

CA Identity Manager™

インストール ガイド (WebSphere)

12.6.4



このドキュメント（組み込みヘルプシステムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。本ドキュメントは、CA が知的財産権を有する機密情報であり、CA の事前の書面による承諾を受けずに本書の全部または一部を複写、譲渡、変更、開示、修正、複製することはできません。

本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし、CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負いません。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本書の制作者は CA および CA Inc. です。

「制限された権利」のもとでの提供：アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2014 CA. All rights reserved. 本書に記載されたすべての商標、商号、サービス・マークおよびロゴは、それぞれの各社に帰属します。

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	11
CA Identity Manager のサンプル インストール	11
例: 単一ノードインストール	12
例: 複数のエンドポイントを用いたインストール	14
例: SiteMinder および CA Identity Manager のインストール	16
高可用性インストール	17
例: 高可用性インストール	19
CA Identity Manager サーバアーキテクチャ	20
プロビジョニング コンポーネントのアーキテクチャ	20
インストールプロセスの全体	21
第 2 章: インストールの前提条件	23
インストール ステータス	23
前提条件として必要な知識	24
必須コンポーネントをインストールする方法	24
ハードウェア要件のチェック	25
CA Directory のインストール	27
FIPS 140-2 暗号化キーの作成	29
暗号化パラメータ ファイルの作成	29
(オプション) SiteMinder との統合	30
Portal データベースの作成	32
WebSphere アプリケーション サーバ	33
Solaris の要件	35
Linux の要件	36
IPv6 のサポート	38
インストール チェックリストを完了します。	40
UNIX およびコンソール モードのインストール	44
Non-Provisioning インストール	44
第 3 章: 単一ノードインストール	45
インストール ステータス	45
CA Identity Manager コンポーネント	46
単一ノードインストールを実行する方法	47

CA Identity Manager コンポーネントのインストール.....	47
ユーザ プロファイルのワークフローの設定	49
CA Identity Manager サーバの起動の確認.....	50
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	52
リモートプロビジョニング マネージャの設定	53

第 4 章: WebSphere クラスタへのインストール 55

インストール ステータス	55
WebSphere クラスタのセットアップ	56
WebSphere クラスタの前提条件	57
各 Node への WebSphere 7 のインストール.....	58
1 つのメンバを持つクラスタの作成	59
CA Identity Manager を WebSphere クラスタにインストールする方法	59
インストールによって作成されるオブジェクト	60
Deployment Manager のインストールの実行.....	61
クラスタ メンバの追加.....	65
中核的なグループ ポリシーの割り当て	65
クラスタ メンバのワークフローの設定	66
Web サーバ用のプロキシプラグインの設定.....	67
仮想ホスト エイリアスの設定	68
WebSphere クラスタの開始	69
クラスタ化されたインストールの確認	69
リモートプロビジョニング マネージャの設定	70

第 5 章: 個別データベース設定 71

インストール ステータス	71
個別データベースの作成.....	72
個別データベースを作成する方法	73
MS SQL Server データベース インスタンスの作成.....	73
Oracle データベース インスタンスの作成.....	74
JDBC リソースの作成.....	74
データソースの編集.....	76
接続プールプロパティの設定	78
SQL スクリプトの実行.....	79
ワークフローのスクリプトの実行	81

第 6 章: 手動による EAR のデプロイ 83

手動でデプロイする方法	83
-------------------	----

手動デプロイの前提条件.....	84
プライマリ リソースの作成.....	84
中核的なグループ ポリシーの割り当て.....	86
EAR ファイルの生成.....	87
castylesr5.1.1.ear ファイルの展開方法.....	87
iam_im.ear のデプロイ.....	88
JACL スクリプトによる iam_im.ear のデプロイ.....	88
WebSphere 管理コンソールからの iam_im.ear のデプロイ.....	89
ポリシー サーバとワークフローのオブジェクトの作成.....	92
メッセージ駆動型ビーン リスナー バインディングの作成.....	93
user_console.war の編集.....	95
wpServer.Jar の編集.....	95
SiteMinder への接続.....	96
RCM への接続.....	97
プロビジョニング サーバの共有秘密キーの作成.....	99
クラスタ用のポスト デプロイ 手順の実行.....	99
クラスタ メンバの追加.....	99
中核的なグループ ポリシーの割り当て.....	100
クラスタ メンバのワークフローの設定.....	100
Web サーバ用のプロキシプラグインの設定.....	101
WebSphere クラスタの開始.....	102
クラスタ化されたインストールの確認.....	103

第 7 章: レポート サーバのインストール 105

インストール ステータス.....	105
レポートिंगのアーキテクチャ.....	106
レポートの考慮事項.....	107
ハードウェア要件.....	107
レポート サーバをインストールする方法.....	108
レポートインストール前のチェックリスト.....	108
レポート情報.....	110
レポート サーバ用ポートを開く.....	111
CA レポート サーバのインストール.....	112
レジストリ スクリプトの実行.....	116
JDBC JAR ファイルのコピー.....	117
プロキシ サーバのバイパス.....	118
デフォルト レポートの展開.....	119
BusinessObjects XI 3.x のインストール後の手順.....	120
WebSphere でのレポート サーバ接続のセキュリティ保護.....	121

レポート インストールの確認	122
サイレント インストール	123
レポートをアンインストールする方法	123
残存アイテムの削除	123

第 8 章: コネクタ サーバのインストール 125

コネクタ サーバの前提条件	125
システム要件	125
タイムゾーンの考慮事項	125
ファイルの場所	126
32 ビットおよび 64 ビット アプリケーション	126
Linux の要件	127
CA IAM CS のインストール	128
プロビジョニング サーバの登録	131
C++ Connector Server のインストール	131
CA IAM CS のサイレント インストール	132
CA IAM CS 用 SDK のインストール	133
コネクタ サンプルのインストール	133
JDBC サポートのセットアップ	134
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	135
Sybase コネクタ用ライセンス ファイルのセットアップ	137
SQL Server コネクタの Windows 認証をセットアップ	138
コネクタのセットアップに関する詳細情報	139

第 9 章: 高可用性プロビジョニングのインストール 141

インストール ステータス	141
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	142
冗長プロビジョニング ディレクトリ	142
代替プロビジョニング ディレクトリのインストール	143
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	145
冗長プロビジョニング サーバ	146
プロビジョニング サーバのルータ DSA	147
プロビジョニング サーバのインストール	148
プロビジョニング サーバのフェイルオーバーの設定	150
冗長コネクタ サーバ	151
複数のコネクタ サーバのインストール	151
コネクタ サーバフレームワーク	151
負荷分散およびフェイルオーバー	153

信頼性および拡張性.....	153
Multi-Platform のインストール.....	154
コネクタ サーバの設定.....	155
Solaris 上の C++ Connector Server.....	161
プロビジョニング クライアントのフェイルオーバー.....	161
ユーザ コンソール フェイルオーバーの有効化.....	162
プロビジョニング マネージャ フェイルオーバーの有効化.....	162
プロビジョニング マネージャ フェイルオーバーのテスト.....	163

付録 A: アンインストールと再インストール 165

CA Identity Manager をアンインストールする方法.....	165
管理コンソールを使用した CA Identity Manager オブジェクトの削除.....	166
ポリシー ストアからの CA Identity Manager スキーマの削除.....	166
SQL Policy Store からの CA Identity Manager スキーマの削除.....	166
LDAP ポリシー ストアからの CA Identity Manager スキーマの削除.....	167
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.....	168
WebSphere からの CA Identity Manager の削除.....	169
CA Identity Manager の再インストール.....	171

付録 B: 無人インストール 173

Administrative UI の無人インストールを実行する方法.....	173
設定ファイルの変更.....	173
初期選択.....	174
CA Identity Manager サーバ.....	175
プロビジョニング コンポーネント.....	177
SiteMinder の拡張機能.....	177
設定ファイルフォーマット.....	179

付録 C: ログ ファイルのインストール 185

Windows のログ オンファイル.....	185
UNIX のログ ファイル.....	186

付録 D: CA Identity Manager によって開始される Windows サービス 187

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](#) (P. 11)

[例: 単一ノードインストール](#) (P. 12)

[例: 複数のエンドポイントを用いたインストール](#) (P. 14)

[例: SiteMinder および CA Identity Manager のインストール](#) (P. 16)

[高可用性インストール](#) (P. 17)

[インストールプロセスの全体](#) (P. 21)

CA Identity Manager のサンプル インストール

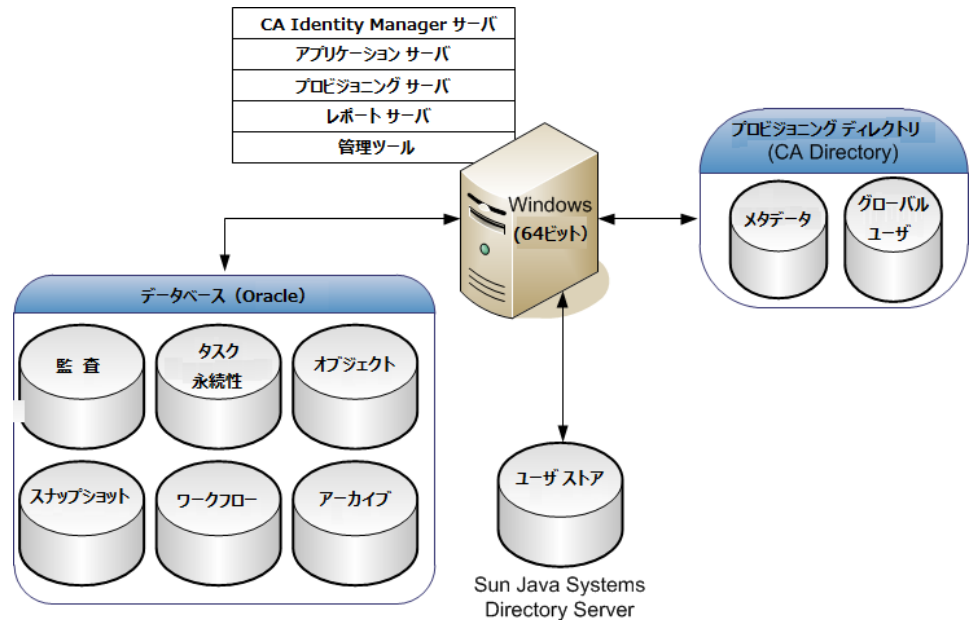
CA Identity Manager では、ユーザの ID と、エンドポイント システムのアプリケーションおよびアカウントに対するユーザ アクセスを制御できます。必要とする機能に基づいて、インストールする CA Identity Manager コンポーネントを選択します。

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。

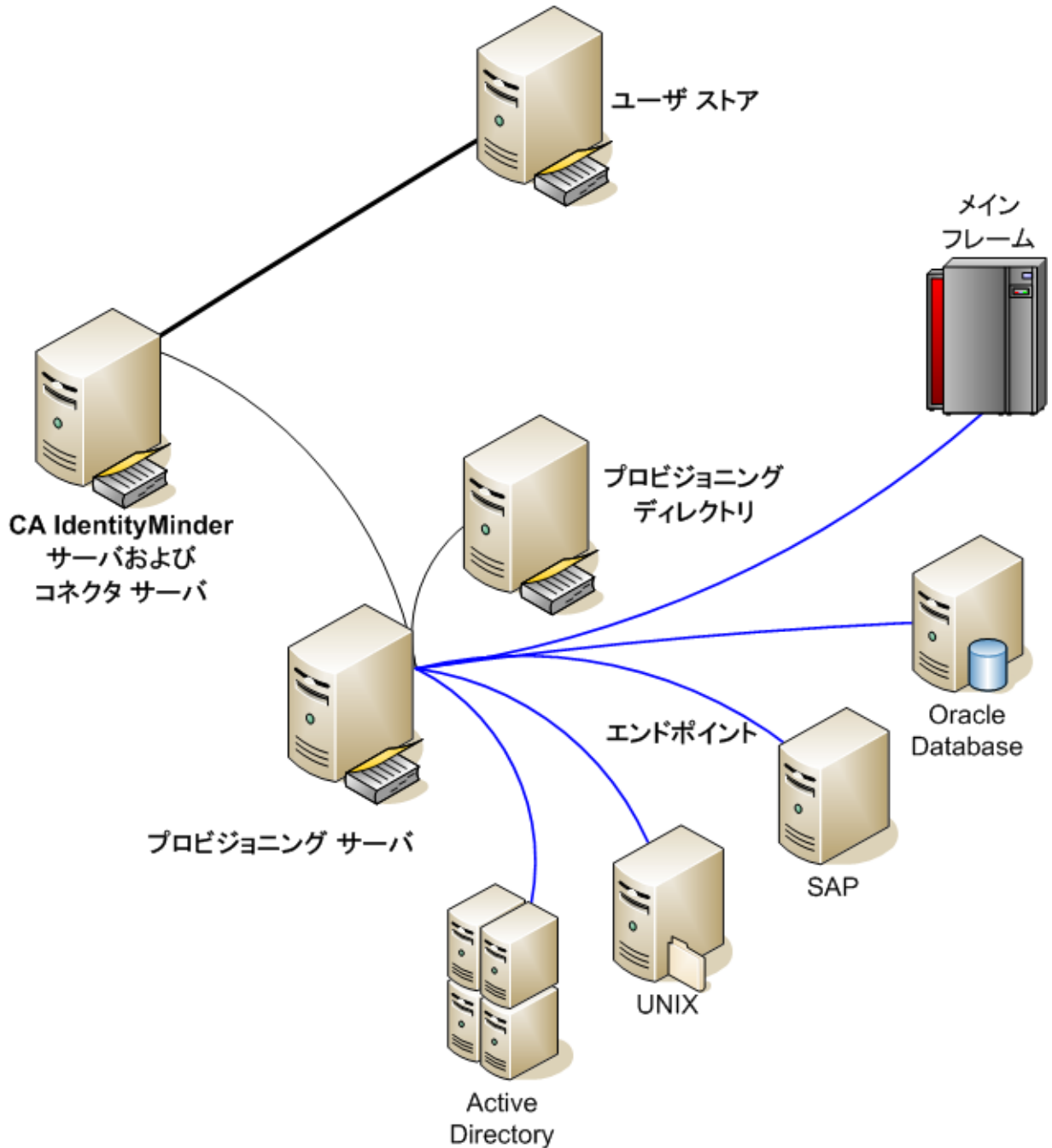
注: このアプリケーションは Windows 上でのみ実行されます。

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。

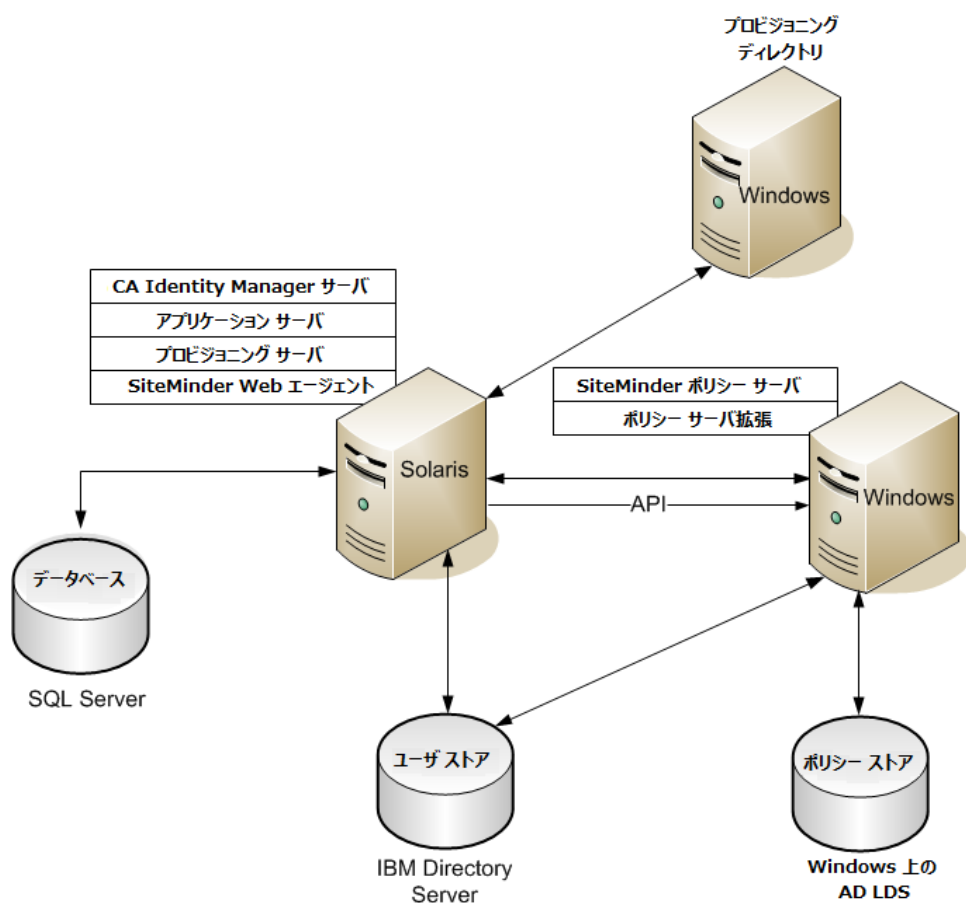
標準インストールシナリオでは、ユーザストアおよびプロビジョニングディレクトリ用の個別のシステムを含み、引き続き同期化されます。

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。

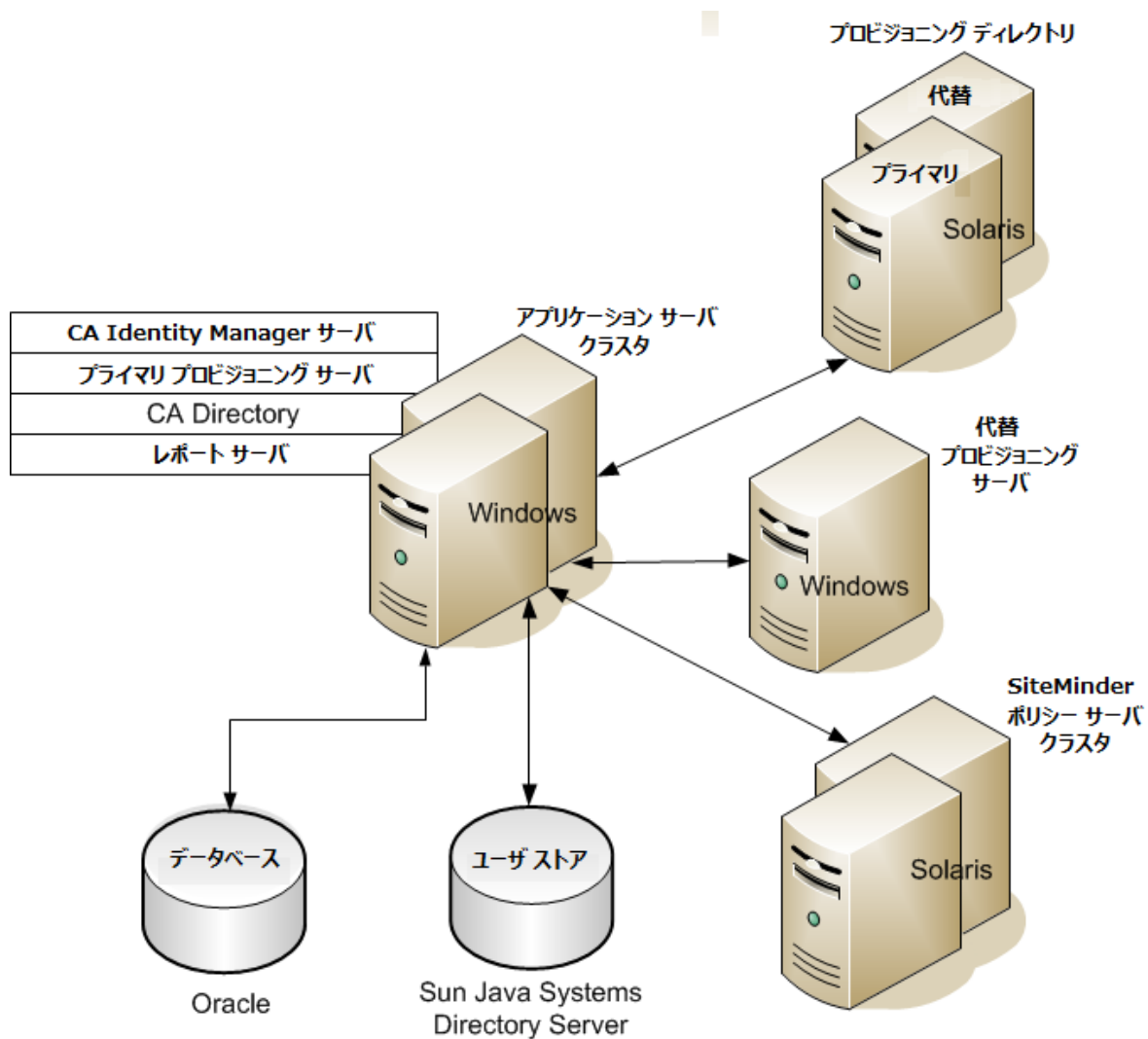
- フェイルオーバー -- プライマリ システムが故障するか、または何らかの理由で一時的にオフラインになった場合、別のシステムに自動的に切り替えます。
- 負荷分散 -- 優れたパフォーマンスが維持され、単一のデバイスが圧倒されることがないように、コンピュータ ネットワーク全体に処理および通信アクティビティを平等に配布します。
- さまざまな展開層が動的なビジネス要件に役立つ柔軟性を提供します。

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ーを可能にし、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ー優先順位に従って、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にします。

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ー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 \(P. 23\)](#)

[前提条件として必要な知識 \(P. 24\)](#)

[必須コンポーネントをインストールする方法 \(P. 24\)](#)

[UNIX およびコンソールモードのインストール \(P. 44\)](#)

[Non-Provisioning インストール \(P. 44\)](#)

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	<ol style="list-style-type: none">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。
	<ol style="list-style-type: none">2. 以下のインストールのいずれかを実行します。<ul style="list-style-type: none">■ 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
	<ol style="list-style-type: none">3. (オプション) 個別のデータベースを作成します。
	<ol style="list-style-type: none">4. (オプション) レポートサーバをインストールします。
	<ol style="list-style-type: none">5 (オプション) フェイルオーバー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。
 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

コンポーネント	最小	推奨
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	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
使用可能なディスク領域	<p>エンドポイントアカウントの数に応じて、2 GB から 10 GB。</p> <ul style="list-style-type: none"> ■ 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あたり 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あたり 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あたり 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あたり 2 GB (合計 8 GB) 	<p>エンドポイントアカウントの数に応じて、2 GB から 10 GB。</p> <ul style="list-style-type: none"> ■ 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あたり 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あたり 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あたり 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あたり 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。

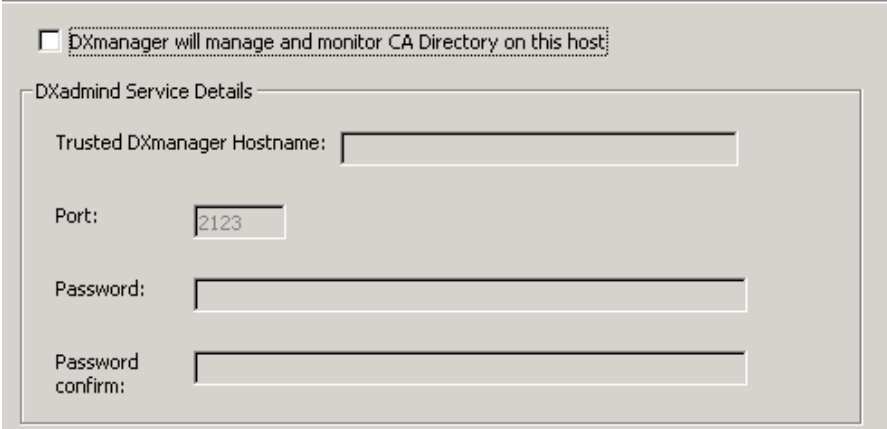
コンポーネント	最小
CPU	Intel (またはその互換) 3.1 GHz (Windows または Red Hat Linux) SPARC 2.5 GHz (Solaris)
メモリ	8 GB
使用可能なディスク領域	アカウントの数に応じて、14 GB ~ 6 GB
プロセッサ	64 ビットのプロセッサおよびオペレーティングシステム、デュアルコア
スワッピング/ページングスペース	6 GB

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。

WebSphere アプリケーション サーバ

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。CA Identity Manager アプリケーションサーバとして WebSphere を使用する場合は、以下の手順に従います。

WebSphere のインストール

CA Identity Manager 12.6.4 は Websphere 7、8.0、または 8.5 と連携します。IBM WebSphere の新バージョンを必要とする場合は、IBM ドキュメントに述べられているような WebSphere サーバをインストールします。インストール中に、これらのアクションを実行します。

- Web サーバの適切なプラグインを選択します。
- サーバおよびクライアントのオプションを選択します。
- サーバの最新の FixPack および必要な JDK をインストールします。

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。

Websphere のセルおよびノードの名前を作成する際は、すべてのオペレーティングシステムで大文字と小文字を区別することを念頭においてください。CA Identity Manager をインストールするときに、これらの名前の大文字と小文字が正しいことを確認してください。

グローバル セキュリティの無効化

インストールの前にセキュリティを無効にすることをお勧めします。[Security Enabled] オプションがオフになっていることを確認してください。このアクションにより、問題なくプロファイルを作成できるようになります。

WebSphere の確認

WebSphere が動作していることを確認するために、以下のテストを使用します。

- 以下の URL の IBM の snoop ユーティリティにアクセスして、WebSphere アプリケーションサーバが正しくインストールされているかどうかテストします。

`http://hostname:port/snoop`

以下に例を示します。

`http://MyServer.MyCompany.com:9080/snoop`

WebSphere が正しくインストールされている場合、ブラウザに [Snoop Servlet--Request Client Information] ページが表示されます。

- Web サーバをインストールする場合、WebSphere アプリケーションサーバプラグインが正しくインストールされてことをテストします。URL にアプリケーションサーバポートを含めないで、以下の IBM の snoop ユーティリティを使用します。

`http://hostname/snoop`

以下に例を示します。

`http://MyServer.MyCompany.com/snoop`

WebSphere が正しくインストールされている場合、ブラウザに同じ [Snoop Servlet—Request Client Information] ページが表示されます。これは、プロファイルが作成され、プラグインで設定される少なくとも 1 つのサーバがあることを意味します。

WebSphere のヘルプの詳細については、IBM カスタマ サポートにお問い合わせください。

CA Identity Manager 用の WebSphere の設定

ユーザの CA Identity Manager インストールが WebSphere で成功したことを確認するには、以下の手順に従います。

1. WebSphere 設定の変更を管理コンソールを介して保存します（マスタ構成に保存します）。
2. アプリケーションサーバをシャットダウンします。
3. 以下のフォルダのコンテンツを削除します。
 - 一時ディレクトリ：
 - Windows の場合： %temp%
 - UNIX の場合： /tmp/*
 - `WebSphere_home/profiles/WAS_PROFILE/temp/*`
 - `WebSphere_home/profiles/WAS_PROFILE/wstemp/*`
 - `WebSphere_home/profiles/WAS_PROFILE/tranlog/*`
 - `WebSphere_home/profiles/WAS_PROFILE/configuration/*`
 - `WebSphere_home/deploytool/itp/configuration/org.*`(このディレクトリに、`config.ini` のみを残す)
4. `WebSphere_home/profiles/WAS_PROFILE/properties/soap.client.props` ファイルで、`com.ibm.SOAP.requestTimeout` を 1800 以上に設定します。

注: 詳細については、WebSphere のマニュアルを参照してください。

重要: CA Identity Manager インストールの開始前に、WebSphere アプリケーションサーバを再起動してください。

Microsoft SQL での XA トランザクションの有効化

Microsoft SQL Server で WebSphere を使用している場合は、Microsoft SQL Server 上での XA トランザクションを有効にします。CA Identity Manager は、データベース トランザクションを正しく動作させるための XA データ ソースを必要とします。

以下の手順に従います。

1. Microsoft の Web サイトから [SQL Server JDBC Driver Version 2.0](#) をダウンロードします。

注: そのダウンロードは、ユーザが承認すべき使用許諾契約である HTML ファイルをまず示す場合があります。

2. JDBC ドライバをインストールするためにプログラムを実行します。
3. Microsoft のトピック「[Understanding XA Transactions](#)」に含まれる以下の 2 つの手順を実行します。
 - Running the MS DTC Service (MS DTC サービスを実行する)
 - Configuring the JDBC Distributed Transaction Components (JDBC 分散トランザクション コンポーネントを構成する)

これらの手順を実行する際に、以下が満たされていることを確認します。

- `xa_install.sql` スクリプトを実行する場合、スクリプトの完全なメッセージを取得していることを確認します。ユーザはドロップ テーブル エラーを無視できます。これは、このスクリプトを初めて実行したときに表示されます。
- `SqlJDBCXAUser` ロールにユーザを追加する場合、マスタ データベースにそのユーザを追加します。

SSL の環境設定

ユーザがアプリケーション サーバをアップグレードして、SSL を備えるユーザ ディレクトリを使用している場合は、SSL がアップグレード前にユーザのアプリケーション サーバで設定されていること確認してください。

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_semnu=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 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

注: Microsoft Windows プラットフォーム上では、CA IAM CS は IPv6 をサポートしません。CA Identity Manager r12.5 のリリース時点で IPv6 に対応する JDK はありません。IPv6 で動作する JDK がリリースされれば、[CA Support](#) にある CA Identity Manager サポート マトリックスが更新されます。

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 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、このシステム上に IPv6 サービスをインストールし、無効のままにします。

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。	

WebSphere 情報

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

フィールド名	説明	回答
WebSphere Install Folder	アプリケーション サーバのホーム ディレクトリの場所。	

フィールド名	説明	回答
Server Name	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。	
Profile Name	CA Identity Manager に対して使用するプロファイルの名前。	
Cell Name	アプリケーション サーバが存在するセルの名前。	
Node Name	アプリケーション サーバが存在するノードの名前。	
Cluster Name	高可用性実装のクラスタ名。ユーザが CA Identity Manager をクラスタ化された環境へのインストールを予定している場合にのみ必要です。	
Access URL and port	CA Identity Manager サーバ (アプリケーション サーバをホストするシステム) をホストするシステムのアプリケーション URL およびポート番号。	

データベース接続情報

Oracle または Microsoft SQL Server のデータベースがすでに設定されて動作している必要があります。 CA Identity Manager インストール中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用に作成されたデータベースのデータベースタイプ (ベンダー/バージョン)。	
Host Name	データベースがあ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提供することに注意してください。	
Port Number	データベースのポート番号。	

フィールド名	説明	回答
Database Name	データベース識別子。	
Username	データベース アクセス用のユーザ名。 注: スキーマを手動でインポートすることを予定している場合以外は、ユーザがデータベースに対する管理者権限を持っている必要があります。	
Password	管理者権限のあるユーザ アカウント用のパスワード。	

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。	

フィールド名	説明	回答
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。	
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](#) (P. 45)

[CA Identity Manager コンポーネント](#) (P. 46)

[単一ノードインストールを実行する方法](#) (P. 47)

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。
X	2. 以下のインストールのいずれかを実行します。 <ul style="list-style-type: none">■ 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) フェイルオーバー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。

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

CA Identity Manager の基本的なインストールを実行するために以下のチェックリストを使用します。



手順

1. CA Identity Manager コンポーネントを、必要なシステムにインストールします。
2. CA Identity Manager サーバが起動することを確認します。
3. リモート システムにインストールされている場合は、プロビジョニング マネージャを設定します。
4. 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

実稼働環境については、データ サーバ用に個別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) が 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上にあることをお勧めします。SiteMinder をインストールしている場合は、それを個別のシステム上に存在させることもあります。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、必要なシステムへのインストールを実行します。以下の手順では、インストーラを実行する手順は、ユーザのインストール メディアの最上位レベル フォルダにあるこのプログラムに参照しています。

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

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

インストールする各コンポーネントについて、ホスト名とパスワードなど、[インストーラ画面で必要な情報 \(P. 40\)](#)を持っていることを確認してください。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 \(P. 185\)](#)を確認します。

SiteMinder の拡張機能をインストールする方法

1. SiteMinder がインストールされているシステムに、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. リモート 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 を個別のシステムにインストールしている場合は、そこに SiteMinder の拡張機能もインストールしたことを確認してください。
2. 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。
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 サーバを選択します。
5. ローカルシステムに SiteMinder がある場合は、[Extensions for SiteMinder] を選択します。それがリモートシステムにある場合は、[Connect to 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 root（Solaris の場合）として、システムにログインします。
2. このシステムに 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、[CA Identity Manager Provisioning Directory Initialization] を選択します。
4. 展開サイズに関する質問に答えます。将来の増加に対応できるようにするには、以下のガイドラインを考慮してください。
 - コンパクト -- 10,000 以下のアカウント
 - 基本 -- 400,000 以下のアカウント
 - 中規模 -- 600,000 以下のアカウント
 - 大規模 -- 600,000 を超えるアカウント

5. 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、必要に応じて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。

Provisioning Directory Information

The Provisioning Server stores its data in a repository called the Provisioning Directory. To configure Provisioning Directory, enter the following information.

Provisioning Directory Host:	<input type="text" value="us-west3"/>
Provisioning Directory Shared Secret:	<input type="password" value="*****"/>
Confirm Shared Secret:	<input type="password" value="*****"/>

プロビジョニング サーバ証明書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 root（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いて、リモート プロビジョニング ディレクトリの詳細を得られることを確認してください。
3. インストーラを実行し、[CA Identity Manager Provisioning Server] を選択します。

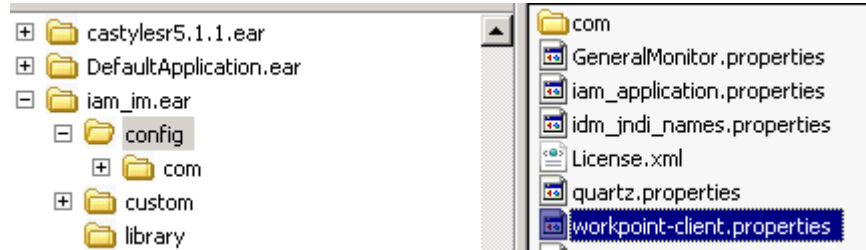
ユーザ プロファイルのワークフローの設定

インストールのデフォルト WebSphere プロファイルを使用していない場合は、WebSphere Server のワークフローを設定します。

以下の手順に従います。

1. WebSphere コンソールの起動
2. [Servers] - [Server Types] - [Application Servers] - [server_name] に移動します。
3. [Communications] の下で、[Ports] を展開します。
4. BOOTSTRAP_ADDRESS に使用されるポートをメモしておきます。

5. iam_im.ear/config にある Workpoint-client.properties ファイルを編集します。



6. このファイルの WebSphere セクションを見つけます。
java.naming.provider.url=iiop://localhost:2809
7. 2809 を BOOTSTRAP_ADDRESS 用に使用されるプロファイルのポートに置き換えます。
8. このサーバを再起動します。

CA Identity Manager サーバの起動の確認

以下の手順に従います。

1. 以下のようにして、CA Identity Manager を起動します。
 - **Windows の場合 :**
[スタート]-[すべてのプログラム]-[IBM WebSphere]-[Application Server Network Deployment *version*] - [Profiles] - [Profile Name] をクリックします。

注: ステータス情報を表示するには、ファースト ステップ コンソールを使用します。これには前述したサーバ開始コマンドと同じ場所からアクセスします。ファースト ステップ コンソールで、[Start the Server] を選択します。

■ **UNIX の場合 :**

- a. コマンドラインから `websphere_home/profiles/profile_name/bin` に移動します。
- b. 以下のコマンドを入力します。

```
startserver websphere_server
```

以下のメッセージが表示されれば、サーバはスタートアップ プロセスを完了しました。

```
Server server1 is open for e-business
```

2. 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。

3. 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
```

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)

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。

以下の手順に従います。

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。

第 4 章: WebSphere クラスタへのインストール

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 \(P. 55\)](#)

[WebSphere クラスタのセットアップ \(P. 56\)](#)

[CA Identity Manager を WebSphere クラスタにインストールする方法 \(P. 59\)](#)

[WebSphere クラスタの開始 \(P. 69\)](#)

[クラスタ化されたインストールの確認 \(P. 69\)](#)

[リモートプロビジョニングマネージャの設定 \(P. 70\)](#)

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。
X	2. 以下のインストールのいずれかを実行します。 <ul style="list-style-type: none">■ 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) フェイルオーバー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。

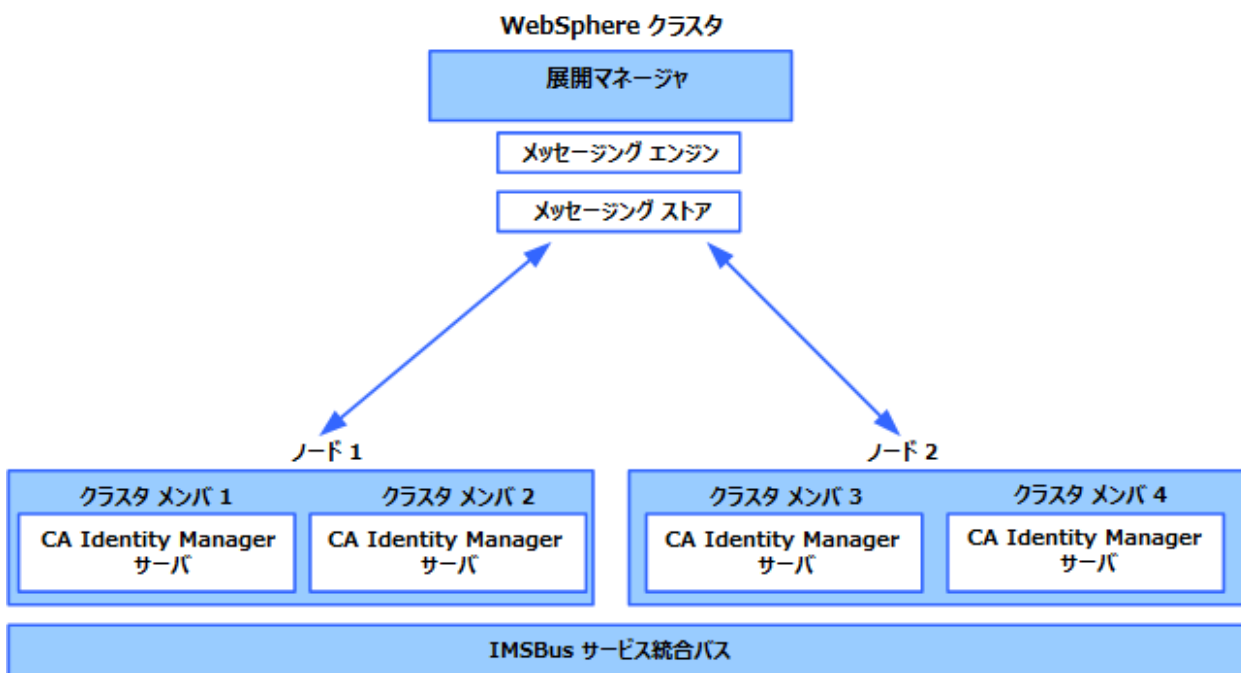
WebSphere クラスタのセットアップ

WebSphere クラスタ用にソフトウェアをインストールするときは、以下をセットアップします。

- 1つの WebSphere Deployment Manager -- ノードエージェントを介して、セルの他の連合プロファイルを管理します。
- 1つ以上のノード -- 各ノードには1つまたは複数のクラスタメンバ（サーバとも呼ぶ）が含まれます。それは CA Identity Manager サーバを実行させます。
- ノードエージェント -- Deployment Manager と連合プロファイルとの間の通信を管理するプロセス。
- サービス統合バス -- WebSphere 内のリソースをグループ化して、管理を簡略化します。WebSphere クラスタはバスのメンバとして追加されます。
- メッセージエンジン -- サービス統合バスのメンバ用のメッセージ機能を提供します。1つのメッセージエンジンがクラスタに対して存在します。
- メッセージストア -- メッセージエンジンのメッセージおよびトランザクションステータスを格納します。
- Web サーバ -- 適切なサーバにロードを分配し、SiteMinder がインストールされている場合は、クラスタメンバへのアクセスを保護します。

以下の図は、Deployment Manager、メッセージエンジン、メッセージストア、ノード、およびクラスタメンバの関係を示します。CA Identity Manager サーバは、Deployment Manager システムから各クラスタメンバにインストールされます。

注: これらのコンポーネントの詳細については、「[WebSphere System Management and Administration Redbook](#)」を参照してください。



WebSphere クラスタの前提条件

WebSphere クラスタ上の CA Identity Manager を設定する前に、WebSphere クラスタを作成するための概念および手順に精通する必要があります。WebSphere クラスタの詳細については、IBM WebSphere のドキュメントを参照してください。

また、「Installation Prerequisites」章の手順を必ず実行してください。

各 Node への WebSphere 7 のインストール

クラスタ メンバ用に使用した各システムに、WebSphere 7 をインストールします。

以下の手順に従います。

1. IBM WebSphere Application Server Network Deployment ソフトウェアを、各クラスタ メンバにインストールします。
2. プロファイル作成ウィザードを使用して、各ノードのデフォルト プロファイルを作成します。

このプロファイルを使用して、Deployment Manager への接続を設定します。

3. 以下のように各ノードを開始します。
 - a. 管理対象ノードがあるシステム上の
`was_home¥WebSphere¥AppServer¥bin` に移動します。
 - b. `startNode.bat¥.sh` コマンドを実行します。
4. 単一セルが、それと関連付けられたすべてのノードを以下の場所に持っていることを確認します。

`was_home/profiles/Deployment_Manager_Profile/config/cells/Cell_Name/Nodes/`
フォルダ名として表示されているすべての連合ノードを見てください。

ブートストラップ ポート (デフォルト : 2809) が一意でない場合、プロファイルの作成は時には失敗することがあります。作成されたプロファイルのログ フォルダ内の `pctLog.txt` ファイルのエラー メッセージをチェックできます。以下に例を示します。

```
(Oct 10, 2007 6:45:55 PM), Install,  
com.ibm.ws.install.ni.ismp.actions.ISMPWSPprofileLaunchAction, err, INSTCONFFAILED:  
Cannot complete required configuration actions after the installation. The  
configuration failed. The installation is not successful. Refer to C:¥Program  
Files¥IBM¥WebSphere¥AppServer¥logs¥wasprofile¥wasprofile_create_CustomIMFromNode.  
log for more details.
```

`wasprofile_create_CustomIMFromNode.log` の検査によると、この失敗は、一意でないブートストラップ ポートが原因でした。

1つのメンバを持つクラスタの作成

単一メンバを持つクラスタを設定します。CA Identity Manager をインストールした後、他のクラスタメンバを以下の手順で追加します。

以下の手順に従います。

1. 管理コンソールで、ノードが同期済みステータスを表示することを確認します。
2. クラスタ作成ウィザードを使用して、1つのメンバを持つクラスタを作成します。

このウィザードを使用する際に作成するクラスタ名およびサーバノード名に注意してください。サーバノードは、クラスタメンバノードです。

3. クラスタメンバを停止しますが、ノードエージェントは実行させておきます。

CA Identity Manager を WebSphere クラスタにインストールする方法

以下の手順では、CA Identity Manager を WebSphere クラスタにインストールする方法について説明します。



手順

1. 展開マネージャからインストールを実行します。
 2. クラスタメンバを追加します。
 3. 中核的なグループポリシーを割り当てます。
 4. クラスタメンバのワークフローを設定します。
 5. プロキシプラグインを設定します。
-

インストールによって作成されるオブジェクト

以下の手順で説明するように、CA Identity Manager をインストールします。インストール中に、以下の EAR がクラスタ ドメインにインストールされます。

- iam_im.ear
- ca-stylesr5.1.1.ear

インストール中にクラスタ名を入力すると、以下のプライマリ リソースが設定されます。

- クラスタのターゲットとなる配布キュー/トピック
- クラスタのターゲットとなる接続ファクトリ
- クラスタのターゲットとなるデータ ソース
- iam_im-IMSBUS、CA Identity Manager のサーバ統合バス
- クラスタのメッセージエンジンストア
- メッセージエンジンによって使用される中核的なグループ ポリシー

Deployment Manager のインストールの実行

WebSphere クラスタを作成すると、CA Identity Manager をそれにインストールできます。CA Identity Manager をすべてのクラスタ メンバにインストールするには、この手順およびこれに続く手順を使用します。

注: CA Identity Manager の前のリリースでは、メッセージストアおよびメッセージエンジンの作成は手動のプロセスでした。本リリースでは、空のメッセージストアデータベースを作成し、CA Identity Manager インストーラを実行する際、そのデータベース名を提供します。その後 WebSphere はメッセージストアテーブルを設定し、メッセージエンジンを作成し、クラスタ内の各ノードに挿入します。アプリケーション ear およびバイナリをデプロイします。

以下の手順に従います。

1. Microsoft SQL サーバを使用している場合は、以下の手順を実行します。
 - a. SQL 管理コンソールを開きます。
 - b. メッセージストア データベースを所有するユーザを見つけます。
 - c. そのユーザのデフォルト スキーマを `dbo` に設定します。
2. Deployment Manager を有するシステムにログインします。
 - Windows で、Windows 管理者としてログインします。
 - UNIX で、`root` としてログインします。
3. 1 番目のクラスタ メンバ（これまで設定したただ 1 つのクラスタ メンバ）を停止します。
4. そのクラスタ メンバのノードエージェントを開始します。
5. WebSphere Deployment Manager を停止します。
6. Deployment Manager をホストするシステムで、CA Identity Manager インストールを実行します。
 - 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、ホスト名およびポートなどインストーラが必要とする情報を収集してあることを確認してください。

7. 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。

注: 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。ユーザの前のインストールが CA Identity Manager r12 だった場合、一部のシナリオにそれらが表示されます。

8. 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、必要に応じて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。

Provisioning Directory Information

The Provisioning Server stores its data in a repository called the Provisioning Directory. To configure Provisioning Directory, enter the following information.

Provisioning Directory Host:	<input type="text" value="us-west3"/>
Provisioning Directory Shared Secret:	<input type="password" value="*****"/>
Confirm Shared Secret:	<input type="password" value="*****"/>

9. 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。
[WebSphere] セクションには、以下のフィールドがあります。

WebSphere Install Folder

WebSphere がインストールされているフォルダまたはディレクトリ。Windows または UNIX ファイルシステムにこの場所が表示されます。

Server Name

WebSphere クラスタ内の 1 番目のクラスタ メンバ。 WebSphere コンソールにこの名前が表示されます。

Profile Name

展開マネージャのプロファイル。 Windows または UNIX ファイルシステムのパスにこの名前が表示されます。

was_home/profiles/Deployment_Manager_Profile

Cell Name

WebSphere コンソールで表示できる展開マネージャのセル。

注: セル名は、すべてのオペレーティング システムで大文字と小文字が区別されます。 大文字と小文字を正しく使用していることを確認してください。

Node Name

この画面で入力したサーバ名が含まれるノード。 WebSphere コンソールにこの名前が表示されます。

注: ノード名は、すべてのオペレーティング システム内で大文字と小文字が区別されます。 大文字と小文字を正しく使用していることを確認してください。

Cluster Name

クラスタの名前です。 WebSphere コンソールにこの名前が表示されます。

Access URL and port

負荷分散に使用される Web Server の URL およびポート番号。

For automatic deployment, enter the application server information.
Enter the fully-qualified URL with port number in Access URL field.

For manual deployment, select the check box to generate EARs.
No additional information is required.

WebSphere Install Folder:

Server Name:

Profile Name:

Cell Name:

Node Name:

Cluster Name:

Access URL and port:

10. メッセージストアセクションの入力を完了させます。インストーラは、提供する以下の情報に基づいてメッセージエンジンのメッセージストアとして JDBC データ ソースを作成します。

- ホスト名
- ポート
- データベース名
メッセージストア データベースを入力します。
- ユーザ名
メッセージストア データベースを所有するユーザを入力します。

- パスワード
- スキーマ名

Microsoft SQL Server の場合は、「dbo」と入力します。

Oracle の場合は、メッセージストア データベースを所有するユーザを入力します。

インストール中に問題が発生する場合は、インストール ログを検査します。

重要: クラスタはまだ機能しないため、開始しないでください。残りの手順を完了すると、クラスタを起動する準備が整います。

クラスタメンバの追加

最初のクラスタメンバをテンプレートとして使用して、クラスタにメンバを追加できるようになります。

以下の手順に従います。

1. Deployment Manager の管理コンソールで、[Servers] - [Clusters] に移動します。
2. プロファイルを作成したノードの 1 つを選択して、クラスタメンバを追加します。
3. 展開マネージャシステムから、sqljdbc.jar (Microsoft SQL Server の場合) または ojdbc14.jar (Oracle の場合) をクラスタメンバにコピーします。

展開マネージャシステムでは、JAR ファイルは WAS_INSTALL_ROOT/lib ディレクトリにあります。このクラスタメンバのシステム上の同じフォルダにこれをコピーします。

4. クラスタに追加される各クラスタメンバに対してこの手順を繰り返します。

中核的なグループポリシーの割り当て

クラスタでの高可用性および作業負荷管理を有効にするために、メッセージエンジンに対して中核的なグループポリシーが現在存在しています。このポリシー、IMSPolicy は、メッセージエンジンに優先使用するクラスタメンバを定義します。そのクラスタメンバが失敗した場合、メッセージエンジンは別のクラスタメンバに切り替えますが、再度利用可能になると、優先クラスタメンバに戻ります。

このポリシーにクラスタ メンバを追加するには、各クラスタ メンバに対してそれぞれ 1 回、以下の手順を実行します。このトピックの詳細については、「[WebSphere v7 System Management and Administration Redbook](#)」の「Setting up Preferred Servers in the Default Messaging Provider」のセクションを参照してください。

以下の手順に従います。

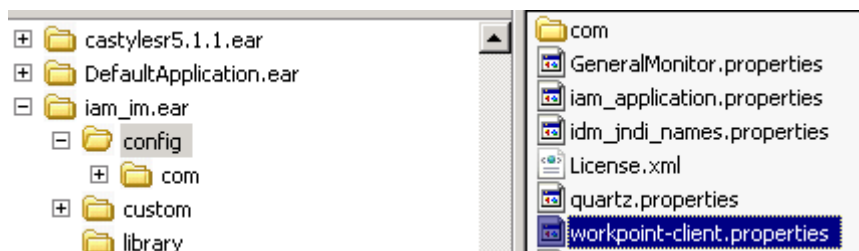
1. WebSphere コンソールで、[IMSpolicy] を見つけます。
これは、[Core Group] - [Default Core Group] - [Policies] にあります。
2. [Preferred Servers] を選択します。
コア グループ サーバのリストが表示されます。
3. [Preferred Servers] の下に各クラスタ メンバを追加します。
ノードエージェントまたは Deployment Manager を選択しないでください。
リストの最初のクラスタ メンバは、通信するエンジンがデフォルトで使用されるものです。使用される順番に表示されるまで、クラスタ メンバをリスト内で上または下へ移動します。
4. [OK] をクリックして変更内容を保存します。

クラスタ メンバのワークフローの設定

CA Identity Manager をインストールした Deployment Manager システムから、各クラスタ メンバのワークフローを設定します。

以下の手順に従います。

1. WebSphere コンソールの起動
2. [Servers] - [Server Types] - [Application Servers] - [server_name] に移動します。
3. [Communications] の下で、[Ports] を展開します。
4. BOOTSTRAP_ADDRESS ポートの値をメモしておきます。
5. iam_im.ear/config にある workpoint-client.properties ファイルを編集します。



6. このファイルの WebSphere セクションを見つけます。
7. 2809 (デフォルトポート) を BOOTSTRAP_ADDRESS 用に使用されるプロファイルのポートに置き換えます。
8. 各ディレクトリに対してこの手順を繰り返します。
9. クラスタメンバを再起動します。

Web サーバ用のプロキシプラグインの設定

WebSphere が Web サーバと通信できるように、プロキシプラグインをインストールします。

以下の手順に従います。

1. Web サーバ用のプロキシプラグインのインストールについては、「[WebSphere System Management and Administration Redbook](#)」を参照してください。「Session Management」の章で、このプラグインについて説明しています。
2. プラグインをアクティブ化するために、Web サーバを再起動します。
 - IIS Web サーバの場合 -- マスタ WWW サービスで、WebSphere プラグイン (sePlugin) が SiteMinder Web エージェントプラグインの後に表示されること、および WebSphere プラグインが正常に起動することを確認してください。
 - Sun Java System Web Server の場合 -- WebSphere プラグイン (libns41_http.so) が SiteMinder Web エージェントプラグイン (NSAPIWebAgent.so) の後にロードされることを確認してください。

Sun Java System 6.0 Web Servers の場合は、
<sun_java_home>/https-instance/config/magnus.conf. 内のプラグインの順序をチェックしてください。

Sun Java System 5.x Web Servers の場合は、
<iplanet_home>/https-instance/config/magnus.conf から
<iplanet_home>/https-instance/config/obj.conf に以下の行をコピーします。

```
Init fn="load-modules" funcs="as_init,as_handler,as_term"  
shlib="/export/WebSphere/AppServer/bin/libns41_http.so"  
Init fn="as_init"  
bootstrap.properties="/export/WebSphere/AppServer/config/cells/plugin-cfg  
.xml"
```

以下を、AuthTrans fn="SiteMinderAgent" in the obj.conf ファイルの後に追加します。

```
Service fn="as_handler"
```

- Apache Web サーバの場合 -- Dynamic Shared Object (DSO) Support セクションの *Apache_home/config/httpd.conf* で、SiteMinder Web エージェントプラグイン (mod2_sm.so) が WebSphere プラグイン (mod_ibm_app_server_http.so) の前にロードされることを確認してください。

仮想ホスト エイリアスの設定

クラスタ内の最初のノード以外の任意のノードへのアクセスを有効にするには、WC_defaulthost ポートの値を仮想ホスト エイリアスとして使用します。

以下の手順に従います。

1. [General Properties] ページに移動します。
2. [Communications] セクションを見つけます。
3. WC_defaulthost ポートの値をメモしておきます。
4. [Hosts Alias] ページに移動します。

このページは、[Environment] - [Virtual host] のデフォルトホストの下にあります。

5. 2 番目のノード上のポートを確認します。

この値は、[General Properties] ページの WC_defaulthost の値と一致する必要があります。

6. 値が異なる場合は、[General Properties] の値と一致させるためにホストエイリアスを変更します。
7. 最初の 2 つのノード以外の各ノードに対してこの手順を繰り返します。

WebSphere クラスタの開始

WebSphere クラスタを開始するには、展開マネージャを開始し、次に、各管理対象のノードを開始します。

以下の手順に従います。

1. CA Identity Manager をサポートするポリシー サーバを開始します。
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 環境の作成または変更、WorkPoint 設定の変更の際に、1 つのポリシー サーバのみが実行されている必要があります。
2. 展開マネージャを実行します。
3. 最初の管理対象のノードで、以下の手順に従います。
 - a. `was_home¥WebSphere¥AppServer¥bin` に移動します。
 - b. `startNode.bat¥.sh` コマンドを実行します。
1 番目の管理対象のノードが開始します。
4. クラスタ内の各ノードで手順 3 を繰り返します。
5. Deployment Manager 上の WebSphere 管理コンソールの [Servers] - [Clusters] - [*cluster_name*] - [Cluster Members] で、各クラスタ メンバを開始します。
6. Deployment Manager 上の WebSphere 管理コンソールの [Service integration] - [Buses] - [iam_im-IMSBUS] - [Messaging Engines] で、クラスタの通信エンジンが実行されることを確認してください。
7. SiteMinder Web エージェントをインストールしている場合は、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。

以下の手順に従います。

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`

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。

以下の手順に従います。

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します。

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 \(P. 71\)](#)

[個別データベースの作成 \(P. 72\)](#)

[個別データベースを作成する方法 \(P. 73\)](#)

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。 <ul style="list-style-type: none">■ 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
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) フェイルオーバー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。

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 つと置換する場合があります。

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\imrexpertools\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 の個別のデータベースを作成する方法



手順

1. CA Identity Manager 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. JDBC リソースを作成します。
3. データ ソースを編集します。
4. 接続プールプロパティを設定します。
5. (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

以下の手順に従います。

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ます、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

以下の手順に従います。

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。

JDBC リソースの作成

以下の手順に従います。

1. WebSphere 管理コンソールで、[Resources] - [JDBC] - [JDBC Providers] をクリックします。
2. スコープについては、Node=manualNode、Server=server-name を選択します。
3. [新規作成] をクリックします。

4. データベースに対するユーザの選択に応じて、[Create New JDBC provider] ページに入力します。以下の例では、JDBC プロバイダとして Microsoft SQL Server を表示します。

Create new JDBC provider

Set the basic configuration values of a JDBC provider, which encapsulates the specific vendor JDBC driver implementation classes that are required to access the database. The wizard fills in the name and the description fields, but you can type different values.

Scope
cells:manualCell:nodes:manualNode:servers:server1

Database type
SQL Server

Provider type
Microsoft SQL Server JDBC Driver

Implementation type
XA data source

Name
Microsoft SQL Server JDBC Driver (XA)

5. データベース クラス ページ情報を入力します。Microsoft SQL Server 用のディレクトリの場所が、以下の例に表示されます。

Enter database class path information

Set the environment variables that represent the JDBC driver class files, which WebSphere(R) Application Server uses to define your JDBC provider. This wizard page displays the file names; you supply only the directory locations of the files. Use complete directory paths when you type the JDBC driver file locations. For example: C:\SQLLIB\java on Windows(R) or /home/db2inst1/sqllib/java on Linux(TM).

If a value is specified for you, you may click Next to accept the value.

Class path:
\${MICROSOFT_JDBC_DRIVER_PATH}/sqljdbc.jar

Directory location for "sqljdbc.jar" which is saved as WebSphere variable \${MICROSOFT_JDBC_DRIVER_PATH}
\${WAS_LIBS_DIR}/sqljdbc.jar

Native library path
Directory location which is saved as WebSphere variable \${MICROSOFT_JDBC_DRIVER_NATIVEPATH}

6. [Summary] ページを確認してから、[Finish] をクリックします。

データソースの編集

以下の手順に従います。

1. WebSphere 管理コンソールで、[Resources] - [JDBC] - [Data sources] をクリックします。
2. スコープについては、Node=manualNode、Server=server-name を選択します。
3. [New] をクリックし、以下のようにデータソースを作成します。
 - データソース名には、「iam_im Object Store Data Source」と入力します。
 - JNDI名には、「iam/im/jdbc/jdbc/objectstore」と入力します
4. JDBC プロバイダを選択します。
5. 環境についてデータベース固有のプロパティを入力します。

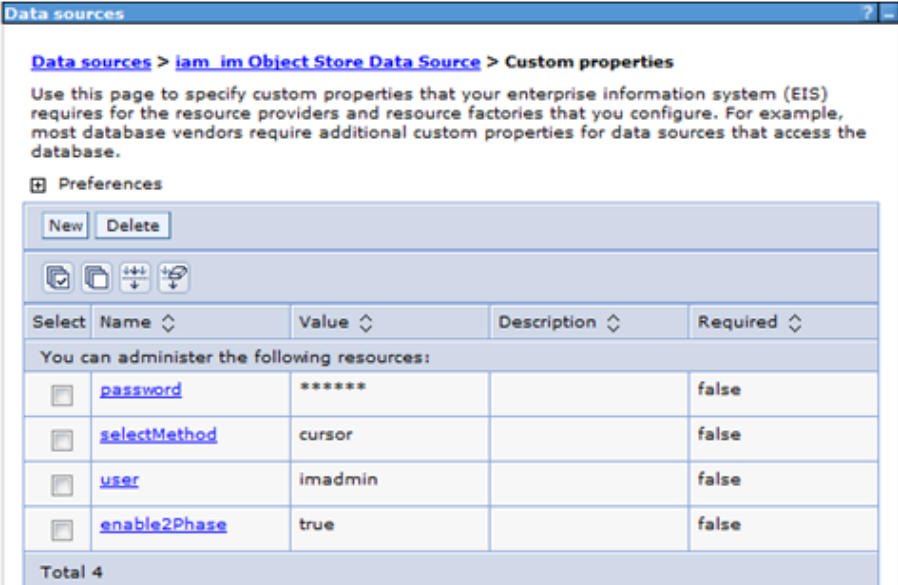
Name	Value
Database name	imstore
Port number	1433
Server name	localhost

Use this data source in container managed persistence (CMP)

6. セットアップセキュリティエイリアスについては、デフォルトを受け入れます。
7. [Summary] ページで、[Finish] をクリックします。
8. マスタ設定に変更を直接保存します。
9. 以下の手順に従って、データソースにカスタムプロパティを追加します。
 - a. データソースページで、[iam_im Object Store Data Source] を選択します。
 - b. [Additional Properties] で、[Custom properties] を選択します。

- c. ユーザのデータベースに応じて、以下のプロパティを追加します。
- **SQL** : user=<username>、password=<password>、enable2Phase=true、selectMethod=cursor
 - **Oracle** : user=<username>、password=<password>

注: JDBC プロバイダが「XA」として作成されていることを確認してください。



The screenshot shows the 'Data sources' configuration page for 'iam_im Object Store Data Source' under 'Custom properties'. The page includes a 'Preferences' section with a table of properties. The table has columns for 'Select', 'Name', 'Value', 'Description', and 'Required'. The properties listed are: password (value: *****), selectMethod (value: cursor), user (value: imadmin), and enable2Phase (value: true). All properties are marked as 'Required: false'.

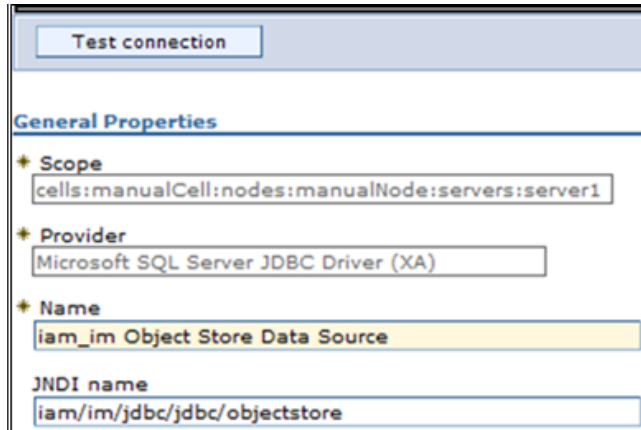
Select	Name	Value	Description	Required
<input type="checkbox"/>	password	*****		false
<input type="checkbox"/>	selectMethod	cursor		false
<input type="checkbox"/>	user	imadmin		false
<input type="checkbox"/>	enable2Phase	true		false

Total 4

10. マスタ設定に変更を直接保存します

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

11. データ ソース接続をテストします。



失敗は通常、クラスパスまたはクレデンシヤルに関連しています。テスト接続が合格したら、データ ソース設定は完全です。

12. 追加の 4 つのデータ ソースを設定する必要があります。この手順を繰り返しますが、以下のテーブルのデータ ソースおよび JNDI 名を使用します。

データソース	JNDI 名
iam_im Task Persistence Data Source	iam/im/jdbc/jdbc/idm
iam_im Workflow Data Source	iam/im/jdbc/jdbc/WPDS
iam_im Snapshots Data Source	iam/im/jdbc/jdbc/reportsnapshot
iam_im Archive Data Source	iam/im/jdbc/jdbc/archive

接続プール プロパティの設定

すべてのデータ ソースについて適切なパフォーマンスを保証するには、デフォルト接続プール値を編集する必要があります。接続プールプロパティを以下のよう設定します。

- 接続タイムアウト： 10
- 最大接続数： 200

- 最小接続数 : 5
- リープ時間 : 150
- 未使用タイムアウト : 300
- 期限切れタイムアウト : 300
- ポリシー パージ : FailingConnectionOnly

SQL スクリプトの実行

CA Identity Manager の起動時に、SQL スクリプトはデータベースに対して自動的に実行されますが、ユーザ自身が SQL スクリプトを実行する場合は、アプリケーション サーバを再起動する前に以下の手順に従ってください。

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。

以下の手順に従います。

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\imreexport\db\sqlserver\ims_mssql_report.sql
 - Windows 上の Oracle : C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\imreexport\db\oracle\ims_oracle_report.sql
 - UNIX 上の Oracle :
/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/imreexport/db/oracle/ims_oracle_report.sql
 - ワークフロー：「ワークフローのスキプトの実行」のセクションを参照してください。
3. スクリプトを実行します。
 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。

ワークフローのスキプトの実行

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

以下の手順に従います。

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 sqjjdbc.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: 手動による EAR のデプロイ

このセクションには、以下のトピックが含まれています。

- [手動でデプロイする方法 \(P. 83\)](#)
- [手動デプロイの前提条件 \(P. 84\)](#)
- [プライマリ リソースの作成 \(P. 84\)](#)
- [中核的なグループ ポリシーの割り当て \(P. 86\)](#)
- [EAR ファイルの生成 \(P. 87\)](#)
- [castylesr5.1.1.ear ファイルの展開方法 \(P. 87\)](#)
- [iam_im.ear のデプロイ \(P. 88\)](#)
- [ポリシー サーバとワークフローのオブジェクトの作成 \(P. 92\)](#)
- [メッセージ駆動型ビーン リスナー バインディングの作成 \(P. 93\)](#)
- [user_console.war の編集 \(P. 95\)](#)
- [wpServer.Jar の編集 \(P. 95\)](#)
- [SiteMinder への接続 \(P. 96\)](#)
- [RCM への接続 \(P. 97\)](#)
- [プロビジョニング サーバの共有秘密キーの作成 \(P. 99\)](#)
- [クラスタ用のポストデプロイ手順の実行 \(P. 99\)](#)

手動でデプロイする方法

手動で CA Identity Manager 12.6.4 をデプロイするには、WebSphere 7 で以下の手順を実行します。手順についてはこの章で説明します。



手順

1. 前提条件をレビューします。
 2. プライマリ リソースを作成します。
 3. クラスタがある場合は、コア グループ ポリシーを割り当てます。
 4. EAR ファイルを生成します。
 5. ca-styles5.1.1.ear をデプロイします。
 6. iam_im.ear をデプロイします。
 7. ポリシー サーバとワークフローのオブジェクトを作成します。(すべてのインストールに必要。)
 8. メッセージ駆動型ビーン リスナー バインディングを作成します。
-



手順

9. user_console.war を編集します。
10. SiteMinder がインストールされている場合は、それに接続します。
11. RCM がインストールされている場合は、それに接続します。
12. プロビジョニング サーバの共有秘密キーを作成します。
13. クラスタに対してデプロイ以降の手順を実行します。

手動デプロイの前提条件

CA Identity Manager 12.6.4 を手動デプロイの前に、以下の前提条件を確認します。

- [データベースの作成](#) (P. 73) 手順を使用して、必要な JDBC リソースを作成し、データソースを編集し、接続プールプロパティを設定します。
- [WebSphere の前提条件](#) (P. 33) を満たしていることを確認します。
- CA Identity Manager サーバで高可用性が必要な場合は、WebSphere クラスタを作成します。

プライマリリソースの作成

JMS のリソースおよびサービス統合バスを作成するには、WebSphere ツールフォルダにある JACL スクリプトを実行します。ユーザの環境によって、単一ノードまたはクラスタのいずれかの手順を使用します。

単一ノード用プライマリ リソースの作成方法：

以下の手順に従います。

1. コマンドラインを開き、以下の場所に移動します。
`websphere_home/profiles/profile_name/bin`
2. 以下のように `imssetup.jacl` を実行します。
`wsadmin -f websphere_tools/imssetup.jacl myNodeName myServerName`
3. リソースが作成されたことを検証するには、WebSphere の管理コンソールからリソースの設定を確認します。具体的な内容は次のとおりです。
 - a. サービス統合、バスの下を確認します。

b. リソース、JMS の下の以下の項目を確認します。

- キュー接続ファクトリ
- トピック接続ファクトリ
- キュー
- トピック
- アクティベーション設定

各 CA Identity Manager リソースは、iam プレフィックスから始まります。

クラスタ用プライマリ リソースの作成方法：

以下の手順に従います。

1. CreateCoreGroupPolicy.jacl を、WAS_ROOT/bin から 展開マネージャの profile/bin フォルダにコピーします。
2. 以下の変数の IMSCoreGroupPolicy.properties を編集します。
 - \$WAS_CLUSTER\$ - クラスタ名。この変数が含まれる全文字列は通信するエンジン名に相当します。
 - \$WAS_NODE\$ - クラスタ メンバが作成されるノード。展開マネージャのノード名とは異なる場合があります。
 - \$WAS_SERVER\$ - クラスタ メンバの名前。
3. コマンドラインを開き、以下の場所に移動します。
`websphere_home/profiles/profile_name/bin`
4. クラスタの各ノードで `imsSetupCluster.jacl` を以下のように実行します。
`wsadmin -f websphere_tools/imsSetupCluster.jacl NodeName ClusterMemberName ClusterName SchemaName`

注：SchemaName パラメータは `imsSetupCluster.jacl` に渡される文字列で、各クラスタ メンバと関連付けられるメッセージエンジン用スキーマ名を指定します。この文字列は後で変更できます。
5. リソースが作成されたことを検証するには、Webphere の管理コンソールからリソースの設定を確認します。具体的な内容は次のとおりです。
 - a. サービス統合、バスの下を確認します。

b. リソース、JMS の下の以下の項目を確認します。

- キュー接続ファクトリ
- トピック接続ファクトリ
- キュー
- トピック
- アクティベーション設定

各 CA Identity Manager リソースは、iam プレフィックスから始まります。

中核的なグループ ポリシーの割り当て

クラスタでの高可用性および作業負荷管理を有効にするために、メッセージエンジンに対して中核的なグループ ポリシーが現在存在しています。このポリシー、IMSPolicy は、メッセージエンジンに優先使用するクラスタ メンバを定義します。そのクラスタ メンバが失敗した場合、メッセージエンジンは別のクラスタ メンバに切り替えますが、再度利用可能になると、優先クラスタ メンバに戻ります。

このポリシーにクラスタ メンバを追加するには、各クラスタ メンバに対してそれぞれ 1 回、以下の手順を実行します。このトピックの詳細については、[「WebSphere v7 System Management and Administration Redbook」](#)の「Setting up Preferred Servers in the Default Messaging Provider」のセクションを参照してください。

以下の手順に従います。

1. WebSphere コンソールで、[IMSpolicy] を見つけます。

これは、[Core Group] - [Default Core Group] - [Policies] にあります。

2. [Preferred Servers] を選択します。

コア グループ サーバのリストが表示されます。

3. [Preferred Servers] の下に各クラスタ メンバを追加します。

ノードエージェントまたは Deployment Manager を選択しないでください。

リストの最初のクラスタ メンバは、通信するエンジンがデフォルトで使用されるものです。使用される順番に表示されるまで、クラスタ メンバをリスト内で上または下へ移動します。

4. [OK] をクリックして変更内容を保存します。

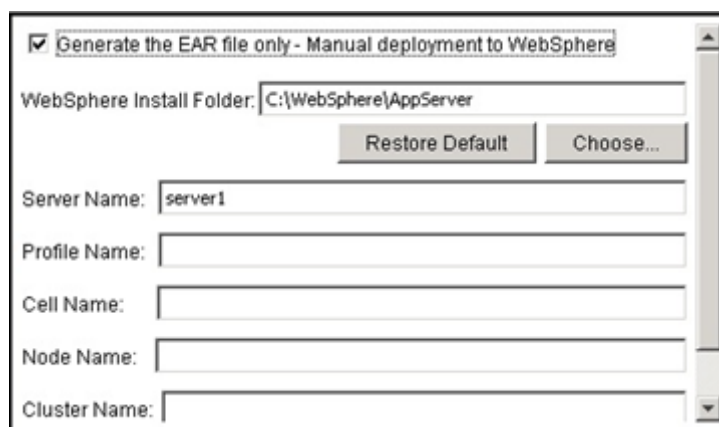
EAR ファイルの生成

以下の手順に従います。

CA Identity Manager インストーラを実行し、[Generate EAR file only] オプションを選択します。インストーラは以下の EAR ファイルを作成します。

- WAS_IMR12.ear : これは圧縮された iam_im.ear (CA Identity Manager アプリケーションの EAR ファイル) です。
- WAS_caStyles.ear : これは圧縮された castyles5.1.1.ear (CA Identity Manager スタイルシートの EAR ファイル) です。

これらのファイルは、インストール中に指定する場所にインストールされます。



また、そのインストールは以下のフォルダを作成します。

- *install_location*\IAM Suite\WebSphere-ear - EAR ファイルおよび展開されたバックアップファイルが含まれています。
- *install_location*\IAM Suite\WebSphere-tools - JACL スクリプトおよび他のツールが含まれています

castylesr5.1.1.ear ファイルの展開方法

EAR ファイルを生成した後に、ca-styles5.1.1.ear のデプロイを開始します。

以下の手順に従います。

1. WebSphere 管理コンソールで、[Applications] - [New Application] - [New Enterprise Application] をクリックします。
2. ca-stylesr5.1.ear ファイルの場所を入力します。

3. すべてのデフォルト設定をそのまま使用します。
4. [Select installation options] の下で、以下のオプションを選択します。
 - アプリケーションの配布
 - リソース用の MBean の作成
5. [Map modules to servers] ページで以下の手順に従います。
 - セルとサーバ名がリスト表示されることを確認します。
 - Module CA Styles r5.1.1 を選択します。
6. [Map virtual hosts for Web modules] ページで、[Web module CA Styles R5.1.1] を選択します。
7. [Virtual host] 列の [default_host] を選択します。
8. [Next] をクリックして、[Finish] をクリックします。
アプリケーションがインストールされています。
9. マスタ設定に直接保存します。
10. [Applications] - [Application Types] - [WebSphere enterprise applications] をクリックします。
11. [castyles5.1.1] を選択し、[Start] をクリックします。
12. ステータスフィールドが [Started] に変わったことを確認します。

iam_im.ear のデプロイ

WebSphere 7 への iam_im.ear のデプロイについて、2つのオプションが存在します。JACL スクリプトを使用することも、WebSphere 管理コンソールを使用することもできます。

JACL スクリプトによる iam_im.ear のデプロイ

iam_im.ear をデプロイする最も単純なメソッドは、JACL スクリプトを使用することです。

以下の手順に従います。

JACL で iam_im.ear をデプロイするには、以下の手順に従います。

1. 圧縮した iam_im.ear ファイルを以下のディレクトリにコピーします。
`websphere_home/profiles/profile_name/bin`
2. コマンドラインを開き、前のディレクトリに移動します。

- 以下のいずれかのコマンドを実行します。

単一ノード : `wsadmin -f WebSphere-tools/imsinstall.jacl path_to_EAR`

クラスタ : `wsadmin -f WebSphere-tools/imsinstall.jacl path_to_EAR ClusterName`

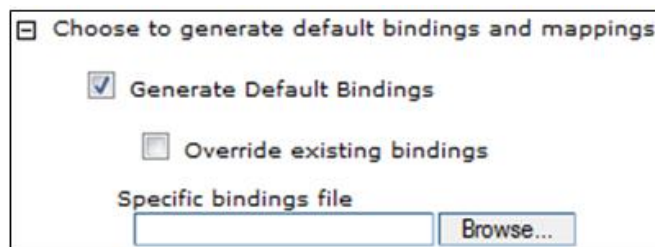
重要: この手順が成功した場合、[user console.war の編集 \(P. 95\)](#)を続行します。この手順が失敗した場合、[WebSphere 管理コンソールから iam_im.ear をデプロイする \(P. 89\)](#)手順を使用します。

WebSphere 管理コンソールからの iam_im.ear のデプロイ

JACL スクリプトを使用した iam_im.ear のデプロイが機能しなかった場合は、代わりにこの手順を使用します。

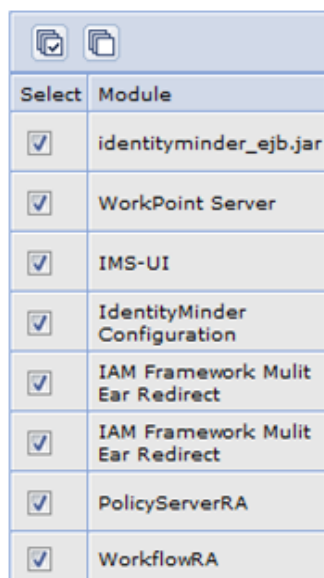
以下の手順に従います。

- WebSphere 管理コンソールにログインします。
- [Applications] - [New Applications] - [New Enterprise Application] をクリックします。
- [Install] をクリックします。
- 生成した EAR ファイルの場所を入力します。
- 以下のようにダイアログ ボックスに入力します。
 - [Fast Path] を選択します。
 - [Choose to generate default bindings and mappings] を展開します。
 - [Generate Default Bindings] を選択します。



- インストール オプションのページで、変更は不要です。

7. [Map modules to servers] ページで以下の手順に従います。
 - a. [Clusters or Servers] フィールドに必要な応じて入力します。
 - b. すべてのモジュールを選択します。



Select	Module
<input checked="" type="checkbox"/>	identityminder_ejb.jar
<input checked="" type="checkbox"/>	WorkPoint Server
<input checked="" type="checkbox"/>	IMS-UI
<input checked="" type="checkbox"/>	IdentityMinder Configuration
<input checked="" type="checkbox"/>	IAM Framework Mult Ear Redirect
<input checked="" type="checkbox"/>	IAM Framework Mult Ear Redirect
<input checked="" type="checkbox"/>	PolicyServerRA
<input checked="" type="checkbox"/>	WorkflowRA

8. [Map virtual hosts to Web modules] ページで、すべてのモジュールを選択します。
9. 以下の例のように、[Summary] ページが表示されることを確認します。

Options	Values
Precompile JavaServer Pages files	No
Directory to install application	
Distribute application	Yes
Use Binary Configuration	No
Deploy enterprise beans	Yes
Application name	iam_im
Create MBeans for resources	Yes
Override class reloading settings for Web and EJB modules	No
Reload interval in seconds	
Deploy Web services	No
Validate Input off/warn/fail	warn
Process embedded configuration	No
File Permission	.*\,dll=755#.*\,so=755#.*\,a=755#.*\,sl=755
Application Build ID	Unknown
Allow dispatching includes to remote resources	No
Allow servicing includes from remote resources	No
Business level application name	
Asynchronous Request Dispatch Type	Disabled
Allow EJB reference targets to resolve automatically	No
Cell/Node/Server	Click here

10. [Finish] をクリックして、ear をデプロイします。
注: この手順の完了には時間がかかる場合があります。
11. マスタ設定にインストールを直接保存します。

ポリシー サーバとワークフローのオブジェクトの作成

JACL スクリプトの使用により iam_im.ear をデプロイすることに成功した場合は、この手順を省略できます。

以下の手順に従います。

1. WebSphere 管理コンソールで、[Servers] - [Server Types] - [WebSphere application servers] をクリックします。
2. [Application servers] ページで、該当する *server-name* をクリックします。
3. [Applications] の下のインストール済みのアプリケーションをクリックします。
4. 表示されるページの [iam_im] をクリックします。
5. [Modules] 下の [Manage Modules] をクリックします。
6. モジュールのリストの [PolicyServerRA] をクリックします。

Select	Module
<input type="checkbox"/>	identityminder_eib.jar
<input type="checkbox"/>	WorkPoint Server
<input type="checkbox"/>	IMS-UI
<input type="checkbox"/>	IdentityMinder Configuration
<input type="checkbox"/>	IAM Framework Multit Ear Redirect
<input type="checkbox"/>	IAM Framework Multit Ear Redirect
<input type="checkbox"/>	PolicyServerRA
<input type="checkbox"/>	WorkflowRA

7. [Additional Properties] 下の [Resource Adapter] をクリックします。
8. [Additional Properties] 下の [J2C connection factories] をクリックします。
9. [New] をクリックし、以下の値でオブジェクトを作成します。

名前 : iam_im-PolicyServerConnection

JNDI 名 : iam/im/rar/nete/rar/PolicyServerConnection

10. 画面の上部にあるメッセージボックスで、マスタ設定に直接保存します。
11. ワークフロー コネクタ オブジェクトを作成するには、以下の手順に従います
 - a. [Manage Modules] ページに戻ります。
このページに移動するには、手順 1～5 を繰り返すか、パンくずリストの [Manage Modules] をクリックします。
 - b. [WorkflowRA] をクリックします。
 - c. [Additional Properties] 下の [Resource Adapter] をクリックします。
 - d. [Additional Properties] 下の [J2C connection factories] をクリックします。
 - e. 以下の値でワークフロー コネクタ オブジェクトを作成します。
名前 : iam_im-Workflow
JNDI 名 : iam/im/rar/Workflow

メッセージ駆動型Beanリスナー バインディングの作成

JACL スクリプトの使用により iam_im.ear をデプロイすることに成功した場合は、この手順を省略できます。

以下の手順に従います。

1. WebSphere 管理コンソールで、[Applications]-[Application Types]-[WebSphere Enterprise Applications] に移動します。
2. [iam_im] をクリックします。
3. [Enterprise Java Bean Properties] 下の [Message Drive Bean listener bindings] を選択します。
4. [Listener bindings] 下の [Activation Specification] をクリックします。
5. identityminder_ejb.jar について、各 EJB モジュールに対して以下の値を入力します。

EJB	Listener Bindings
SubscriberMessageEJB	ターゲット リソース JNDI 名 : iam/im/ACT 送信先 JNDI 名 : iam/im/jms/queue/com.netegrity.ims.msg.queue

EJB	Listener Bindings
ServerCommandsEJB	ターゲットリソース JNDI 名 : iam/im/ServerCommand 送信先 JNDI 名 : iam/im/jms/topic/topic/ServerCommandTopic
RuntimeStatusDetailEJB	ターゲットリソース JNDI 名: iam/im/jms/RuntimeStatusDetailQueue 送信先 JNDI 名 iam/im/jms/queue/queue/RuntimeStatusDetailQueue

6. WorkPoint Server について、各 EJB モジュールに対して以下の値を入力します。

EJB	Listener Bindings
ServerAutomatedActivityMDBean	ターゲットリソース JNDI 名: iam/im/jms/wpServAutoActActSpec 送信先 JNDI 名 : iam/im/jms/queue/queue/wpServAutoActQueue
EventMDBean	ターゲットリソース JNDI 名: iam/im/jms/wpEventActSpec 送信先 JNDI 名 : iam/im/jms/queue/queue/wpEventQueue
UtilityMDBean	ターゲットリソース JNDI 名: iam/im/jms/wpUtilActSpec 送信先 JNDI 名: iam/im/jms/queue/queue/wpUtilQueue

7.7. [OK] をクリックします。

8.8. マスタ設定に変更を直接保存します。

9.9. WebSphere を再起動します。

user_console.war の編集

user_console.war ファイル内のクラス ロード順序をリセットするためにこの手順を使用します。

以下の手順に従います。

1. [Application] - [WebSphere enterprise applications] - [iam_im] をクリックします。
2. [Modules] の下で、[Manage modules] をクリックします。
3. [IMS-UI] をクリックします。
4. クラス ロード順序を以下の選択に設定します。
[Classes loaded with local class loader first (parent last)]
5. マスタ設定に直接保存します。
6. WebSphere アプリケーション サーバを再起動します。

wpServer.Jar の編集

Workpoint Server JAR ファイルの開始ウェイトを変更するには、この手順に従います。

以下の手順に従います。

1. [Application] - [WebSphere enterprise applications] - [iam_im] をクリックします。
2. [Modules] の下で、[Manage modules] をクリックします。
3. Workpoint Server をクリックします。
4. 開始ウェイトを 500 に設定します。
5. マスタ設定に直接保存します。
6. WebSphere アプリケーション サーバを再起動します。

SiteMinder への接続

SiteMinder ポリシー サーバに接続するには、以下の手順に従います。クラスタについて、各クラスタ メンバでこれらの手順を実行します。

以下の手順に従います。

1. WebSphere アプリケーション サーバシステムで、`was_home/bin/` に移動します。
2. `startServer.sh` ファイルを編集します。Start CA IAM Suite セクション下の SMPS 変数に以下のパスを追加します。

```
was_home/profiles/profile_name/installedApps/profile_name/iam_im.ear/library
```

3. WebSphere アプリケーション サーバを起動します。
4. WebSphere 管理コンソールで、[Application servers] - [your_server] - [Install Applications] - [IdentityMinder] - [Manage Modules] - [policyserver.rar] - [IdentityMingerPolicyServerRA] - [J2C connection factories] に移動します。

5. 以下の JNDI 名を持つオブジェクトをクリックします。

```
nete/rar/PolicyServerConnection
```

6. [Custom Properties] をクリックします。

7. 以下のパラメータを設定します。

- ValidateSMHeadersWithPS = true
- Enabled = true
- ConnectionUrl = hostname of the SiteMinder system
- Username = SiteMinder administrative user
- AgentSecret = SiteMinder Agent secret
- AgentName = SiteMinder Agent name
- AgentSecret = SiteMinder Agent secret

8. [SiteMinder Administrative UI] で、ユーザの WebSphere リソースを保護するエージェントのエージェント設定オブジェクトを作成します。

注: エージェント設定を作成する詳細については、「SiteMinder ポリシー サーバ設定ガイド」を参照してください。

9. 以下の場所に移動します。

```
was_home¥config¥cells¥cellname¥applications¥iam_im.ear¥deployments¥IdentityMinder¥user_console.war¥WEB-INF
```

10. web.xml ファイルを編集し、AgentFilter および FrameworkAuthFilter に対して、enabled=false を設定します。以下に例を示します。

```
<filter-name>AgentFilter</filter-name>
<filter-class>com.netegrity.proxy.AgentFilter</filter-class>
</init-param>
  <param-name>EnableAgent</param-name>
  <param-value>false</param-value>
</init-param>
<filter-name>FrameworkAuthFilter</filter-name>

  <filter-class>com.netegrity.webapp.authentication.FrameworkLoginFilter</f
ilter-class>
  </init-param>
    <param-name>Enable</param-name>
    <param-value>false</param-value>
  </init-param>
```

11. SiteMinder システムで CA Identity Manager インストーラを実行し、SiteMinder の拡張機能をインストールします。

RCM への接続

インストールの中に Role and Compliance Manager (RCM) がある場合は、RCM に WebSphere を接続するように設定します。

以下の手順に従います。

1. WebSphere 管理コンソールにログインします。
2. バス送信先として以下のようにキューを作成します。
 - a. [Service Integration] - [Buses] をクリックします。
 - b. [iam_im-IMSBus] をクリックします。
 - c. [Destination Resources] の下で、[Destinations] をクリックします。
 - d. [New] をクリックします。
 - e. [Queue] をクリックします。

- f. [Identifier] については、「AnalyticsNotificationQueue」と入力します。

Create new queue

Create a new queue for point-to-point messaging.

→ **Step 1: Set queue attributes**

Step 2: Assign the queue to a bus member

Step 3: Confirm queue creation

Set queue attributes

Configure the attributes of your new queue

* Identifier
AnalyticsNotificationQueue

Description

3. 以下のように JMS のキューを作成します。
- [Resources] - [JMS] - [Queues] をクリックします。
 - [New] をクリックします。
 - [Default messaging provider] をクリックします。
 - 次のフィールドに以下の値を入力します。

Name

AnalyticsNotificationQueue

JNDI Name

iam/im/jms/queue/analytics/AnalyticsNotificationQueue

Bus Name

IMSBus

Queue Name

AnalyticsNotificationQueue

4. キューの有効化指定を以下のように作成します。
- [Resources] - [MS] - [Activation Specifications] をクリックします。
 - [New] をクリックします。
 - [Default messaging provider] をクリックします。
 - 以下の値を入力します。

Name

AnalyticsNotificationQueueActSpec

JNDI Name

iam/im/jms/analytics/AnalyticsNotificationQueue/ActSpec

送信先 JNDI 名

iam/im/jms/queue/analytics/AnalyticsNotificationQueue

この名前は、手順 3 で作成された JNDI 名と一致している必要があります。

プロビジョニング サーバの共有秘密キーの作成

CA Identity Manager サーバと通信するために共有秘密キーを作成する必要があります。

以下の手順に従います。

1. パスワード ツールを使用して、暗号化された共有秘密キーを生成します。
2. `systemWideProperties.properties` ファイル内のプロビジョニング サーバ共有秘密キーを更新します。

クラスタ用のポスト デプロイ手順の実行

クラスタへの手動 EAR デプロイを実行している場合は、クラスタでのデプロイに適用される以下の手順を実行します。

クラスタ メンバの追加

最初のクラスタ メンバをテンプレートとして使用して、クラスタにメンバを追加できるようになります。

以下の手順に従います。

1. Deployment Manager の管理コンソールで、[Servers] - [Clusters] に移動します。
2. プロファイルを作成したノードの 1 つを選択して、クラスタ メンバを追加します。
3. 展開マネージャ システムから、`sqljdbc.jar` (Microsoft SQL Server の場合) または `ojdbc14.jar` (Oracle の場合) をクラスタ メンバにコピーします。

展開マネージャ システムでは、JAR ファイルは `WAS_INSTALL_ROOT/lib` ディレクトリにあります。このクラスタ メンバのシステム上の同じフォルダにこれをコピーします。

4. クラスタに追加される各クラスタ メンバに対してこの手順を繰り返します。

中核的なグループ ポリシーの割り当て

クラスタでの高可用性および作業負荷管理を有効にするために、メッセージ エンジンに対して中核的なグループ ポリシーが現在存在しています。このポリシー、**IMSPolicy** は、メッセージ エンジンに優先使用するクラスタ メンバを定義します。そのクラスタ メンバが失敗した場合、メッセージ エンジンは別のクラスタ メンバに切り替えますが、再度利用可能になると、優先クラスタ メンバに戻ります。

このポリシーにクラスタ メンバを追加するには、各クラスタ メンバに対してそれぞれ 1 回、以下の手順を実行します。このトピックの詳細については、[「WebSphere v7 System Management and Administration Redbook」](#)の「[Setting up Preferred Servers in the Default Messaging Provider](#)」のセクションを参照してください。

以下の手順に従います。

1. WebSphere コンソールで、**[IMSpolicy]** を見つけます。
これは、**[Core Group]** - **[Default Core Group]** - **[Policies]** にあります。
2. **[Preferred Servers]** を選択します。
コア グループ サーバのリストが表示されます。
3. **[Preferred Servers]** の下に各クラスタ メンバを追加します。
ノードエージェントまたは **Deployment Manager** を選択しないでください。
リストの最初のクラスタ メンバは、通信するエンジンがデフォルトで使用されるものです。使用される順番に表示されるまで、クラスタ メンバをリスト内で上または下へ移動します。
4. **[OK]** をクリックして変更内容を保存します。

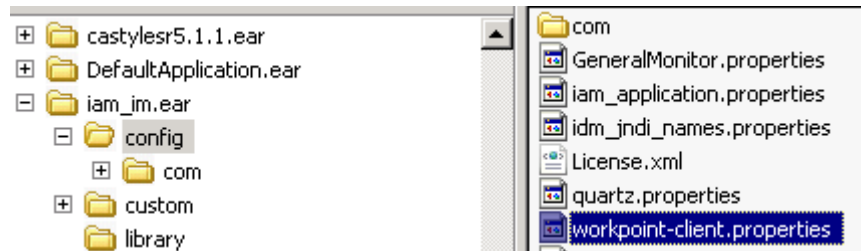
クラスタ メンバのワークフローの設定

CA Identity Manager をインストールした **Deployment Manager** システムから、各クラスタ メンバのワークフローを設定します。

以下の手順に従います。

1. WebSphere コンソールの起動
2. **[Servers]** - **[Server Types]** - **[Application Servers]** - **[server_name]** に移動します。
3. **[Communications]** の下で、**[Ports]** を展開します。

4. BOOTSTRAP_ADDRESS ポートの値をメモしておきます。
5. iam_im.ear/config にある workpoint-client.properties ファイルを編集します。



6. このファイルの WebSphere セクションを見つけます。
7. 2809 (デフォルトポート) を BOOTSTRAP_ADDRESS 用に使用されるプロファイルのポートに置き換えます。
8. 各ディレクトリに対してこの手順を繰り返します。
9. クラスタ メンバを再起動します。

Web サーバ用のプロキシ プラグインの設定

WebSphere が Web サーバと通信できるように、プロキシ プラグインをインストールします。

以下の手順に従います。

1. Web サーバ用のプロキシ プラグインのインストールについては「[WebSphere v7 System Management and Administration Redbook](#)」を参照してください。「Session Management」の章で、このプラグインについて説明しています。
2. プラグインをアクティブ化するために、Web サーバを再起動します。
 - IIS Web サーバの場合 -- マスタ WWW サービスで、WebSphere プラグイン (sePlugin) が SiteMinder Web エージェント プラグインの後に表示されること、および WebSphere プラグインが正常に起動することを確認してください。
 - Sun Java System Web Server の場合 -- WebSphere プラグイン (libns41_http.so) が SiteMinder Web エージェント プラグイン (NSAPIWebAgent.so) の後にロードされることを確認してください。

Sun Java System 6.0 Web Servers の場合は、

<sun_java_home>/https-instance/config/magnus.conf. 内のプラグインの順序をチェックしてください。

Sun Java System 5.x Web Servers の場合は、

<iplanet_home>/https-instance/config/magnus.conf から

<iplanet_home>/https-instance/config/obj.conf に以下の行をコピーします。

```
Init fn="load-modules" funcs="as_init,as_handler,as_term"  
shlib="/export/WebSphere/AppServer/bin/libns41_http.so"  
Init fn="as_init"  
bootstrap.properties="/export/WebSphere/AppServer/config/cells/plugin-cfg  
.xml"
```

以下を、AuthTrans fn="SiteMinderAgent" in the obj.conf ファイルの後に追加
します。

```
Service fn="as_handler"
```

- Apache Web サーバの場合 -- Dynamic Shared Object (DSO) Support セク
ションの *Apache_home/config/httpd.conf* で、SiteMinder Web エージェント
プラグイン (mod2_sm.so) が WebSphere プラグイン
(mod_ibm_app_server_http.so) の前にロードされることを確認してくだ
さい。

WebSphere クラスタの開始

WebSphere クラスタを開始するには、展開マネージャを開始し、次に、各管理対
象のノードを開始します。

以下の手順に従います。

1. CA Identity Manager をサポートするポリシー サーバを開始します。

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 環境の作成または変更、WorkPoint 設定の変更
の際に、1つのポリシー サーバのみが実行されている必要があります。

2. 展開マネージャを実行します。
3. 最初の管理対象のノードで、以下の手順に従います。
 - a. *was_home*¥WebSphere¥AppServer¥bin に移動します。
 - b. *startNode.bat*¥*sh* コマンドを実行します。
1 番目の管理対象のノードが開始します。
4. クラスタ内の各ノードで手順 3 を繰り返します。
5. Deployment Manager 上の WebSphere 管理コンソールの [Servers] - [Clusters]
- [*cluster_name*] - [Cluster Members] で、各クラスタ メンバを開始します。
6. Deployment Manager 上の WebSphere 管理コンソールの [Service integration] -
[Buses] - [*iam_im-IMSBus*] - [Messaging Engines] で、クラスタの通信エン
ジンが実行されることを確認してください。
7. SiteMinder Web エージェントをインストールしている場合は、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。

以下の手順に従います。

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`

第7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 \(P. 105\)](#)

[レポートिंगのアーキテクチャ \(P. 106\)](#)

[レポートの考慮事項 \(P. 107\)](#)

[ハードウェア要件 \(P. 107\)](#)

[レポートサーバをインストールする方法 \(P. 108\)](#)

[WebSphere でのレポートサーバ接続のセキュリティ保護 \(P. 121\)](#)

[レポートインストールの確認 \(P. 122\)](#)

[サイレントインストール \(P. 123\)](#)

[レポートをアンインストールする方法 \(P. 123\)](#)

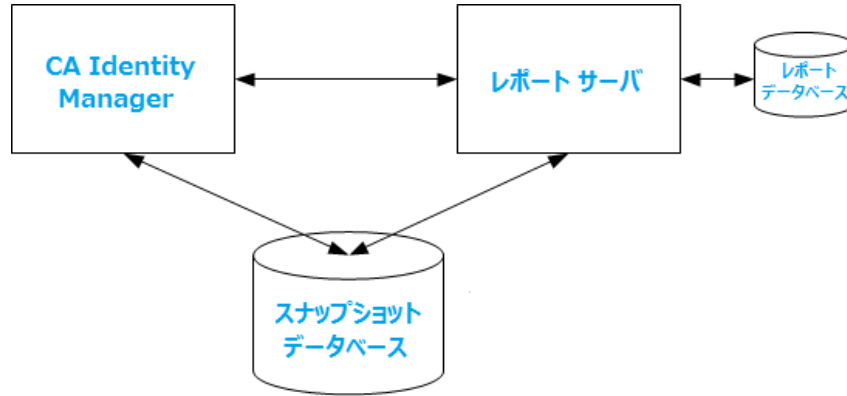
インストールステータス

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。 <ul style="list-style-type: none">■ 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) フェイルオーバー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。

レポートニ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\imreexport\db\sqlserver\ims_mssql_report.sql
 - Oracle : C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\imreexport\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/libOracle 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。	
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。	

フィールド名	説明	回答
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せん。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ため、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。

以下の手順に従います。

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。

以下の手順に従います。

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 `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へ移動します。
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

以下の手順に従います。

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回答します。
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中ではありません。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
```

- 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
```

- 以下のように、Crystal 処理サーバを再起動します。
 - 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。
 - 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

以下の手順に従います。

- 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
- 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。

- 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ン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。

以下の手順に従います。

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。

- 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。
- 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。

以下の手順に従います。

- 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。
- メインダッシュボードの下の [Servers] を選択します。
- [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。
- [Server Name] テキストボックスに、以下を入力します。
`Input.report_server_hostname.InputFileRepository`
- [Save] をクリックします。
- [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。
- [Server Name] テキストボックスに、以下を入力します。
`Output.report_server_hostname.OutputFileRepository`
- [Save] をクリックします。
- [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。

WebSphere でのレポートサーバ接続のセキュリティ保護

CA Identity Manager とレポートサーバは安全性の低い接続を介して通信しています。SSL (Secure Sockets Layer) 接続を使用して、レポートサーバと CA Identity Manager の間の接続をセキュリティ保護できます。

SSL 接続により、データがレポートサーバからアクセスされるときに通信が確実に暗号化されます。SSL を設定する前に、BO (Business Objects) サーバが HTTPS を使用可能であることを確認します。SSL との接続を安全にするために、自己署名証明書を使用するか、または証明局 (CA) の証明書を使用することができます。

[port] ページから [Retrieve] を使用して SSL 接続を設定するには、リモート SSL ポートから署名者証明書を取得します。SSL 設定を使用したハンドシェイク中に、システムは指定されたリモート SSL ホストおよびポートに接続して、署名者証明書を受信します。

以下の手順に従います。

1. WebSphere コンソールで、[Security] タスク下の [SSL certificate and key management] をクリックします。
2. [Related items] 下の [Keystores and certificates] をクリックします。
キーストアのリストが表示されます。
3. キーストアのリストの [NodeDefaultTrustStore] リンクをクリックします。
[General Properties] ページが表示されます。
4. [Additional Properties] 下の [Signer certificates] をクリックします。
5. ポート ボタンの [Retrieve] をクリックします。
6. 以下のフィールドに値を指定します。

Host

SSL ポートから署名者証明書を取得する際に接続するレポートサーバホスト名を指定します。

Port

署名者証明書を取得する際に接続する SSL ポートを指定します。

注: ネットワーク展開環境で、リモート SSL ポートから署名者証明書を取得しようとする際は、適切で安全なソケットレイヤ (SSL) ポート番号を指定します。

- デプロイメント マネージャから署名者証明書を取得する場合は、ポート名、WC_adminhost_secure と関連付けられたポート番号を使用します。

- ノードから署名者証明書を取得する場合は、ポート名、`CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS` と関連付けられたポート番号を使用します。

それらがデプロイメント マネージャまたはベース サーバから取得される前に、証明書がすべて利用可能であることを確認します。

送信接続の SSL 設定

以前に指定された SSL ポートに接続するように SSL 設定を指定します。以前に指定された SSL ポート設定も、取得後に署名者が含まれる SSL 設定です。SSL 設定では、SSL ポートの信頼できる証明書を持っている必要はありません。検証中に取得されてここに表示されます。

Alias

SSL 設定で指定されるキー ストアで参照された署名者証明書の証明書エイリアス名を指定します。

7. [Retrieve Signer Information] をクリックします。

署名者証明書に関する情報が表示されます。

8. [Apply] または [Save] をクリックします。

証明書がキーストアに格納されます。これで、SSL 証明書が設定されます。

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 サーバインストール 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. 123)。

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

以下の手順に従います。

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。

以下の手順に従います。

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 8 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](#) (P. 125)

[CA IAM CS のインストール](#) (P. 128)

[C++ Connector Server のインストール](#) (P. 131)

[CA IAM CS のサイレントインストール](#) (P. 132)

[CA IAM CS 用 SDK のインストール](#) (P. 133)

[コネクタ サンプルのインストール](#) (P. 133)

[JDBC サポートのセットアップ](#) (P. 134)

[コネクタのセットアップに関する詳細情報](#) (P. 139)

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
<i>im-home</i>	C:\Program Files\CA\Identity Manager	/opt/CA/IdentityManager
<i>imps-home</i>	C:\Program Files\CA\Identity Manager\Provisioning Server	/opt/CA/IdentityManager/ProvisioningServer
<i>cs-home</i>	C:\Program Files\CA\Identity Manager\Connector Server	/opt/CA/IdentityManager/ConnectorServer
<i>cs-sdk-home</i>	C:\Program Files\CA\Identity Manager\Connector Server SDK	/opt/CA/IdentityManager/ConnectorServer SDK
<i>conxp-home</i>	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。

以下の手順に従います。

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. 125) 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. 127) 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、インストール場所を変更できませんが、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 \(P. 131\)](#)」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。

以下の手順に従います。

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。

以下の手順に従います。

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。

以下の手順に従います。

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 自体が含まれません。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. 126)

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](#)

以下の手順に従います。

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、DB2 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。

以下の手順に従います。

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_05\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。

以下の手順に従います。

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9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 \(P. 141\)](#)

[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 \(P. 142\)](#)

[冗長プロビジョニング ディレクトリ \(P. 142\)](#)

[冗長プロビジョニング サーバ \(P. 146\)](#)

[冗長コネクタ サーバ \(P. 151\)](#)

[プロビジョニングクライアントのフェイルオーバー \(P. 161\)](#)

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。 <ul style="list-style-type: none">■ 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、フェイルオーバーと負荷分散をサポートします。

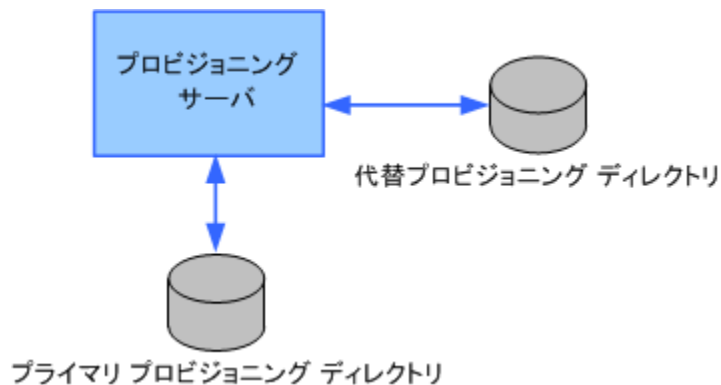
高可用性プロビジョニング コンポーネントをインストールする方法

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ー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ー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ー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

フェイルオーバー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、代替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。



以下の手順に従います。

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。

以下の手順に従います。

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.dxc` 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。

以下の手順に従います。

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。

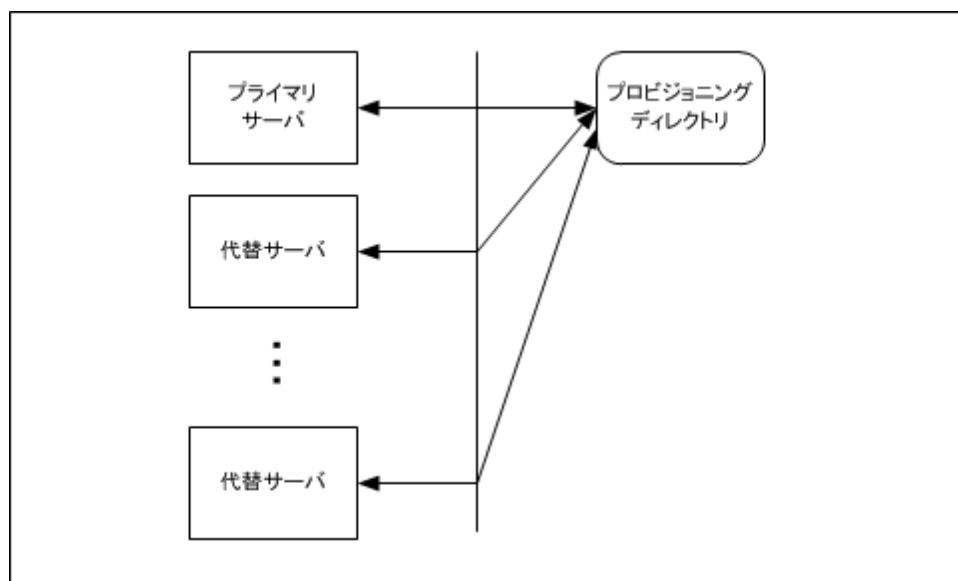
5. 他のすべてのプロビジョニング ディレクトリとプロビジョニング サーバにログインし、手順 2～4 を繰り返します。

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。

以下の手順に従います。

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。

以下の手順に従います。

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.dxc 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。

以下の手順に従います。

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へ移動します。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. プロンプトに回答して、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、プロンプトに回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ーの設定

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ー サーバ定義も読み取り、JIAM フェイルオーバー 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。

複数のコネクタ サーバのインストール

コネクタ サーバの複数のインスタンスをネットワーク ピアとして設定すると、それらは管理アカウントによって使用されるパスワードと自動的に同期します。このため、インストール中に同じアカウント詳細を設定するようお勧めします。

コネクタ サーバの複数インスタンスを同じコンピュータにインストールする場合は、インスタンスがそれぞれ一意のポート番号を使用することを確認します。ポート番号がコネクタ サーバの複数のインスタンスによって使用されると、サーバは予期せぬ動作をします。

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た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、総当た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ー

コネクタ リクエストのフェイルオーバーおよび負荷分散は、`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、フェイルオーバーと負荷分散が発生します。

フェイルオーバーと負荷分散は一体になっていて、別々に制御できません。フェイルオーバーが必要なとき以外、特定のコネクタサーバがアイドル状態のみ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ー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もおり **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ー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 **Windows** 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、**Windows** 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、コ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。

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、操作に必要な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つがユーザー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。

ユーザー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 `$HOME/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++ Connector Server

C++ Connector Server (CCS) を UNIX 上にインストールする場合、いくつかの制限事項があります。詳細については、「Windows および UNIX 上の CCS」を参照してください。

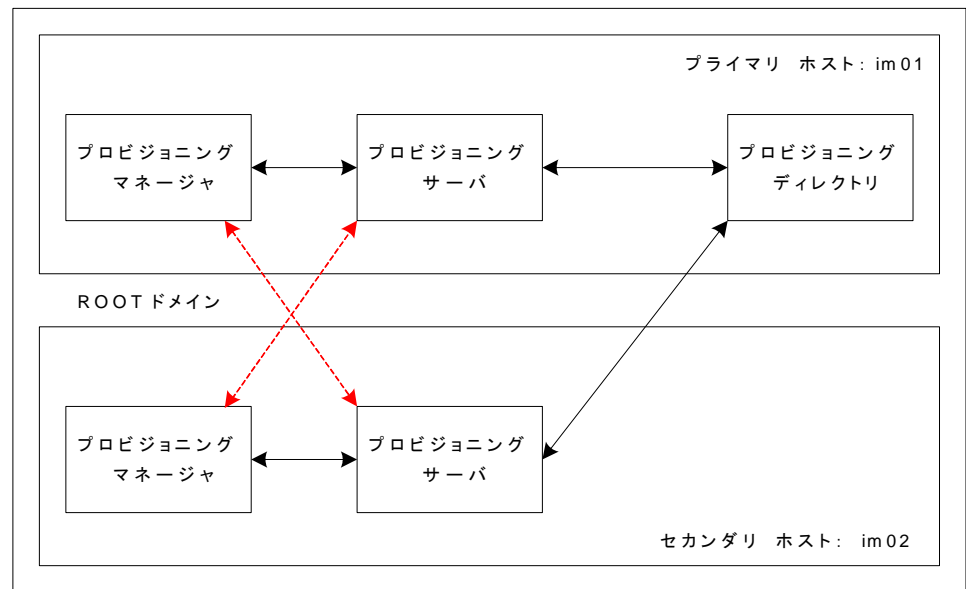
プロビジョニング クライアントのフェイルオーバー

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ーの設定
- 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ー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ーするようにします。



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ーします。

ユーザ コンソール フェイルオーバーの有効化

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。

以下の手順に従います。

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 フェイルオーバーの有効化

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 フェイルオーバーを有効にできます。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ーするように設定されます。

以下の手順に従います。

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] - [フェイルオーバー] タブを選択します。
3. [フェイルオーバーの有効化] 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 フェイルオーバーのテスト

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

以下の手順に従います。

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ー 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 \(P. 165\)](#)

[管理コンソールを使用した CA Identity Manager オブジェクトの削除 \(P. 166\)](#)

[ポリシーストアからの CA Identity Manager スキーマの削除 \(P. 166\)](#)

[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 \(P. 168\)](#)

[WebSphere からの CA Identity Manager の削除 \(P. 169\)](#)

[CA Identity Manager の再インストール \(P. 171\)](#)

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。

以下の手順に従います。

- 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 インターフェイスで、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。
- `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`
- 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	<code>novell¥novell-delete-ims8.ldif</code>

ディレクトリタイプ	LDIF ファイル
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

コンポーネントをインストールした各システムから CA Identity Manager 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 管理ツールを別個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 上で CA Identity Manager ソフトウェア コンポーネントをアンインストールする方法

以下の手順に従います。

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

すべての非プロビジョニング 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コンポーネントをアンインストールします。

注: 管理ツールでプロビジョニング マネージャをインストールしますが、このコンポーネントをアンインストールするにはプロビジョニング マネージャインストーラを使用します。

UNIX で CA Identity Manager ソフトウェア コンポーネントをアンインストールする方法

以下の手順に従います。

1. 以下の場所へ移動します。

```
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
```

画面の指示に従います。

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コンポーネントをアンインストールします。

WebSphere からの CA Identity Manager の削除

CA Identity Manager ソフトウェアをアンインストールした後に、WebSphere 管理コンソールの使用により、またはコマンドラインからのスクリプトの実行によりアプリケーションサーバから CA Identity Manager 設定を削除できます。

管理コンソールを使用して CA Identity Manager を削除する方法

以下の手順に従います。

1. 以下の URL を使用して、WebSphere 管理コンソールを開きます。

```
http://websphere_server:9060/admin
```

2. [Applications] - [Enterprise Applications] を選択します。
3. [Enterprise Applications] 画面で、CA Identity Manager の隣のチェック ボックスをオンにし、[Stop] をクリックします。
4. CA Identity Manager の隣のチェック ボックスをオンにし、[Uninstall] をクリックします。
5. SiteMinder EAR および SiteMinder Agent EAR をインストールした場合は、これらのアプリケーションを停止し、前に説明したようにそれらをアンインストールします。
6. [保存] をクリックします。
7. [Save] をクリックして、マスタ設定への変更内容を保存します。
8. ca-stylesr5.1.1.ear ファイルを削除します。

注: 他の CA 製品がそれを使用していない場合にも、ca-stylesr5.1.1.ear を削除してください。

コマンドラインを使用して CA Identity Manager を削除する方法

以下の手順に従います。

CA Identity Manager は、WebSphere アプリケーション サーバから CA Identity Manager を削除するために使用できる以下の 2 つのスクリプトを含みます。

- **Uninstall** スクリプト (`uninstallApp.jacl`) -- CA Identity Manager アプリケーションを停止し、次いで WebSphere からそれを削除します。
- **Cleanup** スクリプト (`Ims6Cleanup.jacl`) -- `uninstallApp.jacl` の実行により作成されたような、CA Identity Manager リソースを削除します。

注: Cleanup スクリプトを実行すると、同じアプリケーション サーバ上で実行されるすべての CA Identity Manager インストールによって使用されるリソースが削除されます。削除したくない CA Identity Manager インストールが同じシステム上にある場合には、Cleanup スクリプトを実行しないでください。また、このスクリプトは、CA Identity Manager によって作成されたデータ ソースを削除しません。

コマンドラインを使用して CA Identity Manager を削除するには、以下の手順に従います。

1. コマンドラインから、`websphere_home¥bin` に移動します。
2. WebSphere アプリケーション サーバが実行されていることを確認してください。
3. 以下のように Uninstall スクリプトを実行します。
 - **Windows** : `wsadmin -f uninstallApp.jacl`
 - **UNIX** : `./wsadmin.sh -f uninstallApp.jacl`
4. 以下のように Cleanup スクリプトを実行します。
 - **Windows** : `wsadmin -f Ims6Cleanup.jacl websphere_node`
 - **UNIX** : `/wsadmin.sh -f Ims6Cleanup.jacl websphere_node`ここで「`websphere_node`」は、CA Identity Manager がインストールされた WebSphere ノードの名前です。
5. `ca-stylesr5.1.1.ear` ファイルを削除します。

注: 他の CA 製品がそれを使用していない場合にのみ、`ca-stylesr5.1.1.ear` を削除してください。
6. 以下のように、サービス統合バスを削除します。
 - a. WebSphere 管理コンソールで、[Service Integration] - [Buses] に移動します。
 - b. `iam_im-IMSBUS` を削除します。

- c. アプリケーションサーバを停止します。
- d. `websphere_home¥profiles¥websphere_profile¥databases¥com.ibm.ws.sib¥`にある `node_name.server_name.IMSBus directory` 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 \(P. 173\)](#)

[設定ファイルの変更 \(P. 173\)](#)

[設定ファイルフォーマット \(P. 179\)](#)

Administrative UI の無人インストールを実行する方法

以下の手順に従います。

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。
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。 <ul style="list-style-type: none"> ■ 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	命令
DEFAULT_APP_SERVER	Enter、Weblogic、WebSphere、または JBoss
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-5.1
追加の WebLogic パラメータ	
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¥

パラメータ	命令
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_WEBSHERE_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	命令
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。

パラメータ	命令
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。

パラメータ	命令
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\$\nodes\WAS_NODE\$\servers\WAS_SERVER\$

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=
```


付録 C: ログ ファイルのインストール

ログ ファイルは、インストール パッケージをアンパックした場所に基づいて格納されます。以下の例には、これらのデフォルトの場所とは異なるトップレベルのディレクトリがある場合があります。

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. 185)

[UNIX のログ ファイル](#) (P. 186)

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へ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` ディレクトリへ書き込まれています。

付録 D: 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。