

ORACLE IDENTITY FEDERATION

主な機能と利点

ORACLE IDENTITY FEDERATION

Oracle Identity Federation は、以下のプロトコルをサポートします。

- OASIS SAML 2.0
- Liberty Alliance ID-FF 1.1 および 1.2
OASIS SAML 1.0 および 1.1
- WS-Federation

サポートされるプラットフォーム：

- Microsoft Windows
- Red Hat Linux

サポートされるアイデンティティ・リポジトリ：

- Oracle Database
- Oracle Internet Directory
- Microsoft SQL Server
- Microsoft Active Directory
- Sun Java System Directory Server

サポートされるアイデンティティおよびアクセス管理システム：

- Oracle COREid Access & Identity
- Oracle Access Manager
- Oracle Single Sign-On
- CA SiteMinder

Oracle Identity Federation は、業界を代表するフェデレーション・ソリューションであり、既存のアイデンティティおよびアクセス管理システムとともに配備可能な、柔軟性のある内蔵型マルチプロトコル・フェデレーション・サーバーを提供します。Oracle Identity Management のコンポーネントである Oracle Identity Federation は、費用効果が高く、安全なソリューションを提供しており、標準ベースのテクノロジーを使用して、多岐にわたるビジネス・ユニット、パートナー、ベンダー、および顧客間での ID の共有を可能にします。

企業の枠を越えて

Oracle Identity Federation を利用すると、組織は中央ユーザー・リポジトリを作成したり、絶え間なくデータ・ストアを同期したりすることなく、セキュリティ境界を越えてアカウントやアイデンティティに安全にリンクします。標準ベースのプロトコルを実装することによって、Oracle Identity Federation は、ID や資格証明の運用、維持、管理に法外なコストをかけることなく、ベンダー、顧客、およびビジネス・パートナーに対して、ドメイン間でのシングル・サインオンの相互運用を可能にしました。

異機種間アーキテクチャ

Oracle Identity Federation は、サード・パーティのアイデンティティおよびアクセス管理ソリューションと統合可能であるため、組織は既存のインフラストラクチャを利用できます。Oracle Identity Federation は、アイデンティティ・プロバイダ (IdP) として機能することによって、LDAP 準拠のディレクトリ・サーバー、またはデータベースに対してのユーザー認証を行います。また、Oracle Identity Federation は、これらのユーザー・リポジトリからユーザー属性を取得する際、パフォーマンスを向上させるためにダイレクト・コールを行います。サポートされる認証システム、または認可システムがすでに利用されている場合、Oracle Identity Federation は、そのシステムを利用してユーザーを認証し、パートナー・アプリケーションに渡す認証アサーションを作成します。サービス・プロバイダ (SP) の役割を果たすことによって、Oracle Identity Federation は、サポートされる認証システム、または認可システムと通信を行い、認証ユーザーのアクセス権限を特定し、データ・リポジトリからユーザーの属性を取得します。

複数プロトコルのサポート

Oracle Identity Federation は、主要なフェデレーション・プロトコルを実装しており、相互運用性と適合性に関するいくつかのイベントに参加しています。Oracle Identity Federation は、Liberty ID-FF および SAML 2.0 に対する Liberty Alliance 認証を取得しています。

標準ベースの相互運用性を実現するために、Oracle Identity Federation は、オープン・スタンダード・グループによって定義された複数のプロファイルをサポートすることによって、他ベンダーのシステムとのメッセージ交換を迅速に正しく実行しています。Oracle Identity Federation は、以下のプロファイルをサポートします。

Oracle Identity Management 製品

Oracle Access Manager は、異機種間アプリケーション環境でアクセス制御、シングル・サインオン、およびユーザー・プロファイル管理のための重要な機能を実行します。

Oracle Identity Manager は、強力で柔軟なエンタープライズ ID プロビジョニングおよび整合性監視ソリューションで、ディレクトリ、電子メール、データベース、および ERP でのユーザーの作成、更新、削除を自動化します。

Oracle Identity Federation は、識別専用フェデレーション・サーバーを使用して、ドメイン間でのシングル・サインオンを可能にします。このサーバーは完全な内蔵型であり、すぐに使用できます。

Oracle Internet Directory は、強力でスケーラブルな LDAP v3 準拠のディレクトリ・サービスで、Oracle Database 10g プラットフォームの高可用性機能を利用します。

Oracle Virtual Directory は、データの同期化や本来の位置から移動させることなく、インターネットと業界で標準の LDAP、および既存のエンタープライズ・アイデンティティ情報の XML ビューを提供します。

Oracle Web Services Manager は、ポリシー駆動型のセキュリティ機能と管理機能を、既存または新規の Web サービスに追加する包括的なソリューションです。

Oracle Enterprise Single Sign-On は、デスクトップ、クライアント・サーバー、カスタムベース、およびホストベースのアプリケーションといった、ユーザーの全エンタープライズ・リソースに対応する、統合されたサインオン機能と認証機能を提供します。

- SAML 2.0: Browser Artifact, Browser POST, Single Logout, NameIdentifier, X.509 Authentication-Based Attribute Sharing
- Liberty ID-FF 1.x: Browser Artifact, Browser POST, Single Logout, NameIdentifier, Federation Termination
- SAML 1.x: Browser Artifact, Browser POST
- WS-Federation: Passive Requester

また、Oracle Identity Federation は以下の役割を果たすように配備できます。

- Identity Provider
- Service Provider
- Attribute Requestor
- Attribute Responder

証明書の検証

セキュリティは、すべてのエンタープライズ・アーキテクチャにとって必要不可欠な要素であり、デジタル証明は、検証および認証において重要な部分です。Oracle Identity Federation は、デジタル署名と暗号化に対する X.509 証明書をサポートする、証明書の検証ストアを提供します。これによって、管理コンソール内の使いやすいインターフェースを使用して、信頼できる認証局 (CA) と証明書失効リスト (CRL) を管理できます。管理者は、送信 SAML アサーションに対する署名および暗号化と、信頼できるプロバイダからの受信メッセージの検証と認証を行うことができます。

ロード・バランシングおよびフェイルオーバーのサポート

Oracle Identity Federation は、ロード・バランシングとフェイルオーバーをサポートすることによって、ミッション・クリティカルなアプリケーションを支援するように設計されています。Oracle Identity Federation Server の複数インスタンス間でのロード・バランシングとフェイルオーバーを有効にするため、Oracle Identity Federation では、複数の Oracle Identity Federation サーバーからアクセスできる、共有データベース・インスタンスを使用するようにシステムを設定できます。Oracle Identity Federation サーバーが個別の負荷分散アルゴリズムをサポートするように設定して、特定のマシンに障害が発生した場合に、設定されたサーバーをサービスから削除するように指定できます。