesInputBean.chainFile: 連鎖ファイルのファイル名（aaa_chain.pem など）を含む絶対パス。次の場合に使用。installOrRequestCertBean.installOrRequest = "install" の場合、または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"
-W askSeparateDomain.isSeparateDomain: この Identity Server インスタンスをインストールしているマシンが、ターゲットの Active Directory Forest（Oracle Access Manager が使用するように構成されている）とは異なるフォレストにあるかどうかを指定する。	"yes"、"no"
-W askUseImplicitBind.useImplicitBind: インストール・マシンが同じドメインにある場合に、サービス・アカウント資格証明を使用して Active Directory にアクセスするかどうか。"yes" の場合は、adsi_params.xml ファイルにパラメータ useImplicitBind が設定される。	"yes"、"no"

表 15-4 Access Server のサイレント・インストール・パラメータ（続き）

Access Server のパラメータと説明	指定できる値
-W askNTServiceAccount.ntServiceUserAcount: askUseImplicitBind の値を "yes" に設定した場合は、このアカウントでサービスが実行される。".¥Administrator" など。	"< アカウント ID>"
-W askNTServiceAccount.ntServiceUserPassword: askUseImplicitBind の値を "yes" に設定した場合は、サービス・アカウントのパスワード。この値はコマンドラインでの指定を推奨する。	"< パスワード >"

WebGate のパラメータ

表 15-5 に、WebGate のサイレント・インストール・パラメータを示します。

表 15-5 WebGate のサイレント・インストール・パラメータ

WebGate のパラメータと説明	指定できる値
-P webgate.installLocation: インストール・ディレクトリ。デフォルト・ディレクトリは Windows では "C:¥COREid¥WebComponent"、UNIX では "/coreid/WebComponent"。	"< インストール・ディレクトリ >"
-W userInfoBean.user: UNIX 専用。製品の実行に使用されるユーザー ID。	"< ユーザー ID>"
-W userInfoBean.group: UNIX 専用。userInfoBean.user に対応するグループ。	"< グループ ID>"
-W localePanel.defaultLang: メイン・インストールに追加の言語をインストールする場合は必須。	"en-us"
-W localePanel.installLanguages: メイン・インストールに追加の言語をインストールする場合は必須。	"en-us;fr-fr"
-W securityModeBean.securityModeChoices: WebGate のセキュリティ・モード。値 "open" はセキュリティ不使用、値 "simple" は暗号化使用、値 "cert" は独自の CA の実行を意味する。	"open"、"simple"、"cert"
-W openModeBean.serverID: Access Server の ID。インストール前にアクセス・システム・コンソールで指定した値を使用。securityModeBean.securityModeChoices = "open" の場合のみ使用。	"< サーバー ID>"
-W openModeBean.hostName: Access Server のホスト名。securityModeBean.securityModeChoices = "open" の場合のみ使用。	"<IP アドレス >" または "< ホスト名 >"
-W openModeBean.webgateID: WebGate の ID。インストールを実行する前にアクセス・システム・コンソールで入力した ID を使用。securityModeBean.securityModeChoices = "open" の場合のみ使用。	"< 値 >"
-W openModeBean.portNumber: Access Server のポート番号。securityModeBean.securityModeChoices = "open" の場合のみ使用。	"< ポート番号 >"
-W openModeBean.password: WebGate のパスワード（オプション）。securityModeBean.securityModeChoices = "open" の場合のみ使用。	"< パスワード >"
-W simpleModeBean.serverID: Access Server の ID。インストール前にアクセス・システム・コンソールで指定した値を使用。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< 値 >"
-W simpleModeBean.hostName: Access Server のホスト名。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"<IP アドレス >" または "< ホスト名 >"
-W simpleModeBean.webgateID: WebGate の ID。アクセス・システム・コンソールで指定した値を使用。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< 値 >"

表 15-5 WebGate のサイレント・インストール・パラメータ（続き）

WebGate のパラメータと説明	指定できる値
-W simpleModeBean.portNumber: Access Server のポート番号。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< ポート番号 >"
-W simpleModeBean.password: WebGate のパスワード（オプション）。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< パスワード >"
-W simpleModeBean.passphrase: パスフレーズ。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< パスフレーズ >"
-W simpleModeBean.passphraseVerify: パスフレーズ（確認用）。simpleModeInfoBean.passphrase と同じ値を指定。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< パスフレーズ >"
-W certModeBean.serverID: Access Server の ID。インストール前にアクセス・システム・コンソールで指定した値を使用。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< 値 >"
-W certModeBean.hostName: Access Server のホスト名。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"<IP アドレス >" または "< ホスト名 >"
-W certModeBean.webgateID: WebGate の ID（オプション）。アクセス・システム・コンソールで指定した値を使用。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< 値 >"
-W certModeBean.portNumber: Access Server のポート番号。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< ポート番号 >"
-W certModeBean.password: WebGate のパスワード。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< パスワード >"
-W certModeBean.passphrase: パスフレーズ。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< パスフレーズ >"
-W askAutoUpdateWSBean.askAutoUpdateWSField: Web サーバーの構成の自動更新を実行するかどうかを決定する。	"Yes" または "No"
-W askConfFilePathBean.askConfFilePathField: NSAPI の場合、obj.conf を含む Web サーバーの構成ディレクトリの絶対パス（たとえば、/export/Planet/servers/https-oblix/config）。Apache および Apache SSL の場合は、Web サーバーの config ディレクトリ内の httpd.conf の絶対パス（たとえば、/export/apache/conf/httpd.conf）。Apache、Apache SSL および NSAPI Web サーバーに対して、askAutoUpdateWSBean.askAutoUpdateWSField = "Yes" の場合のみ使用。	"< 絶対パス（Apache のためのファイル名を含む）>"
-W certModeBean.passphraseVerify: パスフレーズ（確認用）。certModeInfoBean.passphrase と同じ値を指定。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< パスフレーズ >"
-W installOrRequestCertBean.installOrRequest: アクセス・システムの構成に使用する証明書をインストールするかリクエストするかを決定する。セキュリティ・モードが "cert" に設定されている場合のみ使用。すでに証明書がある場合は "install" を使用する。Oracle Access Manager で証明書をリクエストする場合は "request" を使用する。	"request" または "install"
-W certReqInfoBean.countryName: 国名。DN で有効な 2 文字の国コード。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 国コード >"
-W certReqInfoBean.stateOrProvinceName: 都道府県名。DN で有効な 2 文字のコード。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 都道府県コード >"

表 15-5 WebGate のサイレント・インストール・パラメータ（続き）

WebGate のパラメータと説明	指定できる値
-W certReqInfoBean.localityName: 市町村名。市町村名を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 市町村名 >"
-W certReqInfoBean.organizationName: 組織名。通常、組織名を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 組織名 >"
-W certReqInfoBean.organizationalUnitName: 組織単位名。通常、部門名を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 組織単位名 >"
-W certReqInfoBean.commonName: 共通名。通常、人またはエンティティの名前を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 共通名 >"
-W certReqInfoBean.emailAddress: 電子メール・アドレス。通常、有効な電子メール・アドレスを指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 電子メール・アドレス >"
-W readyToInstallCertBean.readyToInstallField: Oracle Access Manager で証明書をリクエストするように指定した場合、このパラメータによって、インストールのために証明書の準備ができたことが確認される。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。サイレント・モードでは値 "No" の使用を推奨する。Oracle Access Manager インストールが 1 つの手順から次の手順に進むよりも早く、Oracle Access Manager で生成されたリクエストをユーザーが取得して、証明書を受信することは難しいため。	"Yes" または "No"
-W copyCertificatesInputBean.certFile: 証明書は、証明書ファイル、鍵ファイル、連鎖ファイルの 3 ファイルで構成される。このパラメータは、証明書ファイルのファイル名（aaa_cert.pem など）を含む絶対パスを指定する。次の場合に使用。installOrRequestCertBean.installOrRequest = "install" の場合、または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"
-W copyCertificatesInputBean.keyFile: 証明書は、証明書ファイル、鍵ファイル、連鎖ファイルの 3 ファイルで構成される。このパラメータは、鍵ファイルのファイル名（aaa_key.pem など）を含む絶対パスを指定する。次の場合に使用。installOrRequestCertBean.installOrRequest = "install" の場合、または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"
-W copyCertificatesInputBean.chainFile: 証明書は、証明書ファイル、鍵ファイル、連鎖ファイルの 3 ファイルで構成される。このパラメータは、連鎖ファイルのファイル名（aaa_chain.pem など）を含む絶対パスを指定する。次の場合に使用。installOrRequestCertBean.installOrRequest = "install" の場合、または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"

Access Manager SDK のパラメータ

表 15-6 に、Access Manager SDK のサイレント・インストール・パラメータを示します。

表 15-6 SDK のサイレント・インストール・パラメータ

SDK のパラメータと説明	指定できる値
-P sdk.installLocation: インストール・ディレクトリ。デフォルト・ディレクトリは Windows では "C:¥COREid"、UNIX では "/coreid"。	"< インストール・ディレクトリ >"
-W userInfoBean.user: UNIX 専用。製品の実行に使用されるユーザー ID。	"< ユーザー ID>"
-W userInfoBean.group: UNIX 専用。userInfoBean.user に対応するグループ。	"< グループ ID>"

BEA WebLogic SSPI のパラメータ

表 15-7 に、BEA WebLogic SSPI のサイレント・インストール・パラメータを示します。

表 15-7 BEA WebLogic SSPI のサイレント・インストール・パラメータ

BEA SSPI のパラメータと説明	指定できる値
-P bea.installLocation: インストール・ディレクトリ。デフォルト・ディレクトリは Windows では "C:¥COREid"、UNIX では "/coreid"。	"< インストール・ディレクトリ >"
-W localePanel.defaultLang: メイン・インストールに追加の言語をインストールする場合は必須。	"en-us"
-W localePanel.installLanguages: メイン・インストールに追加の言語をインストールする場合は必須。	"en-us;fr-fr"
-W sspiConfigLevel.ConfigMode: 構成オプション。通常オプションでは最小限の入力が必要。拡張オプションではすべてのデフォルトのオーバーライドが可能。	"typical;advanced"
-W verifyUserBean.verifyUserBeanField: 製品をインストールするユーザーが製品を実行する予定のユーザーと同じかどうかを決定する。値が No の場合、インストールは終了する。	"Yes" または "No"
-W sspiAdv1.authResType: Weblogic のユーザーを認証するために Oracle Access Manager セキュリティ・プロバイダがポリシーで使用するリソース・タイプ。wl_authen	wl_authen
-W sspiAdv1.authRes: Weblogic のユーザーを認証するために Oracle Access Manager セキュリティ・プロバイダがポリシーで使用するリソース名。	/Authen/Basic
-W sspiAdv1.authResOp: Weblogic のユーザーを認証するために Oracle Access Manager セキュリティ・プロバイダがポリシーで使用するリソース操作。LOGIN	LOGIN
-W sspiAdv1.authAnonymousRes: Weblogic のユーザーを認証するために、Oracle Access Manager セキュリティ・プロバイダがポリシーで匿名アクセスに対して使用するリソース名。/Authen/Anonymous	Authen/Anonymous
-W sspiAdv1.authUID: ログイン ID。認証の credential_mapping プラグインで使用されるパラメータ。userid	userid
-W sspiAdv1.authPass: 認証スキームのパスワード検証で使用されるパスワード・パラメータ。Password	Password
-W sspiAdv1.authnActionType: アクション・タイプ（アクションが ObSSOCookie から loginId を取得するように構成される）。WL_REALM	WL_REALM

表 15-7 BEA WebLogic SSPI のサイレント・インストール・パラメータ（続き）

BEA SSPI のパラメータと説明	指定できる値
-W sspiAdv1.authnActionName: アクション名（アクションが ObSSOCookie から loginId を取得するように構成される）。uid	uid
-W sspiAdv1.obDummyUser: プロキシ HTTP サーバー上に WebGate がない場合に、SSO を実行するためにフォーム・ログインで使用されるダミーのユーザー名。Obdummyuser	Obdummyuser
-W sspiAdv2.webAppResourceTypes: Web アプリケーションで使用される Weblogic リソース・タイプ（カンマ区切り）。<url>,<web>	<url>,<web>
-W sspiAdv2.roleResType: ユーザーのロールを取得するために Oracle Access Manager セキュリティ・プロバイダがポリシーで使用するリソース・タイプ。	wl_authen
-W sspiAdv2.roleRes: ユーザーのロールを取得するために、Oracle Access Manager セキュリティ・プロバイダがポリシーで使用するリソース名。	/Authen/Roles
-W sspiAdv2.roleResOp: ユーザーのロールを取得するために、Oracle Access Manager セキュリティ・プロバイダがポリシーで使用するリソース操作。	LOGIN
-W sspiAdv2.rolesCacheTTL: ロール・キャッシュ内の要素の TTL（time to live）。	60
-W sspiAdv2.rolesCacheCleanupSchedule: キャッシュから期限切れの要素を削除する間隔（秒）。	60
-W sspiAdv2.roleActionType: ロールを取得するための認可ルール内のアクション・タイプ。	WL_REALM
-W sspiAdv3.notProtecedAction: Oracle Access Manager によって保護されないリソースへのデフォルト・アクセス。	allow、deny、abstain
-W sspiAdv3.abstainMapsTo: 認可結果のマップの禁止（allow、deny）。	allow、deny
-W sspiAdv3.debug: デバッグの設定（本番システムの場合、Off に設定）。	1: On 2: Off
-W securityModeBean.securityModeChoices: BEA SSPI のセキュリティ・モード。値 "open" はセキュリティ不使用、値 "simple" は暗号化使用、"cert" は独自の CA の実行を意味する。	"open"、 "simple"、"cert"
-W openModeBean.serverID: Access Server の ID。インストール前にアクセス・システム・コンソールで指定した値を使用。次の場合のみ使用。 securityModeBean.securityModeChoices = "open" "AccessServer1" など。	"< サーバー ID>"
-W openModeBean.hostName: Access Server がインストールされているホスト名。securityModeBean.securityModeChoices = "open" の場合のみ使用。	"<IP アドレス >" または "< ホスト名 >"
-W openModeBean.accessGateID: Access Gate の ID。次の場合のみ使用。 securityModeBean.securityModeChoices = "open" "WeblogicRealm1" など。	"< 値 >"
-W openModeBean.portNumber: Access Server のポート番号。securityModeBean.securityModeChoices = "open" の場合のみ使用。	"< ポート番号 >"
#-W openModeBean.password: Access Gate のパスワード（設定する場合）。securityModeBean.securityModeChoices = "open" の場合のみ使用。	"< パスワード >"

表 15-7 BEA WebLogic SSPI のサイレント・インストール・パラメータ（続き）

BEA SSPI のパラメータと説明	指定できる値
-W simpleModeBean.serverID: Access Server の ID。インストール前にアクセス・システム・コンソールで指定した値を使用。次の場合のみ使用。 securityModeBean.securityModeChoices = "simple"	"< サーバー ID>"
-W simpleModeBean.hostName: Access Server がインストールされているホスト名。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"<IP アドレス >" または "< ホスト名 >"
-W simpleModeBean.accessGateID: Access Gate の ID。この値は、アクセス・システム・コンソールで指定した値のいずれかと一致する必要がある。次の場合のみ使用。 securityModeBean.securityModeChoices = "simple"	"< 値 >"
-W simpleModeBean.portNumber: Access Server のポート番号。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< ポート番号 >"
#-W simpleModeBean.password: Access Gate のパスワード（設定する場合）。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< パスワード >"
#-W simpleModeBean.passphrase: Access Gate が Access Server と通信するためのパスフレーズ。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< パスフレーズ >"
#-W simpleModeBean.passphraseVerify: Access Gate が Access Server と通信するためのパスフレーズ。このパラメータは、パスフレーズが securityModeBean.passphrase のパスフレーズと一致することを確認する。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< パスフレーズ >"
-W certModeBean.serverID: Access Server の ID。インストール前にアクセス・システム・コンソールで指定した値を使用。この値は、アクセス・システム・コンソールで指定した値のいずれかと一致する必要がある。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< 値 >"
-W certModeBean.hostname: Access Server がインストールされているホスト名。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"<IP アドレス >" または "< ホスト名 >"
-W certModeBean.accessGateID: Access Gate の ID。この値は、アクセス・システム・コンソールで指定した値のいずれかと一致する必要がある。次の場合のみ使用。 securityModeBean.securityModeChoices = "cert"	"< 値 >"
-W certModeBean.portNumber: Access Server のポート番号。次の場合のみ使用。 securityModeBean.securityModeChoices = "cert"	"< ポート番号 >"
-W certModeBean.password: Access Gate のパスワード（設定する場合）。securityModeBean.securityModeChoices = "cert" の場合のみ使用。"password"	"< ポート番号 >"
-W certModeBean.passphrase: Access Gate が Access Server と通信するためのパスフレーズ。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< パスフレーズ >"
-W certModeBean.passphraseVerify: Access Gate が Access Server と通信するためのパスフレーズ。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< パスフレーズ >"

表 15-7 BEA WebLogic SSPI のサイレント・インストール・パラメータ（続き）

BEA SSPI のパラメータと説明	指定できる値
-W installOrRequestCertBean.installOrRequest: アクセス・システムの構成に使用する証明書をインストールするかリクエストするかを決定する。セキュリティ・モードが "cert" に設定されている場合のみ使用。すでに証明書がある場合は "install" を選択する。Oracle Access Manager で証明書をリクエストする場合は "request" を選択する。	"install"、"request"
-W certReqInfoBean.countryName: 国名。通常、DN で有効な 2 文字の国コード。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 国コード >"
-W certReqInfoBean.stateOrProvinceName: 都道府県名。通常、DN で有効な 2 文字の都道府県コード。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 都道府県コード >"
-W certReqInfoBean.localityName: 市町村名。市町村名を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 市町村名 >"
-W certReqInfoBean.organizationName: 組織名。通常、組織名を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 組織名 >"
-W certReqInfoBean.organizationalUnitName: 組織単位名。通常、部門名を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 組織単位名 >"
-W certReqInfoBean.commonName: 共通名。通常、人またはエンティティの名前を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 名前 >"
-W certReqInfoBean.emailAddress: 電子メール・アドレス。通常、有効な電子メール・アドレスを指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 電子メール・アドレス >"
-W readyToInstallCertBean.readyToInstallField: Oracle Access Manager で証明書をリクエストするように指定した場合、このパラメータによって、インストールのために証明書の準備ができたことが確認される。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。サイレント・モードでは "Yes" を使用しないことを推奨する。Oracle Access Manager インストールが 1 つの手順から次の手順に進むよりも早く、Oracle Access Manager で生成されたリクエストをユーザーが取得して、証明書を受信することは難しいため。	"Yes" または "No"
-W copyCertificatesInputBean.certFile: 証明書ファイルのファイル名（aaa_cert.pem など）を含む絶対パス。次の場合に使用。 installOrRequestCertBean.installOrRequest = "install" の場合。または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"
-W copyCertificatesInputBean.keyFile: 鍵ファイルのファイル名（aaa_key.pem など）を含む絶対パス。次の場合に使用。 installOrRequestCertBean.installOrRequest = "install" の場合。または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"

表 15-7 BEA WebLogic SSPI のサイレント・インストール・パラメータ（続き）

BEA SSPI のパラメータと説明	指定できる値
-W copyCertificatesInputBean.chainFile: 連鎖ファイルのファイル名（aaa_chain.pem など）を含む絶対パス。次の場合に使用。 installOrRequestCertBean.installOrRequest = "install" の場合。または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"

WAS レジストリのパラメータ

表 15-8 に、WAS レジストリのサイレント・インストール・パラメータを示します。

表 15-8 WAS レジストリのサイレント・インストール・パラメータ

WAS レジストリのパラメータの説明	指定できる値
-P was_registry.installLocation: インストール・ディレクトリ。デフォルト・ディレクトリは Windows では "C:¥Program Files¥COREid"、UNIX では "/opt/coreid"。	"< インストール・ディレクトリ >"
-W verifyUserBean.verifyUserBeanField: 製品をインストールするユーザーが製品を実行する予定のユーザーと同じかどうかを決定する。値が No の場合、インストールは終了する。	"Yes" または "No"
-W wasConfig.WPHostName: Webpass のホスト名。	"< マシン名 >"
-W wasConfig.WPPortNumber: Webpass のポート番号。	"< ポート番号 >"
-W wasConfig.WPIsProtected: WebPass が WebGate によって保護されているかどうか。	"true" または "false"
-W wasWebPassConfig.cookieDomain: WebGate に設定された Cookie ドメイン。"company.com" など。	"< ドメイン名 >"
-W wasWebPassConfig.cookiePath: WebGate に設定された Cookie パス。"/" など。	"< パス >"
-W wasDSConfig.WPSSL: Websphere に対する Oracle Access Manager コネクタが、SSL モード（https を使用するデータ送信）で Websphere に接続するために WebPass が必要かどうかを決定する。	"true" または "false"
-W wasDSConfig.UserAttr: ユーザー属性。	"uid"
-W wasDSConfig.UserSearchAttr: ユーザー検索属性。	"cn"
-W wasDSConfig.GroupSearchAttr: グループ検索属性。	"cn"
-W wasWSClassesDir.classesDir: WebSphere クラス・ディレクトリのフルパス。	"< パス >"
-W configPortalInput.isPortalTobeUsed: Oracle Access Manager Websphere コネクタは、Websphere ポータル・サーバー統合のために特定のファイルを WebSphere アプリケーション・ディレクトリにコピーする必要がある。このパラメータは、ポータル・サーバーの統合が必要かどうかを確認する。	"true" または "false"
-W wasInfoBean.wasInstallDir: -W configPortalInput.isPortalTobeUsed = "true" の場合、WebSphere アプリケーション・ディレクトリ・パスを入力する。	*$Websphere_install_dir*/AppServer
-W securityModeBean.securityModeChoices: AccessGate モードの構成。値 "open" はセキュリティ不要、値 "simple" は暗号化使用、値 "cert" は独自の CA の実行を意味する。	"open"、"simple" または "cert"

表 15-8 WAS レジストリのサイレント・インストール・パラメータ（続き）

WAS レジストリのパラメータの説明	指定できる値
-W openModeBean.serverID: Access Server の ID。インストール前にアクセス・システム・コンソールで指定した値を使用。securityModeBean.securityModeChoices = "open" の場合のみ使用。	"< サーバー ID>"
-W openModeBean.hostname: Access Server がインストールされているマシン名。securityModeBean.securityModeChoices = "open" の場合のみ使用。	"<IP アドレス >" または "< マシン名 >"
-W openModeBean.accessGateID: AccessGate の ID。securityModeBean.securityModeChoices = "open " の場合のみ使用。	"<AccessGate の ID>"
-W openModeBean.portNumber: Access Server のポート番号。	"< ポート番号 >"
#-W openModeBean.password: AccessGate のパスワード（設定する場合）。securityModeBean.securityModeChoices = "open" の場合のみ使用。	"< パスワード >"
-W simpleModeBean.serverID: Access Server の ID。インストール前にアクセス・システム・コンソールで指定した値を使用。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"<Access Server の ID>"
-W simpleModeBean.hostname: Access Server がインストールされているホスト名。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"<IP アドレス >" または "< マシン名 >"
-W simpleModeBean.accessGateID: AccessGate の ID。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"<AccessGate の ID>"
-W simpleModeBean.portNumber: Access Server のポート番号。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< ポート番号 >"
#-W simpleModeBean.password: Access Gate のパスワード。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< パスワード >"
#-W simpleModeBean.passphrase: Access Gate が Access Server と通信するためのパスフレーズ。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< パスフレーズ >"
#-W simpleModeBean.passphraseVerify: Access Gate が Access Server と通信するためのパスフレーズ。このパラメータは、パスフレーズが simpleModeBean.passphrase と一致することを確認する。securityModeBean.securityModeChoices = "simple" の場合のみ使用。	"< パスフレーズ >"
-W certModeBean.serverID: Access Server の ID。インストール前にアクセス・システム・コンソールで指定した値を使用。この値は、アクセス・システム・コンソールで指定した値のいずれかと一致する必要がある。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< サーバー ID>"
-W certModeBean.hostname: Access Server がインストールされているホスト名。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"<IP アドレス >" または "< マシン名 >"
-W certModeBean.accessGateID: AccessGate の ID。この値は、アクセス・システム・コンソールで指定した値のいずれかと一致する必要がある。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"<AccessGate の ID>"
-W certModeBean.portNumber: Access Server のポート番号。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< ポート番号 >"
#-W certModeBean.password: Access Gate のパスワード（設定する場合）。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< パスワード >"
#-W certModeBean.passphrase: AccessGate が Access Server と通信するためのパスフレーズ。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< パスフレーズ >"

表 15-8 WAS レジストリのサイレント・インストール・パラメータ（続き）

WAS レジストリのパラメータの説明	指定できる値
#-W certModeBean.passphraseVerify: Access Gate が Access Server と通信するためのパスフレーズ。このパラメータは、パスフレーズが certModeBean.passphrase のパスフレーズと一致することを確認する。securityModeBean.securityModeChoices = "cert" の場合のみ使用。	"< パスフレーズ >"
-W installOrRequestCertBean.installOrRequest: アクセス・システムの構成に使用する証明書をインストールするかリクエストするかを決定する。セキュリティ・モードが "cert" に設定されている場合のみ使用。すでに証明書がある場合は "install" を選択する。Oracle Access Manager で証明書をリクエストする場合は "request" を選択する。	"install"、"request"
-W certReqInfoBean.countryName: 国名。通常、DN で有効な 2 文字の国コード。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 国コード >"
-W certReqInfoBean.stateOrProvinceName: 都道府県名。通常、DN で有効な 2 文字の都道府県コード。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 都道府県コード >"
-W certReqInfoBean.localityName: 市町村名。市町村名を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 市町村名 >"
-W certReqInfoBean.organizationName: 組織名。通常、組織名を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 組織名 >"
-W certReqInfoBean.organizationalUnitName: 組織単位名。通常、部門名を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 組織単位名 >"
-W certReqInfoBean.commonName: 共通名。通常、人またはエンティティの名前を指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 名前 >"
-W certReqInfoBean.emailAddress: 電子メール・アドレス。通常、有効な電子メール・アドレスを指定する。証明書のリクエストに使用される情報の一部である。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。	"< 電子メール・アドレス >"
-W readyToInstallCertBean.readyToInstallField: Oracle Access Manager で証明書をリクエストするように指定した場合、このパラメータによって、インストールのために証明書の準備ができたことが確認される。installOrRequestCertBean.installOrRequest = "request" の場合のみ使用。サイレント・モードでは "Yes" を使用しないことを推奨する。Oracle Access Manager インストールが 1 つの手順から次の手順に進むよりも早く、Oracle Access Manager で生成されたリクエストをユーザーが取得して、証明書を受信することは難しいため。	"Yes" または "No"
-W copyCertificatesInputBean.certFile: 証明書ファイルのファイル名（aaa_cert.pem など）を含む絶対パス。次の場合に使用。installOrRequestCertBean.installOrRequest = "install" の場合、または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"
-W copyCertificatesInputBean.keyFile: 鍵ファイルのファイル名（aaa_key.pem など）を含む絶対パス。次の場合に使用。installOrRequestCertBean.installOrRequest = "install" の場合、または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"

表 15-8 WAS レジストリのサイレント・インストール・パラメータ（続き）

WAS レジストリのパラメータの説明	指定できる値
-W copyCertificatesInputBean.chainFile: 連鎖ファイルのファイル名（aaa_chain.pem など）を含む絶対パス。次の場合に使用。installOrRequestCertBean.installOrRequest = "install" の場合、または installOrRequestCertBean.installOrRequest = "request" かつ readyToInstallCertBean.readyToInstallField = "Yes" の場合。	"< ファイル名を含む絶対パス >"
-W localePanel.defaultLang: メイン・インストールに追加の言語をインストールする場合は必須。	"en-us"
-W localePanel.installLanguages: メイン・インストールに追加の言語をインストールする場合は必須。	"en-us;fr-fr"

サイレント・モードでインストールしたコンポーネントのアンインストール

サイレント・モードでインストールしたコンポーネントをアンインストールする方法は、プラットフォームによって異なります。

Windows の場合 : 次のコマンドを実行します。

Component_install_dir¥oblix¥_uninst*component*¥uninstaller.exe -silent

Solaris の場合 : 次のコマンドを実行します。

Component_install_dir/oblix/_uninst*component*/uninstaller.bin -silent

Component_install_dir は、コンポーネントがインストールされているインストール・ディレクトリです（パス名の ¥identity は ID システム、¥access はアクセス・システムを示します）。

GUI またはコンソールを使用してインストールしたコンポーネントを削除する方法は、第 20 章「Oracle Access Manager の削除」を参照してください。

インストール済コンポーネントのクローニングと同期化

コマンドラインまたはインストール GUI を使用してコンポーネントをインストールするかわりに、すでにインストール済のコンポーネントの構成をクローニングすることで、コンポーネントを自動的にインストールできます。

クローニング : コンポーネントのミラー・コピーを作成します。つまり、クローニングでは、すでにインストール済のコンポーネントをテンプレートとして使用して、ローカル・システムまたはリモート・システムにコンポーネントのコピーを作成します。Identity Server または Access Server をクローニングすると、次のことが可能です。

- リモート・システムでのクローン・サーバーの起動
- クローン・サーバーの起動後の再構成
- インストール済の 2 つのコンポーネントの同期化による、構成の部分的なレプリケート

Windows と UNIX では、ディレクトリ oblix/tools/np_sync でコマンド np_sync を使用してコンポーネントをクローニングできます。np_sync ツールについては、15-31 ページの「np_sync の構文とオプション」で説明しています。

同期化 : 同じ Oracle Access Manager コンポーネントが 2 つインストールされており、一方の状態が新しい場合に 2 つを同じ状態にすることができます。同期化によって、類似したプラットフォーム上のインストールをアップグレードまたは修復することができます。2 つのコンポーネントを同期化するには、np_sync ツールの -sync または -sync-all コマンドライン・オプションを使用します。

注意： Web サーバー・プラグインである WebPass、Policy Manager および WebGate では、Web サーバー構成ファイルは np_sync では更新されません。前に説明したように、インストール時に自動的に行うか、インストール後に手動で行う必要があります。

np_sync の使用例

コンポーネントのインストールと構成が終了してから、次のようなコマンドを使用します。

```
np_sync -clone test2.oblix.com /export/home1/np7test2
```

これによって、現在のマシンが、ディレクトリ /export/home1/np7test2 のシステム test2.oblix.com にクローニングされます。

np_sync の構文とオプション

np_sync の基本構文を次に示します。

```
./np_sync -mode [-opts] host destination_dir
```

mode は、sync、sync-all または clone です。次に例を示します。

-sync: -sync コマンドでは、マシンに依存しないファイルのみが更新されます。これらはカスタマイズ・ファイル（テキスト）です。このコマンドを使用して、類似したプラットフォーム上のインストールをアップグレードまたは修復することができます。たとえば、AIX システムと Solaris システムがある場合に、それらを同期化することができます。

-sync-all: -sync-all コマンドでは、カスタマイズ・ファイル（テキスト）の他に、バイナリ、共有ライブラリ、実行可能ファイルなどが対象になります。このコマンドを使用して、類似したプラットフォーム上のインストールをアップグレードまたは修復することができます。

-clone: -clone オプションでは、インストール全体がコピーされます。このオプションには、後で説明する -p port オプションと -n servername オプションも必要になります。

-opts には、次のいずれかを組み合せて指定します。

-u username: UNIX 専用。np_sync コマンドを発行し、ログインしたユーザー以外としてリモート・システムに接続する場合は、-u *username* オプションを使用します。使用する資格証明は変更されませんが、remote-copy コマンドの受信側を実行するユーザーが変更されます。

-rsync: UNIX 専用。rsync コマンドを使用します（rdist がデフォルトで使用されます。15-32 ページの「UNIX の注意事項」を参照してください）。

-ssh: UNIX 専用。rsync を使用するときに、暗号化接続を使用するセキュアなシェル（ssh）を使用してデータを送信します。rsync コマンドを使用するときは、標準の UNIX リモート・シェル接続（rsh または remsh）のかわりに ssh を使用できます。

-path rsyncpath: UNIX 専用。リモート・システムの rsyncpath で rsync を探します（rsync を使用するとき）。

-d: デバッグ・モード。コピーは行われず、更新の内容が示されます。

-l sorter: ソース・ディレクトリとしてソーターを使用します。デフォルトでは、現在の Oracle Access Manager インストール領域（このプログラムがある場所）がソースとして使用されます。

-n servername: Identity Server または Access Server をクローニングする場合は、新しい Oracle Access Manager サーバー名を指定する必要があります。servername に新しいサーバーを指定します。

-p portnumber: Identity Server または Access Server をクローニングする場合は、ポートを指定する必要があります。portnumber に新しいサーバー・ポートを指定します。

Windows 専用

-F: Windows 専用。このオプションではインストールが強制的に実行されます（サニティ・チェックは無視されます）。-F フラグを使用すると、通常のチェックが失敗する場合でもインストールを強制実行できます。途中で失敗したクローニング操作を再実行するときに役立ちます。

-f: Windows 専用。-f フラグではコピーが強制的に実行されます。リモート・システムでのファイル変更回数は無視され、すべての関連ファイルが更新されます。

-r: Windows 専用。このオプションでは、必要な場合にインストール後にリモート・ホストが再起動されます。システム・ライブラリを更新する必要がある場合は、クローニングでこのオプションを使用します。

15-32 ページの「Windows の注意事項」も参照してください。

UNIX の注意事項

UNIX では、.rhosts を使用してリモート・コピー権限を有効にする必要があります。

-clone、-sync-all および -sync コマンド・オプションでコピーされるファイルの正確なリストは、np_sync スクリプトで定義されます。特殊な場合にはこれらのファイルをチューニングする必要があります。

デフォルトでは、UNIX は rdist コマンドを使用してリモート・システムを更新します。Solaris では rdist がリモート・システムの /usr/ucb/ にあるとみなされるため、異なるプラットフォームでは機能しない場合があります。

rdist コマンドは通常は Linux には含まれません。Linux では rsync プログラムを使用できます。通常、rsync プログラムは Solaris、HP-UX または AIX には含まれません。

UNIX では、リモート・システムがリモート・アクセスの権限を付与する必要があります。通常、これにはリモート・システムの .rhosts ファイルが使用されます。このファイルは、*host username* という形式の行で構成されており、*host* はコピー元のシステム、*username* はリモート・コピー・コマンドの発行が許可されたユーザーです。

Windows の注意事項

Windows での np_sync は実行可能プログラム（np_sync.exe）です。

-clone、-sync または -sync-all コマンド・オプションで転送されるファイルは、Windows の np_sync サブディレクトリにあるパターン・ファイルで定義されます。特殊な場合にはパターン・ファイルをチューニングする必要があります。

Windows では、np_sync コマンドによって、クローニングまたは同期化を完了するために必要なネットワーク・ドライブが自動的にマウントされます。ユーザーがプロセスに割り込まない場合は、終了時にネットワーク・ドライブがアンマウントされます。

Windows でのクローニングでも、np_sync ツールによってシステム・レジストリや必要なシステム DLL ファイルが更新され、システム・サービスに適切なエントリがインストールされます。np_sync コマンドではシステム・サービスの起動や停止は行われません。ディレクトリ oblix/tools/NPServMgr/（Windows のみ）にあるプログラム NPServMgr.exe を使用して、Windows システム・サービスの Oracle Access Manager サーバーの起動、停止、追加または削除を行います。

レジストリとシステム・サービスを更新するには、ローカルの Windows ユーザーがリモート・システムのシステム管理者権限を持つ必要があります。このためには、ネットワーク管理者ログインを使用するか、リモート・システムで同じユーザー名とパスワードに管理権限を割り当てます。

注意： システム・ドライブが C: 以外のパーティションにある場合は、-S フラグまたは -R フラグを使用する必要があります。

---

np_sync コマンドではデフォルトのシステム・ディレクトリ C:¥WINNT¥system32 が使用されます。ただし、Windows XP および Windows Server 2003 では、システム・ディレクトリは C:¥Windows¥system32 です。ローカル・システムまたはリモート・システムのオペレーティン

グ・システムが Windows 2000 よりも新しい場合は、np_sync コマンドで次のフラグを使用する必要があります。

ローカル・システム・ディレクトリの場合は -S フラグ

リモート・システム・ディレクトリの場合は -R フラグ

クローン・コンポーネントのアンインストール

次の項では、UNIX および Windows でクローン・コンポーネントをアンインストールする方法について説明します。

- UNIX でのクローン・コンポーネントのアンインストール
- Windows でのクローン・コンポーネントのアンインストール

> **注意：** GUI またはコンソールを使用してインストールしたコンポーネントを削除する方法は、第 20 章「Oracle Access Manager の削除」を参照してください。

UNIX でのクローン・コンポーネントのアンインストール

UNIX システムでのアンインストールの手順を次に示します。

UNIX でアンインストールする手順

1. コンポーネントが WebPass、Policy Manager または WebGate の場合は、対応する Web サーバーの obj.conf ファイルで Oracle Access Manager 固有のエントリを削除します。
2. コンポーネントがプロセス（Identity Server、Access Server）を実行している場合は、プロセスを停止します。
3. コンポーネントのディレクトリを削除します。

Windows でのクローン・コンポーネントのアンインストール

クローン・コンポーネントのアンインストールに InstallShield を使用することはできません。Windows でのアンインストールにはレジストリ・エントリの削除が必要です。また、オラクル社提供のユーティリティを使用して、インストール済サービスを削除する必要があります。

Oracle Access Manager システムのアンインストール

2 つの手順を説明します。

Identity Server と Access Server をアンインストールする手順

1. *Component_install_dir*¥access¥oblix¥tools ディレクトリにある NPServMgr.exe を使用して Identity サービスまたは AAA サービスをアンインストールします。引数を指定せずに NPServMgr.exe を実行すると使用方法が表示されます。
2. コンポーネントに関連するレジストリ・エントリを削除します。
3. Identity Server または Access Server のインストール・ディレクトリを削除します。

WebPass、WebGate および Policy Manager をアンインストールする手順

1. Oracle Access Manager による変更を Web サーバーの obj.conf（NSAPI）または Oracle Access Manager .dll および仮想ディレクトリ（ISAPI）から削除します。
2. コンポーネントのホストである Web サーバー・インスタンスを停止します。
3. レジストリ・エントリを削除します。
4. インストール・ディレクトリを削除します。

第 VI 部

Web サーバーの構成

ここでは Web サーバーの構成情報について説明します。

第 VII 部は、次の章で構成されます。

- 第 16 章「Apache v1.3 Web サーバーおよび Oracle HTTP Server Web サーバーの構成」
- 第 17 章「Oracle Access Manager のための Apache v2、IHS および OHS Web サーバーの構成」
- 第 18 章「WebGates のための Lotus Domino Web サーバーの設定」

16

Apache v1.3 Web サーバーおよび Oracle HTTP Server Web サーバーの構成

この章では、Oracle Access Manager のために Apache v1.3 Web サーバーを構成する方法について説明します。10*g*（10.1.4.0.1）Web コンポーネント（WebPass、Policy Manager、WebGate）は、Oracle HTTP Server（OHS）10*g* R2（10.1.2）もサポートしています。

> **注意：** Oracle HTTP Server（OHS）の実装は、オープン・ソースの Apache v1.3 に基づいています。

次の項目について説明します。

- OHS と Oracle Access Manager について
- Apache v1.3 と Oracle Access Manager について
- Apache v1.3、Oracle HTTP Server（OHS）および Stronghold の要件
- Apache v1.3、OHS および IHS Web サーバーのサポート
- ベース Apache Web サーバーのダウンロードとコンパイル
- プラットフォーム固有のコンパイル・オプション
- AIX のためのプラットフォーム固有の実行時設定
- Oracle Access Manager Web コンポーネントのインストール順序
- Oracle Access Manager Web コンポーネントのための Web サーバー構成の更新
- Oracle Access Manager Web コンポーネントのための Apache 1.3 のチューニング
- OHS クライアント証明書の設定
- Oracle Access Manager Web コンポーネントのための OHS のチューニング
- Web サーバーの起動と停止

> **注意：** 第 17 章「Oracle Access Manager のための Apache v2、IHS および OHS Web サーバーの構成」も参照してください。

OHS と Oracle Access Manager について

OHS はインターネット Web サーバーの拡張機能です。これは、Oracle HTTP Server（OHS）と通信する Oracle Access Manager Web コンポーネントを識別します。Oracle Access Manager 10*g*（10.1.4.0.1）によって、Linux プラットフォームや Windows プラットフォームのスタンドアロン Oracle HTTP Server にインストールできる、WebPass、Policy Manager および WebGate コンポーネントが提供されます。すべてのアプリケーションに対して OHS Web コンポーネントを使用できますが、次の要件に注意する必要があります。

- OHS WebGate を Oracle Single Sign-On と統合できるようにするには、『Oracle Access Manager 統合ガイド』の説明に従って Oracle Application Server にインストールする必要があります。
- OHS WebPass および OHS Access Manager（Policy Manager）コンポーネントは、Oracle Application Server で使用できます。ただし、Apache WebPass と Apache Policy Manager もこのアプリケーションに対してサポートされます。

OHS 10*g* R2（10.1.2）は Apache v1.3 に基づいています。次のような OHS の詳細は、『Oracle HTTP Server 管理者ガイド』を参照してください。

- オラクル社による実装と、基礎になっているオープン・ソース Apache 製品の違い
- Oracle HTTP Server のディレクトリ構造、構成ファイル、構文、モジュール、ディレクティブ
- サーバー・プロセス、ネットワーク接続およびセキュリティ機能の管理

この後で説明する OHS Web コンポーネントの注意事項をよく理解してください。16-11 ページの「OHS クライアント証明書の設定」も参照してください。

Linux での OHS Web コンポーネントの注意事項

Oracle Access Manager 10*g*（10.1.4.0.1）Web コンポーネントを OHS に対して使用する場合、Linux では次の点に注意してください。

- Linux では実行時に `LD_ASSUME_KERNEL=2.4.19` 環境変数を設定する必要があります。Linux の以前のスレッド・モデルがサポートされているためです（ネイティブの posix スレッド・ライブラリ（NPTL）ではない）。
- Linux では Policy Manager とディレクトリ・サーバーの SSL モードでの通信はサポートされていません。
- Linux 上の Apache または OHS に対して Oracle Access Manager Web コンポーネントをインストールするとき、Web サーバーを実行しているのと同じユーザーとしてインストールするように求められます。httpd.conf ファイルの User および Group ディレクティブ・エントリを参照してください。

Linux および Windows プラットフォームでの OHS Web コンポーネントの注意事項

Windows および Linux プラットフォームで OHS に対して Oracle Access Manager 10*g*（10.1.4.0.1）Web コンポーネントを使用する場合、httpd.conf で Windows と Linux 両方のプラットフォームについて Perl モジュールをコメント化する必要があります。

Apache v1.3 と Oracle Access Manager について

ここでは、Apache のプロセスに基づくアーキテクチャが様々な Oracle Access Manager Web コンポーネントにどのように影響するかを説明します。

WebPass から Identity Server へのアクセス

Apache v1 での Identity Server と WebPass の通信 :

- 各 WebPass インスタンスが Identity Server に接続します。
- 各接続がシステム・ソースを利用し、それぞれが n 個のファイル記述子を使用します。
- Apache がプロセスの起動と停止を頻繁に行わずにすむように、Apache のチューニング・パラメータを設定します。Oracle Access Manager の使用に関係なくこの設定は同じです。

Policy Manager

Apache v1 での Policy Manager:

- 各 Web サーバー・プロセスは Policy Manager アプリケーションのインスタンスです。
- 各アプリケーションは、ディレクトリ・サーバーに対して独自の接続を保持します。これはパフォーマンスには直接影響しません。ただし、ディレクトリ・サーバー側に制限が生じることがあります。他のディレクトリ・サーバー・クライアントが関係する場合には考慮してください。
- 複数のプロセスが 1 ユーザーのリクエストに応答します（フレームを構築するために複数の HTTP イベントがトリガーされます）。
- レスポンスの待機時間は予測できません。
- UI の観点ではプロセス数が少ない方が望ましいが、同時ユーザー数が影響を受けます。

WebGate

Apache v1 での WebGate:

- プロセス間の共有キャッシュはありません。
- 各プロセスは、Access Server との独自の接続を保持します。
- プロセスごとに独自の接続があるため、WebGate 接続の数を制限する必要があります。この問題は、Web サーバーと Access Server を実行するシステムのパフォーマンスの影響を部分的に受けます。
- Solaris および Linux プラットフォームの Apache Web サーバーではリバース・プロキシ機能を有効にできます。

例 : UNIX システムでの Apache v1.3 の構成

Apache v1.3 はプロセスベースの Web サーバーです。Apache Web サーバーは、各リクエストを処理するように構成されたフィルタを含むクライアント・プロセスを作成します。結果として、各クライアント・プロセスには WebGate が組み込まれます。

Apache Web サーバーが 250 の MaxClients を使用する（ピーク負荷時）ように構成されている場合、これらすべてのプロセスが実行すると 250 の WebGate が実行時に生成されます。
各 WebGate は、WebGate 定義で指定された接続構成を使用します。たとえば、WebGate 構成で 1 つの Access Server に対して 4 つの接続がある場合、各クライアント・プロセスは構成されている Access Server に対して 4 つの接続を生成します。このため、ピーク負荷時には、Access Server に対して 1000（250 * 4）の接続が生成されます。

Access Server では、各接続がメッセージ・スレッドに対応し、メッセージ・スレッドがソケットからクライアント・リクエストを読み取ります。前述の構成では、ピーク負荷時には 1 つの WebGate のリクエストを処理するためだけに 1000 個のスレッドが生成されます。複数の Apache v1.3 Web サーバーが 1 つの Access Server にアクセスするように構成されている場合、この数は各 Web サーバーからの接続の合計数になります。このように Access Server のスレッド数は膨大になることがあります。

プロセスのスレッド数が増加すると、CPU 使用率やメモリー使用率に関するオーバーヘッドが大きくなります。一部のオペレーティング・システムでは、スレッド数が一定を超えるとスラッシングが開始されるため、Access Server のパフォーマンスに悪影響を与えます。

Apache v1.3 Web サーバーは、リクエストの負荷に基づいてクライアント・プロセスを作成および廃棄します。また、子プロセス間のリクエストのロード・バランスを行います。結果として各子プロセスは最大でも 1 リクエストを処理します。この場合、必要な接続は 1 つの Access Server に対して 1 つのみになります。

1 つの WebGate に 2 ～ 3 の Access Server を構成して、この WebGate から Access Server に対する負荷をロード・バランスすることもできます。次に例を示します。

WebGate1 で、Access Server1 に対して 1 つの接続
Access Server 2 に対して 1 つの接続
Access Server 3 に対して 1 つの接続
MaxConnections=3

この場合、次のようになります。

WebGate1 に対する Web サーバーの最初のリクエストは Access Server1 に送られます。
WebGate1 に対する Web サーバーの 2 番目のリクエストは Access Server2 に送られます。
WebGate1 に対する Web サーバーの 3 番目のリクエストは Access Server3 に送られます。
WebGate1 に対する Web サーバーの 4 番目のリクエストは Access Server に送られます。
このように続きます。

ただし、子プロセスの存続期間内に 1 リクエストが Web サーバーから WebGate1 に送信される場合は、AccessServer2 と AccessServer3 の接続 1 は使用されないことがあります。

まとめると、Apache v1.3 のような複数プロセス Web サーバーでは、1 つの Access Server に対して 1 つの接続しか必要ありません。

Apache v2 の場合、2 つの mpm モード（worker_mpm および pre-fork_mpm）で作動するように Web サーバーを構成できます。worker_mpm では、リクエストのロード・バランスのために Web サーバーにスレッドが作成されます。この場合、生成されるプロセス数を決定するために ThreadsPerChild と MaxClients が使用されます。アクティブな子プロセスの最大数は、MaxClients ディレクティブを ThreadsPerChild ディレクティブで割った数値です。各プロセスには WebGate が含まれます。pre-fork mpm の場合、Apache v1.3 と同様の動作になり、リクエスト当たりに 1 つの子プロセスが作成されます。詳細は、第 17 章「Oracle Access Manager のための Apache v2、IHS および OHS Web サーバーの構成」を参照してください。

Apache v1.3、Oracle HTTP Server（OHS）および Stronghold の要件

Oracle Access Manager 10*g*（10.1.4.0.1）の HTML ページでは UTF-8 エンコーディングが使用されます。Apache ベースの Web サーバーでは、管理者が AddDefaultCharset ディレクティブを使用して、送出されるすべての HTML ページのデフォルト・キャラクタ・セットを指定できます。このディレクティブは、HTML ページを生成するアプリケーションで指定されるすべてのキャラクタ・セットよりも優先されます。AddDefaultCharset ディレクティブで UTF-8 以外のキャラクタ・セットを有効にすると、Oracle Access Manager の HTML ページが文字化けします。

Oracle Access Manager 10*g*（10.1.4.0.1）の HTML ページを正しく表示するには、AddDefaultCharset ディレクティブを Web サーバー構成ファイル（httpd.conf）に次のように指定することをお薦めします。

```
AddDefaultCharset Off
```

このディレクティブの詳細は、Web サーバーのドキュメントを参照してください。

また、Apache v1.3、OHS または Stronghold Web サーバーを実装するには、システムが次の要件を満たすことも必要です。

- WebGate および WebPass のための動的共有オブジェクト（DSO）のサポート。つまり、Apache では mod_so を有効にする必要があります。

  注意： DSO はすべての Oracle Access Manager プラグインで必要です。

- WebPass ではマルチスレッドが必要です。
- WebGate と WebPass を同じ Web サーバーにインストールする場合は、DSO と WebPass のためのマルチスレッドが必要です。
- Apache Web サーバーを構築するには、パスで gcc コマンドと make コマンドにアクセスできる必要があります。または、別の ANSI 準拠 C コンパイラを使用できます。
- Solaris および Linux プラットフォームの Apache Web サーバーではリバース・プロキシ機能を有効にできます。
- Linux 上の Apache または OHS に対して Oracle Access Manager Web コンポーネントをインストールするとき、Web サーバーを実行しているのと同じユーザーとしてインストールするように求められます。httpd.conf ファイルの User および Group ディレクティブ・エントリを参照してください。

Apache v1.3、OHS および IHS Web サーバーのサポート

Apache v1.3 の最新バージョンには重要なセキュリティの修正が含まれています。最新リリースの Apache 1.3 の使用を強くお薦めします。詳細は、次を参照してください。

```
http://apache.org
```

ベース Apache 1.3 Web サーバーは、ブラウザ接続で SSL（`https://` リクエストへの応答）を使用しません。SSL サポートのためのアドオン・モジュール `mod_ssl` は、次の Web サイトで入手できます。

```
http://www.modssl.org
```

ベース Apache サーバーに対する Oracle Access Manager プラグインは、`mod_ssl` を含む Apache（EAPI 使用とも呼ばれる）のプラグインとは次の点で異なります。

- Oracle Access Manager では mod_ssl を含む Apache のみがサポートされます。

  注意： SSL をサポートするように Apache を構築するときは、`openssl` が `mod_ssl` で必要です。`openssl` は `mod_ssl` を含むように構築される Apache サーバーの一部として必要です。

- Oracle Access Manager の SSL 固有の機能は、Apache-SSL と呼ばれる Apache 1.3 バージョンでは機能しません。

OHS の詳細は、『Oracle HTTP Server 管理者ガイド』を参照してください。Oracle Access Manager 10*g*（10.1.4.0.1）のサポートの詳細は、次の Web サイトの「Certify」タブを参照してください。

```
http://metalink.oracle.com
```

MetaLink の使用手順

1. `http://metalink.oracle.com` に移動します。
2. 指示に従って MetaLink にログインします。
3. 「Certify」タブをクリックします。
4. 「View Certifications by Product」をクリックします。
5. 「Application Server」オプションを選択し、「Submit」をクリックします。
6. 「Oracle Application Server」を選択し、「Submit」をクリックします。

IHS（IBM HTTP Server powered by Apache）は Apache 1.3 の一種です。IHS では異なる実装の SSL が使用されます。Oracle Access Manager では、ベース IHS（非 SSL）と IHS SSL プラグイン・インタフェースの両方をサポートしています。

詳細は、第 2 章「インストールの準備」および 16-7 ページの「ベース Apache Web サーバーのダウンロードとコンパイル」を参照してください。

ベース Apache Web サーバーのダウンロードとコンパイル

この説明は Apache オープン・ソース v1.3 のみに適用されます。Apache 1.3 の最新バージョンは次の Apache Web サイトからダウンロードできます。

```
http://apache.org
```

SSL プラグイン mod_ssl は次の Web サイトで入手できます。

```
http://www.modssl.org
```

これらのサイトには、Apache または mod_ssl で必要なその他のソフトウェア（openssl など）のサイトが示されています。Apache Web サーバーのコンパイル方法は、ソフトウェア・ディストリビューションに含まれています。

Apache Web サーバーで Oracle Access Manager プラグインをサポートするには、モジュール mod-so をサーバー・バイナリにコンパイルする必要があります。

Apache または mod_ssl を含む Apache を mod-so と一緒にコンパイルする手順

1. コンパイルの前に次の構成オプションを含めます。

   ```
   --enable-module=so
   ```

2. 構成が Oracle Access Manager のその他の要件を満たすことを確認し、コンパイルします。

Apache リリース・ノート

次の URL には、最新バージョンの Apache の情報と Apache サーバーのバイナリ・ファイルを入手できるリンクがあります。

```
http://www.apache.org/dist/httpd/Announcement.html
```

その他の役立つリンク

次のリンクでは、Apache リリースの構築やソース・コードに関する情報が提供されます。

- 最新のサポートの詳細は、次のサイトで Oracle*MetaLink* または Oracle Technology Network（OTN）を参照してください。

  ```
  http://metalink.oracle.com.
  ```

  問題の解決方法が見つからない場合は、サービス・リクエストを記録します。

  ```
  http://www.oracle.com/technology/deploy/security/index.html
  ```

- 「Apache source code」: `http://www.apache.org/dist/httpd`
- 「Mod_SSL source code」: `http://www.modssl.org/source/`
- 「OpenSSL source code」: `http://www.openssl.org/source/`
- 「What is ApacheSSL」: `http://www.apache-ssl.org/#What_is_Apache-SSL`
- 「Compiling and Installing Apache 1.3」: `http://httpd.apache.org/docs/install.html`
- 「ApacheSSL build instructions for Win32」: `http://www.galatea.com/flashguides/apache-ssl-win32.xml`
- 「How to build an Apache Unix release」: `http://httpd.apache.planetmirror.com/dev/how-to-release.html`
- 「How to build a release of Apache for Windows」: `http://httpd.apache.planetmirror.com/dev/how-to-release-win32`

プラットフォーム固有のコンパイル・オプション

一部のオペレーティング・システムでは構成時に追加のオプションが必要です。ここに示すオプションの一部は、Apache 1.3 の一部のリリースでは重複する可能性がありますが、それ以外のリリースで必要です。

次に、プラットフォームごとのオペレーティング・システム構成コマンドの環境設定を示します。

Solaris:

```
CFLAGS=-D_REENTRANT
LDFLAGS=-lpthreads
```

AIX:

```
CFLAGS=-D_REENTRANT
LDFLAGS=-lpthreads
```

HP-UX:

```
CFLAGS=-D_REENTRANT
LDFLAGS="-lcl -lpthreads"
```

HP-UX では、PA-RISC1 コンパイル・オプション（デフォルト）を使用する必要があります。PA-RISC2（64 ビット）オプションは使用しないでください。PA-RISC2 を使用すると、「missing symbol」、「bad magic number」、「share object is garbled」のようなロード・エラーを受け取ります。Apache EAPI（mod_ssl）コンパイル済モジュールをプレーンな Apache サーバーにロードすると、どのオペレーティング・システムでも同様のエラーが表示されます。

AIX のためのプラットフォーム固有の実行時設定

AIX では、環境変数 AIXTHREAD_SCOPE を値 S（大文字）に設定する必要があります。そうしないと、ワーカー・プロセスの終了時にセグメント・エラーが発生することがあります。ただし、WebGate によるコンテンツ配信、認証または認可決定には影響しません。

また、AIX では、次のディレクティブを httpd.conf ファイルに指定することをお薦めします。

```
AcceptMutex fcntl
```

このディレクティブがサポートされているのは Apache 1.3.24 以上のみです。WebGate によるコンテンツ配信、認証または認可決定には影響しません。ただし、（/server-status URL を介して）他のプラットフォームでの Apache の動作がよくわかっている場合は、この設定の使用をお薦めします。

Oracle Access Manager Web コンポーネントのインストール順序

Oracle Access Manager Web コンポーネント（WebPass、Policy Manager および WebGate）は特定の順序でインストールする必要があります。次に例を示します。

WebPass
Policy Manager
WebGate

詳細は、1-2 ページの「インストール・タスクの概要」を参照してください。

Oracle Access Manager Web コンポーネントのための Web サーバー構成の更新

Oracle Access Manager Web コンポーネント（WebPass、Policy Manager および WebGate）のインストール時には、Apache Web サーバー構成ファイル（httpd.conf）の手動または自動更新を選択できます。Web サーバー構成ファイルは自動で更新することをお薦めします。httpd.conf の手動更新を選択すると手順が指示されます。

Oracle Access Manager Web コンポーネントをインストールするとき、Web サーバー構成ファイルの場所を指定するように求められます。Apache では httpd.conf のフルパスを入力します。たとえば、httpd.conf ファイルは *Apache_install_dir*/conf ディレクトリにあります。

Oracle Access Manager Web コンポーネントをインストールして Web サーバー構成を最初に更新した後で、httpd.conf ファイルを再更新する必要がある場合、*Component_install_dir*/oblix/apps/common/docs/config.htm の config.htm ファイルを参照してください。または、*Component_install_dir*/oblix/tools/setup/InstallTools/ManageHttpConf にある ManageHttpConf プログラムを使用してください。オプションを指定せずに ManageHttpConf を実行すると、使用方法が表示されます。

Oracle Access Manager Web コンポーネントのための Apache 1.3 のチューニング

Apache 1.3 は、複数の http リクエストを一度に処理するためのプロセス・モデルを使用します。これは、他の Web サーバーで採用されている、複数のリクエストを同時に 1 プロセスで管理するシングル・プロセス（スレッド）モデルとは異なります。Apache の各下位ワーカー・プロセスが、その他の各ワーカー・プロセスの受信 http リクエストに個別に応答します。

Apache サーバー構成ファイル（httpd.conf）のいくつかのパラメータが、Apache サーバーによるワーカー・プロセスの作成または廃棄の決定に影響します。次のパラメータはサーバーのパフォーマンスに影響します。

- **MaxServers:** システムが処理できる同時 http リクエストの数は、システムの最大パフォーマンスによって異なります。
- **Performance Tuning:** システムのパフォーマンス・チューニングは、Apache 提供の ab プログラムなどの http 負荷生成ツールを使用して行う必要があります。
- **MaxSpareServers:** アイドル状態の子サーバー・プロセスの必要な最大数を設定します。アイドル・プロセスとは、リクエストを処理していないプロセスです。`MaxSpareServers` を超えるアイドル・プロセスがある場合、親プロセスが過剰なプロセスを停止します。

  サーバーの状態をできるだけ安定させるには、`MaxSpareServers` に高い値を設定します。この値を最大の 255 に設定すると、すべての Apache ワーカー・プロセスが無制限に使用可能になります。ただし、低負荷時のワーカー・プロセスのリサイクルは行われません。
- **MaxClients:** サポートできる同時リクエスト数の制限を設定します。この数を上回る子サーバー・プロセスは作成されません。`MaxClients` の制限を超えて接続しようとすると、通常は、`ListenBacklog` ディレクティブに基づく数までがキューに入ります。別のリクエストが終了して子プロセスが解放されると、接続が処理されます。
- **MaxClientRequests:** Apache では、ワーカー・プロセスが少しずつ獲得したシステム・リソースが増えすぎて効率が悪くなることを防ぐ安全メカニズムが提供されます。`MaxClientRequests` を 0 より大きな値に設定することで、ワーカー・プロセスが応答できるリクエスト数を制限できます。そのプロセスが終了すると、必要が生じた時点ですぐに新しいワーカー・プロセスに替わられます。この安全メカニズムに問題はありませんが、Oracle Access Manager Web コンポーネント（プラグイン）の起動の遅延が Web ブラウザで認識されます。

  このパラメータを使用する場合は、エンド・ユーザーが起動の遅延に気付かないように十分に高い値を設定してください。Oracle Access Manager プラグインは、この安全メカニズムがなくても Web サーバーで実行するように設計されています。

- **MinSpareServers:** アイドル状態の子サーバー・プロセスの必要な最小数を設定します。アイドル・プロセスとは、リクエストを処理していないプロセスです。アイドル・プロセスが MinSpareServers よりも少ない場合、親プロセスは、最高で 1 秒当たり 1 つのペースで新しい子プロセスを作成します。このパラメータは Policy Manager で使用します。

  注意： このディレクティブを値 *m* に設定すると、*n* 個のアクティブ・クライアント・リクエストがある場合に、少なくとも *n* + *m* 個の httpd プロセスが必ず実行されます。

  Oracle Access Manager プラグインの初期化が最初のリクエストまで行われないという事実のため、`MinSpareServers` パラメータに高い値を設定しても最小限の利点しか得られません。ただし、このパラメータはできるだけ高い値にしておくと役立ちます。専用 Web サーバー・システムの場合は、この設定によって非常に高い負荷が発生することはありません。

- **StartServer:** MinSpareServers パラメータの場合と同じく、StartServers パラメータの利点は Oracle Access Manager プラグインの初期化遅延のために限られます。

ここで説明したパラメータの適切な値は、予期される負荷や関連するシステム（Access Server や LDAP サーバーなど）のパフォーマンス・クラスによって異なります。

非常に高いパフォーマンスのシステムで高負荷が予想される場合は、ワーカー・プロセス数の制限を高くして Apache サーバーを再コンパイルできます。このようなシステムでは、瞬間的な負荷の急上昇に対処する際に、StartServers パラメータや MinSpareServers パラメータによるパフォーマンスへの大きな影響を確認できます。

場合によっては、Access Server を適切に運用できるようにオペレーティング・システムの制限を調整する必要があります。特に、1 つの Access Server で使用できるファイル記述子の最大数はデフォルト値よりも増やすことをお薦めします。各 Apache ベース WebGate と 1 つの Access Server の間に複数の接続を構成すると、すぐにデフォルト制限を上回ります。

Policy Manager のチューニング・ファクタ

Policy Manager のパフォーマンスは、Apache と Policy Manager 両方の構成パラメータの影響を受けることがあります。Apache に対して Policy Manager をチューニングする際には次のファクタを考慮する必要があります。

- アイドル状態の子プロセスがあると、新しい受信リクエストがすぐに処理されます。予備の子プロセスが多いほど、処理の開始が速くなります。
- 各子プロセスはディレクトリ・サーバーに対して別の接続を開きます。子プロセスが多いほど、ディレクトリ・サーバーとの接続も多くなります。

各ユーザーが 1 つのブラウザを使用すると仮定すると、イメージ、js、HTML に対する 4 ～ 5 個の同時リクエストがブラウザから Web サーバーに送られます。同時ユーザーが 4 名と仮定すると、Web サーバーに対する同時リクエストの合計数は 20（4 * 5）になります。

このようなファクタがある場合、新しいユーザーを処理する速さとディレクトリ・サーバーの接続数のバランスを取るためには、次の設定をお薦めします。

- `MaxClients` = 25
- `MinSpareServers` = 4
- `MaxSpareServers` = 5

注意： Policy Manager は Web サーバーの起動時には接続を開きません。Policy Manager は最初のリクエスト時に接続を作成します。

Policy Manager が接続を作成するときの遅延を埋め合せるために、すべてのディレクトリ・サーバー・プロファイルですべてのディレクトリ・サーバー接続を 1 に設定するように Policy Manager を構成できます。この場合、次のように Apache を構成できます。

- `MinSpareServers` = 1
- `MaxSpareServers` = 2
- `MaxServers` = 2

このように設定すると、Policy Manager は、最初のリクエストでの遅延があったとしても適切な速さで応答します。

OHS クライアント証明書の設定

cert_decode および credential_mapping プラグインを使用するときは、`+EarlierEnvVars` と `+ExportCertData` を OHS Web サーバー構成ファイルの既存の SSL オプションに追加して、アクセス・システム・クライアント証明書の認証スキームが、SSL 対応 OHS で適切に作動することを確認する必要があります。次に例を示します。

credential_mapping:

```
obMappingBase="o=company,c=us",obMappingFilter=
"(&(objectclass=InetOrgPerson)(mail=%certSubject.E%))"
```

ssl.conf に次のオプションを指定する必要があります。

```
SSLOptions +StdEnvVars +ExportCertData +EarlierEnvVars
```

ssl オプションを追加する手順

1. OHS Web サーバーの構成ファイルを探して、テキスト・エディタで開きます。次に例を示します。

   $ORACLE_HOME/Apache/Apache/conf/ssl.conf

2. ssl.conf ファイルの既存の SSL オプションに次の情報を追加します。次に例を示します。

   ```
   SSLOptions +StdEnvVars +ExportCertData +EarlierEnvVars
   ```

3. ファイルを保存して Web サーバーを再起動します。

Oracle Access Manager Web コンポーネントのための OHS のチューニング

OHS に対して Oracle Access Manager Web コンポーネントをインストールした後で、次の手順を実行する必要があります。

注意： 前に説明したように、OHS に対して Oracle Access Manager Web コンポーネントをインストールする前に、コンポーネントをインストールするユーザーと一致するように httpd.conf ファイルでユーザーとグループを変更してください。

Oracle Access Manager Web コンポーネントのために OHS をチューニングする手順

1. opmn を停止します。
2. opmn.xml ファイルで項目を次のように調整します。

```
<ias-component id="HTTP_Server">
<process-type id="HTTP_Server" module-id="OHS2">
         <environment>
                <variable id="LD_ASSUME_KERNEL" value="2.4.19"/>
         </environment>
          <module-data>
            <category id="start-parameters">
              <data id="start-mode" value="ssl-disabled"/>
            </category>
          </module-data>
          <process-set id="HTTP_Server" numprocs="1"/>
        </process-type>
      </ias-component>
```

3. Policy Manager の httpd.conf ファイルで、次の行をコメントにします。

```
#LoadModule perl_module modules/mod_perl.so
#LoadModule php4_module modules/mod_php4.so
```

Web サーバーの起動と停止

次の項では、UNIX および Windows での Apache サーバーの実行に関する情報を説明します。

- OHS Web サーバーの起動と停止
- UNIX での Apache の起動と停止
- Windows での Apache の起動と停止

OHS Web サーバーの起動と停止

OHS Web サーバーの起動と停止は、v1.3 と v2 の両方ともすべてのプラットフォームで同じ手順です。

OHS Web サーバーを起動する手順

1. 次のディレクトリを探して移動します。

   $ORACLE_HOME¥opmn¥bin¥

2. コマンドラインで次のコマンドを入力します。

```
opmnctl/startproc process-type=HTTP_Server
```

OHS Web サーバーを停止する手順

1. 次のディレクトリを探して移動します。

   $ORACLE_HOME¥opmn¥bin¥

2. コマンドラインで次のコマンドを入力します。

```
opmnctl/stopproc process-type=HTTP_Server
```

UNIX での Apache の起動と停止

次に示すように、通常、Apache Web サーバーの起動または停止には 1 つの手順を実行します。

UNIX での Apache Web サーバーの停止

UNIX で Apache Web サーバーを停止するには、次のようにします。

1. *Apache_install_dir*/bin ディレクトリに移動します。
2. コマンドラインで次のように `apachectl stop` コマンドを使用してサーバーを停止します。

```
./apachectl stop
```

UNIX での Apache Web サーバーの起動と停止

UNIX で Apache Web サーバーを起動および停止するには、次のようにします。

1. *Apache_install_dir*/bin ディレクトリに移動します。
2. コマンドラインで次のように `apachectl` コマンドを使用して、サーバーを停止して再起動します。

```
./apachectl start
```

SSL モードでのサーバーの起動

SSL モードでサーバーを起動するには、次のようにします。

1. *Apache_install_dir*/bin ディレクトリに移動します。
2. コマンドラインで次のように `apachectl startssl` コマンドを使用して、SSL モードでサーバーを起動します。

```
./apachectl startssl
```

Windows での Apache の起動と停止

Apache Web サーバーを起動する方法は、Windows サービスとして実行するか、アプリケーションとして実行するかによって異なります。次の手順を参照してください。

アプリケーションとして実行す Web サーバーを停止する手順

1. Windows のコマンドラインで、[Ctrl] キーを押しながら文字 [c] を入力します。

Windows サービスとして実行する Web サーバーを停止する手順

1. Windows の「サービス」ウィンドウで、Web サーバーのサービス名を探します。
2. 「サービスの停止」アイコンをクリックします。

Windows サービスとして実行する Web サーバーを起動する手順

1. *Apache_install_dir*/bin ディレクトリに移動します。
2. コマンドラインに次のコマンドを入力します。

```
apache.exe -k start
```

アプリケーションとして実行する Web サーバーを起動する手順

1. Windows の「サービス」ウィンドウで、Web サーバーのサービス名を探します。
2. 「サービスの開始」アイコンをクリックします。

17

Oracle Access Manager のための Apache v2、IHS および OHS Web サーバーの構成

Oracle Access Manager では、Apache v2 Web サーバー、IBM HTTP Server（IHS）powered by Apache v2 および Oracle HTTP Server（OHS）に対応する Web コンポーネント（Policy Manager、WebPass および WebGate）を提供しています。

この章では、3 種類の Web サーバーの構成を詳しく説明します。

OHS と Oracle Access Manager について

OHS2 は Internet Web サーバーの拡張機能です。これは、オープン・ソース Apache v2 に基づく Oracle HTTP Server（OHS）と通信する Oracle Access Manager Web コンポーネントを識別します。Oracle Access Manager 10*g*（10.1.4.0.1）によって、Linux プラットフォームや Windows プラットフォーム上のスタンドアロン Oracle HTTP Server にインストールできる WebPass、Policy Manager（以前の Access Manager）および WebGate コンポーネントが提供されます。

Linux: Oracle_Access_Manager10_1_4_0_1_linux_OHS2_WebPass
Linux: Oracle_Access_Manager10_1_4_0_1_linux_OHS2_Access_Manager
Linux: Oracle_Access_Manager10_1_4_0_1_ linux_OHS2_WebGate

Windows: Oracle_Access_Manager10_1_4_0_1_ Win32_OHS2_WebPass
Windows: Oracle_Access_Manager10_1_4_0_1_Win32_OHS2_Access_Manager
Windows: Oracle_Access_Manager10_1_4_0_1_ Win32_OHS2_WebGate

OHS Web コンポーネントはどのアプリケーションでも使用できます。ただし、場合によっては OHS Web コンポーネントを使用する必要があります。次に例を示します。

- OHS WebGate を Oracle Single Sign-On と統合できるようにするには、『Oracle Access Manager 統合ガイド』の説明に従って Oracle Application Server にインストールする必要があります。インストール時に、WebGate は OHS にモジュールとしてインストールされます。
- OHS WebPass および OHS Access Manager（Policy Manager）コンポーネントは、Oracle Application Server で使用できます。ただし、Apache WebPass と Apache Policy Manager もこのアプリケーションに対してサポートされます。

OHS2 Web コンポーネントは Apache v2 に基づいています。次のような OHS の詳細は、『Oracle HTTP Server 管理者ガイド』を参照してください。

- オラクル社による実装と、基礎になっているオープン・ソース Apache 製品の違い
- Oracle HTTP Server のディレクトリ構造、構成ファイル、構文、モジュール、ディレクティブ
- サーバー・プロセス、ネットワーク接続およびセキュリティ機能の管理

17-9 ページの「Web サーバーの準備」で説明している OHS Web コンポーネントの要件を確認してください。

Apache および IHS v2 Web コンポーネントでの Oracle Access Manager について

Oracle Access Manager では、Oracle HTTP Server だけでなく、Apache v2 Web サーバーや IBM HTTP Server にもコンポーネントが提供されます。IBM HTTP Server（IHS）は Apache v2 の一種です。特に明記しないかぎり、この後の情報は 3 種類すべてに適用されます。

- Apache v2.0.5.2 対応の 10*g*（10.1.4.0.1）WebPass、Policy Manager および WebGate
- Apache v2.0.48 対応の 10*g*（10.1.4.0.1）WebGate（リバース・プロキシをアクティブ化可能）
- IBM HTTP Server（IHS）powered by Apache v2.0.47 対応の 10*g*（10.1.4.0.1）WebGate（リバース・プロキシをアクティブ化可能）

注意： 最新のサポート情報は、次のサイトの「Certify」タブを参照してください。

`http://metalink.oracle.com`

プラットフォーム固有の各インストール・パッケージでは、プレーン Apache モードと SSL 対応 Apache モードの両方がサポートされています。次に例を示します。

AIX: Oracle_Access_Manager10_1_4_0_1_power-aix_IHS2_WebGate

Linux: Oracle_Access_Manager10_1_4_0_1_linux_Apache2_Access_Manager

Linux: Oracle_Access_Manager10_1_4_0_1_ linux_Apache2_WebGate

Linux: Oracle_Access_Manager10_1_4_0_1_linux_Apache2_WebPass

Solaris: Oracle_Access_Manager10_1_4_0_1_sparc-s2_Apache2_WebGate

Windows: Oracle_Access_Manager10_1_4_0_1_Win32_APACHE2_WebGate

以前の Oracle Access Manager のリリースでは、プラットフォーム固有のインストール・パッケージはプレーン・モードと SSL 対応モードに分かれていました。たとえば、プラットフォームごとに、APACHE_WebGate と APACHESSL_WebGate のように 2 つの WebGate ファイルが用意されていました。

これらの Web サーバーをサポートするための Oracle Access Manager コンポーネントの機能の変更はありません。Oracle Access Manager の認証は、HTTP Basic、フォームまたは SSL クライアント証明書を使用して WebGate を介して行われます。認証されたユーザーによる Web リソースの認可や、他の Web サーバーまたはアプリケーションとのシンプル・ドメイン SSO またはマルチ・ドメイン SSO も、WebGate を介して行われます。

重要： この章の情報は WebGate を中心に説明しています。ただし、Policy Manager コンポーネントおよび WebPass コンポーネントにも同じく適用されます。

Apache HTTP サーバーについて

Apache HTTP サーバーは、Apache Software Foundation のオープンソース HTTP サーバー・プロジェクトです。プロジェクトの目標は、現行の HTTP 標準を満たす、セキュアで効率が高い拡張可能なサーバーと HTTP サービスを提供することです。

詳細は、17-5 ページの「Apache v2 アーキテクチャと Oracle Access Manager について」を参照してください。

IBM HTTP Server について

IBM HTTP Server（IHS）は Apache v2 の一種です。IBM HTTP Server の一部は、Apache Group によって開発されたソフトウェアに基づいています。IBM HTTP Server コンポーネントには、OpenSSL プロジェクトで開発されたソフトウェアや Eric Young によって開発されたソフトウェアも含まれます。

1-3 ページの「Apache v2 アーキテクチャと Oracle Access Manager について」で説明した Apache アーキテクチャおよび Oracle Access Manager の詳細は IHS にも適用されますが、次の例外があります。

- 以前のバージョンの IHS では、mod_ibm_ldap モジュールを使用するために別の IDS クライアントが必要でした。IHS powered by Apache v2.0.47 ではこの要件はありません。
- IHS v2.0.47 は FIPS 140-2 をサポートしています。FIPS のサポートはデフォルトでは無効になっています。FIPS サポートを有効にするには、SSLFIPSEnable ディレクティブを httpd.conf ファイルに追加します。FIPS サポートを無効にする場合も、同様に SSLFIPSDisable ディレクティブを使用します。
- AIX では、IHS v2.0.47 をインストールする前に適切なランタイム・ライブラリがインストールされていることを確認します。

たとえば、AIX 5.1 では、IHS v2.0.47 をインストールする前に xlC.rte 6.0 ランタイム・ライブラリ（xlC.rte.6.0.0.0 など）をインストールする必要があります。このライブラリは、SSL をインストールして IHS v2 で使用する場合に AIX に必要です。このライブラリは次の Web サイトからダウンロードできます。

```
http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp
```

Apache と IBM HTTP リバース・プロキシ・サーバーについて

通常、リバース・プロキシは次の状況で使用されます。

- ファイアウォールで保護されたサーバーにインターネット・ユーザーがアクセスできるようにする場合
- いくつかのバックエンド・サーバーでロード・バランスを行う場合、または速度が遅いバックエンド・サーバーにキャッシングを提供する場合
- いくつかのサーバーを同じ URL 空間に入れる場合

proxy_module は、Apache および IHS powered by Apache のプロキシやゲートウェイを実装します。クライアントには特別な構成は必要ありません。リバース・プロキシは通常の Web サーバーと変わりません。クライアントは、いつものように、リバース・プロキシのネームスペースにコンテンツをリクエストします。そのようなリクエストの送信先を決定するのがリバース・プロキシです。コンテンツが返されるときにはリバース・プロキシが発信元のように見えます。

重要： proxy_module を使用して、FTP、CONNECT（SSL 用）、HTTP/0.9、HTTP/1.0 および HTTP/1.1 のプロキシ機能を実装できます。ただし、WebGate でサポートされるのはリバース・プロキシ機能のみです。

詳細は、17-8 ページの「Apache v2 Web サーバーの要件」を参照してください。

Apache v2 アーキテクチャと Oracle Access Manager について

Apache v2 Web サーバーは、スレッド・セーフの Oracle Access Manager ライブラリと互換性のある、マルチスレッドおよびマルチプロセスのハイブリッド・アーキテクチャを提供します。

重要 : 特に明記しないかぎり、この説明の詳細すべては、Apache v2 および IHS v2 Web サーバー、Policy Manager、WebPass、WebGate に同様に適用されます。

標準のモジュール・セットの他に、Apache v2 Web サーバーにはマルチプロセス・モジュール（MPM）が含まれています。これによって、マシンのネットワーク・ポートをバインドし、リクエストを受け入れて処理します。Apache または IHS v2 に対して Oracle Access Manager コンポーネントをインストールする前に、次のように適切な MPM をサーバーにコンパイルしてアクティブ化する必要があります。

- **Windows の場合 :** mpm_winnt は Windows プラットフォームのデフォルト MPM です。mpm_winnt は、Apache 1.3 で使用される POSIX レイヤーのかわりにネイティブのネットワーク機能を使用できます。
- **UNIX の場合 :** プリフォーク MPM は、UNIX プラットフォームでの Apache v2 Web サーバーのデフォルト MPM です。プリフォーク MPM は、Apache v1.3 と似た方法でリクエストを処理する、非スレッドのプリフォーク Web サーバーを実装します。

注意 : UNIX 上の Apache を mpm_worker_module とコンパイルする場合、UNIX 環境用の Apache ソースの thread.c ファイルを 17-35 ページの「ヒントとトラブルシューティング」の説明に従って変更する必要があります。

- **AIX の場合 :** ワーカー MPM は、AIX プラットフォームでの IHS v2 のデフォルト MPM です。ワーカー MPM は、マルチプロセスとマルチスレッドのハイブリッド・サーバーを実装します。この MPM を制御するために使用される最も重要なディレクティブは、ThreadsPerChild と MaxClients です。詳細は、17-33 ページの「Oracle Access Manager Web コンポーネントのための Apache または IHS v2 のチューニング」を参照してください。

Apache v2 Web サーバーには、Apache Portable Runtime（APR）ライブラリが含まれています。これは、プラットフォーム固有の実装のためのインタフェースを提供します。これにより、プラットフォームの種類にかかわらず同一ではないまでも予測可能な動作が API 開発者に保障され、条件付きコンパイル #lfdefs のニーズが解消されます。下位互換性は include/apu_compat.h ファイルでサポートされますが、Apache v2 APR の使用をお薦めします。

詳細は、Apache v2 のドキュメントを参照してください。17-33 ページの「Oracle Access Manager Web コンポーネントのための Apache または IHS v2 のチューニング」も参照してください。

次の項で説明しますが、Apache アーキテクチャは様々な方法で Oracle Access Manager コンポーネントに影響しています。詳細は、17-6 ページの「互換性とプラットフォームのサポート」を参照してください。

Apache v1.3 および v2 に対してインストールされる WebPass の場合

- 各 WebPass インスタンスが Identity Server に接続します。
- 各接続がシステム・ソースを利用し、それぞれが n 個のファイル記述子を使用します。
- Apache がプロセスの起動と停止を頻繁に行わずにすむように、Apache のチューニング・パラメータを設定する必要があります。Oracle Access Manager の使用に関係なくこの設定は同じです。

Apache v1.3 および v2 に対してインストールされる Policy Manager の場合

- 各 Web サーバー・プロセスは Policy Manager アプリケーションのインスタンスです。
- 各アプリケーションは、ディレクトリ・サーバーに対して独自の接続を保持します。これはパフォーマンスには直接影響しません。ただし、ディレクトリ・サーバー側に制限が生じることがあります。他のディレクトリ・サーバー・クライアントが関係する場合には考慮してください。
- 複数のプロセスが 1 ユーザーのリクエストに応答します（フレームを構築するために複数の HTTP イベントがトリガーされます）。
- レスポンスの待機時間は予測できません。
- UI の観点ではプロセス数が少ない方が望ましいが、同時ユーザー数が影響を受けます。

IHS、Apache v1.3 および v2 に対してインストールされる WebGate の場合

- プロセス間の共有キャッシュはありません。
- 各プロセスは、Access Server との独自の接続を保持します。このため、WebGate の接続数を制限する必要があります。この問題は、Web サーバーと Access Server を実行するシステムのパフォーマンスの影響を部分的に受けます。

注意： Apache v2（および Apache v2 に基づくその他の製品）に対応する WebGate は、他の Web サーバーに対応する他の WebGate、WebPass および Policy Manager コンポーネントを含むインストールで使用できます。

Apache および IHS v2 Web サーバーの制限事項

Apache v2 Web サーバーの制限のため、Oracle Access Manager フォームベース認証スキーム用に構成されたプラグインは、次の状況では変数を渡すことができません。

- オプションのチャレンジ・パラメータ passthrough:Yes が、ログイン資格証明を後処理プログラムに渡すために認証スキームに含まれている場合
- フォームのアクションが、渡されるヘッダーと変数をすべてダンプする CGI スクリプトであり、メソッドが HTTP POST メソッドを使用してコールされる場合

次に例を示します。

```
<html>
<form name="myloginform" action="/access/...cgi" method="post">
```

互換性とプラットフォームのサポート

最新のサポート情報は、次のサイトの「Certify」タブを参照してください。

```
http://metalink.oracle.com
```

Apache v2、OHS2 および IHS v2 に対応する Oracle Access Manager Web コンポーネントは、インストール内の 1 つの WebGate とすることも、他の WebGate と混在させることも可能です。詳細は、2-7 ページの「アクセス・システムのガイドライン」を参照してください。

OHS、IHS または Apache v2 Web サーバーの要件

Oracle Access Manager 10*g*（10.1.4.0.1）の HTML ページでは UTF-8 エンコーディングが使用されます。Apache ベースの Web サーバー（Apache、Oracle HTTP Server（OHS）、IBM HTTP Server（IHS）など）では、管理者が `AddDefaultCharset` ディレクティブを使用して、送出されるすべての HTML ページのデフォルト・キャラクタ・セットを指定できます。このディレクティブは、HTML ページを生成するアプリケーションで指定されるすべてのキャラクタ・セットよりも優先されます。`AddDefaultCharset` ディレクティブで UTF-8 以外のキャラクタ・セットを有効にすると、Oracle Access Manager の HTML ページは文字化けします。

Oracle Access Manager 10*g*（10.1.4.0.1）HTML ページを正しく表示するには、`AddDefaultCharset` ディレクティブを Web サーバー構成ファイル（httpd.conf）に次のように指定することをお薦めします。

```
AddDefaultCharset Off
```

このディレクティブの詳細は、Web サーバーのドキュメントを参照してください。

次の項目では、注意する必要があるその他の事項について説明します。

- Linux での OHS Web サーバーの準備
- Linux および Windows プラットフォームでの OHS Web サーバーの準備
- OHS クライアント証明書の設定
- IHS2 Web サーバーの要件
- Apache および IHS v2 リバース・プロキシ・サーバーの要件
- Apache v2 Web サーバーの要件

重要： 特に明記しないかぎり、ここに示す情報は、WebPass、Policy Manager および WebGate コンポーネントに同じように適用されます。

IHS2 Web サーバーの要件

ここでは、Oracle Access Manager のための IHS v2 固有の要件を説明します。IHS v2 では、バイナリを得るためにソース・コードをコンパイルすることはありません。ただし、次の要件が IHS v2 Web サーバーに適用されます。

- AIX での SSL 対応構成では、xLC.rte.6.0 ランタイム・ライブラリが必要です。
- SSL 対応構成では GSKit7 が必要です。これは、`https://techsupport.services.ibm.com/server/aix.fdc` からダウンロードできます。

Apache および IHS v2 リバース・プロキシ・サーバーの要件

前に説明したように、proxy_module によってプロキシやゲートウェイが実装されます。クライアントには特別な構成は必要ありません。proxy_module を使用して、FTP、CONNECT（SSL 用）、HTTP/0.9、HTTP/1.0 および HTTP/1.1 のプロキシ機能を実装できますが、特定の Oracle Access Manager Apache および IHS v2 WebGate ではリバース・プロキシ機能しかサポートされません。詳細は、17-6 ページの「互換性とプラットフォームのサポート」を参照してください。

Apache Web サーバーの場合 : Oracle Access Manager でリバース・プロキシ機能を使用するには、構成コマンドにプロキシ・モジュールを含める必要があります。次に例を示します。

--enable-proxy: Apache プロキシ・モジュール

--enable-proxy-connect: Apache プロキシ CONNECT モジュール

--enable-proxy-ftp: Apache プロキシ FTP モジュール

--enable-proxy-http: Apache プロキシ HTTP モジュール

また、mod_proxy モジュールと mod_proxy_http モジュールをサーバーに動的にロードする必要があります。リバース・プロキシをアクティブ化するには、ProxyPass ディレクティブ、または RewriteRule ディレクティブの [P] フラグを使用します。

IHS Web サーバーの場合 : IHS Web サーバーをインストールした後で、次のディレクトリにある httpd.conf ファイルのリバース・プロキシ構成を完了する必要があります。

IHS_install_dir/conf ディレクトリ

詳細は、17-21 ページの「リバース・プロキシのアクティブ化」を参照してください。

Apache v2 Web サーバーの要件

ここでは、Oracle Access Manager のための Apache v2 固有の要件を説明します。詳細は Apache のドキュメントを参照してください。

PATH 変数 : UNIX システムでは、Apache v2 をコンパイルする前に、PATH 変数に gcc の場所を指定する必要があります。ただし、Sun C コンパイラの場所は PATH 変数に指定しないでください。Windows システムでは、コマンドライン・ツールまたは Visual Studio IDE Workbench を使用して Apache を構築できます。コマンドラインでの構築には、PATH、INCLUDE、LIB およびその他の変数に環境が反映されていることが必要です。これらは、vcvars32 バッチ・ファイルで構成できます。

マルチプロセス・モジュール（MPM）: Apache v2 では、マシンのネットワーク・ポートをバインドし、リクエストを受け入れて処理するために、デフォルトの MPM が各プラットフォームに提供されています。Apache は一度に 1 つの MPM を使用する必要があります。コンパイル時に MPM が選択されていない場合、デフォルトの MPM が Web サーバーにロードされます。コンパイル時に MPM をアクティブ化できます。

mod_ssl: Oracle Access Manager は、SSL 対応通信の有無に関係なく Apache をサポートしています。ベース Apache Web サーバーは、ブラウザ接続には SSL を使用せず、HTTPS リクエストには応答しません。SSL 対応通信では、Oracle Access Manager は mod_ssl を含む Apache のみをサポートします。Oracle Access Manager の SSL 固有機能は Apache-SSL では作動しません。

mod_ssl は OpenSSL に依存して、暗号エンジンを提供します。mod_ssl は OpenSSL ライブラリのインタフェースを提供します。OpenSSL ライブラリは、Secure Sockets Layer プロトコルと Transport Layer Security プロトコルを使用して Strong Encryption を提供します。

以前のバージョンの Apache では、mod_ssl モジュールを個別にダウンロードしてサーバーにコンパイルする必要がありました。Apache HTTP サーバー v2 の場合、モジュール mod_ssl は、構成時に有効にできるロード可能なモジュールとして提供されています。

マルチスレッド : マルチスレッドは、Apache v1.3.27 以上に対する WebPass のインストールに必要です。Apache v2 対応の WebGate は、Apache 1.3.27 以上の Web サーバーに対応する WebPass、Policy Manager および WebGate を含む Oracle Access Manager インストールで使用できます。

動的共有オブジェクト（DSO）: DSO のサポートはすべての Oracle Access Manager プラグイン（WebGate および WebPass）で必要です。基本的なコア・サーバー機能を拡張する Apache モジュールは、Apache バイナリに永続的に組み込むために静的にコンパイルするか、動的にコンパイルして個別に格納し、実行時に再コンパイルせずにロードすることができます。Apache v1.3 では、mod_so はコンパイルする必要がありました。Windows システムの Apache v2 では、mod_so はベース・モジュールであり必ず含まれています。UNIX の Apache v2 では、通常、ロードされるコードは共有オブジェクト・ファイルに含まれます。

注意： 動的にロードした Apache 1.3 モジュールを Apache v2 で直接使用することはできません。Apache v2 に動的にロードしたり、Apache v2 にコンパイルしたりするには、Apache v1.3 モジュールを変更する必要があります。

---

mod_perl: mod_perl によって、Perl プログラミング言語が Apache Web サーバーに埋め込まれます。Perl がなくても Apache v2 を構築してインストールできますが、Perl で記述されたサポート・スクリプトを使用できません。

注意： Apache v.1.3.2x の場合、一部のオペレーティング・システムでは構成時に追加のオプションが必要でした。Apache v2 を構築する場合、追加の変数を設定する必要はありません。

Web サーバーの準備

Oracle Access Manager Web コンポーネントのためにホスト・マシンを準備する方法と手順は、特定の Web サーバーおよびプラットフォームによって異なります。タスクの概要について次に説明します。

Oracle Access Manager でリバース・プロキシ機能を使用するには、17-4 ページの「Apache と IBM HTTP リバース・プロキシ・サーバーについて」で説明したように構成コマンドにプロキシ・モジュールを含める必要があります。17-21 ページの「リバース・プロキシのアクティブ化」も参照してください。

タスクの概要 : Web サーバーの準備と Oracle Access Manager のインストール

1. 次に説明するように、IHS v2 Web サーバーをインストールするか、Apache v2 Web サーバーをコンパイルしてインストールします。
   - IHS v2 Web サーバーの準備
   - Linux での Apache および OHS Web サーバーの準備
   - Linux での OHS Web サーバーの準備
   - Linux および Windows プラットフォームでの OHS Web サーバーの準備
   - OHS クライアント証明書の設定
   - UNIX での Apache v2 Web サーバーの準備
   - AIX での Apache v2 SSL Web サーバーの準備
   - Windows での Apache v2 Web サーバーの準備
2. 必要であれば、17-21 ページの「リバース・プロキシのアクティブ化」の説明に従ってリバース・プロキシ機能をアクティブ化します。
3. このガイドの該当する項目の説明に従って Oracle Access Manager コンポーネントをインストールします。
4. 17-26 ページの「Oracle Access Manager Web コンポーネントに関する httpd.conf 更新の確認」の説明に従って、Web サーバーの構成を完了します。
5. 17-33 ページの「Oracle Access Manager Web コンポーネントのための Apache または IHS v2 のチューニング」を参照してください。

注意： この後のすべての手順で、パス名の変数、モジュールおよびオプションは手順を説明するための例です。これらは環境によって異なります。詳細は、Web サーバーのドキュメントを参照してください。

IHS v2 Web サーバーの準備

IHS v2 対応の WebGate を受け入れて使用するように IHS v2 Web サーバーを準備するには、環境と要件によって異なりますが、次の 1 つ以上の手順を実行する必要があります。

- IHS v2 インストールのためのホストの準備
- IBM HTTP Server v2 のインストール
- SSL 機能の設定
- セキュアな仮想ホストの起動
- リバース・プロキシのアクティブ化

適切な手順を完了すると、IHS v2 対応 WebGate をインストールできるようになります。

IHS v2 インストールのためのホストの準備

IHS Web サーバーをインストールする前に、次の手順を実行してホスト・マシンを設定する必要があります。詳細は、17-7 ページの「IHS2 Web サーバーの要件」および 17-8 ページの「Apache v2 Web サーバーの要件」を参照してください。

この例では AIX 5.1 でのインストールを示します。これらは環境によって異なります。

IHS v2 のインストールを準備する手順

1. ホスト・マシンで、IBM Developer Kit および Java Technology Edition version 1.4 を次のサイトからダウンロードしてインストールします。

   ```
   http://www.ibm.com/java/jdk
   ```

   IBM Developer Kit には WebSphere アプリケーション・サーバーが含まれています。また、このサイトから WebSphere アプリケーション・サーバーをダウンロードすることもできます。

2. ホスト・マシンで、次のサイトから AIX 5.1 用の xlC.rte 6.0 ランタイムをダウンロードしてインストールします。これは GSKit7 ランタイム実行可能ファイルで必要になります。

   ```
   https://techsupport.services.ibm.com/server/aix.fdc
   ```

3. ホスト・マシンに、IBM HTTP Server インストール・イメージを圧縮解除するための新しいディレクトリを作成します。

4. ホスト・マシンで、次の Web サイトから IBM HTTP Server インストール・イメージをダウンロードします。

   ```
   http://www-306.ibm.com/software/webservers/httpservers/
   ```

5. ホスト・マシンの新しいディレクトリでインストール・イメージを圧縮解除します。

   次に例を示します。

   ```
   tar -xf IHS.tar
   ```

   オペレーティング・システムによって異なりますが、次のようなファイル・リストが表示されます。

   ```
   gskit.sh
   setup.jar
   gskta.rte (a GSKit runtime executable for AIX)
   ```

   次の説明に従ってインストールを開始する準備ができました。

6. 17-11 ページの「IBM HTTP Server v2 のインストール」に進みます。

IBM HTTP Server v2 のインストール

この後の手順では、IBM HTTP Web Server の典型的なインストールを、順を追って説明します。あるいは、サイレント・インストールの実行を選択することもできます。その場合、silent.res ファイルを `java -jar setup.jar` -silent -options silent.res コマンドで使用します。silent.res テキスト・ファイルを編集してサイレント・インストールのオプションをカスタマイズできます。すべてのオプションはデフォルトでは true に設定されています。オプションを無効にする場合は値を false に設定します。

IBM HTTP Web Server powered by Apache v2 をインストールする手順

1. 前の例でマシンにインストールした Java Technology Edition version 1.4 を指すようにパスを設定します。次に例を示します。

   ```
   export PATH=$PATH:/usr/java14/java/bin
   ```

2. インストール・イメージを圧縮解除したディレクトリで、次のコマンドを入力します。

   ```
   java -jar setup.jar
   ```

3. インストールを実行する際の言語を選択します。

   「Welcome to the InstallShield Wizard for the IBM HTTP Server」が表示されます。

4. 「Next」をクリックして「Welcome」画面を閉じます。

5. ディレクトリ名を指定します。次に例を示します。

   ```
   AIX: /usr/IBMIHS/
   ```

6. 「Next」をクリックして続行します。

   標準、カスタムまたは開発者向けのインストール・オプションが表示されます。標準インストールを選択すると、組み込まれる内容すべてを含むリストとイメージのサイズが表示されます。カスタム・インストールを選択すると、コンポーネント・リストが表示されます。インストールしないコンポーネントは横のボックスからチェックを外します。

7. 実行するインストールのタイプを選択して、「Next」をクリックします。次に例を示します。

   ```
   Typical
   ```

   次のメッセージが表示されます。「Cancel」をクリックしてインストールを停止できます。

   ```
   Installing IBM HTTP Server. Please wait.
   ```

   次のメッセージも表示されます。「Cancel」をクリックしてインベントリの更新を停止できます。

   ```
   Updating the inventory.
   ```

8. 「Finish」をクリックしてインストールを完了します。

9. 次のように apachectl コマンドを使用して、IHS サーバーを停止して起動します。

   たとえば、次のようにします。

   ```
   IHS2_install_dir/bin
   ./apachectl stop
   ./apachectl start
   ```

   IHS2_install_dir は、IHS v2 Web サーバーをインストールしたディレクトリです。

IHS v2 対応 WebGate のインストールの前または後に、IHS v2 Web サーバーを次のモードで構成できます。

- SSL 機能の設定
- セキュアな仮想ホストの起動
- リバース・プロキシのアクティブ化
- Oracle Access Manager Web コンポーネントのインストール

SSL 機能の設定

SSL 機能を設定する必要がある場合は、IHS v2 対応 WebGate のインストールの前または後に次の手順を実行します。

デフォルト構成ファイルを使用して IHS v2 の SSL を設定する手順

1. 次のファイルを探して開きます。

   IHS2_install_dir/conf/httpd.conf

2. SSLEnable ディレクティブを指定して SSL を有効にします。
3. Keyfile ディレクティブと、有効にするその他の SSL ディレクティブを指定します。
4. 次のように IHS サーバーを停止してから起動します。たとえば、次のようにします。

   ```
   IHS2_install_dir/bin
   ./apachectl stop
   ./apachectl start
   ```

   IHS2_install_dir は、IHS v2 Web サーバーをインストールしたディレクトリです。

5. 次の手順に進みます。
   - セキュアな仮想ホストの起動
   - リバース・プロキシのアクティブ化
   - Oracle Access Manager Web コンポーネントのインストール

セキュアな仮想ホストの起動

セキュアな仮想ホストを起動する必要がある場合は、IHS v2 対応 WebGate のインストールの前または後に次の手順を実行します。

IHS v2 のセキュアな仮想ホストを起動する手順

1. 次のファイルを探して開きます。

   ```
   IHS2_install_dir/conf/httpd.conf
   ```

   IHS2_install_dir は、IHS v2 Web サーバーをインストールしたディレクトリです。

2. SSLEnable ディレクティブを構成ファイルの仮想ホスト・スタンザに指定して、仮想ホストの SSL を有効にします。

   仮想ホストには、キャッシュ・ディレクティブを除く任意のディレクティブを指定できます。

3. Keyfile ディレクティブと、この特定の仮想ホストで有効にするその他の SSL ディレクティブを指定します。
4. conf ファイルの LoadModule ディレクティブを使用して mod_ibm_ssl.so をロードします。
5. 次のように IHS 仮想ホストを停止してから起動します。たとえば、次のようにします。

   ```
   IHS2_install_dir/bin
   ./apachectl stop
   ./apachectl start
   ```

   注意： SSL 実装の起動と停止の指示は、SSL に対応しない実装の場合と同じです。

6. 次の手順に進みます。
   - リバース・プロキシのアクティブ化
   - Oracle Access Manager Web コンポーネントのインストール

Linux での Apache および OHS Web サーバーの準備

Linux 上の Apache または OHS に対して Oracle Access Manager Web コンポーネントをインストールするとき、Web サーバーを実行しているのと同じユーザーとしてインストールするように求められます。httpd.conf ファイルの User および Group ディレクティブ・エントリを参照してください。

Red Hat Enterprise Linux 4 で、ベンダーでバンドルされている Apache v2 に対して Oracle Access Manager Web コンポーネントをインストールする場合は、すべての Oracle Access Manager Web コンポーネントが Web サーバーのユーザーとグループ（デフォルト : apache）に対してインストールされることを確認します。17-33 ページの「Oracle Access Manager Web コンポーネントのための Apache または IHS v2 のチューニング」も参照してください。

Linux での OHS Web サーバーの準備

Oracle Access Manager 10*g*（10.1.4.0.1）Web コンポーネントを OHS に対して使用する場合、Linux では次の点に注意してください。

- Linux では実行時に `LD_ASSUME_KERNEL=2.4.19` 環境変数を設定する必要があります。Linux の以前のスレッド・モデルがサポートされているためです（ネイティブの posix スレッド・ライブラリ（NPTL）ではない）。
- Linux では Policy Manager とディレクトリ・サーバーの SSL モードでの通信はサポートされていません。

Linux および Windows プラットフォームでの OHS Web サーバーの準備

Windows および Linux プラットフォームで OHS に対して Oracle Access Manager 10*g*（10.1.4.0.1）Web コンポーネントを使用する場合、httpd.conf で Windows と Linux 両方のプラットフォームについて Perl モジュールと PHP モジュールの両方をコメント化する必要があります。

注意 : Linux 上の OHS に対して Oracle Access Manager Web コンポーネントをインストールするとき、Web サーバーを実行しているのと同じユーザーとしてインストールするように求められます。httpd.conf ファイルの User および Group ディレクティブ・エントリを参照してください。

OHS クライアント証明書の設定

cert_decode および credential_mapping プラグインを使用するときは、+EarlierEnvVars と +ExportCertData を OHS Web サーバー構成ファイルの既存の SSL オプションに追加して、アクセス・システム・クライアント証明書の認証スキームが、SSL 対応 OHS で適切に作動することを確認する必要があります。次に例を示します。

credential_mapping:

```
obMappingBase="o=company,c=us",obMappingFilter=
    "(&(objectclass=InetOrgPerson)(mail=%certSubject.E%))"
```

ssl.conf に次のオプションを指定する必要があります。

```
SSLOptions +StdEnvVars +ExportCertData +EarlierEnvVars
```

ssl オプションを追加する手順

1. OHS Web サーバーの構成ファイルを探して、テキスト・エディタで開きます。次に例を示します。

   $ORACLE_HOME/ohs/conf/ssl.conf

2. ssl.conf ファイルの既存の SSL オプションに次の情報を追加します。たとえば、次のようにします。

   ```
   SSLOptions +StdEnvVars +ExportCertData +EarlierEnvVars
   ```

3. ファイルを保存して Web サーバーを再起動します。

UNIX での Apache v2 Web サーバーの準備

ここでは、UNIX プラットフォーム（Solaris、UNIX、Linux、AIX など）での Oracle Access Manager のための Apache v2 HTTP Web サーバーの準備の概要と手順について説明します。17-18 ページの「AIX での Apache v2 SSL Web サーバーの準備」も参照してください。

Apache v2 は、プレーンまたは SSL 対応として構成、構築およびインストールが可能です。Apache ソース・ファイルをダウンロードして抽出した後で、スクリプト（UNIX では構成スクリプト、Windows では make スクリプト makefile.win）を使用して環境に応じたソース・ツリーをコンパイルします。

注意： プラットフォームに関係なく基本要件は同じです。ただし、この後の説明と手順では UNIX プラットフォームを中心に扱います。詳細は、17-18 ページの「AIX での Apache v2 SSL Web サーバーの準備」を参照してください。

UNIX プラットフォームで Apache v2 を構成するときは、./configure コマンドの -prefix= オプションを使用してインストール・ディレクトリのパス名を指定します。構成時に環境に適したモジュールを有効にできます。たとえば、動的モジュールをコンパイルに含めると、mod_so が自動的にサーバーに組み込まれます。ただし、構成コマンドに -enable-so オプションを含めて、サーバーが DSO をロードできるようにしてください。複数の Perl インタプリタをインストールしている場合、-with-perl オプションを指定して、構成時に正しいインタプリタが選択されるようにできます。

構成コマンドには、mod_ssl を有効にして MPM をアクティブ化するオプションも含めることができます。構成の後で、./httpd -l を使用してサーバーにコンパイルされたすべてのモジュールをリストし、選択された MPM を確認できます。

Apache の構成が終了したら、make コマンドを使用して Apache パッケージを形成する様々な部品を構築し、構成時に -prefix= オプションで指定したインストール・ディレクトリにパッケージをインストールします。

手順と例は、次の手順と Apache のドキュメントを参照してください。

- UNIX でプレーン Apache v2 を準備する手順
- UNIX で SSL 対応 Apache v2 を準備する手順
- Windows で Apache v2 を準備する手順
- リバース・プロキシのアクティブ化

この後の手順で、パス名の変数、モジュールおよびオプションは手順を説明するための例です。これらは環境によって異なります。詳細は、Web サーバーのドキュメントを参照してください。Apache v2.0.48 と v2.0.52 で構築手順に違いはありません。

UNIX でプレーン Apache v2 を準備する手順

1. 適切なコンパイラや構築ツールに関して、環境が Apache の要件を満たしていることを確認します。次の Web サイトにある Apache ドキュメントを参照してください。

   ```
   http://httpd.apache.org/docs-2.0/install.html#requirements
   ```

   注意： Apache v2 と Oracle Access Manager プラグインでサポートされるコンパイラのバージョンに関してわかっている制限はありません。Apache のドキュメントを参照してください。

2. Apache ドキュメントの説明に従って、変更されていない完全なバージョンの Apache HTTP サーバー v2 をダウンロードします。たとえば、次のようにします。

   ```
   http://httpd.apache.org/download.cgi
   ```

   注意： 必要であれば Perl をダウンロードしてください。

3. Apache ドキュメントの説明に従って、tarball からソース・ファイルを抽出します（圧縮解除してから untar を実行）。次に例を示します。

   ```
   gzip -d httpd-2_0_48.tar.gz
   tar -xvf httpd-2_0_48.tar
   ```

   Apache ソース・ツリーの構成例として次の手順を使用できます。UNIX 上の Apache を mpm_worker_module とコンパイルする場合は、17-35 ページの「ヒントとトラブルシューティング」を参照してください。

   注意： Oracle Access Manager でリバース・プロキシ機能を使用するには、17-4 ページの「Apache と IBM HTTP リバース・プロキシ・サーバーについて」で説明したように構成コマンドにプロキシ・モジュールを含める必要があります。

4. Apache ドキュメントの詳細を参照して、Apache ソース・ツリーを構成し、必要なモジュールを有効化（すなわちアクティブ化）します。次に例を示します。

   ```
   cd apache_source_dir
   ./configure --prefix=apache_install_dir --enable-so ¥ --with-mpm='prefork'
    --with-perl=perl_interpreter_path ¥ --with-port=non_ssl_port_number
   ```

   apache_source_dir は Apache を抽出したディレクトリ、*apache_install_dir* は Apache をインストールするディレクトリです。

5. make コマンドを使用して、構成した Apache パッケージをコンパイルします。たとえば、次のようにします。

   ```
   make
   ```

6. 前に --prefix= オプションを使用して指定した構成済ディレクトリ・パスに Apache パッケージをインストールします。次に例を示します。

```
make install
```

7. Apache ドキュメントの指示に従ってインストールをカスタマイズします。

   たとえば、次の基本的な値を設定するために httpd.conf をチューニングする必要があります。

```
ServerName
User/owner of the WebServer
Group
```

> **注意：** すべての値のリストを表示するには、./configure --help コマンドを使用します。

8. Apache Web サーバーを停止してから再起動し、*apache_install_dir*/bin ディレクトリでコマンドを使用してインストールをテストします。たとえば、次のようにします。

```
./apachect1 stop
./apachectl start
```

9. 環境に応じて次の適切なタスクに進みます。
   - UNIX で SSL 対応 Apache v2 を準備する手順
   - UNIX での Apache v2 Web サーバーの準備
   - リバース・プロキシのアクティブ化
   - Oracle Access Manager Web コンポーネントのインストール

次の手順では、UNIX での SSL 対応 Apache v2 Web サーバーの準備方法を説明します。Apache mod_ssl はロード可能ですが、このインストールでは SSL/TLS 用の Open Source ツールキットが必要です。ここでも、必要であれば Perl をダウンロードしてください。使用しているプラットフォームが AIX の場合は、17-18 ページの「AIX での Apache v2 SSL Web サーバーの準備」で詳細を確認してください。

UNIX で SSL 対応 Apache v2 を準備する手順

1. 適切なコンパイラや構築ツールに関して、環境が Apache の要件を満たしていることを確認します。次の Web サイトにある Apache ドキュメントを参照してください。

```
http://httpd.apache.org/docs-2.0/install.html
```

2. Apache ドキュメントの説明に従って、変更されていない完全なバージョンの Apache HTTP サーバー v2 と Open Source をダウンロードします。

```
http://httpd.apache.org/download.cgi
http://www.openssl.org/
```

3. Apache ドキュメントの説明に従って、tarball からソース・ファイルを抽出します（圧縮解除してから untar を実行）。次に例を示します。

```
gzip -d httpd-2_0_48.tar.gz
tar -xvf httpd-2_0_48.tar
gzip -d openssl-0_9_6f.tar.gz
tar -xvf openssl-0_9_6f.tar
```

4. Apache ドキュメントの説明に従って OpenSSL ソース・ツリーを構成します。次に例を示します。

```
cd openssl_source_dir
./configure -fPIC --prefix=openssl_install_dir
```

   openssl_source_dir は OpenSSL を抽出したディレクトリ、*openssl_install_dir* は構成済 OpenSSL パッケージをインストールするディレクトリです。

5. make コマンドと --prefix= オプションを使用して構成したインストール・ディレクトリに OpenSSL パッケージをコンパイルします。たとえば、次のようにします。

```
make
```

6. make test コマンドを発行して、OpenSSL のサニティ・テストを行い、必要なツールの正しいバージョンをチェックします。たとえば、次のようにします。

```
make test
```

7. 前に --prefix= オプションを使用して指定した構成済ディレクトリ・パスに OpenSSL パッケージをインストールします。次に例を示します。

```
make install
```

8. Apache ドキュメントの説明に従って、Apache ソース・ツリーを構成し、必要なモジュールを有効化（すなわちアクティブ化）します。次に例を示します。

```
cd apache_source_dir ./configure --prefix=apache_install_dir
 --enable-so ¥ --with-mpm='prefork' --with-perl=perl_interpreter_path ¥
--with-port=non_ssl_port --enable-ssl ¥ --with-ssl=openssl_install_dir
```

apache_source_dir は Apache を抽出したディレクトリ、*apache_install_dir* は Apache をインストールするディレクトリ、*openssl_install_dir* は構成済 OpenSSL パッケージをインストールしたディレクトリです。

9. make コマンドを使用してコンパイルを行い、--prefix= オプションを使用して構成したインストール・ディレクトリに Apache SSL 対応パッケージを構築します。たとえば、次のようにします。

```
make install
```

10. 前に --prefix= オプションを使用して指定した構成済ディレクトリ・パスに Apache SSL 対応パッケージをインストールします。次に例を示します。

```
make install
```

openssl_install_dir/bin/ にある openssl ツールを使用して SSL を有効にするには、Apache v2 サーバーの証明書を明示的に作成する必要があります。make certificate コマンドは Apache v2 では機能しません。

11. OpenSSL ドキュメントの説明に従って、*openssl_install_dir*/bin ディレクトリの OpenSSL ツールを使用して証明書を作成します。"Common Name" は完全修飾されたホスト名であることに注意してください。

12. Apache ドキュメントの指示に従ってインストールをカスタマイズします。

- 次の基本的な値を設定するために httpd.conf をチューニングします。

```
ServerName
User/owner of the WebServer
`Group
```

- 次の基本的な値を設定するために ssl.conf をチューニングします。

```
 Listen 7000
 <VirtualHost _default_:7000>
 ServerName ps0733.persistent.co.in:7000
 SSLCertificateFile /home/qa/software/ws/apache/
 apache-2.0.48_ssl_7000/conf/ssl.crt/server.crt
 SSLCertificateKeyFile /home/qa/software/ws/apache?
 apache-2.0.48_ssl_7000/conf/ssl.key/server.key
```

13. Apache Web サーバーを停止してから再起動し、*apache_install_dir*/bin ディレクトリでコマンドを使用してインストールをテストします。次に例を示します。

```
./apachectl stop
./apachectl startssl
```

14. 次の適切な手順に進みます。

- リバース・プロキシのアクティブ化
- Oracle Access Manager Web コンポーネントのインストール

AIX での Apache v2 SSL Web サーバーの準備

Apache v2 SSL Web サーバーを構築するとき、OpenSSL ライブラリ libssl.a のシンボルが Apache の httpd 実行可能ファイルにエクスポートされます。Oracle Access Manager で必要な OpenSSL ライブラリのシンボルを次に示します。

- SSL_get_peer_certificate( )
- i2d_X509( )

AIX プラットフォームでのリンクとバインドの際に、未使用すなわち未参照のシンボルは削除されます。このため、Oracle Access Manager で必要なこの 2 つのシンボルは httpd 実行可能ファイルには含まれません。

openssl-0.9.7d を使用して AIX でコンパイルを行う必要があります（openssl-0.9.7e は AIX ではコンパイルを行いません）。残りの手順は UNIXopenssl-0.9.7d の場合と同じです。

クライアント証明書認証 : クライアント証明書認証を AIX プラットフォームで使用している場合は、AIX での dlsym の問題に適用する次のホット・フィックスが含まれる AIX 5.2 Maintenance Level 4 を使用してください。

```
http://www-1.ibm.com/support/docview.wss?uid=isg1IY63366
```

Apache v2 のために AIX プラットフォームを準備する手順

1. AIX プラットフォームが、39 ページの「Oracle Access Manager のインストールの準備」で説明した Oracle Access Manager のシステム要件を満たすことを確認します。
2. 詳細は 17-14 ページの「UNIX での Apache v2 Web サーバーの準備」を参照してください。また、Apache v2 Web サーバーを構築するときは、次のようにします。
   - openssl-0.9.7d を使用して、AIX のために Web サーバーをコンパイルします。
   - 次のように make コマンドを使用します。

     ```
     make MFLAGS=EXTRA_LDFLAGS='-Wl,-bE:OpenSSL_Symbols.exp'
     ```

OpenSSL_Symbols.exp は、必要な 2 つのシンボルを含むファイルです。シンボルは、このようにエクスポート・ファイルを使用してエクスポートする必要があります。

注意 : AIX では、-bnog（シンボルのガベージ・コレクションを抑止する）、-bexpal（すべてのシンボルをエクスポートする）および -uSymbolName（特定の 1 つのシンボルをエクスポートする）の方法ではシンボルをエクスポートしないでください。

Windows での Apache v2 Web サーバーの準備

次に、Windows での Apache v2 のインストールと構成の方法に関して、UNIX での Apache v2 とどのように異なるかを示します。詳細は、Apache のドキュメントを参照してください。

インストール時 : Apache は、選択したインストール・ディレクトリを反映するように ¥conf サブディレクトリのファイルを構成します。このディレクトリに構成ファイルがすでに存在する場合は、対応するファイルの新しいコピーが拡張子 .ORIG として作成されます。たとえば、¥conf¥httpd.conf.ORIG となります。

インストール後 : Apache が ¥conf サブディレクトリのファイルを使用して構成されます。これらは UNIX バージョンの構成に使用されるのと同じファイルです。ただし、わずかに違いがあります。

¥conf サブディレクトリの構成ファイルを編集し、環境に合せて Apache をカスタマイズする必要があります。これらのファイルはインストール時に構成されます。Apache はインストール・ディレクトリから実行する準備が整っています。このとき、ドキュメント・サーバーはサブディレクトリ htdocs から実行できます。Apache の使用を開始する前に多くのオプションを設定する必要があります。たとえば、Apache はポート 80 でリスニングしますが、これは、構成ファイルの Listen ディレクティブを変更した場合や現行ユーザーのみに Apache をインストールした場合を除きます。

マルチスレッド : Windows 対応の Apache はマルチスレッドです。つまり、UNIX の場合のように各リクエストに個別のプロセスを使用することはありません。また、通常は 2 つの Apache プロセスのみが実行しています。親プロセスとリクエストを処理する子プロセスです。子プロセス内では各リクエストが個別のスレッドで処理されます。

UNIX 形式の名前 : Apache の内部では UNIX 形式の名前が使用されます。ファイル名を引数として受け取るディレクティブでは、UNIX ファイル名ではなく Windows ファイル名を使用する必要があります。ただし、円記号ではなくスラッシュを使用してください。ドライブ名は使用できます。ただし、ドライブ名を省略すると、Apache 実行可能ファイルのあるドライブとみなされます。

LoadModule ディレクティブ : Windows 対応 Apache には、サーバーを再コンパイルせずに実行時にモジュールをロードする機能が含まれています。Apache を普通にコンパイルすると、いくつものオプション・モジュールが ¥Apache2¥modules ディレクトリにインストールされます。これらのモジュールまたは他のモジュールをアクティブ化するには、LoadModule ディレクティブを使用する必要があります。たとえば、ステータス・モジュールをアクティブ化するには、次のように指定します（この他に、access.conf で status-activating ディレクティブを使用します）。

```
LoadModule status_module modules/mod_status.so
```

UNIX では、ロードされるコードは通常は共有オブジェクト・ファイル（拡張子 .so）に含まれますが、Windows では .so または .dll 拡張子になります。

プロセス管理ディレクティブ : これらのディレクティブも Windows 対応の Apache では異なります。

エラー・ログ : Apache の起動時には、すべてのエラーが Windows イベント・ログに記録されます。これは、error.log ファイルのバックアップになります。詳細は、Apache のドキュメントを参照してください。

Apache Service Monitor: Apache には Apache Service Monitor ユーティリティが含まれています。これにより、ネットワークのすべてのマシンで、インストールされているすべての Apache サービスの状態を表示および管理できます。Apache サービスをモニターで管理するには、まずこのサービスをインストールする必要があります。Apache は Windows 上のサービスとして実行できます。詳細は、Apache のドキュメントを参照してください。

起動、再起動、停止 : Apache をサービスとして実行することをお薦めします。通常、Apache サービスの起動、再起動および停止は、Apache Service Monitor や、NET START Apache2、NET STOP Apache2 などのコマンドを使用して行います。標準の Windows サービス管理も使用できます。

apache コマンドを使用してコマンドラインから Apache を操作できます。起動して実行している Apache を停止するには、[Ctrl] を押しながら [C] を押します。インストール時に「スタート」メニューから Apache を実行することもできます。

注意： [Ctrl] と [C] を同時に押すと、Apache は現行の操作を終了したり正常にクリーンアップしたりすることができません。

Apache サービス・アカウント：デフォルトでは、すべての Apache サービスがシステム・ユーザー（LocalSystem アカウント）として実行するように登録されています。LocalSystem アカウントには、Windows 保護メカニズムを介したネットワーク権限はありません。ただし、LocalSystem アカウントにはローカルの様々な権限があります。1 つ以上の Apache サービスを実行するために別のアカウントを作成する方法の詳細は、Apache のドキュメントを参照してください。

Windows で Apache v2 を準備する手順

1. 次の Web サイトにある Apache ドキュメントの説明を参照して、環境が Apache の要件を満たしていることを確認します。

   ```
   http://httpd.apache.org/docs-2.0/install.html
   ```

   Windows でのインストールに対して、Apache v2 をダウンロードできる HTTP および FTP ミラーのリストがオンラインで提供されます。

   次の手順を完了したら、.msi 拡張子が付いた Windows 対応の Apache バージョンをダウンロードしてください。

2. Apache ドキュメントの説明に従って、変更されていない完全なバージョンの Apache HTTP サーバー v2（および OpenSSL）をダウンロードします。たとえば、次のようにします。

   ```
   http://httpd.apache.org/download.cgi
   http://www.openssl.org/
   ```

3. Apache ドキュメントの説明に従って、Apache v2 をインストールします（ダウンロードした .msi ファイルを実行し、要求される情報を指定します）。

4. .default.conf ファイルを探し、新しい設定を確認し、必要であれば既存の構成ファイルを更新します。

5. コンソール・ウィンドウで、またはサービスとして、Apache を起動します。

6. ブラウザを起動し、次の URL を入力してサーバーに接続し、デフォルト・ページにアクセスします。たとえば、次のようにします。

   ```
   http://localhost/
   ```

   「welcome」ページと Apache マニュアルへのリンクが表示されます。表示されない場合は、logs サブディレクトリの error.log ファイルを調べてください。

   基本インストールが機能するようになったら、¥conf サブディレクトリのファイルを編集してインストールを適切に構成する必要があります。

7. Apache ドキュメントの説明に従って、環境に合うように Apache インストールを構成します。

8. カスタマイズした環境をテストします。

9. 必要であれば次の手順に進みます。

   - リバース・プロキシのアクティブ化
   - Oracle Access Manager Web コンポーネントのインストール

リバース・プロキシのアクティブ化

Apache v2 および IHS v2 powered by Apache 対応の WebGate では、リバース・プロキシがサポートされます（アクティブ化を選択した場合）。リバース・プロキシ機能を実装する手順は環境によって異なります。

- Apache v2 Web サーバーでリバース・プロキシをアクティブ化する手順
- IHS v2 Web サーバーでリバース・プロキシをアクティブ化する手順

Apache v2 Web サーバーでのリバース・プロキシのアクティブ化

Oracle Access Manager のリバース・プロキシ機能を利用するには、Web サーバーの構成コマンドに Apache プロキシ・モジュールを含める必要があります。また、mod_proxy モジュールと mod_proxy_http モジュールをサーバーに動的にロードする必要があります。リバース・プロキシをアクティブ化するには、ProxyPass ディレクティブ、または RewriteRule ディレクティブの [P] フラグを使用します。

リバース・プロキシ機能をアクティブ化するには、ProxyPass ディレクティブ、または RewriteRule ディレクティブの [P] フラグを使用します。リバース・プロキシを構成するために ProxyRequests をオンにする必要はありません。リバース・プロキシを使用するとき（ProxyPass ディレクティブで ProxyRequests Off を指定）アクセス制御はそれほど重要ではなくなります。明確に構成したホストにしかクライアントが接続できないためです。プロキシへのアクセスは <Proxy> 制御ブロックを使用して制御できます。

Apache v2 Web サーバーでリバース・プロキシをアクティブ化する手順

1. 17-4 ページの「Apache と IBM HTTP リバース・プロキシ・サーバーについて」を確認します。
2. 必要であれば、Apache プロキシ・モジュールを Web サーバーの構成コマンドに含めます。

   次に例を示します。

   ```
   --enable-proxy
   --enable-proxy-connect
   --enable-proxy-ftp
   --enable-proxy-http
   ```

   詳細は、Apache のドキュメントを参照してください。
3. 次のように、ProxyPass ディレクティブを使用するか RewriteRule ディレクティブの [P] フラグを使用して、リバース・プロキシをアクティブ化します。

   ```
   Reverse Proxy
   ProxyRequests Off
   <Proxy *>
    Order deny,allow
    Allow from all
   </Proxy>
   ProxyPass /foo http://foo.example.com/bar
   ProxyPassReverse /foo http://foo.example.com/bar
   ```
4. 次のように、<Proxy> 制御ブロックを使用してプロキシへのアクセスを制御します。

   ```
   <Proxy *>
    Order Deny,Allow
    Deny from all
    Allow from 192.168.0
   </Proxy>
   ```
5. まだ実行していない場合は、17-24 ページの「Oracle Access Manager Web コンポーネントのインストール」を実行します。

IHS v2 Web サーバーでのリバース・プロキシのアクティブ化

Web サーバーをインストールした後で、次の手順を実行します。

IHS v2 Web サーバーでリバース・プロキシをアクティブ化する手順

1. 17-4 ページの「Apache と IBM HTTP リバース・プロキシ・サーバーについて」を確認します。
2. 17-10 ページの「IHS v2 Web サーバーの準備」の説明に従って IHS v2 Web サーバーをインストールします。
3. httpd.conf ファイルの Dynamic Shared Object セクションに、次の行を（コメント化せずに）組み込んでモジュールをロードします。

   IHS_install_dir/conf/httpd.conf

```
LoadModule access_module modules/mod_access.so
LoadModule auth_module modules/mod_auth.so
LoadModule auth_dbm_module modules/mod_auth_dbm.so
LoadModule include_module modules/mod_include.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule env_module modules/mod_env.so
LoadModule unique_id_module modules/mod_unique_id.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule mime_module modules/mod_mime.so
LoadModule dav_module modules/mod_dav.so
LoadModule autoindex_module modules/mod_autoindex.so
LoadModule asis_module modules/mod_asis.so
LoadModule info_module modules/mod_info.so
LoadModule cgid_module modules/mod_cgid.so
LoadModule dav_fs_module modules/mod_dav_fs.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
LoadModule dir_module modules/mod_dir.so
LoadModule imap_module modules/mod_imap.so
LoadModule actions_module modules/mod_actions.so
LoadModule userdir_module modules/mod_userdir.so
LoadModule alias_module modules/mod_alias.so
LoadModule rewrite_module modules/mod_rewrite.so
```

4. IfModule mod_proxy.c タグの下のディレクティブ -- 次の説明と例に基づいて確認します。
   - Allow 条件と Deny 条件が適切にコメント化されているかどうか。

     次に例を示します。

```
   <Proxy *>
      Order deny, allow
#    Deny from all
      Allow from all
#   Allow from .domain.com
</Proxy>
```

   - 保護する URL が、ProxyPass ディレクティブと ProxyPassReverse ディレクティブの両方に記述されているかどうか。

     次に例を示します。

```
<IfModule mod_proxy.c>
ProxyRequests Off
ProxyPass /testproxy http://bedford: 8809/testrev/
ProxyPassReverse /testproxy http://bedford: 8809/testrev/
ProxyPass /test2 http://bedford: 8809/testrev/
ProxyPassReverse /test2 http://bedford: 8809/testrev/
```

5. httpd.conf ファイルを変更した場合は Web サーバーを再起動します。
6. **テスト :** プロキシ URL にアクセスするには、`http://<proxy_host>:80/testproxy/` にアクセスします。

> **注意 :**
>
> テスト時には、URL の最後にスラッシュがあることを確認します。最後にスラッシュがないためにリソースにアクセスできないことがあります。

7. リバース・プロキシ・サーバーでの SSL の有効化 : IHS デフォルト・ページのドキュメントを使用します。

   たとえば、httpd.conf ファイルの DSO セクションのサンプル SSL 設定では、ibm_ssl_module が次のようにロードされます。

   ```
   LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
   ```

8. 次のディレクティブを httpd.conf ファイルに指定します。

   ```
   SSLEnable
      Keyfile /opt/IBMIHS/bin/key.kdb
      SSLClientAuth none
      SSLProxyEngine on
   ```

9. サーバーを再起動します。
10. Web サーバーの URL にアクセスし、ブラウザに証明書が与えられることを確認します。

> **注意 :** Web サーバーをオープン・モードに戻すには、前のディレクティブをコメント化してサーバーを再起動します。

11. **key.kdb:** key.kdb を生成するには、*IHS_install_dir*/bin ディレクトリにある ikeyman ユーティリティを（できれば GUI モードで）使用します。

> **注意 :** ikeyman ユーティリティでは gsk7bas ユーティリティが使用されます。ただし、gsk7bas には修正パック PQ83048 を適用する必要があります。

12. まだ実行していない場合は、17-24 ページの「Oracle Access Manager Web コンポーネントのインストール」を実行します。

Oracle Access Manager Web コンポーネントのインストール

前に説明したように、オラクル社では、各プラットフォームの各 Web コンポーネント用にインストール・パッケージを用意しており、それぞれのパッケージがプレーンと SSL 対応両方のインストールを処理します。すべてのタイプの Oracle Access Manager Web コンポーネントをデプロイで使用できます。`https://metalink.oracle.com` の「Certify」タブを参照してください。

Oracle Access Manager Web コンポーネントのインストールを開始する前に、次のすべてのタスクを完了していることを確認します。

- 17-9 ページの「Web サーバーの準備」のすべてのアクティビティの実行
- 17-21 ページの「リバース・プロキシのアクティブ化」のすべてのアクティビティの実行（環境別）
- 第 2 章「インストールの準備」のすべてのアクティビティの実行
- 「タスクの概要 : Oracle Access Manager のインストール」の確認

詳細は、このガイドの各章を参照してください。すべての前提条件を満たさない場合、インストールに悪影響を及ぼすことがあります。

Oracle Access Manager コンポーネントのインストールは、すべてのプラットフォームと Web サーバーで類似しています。コンポーネントのインストール中に、Oracle Access Manager のための Web サーバー構成を自動更新するかどうかを確認された場合は、自動更新することをお薦めします。

タスクの概要 : Oracle Access Manager のインストール

1. Oracle Access Manager をインストールする前に、17-24 ページの「Oracle Access Manager Web コンポーネントのインストール」のすべてのアクティビティを実行します。
2. **Identity Server:** 第 4 章「Identity Server のインストール」の説明に従って、プラットフォームに適したパッケージを調べて Identity Server をインストールし、インストールが機能していることを確認します。
3. **WebPass:** プラットフォームに適したインストール・パッケージを調べて、次のアクティビティを実行します。
   - Oracle Access Manager のための Web サーバー構成の手動更新
   - Oracle Access Manager Web コンポーネントに関する httpd.conf 更新の確認
   - Oracle Access Manager Web コンポーネントのための Apache または IHS v2 のチューニング
4. **Policy Manager:** プラットフォームに適したインストール・パッケージを調べて、次のアクティビティを実行します。
   - Oracle Access Manager のための Web サーバー構成の手動更新（必要な場合）
   - Oracle Access Manager Web コンポーネントに関する httpd.conf 更新の確認
   - Oracle Access Manager Web コンポーネントのための Apache または IHS v2 のチューニング
5. **Access Server:** 第 8 章「Access Server のインストール」の説明に従って、プラットフォームに適したインストール・パッケージを調べて Access Server をインストールします。
6. **WebGate:** プラットフォームに適したインストール・パッケージを調べて、次のアクティビティを実行します。
   - 第 9 章「WebGate のインストール」
   - Oracle Access Manager のための Web サーバー構成の手動更新（必要な場合）
   - Oracle Access Manager Web コンポーネントに関する httpd.conf 更新の確認
   - Oracle Access Manager Web コンポーネントのための Apache または IHS v2 のチューニング

7. Oracle Access Manager をインストールした後で、次のアクティビティを実行できます。
   - 『Oracle Access Manager ID および共通管理ガイド』で説明されている Oracle Access Manager の構成
   - 『Oracle Access Manager カスタマイズ・ガイド』で説明されている Oracle Access Manager のカスタマイズ
   - 『Oracle Access Manager 統合ガイド』で説明されている統合の実行

Oracle Access Manager のための Web サーバー構成の手動更新

Oracle Access Manager のための Web サーバー構成ファイルは自動で更新することをお薦めします。Oracle Access Manager のインストール時に、Web サーバー・インストールを自動的に更新するかどうかを確認されます。「いいえ」を選択した場合、これを手動で実行する必要があります。

注意： Oracle Access Manager のインストール中に手動構成プロセスを起動した場合、Web ブラウザの起動は省略してファイルを開くことができます（次に示す WebGate Web サーバーの手順で必要な場合）。

Oracle Access Manager のために Web サーバーを手動で構成する手順

1. Web ブラウザを起動し、必要に応じて次のファイルを開きます。たとえば、次のようにします。

   WebGate_install_dir/access/oblix/lang/langTag/docs/config.htm

   /*WebGate_install_dir* は WebGate をインストールしたディレクトリです。

2. Apache v2 Web サーバーまたは IHS v2 Web サーバーのリンクを選択します。
3. 表示されるすべての指示に従い、Web サーバーの設定時に変更する必要があるすべてのファイルのバックアップ・コピーを作成して、やりなおす必要がある場合に利用できるようにします。

   設定によっては、新しいブラウザ・ウィンドウが起動されます。または、情報を入力するためにコマンド・ウィンドウを起動する必要があります。このため、元の設定指示に戻ってすべてを実行し、該当する Oracle Access Manager ファイルを Web サーバーが認識できるようにします。

   注意： 誤ってウィンドウを閉じた場合は、手順 1 に戻ってもう一度適切なリンクをクリックします。

   ---

4. 17-26 ページの「Oracle Access Manager Web コンポーネントに関する httpd.conf 更新の確認」に進みます。

Oracle Access Manager Web コンポーネントに関する httpd.conf 更新の確認

次の手順を実行して、Apache または IHS v2 の httpd.conf ファイルに Oracle Access Manager のための Web サーバー構成の更新が含まれていることを確認することをお薦めします。詳細は、次を参照してください。

- WebPass の詳細の確認
- Policy Manager の詳細の確認
- WebGate の詳細の確認
- 言語エンコーディングの確認

IHS Web サーバーでリバース・プロキシに関して httpd.conf を更新するには、17-22 ページの「IHS v2 Web サーバーでのリバース・プロキシのアクティブ化」を参照してください。Web サーバーに関して httpd.conf をカスタマイズするには、Web サーバーのドキュメントを参照してください。

WebPass の詳細の確認

ここでは、Oracle Access Manager に関する更新を行った後の httpd.conf ファイルの WebPass セクションの例を示します。具体的な詳細は環境によって異なります。この例は、Oracle Access Manager に関して httpd.conf がどのように変わるかを説明するために示します。

httpd.conf の WebPass エントリを確認する手順

1. 更新された httpd.conf ファイルを WebPass のホスト・マシンで探します。
2. httpd.conf ファイルを開いて、WebPass をプラットフォームにロードするセクションがあることを確認します。次に例を示します。

```
# Note: Copy the following lines only if they do not already exist in your
httpd.conf
##**** BEGIN Oblix NetPoint WebPass Specific ****
include "/home/netpoint/703/wp/identity/oblix/.apacheconfig"
    LoadFile "/home/netpoint/703/wp/identity/oblix/lib/libgcc_s.so.1"
    LoadFile "/home/netpoint/703/wp/identity/oblix/lib/libstdc++.so.5"
<IfModule mod_ssl.c>
    LoadModule OBWebPass_Module "/home/netpoint/703/wp/identity/oblix/apps/
webpass/bin/libwebpassssl.so"
</IfModule>
<IfModule !mod_ssl.c>
    LoadModule OBWebPass_Module "/home/netpoint/703/wp/identity/oblix/apps/
webpass/bin/libwebpass.so"
</IfModule>
obwebpassinstalldir "/home/netpoint/703/wp/identity"
    Alias /identity/oblix  "/home/netpoint/703/wp/identity/oblix/"
<Directory "/home/netpoint/703/wp/identity/oblix/">
        DirectoryIndex index.htm index.html
    </Directory>
<Location /identity/oblix/apps/asynch/bin/asynch.cgi>
        SetHandler asynch
    </Location>
<Location /identity/oblix/apps/common/bin/common.cgi>
        SetHandler common
    </Location>
<Location /identity/oblix/apps/corpdir/bin/corpdir.cgi>
        SetHandler corpdir
    </Location>
<Location /identity/oblix/apps/admin/bin/corpdir_admin.cgi>
        SetHandler corpdiradmin
    </Location>
```

```
<Location /identity/oblix/apps/admin/bin/front_page_admin.cgi>
        SetHandler front_pageadmin
    </Location>
<Location /identity/oblix/apps/admin/bin/genconfig.cgi>
        SetHandler genconfig
    </Location>
<Location /identity/oblix/apps/groupservcenter/bin/groupservcenter.cgi>
        SetHandler groupservcenter
    </Location>
<Location /identity/oblix/apps/admin/bin/groupservcenter_admin.cgi>
        SetHandler groupservcenteradmin
    </Location>
<Location /identity/oblix/apps/help/bin/help.cgi>
        SetHandler help
    </Location>
<Location /identity/oblix/apps/lost_pwd_mgmt/bin/lost_pwd_mgmt.cgi>
        SetHandler lost_pwd_mgmt
    </Location>
<Location /identity/oblix/apps/objservcenter/bin/objservcenter.cgi>
        SetHandler objservcenter
    </Location>
<Location /identity/oblix/apps/admin/bin/objservcenter_admin.cgi>
        SetHandler objservcenteradmin
    </Location>
<Location /identity/oblix/apps/querybuilder/bin/querybuilder.cgi>
        SetHandler querybuilder
    </Location>
<Location /identity/oblix/apps/selector/bin/selector.cgi>
        SetHandler selector
    </Location>
<Location /identity/oblix/apps/admin/bin/servcenter_admin.cgi>
        SetHandler servcenteradmin
    </Location>
<Location /identity/oblix/apps/admin/bin/setup_admin.cgi>
        SetHandler setupadmin
    </Location>
<Location /identity/oblix/apps/admin/bin/sysmgmt.cgi>
        SetHandler sysmgmt
    </Location>
<Location /identity/oblix/apps/userservcenter/bin/userservcenter.cgi>
        SetHandler userservcenter
    </Location>
<Location /identity/oblix/apps/admin/bin/wrsc_admin.cgi>
        SetHandler wrscadmin
    </Location>
##**** END Oblix NetPoint WebPass Specific ****
```

Policy Manager の詳細の確認

ここでは、Oracle Access Manager に関する更新を行った後の httpd.conf ファイルの Policy Manager セクションの例を示します。具体的な詳細は環境によって異なります。この例は、Oracle Access Manager に関して httpd.conf がどのように変わるかを説明するために示します。

httpd.conf の Policy Manager エントリを確認する手順

1. 更新された httpd.conf ファイルを Policy Manager のホスト・マシンで探します。
2. httpd.conf ファイルを開いて、Policy Manager をプラットフォームにロードするセクションがあることを確認します。次に例を示します。

```
#*** BEGIN Oblix NetPoint Access Manager Specific ****
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libgcc_s.so.1"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libstdc++.so.5"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobnspr4.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobplc4.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobplds4.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobsoftokn3.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobnss3.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobssl3.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobldap50.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobprldap50.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobssldap50.so"
Alias /access/oblix "/home/netpoint/703/wp/access/oblix/"
<IfModule mod_ssl.c>
   LoadModule OBAccessManager "/home/netpoint/703/wp/access/oblix/lib/
webpluginsssl.so"
</IfModule>
<IfModule !mod_ssl.c>
   LoadModule OBAccessManager "/home/netpoint/703/wp/access/oblix/lib/
webplugins.so"
</IfModule>
obinstalldir "/home/netpoint/703/wp/access"
<Location /access/oblix/apps/front_page/bin/front_page.cgi>
     SetHandler obfrontpage
</Location>
<Location /access/oblix/apps/common/bin/common.cgi>
     SetHandler obcommon
</Location>
<Location /access/oblix/apps/admin/bin/genconfig.cgi>
     SetHandler obgenconfig
</Location>
<Location /access/oblix/apps/admin/bin/sysmgmt.cgi>
     SetHandler obsysmgmt
</Location>
<Location /access/oblix/apps/admin/bin/setup_admin.cgi>
     SetHandler obsetupadmin
</Location>
<Location /access/oblix/apps/admin/bin/front_page_admin.cgi>
     SetHandler obfrontpageadmin
</Location>
<Location /access/oblix/apps/admin/bin/wrsc_admin.cgi>
    SetHandler obwrscadmin
</Location>
<Location /access/oblix/apps/help/bin/help.cgi>
    SetHandler obhelp
</Location>
<Location /access/oblix/apps/policyservcenter/bin/policyservcenter.cgi>
    SetHandler obpolicyservcenter
</Location>
#*** END Oblix NetPoint Access Manager Specific ****
```

WebGate の詳細の確認

ここでは、httpd.conf ファイルの WebGate セクションの例を示します。詳細は環境によって異なります。この例は、httpd.conf がどのように変わるかを説明するために示します。

httpd.conf の WebGate セクションを確認する手順

1. 更新された httpd.conf ファイルを WebGate のホスト・マシンで探します。
2. httpd.conf ファイルを開いて、WebGate をプラットフォームにロードするセクションがあることを確認します。

   次に例を示します。

   Windows の場合

```
#*** BEGIN Oblix NetPoint WebGate Specific ****
<IfModule mod_ssl.c>
LoadModule obWebgateModule
"WebGate_install_dir¥access¥oblix¥apps¥webgate¥bin¥webgatessl.dll"
      WebGateInstalldir "WebGate_install_dir"
      WebGateMode PEER
      </IfModule>
<IfModule !mod_ssl.c>
LoadModule obWebgateModule
"WebGate_install_dir¥access¥oblix¥apps¥webgate¥bin¥webgate.dll"
      WebGateInstalldir "WebGate_install_dir"
      WebGateMode PEER
      </IfModule>
<Location "¥oberr.cgi">
SetHandler obwebgateerr
      </Location>
      <LocationMatch "/*">
      AuthType Oblix
      require valid-user
      </LocationMatch>
#*** END Oblix NetPoint WebGate Specific ****
```

   UNIX の場合

```
#*** BEGIN Oblix NetPoint WebGate Specific ****
LoadFile "/home/qa/netpoint/703/c1-copy/wg/access/oblix/lib/libgcc_s.so.1"
LoadFile "/home/qa/netpoint/703/c1-copy/wg/access/oblix/lib/libstdc++.so.5"
<IfModule mod_ssl.c>
   LoadModule obWebgateModule "/home/qa/netpoint/703/c1-copy/wg/access/oblix/
apps/webgate/bin/webgatessl.so"
</IfModule>
<IfModule !mod_ssl.c>
   LoadModule obWebgateModule "/home/qa/netpoint/703/c1-copy/wg/access/oblix/
apps/webgate/bin/webgate.so"
</IfModule>
WebGateInstalldir "/home/qa/netpoint/703/c1-copy/wg/access"
WebGateMode PEER
<Location /access/oblix/apps/webgate/bin/webgate.cgi>
SetHandler obwebgateerr
</Location>
<Location "/oberr.cgi">
SetHandler obwebgateerr
</Location>
<LocationMatch "/*">
AuthType Oblix
require valid-user
</LocationMatch>
#*** END Oblix NetPoint WebGate Specific ****
```

UNIX での注意事項

HP-UX で Apache v2 を実行するときは、共有メモリーが機能しない場合があるため、User または Group について nobody を使用しないでください。かわりに、"Oblix" という Group に対して User Name としてログイン名を使用します（または User Name として "www"、Group Name として "others" を使用）。HP-UX の "www" は Solaris の "nobody" と同じです。

HPUX 11.11 で Apache v2 を実行するときは、Apache httpd.conf ファイルの AcceptMutex ディレクティブを "fcntl" に設定してください。このディレクティブがない場合は、httpd.conf ファイルに追加します（AcceptMutex fcntl）。詳細は、http://issues.apache.org/bugzilla/show_bug.cgi?id=22484 を参照してください。

UNIX での実装の詳細は、17-35 ページの「ヒントとトラブルシューティング」を参照してください。

AIX での IHS の場合

```
#*** BEGIN Oblix NetPoint WebGate Specific ****
   LoadModule obWebgateModule DR/oblix/apps/webgate/bin/webgate.so
   WebGateInstalldir DR
   WebGateMode PEER
   <Location "/oberr.cgi">
      SetHandler obwebgateerr
   </Location>
   <LocationMatch "/*">
      AuthType Oblix
         require valid-user
   </LocationMatch>
#*** END Oblix NetPoint WebGate Specific ****
```

3. chmod -r username:groupname directory/file を使用して、ディレクトリまたはファイルの User Name と Group Name を変更します。

   このとき、httpd.conf ファイルの User パラメータと Group パラメータも同様に変更する必要があります。

4. 詳細は、17-33 ページの「Oracle Access Manager Web コンポーネントのための Apache または IHS v2 のチューニング」を参照してください。Apache v2 対応の Oracle Access Manager の実装を完了するために必要なその他の手順があれば実行します。

重要： 次の手順は、WebGate 関連の変更を httpd.conf ファイルから削除する必要がある場合のみ使用します。その後で、WebGate のための Apache v2 Web サーバーの構成を新たに実行します。

---

httpd.conf の更新を新たに開始する手順

1. 元の httpd.conf ファイルをリストアして、存在するすべての Oracle Access Manager エントリを削除します。
2. 次のいずれかの方法を使用して Oracle Access Manager のために httpd.conf ファイルを更新します。
   - ファイル *Component_install_dir*/access/oblix/lang/LangTag/docs/config.htm を開き、17-25 ページの「Oracle Access Manager のための Web サーバー構成の手動更新」の説明に従って手動構成を実行します。
   - *Component_install_dir*/access/oblix/tools/setup/InstallTools/ManageHttpConf の ManageHttpConf プログラムをオプションなしで起動して、使用方法の指示を表示します。

   注意： WebGate エントリが httpd.conf ファイルに存在する状態で ManageHttpConf プログラムを実行すると、エラー・メッセージが出力され、httpd.conf ファイルが更新されません。
3. 17-33 ページの「Oracle Access Manager Web コンポーネントのための Apache または IHS v2 のチューニング」のアクティビティを完了すると、次の作業を行えるようになります。
   - 『Oracle Access Manager ID および共通管理ガイド』で説明されている Oracle Access Manager の構成
   - 『Oracle Access Manager カスタマイズ・ガイド』で説明されている Oracle Access Manager のカスタマイズ
   - 『Oracle Access Manager 統合ガイド』で説明されている統合の実行

言語エンコーディングの確認

前に説明したように、Oracle Access Manager HTML ページでは UTF-8 エンコーディングが使用されます。Apache ベースの Web サーバーでは、管理者が `AddDefaultCharset` ディレクティブを使用して、送出されるすべての HTML ページのデフォルト・キャラクタ・セットを指定できます。これは、HTML ページを生成するアプリケーションによるキャラクタ・セットの指定よりも優先されます。`AddDefaultCharset` ディレクティブで UTF-8 以外のキャラクタ・セットを有効にすると、Oracle Access Manager の HTML ページは文字化けします。

適切な言語エンコーディングを確認する手順

1. httpd.conf ファイルを開きます。
2. `AddDefaultCharset` ディレクティブを探します。
3. 次のいずれかのアクティビティを実行して、Oracle Access Manager HTML ページの適切なエンコーディングを設定します。
   - `AddDefaultCharset` ディレクティブを Off に設定します。
   - `AddDefaultCharset` ディレクティブをコメント化します。
4. httpd.conf ファイルを保存して Web サーバーを再起動します。

Oracle Access Manager Web コンポーネントのための OHS のチューニング

OHS に対して Oracle Access Manager Web コンポーネントをインストールした後で、次の手順を実行する必要があります。

> **注意：** 前に説明したように、OHS に対して Oracle Access Manager Web コンポーネントをインストールする前に、コンポーネントをインストールするユーザーと一致するように httpd.conf ファイルでユーザーとグループを変更してください。

Oracle Access Manager Web コンポーネントのために OHS をチューニングする手順

1. opmn を停止します。
2. opmn.xml ファイルで項目を次のように調整します。

```
<ias-component id="HTTP_Server">
<process-type id="HTTP_Server" module-id="OHS2">
         <environment>
                <variable id="LD_ASSUME_KERNEL" value="2.4.19"/>
         </environment>
          <module-data>
            <category id="start-parameters">
              <data id="start-mode" value="ssl-disabled"/>
            </category>
          </module-data>
          <process-set id="HTTP_Server" numprocs="1"/>
        </process-type>
      </ias-component>
```

3. Policy Manager の httpd.conf ファイルで、次の行をコメントにします。

```
#LoadModule perl_module modules/mod_perl.so
#LoadModule php4_module modules/mod_php4.so
```

OHS Web サーバーの起動と停止

OHS Web サーバーの起動と停止は、v1.3 と v2 の両方ともすべてのプラットフォームで同じ手順です。

OHS Web サーバーを起動する手順

1. 次のディレクトリを探して移動します。

   $ORACLE_HOME¥opmn¥bin¥

2. コマンドラインで次のコマンドを入力します。

```
opmnctl/startproc process-type=HTTP_Server
```

OHS Web サーバーを停止する手順

1. 次のディレクトリを探して移動します。

   $ORACLE_HOME¥opmn¥bin¥

2. コマンドラインで次のコマンドを入力します。

```
opmnctl/stopproc process-type=HTTP_Server
```

Oracle Access Manager Web コンポーネントのための Apache または IHS v2 のチューニング

特に明記しないかぎり、次に示す情報は、Apache および IHS v2 の両方と、Policy Manager、WebPass および WebGate コンポーネント（プラグイン）に適用されます。OHS の詳細は、『Oracle HTTP Server 管理者ガイド』を参照してください。

Red Hat Enterprise Linux 4 にバンドルされている Apache v2: SELinux（セキュリティ強化 Linux）は、必須アクセス制御メカニズムが自動的に有効化される実装です。Red Hat のドキュメントで説明されているように、SELinux ポリシーを使用すると、システム・デーモンに関する特定の定義済システム・ディレクトリ（/etc/httpd/conf、/usr/sbin/apachect、/var/log/ など）にアクセスすることができます。

バンドル済 Apache Web サーバーに Oracle Access Manager Web コンポーネントをインストールした場合は、Apache プロセスが Oracle Access Manager インストール・ファイルにアクセスできるように、特定のポリシーを追加する必要があります。

バンドル済 Apache Web サーバーは、セキュリティ・コンテキストが `context=user_u:system_r:unconfined_t` として定義されたユーザー "apache" として実行します。この結果、Oracle Access Manager Web コンポーネントがいずれかのユーザー・フォルダにインストールされると、Apache Web サーバーは起動しません。

$SELINUX_SRC 変数は、SELinux ポリシー・ソース・ディレクトリを表します。デフォルト値は /etc/selinux/targeted/src/policy です。ただし、実際の環境は異なる場合があります。システムの実際の値については、システム管理者に問い合せてください。

Oracle Access Manager のポリシーを Red Hat Enterprise Linux 4 バンドルの Apache に追加する手順

1. 各 Oracle Access Manager Web コンポーネントをインストールした後で、'root' ユーザーとしてログインします。
2. すべての Oracle Access Manager Web コンポーネントが Web サーバーのユーザーとグループ（デフォルト : apache）に対してインストールされていることを確認します。
3. oracle_access_manager.te ポリシー・ファイルを *$SELINUX_SRC*/domains/programs/ ディレクトリに作成し、次のルールを追加します。

```
type oracle_access_manager_t, file_type, sysadmfile;
allow httpd_t oracle_access_manager_t:file { rw_file_perms create rename
link unlink setattr execute };
allow httpd_t oracle_access_manager_t:dir  { rw_dir_perms create append
rename link unlink setattr };
```

4. oracle_access_manager.fc ファイル・コンテキストをディレクトリ *$SELINUX_SRC*/file_contexts/program に作成し、Oracle Access Manager Web コンポーネントのインストール・ディレクトリを登録します（最後の identity または access は含めない）。次に例を示します。

```
Oracle_Access_Manager_install_dir(/.*)?
system_u:object_r:oracle_access_manager_t
```

> **注意 :** WebGate を Access Manager と別のディレクトリにインストールした場合は、WebGate のインストール・ディレクトリを別に登録してください。

5. 次のようにポリシー・ファイルをコンパイルしてデプロイします。

```
cd $SELINUX_SRC
run make load
Label Oracle Access Manager files
run restorecon -R Oracle_Access_Manager_install_dir (without the identity or access
suffix)
```

Apache v2 のディレクティブ : Apache 1.3 は、複数の HTTP リクエストを一度に処理するためにプロセス・モデルを使用します。これは、他の Web サーバーで採用されている、複数のリクエストを同時に 1 プロセスで管理するシングル・プロセス（スレッド）モデルとは異なります。Apache v1.3 Web サーバーおよび Oracle Access Manager の詳細は、第 16 章「Apache v1.3 Web サーバーおよび Oracle HTTP Server Web サーバーの構成」を参照してください。

注意 : Apache v2 のプリフォーク MPM のみが、Apache v1.3 と同じプロセス・モデルを使用して HTTP リクエストを処理します。その他すべての MPM では、Apache v2 はハイブリッド・プロセススレッド・モデルを使用します。

Apache v2 Web サーバー構成ファイル（httpd.conf）のいくつかのディレクティブは、Apache Web サーバーがワーカー・プロセスの作成または廃棄を決定する方法に影響します。次のパラメータは Apache v2 Web サーバーのパフォーマンスに影響します。

- **ThreadsPerChild:** このディレクティブは、各子プロセスが作成するスレッド数を設定します。子プロセスは、この数のスレッドを起動時に作成し、追加作成は行いません。
  - mpm_winnt（子プロセスが 1 つのみ）のような MPM を使用する場合は、サーバーの負荷全体を処理するのに十分な値にこの数を設定してください。
  - mpm_worker（複数の子プロセス）のような MPM を使用する場合は、サーバーの典型的な負荷を処理するのに十分な値にスレッドの合計数を設定してください。
- **MinSpareThreads:** この値は mpm_worker でのみ使用されます。Oracle Access Manager プラグインの初期化は最初のリクエストまで行われないため、このディレクティブに高い値を設定しても最小限の利点しか得られません。ただし、このパラメータはできるだけ高い値にしておくと役立ちます。
- **MaxSpareThreads:** この値は mpm_worker でのみ使用されます。MaxSpareThreads の値は、MinSpareThreads と ThreadsPerChild の合計以上に設定する必要があります。そうでない場合、Apache HTTP サーバーによって自動的に修正されます。

  推奨事項 : 高い値を設定してください。専用サーバーの場合には問題になりません。
- **MaxSpareServers:** Apache v2 では、これはプリフォーク MPM モデルのみで使用されます。サーバーの状態をできるだけ安定させるには、MaxSpareServers に高い値を設定します。この値を最大の 255 に設定すると、すべての Apache ワーカー・プロセスが無制限に使用可能になります。ただし、低負荷時のワーカー・プロセスのリサイクルは行われません。
- **MinSpareServers:** Apache v2 では、これはプリフォーク MPM モデルのみで使用されます。Oracle Access Manager プラグインの初期化が最初のリクエストまで行われないため、MinSpareServers パラメータに高い値を使用しても最小限の利点しか得られません。ただし、このパラメータはできるだけ高い値にしておくと役立ちます。専用 Web サーバー・システムの場合は、この設定によって非常に高い負荷がかかることはありません。
- **MaxClients:** IHS v2 でワーカー MPM を使用するとき、MaxClients によって、サーバー・クライアントが使用できるスレッドの合計数が制限されます。ハイブリッド MPM の場合、デフォルト値は 16（ServerLimit）に 25（ThreadsPerChild）をかけた値です。MaxClients の値を増やして、16 個を超えるプロセスが必要になる場合は、ServerLimit も増やす必要があります。

ここで説明したパラメータの適切な値は、予期される負荷や関連するシステム（Access Server や LDAP サーバーなど）のパフォーマンス・クラスによって異なります。

非常に高いパフォーマンスのシステムで高負荷が予想される場合は、ワーカー・プロセス数の制限を高くして Apache サーバーを再コンパイルできます。このようなシステムでは、瞬間的な負荷の急上昇に対処する際に、StartServers パラメータや MinSpareServers パラメータによるパフォーマンスへの大きな影響を確認できます。

場合によっては、Access Server を適切に運用できるようにオペレーティング・システムの制限を調整する必要があります。特に、1 つの Access Server で使用できるファイル記述子の最大数はデフォルト値よりも増やすことをお薦めします。各 Apache ベース WebGate と 1 つの Access Server の間に複数の接続を構成すると、すぐにデフォルト制限を上回ります。

詳細は、Apache のドキュメントを参照してください。

ヒントとトラブルシューティング

次に、役に立つ追加情報を示します。

- HP-UX での Apache v2
- Red Hat Enterprise Linux 4 にバンドルされた Apache v2
- UNIX 上の Apache v2 と mpm_worker_module

HP-UX での Apache v2

HP-UX で Apache v2 を実行するときは、共有メモリーが機能しない場合があるため、User または Group について nobody を使用しないでください。かわりに、"Oblix" という Group に対して User Name としてログイン名を使用します（または User Name として "www"、Group Name として "others" を使用）。HP-UX の "www" は Solaris の "nobody" と同じです。

HPUX 11.11 で Apache v2 を実行するときは、Apache httpd.conf ファイルの AcceptMutex ディレクティブを "fcntl" に設定してください。このディレクティブがない場合は、httpd.conf ファイルに追加します（AcceptMutex fcntl）。詳細は、次を参照してください。

```
http://issues.apache.org/bugzilla/show_bug.cgi?id=22484
```

Red Hat Enterprise Linux 4 にバンドルされた Apache v2

ベンダーでバンドルされた Apache に WebPass または WebGate をインストールすると、Web サーバーの起動時に次のエラーが発生することがあります。

```
Error: Cannot load libgcc_s.so.1 library - Permission denied.
```

解決方法 : 17-33 ページの「Oracle Access Manager Web コンポーネントのための Apache または IHS v2 のチューニング」の説明に従って、Oracle Access Manager Web コンポーネントに対する SELinux ポリシー・ルールを変更します。

UNIX 上の Apache v2 と mpm_worker_module

UNIX 上の Apache を mpm_worker_module とコンパイルする場合、UNIX 環境用の Apache ソースの thread.c ファイルを変更する必要があります。

UNIX 環境に合せて thread.c ファイルを変更する手順

1. thread.c ファイルを探します。次に例を示します。

   ```
   APACHE 2.0.52 source/srclib/apr/threadproc/unix/thread.c
   ```

2. 次のコード・セグメントで apr_threadattr_create(apr_threadattr_t **new,apr_pool_t *pool) という名前の関数を探します。

   ```
   **new,apr_pool_t *pool) in the following code segment:
   1-----> apr_status_t stat;
   2
   3-----> (*new) = (apr_threadattr_t *)apr_pcalloc(pool, sizeof(apr_threadattr_t));
   4-----> (*new)->attr = (pthread_attr_t *)apr_pcalloc(pool, sizeof(pthread_attr_t));
   5
   6-----> if ((*new) == NULL || (*new)->attr == NULL) {
   7----->              return APR_ENOMEM;
   8-----> }
   9
   10----->(*new)->pool = pool;
   11----->stat = pthread_attr_init((*new)->attr);
   12
   13-----> if (stat == 0) {
   14----->            return APR_SUCCESS;
   ```

```
15-----> }
16----->#ifdef PTHREAD_SETS_ERRNO
17----->stat = errno;
18----->#endif
19
20----->return stat;
21
```

3. 13 行目の前に次のコードを追加します。

```
int stacksize = 1 << 20;
pthread_attr_setstacksize(&(*new)->attr, stacksize);
```

4. configure、make および make install を実行して、mpm_worker_module を含む Apache Web サーバーを設定します。

ヘルプ情報

Oracle HTTP Server（OHS）の詳細は、次のマニュアルを参照してください。

『Oracle HTTP Server 管理者ガイド』

次の URL では、Apache リリースの構築やソース・コードに関する情報が提供されます。

Apache v2 ドキュメント :

`http://httpd.apache.org/docs-2.0/`

Apache v2 ソース・コード :

`http://httpd.apache.org/download.cgi`

Mod-SSL ドキュメント :

`http://httpd.apache.org/docs-2.0/mod/mod_ssl.html`

OpenSSL ドキュメント :

`http://www.openssl.org/docs/`

OpenSSL ソース・コード :

`http://www.openssl.org/source/`

Apache v2 のコンパイルとインストール :

`http://httpd.apache.org/docs-2.0/install.html#test`

IHS:

`http://www-306.ibm.com/software/webservers/httpservers/doc/v2047/manual/readme.html`

18

WebGates のための Lotus Domino Web サーバーの設定

Domino Web サーバーに WebGate をインストールするには、Domino Enterprise Server を適切にインストールおよび設定しておく必要があります。

この章では、WebGate と一緒に使用するための Lotus Domino のインストールと構成に関するヒントを示します。次の項目について説明します。

- Domino Web サーバーのインストール
- 最初の Domino Web サーバーの設定
- Domino Web サーバーの起動
- SSL の有効化（オプション）
- Domino セキュリティ（DSAPI）フィルタのインストール
- ヒント

> **注意：** この章の情報は、オペレーティング・システム・コマンド、Lotus Notes および Domino Web サーバーの知識があることを前提としています。

Domino Web サーバーのインストール

次では Solaris を中心に説明します。ただし、一部を変更すれば次の手順を他の UNIX システムでも使用できます。

> **注意：** 初めて lotus.com からダウンロードする場合は登録する必要があります。

UNIX で Domino Web サーバーをダウンロードする手順

1. 次の URL から Lotus Domino をダウンロードします。

   ```
   http://www-10.lotus.com/ldd/down.nsf
   ```

2. 作業領域で、ダウンロードしたファイルの untar を実行します。次に例を示します。

   gct@planetearth[/export/users2/gct/temp] 433 : ls C37UUNA.tar

   gct@planetearth[/export/users2/gct/temp] 434 : tar xf C37UUNA.tar

   gct@planetearth[/export/users2/gct/temp] 435 : ls C37UUNA.tar sol/

Domino はユーザー root としてインストールする必要があります。インストール・スクリプトによって、Lotus Domino インストール・ディレクトリにリンクするソフト・リンク /opt/lotus が作成されます。

UNIX に Domino Web サーバーをインストールする手順

1. Domino Web サーバーのインストール・スクリプトを実行します。次に例を示します。

```
gct@planetearth[/export/users2/gct/temp/sol] 441 : su root
Password:
root@planetearth[/export/users2/gct/temp/sol] 1 : ls
install* license.txt script.dat sets/ tools/
root@planetearth[/export/users2/gct/temp/sol] 2 :
root@planetearth[/export/users2/gct/temp/sol] 2 : ./install
=======================================================
Domino Server Installation
=======================================================
Welcome to the Domino Server Install Program.
Type h for help on how to use this program.
Press TAB to begin the installation.
-------------------------------------------------------
Type h for help
Type e to exit installation
Press TAB to continue to the next screen.
-------------------------------------------------------
```

   設定タイプを選択するように求められます。

2. 設定タイプを選択します。次に例を示します。

   ```
   Select Setup type: [Domino Enterprise Server]
   ```

3. 次の点を考慮してインストールを完了します。次に例を示します。

   - デフォルトのプログラム・ディレクトリは /opt/lotus に設定されています。他のディレクトリに上書きすることもできます。たとえば、/export/home/WWW/lotus とします。
   - デフォルトのデータ・ディレクトリは /local/notesdata1 に設定されています。これも他のディレクトリに上書きできます。たとえば、/export/home/WWW/lotus/data1 とします。
   - データ・ディレクトリを所有するように Domino UNIX ユーザーを上書きします。デフォルト・ユーザーは notes に設定されています。これを有効な UNIX ユーザーに変更できます。たとえば、gct または root です。

- 「The UNIX user for this directory must be a member of this group」を上書きします。デフォルト・グループは notes に設定されています。これを有効な UNIX グループ名に変更できます。たとえば、oblix とします。

注意： 次に進む前に、Domino データ・ディレクトリを $PATH に含めてください。

最初の Domino Web サーバーの設定

インストールが正常に終了したら、最初の Domino サーバーを設定する必要があります。

最初の Domino サーバーを設定する手順

1. /opt/lotus/bin/http httpsetup を実行します。

   デフォルトでは Domino はポート 8081 を使用します。

2. ポート 8081 がすでに使用されていないことを確認します。
3. ブラウザを起動して、次の URL を入力します。たとえば、次のようにします。

   `http://hostname:8081`

4. 画面の指示に従います。次の点に注意してください。
   - HTTP を調べて Web サーバーを取得します。
   - 管理者の指定には姓と名前の両方を使用します。
   - 単純なパスワードを作成し、安全な場所に記録します。たとえば、oblixoblix とします。
5. すべてのコマンドは、この Domino Web サーバーに対して構成した UNIX ユーザーとして実行します。

警告： root として実行しないでください。

Domino Web サーバーの起動

最初の Domino Web サーバーの設定が正常に終了したら、起動する必要があります。

Domino サーバーを起動する手順

1. /opt/lotus/bin/server を実行します。
2. ブラウザを起動して、次の URL を入力します。

   たとえば、次のようにします。

   http://*hostname*:*80*/names.nsf

   ログイン名とパスワードの入力を求められます。
3. 「Server-Server」を選択します。
4. 目的のサーバーを選択します。
5. 「Edit Server」を選択します。
6. 「Ports」→「Internet Ports」を選択し、「Web」をクリックします。
7. TCP/IP ポート番号の値を希望のポート番号に変更します。
8. 「Save and Close」をクリックしてすべての変更内容を保存します。
9. /opt/lotus/bin/server を実行してサーバーを再起動します。

SSL の有効化（オプション）

SSL の有効化は WebGate では必須ではありません。ただし、Windows システムの Lotus Notes クライアントから UNIX システムに送るために、キーリング・ファイル（.kyr）と対応するスタッシュ・ファイル（.sth）を生成する必要がある場合は、次の手順を実行します。

キーリング・ファイルとスタッシュ・ファイルを生成する手順

1. Windows システムで Lotus Notes クライアントを起動します。

   次に例を示します。

   「File」→「Databases」を選択し、「Open」をクリックします。

2. 「Server Certificate Admin」を選択します。
3. キーリング・ファイルを作成します。
4. 証明書リクエストを作成します。
5. 信頼できるルート証明書をキーリング・ファイルにインストールします。
6. 証明書をキーリング・ファイルにインストールします。
7. 新たに作成したキーリング・ファイルとスタッシュ・ファイルを Windows システムから UNIX マシンにコピー（すなわち ftp 送信）します。
8. 両方のファイルを Domino データ・ディレクトリに格納します。

SSL を有効化する手順

1. ブラウザを起動して、次の URL を入力します。

   たとえば、次のようにします。

   http://*hostname*:*port*/names.nsf

   ログイン名とパスワードの入力を求められます。

2. 「Server-Server」を選択します。
3. 目的のサーバーを選択します。
4. 「Edit Server」を選択します。
5. 「Ports」→「Internet Ports」を選択し、「Web」をクリックします。
6. 「SSL Key file name」フィールドにキーリング・ファイルの絶対パスを入力します。
7. SSL ポート番号の値を希望のポート番号に変更します。
8. SSL ポートのステータスを有効にします。
9. クライアント証明書の認証について、「Client Certificate」の「Yes」を選択します。
10. 「Save and Close」をクリックしてすべての変更内容を保存します。
11. Web サーバーを再起動します。

    たとえば、次のようにします。

    /opt/lotus/bin/server

Domino セキュリティ（DSAPI）フィルタのインストール

Domino セキュリティ API フィルタ（DSAPI）は、DLL を Domino Web サーバーに登録するための認証方法です。この場合、認証のリクエストが発生すると、Web サーバーは、SSL または基本認証を使用するかわりに WebGate DLL をコールしてユーザーを認証します。

Domino 内での認証はオプションです。Oracle Access Manager DSAPI フィルタを使用して行います。デフォルトの Web サーバーでサポートされない特定の認証機能を実装できます。

タスクの概要 : WebGate とフィルタのインストールの完了

1. WebGate を Domino Web サーバーにインストールする前に、前に説明したすべての手順を完了してください。
2. 9-1 ページの「WebGate のインストール」の説明に従って、WebGate のインストールと Web サーバーの更新を実行します。
3. 18-5 ページの「WebGate インストールの完了」を参照して、説明されている 2 つのオプションから 1 つを選択します。

WebGate インストールの完了

Domino Web サーバーで WebGate DLL を使用できるようにするには、サーバー・ドキュメントの「Internet Protocols」タブの下の「HTTP」タブにある「DSAPI filter file names」フィールドで、認証のためにコールされるように DLL（DSAPI ライブラリ）の名前を編集する必要があります。

> **注意 :** 相対パスは、Domino の実行可能ファイル・ディレクトリに基づきます。DSAPI フィルタ・ライブラリは、イベントを処理するときにこのリストの順にコールされます。

フィルタをインストールするには次の 2 つの方法があります。

- Web ブラウザと names.nsf を使用（オプション 1）
- Lotus Notes ワークステーションと Address Book を使用（オプション 2）

オプション 1: names.nsf にアクセスするために DSAPI フィルタを設定する手順

1. names.nsf の URL に移動してログインします。次に例を示します。

   `http://hostname:port/names.nsf`

2. 「Server-Servers」リンクをクリックします。

   Java アプレットがロードされます。

3. リストからサーバーを選択します。
4. 「Edit Server」リンクをクリックして「Edit」モードにします。
5. 「Internet Protocols」リンクをクリックします。

   デフォルトでは「HTTP」タブが選択され、情報が「Edit」モードで表示されます。

6. 「DSAPI filter file names:」で DSAPI を探し、libwebgate.so ファイルの絶対パスを入力します。
7. 変更内容を保存します。
8. Domino http サーバー・タスクを再起動します。

オプション 2: Lotus Notes を介して Address Book にアクセスする手順

1. Domino Name and Address book を開きます。たとえば、次のように選択します。

   「File」→「Database」→「Open」を選択し、「Address Book」をクリックします。

2. サーバー表示に切り替えて、サーバー・ドキュメントを開きます。
3. サーバー・ドキュメントを編集します。
4. 「Internet Protocols」タブをクリックします。

   デフォルトでは「HTTP」タブが選択され、情報が「Edit」モードで表示されます。

5. 「DSAPI filter file names:」で DSAPI を探し、libwebgate.so ファイルの絶対パスを入力します。
6. 変更内容を保存します。
7. Domino http サーバー・タスクを再起動します。

ヒント

インストールで役立つヒントを次に示します。

認証イベントの失敗 : Domino Web サーバーでは、Oracle Access Manager を介した URL のリダイレクトが機能しないことがあります。認証タイプが Basic Over LDAP に設定され、リダイレクトされる URL が次のいずれかで記述されている場合です。

同じ Web サーバーに存在する相対パス
ホスト識別子文字列の組合せで定義されたマシン名を含む、同じ Web サーバー上のフルパス URL

認証イベントの失敗を解決するには、ホスト識別子グループに定義されていないマシン名を含むようにリダイレクト URL を設定する必要があります。たとえば、マシンの IP アドレスを使用します。

この問題は、フォームベースの認証タイプでは発生しません。

ヘッダー変数 : クライアント証明書認証スキームを使用するとき、Lotus Notes Domino Web サーバーにインストールした WebGate に REMOTE_USER 以外のヘッダー変数を渡すことができない場合があります。

たとえば、クライアント証明書認証が行われるリクエストにはヘッダー変数を設定できません。ただし、他のすべてのリクエストにはヘッダー変数を設定できます。

第 VII 部

製品の削除、ヒント、トラブルシューティング

ここでは、Oracle Access Manager 10*g*（10.1.4.0.1）の削除、ヒントおよびトラブルシューティングについて説明します。

第 VIII 部は、次の章で構成されます。

- 第 19 章「重要な注意事項」
- 第 20 章「Oracle Access Manager の削除」

19

重要な注意事項

Oracle Access Manager 10*g*（10.1.4.0.1）をインストールする際に、この章で重要な注意事項を参照するように指示されることがあります。次の項目について説明します。

クライアントでの Java および JavaScript の有効化

Oracle Access Manager コンポーネントでは、Java および JavaScript がよく使用されます。Oracle Access Manager が適切に作動するためには、ブラウザで Java と JavaScript の両方を有効にする必要があります。

クライアントで Java および JavaScript を有効化する手順

1. ブラウザ・ベンダー独自の方法に従ってブラウザで Java を有効にします。
2. ブラウザ・ベンダー独自の方法に従ってブラウザで JavaScript を有効にします。

MIME タイプ設定の変更

Oracle Access Manager コンポーネントを使用すると、ユーザーは、あらゆるタイプの ASCII ファイルまたはバイナリ・ファイル（.doc、.txt、.gif など）を公開および共有できます。ユーザーがこれらのファイルを適切な製品を使用して表示するには、サーバーが各ファイルを対応する MIME タイプにマップする必要があります。一般的なファイル形式に対する MIME タイプ・マッピングのセットを次のファイルで提供しています。

IdentityServer_install_dir¥identity¥oblix¥apps¥admin¥bin¥mime_types.lst
IdentityServer_install_dir¥identity¥oblix¥apps¥admin¥bin¥mime_types.xml

WebPass_install_dir¥identity¥oblix¥apps¥admin¥bin¥mime_types.lst
WebPass_install_dir¥identity¥oblix¥apps¥admin¥bin¥mime_types.xml

.xml バージョンのファイルは Identity Server で使用されます。.lst バージョンのファイルは WebPass Java アプレットで使用されます。ファイルの両方のバージョンが一致する必要があります。また、ファイルの両方のバージョンが、*IdentityServer_install_dir* と *WebPass_install_dir* に存在する必要があります。

ほとんどの一般的なファイル・タイプはすでに mime_types.lst ファイルに含まれているため、ファイルを変更する必要はありません。ただし、mime_types.lst を変更する必要がある場合は、次の指示に従ってください。

mime_types ファイルを編集する手順

1. 次のファイルを探してテキスト・エディタで開きます。

   IdentityServer_install_dir¥identity¥oblix¥apps¥admin¥bin¥mime_types.lst

2. 新しいマッピングを追加してファイルを保存します（各行に 1 つのマッピングのみが含まれるようにし、MIME タイプと拡張子を :（コロン）で区切ります）。次に例を示します。

   ```
   image/gif:gif
   ```

3. 次のファイルを探してテキスト・エディタで開きます。

   IdentityServer_install_dir¥identity¥oblix¥apps¥admin¥bin¥mime_types.xml

4. 新しいマッピングを追加してファイルを保存します（各行に 1 つのマッピングのみが含まれるようにし、MIME タイプを次のように指定します）。次に例を示します。

   ```
   <NameValPair ParamName="image/gif" Value="gif" />
   ```

5. これら 2 つのファイルを WebPass インストール・ディレクトリにコピーします。次に例を示します。

   コピー元 :

   IdentityServer_install_dir¥identity¥oblix¥apps¥admin¥bin¥mime_types.lst
   IdentityServer_install_dir¥identity¥oblix¥apps¥admin¥bin¥mime_types.xml

   コピー先 :

   WebPass_install_dir¥identity¥oblix¥apps¥admin¥bin¥mime_types.lst
   WebPass_install_dir¥identity¥oblix¥apps¥admin¥bin¥mime_types.xml

各ユーザーの一意 ID の選択

各 Oracle Access Manager ユーザーは、一意の ID（ログイン名すなわちアカウント名とは別）を持つ必要があります。通常、一意 ID は、従業員番号や社会保障番号またはその他のタイプの ID になります。

一意 ID には特に制限はありません。たとえば、数値にする必要はありません。ただし、一意 ID を選択するときは注意してください。システムでは、この ID をデータ・ファイルに埋め込む必要があるだけではなく、すべてのユーザーが自分の ID を認識することが求められます。

オラクル社への問合せ

オラクル社に問い合せるには次のような方法があります。

情報 :

`http://www.oracle.com/corporate/contact/index.html`

サポート・サービス :

`http://www.oracle.com/support/contact.html`

最新のサポート情報は、次のサイトの「Certify」タブを参照してください。

`http://www.metalink.oracle.com`

- MetaLink にログインします。
- 「Certify」タブをクリックします。
- 「View Certifications by Product」をクリックします。
- 「Application Server」オプションを選択し、「Submit」をクリックします。
- 「Oracle Application Server」を選択し、「Submit」をクリックします。

20

Oracle Access Manager の削除

この章では、Oracle Access Manager コンポーネントを削除するときに必要になる重要な情報を示します。次の項目について説明します。

> **注意：** すべての手順を完了しないと、削除やその後のインストールに悪影響を及ぼすことがあります。クローン・コンポーネントまたはサイレント・モードでインストールしたコンポーネントの削除の詳細は、第 15 章「コンポーネントのレプリケート」を参照してください。

Oracle Access Manager コンポーネントのアンインストール

Oracle Access Manager コンポーネントのインストール時には、特定の操作を行った後に情報が保存されます。情報が保存されるまでは、前に戻って、詳細を指定しなおすことができます。ただし、コンポーネントがインストール中であると通知された後は、ファイル・システムに Oracle Access Manager ファイルが追加されています。

注意： コンポーネントがインストール中というメッセージを受け取った後で、すべての手順を完了せずにインストール・プロセスをキャンセルした場合は、Oracle Access Manager 関連の情報を削除してシステムを前の状態にリストアする必要があります。

Oracle Access Manager コンポーネントを削除するには、次に説明するいくつかの手順を完了する必要があります。Oracle Access Manager に対する変更は、自動的に処理されないため、Uninstaller プログラムが終了してから手動で変更内容を削除する必要があります。

言語パック：インストールされている各言語パックは、それぞれ削除する必要があります。これには、コンポーネントのアンインストール・ディレクトリにある該当するファイル（*Component_install_dir*¥identity | access¥_uninst*Component*LP_*langtag*¥uninstaller.exe）を使用します。たとえば、Identity Server と WebPass を韓国語言語パックを含むようにインストールしたとします。各コンポーネント・ホストで韓国語言語パックをアンインストールした後、Identity Server サービスと WebPass Web サーバー・インスタンスの両方を停止して再起動してください。これによって、対応するコンポーネントが適切な言語サポートを含むように再初期化されます。インストール時に選択されるデフォルト管理者言語に関連付けられている言語パックの削除はサポートされていません。

警告：インストール時に選択されたデフォルトの管理者言語に関連付けられている言語パックは削除（アンインストール）しないでください。インストール時に選択されたデフォルトの管理者言語に関連付けられている言語パックを誤って削除した場合は、E-17 ページの「言語の問題」を参照してください。

スキーマとデータの変更：Oracle Access Manager を削除し、同じディレクトリ・インスタンスを使用して再インストールする場合は、Oracle Access Manager 構成ツリーのみを削除してください。この場合、ディレクトリ・インスタンスから Oracle Access Manager スキーマを削除する必要はありません。Identity Server を再インストールするときに、スキーマ（すでに存在する）を更新するかどうかを確認されたら「いいえ」を選択します。「はい」を選択すると、「スキーマがすでに存在します」というエラー・メッセージが生成されます。

ただし、Oracle Access Manager を削除して、別のディレクトリ・インスタンスとして再インストールする場合（または再インストールを行わない場合）は、構成データを手動でディレクトリ・サーバーから削除する必要があります。Oracle Access Manager スキーマの拡張機能も、ディレクトリ・サーバーに提供されているクリーンアップ・ファイルを使用して削除してください。Identity Server と Policy Manager からもデータを削除する必要があります。

ディレクトリ・サーバーのタイプによって異なりますが、1 つまたは 2 つのクリーン・アップファイルが用意されています。たとえば、VDS については、スキーマ拡張機能のクリーンアップ・ファイルはユーザー・データ専用として提供されています。ただし、NDS、IPlanet および Oracle Internet Directory については、スキーマ拡張機能クリーンアップ・ファイルは、ユーザー・データと Oblix（構成データ）両方に対して提供されています。スキーマ拡張機能クリーンアップ・ファイルの名前は、ディレクトリのタイプを表す略称で始まり、削除するデータのタイプがその後に付いています。

たとえば、次のようなファイルが Identity Server と Policy Manager のインストール・ディレクトリにあります。

- *DirectoryName*_**user_schema_delete.ldif:** 特に指定されたディレクトリ用の Oracle Access Manager ユーザー・データのクリーンアップ・ファイル。構成データとは別のディレクトリ・インスタンスに存在するユーザー・データを削除します。
- *DirectoryName*_**oblix_schema_delete.ldif:** 特に指定されたディレクトリ用の Oracle Access Manager 構成データのクリーンアップ・ファイル。ユーザー・データと構成データの両方が同じディレクトリ・インスタンスにある場合に両方を削除します。
- **OID_oblix_schema_index_delete.ldif:** Oracle Internet Directory 専用の Oracle Access Manager クリーンアップ・ファイル。Oracle Internet Directory から Oracle Access Manager 属性インデックスを削除します（対応する Oracle Access Manager のデータとスキーマ用のクリーンアップ・ファイルを使用する前または後）。
- **OID_user_index_delete.ldif:** ユーザー・データのホストとして別のインスタンスが使用される場合の Oracle Internet Directory 専用の Oracle Access Manager クリーンアップ・ファイル。

ディレクトリ・ベンダーによってはスキーマ・クリーンアップ・ファイルを提供していません。たとえば、ActiveDirectory や Active Directory アプリケーション・モード（ADAM）にはこのようなファイルはありません。

注意： Oracle Access Manager を削除し、同じディレクトリ・インスタンスを使用するように再インストールする場合は、Oracle Access Manager 構成ツリーのみを削除してください。この場合、ディレクトリ・インスタンスから Oracle Access Manager スキーマを削除する必要はありません。Identity Server を再インストールするときに、スキーマ（すでに存在する）を更新するかどうかを確認されたら「いいえ」を選択します。「はい」を選択すると、「スキーマがすでに存在します」というエラー・メッセージが生成されます。

Oracle Internet Directory を使用する際の Oracle Access Manager の削除と再インストールの詳細は、E-22 ページの「Oracle Internet Directory に対する Oracle Access Manager の再インストール」を参照してください。

Web サーバー構成の変更：インストール中に行った Web サーバー構成の変更は、Oracle Access Manager コンポーネント（WebPass、Policy Manager、WebGate）をアンインストールしてから手動で元に戻す必要があります。たとえば、IIS WebPass に対して ISAPI transfilter がインストールされます。ただし、WebPass をアンインストールしてもこれは自動的には削除されません。また、作成された Web サービス拡張機能と、ID ディレクトリへのリンクも削除されません。このような情報は手動で削除する必要があります。これらは削除する必要がある情報の一例です。すべてではありません。さらに、Oracle Access Manager コンポーネント（WebPass、Policy Manager、WebGate）について Web サーバー構成ファイルに手動で行ったすべての変更を削除する必要があります。各コンポーネントに追加される内容の詳細は、第 VI 部「Web サーバーの構成」を参照してください。

Oracle Access Manager コンポーネントをアンインストールする手順

1. 削除するコンポーネントの Identity Server または Access Server サービス（または WebPass、Policy Manager、WebGate Web サーバー）をオフにします。

   注意： Web サーバーをオフにしないと、アンインストールが失敗する場合があり、バックアップ・フォルダが削除されません。この場合は、バックアップ・フォルダを手動で削除する必要があります。

2. **言語パック：**次の手順を実行して、インストールされている 1 つ以上の言語パック（デフォルトの管理者言語（ロケール）として選択されたもの以外）を削除します。:

   - コンポーネントのアンインストール・ディレクトリで適切な言語パック・ファイルを探します。次に例を示します。

     Component_install_dir¥uninstIdentityLP_fr-fr
     ¥uninstaller.exe

   - 言語パックのアンインストーラ・プログラムを実行してファイルを削除します。
   - 関連するコンポーネントから同じ言語パックを削除するにはこのプロセスを繰り返します。
   - Identity Server サービスと WebPass Web サーバー・インスタンスの両方を停止して再起動し、適切な言語サポートを含むようにコンポーネントを再初期化します。
   - このプロセスを繰り返して、各言語パック（デフォルトの管理者言語（ロケール）として選択されているもの以外）を削除します。次に例を示します。

     Component_install_dir¥uninstIdentityLP_ja-jp
     ¥uninstaller.exe

3. 次の手順を実行して、すべての Oracle Access Manager 構成データをディレクトリ・サーバー・インスタンスから削除し、必要であれば、Oracle Access Manager スキーマ拡張機能をディレクトリ・サーバーから削除します。

   - ディレクトリ・ベンダーの指示に従って、Oracle Access Manager 構成ツリーをディレクトリ・サーバー・インスタンスから削除します。
   - 該当するコンポーネントのディレクトリで ldapmodify ツールを探します。次に例を示します。

     Component_install_dir¥oblix¥tools¥ldap_tools

   - **すべてのディレクトリ：**ldapmodify ツールを使用して、ディレクトリ・サーバーに対応するスキーマ・クリーンアップ・ファイルを次のディレクトリからアップロードし、ディレクトリから Oracle Access Manager スキーマ拡張機能を削除します。次に例を示します。

     Component_install_dir¥oblix¥data.ldap¥common¥
     ¥*DirectoryName*_*_schema_delete.ldif

     Component_install_dir は特定の Oracle Access Manager コンポーネント（たとえば、Identity Server または Policy Manager）のインストール・ディレクトリ、*DirectoryName*_*_schema_delete.ldif は特定のディレクトリとデータ・タイプに対応するクリーンアップ・ファイルです。

- **Oracle Internet Directory:** 前のアクティビティを完了した後、Oracle Access Manager スキーマ拡張機能を Oracle Internet Directory から削除するには、ldapmodify ツールを使用して Oracle Internet Directory 属性インデックス・クリーンアップ・ファイルをアップロードし、Oracle Access Manager 属性インデックスを削除します。次に例を示します。

  Component_install_dir¥oblix¥data.ldap¥common¥
  OID_oblix_schema_index_delete.ldif
  OID_user_index_delete.ldif（ユーザー・データのホストとして別のインスタンスが使用される場合）

Oracle Access Manager コンポーネントのインスタンスが 1 つしかない場合は、手順 4 を実行して削除します。コンポーネントの複数のインスタンスがある場合は、手順 5 も参照してください。

4. 特定のコンポーネントのアンインストーラ・プログラムを探して実行し、Oracle Access Manager のファイルを削除します。次に例を示します。

   IdentityServer_install_dir¥identity¥_uninstIdentity¥uninstaller.exe

   WebPass_install_dir¥identity¥_uninstWebPass¥uninstaller.exe

   このようになります。

   注意 : UNIX システムでは uninstall.bin を使用します。

5. **複数インスタンス :** コンポーネントの複数のインスタンスがあるときに、1 つまたはすべてを削除する場合は、次のようにプラットフォーム特有の方法を使用する必要があります。
   - **Windows:** 最後のコンポーネントは、「アプリケーションの追加と削除」でアンインストールできます。それ以外は、¥identity または ¥access の ¥uninstComponent ディレクトリからアンインストール・プログラムを実行してアンインストールできます。
   - **UNIX:** 常に uninstall.bin を実行する必要があります。
6. Web サーバー構成から Oracle Access Manager 関連の更新を削除します。特定の Web サーバーの詳細は、第 VI 部「Web サーバーの構成」を参照してください。
7. 必要であれば Web サーバーを再起動します。
8. コンポーネントのインストール・ディレクトリが残っている場合は削除します（特に製品を再インストールする予定があるとき）。

Identity Server インスタンス名のリサイクル

状況によっては、既存の Identity Server 名を再利用する場合があります。たとえば、Oracle Access Manager をテスト環境から本番環境に移す場合や、なんらかの理由で Identity Server を削除する必要がある場合は、既存の Identity Server 名を使用すると便利です。

システム・コンソールで元の Identity Server 名を削除しないと、新しいインスタンスの設定の後でログインしたときに、「アプリケーションが設定されていません」というメッセージが表示されることがあります。Identity Server 名をリサイクルするときは、アプリケーションを設定してログインするために特別な手順を実行する必要があります。

この後の手順では、同じインストール内にもう 1 つの Identity Server と WebPass の設定があると仮定します。

Identity Server インスタンス名をリサイクルする手順

1. 次の場所にあるディレクトリ・サーバーから Identity Server 名を削除します。

   「Oblix」→「Policies」→「WebResrcDB」→「< 名前 >」

2. 第 6 章「ID システムの設定」の説明に従って Identity Server の設定を再実行します。

3. ID システム・コンソールに移動し、作動しない Identity Server インスタンスを削除します。次に例を示します。

   「ID システム・コンソール」→「システム構成」→「Identity Server」→「< 名前 >」→「削除」

4. 『Oracle Access Manager ID および共通管理ガイド』の説明に従って、「すべての Identity Server をリスト」ページで同じ ID を使用してインスタンスを再作成します。次に例を示します。

   追加

   名前
   ホスト名
   ポート
   トランスポート・セキュリティ

第 VIII 部

付録

ここでは、サード・パーティのコンポーネントに対するインストール、ディレクトリ証明書の追加やインストール後のディレクトリ・サーバー・ホストの変更といった頻度の低いタスクの実行、およびトラブルシューティングのヒントについて説明します。

第 IV 部は、次の付録で構成されます。

- 付録 A「Active Directory に対する Oracle Access Manager のインストール」
- 付録 B「ADAM に対する Oracle Access Manager のインストール」
- 付録 C「Oracle Access Manager インストール後のディレクトリ証明書の追加」
- 付録 D「ディレクトリ・サーバー・ホストの変更」
- 付録 E「インストールの問題のトラブルシューティング」

A

Active Directory に対する Oracle Access Manager のインストール

この付録では、Active Directory と一緒に使用する際の Oracle Access Manager の前提条件、インストールおよび設定についてまとめています。次の項目について説明します。

- Active Directory について
- Oracle Access Manager と Active Directory について
- Oracle Access Manager と Active Directory Forest について
- Active Directory に対するインストールと設定の考慮事項
- Active Directory に対する Oracle Access Manager のインストール
- Active Directory のヒントとトラブルシューティング

また、Oracle Access Manager と Active Directory の間の通信プロトコルとして、LDAP（デフォルト）、LDAP over SSL および Active Directory Service Interfaces（ADSI）（オプション）のすべてを使用する構成についての基本情報も示します。

『Oracle Access Manager ID および共通管理ガイド』にも次の項目の詳細が含まれています。

- ADSI のための Oracle Access Manager の構成
- LDAP を使用する Active Directory のための Oracle Access Manager の構成
- Active Directory に対する Oracle Access Manager のデプロイと Active Directory の特定機能のための Oracle Access Manager の構成
- .NET 機能のための Oracle Access Manager の構成

Active Directory について

ここでは、Active Directory の動作の概要について説明します。A-3 ページの「Oracle Access Manager と Active Directory について」も参照してください。Active Directory は、ネットワークの 1 つ以上のドメインにオブジェクトの情報を格納して、その情報をユーザーやネットワーク管理者が使用できるようにします。

- Active Directory のドメインはオブジェクトのコレクションの管理境界を定義し、この境界はネットワーク上の特定のユーザー・グループに関連します。
- ドメイン・コントローラは、ディレクトリ・パーティション（ネーミング・コンテキスト）を格納します。これは、不連続の単位としてレプリケートされた、Active Directory の論理分散セグメントに対応しています。

複数のツリーまたはドメインをサポートする Active Directory は、Active Directory Forest と呼ばれます。Active Directory は、ディレクトリ情報の論理的階層編成として構造化データ・ストアを使用します。Active Directory に含まれる内容を次に示します。

- ディレクトリに含まれるオブジェクトや属性のクラスを定義するスキーマ、これらのオブジェクトのインスタンスに対する制約と制限、これらのオブジェクト名の形式。
- ドメイン・コントローラは、ディレクトリ・パーティション（ネーミング・コンテキスト）を格納します。これは、不連続の単位としてレプリケートされた、Active Directory の論理分散セグメントに対応しています。

複数のツリーまたはドメインをサポートする Active Directory は、Active Directory Forest と呼ばれます。Active Directory は、ディレクトリ情報の論理的階層編成として構造化データ・ストアを使用します。Active Directory に含まれる内容を次に示します。

- ディレクトリに含まれるオブジェクトや属性のクラスを定義するスキーマ、これらのオブジェクトのインスタンスに対する制約と制限、これらのオブジェクト名の形式。
- グローバル・カタログ。Active Directory のフォレストのすべてのオブジェクトのコピーを格納するドメイン・コントローラです。アプリケーションやクライアントがフォレスト内の任意のオブジェクトを探すときに問い合せることができます。これは Oracle Access Manager では不要になりました。
- 問合せと索引のメカニズム。オブジェクトとそのプロパティをネットワーク・ユーザーまたはアプリケーションが公開して検索できます。
- レプリケーション・サービス。スキーマ、構成、アプリケーション、およびドメイン・コントローラ間のドメイン・ディレクトリ・パーティションを同期化し、ネットワーク上にディレクトリ・データを分散します。

ドメイン・コントローラとパーティション

Active Directory Forest 内のすべての Active Directory サーバー（ドメイン・コントローラ）は、レプリケーションを行い、そのドメインのすべてのディレクトリ情報の完全なコピーを含みます。ディレクトリ・データを変更すると、ドメイン内のすべてのドメイン・コントローラにレプリケートされます。

Active Directory Forest のすべてのドメイン・コントローラには、3 つの書込み可能なフル・ディレクトリ・パーティションが格納されています。Active Directory のディレクトリ・パーティションは、フォレスト内の他のドメイン・コントローラに 1 つのユニットとしてレプリケートされる、連続した Active Directory サブツリーです。ドメイン・コントローラには同じサブツリーのレプリカが含まれます。

1 つのドメイン・コントローラには常に少なくとも 3 つのディレクトリ・パーティションがあります。

- スキーマ : フォレストごとに 1 つ。ディレクトリのクラスと属性の定義を含みます。
- 構成 : フォレストごとに 1 つ。レプリケーション・トポロジと関連するメタデータを含みます。
- ドメイン : 1 つのフォレストに多数。1 ドメインに対してドメイン当たりのオブジェクトを含む 1 つのサブツリーを含みます。

Oracle Access Manager と Active Directory について

Oracle Access Manager では、Windows Server 2000 および Windows 2003 Server プラットフォームでの Active Directory をサポートしています。Windows Server 2003, Web Edition を実行するサーバーでは、次のようになります。

- Windows Server 2003, Web Edition を実行するサーバーには Active Directory をインストールできません。
- Windows Server 2003 Web Edition サーバーを Active Directory ドメインにメンバー・サーバー（ドメイン・コントローラではない）として追加できます。

Oracle Access Manager では、ユーザー・データを構成データやポリシー・データとは別のタイプのディレクトリ・サーバーに格納することができます。詳細は、2-22 ページの「データ記憶域の要件」および A-10 ページの「ADSI オプションの考慮事項」を参照してください。Oracle Access Manager ではグローバル・カタログの使用は必要ありません。

Oracle Access Manager では、構造型オブジェクト・クラスと補助オブジェクト・クラスがサポートされます。構造型オブジェクト・クラスはスタンドアロン可能です。Oracle Access Manager アプリケーション内で使用するために必要な基本属性を含んでいます。構造型オブジェクト・クラスは、Oracle Access Manager アプリケーションでタブを作成するときに割り当てる必要があります。補助オブジェクト・クラスはスタンドアロン不可です。構造型オブジェクト・クラスにはなくてもよい補足的な属性（請求書送付先、チャレンジ・フレーズ、チャレンジ・フレーズのレスポンスなど）を含んでいるためです。補助オブジェクト・クラスは、既存の構造型オブジェクト・クラスに基づくエントリに割り当てる必要があります。

Oracle Access Manager では、User と Group に加えて、InetOrgperson と GroupofUniqueNames がそれぞれ標準の Person オブジェクト・クラスおよび Group オブジェクト・クラスとしてサポートされます。また、Oracle Access Manager では、静的リンク補助クラスと動的リンク補助クラスがサポートされます。

詳細は、A-5 ページの「Oracle Access Manager と Active Directory Forest について」および A-8 ページの「Active Directory に対するインストールと設定の考慮事項」を参照してください。

静的リンク補助クラスについて

Windows Server 2000 では、Active Directory は静的リンク補助クラスのみをサポートし、スキーマ定義そのもので補助クラスを別の objectclass に静的にリンクできるようにしていました。静的リンク・オブジェクト・クラスは、スキーマ内で、オブジェクト・クラスの classSchema 定義の auxiliaryClass 属性または systemAuxiliaryClass 属性に含まれています。静的リンク・オブジェクト・クラスは、関連付けられるクラスのすべてのインスタンスの一部です。静的リンク補助クラス（Oracle Access Manager のデフォルト）に関して Active Directory に実装するスキーマを設計するときは、次のようにします。

- oblixOrgPerson オブジェクトと oblixPersonPwdPlicy オブジェクトをユーザー（Person）オブジェクト・クラスに定義します。
- oblixGroup と oblixAdvancedGroup を Group オブジェクト・クラスに定義します。

詳細は、A-18 ページの「静的リンク補助クラスのためにスキーマを変更する手順」を参照してください。

動的リンク補助クラスについて

Windows 2003 Server では、Active Directory は、個々のオブジェクト（オブジェクトのクラス全体ではない）への補助クラスの動的なリンクをサポートしています。この場合、あるエントリのオブジェクトの objectclass 属性の値に、補助オブジェクト・クラスの名前を追加します。補助クラスに必須属性がある場合は、それらも同時に設定する必要があります。

動的リンクにより、クラス全体のスキーマ定義を拡張してフォレスト全体に影響を与えずに、個々のオブジェクトに追加の属性を格納できます。たとえば、企業は動的リンクを使用することで、販売固有の補助クラスを販売員のユーザー・オブジェクトに追加し、他の部署固有の補助クラスを他の部署の従業員のユーザー・オブジェクトに追加できます。

Oracle Access Manager では静的な補助スキーマが提供されます。これにより、補助クラスとそれに対応する構造型オブジェクト・クラスの関連がスキーマに指定されます。静的補助クラスを使用すると、Oracle Access Manager は、追加や削除のために補助クラスの objectclass 属性を更新しません。動的補助のサポートでは、そのような別のスキーマ・ファイルはなく、Oracle Access Manager は必要に応じて objectclass 属性を補助クラス名で更新します。

Identity Server の設定およびアクセス・システムのインストールと設定の際に、ターゲット・ディレクトリで動的リンク補助クラスをサポートするかどうかが確認されます。次に示す概要で、動的リンク補助クラスを実行時に Oracle Access Manager に関連付けよためのタスクを説明しています。

Oracle Access Manager では、静的リンク補助クラスと動的リンク補助クラスをサポートしていますが、両方は同時にサポートされません。

警告：動的補助クラスがサポートされるのは、フォレストのすべてのドメイン・コントローラが Windows Server 2003 を実行しており、フォレストの機能モデルが Windows Server 2003 である場合です。2003 ドメイン・コントローラとそれ以前のドメイン・コントローラが混在する環境はサポートされません。フォレストのレベルを上げた後には Active Directory サーバーを再起動してください。

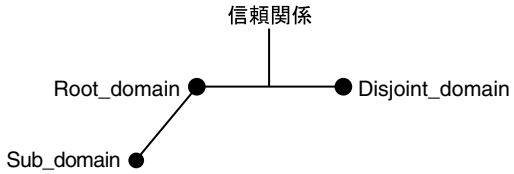
タスクの概要：動的リンク補助クラスの有効化

1. Oracle Access Manager をインストールする前に、Active Directory のドメインとフォレストの機能が、Microsoft 社のドキュメントに説明されているように Windows 2003 Server レベルで作動していることを確認する必要があります。
2. ID システムのインストールと設定の際に、第 4 章「Identity Server のインストール」と第 6 章「ID システムの設定」の説明に従って動的リンク補助クラスを指定します。
3. Policy Manager のインストールと設定の際に、第 7 章「Policy Manager のインストール」の説明に従って動的リンク補助クラスを指定します。
4. Access Server のインストールの際に、第 8 章「Access Server のインストール」の説明に従って動的リンク補助クラスを指定します。
5. インストールと設定の後で、『Oracle Access Manager ID および共通管理ガイド』の説明に従って Oracle Access Manager で動的補助クラスのサポートを構成します。

Oracle Access Manager と Active Directory Forest について

Oracle Access Manager の以前のバージョンでは、1 つの Active Directory Forest 内にしか Oracle Access Manager をインストールすることができませんでした。図 A-1 に、3 つのドメイン Root_domain、Sub_domain および Disjoint_domain を含む 1 つの Active Directory Forest を示します。

図 A-1 3 つのドメインを含む 1 つの Active Directory Forest



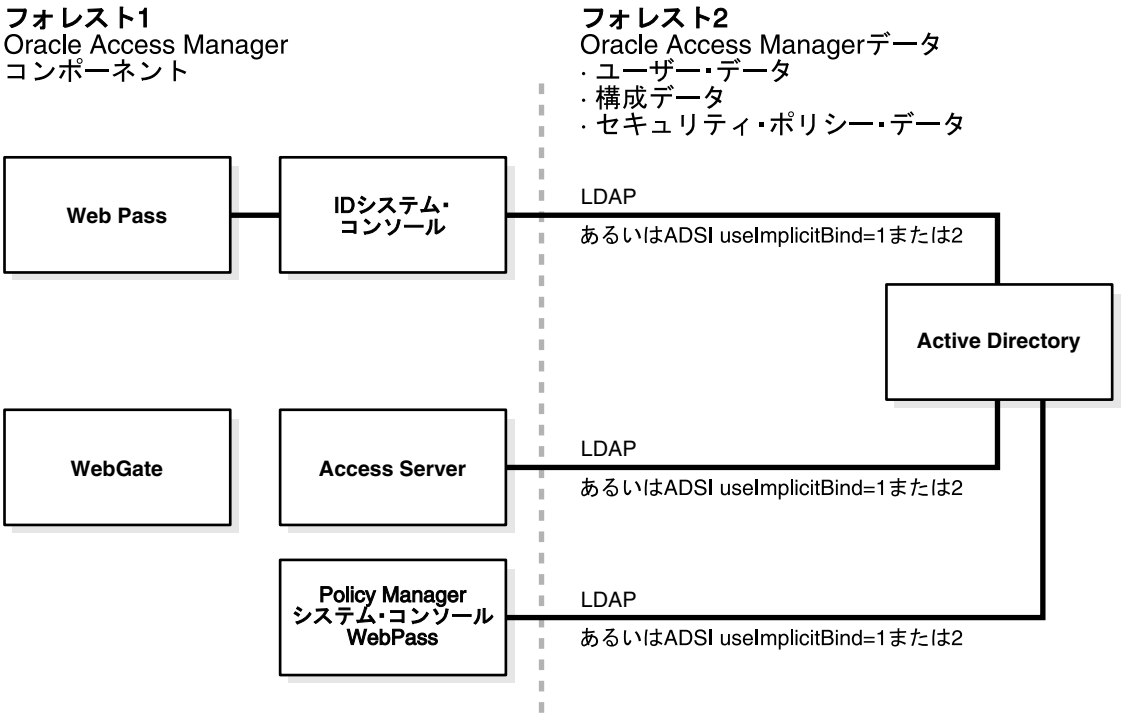
現在、Oracle Access Manager コンポーネントは、Active Directory Forest 内に Oracle Access Manager のユーザー・データ、構成データおよびポリシー・データと一緒に存在することも、Oracle Access Manager データを含むフォレストの外部に存在することもできます。

Oracle Access Manager コンポーネントを 1 つの Active Directory Forest 内にインストールした場合は、Oracle Access Manager と Active Directory の間で次のいずれかの通信プロトコルを使用できます。

- LDAP（デフォルト）
- LDAP over SSL
- ADSI

図 A-2 に、1 つのフォレスト（フォレスト 1）にインストールされた Oracle Access Manager コンポーネントを示します。ユーザー・データ、構成データおよびポリシー・データはもう 1 つのフォレスト（フォレスト 2）にあります。このタイプの構成は、フォレスト外の Oracle Access Manager とも呼ばれます。ADSI の使用はオプションです。

図 A-2 フォレスト外の Oracle Access Manager



2 フォレスト構成では、1 つのフォレストにある 1 つのドメイン・コントローラ（スキーマ・マスター）が、スキーマ・ディレクトリ・パーティションに対するすべての変更を処理します。1 フォレストにつき 1 つのドメイン・コントローラ（ドメインネーミング・マスター）が、ドメイン名がフォレスト内で一意になるように管理し、外部ディレクトリに対するオブジェクトのクロスリファレンスが維持されるようにします。詳細は、Microsoft 社のドキュメントを参照してください。

2 フォレスト構成では、ユーザー・データ、ポリシー・データおよび構成データを含むフォレストと Oracle Access Manager サーバーがインストールされているフォレストとの間に信頼関係を設定する必要はありません。

1 つのフォレストに構成データとポリシー・データを含み、別のフォレストにユーザー・データを含む環境も可能です。

親子ドメインでの Oracle Access Manager と検索ベース

Active Directory ドメインは、階層を形成する親子関係として編成できます。親ドメインとは、階層内で、1 つ以上の下位ドメイン（子ドメイン）のすぐ上にあるドメインです。子ドメインも、1 つ以上の子ドメインの親になることができます。Oracle Access Manager の検索ベースによって、データが格納されるディレクトリ情報ツリーのノードと、すべての検索に対する最高位のベースが定義されます。ただし、子ドメイン内のエントリを探すことはできません。デフォルトの Oracle Access Manager ディレクトリ・サーバー・プロファイルは、Root_domain のみに対して作成されます。インストール内のその他のドメイン（たとえば、Disjoint_domain や Sub_domain）のディレクトリ・プロファイルは設定する必要があります。詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

アクセス・システムでは、認証時には credential_mapping プラグインを使用してサブツリーレベルの検索が実行されます。また、認可時にも、検索がサブツリーレベルで行われることが LDAP ルール（たとえば LDAP URL）によって明示的に指定されていると、サブツリーレベルの検索が実行されます。LDAP URL を含む ObMyGroups アクションを使用すると、ユーザーが所属するすべてのグループが返されます。表 A-1 に、親子ドメインをサポートする構成をまとめています。

表 A-1 親子ドメインをサポートする構成

機能	親子ドメインの構成
認証	資格証明のマッピングを使用して、親ドメインと子ドメインの両方に対してユーザーを認証する。 Oracle Access Manager credential_mapping プラグインを使用して、ユーザーの DN を取得できる。Active Directory Forest の場合、credential_mapping プラグインの典型的なパラメータは次のとおり。 credential_mapping?ObMappingBase="%domain%, ObMappingFilter="(&(objectclass=user) (samaccountname=%login%))", Obdomain="domain" accountname=%login%))", Obdomain="domain"
認可	複数の LDAP URL を認可ルール内で使用する。
ObMyGroups	LDAP URL を含む ObMyGroups を使用する。ユーザーが親ドメインと子ドメイン両方のグループに所属する場合は、各ドメインのグループに対して別のヘッダー変数を定義する必要がある。 URL なしで ObMyGroups を使用すると、アクセス・システムの検索ベースのみからグループが返される。検索ベースが親ドメインのものである場合、子ドメインのグループはまったく取得されない。 たとえば、2 つのドメインがあり、両方の検索ベースからグループを取得する場合は、次のように指定する。 dc=goodwill,dc=oblix,dc=com and dc=dilbert,dc=goodwill,dc=oblix,dc=com この場合は、各ドメインに 1 つずつ 2 つのヘッダー変数が必要。 Return Type Name Retrun Attribute headervar HTTP_PARENT_GROUP "obmygroups:ldap:///dc=goodwill,dc=oblix,dc=com??sub?(group_type=role)" headervar HTTP_CHILD_GROUP "obmygroups:ldap:///dc=dilbert,dc=goodwill,dc=oblix,dc=com??sub?(group_type=role)" HTTP_PARENT_GROUP: "dc=goodwill,dc=oblix,dc=com" ツリー（ログイン・ユーザーがメンバー、group_type が "role"）のすべてのグループが返される。 HTTP_CHILD_GROUP: "dc=dilbert,dc=goodwill,dc=oblix,dc=com" ツリー（ログイン・ユーザーがメンバー、group_type が "role"）のすべてのグループが返される。

Active Directory に対するインストールと設定の考慮事項

Active Directory に対する Oracle Access Manager のインストールを開始する前に見なおすことができるように、各考慮事項の概要を次のようにまとめています。

Active Directory のスキーマ選択

Active Directory 2000 と Active Directory 2003 のスキーマ、およびそれらのスキーマが Oracle Access Manager に適用される方法にはいくつかの違いがあります。

鍵の違い : Windows 2000 スキーマ（ADSchema.ldif）と Windows 2003 スキーマ（dotnetschema.ldif）（Oracle Access Manager に関連）の鍵の大きな違いは、inetOrgPerson と groupofuniquenames をサポートするかどうかです。これら 2 つのオブジェクト・クラスは、他のほとんどの LDAP ディレクトリに存在しており、Windows 2003 スキーマには正式に追加されました。inetOrgPerson オブジェクト・クラスの追加により、このオブジェクト・クラスを使用して Oracle Access Manager を構成することができます。Windows 2000 の場合のように手動でこのオブジェクト・クラスを追加する必要はありません。

Oracle Access Manager スキーマ・ファイルへの影響 : Oracle Access Manager Windows 2000 スキーマ・ファイル（ADschema.ldif）と Windows 2003 スキーマ・ファイル（ADdotnetschema.ldif）の主な違いについて次に説明します。

- 次のエントリは、ADSchema.ldif にはありますが ADdotnetschema.ldif にはありません。

  dn: cn=groupOfUniqueNames,cn=schema,cn=configuration,<domain-dn>

  dn: cn=uniquemember,cn=schema,cn=configuration,<domain-dn>

- oblixgroupofuniquenames クラス定義は 2 つのファイルで異なります。これは、2000 スキーマ・ファイルでの groupofuniquenames の定義方法と、Microsoft 社による 2003 スキーマでの groupofuniquenames の実装方法の違いによるものです。

2 つのスキーマの objectclass の違い : 2 つのスキーマの objectclass がどのように異なるかを次に示します。

- **ADSchema.ldif**:

  必須属性 : 必須の属性はありません。

  オプション属性 :

  obuniquemember

  businesscategory

  obver

- **ADdotNetschema.ldif**:

  必須属性

  cn

  businesscategory

  obuniquemember

  obver

  description

  o

ou

owner

seeAlso

uniqueMember

ロードするスキーマの決定

ADschema.ldif というファイルが Windows 2000 の Oracle Access Manager スキーマ・ファイル、ADdotnetschema.ldif というファイルが Windows 2003 の Oracle Access Manager スキーマ・ファイルです。環境にロードするスキーマを決めるときは、次の点を考慮してください。

ADdotnetschema.ldif: Windows 2000 と Windows 2003 のどちらを実行しているかに関係なく、Active Directory 2003 スキーマをロードしている場合は、.NETSchema（Windows 2003 スキーマ）を使用して Oracle Access Manager をインストールします。

たとえば、企業によっては、Windows 2003 へのアップグレード準備として既存の Windows 2000 ドメインに Windows 2003 スキーマをロードしていることがあります。

このような場合は、Oracle Access Manager をインストールするときに ADdotnetschema.ldif ファイルを使用する必要があります。

ADschema.ldif: Windows 2000 スキーマがある場合は Windows 2000 スキーマをロードします。

注意 : スキーマ・ファイルを手動でロードしない場合は、Windows 2003 をインストールしているかという質問に対するユーザーの回答に基づいて、使用するスキーマ・ファイルをインストーラが決定します。Windows 2003 をインストールしていると回答した場合は、インストーラが ADdotnetschema.ldif を使用します。

スキーマ・タイプの判別 : 環境に Windows 2000 スキーマと Windows 2003 スキーマのどちらがあるかを判別する簡単な方法は、スキーマ・スナップインを使用して、2003 スキーマの新しい文字列構文を検索することです。次に例を示します。

- 2000 スキーマでは、文字列型に attributesyntax 2.5.5.12 の Unicode 形式が使用されていました。
- 2003 スキーマでは、新しい構文 IA5 attributesyntax 2.5.5.5., omysyntax: 22 に変更されています。

すべての構成

Active Directory に対するすべての Oracle Access Manager インストールの概要を次に説明します。

Identity Server とアクセス・システムのインストールと設定の手順では、時間を節約しエラーを防ぐために自動スキーマ更新を受け入れることをお薦めします。後でいつでも変更できます。ただし、手動スキーマ更新の場合、環境によっては設定プロセスで次の 1 つ以上のファイルを使用する必要があります。

- Windows 2003 の動的リンク補助クラスでは、次の 1 ファイルのみが必要です。

  ¥*install_dir*¥identity | access¥oblix¥data¥common¥ADDotNetSchema.ldif

  ```
  ldifde -i credentials -c "<domain-dn>" "your domain" -f ADDotNetSchema.ldif
  ```

- Windows 2003 の静的リンク補助クラスでは、次の 2 つのファイルが両方とも必要です。

  ¥*install_dir*¥identity | access¥oblix¥data¥common¥ADDotNetSchema.ldif

  ¥*install_dir*¥identity | access¥oblix¥data¥common¥ADAuxSchema.ldif

- Windows 2000 では次の 1 ファイルのみが必要です。

  ¥*install_dir*¥identity | access¥oblix¥data¥common¥ADSchema.ldif

次のメンバーに管理ユーザーのプロパティを追加することをお薦めします。

メイン管理者

スキーマ管理者

グループ・ポリシー管理者

エンタープライズ管理者

ドメイン管理者

ユーザー、管理者

次のガイドラインは、Active Directory と一緒に使用する Oracle Access Manager のすべての構成に適用されます。

ガイドライン : Active Directory に対する Oracle Access Manager のインストール

1. Oracle Access Manager のインストールと設定の際には、使用する Active Directory のバージョンを指定し、関連する質問に適切に回答してください。
2. Oracle Access Manager のインストールと設定の際には、Identity Server、Policy Manager および Access Server で同じ構成 DN を使用します。

注意 : マルチ・ドメイン・フォレストのログイン名は、Access Server DB プロファイルの表示名です。

---

3. インストールと設定の後で、『Oracle Access Manager ID および共通管理ガイド』の説明に従って、Active Directory の認証スキーム（1 つまたは複数）を作成または変更できます。
4. インストールと設定の後で、次の行を Identity Server の globalparams.xml に追加して、Active Directory 上の大容量の動的グループを拡張できます。

```
<SimpleList>
<NameValPair ParamName="maxForRangedMemberRetrieval"
Value="1500"/
</SimpleList>
```

ADSI オプションの考慮事項

ADSI を使用する構成の概要を次に説明します。ADSI の使用はオプションです。

ADSI の資格証明は、フォレスト全体にバインドするために使用されます。1 つのフォレストは複数の Active Directory ホストを含むことができます。ユーザー・データと構成データが別のフォレストの別の Active Directory ホストに格納されている場合は、ADSI を使用してこれらのデータに同時に接続することはできません。詳細は、E-4 ページの「この DB プロファイルで ADSI を有効化できない（Active Directory）」を参照してください。

ADSI では、フォレストの様々なドメインについて具体的なホストやポート番号は必要ありません。ADSI は、次のような LDAP URL を使用して Active Directory のホストに接続します。

```
LDAP://domain.oracle.com/ou=oblix,dc=domain,dc=oblix,dc=com
```

ユーザー・データと構成データが同じフォレストの別の Active Directory ホストに格納されている場合は、ADSI を使用してこれらのデータに接続できます。データの検索と変更は、ドメインネーミング・コンテキストを使用して、フォレストのそれぞれの Active Directory サーバーで行われます。

インストールの際に、構成データをユーザー・データ・ディレクトリに格納するかどうかを確認されます。ユーザー・データと構成データが同じフォレストの別の Active Directory ホストに格納されており、ユーザー・ツリーに ADSI を使用するときは、構成データをユーザー・データ・ディレクトリに格納するように指定してください。ユーザー・データと構成データを別に格納するように指定すると、ADSI を使用して構成データ・ディレクトリ・サーバーに接続できなくなり、「ID システム・コンソール」ページで「ADSI」を選択して構成データの DB プ

ロファイルを作成できなくなります。ただし、LDAP を使用すれば構成データ・ディレクトリ・サーバーに接続できます。

- フォレスト全体で ADSI を使用するとき、マスター管理者の資格証明は、フォレスト全体の管理権限を含むエンタープライズ管理者の資格証明であることが必要です。

  フォレスト全体で同じユーザー・ツリー資格証明を有効にする必要があります。ユーザー・ツリーに対して ADSI を構成し、構成ツリーとポリシー・ツリーに対して LDAP を構成するように決めた場合は、設定が完了した後で、globalparams ファイルのパラメータを変更して、適切なプロファイルを定義することができます。『Oracle Access Manager ID および共通管理ガイド』の説明を参照してください。

- Oracle Access Manager のデータとコンポーネントが同じドメインにあるときは、ID システムをインストールおよび設定した後で、パスワード変更権限を持つ特権管理ユーザーのコンテキストで Identity Server を実行する必要があります。

- 別のフォレストにある構成データおよびポリシー・データとは別の Active Directory サーバーにユーザー・データを格納するとき、いずれかに接続するために ADSI を使用できますが、両方に接続することはできません。

  – **Oracle Access Manager のインストール時 :** 構成データをユーザー・データと一緒に格納するかどうかを確認されたら「はい」を選択し、ユーザー・データ・ディレクトリ・サーバーには「ADSI」を選択します（構成データに対する ADSI については確認されません）。

  – **Oracle Access Manager の設定時 :** DB プロファイルのディレクトリ・タイプを次のように指定します。

    ユーザー DB プロファイル : Microsoft Active Directory および ADSI
    構成 DB プロファイル : Microsoft Directory のみ（ADSI なし）

- Oracle Access Manager のコンポーネントが 1 つのドメインにありデータがもう 1 つのドメインにある場合は、Oracle Access Manager コンポーネントと Active Directory の間で ADSI または LDAP を使用できます。

インストールと設定の際に、Oracle Access Manager は、Identity Server 上の adsi_params.xml ファイルと Policy Manager 上の adsi_params.lst ファイルの特定のパラメータを自動的に更新します。これらのファイルのパスを次に示します。

¥*IdentityServer_install_dir*¥identity¥oblix¥config¥adsi_params.xml

¥*AccessServer_install_dir*¥access¥oblix¥config¥adsi_params.xml

これらのファイルには、ユーザー・バインド DN の useImplicitBind 値が含まれています。表 A-2 に、指定可能なバインド・パラメータをまとめています。

表 A-2 指定可能なバインド・パラメータのまとめ

useImplicitBind 値	定義	説明
0	現在のプロセスの暗黙の資格証明をバインドで使用する。	1 つの Active Directory Forest adsi_params.xml ファイルでの Identity Server のデフォルト。
1	ユーザーの DN による明示的な資格証明をバインドで使用する。	2 つの Active Directory Forest adsi_params.xml ファイルと .lst ファイルで useImplicitBind 値を 1 に設定する。

表 A-2 指定可能なバインド・パラメータのまとめ（続き）

useImplicitBind 値	定義	説明
2	バインドで userPrincipalName を使用する。	2 つの Active Directory Forest ■ adsi_params.lst ファイルでの Policy Manager のデフォルト。 ■ Oracle Access Manager コンポーネントが Oracle Access Manager データとは別のドメインにある場合の推奨値。 ■ UPN を adsi_params.xml ファイルの adsiUPN パラメータに指定。

ADSI の使用時に設定する各パラメータについて次に説明します。

- **useImplicitBind**=1: useImplicitBind の値が 1 の場合は、Identity Server でサービス・ログイン資格証明を設定する必要はありません。Oracle Access Manager のコンポーネントとデータが別のフォレストにある場合は、useDNSPrefixedLDAPPaths=true を設定します。
- **implicitBind**=0: implicitBind=0 を使用する場合は、IIS 匿名ユーザーの権限をドメイン・ユーザーに設定する必要はありません。デフォルトは、implicitBind=0、useDNSPrefixedLDAPPaths=false です。

  この場合、ADSI は Active Directory サーバーにバインドするためにプロセスのコンテキストを使用します。デフォルトでは、匿名ユーザー（IWAM*）にはディレクトリ・サーバーの権限はありません。
- **useDNSPrefixedLDAPPath:** adsi_params.xml ファイルおよび adsi_params.lst ファイルの useDNSPrefixedLDAPPath パラメータを使用して、ドメイン名を LDAP 文字列の接頭辞にすることができます。デフォルト値は false です。

ガイドライン : ADSI の設定

1. Oracle Access Manager をインストールする前に、Microsoft 社のドキュメントおよび A-14 ページの「環境の設定」の説明に従って、Active Directory を設定する必要があります。
2. Identity Server のインストールの際に、第 4 章「Identity Server のインストール」と A-16 ページの「ID システムのインストール」の説明に従って ADSI を有効にします。
3. ID システムを設定する前に、A-17 ページの「ADSI の設定（オプション）」の手順を実行します。
4. ID システムの設定の際に、第 6 章「ID システムの設定」と A-17 ページの「ID システムの設定」の説明に従って ADSI を指定します。
5. Policy Manager のインストールと設定の際に、第 7 章「Policy Manager のインストール」と A-20 ページの「アクセス・システムのインストールと設定」の説明に従って ADSI を指定します。
6. Access Server のインストールの際に、第 8 章「Access Server のインストール」の説明に従って ADSI を有効にし、A-22 ページの「Access Server での ADSI の設定（オプション）」にある追加の手順を実行します。

   図 18 のように Oracle Access Manager コンポーネントと Oracle Access Manager データが別のフォレストにある場合は、ID システムとアクセス・システムを設定する前に、次のタスクを実行します。

7. インストールと設定の後で、Oracle Access Manager adsi_params ファイルでパラメータと値が次のように設定されていることを確認してください。次に例を示します。

   ¥*IdentityServer_install_dir*¥identity¥oblix¥config¥adsi_params.xml

   ¥*AccessServer_install_dir*¥access¥oblix¥config¥adsi_params.xml

   ```
   NameValPair ParamName="useDNSPrefixedLDAPPaths
   Value="true"
   ```

   ¥*IdentityServer_install_dir*¥identity¥oblix¥config¥adsi_params.xml

   ```
   NameValPair ParamName="adsiCredential"
   Value="cn=Administrator,cn=users,dc=goodwill,dc=oblix,dc=com"
   ```

adsi_params ファイルおよびパラメータの詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

LDAP オープン・バインドの考慮事項

次に概要を示します。

LDAP オープン・バインドは、Oracle Access Manager とディレクトリ・サーバーの間のデフォルト（指定がない場合に使用される）の通信方法です。LDAP オープン・バインドを Oracle Access Manager コンポーネントと Active Directory の間で使用する場合は、Oracle Access Manager のインストールと設定の際に追加の手順を実行することをお薦めします。

ガイドライン : LDAP オープン・バインドの設定

1. Oracle Access Manager をインストールする前に、Microsoft 社のドキュメントと 395 ページの「環境の設定」の説明に従って、Active Directory を設定する必要があります。
2. ID システムのインストールと設定の際に、Oracle Access Manager と Active Directory の間に SSL 接続がないことを必ず指定してください。
3. Access Server のインストールの後で、LDAP のフェイルオーバー情報とタイムアウト、およびポート番号を指定するように求められます。
   - Access Server を Active Directory に対してインストールするときは、『Oracle Access Manager ID および共通管理ガイド』の説明に従って必ずタイムアウトを構成してください。
   - フェイルオーバー情報は、後から『Oracle Access Manager デプロイメント・ガイド』の説明に従って再構成できます。

LDAP over SSL の考慮事項

次に概要を示します。

LDAP over SSL を Oracle Access Manager コンポーネントと Active Directory の間で使用する場合は、Oracle Access Manager のインストールと設定の際に追加の手順を実行してください。

ガイドライン : SSL の設定

1. Oracle Access Manager をインストールする前に、A-14 ページの「環境の設定」の説明に従って、マシンに証明書があることを確認します。
2. インストールと設定の後で、『Oracle Access Manager ID および共通管理ガイド』の説明に従ってディレクトリ・サーバーとの通信を再構成できます。

   ADSI を有効化した状態でディレクトリ・サーバーとの通信を再構成する場合は、adsi_params.xml ファイルと adsi_params.lst ファイルを編集して暗号化パラメータを false にリセットする必要もあります。

Active Directory に対する Oracle Access Manager のインストール

これまでに説明した考慮事項に注意して、Active Directory の設定と Oracle Access Manager のインストールを行うことができます。次に、すべての手順と実行する順序を説明します。

タスクの概要 : Active Directory に対する Oracle Access Manager のインストール

1. 「環境の設定」
2. 「ID システムのインストール」
3. 「ID システムの設定」
4. 「ID システム設定の検証」
5. 「アクセス・システムのインストールと設定」

タスク概要のこれらの項目には複数の手順が含まれることがあります。その場合は、さらにタスク概要を示して、手順を実行する順序を説明します。

環境の設定

次に、Oracle Access Manager コンポーネントをインストールする前に Active Directory を設定する方法の概要を示します。

タスクの概要 : 環境の設定

1. A-14 ページの「ドメイン・コントローラの設定」
2. A-14 ページの「証明書サーバーのインストール」
3. A-15 ページの「証明書の取得」

ドメイン・コントローラの設定

Oracle Access Manager コンポーネントをインストールする前に、ドメイン・コントローラを設定する必要があります。

警告 : 動的リンク補助クラスを有効化する予定がある場合は、Microsoft 社のドキュメントの説明に従って、ドメインとフォレストの両方を Windows 2003 Server レベルに上げる必要があります。

ドメイン・コントローラを準備する手順

1. Microsoft 社の指示に従って、Active Directory Forest の各マシンのドメイン・コントローラを設定して構成します。
2. Microsoft 社の指示に従って、すべての補助クラスについて、動的リンク補助クラスと静的リンク補助クラスのどちらの方法にするかを指定します。

証明書サーバーのインストール

LDAP over SSL を使用する場合、Microsoft CA Certificate Server をインストールして証明書を取得する必要があります。

注意 : LDAP（デフォルト）または ADSI を使用している場合、この説明は必要ありません。

証明書サーバーは Active Directory Forest の任意のマシンにインストールできます。ただし、Active Directory Forest のルート・ドメインにインストールすることをお薦めします（たとえば

Root_domain)。有効化すると、すべてのドメイン・コントローラが証明書を自動的にリクエストして、SSL ポート 636 を使用して LDAP をサポートします。

他のドメイン・コントローラに Microsoft CA Certificate Server を設定する手順

1. Microsoft 社の指示に従って、他のドメイン・コントローラが証明書を自動的にリクエストできるようにポリシーを設定します。
2. Microsoft 社のドキュメントに従い、Microsoft CA Certificate Server を設定して構成します。

証明書の取得

証明書サーバーを設定したら、証明書サーバーをインストールしたマシンから Microsoft CA 証明書を取得して、Oracle Access Manager コンポーネントをインストールするマシンに保存する必要があります。たとえば、Identity Server の Root_domain に保存します。

警告： 証明書は SSL が有効化されている各マシンに必要です。

タスクの概要：証明書の取得と設定

1. A-15 ページの「対象の Identity Server の証明書を取得する手順」
2. A-15 ページの「証明書を設定する手順」

対象の Identity Server の証明書を取得する手順

1. Identity Server をインストールするマシンで、Microsoft CA Certificate Server がインストールされているマシンにナビゲートします。次に例を示します。

   http://*Root_domain*/certsrv/
2. 「Retrieve the CA certificate or certificate revocation list」を選択します。
3. 「Base64 encoded」を選択します。
4. 「Download CA certificate」リンクをダブルクリックします。
5. 「Save this file on the machine where you will install the Identity Server」を選択します。
6. ディレクトリとファイル名を入力します。
7. Identity Server をインストールするときのためにこのファイルのフルパスを記録します。次に例を示します。

   F:¥OracleAccessManager¥certnew.cer

ID システムをインストールする準備ができました。A-15 ページの「証明書を設定する手順」も参照してください。

証明書を設定する手順

1. 証明書サーバーにナビゲートします。次に例を示します。

   http://*Root_domain*/certsrv/
2. 証明連鎖をファイルにダウンロードして、証明書を保存します。

   次に説明するように、このファイルをインポートしてローカル・コンピュータに保存するとき、現在ログインしているユーザーの個人用証明書ストアに CA が IE によってインポートされます（デフォルト）。

3. ファイルをローカル・コンピュータ上の信頼できるルート CA ストアにインポートします。次に例を示します。

   「Internet Explorer」→「ツール」→「インターネット オプション」を選択します。

   「コンテンツ」→「証明書」→「信頼されたルート証明機関」→「フレンドリ名」→「インポート」→「次へ」を選択します。

   「参照」をクリックして「ファイル名」を指定し、「次へ」→「信頼されたルート証明機関」→「ローカル・コンピュータ」をクリックします。

ID システムのインストール

Active Directory の準備設定が終了したら、Identity Server と WebPass（ID システムの主要な 2 つのコンポーネント）をインストールする必要があります。

タスクの概要 : Active Directory に対する ID システムのインストール

1. A-16 ページの「ID システムのインストール」
2. A-17 ページの「ADSI の設定（オプション）」

ID システムのインストール

インストールと設定の際には、他のディレクトリ・サーバーに対して Oracle Access Manager をインストールするユーザーの場合と同じ質問に答えるように求められます。その他に、ADSI と動的リンク補助クラスのオプションを指定するように求められます。

Identity Server をインストールする手順

1. A-8 ページの「Active Directory に対するインストールと設定の考慮事項」と 2-22 ページの「データ記憶域の要件」を確認します。
2. 必要であれば、A-14 ページの「環境の設定」を実行します。
3. 第 4 章「Identity Server のインストール」の指示に従い、Active Directory 環境の仕様やプリファレンスを設定します。

   指定するバインド DN は、属性の変更および読取りとスキーマのアクセスに十分な権限があれば、どのユーザーのものでもかまいません。LDAP または SSL を使用する場合にはパスワードの変更権限も必要です。ADSI では Identity Server サービス資格証明書が適切であることが必要です。

4. Active Directory 上の大容量の動的グループを拡張する場合は、次の行を globalparams.xml ファイルに追加して Identity Server を再起動します。

   ¥*IdentityServer_install_dir*¥identity¥oblix¥apps¥common¥bin¥globalparams.xml

   ```
   <SimpleList >
   <NameValPair ParamName="maxForRangedMemberRetrieval" Value="1500"/>
   </SimpleList>
   ```

ID システムのインストールを完了する手順

1. 第 5 章「WebPass のインストール」の手順に従います。
2. 環境に応じて次のいずれかのタスクを実行します。
   - A-17 ページの「ADSI の設定（オプション）」の説明に従って ADSI を設定します。
   - A-17 ページの「ID システムの設定」の説明に従って ID システムの設定を完了します。

ADSI の設定（オプション）

オプションの ADSI を使用する場合は、次のタイミングで、この後に示す手順を実行する必要があります。

- ID システム（Identity Server および WebPass）のインストールの直後
- ID システムの設定前

デフォルトでは ADSI によって暗黙のバインドが使用されます。これは、Windows 2000 Server および Windows Server 2003 サービスのログイン資格証明に対応しています。詳細は、A-10 ページの「ADSI オプションの考慮事項」および『Oracle Access Manager ID および共通管理ガイド』を参照してください。

ID システムの設定前に ADSI を設定する手順

1. ¥*IdentityServer_install_dir*¥identity¥oblix¥config¥adsi_params.xml で、環境に応じたバインド・メカニズムを選択します。次に例を示します。

   - **単一フォレストの場合の ADSI:**

     ```
     <NameValPair ParamName="useImplicitBind"
     Value="0"/>
     ```

   - **Oracle Access Manager とデータが別のフォレストにある場合の ADSI:**

     ```
     <NameValPair ParamName="useImplicitBind"
     Value="1"/>
     <NameValPair ParamName="useDNSPrefixedLDAPPaths"
     Value="true">
     ```

2. **When useImplicitBind=0:** Identity Server のサービス・ログイン資格証明をドメインの管理ユーザー（Identity Server のインストール時にルート・バインド DN として指定したユーザーと同じ権限を持つ）に設定します。
3. 次の「ID システムの設定」の説明に従って ID システムを設定します。

ID システムの設定

Identity Server コンポーネントと WebPass コンポーネントをインストールしたら、ID システムを設定する準備ができています。

次に、ID システムの設定が成功するように、設定前や設定時に実行することを示します。いくつかの状況について説明します。

- Active Directory の属性の有効化

  注意： Active Directory の特定の属性を有効化しない場合は、6-5 ページの「ID システムの設定」に直接進みます。

- パスワード変更権限の有効化
- ID システムの設定

Active Directory の属性の有効化

Active Directory の特定の属性を有効化するには、次の手順を実行する必要があります。たとえば、userPrincipalName をログイン属性として使用するため、この属性を ID システムの設定時に使用できるようにするには、ID システムの設定前に次のアクティビティを完了する必要があります。

注意： Active Directory の特定の属性を有効化しない場合は、この手順を実行せずに A-18 ページの「ID システムの設定」に直接進みます。

Active Directory の属性を有効化する手順

1. ad_exlude_attrs.xml ファイルと exclude_attrs-ad.xml ファイルを探します。次に例を示します。

   ¥*IdentityServer_install_dir*¥identity¥oblix¥data.ldap¥common¥ad_exlude_attrs.xml

   ¥*IdentityServer_install_dir*¥identity¥oblix¥data.ldap¥common¥exclude_attrs-ad.xml

2. これらのファイルを編集して、ID システムのユーザー・プロファイルで Active Directory の特定の属性を使用可能にします。次に例を示します。

```
<ValNameList ListName="userPrincipalName">
<NameValPair ParameterName="appliesto" Value="None" />
```

静的リンク補助クラスのためにスキーマを変更する手順

1. スキーマを変更して、oblixOrgPerson オブジェクトと oblixPersonPwdPlicy オブジェクトをユーザー・オブジェクト・クラスに追加し、oblixGroup と oblixAdvancedGroup を Group オブジェクト・クラスに追加します。
2. このように変更した後で MMC スキーマ・マネージャ・アプリケーションでスキーマのリロードを実行します。スキーマの変更がすべてのドメイン・コントローラにレプリケートされるまで約 15 分かかります。

パスワード変更権限の有効化

Oracle Access Manager のデータとコンポーネントが同じフォレストにあるときは、パスワード変更権限を持つ特権管理ユーザーのコンテキストで Identity Server を実行する必要があります。

注意： LDAP over SSL の場合、Identity Server にサービスの資格証明を設定する必要はありません。

ID システムの設定

これまでのタスクを完了したら、Active Directory Forest に対して Root_domain を使用して ID システムを設定する準備ができています。

Active Directory Forest に ID システムを設定する手順

1. 次の ID システムの設定ページにナビゲートします。

   http://*hostname:port*/identity/oblix

2. 「ID システム・コンソール」をクリックし、「セットアップ」をクリックして、プロセスを起動します。
3. 第 6 章「ID システムの設定」の手順に従います。
   - 該当する場合は ADSI を有効化します。
   - 該当する場合は、「動的補助オブジェクト・クラス」ボックスを選択します。

4. 設定が完了したら、次に示すタスクを実行できます。
   - A-19 ページの「ID システム設定の検証」の説明に従って ID システムの設定を検証します。
   - 必要であれば、『Oracle Access Manager ID および共通管理ガイド』の説明に従って、その他のドメインのディレクトリ・サーバー・プロファイルを定義します。

     注意： ADSI を使用している場合、デフォルト・ディレクトリ・プロファイルとその他のディレクトリ・プロファイルに関する ADSI 有効化の詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

   - 必要であれば、『Oracle Access Manager ID および共通管理ガイド』の説明に従って、disjoint ドメインの disjoint 検索ベースを設定します。
   - 401 ページの「アクセス・システムのインストールと設定」の説明に従って、アクセス・システムをインストールして設定します。

ID システム設定の検証

アクセス・システムのインストールを開始する前に、ID システムが設定されて正常に Active Directory と一緒に機能していることを検証するようにお薦めします。

ID システムの設定を検証する手順

1. ID システムのログイン・ページにナビゲートします。

   http://*hostname*:*port*/identity/oblix

2. ログイン・ページのドロップダウン・リストに表示されるすべてのドメイン名を確認します。
3. ログインします。
4. 「ディレクトリ・オプションの構成」ページにナビゲートし、disjoint 検索ベースがリストされていることを確認します。

   ID システム・コンソールで、「システム管理」→「システム構成」→「ディレクトリ・オプション」を選択します。

   注意： disjoint 検索ベースがリストされていない場合は、ここで追加することができます。詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

   ID システムが正常に作動していることを検証したら、アクセス・システムをインストールして設定できます。

アクセス・システムのインストールと設定

アクセス・システムを Active Directory Forest にインストールするときは、次の項目を参照してください。

- アクセス・システムのインストール準備
- アクセス・システムのインストールと設定
- Access Server での ADSI の設定（オプション）

アクセス・システムのインストール準備

アクセス・システムのインストールを試行する前に、次の手順が完了していることを確認してください。

アクセス・システムのインストールと設定を準備する手順

1. A-8 ページの「Active Directory に対するインストールと設定の考慮事項」を確認します。
2. A-16 ページの「ID システムのインストール」の説明に従って ID システムをインストールします。
3. A-17 ページの「ID システムの設定」の説明に従って ID システムを設定します。
4. A-19 ページの「ID システム設定の検証」の説明に従って ID システムを検証します。

警告：マシンがドメイン・コントローラではなく、他の Oracle Access Manager データと同じフォレストにある場合、ADSI のために Policy Manager ホストを準備するには、useImplicitBind=1（または 2）、useDNSPrefixedLDAPPaths=true を指定してください。

アクセス・システムのインストールと設定

この環境でアクセス・システムをインストールして設定するには、ガイドとして次の手順を使用します。

- Policy Manager をインストールして設定する手順
- Access Server と WebGate をインストールして設定する手順

Policy Manager をインストールして設定する手順

1. Oracle Access Manager のインストールを開始する前に、必要であれば、ADSI または LDAP over SSL の証明書が各マシンにあることを確認します。

   構成データ、ユーザー・データおよび Oracle Access Manager ポリシー・データを同じディレクトリ・サーバーに置く場合のみ、Identity Server のインストールで使用したのと同じディレクトリ・サーバーの詳細を次の手順で使用します。また、バインド DN として指定した識別名に、ディレクトリ情報ツリー（DIT）のユーザー・ブランチと構成ブランチに対する全面的な権限があることを確認します。

2. 7-3 ページの「Policy Manager のインストール」の説明に従って Policy Manager をインストールします。
   - 該当する場合は、ADSI を使用する Active Directory を選択します。
   - 該当する場合は、動的リンク補助クラスを選択します。
3. 7-10 ページの「Policy Manager の設定」の説明に従って Policy Manager を設定します。次の点を考慮してください。
   - ADSI の場合は、「ADSI を有効化」を選択し、userPrincipleName をバインド DN として入力し（たとえば user@company.com）、設定を完了します。
   - LDAP オープン・バインドの場合は、『Oracle Access Manager アクセス管理ガイド』を参照して Policy Manager の設定を完了します。

警告：Oracle Access Manager サーバーのコンポーネントとデータが別のフォレストにある場合のみ、次の手順を実行します。

4. ¥*PolicyManager_install_dir*¥access¥oblix¥config¥adsi_params.lst ファイルの useDNSPrefixedLDAPPaths 値が true に設定されていることを確認します。次に例を示します。

```
<NameValPair
ParamName="useDNSPrefixedLDAPPaths"
Value="true" />
```

5. ¥*PolicyManager_install_dir*¥access¥oblix¥apps¥common¥bin¥globalparams.lst ファイルで forceExplicitBindUsingDN を確認し、値を true に設定します。次に例を示します。

```
forceExplicitBindUsingDN:true
```

6. Identity Server および WebPass Web サーバーを再起動します。

Access Server と WebGate をインストールして設定する手順

1. Oracle Access Manager のインストールを開始する前に、必要であれば、ADSI または LDAP over SSL の証明書が各マシンにあることを確認します。
2. 187 ページの「Access Server のインストール」の説明に従って Access Server をインストールします。次の項目を考慮してください。
   - 該当する場合は、「ADSI を使用する Active Directory」を選択し、求められたら adsiCredential と adsiPassword を入力します。その後、Access Server を再起動する前に、404 ページの「Access Server での ADSI の設定（オプション）」を実行します。

     adsiCredential と adsiPassword は、暗号化パスワードを生成するために必要です。このパスワードは、ADSI を使用する Active Directory に明示的にバインドするときに使用できます。Oracle Access Manager には暗号化ツールは含まれていないため、求められたときに adsiCredential と adsiPassword の値を入力する必要があります。

     該当する場合は、動的補助クラスを選択します。

     注意：ユーザー・データ、構成データおよびポリシー・データを格納する場所と、ディレクトリ・サーバーの構成の詳細について、確認を求められます。

     Active Directory 2000 を使用する場合は手順 3 を実行する必要があります。Active Directory 2000 では、同一 LDAP 接続の様々な Oracle Access Manager スレッドから受信する同時バインド・リクエストがサポートされないためです。詳細は、A-22 ページの「Active Directory のヒントとトラブルシューティング」を参照してください。
3. **Active Directory 2000:** Access Server で、globalparams.lst ファイルを開き、exclusiveAuthnConnection という新しいフラグを true に設定して追加します。これによって、ディレクトリ・サーバーに送信されるバインド・リクエストに対して、Oracle Access Manager スレッドが強制的に別の LDAP 接続を使用するようになります。
4. **WebGate:** 第 9 章「WebGate のインストール」の説明に従って WebGate をインストールして構成します。

   Active Directory での認証と認可、および Active Directory の特定の機能に対する Oracle Access Manager の構成の詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

Access Server での ADSI の設定（オプション）

ADSI の使用（オプション）を選択した場合は、次の時点で Access Server に ADSI を設定する必要があります。

- Access Server のインストール後
- Access Server の再起動前

Access Server で ADSI を設定する手順

1. 管理ユーザーとしてドメインにログインします。
2. Access Server のサービス・ログイン資格証明をドメインの管理ユーザーに設定します。

   このユーザーは、Policy Manager と Access Server のインストール時に「ルート DN」に指定したユーザーと同じ権限を持つ必要があります。
3. adsi_params.lst ファイルで適切なバインド・メカニズムを選択します。たとえば、2 フォレスト構成では次のようになります。

   ¥*AccessServer_install_dir*¥access¥oblix¥config¥adsi_params.xml

   ```
   useImplicitBind Value="1"
   ```

   デフォルトでは、Access Server の useImplicitBind は 1 フォレスト構成用に 0 に設定されています。ADSI では暗黙のバインドが使用されます。これは、Windows 2000 Server または Windows Server 2003 サービスのログイン資格証明に対応しています。ADSI バインド・メカニズムの詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

   手順 4 と 5 は環境に応じて実行します。
4. Oracle Access Manager コンポーネントを Active Directory Forest 外にインストールしているときは、adsi_params.lst の useDNSPrefixedLDAPPaths パラメータの値が true に設定されていることを確認する必要があります。次に例を示します。

   ```
   useDNSPrefixedLDAPPaths Value="true"
   ```
5. Oracle Access Manager コンポーネントとデータを別のフォレストにインストールしているときは、globalparams.lst ファイルで forceExplicitBindUsingDN パラメータ値を true に設定します。次に例を示します。

   ¥*AccessServer_install_dir*¥access¥oblix¥apps¥common¥bin¥globalparams.lst

   ```
   forceExplicitBindUsingDN Value="true"
   ```
6. Active Directory での認証と認可、および Active Directory の機能に対する Oracle Access Manager の構成の詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

Active Directory のヒントとトラブルシューティング

詳細は、E-4 ページの「Active Directory の問題」を参照してください。

B

ADAM に対する Oracle Access Manager のインストール

Oracle Access Manager では、スタンドアロン・ディレクトリ・サーバーとして Microsoft Active Directory アプリケーション・モード（ADAM）をサポートしています。この付録では次の項目について説明します。

- Oracle Access Manager と ADAM について
- ADAM と Active Directory の違い
- サポートの要件
- ADAM に対する Oracle Access Manager のインストール
- Oracle Access Manager のサイレント・モード・インストールのパラメータ
- ADAM の問題のトラブルシューティング

Oracle Access Manager 10*g*（10.1.4.0.1）へのアップグレードは、『Oracle Access Manager アップグレード・ガイド』を参照してください。

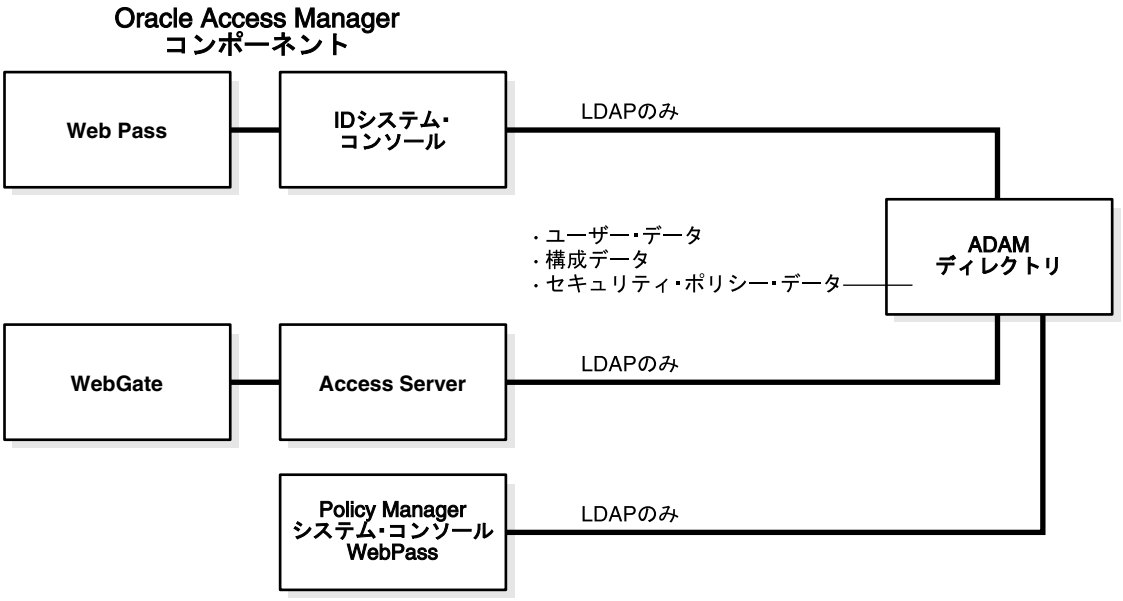
Oracle Access Manager と ADAM について

ここでは、ADAM の概要を説明してから、ADAM を Oracle Access Manager のディレクトリ・サーバーとして使用する場合の詳細を示します。ADAM と Active Directory の違いについても説明します。

注意： Oracle Access Manager では、ユーザー・データを別のタイプのディレクトリ・サーバーに格納することや、Oracle Access Manager の構成データとポリシー・データを ADAM の 1 つ以上のインスタンスに格納することができます。つまり、たとえば、ユーザー・データを Active Directory に、構成データとポリシー・データを ADAM に格納することが可能です。構成データとポリシー・データは、同じディレクトリ・サーバー・タイプに格納する必要があります。

Oracle Access Manager は、ADAM と一緒に 1 台のマシンにインストールする場合も、図 B-1 のように分散環境にインストールする場合も、スタンドアロン・ディレクトリ・サーバーとしての ADAM をサポートします。

図 B-1 Oracle Access Manager のスタンドアロン・ディレクトリ・サーバーとしての ADAM



ADAM は、.NET Active Directory と同じ記憶域管理とプログラミング・モデルを使用します。また、ADAM は、Active Directory と似たレプリケーション・モデルおよび管理モデルを提供します。ただし、ADAM は、Active Directory および Active Directory のドメインやフォレストには依存しません。ADAM には、Active Directory インフラストラクチャの特性や、Windows オペレーティング・システムのためのディレクトリ・サービスは含まれません。また、ドメイン・コントローラも必要としません。ADAM は、オペレーティング・システムのサービスではなく独立したサービスとして実行します。

通常、ADAM は専用ディレクトリ・サービスをアプリケーションに提供します。これには、データ・ストアそのものやデータ・ストアにアクセスするサービスが含まれます。たとえば、ADAM は、小規模事業体向けにアプリケーション固有のディレクトリ・ストアを提供できます。ADAM の情報は、特定のローカル・スキーマの変更を必要とすることがあります。小さなユーザー・グループのみに関連付けることができ、広範に分散する必要はありません。

一意の ADAM インスタンスをインストールするたびに、インスタンスの名前とポートを指定します。名前によって、ファイル、サービス、レジストリおよびポートが結び付けられます。ポートは LDAP および SSL に対して構成できます。ADAM スキーマを Oracle Access Manager

関連の情報で拡張するには、オープン LDAP ポートが必要です。ADAM のための Oracle Access Manager スキーマの変更はありません。

詳細は、次を参照してください。

- ADAM のインスタンスとパーティション
- ADAM スキーマ
- ADAM のための Oracle Access Manager スキーマ拡張機能
- Windows のユーザーとセキュリティ・プリンシパル
- Oracle Access Manager のディレクトリ・プロファイル
- ADAM インスタンスのレプリケーション
- Oracle Access Manager および ADAM での ADSI
- ADAM と API
- 認証、認可およびパスワード変更

ADAM のインスタンスとパーティション

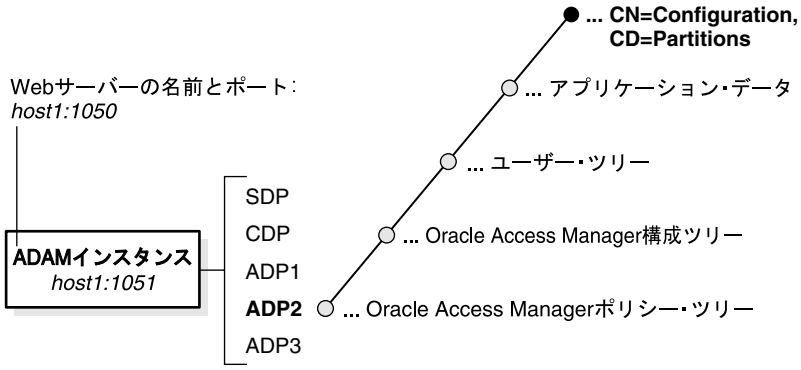
一意の ADAM インスタンスをインストールする際に、スキーマ・ディレクトリ・パーティション（SDP）と構成ディレクトリ・パーティション（CDP）が作成されます。ADAM にはドメイン・パーティションはありません。一意の各インスタンスは個別に構成でき、ADAM のインストールと設定の際またはその後で作成される複数のアプリケーション・ディレクトリ・パーティション（ADP）を含むことができます。

> **重要：** Oracle Access Manager をインストールする前に、アプリケーション・ディレクトリ・パーティションを ADAM に作成してください。Oracle Access Manager は、ADAM に ADP を作成しません。

ADAM ADP は、Active Directory の ADP と似ています。各 ADAM ADP には、ADAM インスタンスのデータ（オブジェクト）が含まれます。ただし、ADAM ADP はセキュリティ・プリンシパル（リソースへのアクセスを制御するために自動的にセキュリティ ID（SID）が割り当てられるアカウント・ホルダー）を格納することはできません。アプリケーションおよびサービスは、アプリケーション固有のデータを格納するために ADAM ADP を使用できます。レプリケーションの必要性が高い、非常に揮発性が高い情報を含むこともできます。このような情報は、ネットワーク・オペレーティング・システム（NOS）のディレクトリに格納するとリソースに負荷がかかることがあります。

当初、Oracle Access Manager は、1 つの ADAM インスタンス内の 1 つの ADP をサポートしていました。図 B-2 に示すように、ADP は、アプリケーション固有のデータだけでなく、ユーザー・ツリー、Oracle Access Manager 構成ツリー、Oracle Access Manager ポリシー・ツリーを含むことができます。

図 B-2 1 つの ADAM のインスタンスと複数のパーティション



注意: Oracle Access Managerでは、単一インスタンスまたは複数インスタンスでの複数ADPをサポートしています。また、マスター・インスタンスとそのレプリカもサポートします。

注意: Oracle Access Managerでは、構成およびポリシーDNのためにorganizationalUnitのobjectclass属性値を含むノードが必要です。これは、ouを作成するとデフォルトで追加されます。

注意： Oracle Access Manager は、複数の ADAM インスタンスと複数の ADP をサポートしています。現在は、ユーザー・データを異なるディレクトリ・サーバー・タイプに格納できます。たとえば、Oracle Access Manager の構成データとポリシー・データを ADAM に格納するときは、単一 ADAM ADP またはインスタンス、または別の ADAM ADP またはインスタンスに格納することができ、ユーザー・データを Active Directory に格納することが可能です。

ADAM スキーマ

ADAM は、Windows Server 2003 プラットフォームの Active Directory と同様に、動的リンク補助クラスをサポートしています。Oracle Access Manager は、動的リンクと静的リンク両方の補助クラスをサポートしています。

ADAM スキーマには、ADAM が構成設定内でアクセスできるオブジェクト・クラスの定義が含まれます。また、スキーマには、ADAM が ADAM オブジェクト内でアクセスできる属性の定義も含まれます。構成設定の詳細は、B-8 ページの「ADAM インスタンスのレプリケーション」を参照してください。

ADAM スキーマには柔軟性があります。ネームスペースの制約はありません。ADAM は、様々なタイプの情報（スキーマ、サイト、パーティションおよびサービス）に X.500 形式のネーミング・コンテキスト（o=,c=）を使用できます。ADP 内では、ユーザー検索ベース、構成 DN およびポリシー・ベースを同じにすることも（o=company,c=us）、変えることもできます。

注意： Oracle Access Manager では、構成およびポリシー DN のために organizationalUnit（ou）の objectclass 属性値を含むノードが必要です。これは、ou を作成するとデフォルトで追加されます。

異なるネームスペースの例を次に示します。

検索ベース : o=*company*,c=us
構成 DN: ou=config,o=*company*,c=us
ポリシー・ベース : ou=policy,o=*company*,c=us

注意 : ユーザー・データを別のタイプのディレクトリ・サーバーに格納し、Oracle Access Manager の構成データとポリシー・データを 1 つ以上の ADP または 1 つ以上の ADAM インスタンスに格納するときは、様々なネームスペースが必要になります。

ADAM のスキーマは Active Directory のスキーマと似ていますが、ユーザー・オブジェクト・クラスは ADAM と Active Directory では異なります。ADAM にはセキュリティ・プリンシパルは付いていません。たとえば、*saMAccountName* は Active Directory ではユーザーとグループのために必須ですが、ADAM にはありません。ただし、*grouptype* は必須です。

ADAM グループ・オブジェクト・クラス "group" の grouptype 属性に指定できるのは、次に示す値のみです。これらは、メタ属性構成アプレットで「表示タイプ」のラジオ・ボタンを使用して、オブジェクト・クラスについて構成する必要があります（「ID システム・コンソール」→「Group Manager」→「タブの構成」→「属性の変更」）。

global - 2
domain local - 4
universal - 8
secure domain - -2147683644
secure global - -2147482646

Active Directory では password 属性は unicodePwd です。ADAM の password 属性は *userpassword* です。*uid* 属性には、セマンティク型「ログイン」がデフォルトで割り当てられます。

Active Directory アプリケーション・モード（ADAM）のスキーマは、Ldifde.exe コマンドライン・ツールを使用して拡張することができます。

ADAM のための Oracle Access Manager スキーマ拡張機能

ADAM のための Oracle Access Manager スキーマ拡張機能は、Windows セキュリティ・プリンシパルの資格証明を使用してロードする必要があります。ただし、実行時には、Oracle Access Manager は ADAM 内のユーザーのみと通信し、セキュリティ・プリンシパルとは通信しません。詳細は、B-7 ページの「Windows のユーザーとセキュリティ・プリンシパル」を参照してください。

Oracle Access Manager をインストールするときに、ADAM スキーマを手動で更新する必要があります。ユーザー・データ・ディレクトリのインスタンスが、構成およびポリシーのデータ・ディレクトリ・インスタンスと異なる場合は、ADAM_user_schema_add.ldif ファイルを手動でアップロードする必要があります。

構成データ・ディレクトリ・インスタンスでは、ADAM_oblix_schema_add.ldif ファイルを手動でアップロードする必要があります。静的補助クラスを使用するときは、ADAMAuxSchema.ldif ファイルを手動でアップロードする必要があります。

ポリシー・データ・ディレクトリのインスタンスが、構成データ・ディレクトリのインスタンスと異なる場合は、ADAM_oblix_schema_add.ldif ファイルを手動でアップロードする必要があります。静的補助クラスを使用するときは、ADAMAuxSchema.ldif ファイルを手動でアップロードする必要があります。

Oracle Access Manager では、User と Group に加えて、InetOrgperson と GroupofUniqueNames がそれぞれ標準の Person オブジェクト・クラスおよび Group オブジェクト・クラスとしてサポートされます。すでに使用中のオブジェクト・クラスがあれば、特定のオブジェクト・クラスを使用する必要はありません。また、Oracle Access Manager では、静的リンク補助クラスと動的リンク補助クラスがサポートされます。

ADAM スキーマは、単純な LDAP バインドでは変更できません。ldapmodify ではなく ldifde を使用して変更する必要があります。現在、ldifde は ADAM 上の SSL ポートへのバインドをサポートしていません。このため、ADAM スキーマを Oracle Access Manager のために拡張できるのはオープン・ポートの場合のみです。Identity Server のインストールの際に、SSL 接続を指定して ADAM の SSL 証明書を取得し、その後、スキーマ更新でオープン・ポート番号を指定することができます。

注意： ADAM では、スキーマの更新は、オープン・ポートと Windows セキュリティ・プリンシパルの資格証明を使用して完了する必要があります。

Oracle Access Manager では、Oracle Access Manager の構成ディレクトリとユーザー・ディレクトリのために次のスキーマ・ファイルが提供されます。スキーマを手動で更新するには、次のファイルを使用する必要があります。

IdentityServer_install_dir¥identity¥oblix¥data.ldap¥common¥
ADAM_oblix_schema_add.ldif
ADAM_user_schema_add.ldif

また、静的リンク補助クラスを使用している場合は、次のファイルに対して ldifde コマンドを実行する必要もあります。

IdentityServer_install_dir¥identity¥oblix¥data.ldap¥common¥
ADAMAuxSchema.ldif

スキーマを手動で更新するための ldifde コマンドの例を次に示します。表 B-1 でも説明します。詳細は、Microsoft 社のドキュメントを参照してください。

ldifde -k -b
"<*user_distinguished_name*>""<*domain_name*>""<*user_password*>"
-c"<GUID>"<*ADAM_instance_ID*> -i -f ADAM_oblix_schema_add -s
<*ADAM_server_name*> -t <*port*>

表 B-1 ADAM のための ldifde コマンドの説明

オプション	説明
-k	このオプションはエラーを無視する。
-b "<*user_distinguished_name*>" "<*domain_name*>" "<*user_password*>" 例 : cn=administrator,o=oblix.com,c=us password	スキーマを拡張するための各値 : ■ Windows セキュリティ・プリンシパルのユーザー名 ■ ADAM がインストールされているマシンのドメイン名 ■ パスワード
-c "<GUID>" <*ADAM_instance_ID*>	このオプションでは、"<GUID>" は他の値で置き換えずにそのまま使用する。引用符も含める。<*ADAM_instance_ID*> は、ldp.exe などのツールを使用して ADAM ルート DSE で置き換える。最初に接続したときにルート DSE が表示される。たとえば、ADAM ルート DSE 値は EC31B31B-19FC-4FD4-8590-3BD57D6A3E77。
-i	-i オプションはインポート・オプションを指定する。
-f <filename>	-f オプションはファイルを指定する。値には、インポートするファイル名を指定する。 例 : ADAM_oblix_schema_add.ldif ADAMAuxSchema.ldif
-s <*ADAM_server_name*>	この値は、ADAM がインストールされているマシンのドメイン名。
-t <*port* >	この値は、このインスタンスがスキーマの更新をリスニングするポート番号（オープン・ポートが必要）。

Windows のユーザーとセキュリティ・プリンシパル

ADAM は、ユーザー資格証明をサポートし、認証とアクセス制御に Windows セキュリティ・プリンシパル資格証明を使用します。たとえば、Windows セキュリティ・プリンシパルは、ユーザーを定義して ADAM ディレクトリ・ストアのインスタンスをレプリケートする権限を提供します。一方、Oracle Access Manager では、ADAM スキーマを更新するためだけに Windows セキュリティ・プリンシパル資格証明が必要です。

スキーマ更新のための Windows セキュリティ・プリンシパル : Oracle Access Manager Identity Server を ADAM に対してインストールし、スキーマを更新するときは、次のようにディレクトリ・サーバーの詳細を指定する必要があります。

- **自動スキーマ更新 :** 使用できません。スキーマは手動で更新する必要があります。
- **手動スキーマ更新 :** スキーマを手動で拡張するときは、B-5 ページの「ADAM のための Oracle Access Manager スキーマ拡張機能」の説明に従って、Windows セキュリティ・プリンシパルの名前とパスワードを ldifde コマンドに指定する必要があります。次に例を示します。

  -b "<*user_distinguished_name*>""<*domain_name*>""<*user_password*>"

ルート（バインド）DN に対する ADAM 内の Windows ユーザー : 実行時に、Oracle Access Manager は ADAM 内のユーザーのみと通信し、Windows セキュリティ・プリンシパルとは通信しません。ID システムの設定の際に、ADAM のルート（バインド）DN とそのユーザーのパスワードを、ユーザー・データ構成のディレクトリ・サーバーを指定するページで指定する必要があります。これは、管理者権限を持つ、ADAM 内のバインド可能なユーザーの名前であることが必要です。

管理者権限を持つ、ADAM 内のバインド可能なユーザーのルート DN 名
管理者権限を持つ、ADAM 内のバインド可能なユーザーのルート DN パスワード

ms-bindable-object 補助オブジェクト・クラスを people オブジェクトのために使用しているオブジェクト・クラス（inetOrgPerson など）に追加することで、バインド可能なユーザーを ADAM に作成します。

Oracle Access Manager の管理者は、Windows セキュリティ・プリンシパルではなく、管理権限を持つ ADAM のバインド可能なユーザーであることが必要です。

Oracle Access Manager のディレクトリ・プロファイル

Oracle Access Manager を設定すると、通常、Identity Server、Policy Manager および Access Server に対して個別のディレクトリ・プロファイルが作成されます。ID システムの設定時に、SSL 対応ポートを指定して、Oracle Access Manager 内のディレクトリ・プロフィルを適切に構成します。

Oracle Access Manager をインストールした後のディレクトリ・プロファイルの構成の詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

ADAM インスタンスのレプリケーション

ADAM インスタンスのレプリケーションによって構成設定が作成されます。構成設定内のすべての ADAM インスタンスは、共通のスキーマ・パーティションと構成パーティションをレプリケートします。ADP（o=company,c=US など）もレプリケートできます。完全レプリケートのみが Oracle Access Manager でサポートされています。

Oracle Access Manager では、フェイルオーバー、およびマスター・インスタンスとレプリカの間のロード・バランシングが提供されます。ただし、Oracle Access Manager は、ADAM での ADSI はサポートしていません。詳細は、B-8 ページの「Oracle Access Manager および ADAM での ADSI」を参照してください。

通常、ADAM の複数インスタンスは 1 つのサーバーで同時に実行できます。各インスタンスには独自のスキーマと構成が含まれます。

注意： フォレスト内に ADAM インスタンスをレプリケートすることはできません。本番環境では、同じ構成設定内の ADAM インスタンスが同じマシンに存在することはできません。詳細は、Microsoft 社のドキュメントを参照してください。

Oracle Access Manager および ADAM での ADSI

ADSI は Active Directory 環境でのフェイルオーバーのサポートを提供し、Oracle Access Manager は Active Directory での ADSI をサポートします。ADAM は Active Directory Service Interfaces（ADSI）をサポートしています。ただし、Oracle Access Manager は、ADAM での ADSI はサポートしていません。

ADAM には、ドメイン・コントローラがないため、Oracle Access Manager ディレクトリ・サーバー固有のフェイルオーバーと接続管理ツールキットをお薦めします。フェイルオーバーとロード・バランシングの詳細は、『Oracle Access Manager デプロイメント・ガイド』を参照してください。

ADAM と API

ADAM は、標準アプリケーション・プログラミング・インタフェース（API）を使用してアプリケーション・データにアクセスします。これには、Active Directory API、Lightweight Data Access Protocol および System-Directory Services が含まれます。

ADAM では、Messaging Application Programming Interface（API）はサポートされません。このため、Microsoft Exchange は ADAM を使用できません。詳細は、Microsoft 社のドキュメントを参照してください。

認証、認可およびパスワード変更

認証と認可のプロセスは、ADAM ではなく Oracle Access Manager で管理する必要があります。これにより、認証と認可について Oracle Access Manager の "rules" と ADAM の "rules" の競合が回避されます。Oracle Access Manager の認証と認可のプロセスは、ADAM と Active Directory のどちらを使用する場合も同じです。詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

Oracle Access Manager と一緒に使用する場合、ADAM は Active Directory を指すプロキシ・オブジェクトを使用できません。ユーザーは、ADAM 内で有効化され、パスワードを持っている必要があります。

Active Directory と Oracle Access Manager を一緒に使用するとき、固有のパスワード管理または Oracle Access Manager を使用できます。パスワード管理は ADAM にも含まれます。Active Directory と ADAM は両方とも、セキュアな接続（SSL または ADSI）に対するパスワード変更をサポートしています。ただし、Oracle Access Manager では、ADAM に対する ADSI がサポートされないため、ADAM でのパスワード変更には SSL を使用する必要があります。

ADAM と Active Directory の違い

ADAM と Active Directory の違いを次の表にまとめています。

表 B-2 Oracle Access Manager に対する ADAM と Active Directory の違い

説明
ADAM と Active Directory は、同じネットワークで同時に稼働できる。Oracle Access Manager では、それぞれを個別または一緒に使用可能。
ADAM の情報は、特定のローカル・スキーマの変更を必要とすることがある。小さなユーザー・グループのみに関連付けることができ、広範に分散する必要はない。
アプリケーションとサービスは、アプリケーション固有データの格納に ADAM ADP を使用できる。レプリケーションの必要性が高い、非常に揮発性の高い情報も格納できる。
ADAM にはセキュリティ・プリンシパルは付いていない。たとえば、saMAccountName は、Active Directory ではユーザーとグループのために必須だが、ADAM にはない。
ADAM の password 属性は userpassword。
Oracle Access Manager では、ADAM スキーマの更新に Windows セキュリティ・プリンシパル資格証明が必要。実行時には、Oracle Access Manager は ADAM 内のユーザーのみと通信し、セキュリティ・プリンシパルとは通信しない。
Active Directory と ADAM の両方とも ADSI をサポートしている。ただし、Oracle Access Manager では、ADSI は Active Directory のみでサポートされる。暗黙のバインドは Active Directory のみで使用可能、ADAM では使用不可。
Active Directory と ADAM の両方ともパスワード変更をサポートしている。ADAM を使用する Oracle Access Manager では、パスワード変更のために SSL 対応ポートが必要。

ADAM の詳細は、Microsoft 社のドキュメントを参照してください。

サポートの要件

ADAM と Active Directory は、同じネットワークで同時に稼働できます。Oracle Access Manager では、ADAM 単独の使用もサポートしています。また、Oracle Access Manager では、ユーザー・データを構成データやポリシー・データと別に格納するために、ADAM と Active Directory の使用や ADAM と他のディレクトリ・サーバー・タイプの使用もサポートしています。

- すべてのユーザー・データは、同じディレクトリ・サーバー・タイプに格納する必要があります。
- 構成データとポリシー・データは、同じディレクトリ・サーバー・タイプに格納する必要があります。
- Oracle Access Manager では、構成およびポリシー DN のために organizationalUnit（ou）の objectclass 属性値を含むノードが必要です。

Oracle Access Manager 10*g*（10.1.4.0.1）での LDAP のサポートは、`https://metalink.oracle.com` の「Certify」タブを参照してください。

スキーマの更新は、ldifde コマンドを使用して手動で実行する必要があります。
詳細は、B-5 ページの「ADAM のための Oracle Access Manager スキーマ拡張機能」を参照してください。

ADAM に対する Oracle Access Manager のインストール

次のタスクがインストール手順に含まれます。

タスクの概要 : ADAM に対する Oracle Access Manager のインストール

1. 第 I 部「インストールの計画と前提条件」の説明に従って環境を準備します。
2. B-10 ページの「Oracle Access Manager のための ADAM の準備」の説明に従って ADAM を準備します。

> **注意 :** Oracle Access Manager では、構成およびポリシー DN のために organizationalUnit（ou）の objectclass 属性値を含むノードが必要です。

3. B-12 ページの「ADAM に対する ID システムのインストールと設定」の説明に従って、ID システムをインストールして設定します。
4. アクセス・システムを環境に含める場合は、B-14 ページの「ADAM に対するアクセス・システムのインストール」の説明に従ってアクセス・システムをインストールして設定します。
5. Oracle Access Manager のインストールと設定が正常に終了したら、次の任意のアクティビティを実行します。
   - 『Oracle Access Manager ID および共通管理ガイド』の説明に従って ADAM ユーザーを Oracle Access Manager に追加します。
   - Microsoft 社のドキュメントの説明に従って ADAM インスタンスをレプリケートします。
   - 『Oracle Access Manager デプロイメント・ガイド』の説明に従って、ADAM のマスターとレプリカのためにフェイルオーバーとロード・バランシングを構成します。

Oracle Access Manager のための ADAM の準備

この後の手順では、Oracle Access Manager が認証と認可を管理できるように、ADAM インスタンスと ADP を準備する方法を説明します。一意の ADAM インスタンスをインストールし、ユーザー・データのために ADP と最上位 DN を作成し、ADAM にユーザーを作成します。次の重要事項に注意してください。

ADP: ADAM 内でアプリケーション・ディレクトリ・パーティションを作成する必要があります。Oracle Access Manager は ADP を作成しません。

管理者 : 少なくとも 1 つのアカウントを ADAM インスタンス管理者として指定する必要があります。ADAM インスタンス管理者は、ID システムの設定時にマスター管理者として指定する必要もあります。マスター管理者は、Windows セキュリティ・プリンシパルではなく、管理権限を持つ ADAM のバインド可能なユーザーであることが必要です。

構成およびポリシー DN: Oracle Access Manager では、構成およびポリシー DN のために organizationalUnit（ou）の objectclass 属性値を含むノードが必要です。

ADSI: Oracle Access Manager では、ADAM での ADSI はサポートされません。ADAM では、Oracle Access Manager ディレクトリ・サーバー固有のフェイルオーバーおよび接続管理ツールキットを使用する必要があります。

プロキシ・オブジェクトによるバインド : Oracle Access Manager では、ADAM プロキシ・オブジェクトを介したバインドはサポートされません。

> **注意 :** 次の手順を完了しないと、Oracle Access Manager のインストールが正常に終了しない場合があります。ADAM のインストールやインスタンスの設定などのタスクの詳細、および ADAM ADSI Edit や Ldp.exe などのツールの詳細は、ADAM のダウンロードに含まれる Microsoft 社のドキュメントを参照してください。

Oracle Access Manager のために ADAM をインストールする手順

1. ADAM のダウンロードに含まれる Microsoft 社のドキュメントの説明を読んで、ADAM の概念、操作およびツールをよく理解します。
2. ADAMSetup.exe を ADAM のインストール・ディレクトリから実行して、Windows Server 2003 マシンに一意の ADAM インスタンスをインストールします。

   インストール・プログラムのこの後の画面で、次のような情報の指定や操作の実行を求められます。

   a. 一意のインスタンス

   b. 有効なインスタンス名（たとえば、OracleAccessManager）

   c. このインスタンスを実行するポート番号

   d. アプリケーション・ディレクトリ・パーティションの作成（「Yes」または「No」）

      * 「Yes」は新しいパーティションを作成します。たとえば、o=company, c=us,（デフォルト）。

      * 「No」の場合、すでに存在しているパーティションを指定します。

   e. ADAM をインストールするディレクトリ

   f. サービス・アカウントの選択（この後の処理に使用するアカウントを選択します）

      * ネットワーク・サービス・アカウント（デフォルト）

      * カスタム・アカウント（このアカウントをアクティブにします）

   g. 選択したアカウントへの権限の割当て

   h. ユーザーの LDIF ファイルのインポート（たとえば MS_User.ldf）
3. 次の操作を行います。

   a. Oracle Access Manager のために ADAM スキーマを拡張するためのオープン LDAP ポート番号と、Oracle Access Manager でのパスワード変更、認証および認可のための SSL 対応ポートを指定します。

   b. ユーザー・データおよび Oracle Access Manager の構成データとポリシー・データを格納する（あるいは、ユーザー・データは別のディレクトリ・サーバー・タイプに格納して、構成データとポリシー・データを格納する）ためのアプリケーション・ディレクトリ・パーティション（ネーミング・コンテキスト）を作成します。インスタンスに存在していない識別名を指定してください。
4. ADAM インスタンスを起動します。

   たとえば、「スタート」→「プログラム」→「ADAM」→「ADAM ADSI EDIT」を選択します。
5. 「ADAM ADSI EDIT」を右クリックし、メニューから「Connect」を選択します。

   次のオプションを含むユーザー画面が表示されます。

   a. **Connection Name:** OAM など

   b. **Host Name:** ローカル・ホスト

   c. **Port:** 作成したインスタンスのポート番号

   d. **DN:** バインド DN

   e. **Credentials**

注意： ms-bindable-object を ADAM に追加する必要があります。詳細は、B-7 ページの「Windows のユーザーとセキュリティ・プリンシパル」を参照してください。

---

6. バインド可能な ADAM ユーザー・アカウントを作成して有効化し、ADAM ADSI Edit を使用して、マスター管理者として指定するユーザーを次のように member 属性に追加します。

   ```
   CN=Administrators,CN=Roles,CN=Configuration,CN={your GUID}
   ```

7. ユーザー・パスワードをリセットします。
8. ユーザーをアクティブ化します。
9. ADAM インスタンスのディレクトリ・パーティションを管理します。
10. ADAM 構成設定を管理します。
11. 次に進む前に、ADAM のインストールが正常に作動していることを確認します。

ADAM に対する ID システムのインストールと設定

ここで説明する手順では、B-10 ページの「Oracle Access Manager のための ADAM の準備」のすべての手順を完了していることが前提です。開始する前に、次に示すいくつかの重要な項目について確認してください。

スキーマの更新 : Oracle Access Manager のための ADAM スキーマの更新はオープン・ポートを使用して実行する必要があります。詳細は、B-5 ページの「ADAM のための Oracle Access Manager スキーマ拡張機能」を参照してください。

スキーマの更新は、Windows セキュリティ・プリンシパルの資格証明を使用して実行する必要があります。ただし、ID システムの設定時に指定するルート（バインド）DN は、ADAM 内に明示的な物理的位置のあるユーザーであることが必要です。詳細は、B-7 ページの「Windows のユーザーとセキュリティ・プリンシパル」を参照してください。

ID システムの設定 : ID システムの設定の際に、パスワード変更のために SSL 対応接続を指定する必要があります。詳細は、B-8 ページの「認証、認可およびパスワード変更」を参照してください。

管理者 : ID システムの設定時に指定するマスター管理者は、Windows セキュリティ・プリンシパルではなく、管理権限を持つ ADAM ユーザーであることが必要です。

この後の手順では、Oracle Access Manager および ADAM に固有な情報を示します。各 Oracle Access Manager コンポーネントのインストールの詳細は、このガイドの該当する章を参照してください。

Identity Server をインストールして ADAM スキーマを更新する手順

1. ダウンロードした Identity Server インストール・パッケージを選択してインストールを開始します。
2. インストール・ディレクトリ、トランスポート・セキュリティ・モード、および Oracle Access Manager のための Identity Server 構成の詳細を指定します。
3. Identity Server と ADAM の間で SSL を使用するように「はい」を選択し、証明書に関するすべての質問に回答します。後で、Oracle Access Manager のために ADAM スキーマを拡張するようにオープン・ポートを指定することができます。
4. ADAM に関する詳細を次のように指定します。
   a. **ディレクトリ・サーバー・タイプ :**「ディレクトリ・サーバー」ドロップダウン・リストから「Active Directory アプリケーション・モード」を選択して ADAM を指定します。
   b. **データの場所 :** 構成データとユーザー・データを別に格納するかどうかを指定します。
   c. **スキーマの更新 :** 表示される手順を確認して、スキーマを手動で更新します。

      インストール・プロセスを続行し、手順 6 と 7 の説明に従ってスキーマを更新します。
5. B-12 ページの「Identity Server をインストールして ADAM スキーマを更新する手順」の説明に従って、Identity Server のインストールを終了し、Identity Server を起動します。

6. **手動スキーマ更新の準備 :** 手順 7 で手動スキーマ更新を実行する前に、次のファイルの <guid> を実際の GUID で置き換えてください。

   - ADAM_oblix_schema_add.ldif
   - ADAM_oblix_user_schema_add.ldif
   - ADAMAuxSchema_add.ldif

7. **手動スキーマ更新 :** 必要であれば、適切なファイルと ldifde コマンドを使用してドメイン・ユーザーとしてスキーマを手動で更新し、Identity Server を再起動します。次に例を示します。

   IdentityServer_install_dir¥identity¥oblix¥data.ldap¥common¥

   ADAM_oblix_schema_add.ldif
   ADAM_oblix_user_schema_add.ldif

```
ldifde -k -b <cn=administrator,o=company,c=us password> -c"<GUID>"
<ADAM_instance_ID> -i -f ADAM_oblix_schema_add.ldif -s <ADAM_server_name>
-t <port>

ldifde -k -b <cn=administrator,o=company,c=us password> -c"<GUID>"
<ADAM_instance_ID -i -f ADAM_oblix_user_schema_add.ldif
-s ADAM_server_name -t <port>
```

   注意 : 前の例の Windows セキュリティ・プリンシパルの名前とドメインはサンプルです。環境によって異なります。

   動的補助クラスを使用する予定がない場合は、前述のコマンドを実行した後で次のようにします。

   - ldifde コマンドを使用して、静的リンク補助クラスのための Oracle Access Manager スキーマ・ファイル ADAMAuxSchema.ldif を *IdentityServer_install_dir*¥identity¥oblix¥data.ldap¥common ディレクトリからインポートします。
   - オブジェクト・クラス oblixorgperson と oblixgroup が、Person オブジェクト・クラスと Group オブジェクト・クラスそれぞれに補助クラスとして明示的に追加されていることを確認します。

   注意 : スキーマを手動で更新したら必ず Identity Server を再起動してください。

   この後の手順では、WebPass をインストールし ADAM に対して ID システムを設定する際に指定する必要がある情報をまとめています。

WebPass をインストールして ID システムを設定する手順

1. B-14 ページの「WebPass をインストールして ID システムを設定する手順」の説明に従って、ダウンロードした WebPass をインストールします。
2. B-12 ページの「ADAM に対する ID システムのインストールと設定」の説明に従って ID システムの設定を開始し、ADAM に関する詳細を次のように指定します。
   a. **ディレクトリ・サーバー・タイプ :** ディレクトリ・サーバー・タイプを指定するときに Microsoft Active Directory アプリケーション・モードを選択し、環境で該当する場合は動的補助オブジェクト・クラスを選択します。
   b. **ディレクトリ・サーバーの場所 :** ADAM について次のように指定します。

      ポート番号 : 実行時に使用されるポートを指定します（パスワード変更のために SSL が必要です）。

      ルート DN: バインド DN として管理権限を持つ、ADAM のバインド可能なユーザーの名前。Windows セキュリティ・プリンシパルは指定しないでください。

      ルート・パスワード : ADAM のバインド可能なユーザーのパスワード。

      ディレクトリ・サーバー・セキュリティ・モード : パスワード変更のために SSL を指定します。
3. 通常どおりに ID システムの設定を終了します。
4. ID システムの設定が終了したら、続けて次の任意のアクティビティを実行します。
   - アクセス・システムを環境に含める場合は、B-14 ページの「ADAM に対するアクセス・システムのインストール」の説明に従って ADAM に対してアクセス・システムをインストールします。
   - 『Oracle Access Manager ID および共通管理ガイド』の説明に従って ADAM ユーザーを Oracle Access Manager に追加します。
   - Microsoft 社のドキュメントの説明に従って ADAM インスタンスをレプリケートします。
   - 『Oracle Access Manager デプロイメント・ガイド』の説明に従って、ADAM のマスターとレプリカのためにフェイルオーバーとロード・バランシングを構成します。

ADAM に対するアクセス・システムのインストール

アクセス・システム（オプション）には、Policy Manager、Access Server および WebGate が含まれます。この後の手順では、オプションのアクセス・システムを ADAM に対してインストールおよび設定するための詳細を説明します。

詳細は、次の手順を参照してください。

- ADAM に対して Policy Manager をインストールする手順
- Access Server をインストールする手順
- ADAM に対して Policy Manager を設定する手順
- WebGate をインストールする手順

ADAM では、ポリシー・データをユーザー・データや Oracle Access Manager 構成データと一緒に格納することできます。また、Oracle Access Manager では、構成データ、ユーザー・データおよびポリシー・データのそれぞれに対する個別の ADAM インスタンスもサポートしています。

ADAM に対して Policy Manager をインストールする手順

1. B-15 ページの「ADAM に対して Policy Manager をインストールする手順」の説明に従って、Policy Manager のインストール・パッケージを探して起動し、インストール・ディレクトリを指定します。
2. ディレクトリ・サーバー・タイプを確認されたら、Microsoft Active Directory アプリケーション・モードを選択します。
3. 環境で動的リンク補助オブジェクト・クラスを有効にする場合は「はい」、そうでない場合は「いいえ」を選択します。
4. インストールの後でスキーマを手動で更新します。

   注意 : 自動スキーマ更新はサポートされていません。

5. ディレクトリ・サーバー・セキュリティ・モードを指定します。ADAM でのパスワード変更には SSL 対応が必要です。
6. B-15 ページの「ADAM に対して Policy Manager をインストールする手順」の説明に従い、アクセス・システムのトランスポート・セキュリティ・モードを指定し、Web サーバーを構成し、Policy Manager をインストールします。
7. 次の手順に進んで、Policy Manager を設定します。

ADAM に対して Policy Manager を設定する手順

1. B-15 ページの「ADAM に対して Policy Manager をインストールする手順」の説明に従って Policy Manager の設定プロセスを開始し、ADAM に関する詳細を次のように指定します。
   a. **ディレクトリ・サーバー・タイプ :** ディレクトリ・サーバー・タイプを指定するときに Microsoft Active Directory アプリケーション・モードを選択し、環境で該当する場合は動的補助オブジェクト・クラスを選択します。
   b. **ディレクトリ・サーバー詳細 :** ADAM について次のように指定します。

      ポート番号 : 実行時に使用されるポートを指定します（パスワード変更のために SSL が必要です）。

      ルート（バインド）DN: Identity Server の設定時に指定したルート DN を指定します。Windows セキュリティ・プリンシパルは使用しないでください。

      パスワード : バインド DN ユーザーのパスワードを指定します。

      ディレクトリ・サーバー・セキュリティ・モード : パスワード変更のために SSL を指定します。
2. ADAM の検索ベース、構成 DN およびポリシー・ベースを指定します。詳細は、B-4 ページの「ADAM スキーマ」を参照してください。
3. B-15 ページの「ADAM に対して Policy Manager を設定する手順」の説明に従って Policy Manager の設定プロセスを終了します。

   注意 : この設定の終了時に警告が表示され、Oracle Access Manager のポリシーを有効化する前に匿名ユーザーを作成するように指示されることがあります。

4. ADAM 内で、Policy Manager の設定時に指定した検索ベースの最上位に、OblixAnonymous ユーザーが作成されていることを確認します。
5. 次の手順に進んで、Access Server をインストールします。

Access Server をインストールする手順

1. 191 ページの「Access Server インスタンスの作成」の説明に従って、アクセス・システム・コンソールで Access Server インスタンスを作成します。
2. B-16 ページの「Access Server をインストールする手順」の説明に従って、Access Server のインストール・パッケージを探して起動し、インストール・ディレクトリを指定します。
3. Access Server のトランスポート・セキュリティ・モードを選択します。
4. 求められたら ADAM の詳細を指定します。
   - **SSL:** SSL はパスワード変更のために必要です。
   - **ポート番号 :** 実行時に使用されるディレクトリ・サーバーのポート。
   - **バインド（ルート）DN:** Identity Server と Policy Manager の設定時に指定したルート DN。Windows セキュリティ・プリンシパルは使用しないでください。
   - **パスワード :** バインド DN のパスワード。
   - **ディレクトリ・サーバー・タイプ :** Active Directory アプリケーション・モード。
5. 環境で動的リンク補助クラスを有効にする場合は「はい」、そうでない場合は「いいえ」を選択します。
6. ディレクトリ・サーバーの証明書ファイルのパスを指定します。
7. Access Server ID、構成 DN およびポリシー・ベースを指定します。これらは ADP 内で一意とすることができます。次に例を示します。

   Access Server ID: *Access_Server_1014_A*

   構成 DN: ou=*config*,o=*company*,c=us

   ポリシー・ベース : ou=*policy*,o=*company*,c=us

   注意 : この例では、すべてのデータを 1 つの ADAM インスタンスと ADP に格納していると仮定しています。

8. 197 ページの「Access Server のインストールの終了」の説明に従って Access Server のインストールを終了します。
9. 次の手順に進んで、WebGate をインストールします。

WebGate をインストールする手順

1. B-16 ページの「WebGate をインストールする手順」の説明に従って、アクセス・システム・コンソールで WebGate インスタンスを作成します。
2. 207 ページの「WebGate および Access Server の関連付け」の説明に従って WebGate を Access Server に関連付けます。
3. B-16 ページの「WebGate をインストールする手順」の説明に従って WebGate をインストールします。
4. アクセス・システムのインストールと設定が終了したら、次の任意のアクティビティを実行します。
   - 『Oracle Access Manager ID および共通管理ガイド』の説明に従って ADAM ユーザーを Oracle Access Manager に追加します。
   - Microsoft 社のドキュメントの説明に従って ADAM インスタンスをレプリケートします。
   - 『Oracle Access Manager デプロイメント・ガイド』の説明に従って、ADAM のマスターとレプリカのためにフェイルオーバーとロード・バランシングを構成します。

Oracle Access Manager のサイレント・モード・インストールのパラメータ

Oracle Access Manager サイレント・モード・インストーラには、スタンドアロン・ディレクトリ・サーバーとして ADAM をサポートするためにいくつかの変更が加えられています。詳細は、次を参照してください。

- ADAM のための Identity Server サイレント・モード・インストーラ
- ADAM のための Policy Manager サイレント・モード・インストーラ
- ADAM のための Access Server サイレント・モード・インストーラ

注意 : 動的補助フラグは、Windows 2003 上の Active Directory の場合と同様に、Oracle Access Manager で ADAM に対して構成できます。

ADAM のための Identity Server サイレント・モード・インストーラ

Identity Server サイレント・インストーラには、ADAM のために次の変更が加えられています。

- **Windows ユーザー名と Windows ドメイン :** ADAM スキーマを更新するために、Windows セキュリティ・プリンシパル名、Windows ドメイン名およびパスワードを指定します。これはバインド DN としては使用されません。
- **自動スキーマ更新 :** ADAM に対してサポートされていません。
- **手動スキーマ更新 :** Windows Server 2003 に最初に Identity Server をインストールする際に手動スキーマ更新を指定するには、次のようにします。

  ```
  -W updateDSInfo.updateDSInfoChoice="No"
  ```

  内容は次のとおりです。

  `-W updateDSInfo.updateDSInfoChoice="No"` によって、手動スキーマ更新が指定されます。

- **ADAM のための Windows ドメイン名 :** ADAM のための Windows ドメイン名を指定するには、次のようにします。

  ```
  -W dsInfoInput.domainName="domainname.com
  ```

  内容は次のとおりです。

  `-W dsTypeInput.dsType=9`（ADAM）の場合に、`-W dsInfoInput.domainName` によって ADAM のための Windows ドメイン名が指定されます。

  "*domainname*.com" は、ADAM マシンが存在するドメイン名です。正しくないドメイン名を指定すると、ディレクトリの認証が失敗します。

注意 : これは新しいパラメータです。既存のサイレント・インストーラ・パラメータの変更や置換ではありません。

ADAM のための Policy Manager サイレント・モード・インストーラ

Policy Manager のインストール時に ADAM をディレクトリ・サーバー・タイプとして指定するには、次のようにします。

```
-W dsTypeInput.dsType="9"
```

内容は次のとおりです。

`-W dsTypeInput.dsType` によって、ポリシー・データが格納されるディレクトリ・サーバー・タイプが指定されます。

次のタイプがサポートされています。

- 2: Sun 5.x
- 3: NDS
- 5: Active Directory
- 7: Active Directory（Windows Server 2003）
- 9: Active Directory アプリケーション・モード

環境に該当する場合は、後で動的補助オブジェクト・クラスを選択します。ADAM の場合、オプション `-W updateDSInfo.updateDSInfoChoice` は適用されません。かわりに、`-W updateDSInfo.updateDSInfoChoice = "Yes"` を使用してポリシー・ディレクトリ・サーバー・タイプを指定します。

ADAM のための Access Server サイレント・モード・インストーラ

Access Server のインストール時に ADAM をディレクトリ・サーバー・タイプとして指定するには、次のようにします。

```
-W oblixDSInfoBean.dsType="MSADAM"
```

内容は次のとおりです。

`-W oblixDSInfoBean.dsType` によって、構成ディレクトリ・サーバーのタイプが指定されます。

`"MSADAM"` は Microsoft Active Directory アプリケーション・モードを表します。

ADAM の問題のトラブルシューティング

詳細は、E-6 ページの「ADAM の問題」を参照してください。

C

Oracle Access Manager インストール後のディレクトリ証明書の追加

この付録では、Oracle Access Manager のアンインストールと再インストールを行わずに、ディレクトリ・サーバーの通信モードを SSL 対応に変更したり、複数のディレクトリ・サーバーへの接続のために証明書を追加したりする際に必要な情報を提供します。次の項目について説明します。

ディレクトリ証明書について

Identity Server、Policy Manager および Access Server のインストールの際に、2-20 ページの「ディレクトリ・サーバーの通信の保護」の説明に従って、ディレクトリ・サーバーの通信モードをオープンまたは SSL 対応のいずれかに指定します。証明書は、Oracle Access Manager をインストールする前にディレクトリ・サーバーに格納しておく必要があります。LDAP SSL 証明書の証明書ストア形式は、Oracle Access Manager 10*g*（10.1.4.0.1）では cert8.db です。

Oracle Access Manager をインストールした後で、SSL を有効化することがあります。たとえば、オープン通信モードから SSL 対応モードに変更する場合や、別のディレクトリ・サーバーに接続するためにディレクトリ証明書を追加する場合です。

このような場合、Oracle Access Manager をアンインストールして再インストールすることも可能ですが、次の手順を使用すると、Identity Server、Policy Manager および Access Server で必要な cert8.db ファイルを作成できます。

注意： Oracle Access Manager 10*g*（10.1.4.0.1）は、cert7.db（アップグレード済の環境）と cert8.db（新規インストール）の両方で機能します。

デフォルトの証明書ストアの形式および名前は、cert7.db から cert8.db に変更されています。Oracle Access Manager 10*g*（10.1.4.0.1）にアップグレードした場合は、継続して元の LDAP SSL 証明書ストア（cert7.db）を使用します。configureAAAServer、setup_ois または setup_accessmanager ユーティリティを実行すると、証明書ストアの形式と名前が自動的に cert8.db に変更されます。

タスクの概要 : Oracle Access Manager インストール後のディレクトリ SSL の有効化

1. C-3 ページの「前提条件」をすべて実行します。
2. C-3 ページの「新しい証明書ストアの作成」の説明に従って新しい証明書ストアを作成します。
3. C-4 ページの「証明書の追加」の説明に従って新しいストアを移入します。
4. C-5 ページの「ディレクトリ・サーバー構成の変更」の説明に従って、Oracle Access Manager でディレクトリ・プロファイルを変更します。
5. 必要に応じて、ここまでの手順を Policy Manager と Access Server について繰り返します。または、必要に応じて、新しい証明書を含むストアを Policy Manager と Access Server にコピーします。
6. Oracle Access Manager およびディレクトリ・サーバーでの、プラットフォームに対応するユーティリティ（UNIX では start_setup_ois、Windows では setup_ois）を使用したトランスポート・セキュリティ変更の詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

前提条件

SSL モードで通信を行うすべてのディレクトリ・サーバーには、認証局から取得した Base 64 エンコードのルート証明書のコピーが必要です。コピーは、Identity Server がディレクトリ・サーバーとの SSL 接続を確立するために使用する cert8.d ストアに格納する必要があります。

注意： cert8.db ファイルが ¥*Component_install_dir*¥identity¥oblix¥config にある場合は、次の手順を開始する前にそのファイルを削除してください。

Active Directory を使用する場合、すべてのドメイン・コントローラで SSL を有効化し、Base64 エンコード形式での Microsoft CA ルート証明書のコピーが必要です。

新しい証明書ストアの作成

次の手順では、新しい cert8.db 証明書ストアの作成方法を順に示します。Identity Server、Policy Manager および Access Server でこのタスクを実行できます。開始する前に前提条件を満たしていることを確認してください。

表 C-1 に、データ・ストアの作成に使用するコマンドに指定するオプションを示します。

表 C-1 データ・ストア作成のオプション

オプション	説明
-d directory	cert8.db ストアのディレクトリの指定
-N	新しい証明書データベースの作成

新しい証明書ストアを作成する手順

1. Base64 エンコードの CA ルート証明書のコピーを CA から取得し、インストールした Identity Server のホスト・マシンに格納します。
2. *IdentityServer_install_dir*¥identity¥oblix¥tools¥certutil で certutil ユーティリティを探します。
3. コマンド・ウィンドウで次のように入力します。

   C:¥IdentityServer_install_dir¥identity¥oblix¥tools¥certutil>certutil -d *c:¥IdentityServer_install_dir*¥identity¥oblix¥config -N

   cert8.db ストアのパスワードを求められます。この鍵または将来使用するすべての鍵を暗号化するためにパスワードを入力してください。パスワードは 8 文字以上で、英字以外の文字を少なくとも 1 つ含む必要があります。
4. cert8.db ストアのパスワードを入力し、さらに再入力します。

   cert8.db ストアが Identity Server に作成され、移入する準備ができました。

証明書の追加

新しい cert8.db ストアを作成したら、CA ルート証明書を追加する必要があります。表 C-2 に、このタスクを完了するためのコマンド・オプションを示します。

表 C-2 データ・ストアに証明書を追加するためのオプション

オプション	説明
-d directory	値は cert8.db ストアのフルパス。
-A	証明書をストアに追加。
-a	ASCII エンコードの証明書を指定。
-n	証明書のニックネームを指定。
-t C,,	trust 属性を指定。C,, は証明書に対して信頼できる CA を示す（SSL 専用、有効な CA を意味する）。
-i CAROOT.cer	入力を指定。CAROOT.cer は Base64 エンコード CA ルート証明書の名前。
-L	データ・ストア・ディレクトリの証明書リストを要求。

データ・ストアに証明書を追加する手順

1. コマンド・プロンプトで、次のように入力して証明書をデータ・ストアに追加します。

   C:¥OracleAccessManager¥identity¥oblix¥tools¥certutil>certutil -d C:¥OracleAccessManager¥identity¥oblix¥config -A -a -n CAROOT -t C,, -i CAROOT.cer

2. cert8.db ストア・ディレクトリの内容をリスト表示するコマンドを使用して、証明書が cert8.db ストアに追加されたことを確認します。

   次に例を示します。

   C:¥OracleAccessManager¥identity¥oblix¥tools¥certutil> certutil -d C:¥OracleAccessManager¥identity¥oblix¥config -L

   表 C-3 にリスト・コマンドの結果例を示します。リスト・コマンドを使用して、ニックネームが CAROOT というデータベースに証明書が追加されたことを確認します。

表 C-3 リスト・コマンドの結果例

証明書名	trust 属性
CAROOT	C,,
Example.com Code Signing CA	,,C
Example.com Individual CA	,C,
Example.com Server CA	CG,,

ディレクトリ・サーバー構成の変更

証明書を追加したら、ID システム・コンソールでディレクトリ・サーバー構成のプロセスを完了する必要があります。

ディレクトリ・プロファイルを変更する手順

1. ID システム・コンソールにナビゲートし、「システム構成」を選択して「ディレクトリ・オプション」をクリックします。
2. 「プロファイルの構成」ラベルの下の「ディレクトリ・サーバー」をクリックします。
3. 適切な「ディレクトリ・サーバー・セキュリティ・モード」* を選択します。

   注意 : アスタリスク（*）が付いたフィールドを変更した場合は、製品の設定をやりなおす必要があります。ID システム設定の再実行の詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

4. Identity Server を再起動して、ディレクトリ・サーバーの変更を有効にします。
5. プロセスの起動メッセージを見て、Identity Server が SSL モードまたは証明書モードで実行していることを確認します。

   次に例を示します。

   UNIX: プロセスが開始したことを知らせるメッセージがコンソールに返されます。ポート番号と通信モードがメッセージに含まれています。

   Windows: 「イベント ビューア」の「アプリケーション」でポート番号と通信モードを確認します。

6. Policy Manager と Access Server のストアを作成して移入し、それらのディレクトリ・プロファイルを構成し、Policy Manager Web サーバーおよび Access Server を再起動します。

   注意 : ディレクトリ・サーバーと CA の詳細が、ディレクトリと通信するすべての Oracle Access Manager コンポーネントで同じ場合は、Identity Server の cert8.db ストアを Policy Manager と Access Server にコピーできます。すべての手順を完了して構成を終了し、構成内容を確認します。

インストール後のトランスポート・セキュリティ・モードの変更の詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

D

ディレクトリ・サーバー・ホストの変更

ここでは、新しいディレクトリ・サーバー・ホストを認識するように Oracle Access Manager を再構成する方法を説明します。次の項目について説明します。

ディレクトリ・サーバー・ホストの変更について

Oracle Access Manager をインストールして設定した後で、Oracle Access Manager が通信するディレクトリ・サーバーのホスト・マシンを変更する場合があります。変更した場合は、新しいディレクトリ・サーバー・ホストを認識するように Oracle Access Manager を再構成する必要があります。

タスクの概要 : ディレクトリ・サーバー・ホストの変更

1. 停止時間の最短化
2. 新しいディレクトリ・サーバー・インスタンスの準備
3. プライマリ Identity Server の再構成
4. Policy Manager の再構成
5. Access Server の再構成

停止時間の最短化

新しいディレクトリ・サーバー・インスタンス（別のホストに移されたインスタンス）と通信するために Oracle Access Manager を再構成するとき、停止時間が発生します。停止時間を最小限に抑えるには、Oracle Access Manager Web コンポーネントと Access Server および Identity Server のフェイルオーバーを構成します。

Oracle Access Manager はフェイルオーバーを利用して、本来のリクエスト先に障害がある場合に別のサーバーにリクエストをリダイレクトし、中断のないサービスを提供します。フェイルオーバーを実行するには、プライマリ・サーバーとセカンダリ・サーバーを構成し、フェイルオーバー・プロセスに関して特定のパラメータを指定します。Oracle Access Manager Web コンポーネントは、最初はプライマリ・サーバーにアクセスしようとします。プライマリ・サーバーが使用できない場合に、セカンダリ・サーバーへの接続が試行されます。

- WebPass のリクエストは、セカンダリ Identity Server にリダイレクトされます。
- WebGate のリクエストは、セカンダリ Access Server にリダイレクトされます。

タスクの概要 : 停止時間の最短化

1. Identity Server と WebPass のフェイルオーバーの構成
2. Access Server と WebGate のフェイルオーバーの構成

これらのタスクを実行すると、新しいディレクトリ・サーバー・インスタンスに対してプライマリ Identity Server および Access Server を再構成したときに、ユーザーが中断のないサービスを利用できるようになります。

フェイルオーバーの詳細は、『Oracle Access Manager デプロイメント・ガイド』を参照してください。

Identity Server と WebPass のフェイルオーバーの構成

セカンダリ Identity Server を設定すると、新しいディレクトリ・サーバー・インスタンスとの通信のためにプライマリ Identity Server を停止して再構成するとき、WebPass がセカンダリ Identity Server にフェイルオーバーされます。

Identity Server と WebPass のフェイルオーバーを構成する手順

1. 次の要件を満たす 2 番目の Identity Server がインストールされていることを確認します。
   - 2 番目の Identity Server は、既存のディレクトリ・サーバーと通信する必要があります。
   - 2 番目の Identity Server は、既存の WebPass にセカンダリ・サーバーとして関連付ける必要があります。

   注意 : Oracle Access Manager のインストールに、これらの条件を満たす 2 番目の Identity Server が含まれない場合は、条件を満たす Identity Server をインストールする必要があります。詳細は、4-3 ページの「複数の Identity Server のインストールの概要」を参照してください。

2. セカンダリ Identity Server と WebPass の間でフェイルオーバーを構成します。
   a. ID システム・コンソールで、「構成」→「WebPass」→「< 名前 >」を選択し、「変更」をクリックします。

      WebPass の構成の詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

   b. 次の情報を入力して、変更内容を保存します。

      フェイルオーバーしきい値 : Web コンポーネントからプライマリ Access Server または Identity Server に対して開く必要がある接続数を入力します。

      Identity Server タイムアウトしきい値 : Web コンポーネントが応答しないサーバーを待機する時間（秒）を指定する、タイムアウトしきい値を入力します。この時間を過ぎると、接続不可と判断して別のサーバーへのアクセスを試行します。

      スリープ時間（秒）: 間隔を秒数で入力します。有効接続数が、構成された最大接続数と等しいかどうかを WebGate が確認する間隔です。

3. すべての Identity Server を使用するように、関連するディレクトリ・プロファイルを構成します。
   a. 「システム・コンソール」で、LDAP ディレクトリ・サーバー・プロファイルのリストを探します。

      ID システム・コンソールで「システム構成」を選択して「ディレクトリ・オプション」をクリックします。

      「プロファイルの構成」ページが表示されます。ディレクトリ・サーバー情報の他に「LDAP ディレクトリ・サーバー・プロファイルの構成」セクションと「RDBMS プロファイルの構成」セクションが含まれます。

   b. 「LDAP ディレクトリ・サーバー・プロファイルの構成」見出しの下で、Identity Server プロファイルの名前を選択します。

      LDAP ディレクトリ・サーバー・プロファイルの構成

      < 名前 >

      「ディレクトリ・サーバー・プロファイルの変更」ページ

   c. 「ディレクトリ・サーバー・プロファイルの変更」ページの「使用」フィールドで「すべての Identity Server」を選択します。

   d. 変更を保存します。

4. 次の「Access Server と WebGate のフェイルオーバーの構成」に進みます。

Access Server と WebGate のフェイルオーバーの構成

Identity Server の場合と同じく、セカンダリ Access Server を設定すると、新しいディレクトリ・サーバー・インスタンスとの通信のためにプライマリ Access Server を停止して再構成するときに、WebGate がセカンダリ Access Server にフェイルオーバーされます。

Access Server と WebGate のフェイルオーバーを構成する手順

1. 次の要件を満たす 2 番目の Access Server がインストールされていることを確認します。
   - 2 番目の Access Server は、Oracle Access Manager の構成データとポリシー・データを含む既存のディレクトリ・サーバーと通信する必要があります。
   - 2 番目の Access Server は、既存の WebGate にセカンダリ・サーバーとして関連付ける必要があります。

   注意： Oracle Access Manager のインストールに、これらの条件を満たす 2 番目の Access Server が含まれない場合は、条件を満たす Access Server をインストールする必要があります。詳細は、8-3 ページの「複数の Access Server のインストールの概要」を参照してください。

2. 『Oracle Access Manager デプロイメント・ガイド』の説明に従って、次のようにセカンダリ Access Server と WebGate のフェイルオーバーを構成します。
   a. アクセス・システム・コンソールで、「アクセス・システム構成」→「AccessGate 構成」→「すべて」→「実行」を選択し、該当する名前をクリックします。

      「AccessGate の詳細」ページが表示されます。WebGate の構成の詳細は、『Oracle Access Manager アクセス管理ガイド』を参照してください。

   b. 「変更」ボタンをクリックし、次の情報を入力して変更内容を保存します。

      フェイルオーバーしきい値：Web コンポーネントからプライマリ Oracle Access Manager サーバーに対して開く必要がある接続数を入力します。

      Access Server タイムアウトしきい値：Web コンポーネントが応答しない Oracle Access Manager サーバーを待機する時間（秒）を入力します。この時間を過ぎると、接続不可と判断して別のサーバーへのアクセスを試行します。

      スリープ時間（秒）：間隔を秒数で入力します。有効接続数が、構成された最大接続数と等しいかどうかを WebGate が確認する間隔です。

3. すべての Access Server を使用するように、関連するディレクトリ・サーバー・プロファイルを構成します。
   a. アクセス・システム・コンソールで、LDAP ディレクトリ・サーバー・プロファイルのリストを探します。

      「アクセス・システム・コンソール」→「システム構成」→「サーバー設定」

      「サーバー設定の表示」ページが表示されます。ディレクトリ・サーバー情報の他に「LDAP ディレクトリ・サーバー・プロファイルの構成」セクションと「RDBMS プロファイルの構成」セクションが含まれます。

   b. 「LDAP ディレクトリ・サーバー・プロファイルの構成」見出しの下で、Access Server プロファイルの名前を選択します。

      LDAP ディレクトリ・サーバー・プロファイルの構成

      < 名前 >

c. 「ディレクトリ・サーバー・プロファイルの変更」ページの「使用」フィールドで「Access Server」の横のボタンを選択し、リストから「すべてのサーバー」を選択します。次に例を示します。

```
Used By      o All components
             o Identity Servers
             o Access servers
                  All Servers
```

4. 変更を保存します。
5. 次の「新しいディレクトリ・サーバー・インスタンスの準備」に進みます。

新しいディレクトリ・サーバー・インスタンスの準備

新しいディレクトリ・サーバー・インスタンスが、Oracle Access Manager が通信するディレクトリ・サーバー・インスタンスの正確なレプリカであることを確認してください。つまり、スキーマ、ユーザー・データ、Oracle Access Manager 構成データおよびポリシー・データが一致する必要があります。さらに、次の要件があります。

- 既存のディレクトリ・サーバー・インスタンスにいずれかのデータが個別に格納されている場合、新しいディレクトリ・サーバー・インスタンスはその構成と一致する必要があります。
- 既存のディレクトリ・サーバーが SSL を使用している場合、新しいディレクトリ・サーバーには、既存のディレクトリ・サーバーに証明書を発行したのと同じルート CA が発行した証明書が必要です。

新しいディレクトリ・サーバー・インスタンスを準備するときは、次の点によく注意してください。

- ポリシー・データが構成データとは別のディレクトリ・サーバーに格納されている場合（o=oblix）、ポリシー・データの LDIF をエクスポートしてからインポートすることも必要です。
- NetPoint 6.5 以上を使用している場合、obcontainerId=DBAgents,<*Configuration DN*>... の下のエントリ（Policy Manager と Access Server に関連付けられている）を削除する必要があります。

注意： DB エージェントのエントリを削除するとき、コンテナ（obcontainerId=DBAgents）は削除しないでください。

新しいディレクトリ・サーバー・インスタンスを準備する手順

1. 次に示す ldapsearch コマンドを使用して、Oracle Access Manager の元の構成ツリー（o=oblix）を既存のディレクトリ・サーバー・インスタンスから LDIF ファイルにエクスポートします。ポリシー・データが別に格納されている場合は、ポリシー・データについても同じ操作を繰り返します。次に例を示します。

```
ldapsearch -h DS_hostname -p DS_port_number -b Configuration_DN (o=oblix...)
-D bind_dn -w password -s sub  (objectClass=*) > Oblix_Data_original.ldif
```

DS_hostname は新しいディレクトリ・サーバー・インスタンスのホスト・マシン名（データのエクスポート元）、*DS_port_number* はディレクトリ・サーバーがリスニングしているポート、*bind_dn* は Oracle Access Manager の DN、*password* はバインド DN のパスワード、*Oblix_Data_original.ldif* は構成データの ldif ファイルの名前です。

2. コンテナ（obcontainerId=DBAgents）は削除せずに DB エージェントのエントリを削除します。次に例を示します。

```
obcontainerId=DBAgents,<Configuration DN>…
```

3. 次に示す ldapmodify コマンドを使用し、変更した LDIF を新しいディレクトリ・サーバー・インスタンスにインポートします。次に例を示します。

```
ldapmodify -h DS_hostname -p DS_port_number -D bind_dn -w password -a -f
Oblix_Data_modified.ldif
```

DS_hostname は新しいディレクトリ・サーバー・インスタンスのホスト・マシン名（データのインポート先）、*DS_port_number* はディレクトリ・サーバーがリスニングしているポート、*bind_dn* は Oracle Access Manager 構成データの DN、*password* はバインド DN のパスワード、*Oblix_Data_modified.ldif* は構成データの ldif ファイルの名前です。

4. 「プライマリ Identity Server の再構成」に進み、新しいディレクトリ・サーバー・インスタンスのディレクトリ・サーバー・プロファイルを ID システム・コンソールに追加します。

プライマリ Identity Server の再構成

次の手順では、プライマリ Identity Server（既存のディレクトリ・サーバー・インスタンスと通信している）が新しいディレクトリ・サーバー・インスタンスと通信するように、再構成する方法を説明します。

新しいディレクトリ・サーバー・インスタンスと通信するように Identity Server を構成する手順

1. ID システム・コンソールで「システム構成」→「ディレクトリ・プロファイル」を選択し、「ディレクトリ・サーバー」をクリックします。
2. 「ディレクトリ・サーバー構成」ページで、新しいディレクトリ・サーバー・インスタンスを反映するように次の情報を変更し、変更内容を保存します。

   マシン * : *new_hostname.domain*.com

   ポート番号 * : *new_host_port*

   アスタリスク（*）が付いたフィールドを変更した場合は、ID システムの設定を手動で再実行する必要があります。
3. セカンダリ・サーバーを除くすべての Identity Server を停止します（複数のサーバーが実行している場合）。
4. 実行している 1 つの Identity Server ホストで、setup.xml ファイルを開きます。

   IdentityServer_install_dir¥identity¥oblix¥config¥setup.xml
5. status パラメータを削除し（または、status パラメータの値を "done" から "incomplete" に変更し）、ファイルを保存します。次に例を示します。

```
<NameValPair ParamName="status" Value="incomplete"></NameValPair>
```

6. この Identity Server を再起動します。
7. Web ブラウザで ID システム・コンソールを起動します。

   ID システムの初期設定のページと似ている「セットアップ」ページが表示されます。
8. 「セットアップ」ボタンをクリックして、設定プロセスを進めます。
   a. 次のように新しいディレクトリ・サーバー・インスタンスの情報を指定します。

      ホスト : 新しいユーザー・データ・ディレクトリ・サーバーの DNS ホスト名

      ポート番号 : 新しいユーザー・データ・ディレクトリ・サーバーのポート番号

      注意 : ユーザー・データが構成データとは別に格納されている場合、同様のページが表示されます。そこで構成データ・ディレクトリの情報を入力します。ただし、その手順についてはここでは省略します。

   b. 第 6 章「ID システムの設定」の説明に従って設定を完了します。

9. 新しい情報を反映するように Identity Server を再起動します。
10. 「システム・コンソール」で、新しいデータベース・プロファイルが作成されたことを確認します。
    a. 「ディレクトリ・プロファイル」ページにナビゲートします。

       ID システム・コンソールで「システム構成」を選択して「ディレクトリ・プロファイル」をクリックします。

    b. 「プロファイルの構成」ページの「LDAP ディレクトリ・サーバー・プロファイルの構成」見出しの下で、関連するプロファイル名を選択します。

    c. 「ディレクトリ・サーバー・プロファイルの変更」ページで、新しいデータベース・インスタンスの名前を探し、新しいマシンとポート番号を確認します。

       注意 : さらに DB プロファイルが必要であれば作成できます。詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

11. 次の「Policy Manager の再構成」に進みます。

Policy Manager の再構成

新しいディレクトリ・サーバー・インスタンスを使用するように Policy Manager を再構成する必要があります。

新しいディレクトリ・サーバー・インスタンスに対して Policy Manager を再構成する手順

1. 次のようにアクセス・システム・コンソールでサーバー設定を表示します。

   アクセス・システム・コンソールで「アクセス・システム構成」→「サーバー設定」を選択して「ディレクトリ・サーバー」をクリックします。

2. 「ディレクトリ・サーバー構成」ページで、新しいディレクトリ・サーバー・インスタンスを反映するように次の情報を変更し、変更内容を保存します。

   マシン * : *new_hostname.domain*.com

   ポート番号 * : *new_host_port*

   アスタリスク（*）が付いたフィールドを変更した場合は、Policy Manager の設定を手動で再実行する必要があります。

3. 1 つを除きすべての Policy Manager Web サーバーを停止します（複数のサーバーが実行している場合）。
4. 実行している 1 つの Policy Manager ホストで、setup.lst ファイルを開きます。

   PolicyManager_install¥dir¥oblix¥config¥setup.lst

5. status パラメータを削除し（または、status パラメータの値を "done" から "incomplete" に変更し）、ファイルを保存します。次に例を示します。

   ```
   <NameValPair ParamName="status" Value="incomplete"></NameValPair>
   ```

6. Policy Manager Web サーバーを再起動します。
7. Web ブラウザでアクセス・システム・コンソールを起動します。

   アクセス・システムの初期設定時に表示されるのと似ている「セットアップ」ページが表示されます。ユーザー・データ、構成データおよびポリシー・データが格納されているディレクトリ・サーバーの詳細を指定する必要があります。また、各データ・タイプのディレクトリ・サーバーの情報を指定することを求められます。

8. 「セットアップ」を再び起動し、求められたら次の情報を指定します。
   - ユーザー・データと構成データが一緒に格納されている場合は、ポリシー・データを格納する場所を指定するように求められます。
   - データが個別に格納されている場合は、構成データの詳細を指定するように求められます。

   この詳細は、2-22 ページの「データ記憶域の要件」を参照してください。
9. 求められたら、次のように新しいディレクトリ・サーバー・インスタンスの情報を指定します。
   a. 次のように新しいディレクトリ・サーバー・インスタンスの情報を指定します。

      ホスト : 新しいディレクトリ・サーバーの DNS ホスト名

      ポート番号 : 新しいディレクトリ・サーバーのポート番号

      注意 : データの格納方法によっては、ポリシー・データのために別の画面が表示されることがあります。ただし、その手順についてはここでは省略します。

   b. 7-10 ページの「Policy Manager の設定」の説明に従って設定を完了します。
10. 設定が完了したら、他の Policy Manager Web サーバーを再起動します。

    他の Policy Manager に新しい情報が反映されます。
11. 次のようにアクセス・システム・コンソールで新しいデータベース・インスタンスを確認します。
    a. 次のようにアクセス・システム・コンソールでサーバー設定を表示します。

       アクセス・システム・コンソールで「アクセス・システム構成」→「サーバー設定」を選択します。

    b. 「サーバー設定の表示」ページの「LDAP ディレクトリ・サーバー・プロファイルの構成」見出しの下で、関連するプロファイル名を選択します。

    c. 「ディレクトリ・サーバー・プロファイルの変更」ページで、新しいデータベース・インスタンスの名前を探し、新しいマシンとポート番号を確認します。

       注意 : さらに DB プロファイルが必要であれば作成できます。詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

12. 「Access Server の再構成」の説明に従って Access Server の設定を再実行します。

Access Server の再構成

Policy Manager の設定を手動で再実行したら、次に示すように Access Server を再構成する必要があります。configureAAAServer ツールの使用方法の詳細は、『Oracle Access Manager アクセス管理ガイド』を参照してください。

新しいディレクトリ・サーバー・インスタンスに対して Access Server を再構成する手順

1. configureAAAServer ツールを探します。次に例を示します。

   AccessServer_install_dir¥access¥oblix¥tools¥configureAAAServer

2. configureAAAServer ツールで次のコマンドを使用して Access Server を設定します。たとえば、次のようにします。

   configureAAAServer install -i *AccessServer_install_dir/util/access*

3. 新しいディレクトリ・サーバー・インスタンスが存在するホストの新しい情報を指定します。
4. Access Server を再起動します。
5. 次のようにアクセス・システム・コンソールで新しいデータベース・インスタンスを確認します。
   a. 次のようにアクセス・システム・コンソールでサーバー設定を表示します。

      「アクセス・システム・コンソール」→「システム構成」→「サーバー設定」

   b. 「サーバー設定の表示」ページの「LDAP ディレクトリ・サーバー・プロファイルの構成」見出しの下で、関連するプロファイル名を選択します。
   c. 「ディレクトリ・サーバー・プロファイルの変更」ページで、新しいデータベース・インスタンスの名前を探し、新しいマシンとポート番号を確認します。

   デフォルトの他にもう 1 つのデータベース・プロファイルが作成されていることがあります。ポリシー・ツリーと構成ツリーが同じディレクトリ・サーバーにあるが、それぞれの接尾辞が異なる場合です。

注意： さらに DB プロファイルが必要であれば作成できます。詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

E

インストールの問題のトラブルシューティング

この付録では、一般的な問題のトラブルシューティングと解決のためのヒントを示します。ここでは、次の項目について説明します。

ブラウザの問題

次の問題はブラウザ固有です。

文字表示の問題

Apache ベースの Web サーバー（Apache、Oracle HTTP Server（OHS）、IBM HTTP Server（IHS）など）を使用するときに、Oracle Access Manager HTML ページが文字化けすることがあります。

Oracle Access Manager 10*g*（10.1.4.0.1）の HTML ページでは UTF-8 エンコーディングが使用されます。Apache ベースの Web サーバーでは、管理者が AddDefaultCharset ディレクティブを使用して、HTML ページのデフォルト・キャラクタ・セットを指定できます。AddDefaultCharset ディレクティブで UTF-8 以外のキャラクタ・セットを有効にすると、Oracle Access Manager の HTML ページが文字化けします。

Oracle Access Manager 10*g*（10.1.4.0.1）の HTML ページを正しく表示するには、AddDefaultCharset ディレクティブを Web サーバー構成ファイル（httpd.conf）で次のように無効化することをお薦めします。

```
AddDefaultCharset Off
```

Sun VM v1.4.2_04 での Microsoft Internet Explorer 6

この構成では、コンテナ制限ポリシーを作成し、ユーザーが包含制限イベントの通知を受けるように指定して、人セレクタで**「完了」**をクリックしたときに、**「保存」**、**「取消」**および**「リセット」**のボタンが表示されず、ポリシーを保存できません。

この問題に対処する手順

1. `oblixbaseparams.xml` ファイルを開きます。

   `IdentityServer_install_dir¥identity¥oblix¥apps¥common¥bin¥oblixbaseparams.xml`

2. セクション `applet_customizations` で、問題が発生したアプレットのサブセクションを探します。たとえば、`containmentlimit_applet` サブセクションです。
3. このアプレットの幅と高さのパラメータを適切に調整して、問題を解決します。たとえば、`applet_dimension_height` パラメータの値を 530 に変更します。
4. Identity Server を再起動します。
5. 新しいブラウザ・ウィンドウを開いて同じアプレットを表示します。

Internet Explorer でリソースを認証できない

Oracle Access Manager の以前のリリースでは Latin-1 エンコーディングしかサポートされていませんでした。ただし、10*g*（10.1.4.0.1）では UTF-8 エンコーディングがサポートされています。このためこの問題は発生しません。

症状 : Internet Explorer で「リソースを認証できない」エラーが発生します。

原因 : Internet Explorer によって、URL の UTF 文字を常に変換する拡張オプションが提供されています。Oracle Access Manager もこの処理を自動的に行います。両方を有効にしていると認証のエラーが引き起こされます。

解決方法 : IE での「リソースを認証できない」エラーを解消するには、次の手順を実行します。

この問題を解消する手順

1. テキスト・エディタで `globalparams.xml` ファイルを開きます。このファイルは次の 2 箇所に格納されています。両方を編集してください。
   - `¥IdentityServer_install_dir¥identity¥oblix¥apps¥common¥bin¥globalparams.xml`
   - `¥AccessServer_install_dir¥access¥oblix¥apps¥common¥bin¥globalparams.xml`
2. `doUtfConversion` パラメータを NO に設定し、変更内容を保存します。

   注意 : UTF-8 データをインポートした後でこのように設定した場合は、Web サーバーを再起動し、すべてのブラウザを閉じてから新しいブラウザ・ウィンドウを開きます。

3. Microsoft Internet Explorer で、**「ツール」**メニュー→**「インターネット オプション」**を選択します。
4. 「インターネット オプション」ダイアログ・ボックスで**「詳細設定」**タブを選択します。
5. 「ブラウズ」の下の**「常に UTF-8 として URL を送信する」**チェック・ボックスの選択を解除します。

ディレクトリ・サーバーの問題

ここでは、いくつかのディレクトリ・サーバーの問題について説明します。

- Active Directory の問題
- ADAM の問題

E-11 ページの「Oracle Virtual Directory の実装の問題」も参照してください。

Active Directory の問題

Active Directory 2000 では、様々な Oracle Access Manager スレッドからの同時バインド・リクエストの同一 LDAP 接続での受信はサポートしていません。

Oracle Access Manager サーバーはマルチスレッドであり、ディレクトリ・サーバーに対する複数の LDAP 接続のプールを管理しています。複数の Oracle Access Manager スレッドが、リクエストを効率よく処理するために LDAP 接続を共有できます。ただし、Active Directory 2000 では、様々な Oracle Access Manager スレッドからの同時バインド・リクエストの同一 LDAP 接続での受信はサポートしていません。このため、認証障害が発生したような状態になることがあります。

この状況を回避する手順

1. Access Server で、globalparams.lst ファイルを探してエディタで開きます。
2. exclusiveAuthnConnection という新しいフラグを追加し、true に設定します。

   これにより、Oracle Access Manager スレッドが、ディレクトリ・サーバーに送信するバインド・リクエストで別の LDAP 接続を使用するように強制されます。

詳細は、次の項目を参照してください。

- Active Directory の検索停止
- この DB プロファイルで ADSI を有効化できない（Active Directory）
- Active Directory の動的リンク補助クラス
- 付録 A「Active Directory に対する Oracle Access Manager のインストール」

Active Directory の検索停止

症状 : 400 のポリシー・ドメインが Oracle Access Manager に作成されました。それぞれに 10 のリソースと 10 のポリシーが含まれています。Policy Manager の globalparams.xml ファイルで `limitAMPolicyDomainResourceDisplay` が `true` に設定されています。**「検索」**アイコンを選択すると、「製品により次のメッセージが生成されました。問題を解決するには Web マスターに連絡してください。」というエラー・ページが表示されます。

原因 : ポリシー・ドメインの数が現在の制限を超えています。

解決方法 : Active Directory ではポリシー・ドメインが 350 を超えないようにします。

この DB プロファイルで ADSI を有効化できない（Active Directory）

Oracle Access Manager では、ID システム・コンソールを使用して、ユーザー・データの DB プロファイルを ADSI と LDAP の間で変更できます。ただし、Oracle Access Manager では、「システム・コンソール」を使用して構成またはポリシーの DB プロファイルを ADSI と LDAP の間で変更することはできません。

症状 : ユーザー・データは LDAP を使用する Active Directory Forest に格納され、構成データとポリシー・データは ADSI を使用する別の Active Directory Forest に格納されているとします。ID システム・コンソールを使用して構成データ DB プロファイルの ADSI フラグを LDAP に変更すると、Oracle Access Manager のサーバーとサービスを再起動しても、依然として ADSI フラグが有効になっており、次のメッセージが表示されます。

「別のフォレスト内のユーザーまたは構成 DB プロファイルに対して ADSI を有効化することができます。この DB プロファイルには ADSI が有効化できません。」

さらに、ユーザー・データの DB プロファイルを ADSI に変更しようとするとエラーが発生します。これは、Oracle Access Manager が、構成データとポリシー・データの DB プロファイルを ADSI 対応として認識するためです。

解決方法 : 設定プログラムを再実行して、構成データとポリシー・データの DB プロファイルを変更します。

Active Directory の動的リンク補助クラス

Active Directory を Windows Server 2003 にインストールした場合、動的リンク補助クラスで問題が発生したときは、次のすべての項目を完了していることを確認してください。

> **関連項目：** 詳細は、付録 A「Active Directory に対する Oracle Access Manager のインストール」を参照してください。

Active Directory で動的リンク補助クラスを有効化する手順

1. Oracle Access Manager をインストールする前に、Active Directory のドメインとフォレストの機能が Windows 2003 Server レベルで作動していることを確認する必要があります。

   Microsoft ドキュメントの説明に従って、ドメインとフォレストの両方を Windows 2003 Server レベルに上げる必要があります。

2. Identity System のインストールと設定で、求められたときに動的リンク補助クラスを指定します。

3. Policy Manager のインストールと設定で、求められたときに動的リンク補助クラスを指定します。

4. Access Server のインストールで、求められたときに動的リンク補助クラスを指定します。

5. 設定の後、次のファイルで `dynamicAuxiliary` フラグが true に設定されていることを確認してください。

   - ¥*IdentityServer_install_dir*¥identity¥oblix¥data.ldap¥common¥ldapconfigdbparams.xml
   - ¥*PolicyManager_install_dir*¥access¥oblix¥data.ldap¥common¥ldapconfigdbparams.lxml
   - ¥*AccessServer_install_dir*¥access¥oblix¥data.ldap¥common¥ldapconfigdbparams.xml

   ```
   NameValPair ParamName= "dynamicAuxiliary" Value= "true"
   ```

   また、Oracle Access Manager によって次のファイルの `dynamicAuxiliary` タグが true に設定されます。

   - ¥*IdentityServer_install_dir*¥identity¥oblix¥config¥setup.xml

   > **注意：** このディレクトリは静的な関連付けを探すのに最適です。

6. 『Oracle Access Manager ID および共通管理ガイド』の説明に従って、動的補助クラスをサポートするように Oracle Access Manager を構成します。

ADAM の問題

詳細は、付録 B「ADAM に対する Oracle Access Manager のインストール」を参照してください。

ADAM: 構成 DN または検索ベースが見つかりません。

存在するか確認してください。

このエラー・メッセージは、構成 DN とポリシー DN で ous を使用していないことを示す場合があります。

ADAM ディレクトリ・サーバーのセキュリティ

ADAM スキーマは、オープン・ポートを介して更新する必要があります。詳細は、E-7 ページの「ADAM のスキーマ更新」を参照してください。

パスワード変更は、SSL 対応ポートを介してのみ実行できます。詳細は、E-6 ページの「ADAM のパスワード変更」を参照してください。

ADAM のオブジェクト・クラス

ADAM では、ユーザー・オブジェクト・クラスの指定は Active Directory と異なります。Active Directory で必須の samaccountname は ADAM には存在しません。grouptype は ADAM でも必須です。設定時に属性を自動的に構成すると、Oracle Access Manager によって grouptype 属性が構成されます。

動的補助クラスを使用する予定がない場合は、手動スキーマ更新に関して次の点に注意してください。

- B-12 ページの「ADAM に対する ID システムのインストールと設定」の説明に従って、*IdentityServer_install_dir*¥identity¥oblix¥data.ldap¥common¥ADAM_oblix_schema_add.ldif を使用してスキーマを手動で更新します。
- ldifde コマンドを使用して、Oracle Access Manager スキーマ・ファイル ADAMAuxSchema.ldif を *IdentityServer_install_dir*¥identity¥oblix¥data.ldap¥common ディレクトリからインポートします。
- オブジェクト・クラス oblixorgperson と oblixgroup が、Person オブジェクト・クラスと Group オブジェクト・クラスそれぞれに補助クラスとして明示的に追加されていることを確認します。

ADAM のパスワード変更

パスワード変更には SSL が必要です。パスワードの変更で問題が発生した場合、ディレクトリ・サーバーの固有のパスワード・ポリシーが無視されていることがあります。

ユーザーを作成するときに、ユーザーがパスワードを持つようにしてください。ユーザーをアクティブ化して操作が失敗した場合、ユーザーにパスワードがないことがあります。

ユーザーは ADAM 内で有効化する必要があります。Oracle Access Manager の User Manager でユーザーを検索し、検索結果にそのユーザーが含まれない場合は、オブジェクト・クラスの msDS-UserAccountDisabled= user 属性が無効か有効かを調べます。

ADAM のスキーマ更新

Oracle Access Manager をインストールするときに、ADAM スキーマを手動で更新する必要があります。

ユーザー・データ・ディレクトリのインスタンスが、構成およびポリシーのデータ・ディレクトリ・インスタンスと異なる場合は、ADAM_user_schema_add.ldif ファイルを手動でアップロードする必要があります。

構成データ・ディレクトリ・インスタンスでは、ADAM_oblix_schema_add.ldif ファイルを手動でアップロードする必要があります。静的補助クラスを使用するときは、ADAMAuxSchema.ldif ファイルを手動でアップロードする必要があります。

ポリシー・データ・ディレクトリのインスタンスが、構成データ・ディレクトリのインスタンスと異なる場合は、ADAM_oblix_schema_add.ldif ファイルを手動でアップロードする必要があります。静的補助クラスを使用するときは、ADAMAuxSchema.ldif ファイルを手動でアップロードする必要があります。

現在、ldifde（ADAM スキーマの拡張に使用）では、SSL ポートへのバインドはサポートされていません。スキーマの更新で問題が発生する場合は、Identity Server のインストール時にオープン ADAM ポートを指定したことを確認してください。サポートされない状況でも、Identity Server のインストール時に証明書をインストールして SSL を指定することは可能です。

ID システムの問題

ここでは、発生する可能性がある次の Identity Server の問題について説明します。

アプリケーションが設定されていない

状況によっては、既存の Identity Server 名を再利用する場合があります。たとえば、Oracle Access Manager をテスト環境から本番環境に移す場合や、なんらかの理由で Identity Server を削除する必要がある場合は、既存の Identity Server 名を使用すると便利です。

システム・コンソールで元の Identity Server 名を削除しないと、新しいインスタンスの設定の後でログインしたときに、「アプリケーションが設定されていません」というメッセージが生成されることがあります。Identity Server 名をリサイクルするときは、アプリケーションを設定してログインするために特別な手順を実行する必要があります。詳細は、20-6 ページの「Identity Server インスタンス名のリサイクル」を参照してください。

ID システムを設定できない

Identity Server と WebPass が、下位 CA から発行された証明書を使用して証明書モードでインストールされているとき、**「ID システム・コンソール」**リンクをクリックして ID システムの設定を開始すると、空白のページが表示されることがあります。イベント・ビューアに、原因を特定せずに Oracle Access Manager のエラーが表示される場合があります。

下位 CA で生成された証明書を使用するときは、ルート CA の証明書が下位 CA の証明書と一緒に `xxx_chain.pem` に存在する必要があります。検証を適切に行い、ID システムを正常に設定するためには、両方の証明書が存在する必要があります。

> **関連資料 :** 詳細は、『Oracle Access Manager ID および共通管理ガイド』のトランスポート・セキュリティ・モードの項を参照してください。

Access Server または Identity Server の可用性チェック

Access Server が実行しているかどうかを確認するには、サーバーがリスニングしているポートを使用してサーバーに Telnet でアクセスします。ポート 6021 で `myserver.mycompany.com` というサーバーで実行している Access Server への Telnet セッションを次に示します。

```
myserver% telnet myserver.mycompany.com 6021
Trying 192.168.5.18. . .
Connected to myserver.mycompany.com.
Escape character is '^]'.
^]
telnet> q
Connection closed.
myserver%
```

この例に対するシステムのレスポンスは次のようになります。

```
Connected to myserver.mycompany.com.
Escape character is '^]'.
```

これは、Access Server が Telnet リクエストを受け入れて、作動していることを示します。サーバーのインストール時にリスニングするように指定されているポートで、そのサーバーに接続できない場合は、Access Server に問題があります。次のような問題が含まれます。

- 接続がファイアウォールで妨げられています。
- サーバーが実行していません。

接続が開いているかどうかを確認するためにファイアウォールを調べます。Access Server プロセスが実行しているかどうかを調べます。アクセス・システム・サーバーで `netstat` コマンドを使用すると、Access Server のインストール時に指定したポートを使用してサーバーが通信しているかどうかを確認できます。

DB プロファイルを取得できない

症状 : 「DB マネージャの初期化中に Identity2 で使用される DB プロファイルを取得できませんでした。Identity2 に有効な DB プロファイルが存在することを確認してください。」というメッセージを受け取ります。

原因 : 次の場合に発生することがあります。

- 2 番目（またはそれ以降）の Identity Server をインストールした場合
- インストール時に、「これは、この LDAP ディレクトリ・サーバーのネットワーク内で最初の Identity Server のインストールですか。」という質問に「はい」と答えた場合
- Identity Server および Web サーバーを再起動した場合

解決方法 : Identity Server をアンインストールしてから再インストールするときに、「これは、この LDAP ディレクトリ・サーバーのネットワーク内で最初の Identity Server のインストールですか。」という質問に「いいえ」と答えます。

Identity Server が起動しない

症状 : ID システムの設定時に、Identity Server と Web サーバーを再起動するように求められます。長い間待機した後に、ブラウザから「ページを表示できません。」というメッセージが返されます。

原因 : Web ブラウザが、Identity Server のレスポンスを待機中にタイムアウトになることがあります。これは、ディレクトリ・サーバーの詳細を指定し、ユーザー・オブジェクト・クラスと Group オブジェクト・クラスを自動的に構成した後で発生します。スキーマ更新がブラウザのタイムアウトよりも長くかかるためです。

解決方法 : しばらく待機してからブラウザをリフレッシュして続行します。

Identity Server が起動しない場合は、問題の原因について次の 3 つの項目を調べてください。

Identity Server をトラブルシューティングする手順

1. LDAP ディレクトリに不要なデータがないことを確認します。次に例を示します。
   - 構成ブランチが空か
   - 構成ブランチに正しいデータがあるか
   - 構成ブランチに、別の Identity Server エントリを含む、以前のインストールのデータがあるか
2. 次のファイルが適切なことと正しいフォルダにあることを確認します。
   - ¥*IdentityServer_install_dir*¥identity¥oblix¥config¥configinfo.xml
   - ¥*IdentityServer_install_dir*¥identity¥oblix¥config¥ois_server_config.xml
   - ¥*IdentityServer_install_dir*¥identity¥oblix¥config¥setup.xml
3. Identity Server のために選択したポートが別のアプリケーションで使用中でないことを確認します。

ID システムのコンポーネントでの障害発生

症状 : RedHat Linux 上の ID システムのコンポーネントで、oblog_config.xml ファイルの "MAX_ROTATION_SIZE" を 10000 KB に減らしたときに、新しい NPTL ベースのランタイム・ライブラリに対して障害が発生することがあります。

解決方法 : LD_ASSUME_KERNEL 環境変数を設定してから、Web サーバー、WebLogic コンポーネントと WebSphere コンポーネント（10*g*（10.1.4.0.1）Software Developer Kit に統合されている）、および Oracle Access Manager Web コンポーネント（WebPass、WebGate および Access Manager）を起動します。次に例を示します。

```
# export LD_ASSUME_KERNEL=2.4.19
```

これにより、Linux 動的リンカーが古いランタイム・ライブラリを使用するようになります。

WebGate インストール後の IdentityXML コールの失敗

IdentityXML コールで認証資格証明が必要となることがあります。WebPass を保護する WebGate がない場合は、基本の資格証明メカニズムが使用されます。このメカニズムは、ユーザー名とパスワードが SOAP リクエスト自体に埋め込まれた形式です。ただし、後から WebGate をインストールしたときは、SSO トークンによる認証を使用するように IdentityXML コールを変更する必要があります。

最初に OBSSOCookie を取得して、そのトークンを以降のすべてのコールに渡すように、IdentityXML コールを変更する必要があります。この変更の例は、『Oracle Access Manager 開発者ガイド』を参照してください。デプロイされた IdentityXML 関数のコード例と ObSSOCookie の例で詳細を確認します。

設定後に WebPass 識別子が使用できない

インストール時に入力する Identity Server 識別子は、一意であることが必要です。また、WebPass のインストール時に入力する WebPass 識別子とも異なる必要があります。

インストール時に入力する WebPass 識別子が Identity Server のインストール時に入力した識別子と一致する場合、WebPass 識別子は作成されません。したがって、設定後も ID システム・コンソールで使用することができません。

WebPass を再構成する手順

次の手順を実行して WebPass を再構成します。

1. `setup_webpass` ユーティリティを探します。次に例を示します。

   WebPass_install_dir¥identity¥oblix¥tools¥setup¥setup_webpass.exe

   WebPass_install_dir は WebPass をインストールしたディレクトリです（たとえば、`c:¥OracleAccessManager¥identity`）。

2. 次のオプションを使用して `setup_webpass` ユーティリティを実行します。

```
setup_webpass -i <WebPass_install_dir> [-q] [-n <WebPass ID>]
[-h <OIS hostname>] [-p <OIS port #>] [-s <open|simple|cert>]
[-P <simple|cert mode password>] [-c (request|install)]
[-W iis]
```

シンプル・モードまたは証明書モードの WebPass パスワードを変更する手順

次の手順を実行して、シンプル・モードまたは証明書モードの WebPass パスワードを変更します。

1. `setup_webpass` ユーティリティを探します。次に例を示します。

   WebPass_install_dir¥identity¥oblix¥tools¥setup¥setup_webpass.exe

2. 次のオプションを使用して `setup_webpass` ユーティリティを実行します。

```
setup_webpass -i <WebPass_install_dir> -k
```

WebPass モードを再構成する手順

次の手順を実行して WebPass モードを再構成します。

1. `setup_webpass` ユーティリティを探します。次に例を示します。

   WebPass_install_dir¥identity¥oblix¥tools¥setup¥setup_webpass.exe

2. 次のオプションを使用して `setup_webpass` ユーティリティを実行します。

```
setup_webpass -i <WebPass_install_dir> -m
```

IIS と Windows の問題

Oracle Access Manager インストールを実行するアカウントには管理権限が必要です。Identity Server および Access Server サービスの実行に使用されるユーザー・アカウントには、「サービスとしてログオン」権限が必要です。これは、**「管理ツール」→「ローカル セキュリティ ポリシー」→「ローカル ポリシー」→「ユーザー権利の割り当て」→「サービスとしてログオン」**を選択して設定できます。

IIS 6 Web サーバーの場合のみ、WWW サービスを IIS 5.0 分離モードで実行する必要があります。これは、ISAPI ポストゲート・フィルタで必要となります。通常、これは Oracle Access Manager のインストール時に自動的に設定されます。インストールされない場合は、デフォルト Web サイトで手動で設定する必要があります。

IIS WebGate のインストール時に、IIS WebGate のために /access ディレクトリの様々な権限の設定が必要となるのは、NTFS をサポートするファイル・システムにインストールする場合のみです。たとえば、FAT32 ファイル・システムを実行している Windows 2000 マシンに、シンプル・モードまたは証明書モードで ISAPI WebGate をインストールするとします。最後のインストール・パネルには、FAT32 ファイル・システム上で設定できない様々な権限を手動で設定するための指示が表示されます。この場合、この指示は無視してください。

Oracle Virtual Directory の実装の問題

Oracle Virtual Directory での実装に影響する、次のいくつかの条件に注意する必要があります。

- ディレクトリ・サーバーの問題
- 複数値属性の問題
- セカンダリ・データ・ストアの問題
- 予期しないグループ削除の問題

詳細は、第 10 章「Oracle Virtual Directory を使用した Oracle Access Manager の設定」を参照してください。

ディレクトリ・サーバーの問題

Active Directory または ADAM の検索の問題 : Oracle Virtual Directory を Active Directory ディレクトリ・サーバーまたは ADAM ディレクトリ・サーバーと一緒に使用する場合、検索で「次と類似する」演算子を使用できません。

原因 : Active Directory または ADAM ディレクトリ・サーバーでは、「次と類似する」検索がサポートされていません。

回避方法 : Active Directory または ADAM ディレクトリ・サーバーでは、「次と類似する」検索を使用しないでください。

複数値属性の問題

属性変更ワークフローを使用して複数値属性を変更できません。

原因 : デフォルトの Oracle Virtual Directory スキーマには、Sun Directory Server スキーマと同様に複数値属性が含まれます。Active Directory では属性の構文が一致しない場合があります。たとえば、Active Directory ではメール・アドレスは単一値ですが、Sun Directory Server と Oracle Virtual Directory では複数値です。

たとえば、Oracle Virtual Directory が Active Directory および Sun Directory Server と通信するとき、属性変更ワークフローを作成して Sun Directory Server でユーザーの複数値属性（メール・アドレスなど）を変更しようとすると、属性は変更されますが、Active Directory ではコミットが失敗して属性が変更されません。

回避方法 : 複数値属性を変更しないでください。

セカンダリ・データ・ストアの問題

1. **サブツリー検索 :** データベース分割プロファイルがあると、セカンダリ表に存在する属性から属性を導出できません。

   原因 : Oracle Access Manager は、セカンダリ・データ・ストアの属性に対してサブツリー検索を実行できません。

   たとえば、マッピング・テンプレート CustomOracleDBMapping_mpy.xml を使用して、InetOrgPerson に導出属性を次のように定義したとします。

   - **属性名 :** MyAttr
   - **表示名 :** MyAttr
   - **一致する属性 :** employeenumber
   - **参照属性 :** employeenumber
   - **オブジェクト・クラス :** InetOrgPerson

   ユーザー（たとえば Rohit）を検索してプロファイルを表示するとき、employeenumber 属性の値を確認できますが、myAttr 値は空になっています。

   次の例では、データベースと分割プロファイル、次のアダプタ・テンプレートがあります。

   CustomOracleAdaptorSplitPrimary_adapter_template.xml

   CustomOracleAdaptorSplitSecondary1-1_adapter_template.xml

   CustomOracleAdaptorSplitSecondary1-M_adapter_template.xml

   CustomAdapterJoinView_adapter_template.xml

   回避方法 : セカンダリ・データ・ストアの属性を構成しないでください。

2. **ユーザーの作成ワークフロー :** ユーザーの作成ワークフローを定義すると、Oracle Access Manager で、Oracle Virtual Directory のセカンダリ・ビューから属性を選択できるようになります。実行時には、ユーザー・エントリがプライマリ・ビューに作成されます。ただし、ワークフローは失敗し、これらのエントリを Oracle Access Manager が使用することはできません。

   原因 : Oracle Access Manager はすべての属性を Oracle Virtual Directory から取得するため、どの属性がセカンダリ・データ・ストアではなくプライマリ・データ・ストアから取得されたかはわかりません。

   回避方法 : セカンダリ・データ・ストアの属性を構成しないでください。

予期しないグループ削除の問題

少なくとも 1 つの LDAP ディレクトリと少なくとも 1 つのデータベース表をフェデレートする Oracle Virtual Directory 仮想ディレクトリに対して Oracle Access Manager を設定したとき、LDAP ディレクトリのグループからメンバーを削除しようとすると、グループ全体がそのディレクトリから削除されます。

原因 : パフォーマンスの理由から Oracle Virtual Directory は、ユーザーが削除を指定したメンバーのみを Oracle Access Manager に返します。これに対して、標準の LDAP ディレクトリ・サーバーはグループのすべてのメンバーを返します。

このような Oracle Virtual Directory の変則的な動作のために、ID システムを使用してグループからメンバーを削除しようとするときに影響が生じます。標準の LDAP ディレクトリ・サーバーはグループのすべてのメンバーを返すため、Oracle Access Manager は、1 メンバーが削除された後も残りのメンバーを認識します。ただし、Oracle Virtual Directory はグループ内の削除指定された 1 メンバーのみを Oracle Access Manager に返します。Oracle Access Manager は、返されたメンバーを削除するとその他のグループ・メンバーを認識できません。このため、グループが空になったとみなして、グループとすべてのメンバーを削除します。

重要 : これは、グループの uniqueMember だけではなくすべての DN 属性に共通します。複数値を持つことができるすべての DN 属性に回避方法を適用する必要があります。

回避方法 : 10-58 ページの「Oracle データベース用のマッピング・スクリプトのカスタマイズ」にあるカスタマイズ・ファイルを参照してください。また、ID システムがダミー・ユーザーをバックエンド・データベースに書き込むことを防ぐために次の詳細に注意します。

```
Workaround to prevent COREid from writing dummy user to backend database
if haveAttributeValue('uniqueMember','cn=Dummy User'):
#removeAttributeValue('uniqueMember','cn=Dummy User')
if operation != 'modify':
removeAttributeValue('uniqueMember','cn=Dummy User')
else:
change = removeAttribute('uniqueMember')[0]
change.values.remove(DistinguishedName('cn=Dummy User'))
addEntryChange(change)
```

インストールの問題

インストール中または直後に次の問題が発生します。

- Access Server のインストール停止
- インストール後に CGI プログラムが実行しない
- Windows にインストールした場合のファイル置換警告
- 「不正な資格証明エラー（49）」でのインストール失敗
- インストーラが DLL ファイルの置換を求める
- GUI モードでの UNIX インストールの実行
- Windows インストールの中止
- AIX でのインストール時にルート以外のユーザーとして実行する
- インストール・ディレクトリの指定
- インストールのテスト
- 「Person オブジェクト・クラス」ページから進めない
- AIX での Apache Web サーバーに対する WebGate のインストール

Access Server のインストール停止

症状 : このサーバーに対する DB プロファイルがないというメッセージが出て、Access Server のインストールが停止します。

解決方法 : 次の手順を実行します。

1. ブラウザで Policy Manager の WebPass インスタンスの URL を指定して、アクセス・システム・コンソールにナビゲートします。次に例を示します。

   `http://`*`hostname`*`:`*`port`*`/access/oblix`

   hostname は WebPass インスタンスの Web サーバー・ホスト、*port* は WebPass Web サーバー・インスタンスの HTTP ポート番号を示し、`/access/oblix` はアクセス・システム・コンソールを指します。

2. 「アクセス・システム・コンソール」リンクを選択して、マスター管理者権限を持つユーザーとしてログインします。

3. **「アクセス・システム構成」**タブ→**「Access Server 構成」**（左側の列）→**「AccessServer_Link」**を選択します。

4. 詳細ページの一番下の**「DB プロファイルの関連付け」**ボタンをクリックします。

5. ページの一番下の**「AccessServer_default_user_profile」**リンクをクリックします。

6. すべてのサーバーまたは適切なサーバーが指定された状態で、**「AAA Servers」**がオンになっていることを確認します。

7. ページの一番下でプロファイルが有効になっていることを確認します。

8. **「保存」**をクリックします。

9. ログアウトして Access Server のインストールを続行します。

インストール後に CGI プログラムが実行しない

症状 : Oracle Access Manager をインストールした後で、Web サーバーの CGI プログラムが実行しません。

解決方法 : 次の手順を実行します。

1. `../https:server name/config directory obj.conf` ファイルで、他の Oracle Access Manager Init 関数の前に次の行を追加します。

   ```
   Init fn="Init-cgi" timeout-300 LateInit="yes"
   ```

   このとおりに正確に入力してください。

2. Web サーバーを再起動します。

Windows にインストールした場合のファイル置換警告

症状 : Identity Server を新しいマシンにインストールするとき、インストーラが `winnt/system32/Msvcrt.dll` ファイルを更新されたファイルで置換しようとすることがあります。このファイルは Windows でロックされているため、「ファイルがロックされているため置換できません。」というメッセージが表示されます。

原因 : インストーラが、Windows オペレーティング・システムでロックされているファイルを置換しようとすることがあります。

解決方法 : 警告ボックスで「再起動」をクリックして DLL を置換します。

「不正な資格証明エラー（49）」でのインストール失敗

症状 : 資格証明が有効でも、GUI での Identity Server のインストールが「不正な資格証明エラー（49）」で失敗します。

原因 : サード・パーティ Installshield の ISMP フレームワークの既知の問題です。インストール時に記号 $ を含む入力が指定されると、インストーラが予測不能な解釈を行うことがあります。たとえば、最初の Identity Server のスキーマ更新時に指定するバインド・パスワードが `Admin$$` の場合、ISMP はこれを `Admin$` と解釈してスキーマ更新ツールを起動するため、更新が「不正な資格証明エラー（49）」で失敗します。

回避方法 : 特定のツールの起動時にこの問題が発生する場合は、コマンドラインからツールを実行してください。

注意 : 同じパスワードを使用するすべての Oracle Access Manager インストーラが、同様の資格証明の問題によって失敗することがあります。

インストーラが DLL ファイルの置換を求める

症状 : 同じマシンに下位 Oracle Access Manager コンポーネントをインストールする際、または同じマシンにコンポーネントの 2 つ目のインスタンスをインストールする際に、ユーザーは次の 1 つ以上の DLL ファイルを置換するように求められます。前回のインストール時にファイルを更新している場合も、置換を求められます。

- messagedll.dll
- `mtl70mt.dll`

原因 : これらの DLL は Oracle Access Manager の DLL ではありません。これらの DLL にはバージョン情報が含まれないため、Oracle Access Manager は、DLL の日付スタンプを使用してファイルを置換する必要があるかどうかを検証します。その後のインストールでは、日付スタンプが古いためにユーザーがファイルの置換を求められます。

解決方法 : **「OK」**をクリックして DLL を置換します。

GUI モードでの UNIX インストールの実行

症状 : UNIX で GUI によるインストールを開始すると、フォントとスクロール・バーに関する警告を受け取ることがあります。

解決方法 : このような警告は無視できます。これらは、インストール・ウィザードの GUI の表示変更を示すものです。

Windows インストールの中止

症状 : Windows インストール・ウィザードを強制終了（[Ctrl]+[C] を押すか「タスク マネージャ」を使用して終了）すると、ウィザードはファイルを適切にクリーンアップできず、大容量のデータが `TEMP` ディレクトリに残ります。

解決方法 : ファイルを手動で削除します。

AIX でのインストール時にルート以外のユーザーとして実行する

Install Shield をルート以外のユーザーとして AIX で実行するには、次のように環境変数を設定します。

```
AIX_ISMP_SUPPORT=NONROOT
```

インストール・ディレクトリの指定

Oracle Access Manager コンポーネントは、標準の英数字のみでパス名が構成されるディレクトリにインストールします。すべてのファイルおよびパス名は英語の文字のみで指定してください。ファイルおよびパス名に、国際文字は使用できません。

インストールのテスト

Oracle Access Manager のインストールが終了したら、インストールをテストします。

Oracle Access Manager のインストールをテストする手順

次の手順を実行して、Oracle Access Manager のインストールをテストします。

1. すべてのブラウザを閉じます。
2. Access Server を停止します。
3. Oracle Access Manager で保護されているページを開こうとしてみてください。

   ログインを認証できなかったことを示す Oracle Access Manager の操作エラーを受け取ります。
4. Access Server および Web サーバーを再起動します。
5. 手順 3 と同様に同じページに接続してみます。指定したページが開きます。

「Person オブジェクト・クラス」ページから進めない

症状 : インストールと設定の際に「Person オブジェクト・クラス」ページから先に進めません。

原因 : おそらくディレクトリのスキーマが無効です。

解決方法 : ディレクトリ・スキーマに対して行った変更を確認し、適切に変更されているかどうかを調べます。

AIX での Apache Web サーバーに対する WebGate のインストール

症状 : AIX で実行している Apache Web サーバーに SSL モードで WebGate をインストールします。`sample.obj.conf` ファイルから `httpd.conf` ファイルに変更します。`httpd.conf` ファイルに変更した後で、Apache Web サーバーが起動できなくなります。次のメッセージが表示されます。

「サーバー証明書連鎖ファイルの名前が httpd.conf に ca.cert としてハードコードされています。」

解決方法 : ユーザーのサーバー証明書連鎖ファイルの実際の名前と一致するように Server-Certificate-Chain-filename を変更します。

言語の問題

次に、発生する可能性がある問題の解決方法を示します。

パスワード・メッセージの文字化け

問題 : いくつかの言語パックがあるときに、コンソールからインストーラを実行すると、「パスワードを入力」という文字列が正しく表示されません。LDAP パスワードの入力を求める表示が文字化けすることがあります。

解決方法 : ほとんどの場合に対応する解決方法は、Oracle Access Manager のインストールを実行するコンピュータに、使用可能なすべての言語サポートをインストールすることです。言語で必要なすべてのフォントがインストールされるようにしてください。マシンにローカルでログインし、ログイン画面に表示される言語を選択します。

追加の管理者言語パックのインストール

症状 : アクセス・システムのコンポーネントに追加の管理者言語パックをインストールする場合、事前に ID システムに同じ言語パックをインストールしていると、Policy Manager で新しい管理者言語を表示できないことがあります。

解決方法 : 次の手順を実行して、新しい管理者言語を有効にします。

アクセス・システムの追加の管理者言語を有効化する手順

1. ID システムのすべてのコンポーネントに対して新しい管理者言語をインストールします。
2. アクセス・システムのコンポーネントに対して新しい管理者言語をインストールします。
3. ID システム・コンソールを使用して、次のように管理者言語を有効化します。
   - 管理者言語がすでに有効化されている場合は無効化します。
   - 管理者言語（現在、ID システムとアクセス・システム両方のコンポーネントにインストールされている）を有効化します。
4. 該当する Oracle Access Manager サーバー・サービス（たとえば、Identity Server および Access Server サービス）と Web コンポーネント（WebPass、Policy Manager および WebGate）の Web サーバー（Apache、IIS、Sun ONE など）を再起動します。

同じディレクトリへの Policy Manager と WebGate の言語パックのインストール

症状 : Policy Manager、言語パック、WebGate の順に同じディレクトリにインストールすると、WebGate が、インストールされた管理者言語を使用しません。

原因 : Policy Manager、言語パック、WebGate の順に同じディレクトリにインストールすると、言語が Policy Manager のみに対してインストールされます。この場合、Policy Manager と WebGate の両方が同じ obnls.xml ファイルを共有します。

解決方法 : WebGate に対して同じ言語パックをインストールします。

症状 : Policy Manager、言語パック、WebGate の順に同じディレクトリにインストールした場合、Policy Manager が、インストールされた言語を使用しません。

原因 : WebGate のインストール時に、Policy Manager インストール・ディレクトリの obnls.xml を上書きするかどうかを確認されることがあります。「はい」を選択すると、Policy Manager の obnls.xml ファイル（追加の言語パック・エントリが含まれる）が新しい obnls.xml ファイル（インストール済言語すべてのリストが含まれない）で置換されます。この結果、Policy Manager が、追加の管理者言語に対応できなくなります。

解決方法 : WebGate のインストール時に、Policy Manager インストール・ディレクトリの obnls.xml の上書きを確認されたら、必ず「いいえ」を選択します。「はい」を選択すると、Policy Manager の場合と同様に WebGate にすべての言語をインストールする必要があります。

デフォルト管理者言語パックの削除

インストール時に選択されたデフォルトの管理者言語に関連する言語パックの削除はサポートされていません。

デフォルト管理者言語を誤ってアンインストールした場合は、次の手順を実行して元に戻すことができます。

デフォルト管理者言語をリストアする手順

1. 削除したデフォルト管理者言語のために、次のような内容の 1 つのオプション・ファイル（たとえば options.txt）を作成します。

   ```
   -W ObPropBean.defaultLocale="ko-kr"
   ```

   この例の ObPropBean.defaultLocale の値 "ko-kr"（韓国語）は、このインストールで選択されたデフォルト管理者言語のロケールです。

2. 次の例のように、各コンポーネントにデフォルト管理者言語パックを再インストールします。

   ID システム :

   ```
   Oracle_Access_Manager10_1_4_0_1_KO_Win32_LP_Identity_System.exe
   -options options.txt
   ```

   アクセス・システム :

   ```
   Oracle_Access_Manager10_1_4_0_1_KO_Win32_LP_Access_System.exe
   -options options.txt
   ```

3. 各コンポーネントにデフォルト管理者言語パックを再インストールしたら、サーバー・サービス（Identity Server と Access Server）と、WebPass、Policy Manager および WebGate の Web サーバー OHS または IIS を再起動します。

ログインの問題

ここでは、ログイン時に発生する可能性がある次の問題について説明します。

Identity Server にログインしていますが、アクセス・システムからログアウトしています。

「Identity Server にログインしていますが、アクセス・システムからログアウトしています。」というメッセージが、次の 1 つ以上のイベントによって表示されることがあります。次に例を示します。

- アクセス・システムのコンポーネントを設定した後で Identity Server を再起動しなかった場合
- Identity Server と Access Server が別のマシンで実行しており、クロックが別の時刻に設定されている場合

  この場合は、ログインの slack パラメータを変更するか、システム・クロックを同期化します。
- ID システムをポリシー・ドメインで保護しているが、アクセス・システムは保護していない（またはその逆）の場合

  両方のシステムを保護する必要があります。
- 共有シークレットを再生成する必要がある場合

共有シークレットを再生成する手順

1. ディレクトリ・サーバーから共有シークレットを削除します。
2. アクセス・システム・コンソールにログインします。
3. 「アクセス・システム構成」→「共通情報の構成」→「共有シークレット」を選択します。
4. 新しい共有シークレットを生成します。

インストール後に Windows 2000 ユーザーがログインできない

症状 : Oracle Access Manager のインストール後にユーザーがログインできません。

原因 : ユーザー・データを Active Directory にインポートすると、すべてのパスワードが消去されます。これは Active Directory のセキュリティの機能です。

解決方法 : Active Directory の「User and Computer MMC」で「Change password on next login」チェック・ボックスの選択が解除されていることを確認します。パスワードを変更するよう、ユーザーに指示します。

Policy Manager では、Password 属性のアクセス制御を有効化します。これで、パスワードを変更するためのサービス・チケットを、ユーザーが強制的に作成するようになります。

ログイン・プロンプトが繰返し表示される

症状 : ユーザーに対してログイン・プロンプトが繰返し表示されます。

原因 : これは、Oracle Access Manager をインストールした Web サーバーで、Web ブラウザによるセキュリティ・ポリシーを施行している場合に発生することがあります。

解決方法 : Oracle Access Manager のセキュリティを有効化し、ブラウザのセキュリティを無効化します。

IIS で Oracle Access Manager にログインできない

症状 : /identity または /access ディレクトリを表示しようとする場合、または「システム・コンソール」リンクや「Policy Manager」リンクをクリックした場合に、予測できない動作（ファイル・ダウンロードのためのダイアログ・ボックスの表示など）が発生することがあります。

原因 : これは、Oracle Access Manager をインストールした Web サーバーで、Web ブラウザによるセキュリティ・ポリシーを施行している場合に発生することがあります。Oracle Virtual Directory に「スクリプトのみ」権限がある場合、ユーザーはアクセス・システム・コンソールまたは Policy Manager にログインできません。

解決方法 : Oracle Virtual Directory の権限を「スクリプトのみ」から「スクリプトと実行可能ファイル」に変更します。

Oracle Virtual Directory の権限を変更する手順

1. Oracle Access Manager に対して構成されているマシンを選択します。
2. デフォルト Web サイトを開きます。
3. **identity** または **access**（ID システムまたはアクセス・システムのインストール時に作成した仮想ディレクトリ）を右クリックします。
4. **「プロパティ」**を選択し、**「スクリプトと実行可能ファイル」**を選択します。

Oracle Access Manager のアクセス制限

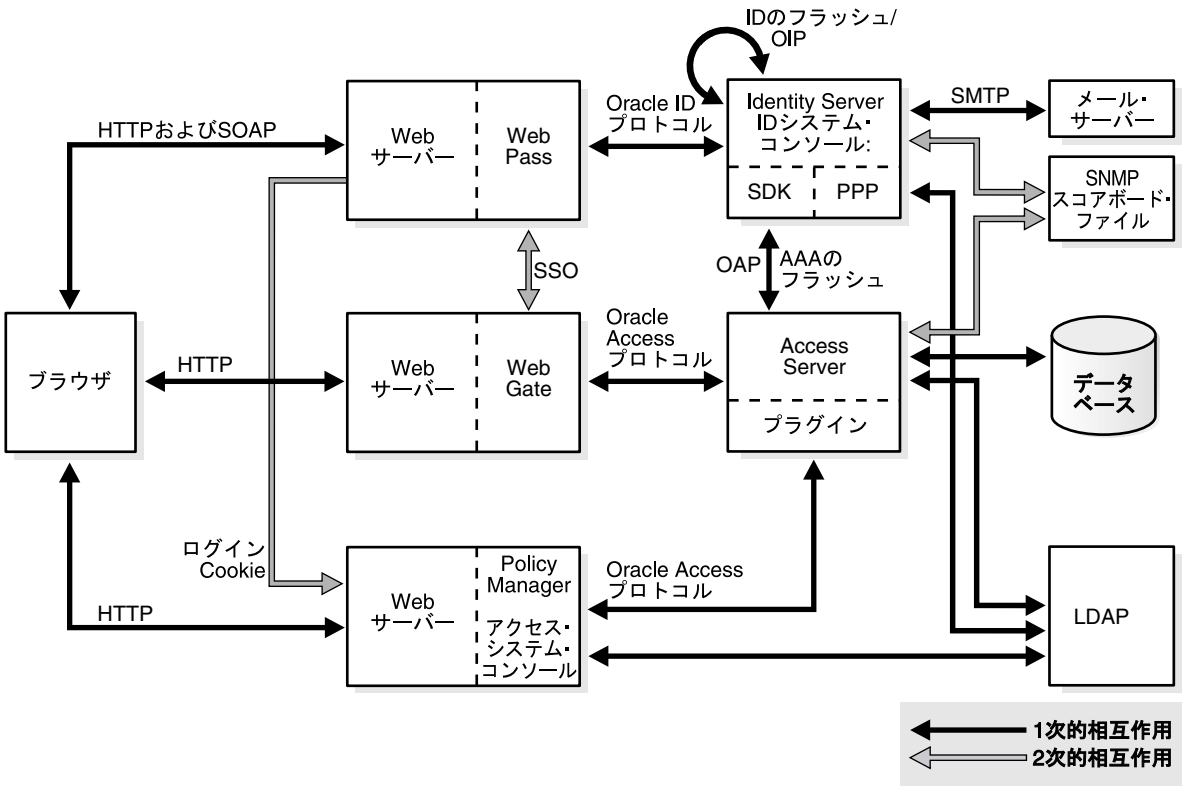
症状 : インストール後、Oracle Access Manager によってリソースへのアクセスが保護されますが、Oracle Access Manager そのものへのアクセスはまだ制限されていません。

解決方法 : Policy Manager を使用して Oracle Access Manager へのアクセスを制限します。

Policy Manager の問題

有効なディレクトリを指すように TEMP 環境変数を設定する必要があります。図 E-1 に示すように、システム全体でこのように設定することをお薦めします。ただし、IIS ユーザーに対しても TEMP 変数を設定できます。

図 E-1 TEMP 環境変数の設定



この変数がないと、Policy Manager は一時的な中間ファイルをルート・ディクトリに作成しようとします。そのレベルにファイルを作成する権限が IIS にない場合、次のような状況でエラーが発生します。次に例を示します。

- Policy Manager を設定するとき
- アクセス・システム・コンソールのメイン・ページで「**Policy Manager**」または「**アクセス・システム・コンソール**」リンクを選択するとき

  この場合、設定ページに、TEMP ディレクトリを見つけられないことを警告するエラー・メッセージが表示されることがあります。

Policy Manager のポリシー・プロファイルを削除できない

症状 : オプションの Policy Manager をアンインストールし、*PolicyManager_install_dir* の setup* ファイルと config* ファイルを削除した後で、「ポリシー・ベースにアクセスするディレクトリ・サーバー・プロファイルは削除できません。」というメッセージを受け取ります。ユーザー・データと構成データの Policy Manager プロファイルは、ID システム・コンソールで削除できますが、ポリシー・データのプロファイルは削除できません。

解決方法 : オプションの Policy Manager をアンインストールした後、残りの Policy Manager ポリシー・プロファイルを削除する前に、次の手順を実行する必要があります。

残りの Policy Manager ポリシー・プロファイルを削除する手順

残りの Policy Manager ポリシー・プロファイルを削除するには、次の手順を実行します。

1. Policy Manager をアンインストールします。
2. ディレクトリ・サーバーで、oblix 関連のすべてのエントリを削除します。必ず、最上位ノードから `obpolicybase` 属性を削除してください。次に例を示します。

   ```
   o=Oblix,o=oblixdata,c=uk
   ```

3. Identity Server を再起動します。
4. ID システム・コンソールで Policy Manager ポリシー・プロファイルを削除します。

関連項目 : Policy Manager に影響する問題の詳細は、次の項目を参照してください。

- Active Directory の検索停止
- Active Directory の動的リンク補助クラス
- インストール後に Windows 2000 ユーザーがログインできない
- IIS で Oracle Access Manager にログインできない
- Oracle Access Manager のアクセス制限

Oracle Internet Directory に対する Oracle Access Manager の再インストール

Oracle Access Manager を削除し、同じディレクトリ・インスタンスを使用して再インストールする場合は、Oracle Access Manager 構成ツリーのみを削除してください。この場合、ディレクトリ・インスタンスから Oracle Access Manager スキーマを削除する必要はありません。Identity Server を再インストールするときに、スキーマ（すでに存在する）を更新するかどうかを確認されたら「いいえ」を選択します。「はい」を選択すると、「スキーマがすでに存在します」というエラー・メッセージが生成されます。

ディレクトリ・ベンダーのツールと指示を使用して、Oracle Access Manager 構成ツリーをディレクトリ・サーバー・インスタンスから削除します。たとえば、Oracle Internet Directory では、Oracle Internet Directory 管理コンソールを使用できます。ただし、依存状態があることや再起的削除が不可能であることから、親オブジェクトを単に削除することはできません。

Oracle Internet Directory からコンソールを使用して Oracle Access Manager スキーマを削除しないようにお薦めします。かわりに、*Component_install_dir*¥identity¥access¥oblix¥data.ldap¥common の LDIF ファイルを使用することをお薦めします。次に例を示します。

- **OID_oblix_schema_index_delete.ldif:** Oracle Access Manager 属性インデックス・クリーンアップ・ファイル。スキーマのクリーンアップの前または後に、Oracle Access Manager インデックスを削除します。
- **OID_user_schema_delete.ldif:** Oracle Internet Directory 用の Oracle Access Manager ユーザー・データ・クリーンアップ・ファイル。構成データとは別のディレクトリ・インスタンスにあるユーザー・データを削除します。

- **OID_oblix_schema_delete.ldif:** Oracle Internet Directory 用の Oracle Access Manager 構成データ・クリーンアップ・ファイル。同じディレクトリ・インスタンスにあるユーザー・データと構成データの両方を削除します。

ユーザー・データと構成データが同じディレクトリ・インスタンスにあるときは、OID_oblix_schema_delete.ldif のみを使用する必要があります。これによってユーザー・スキーマ・オブジェクトも削除されるためです。ただし、別のディレクトリ・インスタンスにユーザー・データのみがある場合は、OID_user_schema_delete.ldif を使用する必要があります。ただし、どちらの場合も属性インデックスの削除には OID_oblix_schema_delete.ldif を使用してください。

手順は、第 20 章「Oracle Access Manager の削除」を参照してください。

削除の問題

コンポーネント・ファイルが指定のインストール・ディレクトリに抽出された後で、コンポーネントのインストールが終了した場合（つまりユーザーが終了した場合）、同じ場所に再インストールする前に、そのコンポーネントに対してアンインストーラを実行し、インストール・ディレクトリを削除する必要があります。単にインストール・ディレクトリを削除して、同じ場所にコンポーネントを再インストールしようとすると、vpd.properties ファイルが一貫性のない状態になり、再インストールが機能しません。

たとえば、コンポーネント・ファイルが抽出された後で WebGate のインストールを終了し、WebGate アンインストーラを使用せずにインストール・ディレクトリを手動で削除したとします。この場合、抽出されたファイルは削除されますが、vpd.properties ファイルは削除されません。このため、vpd.properties ファイルが一貫性のない状態になり、正常にインストールできなくなります。

削除と再インストールの問題を避けるために適した方法は、コンポーネントのアンインストーラ・プログラムを実行し、インストール・ディレクトリを削除した後で、コンポーネントを再インストールすることです。ただし、（アンインストーラを実行せずに）コンポーネントのインストール・ディレクトリを手動で削除してから、vpd.properties をバックアップして削除し、コンポーネントのインストールを開始した後で、vpd.properties ファイルをリストアすることもできます。

詳細は、第 20 章「Oracle Access Manager の削除」を参照してください。

トランスポート・セキュリティ・モードの問題

Oracle Access Manager では、3 つのトランスポート・セキュリティ・モード（オープン、シンプルまたは証明書）がサポートされています。オープンは、最初に実装するときは容易ですが、セキュアではありません。

オープンで開始して後から変更するかわりに、必要なトランスポート・セキュリティ・モードを設定して Oracle Access Manager をインストールすることをお薦めします。トランスポート・セキュリティ・モードの変更方法はこの後で説明します。詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

ID システムでトランスポート・セキュリティ・モードを変更する手順

1. 各 Identity Server で、*IdentityServer_install_dir*/identity/oblix/tools/certutil にある Identity Server の certutil プログラムを実行します。

   Identity Server は WebPass の前に構成しておく必要があります。ID システムのすべてのコンポーネントで同じパスワードと PEM キーを使用する必要はありません。

2. 各 WebPass で、*WebPass_install_dir*/identity/oblix/tools/gencert にある WebPass の `gencert` プログラムを実行します。

アクセス・システムでトランスポート・セキュリティ・モードを変更する手順

1. 各 Access Server で、*AccessServer_install_dir*/access/oblix/tools/configureAAAServer にある configureAAAServer プログラムを実行します。

   Access Server は WebGate の前に構成しておく必要があります。アクセス・システムのすべてのコンポーネントでは同じパスワードと PEM キーを使用します。

2. 各 WebGate で、*WebGate_install_dir*/access/oblix/tools/configureWebGate にある configureWebGate プログラムを実行します。

ユーザー・ディレクトリの問題

ディレクトリに関する問題を次に示します。

レプリケートされたディレクトリへのユーザーの追加

Sun ディレクトリ・サーバーをレプリケートして、ユーザーの変更を行うと、書込みが遅れることが通知されます。ただし、新しいユーザーの作成中には通知されません。

コンシューマに対して構成された新しいユーザーが ID システムのページに表示されるのは、サプライヤとコンシューマの間で次に同期化が行われるときです。

同期化をすぐに実行するか、スケジュールに基づいて実行するかは、レプリケーションの指定方法によって異なります。

データ破損

症状 : 「システム・コンソール」またはいずれかのアプリケーションで機能を使用しているときに、Oracle Access Manager がバグ・レポートまたはエラー・メッセージの表示を始めます。これは、データ破損のために発生することがあります。データ破損の診断は困難な場合があります。ディレクトリ・インタフェース・ツールの表示ではデータが有効に見えても、実際のデータ・ファイルが破損していることがあります。これを確認する 1 つの方法は、ldapsearch のような別のツールを使用して同じ検索を実行することです。予期するデータが返されない場合は、データが破損しています。

解決方法 : 最適な解決方法についてディレクトリのベンダーに問い合せます。可能であれば、ディレクトリ・データを LDIF にエクスポートして、LDIF でエラーを調べます。データに明らかなエラーがある場合は、エラーを適切に修正し、修正したデータをインポートします。

Web サーバーの問題

Web サーバーでは次の問題が発生する可能性があります。

- Apache Web サーバーでの Access Server の障害
- エラー、アクセス不可、予測できない動作
- Sun Web サーバー起動時の PCLOSE エラー
- Oracle HTTP Server（OHS）の起動失敗
- IIS DLL の削除と再インストール

Apache Web サーバーでの Access Server の障害

症状 : Apache Web サーバーを実行しているときに、次のメッセージが表示されて Access Server で障害が発生します。

```
libthread panic: cannot create new lwp
(PID: 9035 LWP 2). stackrace:
ff3424cc
0
```

この症状は、Apache Web サーバーが自らのインスタンスをさらに起動したために引き起こされることがあります。1 つ以上の WebGate と Access Server の間の多数の接続を処理するために、追加のインスタンスが必要であるとサーバーが判断した場合に発生します。

追加のインスタンスによってさらに接続数が増え、Access Server の接続数を超過します。

解決方法 : `MinSpareServers`、`MaxSpareServers`、`StartServers` および `MaxClients` パラメータの数値を減らします。

Access Server の構成ディレクトリで、`http.d` 構成ファイルを開きます。

次のパラメータ設定をお薦めします。

- `MinSpareServers` 1
- `MaxSpareServers` 5
- `StartServers` 3
- `MaxClients` 5

エラー、アクセス不可、予測できない動作

症状 : Oracle Access Manager を UNIX にインストールするときに、Web サーバー・インスタンスの作成に使用したのとは違うユーザー ID を使用すると、Oracle Access Manager が不安定になることがあります。次のような動作が発生することがあります。

- ランダムなバグ・レポート・ページ
- ログ・ファイルの書込み失敗エラー
- Web ページのアクセス不可

解決方法 : chown コマンドを使用してファイルの権限を変更します。Oracle Access Manager ディレクトリを、Web サーバー・インスタンスの作成に使用したのと同じユーザー ID に変更します。

Oracle HTTP Server（OHS）の起動失敗

WebPass、WebGate または Policy Manager インスタンスを Oracle HTTP Server（OHS）にインストールした後で、サーバーが起動しなくなります。これは、Oracle Access Manager によって以前の Linux スレッド・モデルが使用されているために起こります。

解決方法 : 次に示すように、httpd.conf ファイルで perl モジュールをコメント化し、LD_ASSUME_KERNEL 環境変数を更新してから再起動します。

OHS の起動失敗を解決する手順

1. 次の場所にある httpd.conf ファイルの perl モジュールをコメント化します。

   OHS v1.3: *`OH$`*`/Apache/Apache/conf/httpd.conf`

   OHS v2: *`OH$`*`/ohs/conf/httpd.conf`

2. LD_ASSUME_KERNEL の値を更新するには、テキスト・エディタで次のファイルを開きます。

   `OH$``/opmn/conf/opm.xml`

3. 次の行を探します。

```
<process-type id="HTTP_Server" module-id="OHS">
```

4. 前の手順で探した行の下に次の情報を追加します。

```
<environment>
<variable id="LD_ASSUME_KERNEL" value="2.4.19" />
</environment>
```

5. このファイルを保存します。
6. 次のコマンドを実行して変更内容を実装します。

```
opmnctl stopall
opmnctl startall
```

Sun Web サーバー起動時の PCLOSE エラー

症状 : Sun Web サーバーを起動しようとすると、次のようなエラーを受け取ります。

```
Unable to start, PCLOSE
```

解決方法 : 次のような問題がこのエラーの原因になります。

- `obj.conf` ファイルの構文エラー
- `obj.conf` ファイルの先頭の空白
- Web サーバー・インスタンスの作成に使用したのとは違うユーザー ID での Oracle Access Manager のインストール
- `obj.conf` ファイルの最後の改行

IIS DLL の削除と再インストール

Oracle Access Manager を Microsoft 社の IIS Web サーバーで実行している場合、Oracle Access Manager を再インストールするときに、次の ISAPI フィルタを手動でアンインストールおよび再インストールする必要があります。

- `tranfilter.dll`
- `oblixlock.dll`（WebGate をインストールした場合）
- `webgate.dll`（WebGate をインストールした場合）

IIS DLL を削除して再インストールする手順

1. Oracle Access Manager をアンインストールします。
2. 前述の DLL を手動でアンインストールします。
3. Active Directory に対して Oracle Access Manager を再インストールします。
4. DLL を手動で再インストールします。

注意 : これらのフィルタは、使用している IIS のバージョンによって異なる可能性があります。これらのフィルタが存在しない、またはその他のフィルタが存在する場合は、オラクル社に問い合せて、存在するフィルタを削除する必要があるかどうかを確認します。

WebGate の問題

WebGate では次の問題が発生する可能性があります。

Access Server と WebGate の名前

Access Server と WebGate の名前には、英語キーボードにない文字を使用することはできません。

アクセス・システム・コンソールの「AccessGate の変更」ページの説明では大文字と小文字は区別されません。たとえば、説明で大文字と小文字を変更しても、その他の部分を変更しないと、保存しても変更が表示されません。この問題に対処するには、変更を認識できるようにその他の情報を追加または変更します。

AccessGate の説明で大文字と小文字を変更する手順

1. **「アクセス・システム・コンソール」→「アクセス・システム構成」→「AccessGate 構成」**にナビゲートします。
2. 特定の AccessGate を検索するか、**「実行」**ボタンを選択してすべての AccessGate のリストを表示します。
3. 変更する WebGate のリンクをダブルクリックします。
4. ページの一番下の**「変更」**をクリックします。
5. 大文字と小文字を変更し、新しい情報を加えた新しい説明を入力します。次に例を示します。

   変更前 : webgate

   変更後 : WebGate with IIS 6.0

WebGate 診断の有効化

WebGate のインストールと構成の後で、ブラウザに次の WebGate 診断の URL を指定します。

```
http(s)://host:port/access/oblix/apps/webgate/bin/webgate.cgi?progid=1
```

host と *port* は WebGate のホスト名と Web サーバー・インスタンスのポート番号です。診断ページが開かない場合は、WebGate が正しくインストールされていません。

WebGate インストール後のエラー・メッセージ

症状 : Solaris コンピュータでデバッグを有効にして Access Server を実行しているときに、その Access Server を使用する Windows サーバーに WebGate をインストールすると、Access Server のデバッグ・ログに次のようなメッセージが表示されることがあります。

```
Got a client!
SSL handshake failed:
error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned
```

解決方法 : このようなメッセージは問題ありません。無視できます。

同じディレクトリへの WebGate と Identity Server のインストール

ID システムの保護を最大にするには、WebGate と ID システムを同じディレクトリにインストールします。

Access Server 停止エラーの受取り

症状 : Access Server に接続しようとすると、停止していることを示すエラーを受け取ります。

解決方法 : 様々な Oracle Access Manager コンポーネントの各ホスト・コンピュータのクロックは、誤差が 75 秒以内であることが必要です。クロックの誤差が 75 秒を超える場合、インストール環境に障害が発生します。

WebGate が Access Server に接続できない

症状 : ID システムを起動しようとすると次のエラーを受け取ります。

```
Access Server error
WebGate cannot connect to Access Server
```

原因 : WebGate を「システム・コンソール」で構成するときは、各 WebGate を少なくとも 1 つの Access Server にリンクする必要があります。

解決方法 : Policy Manager で WebGate を Access Server に関連付けます。その後、WebGate を構成します。

その他の問題

次にその他の問題について説明します。

- キャッシュをフラッシュできない
- マスター管理者への表示権限の付与
- アイドル・セッション時間、最大 Cookie セッション時間
- セキュア・モードでのディレクトリのロード
- ピアが Oracle Access プロトコルを使用しない
- レプリケーション試行後のバグ・レポートの受取り
- 検索と問合せのエラー・メッセージ（「不良 4547」）
- Identity Server にログインしていますが、アクセス・システムからログアウトしています。

キャッシュをフラッシュできない

症状 : Policy Manager がシンプル・トランスポート・セキュリティ・モードまたは証明書トランスポート・セキュリティ・モードを使用する場合、Policy Manager からキャッシュをフラッシュするには証明書が必要です。Policy Manager が、シンプル・モードまたは証明書モードでインストールされた WebGate で保護されている場合は、証明書が存在するため問題ありません。ただし、WebGate をシンプル・モードまたは証明書モードでインストールしていない場合は、Policy Manager が Access Server と通信できないため、アクセス・システム・キャッシュを更新できません。

解決方法 : WebGate のないシステムでは、GenCert ツールを使用して証明書を生成します。このツールは *IdentityServer_install_dir*/identity/oblix/tools に格納されています。*IdentityServer_install_dir* は Identity Server インストール・ディレクトリです。

キャッシュをフラッシュするために証明書を生成するには、次のように入力します。

```
genCert install_dir
```

IdentityServer_install_dir は、Identity Server インストール・ディレクトリです。このファイルをインストール・ディレクトリに書き込むための権限が必要です。

マスター管理者への表示権限の付与

マスター管理者は、Oracle Access Manager のインストールおよび設定の際に指定します。最上位のマスター管理者でも、特に割り当てないかぎり、属性の表示権限はありません。

管理者には、ディレクトリ・ツリーの一番上のレベルで cn 属性（通常はフルネームとして構成される）を表示する権限が必要です。これにより、管理者は、他のユーザーに対して属性のアクセス制御を構成できます。

> **関連資料 :** このタスクの実行の詳細は、『Oracle Access Manager ID および共通管理ガイド』を参照してください。

アイドル・セッション時間、最大 Cookie セッション時間

症状 : シンプルまたは証明書トランスポート・セキュリティ・モードを使用している場合、ユーザーのブラウザは資格証明をキャッシュして、WebGate セッションがタイムアウトになると自動的にそれらを再送信します。このため、タイムアウトの設定が機能していないように見えます。実際には、ユーザー側のアクションはありませんが、新しい認証交換が行われています。

解決方法 : フォームベースの認証を使用します。ブラウザはフォームベースの認証情報をキャッシュしません。

セキュア・モードでのディレクトリのロード

SSL をアクティブ化するとディレクトリをロードする時間が大幅に長くなることがあります。ディレクトリをロードしてから、Web サーバーとディレクトリ・サーバーの SSL をアクティブ化してください。

ピアが Oracle Access プロトコルを使用しない

症状 : 正しくない TCP ポートに設定された Oracle Access Manager 以外のプログラムが Access Server と通信しようとすると、Access Server のデバッグ出力にエラーが生成されます。Access Server のデバッグ出力に次のエラーが表示されます。

```
Peer does not use NetPoint Access Protocol. Connection dropped.
```

Access Server のデバッグ出力のメッセージが生成されることを除き、Oracle Access Manager インストールへの影響はありません。ただし、Oracle Access Manager 以外のピアが Access Server と通信しようとすると失敗します。

解決方法 : TCP ポート番号を調べます。接続に誤りがあります。

レプリケーション試行後のバグ・レポートの受取り

Oracle Access Manager は、デフォルトでは、Sun でのレプリケーションをサポートしていません。

症状 : Sun のコンシューマまたはスレーブに書込みを行うと、バグ・レポート・フォームを受け取ります。

解決方法 : `enableLDAPReferral` パラメータを次のように更新します。

1. テキスト・エディタで `ldapconfigdbparams.xml` ファイルを開きます。このファイルは次の 2 箇所に格納されています。両方を編集してください。
   - *IdentityServer_install_dir*/identity/oblix/data/common/ldapconfigdbparams.xml
   - *Access_Server_install_dir*/access/oblix/data/common/ldapconfigdbparams.xml
2. `enableLDAPReferral` パラメータを true に変更します。
3. 変更内容を保存します。
4. コンシューマまたはスレーブの Web サーバーを再起動します。

検索と問合せのエラー・メッセージ（「不良 4547」）

症状 : 検索または問合せを実行すると、「不正なリクエスト」というメッセージを受け取ります。

原因 : ブラウザに対して、検索または問合せの文字列が長すぎます。ブラウザでは検索や問合せの文字列を URL として処理します。文字列が URL の最大長を超えるとエラーが生成されます。

解決方法 : 検索または問合せの文字列を短くします。

Identity Server にログインしていますが、アクセス・システムからログアウトしています。

症状 : 「Identity Server にログインしていますが、アクセス・システムからログアウトしています。」というメッセージを受け取ります。この問題が発生するのは、Access ドメイン・ポリシーが無効で Identity ドメイン・ポリシーが有効な場合に、Policy Manager に有効なユーザーとしてログインしたときです。

解決方法 : セキュリティのため、Policy Manager にログインするときは、Policy Manager（/access）のポリシーと Identity ドメイン（/identity）のポリシーを有効にして保護する必要があります。

FrontPage が Oracle Access Manager で正しく動作するためには、Oracle Access Manager がすべての認証と認可を実行できるように IIS を設定する必要があります。

Oracle Access Manager ですべての認証と認可を実行できるようにする手順

1. Web サーバーは、Web コンテンツを含むすべてのディレクトリを全面的に制御できるユーザーとして実行する必要があります。
2. Web サーバーの MMC を使用して、**「directory security」**タブをクリックします。
3. 匿名ユーザーと認証の**「Edit」**ボタンをクリックします。

   「allow anonymous users」チェック・ボックスのみが選択されていることを確認します。他の 2 つのチェック・ボックス（**「basic authentication」**と**「nlm authentication」**）は選択を解除します。
4. FrontPage サーバー管理ツール（FrontPage のバージョンごとに異なる）を使用して、Web サーバー・プロセス・ユーザー（IUSR_OBLIX など）を FrontPage の admin に追加します。

索引

A

B

C

D

E

G

I

J

K

L

M

N

O

P

R

S

T

U

W

X

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

な

に

ね

は

ひ

ふ

へ

ほ

ま

ゆ

よ

り

る

れ

ろ

わ