Sun Identity Manager の概要

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 821–0060
2009 年 2 月

090729@22510

目次

はじめに 5

1 製品の概要 11
アイデンティティー管理とは 11
Identity Manager と他の IT システムのインタフェース 12
ユーザーが Identity Manager に接続する方法 13
Identity Manager Service Provider とは 14
Sun のその他のアイデンティティー管理製品について 15
Sun Java System Directory Server Enterprise Edition とは 15
OpenSSO Enterprise とは 15
Sun Role Manager とは 16

2 製品のアーキテクチャー 17
Identity Manager のコンポーネントについて 17
アプリケーション層について 18
データベース層について 19
管理リソース層について 19
ユーザー層について 20
システムの分離と物理的な近接性のガイドラインについて 21
SPML と Web サービスのシステムアーキテクチャーについて 22
Identity Manager Service Provider のシステムアーキテクチャーについて 22

3 クラスタ化と高可用性 25
可用性の必要性の評価 25
ダウンタイムのコストの評価 25
ダウンタイムの原因について 27
投資利益率の計算 27

Identity Manager の高可用性機能セットについて 28
リポジトリの高可用性化 28
アプリケーションサーバーの高可用性化 29
Gateway の高可用性化 30
推奨される HA アーキテクチャーについて 31
推奨される Service Provider の HA アーキテクチャーについて 32
障害のシナリオについて 34
シナリオ 1: ワークフローなし 34
シナリオ 2: ワークフローの実行中 35
シナリオ 3: ワークフローが一時休止中またはスリープ中 36
シナリオ 4: 作業項目の編集中 36
シナリオ 5: スケジュールタスクの実行中 37
シナリオ 6: スケジュールタスクが一時休止中 38
シナリオ 7: Web サービスのワークフロー要求が Identity Manager でまだ受信されていない 38
シナリオ 8: Web サービスワークフロー要求が Identity Manager で実行中 39
セッションアフィニティーとセッション持続性に関する FAQ 40

はじめに

Sun Identity Manager 8.1 Overviewでは、Sun™ Identity Manager の概要と、その機能を示します。本書では、Identity Manager 製品のアーキテクチャーについて、および高可用性配備の計画方法について説明します。

対象読者

このガイドは、Sun Identity Manager 8.1 とその関連ソフトウェアについての理解を深めたいと考えている、IT 分野の専門ユーザーを対象としています。Identity Manager を評価中の IT ユーザーや、Identity Manager の配備を始めたばかりの IT ユーザーにも役立ちます。

内容の紹介

このガイドは、次の章で構成されています。

第 1 章「製品の概要」では、Identity Manager の目的と、アプリケーションの主な機能について説明します。

第 2 章「製品のアーキテクチャー」では、Identity Manager のアーキテクチャー、Service Provider のアーキテクチャー、および Web サービスのアーキテクチャーについて説明します。システムの分離や物理的な近接性についてのガイドラインも示します。

第 3 章「クラスタ化と高可用性」では、高可用性/耐障害性 (HA/FT) を備えた Identity Manager 環境の実装方法について説明します。Identity Manager の配備で必要な可用性の規模を評価する際にも役立ちます。

関連マニュアル

Sun Identity Manager 8.1 のドキュメントセットには、次のマニュアルが含まれています。

主な対象読者	タイトル	説明
すべてのユーザー	『Sun Identity Manager の概要』	Identity Manager の機能についての概要を説明しています。製品のアーキテクチャー情報や、Identity Manager を Sun Open SSO Enterprise や Sun Role Manager などの他の Sun 製品と統合する方法について説明しています。
	『Sun Identity Manager 8.1 リリースノート』	既知の問題、修正された問題、および Identity Manager のドキュメントセットに記載されていない最新情報を説明しています。
システム管理者	『Installation Guide』	Identity Manager と、Sun Identity Manager Gateway や PasswordSync などのオプションコンポーネントをインストールする方法を説明しています。
	『Upgrade Guide』	古いバージョンの Identity Manager を新しいバージョンにアップグレードする方法について説明しています。
	『System Administrator's Guide』	システム管理者が Identity Manager のインストールを管理、調整、およびトラブルシューティングする際に役立つ情報と操作方法を説明しています。
ビジネス管理者	『Business Administrator's Guide』	Identity Manager のプロビジョニングおよび監査機能の使用方法を説明しています。ユーザーインタフェース、ユーザーとアカウントの管理、レポート機能などの情報についても説明しています。

主な対象読者	タイトル	説明
システムインテグレータ	『Deployment Guide』	Identity Manager を複雑な IT 環境に配備する方法を説明しています。アイデンティティー属性、データの読み込みと同期、ユーザーアクションの設定、カスタムブランディングの適用などの話題も説明しています。
	『Deployment Reference』	ワークフロー、フォーム、ビュー、ルール、および XPRESS 言語について説明しています。
	『Resources Reference』	リソースアダプタのインストール、設定、および使用方法の情報を説明しています。
	『Service Provider 8.1 Deployment』	Identity Manager Service Provider の配備方法と、ビュー、フォーム、およびリソースの標準 Identity Manager 製品との違いを説明しています。
	『Web Services Guide』	SPML サポートの設定方法、サポートされる SPML 機能とサポートの理由、およびフィールドでサポートを拡張する方法について説明しています。

ドキュメントの更新

Sun Identity Manager のドキュメントに対する修正と更新は、Identity Manager Documentation Updates の Web サイトで公開されます。

`http://blogs.sun.com/idmdocupdates/`

RSS フィードリーダーを使用して Web サイトを定期的に確認し、更新を利用できる場合に通知を受けることができます。サイトを購読するには、フィードリーダーをダウンロードして、ページの右側の「Feeds」の下にあるリンクをクリックします。バージョン 8.0 から、メジャーリリースごとのフィードを利用できます。

関連するサードパーティー Web サイト

このドキュメントでは、サードパーティー URL を参照して、追加の関連情報を提供します。

注 – このドキュメントで取り上げる他社の Web サイトが使用可能かどうかについて、Sun は関知いたしません。Sun は、このようなサイトまたはリソースで得られるあらゆる内容、広告、製品、およびその他素材を保証するものではなく、責任または義務を負いません。Sun は、このようなサイトまたはリソースで得られるあらゆるコンテンツ、製品、またはサービスによって生じる、または生じたと主張される、または使用に関連して生じる、または信頼することによって生じる、いかなる損害または損失についても責任または義務を負いません。

ドキュメント、サポート、トレーニング

Sun の Web サイトでは、次の追加リソースに関する情報を入手できます。

- ドキュメント (http://www.sun.com/documentation/)
- サポート (http://www.sun.com/support/)
- トレーニング (http://www.sun.com/training/)

ご意見、ご要望の送付先

Sun ではドキュメントの品質向上のため、お客様のご意見、ご要望をお受けしております。ご意見をお寄せいただくには、http://docs.sun.com にアクセスして、「Feedback」をクリックしてください。

書体の表記規則

次の表は、本書で使用する表記上の規則について説明しています。

表 P–1 書体の表記規則

字体または記号	意味	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力を示します。	.login ファイルを編集します。 すべてのファイルを一覧表示するには、ls -a を使用します。 machine_name% you have mail.

表 P–1 書体の表記規則 *(続き)*

字体または記号	意味	例
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力とは区別して示します。	`machine_name%` **`su`** `Password:`
aabbcc123	変数を示します。実際の名前または値で置き換えます。	ファイルを削除するコマンドは、`rm` *filename* です。
AaBbCc123	書名、新しい用語、強調する語句を示します。	『ユーザーズガイド』の第 6 章を参照してください。 キャッシュは、ローカルに保存されたコピーです。 ファイルを保存しないでください。 注意: 一部の強調語句は、オンラインでは太字で示されます。

コマンドのシェルプロンプトの例

次の表は、C シェル、Bourne シェル、および Korn シェルの、デフォルトの UNIX® システムプロンプトとスーパーユーザーのプロンプトを示しています。

表 P–2 シェルプロンプト

シェル	プロンプト
C シェル	`machine_name%`
C シェル (スーパーユーザーの場合)	`machine_name#`
Bourne シェルおよび Korn シェル	`$`
Bourne シェルおよび Korn シェル (スーパーユーザーの場合)	`#`

◆ ◆ ◆ 第 1 章

1 製品の概要

この章では、Sun™ Identity Manager の目的と、アプリケーションの主要な機能について説明します。Sun が提供しているその他のアイデンティティー管理製品についても、簡単に説明します。

この章では次のトピックを説明します。

- 11 ページの「アイデンティティー管理とは」
- 12 ページの「Identity Manager と他の IT システムのインタフェース」
- 13 ページの「ユーザーが Identity Manager に接続する方法」
- 14 ページの「Identity Manager Service Provider とは」
- 15 ページの「Sun のその他のアイデンティティー管理製品について」

アイデンティティー管理とは

Sun Identity Manager を利用すると、複数の IT システム間でユーザーアカウントの作成、更新、および削除の処理を自動化できます。この処理をまとめて、「プロビジョニング」(ユーザーアカウントの作成と更新) および「プロビジョニング解除」(ユーザーアカウントの削除) と呼んでいます。

たとえば、新しく従業員が入社すると、Identity Manager はこの従業員にアクセス権を与えるために必要な承認を取得するワークフローを実行します。必要な承認を取得したら、Identity Manager は会社の人事システム (PeopleSoft)、電子メールシステム (Microsoft Exchange)、およびエンタープライズアプリケーション (SAP) に、従業員のユーザーアカウントを作成します。社内で従業員がロールを変更したら、Identity Manager はユーザーアカウントを更新し、新しいロールで必要なリソースにアクセスできるようにアクセス権を拡張します。また、従業員が退職する場合、Identity Manager はユーザーのアカウントを自動的に削除して、それ以降のアクセスを禁止します。

Identity Manager では、継続的に監査ポリシーを実施することもできます。「監査ポリシー」は、ユーザーに許可するアクセス、または許可しないアクセスの種類を指

定します。たとえば米国では、同じユーザーが買掛管理システムと売掛管理システムの両方にアクセスすることは、Sarbanes-Oxley (SOX) 法にに違反します。これは、職務権限の分離違反として知られています。Identity Manager では、これらのさまざまな違反をチェックする監査を実行し、違反が検出された場合は、設定に従って自動的にアクセス権を削除したり、管理者に通知を送信することができます。この処理を「是正」と呼びます。

Identity Manager と他の IT システムのインタフェース

Identity Manager では、管理対象のアプリケーションやその他の IT システムを「リソース」と呼びます。Identity Manager は「アダプタ」または「コネクタ」をインタフェースとして使用して、これらのリソースに接続します。

アダプタおよびコネクタは、Identity Manager サーバーにインストールされます (Identity Manager は、ターゲットリソースにインストールされる特別なソフトウェア (「エージェント」) を必要としません)。多数の Identity Manager アダプタおよびコネクタが用意されています。また、標準プロトコルや公開されているアプリケーションプログラミングインタフェース (API) を使用して、任意のリソースと通信する新しいアダプタまたはコネクタを作成することもできます。Identity Manager にはさまざまなアダプタおよびコネクタが付属しており、一般的なほとんどのリソースと通信できます。さらに、プログラマはテンプレートとスケルトンコードを利用して、アダプタやコネクタを追加作成することができます。

一部のリソースとは直接通信することができません。この場合は、Sun Identity Manager Gateway を使用する必要があります。Gateway が必要なリソースには、Exchange や Windows Active Directory などの Microsoft 製品や、eDirectory (以前の Netware Directory Services) などの Novell 製品などがあります。これらの場合、Identity Manager は Gateway と直接通信を行い、Gateway がインタフェースとなってリソースに接続します。

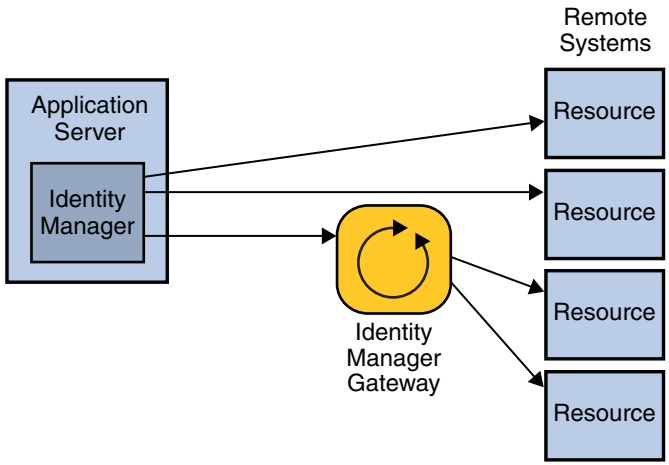

図 1–1　Identity Manager が直接接続できるリソースと、Identity Manager Gateway が必要なリソース

Identity Manager がサポートするリソースのリストについては、『Sun Identity Manager 8.1 リリースノート』の「サポートされているリソース」を参照してください。

ユーザーが Identity Manager に接続する方法

Identity Manager には、管理者用のユーザーインタフェース (UI) と、エンドユーザー用のインタフェースが用意されています。Identity Manager を使用するには、管理者とエンドユーザーは Web ブラウザを使用して Identity Manager にログオンします。

- 管理者は「管理者インタフェース」を使用して、ユーザーの管理、リソースの設定と割り当て、権限とアクセスレベルの定義、監査ポリシーの確立、コンプライアンスの管理、およびビジネス管理者とシステム管理者に関するその他の職務を実行します。
- エンドユーザーは「エンドユーザーインタフェース」を使用して、パスワードの変更、ユーザーの秘密の質問に対する回答の設定、IT システムへのアクセスの要求、委任された割り当ての管理など、自身で行う範囲のタスクを実行します。

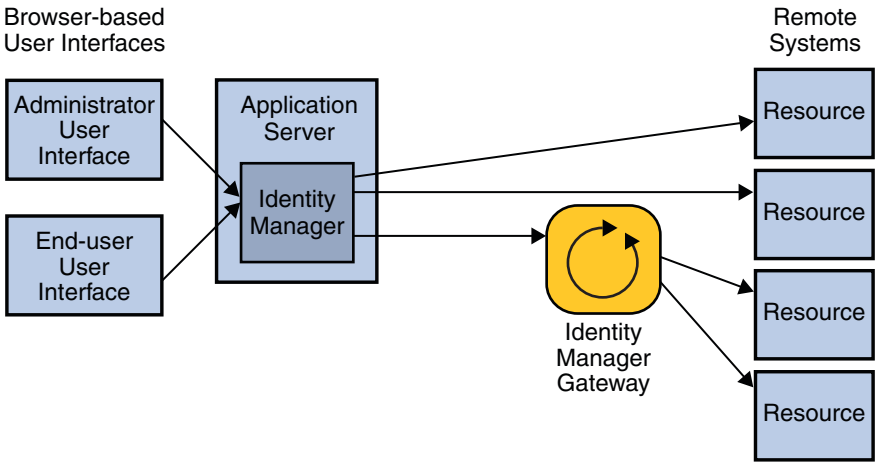

図 1–2　管理者インタフェースおよびエンドユーザーインタフェースを使用して Identity Manager に接続するユーザー

また、企業では SPML (Service Provisioning Markup Language) を使用して、独自のユーザーインタフェースを作成したり、既存のフロントエンドシステムと Identity Manager を統合することもできます。

その他の Identity Manager インタフェースには、次のものがあります。

- IVR (Interactive Voice Response) 電話インタフェース。エンドユーザーは電話を使用して Identity Manager の機能を実行できます。
- Identity Manager IDE (統合開発環境)。Identity Manager をカスタマイズするために、ソフトウェア開発者によって使用されます。
- Identity Manager コンソール。管理者が使用できるコマンド行インタフェースです。

Identity Manager Service Provider とは

Identity Manager Service Provider は、エクストラネットに重点を置いたスケーラブルなアイデンティティー管理機能です。LDAP ディレクトリサーバーに保存された大量のエンドユーザーアカウントをプロビジョニングおよび保守することができます。Service Provider 機能では、多数の管理者アカウントを管理したり、LDAP アカウントデータを他のリソースと同期することもできます。

Service Provider 機能は、Identity Manager で利用可能な機能のサブセットを使用します。たとえば、監査機能はエクストラネット環境ではほとんど役に立たないため、利用できません。

標準の Identity Manager と Service Provider 機能の違いについては、『Sun Identity Manager Service Provider 8.1 Deployment』の「Service Provider Features」を参照してください。

独立したアドオン製品として利用可能にすれば、Service Provider は Identity Manager に組み込まれます。ただし、Service Provider 機能を利用するには特別な計画が必要です。

- Identity Manager Service Provider のシステムアーキテクチャーについては、22 ページの「Identity Manager Service Provider のシステムアーキテクチャーについて」を参照してください。
- 高可用性を備えた Identity Manager Service Provider アーキテクチャーの計画については、32 ページの「推奨される Service Provider の HA アーキテクチャーについて」を参照してください。
- Identity Manager を配備して Service Provider 機能を利用する方法については、『Sun Identity Manager Service Provider 8.1 Deployment 』を参照してください。

Sun のその他のアイデンティティー管理製品について

Identity Manager の他に、Sun では Sun Java™ System Directory Server Enterprise Edition、Sun OpenSSO Enterprise、Sun Role Manager などのアイデンティティー管理ソリューションを提供しています。これらの製品は Identity Manager を補完するもので、たとえば Role Manager は Identity Manager の機能を拡張することができます。

Sun Java System Directory Server Enterprise Edition とは

Sun Java System Directory Server Enterprise Edition は、アイデンティティー情報用のスケーラブルで高いパフォーマンスを備えた LDAP データストアです。Directory Server Enterprise Edition は、中心となるディレクトリサービスと、その他の補完的なデータサービスを提供します。競合するディレクトリサービスには、Microsoft の Active Directory や Novell の eDirectory があります。

OpenSSO Enterprise とは

Sun OpenSSO Enterprise (以前の Sun Java System Access Manager および Sun Java System Federation Manager) は、内部および外部のアプリケーションや Web サービスに対して、幅広いセキュリティーポリシーを集中的に実施します。安全で集中化されたアクセス制御とシングルサインオン (SSO) 機能が提供されます。また、連携アイデンティティー管理では、異なるディレクトリサービス、セキュリティー、および認証

テクノロジを利用している企業間で、アプリケーションを共有することができます。連携パートナーは相互に信頼して、それぞれのユーザーを認証し、サービスにアクセスする権限を保証します。

Sun Role Manager とは

Sun Role Manager (以前の Vaau RBACx) は、アクセス管理をユーザーごとではなく企業内のユーザーのロールに基づいて行うことで、アクセス制御コンプライアンスを簡潔にします。使用法や企業ポリシーに基づいたロールを作成することで、アクセスを詳細に監視して、より効果的で安全性の高い適切な方法で管理することができます。

◆ ◆ ◆ 第 2 章

製品のアーキテクチャー

この章では、Sun™ Identity Manager 製品のアーキテクチャーについて説明します。

この章は次のトピックで構成されています。

- 17 ページの「Identity Manager のコンポーネントについて」
- 21 ページの「システムの分離と物理的な近接性のガイドラインについて」
- 22 ページの「SPML と Web サービスのシステムアーキテクチャーについて」
- 22 ページの「Identity Manager Service Provider のシステムアーキテクチャーについて」

Identity Manager のコンポーネントについて

Identity Manager は、 Java 2 Platform, Enterprise Edition (J2EE™ プラットフォーム) の Web アプリケーションです。J2EE プラットフォームは、業界標準のサービス、API、およびプロトコルのセットで構成され、Web ベースの多層エンタープライズアプリケーションを開発するための機能を提供します。

Identity Manager のシステムアーキテクチャーは、4 つの論理層に分類されます。

- ユーザー層
- アプリケーション層
- データベース層
- 管理リソース層

以降の節では、各層について説明します。最初に、アプリケーション層について説明します。

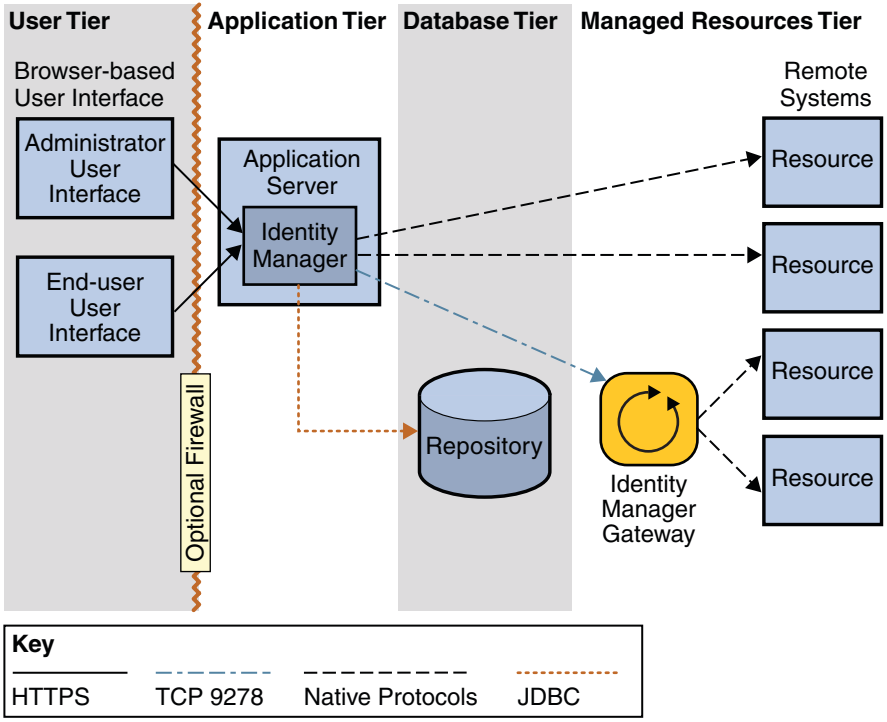

図 2–1 Identity Manager のシステムアーキテクチャー

アプリケーション層について

Identity Manager (または Identity Manager サーバー) は、アプリケーションサーバー内の J2EE Web コンテナにインストールされます。Identity Manager サーバーは、JSP™ ファイル、HTML、画像、および Java™ クラスで構成されます。他の IT システム (「リソース」) とのインタフェースとなるアダプタおよびコネクタも、アプリケーションサーバー上の Identity Manager 内に配置されます。

注 – サポートされるアプリケーションサーバーのリストについては、『Sun Identity Manager 8.1 リリースノート』の「アプリケーションサーバー」を参照してください。

Identity Manager は Web アプリケーションであるため、ユーザーインタフェースはアプリケーションサーバー上に存在し、表示されるページは要求ごとにユーザー層に提供されます。

Identity Manager のインストールに関しては、アプリケーションサーバーへのインストールがもっとも簡単です。グラフィカルなウィザードベースのインストーラが用

意されているほか、UNIX® システムではコマンド行インストーラも利用できます。Identity Manager 内でアクションを実行する Java クラスを実行する場合は、アプリケーションサーバーに Java Development Kit (JDK™) がバンドルまたはインストールされている必要があります。

データベース層について

Identity Manager は、プロビジョニングと状態の情報をすべて Identity Manager の「リポジトリ」に格納します。リポジトリは、Identity Manager のすべての設定データを格納するテーブルで構成されます。Identity Manager は、ここでデータの検索やオブジェクトのロックを実行します。リポジトリには、Identity Manager で実行されたアクションの履歴を記録する監査ログも含まれます。Identity Manager のデータは XML 形式で保存されます。リポジトリは、ローカルファイルまたはリレーショナルデータベースに作成できます。ただし、運用環境ではリレーショナルデータベースが必要です。

注 – サポートされるデータベースサーバーのリストについては、『Sun Identity Manager 8.1 リリースノート』の「リポジトリデータベースサーバー」を参照してください。

各ユーザーについてのアイデンティティー情報が最小限必要な量を超える場合、ユーザーデータは Identity Manager に保持されません。Identity Manager でユーザーを識別および区別するために必要な属性 (たとえば、「名前」や「電子メールアドレス」) だけが、リポジトリに保存されます。

Identity Manager は、直接 JDBC 接続を通してリポジトリに接続できます。また、アプリケーションサーバーで利用可能なデータソース機能を使用することもできます。

Identity Manager Service Provider 機能では、ユーザー情報を格納するための LDAP リポジトリも必要です。詳細は、22 ページの「Identity Manager Service Provider のシステムアーキテクチャーについて」を参照してください。

管理リソース層について

管理リソース層は、ユーザーアカウントのプロビジョニングおよびプロビジョニング解除の対象となる、アプリケーションと IT システムで構成されます。Identity Manager Gateway も含まれます。これは、Identity Manager が特定のリソースとのやり取りを行えるようにするヘルパーアプリケーションです。

アダプタとコネクタは、ユーザーアカウントの作成、更新、削除、読み取り、パスワード変更機能の実行など、ユーザー管理機能を提供します。アダプタとコネクタは、リモートシステムからアカウント情報を抽出することもできます。

注 – ほとんどの場合、Identity Managerはユーザーデータをリモートシステムで管理し、自身のデータストアにはこれらのデータを保持しません。

Sun Identity Manager Gatewayを使用する必要がある一般的なリソースには、Microsoft Exchange、Windows Active Directory、Novell eDirectory (以前のNetware Directory Services)、Lotus Dominoなどがあります (すべての製品のリストについては、『Sun Identity Manager 8.1 リリースノート』の「Sun Identity Manager Gateway」を参照してください)。 Gatewayは Windowsにサービスとしてインストールされ、TCPポート 9728を使用して Identity Managerと通信を行います。通信は Identity Managerから開始され、専用の暗号化プロトコルが使用されます。続いて、Gatewayがリソースのネイティブプロトコルを使用して管理リソースに接続します。

インストール方法の違いにより、アダプタおよびコネクタには「Identity Managerアダプタおよびコネクタ」と「カスタムアダプタおよびコネクタ」の2種類があります。Identity Managerアダプタおよびコネクタは、Identity Managerにプリインストールされています。カスタムアダプタおよびコネクタは、アプリケーションサーバー上の Identity Managerインストールディレクトリ内の指定されたディレクトリにコピーする必要があります。

カスタムアダプタおよびコネクタは、Identity Managerの「Resource Extension Facility (REF)」キットを使用して簡単に作成できます。REFキットには、APIと多数のテンプレートアダプタが用意されており、開発プロセスをすぐに始めることができます。簡単なリソース機能は、8つの Javaメソッドを実装するだけで実現できます。

ユーザー層について

ユーザー層は、ユーザーインタフェースのいずれかを使用して Identity Managerとやり取りを行う、管理者とエンドユーザーで構成されます。製品のメインユーザーインタフェースは、HTTPS上で Identity Managerと通信を行う Webブラウザです。ブラウザベースの UIには、「管理者インタフェース」と「エンドユーザーインタフェース」の2つがあります。これらは主に HTMLで構成されていますが、一部の機能では Javaアプレットが使用されています。

図 2–1では、わかりやすくするために管理者ユーザーインタフェースとエンドユーザーインタフェースのみを示しています。ユーザー層にはその他のユーザーインタフェースも存在します。これらのユーザーインタフェースには、IVR電話インタフェース、Identity Manager IDE、SPML Webサービスインタフェース、Identity Managerコンソールなどがあります。

システムの分離と物理的な近接性のガイドラインについて

この節では、Identity Manager の各コンポーネントの実行に適したサーバーについて、基本的なガイドラインを説明します。また、遅延やネットワークの輻輳によって発生するパフォーマンスの問題を最小化するために、物理的に近付けて設置すべきコンポーネントについての推奨事項も説明しています。

注 – ここでは基本的なガイドラインだけを説明します。高可用性を備えた Identity Manager アーキテクチャーの設計については、第 3 章「クラスタ化と高可用性」を参照してください。

開発環境では、アプリケーションサーバーとデータベースは同じマシンに配置できます。ただし、テストおよび運用環境では、Identity Manager のインスタンスを専用のサーバーにインストールしてください。リレーショナルデータベースにも専用のサーバーが必要です。

必要な場合は、Identity Manager Gateway を 1 台以上の Windows マシンにインストールします。Gateway は軽量なコンポーネントなので、専用サーバーは必要ありません。Gateway が管理するすべての Windows ドメインは、同じフォレストに所属している必要があります。フォレスト境界を越えるドメインの管理はサポートされていません。複数のフォレストがある場合は、各フォレストに少なくとも 1 つの Gateway をインストールしてください。運用環境では、Gateway の可用性を高くする必要があります。詳細は、30 ページの「Gateway の高可用性化」を参照してください。

運用環境でネットワークトラフィックがもっとも多く発生するのは、データベースサーバーとアプリケーションサーバーの間です。これらの 2 つの環境は、同一の LAN 上に配置して、ネットワークホップをできるだけ小さくする必要があります。Gateway インスタンスと管理リソースは、Identity Manager と同じネットワーク上に配置する必要はありません。

Service Provider の設定で Identity Manager を外部ユーザーに対して使用する場合は、Web サーバーのセットを DMZ に設定してください。詳細は、32 ページの「推奨される Service Provider の HA アーキテクチャーについて」を参照してください。

SPML と Web サービスのシステムアーキテクチャーについて

Service Provisioning Markup Language (SPML) と Identity Manager Web サービスを使用すると、Identity Manager のカスタムフロントエンドを実装できます。Identity Manager は、SPML のメッセージと応答を HTTPS プロトコルを使用して送受信します。

SPML と Web サービスの詳細は、『Sun Identity Manager 8.1 Web Services 』を参照してください。

Identity Manager Service Provider のシステムアーキテクチャーについて

Identity Manager Service Provider 機能を実装する場合は、5 番目の層が必要です。この層は Web 層と呼ばれ、DMZ に設置された 1 つ以上の Web サーバーで構成されます。Web 層にインストールされる Identity Manager のコンポーネントはありません。DMZ の Web サーバーが Web ページの要求に応答して、アプリケーション層の 1 つまたは複数のアプリケーションサーバーをサポートします。Web 層に 1 つ以上の Web サーバーを追加することでスケーラビリティが拡張され、DMZ に Web サーバーを設置することでネットワークのセキュリティーが強化されます。

Service Provider 機能では LDAP リポジトリも必要です。このリポジトリはデータベース層に存在します。LDAP リポジトリは管理リソースにできるため、LDAP サーバーは管理リソース層に存在していると考えることもできます。

注 – Service Provider のみの実装では、LDAP リポジトリに加えて Identity Manager リポジトリの使用も推奨されますが、必須ではありません。Identity Manager リポジトリが配備されていない場合は、特定のレポート機能など、一部の機能を利用できません。

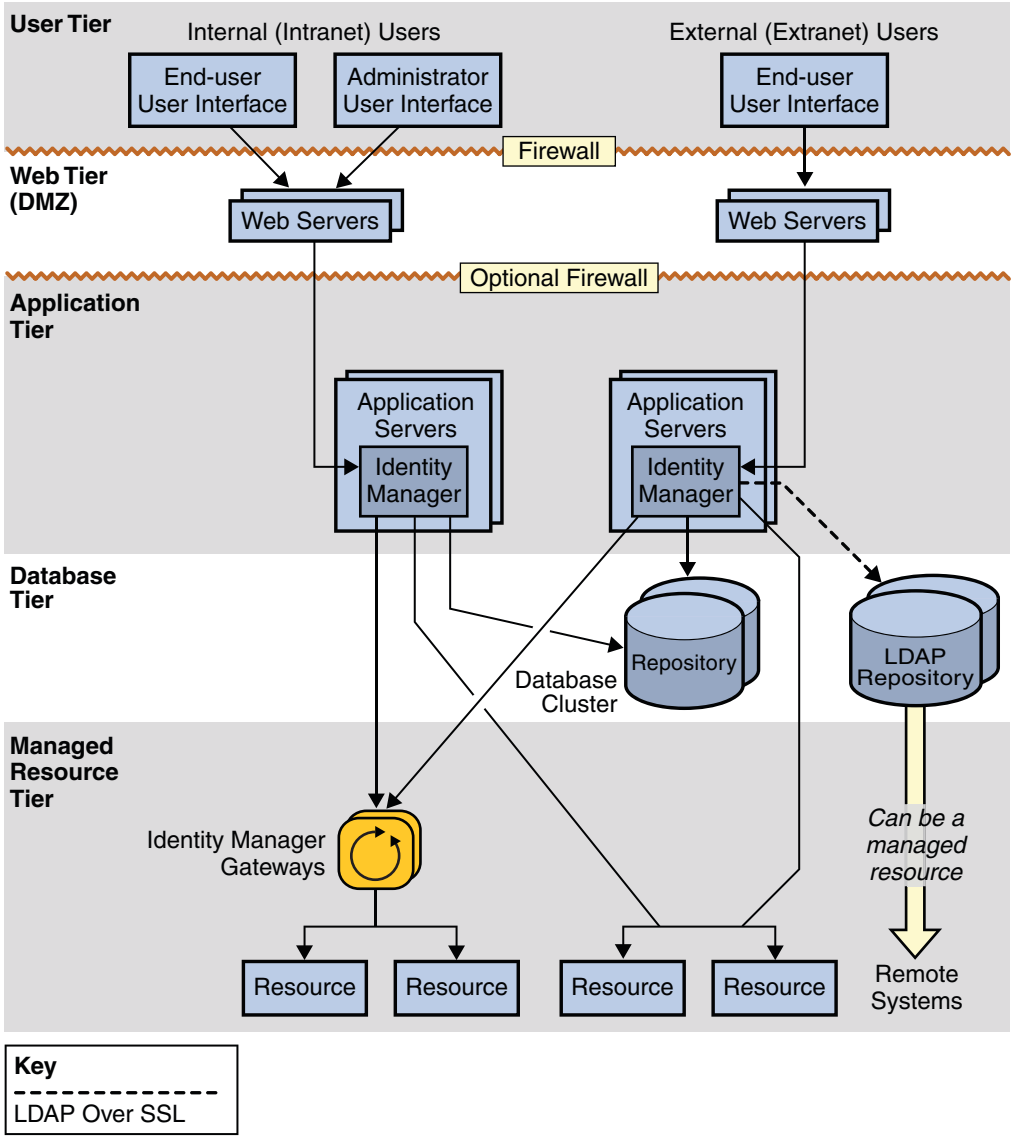

図 2–2　Identity Manager Service Provider のシステムアーキテクチャー

◆ ◆ ◆ 第 3 章

クラスタ化と高可用性

この章では、高可用性と耐障害性 (HA/FT) を備えた Identity Manager 環境の実装方法について説明します。

注 – Web サーバー、アプリケーションサーバー、およびデータベースプロバイダで高可用性配備を保証するためのベストプラクティスについては、各製品のマニュアルを参照してください。Web サーバーに関するベンダー独自の推奨事項がある場合は、このガイドよりも優先されます。

- 25 ページの「可用性の必要性の評価」
- 28 ページの「Identity Manager の高可用性機能セットについて」
- 31 ページの「推奨される HA アーキテクチャーについて」
- 32 ページの「推奨される Service Provider の HA アーキテクチャーについて」
- 34 ページの「障害のシナリオについて」
- 40 ページの「セッションアフィニティーとセッション持続性に関する FAQ」

可用性の必要性の評価

この節では、ユーザーに固有の配備で必要な可用性の規模を評価する方法を説明します。

ダウンタイムのコストの評価

Identity Manager は、一般ユーザーがすでにアクセスしているシステムおよびアプリケーションと、これらのユーザー間のトランザクションパス上に存在しないため、Identity Manager のダウンタイムはそれほど大きな問題にはなりません。Identity Manager を利用できなくても、エンドユーザーはプロビジョニングされたアカウントを通してリソースにアクセスできます。

Identity Manager のダウンタイムの主なコストは、生産性の損失です。Identity Manager が停止した場合、エンドユーザーはロックアウトされているシステムやプロビジョニングされていないシステムに、Identity Manager を使用してアクセスすることができません。

ダウンタイムのコストを計算するためにまず必要な項目は、エンドユーザーが企業内のコンピューターリソースにアクセスできないことによって生じる生産性損失の平均コストです。この値を「人時生産性」と呼んでいます。

その他の必要な項目は、Identity Manager を常に使用する必要があるエンドユーザーの、全ユーザーに対する割合です。この全ユーザーには、プロビジョニングが必要な新入社員や、自分のパスワードを忘れてしまったエンドユーザー (パスワード管理が配備されている場合) が含まれます。

次のような条件を仮定します。

従業員の総数	20,000 人
1 日のパスワードリセット数	130
1 日の新入社員の数	30 人
1 日の勤務時間	8 時間

この場合、次のように計算できます。

- Identity Manager を必要とする 1 時間あたりの従業員の数 = (130 + 30) / 8 = 20
- Identity Manager を必要とする 1 時間あたりの従業員のパーセント = 20 / 20,000 = .1% (1000 人に 1 人)

これらの値を使用して、Identity Manager が停止した場合のコストを次のように評価できます。

人時生産性	100 ドル	
生産性の喪失	.5	(システムにアクセスできないことにより生産性が 50% 低下)
影響を受ける従業員の数	20 人	
小計	1,000 ドル	
機能停止の期間	2 時間	

直接的な損失の合計	2,000 ドル

この例は、Identity Manager で管理されているユーザーの数が多くても、システムにアクセスするために常に Identity Manager を必要とするユーザー数は通常少ないことを示しています。

また、Identity Manager のようなシステムを復元するために必要な時間は、Identity Manager で自動実行しているプロビジョニング処理を手動で実行するために必要な時間よりも、通常は短いということも考慮してください。したがって、Identity Manager のダウンタイムではコストが必要になりますが、通常そのコストは、リソースへのアクセス権を手動でユーザーに設定するコストよりも小さくなります。

ダウンタイムの原因について

Identity Manager の高可用性配備を計画するときに、ダウンタイムの原因を検討することは価値があります。

ダウンタイムの原因には次のようなものがあります。

- オペレータの誤り
- ハードウェアの障害
- ソフトウェアの障害
- 計画されたダウンタイム (ハードウェアおよびソフトウェアのアップグレード)
- 不十分なパフォーマンス (知覚されるダウンタイム)

投資利益率の計算

Identity Manager は、生産性の損失を自動的に処理して削減します。高可用性を備えた Identity Manager アーキテクチャーでは、ダウンタイムを最小化し、生産性の損失を回避することで投資利益を実現します。

ダウンタイムのコストを使用して、Identity Manager で最終的に必要な可用性の規模を判断できます。一般的には、Identity Manager が高可用性を備えるように適正な投資を行うことが目標です。

投資のコストを計算する際は、HA/FT ハードウェアおよびソフトウェアの購入のみで、利用可能なソリューションの実装が完了するわけではないことに注意してください。運用の知識を持つスタッフの費用も、別のコストとして必要です。

Identity Managerの高可用性機能セットについて

Identity Managerは、HAインフラストラクチャーを利用できる場合、これを利用するように設計されています。たとえば、Identity Managerは高可用性の達成にアプリケーションサーバークラスタを必要としませんが、クラスタが存在する場合はこれを利用できます。

次の図は、非冗長アーキテクチャーに配備されたIdentity Managerの主要コンポーネントを示しています。次の節からは、Identity Managerリポジトリ、アプリケーションサーバー、およびゲートウェイを高可用性化する方法について説明します。

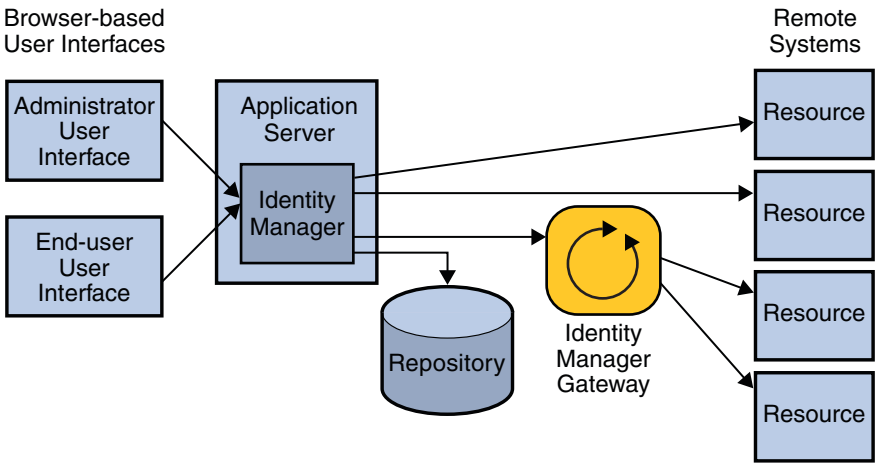

図3–1　Identity Managerの標準的なシステムアーキテクチャー

注 – 遅延やネットワークの輻輳によって発生するパフォーマンスの問題を最小化するために、どのコンポーネントを近付けて配置するべきかについては、21ページの「システムの分離と物理的な近接性のガイドラインについて」を参照してください。

リポジトリの高可用性化

Identity Managerは、プロビジョニングと状態の情報をすべてIdentity Managerリポジトリに格納します。

Identity Managerリポジトリを格納するデータベースインスタンスの可用性は、高可用性を備えたIdentity Managerの配備でもっとも重要です。リポジトリはIdentity

Managerのインストール全体を表し、そこに含まれるデータは他の重要なデータベースアプリケーションと同様に保護する必要があります。最低でも、定期的なバックアップの実行が必要です。

注 – パフォーマンス (1秒あたりのトランザクション数) の大幅な低下につながるため、Identity Managerリポジトリを VMware仮想マシンなどの仮想プラットフォームでホストしないでください。

作成できるリポジトリのイメージは1つだけです。Identity Manager用に2つのデータベースを用意して、これらを夜間に同期することはできません。データベースのクラスタ化またはミラーリング機能を利用して、耐障害性を提供することをお勧めします。

アプリケーションサーバーの高可用性化

Identity Managerをアプリケーションサーバークラスタ内で実行すると、クラスタで提供される可用性や負荷分散を利用することができます。ただし、Identity ManagerはクラスタJ2EE機能を使用しません。

Identity Managerは、Servlet APIを通して利用できるHTTPセッションオブジェクトを使用します。このセッションオブジェクトは、ユーザーがログインしたりアクションを実行したときに、ユーザーのアクセスを追跡します。クラスタ環境では、セッション中にユーザーの要求を複数のノードに処理させることもできます。ただし、通常はこのような処理を推奨しません。ほとんどのインストールでは、同一セッションにおけるユーザーの要求は、すべて同じサーバーに送信するように設定されます。

クラスタを設定しなくても、Identity Managerを実行するアプリケーションサーバーに可用性や機能を追加することができます。このためには、Identity Managerを実行する複数のアプリケーションサーバーをインストールし、これらのアプリケーションサーバーを同じリポジトリに接続して、すべてのアプリケーションサーバーの前に「セッションアフィニティー」を設定したロードバランサを配置します。

注 – セッションアフィニティーについては、40ページの「セッションアフィニティーとセッション持続性に関するFAQ」を参照してください。

Identity Managerは、スケジュールされた調整タスクなど、特定のタスクをバックグラウンドで実行します。これらのタスクはデータベースに格納され、任意のIdentity Managerサーバーによって実行可能です。別のノードへのフェイルオーバーが必要な場合でも、Identity Managerはデータベースを使用して、常にこれらのタスクが最後まで実行されることを保証します。

アプリケーションサーバーノードでの **Active Sync** クラスタ化の設定

`Waveset.properties` ファイルの `sources.hosts` の設定は、複数インスタンス環境で Active Sync 要求の実行にどのホストを使用するかを制御します。この設定では、ソースアダプタを実行できるホストのリストを提供します。この設定に *localhost* または *null* を指定すると、ソースアダプタは Web ファームの任意のホストで実行できます (デフォルト)。リストに 1 つまたは複数のホストを指定すると、アダプタの実行をリストの内容に制限できます。特定のホストを使用するように、別のシステムから更新を受け取った場合は、`sources.hosts` 設定を使用してホスト名を記録します。

また、`sources.` *resourceName*`.hosts` という名前のプロパティーを定義して、リソースの Active Sync タスクをどこで実行するかを制御できます。*resourceName* は、指定するリソースオブジェクトの名前で置き換えてください。

Gateway の高可用性化

Identity Manager は、サーバーから直接アクセスできないリソースを管理するために、軽量なゲートウェイを必要とします。これらのリソースには、プラットフォームに固有のクライアント側 API 呼び出しを必要とするシステムが含まれます。たとえば、Identity Manager が UNIX ベースのアプリケーションサーバーで動作している場合、管理対象の NT ドメインまたは Active Directory ドメインに対して NTLM または ADSI 呼び出しを行うことはできません。これらのリソースを管理するために Identity Manager はゲートウェイを必要とするため、Identity Manager Gateway が高可用性を備えていることは重要です。

Gateway がシングルポイント障害となることを避けるために、複数のマシンで Gateway インスタンスを実行することをお勧めします。メインの Gateway インスタンスに障害が発生したときにフェイルオーバーを提供するように、ネットワークルーティングデバイスを設定してください。フェイルオーバーデバイスではスティッキーセッションを設定し、単純なラウンドロビンスキーマを使用します。負荷分散を行うデバイスの背後には、Gateway を配置しないでください。これはサポートされていない設定で、Identity Manager の特定の機能で障害が発生します。

Gateway が管理するすべての Windows ドメインは、同じフォレストに所属している必要があります。フォレスト境界を越えるドメインの管理はサポートされていません。複数のフォレストがある場合は、各フォレストに少なくとも 1 つの Gateway をインストールしてください。

Win32 監視ツールを設定すると、Win32 ホスト上の `gateway.exe` プロセスを監視することができます。`gateway.exe` で障害が発生した場合、プロセスは自動的に再起動します。

推奨される HA アーキテクチャーについて

次の図は、既存の Web アプリケーションインフラストラクチャーがない場合に、Sun が推奨する Identity Manager アーキテクチャーを示しています。

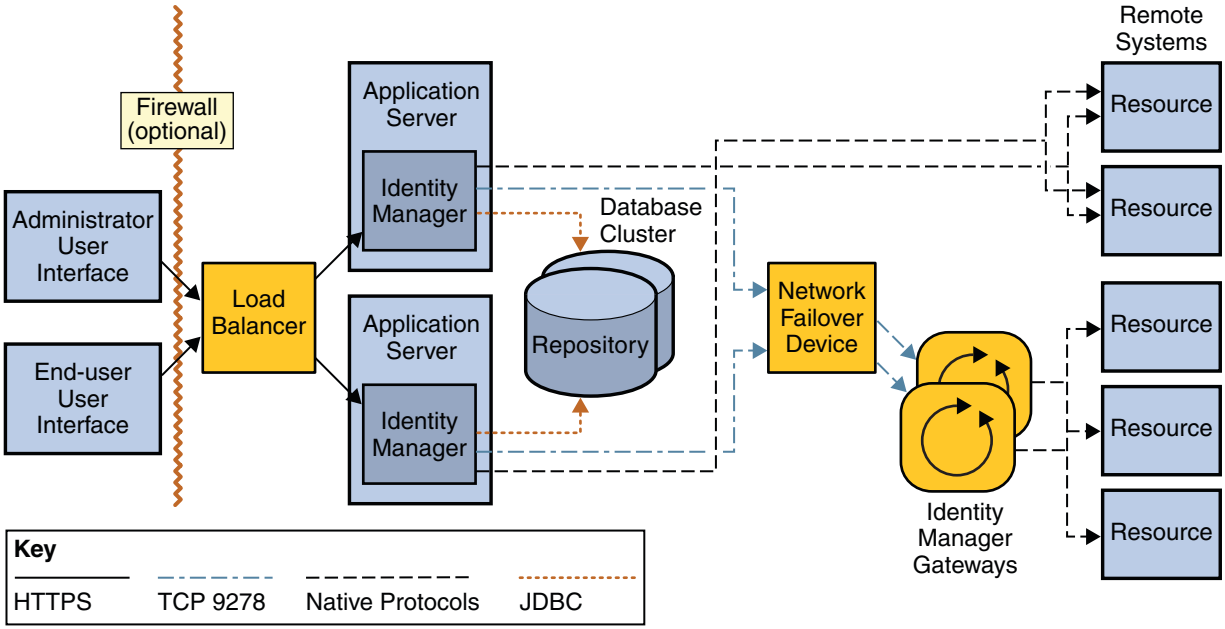

図 3–2　Identity Manager の高可用性アーキテクチャー

実際の配備では、できるだけ既存の冗長アプリケーションサーバーインフラストラクチャーを利用してください。このアーキテクチャーで注目すべき点は、アプリケーションサーバーの冗長性を実現するためにロードバランサだけを使用していることです。セッションアフィニティーを有効にしたロードバランサは、障害が発生したアプリケーションサーバーのインスタンスを検出し、アクティブなインスタンスにフェイルオーバーします。ロードバランサは、ユーザーの要求をクラスタ内のサーバーに分散することで、Web 環境に水平方向の拡張を提供するためにも利用できます。

これは簡単なアーキテクチャーですが、稼働時間の特性はより複雑な配備と比較しても劣りません。単純であるため、保守および監視すべきソフトウェアや、障害が発生する可能性のあるソフトウェアがわずかしかありません。もっとも多いダウンタイムの原因は人為的な誤りであるため、相対的に単純なソリューションは複雑なソリューションよりも優れた稼働時間特性を達成できます。普遍的に正しい答えはありません。ダウンタイムの原因をすべて理解し、投資に対して最高の可用性を得られるアーキテクチャーを選択することが重要です。

注 – Identity Manager のような Web アプリケーションで設定できる HA アーキテクチャーをすべて説明することは不可能です。

Identity Manager はさまざまな組み合わせで配備可能であるため、Identity Manager を配備するときに既存のインフラストラクチャーを識別して、それらをできるだけ利用するともっとも経済的です。

推奨される Service Provider の HA アーキテクチャーについて

Identity Manager Service Provider 機能を利用する場合は、ユーザー層とアプリケーション層の間に Web 層を追加することを推奨します。Web 層は、ファイアウォールによってアプリケーション層から分離された非武装ゾーン (DMZ) に設置される、1 つ以上の Web サーバーで構成されます。

Service Provider 機能を利用する場合は、LDAP リポジトリが必要です。Identity Manager でエクストラネットのクライアントのみをサポートする場合は、標準の Identity Manager リポジトリの使用をお勧めしますが、これは必須ではありません。また、Identity Manager がイントラネットユーザーとエクストラネットユーザーの両方をサポートする場合は、LDAP リポジトリと標準の Identity Manager リポジトリが必要です。

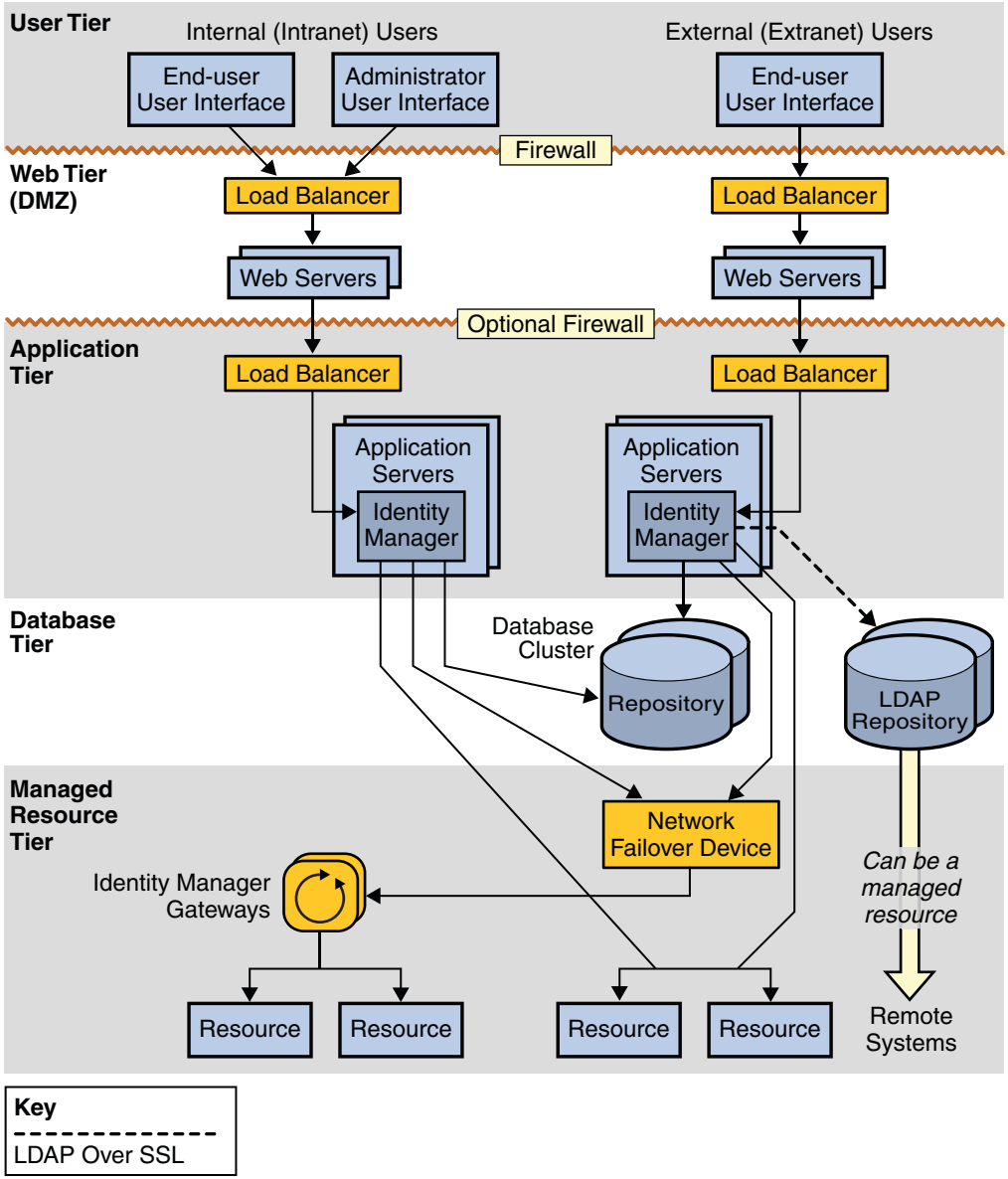

図 3–3　Identity Manager Service Provider の高可用性アーキテクチャー

障害のシナリオについて

この節では 8 つの障害のシナリオを示し、セッション持続性が有効な配備とセッション持続性が無効な配備を比較します。

- セッション持続性が「有効」な配備では、ロードバランサでセッションアフィニティーが有効です。配備には、セッションの変更が物理的に分離されているリポジトリノードに書き込まれるなど、何らかのセッション持続性が有効な同一クラスタの複数のインスタンスが含まれます。
- セッション持続性が「無効」な配備では、ロードバランサでセッションアフィニティーが有効で、同じクラスタに属していない複数のインスタンスが含まれます。

シナリオ 1: ワークフローなし

シナリオの説明

エンドユーザーまたは管理者は、ワークフローの一部でないフォームを編集しています。ユーザーがセッションを確立していたインスタンスが停止します。

セッション持続性が無効な場合

ユーザー体験: 非透過的なフェイルオーバー。フォームを送信すると、ユーザーはログインページに戻されます。

回復手順: ユーザーは自分のユーザー名とパスワードを再入力します。Identity Manager はフォームを処理して、ログイン直後のページに結果を表示します。

セッション持続性が有効な場合

ユーザー体験: ユーザーのフォームは送信され、結果が返されます。ユーザーはログオフせず、再ログインの必要はありません。

回復手順: ユーザーのアクションは必要ありません。

その他のシナリオの例

- インスタンスが停止したときに、エンドユーザーがログインしていて、ユーザーまたはその他のリポジトリオブジェクトの検索結果を取得していた。
- インスタンスが停止したときに、管理者が管理者インタフェースを使用して「パスワードのリセット」または「ユーザーの編集」の要求を送信しようとしていた。

シナリオ 2: ワークフローの実行中

シナリオの説明

エンドユーザーまたは管理者が、ワークフローをトリガーするフォームを送信しています。ワークフローを実行しているインスタンスと、ユーザーのセッションが存在するインスタンスは、一部の定期タスクで別にできる場合を除いて、通常は同じになります。このインスタンスが、ワークフローの実行中に停止します。

セッション持続性が無効な場合

ユーザー体験: 非透過的なフェイルオーバー。フォームの送信により、ユーザーはログインページに戻されます。実行中のワークフロータスクのインスタンスはリポジトリにあるべきですが、実行のノードが停止しているため、ワークフローの状態は「終了」になります。

回復手順: ワークフローをもう一度送信する必要があります。再送信を行うには、ノードで障害が発生する前にワークフローのトリガーに使用したフォームに戻り、同じ情報を入力する必要があります。

同じ要求データを送信することで、動作する場合もありますが、動作しない場合もあります。ワークフローの実行中に複数のリソースに対してプロビジョニングが実行され、これらのリソースの一部が障害発生前にプロビジョニングされている場合、ユーザーからのワークフローの再送信では、「すでにプロビジョニングされた」リソースを考慮する必要があります。終了したワークフローは、`TaskInstance` オブジェクトで `resultLimit` が期限切れになるまで、リポジトリで待機しています。

セッション持続性が有効な場合

ユーザー体験: 非透過的なフェイルオーバー。ユーザーのセッションは維持され、新しいインスタンスで再確立されるため、ユーザーのログアウトは発生しません。ただし、ワークフローが終了するため、フォームの送信はエラーになる可能性があります。このフェイルオーバーは、回復アクションが必要であるため非透過的です。

回復手順: セッション持続性が無効な場合と同じです。ユーザーは、前回のワークフローをトリガーした要求を、同じパラメータまたは修正したパラメータを使用して再送信する必要があります。

その他のシナリオの例

- エンドユーザーが Identity Manager アカウントを作成する自己登録要求を送信したときに、インスタンスが停止した。
- 管理者が処理中の「パスワードリセット」要求を送信したときに、インスタンスが停止した。

シナリオ 3: ワークフローが一時休止中またはスリープ中

シナリオの説明

このシナリオは、ワークフローが開始されているが、承認者による手動アクションを待機中である場合です。

セッション持続性が無効な場合

ユーザー体験: 承認者がまだログインしていない場合、承認者に関しては透過的なフェイルオーバー。ノードで障害発生したあと、承認者がログインすると、現在ダウンしているノードからトリガーされた要求であっても、承認要求は承認者の受信箱に表示されます。

回復手順: ユーザーのアクションは必要ありません。

セッション持続性が有効な場合

ユーザー体験: セッション持続性が無効な場合と同じです。

回復手順: セッション持続性が無効な場合と同じです。

その他のシナリオの例

- 従業員の入社日または退社日までスリープする手動のアクションなど、ワークフローがスリープ状態である。
- ユーザーの作成要求を送信した管理者が、承認者がログインして要求を承認するのを待機している。承認者が要求を承認する前に、要求の送信元であるノードで障害が発生した。

シナリオ 4: 作業項目の編集中

シナリオの説明

このシナリオは、ユーザーが作業項目を編集中で、ユーザーがセッションを確立していたノードが作業項目を送信する前に停止する場合です。

セッション持続性が無効な場合

ユーザー体験: 非透過的なフェイルオーバー。作業項目の編集フォームを送信すると、ユーザーはログオフし、ログインページに戻されます。

回復手順: ログイン資格を再送信すると、ユーザーの作業項目が「完了」にマークされ、ワークフローはそこから再開されます。ワークフローは、ユーザーの手動アクションが「完了」にマークされた場所から、新しい実行モードによって取得されます。

セッション持続性が有効な場合

ユーザー体験: 作業項目の編集フォームを送信すると、ユーザーには送信の結果が表示されます。たとえば、カスタムワークフローの次のフォームや成功のメッセージが表示されます。

回復手順: ユーザーのアクションは必要がありません。

その他のシナリオの例

- エンドユーザーが、カスタムワークフローの手動アクションに関連付けられたフォームに入力している (たとえば、特定のリソースへのアクセスを要求している)。要求が送信される前に、ユーザーがセッションを確立していたノードで障害が発生する。
- 管理者が Identity Manager にログインして、承認要求を開いて編集している。要求が送信される前に、管理者がセッションを確立していたノードで障害が発生する。

シナリオ 5: スケジュールタスクの実行中

シナリオの説明

このシナリオは、調整の実行中やレポートの実行中に、ノードで障害が発生した場合です。

セッション持続性が無効な場合

ユーザー体験: スケジュールタスクが途中で終了します。

回復手順: 実行中に終了したスケジュールタスクは、再起動する必要があります。タスクは最初から実行されます (障害が発生した場所から再開されるのではありません)。新しいタスクを作成および開始する場合と同様です。

セッション持続性が有効な場合

ユーザー体験: セッション持続性が無効な場合と同じです。

回復手順: セッション持続性が無効な場合と同じです。

その他のシナリオの例

- Active Sync アダプタが、障害が発生したノードで実行するように設定されている。

シナリオ 6: スケジュールタスクが一時休止中

シナリオの説明

このシナリオは、ユーザーのカスタムワークフローに、後日、特定のノードで実行するスケジュールタスクが含まれている場合です。予定日になる前に、タスクがスケジュールされたノードで障害が発生します。

セッション持続性が無効な場合

ユーザー体験: このタスクを予定時刻に実行することを保証するために必要な回復アクションに関して、フェイルオーバーは透過的です。

回復手順: スケジュールタスクは、予定時刻になったときに有効なノードに引き継がれます。

セッション持続性が有効な場合

ユーザー体験: セッション持続性が無効な場合と同じです。

回復手順: セッション持続性が無効な場合と同じです。

その他のシナリオの例

- ユーザーのアカウント作成処理で、延期タスクスキャナを使用して、入社日にアカウントを有効にし、退社日にアカウントを無効にするように実装している。入社日および退社日になる前に、タスクがスケジュールされたノードで障害が発生する。
- レポートをあとで実行するようにスケジュールしたり、調整を特定の日時に実行するようにスケジュールしたとき、予定の日時になる前に、タスクをスケジュールしたノードで障害が発生する。

シナリオ 7: Web サービスのワークフロー要求が Identity Manager でまだ受信されていない

シナリオの説明

このシナリオは、Identity Manager の GUI を使用せずにプロビジョニングを開始する場合です。SPML やその他のカスタム Web サービスインタフェースを使用して Identity Manager を内部的に呼び出すアプリケーションによって、ユーザーインタ

フェースが提供されています。この場合、UI を使用するユーザーに関連するユーザーセッションは、呼び出し元のアプリケーションを通して管理されます。Identity Manager では、要求はすべて「soapadmin」として開始されます。

このようなユースケースで、Identity Manager エンドポイントを経由して要求をまだ受信していないときに、対象のノードで障害が発生する場合を考えます。

セッション持続性が無効な場合

ユーザー体験: 透過的なフェイルオーバー。SOAP 管理者の資格は、ネットワーク経由で、または Identity Manager の `Waveset.properties` 設定で各 SOAP 要求に渡されます。この SOAP 要求を受信するノードが、停止前に要求を受信していなければ、セッション持続性の状態にかかわらずフェイルオーバーは透過的です。

回復手順: 必要なアクションはありません。SOAP 要求は、それを実行する有効なノードに送信されます。

セッション持続性が有効な場合

ユーザー体験: セッション持続性が無効な場合と同じです。

回復手順: セッション持続性が無効な場合と同じです。

シナリオ 8: Web サービスワークフロー要求が Identity Manager で実行中

シナリオの説明

このシナリオはシナリオ 7 に似ています。唯一の違いは、ノードで障害が発生したときに、ワークフローが実行中である (ノードが SOAP 要求をすでに受信している) ことです。

セッション持続性が無効な場合

ユーザー体験: このシナリオは、シナリオ 2 (ワークフローの実行中) と同様です。ワークフローは「終了」とマークされ、ユーザーには SOAP 要求の結果としてエラーが表示されます。

回復手順: ユーザーは他社アプリケーションのユーザーインタフェースを使用して、ワークフローのどこで障害が発生したかに応じて、同じパラメータまたは修正したパラメータを指定してフォームを再送信する必要があります。

セッション持続性が有効な場合

ユーザー体験: セッション持続性が無効な場合と同じです。

回復手順: セッション持続性が無効な場合と同じです。

セッションアフィニティーとセッション持続性に関する FAQ

アプリケーションサーバーを水平方向に拡張する場合は、セッションアフィニティーを有効にするべきですか。

はい。

アプリケーションサーバーを水平方向に拡張する場合は、セッション持続性を有効にするべきですか。

ごく一部の状況ではセッション持続性の有無によって透過的なフェイルオーバーができるかどうかが決まりますが、こうした状況での透過的なフェイルオーバーをビジネス要件で重視している場合を除いて、セッション持続性の使用はお勧めしません。セッション持続性によってパフォーマンスのオーバーヘッドが発生するため、ビジネス要件で透過的なフェイルオーバーが絶対に必要な場合を除いて、セッション持続性を無効のままにしてください。

34 ページの「障害のシナリオについて」で説明している障害のシナリオでは、8 つのシナリオのうち 6 つは、セッション持続性が有効であるかどうかにかかわらず、エンドユーザーの体験や必要な回復アクションに違いはありませんでした。シナリオ 1 と 4 のみで、セッション持続性が有効なシナリオとセッション持続性が無効なシナリオで違いがありました。

これらの 2 つのシナリオでは、セッション持続性によりフェイルオーバーの透過性が提供されますが、これによりパフォーマンスに影響が出ます。セッションオブジェクトのサイズ、セッション持続性に使用されているリポジトリ、および特定のアプリケーションサーバーのセッション管理コードの最適化に基づいて、パフォーマンスのオーバーヘッドは 10 % から 20% の範囲またはそれ以上になります。

水平方向に拡張する場合、クラスタ内に複数のアプリケーションサーバーインスタンスを設定するべきですか。

セッション持続性が必要でなければ、複数のアプリケーションサーバーインスタンスは必ずしも必要ではありません。セッション持続性が有効でないフェイルオーバーは、すべてのアプリケーションサーバーノードが 1 つのクラスタにない場合でも設定できます。