CA Identity Manager™

インストール ガイド（JBoss）

12.6.5

ca technologies

CA Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- CA CloudMinder™ Identity Management
- CA ディレクトリ
- CA Identity Manager ™
- CA Identity Governance（旧 CA GovernanceMinder）
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder ™

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

目次

第 1 章: インストールの概要

このガイドは、CA Identity Manager をインストールするための手順を提供し、プロビジョニングと CA SiteMinder などの、インストールのオプション コンポーネントについても説明します。

このセクションには、以下のトピックが含まれています。

CA Identity Manager のサンプル インストール

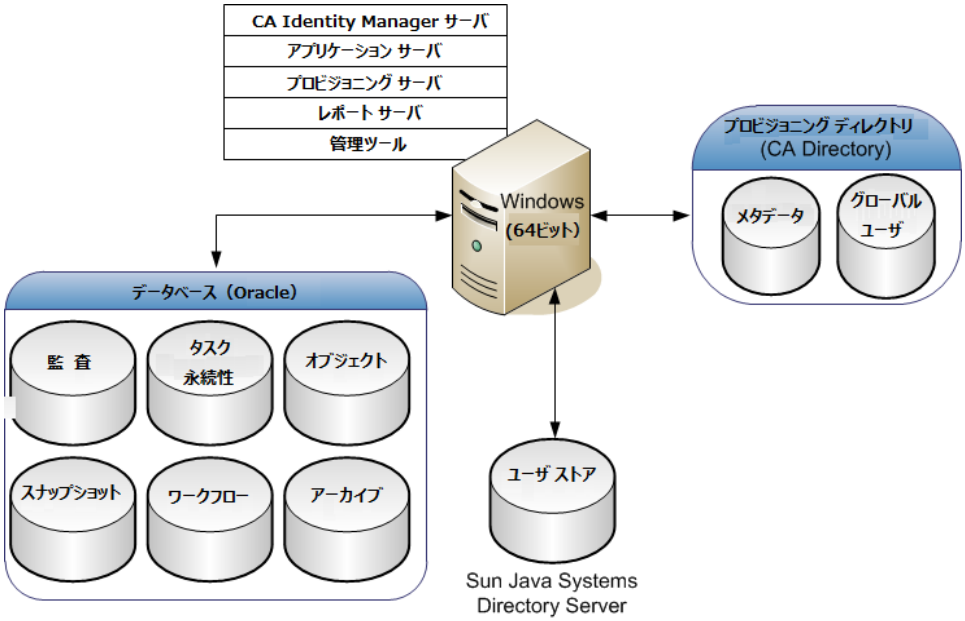
CA Identity Manager では、ユーザの ID と、エンドポイント システムのアプリケーションおよびアカウントに対するユーザ アクセスを制御できます。必要とする機能に基づいて、インストールする CA Identity Manager コンポーネントを選択します。

すべての CA Identity Manager インストールで、CA Identity Manager サーバはアプリケーション サーバにインストールされます。 その他の必要なコンポーネントは CA Identity Manager インストーラを使用してインストールします。

以降のセクションでは、高レベルでの CA Identity Manager の実装例を示します。

例: 単一ノード インストール

単一ノード インストールでは、1 つのアプリケーション サーバ ノード上に CA Identity Manager サーバがインストールされます。 また、各プロビジョニング コンポーネントの 1 つのコピーがインストールされますが、コンポーネントは異なるシステム上にインストールできます。 以下の図は、単一ノードへの CA Identity Manager インストールの例で、同じシステム上にプロビジョニング サーバ、別のシステム上にプロビジョニング ディレクトリがあります。



この例は、プラットフォームの選択肢も示します。 この場合は、以下が行われます。

- CA Identity Manager サーバは Windows 上にインストールされます。
- ユーザ ストアは Sun Java Systems Directory サーバ上にあります。
- データベースは Oracle 上にあります。

これらのプラットフォームは単なる例です。 他のプラットフォームを代わりに選択できます。

CA Identity Manager サーバ

CA Identity Manager 内のタスクを実行します。 J2EE CA Identity Manager アプリケーションには、管理コンソール (環境設定用) およびユーザ コンソール (環境管理用) が含まれます。

CA Identity Manager 管理ツール

CA Identity Manager を設定および使用するためのツールおよびサンプルを提供します。 ツールには、Connector Xpress、Java コネクタ サーバ SDK、設定ファイル、スクリプト、ユーティリティ、および CA Identity Manager API と API サンプルと共にカスタム オブジェクトのコンパイルに使用する JAR ファイルが含まれます。 プロビジョニング マネージャおよび WorkPoint Designer も管理ツールに含まれています。

ほとんどの管理ツールのデフォルトの場所は、以下のとおりです。

- **WIndows：** C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools
- **UNIX：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

ただし、プロビジョニング マネージャのデフォルトの場所（Windows にインストールされる場合のみ）は、以下のとおりです。

C:¥Program Files¥CA¥Identity Manager¥Provisioning Manager

注: Tools¥db ディレクトリには、データベース スキーマについて説明するドキュメントも含まれます。

レポート サーバ

CA Business Intelligence を使用します。 このサーバを使用してスナップショット データベースからデータを組み込みます。 これには、CA Identity Manager オブジェクト ストアおよび CA Identity Manager ユーザ ストアからの情報が含まれます。 スナップショット レポートの例は、ユーザ プロファイル レポートです。 また、無効なスナップショットを応用して、レポートを作成できます。 これには、監査データベースなど他のデータ ソースからのデータが含まれます。

CA Identity Manager データベース

CA Identity Manager のデータを格納します。 データベースは、監査、タスク永続性、スナップショット（レポート）、ワークフロー、および CA Identity Manager オブジェクトの情報を格納します。 各データベースは、リレーショナル データベースである必要があります。

注: サポートされているリレーショナル データベースの一覧については、CA サポート サイトで CA Identity Manager サポート マトリックスを参照してください。

CA Identity Manager ユーザ ストア

ユーザとその情報を含みます。 このストアは、会社によってすでに使用中の既存ユーザ ストアである場合があります。 このユーザ ストアは、LDAP データベースまたはリレーショナル データベースの場合があります。

注: CA Identity Manager のユーザ ストアのセットアップの詳細については、「*設定ガイド*」を参照してください。

CA Identity Manager プロビジョニング サーバ

エンドポイント システムのアカウントを管理します。同じシステムまたは別のシステムに、コネクタ サーバもインストールできます。これはエンドポイントに対する Java または C++ ベースのコネクタを管理します。

CA Identity Manager プロビジョニング ディレクトリ

CA Directory に対するプロビジョニング ディレクトリ スキーマを指定します。 このスキーマにより CA Directory 内に Directory System Agent（DSA）をセットアップします。CA Identity Manager ユーザ ストアが、プロビジョニング ディレクトリである場合もあります。

CA Identity Manager プロビジョニング マネージャ

グラフィカル インターフェースを通じてプロビジョニング サーバを管理します。このツールは、アカウント テンプレートを使用してアカウントを同期するような管理タスクに使用されます。プロビジョニング マネージャは CA Identity Manager 管理ツールの一部としてインストールされるか、またはそれらのツールとは別個にインストールできます。

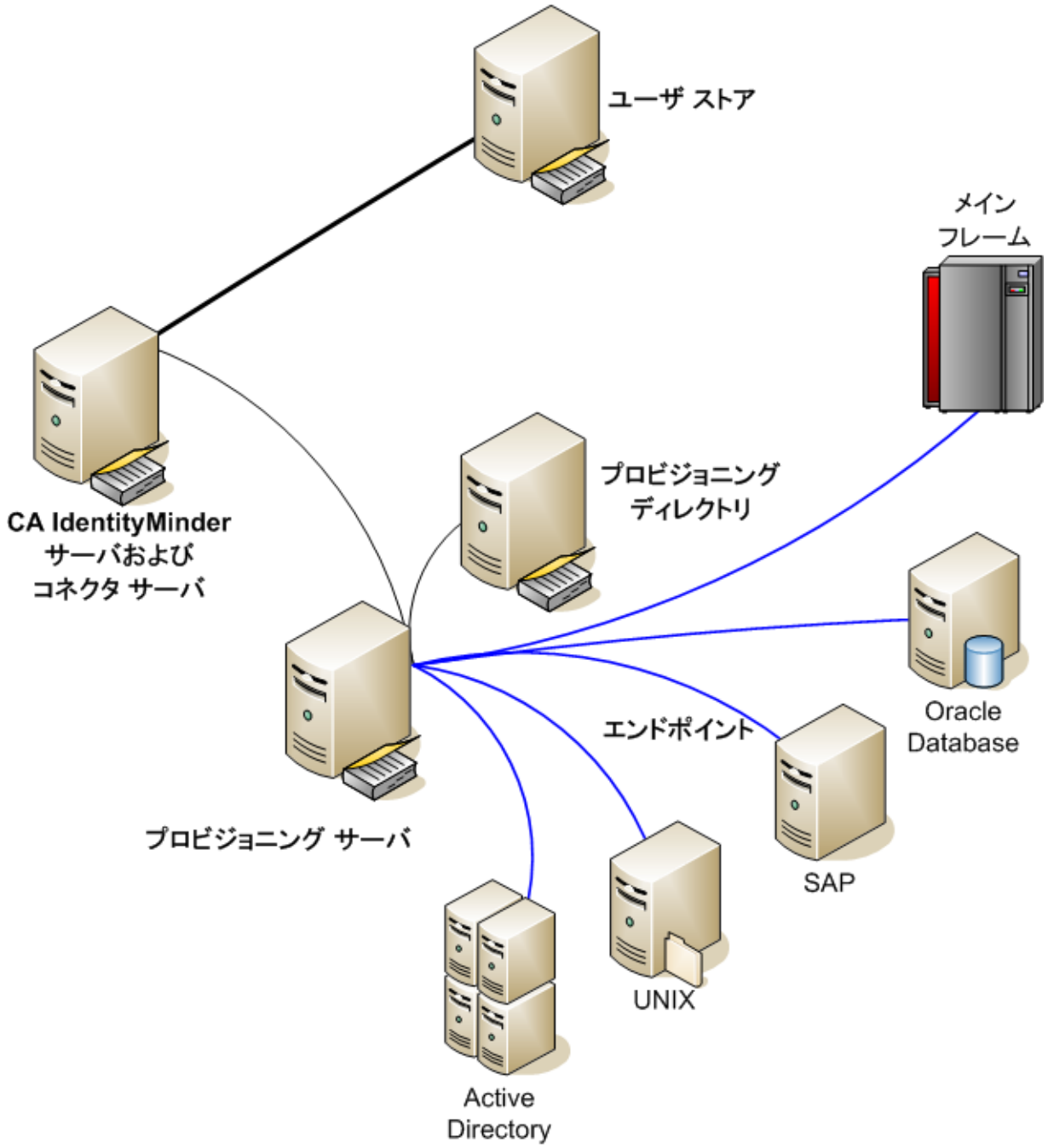
注: このアプリケーションは Windows 上でのみ実行されます。

例: 複数のエンドポイントを用いたインストール

プロビジョニング サーバのインストールによって、管理者は電子メール サーバ、データベース、他のアプリケーションなどのエンドポイントのアカウントをエンド ユーザに提供できるようになります エンドポイント システムと通信するには、SAP コネクタなど、エンドポイント固有のコネクタ用のコネクタ サーバをインストールします。

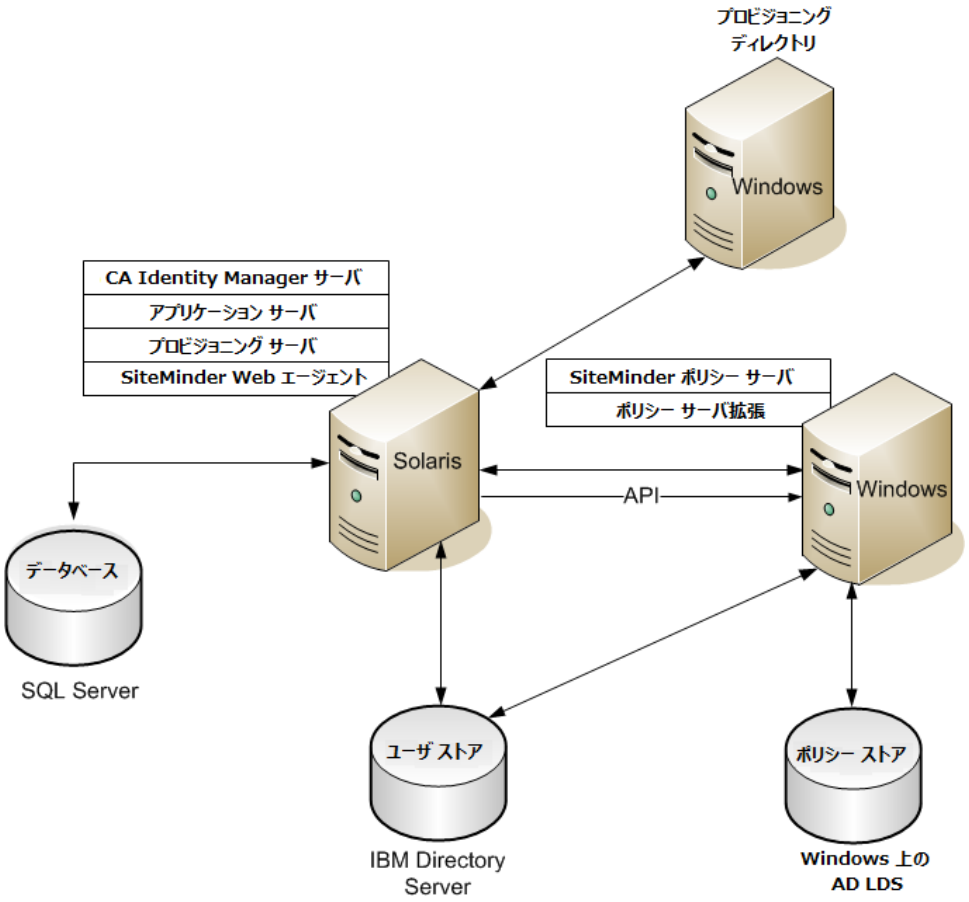
標準インストール シナリオでは、ユーザ ストアおよびプロビジョニング ディレクトリ用の個別のシステムを含み、引き続き同期化されます。

この例では、CA Identity Manager を使用して、Active Directory、UNIX、SAP、Oracle、およびメインフレーム システムのアカウントへのアクセスを提供する方法を示します。



例 : SiteMinder および CA Identity Manager のインストール

CA Identity Manager は SiteMinder ポリシー サーバと統合でき、これによりユーザ環境に高度な認証および保護を提供します。 以下の図は、認証と認可用の CA SiteMinder ポリシー サーバを使用した CA Identity Manager インストールの例です。



SiteMinder 要素は以下のように定義されます。

SiteMinder Web エージェント

SiteMinder ポリシー サーバと連携して、ユーザ コンソールを保護します。 CA Identity Manager サーバ を有するシステムにインストールされます。

SiteMinder ポリシー サーバ

CA Identity Manager 用の高度な認証と認可、およびパスワード サービスやシングル サインオン などの機能を提供します。

SiteMinder ポリシー サーバの拡張

SiteMinder ポリシー サーバが CA Identity Manager をサポートできるようにします。CA Identity Manager 実装において、各 SiteMinder ポリシー サーバ システムに拡張機能をインストールします。

CA Identity Manager コンポーネントは、前の例の単一ノード インストールで定義されています。ただし、この例では、異なるプラットフォームにコンポーネントがインストールされます。 CA Identity Manager データベースは、Microsoft SQL Server 上にあり、ユーザ ストアは IBM Directory Server 上にあります。 SiteMinder ポリシー ストアは Windows 上の AD LDS にあります。 Windows はポリシー ストアにサポートされている複数のプラットフォームのうちの 1 つです。

高可用性インストール

CA Identity Manager をインストールする前に、実装の目標を考慮してください。 たとえば、1 つの目標は、一貫して優れたパフォーマンスを提供する回復力の実装です。 別の目標としては、拡張性です。

高可用性実装は以下の機能を提供します。

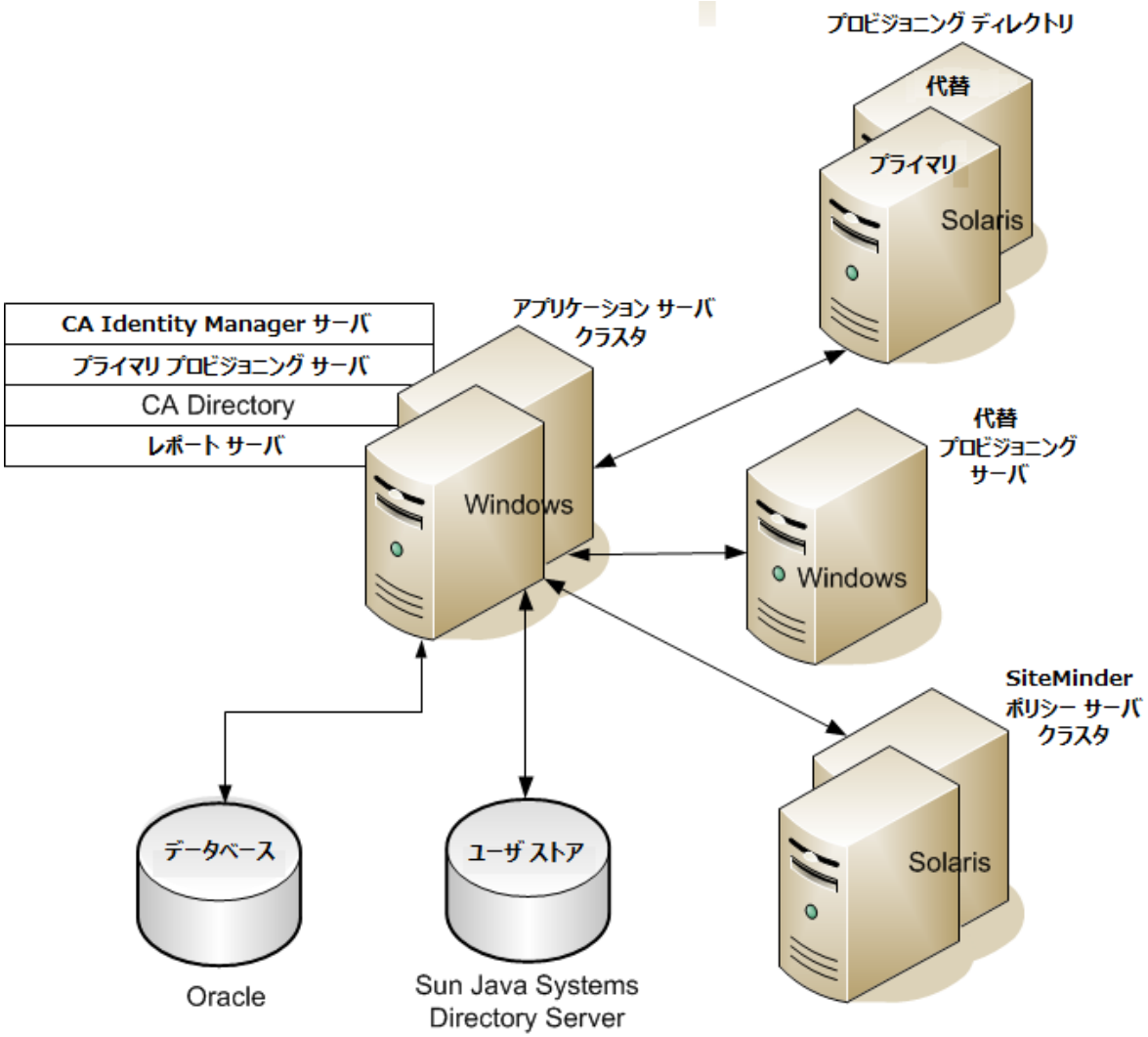
- フェイルオーバ -- プライマリ システムが故障するか、または何らかの理由で一時的にオフラインになった場合、別のシステムに自動的に切り替えます。
- 負荷分散 -- 優れたパフォーマンスが維持され、単一のデバイスが圧倒されることがないように、コンピュータ ネットワーク全体に処理および通信アクティビティを平等に配布します。
- さまざまな展開層が動的なビジネス要件に役立つ柔軟性を提供します。

これらの高可用性機能を提供するために、以下の実装オプションが存在します。

- CA Identity Manager サーバがアプリケーション サーバ クラスタにインストールされて、クラスタ内のノードへのフェイルオーバを可能にし、中断されないアクセスをユーザに提供します。アプリケーション サーバは 64 ビット形式も可能で、これは 32 ビット アプリケーション サーバより高いパフォーマンスを提供します。
- プロビジョニング サーバは、CA Directory ルータを使用してプロビジョニング ディレクトリにトラフィックをルーティングします。
- CA Identity Manager には、ディレクトリまたは管理対象システムごとに設定するコネクタ サーバが含まれます。 複数のコネクタ サーバのインストールにより、回復力が向上します。各コネクタ サーバも LDAP サーバであり、プロビジョニング サーバと同様です。

例: 高可用性インストール

以下の図は、CA Identity Manager サーバ、プロビジョニング サーバ、プロビジョニング ディレクトリ、および SiteMinder ポリシー サーバに高可用性を提供する例です。 代替コンポーネントおよびクラスタの使用により、高可用性機能を提供します。



この図は高可用性を示し、SiteMinder の図と対照させて、コンポーネントに使用される異なるプラットフォームを示しています。 たとえば、データベースは、前の図で示された Microsoft SQL Server の代わりに Oracle を使用しています。

CA Identity Manager サーバ アーキテクチャ

CA Identity Manager 実装は、下記の 3 層を含む、ハードウェアとソフトウェアの組み合わせを含む多層環境にまたがる場合があります。

- Web サーバ層
- アプリケーション サーバ層
- ポリシー サーバ層（オプション）

各層は、同じ機能を実行してその層の作業負荷を共有するサーバのクラスタを含むことができます。 各クラスタを別々に設定するので、必要な場所にのみサーバを追加できます。 たとえば、クラスタ化された CA Identity Manager 実装では、複数のシステムを持つグループはすべて、CA Identity Manager サーバをインストールできます。これらのシステムは、CA Identity Manager サーバが実行した作業を共有します。

注: 異なるクラスタからのノードが同じシステム上に存在できます。たとえば、アプリケーション サーバ ノードを、ポリシー サーバ ノードと同じシステム上にインストールできます。

プロビジョニング コンポーネントのアーキテクチャ

プロビジョニングは、以下の 3 つの層で高可用性ソリューションを提供します。

- クライアント層

  クライアントは、CA Identity Manager ユーザ コンソール、CA Identity Manager 管理コンソール、およびプロビジョニング マネージャです。 地理的な場所、組織単位、ビジネス機能、セキュリティ要件、プロビジョニング作業負荷、または他の管理ニーズに基づいてまとめられるクライアントをグループ化できます。 通常、クライアントを管理対象のエンドポイントの近くに保持することをお勧めします。

- プロビジョニング サーバ層

  クライアントはそのフェイルオーバ 優先順位に従って、プライマリおよび代替プロビジョニング サーバを使用します。 クライアント リクエストは、最初のサーバが失敗するまで、そのサーバに送信され続けます。 言いかえれば、サーバが失敗するまで、その接続はアクティブのままです。 失敗した場合、クライアントは、次に利用可能なサーバを検索するために、設定済みサーバの優先順リストを確認します。

プロビジョニング サーバは、動作する複数のコネクタ サーバを持つことができます。コネクタ サーバはそれぞれ異なるセットのエンドポイントの操作を処理します。 そのため、組織は、ネットワーク内のエンドポイントに近いシステム上にコネクタ サーバを展開できます。たとえば、多数の UNIX などのエンドポイントがあるとします。 このような場合は、1 つのコネクタ サーバを各サーバ上にインストールし、各コネクタ サーバがそれぞれインストールされているサーバ上のエンドポイントのみを制御するようします。

また、コネクタ サーバをエンドポイントの近くにインストールすると、エンドポイント上のアカウント管理における遅延が軽減されます。

- CA Directory 層（プロビジョニング ディレクトリ）

  プロビジョニング サーバは、CA Directory ルータを使用して、プライマリおよび代替プロビジョニング ディレクトリに優先順にリクエストを送信します。

インストール プロセスの全体

CA Identity Manager をインストールするには、以下の手順を実行します。

1. 前提条件のハードウェアおよびソフトウェアをインストールし、必要に応じてシステムを設定します。
2. CA Identity Manager サーバを単一ノードまたはアプリケーション サーバ クラスタにインストールします。
3. （オプション）個別のデータベースを設定します。
4. （オプション）レポート サーバをインストールします。
5. （オプション）高可用性プロビジョニング機能用の代替プロビジョニング ディレクトリ、代替プロビジョニング サーバ、およびコネクタ サーバをインストールします。

注: 本書では、CA Identity Manager の機能またはコンポーネントのインストールまたは設定の手順のチェックリストが各章に含まれています。 そのセクションのタイトルには「方法」が付いています。

第 2 章: インストールの前提条件

このセクションには、以下のトピックが含まれています。

インストール ステータス

以下の表は、インストール プロセスのどこにいるかユーザに示します。

現時点	インストール プロセスの手順
X	**1. 前提条件のハードウェアおよびソフトウェアをインストールし、必要なシステムを設定します。**
	2. 以下のインストールのいずれかを実行します。 ■ 単一ノード インストール ■ アプリケーション サーバ クラスタ上のインストール
	3. （オプション）個別のデータベースを作成します。
	4. （オプション）レポート サーバをインストールします。
	5 （オプション）フェイルオーバと負荷分散をサポートするために、代替プロビジョニング ディレクトリ、代替プロビジョニング サーバ、およびコネクタ サーバをインストールします。

前提条件として必要な知識

本書では、ユーザが Java、J2EE 標準、およびアプリケーション サーバ技術に精通していることを想定しています。 本書では、読者が以下の技術知識を持っていることを想定しています。

- J2EE アプリケーション サーバおよび多層アーキテクチャについての理解。
- 以下などのタスクを含め、アプリケーション サーバをインストールおよび管理した経験。
  - アプリケーション サーバの起動
  - 単一ノードのインストール
  - 高可用性をサポートするためのクラスタのインストール
- リレーショナル データベースを管理した経験
- （オプション） SiteMinder 概念、用語、およびポリシー サーバ設定タスクについての熟知

必須コンポーネントをインストールする方法

スタンドアロンまたはクラスタのインストールに必要な CA Identity Manager の前提条件のハードウェアおよびソフトウェアをインストールする方法

✓	手順
	1. システムがハードウェア要件を満たしていることを確認します。
	2. CA Directory をインストールします。
	3. （オプション） FIPS キーを作成します。
	4. （オプション）暗号化パラメータ ファイルを作成します。
	5. （オプション） SiteMinder と統合します
	6. データベースを作成します。
	7. アプリケーション サーバをセットアップします。
	8. Solaris または Linux にインストールする場合は、要件を満たします。

✓	手順
	9. IPv6 システムにインストールする場合は、IPv6 要件を満たします。
	10. CA Identity Manager インストール プログラムに必要な情報を使って、インストール ワークシートに入力します。

ハードウェア要件のチェック

CA Identity Manager サーバ

以下の要件は、CA Identity Manager サーバをインストールするシステムにインストールするアプリケーション サーバの要件を考慮しています。

コンポーネント	最小	推奨
CPU	Intel（またはその互換）2.0 GHz（Windows または Red Hat Linux）、 SPARC 1.5 GHz （Solaris）または POWER4 1.1 GHz （AIX）	デュアル コア Intel（またはその互換）3.0 GHz（Windows または Red Hat Linux）、デュアル コア SPARC 2.5 GHz （Solaris） POWER5 1.5 GHz （AIX）
メモリ	4 GB	8 GB
使用可能なディスク領域	4 GB	8 GB
一時領域	2 GB	4 GB
スワッピング/ページング スペース	2 GB	4 GB
プロセッサ	中規模および大規模での展開には、64 ビット プロセッサおよびオペレーティング システム、デュアル コア	64 ビットのプロセッサおよびオペレーティング システム、デュアル コア

プロビジョニング サーバまたはスタンドアロン コネクタ サーバ

コンポーネント	最小	推奨
CPU	Intel（またはその互換）2.0 GHz（Windows または Red Hat Linux） SPARC 1.5 GHz （Solaris）	デュアル コア Intel（またはその互換）3.0 GHz（Windows または Red Hat Linux） SPARC 2.0 GHz （Solaris）
メモリ	4 GB	8 GB
使用可能なディスク領域	4 GB	8 GB
プロセッサ	中規模および大規模での展開には、64 ビット プロセッサおよびオペレーティング システム、デュアル コア	64 ビットのプロセッサおよびオペレーティング システム、デュアル コア

プロビジョニング ディレクトリ

コンポーネント	最小	推奨
CPU	Intel （またはその互換） 1.5 GHz（Windows または Red Hat Linux） SPARC 1.0 GHz （Solaris）	デュアル コア Intel（またはその互換）2.5 GHz （Windows または Red Hat Linux） SPARC 1.5 GHz （Solaris）
メモリ	4 GB	8 GB

コンポーネント	最小	推奨
使用可能なディスク領域	エンドポイント アカウントの数に応じて、2 GB から 10 GB。 ■ コンパクト -- 10,000 以下のアカウント、1 つのデータ ファイル当たり 0.25 GB （合計 1 GB） ■ 基本 -- 400,000 以下のアカウント、1 つのデータ ファイル当たり 0.5 GB （合計 2 GB） ■ 中規模 -- 600,000 以下のアカウント、1 つのデータ ファイル当たり 1 GB （合計 4 GB） ■ 大規模 -- 600,000 を超えるアカウント、1 つのデータ ファイル当たり 2 GB （合計 8 GB）	エンドポイント アカウントの数に応じて、2 GB から 10 GB。 ■ コンパクト -- 10,000 以下のアカウント、1 つのデータ ファイル当たり 0.25 GB （合計 1 GB） ■ 基本 -- 400,000 以下のアカウント、1 つのデータ ファイル当たり 0.5 GB （合計 2 GB） ■ 中規模 -- 600,000 以下のアカウント、1 つのデータ ファイル当たり 1 GB （合計 4 GB） ■ 大規模 -- 600,000 を超えるアカウント、1 つのデータ ファイル当たり 2 GB （合計 8 GB）
プロセッサ	中規模および大規模での展開には、64 ビット プロセッサ、64 ビット オペレーティング システム、および CA Directory （64 ビット バージョン）	64 ビットのプロセッサおよびオペレーティング システム

1 つのシステム上のすべてのコンポーネント

運用環境として、単一の物理システム上で CA Identity Manager 製品をホストすることはお勧めしません。 ただし、それを行う場合のハードウェア要件は以下のとおりです。

コンポーネント	最小
CPU	Intel （またはその互換） 3.1 GHz （Windows または Red Hat Linux） SPARC 2.5 GHz （Solaris）
メモリ	8 GB
使用可能なディスク領域	アカウントの数に応じて、14 GB ～ 6 GB
プロセッサ	64 ビットのプロセッサおよびオペレーティング システム、デュアル コア

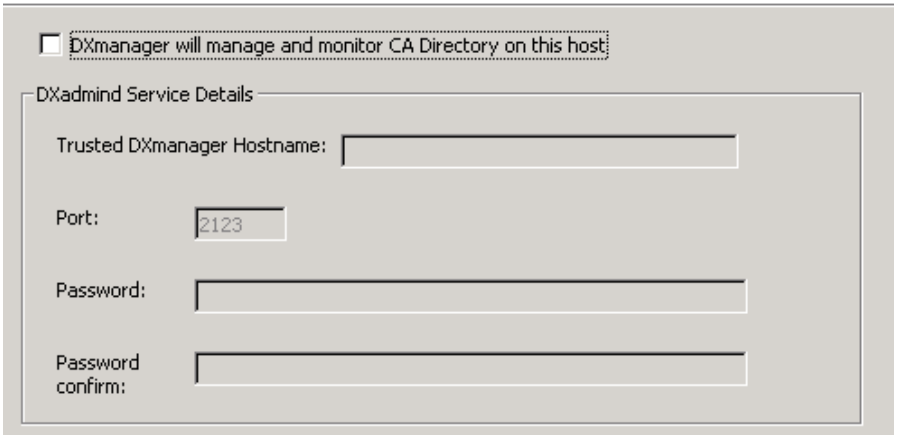
コンポーネント	最小
スワッピング/ページング スペース	6 GB

CA Directory のインストール

CA Identity Manager をインストールする前に、以下の手順に従って CA Directory をインストールします。

1. プロビジョニング ディレクトリをインストールする予定のシステムに CA Directory をインストールします。 サポートされている CA Directory のバージョンは、ユーザのインストール メディアに含まれています。 インストールの詳細については、サポート サイトから CA Directory のマニュアルをダウンロードしてください。

   注: インストーラが DXManager の dxadmind のインストールについて尋ねたら、安全にこのオプションをオフにできます。 プロビジョニング ディレクトリは DXManager を使用しません。



2. プロビジョニング サーバをインストールする予定のシステムに、CA Directory の第 2 のコピーをインストールします。 このインストールはルーティングが目的で、プロビジョニング サーバをリモート プロビジョニング ディレクトリと通信できるようにします。

重要: インストールの前にすべての 対ウイルス ソフトウェアを無効にすることをお勧めします。 インストール中に、対ウイルス ソフトウェアが有効になると、問題が発生する場合があります。 インストールが完了した後に、対ウイルス ソフトウェア を再度有効にしたことを確認してください。

FIPS 140-2 暗号化キーの作成

CA Identity Manager インストーラを実行するとき、FIPS 140-2 コンプライアンス モードを有効にするオプションを与えられます。 CA Identity Manager が FIPS 140-2 をサポートするには、CA Identity Manager 環境内のすべてのコンポーネントが FIPS 140-2 を利用可能である必要があります。 インストール中に FIPS 140-2 を有効にするために、FIPS 暗号化キーが必要です。 FIPS キーを作成するためのパスワード ツールは、PasswordTool¥bin のインストール メディアにあります。

重要: すべてのインストールで同じ FIPS 140-2 暗号化キーを使用します。 パスワード ツールに生成されたキー ファイルを即座に保護したことを確認します。

SiteMinder を使用している場合は、必ず CA Identity Manager インストールの後に正しく ra.xml ファイルを設定します。 詳細については、「*設定ガイド*」の手順「Adding SiteMinder to an Existing CA Identity Manager Deployment」を参照してください。

暗号化パラメータ ファイルの作成

CA Identity Manager サーバのインストール中に、暗号化パラメータを設定するオプションがあります。 この機能を使用し、CA Identity Manager によって使用されるすべての暗号化アルゴリズムのキーの長さ、FIPS 暗号化キーのシード サイズおよび IV サイズ、非 FIPS アルゴリズム（RC2 と PBE）のキー全体など、ユーザ定義のパラメータを提供することにより暗号化コードをカスタマイズします。

パラメータは、プロパティ ファイルとして次の可能なキーで指定される必要があります。PBKey、PBSalt、PBKeySize、RCKey、RCKeySize、AEKey、AEKeySize、AESeedSize、AEIVSize

暗号化アルゴリズムによって許可されている有効なキー サイズ値を以下に示します。

- PBE と RC2 については、キーの最大長は 128 バイトです。
- AES については、有効なキー サイズは 16、24 および 32 バイトです。

重要: すべてのインストールで同じ暗号化パラメータを使用します。インストール後に暗号化パラメータを変更しないでください。

（オプション）SiteMinder との統合

SiteMinder ポリシー サーバは、「*SiteMinder インストール ガイド*」に述べられているように、ユーザがインストールするオプション コンポーネントです。 ポリシー サーバを高可用にする予定の場合は、それをポリシー サーバ クラスタとして設定します。また、CA Identity Manager との通信を有効にするには、JCE ライブラリをインストールします。

ポリシー サーバをインストールする方法

1. SiteMinder ポリシー サーバをインストールします。 詳細については、「CA SiteMinder ポリシー サーバ インストール ガイド」を参照してください。
2. ポリシー サーバを高可用にするには、ポリシー サーバ クラスタ内に存在する必要がある各ノードにこれをインストールします。

   注: クラスタ内の各ポリシー サーバは、それぞれ同じポリシー ストアを使用します。
3. ユーザが CA Identity Manager サーバをインストールする予定のシステムからポリシー サーバをホストするシステムで、ping を実行できることを確認します。

CA Identity Manager の SiteMinder の拡張機能をインストールする方法

CA Identity Manager サーバをインストールする前に、各ポリシー サーバに対する拡張機能を追加します。 ポリシー サーバが CA Identity Manager サーバをインストールする予定のシステム上にあるとします。 このときは、拡張機能および CA Identity Manager サーバを同時にインストールできます。 この場合、この手順を省略します。

1. CA SiteMinder サービスを停止します。
2. デフォルトのディレクトリの場所を、SiteMinder インストール領域のルートに設定します。
3. 以下のコマンドを発行します。

   ```
   ./stop-all
   ```

   すべての SiteMinder 実行可能ファイルはシャット ダウンします。
4. CA Identity Manager の SiteMinder の拡張機能をインストールします。 以下のタスクのいずれかを実行します。

   - **Windows：** ユーザのインストール メディアから、最上位レベルのフォルダ内の以下プログラムを実行します。

     ```
     ca-im-release-win32.exe
     ```

   - **UNIX：** ユーザのインストール メディアから、最上位レベルのフォルダ内の以下プログラムを実行します。

     ```
     ca-im-release-sol.bin
     ```

   release は、CA Identity Manager の現在のリリースを表します。

5. ［Extensions for SiteMinder］を選択します。
6. インストール ダイアログ ボックス内の手順を完了します。
7. 以下のコマンドを発行します。

   ```
   ./stop-all
   ```

   すべての SiteMinder 実行可能ファイルはシャット ダウンします。
8. 以下のコマンドを発行します。

   ```
   ./start-all
   ```

   すべての SiteMinder サービスが開始します。

JCE ライブラリをインストールする方法

CA SiteMinder も使用する場合、CA Identity Manager サーバは JCE （Java Cryptography Extension）ライブラリを必要とします。

CA Identity Manager サーバをインストールする前に、以下の手順を実行します。

1. Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files をダウンロードしてインストールします。
2. ユーザのアプリケーション サーバと JDK で動作するものを選択します。

   ダウンロード ZIP ファイルには、インストール手順を備えた Readme テキスト ファイルが含まれます。

Portal データベースの作成

CA Identity Manager には、監査、スナップショット（レポート）、ワークフローおよびタスク永続性用のオブジェクトおよびデータを格納するためのリレーショナル データベースが必要です。 Oracle または Microsoft SQL Server がサポートされているバージョンをインストールし、データベースを作成します。

CA Identity Manager のインストール時、アプリケーション サーバが起動されるときに、すべてのデータベース スキーマが自動的に作成されます。ただし、CA Identity Manager をインストールした後に、監査、スナップショット（レポート）、ワークフロー、およびタスク永続性用の個別のデータベースを設定できます。 これらのデータベースを作成するには、個別のデータベースの設定についての章を参照してください。

JBoss のインストール

CA Identity Manager 12.6.5 は、JBoss 5.0 および 5.1 Enterprise Application Platform（EAP）、5.1 オープン ソース、および JBoss 6.1（EAP）で動作します。 したがって、バージョンが 5.0 より古い場合は、新しい JBoss バージョンをインストールしてください。新バージョンのファイルは、旧バージョンと同じシステムに共存させることができますが、旧バージョンとは異なる場所にインストールします。 また、使用する JBoss のバージョンに対応していることがサポート マトリックスに示されている JDK をインストールしてください。

注: サポートされているプラットフォームとバージョンの一覧については、CA サポートの CA Identity Manager サポート マトリックスを参照してください。

アプリケーション サーバとして JBoss を使用する際には、以下の点に注意してください。

- CA Identity Manager サーバは、サポートされているアプリケーション サーバ上で展開される J2EE アプリケーションです。

  JBoss 5 の場合、iam_im.ear は *jboss_home*/server/default/deploy フォルダに展開されます。クラスタ化されたインストールの場合、iam_im.ear は j boss_home/server/all/deploy に展開されます。

- Policy XPress の機能が拡張され、Policy XPress を Web サービス インターフェースを提供する外部アプリケーションと統合できるように、Web Services SOAP（基本認証メソッドで）、および REST（基本認証、プロキシ認証、および OAuth 認証メソッドで）をサポートするようになりました。 Policy XPress Web Services（SOAP および REST）を JBoss 5.1 コミュニティ版で使用するには、以下の jar ファイルをお使いの JBoss 5.1 コミュニティ版の "¥lib¥endorsed" ディレクトリに "client" ディレクトリからコピーしてアプリケーション サーバを再起動します。

  - jbossws-native-jaxrpc.jar
  - jbossws-native-jaxws.jar
  - jbossws-native-jaxws-ext.jar
  - jbossws-native-saaj.jar

注: EAP バージョンの場合は、これらのファイルをコピーする必要はありません。

JBoss 6.1 の場合、iam_im.ear は *jboss_home*/server/default/deploy フォルダに展開されます。

重要: deploy ディレクトリ内のデータ ストア ファイルが変更された場合、JBoss はそのデータ ストアへの接続を失い、再起動が必要となります。

- CA Identity Manager Server をインストールする前に JDK の必要なバージョンをインストールしてください。JDK は、以下の URL の Oracle Web サイトからダウンロードできます。

  http://www.oracle.com/technetwork/java/index.html

Solaris の要件

プロビジョニング サーバの要件

/etc/system を確認して、以下の最小の IPC カーネル パラメータ値を確認します。

- set msgsys:msginfo_msgmni=32
- set semsys:seminfo_semmni=256
- set semsys:seminfo_semmns=512
- set semsys:seminfo_semmnu=256
- set semsys:seminfo_semume=128
- set semsys:seminfo_smmsl=128

- set shmsys:shminfo_shmmni=128
- set shmsys:shminfo_shmmin=4

Solaris 9 または 10 の要件

Solaris 9 または 10 上にプロビジョニング ソフトウェアをインストールする前に、必要なパッチをダウンロードし、インストールしてください。

1. 以下の場所からプロビジョニング SDK 用の Sun Studio 10 のパッチをダウンロードします。

   `http://developers.sun.com/prodtech/cc/downloads/patches/ss10_patches.html`

2. パッチ 117830 をダウンロードしてインストールします。

   注: Sun Studio 11 にはパッチは必要ありません。

3. 以下の場所からすべてのプロビジョニング コンポーネント用の Solaris 9 のパッチをダウンロードします。

   `http://search.sun.com/search/onesearch/index.jsp`

4. 9_recommended.zip をダウンロードしてインストールします。

Linux の要件

これらの要件は、Linux システムに存在します。 ユーザが Red Hat インストールを登録している場合は、yum を使用してパッケージをインストールすることをお勧めします。そうでない場合は、rpm を使用してパッケージをインストールできます。

あるいは、依存性を解決するために［Add/Remove Software］を使用して、［Only Native Packages］フィルタ オプションをオフにします。 この方法を用いて、必要な i686 アーキテクチャ依存性を選択してインストールします。

注: i686 サフィックスは、ライブラリが x86 プロセッサの場合、32 ビットであることを指定します。

CA Identity Manager サーバ

Red Hat 5.x	Red Hat 6.x
glibc-2.5-65.i686.rpm	glibc-2.12-1.47.el6.i686.rpm

Red Hat 5.x	Red Hat 6.x
libXext-1.0.1-2.1.i386.rpm	libXext-1.1-3.el6.i686.rpm
libXtst-1.0.1-3.1.i386.rpm	libXtst-1.0.99.2-3.el6.i686.rpm
ncurses-devel-5.5-24.20060715.i386.rpm	ncurses-devel-5.7-3.20090208.el6.i686.rpm
ksh-20100202-1.el5_6.6.x86_64.rpm	ksh-20100621-12.el6.x86_64.rpm

プロビジョニング サーバ

Red Hat 5.x	Red Hat 6.x
compat-libstdc++-296-2.96-138.i386.rpm	compat-libstdc++-296-2.96-144.el6.i686.rpm
libstdc++-4.1.2-51.el5.i386.rpm	libstdc++-4.4.6-3.el6.i686.rpm
libidn-0.6.5-1.1.i386.rpm	libidn-1.18-2.el6.i686.rpm
libgcc-4.1.2-52.el5.i386.rpm	libgcc-4.4.6-3.el6.i686.rpm

CA IAM コネクタ サーバ

Red Hat 5.x については、CA IAM CS 用のパッケージは不要です。Red Hat 6.x については、以下のパッケージを以下の順番でインストールします。

1. glibc-2.12-1.25.el6.i686.rpm
2. libX11-1.3-2.el6.i686.rpm
3. libxcb-1.5-1.el6.i686.rpm
4. libXtst-1.0.99.2-3.el6.i686.rpm
5. libXau-1.0.5-1.el6.i686.rpm
6. libXi-1.3-3.el6.i686.rpm
7. libXext-1.1-3.el6.i686.rpm
8. nss-softokn-freebl-3.12.9-3.el6.i686.rpm
9. libXmu-1.0.5-1.el6.i686.rpm
10. libXft-2.1.13-4.1.el6.i686.rpm
11. libXpm-3.5.8-2.el6.i686.rpm

Linux および FIPS の場合

有効な FIPS を持つ Linux システムで、十分なエントロピーが利用可能であることを確認します。 CA Identity Manager は、重要な暗号の機能を実行するために /dev/random からのランダム データを必要とします。 /dev/ ランダム内のデータが使い尽くされた場合、CA Identity Manager プロセスはランダム データが利用可能になるのを待つ必要があります。 この待機により、パフォーマンスが低下します。rngd-tools および rng-tools を使用して、/dev/random に十分なデータがあり、読み取りプロセスがブロックされないことを確認してください。

IPv6 のサポート

CA CA Identity Manager は、以下のオペレーティング システムで IPv6 をサポートします。

- Solaris 10
- Windows XP SP2 以上
- Windows 2003 SP2 以上
- Windows 2008 以上

JBoss での IPv6 JDK 要件

IPv6 をサポートする、以下の JDK が必要です。

アプリケーション サーバ	JDK の要件
JBoss （スタンドアロン）	JDK 1.6（JBoss 5 用） JDK 1.7（JBoss 6.1 用）
IPv4/IPv6 スタックを使用する JBoss クラスタ	JDK 1.6（JBoss 5 用） JDK 1.7（JBoss 6.1 用）
JBoss クラスタ	Solaris *専用の* JDK 1.6（JBoss 5.x 用） Solaris *専用の* JDK 1.7（JBoss 6.1.x 用）

IPv6 設定に関する注意事項

IPv6 をサポートする CA Identity Manager 環境を設定する前に、以下の点に注意してください。

- CA Identity Manager で IPv6 アドレスをサポートするには、<idngr> 実装（オペレーティング システム、JDK、ディレクトリ サービス、およびデータベースなど）のすべてのコンポーネントでも IPv6 アドレスがサポートされている必要があります。
- CA CA Identity Manager を SiteMinder と統合する場合、アプリケーション サーバの Web サーバ プラグインも IPv6 をサポートしている必要があります。
- JDBC 接続を使用して、CA Identity Manager から SiteMinder または任意のデータベースに接続する際に、IP アドレスではなく、ホスト名を指定します。
- レポート サーバはデュアル スタック ホストにインストールできます。デュアル スタック ホストは IPv4 と IPv6 の両方をサポートしますが、サーバとの通信は IPv4 で行う必要があります。
- 管理コンソールでレポート サーバへの接続を設定する際に、サーバ名を IPv4 形式にする必要があります。

- CA Identity Manager は IPv6 リンク ローカル アドレスをサポートしません。
- IPv4/6 環境で、複数のアドレス上でリスニングを行うように CA Directory DSA を設定するには、アドレスを DSA ナレッジ ファイルに追加する必要があります。詳細については、CA Directory のマニュアルを参照してください。
- IPv6 を使用する Windows 2008 システムで、IPv4 ループバック アドレスが有効であることを確認します。 そうでない場合は、C++ Connector Server は開始しません。

IPv6 のみでの Windows 2008 上のプロビジョニング ディレクトリがサポートされない

Sun Java システムの制限により、IPv6 ネットワーク サービスがアンインストールされた Windows 2008 サーバ上でのプロビジョニング ディレクトリはサポートされません。

この問題を回避するには、システム上に IPv6 サービスをインストールし、無効にしておきます。

インストール チェックリストを完了します。

CA Identity Manager インストール プログラムは、以前にインストールされたソフトウェアおよびユーザがインストールしようとしているソフトウェアについての情報をユーザに要求します。 インストーラ画面でホスト名（IP アドレスではない）を提供していることを確認します。

注: 以下のインストール ワークシートを使用して、この情報を記録します。インストールを開始する前に、ワークシートに記入することをお勧めします。

プロビジョニング ディレクトリ

CA Identity Manager インストール中に必要な、以下のプロビジョニング ディレクトリおよびプロビジョニング サーバの情報を記録します。

フィールド名	説明	回答
Provisioning Directory Hostname	それがリモートである場合は、プロビジョニング ディレクトリ システムのホスト名。 プライマリおよび任意の代替プロビジョニング ディレクトリのホスト名が必要です。	
共有秘密キー	プロビジョニング ディレクトリの特別のパスワード。 プライマリおよび任意の代替プロビジョニング ディレクトリに対して同じパスワードを使用します。	
Provisioning Server Hostname	プライマリおよび任意の代替プロビジョニング サーバのホスト名。	

JBoss 情報

CA Identity Manager のインストール中に必要な以下の JBoss 情報を記録します。

フィールド名	説明	回答
JBoss フォルダ	アプリケーション サーバのホーム ディレクトリの場所。	
アクセス URL およびポート	以下の事例のいずれかの URL およびポート番号。 ■ 単一ノード インストールの場合は、CA Identity Manager サーバをホストするシステム (アプリケーション サーバをホストするシステム)。 ■ クラスタ インストールの場合は、負荷分散を提供する Web サーバ。	

フィールド名	説明	回答
Java 仮想マシン	JDK 用 Java 実行可能ファイルへのパス	

データベース接続情報

Oracle または Microsoft SQL Server データベース がすでに設定されており動作していることを確認します。 CA Identity Manager インストール時に必要な以下のデータベース情報を記録します。

フィールド名	説明	回答
データベース タイプ	タスク永続性、ワークフロー、監査、レポート、オブジェクト ストレージ、およびタスク永続性アーカイブに対して作成されるデータベースのタイプ（ベンダー/バージョン）。	
Host Name	データベースが存在するシステムのホスト名。 **注**: IP アドレスではなく、ホスト名を指定したことを確認してください。	
Port Number	データベースのポート番号。	
Database Name	データベース識別子。	
Username	データベース アクセス用ユーザ名。 **注**: スキーマを手動でインポートしない場合は、データベースに対する管理者権限が必要です。	
Password	管理者権限を持つユーザ アカウントのパスワード。	

ログイン情報

プロビジョニング コンポーネントのインストール中に必要な以下のパスワードを記録します。

フィールド名	説明	回答
ユーザ名	プロビジョニング コンポーネントにログインするために作成するユーザ名。 この製品をインストールする場合は、ユーザ名に「siteminder」を使用しないでください。 この名前は CA SiteMinder と競合します。	
Provisioning Server password	この Server のパスワード。	
C++ Connector Server password	このサーバについてはパスワードが必要です。 各 C++ Connector Server は一意のパスワードを持つことができます。	
Provisioning Directory password	プロビジョニング サーバがプロビジョニング ディレクトリに接続するために使用するパスワード。 代替プロビジョニング サーバについては、プライマリ プロビジョニング サーバに対して作成されたプロビジョニング ディレクトリのパスワードを入力します。	

SiteMinder 情報

CA Identity Manager を保護するために SiteMinder ポリシー サーバを使用する予定の場合は、以下の情報を記録してください。

フィールド名	説明	回答
Policy Server Host Name	SiteMinder ポリシー サーバのホスト名を指定してください。	

フィールド名	説明	回答
SiteMinder Administrator Name	SiteMinder ポリシー サーバの管理者ユーザ名。	
SiteMinder 管理者パスワード	SiteMinder ポリシー サーバの管理者ユーザのパスワード。	
SiteMinder Folder（Solaris のみ）	SiteMinder ポリシー サーバがインストールされているシステム上の SiteMinder の場所。	
SiteMinder Agent Name	SiteMinder に接続するために CA Identity Manager が使用する SiteMinder エージェントの名前。	
SiteMinder Shared Secret	指定されたエージェント名の共有秘密キー。	

UNIX およびコンソール モードのインストール

このガイドの例では、インストール プログラムの Solaris 実行可能ファイル名を提供します。 ただし、AIX または Linux にインストールする場合があります。

- AIX の場合は、次を使用します。ca-im-*release*-aix.bin
- LINUX の場合は、次を使用します。ca-*release*-linux.bin

release は、CA Identity Manager の現在のリリースを表します

UNIX ワークステーションなどのコンソール モードでインストールを実行している場合は、別のオプションをコマンド ラインに追加します。

- 主なインストールの場合は、-i コンソールを追加します。 以下に例を示します。
  `./ca-im-release-sol.bin -i console`
- プロビジョニング コンポーネントのインストールの場合は、-console をセットアップ コマンドに追加します。

Non-Provisioning インストール

本ガイドでは、プロビジョニング ソフトウェアをインストールするためのオプションを提供するインストーラの Windows および Solaris のプログラム名を参照しています。 プロビジョニング オプションを参照しない場合は、以下のインストーラを使用できます。

- Windows では、IMWithoutProvisioning¥ca-im-Web-*release*-win.bat を使用する
- Solaris では、IMWithoutProvisioning/ca-im-web-*release*-sol.sh を使用する

release は、CA Identity Manager の現在のリリースを表します。

第 3 章: 単一ノードインストール

このセクションには、以下のトピックが含まれています。

インストール ステータス

以下の表では、インストール プロセスにおける現在の手順を示します。

現在の手順	インストール プロセスの手順
	1. あらかじめ必要なハードウェアおよびソフトウェアをインストールし、要件に従ってシステムを設定します。
X	**2. 以下のインストールの 1 つを実行します。** ■ **単一ノードインストール** ■ **アプリケーション サーバ クラスタへのインストール**
	3. （オプション）別個のデータベースを作成します。
	4. （オプション）レポート サーバをインストールします。
	5 （オプション）代替プロビジョニング ディレクトリ、代替プロビジョニング サーバ、およびコネクタ サーバをインストールして、フェイルオーバと負荷分散をサポートします。

CA Identity Manager コンポーネント

単一ノード インストールでは、各コンポーネントの 1 つのコピーをインストールしますが、インストール先に複数のシステムを使用します。

注: 高可用性のためにコンポーネントの複数のコピーをインストールする場合は、クラスタ上のインストールおよび高可用性プロビジョニング インストールについての章を参照してください。

ユーザのサイトで以下の各コンポーネントの 1 つをシステムにインストールします。

- CA Identity Manager サーバ -- 製品の基本的な機能を提供するサーバをインストールします。
- CA Identity Manager 管理ツール -- プロビジョニング マネージャ（Windows システム上で実行される）、CA IAM CS 用の SDK、および Connector Xpress などのツールをインストールします。

  Connector Xpress は動的なコネクタを管理し、それらをエンドポイントにマップし、ルーティング ルールを確立します。 動的なコネクタは、SQL データベースおよび LDAP ディレクトリのプロビジョニングと管理を行えるようにします。
- CA Identity Manager プロビジョニング サーバ -- CA Identity Manager 内のプロビジョニングを有効にします。 このサーバのインストールには、C++ Connector Server が含まれます。 これは、C++ コネクタを使用するエンドポイントを管理します。
- CA IAM CS -- Java コネクタを使用するエンドポイントを管理します。プロビジョニング サーバのインストール時に、CA IAM CS はプロビジョニング サーバと共に登録されます。
- CA Identity Manager プロビジョニング ディレクトリ初期化 -- プロビジョニング データを格納するために CA Directory インスタンスを設定します。CA Directory がインストールされている各システム上でインストール プログラムを使用します。
- SiteMinder の拡張機能 -- CA Identity Manager を保護するために使用している場合は、SiteMinder ポリシー サーバを拡張します。 CA Identity Manager サーバをインストールする前に、ポリシー サーバと同じシステムにこれらの拡張機能をインストールします。

単一ノード インストールを実行する方法

以下のチェックリストを使用して CA Identity Manager の基本インストールを実行します。

✓	手順
	1. CA Identity Manager を必要なシステムにインストールします。
	2. 必要な場合は、IPv6 のサポートを設定します。
	3. CA Identity Manager サーバが起動することを確認します。
	4. リモート システムにインストールした場合は、プロビジョニング マネージャを設定します。
	5. オプションのプロビジョニング コンポーネントをインストールします。

CA Identity Manager コンポーネントのインストール

運用環境の場合は、データ サーバには別個のシステムを使用します。 たとえば、プロビジョニング ディレクトリおよびデータベース（SQL または Oracle）は、CA Identity Manager サーバ およびプロビジョニング サーバとは別のシステムにインストールすることを推奨します。SiteMinder をインストールする場合も、別個のシステムにインストールできます。管理ツールは、任意のシステムにインストールできます。

CA Identity Manager インストーラを使用して、必要なシステムでインストールを実行してください。 下記のインストーラ実行手順では、インストール メディアの最上位フォルダにある以下のプログラムを参照します。

- **Windows の場合：**
  `ca-im-release-win32.exe`
- **UNIX の場合：**
  `ca-im-release-sol.bin`

release は、CA Identity Manager の現在のリリースです。

インストールするコンポーネントごとに、ホスト名やパスワードなど、インストーラ画面で必要となる情報 (P. 39)を確認しておいてください。インストール中に問題が発生した場合は、インストール ログ (P. 187)を検証してください。

SiteMinder の拡張をインストールする方法

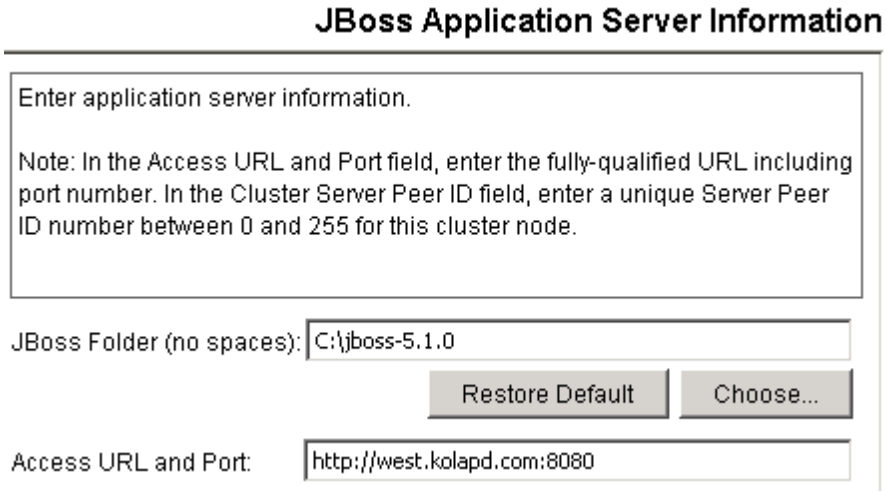
1. ローカル管理者（Windows の場合）またはルート（Solaris の場合）として、SiteMinder が インストールされているシステムにログインします。
2. SiteMinder サービスを停止します。
3. インストーラを実行し、［Extensions for SiteMinder］を選択します。

CA Identity Manager サーバをインストールする方法

1. SiteMinder を別個のシステムにインストールした場合は、SiteMinder の拡張もそれと同じシステムにインストールします。
2. ローカル管理者（Windows の場合）またはルート（Solaris の場合）として、アプリケーション サーバがインストールされているシステムにログインします。
3. アプリケーション サーバを停止します。

4. インストーラを実行し、［CA Identity Manager Server］を選択します。

   必ず JBoss の設定と一致するポート番号を指定してください。 デフォルトでは、ポート 1099 および 8080 が使用されます。 ただし、システム上の他のアプリケーションがこれらのポートを使用すると、競合が発生します。 たとえば、Oracle は、デフォルトではポート 8080 で XDB サービスを開始します。 その場合は、別のポートを使用するように JBoss またはもう一方のアプリケーションを設定してください。



5. SiteMinder がローカル システムにある場合は、［Extensions for SiteMinder］を選択します。 SiteMinder がリモート システムにある場合は、［Existing SiteMinder Policy Server］を選択します。

プロビジョニング ディレクトリをインストールする方法

1. ローカル管理者（Windows の場合）またはルート（Solaris の場合）としてシステムにログインします。
2. システムに CA Directory がすでにインストールされていることを確認します。

3. インストーラを実行して、CA Identity Manager Provisioning Directory Initialization］を選択します。
   展開サイズに関する質問に答えます。
4. 将来の成長の余地を残しながら、以下のガイドラインに従います。
   - コンパクト -- 10,000 までのアカウント
   - 基本 -- 400,000 までのアカウント
   - 中規模 -- 600,000 までのアカウント
   - 大規模 -- 600,000 を超えるアカウント

   注: 既存の CA Identity Manager インストールにプロビジョニング ディレクトリをインストールする場合は、必ず展開サイズを十分に取ってください。さもないと、データ ファイルにロードされる際にデータがフィットしないので、エラーが発生します。

プロビジョニング サーバをインストールする方法

1. ローカル管理者（Windows の場合）またはルート（Solaris の場合）としてシステムにログインします。
2. CA Directory がすでにインストールされており、リモートのプロビジョニング ディレクトリ の詳細情報があることを確認します。
3. インストーラを実行し、［CA Identity Manager Provisioning Server］を選択します。

IPv6 サポートの設定

IPv6 をサポートする JBoss システム上にインストールする場合は、いくつかの設定を行う必要があります。

次の手順に従ってください:

1. *jboss_installation*¥bin にある run.bat/sh ファイルまたは standalone.bat/shh を開きます。
2. IDM_OPTS エントリの以下の*いずれか*のプロパティをコメント解除します。
   - IPv6/IPv4 のみのシステムでは、以下のエントリをコメント解除します。
     `#IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv6Addresses=true"`
   - IPv6/IPv4 システムでは、以下のエントリをコメント解除します。
     `#IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv4Stack=true"`

     注: これらは UNIX 用に表示されるプロパティですが、Windows でも同じプロパティが REM の後で表示されます。
3. ファイルを保存します。

CA Identity Manager サーバのインストールの確認

CA Identity Manager を起動するには、JBoss 5.x の run.bat/sh ファイルまたは JBoss 6.1 EAP の standalone.bat/sh ファイルを使用します。 このファイルは、JBoss がインストールされている bin ディレクトリにあります。

次の手順に従ってください:

1. CA Identity Manager サーバによって使用されるデータベースを起動します。
2. 以下のように CA Identity Manager サーバを起動します。
   - **Windows の場合：** ［スタート］-［すべてのプログラム］-［CA］-［Identity Manager］-［Start Identity Manager Server］に移動します。
   - **UNIX の場合：** *jboss_home*/bin ディレクトリから、以下のコマンドを入力します。
     ```
     ./run.sh
     ```
3. サーバが起動するまで待機します。 以下のメッセージがコンソール ウィンドウに表示されます。

   ```
   DATE+TIME INFO  [com.sun.jersey.server.impl.application.WebApplicationImpl]
   (main) Initiating Jersey application, version 'Jersey: 1.1.5.1 DATE+TIME'
   ```
4. 管理コンソールにアクセスし、以下のポイントを確認します。
   - ブラウザから以下の URL にアクセスできます。

     http://*im_server*:*port*/iam/immanage

     以下に例を示します。

     http://MyServer.MyCompany.com:*port-number*/iam/immanage
   - 管理コンソールが開きます。
   - アプリケーション サーバ ログにエラーが表示されません。
   - ディレクトリ リンクをクリックした場合、ユーザはエラー メッセージを受信しません。
5. 以下の URL 形式を使用して、アップグレードされた環境にアクセスできることを確認してください。

リモート プロビジョニング マネージャの設定

プロビジョニング マネージャをプロビジョニング サーバから別のシステムにインストールした場合、サーバへの通信を設定します。

注: プロビジョニング マネージャをインストールするには、CA Identity Manager 管理ツールを Windows システムにインストールします。

次の手順に従ってください:

1. プロビジョニング マネージャをインストールした Windows システムにログインします。
2. ［スタート］-［プログラム］-［CA］-［Identity Manager］-［Provisioning Manager Setup］に移動します。
3. プロビジョニング サーバのホスト名を入力します。
4. ［構成］をクリックします。
5. 代替プロビジョニング サーバについては、プルダウン リストからドメイン名を選択します。
6. ［OK］をクリックします。

   これでプロビジョニング マネージャを起動し、設定したドメイン名を参照できるようになります。

オプション プロビジョニング コンポーネントのインストール

CA Identity Manager のオプションのプロビジョニング コンポーネントは、im-pc-*release*.zip にあります。

release は、CA Identity Manager の現在のリリースを表します。

ZIP ファイルの内容は、以下のとおりです。

リモート エージェント

これらのコンポーネントをインストールするには、プロビジョニング コンポーネントメディア（¥RemoteAgent の下）から固有のエージェント インストーラを実行します。IPv6 サポートを望む場合は、ユーザのエージェントをインストールする必要があります。

パスワード同期エージェント

このコンポーネントをインストールするには、プロビジョニング コンポーネント メディア（¥Agent 下）からパスワード同期エージェント インストーラを実行します。

クレデンシャル プロバイダ

このコンポーネントをインストールするのは、プロビジョニング コンポーネント メディア（¥Agent 下）からクレデンシャル プロバイダ インストーラを実行します。

Bulk Loader クライアント/PeopleSoft フィード

このコンポーネントをインストールするには、プロビジョニング コンポーネント メディア（¥Clients 下）から Bulk Loader Client インストーラを実行します。

CA IAM Server 2000 SDK

このコンポーネントをインストールするには、CA Identity Manager メディア（¥Provisioning 下）から CA IAM コネクタ サーバ SDK インストーラを実行します。

CCI スタンドアロン

このコンポーネントをインストールするには、プロビジョニング コンポーネント メディア（¥Infrastructure の下）から CCI スタンドアロン インストーラを実行します。

CA Identity Manager インストーラは、デフォルトではすべてのコネクタをインストールします。 ただし、管理しているエンドポイント システムにエージェントをインストールしないと、関連のコネクタを使用できない場合があります。

コネクタはプロビジョニング サーバ上で実行されて、エンドポイントによって管理されているシステムと通信します。 たとえば、プロビジョニング サーバに ADS コネクタがインストールされた場合にのみ、Active Directory Services （ADS）を実行するシステムを管理できます。

注: 各コネクタの詳細については、「コネクタ ガイド」を参照してください。

これらのコンポーネントの詳細については以下のガイドを参照してください。

- クレデンシャル プロバイダ（*管理ガイド*）
- パスワード同期エージェント（*管理ガイド*）
- Connector Xpress （*Connector Xpress ガイド*）
- コネクタで使用するエージェント（*コネクタ ガイド*）

第 4 章: JBoss クラスタでのインストール

このセクションには、以下のトピックが含まれています。

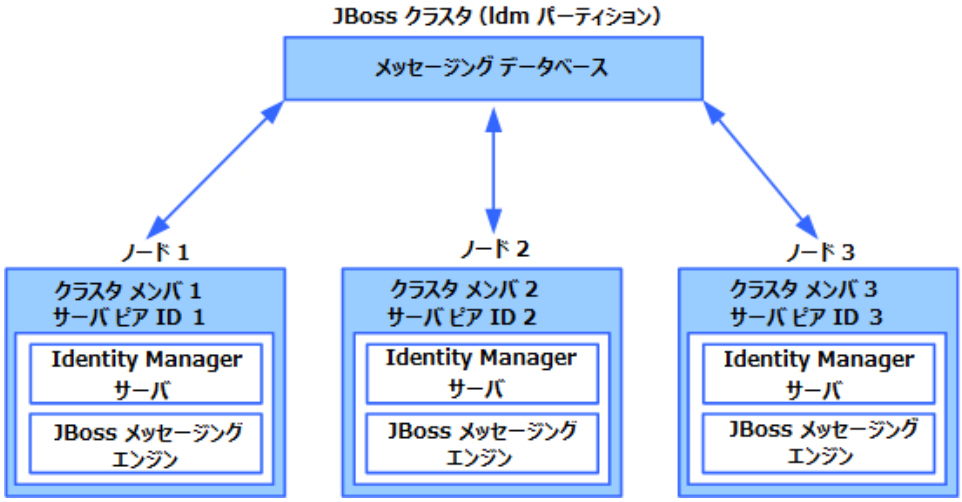
JBoss クラスタでのサンプル インストール

以下のトピックでは、CA Identity Manager 12.6.5 によってサポートされる JBoss クラスタ アーキテクチャについて説明します。

JBoss 5 クラスタ上の CA Identity Manager

JBoss クラスタ化を設定する際に、ユーザはマスタ ノードを作成します。このノードは、通常、クラスタで最初に起動するノードです。 その他のノードは、起動すると、マスタ ノードから展開ファイルを受信します。マスタ ノードに障害が発生すると、別のノードが新しいマスタ ノードになります。

以下の JBoss 5 の図は、ノードとクラスタ メンバの関係を示しています。各ノードには、1 つのクラスタ メンバが含まれます。クラスタの各メンバには一意のサーバ ピア ID があります。マスタ ノードは、最初に作成されたと想定すると、クラスタ メンバ 1 になります。



この図では、メッセージング データベースはクラスタ メンバがメッセージを共有するためのセントラル ストアです。また、ノードには、それぞれ 以下の 3 つのコンポーネントが含まれます。

CA Identity Manager サーバ

製品のコア機能を提供します。

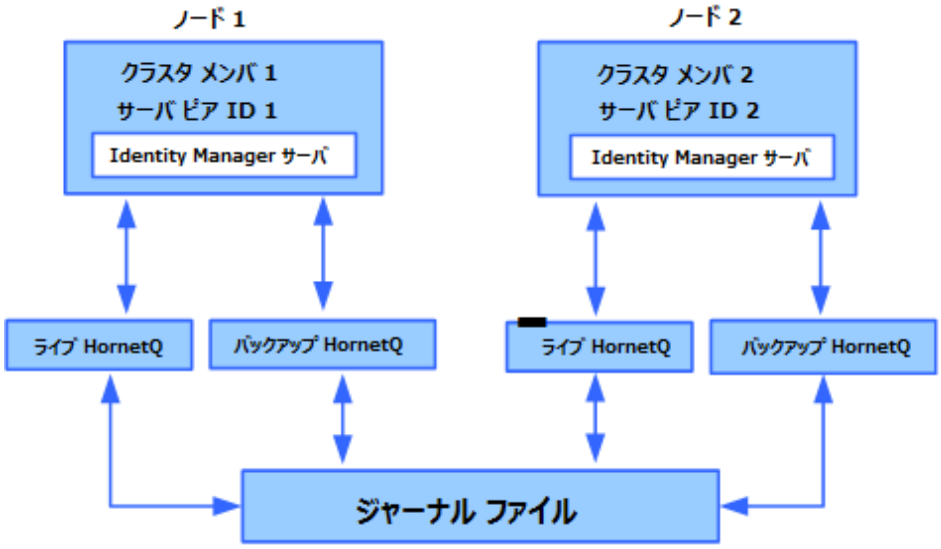
JBoss メッセージ エンジン

JMS を使用して、クラスタのメンバ用のメッセージ機能を提供します。

JBoss 6.1 クラスタ上の CA Identity Manager

JBoss Enterprise Application Platform（EAP）6.1 では、CA Identity Manager は、ノード間の通信にユニキャストまたはマルチキャストのいずれかの方式を使用するクラスタをサポートします。 いずれかのタイプのクラスタで、マスタ ノードを作成します。マスタ ノードは、通常、クラスタ内で最初に起動するノードです。 その他のノードは、起動すると、マスタ ノードから展開ファイルを受信します。 マスタ ノードに障害が発生すると、別のノードが新しいマスタ ノードになります。

たとえば、2 ノードのクラスタがあるとします。 以下の図は、ノードとクラスタ メンバの関係を示しています。 各ノードには、1 つのクラスタ メンバが含まれます。 クラスタの各メンバには一意のサーバ ピア ID があります。 マスタ ノードは、最初に作成されたと想定すると、クラスタ メンバ 1 になります。



この図には、以下のコンポーネントがあります。

CA Identity Manager サーバ

製品のコア機能を提供します。

HornetQ のライブおよびバックアップ インスタンス

クラスタ メンバにメッセージ機能を提供します。 各ノードで、2 つの HornetQ インスタンス（ライブ インスタンスとバックアップ インスタンス）を設定します。

ジャーナル ファイル

データベースを使用せずにジャーナル ファイルによって HornetQ メッセージを永続化させます。ジャーナル ファイルを格納するように各 HornetQ インスタンスを設定します。 この例では、すべてのノードが、ストレージ エリア ネットワーク （SAN）サーバ上にある一連のジャーナル ファイルを共有しています。 このシナリオは、「共有ストア」と呼ばれます。

インストール時に共有ストアではなくレプリケーションを選択すると、ジャーナル ファイルは各ノードに格納されます。

インストール ステータス

以下の表では、インストール プロセスにおける現在の手順を示します。

現在の手順	インストール プロセスの手順
	1. あらかじめ必要なハードウェアおよびソフトウェアをインストールし、要件に従ってシステムを設定します。
X	**2. 以下のインストールの 1 つを実行します。** ■ **単一ノードインストール** ■ **アプリケーション サーバ クラスタへのインストール**
	3. （オプション）別個のデータベースを作成します。
	4. （オプション） レポート サーバをインストールします。
	5. （オプション）代替のプロビジョニング ディレクトリ、代替のプロビジョニング サーバ、およびコネクタ サーバをインストールして、フェイルオーバと負荷分散をサポートします。

ユニキャストまたはマルチキャストの使用の決定

CA Identity Manager を JBoss 6.1 EAP にインストールする場合、メッセージ機能プロトコルとしてユニキャストまたはマルチキャストのいずれかを使用できます。 このプロトコルは、クラスタ内のノード間の通信手段です。 組織で最良な選択を行うために、両方のオプションをテストすることをお勧めします。

以下のような場合には、ユニキャストの使用を検討します。

- JBoss クラスタ内のサーバが異なるサブネット上にある（この状況は、一般に、JBoss クラスタを仮想マシン上にインストールする場合に発生します）。
- ネットワーク輻輳が懸念される（ユニキャストは、クラスタ ノード間で送信されるパケット数の削減に役立ちます）。

以下のような場合には、マルチキャストの使用を検討します。

- 単一ネットワーク上に JBoss をデフォルト展開する。
- クラスタ用に JBoss 5 を必要としている。

JBoss 5 クラスタへのインストール

以下の手順では、複数の JBoss アプリケーション サーバをサーバごとに同じ CA Identity Manager アプリケーションを含むように設定する方法について説明します。 このタイプのクラスタでは、各 JBoss アプリケーション サーバは、他のアプリケーション サーバと無関係に動作します。ただし、それらのサーバは JMS メッセージによってロードを共有します。

✓	手順
	1. デフォルト マルチキャスト アドレスをテストします。
	2. マスタ ノードを作成します。
	3. クラスタ ノードを追加します。
	4. JK コネクタを設定します。

デフォルト マルチキャスト アドレスのテスト

以下の手順で、デフォルト マルチキャスト アドレスを使用できるかどうかをテストします。 実行スクリプトではマルチキャスト アドレスを使用します。このアドレスは、デフォルト アドレスか、ネットワーク管理者によって提供された代替アドレスのいずれかです。

テストの最初の部分は成功しても、後の部分は失敗する可能性があります。そのため、インストールのマルチキャストの信頼性を確認するために、さまざまな角度から完全なテストを実行してください。

次の手順に従ってください:

1. JBoss と JDK をコンピュータにインストールします。
2. 最初のノードで、以下のように送信プログラムを実行します。
   a. lib フォルダに移動します。
      - JBoss 5 ノードでは、jboss-home-1/server/all/lib に移動します。
      - JBoss 6.1 ノードでは、jboss-eap-6.1¥modules¥system¥layers¥base¥org¥jgroups¥main に移動します
   b. 以下のコマンドを実行します。

      java -cp jgroups-3.2.7.Final-redhat-1.jar org.jgroups.tests.McastSenderTest -mcast_addr 224.10.10.10 -port 5555
3. クラスタ内の他のノードで、以下のように受信プログラムを実行します。
   a. lib フォルダに移動します。
      - JBoss 5 ノードでは、jboss-home-1/server/all/lib に移動します。
      - JBoss 6.1 ノードでは、jboss-eap-6.1¥modules¥system¥layers¥base¥org¥jgroups¥main に移動します
   b. 以下のコマンドを実行します。

      java -cp jgroups-3.2.7.Final-redhat-1.jar org.jgroups.tests.McastReceiverTest -mcast_addr 224.10.10.10 -port 5555

4. 最初のノードから、以下のようにメッセージを送信します。
   a. 最初のノードのコンソールで、任意のテキストを入力し、Enter キーを押します。
   b. テキストの送信を確認する応答が表示されることを確認します。
   c. そのメッセージがクラスタ内の他のすべてのノードのコンソールに表示されることを確認します。
   d. 送信または受信のテストが失敗した場合は、ネットワーク管理者に有効なマルチキャスト アドレスを提供するように要求し、このテストを繰り返します。

JBoss 5 用のマスタ ノードの作成

マスタ ノード（クラスタ内の最初のノード）を作成することによって、JBoss 5 クラスタの作成を開始します。

次の手順に従ってください:

1. JBoss と JDK をコンピュータにインストールします。
2. CA Identity Manager インストール プログラムを起動します。
   - Windows： ユーザのインストール メディアから、以下のプログラムを実行します。

     `ca-im-release-win32.exe`
   - UNIX： ユーザのインストール メディアから、インストール プログラムを実行します。たとえば、Solaris の場合は以下のとおりです。

     `ca-im-release-sol.bin`

   release は、CA Identity Manager の現在のリリースを表します。

   重要: ユーザ名、ホスト名、ポートなどインストーラによって必要とされる情報を収集したことを確認してください。

3. 以前のリリースの CA Identity Manager と同じ値を入力することにより、データベース クレデンシャルを必要とするセクションを完了します。

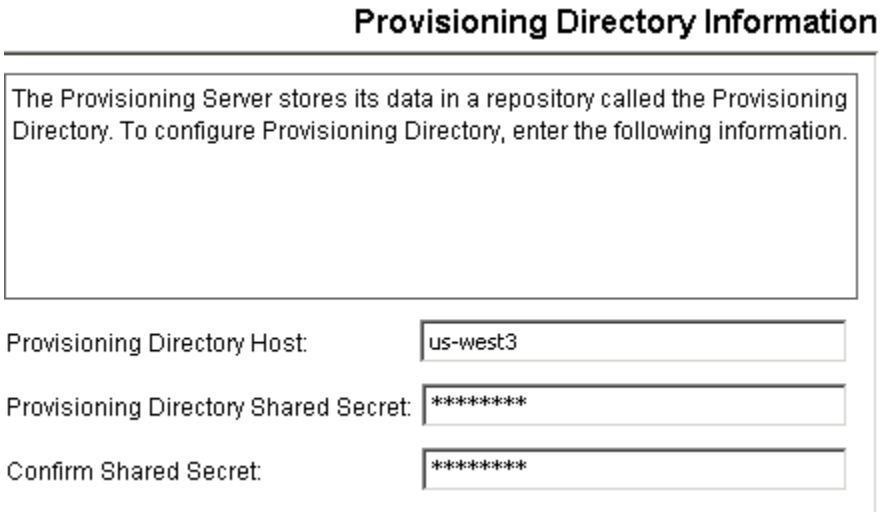
   CA Identity Manager r12 から使用しはじめた場合、タスク永続性、ワークフロー、監査、およびレポート用に異なるデータベース ストアを使用しているときは、インストール後に、個別のストアを指すようにデータ ソースを手動で更新してください。

   注: インストール時に、ワークフロー データベースをアップグレードして、タスク永続性データを移行するオプションを参照する場合は、それらのオプションを有効にします。

4. CA Identity Manager サーバなど、このシステムに必要なあらゆるコンポーネントを組み込むことにより、［Select Components］セクションを完了します。

5. インストールの要件に基づいてその他のセクションを完了します。

6. インストール中にパスワードまたは共有秘密を入力する際には、必要なときに思い出せるパスワードを指定してください。



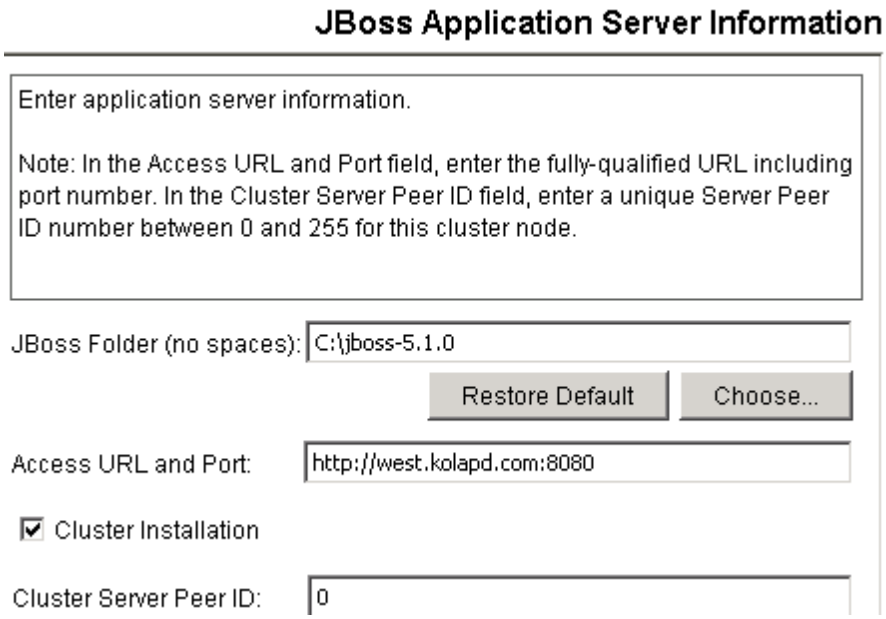
7. 以下のように、［JBoss Application Server Information］ページを完了します。

   a. 負荷分散用 Web サーバの URL とポート番号を使用して、アクセス サーバの URL とポート番号を入力します。

   b. ［Cluster Installation］を選択します。

   c. ピア ID （0 ～ 255 の一意の数字）を入力します。 そのピア ID を記録し、他のノードには別の数字を使用します。

数式 1: ユーザが JBoss 情報を入力します。



8. マルチキャスト アドレス テストが失敗した場合は、次の 2 つの手順（Windows 用または Solaris 用）のいずれかを実行します。
9. Windows システムでは、*jboss_home*¥bin ディレクトリにある run.bat を編集します。
   a. 次のように始まる行を見つけます。
      ```
      ARGS="${ARGS}
      ```
   b. 次のように -u 引数を先頭に付けたマルチキャスト アドレスを追加します。
      ```
      ARGS="${ARGS} -g IdmPartition -Djboss.messaging.ServerPeerID=PeerID -u multicast-address"
      ```
   c. IPv6/IPv4 をサポートするシステムにインストールする場合は、IDM_OPTS エントリをコメント解除します。
      ```
      set IDM_OPTS=%IDM_OPTS% -Djava.net.preferIPv4Stack=true
      ```
10. Solaris システムでは、*jboss_home*¥bin ディレクトリにある run.sh を編集します。
    a. 次のように始まる行を見つけます。
       ```
       ARGS="${ARGS}
       ```
    b. 次のように -u 引数を先頭に付けたマルチキャスト アドレスを追加します。
       ```
       ARGS="${ARGS} -g IdmPartition -Djboss.messaging.ServerPeerID=PeerID -u multicast-address"
       ```

c. IPv6 をサポートするシステムにインストールする場合は、以下の IDM_OPTS エントリのプロパティの 1 つを変更します。

- IPv6/IPv4 のみのシステムでは、以下のエントリをコメント解除します。

```
IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv6Addresses=true"
```

- IPv6/IPv4 システムでは、以下のエントリをコメント解除します。

```
IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv4Stack=true"
```

インストール中に問題が発生した場合は、インストール ログ (P. 187)を調べます。

JBoss 5 用のクラスタ ノードの追加

各クラスタ ノードは別個のシステムにインストールすることを推奨します。ただし、すべてのノードを 1 つのシステムにインストールする場合は、各ノードに個別の jboss_home が必要です。 この予防措置は、*jboss_home*/bin ディレクトリ内で workpoint.log に関する競合を回避するために必要です。

次の手順に従ってください:

1. JBoss と JDK をコンピュータにインストールします。
2. そのシステムに CA Identity Manager サーバをインストールします。
   - Windows： ユーザのインストール メディアから、以下のプログラムを実行します。
     `ca-im-release-win32.exe`
   - UNIX： ユーザのインストール メディアから、以下のプログラムを実行します。
     `ca-im-release-sol.bin`

   release は、CA Identity Manager の現在のリリースを表します。
3. FIPS、SiteMinder、データベース、および共有秘密の詳細に関して同じ値を指定し、その他のマスタ ノード用に入力されたすべての値を必ず指定してください。
4. ［Cluster Installation］を選択します。
5. 作成した他のノードとは異なる ピア ID を入力します。
6. マルチキャスト アドレス テストが失敗した場合は、run.bat または run.sh ファイルにある MULTI_CAST_ADDRESS の値を編集します。 一意のマルチキャスト アドレスを入力してください。
7. IPv6 をサポートするシステムにインストールする場合は、以下に示す、standalone.bat または standalone.sh ファイルの IDM_OPTS エントリのプロパティの 1 つを変更します。
   - Solaris 上の IPv6 のみのシステムでは、以下のエントリをコメント解除します。
     `IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv6Addresses=true"`
   - IPv6/IPv4 システムでは、以下のエントリをコメント解除します。
     `IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv4Stack=true"`

インストール中に問題が発生した場合は、インストール ログ (P. 187)を調べます。

JBoss 6.1 クラスタへのインストール

以下の手順では、複数の JBoss アプリケーション サーバをサーバごとに同じ CA Identity Manager アプリケーションを含むように設定する方法について説明します。 このタイプのクラスタでは、各 JBoss アプリケーション サーバは、他のアプリケーション サーバと無関係に動作します。ただし、それらのサーバは JMS メッセージによってロードを共有します。

✓	手順
	1. ユニキャストを使用する予定かマルチキャストを使用する予定かを決定します。
	2. デフォルト マルチキャスト アドレスをテストします (マルチキャストを使用する予定の場合) 。
	3. マスタ ノードを作成します。
	4. クラスタ ノードを追加します。
	5. ジャーナル ファイルを設定します。
	6. JK コネクタを設定します。

デフォルト マルチキャスト アドレスのテスト

以下の手順で、デフォルト マルチキャスト アドレスを使用できるかどうかをテストします。 実行スクリプトではマルチキャスト アドレスを使用します。このアドレスは、デフォルト アドレスか、ネットワーク管理者によって提供された代替アドレスのいずれかです。

テストの最初の部分は成功しても、後の部分は失敗する可能性があります。そのため、インストールのマルチキャストの信頼性を確認するために、さまざまな角度から完全なテストを実行してください。

次の手順に従ってください:

1. JBoss と JDK をコンピュータにインストールします。

2. 最初のノードで、以下のように送信プログラムを実行します。
   a. lib フォルダに移動します。
      - JBoss 5 ノードでは、jboss-home-1/server/all/lib に移動します。
      - JBoss 6.1 ノードでは、jboss-eap-6.1¥modules¥system¥layers¥base¥org¥jgroups¥main に移動します
   b. 以下のコマンドを実行します。

      java -cp jgroups-3.2.7.Final-redhat-1.jar org.jgroups.tests.McastSenderTest -mcast_addr 224.10.10.10 -port 5555
3. クラスタ内の他のノードで、以下のように受信プログラムを実行します。
   a. lib フォルダに移動します。
      - JBoss 5 ノードでは、jboss-home-1/server/all/lib に移動します。
      - JBoss 6.1 ノードでは、jboss-eap-6.1¥modules¥system¥layers¥base¥org¥jgroups¥main に移動します
   b. 以下のコマンドを実行します。

      java -cp jgroups-3.2.7.Final-redhat-1.jar org.jgroups.tests.McastReceiverTest -mcast_addr 224.10.10.10 -port 5555
4. 最初のノードから、以下のようにメッセージを送信します。
   a. 最初のノードのコンソールで、任意のテキストを入力し、Enter キーを押します。
   b. テキストの送信を確認する応答が表示されることを確認します。
   c. そのメッセージがクラスタ内の他のすべてのノードのコンソールに表示されることを確認します。
   d. 送信または受信のテストが失敗した場合は、ネットワーク管理者に有効なマルチキャスト アドレスを提供するように要求し、このテストを繰り返します。

JBoss 6.1 用のマスタ ノードの作成

マスタ ノード（クラスタ内の最初のノード）を作成することによって、JBoss 6.1 クラスタの作成を開始します。

次の手順に従ってください:

1. JBoss と JDK をコンピュータにインストールします。
2. CA Identity Manager インストール プログラムを起動します。
   - Windows： ユーザのインストール メディアから、以下のプログラムを実行します。
     `ca-im-release-win32.exe`
   - UNIX： ユーザのインストール メディアから、インストール プログラムを実行します。たとえば、Solaris の場合は以下のとおりです。
     `ca-im-release-sol.bin`

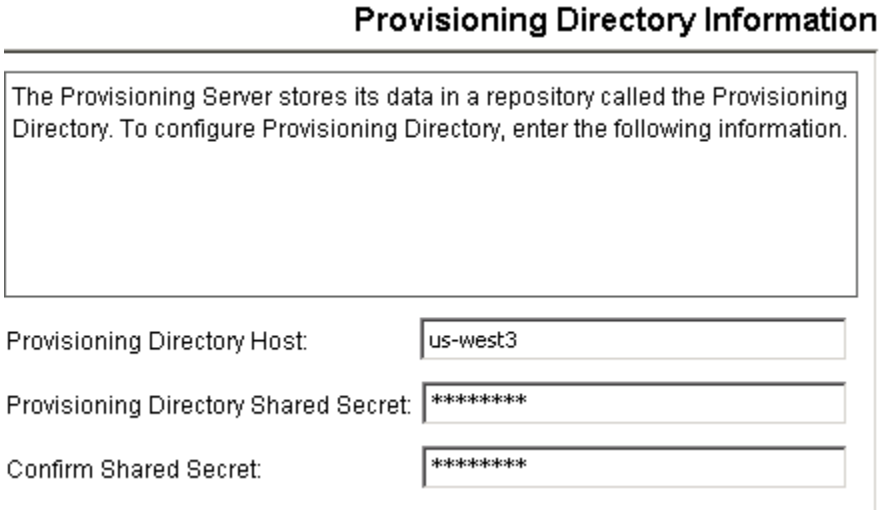
   release は、CA Identity Manager の現在のリリースを表します。

   重要: ユーザ名、ホスト名、ポートなどインストーラによって必要とされる情報を収集したことを確認してください。
3. 以前のリリースの CA Identity Manager と同じ値を入力することにより、データベース クレデンシャルを必要とするセクションを完了します。

   CA Identity Manager r12 から使用しはじめた場合、タスク永続性、ワークフロー、監査、およびレポート用に異なるデータベース ストアを使用しているときは、インストール後に、個別のストアを指すようにデータ ソースを手動で更新してください。

   注: インストール時に、ワークフロー データベースをアップグレードして、タスク永続性データを移行するオプションを参照する場合は、それらのオプションを有効にします。

4. CA Identity Manager サーバおよびユーザに必要な他のコンポーネントをこのシステムに含めることにより、コンポーネントの選択セクションを完了させます。
5. インストールの要件に基づいて他のセクションを完了させます。
6. インストールでパスワードまたは共有秘密キーを入力するときは、必要なときに思い出すことができるパスワードを確実に入力してください。



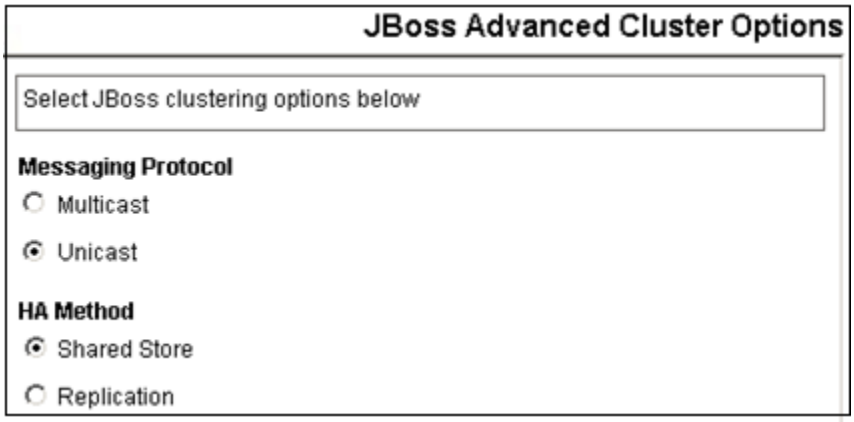
7. 以下のように、［JBoss Application Server Information］ページへの入力を完了します。
   a. 負荷分散用 Web サーバの URL とポート番号を使用して、アクセスサーバの URL とポート番号を入力します。
   b. ［Cluster Installation］を選択します。
   c. ピア ID （0 ～ 255 の一意の数字）を入力します。 そのピア ID を記録し、他のノードには別の数字を使用します。

8. クラスタの詳細オプションを選択します。
   - メッセージ機能プロトコルとしてマルチキャストまたはユニキャストを選択します。
   - 高可用性に関して共有ストアまたはレプリケーションを選択します。

     共有ストアには、ジャーナル ファイルを格納するためのストレージ エリア ネットワーク（SAN）サーバが必要です。

     レプリケーションでは、ジャーナル ファイルが各ノードに格納されます。

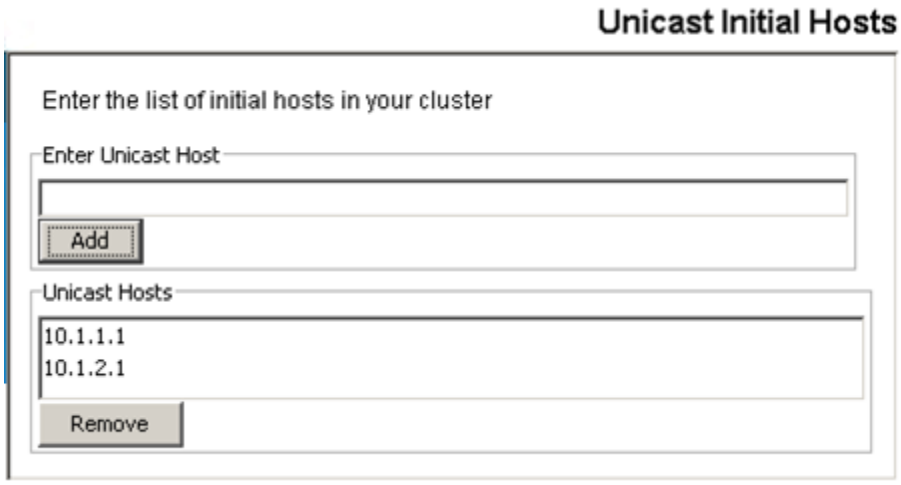
図 1: 詳細設定オプションの選択



9. マルチキャストを選択した場合は、次の手順にスキップします。

   JBoss がインストールされているシステムのユニキャスト初期ホストのリストを提供します。

図 2: JBoss クラスタ内の初期ホストの追加



10. ユニキャストを選択した場合は、次の手順にスキップします。

    マルチキャスト アドレス テストが失敗した場合は、standalone.bat または standalone.sh ファイルにある MULTI_CAST_ADDRESS の値を編集します。 一意のマルチキャスト アドレスを入力してください。

11. IPv6 をサポートするシステムにインストールする場合は、以下に示す、standalone.bat または standalone.sh ファイルの IDM_OPTS エントリのプロパティの 1 つを変更します。

    - Solaris 上の IPv6 のみのシステムでは、以下のエントリをコメント解除します。

      ```
      IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv6Addresses=true"
      ```

    - IPv6/IPv4 システムでは、以下のエントリをコメント解除します。

      ```
      IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv4Stack=true"
      ```

12. インストール中に問題が発生した場合は、インストール ログ (P. 187) を調べます。

JBoss 6.1 用のクラスタ ノードの追加

各クラスタ ノードは別個のシステムにインストールすることを推奨します。ただし、すべてのノードを 1 つのシステムにインストールする場合は、各ノードに個別の jboss_home が必要です。 この予防措置は、*jboss_home*/bin ディレクトリ内で workpoint.log に関する競合を回避するために必要です。

次の手順に従ってください:

1. JBoss と JDK をコンピュータにインストールします。
2. そのシステムに CA Identity Manager サーバをインストールします。
   - Windows： ユーザのインストール メディアから、以下のプログラムを実行します。
     `ca-im-release-win32.exe`
   - UNIX： ユーザのインストール メディアから、以下のプログラムを実行します。
     `ca-im-release-sol.bin`

   release は、CA Identity Manager の現在のリリースを表します。
3. FIPS、SiteMinder、データベース、および共有秘密の詳細に関して同じ値を指定し、その他のマスタ ノード用に入力されたすべての値を必ず指定してください。
4. ［Cluster Installation］を選択します。
5. 作成した他のノードとは異なる ピア ID を入力します。
6. クラスタの詳細オプションを選択します。マスタ ノードの手順で選択したものを選択してください。
7. マルチキャストを選択した場合は、次の手順にスキップします。

   マスタ ノードに提供したものと同じユニキャスト初期ホストのリストを確認します。
8. ユニキャストを選択した場合は、次の手順にスキップします。

   マルチキャスト アドレス テストが失敗した場合は、standalone.bat または standalone.sh ファイルにある MULTI_CAST_ADDRESS の値を編集します。 一意のマルチキャスト アドレスを入力してください。

9. IPv6 をサポートするシステムにインストールする場合は、以下に示す、standalone.bat または standalone.sh ファイルの IDM_OPTS エントリのプロパティの 1 つを変更します。
   - Solaris 上の IPv6 のみのシステムでは、以下のエントリをコメント解除します。
     ```
     IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv6Addresses=true"
     ```
   - IPv6/IPv4 システムでは、以下のエントリをコメント解除します。
     ```
     IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv4Stack=true"
     ```

インストール中に問題が発生した場合は、インストール ログ (P. 187)を調べます。

ジャーナル ファイルの設定

JBoss 6.1 EAP に高可用性を実装するために、CA Identity Manager は、HornetQ メッセージ プロバイダを使用します。 HornetQ は、データベースを使用せずにジャーナル ファイルによってメッセージを永続化させます。CA Identity Manager は、以下のインストールの選択に基づいてジャーナル ファイルを格納します。

- レプリケーション方式 -- CA Identity Manager は、各ノードにジャーナル ファイルを格納します。
- 共有ストア -- CA Identity Manager は、ストレージ エリア ネットワーク（SAN）サーバにジャーナル ファイルを格納します。

レプリケーション用のジャーナル ファイル

インストール時にレプリケーションを選択した場合は、インストール プログラムによって、2 つの HornetQ インスタンス（ライブ インスタンスおよびバックアップ）を使用して最初のノードが設定されています。 各追加ノードで、ライブとバックアップの HornetQ インスタンスを設定してください。

次の手順に従ってください:

1. クラスタの 2 番目のノードで、以下の場所に移動します。
   ```
   jboss_home/standalone/configuration
   ```
2. standalone-full-ha.xml ファイルを編集します。

3. 「*node1*」をすべて「*node2*」に置き換えます。
4. 「*node2*」をすべて「*node1*」に置き換えます。
5. 3 ノード以上のクラスタについては、同様の方法で standalone-full-ha.xml を編集します。

   たとえば、3 ノード クラスタに関して以下の変更を加えます。

   - ノード 1
     - ライブ HornetQ は、バックアップ グループ「*node1*」のメンバです。
     - バックアップ HornetQ は、バックアップ グループ「*node2*」のメンバです。
   - ノード 2
     - ライブ HornetQ は、バックアップ グループ「*node2*」のメンバです。
     - バックアップ HornetQ は、バックアップ グループ「*node3*」のメンバです。
   - ノード 3
     - ライブ HornetQ は、バックアップ グループ「*node3*」のメンバです。
     - バックアップ HornetQ は、バックアップ グループ「*node1*」のメンバです。

共有ストア用のジャーナル ファイル

インストール時に共有ストアを選択した場合は、各ノードで 2 つの HornetQ インスタンス（ライブ インスタンスおよびバックアップ）を設定します。 ジャーナル ファイルをストレージ エリア ネットワーク（SAN）サーバに格納するように各インスタンスを設定します。

次の手順に従ってください:

1. 各ノードへのパスを使用して SAN サーバを作成します。

   たとえば、2 ノード クラスタの場合は、*//network-path/node1* と *//network-path/node2* のパスを使用して SAN サーバを設定します。

2. 最初のノードで、以下の場所に移動します。
   jboss_home/standalone/configuration
3. standalone-full-ha.xml ファイルを編集します。
4. ファイルの <hornetq-server> セクションを見つけます。
5. セクションをコメント解除し、正しいディレクトリのパスを設定します。

```
<!-- un mark this for node 1 and set your path until node1jr
<paging-directory path="//network/path/node1jr/paging"/>
   <bindings-directory path="//network/path/node1jr/bindings"/>
   <journal-directory path="//network/path/node1jr/journal"/>
   <large-messages-directory
path="//network/path/node1jr/large-messages"/>
-->
```

6. ファイルの <hornetq-server name="backup"> セクションを見つけます。
7. このセクションをコメント解除し、正しいディレクトリのパスを設定します。

```
<!-- un mark this for node 1 backup (which is node2jr) and set your
path until node2jr
 <paging-directory path="//network/path/node2jr/paging"/>
 <bindings-directory path="//network/path/node2jr/bindings"/>
 <journal-directory path="//network/path/node2jr/journal"/>
 <large-messages-directory
path="//network/path/node2jr/large-messages"/>
-->
```

8. クラスタの 2 番目のノードについて上記の手順を繰り返します。ただし、「*node1*」を「*node2*」に、「*node2*」を「*node1*」に置き換えて実行してください。
9. 3 ノード以上のクラスタについては、同様の方法で standalone-full-ha.xml ファイルを編集します。

   たとえば、3 ノード クラスタで、以下の変更を加えます。

   - ノード 1
     - ライブ HornetQ は、*network-path*/*node1* を指します。
     - バックアップ HornetQ は、*network-path*/*node2* を指します。
   - ノード 2
     - ライブ HornetQ は、*network-path*/*node2* を指します。
     - バックアップ HornetQ は、/network/path/*node3* を指します。

- ノード 3
  - ライブ HornetQ は、*network-path*/*node3* を指します。
  - バックアップ HornetQ は、*network-path*/*node1* を指します。

JBoss 6.1 用のマスタ ノードの作成

マスタ ノード（クラスタ内の最初のノード）を作成することによって、JBoss 6.1 クラスタの作成を開始します。

次の手順に従ってください:

1. JBoss と JDK をコンピュータにインストールします。
2. CA Identity Manager インストール プログラムを起動します。
   - Windows： ユーザのインストール メディアから、以下のプログラムを実行します。
     `ca-im-release-win32.exe`
   - UNIX： ユーザのインストール メディアから、インストール プログラムを実行します。たとえば、Solaris の場合は以下のとおりです。
     `ca-im-release-sol.bin`

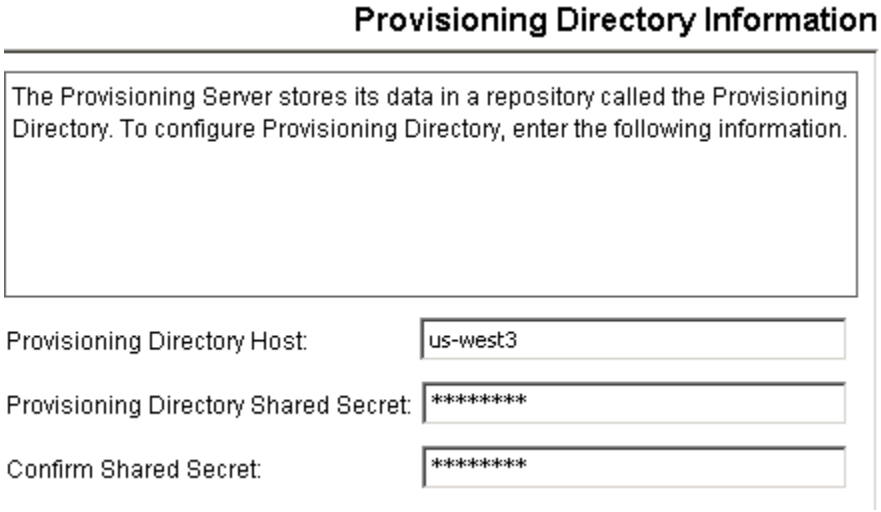
   release は、CA Identity Manager の現在のリリースを表します。

   重要: ユーザ名、ホスト名、ポートなどインストーラによって必要とされる情報を収集したことを確認してください。
3. 以前のリリースの CA Identity Manager と同じ値を入力することにより、データベース クレデンシャルを必要とするセクションを完了します。

   CA Identity Manager r12 から使用しはじめた場合、タスク永続性、ワークフロー、監査、およびレポート用に異なるデータベース ストアを使用しているときは、インストール後に、個別のストアを指すようにデータ ソースを手動で更新してください。

   注: インストール時に、ワークフロー データベースをアップグレードして、タスク永続性データを移行するオプションを参照する場合は、それらのオプションを有効にします。

4. CA Identity Manager サーバおよびユーザに必要な他のコンポーネントをこのシステムに含めることにより、コンポーネントの選択セクションを完了させます。
5. インストールの要件に基づいて他のセクションを完了させます。
6. インストールでパスワードまたは共有秘密キーを入力するときは、必要なときに思い出すことができるパスワードを確実に入力してください。



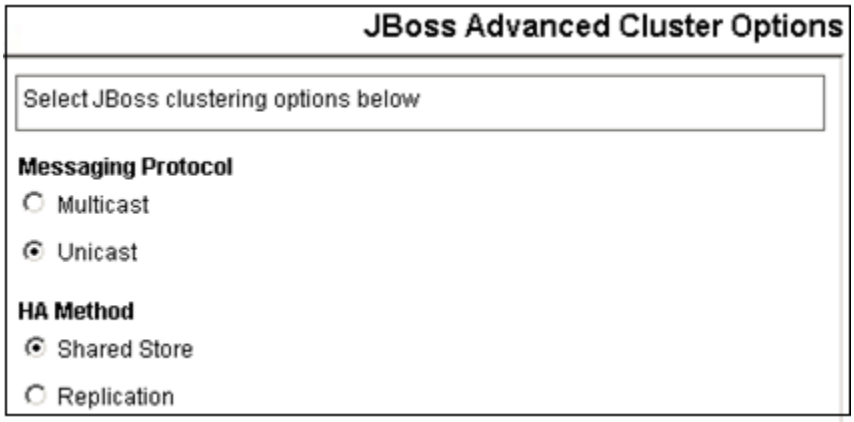
7. 以下のように、［JBoss Application Server Information］ページへの入力を完了します。
   a. 負荷分散用 Web サーバの URL とポート番号を使用して、アクセス サーバの URL とポート番号を入力します。
   b. ［Cluster Installation］を選択します。
   c. ピア ID （0 ～ 255 の一意の数字）を入力します。 そのピア ID を記録し、他のノードには別の数字を使用します。

8. クラスタの詳細オプションを選択します。
   - メッセージ機能プロトコルとしてマルチキャストまたはユニキャストを選択します。
   - 高可用性に関して共有ストアまたはレプリケーションを選択します。

     共有ストアには、ジャーナル ファイルを格納するためのストレージ エリア ネットワーク（SAN）サーバが必要です。

     レプリケーションでは、ジャーナル ファイルが各ノードに格納されます。

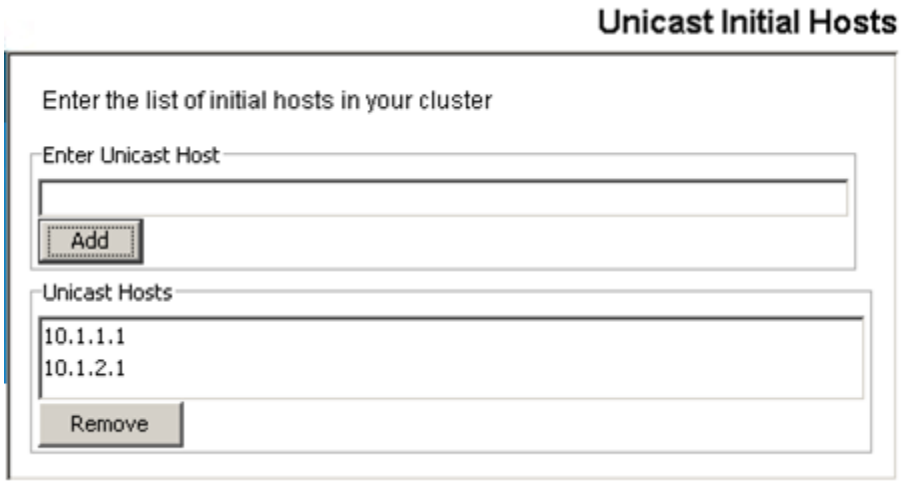
図 3: 詳細設定オプションの選択



9. マルチキャストを選択した場合は、次の手順にスキップします。

   JBoss がインストールされているシステムのユニキャスト初期ホストのリストを提供します。

図 4: JBoss クラスタ内の初期ホストの追加



10. ユニキャストを選択した場合は、次の手順にスキップします。

    マルチキャスト アドレス テストが失敗した場合は、standalone.bat または standalone.sh ファイルにある MULTI_CAST_ADDRESS の値を編集します。 一意のマルチキャスト アドレスを入力してください。

11. IPv6 をサポートするシステムにインストールする場合は、以下に示す、standalone.bat または standalone.sh ファイルの IDM_OPTS エントリのプロパティの 1 つを変更します。

    - Solaris 上の IPv6 のみのシステムでは、以下のエントリをコメント解除します。

      ```
      IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv6Addresses=true"
      ```

    - IPv6/IPv4 システムでは、以下のエントリをコメント解除します。

      ```
      IDM_OPTS="$IDM_OPTS -Djava.net.preferIPv4Stack=true"
      ```

12. インストール中に問題が発生した場合は、インストール ログ (P. 187) を調べます。

<JK> コネクタの設定

次の手順に従ってください:

1. 以下のリンクの手順に基づいて JK コネクタをインストールします。

   http://community.jboss.org/wiki/usingmodjk12withjboss

2. この手順を使用する場合、以下に注意します。

   a. modjk ワーカーを設定する際には、以下の場所にある workers.properties ファイルを使用します。

      Windows の場合： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥samples¥ConnectorConfiguration¥windows¥IIS_JBoss

      UNIX の場合： /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/samples/Cluster/JBoss/ConnectorConfiguration

   b. このファイルで、worker.worker*N*.* （作業者名）を対応するノードの Peer ID に置換します。

      2 つを超えるノードがある場合は、各追加ノードの worker.workerN.* セットをコピーし、作業者名を変更します。

   c. 対応するノードのホスト名を worker.worker*N*.host フィールドに入力します。

      たとえば、myhostA、myhostB および myhostC という名前の（Peer ID 1、2、および 3 を使用） 3 つの JBoss ホストに CA Identity Manager サーバがインストールされているクラスタを想定します。workers.properties ファイルが以下のように表示されます。

```
worker.worker1.port=8009
worker.worker1.host=myhostA
.
.
worker.worker1.recovery_options=28

worker.worker2.port=8009
worker.worker2.host=myhostB
.
.
```

```
worker.worker2.recovery_options=28

worker.worker3.port=8009
worker.worker3.host=myhostC
.
.
worker.worker3.recovery_options=28
.
.
worker.router.balance_workers=worker1,worker2,worker3
```

d. 上記の場所にある uriworkermap.properties ファイルを、*APACHE_HOME*/conf にコピーします。

e. Tomcat にセッション維持性を設定する手順は省略します。 この機能は、インストーラによって、workers.properties ファイルにおいてすでに設定されています。

JBoss クラスタの開始

すべての設定が完了したら、以下の順序ですべてのサーバを起動します。

次の手順に従ってください:

1. CA Identity Manager をサポートする SiteMinder ポリシー サーバの 1 つを起動します。

   注: ポリシー サーバ クラスタがある場合は、CA Identity Manager ディレクトリの作成、CA Identity Manager 環境の作成/変更、または WorkPoint 設定の変更を行っている間は、1 つのポリシー サーバのみを実行してください。

2. コマンドラインで、次のディレクトリに移動します。

   jboss_home/bin

3. 以下のコマンドを入力して、CA Identity Manager サーバを起動します。
   - Windows 上の JBoss 5 の場合

     run.bat -c all
   - UNIX 上の JBoss 5 の場合

     ./run.sh -c all
   - Windows 上の JBoss 6.1 の場合

     standalone.bat
   - UNIX 上の JBoss 6.1 の場合

     ./standalone.sh
4. サーバが起動したことを示すメッセージが表示されるまで待機します。以下のメッセージに類似したメッセージが、コンソール ウィンドウに表示されます。

   ```
   DATE+TIME INFO  [com.sun.jersey.server.impl.application.WebApplicationImpl]
   (main) Initiating Jersey application, version 'Jersey: 1.1.5.1 DATE+TIME'
   ```
5. SiteMinder Web エージェントをインストール済みの場合は、SiteMinder Web エージェントおよびアプリケーション サーバ プロキシ プラグインをインストールした Web サーバ を起動します。

クラスタ化されたインストールの確認

すべての手順を完了して、クラスタを開始したときに、インストールが成功したことをチェックしてください。

次の手順に従ってください:

1. CA Identity Manager サーバによって使用されるデータベースを開始します。
2. 停止していた余分なポリシー サーバおよび CA Identity Manager ノードを開始します。

3. 管理コンソールにアクセスし、以下のポイントを確認します。
   - ブラウザから以下の URL にアクセスできます。

     http://*im_server*:*port*/iam/immanage

     以下に例を示します。

     http://MyServer.MyCompany.com:*port-number*/iam/immanage
   - 管理コンソールが開きます。
   - アプリケーション サーバ ログにエラーが表示されません。
   - ディレクトリ リンクをクリックした場合、ユーザはエラー メッセージを受信しません。
4. 以下の URL 形式を使用して、アップグレードされた環境にアクセスできることを確認してください。

   http://*im_server*:*port*/iam/im/*environment*

Linux システムでのパフォーマンスの改善

JBoss クラスタ内の Linux システムでは、ディレクトリまたは環境の作成が非常に遅くなります。そこで、パフォーマンスを改善するため、run.sh ファイルの JAVA_OPTS を変更します。 以下のように、太字で表示されたテキストを追加してください。

```
JAVA_OPTS="$IDM_OPTS $DEBUG_OPTS -Djava.security.policy=workpoint_client.policy
-Xms256m -Xmx1024m -XX:MaxPermSize=256m
-XX:+AggressiveOpts -XX:+UseConcMarkSweepGC -XX:+UseParNewGC
-XX:ReservedCodeCacheSize=50m
```

リモート プロビジョニング マネージャの設定

プロビジョニング マネージャをプロビジョニング サーバから別のシステムにインストールした場合、サーバへの通信を設定します。

注: プロビジョニング マネージャをインストールするには、CA Identity Manager 管理ツールを Windows システムにインストールします。

次の手順に従ってください:

1. プロビジョニング マネージャをインストールした Windows システムにログインします。
2. ［スタート］-［プログラム］-［CA］-［Identity Manager］-［Provisioning Manager Setup］に移動します。
3. プロビジョニング サーバのホスト名を入力します。
4. ［構成］をクリックします。
5. 代替プロビジョニング サーバについては、プルダウン リストからドメイン名を選択します。
6. ［OK］をクリックします。

   これでプロビジョニング マネージャを起動し、設定したドメイン名を参照できるようになります。

オプション プロビジョニング コンポーネントのインストール

CA Identity Manager のオプションのプロビジョニング コンポーネントは、im-pc-*release*.zip にあります。

release は、CA Identity Manager の現在のリリースを表します。

ZIP ファイルの内容は、以下のとおりです。

リモート エージェント

これらのコンポーネントをインストールするには、プロビジョニング コンポーネントメディア（¥RemoteAgent の下）から固有のエージェント インストーラを実行します。IPv6 サポートを望む場合は、ユーザのエージェントをインストールする必要があります。

パスワード同期エージェント

このコンポーネントをインストールするには、プロビジョニング コンポーネント メディア（¥Agent 下）からパスワード同期エージェント インストーラを実行します。

クレデンシャル プロバイダ

このコンポーネントをインストールするのは、プロビジョニング コンポーネント メディア（¥Agent 下）からクレデンシャル プロバイダ インストーラを実行します。

Bulk Loader クライアント/PeopleSoft フィード

このコンポーネントをインストールするには、プロビジョニング コンポーネント メディア（¥Clients 下）から Bulk Loader Client インストーラを実行します。

CA IAM CS SDK

このコンポーネントをインストールするには、CA Identity Manager メディア（¥Provisioning の下）から、CA IAM CS SDK のインストーラを実行します。

CCI スタンドアロン

このコンポーネントをインストールするには、プロビジョニング コンポーネント メディア（¥Infrastructure の下）から CCI スタンドアロン インストーラを実行します。

CA Identity Manager インストーラは、デフォルトではすべてのコネクタをインストールします。 ただし、管理しているエンドポイント システムにエージェントをインストールしないと、関連のコネクタを使用できない場合があります。

コネクタはプロビジョニング サーバ上で実行されて、エンドポイントによって管理されているシステムと通信します。 たとえば、プロビジョニング サーバに ADS コネクタがインストールされた場合にのみ、Active Directory Services （ADS）を実行するシステムを管理できます。

注: 各コネクタの詳細については、「コネクタ ガイド」を参照してください。

これらのコンポーネントの詳細については以下のガイドを参照してください。

- クレデンシャル プロバイダ（*管理ガイド*）
- パスワード同期エージェント（*管理ガイド*）
- Connector Xpress （*Connector Xpress ガイド*）
- コネクタで使用するエージェント（*コネクタ ガイド*）

第 5 章: 個別データベース設定

このセクションには、以下のトピックが含まれています。

インストール ステータス

このテーブルでは、インストール プロセスにおける現在のステータスがわかります。

現在のステータス	インストール処理の手順
	1. あらかじめ必要なハードウェアとソフトウェアをインストールし、要件に応じてシステムを設定します。
	2. 次のインストールの 1 つを実行します。 ■ 単一ノードへのインストール ■ アプリケーション サーバ クラスタへのインストール
X	**3. （オプション）個別のデータベースを作成します。**
	4. （オプション）レポート サーバをインストールします。
	5. （オプション）代替のプロビジョニング ディレクトリ、代替のプロビジョニング サーバ、およびコネクタ サーバをインストールして、フェイルオーバと負荷分散をサポートします。

個別データベースの作成

CA Identity Manager には、監査、スナップショット（レポート）、ワークフローおよびタスク永続性用のオブジェクトおよびデータを格納するためのリレーショナル データベースが必要です。CA Identity Manager のインストール時、アプリケーション サーバが起動されるときに、すべてのデータベース スキーマが自動的に作成されます。 ただし、スケーラビリティを目的として、個別のデータベースを作成し、インストール中に CA Identity Manager によって最初に作成された既存のデータベース スキーマのいずれか 1 つと置換する場合もあります。

以下についてデータベース インスタンスを作成できます。

- ワークフロー
- 監査
- タスク永続性
- オブジェクト ストア
- スナップショット（レポート）
- アーカイブ（タスク永続性アーカイブ）

重要: CA Identity Manager データベース スキーマ ファイル用の Windows デフォルトの場所を以下に示します。

- ワークフロー： このセクションを参照し、CreateDatabase スクリプトを実行します。
- 監査： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥db
- タスク永続性 : C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥db
- オブジェクト ストア： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥db
- スナップショット（レポート）： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥imrexport¥tools¥db
- アーカイブ（タスク永続性アーカイブ）： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager ¥tools¥db

個別データベースを作成する方法

CA Identity Manager 用個別データベースを作成する方法

✓	手順
	1. CA Identity Manager 用の Microsoft SQL Server または Oracle データベースのインスタンスを作成します。
	2. データ ソースを編集します。
	3. （オプション） SQL スクリプトを実行します。

MS SQL Server データベース インスタンスの作成

次の手順に従ってください：

1. SQL サーバでデータベース インスタンスを作成します。
2. ユーザを作成し、ユーザのプロパティを編集して、このユーザにデータベースに対して必要な権限（public および db_owner 権限など）を付与します。

   注: ユーザは、データベースを作成するための .sql スクリプトによって作成されたすべてのテーブルに対して少なくとも選択、挿入、更新、および削除の権限を持っている必要があり、これらのスクリプトで定義されたすべてのストアド プロシージャ（該当する場合）を実行できる必要があります。
   たとえば、ユーザは、テーブルについてのこれらの許可が以下のデフォルトの場所で定義されている必要があります。

   C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥db¥taskpersistence¥sqlserver¥idm_db_sqlserver.sql
3. ユーザのプロパティの編集中、先ほど作成したデータベースをユーザのデフォルト データベースとして設定します。
4. データベースがインストールされているサーバの［SQL Server のプロパティ］ダイアログ ボックスの［セキュリティ］タブで、［認証］設定が「SQL Server」の値であることを確認します。

注: Microsoft SQL Server の詳細については、Microsoft SQL Server のドキュメントを参照してください。

Oracle データベース インスタンスの作成

次の手順に従ってください:

1. 新規表スペースを作成します。
2. 新規ユーザを作成します。
3. 新規データベースへのユーザ権限を付与します。
   - テーブルの作成/変更/ドロップ
   - ビューの作成/変更/ドロップ
   - インデックスの作成/変更/ドロップ
   - ストアドプロシージャの作成/置換/ドロップ
   - 機能の作成/置換/ドロップ
   - シーケンスの作成/ドロップ
   - トリガの作成/置換/ドロップ
   - タイプの作成/置換/ドロップ
   - レコードの挿入/選択/削除
   - CREATE SESSION/データベースへの接続
4. ユーザへの DBA 権限の付与

注: Oracle の詳細については、Oracle のドキュメントを参照してください。

データ ソースの編集

次の手順に従ってください:

1. テキスト エディタで、以下のいずれかのファイルを開きます。
   - JBoss 6.1 -- standalone-full.xml（クラスタ化されたインストールの場合は、standalone-full-ha.xml）
   - JBoss 5.x -- jboss_home/server/default/deploy ディレクトリ（クラスタ化されたインストールの場合は、jboss_home/server/all/deploy ディレクトリ）にある適切なデータ ソース記述子）

   JNDI データ ソース記述子を以下に示します。
   - タスク永続性： iam/im/jdbc/jdbc/idm
   - ワークフロー： iam/im/jdbc/jdbc/WPDS

- 監査： iam/im/jdbc/auditDbDataSource
- スナップショット： iam/im/jdbc/jdbc/reportsnapshot
- オブジェクト ストア： iam/im/jdbc/jdbc/objectstore
- アーカイブ： iam/im/jdbc/jdbc/archive

2. データ ソース記述子内の DatabaseName、User、および Password を新しいデータベース用の適切な値に変更します。

   重要: ご使用のバージョンの JBoss では、ユーザ名とパスワードが jboss_home¥server¥default¥conf¥login-config.xml に格納されている場合があります。その場合、FIPS のサポートに必要な JBoss セキュリティ レルムを作成できます。このアプローチを使用すると、クリア テキストでユーザ名とパスワードが表記されることも回避できます。詳細については、「設定ガイド」を参照してください。

CA Identity Manager を再起動すると、データベース スキーマ（SQL スクリプト）が自動的に適用されます。

SQL スクリプトの実行

CA Identity Manager が開始されると、データベースに対して SQL スクリプトが自動的に実行されます。ただし、SQL を自分で実行したい場合は、アプリケーション サーバを再起動する前に以下の手順を行います。

これらのスクリプトは、CA Identity Manager 管理ツールでインストールされます。

次の手順に従ってください:

1. 以下のいずれかを実行します。
   - Microsoft SQL Server： クエリ アナライザ: ツールを開き、必要なスクリプトを選択します。
   - Oracle： 必要なスクリプトの SQL プロンプトを開きます。
2. データベースの作成目的に応じて以下のいずれかのスクリプト（デフォルトの Windows の場所と共に表示）を選択します。
   - タスク永続性：
     - Microsoft SQL Server： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥db¥taskpersistence¥sqlserver¥idm_db_sqlserver.sql
     - Windows 上の Oracle: C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥db¥taskpersistence¥oracle9i¥idm_db_oracle.sql
     - UNIX 上の Oracle： /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/db/taskpersistence/oracle9i/idm_db_oracle.sql
   - 監査：
     - Microsoft SQL Server: C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥db¥auditing¥sqlserver¥ims_mssql_audit.sql
     - Windows 上の Oracle: C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥db¥auditing¥oracle¥ims_oracle_audit.sql
     - UNIX 上の Oracle： /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/db/auditing/oracle/ims_oracle_audit.sql

- スナップショット：
  - Microsoft SQL Server: C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥imrexport¥db¥sqlserver¥ims_mssql_report.sql
  - Windows 上の Oracle: C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥imrexport¥db¥oracle¥ims_oracle_report.sql
  - UNIX 上の Oracle：/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/imrexport/db/oracle/ims_oracle_report.sql
- ワークフロー：「ワークフローのスクリプトの実行」のセクションを参照してください。
- オブジェクト ストア：
  - Windows 上の Oracle: C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥db¥oracle_objectstore.sql
  - Microsoft SQL Server： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥db¥sql_objectstore.sql
  - UNIX 上の Oracle：/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/db/oracle_objectstore.sql
- アーカイブ スクリプト：
  - Microsoft SQL Server： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥db¥taskpersistence¥sqlserver¥archive_db_sqlserver.sql
  - Windows 上の Oracle: C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥db¥taskpersistence¥oracle9i¥archive_db_oracle.sql
  - UNIX 上の Oracle：/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/db/taskpersistence/oracle9i/archive_db_oracle.sql

3. スクリプト ファイルを実行します。
4. スクリプトを実行したときに、エラーが表示されなかったことを確認します。

ワークフローのスクリプトの実行

CA Identity Manager には、新規ワークフロー データベース インスタンスをセットアップするための SQL スクリプトが含まれます。

CreateDatabase スクリプトを実行する方法

次の手順に従ってください:

1. スクリプトを実行する前に、CreateDatabase.bat または .sh スクリプト内の DB_CLASSPATH 属性に対する sqljdbc.jar へのパスを追加します。
2. コマンド プロンプトから、CreateDatabase.bat または sh を実行します。このファイルのデフォルトの場所は、以下のとおりです。

   Windows： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥Workpoint¥install.

   UNIX：
   /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/Workpoint/install.

   コマンド プロンプト ウィンドウおよび WorkPoint アプリケーションが表示されます。
3. ドロップダウン リストからデータベース タイプを選択します。
4. 設定ユーティリティのフィールドに入力するには、以下のガイドラインを使用します。
   - JDBC クラス パラメータについては、以下を入力します。

     Oracle： oracle.jdbc.driver.OracleDriver

     SQL Server： com.microsoft.sqlserver.jdbc.SQLServerDriver
   - JDBC URL については、以下を入力します。

     Oracle： jdbc:oracle:thin:@*wf_db_system*:1521:*wf_oracle_SID*

     SQL Server： jdbc:sqlserver://*wf_db_system*:1433;databaseName=*wf_db_name*
   - データベース ユーザ ID パラメータについては、ワークフロー データベースを作成するとき作成したワークフロー ユーザを入力します。
   - パスワード パラメータについては、ワークフロー ユーザに対して作成したパスワードを入力します。
   - データベース ID については、「WPDS」を入力します

5. デフォルトのチェック ボックスの選択を使用します。
6. ［初期化］ボタンをクリックします。

   設定が完了すると、以下のようなメッセージがコマンド プロンプト ウィンドウに表示されます。

   `The create database process finished with 0 errors.`（データベース作成プロセスはエラー `0` で終了しました。）
7. アプリケーション サーバを再起動します。

第 6 章: レポート サーバのインストール

このセクションには、以下のトピックが含まれています。

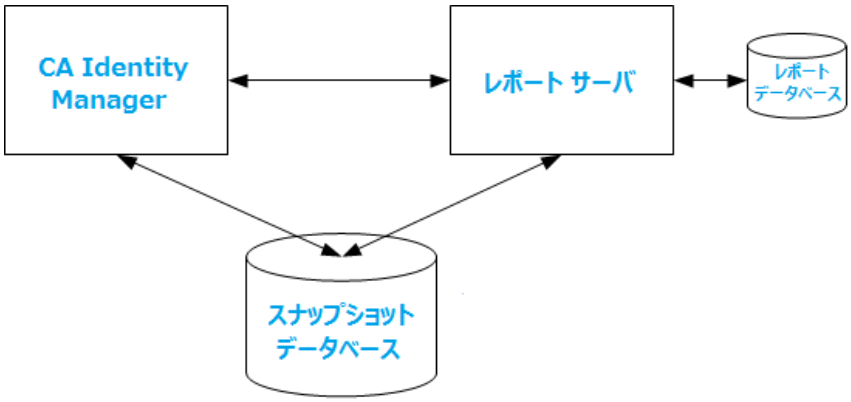
インストール ステータス

以下の表は、インストール プロセスのどこにいるかユーザに示します。

現時点	インストール プロセスの手順
	1. 前提条件のハードウェアおよびソフトウェアをインストールし、必要に応じてシステムを設定します。
	2. 以下のインストールのいずれかを実行します。 ■ 単一ノード インストール ■ アプリケーション サーバ クラスタ上のインストール
	3. （オプション）個別のデータベースを作成します。
X	**4. （オプション）レポート サーバをインストールします。**
	5. （オプション）レポート サーバで SSL 証明書を設定します。
	6. （オプション）フェイルオーバと負荷分散をサポートするために、代替プロビジョニング ディレクトリ、代替プロビジョニング サーバ、およびコネクタ サーバをインストールします。

レポーティングのアーキテクチャ

CA Identity Manager では、レポートのセットアップに、以下の図の 3 つの主要コンポーネントが必要です。



注: この図のスナップショット データベースは、監査データベースまたはワークフロー データベースである場合もあります。

レポート サーバ

別名 CA Business Intelligence のこのサーバは、CA Identity Manager およびスナップショット データベースと直接通信して、レポートを生成します。

レポート データベース

CA レポート サーバ（Business Objects）が独自データを格納するデータベース。

CA Identity Manager

CA Identity Manager により、レポート データベースに CA Identity Manager オブジェクト データをエクスポートできるようになります。

スナップショット データベース

CA Identity Manager 内のオブジェクトのスナップショット データを含む別個のデータベース

重要: レポート サーバは Business Objects Enterprise を使用します。ユーザ環境にすでにレポート サーバがあり、CA Identity Manager と共にそれを使用する場合、CA Identity Manager が必要とする最小バージョンは CA Business Intelligence 3.2 SP1 です。

レポートの考慮事項

レポート サーバをインストールする前に、以下を考慮します。

- レポート サーバのインストールは、最大で 2 時間かかる場合があります。
- レポート サーバをインストールするコンピュータに JBoss がインストールされていると、ポート競合が発生する場合があります。 Apache Tomcat が Web サーバである場合、以下のファイル内で JBoss ポート情報を見つけられます。
  - jboss-service.xml

    デフォルトの場所： *jboss_home*¥server¥*server_configuration*¥conf
  - server.xml

    デフォルトの場所： *jboss_home*¥server¥*server_configuration*¥deploy¥jboss-web.deployer

  jboss_home

  JBoss のインストール パスを指定します。

  server_configuration

  サーバ設定の名前を指定します。

  デフォルト値： default

  注: これらのファイルのいずれかに変更を加える場合は、JBoss を再起動します。

ハードウェア要件

レポート サーバのハードウェア要件はオペレーティング システムに基づいています。 *installer-media-root-directory/Docs* フォルダ内のユーザのオペレーティング システムと一致するファイル名を持つ PDF を参照します。

注: サポートされている OS バージョンおよびデータベースの詳細については、Business Objects Web サイトを参照してください。

レポート サーバをインストールする方法

以下のチェックリストでは、CA Identity Manager のレポート機能をインストールする手順について説明します。

✓	手順
	1. レポート インストール前のチェックリストを確認します。
	2. レポート情報を収集します。
	3. レポート サーバが必要とするポートを開きます。
	4. レポート サーバ（CA Business Intelligence）および Service Packs をインストールします。
	5. レジストリ スクリプトを実行します。
	6. JDBC JAR ファイルをコピーします。
	7. プロキシ サーバをバイパスします。
	8. デフォルト レポートを展開します。
	9. インストール後の手順を実行します。

注: インストール後のレポートの設定の詳細については、「管理ガイド」を参照してください。

レポート インストール前のチェックリスト

レポート サーバをインストールする前に、最小限のシステムおよびデータベースの要件を満たしているか確認するために、以下のチェックリストを印刷します。

- レポート サーバをインストールする Windows または UNIX システムが、最小限のシステム要件を満たしているか確認します。
- レポート データベースとして MySQL を使用しているか確認します。

- スナップショット データベースのデータベース インスタンスを作成する場合は、新しいデータベース上で以下のスクリプトを実行します。
  - Microsoft SQL： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥imrexport¥db¥sqlserver¥ims_mssql_report.sql
  - Oracle： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥imrexport¥db¥oracle¥ims_oracle_report.sql

    これらのスクリプトを実行するために、データベース ユーザには次のものが必要です。グローバルなクエリ リライト許可を使用してテーブル、インデックス、セッションおよびビューを作成するための、DBA、接続、およびリソースのロールならびにシステム権限。
- UNIX 上で、ローカル .profile ファイル内にグローバルとして以下のパラメータを設定します。
  - ORACLE_BASE: Oracle がインストールされている最上位のディレクトリ。
  - ORACLE_HOME: ORACLE_BASE 下の Oracle のルート ディレクトリへのパス
  - LD_LIBRARY_PATH： $ORACLE_HOME/lib32:$ORACLE_HOME/lib

    Oracle が 64 ビット インストールである場合は、lib32 を使用します。SQL Plus を使用して、Oracle データベース インスタンスに接続し、64 ビット インストールかどうかを判別します。
  - ORACLE_SID： tnsnames.ora ファイルで使用される SID 名。
  - JAVA_HOME： Java のルート ディレクトリへのパス。 Business Objects は以下の場所に JDK をインストールします。
    `report_server_home/jre`

    注: JDK 1.5 はレポートがサポートされている最小バージョンです。

- PATH：
  $LD_LIBRARY_PATH:$JAVA_HOME:$JAVA_HOME/bin:$ORACLE_HOME/bin:$PATH
- LC_ALL： en_US.UTF-8

  注: CASHCOMP 環境変数が空であることを確認してください。

- UNIX システムの場合
  - 3 GB の空きディスク領域が /tmp 下に必要です。
  - レポート サーバをインストールするには、root 以外のユーザ アカウントへのアクセスが必要です。

    このユーザはローカル ファイル システムにホーム ディレクトリを持っている必要があります。 たとえば、以下のコマンドはローカル ホーム ディレクトリを持つユーザを作成します。

    ```
    useradd -u 505 -g 0 -d /export/home/cabi -m cabi
    ```

    また、インストール グループおよび root ユーザがメンバであるグループに、root 以外のユーザを追加します。
  - データベース サーバがレポート サーバと同じシステム上にない場合は、/etc/hosts ファイルにデータベース サーバ名を入力します。（DNS がある場合、この手順は不要です。）
  - 問題が発生する場合は、以下の場所の下の SDK.log を検査します。

    /opt/CA/SharedComponents/CommonReporting3/ca-install.log

    /opt/CA/SharedComponents/CommonReporting3/CA_Business_Intelligence_InstallLog.log

レポート情報

レポート サーバ インストール中に必要な以下の情報を記録します。

フィールド名	説明	回答
管理者パスワード	Business Objects Infoview コンソールにログインするためのパスワードを定義します。	
User Name	レポート データベースのユーザ名を識別します。	

フィールド名	説明	回答
Password	レポート データベースの管理パスワード クレデンシャルを識別します。	
Pre-Installed Tomcat Information	Tomcat の以前のインストールについてのパスおよびポート番号を識別します。 ユーザが Tomcat の以前のインストールを使用しない場合、レポート サーバ インストーラは Tomcat をインストールできます。	
Tomcat Port Numbers	Tomcat の接続、リダイレクト、およびシャットダウンのポート。 **注**: レポート サーバを CA Identity Manager と同じシステムにインストールする場合は、CA Identity Manager をインストールする際にアプリケーション サーバ URL に対して指定したポート番号と Tomcat 接続ポートが矛盾しないことを確認します。	

レポート サーバ用ポートを開く

CA Identity Manager およびレポート サーバが正常に通信するには、以下のポートが開かれている必要があります。

- 集中管理サーバ （CMS）ポート： 6400
- レポート サーバ Web アプリケーション ポート：
  - JBoss/Tomcat： 8080
  - WebLogic： 7001
  - WebSphere： 9080

以下の点に注意してください。

- このポートは CA Identity Manager サーバのアプリケーション サーバ ポートではありません。
- Web サーバ ポートはレポート サーバ インストール中に提供されます。 ユーザがインストール中に別のポートを使用する場合は、レポート サーバが実稼働で展開されているとき、それらのポートがファイアウォールを介して開いている必要があります。
- レポート サーバは、CA Identity Manager によって使用されるアプリケーション サーバに接続しません。

- CA Identity Manager がレポートおよび監査データベース用に設定したすべてのデータベース ポート。 CA Identity Manager サーバは、レポート サーバにデータベース情報を送信する必要があるので、これらのポートが開かれている必要があります。 たとえば、スナップショット データベースが Oracle データベースである場合、レポート サーバはアウトバウンドに開いた Oracle ポートを必要とします。

CA レポート サーバのインストール

サポートされる Windows または UNIX システムにレポート サーバをインストールできます。 以下のセクションでは、Windows および UNIX インストール ウィザードを使用してレポート サーバをインストールする方法を詳述します。

重要: 実稼働環境の場合は、CA Identity Manager サーバを有するシステムからレポート サーバを別個のシステムにインストールします。 レポート サーバをデモンストレーション目的のための CA Identity Manager サーバと同じシステムにインストールする場合、JBoss がデフォルト Tomcat ポート 8080 および 1099 のポートを使用しているときは、それらのポートを選択しないでください。

注: CA Identity Manager は、CA Business Intelligence 3.3 SP1（これは Business Objects XI 3.0 SP6 です）をサポートします。

Windows インストーラの実行

レポート サーバ メディアにある Windows インストール ウィザード（Disk1¥InstData¥VM¥Install.exe）を使用して、レポート サーバをインストールします。

注: CA Support サイトの CA Identity Manager 製品ダウンロードで、レポート サーバをダウンロードすることができます。

レポート サーバをインストールする手順を以下に示します。

次の手順に従ってください:

1. アプリケーションをすべて終了します。
2. レポート サーバをダウンロードして解凍します。
3. Disk1¥InstData¥VM に移動し、インストールの実行プログラムをダブルクリックします。

   インストール ウィザードが起動されます。
4. レポート サーバをインストールするために収集されたレポート情報を使用します。

   以下の点に注意してください。

   - インストール中に、新規インストールを選択します。この選択は、レポート データベースとして MySQL を使用することを確認するのに役立ちます。 デフォルト以外のポートがポート競合を回避するように設定する必要がある場合は、カスタム インストールを選択しますが、必ずレポート データベースに MySQL を選択します。
   - IIS を選択解除して、Web サーバとして Tomcat を選択します。
   - レポート サーバを CA Identity Manager と同じシステムにインストールしている場合は、Tomcat 接続ポートを慎重に選択します。そのポートが、CA Identity Manager のインストール時にアプリケーション サーバ URL に対して指定したポート番号と矛盾しないことを確認してください。ただし、実稼働環境内の CA Identity Manager サーバとは異なるシステムにレポート サーバをインストールすることをお勧めします。
5. インストール設定を確認し、［インストール］をクリックします。

   レポート サーバがインストールされます。

UNIX インストーラの実行

以下のコマンドの実行により、インストール ファイルに実行許可を追加します。

```
chmod+x /cabi-linux-3_2_00/cabiinstall.sh
```

重要: さまざまなサブネットにわたって実行された場合、インストーラがクラッシュすることがあります。この問題を回避するには、レポート サーバをホスト システムに直接インストールします。

レポート サーバをインストールするには、以下の手順を実行します。

次の手順に従ってください:

1. レポート サーバをインストールするために作成した root 以外のユーザとしてログインします。
2. すべてのアプリケーションを終了します。
3. レポート サーバをダウンロードしてを tar ファイルを解凍します。

   注: CA Support サイトの CA Identity Manager 製品ダウンロードで、レポート サーバをダウンロードすることができます。
4. コマンド ウィンドウを開けて、インストール プログラムがある場所に移動します。
5. 以下のコマンドを入力します。

   ```
   /cabi-solaris-3_2_00/cabiinstall.sh
   ```
6. レポート サーバをインストールするために収集されたレポート情報を使用します。

   以下の点に注意してください。

   - インストール中に、新規インストールを選択します。この選択は、レポート データベースとして MySQL を使用することを確認するのに役立ちます。 デフォルト以外のポートがポート競合を回避するように設定する場合は、カスタム インストールを選択しますが、必ずレポート データベースに MySQL を選択します。
   - Web サーバとして Tomcat を選択します。
   - インストーラは、/opt/CA/SharedComponents/CommonReporting3 にレポート サーバをインストールします。 別の場所を指定して、インストール場所を変更することはできません。/opt/CA ディレクトリに対しては root 以外のユーザ権限が必要なので、それがないとインストールは失敗します。

7. インストール設定を確認し、［インストール］をクリックします。

   レポート サーバがインストールされます。

Linux インストーラの実行

次の手順に従ってください:

1. X-サーバをクライアント オペレーティング システム上にインストールして起動します。

   以下の場所から X-Win32 をダウンロードできます。

   ```
   http://www.starnet.com/products/xwin32/download.php
   ```

2. Business Objects インストール アカウントを使用して、Linux にログオンし、以下のコマンドを実行します。

   ```
   bash$ export DISPLAY=$YOURXWin32ClientMACHINENAME:0.0
   bash$ echo &DISPLAY
   bash$ cd $INSTALLDIR/bobje/setup/
   bash$ source env.sh
   bash$ regedit
   ```

   「$INSTALLDIR」はレポート サーバがインストールされている場所です。

3. X-win32 クライアント システムに切り替えます。

   設定が成功したことを示す Registry Editor メッセージが表示されます。

4. 以下の HKEY_LOCAL_MACHINE の場所の下にレジストリ カテゴリを作成します。

   ```
   HKEY_LOCAL_MACHINE¥Software¥Business Objects¥Suite 12.0¥Crystal
   Reports¥DatabaseOptions
   ```

5. DatabaseOptions カテゴリ下に MergeConnectionProperties という名前のキーを追加し、値を「Yes」に設定します。

6. 以下の場所 HKEY_CURRENT_USER の下に MergeConnectionProperties という名前のキーを追加します。

   ```
   HKEY_CURRENT_USER¥Software¥Business Objects¥Suite 12.0¥Crystal
   Reports¥DatabaseOptions
   ```

7. MergeConnectionProperties の値を「Yes」に設定します。

8. インストールが成功したことを確認するために、Infoview 内のレポートをリフレッシュまたはスケジュールします。

レジストリ スクリプトの実行

CA Identity Manager がレポート サーバ内のレポートのデータ ソースを変更するように、mergeConnection スクリプトを実行します。

注: 64 ビット システムでは、この手順を省略します。 レポート サーバは 32 ビット アプリケーションです。したがって、レジストリの 32 ビット側を使用します。 64 ビット システムで、SysWOW64 から REGEDT32 を直接開き、タイプが「REG_SZ」で値が「Yes」の MergeConnectionPropertie キーを作成します。 以下の場所にキーを作成します。

```
@HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Business Objects¥Suite 12.0¥Crystal Reports
```

Windows では、以下の手順に従います。

1. CA Identity Manager 管理ツールキットを有するシステムからレポート サーバに mergeConnection スクリプトをコピーします。 ツールキットを有するシステムで、このスクリプトのデフォルトの場所は以下のとおりです。

   C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥ReportServerTools

2. mergeconnections_3.0.reg スクリプトを実行して、表示されるプロンプトに応答します。
3. ［スタート］-［Program Files］-［CA］-［Report Server］-［Central Configuration Manager］をクリックします。
4. Tomcat および BO サーバ サービスを含むすべてのサービスが開始します。

UNIX および Linux では、以下の手順に従います。

1. mergeconnections スクリプト内の Windows 制御文字をチェックします。

   バイナリ モードの FTP を使用してソフトウェアをダウンロードした場合、これらの文字はこのスクリプトの中にありません。 別のダウンロード方法を使用した場合は、これらの文字を削除するために dos2unix コマンドを使用します。

2. CA Identity Manager 管理ツールキットを有するシステムからレポート サーバに mergeconnections_3.0.cf スクリプトをコピーします。 ツールキットを有するシステムで、このスクリプトのデフォルトの場所は以下のとおりです。

   /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/ReportServerTools

   レポート サーバ システムで、このスクリプトを以下の場所に配置します。

   installation-directory/bobje/enterprise120/generic

3. BusinessObjects Enterprise 用の環境変数のソースは以下のとおりです。

   source installation-directory//bobje/setup/env.sh

4. 以下のとおり、以下のスクリプトを実行します。

   ```
   ./configpatch.sh mergeconnections_3.0.cf
   ```

   入力を促されたとき、オプションとして［1］を選択します。

   注: Linux システムでは、スクリプトを実行する前に、以下のように環境変数を設定します。

   ```
   export _POSIX2_VERSION=199209
   ```

5. 以下のように、Crystal 処理サーバを再起動します。

   a. レポート サーバをインストールするために使用した root 以外のユーザとしてログインします。

   b. 以下のコマンドを発行します。

      ```
      cd /opt/CA/SharedComponents/CommonReporting3/bobje
      ./stopservers
      ./startservers
      ```

JDBC JAR ファイルのコピー

次の手順に従ってください:

1. CA Identity Manager 管理ツールキットがインストールされている jdbcdrivers フォルダに移動します。 デフォルトの場所は以下のとおりです。
   - Windows： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥lib¥jdbcdrivers
   - UNIX： /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/lib/jdbcdrivers
2. ojdbc14.jar （Oracle の場合）または sqljdbc.jar （SQL Server の場合）を以下の場所にコピーします。
   - Windows： CA¥SC¥CommonReporting3¥common¥4.0¥java¥lib
   - UNIX： /opt/CA/SharedComponents/CommonReporting3/bobje/java/lib

   注: レポート サーバと互換性のある 1.2 ドライバを使用するために Tools¥lib¥jdbcdrivers¥1.2 から sqljdbc.jar をコピーします。
3. 以下の場所にある CRConfig.xml ファイルを開きます。
   - Windows： CA¥SC¥CommonReporting3¥common¥4.0¥java
   - UNIX： /opt/CA/SharedComponents/CommonReporting3/bobje/java
4. JDBC JAR ファイルの場所をクラスパスに追加します。 例：
   - Windows の場合：
     <Classpath>report_server_home¥common¥4.0¥java¥lib¥sqljdbc.jar;
     report_server_home¥ common¥4.0¥java¥lib¥ojdbc14.jar
     …</Classpath>
   - UNIX の場合：
     <Classpath>${BOBJEDIR}/java/lib/sqljdbc.jar:${BOBJEDIR}/java/lib/ojdbc14.jar:…</Classpath>

5. ファイルを保存します。
6. 以下のように Web サーバを再起動します。
   - Windows の場合、以下の手順に従います。
     a. ［スタート］-［すべてのプログラム］-［BusinessObjects XI *version*］-［BusinessObjects Enterprise］-［Central Configuration Manager］に移動します。

        Central Configuration Manager が開きます。

     b. すべてのサービスを選択し、［Restart］をクリックします。
   - UNIX の場合、以下の手順に従います。

     ```
     cd /opt/CA/SharedComponents/CommonReporting3/bobje
     ./stopservers
     ./startservers
     ```

プロキシ サーバのバイパス

CA Identity Manager がインストールされているシステムで要求送信のチャネルにプロキシ サーバを使用している場合、プロキシ サーバをバイパスする必要があります。 詳細については、「Java Networking and Proxies」を参照してください。

デフォルト レポートの展開

CA Identity Manager には、レポートに使用できるデフォルト レポートが付属しています。BIConfig は、固有の XML 形式を使用して CA Identity Manager 用のこれらのデフォルト レポートをインストールするユーティリティです。

レポート サーバの旧バージョンからアップグレードしている場合は、まず中央管理コンソールを使用して CA Identity Manager Reports フォルダを削除します。 既存のレポートは動作しません。 その後、新しいレポート サーバのデフォルト レポートを展開できます。

重要: このプロセスはすべてのデフォルト レポートを更新します。 デフォルト レポートをカスタマイズした場合は、更新を実行する前にそれらを必ずバックアップしてください。

次の手順に従ってください:

1. レポート サーバに関する以下の情報を収集します。
   - ホスト名
   - 管理者名
   - 管理者パスワード
   - スナップショット データベースのタイプ
2. Reports installer-root-directory/disk1/cabi/biconfig フォルダから *im_admin_tools_dir*/ReportServerTools フォルダにすべてのコンテンツをコピーします。
3. JAVA_HOME 変数を、インストールした JDK1.5 の 32 ビット バージョンに設定します。
4. 以下のいずれかのコマンドを実行します。
   - Microsoft SQL スナップショット データベースの場合：

     ```
     biconfig -h "hostname" -u "administrator_name" -p "administrator_password"
     -f "ms-sql-biar.xml"
     ```

   - Oracle スナップショット データベースの場合：

     ```
     biconfig -h "hostname" -u "administrator_name" -p "administrator_password"
     -f "oracle-biar.xml"
     ```

   注: UNIX オペレーティング環境で、biconfig.sh が実行許可を持っていることを確認します。

5. 手順 4 でコマンドを実行した場所にある biconfig.log ファイルを表示します。
6. デフォルト レポートが正常にインストールされたことを確認します。ログ ファイルの末尾のステータスを調べます。正常なインストールは、以下のように示されます。

```
ReportingDeployUtility - Reporting utility program terminated and return code = 0
```

BusinessObjects XI 3.x のインストール後の手順

レポート タスクを実行し、「Server Input% not found or server may be down" error message 」というエラー メッセージを受信した場合は、以下の手順を実行します。

次の手順に従ってください:

1. レポート サーバ インストール中に入力したユーザ名およびパスワードを使用して、中央管理コンソールにログインします。
2. メイン ダッシュボードの下の［Servers］を選択します。
3. ［Server Name］欄の下の［Input File Repository server］を探して、名前をダブルクリックします。
4. ［Server Name］テキスト ボックスに、以下を入力します。

   Input.*report_server_hostname*.InputFileRepository
5. ［Save］をクリックします。
6. ［Server Name］欄の下の［Output File Repository server］を探して、名前をダブルクリックします。
7. ［Server Name］テキスト ボックスに、以下を入力します。

   Output.*report_server_hostname*.OutputFileRepository
8. ［Save］をクリックします。
9. ［Server List］内のサーバを選択して、すべてのサーバを再起動します。

JBoss/WebLogic の CA Identity Manager およびレポート サーバ接続を保護する方法

CA Identity Manager とレポート サーバは保護されていない接続で通信します。SSL（Secure Sockets Layer）接続を使用すると、レポート サーバと CA Identity Manager 間の接続を保護することができます。

SSL 接続は、レポート サーバからデータがアクセスされるときに通信が暗号化されることを保証します。SSL を設定する前に、BO（Business Object）サーバで HTTPS が有効なことを確認してください。SSL で接続を保護するには、自己署名証明書または CA（認証局）から の証明書を使用できます。

自己署名証明書を使用して、SSL 証明書を設定するには、以下の手順に従います。

1. 証明書を生成するツールを使用して、BO サーバで使用されたキーストアから証明書をエクスポートします。
2. CA Identity Manager がインストールされているディレクトリに証明書をコピーします。
3. Java 信頼ストアに証明書をインポートします（cacerts）。 CA Identity Manager サーバによって現在使用されている Java バージョンにも証明書がインポートされていることを確認します。
4. 変更を有効にするため、アプリケーション サーバを再起動します。
5. CA Identity Manager で、［システム］-［レポート］-［レポート サーバ接続］に移動します。 ［セキュア接続］オプションを選択します。
6. ［テスト接続］をクリックして、接続を確認します。

以下の手順は、Keytool ユーティリティを使用して、証明書をエクスポート/インポートする例を示しています。

次の手順に従ってください:

1. BO サーバで、コマンド プロンプトを開き、以下のコマンドを入力して、キーストアから証明書をエクスポートします。

   Windows の場合：

   ```
   ..¥jvm¥bin¥keytool -export -alias testcert -file certificate.cer -keystore
   c:¥cert¥.keystore  –storepass <keystore password>
   ```

   Linux または Solaris の場合：

```
../jvm/bin/keytool -export -alias testcert -file certificate.cer -keystore
/root/.keystore  –storepass <keystore password>
```

2. CA Identity Manager がインストールされているディレクトリに証明書をコピーします。
3. CA Identity Manager サーバで、コマンド プロンプトを開き、以下のコマンドを入力してキーストアに証明書をインポートします。

   Windows の場合：

   ```
   ..¥jvm¥bin¥Keytool -import - trustcacerts –file c:¥cert¥certificater.cer –alias
   testcert -keystore JAVA_HOME¥jre¥lib¥security¥cacerts -storepass password
   ```

   Linux または Solaris の場合：

   ```
   ../jvm/bin/Keytool -import - trustcacerts –file /root/certificater.cer –alias
   testcert -keystore JAVA_HOME/jre/lib/security/cacerts -storepass password
   ```

   証明書が正常にインストールされます。

注: レポート サーバに SSL を設定するには、ベンダー固有のドキュメントを参照することを推奨します。 レポート サーバは Tomcat サーバと IIS サーバをサポートします。

レポート インストールの確認

レポートが正しくインストールされていることを確認するには、以下の手順に従います。

- 中央管理コンソールで、すべてのサービスが実行されていることを確認します。
- ユーザのレポート データベースが実行されていることを確認します。

注: インストール後のレポートの設定の詳細については、「管理ガイド」を参照してください。

サイレント インストール

レポート サーバのサイレント インストールの詳細については、「CA Business Intelligence インストール ガイド」を参照してください。レポート サーバ インストーラ ファイルを解凍する場合、レポート サーバ ドキュメントは以下のいずれかの場所で利用可能です。

- **Windows**： *install_root_directory*¥Docs¥CABI_Impl_ENU.pdf
- **UNIX**： *install_root_directory*/Docs/ENU/CABI_Impl_ENU.pdf

レポートをアンインストールする方法

システムでポリシー サーバが不要になった場合は、アンインストールします。 **注**: 詳細については、CA Business Intelligence のドキュメントを参照してください。

レポート サーバをアンインストールした後に、残存するアイテムを削除します (P. 118)。

残存アイテムの削除

以下のセクションでは、できるだけシステムをクリーンに保ち、同じシステムへのレポート サーバの再インストールが失敗するのを防ぐために、レポート サーバをアンインストールした後に手動で削除する必要があるアイテムの詳細について説明します。

Windows アイテムの削除

次の手順に従ってください:

1. *report_server_home* に移動します。

   report_server_home は、レポート サーバのインストール パスを示します。

2. BusinessObjects Enterprise 12 フォルダを開き、以下のフォルダを削除します。
   - Data
   - java
   - Logging

- Samples
- Web Content
- Web Services
- win32x86

3. Report Server フォルダに戻ります。
4. 共通フォルダを開きます。
5. 4.0 フォルダを開き、以下のフォルダを削除します。
   - crystalreportviewers115
   - j ava

残っていたアイテムの削除が完了しました。

UNIX アイテムの削除

UNIX 上に残存するレポート サーバ アイテムを削除する手順を以下に示します。

次の手順に従ってください:

1. コマンド プロンプトから、以下の場所に移動します。

   /opt/CA/SharedComponents

2. CommonReporting3 を削除します。

残存アイテムの削除が完了しました。

第 7 章: コネクタ サーバのインストール

このセクションには、以下のトピックが含まれています。

コネクタ サーバの前提条件

コネクタ サーバ インストールを準備する手順については、以下のセクションを参照してください。

システム要件

CA IAM CS を、プロビジョニング サーバまたは CA Identity Manager サーバと同じコンピュータにインストールする必要はありません。

一部のコネクタは、エンドポイント上のエージェントを必要とします。詳細については、「コネクタ ガイド」および「エンドポイントガイド」を確認してください。

CA IAM CS のインストール プログラムには、独自の Java 仮想マシンが含まれます。したがって、Java を個別にインストールする必要はありません。

タイムゾーンの考慮事項

典型的な環境において、時刻は、プロビジョニング サーバ内、および CA IAM CS によって参照されるさまざまなエンドポイントに格納されます。コンポーネントは、同じタイム ゾーンを持つサーバ上で実行される必要はありません。 ただし、すべてのコンポーネントが同じ絶対時間を使用する必要があります。

ファイルの場所

下記の表に、Windows および UNIX のデフォルト ディレクトリを示します。実際のインストール ディレクトリは、オペレーティング システム、およびインストール プロセス中のユーザの選択に依存します。

パス表記法	デフォルト ディレクトリ	
	Windows	UNIX
im-home	C:¥Program Files¥CA¥Identity Manager	/opt/CA/IdentityManager
imps-home	C:¥Program Files¥CA¥Identity Manager¥Provisioning Server	/opt/CA/IdentityManager/ProvisioningServer
cs-home	C:¥Program Files¥CA¥Identity Manager¥Connector Server	/opt/CA/IdentityManager/ConnectorServer
cs-sdk-home	C:¥Program Files¥CA¥Identity Manager¥Connector Server SDK	/opt/CA/IdentityManager/ConnectorServer SDK
conxp-home	C:¥Program Files¥CA¥Identity Manager¥Connector Xpress	/opt/CA/IdentityManager/ConnectorXpress

32 ビットおよび 64 ビット アプリケーション

CA IAM CS は 64 ビット アプリケーションです。C++ Connector Server（CCS）は 32 ビット アプリケーションです。 64 ビット オペレーティング システムにインストールされる場合、CCS は 32 ビット アプリケーションとして実行されます。

一部のコネクタは、サードパーティ クライアントが CCS ホスト上に存在することを要求します。 たとえば、Oracle Applications は Oracle Client を必要とし、DB2 は DB2 Connect を必要とします。 これらのサードパーティ アプリケーションの一部には、32 ビットおよび 64 ビット モードの両方があります、 CCS でエンドポイントを管理する場合は、32 ビット クライアントをインストールします。

Linux の要件

Red Hat 5.x については、CA IAM CS 用のパッケージは不要です。Red Hat 6.x については、以下のパッケージを以下の順番でインストールします。

1. glibc-2.12-1.25.el6.i686.rpm
2. libX11-1.3-2.el6.i686.rpm
3. libxcb-1.5-1.el6.i686.rpm
4. libXtst-1.0.99.2-3.el6.i686.rpm
5. libXau-1.0.5-1.el6.i686.rpm
6. libXi-1.3-3.el6.i686.rpm
7. libXext-1.1-3.el6.i686.rpm
8. nss-softokn-freebl-3.12.9-3.el6.i686.rpm
9. libXmu-1.0.5-1.el6.i686.rpm
10. libXft-2.1.13-4.1.el6.i686.rpm
11. libXpm-3.5.8-2.el6.i686.rpm

非 FIPS モードインストールの場合、Linux では、エントロピーを生成する以下のコマンドが必要です。

```
/sbin/rngd -r /dev/urandom -o /dev/random -t 1
```

CA IAM CS のインストールが成功しない場合は、このコマンドを繰り返してください。

CA IAM CS のインストール

Java コネクタをホスト、ルーティング、管理するために、CA IAM CS をインストールします。 複数の CA IAM CS をインストールする場合は、追加のガイドラインとして、高可用性プロビジョニング インストールについての章を参照してください。

重要: CA IAM CS またはその SDK をインストールする前に、すべてのアンチウイルス ソフトウェアを無効にすることをお勧めします。 インストール プロセス中にアンチウイルス ソフトウェアが有効な場合、問題が発生するおそれがあります。 インストールの完了後に、忘れずに対ウイルス保護を再び有効にしてください。

次の手順に従ってください:

1. Windows 管理者、あるいは UNIX または Linux の root ユーザとしてシステムにログインします。
2. コネクタ サーバをホストするすべてのコンピュータの時間設定 (P. 121)が一致していることを確認します。
3. Linux システムについては、前提条件となるパッケージ (P. 123)がインストールされていることを確認します。
4. インストーラを起動します。

   すべての CA Identity Manager コンポーネントをインストールするメイン インストーラを使用して、CA IAM CS をインストールできます。 または、以下のサブフォルダに移動して、セットアップファイルを実行できます。

   ```
   Provisioning¥ConnectorServer
   ```
5. セットアップ タイプ（［Typical］または［Custom］）を選択します。［Typical］を選択した場合、インストール場所は変更できませんが、他はすべて変更できます。
6. インストール パスを入力します（［Custom］セットアップ タイプの場合のみ）。

7. Connector Server C++ Management を、以下のように設定します。
   - ［None］-- CCS をインストールしません。後から CCS をインストールする場合、CCS は CA IAM CS によって管理されません。
   - ［Local］-- CCS を CA IAM CS と同じコンピュータにインストールします。 CCS は CA IAM CS によって管理されます。
   - ［Remote］-- 既存のリモート CCS を管理するように CA IAM CS を設定します。
8. （推奨） CA IAM CS インストールをプロビジョニング サーバに登録してください。 詳細については、「プロビジョニング サーバの登録 (P. 128)」を参照してください。

   以下の情報を使用します。

   ドメイン

   プロビジョニング サーバのドメインを定義します。

   サーバ ホスト

   プロビジョニング サーバを定義します。

   サーバ ポート

   プロビジョニング サーバが実行されるポートを定義します。

   ユーザ名

   プロビジョニング サーバの管理者を指定します。

   パスワード

   プロビジョニング サーバの管理者パスワードを定義します。
9. （オプション）クラウド CA IAM CS に登録します。 クラウド バージョンのコネクタ サーバとオンプレミス バージョンを接続させると、2 つのコネクタ サーバは通信を行い、クラウドおよびオンプレミスのエンドポイントへの接続を管理することができます。

10. パスワードおよび以下のポートを設定します。

メッセージ ブローカー ポート

メッセージ ブローカーは、さまざまなコンピュータ上の CA IAM CS のインスタンス間のメッセージを送信します。

- HTTP ポート（デフォルト 22001）
- HTTPS ポート（デフォルト 22002）

Web ポート

以下のポートを使用し、Web インターフェースを介して CA IAM CS にログインできます。

- HTTP ポート（デフォルト 20080）
- HTTPS ポート（デフォルト 20443）

RMI レジストリ ポート

このポートを使用し、実行中の Java プロセスに関する情報を表示できます（デフォルト 1099）。

11. （オプション）HTTP プロキシを設定します。このプロキシの詳細は、以下の応用に使用できます。

    - クラウド コネクタ サーバと通信するとき。
    - Google Apps または Salesforce のエンドポイントを作成するとき。これらのエンドポイントについては、この HTTP プロキシを使用できるか、どのプロキシも使用できないかのいずれかです。 別のプロキシを指定できません。 HTTP プロキシ詳細を変更するには、再度このインストール プログラムを実行して、新しいプロキシ詳細を入力します。

    注: 組織がインターネットに直接接続している場合は、HTTP プロキシをセットアップしないことをお勧めします。

    以下の情報を使用して、HTTP プロキシをセットアップしてください。

    ホスト

    エンドポイントに接続するために使用する HTTP プロキシ サーバの名前を指定します。

    ポート

    CA IAM CS が HTTP プロキシにアクセスできるポートを指定します。

    ドメイン

    HTTP プロキシのドメインを指定します。

    ユーザ名

    プロキシ サーバにログインするために使用するユーザ名を指定します。

    注: 組織のプロキシ サーバが認証を必要とする場合は、ユーザ名とパスワードを指定することをお勧めします。

    パスワード

    HTTP プロキシのドメイン パスワードを指定します。

12. （オプション） FIPS 140-2 準拠モードをアクティブ化します。
13. ［次へ］をクリックします。

    インストール プログラムは CA IAM CS をインストールして、新規サービスを作成します。 Windows 上で、これはサービスに追加されます。また、UNIX 上で、これはスクリプトに相当します。

プロビジョニング サーバの登録

常にプロビジョニング サーバに CA IAM CS を登録することをお勧めします。 登録によって、プロビジョニング サーバに、インストールされた CA IAM CS を使用してそれに対して展開されたすべての静的なコネクタを管理させます。 別のコネクタ サーバに特定の静的または動的なコネクタを管理させる場合は、Connector Xpress を使用して、コネクタを管理する CA IAM CS のインスタンスを指定できます。

また、コネクタがすでに CA IAM CS の特定のインスタンスに展開されている プロビジョニング サーバにおいて、Connector Xpress を使用して新しい名前空間を作成することもできます。 バンドルされたテンプレート ファイルを使用するか、またはそれらが利用可能でない場合は、コネクタのメタデータをインポートしてプロジェクトを作成します。 メタデータが利用可能な場合は、新しい名前空間を展開します。

注: 詳細については、「Connector Xpress ガイド」を参照してください。

C++ Connector Server のインストール

CA IAM CS をインストールするときに、C++ Connector Server （CCS）をインストールできます。 このトピックでの手順は、単一コネクタ サーバにも適応できます。1 つまたは複数の CCS をインストールする予定がある場合は、高可用性プロビジョニングのインストールについての章を参照してください。

次の手順に従ってください:

1. インストール パッケージをアンパックしたところで、以下のプログラムを実行します。
   - **Windows の場合 :**
     `Provisioning¥Provisioning Server¥setup.exe`
   - **UNIX の場合 :**
     `Provisioning/ProvisioningServer¥setup.bin`
2. インストーラ ダイアログ ボックス内の手順を完了します。

   このインストール プログラムは、ユーザに代替 プロビジョニング サーバをインストールするオプションも与えます。 ただし、そのコンポーネントについては、別の手順が適用されます。

CA IAM CS のサイレント インストール

CA IAM CS をサイレント インストールできます。サイレント インストールを実行する前に、応答ファイルを作成します。

注: 応答ファイルの生成時および実行時には、完全修飾パス名を使用します。たとえば、responsefile.txt は有効ではありませんが、C :¥r esponsefile.txt は有効です。

次の手順に従ってください:

1. コマンド ウィンドウで、解凍されたインストール ファイル内の以下の場所に移動します。

   ```
   Servers/ConnectorServer
   ```

2. 応答ファイルを作成するには、以下のコマンドを入力してから、テンプレートに必要な値を入力します。

   ```
   setup –options-template filename
   ```

3. 以下のコマンドを使用して、サイレント インストールを開始します。

   ```
   setup –options filename -silent
   ```

注: 応答ファイルを作成し、同時に CA IAM CS をインストールするには、以下のコマンドを使用します。

```
setup -options-record filename
```

CA IAM CS 用 SDK のインストール

わかりやすい例を見てコネクタを書き込む方法について学習するには、CA IAM CS 用 SDK およびサンプル コネクタをインストールします。 これらの例については、「*Connectors Programming Guide*」で説明します

重要: CA IAM CS をインストールしたコンピュータとは別のコンピュータに SDK をインストールします。

次の手順に従ってください:

1. CA Identity Manager インストールのダウンロードまたは他のメディアを見つけて、製品ファイル（ZIP または TAR）を解凍します。
2. 以下のサブ フォルダに移動します。

   `Provisioning/ConnectorServerSamples`

   注: このフォルダ内の圧縮ファイル *jcs-connector-sdk* には SDK 自体が含まれます。他のファイルには、各々 1 つのサンプル コネクタが含まれます。
3. ファイルをこのフォルダから以下のサブフォルダにコピーします。

   `Provisioning/ConnectorServer`
4. CA IAM CS のインストール プログラムを実行します。

注: CA IAM CS 用 SDK の詳細については、*cs-sdk-home*/Readme.txt をご覧ください。

詳細情報:

ファイルの場所 (P. 122)

コネクタ サンプルのインストール

重要: テスト環境でのみサンプル コネクタを使用することをお勧めします。 サンプル コネクタはサポートされていません。 そのため、これらのサンプルのアンインストール プログラムはありません。

インストールを実行する前に、オペレーティング環境に対応するインストーラおよびサンプル アーカイブを同じフォルダに解凍します。

JDBC サポートのセットアップ

一部のコネクタは、ユーザ自身が JDBC 接続をアクティブにする必要があります。一部のドライバおよびライセンスを CA IAM CS と共に適法に出荷できないか、またはこれらのコネクタが有効化の前に追加の手動設定を必要とするため、インストーラによりこれらのコネクタをアクティブにすることができません。

重要: コネクタ サーバを新しいバージョンにアップグレードしたら、以下の手順を再度実行してください。

DB2 for z/OS コネクタ用ライセンス ファイルのセットアップ

DB2 for z/OS コネクタは JDBC を使用しますが、DB2 エンドポイントに接続するには、ライセンス ファイルが必要です。 ライセンス ファイルを利用できるのは、DB2 Connect のライセンスを持っている場合のみです。

詳細については、以下の IBM 技術情報を参照してください。

- IBM 技術情報： Location of the db2jcc_license_cisuz.jar file
- IBM 技術情報： DB2 JDBC driver is not licensed for connectivity

次の手順に従ってください：

1. CA IAM CS をインストールまたはアップグレードします。

   インストールでは CA IAM CS がプロビジョニング サーバと共に登録され、DBZ エンドポイント タイプを作成し、関連するメタデータを入力します。

2. DB2 Connect アクティベーション CD の以下の場所にある *db2jcc_license_cisuz.jar* を見つけます。

   `/db2/license`

3. ライセンス ファイルを CA IAM CS コンピュータの以下の場所にコピーします。

   cs_home`/jcs/resources/jdbc`

4. 同じ場所で *jdbc_db2_zos* スクリプトを実行します。

   このスクリプトは、ライセンス ファイルを含むバンドルを作成します。このバンドルは、CA IAM CS を使用して展開します。

5. CA IAM CS にログインします。
6. 一番上の［コネクタ サーバ］タブをクリックします。
7. ［コネクタ サーバ管理］領域で、［バンドル］タブをクリックします。
8. 新しいバンドルを追加します。

   注: コネクタ サーバ GUI から OSGI バンドルを展開するか、または ca-home/jcs/data/bundles/restore に jar ファイルをコピーできます。 次に、コネクタ サーバを再起動し、それがロードされるまで最大 10 分待機します。

   a. 右側の［バンドル］領域で、［追加］をクリックします。
   b. スクリプトが作成したバンドルを参照し、このコネクタが利用可能になるコネクタ サーバを選択します。

c. ［OK］をクリックします。

新しいバンドルが、［バンドル］リストに表示されます。

9. ［バンドル］リストからメイン コネクタ バンドルを探し、リストでその名前を右クリックし、ポップアップ メニューから［インポートのリフレッシュ］を選択します。

CA IAM CS は、DB2 エンドポイントに接続できるようになりました。

Sybase コネクタ用ライセンス ファイルのセットアップ

Sybase エンドポイントに接続するには、CA IAM CS では、JDBC 用 Sybase SDK のファイルが必要です。 また、Sybase のライセンスが必要です。

注: Sybase は DYN/JDBC エンドポイントとしてのみ管理できます。

次の手順に従ってください:

1. 以下のドライバ ファイルを見つけます。http://www.sybase.com からダウンロードできます。また、Sybase 製品のメディアにも含まれています。

   `jConnect-6_05.zip`

2. ZIP から以下のファイルを抽出します。

   `jConnect-6_0¥classes¥jconn3.jar`

3. jconn3.jar ファイルを以下の場所にコピーします。

   `conxp_home/lib/`

4. すべての Connector Xpress セッションを停止して再起動します。
5. コマンド ウィンドウで、以下の場所に移動します。

   `cs-home/jcs/resources/jdbc`

6. 以下のスクリプトを実行します。
   - Windows： jdbc_sybase_post_install.bat
   - UNIX： jdbc_sybase_post_install

   このスクリプトは、ライセンス ファイルを含むバンドルを作成します。このバンドルは、CA IAM CS を使用して展開します。
7. CA IAM CS にログインします。
8. 一番上の［コネクタ サーバ］タブをクリックします。
9. ［コネクタ サーバ管理］領域で、［バンドル］タブをクリックします。
10. 新しいバンドルを追加します。

    注: コネクタ サーバ GUI から OSGI バンドルを展開するか、または ca-home/jcs/data/bundles/restore に jar ファイルをコピーできます。 次に、コネクタ サーバを再起動し、それがロードされるまで最大 10 分待機します。

    a. 右側の［バンドル］領域で、［追加］をクリックします。

b. スクリプトが作成したバンドルを参照し、このコネクタが利用可能になるコネクタ サーバを選択します。

c. ［OK］をクリックします。

新しいバンドルが、［バンドル］リストに表示されます。

11. ［バンドル］リストからメイン コネクタ バンドルを探し、リストでその名前を右クリックし、ポップアップ メニューから［インポートのリフレッシュ］を選択します。

CA IAM CS は、Sybase エンドポイントに接続できるようになりました。

SQL Server コネクタの Windows 認証をセットアップ

Windows 上での Microsoft SQL ネイティブ認証をアクティブ化できるのは、Connector Xpress および CA IAM CS の両方が Windows オペレーティング システム上で実行されている場合のみです。 必要なライブラリ sqljdbc_auth.dll は、Connector Xpress にバンドルされています（Microsoft の Web サイトからダウンロードすることもできます）。

Connector Xpress の使用を予定している場合は、Microsoft SQL Server エンドポイントと同じドメインで Connector Xpress を実行する必要があります。また、適切なデータベース インスタンスにアクセスできるように、SQL Server を設定しておく必要があります。

次の手順に従ってください:

1. 必要な Windows ユーザとして実行するように CA IAM CS サービスを更新します。

   デフォルトでは、このサービスは、ローカル システム ユーザとして実行するように設定されています。 ただし、信頼できる認証を使用している場合は、ドメイン ユーザとしてサービスを実行します。以下の手順を実行します。

   a. ［スタート］-［コントロール パネル］-［管理ツール］-［サービス］をクリックします。

   b. ［CA Identity Manager-Connector Server (Java)］を右クリックして、［プロパティ］を選択します。

   c. ［アカウント］チェック ボックスをオンにし、サービスを実行するドメイン ユーザの詳細を入力します。

2. CA IAM CS サービスを停止して再起動します。

3. Connector Xpress で Microsoft SQL データ ソースをセットアップする場合は、［Edit Sources］ダイアログ ボックスの［Native］チェック ボックスをオンにします。

   Connector Xpress は、接続に使用される JDBC URL に以下を追加します。

   ```
   integratedSecurity=true
   ```

   注: データ ソースの設定の詳細については、「Connector Xpress ガイド」を参照してください。

コネクタのセットアップに関する詳細情報

コネクタおよび必須コンポーネントの詳細については、「コネクタ ガイド」を参照してください。 このガイドでは、どのコンポーネントをどこにインストールするかについて説明し、各エンドポイント タイプの特定の手順についても説明します。

第 8 章: 高可用性プロビジョニングのインストール

この章のガイドラインに基づいて、代替プロビジョニング サーバとプロビジョニング ディレクトリ、および C++ コネクタと Java コネクタ用のコネクタ サーバをインストールすることにより、プロビジョニング コンポーネントの高可用性を実装してください。

このセクションには、以下のトピックが含まれています。

インストール ステータス

以下の表は、インストール プロセスのどこにいるかユーザに示します。

現時点	インストール プロセスの手順
	1. 前提条件のハードウェアおよびソフトウェアをインストールし、必要なシステムを設定します。
	2. 以下のインストールのいずれかを実行します。 ■ 単一ノード インストール ■ アプリケーション サーバ クラスタ上のインストール
	3. （オプション）別個のデータベースを作成します。
	4. （オプション）レポート サーバをインストールします。
X	**5. （オプション）代替プロビジョニング ディレクトリ、代替プロビジョニング サーバ、およびコネクタ サーバをインストールして、フェイルオーバと負荷分散をサポートします。**

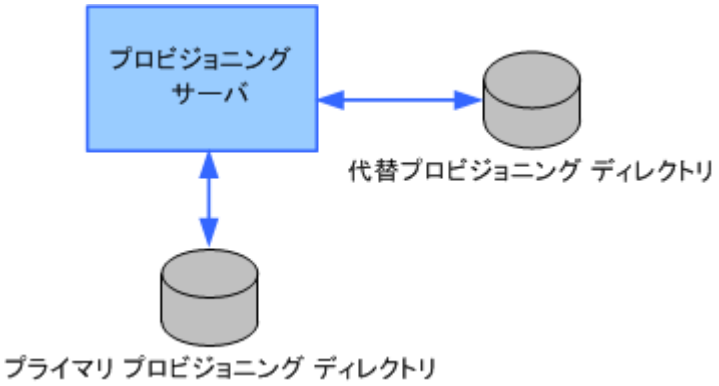
高可用性プロビジョニング コンポーネントをインストールする方法

以下の表では、高可用性のプロビジョニング コンポーネントのインストールに関連する手順について説明します。

✓	手順
	1. 負荷分散とフェイルオーバのためにプライマリと代替のプロビジョニング サーバおよびプロビジョニング ディレクトリをインストールします。
	2. 負荷分散とフェイルオーバのために複数のコネクタ サーバをインストールします。
	3. プロビジョニング サーバのクライアントをフェイルオーバできるようにします。

冗長プロビジョニング ディレクトリ

フェイルオーバをサポートするために、プライマリおよび代替のプロビジョニング ディレクトリをインストールできます。たとえば、プロビジョニング サーバとプライマリ プロビジョニング ディレクトリのある 2 つのシステムがある場合が考えられます。 別のシステムに、代替プロビジョニング ディレクトリがあります。プライマリ プロビジョニング ディレクトリが失敗すると、代わりのプロビジョニング ディレクトリが自動的に割り当てられます。



次の手順に従ってください:

1. インストール パッケージをアンパックした場所からプロビジョニング ディレクトリ インストーラを使用して、プライマリ プロビジョニング ディレクトリをインストールします。
   - **Windows の場合：**
     UnpackedInstall-Package¥Provisioning¥Provisioning Directory¥setup.exe
   - **UNIX の場合：**
     Unpacked-Install-Package/Provisioning/ProvisioningDirectory/setup
2. 1 つ以上の代替プロビジョニング ディレクトリをインストールします。次のセクションを参照してください。

代替プロビジョニング ディレクトリのインストール

必要な前提条件設定を完了したら、代替プロビジョニング ディレクトリをインストールできます。

次の手順に従ってください:

1. 代替プロビジョニング ディレクトリをインストールする予定のシステムに ローカル管理者（Windows の場合）または root（Solaris の場合）としてログインします。
2. そのシステムに CA Directory がインストールされていることを確認します。
3. プライマリ プロビジョニング ディレクトリについて以下のいずれかが該当する場合、%DXHOME%/config/schema ディレクトリにカスタム スキーマ ファイルをコピーします。
   - COSX （etrust_cosx.dxc）が変更されている
   - LDA コネクタ（etrust_lda.dxc）がインストールされている
   - カスタム C++ コネクタ スキーマが作成されている

   プロビジョニング ディレクトリのインストールでは、etrust_*.dxc という名前の付いたエキストラのスキーマ ファイルについて %DXHOME%/config/schema ディレクトリをチェックし、それらをグループ スキーマ ファイル、impd.dxg に追加します。 カスタム スキーマ ファイルがローカルにコピーされていないと、プロビジョニング ディレクトリ間のデータ レプリケーションは失敗します。

4. インストール パッケージをアンパックした場所からプロビジョニング ディレクトリ インストーラを実行します。
   - **Windows の場合：**
     UnpackedInstall-Package¥Provisioning¥Provisioning Directory¥setup.exe
   - **UNIX の場合：**
     Unpacked-Install-Package/Provisioning/ProvisioningDirectory/setup
5. ［High Availability］を選択し、他のプロビジョニング ディレクトリがインストールされているシステムのホスト名、およびどのシステムがプライマリ プロビジョニング ディレクトリであるかについて回答します。
6. プライマリ プロビジョニング ディレクトリのインストール時と同じ回答を用い、以下に関する質問に答えます。
   - 展開サイズ
   - 共有秘密キー
   - FIPS キー
7. プライマリ プロビジョニング ディレクトリ からデータをレプリケートする方法および時期に基づいて、以下の質問に答えます。
   プロビジョニング ディレクトリへのレプリケーションを開始しますか。

   以前のリリースからアップグレードしている場合は、レプリケートすべき多量のデータがある場合があります。 レプリケーションをこの時点で開始しない場合は、チェック ボックスをオフにする必要があります。その場合はインストール後に、既存のプロビジョニング ディレクトリから LDIF データ ダンプまたはオンライン バックアップ ファイルをコピーしてそのデータをロードするか、または手動で DSA を開始し、これにより自動レプリケーションを開始する必要があります。

重要: 代替プロビジョニング ディレクトリのインストールが失敗したときは、その前にデータ レプリケーションに問題が発生している可能性があります。 この場合、マスタおよび代替プロビジョニング ディレクトリに、レプリケーションが発生したというレコードがあります。 この時点で代替プロビジョニング ディレクトリを再インストールすると、そのデータはまたレプリケートされません。 代わりに、再インストールする前に、プライマリおよび代替プロビジョニング ディレクトリで高可用性設定コマンドを使用して、代替プロビジョニング ディレクトリを削除し、復元します。

プロビジョニング ディレクトリを持つシステムの再設定

必要に応じて、プロビジョニング ディレクトリを持たせるシステムの設定を変更できます。

次の手順に従ってください:

1. プライマリ プロビジョニング ディレクトリがインストールされているシステムにログインします。
2. コマンド ライン プロンプトで、プロビジョニング ディレクトリをインストールした、高可用性サブディレクトリに移動します。 以下に例を示します。

   ```
   cd C:¥¥Program Files¥CA¥Identity Manager¥Provisioning Directory¥highavailability
   ```

3. 以下のコマンドを入力します。

   ```
   highavailability.bat
   ```

   このコマンドは、次を含む現在の設定のサマリを表示します。ドメイン名、プロビジョニング サーバおよびプロビジョニング ディレクトリのそれぞれのホスト名、ならびにどれがプライマリ プロビジョニング ディレクトリであるか。
4. 追加予定の各代替プロビジョニング ディレクトリのホスト名のプロンプトに応じます。

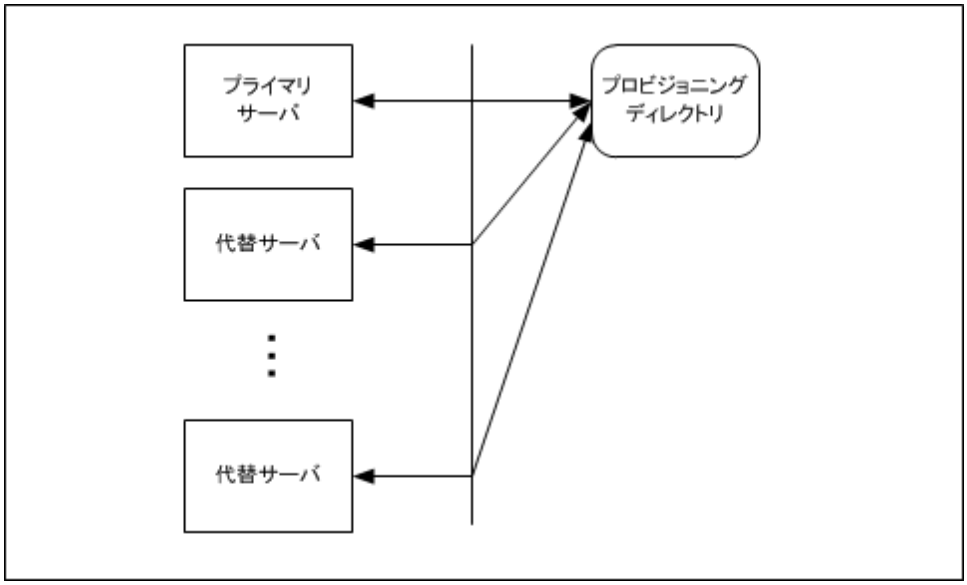
   代替プロビジョニング サーバをインストールする予定の場合は、プロンプトに応答してそれらのホスト名を追加できます。
5. 他のすべてのプロビジョニング ディレクトリとプロビジョニング サーバにログインし、手順 2 ～ 4 を繰り返します。

   各システムの設定は一致する必要があります。

冗長プロビジョニング サーバ

複数のプロビジョニング サーバは、プロビジョニング ドメインの作業負荷を共有して、優れたパフォーマンス、拡張性、および高可用性を提供します。 最初にインストールされたプロビジョニング サーバを、プライマリ プロビジョニング サーバと呼びます。追加のサーバを、代替プロビジョニング サーバと呼びます。

この図で表示されるように、1 つのプライマリプロビジョニング サーバに対して複数の代替プロビジョニング サーバを設定できます。



この図では、3 つのプロビジョニング サーバがプロビジョニング ドメインをサーブするよう設定されています。 すべてのサーバは、プライマリ プロビジョニング サーバ インストールのプロビジョニング ディレクトリを使用するように設定されています。

プロビジョニング サーバのルータ DSA

プロビジョニング サーバは、CA Directory ルータ DSA を介し、プロビジョニング ディレクトリと直接ではなく通信します。ルータ DSA、imps-router は、プロビジョニング サーバ インストーラでインストールされます。 この DSA はプロビジョニング サーバからリクエストを受理し、プレフィックスに応じた適切なプロビジョニング ディレクトリ DSA （impd-co、impd-main、impd-inc、または impd-notify）にルーティングします。

高可用性インストールでは、imps-router DSA は、少なくとも 1 つの代替プロビジョニング ディレクトリ システム上のプロビジョニング ディレクトリ DSA の接続情報を持っています。 プライマリ プロビジョニング ディレクトリ DSA が利用不可になると、ルータ DSA は代替 DSA の使用を試行します。

imps-router DSA は、ポート 20391、20391、20393（それぞれアドレス、SNMP、コンソール用）を割り当てられています。

注: このソフトウェアの以前のリリースでは、etrustadmin DSA がポート 20391 を使用していました。プロビジョニング ディレクトリおよびプロビジョニング サーバが同じシステム上にない場合、プロビジョニング ディレクトリ システム上の 20391 に対する接続は失敗します。 そのため、プロビジョニング サーバ システム上のポート 20391 へのこれらの接続の経路を変更します　。

1 つのシステム上で実行されている CA Directory DSA が別のシステム上の DSA と通信するためには、それらが互いの接続情報を持っている必要があります。したがって、プロビジョニング ディレクトリのインストール中、それに接続できる各プロビジョニング サーバを確認してください。

プロビジョニング サーバのインストール

フェイルオーバをサポートするために、プライマリおよび代替のプロビジョニング サーバをインストールできます。

次の手順に従ってください:

1. インストール パッケージをアンパックした場所からプロビジョニング サーバ インストーラを使用して、プライマリ プロビジョニング サーバをインストールします。
   - **Windows の場合**:
     Unpacked-Install-Package¥Provisioning¥Provisioning Server¥setup.exe
   - **UNIX または Linux の場合**:
     Unpacked-Install-Package/Provisioning/ProvisioningServer/setup
2. 1 つ以上の代替プロビジョニング サーバをインストールします。 次のセクションを参照してください。
3. CA Identity Manager 管理コンソールのプロビジョニングを有効にしたら、代替プロビジョニング サーバのホストとポート番号を入力します。詳細については、「*設定ガイド*」を参照してください。

代替プロビジョニング サーバのインストール

高可用性コマンドに含まれる前提条件設定を実行すると、1 つ以上のプロビジョニング サーバをインストールできます。

次の手順に従ってください:

1. 代替プロビジョニング サーバをホストする各システムに、ローカル管理者（Windows の場合）または root （Solaris の場合）としてログインします。
2. このシステムに CA Directory がインストールされていることを確認します。
3. プライマリ プロビジョニング ディレクトリに対して以下のいずれかが該当する場合、%DXHOME%/config/schema ディレクトリにカスタム スキーマ ファイルをコピーします。
   - COSX （etrust_cosx.dxc）が変更されている
   - LDA コネクタ（etrust_lda.dxc）がインストールされている
   - カスタム C++ コネクタ スキーマが作成されている

   プロビジョニング ディレクトリのインストールでは、etrust_*.dxc という名前の付いたエキストラのスキーマ ファイルについて %DXHOME%/config/schema ディレクトリをチェックし、それらをグループ スキーマ ファイル、impd.dxg に追加します。 カスタム スキーマ ファイルがローカルにコピーされなければ、プロビジョニング サーバはカスタム スキーマをルーティングしません。
4. インストール パッケージをアンパックした場所からプロビジョニング サーバ インストーラを実行します。
   - **Windows の場合**：
     Unpacked-Install-Package¥Provisioning¥Provisioning Server¥setup.exe
   - **UNIX の場合**：
     Unpacked-Install-Package/Provisioning/ProvisioningServer/setup
5. インストーラ ダイアログ ボックス内の手順を完了します。

   インストール中にチェック ボックスをオンにして、プロビジョニング ディレクトリ高可用性を設定できます。 このオプションを選択する場合、すべての代替プロビジョニング ディレクトリのホスト名を入力し、プライマリ プロビジョニング ディレクトリを指定する必要があります。

プロビジョニング サーバを持つシステムの再設定

必要に応じて、プロビジョニング サーバを持たせるシステムの設定を変更できます。

次の手順に従ってください:

1. プライマリ プロビジョニング ディレクトリがインストールされているシステムにログインします。
2. コマンド ライン プロンプトで、プロビジョニング ディレクトリまたはプロビジョニング サーバをインストールした場所に移動します。その場所で、高可用性サブディレクトリを見つけます。 以下に例を示します。

   ```
   cd C:¥¥Program Files¥CA¥Identity Manager¥Provisioning Directory¥highavailability
   ```

3. 以下のコマンドを入力します。

   ```
   highavailability.bat
   ```

   このコマンドでは、ドメイン名、各プロビジョニング サーバおよびプロビジョニング ディレクトリのホスト名など、現在の設定の概要が表示されます。
4. プロンプトに応答して、追加するプロビジョニング サーバごとに必要なホスト名を指定します。

   代替プロビジョニング ディレクトリもインストールする場合は、プロンプトに応答してホスト名を追加できます。
5. プロビジョニング ディレクトリをホストする各システムにログインし、手順 2 ～ 4 を繰り返します。

   各システムの設定は一致する必要があります。

プロビジョニング サーバのフェイルオーバの設定

CA Identity Manager がプライマリ プロビジョニング サーバと代替プロビジョニング サーバを識別するために、管理コンソールの JIAM でサーバ定義を作成します。 ユーザの環境の CA Identity Manager ディレクトリと関連付けられたディレクトリ オブジェクトでこれらの定義を作成します。初期化中、CA Identity Manager は、そのオブジェクトで定義されたどのフェイルオーバ サーバ定義も読み取り、JIAM フェイルオーバ サーバ定義にそれらを追加します。

注: サーバ定義をセットアップする詳細については、「*設定ガイド*」を参照してください。

冗長コネクタ サーバ

コネクタ サーバ フレームワーク（CSF）を使用して、複数のコネクタ サーバを実行し、固有のコンテキストでコネクタ サーバと通信するようにプロビジョニング サーバを設定できます。

その結果、プロビジョニング サーバは以下のことができます。

- プロビジョニング サーバがインストールされているプラットフォームでは利用できないエンドポイント タイプを管理するために、別のプラットフォーム上のコネクタ サーバをサポートします。
- 異なるエンドポイント タイプまたはエンドポイントのセットをそれぞれ管理する複数のコネクタ サーバと通信します。 これにより、エンドポイント タイプまたはエンドポイントを並列に管理して、負荷分散を達成できます。

コネクタ サーバ フレームワーク

複数のコネクタ サーバの使用は、コネクタ サーバ フレームワークと呼ばれます。 コネクタ サーバ フレームワークには、以下の 2 つの重要な特性があります。

- 拡張性 - マルチコネクタ サーバは、1 組のエンドポイント上で作業のロードを共有することができます。

  たとえば、1 つのコネクタ サーバ上のエンドポイント上での長時間の検索は、別のコネクタ サーバによって制御されているエンドポイント上での操作機能に影響を及ぼしません。

- 通信チャネルのセキュリティ - プロビジョニング サーバおよびコネクタ サーバの間の通信は、TLS を使用して暗号化されます。

  エンドポイント タイプが専用プロトコルを使用して、そのプロトコルのコネクタ サーバとエンドポイント間で通信する場合、専用プロトコルの使用範囲はローカル ネットワークどころか、1 つのサーバ内部のローカル通信のみに制限されることがあります。

実装戦略を決めるとき、不正なアクセスから組織内のコネクタ サーバを保護するために、以下の要因を考慮してください。

- コネクタ サーバは、クリア テキストでパスワードを開示するように設定されていることがあります。

  コネクタ サーバを実行するシステムへのアクセス権限、およびコネクタ サーバの設定を変更して。コネクタ サーバを再起動するのに十分な権限を持つどのユーザも、クリア テキストでコネクタ サーバ ログ パスワードを表示させることができます。

  コネクタ サーバは、オープン ソース slapd プロセスに基づいています。slapd プロセス ログをクリア テキストの受信パスワードにする手順は、パブリック ドメイン、たとえば、http://www.openldap.org のマニュアル ページで参照できます。

- コネクタ サーバは、バインド パスワードによってのみ保護されます。

  コネクタ サーバは、それに接続し、Bind DN および Bind パスワードなど適切なクレデンシャルを提供できるあらゆるクライアントを信頼します。 コネクタ サーバは、その接続がプロビジョニング サーバからなのか、またはそうではないのか識別しません。 内部アクセス権限を持つどのユーザも、バインド パスワードを開示し、別のサーバからコネクタ サーバに接続することができるので、そのコネクタ サーバで制御されているエンドポイントに対して管理者権限を持ちます。

- コネクタ サーバはバインド パスワードへの総当り攻撃から保護されていません。

  プロビジョニング サーバと異なりコネクタ サーバは、さまざまなパスワードを用いたバインドの反復試行から保護されていません。そのため、攻撃者は、総当り攻撃によってパスワードを推測できる場合があります。攻撃者がバインド パスワードの推測に成功すると、ロードは攻撃者に対して開かれ、このコネクタ サーバの管理下のエンドポイントを制御できます。

これらの理由により、以下のように実装を設計するようお勧めします。

- 同じ組織単位が、すべてのプロビジョニング サーバおよびコネクタ サーバへの管理アクセスを担当する。
- ユーザのコネクタ サーバはファイアウォールによって適切に保護され、非認可の手段によってポートに到達できないようになっている。
- 非 TLS ポート上のプロビジョニング サーバおよびコネクタ サーバに接続する機能は、実稼働環境で無効化されている必要があります。

複数のコネクタ サーバを 1 台のコンピュータにインストールする場合は、各インスタンスがそれぞれポート番号の一意のセットを使用することを確認します。

負荷分散およびフェイルオーバ

コネクタ リクエストのフェイルオーバおよび負荷分散は、csfconfig または Connector Xpress を使用して定義された CSF 設定に基づいて各プロビジョニング サーバによって達成されます。

各プロビジョニング サーバは、それに適用され、各エンドポイントまたはエンドポイント タイプにアクセスするにはどのコネクタ サーバを使用する必要があるか決定する CSF 設定を確認します 同じエンドポイントまたはエンドポイント タイプをサーブするように設定された複数のコネクタ サーバが存在するとき、フェイルオーバと負荷分散が発生します。

フェイルオーバと負荷分散は一体になっていて、別々に制御できません。フェイルオーバが必要なとき以外、特定のコネクタ サーバがアイドル状態のままであるように指示できません。 そうではなく、2 つ以上のコネクタ サーバを交互に使用するように設定されているプロビジョニング サーバは、通常動作中にこれらのコネクタ サーバに作業を分散します（負荷分散）。 コネクタ サーバの 1 つまたは複数が利用不可になると、残るコネクタ サーバが利用不可なコネクタ サーバにフェイルオーバ サポートを提供します。

信頼性および拡張性

コネクタ サーバ フレームワーク（CSF）により、コネクタ サーバ高可用性機能は、信頼性および拡張性を強化します。

複数のコネクタ サーバにプロビジョニング サーバを対応させることにより、信頼性は増加し、1 つ以上のコネクタ サーバが利用不可になってもプロビジョニング サーバの機能を続行できます。

たとえば、1 つのコネクタ サーバが UNIX エンドポイント タイプを管理し、別のコネクタ サーバが Active Directory エンドポイント タイプを管理し、Active Directory コネクタ サーバは利用不可になった場合、プロビジョニング サーバは今までどおり UNIX エンドポイント タイプを管理できます。

拡張性は、増加するエンドポイント タイプまたはエンドポイントを管理するためにより多くのコネクタ サーバを追加するメカニズムを備えることにより達成されます。たとえば、エンドポイントの数が 100 に増加した場合、プロビジョニング サーバを、20 のコネクタ サーバを持ち、各コネクタ サーバが 5 つのエンドポイント タイプを管理するように設定できます。 または、各コネクタ サーバがフェイルオーバと負荷分散の動作に対して同様に許可するように 10 のエンドポイント タイプの重複セットを管理する、20 個のコネクタ サーバを設定します。

Multi-Platform のインストール

コネクタ サーバ フレームワークは、複数システム上に存在するコネクタ サーバの設定で、システムは Wndows または Solaris システムです。

以下のユース ケースがサポートされています。

- ユース ケース 1
  - プロビジョニング サーバおよびコネクタ サーバは、Solaris システム上にインストールされました。
  - 別のコネクタ サーバは、Windows システムにインストールされ、非マルチプラットフォーム コネクタをサーブしています。

- ユース ケース 2
  - プロビジョニング サーバおよびコネクタ サーバは、Wndows システムにインストールされました。
  - 2 番目のコネクタ サーバは、Solaris システムにインストールされ、マルチプラットフォーム コネクタをサーブします。
  - 3 番目のコネクタ サーバは、リモート Windows システムにインストールされ、他のコネクタをサーブします。
- ユース ケース 3
  - プロビジョニング サーバは、Windows または Solaris システムにインストールされました。また、Connector Server は同じシステムにインストールされました。
  - 複数の追加のコネクタ サーバは、Windows または Solaris システム上にインストールされ、エンドポイント エージェントとしてサーブ。 このシナリオは、コネクタが専用または安全でない通信チャネルを使用しているケースで重要です。このトポロジを使用して、ネットワーク トラフィックの重要なセグメントは、専用のプロトコルによってではなく、ネクタ サーバに対するプロビジョニング サーバの標準的な通信プロトコルによって保護されます。

C++ Connector Server のインストール

CA IAM CS をインストールするときに、C++ Connector Server （CCS）をインストールできます。 このトピックでの手順は、単一コネクタ サーバにも適応できます。1 つまたは複数の CCS をインストールする予定がある場合は、高可用性プロビジョニングのインストールについての章を参照してください。

次の手順に従ってください:

1. インストール パッケージをアンパックしたところで、以下のプログラムを実行します。
   - **Windows の場合 :**
     `Provisioning¥Provisioning Server¥setup.exe`
   - **UNIX の場合 :**
     `Provisioning/ProvisioningServer¥setup.bin`
2. インストーラ ダイアログ ボックス内の手順を完了します。

   このインストール プログラムは、ユーザに代替 プロビジョニング サーバをインストールするオプションも与えます。 ただし、そのコンポーネントについては、別の手順が適用されます。

コネクタ サーバの設定

csfconfig コマンドの使用により、または Connector Xpress の使用によりコネクタ サーバ フレームワークを設定します。 csfconfig コマンドは、プロビジョニング サーバに接続するための Windows レジストリ（またはプロビジョニング サーバに対して作成された UNIX 相当物）内のデータを使用します。 csfconfig コマンドは、1 つのプロビジョニング サーバが実行されるシステム上で実行される必要があります。

このコマンドを使用して、以下の処理を実行できます。

- コネクタ サーバ、ホストおよびポートなどの情報を持つコネクタ サーバ接続オブジェクトを追加または変更します。
- コネクタ サーバがどのエンドポイントまたはエンドポイント タイプに使用されるか定義します。これにより、代替プロビジョニング サーバのこの定義を変える場合もあります。
- コネクタ サーバ接続情報オブジェクトを削除します。

- ドメインのコネクタ サーバ接続オブジェクトをすべてリスト表示します。
- 1 つまたはすべてのコネクタ サーバの 1 つまたはすべてのコネクタ サーバ接続オブジェクトを表示します。

csfconfig コマンドは、グローバル ユーザ クレデンシャルによって提供される認可を使用します。そのため、グローバル ユーザは、適切な ConfigParam および ConfigParamContainer オブジェクトを操作するために必要な管理者権限を有する必要があります。

csfconfig Command

csfconfig コマンドを使用するためのコマンド ライン構文は以下のとおりです。

```
csfconfig [--help[=op]] [operation] [argument]
```

これらのフラグは任意の順で指定できます。ユーザが --help 引数を使用していない場合、操作引数は必要です。

--help［=op］オプションは最小のオンライン ヘルプを提供します。「=op」引数は、操作に必要かまたはオプションの引数をリスト表示するために使用され得ます。 たとえば、「--help=add」は、加算操作の説明を提供します。その一方で「--help」は一般情報を提供します。

ヘルプがリクエストされている場合、他の引数は無視され、リクエストはサーバに送信されません。

注: ドメイン パラメータは、それが常に全体のインストールで使用されるドメインである場合、省略できます。

以下のパラメータが使用可能です。

add

新しい CS 接続オブジェクトを追加します。 名前は、1 つがユーザによって指定されなければ、この操作によって生成されます。 必要な引数: authhost、pass。 オプションの引数: authpwd、br-add、desc、domain、name、 port、 usetls、 debug。

addspec

1 つのプロビジョニング サーバに対するブランチの特殊化を追加します。

ユーザが代替プロビジョニング サーバをインストールした場合、コネクタ サーバがこれらのすべてプロビジョニング サーバ用に使用されないことがあります。 または、さまざまなプロビジョニング サーバが、さまざまなブランチ（エンドポイント タイプまたはエンドポイント）用の同じコネクタ サーバを使用することがあります。 ブランチの特殊化は、1 つのプロビジョニング サーバに固有のブランチのリストです。 特殊化のないプロビジョニング サーバのみが、メイン CS 接続オブジェクトで指定されたブランチを使用します。 必要な引数： auth、name、server。 オプションの引数： authpwd、br-add、domain、debug。

list

CS 接続オブジェクトをすべてリスト表示します。 必要な引数： auth。 オプションの引数： authpwd、domain、debug。

modify

CS 接続オブジェクトを変更します。 必要な引数： auth、name。 オプションの引数： authpwd、br-add、br-rem、desc、domain、host、pass、port、 usetls、 debug。

modspec

addspec によって作成された特殊化を編集します。必要な引数: auth、name、server。 オプションの引数: authpwd、br-add、br-rem、domain、debug。

remove

既存の CS 接続オブジェクトを削除します。必要な引数: auth、name。 オプションの引数： authpwd、debug。

remspec

addspec によって作成された特殊化を削除します。必要な引数: auth、name、server。 オプションの引数： authpwd、domain、debug。

modify

CS 接続オブジェクトを変更します。 必要な引数： auth、name。 オプションの引数： authpwd、br-add、br-rem、desc、domain、host、pass、port、server、tls、usetls。

show

特定の CS 接続オブジェクトを表示するか、または CS 接続オブジェクトをすべて表示します。その出力は、コネクタ サーバのホストおよびポートを表示します（利用可能な場合）。 必要な引数： auth オプションの引数： authpwd、name、domain、debug。

各操作は、「name=value」の形式の複数の引数をとります。スペースは「=」記号の前またはこの記号の後に許可されません。また、値にスペースが含まれる場合、引数はプラットフォーム（Windows または UNIX）用に適切に引用される必要があります。 記述されているものを除き、値は提供され、空でない必要があります。

上述したように、以下の引数が操作に使用されます。

auth=<value>

認証のためにグローバル ユーザを識別します。

値形式： 「name」（name はグローバル ユーザの名前です。）

authpwd=<value>

最初の行上にグローバル ユーザのパスワードを含むファイルを識別します。 この引数が指定されないと、ユーザはパスワードを求められます。

値形式： 任意の適切なオペレーティング システム ファイル パス。

br-add=<value>

新しいブランチ グループを追加します。この引数は、複数のブランチを追加するために、複数回指定される場合があります。

値形式： 「[[endpoint,]endpoint type][@[domain]]」。 すべてのブランチを表すには、「@」単独のブランチを使用します。 特定のエンドポイント タイプまたはエンドポイントを識別するには、「endpoint type」または「endpoint,endpoint type」を追加します。

br-rem=<value>

既存のブランチを削除します。 この引数は、複数のブランチを削除するために、複数回指定される場合があります。

値形式： br-add について指定された形式と同じです。

debug=<value>

コマンドのトレース ログ記録をオンにします。 トレースするメッセージは、ファイル SHOME¥logs¥etaclientYYYYMMDD.log ファイルに書き込まれます。

値形式： 値「yes」はログ記録を有効にします。

desc=<value>

オブジェクトの任意の説明を提供します。加算操作で指定されない場合、これがホスト引数の値のデフォルトになります。

値形式： 任意の文字列。

domain=<value>

デフォルト ドメインを定義します。指定されない場合、認証引数で指定されたドメインがデフォルトとして使用されます。

この値のみがデフォルトになり得るので、このパラメータは常に省略できます。

host=<value>

コネクタ サーバを実行するホストの名前を定義します。

値形式： 任意の正しいホスト名または IP アドレス。

name=<value>

コネクタ サーバの名前を定義します。 Add の中で指定されなければ、csfconfig は名前を割り当てて、作成された名前を表示します。

値形式： 大文字の英語文字（A-Z）、小文字の英語文字（a-z）、数字（0-9）、ハイフン（-）、またはアンダースコア（_）から構成される、大文字と小文字を区別しない 1 字以上の文字列。

pass[=<value>]

コネクタ サーバ接続オブジェクトのパスワードが含まれるファイルを定義します。 値が指定されない場合、プロンプトが表示されます。

値形式： 任意の適切な OS ファイル パス。

重要: 指定する必要があるパスワードは、そのコネクタ サーバをインストールしたときに入力したパスワード、またはインストール後にそのコネクタ サーバシステムで pwdmgr ユーティリティを実行してユーザが変更したパスワード。

port=<value>

オブジェクトのポート番号を定義します。これは、コネクタ サーバが接続をリスンするポートの有効な数である必要があります。

値形式： 整数。

server[=<value>]

addspec、modspec および remspec コマンドで、コネクタ サーバによってサーブされるプロビジョニング サーバの名前を定義します。特殊化が上書きで定義されたブランチ、特定のプロビジョニング サーバについては、add または modify コマンドで CS 設定オブジェクトに定義されたブランチ。

値形式： システムのホスト名コマンドによって返される、プロビジョニング サーバが実行されているホストの名前です。

注: コネクタ サーバ設定オブジェクトは、他のドメイン設定パラメータと共にプロビジョニング ディレクトリに格納されます。 プロビジョニング マネージャでコネクタ サーバ設定パラメータを直接に表示できないか、または変更できない一方で、プロビジョニング マネージャ（システム タスク、ドメイン設定ボタン）を使用して既知のプロビジョニング サーバのリストを取得できます。 リストを開くには、「Servers」パラメータ フォルダを開きます。そうすれば、既知のプロビジョニング サーバがリスト表示されます。

usetls[=<value>]

コネクタ サーバと通信するために TLS が使用されるべきかどうかを示します。値は操作の追加に対してのみのオプションであり、その場合、「yes」がデフォルトになります。

値形式： 文字列の「yes」または「no」。

操作の追加が正常に完了すると、新しく作成された コネクタ サーバ接続オブジェクトの名前がリスト表示されます。 name パラメータがない場合、名前が生成されます。 以下に例を示します。

```
Created CS object with name = SA000
```

ほとんどの操作に対して、成功してもしなくても、ステータスおよびメッセージ（もしあれば）が表示されます。 以下に例を示します。

```
ホスト名、ポート番号、または TLS フラグが正常に変更されました。 ブランチ設定は正常に変更されました。
```

無効なコマンド ライン パラメータなどいくつかのエラーについては、ステータス コードまたはサーバ エラー メッセージが表示されません。 これらの場合で、エラーの単純なステートメントが表示されます。 以下に例を示します。

```
$ csfconfig add
No authentication information supplied.
For on-line help, use "--help [=<op>]
```

csfconfig コマンドの例

UNIX および CA Access Control エンドポイント タイプが、ホスト「sunserver01」上で実行されるコネクタ サーバに処理され、残るエンドポイント タイプがホスト「windows02」上で実行される コネクタ サーバに処理されるよう指定するには、以下のコマンドを発行します。

各コマンド実行の際は、ユーザに etaadmin パスワードを求めるプロンプトが表示されます。

```
csfconfig add ¥
auth=”etaadmin” ¥
br-add=”UNIX – etc” ¥
br-add=”UNIX – NIS-NIS plus Domains” ¥
br-add=”Access Control” ¥
host=”sunserver01” ¥
usetls=”yes”

csfconfig add ¥
auth=”etaadmin” ¥
br-add=”@” ¥
host=”sunserver01” ¥
usetls=”yes”
```

Solaris 上の C++ コネクタ サーバ

Solaris にインストールされた C++ コネクタ サーバは Solaris UNIX ETC および ACC のエンドポイントしか管理できません。 他のすべての コネクタについては、Windows システムに C++ コネクタ サーバをインストールして、Solaris 上のプロビジョニング サーバに登録してください。 この コネクタ サーバはインストール時にデフォルトの C++ コネクタ サーバとして指定します。

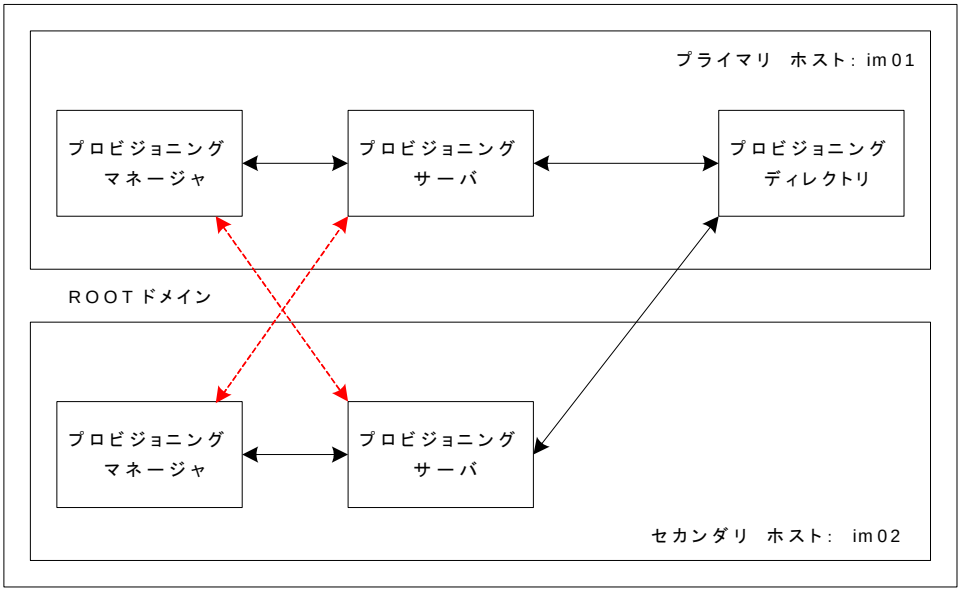
プロビジョニング クライアントのフェイルオーバ

ポリシー サーバ設定には、以下のタスクが含まれます。

- Windows クライアント層フェイルオーバの設定
- ローカル プロビジョニング サーバと通信し、リモート プロビジョニング サーバにフェイルオーバするためのプロビジョニング マネージャの設定

同じ［プロビジョニング マネージャ］ダイアログ ボックスを使用して、これらのタスクを両方とも各サーバ上で順番に実行します。

以下の図で示された設定では、プロビジョニング マネージャが 1 つのプロビジョニング サーバにアイデンティティ プロビジョニングのリクエストを送信して、別のサーバにフェイルオーバするようにします。



プロビジョニング マネージャは、デフォルト プロビジョニング サーバにリクエストを送信し、別のサーバにフェイルオーバします。

ユーザ コンソール フェイルオーバの有効化

CA Identity Manager サーバのアプリケーション サーバが失敗した場合、それはプロビジョニング サーバ更新を受信しません。 その結果、CA Identity Manager ユーザ コンソール はプロビジョニング変更を表示しません。 そのため、CA Identity Manager サーバに対して別の URL を設定する必要があります。

次の手順に従ってください:

1. プロビジョニング マネージャを起動します。
2. ［システム］-［CA Identity Manager セットアップ］をクリックします。
3. クラスタ内の別のシステムのホスト名およびポートを入力します。
4. 環境を入力します。

   これはプライマリ URL 上の環境と同じである必要があります。
5. ［追加］をクリックします。

プロビジョニング マネージャ フェイルオーバの有効化

第 1 および第 2 のホスト サーバ上でプロビジョニング マネージャ フェイルオーバを有効にできます。 この手順が完了すると、各サーバが他方にフェイルオーバするように設定されます。

次の手順に従ってください:

1. プロビジョニング マネージャを起動します。
2. ［ファイル］-［基本設定］-［フェイルオーバ］タブを選択します。
3. ［フェイルオーバの有効化］チェック ボックスをオンにします。 デフォルトでは、ローカル プロビジョニング サーバはすでに定義されています。
4. ［追加］をクリックします。
5. リモート プロビジョニング サーバのホスト名を入力します。

   たとえば、im01 で、im02 のサーバ ホストを入力します。im02 で、im01 のサーバ ホストを入力します。
6. LDAP/TLS ポート値として「20390」、LDAP ポート値として「20389」をそれぞれ入力します。
7. リストでエントリを上下に移動させることにより、優先順序を調節します。
8. ［OK］をクリックします。
9. プロビジョニング マネージャを再起動して、変更を有効にします。

プロビジョニング マネージャ フェイルオーバのテスト

以下の手順に実行することにより、クライアント フェイルオーバの設定をテストできます。

次の手順に従ってください:

1. 1 つのドメイン サーバ上の CA Identity Manager - プロビジョニング サーバ サービスを停止します。
2. このサーバ インストール用のプロビジョニング マネージャを使用して、1 つ以上の操作を発行します。

   CA Identity Manager - プロビジョニング サーバ サービスのローカルな停止後、トラフィックはフェイルオーバ ドメイン サーバにフローします。 それでない場合は、設定を確認し、再度テストを試みます。

付録 A: アンインストールと再インストール

このセクションには、以下のトピックが含まれています。

CA Identity Manager をアンインストールする方法

CA Identity Manager を完全にアンインストールするには、CA Identity Manager ソフトウェア コンポーネントを削除して、ユーザのアプリケーション サーバ内の CA Identity Manager 固有の設定をクリーンアップします。 以下のチェックリストでは、CA Identity Manager をアンインストールする手順について説明します。

✓	手順
	1. 管理コンソールで CA Identity Manager オブジェクトを削除します。
	2. （オプション） SiteMinder を使用した場合は、ポリシー ストアから CA Identity Manager スキーマを削除するか、またはポリシー サーバを削除します。 詳細については、「*CA SiteMinder Web Access Manager Policy Server Installation Guide*」を参照してください。
	3. プロビジョニング ディレクトリおよびプロビジョニング サーバをアンインストールするには、以下の場所から高可用性コマンドを使用します。 *Unpacked-Install-Package*¥Provisioning¥Provisioning Directory¥highavailability
	4. CA Identity Manager コンポーネントをアンインストールします。
	5. アプリケーション サーバから CA Identity Manager 設定情報を削除します。

管理コンソールを使用した CA Identity Manager オブジェクトの削除

ユーザが環境とディレクトリを設定するときに、CA Identity Manager によって自動的に作成されたオブジェクトを削除するには、管理コンソールを使用します。

1. 以下の管理コンソールを開きます。

   http://*im_server*:*port*/iam/immanage
2. ［環境］をクリックします。
3. 既存の［環境］のすべてのチェック ボックスをオンにします。
4. ［削除］をクリックします。
5. ［ディレクトリ］をクリックします。
6. 既存の［ディレクトリ］のすべてのチェック ボックスをオンにします。
7. ［削除］をクリックします。

ポリシー ストアからの CA Identity Manager スキーマの削除

SiteMinder ポリシー サーバを使用していた場合は、ポリシー ストアから CA Identity Manager スキーマを削除します。

SQL Policy Store からの CA Identity Manager スキーマの削除

CA Identity Manager の SiteMinder の拡張機能をインストールしたシステムで、CA Identity Manager スキーマを削除します。 スキーマを削除するコマンドのデフォルトの場所を以下に示します。

- SQL Server の場合:

  C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥policystore-schemas¥MicrosoftSQLServer
- Oracle の場合:

  UNIX:

  /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/policystore-schemas/OracleRDBMS

  Windows: C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager/tools/policystore-schemas/OracleRDBMS

LDAP ポリシー ストアからの CA Identity Manager スキーマの削除

注: ポリシー ストアとして Microsoft Active Directory または Microsoft ADAM を使用している場合、この手順を完了する必要はありません。 これらのポリシー ストアからスキーマ オブジェクトを削除することはできません。ただし、それらを無効にできます。詳細については、ご使用のディレクトリのドキュメントを参照してください。

次の手順に従ってください:

1. 以下のいずれかの操作を完了します。
   - ポリシー ストアとして IBM Directory Server を使用している場合は、IBM Directory Server の Web 管理ユーザ インターフェースで、スキーマ設定のファイル セクションからスキーマ ファイル V3.imsschema60 を削除します。 その後、ディレクトリ サーバを再起動します。

     注: IBM Directory Server からこのスキーマを削除するのに必要な他の手順はありません。 CA Identity Manager ソフトウェア コンポーネントの削除を続行します。
   - ポリシー ストアとして CA Directory を使用している場合は、*dxserver_home*¥config¥schema から etrust_ims.dxc ファイルを削除します。

     ここで *dxserver_home* は CA Directory のインストール場所です。

     注: CA Directory Server からこのスキーマを削除するのに必要な他の手順はありません。 CA Identity Manager ソフトウェア コンポーネントの削除を続行します。
   - ポリシー ストアとして別の LDAP ディレクトリを使用している場合は、手順 2 にスキップします。
2. policystore-schemas フォルダに移動します。 以下はデフォルトの場所です。
   - **Windows：** C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥policystore-schemas
   - **UNIX：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/policystore-schemas

3. ディレクトリからスキーマを削除するには、以下のテーブルの適切な LDIF スキーマ ファイルを使用します。

   注: スキーマ ファイルの削除の詳細については、ご使用のディレクトリのドキュメントを参照してください。

ディレクトリ タイプ	LDIF ファイル
Novell eDirectory	novell¥novell-delete-ims8.ldif
Oracle Internet Directory (OID)	oracle-internet-directory¥oracle-internet-directory-delete-ims8.ldif
Sun Java Systems (Sun One、 iPlanet)	sunone¥sunone-delete-ims8.ldif

CA Identity Manager ソフトウェア コンポーネントのアンインストール

CA Identity Manager コンポーネントをインストールした各システムから、コンポーネントをアンインストールするには、このセクションの手順を使用します。たとえば、CA Identity Manager サーバおよび CA Identity Manager 管理ツールを別々のシステムにインストールした場合は、両方のシステムからコンポーネントをアンインストールします。

Windows の場合

1. ［スタート］ -［コントロール パネル］ -［プログラムの追加/削除］に移動して、CA Identity Manager に選択します。
2. CA Identity Manager を選択します。
3. ［変更と削除］をクリックします。

   プロビジョニング コンポーネント以外のすべてのコンポーネントがアンインストールされます。
4. プロビジョニング コンポーネントについては、個別のコンポーネント インストーラを使用してアンインストールします。

UNIX の場合:

1. 以下の場所に移動します。

   IM_HOME/install_config_info/im-uninstall

2. 以下のスクリプトを実行します。

   ```
   sh uninstall.sh
   ```

   画面に表示された手順に従います。

3. プロビジョニング コンポーネントについては、個別のコンポーネント インストーラを使用してアンインストールします。

JBoss からの CA Identity Manager の削除

CA Identity Manager のアンインストール後、JBoss アプリケーション サーバで必要な追加手順はありません。

JBoss アプリケーション サーバを削除するには、JBoss をインストールしたディレクトリを削除します。

CA Identity Manager の再インストール

再度インストーラを実行することにより、CA Identity Manager ソフトウェア コンポーネントを再インストールできます。 ユーザがインストーラを実行するとき、インストーラはシステムにインストール済みの CA Identity Manager コンポーネントを検出します。システムに当初インストールしたのと同じコンポーネント、または元々システムになかった他のコンポーネントを、再インストールする場合があります。

注: CA Identity Manager 管理ツールの再インストールは、Administrative Tools ディレクトリ内のファイルをすべて置換します。 カスタム ファイルへの上書きを防ぐには、管理ツールがインストールされているディレクトリをバックアップします。

付録 B: 無人インストール

このセクションには、以下のトピックが含まれています。

Administrative UI の無人インストールを実行する方法

次の手順に従ってください：

1. im-installer.properties ファイルを変更します。
2. 以下のコマンドを実行します。
   - **Windows の場合：**
     ```
     ca-im-release-win32.exe -f im-installer.properties -i silent
     ```
   - **UNIX の場合：**
     ```
     ./ca-im-release-sol.bin -f im-installer.properties -i silent
     ```

設定ファイルの変更

無人 CA Identity Manager インストールを有効にするには、テキスト エディタを使用して、im-installer.properties 設定ファイルの設定を変更します。ファイルのデフォルト パラメータは、最初の CA Identity Manager インストール中に入力された情報を反映します。 必要に応じてデフォルト値を変更します。

設定ファイルを変更する場合は、以下の点に注意してください。

- ファイルは最初のインストールまたは設定中に入力した値をすべて保持するので、オリジナルを変更する前にインストーラ プロパティ ファイルのバックアップ コピーを作成します。
- パラメータ名、等号（=）、パラメータ値の間に余分なスペースを追加しないでください。
- すべての Windows のディレクトリ名には、単一の円記号ではなく、ダブル円記号またはスラッシュが含まれる必要があります。

初期選択

基本的なインストールの選択項目については、以下のパラメータの値を入力します。

パラメータ	命令
DEFAULT_NEW_INSTANCE_DISPLAY_NAME	これがフレッシュ インストールである場合は、「New Installation」と入力します。アップグレードの場合は、これは空白になります。

パラメータ	命令
DEFAULT_COMPONENTS	以下の 1 つまたは複数のコンポーネントを入力します。 ■ Server - CA Identity Manager サーバ ■ Exten - ポリシー サーバに対する拡張 ■ Admin - CA Identity Manager 管理ツール ■ Provision - プロビジョニング サーバ ■ Directory - プロビジョニング ディレクトリ 複数のコンポーネントをインストールする場合は、カンマでコンポーネントを区切ります。
DEFAULT_INSTALL_FOLDER	CA Identity Manager サーバ をインストールするディレクトリを入力します。
DEFAULT_GENERIC_USERNAME	インストールされている CA Identity Manager コンポーネントの汎用なログイン情報。
DEFAULT_GENERIC_PASSWORD	インストールされている CA Identity Manager コンポーネントの汎用パスワード情報。
DEFAULT_FIPS_MODE	FIPS 140-2 コンプライアンスを有効にする場合は選択します。
DEFAULT_FIPS_KEY_LOC	FIPS キーの場所へのパスを入力します。

インストール プログラムは、インストールしているコンポーネントに適用されないパラメータを無視します。 たとえば、ユーザが DEFAULT_COMPONENTS を Exten に設定した場合、DEFAULT_PS_ROOT と DEFAULT_USE_SITEMINDER のパラメータのみが使用されます。

CA Identity Manager サーバ

CA Identity Manager サーバをインストールする予定がある場合は、以下に対する値を入力します。

パラメータ	内容
DEFAULT_APP_SERVER	Weblogic、WebSphere、または JBoss を入力します。

パラメータ	内容
DEFAULT_APP_SERVER_URL	CA Identity Manager をホストするアプリケーション サーバの完全な URL を、ポートを含め入力します。
DEFAULT_JAVA_HOME	CA Identity Manager の JRE または JDK へのパス。
追加のデータベース パラメータ	
DEFAULT_DB_HOST	CA Identity Manager データベースをホストするシステムのホスト名を入力します。
DEFAULT_DB_PORT	CA Identity Manager データベースをホストするシステムのポートを入力します。
DEFAULT_DB_NAME	CA Identity Manager データベースの名前を入力します。
DEFAULT_DB_USER	CA Identity Manager データベースの管理者のユーザ名を入力します。
DEFAULT_DB_PASSWORD	CA Identity Manager データベースの管理者ユーザのパスワードを入力します。
DEFAULT_DB_TYPE	CA Identity Manager データベースに使用されたデータベースのタイプを入力します。
追加の **JBoss** パラメータ	
DEFAULT_JBOSS_FOLDER	JBoss アプリケーション サーバをインストールしたシステムのフルパス名を入力します。 例： C:¥jboss-6.1
DEFAULT_JBOSS_CLUSTER_UNICAST	「true」または「false」と入力します。
DEFAULT_JBOSS_CLUSTER_REPLICATION	「true」または「false」と入力します。
DEFAULT_JBOSS_CLUSTER_UNICAST_HOSTNAMES	HOSTNAME[PORT] エントリのカンマ区切りリストを入力します。 例： 10.1.1.1[7600],20.2.2.2[7600],30.3.3.3
追加の **WebLogic** パラメータ	

パラメータ	内容
DEFAULT_BINARY_FOLDER	WebLogic をインストールしたディレクトリの完全なディレクトリ パスを入力します。 例：C:¥Oracle¥Middleware¥weblogic¥
DEFAULT_DOMAIN_FOLDER	CA Identity Manager 用に作成した WebLogic ドメインの完全な パスおよびディレクトリ名を入力します。
DEFAULT_SERVER_NAME	CA Identity Manager 用に作成した WebLogic サーバ インスタンスの名前を入力します。
DEFAULT_BEA_CLUSTER	WebLogic クラスタのクラスタ名を入力します。
追加の **WebSphere** パラメータ	
DEFAULT_WEBSPHERE_FOLDER	WebSphere 用の CA Identity Manager Tools をインストールしたディレクトリのフルパス名を入力します。
DEFAULT_WAS_NODE	アプリケーション サーバが存在するノードの名前を指定します。
DEFAULT_WAS_SERVER	アプリケーション サーバが実行されているシステムの名前を入力します。
DEFAULT_WAS_CELL	アプリケーション サーバが存在するセルの名前を指定します。
WAS_PROFILE	WebSphere プロファイル ファイルの場所を入力します。
DEFAULT_WAS_CLUSTER	WebSphere クラスタのクラスタ名を入力します。

SiteMinder ポリシー サーバを使用している場合は、以下を入力します。

パラメータ	内容
DEFAULT_PS_HOST	管理サーバの完全修飾ドメイン名を入力します。
DEFAULT_PS_USER	ポリシー サーバ管理者のユーザ名を入力します。
DEFAULT_PS_PW	ポリシー サーバ管理者のパスワードを入力します。

プロビジョニング コンポーネント

プロビジョニングをインストールする場合は、以下を入力します。

パラメータ	命令
DEFAULT_CONFIG_REMOTE PROVISIONING	リモート プロビジョニング ディレクトリに接続している場合は、「true」を入力します。
DEFAULT_DEPLOYMENT_SIZE	プロビジョニング ディレクトリ展開のサイズを入力します。
DEFAULT_DIRECTORY_IMPS_HOSTNAMES	Directory に接続しているすべてのプロビジョニング サーバのホスト名を入力します。
DEFAULT_DOMAIN_NAME	既存のプロビジョニング ドメインがない場合、「im」を入力します。
DEFAULT_DIRECTORY_HOST	プロビジョニング ディレクトリがインストールされているシステムのホスト名を入力します。
DEFAULT_DIRECTORY_PORT	プロビジョニング ディレクトリがインストールされているシステムのポート番号を入力します。
DEFAULT_DIRECTORY_PASSWORD	プロビジョニング ディレクトリのパスワードを入力します。

SiteMinder の拡張機能

SiteMinder ポリシー サーバの拡張機能をインストールするには、以下を入力します。

パラメータ	命令
DEFAULT_PS_ROOT	（Solaris のみ）ポリシー サーバがインストールされているディレクトリを入力します。
DEFAULT_USE_SITEMINDER	実装で SiteMinder ポリシー サーバを使用している場合は、「true」を入力します。

設定ファイル フォーマット

im-installer.properties ファイルは CA Identity Manager インストール ディレクトリにあります。 以下に例を示します。

- **Windows**： C:¥Program Files¥CA¥CA Identity Manager¥install_config_info
- **Unix**： /opt/CA/IdentityManager/install_config_info/im-installer.properties

CA Identity Manager インストールで作成された im-installer.properties ファイルの例を以下に示します。

```
############################################################
### IM R12.5SP7 インストーラのサイレント入力プロパティ ファイル ###
############################################################

# コンポーネント リスト
#   有効な値（カンマ区切り、1 つまたは複数） : Server、Exten、Admin、Provision、Directory
DEFAULT_COMPONENTS=

# インストール フォルダ
#    このフォルダ下のサブフォルダに、すべての製品がインストールされます
#    これはユーザによって選択された親製品ルートです
#    たとえば、C:¥¥Program Files¥¥CA¥Identity Manager
DEFAULT_INSTALL_FOLDER=

#汎用なログイン情報
DEFAULT_GENERIC_USERNAME=
#DEFAULT_GENERIC_PASSWORD=<サイレント インストールの場合は、汎用ユーザ パスワードをここに挿入し、行をコメント解除します。>

#オプションで管理コンソール セキュリティを有効にする - デフォルト ユーザは上記の汎用ログイン クレデンシャルを使用して作成されます。
DEFAULT_SECURE_MANAGEMENT_CONSOLE=

# プロビジョニング サーバおよびプロビジョニング ディレクトリの情報。
#   リモートにインストールされたプロビジョニング ディレクトリに対してプロビジョニング サーバを設定（true/false）
DEFAULT_CONFIG_REMOTE_PROVISIONING=

 #ユーザのニーズに応じた展開タイプの選択（1、2、3、4） : 1. コンパクト 2. 基本 3. 中規模（64 Bit のみ） 4. 大規模（64 Bit のみ）
DEFAULT_DEPLOYMENT_SIZE=
DEFAULT_DIRECTORY_IMPS_HOSTNAMES=
DEFAULT_DOMAIN_NAME=
DEFAULT_DIRECTORY_HOST=
DEFAULT_DIRECTORY_PORT
#DEFAULT_DIRECTORY_PASSWORD=<サイレント インストールの場合は、プロビジョニング コンポーネントで使用するパスワードをここに挿入し、行をコメント解除します。>
```

```
#Identity Manager、管理ツール、プロビジョニング マネージャ、およびプロビジョニング サーバでの FIPS 140-2 準拠モード（true/false）
DEFAULT_FIPS_MODE=
#FIPS キー ファイルの完全パス。 例: C:¥¥Program Files¥¥FIPSkey.dat
DEFAULT_FIPS_KEY_LOC=

#機密データ暗号化のためのカスタム暗号化プロパティの使用
DEFAULT_KEY_PARAMS_ENABLED=
#暗号化プロパティ ファイルの絶対パス。 例： C:¥¥Program Files¥¥keyParams.properties
DEFAULT_KEY_PARAMS_LOC=


#Identity Manager のアプリケーション サーバ情報
#    アプリケーション サーバ
#    有効な値： JBoss、WebLogic、WebSphere
DEFAULT_APP_SERVER=
DEFAULT_APP_SERVER_URL=

#JBOSS アプリケーション サーバの JDK へのパス。 他のアプリケーション サーバについての入力は不要です
DEFAULT_JAVA_HOME=

#JBoss 情報
DEFAULT_JBOSS_FOLDER=
DEFAULT_JBOSS_PROFILE=
DEFAULT_JBOSS_SERVER_ID=

#Weblogic 情報
DEFAULT_BINARY_FOLDER=
DEFAULT_DOMAIN_FOLDER=
DEFAULT_SERVER_NAME=
DEFAULT_BEA_CLUSTER=

#WebSphere 情報
DEFAULT_WEBSPHERE_FOLDER=

#WAS_NODE 値： $WAS_HOME$¥installedApps¥$WAS_NODE$ または
$WAS_HOME$¥config¥cells¥$WAS_CCELL$¥nodes¥$WAS_NODE$    これらは同じである必要があります。
DEFAULT_WAS_NODE=

#WAS_SERVER 値： $WAS_HOME$¥config¥cells¥$WAS_CELL$¥n
odes¥$WAS_NODE$¥servers¥$WAS_SERVER$
DEFAULT_WAS_SERVER=

#WAS_CELL 値：$WAS_HOME$¥config¥cells¥$WAS_CELL$
DEFAULT_WAS_CELL=
```

```
#WAS_PROFILE 値： $WEBPHERE_HOME$¥profiles¥$WAS_PROFILE$
WAS_PROFILE=

#WAS_CLUSTER 値： $WAS_HOME$¥config¥cells¥$WAS_CELL$¥clusters¥$WAS_CLUSTER$
DEFAULT_WAS_CLUSTER=

DEFAULT_WAS_NO_AUTO_DEPLOY=$WAS_NO_AUTO_DEPLOY$

#ポリシー サーバ情報
DEFAULT_PS_HOST=
DEFAULT_PS_USER=
#DEFAULT_PS_PW=<サイレント インストールの場合は、PS 管理者ユーザ パスワードをここに挿入し、
行をコメント解除します。>

#8.1 マイグレーション
# SiteMinder エージェント名
DEFAULT_AGENT_NAME=
# SiteMinder の共有秘密キー
#DEFAULT_AGENT_PW=<サイレント インストールの場合は、PS 共有秘密キーをここに挿入し、行をコメ
ント解除します。>
# 自動的なマイグレート。 有効な値（true/false）
DEFAULT_MIGRATE_DIR_ENV=
# エクスポート先のディレクトリ
DEFAULT_DIR_ENV_EXPORT=

#ポリシー サーバ拡張情報
#   CsSmPs-<インスタンス名>フォルダの場所
DEFAULT_PS_ROOT=
#SiteMinder ポリシー サーバおよび SiteMinder Web エージェントを使用して高度なセキュリティを
提供できます
# CA Identity Manager 環境。 有効な値（true/false）
DEFAULT_USE_SITEMINDER=

#データベース情報
DEFAULT_DB_HOST=
DEFAULT_DB_PORT=
DEFAULT_DB_NAME=
DEFAULT_DB_USER=
#DEFAULT_DB_PASSWORD=<サイレント インストールの場合は、データベース パスワードをここに挿入
し、行をコメント解除します。>

#許容値は次のとおりです。mssql2005 または oracle10
DEFAULT_DB_TYPE=

#WAS メッセージ エンジン データベース情報
DEFAULT_ME_HOST=
DEFAULT_ME_PORT=
DEFAULT_ME_NAME=
```

```
DEFAULT_ME_USER=
#DEFAULT_ME_PASSWORD=<サイレント インストールの場合は、データベース パスワードをここに挿入し、行をコメント解除します。>
DEFAULT_ME_SCHEMA=

#IM8.1sp2 からのアップグレード
#       データ ストアが別個のサーバ上に配置されているか、または配置したい場合は、
#       以下のように指定できます。 または、すべてのデータ ストアを同じサーバ上に配置したい場合は、
#       上記の DEFAULT_DB_* プロパティを変更します。

#オブジェクト ストア データストア情報
#DEFAULT_OS_DB_HOST=
#DEFAULT_OS_DB_PORT=
#DEFAULT_OS_DB_NAME=
#DEFAULT_OS_DB_USER=
#DEFAULT_OS_DB_PASSWORD=<サイレント インストールの場合は、データベース パスワードをここに挿入し、行をコメント解除します。>

#タスク永続性データストア情報
#DEFAULT_TP_DB_HOST=
#DEFAULT_TP_DB_PORT=
#DEFAULT_TP_DB_NAME=
#DEFAULT_TP_DB_USER=
#DEFAULT_TP_DB_PASSWORD=<サイレント インストールの場合は、データベース パスワードをここに挿入し、行をコメント解除します。>

#監査データストア情報
#DEFAULT_AUDIT_DB_HOST=
#DEFAULT_AUDIT_DB_PORT=
#DEFAULT_AUDIT_DB_NAME=$AUDIT_DB_USER$
#DEFAULT_AUDIT_DB_PASSWORD=<サイレント インストールの場合は、データベース パスワードをここに挿入し、行をコメント解除します。>

#レポート スナップショット データストア情報
#DEFAULT_RS_DB_HOST=
#DEFAULT_RS_DB_PORT=
#DEFAULT_RS_DB_NAME=
#DEFAULT_RS_DB_USER=
#DEFAULT_RS_DB_PASSWORD=<サイレント インストールの場合は、データベース パスワードをここに挿入し、行をコメント解除します。>

#ワークフロー データストア情報
#DEFAULT_WF_DB_HOST=
#DEFAULT_WF_DB_PORT=
#DEFAULT_WF_DB_NAME=
#DEFAULT_WF_DB_USER=
#DEFAULT_WF_DB_PASSWORD=<サイレント インストールの場合は、データベース パスワードをここに挿入し、行をコメント解除します。>
```

```
# 自動的にワークフロー DB をアップグレードする
DEFAULT_UPGRADE_WF_DB=

# 自動的に永続性タスクをマイグレートする
DEFAULT_MIGRATE_TP=$

# HTTP プロキシ設定
DEFAULT_HTTP_PROXY_ENABLED=
DEFAULT_HTTP_PROXY_HOST=
DEFAULT_HTTP_PROXY_PORT=
DEFAULT_HTTP_PROXY_DOMAIN=
DEFAULT_HTTP_PROXY_USERNAME=
DEFAULT_HTTP_PROXY_PASSWORD=
```

第 9 章: クラスタ化されたインストールの確認

すべての手順を完了して、クラスタを開始したときに、インストールが成功したことをチェックしてください。

次の手順に従ってください:

1. CA Identity Manager サーバによって使用されるデータベースを開始します。
2. 停止していた余分なポリシー サーバおよび CA Identity Manager ノードを開始します。
3. 管理コンソールにアクセスし、以下のポイントを確認します。
   - ブラウザから以下の URL にアクセスできます。

     http://*im_server*:*port*/iam/immanage

     以下に例を示します。

     http://MyServer.MyCompany.com:*port-number*/iam/immanage
   - 管理コンソールが開きます。

- アプリケーション サーバ ログにエラーが表示されません。
- ディレクトリ リンクをクリックした場合、ユーザはエラー メッセージを受信しません。

4. 以下の URL 形式を使用して、アップグレードされた環境にアクセスできることを確認してください。

   http://*im_server*:*port*/iam/im/*environment*

付録 C: インストール ログ ファイル

ログ ファイルは、インストール パッケージを開いた場所に基づいて格納されます。 以下の例の最上位ディレクトリは、それらのデフォルト場所と異なる場合があります。

このセクションには、以下のトピックが含まれています。

Windows のログオンファイル (P. 187)
UNIX のログ ファイル (P. 188)

Windows のログオンファイル

CA Identity Manager インストール中に問題が発生した場合は、以下のログ ファイルを参照してください。

C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥caiamsuite.log

CA Identity Manager サーバ インストーラ ログは以下のデフォルトの場所に書き込まれています。

- C:¥Program Files¥CA¥Identity Manager¥install_config_info （32 ビット システム）
- C:¥Program Files (x86)¥CA¥Identity Manager¥install_config_info (64 ビット システム)

プロビジョニング インストーラ ログはユーザの Temp ディレクトリに書き込まれ、*Install-Directory*¥_uninst ディレクトリにコピーされます。

例:

C:¥Documents and Settings¥*user*¥Local Settings¥Temp¥imps_server_install.log

UNIX のログ ファイル

CA Identity Manager インストールの実行中に問題が発生した場合は、以下の場所で caiamsuite.log ファイルを参照してください。

/opt/CA/IdentityManager/

CA Identity Manager サーバ インストーラ ログは以下のデフォルトの場所に書き込まれています。

/opt/CA/IdentityManager/install_config_info

プロビジョニング インストーラ ログはユーザの Temp ディレクトリに書き込まれています。

付録 D: Windows サービスとしての CA Identity Manager

このセクションには、以下のトピックが含まれています。

Windows サービスとしての CA Identity Manager（JBoss 5）

CA Identity Manager を JBoss 5 システム上のサービスとして設定するには、以下の手順に従います。

次の手順に従ってください:

1. JBoss bin フォルダにある service.bat ファイルを編集します。
2. run.bat 行を見つけます。これは、以下のように表示されます。

   ```
   call run.bat < .r.lock >> run.log 2>&1
   ```

3. JBoss クラスタがある場合は、これらの行を以下のように変更します。

   ```
   call run.bat -c all < .r.lock >> run.log 2>&1
   ```

   このファイルには、この行が 2 つ含まれています。
4. service identity 行を見つけます。これは、以下のように表示されます。

   ```
   set SVCNAME=JBAS50SVC
   set SVCDISP=JBoss Application Server 5.1
   ```

5. これらの行を以下のように変更します。

   ```
   set SVCNAME=CAIMSVC
   set SVCDISP=CA Identity Manager
   ```

6. ファイルを保存します。
7. コマンド プロンプトから、Windows サービスをインストールするために service.bat スクリプトを実行します。

   ```
   service.bat install
   ```

8. サービス ツールを使用して、このサービスのスタートアップの種類を「手動」から「自動」に変更します。
9. CA Identity Manager サービスを起動します。
10. 起動が成功したことを確認するために、JBoss ログを表示します。

Windows サービスとしての CA Identity Manager（JBoss EAP 6.1）

CA Identity Manager を JBoss 6.1 EAP システム上のサービスとして設定するには、以下の手順に従います。

次の手順に従ってください:

1. 以下の URL の Web サイトから必要な jboss-native をダウンロードします。

   `http://www.jboss.org/jbossweb/downloads/jboss-native-2-0-10`

2. ZIP ファイルを抽出し、中身を JBOSS_HOME¥bin フォルダにコピーします。

3. JBOSS_HOME¥bin フォルダ内の service.bat を開き、以下のように変更します。

   a. JAVA_OPTS の行を削除します。

   b. 以下の変数を設定します。

      ```
      set SVCNAME=CAIM
      set SVCDISP=CA Identity Manager
      ```

   c. すべての run.bat コールを standalone.bat に置き換えます。

   d. 以下の行があれば、すべて削除します。

      ```
      call shutdown -S < .s.lock >> shutdown.log 2>&1
      ```

   e. その場所に、以下の行を挿入します。

      ```
      call jboss-cli.bat --connect command=:shutdown >> shutdown.log
      2>&1
      ```

4. JBOSS_HOME¥bin フォルダ内の standalone.conf.bat ファイルを開き、JAVA_OPTS を以下のように定義します。

   ```
   JAVA_OPTS=%JAVA_OPTS% -Xrs
   ```

5. コマンド ライン プロンプトを開き、ディレクトリを JBOSS_HOME¥bin フォルダに変更します。
   ```
   service.bat install
   ```

6. サービス ツールを使用して、このサービスのスタートアップの種類を「手動」から「自動」に変更します。

7. CA Identity Manager のクラスタ インストールの場合は、以下の手順が適用されます。

- クラスタ内の共有されている場所について、ユーザが別のユーザとして CA IM サービスを実行するための十分な権限を持っていることを確認します。
- クラスタ内の各ノードについてこの手順を繰り返します。

付録 E: CA Identity Manager によって開始される Windows サービス

ユーザが CA Identity Manager のすべてのコンポーネントをインストールして起動したときに、Windows 上で開始されるサービスを以下に示します。

- CA Directory *hostname*-impd-co
- CA Directory impd-inc
- CA Directory impd-main
- CA Directory impd-notify
- CA Directory impd-router
- CA Identity Manager Connector Server (C++)
- CA Identity Manager Connector Server (Java)
- CA Identity Manager Provisioning Server
- Enterprise Common Services (Transport)
- Enterprise Common Services GUI Framework
- Enterprise Common Services Store-And-Forward Manager

このサービスのリストは、トラブルシューティングに役立つことがあります。

付録 F: logging.jsp ファイル

JBoss では、logging.jsp ファイルを設定できます。手順については、以下の場所にある Readme.txt ファイルを参照してください。

- Windows の場合： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥samples¥Admin
- UNIX の場合： /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/samples/Admin

Readme.txt ファイルには、同じ場所にある user_console.war フォルダを使用して logging.jsp を設定する方法が示されています。