Informatica®
10.1.1

セキュリティガイド

Informatica セキュリティガイド
10.1.1
2016 年 12 月

faq.html、http://www.slf4j.org/license.html、http://www.iodbc.org/dataspace/iodbc/wiki/iODBC/License、http://www.keplerproject.org/md5/license.html、http://www.toedter.com/en/jcalendar/license.html、http://www.edankert.com/bounce/index.html、http://www.net-snmp.org/about/license.html、http://www.openmdx.org/#FAQ、http://www.php.net/license/3_01.txt、http://srp.stanford.edu/license.txt、http://www.schneier.com/blowfish.html、http://www.jmock.org/license.html、http://xsom.java.net、http://benalman.com/about/license/、https://github.com/CreateJS/EaselJS/blob/master/src/easeljs/display/Bitmap.js、http://www.h2database.com/html/license.html#summary、http://jsoncpp.sourceforge.net/LICENSE、http://jdbc.postgresql.org/license.html、http://protobuf.googlecode.com/svn/trunk/src/google/protobuf/descriptor.proto、https://github.com/rantav/hector/blob/master/LICENSE、http://web.mit.edu/Kerberos/krb5-current/doc/mitK5license.html、http://jibx.sourceforge.net/jibx-license.html、https://github.com/lyokato/libgeohash/blob/master/LICENSE、https://github.com/hjiang/jsonxx/blob/master/LICENSE、https://code.google.com/p/lz4/、https://github.com/jedisct1/libsodium/blob/master/LICENSE、http://one-jar.sourceforge.net/index.php?page=documents&file=license、https://github.com/EsotericSoftware/kryo/blob/master/license.txt、http://www.scala-lang.org/license.html、https://github.com/tinkerpop/blueprints/blob/master/LICENSE.txt、http://gee.cs.oswego.edu/dl/classes/EDU/oswego/cs/dl/util/concurrent/intro.html、https://aws.amazon.com/asl/、https://github.com/twbs/bootstrap/blob/master/LICENSE、および https://sourceforge.net/p/xmlunit/code/HEAD/tree/trunk/LICENSE.txt。

本製品には、Academic Free License（http://www.opensource.org/licenses/afl-3.0.php）、Common Development and Distribution License（http://www.opensource.org/licenses/cddl1.php）、Common Public License（http://www.opensource.org/licenses/cpl1.0.php）、Sun Binary Code License Agreement Supplemental License Terms、BSD License（http:// www.opensource.org/licenses/bsd-license.php）、BSD License（http://opensource.org/licenses/BSD-3-Clause）、MIT License（http://www.opensource.org/licenses/mit-license.php）、Artistic License（http://www.opensource.org/licenses/artistic-license-1.0）、Initial Developer’s Public License Version 1.0（http://www.firebirdsql.org/en/initial-developer-s-public-license-version-1-0/）に基づいて許諾されたソフトウェアが含まれています。

本製品には、ソフトウェア copyright (C) 2003-2006 Joe WaInes, 2006-2007 XStream Committers が含まれています。All rights reserved. 本ソフトウェアに関する許諾および制限は、http://j.org/license.html にある使用条件に従います。本製品には、Indiana University Extreme! Lab によって開発されたソフトウェアが含まれています。詳細については、http://www.extreme.indiana.edu/を参照してください。

本製品には、ソフトウェア Copyright (C) 2013 Frank Balluffi and Markus Moeller が含まれています。All rights reserved. 本ソフトウェアに関する許諾および制限は、MIT ライセンスの使用条件に従います。

特許については、https://www.informatica.com/legal/patents.html を参照してください。

免責: 本文書は、一切の保証を伴わない「現状渡し」で提供されるものとし、Informatica LLC は他社の権利の非侵害、市場性および特定の目的への適合性の黙示の保証などを含めて、一切の明示的および黙示的保証の責任を負いません。Informatica LLC では、本ソフトウェアまたはドキュメントに誤りのないことを保証していません。本ソフトウェアまたはドキュメントに記載されている情報には、技術的に不正確な記述や誤植が含まれる場合があります。本ソフトウェアまたはドキュメントの情報は、予告なしに変更されることがあります。

NOTICES

この Informatica 製品（以下「ソフトウェア」）には、Progress Software Corporation（以下「DataDirect」）の事業子会社である DataDirect Technologies からの特定のドライバ（以下「DataDirect ドライバ」）が含まれています。DataDirect ドライバには、次の用語および条件が適用されます。

1. DataDirect ドライバは、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。
2. DataDirect または第三者は、予見の有無を問わず発生した ODBC ドライバの使用に関するいかなる直接的、間接的、偶発的、特別、あるいは結果的損害に対して責任を負わないものとします。本制限事項は、すべての訴訟原因に適用されます。訴訟原因には、契約違反、保証違反、過失、厳格責任、詐称、その他の不法行為を含みますが、これらに限るものではありません。

本マニュアルの情報は、予告なしに変更されることがあります。お客様が本書内に問題を発見された場合は、書面にて当社までお知らせください。Informatica LLC 2100 Seaport Blvd.Redwood City, CA 94063。

Informatica LLC は、商品性、特定目的への適合性、非侵害性の保証等を含めて、明示的または黙示的ないかなる種類の保証をせず、本マニュアルの情報を「現状のまま」提供するものとします。

発行日: 2018-07-02

目次

序文

Informatica セキュリティガイドには、Informatica ドメインのセキュリティに関する情報が含まれています。Informatica ドメインのセキュリティとドメインに接続される Informatica クライアントのセキュリティ管理に必要な情報が含まれています。本書では、読者が Informatica ドメインおよび Informatica Administrator についての知識を持っていることを前提にしています。また、使用しているネットワークの認証サーバーと認証プロセスについて読者が熟知していることも前提にしています。

Informatica のリソース

Informatica Network

Informatica Network は、 Informatica グローバルカスタマサポート、Informatica ナレッジベースなどの製品リソースをホストします。Informatica Network には、https://network.informatica.com からアクセスしてください。

メンバーは以下の操作を行うことができます。

- 1 つの場所からすべての Informatica のリソースにアクセスできます。
- ドキュメント、FAQ、ベストプラクティスなどの製品リソースをナレッジベースで検索できます。
- 製品の提供情報を表示できます。
- 自分のサポート事例を確認できます。
- 最寄りの Informatica ユーザーグループネットワークを検索して、他のユーザーと共同作業を行えます。

Informatica ナレッジベース

ドキュメント、ハウツー記事、ベストプラクティス、PAM などの製品リソースを Informatica Network で検索するには、Informatica ナレッジベースを使用します。

ナレッジベースには、https://kb.informatica.com からアクセスしてください。ナレッジベースに関する質問、コメント、ご意見の連絡先は、Informatica ナレッジベースチーム（KB_Feedback@informatica.com）です。

Informatica マニュアル

使用している製品の最新のドキュメントを取得するには、https://kb.informatica.com/_layouts/ProductDocumentation/Page/ProductDocumentSearch.aspx にある Informatica ナレッジベースを参照してください。

このマニュアルに関する質問、コメント、ご意見の電子メールの送付先は、Informatica マニュアルチーム（infa_documentation@informatica.com）です。

Informatica 製品可用性マトリックス

製品可用性マトリックス（PAM）には、製品リリースでサポートされるオペレーティングシステム、データベースなどのデータソースおよびターゲットが示されています。Informatica Network メンバである場合は、PAM（https://network.informatica.com/community/informatica-network/product-availability-matrices）にアクセスできます。

Informatica Velocity

Informatica Velocity は、Informatica プロフェッショナルサービスによって開発されたヒントおよびベストプラクティスのコレクションです。数多くのデータ管理プロジェクトの経験から開発された Informatica Velocity には、世界中の組織と協力して優れたデータ管理ソリューションの計画、開発、展開、および維持を行ってきた弊社コンサルタントの知識が集約されています。

Informatica Network メンバである場合は、Informatica Velocity リソース（http://velocity.informatica.com）にアクセスできます。

Informatica Velocity についての質問、コメント、またはアイデアがある場合は、ips@informatica.com から Informatica プロフェッショナルサービスにお問い合わせください。

Informatica Marketplace

Informatica Marketplace は、お使いの Informatica 製品を強化したり拡張したりするソリューションを検索できるフォーラムです。Informatica の開発者およびパートナーの何百ものソリューションを利用して、プロジェクトで実装にかかる時間を短縮したり、生産性を向上させたりできます。Informatica Marketplace には、https://marketplace.informatica.com からアクセスできます。

Informatica グローバルカスタマサポート

Informatica Network の電話またはオンラインサポートからグローバルカスタマサポートに連絡できます。

各地域の Informatica グローバルカスタマサポートの電話番号は、Informatica Web サイト（http://www.informatica.com/us/services-and-training/support-services/global-support-centers）を参照してください。

Informatica Network メンバである場合は、オンラインサポート（http://network.informatica.com）を使用できます。

第 1 章

Informatica セキュリティ入門

この章では、以下の項目について説明します。

Informatica セキュリティの概要

Informatica ドメインを保護することで、ドメインが実行されるネットワークの内部と外部からの脅威から守ることができます。

Informatica ドメインのセキュリティには、次のセキュリティタイプがあります。

インフラストラクチャのセキュリティ

インフラストラクチャのセキュリティは、Informatica ドメインに対する不正アクセスやサービスおよびリソースの改ざんから Informatica ドメインを守ります。インフラストラクチャのセキュリティは、以下の側面を持っています。

- Informatica ドメイン内に送信され保存されるデータの保護
- Informatica ドメインに接続するユーザーおよびサービスの認証
- 外部コンポーネント（リポジトリ、ソース、ターゲット用のクライアントアプリケーションやリレーショナルデータベースを含む）のための接続のセキュリティ。

オペレーショナルセキュリティ

オペレーショナルセキュリティは、Informatica ドメイン内のデータとサービスへのアクセスを制御します。オペレーショナルセキュリティは、以下の側面を持っています。

- 組織内でのユーザーの役割に基づいて、データとメタデータへのユーザーアクセスに制限を設定する
- 組織内でのユーザーの役割に基づいて、Informatica ドメイン内でユーザーが操作を実行する能力に制限を設定する

Informatica は、ドメインへのアクセスを認められたユーザーのリストとドメイン設定情報を、ドメイン環境設定リポジトリ内に保存しています。ドメイン環境設定リポジトリには、Informatica ドメイン内の各ユーザーに割り当てられているグループ、ロール、特権、権限も保存されています。

Informatica では、ユーザーのリストをセキュリティドメインごとに整理します。セキュリティドメインにはユーザーアカウントの集まりが入っています。1 つのドメインに複数のセキュリティドメインを設けることができます。

インフラストラクチャのセキュリティ

インフラストラクチャのセキュリティには、ユーザーとサービスの認証、ドメイン内のセキュアな通信、およびセキュアなデータストレージなどが含まれます。

認証

サービスマネージャは、ドメイン内で実行されるサービスの認証、および Informatica クライアントツールにログインするユーザーの認証を行います。

Informatica ドメインで使用を設定できる認証のタイプは、次のとおりです。

ネイティブ認証

ネイティブ認証とは、Informatica ドメイン内のユーザーアカウントのみが利用できる認証モードです。Informatica ドメインがネイティブ認証を使用するときは、サービスマネージャがドメイン環境設定リポジトリのユーザークレデンシャルと特権を保存し、Informatica ドメイン内のすべてのユーザー認証を実行します。

Informatica ドメインでネイティブ認証を使用する場合、デフォルトで、そのドメインにネイティブのセキュリティドメインが含まれ、すべてのユーザーアカウントがネイティブのセキュリティドメインに属します。

Informatica ではユーザー名とパスワードを使用して、Informatica ドメイン内のユーザーとサービスを認証します。

LDAP（Lightweight Directory Access Protocol）**による認証**

LDAP とは、ネットワーク上のユーザーとリソースにアクセスするためのソフトウェアプロトコルです。Informatica ドメインで LDAP 認証を使用する場合、ユーザーアカウントとユーザークレデンシャルは LDAP ディレクトリサービスに保存されます。ユーザーの特権と権限は、ドメイン環境設定リポジトリに保存されます。ドメイン環境設定リポジトリ内のユーザーアカウントは、定期的に LDAP ディレクトリサービス内のユーザーアカウントと同期させる必要があります。

Informatica ではユーザー名とパスワードを使用して、Informatica ドメイン内の Informatica ユーザーおよびサービスを認証します。

Kerberos **認証**

Kerberos とは、チケットを使用してネットワーク内のユーザーとサービスの認証を行うネットワーク認証プロトコルです。Informatica ドメインで Kerberos 認証を使用する場合、ユーザーのアカウントと資格情報は Kerberos のプリンシパルデータベースに保存されます。これは LDAP ディレクトリサービスの場合もあります。ユーザーの特権と権限は、ドメイン環境設定リポジトリに保存されます。ドメイン環境設定リポジトリ内のユーザーアカウントを、Kerberos のプリンシパルデータベース内のユーザーアカウントと定期的に同期させる必要があります。

Informatica では Kerberos チケットを使用して、Informatica ドメイン内の Informatica ユーザーおよびサービスを認証します。

SAML **ベースのシングルサインオン**

Security Assertion Markup Language（SAML）とは、サービスプロバイダと ID プロバイダ間で認証および承認情報を交換するための XML ベースのデータ形式です。Administrator ツール、Analyst ツール、および Monitoring ツールの Web アプリケーション用に SAML ベースのシングルサインオンを設定できます。

Informatica ドメインでは、Informatica Web アプリケーションがサービスプロバイダで、Microsoft Active Directory フェデレーションサービス（AD FS）が ID プロバイダです。Informatica Web アプリケーションユーザーのアカウントおよび資格情報は Microsoft Active Directory に格納されます。アカウントを Active Directory から Informatica ドメイン内のセキュリティドメインにインポートします。セキュ

リティドメイン内のユーザーアカウントは、定期的に Active Directory ディレクトリサービス内のユーザーアカウントと同期する必要があります。

Kerberos 認証を使用するように設定されている Informatica ドメイン内で SAML ベースのシングルサインオンを有効にすることはできません。

セキュアなドメイン通信

Informatica ドメインには、サービスマネージャおよびドメイン内のサービスと、クライアントアプリケーションとの間で送信されるデータおよびメタデータを保護するための、さまざまなオプションがあります。Informatica では、ドメイン内のコンポーネント間の通信プロトコルとして TCP/IP および HTTP を使用し、ドメイン内のサービスとサービスマネージャの間の通信を保護するために SSL 証明書を使用しています。

SSL/TLS プロトコルは、公開鍵暗号を使用してネットワークトラフィックを暗号化および復号化します。トラフィックの暗号化および復号化に使用される公開鍵は、自己署名または署名された SSL 証明書に格納されます。自己署名証明書は証明書の作成者により署名されます。署名者の ID は検証されないので、自己署名証明書は署名された証明書よりも安全性は低くなります。署名された証明書は、認証機関（CA）によって検証された証明書を求めるユーザーの ID を含む SSL 証明書のことです。セキュリティのレベルを高くするには、CA 署名の証明書をお勧めします。

キーストアには非公開キーと証明書が含まれます。これは資格情報を提供するのに使用されます。トラストストアには信頼できる SSL/TLS サーバーの証明書が含まれます。これは資格情報を検証するのに使用されます。

ドメイン内の接続を保護するには、PEM および JKS 形式のキーストアとトラストストアが必要です。次のプログラムを使用すると、必要なファイルを作成できます。

キーツール

キーツールを使用して、SSL 証明書または証明書署名要求（CSR）と、JKS 形式のキーストアおよびトラストストアを作成します。

キーツールの詳細については、以下の Web サイトに掲載されているドキュメントを参照してください。

http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html

OpenSSL

OpenSSL を使用して、SSL 証明書または CSR を作成し、JKS 形式のキーストアを PEM 形式に変換できます。

OpenSSL の詳細については、以下の Web サイトに掲載されているドキュメントを参照してください。

https://www.openssl.org/docs/

保護する接続のタイプによって、必要なファイルが決まります。

セキュアなデータストレージ

Informatica は、ドメイン環境設定リポジトリ内にデータを保存する前に、パスワードや安全な接続パラメータのような機密データを暗号化します。Informatica は、環境設定ファイルなどの機密データもセキュアディレクトリに保存します。

オペレーショナルセキュリティ

特権、ロール、権限をユーザーまたはユーザーグループに割り当てることで、ユーザーおよびグループの持つことのできるアクセスのレベル、およびドメイン内でユーザーおよびグループが実行できるアクションの範囲を管理することができます。

次の方法を使用して、ドメイン内のユーザーおよびグループのアクセスを管理することができます。

特権

特権により、ユーザーが Informatica クライアントツールで実行できるアクションが決定されます。一連の特権をユーザーに割り当てて、ドメイン内で使用できるサービスへのアクセスを制限することができます。また、特権をグループに割り当てることで、グループ内のすべてのユーザーがサービスに対して同じアクセス権を持つようにすることもできます。

ロール

ロールとは、ユーザーやグループに割り当てることができる特権のセットです。ロールを使用すると、ユーザーへの特権の割り当てをより簡単に管理できます。制限付きの特権があるロールを作成し、ドメインサービスへの限定的なアクセス権があるユーザーおよびグループにそのロールを割り当てることができます。あるいは、関連する特権のロールを作成し、それを同じレベルのアクセスを必要とするユーザーおよびグループに割り当てることもできます。

権限

権限は、オブジェクトに対するユーザーのアクセスレベルを定義しています。特定のアクションを実行する特権を持つユーザーが、特定のオブジェクトに対してアクションを実行する権限を必要としている場合があります。例えば、アプリケーションサービスを管理するには、ユーザーはサービスを管理する特権と、特定のアプリケーションサービスに対する権限を持っている必要があります。

デフォルト管理者グループ

Informatica ドメインには、サービスに対するすべての特権と権限を含んだ、システム定義の管理者グループがあります。管理者グループに追加するユーザーアカウントには、ドメイン内のすべてのサービスおよびオブジェクトへの特権と権限があります。Informatica サービスをインストールする場合、インストーラは管理者グループに属するユーザーアカウントを作成します。デフォルト管理者アカウントを利用して、最初に Administrator ツールにログインすることができます。

ドメイン環境設定リポジトリ

ドメイン環境設定リポジトリには、ドメインの設定やユーザーの特権と権限についての情報が入っています。

Informatica ドメインでネイティブユーザー認証が使用されている場合、そのドメイン環境設定リポジトリにはユーザー資格情報も入っています。ドメインが LDAP 認証または Kerberos 認証を使用している場合、ドメイン環境設定リポジトリにユーザー資格情報はありません。LDAP および Kerberos のユーザー資格情報はすべて、Informatica ドメインの外部、すなわち LDAP ディレクトリサービスまたは Kerberos プリンシパルデータベースの中に保存されます。

インストール中、Informatica ドメインを作成するときに、インストーラがリレーショナルデータベースの中にドメイン環境設定リポジトリを作成します。そのデータベースをドメイン環境設定リポジトリの作成場所として指定する必要があります。リポジトリは、SSL プロトコルで保護されたデータベース上に作成することができます。

セキュリティドメイン

セキュリティドメインとは、Informatica ドメイン内のユーザーアカウントとグループの集合です。

Informatica ドメインは、次のタイプのセキュリティドメインを持つことができます。

ネイティブのセキュリティドメイン

ネイティブのセキュリティドメインには、Administrator ツールで作成および管理されるユーザーとグループが入っています。Informatica はネイティブのセキュリティドメイン内のユーザーアカウントのすべての資格情報をドメイン環境設定リポジトリに格納します。デフォルトでは、インストール中にネイティブのセキュリティドメインが作成されます。インストール後にネイティブのセキュリティドメインを追加したり、削除することはできません。

Informatica ドメインで Kerberos 認証を使用する場合、そのドメインにネイティブのセキュリティドメインを使用することはできません。

LDAP **セキュリティドメイン**

LDAP セキュリティドメインには、LDAP のディレクトリサービスからインポートされたユーザーとグループが入っています。Informatica ドメインで LDAP 認証または Kerberos 認証を使用する場合、LDAP セキュリティドメインを作成して、LDAP ディレクトリサービスからインポートしたユーザーとグループを追加することができます。

Informatica サービスをインストールし、ネイティブまたは LDAP 認証を使用するドメインを作成する場合、インストーラはネイティブのセキュリティドメインを作成します。LDAP セキュリティドメインは作成しません。インストール後に LDAP セキュリティドメインを作成できます。

Informatica サービスをインストールし、Kerberos 認証を使用するドメインを作成する場合は、インストーラは以下の LDAP セキュリティドメインを作成します。

- 内部セキュリティドメイン。インストーラは、*_infaInternalNamespace* という名前を持つ LDAP セキュリティドメインを作成します。_infaInternalNamespace セキュリティドメインには、ユーザーがインストール時に作成したデフォルト管理者ユーザーアカウントが格納されます。インストール後に _infaInternalNamespace セキュリティドメインにユーザーを追加したり、セキュリティドメインを削除することはできません。
- ユーザーレルムのセキュリティドメイン。インストーラは空の LDAP セキュリティドメインを作成し、ドメイン名をインストール時に指定した Kerberos ユーザーレルムの名前にします。インストール後は、Kerberos プリンシパルデータベースからユーザーレルムセキュリティドメインの中にユーザーをインポートすることができます。ユーザーレルムセキュリティドメインを削除することはできません。Kerberos 認証を使用するドメインでコマンドラインプログラムを実行する場合、セキュリティドメインのオプションは、デフォルトでインストール時に作成したユーザーレルムのセキュリティドメインに設定されます。

LDAP セキュリティドメインは、Informatica ドメインで使用される認証が LDAP か Kerberos かにかかわらず、同じ方法で作成および管理することができます。

第 2 章

ユーザー認証

この章では、以下の項目について説明します。

ユーザー認証の概要

Informatica ドメインのユーザー認証は、Informatica サービスをインストールするときに設定する認証のタイプによります。

Informatica ドメインでは、ユーザー認証に以下のタイプを使用することができます。

- ネイティブユーザー認証
- LDAP ユーザー認証
- Kerberos ネットワーク認証
- Security Assertion Markup Language（SAML）ベースのシングルサインオン

ネイティブユーザーアカウントは Informatica ドメインに保存されており、Informatica ドメイン内でのみ使用することができます。

LDAP、Kerberos およびユーザーアカウントは LDAP ディレクトリサービスに保存されており、企業内のアプリケーションで共有することができます。

SAML ベースのシングルサインオンでは、Microsoft Active Directory に格納されたアカウント資格情報に対してユーザーを認証します。アカウントは Active Directory から Informatica ドメイン内のセキュリティドメインにインポートされます。

Informatica ドメインで使用する認証タイプは、インストール中に選択することができます。インストール中に Kerberos 認証を有効にする場合、Kerberos Key Distribution Center (KDC)と連動するように Informatica ドメインを設定する必要があります。Informatica ドメインで必要なサービスプリンシパル名（SPN）を Kerberos プリンシパルデータベースに作成する必要があります。Kerberos プリンシパルデータベースは、LDAP ディレクトリサービスの場合もあります。また、Informatica ドメインの必要に応じて、SPN にキータブファイルを作成して Informatica ディレクトリに格納する必要があります。

Kerberos 認証をインストール中に有効にしなかった場合、インストーラはネイティブの認証を使用するように Informatica ドメインを設定します。インストール後に、LDAP サーバーへの接続を設定し、ネイティブ認証に加えて LDAP 認証も使用するように Informatica ドメインを設定することができます。

ネイティブの認証と LDAP の認証を Informatica ドメインで両方使用してもかまいません。サービスマネージャはセキュリティドメインに基づいてユーザーを認証します。ユーザーがネイティブのセキュリティドメインに属する場合、サービスマネージャはドメイン環境設定リポジトリでユーザーを認証します。ユーザーが LDAP のセキュリティドメインに属する場合、サービスマネージャは認証のためにユーザー名とパスワードを LDAP サーバーに渡します。

ネイティブの認証を Kerberos 認証とともに使用することはできません。Informatica ドメインで Kerberos 認証が使用される場合、すべてのユーザーアカウントが LDAP セキュリティドメインに存在する必要があります。Kerberos サーバーは、ユーザーがネットワークにログインするときにユーザーアカウントを認証します。Informatica クライアントアプリケーションはネットワークログインからの資格情報を使用して Informatica ドメイン内のユーザーを認証します。ネイティブグループおよびロールは引き続きサポートされます。

Informatica Web アプリケーションへの SAML ベースのシングルサインオンは、インストール中でもインストール後でも有効にできます。ただし、SAML ベースのシングルサインオンを有効にする前に、すべての必要なセットアップタスクを完了する必要があります。Kerberos 認証を使用するように設定されている Informatica ドメイン内で SAML ベースのシングルサインオンを有効にすることはできません。

ネイティブユーザー認証

Informatica ドメインでネイティブ認証を使用している場合、サービスマネージャはすべてのユーザーアカウント情報を保存し、Informatica ドメイン内のすべてのユーザー認証を行います。ユーザーがログインすると、サービスマネージャがネイティブのセキュリティドメインを使用してユーザー名とパスワードを認証します。

Informatica ドメインを Kerberos ネットワーク認証を使用するように設定しない場合、Informatica ドメインはデフォルトでネイティブのセキュリティドメインを含めます。ネイティブセキュリティドメインはインストール時に作成され、削除することはできません。Informatica ドメインが持てるのは、1 つのネイティブセキュリティドメインのみです。 ネイティブのセキュリティドメイン内のユーザーアカウントは、Administrator ツールで作成および管理します。サービスマネージャは、ユーザーアカウントに関する詳細（ユーザーの資格情報や特権を含む）をドメイン環境設定リポジトリ内に保存します。

LDAP ユーザー認証

Informatica ドメインを、LDAP ディレクトリサービス内のユーザーが Informatica クライアントアプリケーションにログインできるように設定することができます。Informatica ドメインは、ネイティブユーザー認証に加え、LDAP ユーザー認証も使用することができます。

Informatica ドメインで LDAP ユーザー認証が使用できるようにするには、LDAP サーバーへの接続を設定し、Informatica ドメインにアクセスできる LDAP ディレクトリサービスからユーザーとグループを指定する必要があります。Administrator ツールを使用して、LDAP サーバーへの接続を設定できます。

LDAP セキュリティドメインを LDAP ディレクトリサービスと同期する場合、サービスマネージャは Informatica ドメインへのアクセス権を持つ LDAP ユーザーアカウントのリストを LDAP セキュリティドメインにインポートします。特権と権限を LDAP セキュリティドメイン内のユーザーに割り当てると、サービスマネージャはその情報をドメイン環境設定リポジトリに保存します。サービスマネージャは、ドメイン環境設定リポジトリ内にユーザー資格情報を保存しません。

ユーザーがログインすると、サービスマネージャは、認証のためにユーザー名とパスワードを LDAP サーバーに渡します。

注: サービスマネージャは、LDAP のディレクトリサービスが匿名ログインモードに空白のパスワードを許可することがある場合でも、LDAP のユーザーがパスワードを使ってクライアントアプリケーションにログインするように要求します。

Kerberos 認証

Kerberos ネットワーク認証を使用してネットワーク上のユーザーとサービスを認証するように Informatica ドメインを設定できます。

Kerberos は、チケットを使用してネットワーク内のサービスとノードの認証を行うネットワーク認証プロトコルです。Kerberos では、Key Distribution Center（KDC）を使用してユーザーおよびサービスの ID を確認し、認証されたユーザーアカウントおよびサービスアカウントにチケットを付与します。Kerberos プロトコルでは、ユーザーとサービスはプリンシパルとして認識されます。KDC には、プリンシパルのデータベースとそれらに関連付けられたシークレットキーがあり、それらは ID の証明として使われます。Kerberos は LDAP ディレクトリサービスをプリンシパルデータベースとして使用できます。

Kerberos 認証を使用するには、Kerberos ネットワーク認証を使用するネットワーク上で Informatica ドメインをインストールおよび実行する必要があります。Informatica は、プリンシパルデータベースとしての Microsoft Active Directory サービスとともに、Kerberos 認証を使用するネットワークで動作できます。

Informatica は、クロス、または複数レルムの Kerberos 認証をサポートしていません。サーバーホスト、クライアントマシン、および Kerberos 認証サーバーは、同じレルムにある必要があります。

Informatica ドメインでは、ネットワーク上でパスワードを転送することなくドメイン内のノードとサービスを認証するために、キータブファイルを必要とします。キータブファイルにはサービスプリンシパル名（SPN）と関連付けられた暗号化キーが含まれています。Informatica ドメインでノードとサービスを作成する前に、キータブファイルを作成します。

Informatica Web アプリケーションへの SAML ベースのシングルサインオン

ユーザーが SAML ベースのシングルサインオン（SSO）を使用して Administrator ツール、Analyst ツール、Monitoring ツールの Web アプリケーションにログインできるように Informatica ドメインを設定できます。

Security Assertion Markup Language（SAML）とは、サービスプロバイダと ID プロバイダ間で認証および承認情報を交換するための XML ベースのデータ形式です。Informatica ドメインでは、Informatica Web アプリケーションがサービスプロバイダです。Microsoft Active Directory フェデレーションサービス（AD FS）2.0 が ID プロバイダであり、組織の Active Directory ID ストアに対して Web アプリケーションユーザーを認証します。

Informatica ドメインで SAML ベースのシングルサインオンを使用できるようにするには、Informatica Web アプリケーションのユーザーアカウント用に LDAP セキュリティドメインを作成し、ユーザーを Active Directory からドメインにインポートする必要があります。Administrator ツールを使用して Active Directory サーバーへの接続をセットアップして、ユーザーをセキュリティドメインにインポートできます。

ユーザーが Informatica Web アプリケーションにログインすると、アプリケーションは SAML 認証要求を AD FS に送信します。AD FS は Active Directory のユーザーアカウント情報に対してユーザーの資格情報を認証

し、ユーザーに関するセキュリティ関連情報が含まれる SAML アサーショントークンを Web アプリケーションに返します。

Informatica Web アプリケーションユーザーの認証に使用される SAML トークンを発行するように AD FS を設定します。また、AD FS から ID プロバイダアサーション署名証明書をエクスポートして、証明書をドメイン内の各ゲートウェイノード上にある Informatica のデフォルトのトラストストアファイルにインポートする必要があります。

第 3 章

LDAP セキュリティドメイン

この章では、以下の項目について説明します。

LDAP セキュリティドメインの概要

LDAP のセキュリティドメインには、LDAP ディレクトリサービスからインポートされた一連のユーザーとグループが含まれています。LDAP のセキュリティドメインは、LDAP のユーザー認証または Kerberos のネットワーク認証を使用する場合に作成する必要があります。

Informatica ドメインおよびクライアントアプリケーションへのアクセスを許可する LDAP ディレクトリサービスのユーザーのリストを保存するように LDAP セキュリティドメインを設定します。LDAP セキュリティドメインにユーザーアカウントの資格情報は保存されません。ユーザーが Informatica クライアントにログインするときに、サービスマネージャがそのユーザーアカウントがセキュリティドメインにあるかどうか検証します。ユーザーアカウントが LDAP セキュリティドメインに属している場合、サービスマネージャは LDAP ディレクトリサービスを使用してユーザーを認証します。

Informatica サービスをインストールし、Kerberos 認証を有効にしない場合、デフォルトで Informatica のインストーラがネイティブセキュリティドメインを作成します。インストール後に、ユーザーとグループをネイティブセキュリティドメインに追加できます。Informatica クライアントアプリケーションへのアクセス権を付与するユーザーが LDAP ディレクトリサービス内にいる場合、ネイティブセキュリティドメインに加えて LDAP セキュリティドメインを設定することができます。LDAP サーバーへの接続を設定し、ユーザーおよびグループを LDAP セキュリティドメインにインポートします。

ユーザーが Informatica サービスをインストールし、Kerberos 認証を有効にする場合、Informatica のインストーラが、インストール中にユーザーが指定する Kerberos レルムの名前を使って LDAP セキュリティドメインを作成します。インストール後に、LDAP サーバーへの接続を設定し、LDAP ディレクトリサービスからユーザーおよびグループを LDAP セキュリティドメインにインポートできます。Kerberos 認証を使用する場合、ネイティブのセキュリティドメインは使用できません。

LDAP セキュリティドメインの設定

LDAP ディレクトリサービスからインポートしたユーザーアカウントに対して、LDAP セキュリティドメインを作成することができます。異なるグループのユーザーを整理するために、複数の LDAP セキュリティドメインを作成することができます。

LDAP ディレクトリサービス内で LDAP ユーザおよびグループを作成および管理します。LDAP サーバーへの接続を設定し、検索フィルタを使用して、Informatica ドメインにアクセスできるユーザーとグループを指定します。次に、ユーザーアカウントを LDAP セキュリティドメインにインポートします。LDAP サーバーが SSL プロトコルを使用する場合、SSL 証明書の場所も指定する必要があります。

以下の LDAP ディレクトリサービスからユーザーをインポートすることができます。

- IBM Tivoli Directory Server
- Microsoft Active Directory

  注: Kerberos 認証を使用する場合、Microsoft Active Directory からユーザーのインポートのみ可能です。
- Novell eDirectory
- OpenLDAP
- Sun Java System Directory Server

LDAP セキュリティドメイン内にユーザーをインポートした後に、ロール、特権、権限をユーザーに割り当てることができます。LDAP ユーザーアカウントを、ネイティブグループに割り当て、Informatica ドメイン内でのユーザーのロールに基づいて整理することができます。

Administrator ツールを使用して、LDAP セキュリティドメイン内のユーザーおよびグループを作成、編集、または削除することはできません。LDAP ディレクトリサービスの LDAP ユーザーおよびグループに対して変更を加えてから、LDAP セキュリティドメインを LDAP ディレクトリサービスと同期する必要があります。

LDAP 環境設定ダイアログボックスで、LDAP ディレクトリサービスへの接続の設定と、LDAP セキュリティドメインの作成を行うことができます。また、LDAP 環境設定ダイアログボックスでは、同期スケジュールの設定もできます。

LDAP セキュリティドメインを設定するには、次の手順を実行します。

1. LDAP ディレクトリサービスへの接続の設定
2. セキュリティドメインを設定します。
3. 同期時間をスケジュールします。

手順 1.LDAP サーバーへの接続の設定

Informatica ドメインに対するユーザーアカウントのインポート元になるディレクトリサービスが入っている LDAP サーバーへの接続を設定します。

LDAP サーバーへの接続を設定するときは、サービスマネージャが Informatica ドメイン内のグループにユーザーを割り当てるときに、LDAP ユーザーアカウントの識別名属性の大文字小文字の区別を無視する必要があることを指定します。サービスマネージャが大文字小文字の区別を無視しない場合、サービスマネージャがグループに属するユーザーの一部を割り当てない場合があります。

LDAP サーバーで SSL を使用する場合、Informatica ドメイン内の各ゲートウェイノード上にある cacerts トラストファイルに証明書をインポートする必要があります。詳細については「「自己署名 SSL 証明書の使用」 (ページ 28)」を参照してください。

LDAP ディレクトリサービスへの接続を設定するには、次の手順を実行します。

1. Administrator ツールで、**[セキュリティ]** タブをクリックします。

2. **［アクション］**メニューをクリックし、**［LDAP 設定］**を選択します。
3. **［LDAP の設定］**ダイアログボックスで、**［LDAP の接続方法］**タブをクリックします。
4. LDAP サーバーの接続プロパティを設定します。

   場合によって、LDAP の管理者に連絡して LDAP サーバの情報を入手する必要があります。

   以下の表は、LDAP サーバー設定のプロパティの説明です。

プロパティ	説明
サーバー名	LDAP ディレクトリサービスをホストするマシンのホスト名または IP アドレス。
ポート	LDAP サーバのリスニングポートこれは、LDAP ディレクトリサービスと通信するポート番号です。通常、LDAP サーバのポート番号は 389 です。LDAP サーバが SSL を使用する場合、LDAP サーバのポート番号は 636 です。最大のポート番号は 65535 です。
LDAP ディレクトリサービス	LDAP ディレクトリサービスのタイプ。 次のディレクトリサービスから選択します。 **注:** Kerberos 認証を使用する場合、Microsoft Active Directory を選択する必要があります。
名前	Principal User の識別名(DN)。通常、ユーザ名は、共通名（CN）、組織（O）、および国名（C）により構成されます。Principal User の名前は、ディレクトリへのアクセス権を持つ管理ユーザです。LDAP ディレクトリサービス内の他のユーザエントリの読み取り権限を持つユーザを指定します。匿名ログインの場合はブランクのままにします。詳細については、LDAP ディレクトリサービスのマニュアルを参照してください。
パスワード	Principal User のパスワード。匿名ログインの場合はブランクのままにします。 Kerberos 認証を使用する場合は使用できない。
SSL 認証の使用	LDAP サーバーがセキュアソケットレイヤー（SSL）プロトコルを使用することを示します。
トラスト LDAP 証明書	サービスマネージャにより、LDAP サーバーの SSL 証明書が信頼できるかどうかが判断されます。 このオプションを選択する場合、サービスマネージャは、SSL 証明書を確認しないで LDAP サーバーに接続します。 このオプションを選択しない場合、サービスマネージャは、LDAP サーバーに接続する前に SSL 証明書が認証機関によって署名されていることを確認します。 サービスマネージャが自己署名証明書が有効なものであると認識できるようにするには、使用するトラストストアファイルとパスワードを指定します。
大文字と小文字を区別しない	サービスマネージャでグループにユーザーを割り当てるときに識別名属性の大文字と小文字を区別しないことを示す。このオプションは有効にしてください。

プロパティ	説明
グループメンバシップ属性	ユーザを削除するグループの名前。これは、グループのメンバーであるユーザおよびグループの DN を含む LDAP グループオブジェクト内の属性です。たとえば、*member* または *memberof* です。
最大サイズ	セキュリティドメインにインポートするユーザとグループの最大数。例えば、この値を 100 に設定した場合、最大 100 個のユーザーアカウントをセキュリティドメインにインポートできます。 インポートするユーザがこのプロパティ値を超えた場合、サービスマネージャによってエラーメッセージが生成され、いずれのユーザもインポートされません。インポートするユーザー数が多い場合は、このプロパティに大きい値を設定してください。 デフォルトは 1000 です。

5. [テスト接続]をクリックし、LDAP サーバーへの接続が有効であるか確認します。

手順 2.セキュリティドメインの設定

LDAP ディレクトサービスからインポートするユーザーアカウントおよびグループの組ごとに、セキュリティドメインを作成します。検索ベースおよびフィルタを設定して、セキュリティドメインに入れるユーザーアカウントおよびグループのセットを定義します。サービスマネージャは、ユーザー検索ベースおよびフィルタを使用して、グループをインポートするために、ユーザーアカウントとグループ検索ベースおよびフィルタをインポートします。サービスマネージャは、グループと、グループに属するユーザーのリストをインポートします。グループフィルタに含まれるグループと、ユーザーフィルタに含まれるユーザーアカウントがインポートされます。

LDAP ディレクトリサービスからインポートするユーザーおよびグループの名前は、ネイティブのユーザーおよびグループの名前と同じ規則に従う必要があります。サービスマネージャは、名前がネイティブのユーザーおよびグループ名の規則に準拠していない場合、LDAP ユーザーまたはグループをインポートしません。

注: ネイティブユーザー名と異なり、LDAP ユーザー名は大文字と小文字を区別できます。

LDAP ディレクトリサービスを設定するとき、一意の ID（UID）に対して異なる属性を使用できます。サービスマネージャでは、各 LDAP ディレクトリサービスのユーザーを識別するために、固有の UID が必要になります。セキュリティドメインを設定する前に、LDAP ディレクトリサービスで必要な UID が使用されていることを確認します。

次の表に、各 LDAP ディレクトリサービスに対して必要な UID を示します。

LDAP **ディレクトリサービス**	UID
IBM Tivoli Directory Server	uid
Microsoft Active Directory	sAMAccountName
Novell eDirectory	uid
OpenLDAP	uid
Sun Java System Directory Server	uid

サービスマネージャでは、ユーザーアカウントが有効であるか無効であるかを示す LDAP 属性がインポートされません。Administrator ツールで、LDAP ユーザーアカウントを有効または無効にする必要があります。LDAP ディレクトリサービスでのユーザーアカウントのステータスは、アプリケーションクライアントでのユ

ーザー認証に影響します。 例えば、Informatica ドメインでは有効であるが、LDAP ディレクトリサービスでは無効であるユーザーアカウントがあるとします。 LDAP ディレクトリサービスで、無効なユーザーアカウントのログインを許可する場合、そのユーザーはアプリケーションクライアントにログイン可能になります。 LDAP ディレクトリサービスで、無効なユーザーアカウントのログインを許可しない場合、そのユーザーはアプリケーションクライアントにログインできません。

注: LDAP 接続プロパティを変更して別の LDAP サーバーに接続する場合、サービスマネージャは既存のセキュリティドメインを削除しません。LDAP セキュリティドメインが新規 LDAP サーバーに対して適切であることを確認する必要があります。セキュリティドメインのユーザーおよびグループのフィルタを変更するか、追加のセキュリティドメインを作成することで、Informatica ドメイン内で使用するユーザーおよびグループをサービスマネージャが適切にインポートできるようにします。

LDAP セキュリティドメインを設定するには、次の手順を実行します。

1. Administrator ツールで、**［セキュリティ］**タブをクリックします。
2. **［アクション］**メニューをクリックし、**［LDAP 設定］**を選択します。
3. **［LDAP の設定］**ダイアログボックスで、**［セキュリティドメイン］**タブをクリックします。
4. **［追加］**をクリックします。
5. LDAP クエリの構文を使用して、作成中のセキュリティドメインに含めるユーザーとグループを指定するフィルタを作成します。

   場合によっては LDAP 管理者に問い合わせて、LDAP ディレクトリサービスで使用可能なユーザーおよびグループに関する情報を取得する必要があります。

   次の表で、セキュリティドメインに対して設定可能なフィルタプロパティについて説明します。

プロパティ	説明
セキュリティドメイン	ドメインの名前。この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。128 文字を超えたり、以下の特殊文字を含めたりすることはできません。 , + / < > @ ; \ % ? 名前の最初および最後の文字以外で、ASCII のスペース文字を使用できます。その他のスペース文字は許可されません。
ユーザ検索ベース	LDAP ディレクトリサービス内のユーザ名検索の基点となるエントリの識別名（Distinguished Name：DN）。検索により、オブジェクトの識別名のパスに従ってディレクトリ内のオブジェクトが見つかります。 たとえば、Microsoft Active Directory では、ユーザオブジェクトの識別名は、cn=UserName、ou=OrganizationalUnit、dc=DomainName となり、dc=DomainName により示される一連の相対識別名は、オブジェクトの DNS ドメインを識別します。
ユーザーフィルタ	ディレクトリサービス内のユーザ検索の基準を指定する LDAP クエリー文字列。このフィルタでは、属性タイプ、アサーション値、マッチング基準が指定できます。 たとえば、<>(objectclass=*)</>はすべてのオブジェクトを検索します。(&(objectClass=user)(!)(!(cn=susan)))</>は、「susan」以外のすべてのユーザオブジェクトを検索します。検索フィルタの詳細については、LDAP サーバのマニュアルを参照してください。検索フィルタの詳細については、LDAP ディレクトリサービスのマニュアルを参照してください。

プロパティ	説明
グループ検索ベース	LDAP ディレクトリツリー内のグループ名検索の基点となるエントリの識別名（Distinguished Name：DN）。
グループフィルタ	ディレクトリサービス内のグループ検索の基準を指定する LDAP クエリー文字列。

6. **［プレビュー］**をクリックすると、フィルタパラメータに該当するユーザーとグループのリストのサブセットを表示します。

   プレビューで適切なユーザーおよびグループのセットが表示されない場合は、ユーザーおよびグループのフィルタおよび検索ベースを変更して、適切なユーザーおよびグループを取得します。

7. 別の LDAP セキュリティドメインを追加するには、手順 4～6 を繰り返します。
8. セキュリティドメイン内のユーザーとグループを LDAP ディレクトリサービス内のユーザーとグループと今すぐ同期化するには、**［今すぐ同期］**をクリックします。

   サービスマネージャは、すべての LDAP セキュリティドメイン内のユーザーを、LDAP ディレクトリサービス内のユーザーと同期化します。同期処理が完了するまでの時間は、インポートするユーザーおよびグループの数によって異なります。

9. **［OK］**をクリックして、セキュリティドメインを保存します。

手順 3。 同期時間のスケジュール設定

LDAP セキュリティドメイン内のユーザーおよびグループのリストと、LDAP ディレクトリサービス内のユーザーおよびグループのリストとを、サービスマネージャが定期的に同期するようにスケジュールを設定することができます。

重要: 同期プロセスを開始する前に、LDAP サーバーのホスト名のエントリが/etc/hosts ファイルに含まれることを確認します。サービスマネージャで LDAP サーバーのホスト名を解決できない場合、ユーザー同期が失敗することがあります。

同期中、サービスマネージャは、ユーザーおよびグループを LDAP ディレクトリサービスからインポートします。サービスマネージャは、インポートに使用した検索フィルタに含まれなくなったユーザーまたはグループを LDAP セキュリティドメインから削除します。

デフォルトでサービスマネージャには、LDAP ディレクトリサービスと同期化する時間はスケジュールされていません。LDAP セキュリティドメイン内のユーザーとグループのリストが確実に正確になるようにするために、LDAP セキュリティドメインをサービスマネージャが同期化する一日の時刻をスケジュールすることができます。サービスマネージャは、LDAP セキュリティドメインと LDAP ディレクトリサービスとを、設定した時間に毎日同期化を行います。

注: 同期中は、サービスマネージャが同期対象のユーザーアカウントをロックします。ユーザーアカウントがロックされているときは、サービスマネージャはユーザーアカウントを認証できません。ユーザーがアプリケーションクライアントにログインできない場合があります。 同期の開始時にユーザーがアプリケーションクライアントにログインしている場合、ユーザーがタスクを実行できない場合があります。同期化処理の時間は、同期化するユーザーおよびグループの数によって異なります。使用の混乱を避けるために、大部分のユーザーがログインしていない時間にセキュリティドメインの同期化を行います。 100 を超えるユーザーまたはグループを同期する場合、同期を実行する前に LDAP ディレクトリサービスでのページングを有効にします。LDAP ディレクトリサービスのページングが有効になっていないと、同期化が失敗することがあります。

LDAP セキュリティドメインを LDAP ディレクトリサービスと同期するスケジュールを設定するには、次の手順を実行します。

1. Administrator ツールで、**［セキュリティ］**タブをクリックします。

2. **［アクション］**メニューをクリックし、**［LDAP 設定］**を選択します。
3. **［LDAP の設定］**ダイアログボックスで、**［スケジュール］**タブをクリックします。
4. **［追加］**ボタン（+）をクリックして時間を追加します。

   同期化スケジュールでは、24 時間形式を使用します。

   一日のうちの同期時間は必要に応じて追加することができます。LDAP ディレクトリサービス内のユーザーおよびグループのリストの変更が多い場合は、サービスマネージャを一日に何度も同期するようにスケジュール設定できます。
5. セキュリティドメイン内のユーザーとグループを LDAP ディレクトリサービス内のユーザーとグループと今すぐ同期化するには、**［今すぐ同期］**をクリックします。
6. **［OK］**をクリックして同期化スケジュールを保存します。

   注: サービスマネージャを LDAP ディレクトリサービスと同期化する前に Informatica ドメインを再起動してしまうと、追加した同期化時間の設定が失われます。

LDAP ディレクトリサービスでのネストされたグループの使用

LDAP セキュリティドメインには、ネストされた LDAP グループを含めることができます。Service Manager は、以下の方法で作成された、ネストされたグループをインポートできます。

- 同じ組織単位（OU）下にグループを作成する。
- グループ間の関係を設定する。

例えば、グループ B がグループ A のメンバで、グループ D がグループ C のメンバであるネストされたグループを作成するとします。

1. グループ A、グループ B、グループ C、グループ D を同じ OU 内に作成します。
2. グループ A を編集し、グループ B をメンバとして追加します。
3. グループ C を編集し、グループ D をメンバとして追加します。

ネストされた LDAP グループは、異なる方法で作成された LDAP セキュリティドメインにインポートすることはできません。

自己署名 SSL 証明書の使用

認証機関（CA）によって署名された SSL 証明書を使用する LDAP サーバーに接続できます。デフォルトでは、サービスマネージャ は、自己署名証明書を使用する LDAP サーバーに接続しません。

SSL 証明書を使用する LDAP サーバーに接続するには、Java キーツールキーおよび証明書管理ユーティリティを使用して証明書をドメイン内の各ゲートウェイノード上にある cacerts トラストストアファイルにインポートします。cacerts トラストストアファイルは各ノードの以下のディレクトリにあります。

<Informatica のインストールディレクトリ>\java\jre\lib\security

キーツールユーティリティは、各ノードの以下のディレクトリにあります。

<Informatica installation directory>\java\jre\bin

証明書をインポートしたらノードを再起動します。

LDAP セキュリティドメインの削除

LDAP セキュリティドメイン内のユーザーが、アプリケーションクライアントにアクセスするのを永続的に禁止するために、LDAP セキュリティドメインを削除することができます。 LDAP セキュリティドメインを削除した場合、Service Manager により、LDAP セキュリティドメイン内のすべてのユーザーおよびグループはドメイン環境設定データベースから削除されます。

1. ［LDAP の設定］ダイアログボックスで、**［セキュリティドメイン］**タブをクリックします。

   ［LDAP 設定］ダイアログボックスに、セキュリティドメインのリストが表示されます。
2. 適切なセキュリティドメインを削除しようとしていることを確認するには、セキュリティドメイン名をクリックして、ユーザーおよびグループのインポートに使用するフィルタを表示し、それが削除するセキュリティドメインであることを確認します。
3. セキュリティドメインの横にある **［削除］**ボタンをクリックして、セキュリティドメインを削除します。
4. **［OK］**をクリックして、セキュリティドメインを削除することを確認します。

第 4 章

Kerberos 認証のセットアップ

この章では、以下の項目について説明します。

Kerberos 認証のセットアップ概要

インストール中に Informatica ドメインを作成する場合は、Kerberos 認証を有効にするオプションを選択することができます。インストール中に Kerberos 認証を有効にしない場合、Informatica コマンドラインプログラムを使用して Kerberos 認証を使用するようにドメインを設定できます。

コマンドライン上で Informatica ドメインの Kerberos 認証を設定するには、以下の手順を実行します。

1. LDAP ユーザードメインとユーザーを Microsoft Active Directory から作成します。
2. ネイティブユーザーを LDAP セキュリティドメインに移行します。
3. Kerberos 設定を設定し、構成ファイルを Informatica ディレクトリにコピーします。
4. Informatica ドメインで必要なフォーマットの SPN とキータブファイル名を生成します。
5. SPN とキータブファイル形式のテキストファイルを確認します。
6. SPN とキータブファイルを作成します。
7. Informatica ドメインの Kerberos 認証を設定します。
8. Informatica ドメインでノードを更新します。

9. クライアントマシンを更新します。
10. Informatica ドメインを起動し、Administrator ツールを実行します。

Kerberos 認証および LDAP セキュリティドメインの設定後、ユーザーアカウントが適切な特権および権限を持っていることを確認します。ドメイン内のサービスが予定どおりに実行され、ユーザーがシングルサインオンを使用してログインできることを確認します。

注: ここで説明する手順は、Kerberos 認証を有効にせずに Informatica サービスをインストールしたことを前提としています。インストール中に Kerberos 認証を有効にしていた場合は、『Informatica インストールガイド』の手順に従ってください。

手順 1. LDAP ユーザードメインとユーザーの Microsoft Active Directory からの作成

Kerberos 認証を使用するように Informatica ドメインを設定する前に、すべてのユーザーアカウントが Informatica ドメイン内の LDAP セキュリティドメインにあることを確認します。ユーザーアカウントを Microsoft Active Directory から LDAP セキュリティドメインにインポートする必要があります。

Informatica ドメインのユーザーアカウントが、Microsoft Active Directory を使用しない LDAP セキュリティドメインにある場合は、Microsoft Active Directory にユーザーを移行します。ユーザーアカウントの Microsoft Active Directory への移行の詳細については、LDAP 実装のドキュメントを参照してください。

ドメインのユーザーアカウントがネイティブセキュリティドメインにある場合は、Microsoft Active Directory にユーザーを移行します。LDAP セキュリティドメインを設定して、Microsoft Active Directory サービスへの接続を設定します。次に、ユーザーおよびグループ用にフィルタをセットアップし、Microsoft Active Directory のユーザーアカウントを LDAP セキュリティドメインのユーザーアカウントと同期します。

LDAP ドメインの設定とユーザーアカウントの同期の詳細については、「LDAP セキュリティドメインの設定」 (ページ 23)を参照してください。

手順 2. ネイティブユーザーの特権および権限の LDAP セキュリティドメインへの移行

Informatica ドメインのユーザーアカウントがネイティブセキュリティドメインにある場合、アカウントのすべてのユーザーグループ、ロール、特権、および権限を LDAP セキュリティドメイン内の対応するユーザーアカウントに移行します。Kerberos 認証を使用するように Informatica ドメインを設定した後は、ネイティブセキュリティドメイン内のユーザーアカウントを変更することはできません。

ドメインのユーザーアカウントがネイティブセキュリティドメインにある場合は、LDAP セキュリティドメイン内の対応する Active Directory ユーザーアカウントに、同じグループ、ロール、特権、および権限が必要です。ネイティブユーザーのグループ、ロール、特権、および権限を、LDAP セキュリティドメイン内のユーザーに移行します。次に、グループ、ロール、特権、および権限が正しく移行されたことを確認します。

ドメインのユーザーアカウントがネイティブセキュリティドメインにない場合は、「手順 3。 Kerberos 設定ファイルの設定」 (ページ 35)に進むことができます。

ネイティブユーザーのグループ、ロール、特権、および権限を、LDAP セキュリティドメイン内のユーザーに移行し、以下の手順を実行します。

1. Kerberos 認証のユーザーアカウントを確認します。
2. ユーザー移行ファイルを作成します。
3. infacmd isp migrateusers コマンドを実行します。
4. ユーザーアカウントのグループ、ロール、特権、および権限を確認します。

注: ユーザーアカウントのグループ、ロール、特権、および権限の移行時に問題を回避するには、移行プロセス中にワークフローの実行またはユーザーのグループ、ロール、特権、および権限の変更を行わないようにします。

Kerberos 認証用のユーザーアカウントの確認

ネイティブユーザーアカウントのリストを確認し、Kerberos 認証用の LDAP セキュリティドメインに移行するアカウントを決定します。

Informatica ドメイン内のユーザーアカウントを一覧表示するには、以下のコマンドを実行します。

```
infacmd isp ListAllUsers
```

LDAP セキュリティドメインに移行する各ネイティブユーザーアカウントに対応するアカウントが、Kerberos 認証用に使用する Microsoft Active Directory サービス内に存在する必要があります。

アカウントが Microsoft Active Directory サービスに存在しない場合は、ディレクトリサービスにユーザーアカウントを追加します。Microsoft Active Directory サービスへのユーザーアカウントの追加の詳細については、Microsoft Active Directory マニュアルを参照してください。

注: LDAP セキュリティドメイン内のユーザーアカウントのユーザー名の長さは最大 20 文字です。Microsoft Active Directory サービスにユーザーアカウントを追加する際、ユーザー名の長さは 20 文字を超えないようにしてください。

ユーザー移行ファイルの作成

infacmd isp migrateUsers コマンドは、ユーザー移行ファイルを使用して、LDAP ユーザーに割り当てるグループ、ロール、特権、および権限を決定します。ユーザー移行ファイルは、ネイティブユーザーと、対応する LDAP ユーザーのリストを含むプレーンテキストファイルです。これらのユーザーは、同じグループ、ロール、特権、および権限を必要とします。

ユーザー移行ファイルを作成する際、ユーザーアカウントのセキュリティドメインを指定する必要があります。フォワードスラッシュ（/）でセキュリティドメインとユーザー名を区切ります。カンマ（,）でネイティブユーザーと対応する LDAP ユーザーを区切ります。セキュリティドメインでは大文字と小文字が区別されます。ユーザー名では大文字と小文字が区別されません。

ユーザー移行ファイル内にエントリをリストするには、以下の形式を使用します。

```
Native/<SourceUserName>,LDAP/<TargetUserName>
```

ネイティブユーザーのグループ、ロール、特権、および権限を、異なる LDAP セキュリティドメインのユーザーに移行できます。例えば、ユーザー移行ファイルに以下のユーザーのリストが含まれています。

```
Native/User1,LDAPSecurityDomain/User1
Native/User2,LDAPSecurityDomain/User2
Native/User3,newLDAPSecDomain/User3
```

migrateUser コマンドは、LDAPSecurityDomain の User1 および User2 に、ネイティブセキュリティドメインの User1 および User2 と同じグループ、ロール、特権、および権限を割り当てます。このコマンドは newLDAPSecDomain の User3 に、ネイティブセキュリティドメインの User3 と同じグループ、ロール、特権、および権限を割り当てます。

migrateUsers コマンドは、重複したソースユーザー名またはターゲットユーザー名のエントリをスキップします。

infacmd isp migrateUsers コマンドの実行

グループ、ロール、特権、および権限をネイティブセキュリティドメインのユーザーから LDAP セキュリティドメインのユーザーに移行するには、infacmd migrateUsers コマンドを実行し、使用するユーザー移行ファイルを指定します。

infacmd isp migrateUsers コマンドを実行する前に、ドメイン上の以下のサービスのすべてのインスタンスが実行中であることを確認します。

- アナリストサービス
- コンテンツ管理サービス
- モデルリポジトリサービス
- Metadata Manager サービス
- PowerCenter®リポジトリサービス

PowerCenter リポジトリサービスがノーマルモードで実行中であることを確認します。

ユーザーのグループ、ロール、特権、および権限を移行するには、以下のコマンドを実行します。

```
infacmd isp migrateUsers -dn <DomainName> -un <AdministratorUserName> -pd <AdministratorPassword> -umf <UserMigrationFile>
```

例えば、以下のコマンドでは、um_s.txt ユーザー移行ファイルに基づき、ユーザーのグループ、ロール、特権、および権限を移行します。

```
infacmd isp migrateUsers -dn UMT_Domain -un Administrator -pd Admnistrator -umf C:\UMT\um_s.txt
```

このコマンドは、LDAP ユーザーに割り当てられた接続オブジェクト権限を、ネイティブユーザーの接続オブジェクト権限で上書きします。このコマンドは、ネイティブユーザーおよび対応する LDAP ユーザーのグループ、ロール、特権、およびドメインオブジェクト権限をマージします。

migrateUsers コマンドでは、コマンドを実行するディレクトリに infacmd_umt_<date>_<time>.txt という名前の詳細なログファイルを作成します。

コマンドの詳細については、『*Informatica コマンドリファレンス*』を参照してください。

migrateUsers コマンドのトラブルシューティング

移行のパフォーマンスを改善するには、どうしたらよいですか?

移行のパフォーマンスを向上させるには、以下の手順を実行します。

1. 複数の一意のユーザー移行ファイルを作成し、各ファイルのユーザー数を制限します。
2. migrateUsers コマンドの複数のインスタンスを同時に実行します。

例えば、150 ユーザーのグループ、ロール、特権、および権限を移行するには、それぞれ 50 ユーザーを含む 3 つのユーザー移行ファイルを作成します。次に、migrateUsers コマンドの 3 つのインスタンスを同時に実行します。コマンドの各インスタンスに対し、一意のユーザー移行ファイルを指定します。

migrateUsers コマンドが失敗します。

migrateUsers コマンドが失敗した場合は、以下のリカバリパスを利用できます。

- もう一度 migrateUsers コマンドを実行する。
- ユーザー移行ファイルを変更する。それから、migrateUsers コマンドを実行する。

もう一度コマンドを実行する場合は、同じユーザー移行ファイルを指定します。このコマンドは、LDAP ユーザーに割り当てられた接続オブジェクト権限を、ネイティブユーザーの接続オブジェクト権限で上書きします。このコマンドは、ネイティブユーザーおよび対応する LDAP ユーザーのグループ、ロール、特権、およびドメインオブジェクト権限をマージします。

ユーザー移行ファイルを変更するには、以下の手順を実行します。

1. migrateUsers コマンドを実行したときに作成された詳細ログファイルを表示します。
2. コマンドでユーザー移行ファイルから正常に移行されたユーザーを削除します。
3. migrateUsers コマンドを実行します。

ユーザーアカウントの特権と権限の確認

Kerberos 認証を有効にする前に、LDAP セキュリティドメイン内のユーザーに、正しいグループ、ロール、特権、および権限があることを確認します。infacmd を使用して、LDAP セキュリティドメイン内のユーザーアカウントのグループ、ロール、特権、および権限を確認することができます。

以下のオブジェクトが正しく移行されたことを確認します。

ユーザーおよびグループ

ユーザーアカウントが属しているグループを特定するには、ユーザーと、関連付けられたグループのリストを取得します。以下のコマンドを実行します。

```
infacmd aud getUserGroupAssociation
```

ロール

ドメインユーザーとグループに関連付けられたロールのリストを取得するには、以下のコマンドを実行します。

```
infacmd aud getUserGroupAssociationForRoles
```

特権

ドメイン内のユーザーとグループに割り当てられた特権のリストを取得するには、以下のコマンドを実行します。

```
infacmd aud getPrivilegeAssociation
```

権限

ドメイン内のユーザーとグループに割り当てられた権限のリストを取得するには、以下のコマンドを実行します。

```
infacmd aud getDomainObjectPermissions
```

フォルダやグローバルオブジェクトの権限

ドメインに PowerCenter リポジトリサービスが含まれる場合は、ユーザーアカウントに割り当てられた PowerCenter のフォルダとグローバルリポジトリオブジェクトに対する権限を確認します。PowerCenter リポジトリには以下のオブジェクトが存在する可能性があります。

- フォルダー
- デプロイメントグループ
- ラベル
- クエリ(Q)
- 接続

Kerberos 認証を使用するようにドメインを設定した後は、ネイティブユーザーアカウントを変更できません。

ネイティブユーザーアカウントのグループ、ロール、特権、および権限が正常に LDAP ユーザーアカウントに移行されたことを確認してから、ネイティブユーザーアカウントを削除します。Administrator ツールを使用

して、ユーザーアカウントを削除します。詳細については、「ネイティブユーザーの削除」 (ページ 115)を参照してください。

手順 3。 Kerberos 設定ファイルの設定

Kerberos では、設定情報を *krb5.conf* という名前のファイルに保存します。Informatica では、Kerberos 設定ファイルの中の特定のプロパティを、Informatica ドメインが Kerberos 認証を正しく使用できるように設定する必要があります。krb5.conf という設定ファイル内のプロパティを設定してから、そのファイルを Informatica ディレクトリにコピーする必要があります。

この設定ファイルには、Kerberos レルムや KDC のアドレスなど Kerberos サーバーについての情報が含まれています。Kerberos 管理者に、この設定ファイルのプロパティを設定してファイルのコピーを送付するよう依頼できます。

1. krb5.conf ファイルをバックアップしてから変更します。
2. krb5.conf ファイルを編集します。
3. *libdefaults* セクションで、Informatica が必要とするプロパティを設定または追加します。

   次の表に、libdefaults セクションにプロパティを設定する必要のある値の一覧を示します。

パラメータ	値
default_realm	Informatica ドメインのサービスレルムの名前。
forwardable	クライアントユーザーの資格情報を他のサービスに委譲できるサービスにします。このパラメータを True に設定します。Informatica ドメインでは、他のサービスに対してクライアントユーザーの資格情報を認証するアプリケーションサービスを必要とします。
default_tkt_enctypes	チケット交付チケット（TGT）内のセッションキーの暗号化タイプ。このパラメータを *rc4-hmac* に設定します。Informatica では、*rc4-hmac* の暗号化タイプのみサポートします。
udp_preference_limit	メッセージを KDC に送信する際に Kerberos が使用するプロトコルを決定します。常に TCP を使用するよう udp_preference_limit = 1 を設定します。Informatica ドメインでは TCP プロトコルのみサポートします。udp_preference_limit を他の値に設定した場合、Informatica ドメインが予期せずシャットダウンすることがあります。

4. *realms* セクションで、コロンで区切られた KDC のアドレス内にポート番号を含めます。

   例えば、KDC アドレスが kerberos.example.com でポート番号が 88 の場合、*kdc* パラメータを以下のように設定します。

   ```
   kdc = kerberos.example.com:88
   ```
5. krb5.conf ファイルを保存します。
6. Informatica ディレクトリに設定ファイルをコピーします。

   krb5.conf は、以下のディレクトリにコピーする必要があります。<INFA_HOME>/services/shared/security ドメインに複数のノードがある場合、ドメイン内のすべてのノードの同じディレクトリに krb5.conf をコピーします。

以下の例は、必要なプロパティが設定された krb5.conf の内容です。

```
[libdefaults]
default_realm = AFNIKRB.AFNIDEV.COM
forwardable = true
default_tkt_enctypes = rc4-hmac
udp_preference_limit = 1

[realms]
AFNIKRB.AFNIDEV.COM = {
  admin_server = SMPLKERDC01.AFNIKRB.AFNIDEV.COM
  kdc = SMPLKERDC01.AFNIKRB.AFNIDEV.COM:88
 }

[domain_realm]
afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
.afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
```

Kerberos 設定ファイルに関する詳細は、Kerberos ネットワーク認証のマニュアルを参照してください。

手順 4。 プリンシパル名とキータブ形式の生成

Informatica ドメインを Kerberos 認証を使用して実行する場合、Kerberos のサービスプリンシパル名（SPN）とキータブファイルを Informatica ドメインのノードとプロセスに関連付ける必要があります。Informatica では、パスワードを要求せずにネットワーク内のサービスを認証するキータブファイルを必要とします。

ドメインのセキュリティ要件に基づいて、サービスプリンシパルレベルを以下のレベルのうちの 1 つに設定できます。

ノードレベル

ドメインがテストまたは開発用に使用されていて、高いレベルのセキュリティを必要としない場合は、サービスプリンシパルをノードレベルに設定できます。ノードとそのノードのすべてのサービスプロセスで 1 つの SPN とキータブファイルを使用できます。また、ノードの HTTP プロセスに個別の SPN とキータブファイルを設定する必要があります。

プロセスレベル

ドメインがプロダクション用として使用されていて、高いレベルのセキュリティを必要とする場合は、サービスプリンシパルをプロセスレベルに設定できます。ノードごととノードのプロセスごとに、一意の SPN とキータブファイルを作成します。また、ノードの HTTP プロセスに個別の SPN とキータブファイルを設定する必要があります。

Informatica ドメインでは、サービスプリンシパル名とキータブファイル名は特定の形式に従う必要があります。サービスプリンシパル名とキータブファイル名の正しい形式に従うには、Informatica Kerberos SPN 形式ジェネレータを使用して、Informatica ドメインで必要な形式のサービスプリンシパル名とキータブファイル名のリストを生成します。

ノードレベルのサービスプリンシパルの要件

Informatica ドメインが高いレベルのセキュリティを必要としない場合は、ノードとサービスプロセスで同じ SPN とキータブファイルを共有できます。ドメインでは、ノード内のサービスプロセスごとの個別の SPN を必要としません。

Informatica ドメインでは、以下のノードレベルのコンポーネントに SPN とキータブファイルを必要とします。

LDAP **ディレクトリサービスのプリンシパル識別名（DN）**

LDAP ディレクトリサービスの検索に使用されるバインドユーザーの DN に関するプリンシパル名。キータブファイルの名前は、infa_ldapuser.keytab である必要があります。

ノードプロセス

認証呼び出しを開始または受け入れる Informatica ノード用のプリンシパル名。同じプリンシパル名が、ノード内のサービスの認証に使用されます。ドメイン内のゲートウェイノードごとに個別のプリンシパル名が必要です。

ドメイン内の HTTP **プロセス**

Informatica Administrator など、Informatica ドメイン内のすべての Web アプリケーションサービスのプリンシパル名。ブラウザではこのプリンシパル名を使用して、ドメイン内のすべての HTTP プロセスに対する認証を行います。キータブファイルの名前は、webapp_http.keytab である必要があります。

プロセスレベルのサービスプリンシパルの要件

Informatica ドメインで高いレベルのセキュリティが必要とされる場合は、ノードごと、およびノード内のサービスごとに、個別の SPN とキータブファイルを作成します。

Informatica ドメインでは、以下のプロセスレベルのコンポーネントに SPN とキータブファイルを必要とします。

LDAP **ディレクトリサービスのプリンシパル識別名（DN）**

LDAP ディレクトリサービスの検索に使用されるバインドユーザーの DN に関するプリンシパル名。キータブファイルの名前は、infa_ldapuser.keytab である必要があります。

ノードプロセス

認証呼び出しを開始または受け入れる Informatica ノード用のプリンシパル名。

Informatica Administrator **サービス**

Informatica ドメイン内の他のサービスに対してサービスを認証する Informatica Administrator サービスのプリンシパル名。キータブファイルの名前は、*_AdminConsole.keytab* にする必要があります。

ドメイン内の HTTP **プロセス**

Informatica Administrator など、Informatica ドメイン内のすべての Web アプリケーションサービスのプリンシパル名。ブラウザではこのプリンシパル名を使用して、ドメイン内のすべての HTTP プロセスに対する認証を行います。キータブファイルの名前は、webapp_http.keytab である必要があります。

サービスプロセス

Informatica ドメイン内のノード上で実行されるアプリケーションサービスのプリンシパル名。アプリケーションサービスごとに一意のサービスプリンシパルとキータブファイル名が必要です。

Windows での Informatica Kerberos SPN Format Generator の実行

Informatica Kerberos SPN Format Generator を実行すると、Informatica ドメインで必要な SPN とキータブファイル名の正しいフォーマットを示すファイルを生成できます。

1. Informatica ノードをホストするマシンで、Informatica ディレクトリ<InformaticaDirectory>/Tools/Kerberos に移動します。
2. SPNFormatGenerator.bat ファイルを実行します。

   Informatica Kerberos SPN フォーマットジェネレータの［**ようこそ**］ページが表示されます。
3. ［**次へ**］をクリックします。

[サービスプリンシパルレベル] ページが表示されます。

4. ドメインの Kerberos サービスプリンシパルに設定するレベルを選択します。

   次の表に選択可能なレベルを示します。

レベル	説明
プロセスレベル	ノードごと、およびノードのアプリケーションサービスごとに一意のサービスプリンシパル名（SPN）とキータブファイルを使用するようにドメインを設定します。 ノードごとに必要になる SPN とキータブファイルの数は、ノードで実行されるアプリケーションサービスプロセスの数により変わります。本番ドメインなど、高レベルなセキュリティが必要なドメインには、プロセスレベルオプションを使用します。
ノードレベル	ノードの SPN とキータブファイルを共有するようにドメインを設定します。 このオプションを利用するには、ノードとそのノードで実行されているすべてのアプリケーションサービスで 1 つの SPN とキータブファイルが必要になります。また、ノードのすべての HTTP プロセスに個別の SPN とキータブファイルが必要になります。 テストドメインや開発ドメインなど、高レベルなセキュリティを必要としないドメインには、ノードレベルオプションを使用します。

5. **[次へ]** をクリックします。

   「認証パラメータ - Kerberos 認証」 ページが表示されます。

6. SPN フォーマットを生成するためにドメインパラメータとノードパラメータを入力します。

   次の表に、指定する必要のあるパラメータを示します。

プロンプト	説明
ドメイン名	ドメインの名前。名前は 128 文字以下で、7 ビットの ASCII 文字のみにする必要があります。スペースまたは次のいずれかの文字は使用できません: ` % * + ; " ? , < > \ /
ノード名	Informatica ノードの名前。
ノードのホスト名	ノード作成先のマシンの完全修飾ホスト名または IP アドレス。ノードのホスト名には、アンダースコア（_）文字を使用できません。 **注**: *localhost* は使用しないでください。ホスト名はマシンを明示的に示す必要があります。
サービスレルム名	Informatica ドメインサービスの Kerberos 領域の名前。レルム名は大文字にする必要があります。

   サービスプリンシパルレベルをノードレベルに設定すると、**[+ノード]** ボタンが表示されます。サービスプリンシパルレベルをプロセスレベルに設定すると、**[+ノード]** ボタンと **[+サービス]** ボタンが表示されます。

7. 追加ノードの SPN フォーマットを生成するには、**[+ノード]** をクリックし、ノード名とホスト名を指定します。

   1 つのドメインに複数のノードを入力できます。

8. サービスの SPN フォーマットを生成するには、**[+サービス]** をクリックし、**[ノード上のサービス]** フィールドにサービス名を指定します。

   [ノード上のサービス] フィールドは、サービスプリンシパルをプロセスレベルに設定して **[+サービス]** をクリックした場合のみ表示されます。1 つのノードに対して複数のサービスを入力できます。サービスは、そのサービスが実行されるノードのすぐ下に表示されます。

9. ノードをリストから削除するには、**[-ノード]** をクリックします。

   Informatica SPN Format Generator でノードが削除されます。そのノードにサービスが追加されていた場合は、ノードとともにそれらのサービスも削除されます。

10. ノードからサービスを削除するには、サービス名フィールドをクリアします。
11. **[次へ]** をクリックします。

    SPN Format Generator には、サービスプリンシパルとキータブファイル名のリストが含まれるファイルのパスとファイル名が表示されます。

12. **[完了]** をクリックして SPN Format Generator を終了します。

SPN 形式ジェネレータは、Informatica ドメインで必要な形式の SPN およびキータブファイル名を含むテキストファイルを生成します。

UNIX での Informatica Kerberos SPN Format Generator の実行

Informatica Kerberos SPN Format Generator を実行すると、Informatica ドメインで必要な SPN とキータブファイル名の正しいフォーマットを示すファイルを生成できます。

1. Informatica ノードをホストするマシンで、Informatica ディレクトリ<InformaticaDirectory>/Tools/Kerberos に移動します。
2. シェルコマンドラインで、SPNFormatGenerator.sh ファイルを実行します。
3. **Enter** キーを押して続行します。
4. **Service Principal Level** セクションで、ドメインの Kerberos サービスプリンシパルに設定するレベルを選択します。

   次の表に選択可能なレベルを示します。

レベル	説明
1->Process Level	ノードごと、およびノードのアプリケーションサービスごとに一意のサービスプリンシパル名（SPN）とキータブファイルを使用するようにドメインを設定します。 ノードごとに必要になる SPN とキータブファイルの数は、ノードで実行されるアプリケーションサービスプロセスの数により変わります。本番ドメインなど、高レベルなセキュリティが必要なドメインには、プロセスレベルオプションを使用します。
2->Node Level	ノードの SPN とキータブファイルを共有するようにドメインを設定します。 このオプションを利用するには、ノードとそのノードで実行されているすべてのアプリケーションサービスで 1 つの SPN とキータブファイルが必要になります。また、ノードのすべての HTTP プロセスに個別の SPN とキータブファイルが必要になります。 テストドメインや開発ドメインなど、高レベルなセキュリティを必要としないドメインには、ノードレベルオプションを使用します。

5. SPN フォーマットの生成に必要なドメインパラメータとノードパラメータを入力します。

   次の表に、指定する必要のあるパラメータを示します。

プロンプト	説明
ドメイン名	ドメインの名前。名前は 128 文字以下で、7 ビットの ASCII 文字のみにする必要があります。スペースまたは次のいずれかの文字は使用できません: ` % * + ; " ? , < > \ /
ノード名	Informatica ノードの名前。
ノードのホスト名	ノード作成先のマシンの完全修飾ホスト名または IP アドレス。ノードのホスト名には、アンダースコア（_）文字を使用できません。 **注:** *localhost* は使用しないでください。ホスト名はマシンを明示的に示す必要があります。
サービスレルム名	Informatica ドメインサービスの Kerberos 領域の名前。レルム名は大文字にする必要があります。

   サービスプリンシパルをノードレベルに設定すると、**[ノードを追加しますか?]** というプロンプトが表示されます。サービスプリンシパルをプロセスレベルに設定すると、**[サービスを追加しますか?]** というプロンプトが表示されます。

6. **[ノードを追加しますか?]** プロンプトで「1」と入力して、追加ノードの SPN フォーマットを生成します。次に、ノード名とノードホスト名を入力します。

   複数ノードの SPN フォーマットを生成するには、**[ノードを追加しますか?]** の各プロンプトで「1」と入力し、ノード名とノードホスト名を入力します。

7. **[サービスを追加しますか?]** プロンプトで「1」と入力して、前のノード上で実行されるサービスの SPN フォーマットを生成します。次にサービス名を入力します。

   複数サービスの SPN フォーマットを生成するには、**[サービスを追加しますか?]** の各プロンプトで「1」と入力し、サービス名を入力します。

8. 「2」を入力して、**[サービスを追加しますか?]** または **[ノードを追加しますか?]** プロンプトを終了します。

   SPN Format Generator には、サービスプリンシパルとキータブファイル名のリストが含まれるファイルのパスとファイル名が表示されます。

9. Enter キーを押して SPN Format Generator を終了します。

SPN 形式ジェネレータは、Informatica ドメインで必要な形式の SPN およびキータブファイル名を含むテキストファイルを生成します。

手順 5。SPN とキータブ形式のテキストファイルの確認

Kerberos SPN Format Generator で、Informatica ドメインで必要なサービスプリンシパル名とキータブファイル名のフォーマットを一覧表示する SPNKeytabFormat.txt というテキストファイルを生成します。このリストには、選択したサービスプリンシパルレベルに基づく SPN とキータブファイル名が含まれます。

このテキストファイルを確認し、エラーメッセージがないことを確認してください。

このテキストファイルには以下の情報が含まれます。

エンティティ名

プロセスに関連付けられたノードまたはサービスを特定します。

SPN

Kerberos プリンシパルデータベース内の SPN のフォーマット。SPN では大文字小文字が区別されます。各 SPN タイプのフォーマットは異なります。

SPN のフォーマットは以下のいずれかになります。

キータブのタイプ	SPN フォーマット
NODE_SPN	isp/<*NodeName*>/<*DomainName*>@<*REALMNAME*>
NODE_AC_SPN	_AdminConsole/<*NodeName*>/<*DomainName*>@<*REALMNAME*>
NODE_HTTP_SPN	HTTP/<*NodeHostName*>@<*REALMNAME*> **注:** Kerberos SPN Format Generator によりノードホスト名が検証されます。ノードホスト名が有効でない場合、SPN は生成されません。その代わりに、「ホスト名を解決できません。」というメッセージが表示されます。
SERVICE_PROCESS_SPN	<*ServiceName*>/<*NodeName*>/<*DomainName*>@<*REALMNAME*>

キータブファイル名

Kerberos プリンシパルデータベース内で、関連する SPN 用に作成されるキータブファイルの名前のフォーマット。キータブファイル名では大文字小文字が区別されます。

キータブファイル名は以下のフォーマットに従います。

キータブのタイプ	キータブファイル名
NODE_SPN	<*NodeName*>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<*ServiceName*>.keytab

キータブのタイプ

キータブのタイプ。キータブのタイプは以下のいずれかになります。

- NODE_SPN.ノードプロセスのキータブファイル。
- NODE_AC_SPN.Informatica Administrator サービスのプロセスのキータブファイル。
- NODE_HTTP_SPN.ノード内の HTTP プロセスのキータブファイル。
- SERVICE_PROCESS_SPN.サービスプロセスのキータブファイル。

ノードレベルのサービスプリンシパル

以下の例は、ノードレベルのサービスプリンシパル用に生成される SPNKeytabFormat.txt ファイルの内容を示しています。

```
ENTITY_NAME   SPN                                    KEY_TAB_NAME          KEY_TAB_TYPE
Node01        isp/Node01/InfaDomain@MY.SVCREALM.COM  Node01.keytab         NODE_SPN
```

```
Node01        HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM     webapp_http.keytab    NODE_HTTP_SPN
Node02        isp/Node02/InfaDomain@MY.SVCREALM.COM              Node02.keytab         NODE_SPN
Node02        HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM     webapp_http.keytab    NODE_HTTP_SPN
Node03        isp/Node03/InfaDomain@MY.SVCREALM.COM              Node03.keytab         NODE_SPN
Node03        HTTP/NodeHost03.enterprise.com@MY.SVCREALM.COM     webapp_http.keytab    NODE_HTTP_SPN
```

プロセスレベルのサービスプリンシパル

以下の例は、プロセスレベルのサービスプリンシパル用に生成される SPNKeytabFormat.txt ファイルの内容を示しています。

```
ENTITY_NAME        SPN                                                KEY_TAB_NAME           KEY_TAB_TYPE
Node01             isp/Node01/InfaDomain@MY.SVCREALM.COM              Node01.keytab          NODE_SPN
Node01             _AdminConsole/Node01/InfaDomain@MY.SVCREALM.COM    _AdminConsole.keytab   NODE_AC_SPN
Node01             HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM     webapp_http.keytab     NODE_HTTP_SPN
Node02             isp/Node02/InfaDomain@MY.SVCREALM.COM              Node02.keytab          NODE_SPN
Node02             _AdminConsole/Node02/InfaDomain@MY.SVCREALM.COM    _AdminConsole.keytab   NODE_AC_SPN
Node02             HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM     webapp_http.keytab     NODE_HTTP_SPN
Service10:Node01   Service10/Node01/InfaDomain@MY.SVCREALM.COM        Service10.keytab
SERVICE_PROCESS_SPN
Service100:Node02  Service100/Node02/InfaDomain@MY.SVCREALM.COM       Service100.keytab
SERVICE_PROCESS_SPN
Service200:Node02  Service200/Node02/InfaDomain@MY.SVCREALM.COM       Service200.keytab
SERVICE_PROCESS_SPN
```

手順 6。 サービスプリンシパル名およびキータブファイルの作成

Informatica で要求されるフォーマットの SPN とキータブファイル名のリストを生成した後、Kerberos 管理者に要求を送信し、Kerberos プリンシパルデータベースに SPN を追加してキータブファイルを作成します。

SPN およびキータブファイルを作成する際は、次のガイドラインを使用します。

ユーザープリンシパル名（UPN**）は** SPN **と同じである必要があります。**

サービスプリンシパルのユーザーアカウントを作成する際は、SPN と同じ名前で UPN を設定する必要があります。Informatica ドメイン内のアプリケーションサービスは、操作に応じて、サービスまたはクライアントとして機能することができます。サービスプリンシパルは、同じ UPN と SPN で識別できるように設定する必要があります。

ユーザーアカウントは、1 つの SPN とのみ関連付けます。1 つのユーザーアカウントに複数の SPN を設定することはできません。

Microsoft Active Directory **で委任を有効化します。**

Informatica ドメインでサービスプリンシパルが使用されているすべてのユーザーアカウントで、委任を有効化する必要があります。Microsoft Active Directory サービスで、SPN を設定した各ユーザーアカウントに **［このユーザーを信用して任意のサービスを委任する（Kerberos のみ）］** オプションを設定します。

委任認証が行われるのは、ユーザーが 1 つのサービスで認証され、そのサービスが認証されたユーザーの資格情報を使用して別のサービスに接続する場合です。Informatica ドメイン内のサービスは他のサービスに接続して操作を完了する必要があるため、Informatica ドメインでは Microsoft Active Directory で委任オプションを有効化する必要があります。

例えば、PowerCenter Client が PowerCenter リポジトリサービスに接続する際、クライアントユーザーのアカウントは PowerCenter リポジトリサービスプリンシパルで認証されます。PowerCenter リポジトリサービスが PowerCenter 統合サービスに接続するときに、PowerCenter リポジトリサービスプリンシパルはクライアントユーザーの資格情報を使用して PowerCenter 統合サービスに対する認証を行うこと

ができます。クライアントユーザーのアカウントを PowerCenter 統合サービスでも認証する必要はありません。

ktpass **ユーティリティを使用して、サービスプリンシパルのキータブファイルを作成します。**

Microsoft Active Directory では、キータブファイルを作成するために ktpass ユーティリティが用意されています。Informatica では Microsoft Active Directory でのみ Kerberos 認証をサポートしており、ktpass で作成したキータブファイルのみを認証します。

ノードのキータブファイルは、そのノードをホストするマシンで使用可能である必要があります。デフォルトでは、キータブファイルは下記のディレクトリ<INFA_HOME>/isp/config/keys に格納されます。

Kerberos 管理者からキータブファイルを受け取った際、Informatica ドメインで使用するキータブファイルに指定されたディレクトリに、キータブファイルをコピーします。

サービスプリンシパル名とキータブファイルのトラブルシューティング

Kerberos ユーティリティを使用して、Kerberos 管理者が作成したサービスプリンシパルおよびキータブファイル名が、自分で作成したサービスプリンシパルおよびキータブファイル名に一致することを確認できます。このユーティリティは、Kerberos Key Distribution Center（KDC）のステータスの特定にも使用できます。

setspn、*kinit*、*klist* などの Kerberos ユーティリティは、SPN とキータブファイルの表示と確認に使用できます。これらのユーティリティを使用する場合は、KRB5_CONFIG 環境変数に Kerberos 設定ファイルのパスとファイル名が含まれていることを確認します。

注: 以下の例は、Kerberos ユーティリティを使用して SPN とキータブファイルが有効であることを確認する方法を示しています。この例は、Kerberos 管理者がユーティリティを使用して Informatica ドメインで必要な SPN とキータブファイルを作成する方法とは異なる場合があります。Kerberos ユーティリティの実行の詳細については、Kerberos マニュアルを参照してください。

以下のユーティリティを使用して、SPN とキータブファイルの検証します。

klist

klist を使用して、キータブファイル内の Kerberos プリンシパルとキーを一覧表示できます。キータブファイル内のキーとキータブエントリのタイムスタンプを一覧表示するには、以下のコマンドを実行します。

```
klist -k -t <keytab_file>
```

以下の出力例は、キータブファイル内のプリンシパルを示しています。

```
Keytab name: FILE:int_srvc01.keytab
KVNO Timestamp         Principal
---- ----------------- --------------------------------------------------------
   3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
   3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
   3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
   3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
   3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
```

kinit

kinit を使用して、ユーザーアカウントのチケット交付チケットを要求し、KDC が実行されていてチケットの交付が可能であることを検証できます。ユーザーアカウントのチケット交付チケットを要求するには、以下のコマンドを実行します。

```
kinit <user_account>
```

kinit を使用してチケット交付チケットを要求し、Kerberos 接続の確立に使用可能なキータブファイルであることも検証できます。SPN のチケット交付チケットを要求するには、次のコマンドを実行します。

```
kinit -V -k -t <keytab_file> <SPN>
```

以下の出力の例は、指定されたキータブファイルと SPN のデフォルトキャッシュで作成されたチケット交付チケットを示しています。

```
Using default cache: /tmp/krb5cc_10000073
Using principal: int_srvc01/node01_vMPE/Domn96_vMPE@REALM
Using keytab: int_srvc01.keytab
Authenticated to Kerberos v5
```

setspn

setspn を使用して、Active Directory サービスアカウントの SPN を表示、変更、削除できます。Active Directory サービスをホストするマシンで、コマンドラインウィンドウを開き、コマンドを実行します。

ユーザーアカウントに関連付けられた SPN を表示するには、次のコマンドを実行します。

```
setspn -L <user_account>
```

以下の出力の例は、ユーザーアカウント is96svc に関連付けられた SPN を示しています。

```
Registered ServicePrincipalNames for CN=is96svc,OU=AllSvcAccts,OU=People,
DC=ds,DC=intrac0rp,DC=zec0rp:
       int_srvc01/node02_vMPE/Domn96_vMPE
```

SPN に関連付けられたユーザーアカウントを表示するには、次のコマンドを実行します。

```
setspn -Q <SPN>
```

以下の出力の例は、SPN int_srvc01/node02_vMPE/Domn96_vMPE に関連付けられたユーザーアカウントを示しています。

```
Checking domain DC=ds,DC=intrac0rp,DC=zec0rp
CN=is96svc,OU=AllSvcAccts,OU=People,DC=ds,DC=intrac0rp,DC=zec0rp
        int_srvc01/node02_vMPE/Domn96_vMPE

Existing SPN found!
```

重複 SPN を検索するには、以下のコマンドを実行します。

```
setspn -X
```

以下の出力の例は、1 つの SPN に関連付けられた複数のユーザーアカウントを示しています。

```
Checking domain DC=ds,DC=intrac0rp,DC=zec0rp
Processing entry 1125
HOST/mtb01.REALM is registered on these accounts:
        CN=Team1svc,OU=AllSvcAccts,OU=People,DC=ds,DC=intrac0rp,DC=zec0rp
        CN=MTB1svc,OU=IIS,OU=WPC960K3,OU=WINServers,DC=ds,DC=intrac0rp,DC=zec0rp
```

注: 重複 SPN の検索に長い時間がかかり、大量のメモリを使用する可能性があります。

kdestroy

kdestroy を使用して、アクティブな Kerberos 承認チケットと、チケットが含まれるユーザークレデンシャルのキャッシュを削除できます。パラメータを指定せずに *kdestroy* を実行した場合、デフォルトのクレデンシャルのキャッシュが削除されます。

手順 7。 ドメインに対して Kerberos 認証を設定します。

infasetup を実行して、Informatica ドメインの認証を Kerberos ネットワーク認証に変更します。

注: ドメインを Kerberos 認証を使用するよう設定する前に、すべてのリポジトリオブジェクトがチェックインされていることを確認します。

ドメイン認証を変更する infasetup コマンドを実行すると、コマンドで以下の LDAP セキュリティドメインが作成されます。

- 内部セキュリティドメイン。内部セキュリティドメインは、*_infaInternalNamespace* という名前を持つ LDAP セキュリティドメインです。_infaInternalNamespace セキュリティドメインには、Kerberos 認証の設定時に作成されるデフォルト管理者のユーザーアカウントが含まれます。Kerberos 認証の設定後は、_infaInternalNamespace セキュリティドメインにユーザーを追加することも、このセキュリティドメインを削除することもできません。
- ユーザーレルムのセキュリティドメイン。ユーザーレルムセキュリティドメインは、Kerberos ユーザーレルムと同じ名前を持つ空の LDAP セキュリティドメインです。Kerberos 認証の設定後は、Kerberos プリンシパルデータベースからユーザーレルムセキュリティドメインにユーザーをインポートできます。

infasetup コマンドで管理者ユーティリティアカウントも作成されます。管理者ユーザーのユーザー名を指定します。Kerberos 認証を設定した後、_infaInternalNamespace セキュリティドメインには管理者ユーザーアカウントが含まれています。

Kerberos 認証を使用するようにドメインを設定するには、以下のコマンドを実行します。

```
infasetup switchToKerberosMode
```

1. ゲートウェイノードで、infasetup コマンドを実行してドメインの認証を変更します。

   コマンドプロンプトで、Informatica コマンドラインプログラムがあるディレクトリに移動します。デフォルトでは、コマンドラインプログラムは<InformaticaInstallationDir>/isp/bin ディレクトリにインストールされています。
2. 必要なオプションと引数を指定して infasetup コマンドを実行します。

   以下のコマンドを入力します。

   - Windows: `infasetup switchToKerberosMode`
   - UNIX: `infasetup.sh switchToKerberosMode`

   次の表で、switchToKerberosMode コマンドのオプションについて説明します。

オプション	引数	説明
-administratorName -ad	administrator_name	Kerberos 認証の設定時に作成されるドメイン管理者のアカウントのユーザー名。このユーザーアカウントは Kerberos プリンシパルデータベースに存在する必要があります。 Kerberos 認証を設定した後、このユーザーは *_infaInternalNamespace* セキュリティドメインに含まれています。
-ServiceRealmName -srn	realm _name_of_node_spn	Informatica ドメインサービスが属する Kerberos 領域の名前。レルム名は、大文字小文字が区別され、すべて大文字にする必要があります。 サービスレルム名とユーザーレルム名は同じでなければなりません。

オプション	引数	説明
-UserRealmName -urn	realm _name_of_user_spn	Informatica ドメインユーザーが属する Kerberos 領域の名前。レルム名は、大文字小文字が区別され、すべて大文字にする必要があります。 サービスレルム名とユーザーレルム名は同じでなければなりません。
-SPNShareLevel -spnSL	PROCESS |NODE	ドメインのサービスプリンシパルレベル。このプロパティを以下のいずれかに設定します。 - プロセス。ドメインでは、ノードごと、およびノードのサービスごとに、一意のサービスプリンシパル名（SPN）とキータブファイルを必要とします。ノードごとに必要になる SPN とキータブファイルの数は、ノードで実行されるサービスプロセスの数により変わります。プロダクションドメインなどのドメインが高いレベルのセキュリティを必要とする場合は、プロセスレベルオプションを使用します。 - ノード。ドメインでは、ノードとそのノードで実行されているすべてのサービスで 1 つの SPN とキータブファイルを使用しています。また、ノードのすべての HTTP プロセスに個別の SPN とキータブファイルが必要になります。テストドメインや開発ドメインなどのドメインが高いレベルのセキュリティを必要としない場合は、ノードレベルのオプションを使用してください。 デフォルトは PROCESS です。

switchToKerberosMode コマンドによって、ドメインの認証モードがネイティブまたは LDAP のユーザー認証から Kerberos ネットワーク認証に変わります。

手順 8。ドメイン内のノードの更新

infasetup コマンドを実行して、Kerberos 認証サーバー情報でドメイン内の他のすべてのノードを更新します。

Kerberos 認証サーバー情報を使用して、switchToKerberosMode コマンドを実行したゲートウェイノードを除くすべてのゲートウェイノードと作業ノードを更新します。

ゲートウェイノードと作業ノードを更新するには、次のコマンドを使用します。
infasetup UpdateGatewayNode

UpdateGatewayNode コマンドを使用して、ドメイン内のゲートウェイノードの Kerberos 認証パラメータを設定します。ドメインに複数のゲートウェイノードがある場合、各ゲートウェイノードに対して UpdateGatewayNode コマンドを実行します。

infasetup UpdateWorkerNode

UpdateWorkerNode コマンドを使用して、ドメイン内の作業ノードの Kerberos 認証パラメータを設定します。ドメインに複数の作業ノードがある場合、各作業ノードに対して UpdateWorkerNode コマンドを実行します。

1. Informatica ノードをホストするマシンで、infasetup コマンドを実行してノードを更新します。

   コマンドプロンプトで、Informatica コマンドラインプログラムがあるディレクトリに移動します。デフォルトでは、コマンドラインプログラムは<InformaticaInstallationDir>/isp/bin ディレクトリにインストールされています。

2. 必要なオプションと引数を指定して infasetup を実行します。

   以下のコマンドを入力します。

   - Windows: infasetup UpdateGatewayNode または infasetup UpdateWorkerNode
   - UNIX: infasetup.sh UpdateGatewayNode または infasetup.sh UpdateWorkerNode

   以下のテーブルで、ノードの Kerberos 認証情報を更新するオプションについて説明します。

オプション	引数	説明
-EnableKerberos -krb	enable_kerberos	Kerberos 認証を利用するように Informatica ドメインを設定します。
-ServiceRealmName -srn	realm _name_of_node_spn	Informatica ドメインサービスが属する Kerberos 領域の名前。レルム名は、大文字小文字が区別され、すべて大文字にする必要があります。 サービスレルム名とユーザーレルム名は同じでなければなりません。
-UserRealmName -urn	realm _name_of_user_spn	Informatica ドメインユーザーが属する Kerberos 領域の名前。レルム名は、大文字小文字が区別され、すべて大文字にする必要があります。 サービスレルム名とユーザーレルム名は同じでなければなりません。

手順 9。クライアントマシンの更新

Informatica クライアントをホストするマシンに Kerberos 設定ファイルをコピーし、環境変数を設定します。また、ブラウザが Informatica Web アプリケーションにアクセスするように設定することも必要です。

Kerberos 認証で実行するように Informatica ドメインを設定した後、Informatica クライアントツールで以下のタスクを実行します。

Kerberos **設定ファイルをクライアントマシンにコピーします。**

設定ファイルを、Informatica クライアントをホストする各マシンにコピーします。krb5.conf ファイルをディレクトリ<Informatica Client Directory>/shared/security にコピーする必要があります。

Kerberos **設定ファイルに** KRB5_CONFIG **環境変数を設定します。**

KRB5_CONFIG 環境変数を使用して Kerberos 設定ファイル krb5.conf のパスとファイル名を格納します。Informatica クライアントをホストする各マシンに対して、KRB5_CONFIG 環境変数を設定する必要があります。

Web **ブラウザを設定します。**

Informatica ドメインが Kerberos 認証を使ったネットワーク上で実行されている場合、ブラウザを Informatica の Web アプリケーションにアクセスできるように設定する必要があります。Microsoft Internet Explorer と Google Chrome で、Informatica Web アプリケーションの URL を信頼できるサイトのリストに追加します。Chrome 41 以降を使用している場合は、AuthServerWhitelist ポリシーと AuthNegotiateDelegateWhitelist ポリシーも設定する必要があります。

UNIX **で、シングルサインオン用の資格情報キャッシュファイルを作成します。**

UNIX 上でシングルサインオンを使用して Informatica コマンドラインプログラムを実行するには、資格情報キャッシュファイルを生成して、Kerberos ネットワークでコマンドを実行するユーザーアカウントを認証する必要があります。資格情報キャッシュファイルを生成するには、MIT Kerberos から *kinit* ユーティリティを使用します。資格情報キャッシュファイルにより、ユーザーはユーザー名およびパスワードオプションを使用しなくてもコマンドを実行できます。

資格情報キャッシュファイルを使用する場合は、KRB5CCNAME 環境変数で資格情報キャッシュのデフォルトのパスとファイル名を設定する必要があります。

UNIX 上でシングルサインオンを使用して Informatica コマンドラインプログラムを実行する方法の詳細については、『*Informatica コマンドリファレンス*』を参照してください。

手順 10。Informatica ドメインの起動

Kerberos 認証を使用するように Informatica ドメインを設定したあと、ドメインと Administrator ツールを起動します。

1. Windows では、［コントロールパネル］または［スタート］メニューから Informatica Services の起動を行います。

   Informatica を Windows の［スタート］メニューから起動するには、**［プログラム］** > **［Informatica [バージョン]］** > **［サーバー］**をクリックします。**［Informatica サービスを開始］**をクリックし、**［管理者として実行］**を選択します。

   UNIX では、次のコマンドを実行して Informatica デーモンを起動します。

   ```
   infaservice.sh startup
   ```

   デフォルトで、infaservice.sh は次のディレクトリにインストールされます。<INFA_HOME>/tomcat/bin

2. Informatica Administrator を起動します。

   Administrator ツールを起動するには、URL http://<fully qualified hostname>:<http port>を使用します。Administrator ツールで安全な接続を使用するよう設定した場合は、HTTPS プロトコルを使用します。https://<fully qualified hostname>:<http port>

   Administrator ツールを起動したら、ブラウザの信頼済みサイトのリストにこの URL を追加してください。

3. ユーザーアカウントのセキュリティドメインを選択します。

   Kerberos 認証を使用する場合、ネットワークはシングルサインオンを使用します。ユーザー名とパスワードを使って Administrator ツールにログインする必要はありません。

Kerberos 認証の設定後

ドメインのサービスプリンシパルレベルがプロセスレベルの場合、ドメインには、ドメインで作成するすべてのサービスに対して SPN とキータブファイルが必要です。サービスを有効にする前に、そのサービスで SPN とキータブファイルが使用できることを確認します。そのサービスのためのキータブファイルが Informatica ディレクトリに用意されていない場合、Kerberos でアプリケーションサービスを認証できません。

ドメイン上に作成する予定のアプリケーションサービスで SPN とキータブファイルが使用できない場合は、サービスを有効にする前に SPN とキータブファイルを作成する必要があります。Informatica Kerberos SPN Format Generator を使用して、サービスの SPN とキータブファイル名のフォーマットを生成できます。時間の節約のため、作成するサービスの名前と、実行が行われるノードを決めます。次にユーティリティを実行して、すべてのサービスの SPN とキータブファイル名のフォーマットを一度に生成します。

Informatica Kerberos SPN Format Generator の実行の詳細については、「手順 4。 プリンシパル名とキータブ形式の生成」 (ページ 36)」を参照してください。

Kerberos 管理者に、SPN をプリンシパルデータベースに追加して対応するキータブファイルを作成するリクエストを送信します。

Kerberos 管理者からキータブファイルを受信する際に、キータブファイルに指定されているディレクトリにファイルをコピーします。デフォルトでは、キータブファイルは下記のディレクトリ<INFA_HOME>/isp/config/keys に格納されます。

ドメインのサービスプリンシパルがノードレベルである場合は、追加の SPN とキータブファイルを作成せずにアプリケーションサービスを作成して有効化できます。

カスタム Kerberos ライブラリ

Informatica で使用されるデフォルトの Kerberos ライブラリの代わりに、カスタム Kerberos ライブラリを使用するように Informatica ドメイン内でカスタムまたはネイティブのデータベースクライアントおよび Informatica プロセスを設定できます。

次のようなシナリオでは、カスタム Kerberos ライブラリを使用する必要がある場合があります。

Kerberos **を使用するように設定されていない** Informatica **ドメインでカスタム** Kerberos **ライブラリを使用する。**

このシナリオでは、データベースクライアントはマッピングで使用されるソースまたはターゲットデータベースに接続します。データベースは認証用にカスタム Kerberos ライブラリを使用するように設定されています。ただし、Informatica ドメインは Kerberos 認証を使用するように設定されていません。

データベースクライアントが Informatica 経由でデータベースに接続できるように、カスタムライブラリをデータベースクライアントで使用できるようにできます。ただし、Informatica ドメインプロセスは認証にカスタム Kerberos ライブラリを使用しません。

Kerberos **保護された** Informatica **ドメインでカスタム** Kerberos **ライブラリを使用する。**

このシナリオでは、データベースクライアントはカスタム Kerberos ライブラリを使用するように設定されたソースまたはターゲットデータベースに接続します。ただし、Informatica ドメインは認証にデフォルトの Informatica Kerberos ライブラリを使用するように設定されています。

データベースクライアントが Informatica 経由でデータベースに接続できるようにするために、デフォルトの Informatica Kerberos ライブラリの代わりにカスタム Kerberos ライブラリをロードするように Informatica ドメインを設定できます。すべての Informatica ドメインプロセスおよびサブプロセスでカスタム Kerberos ライブラリを使用します。

必要に応じて、カスタム Kerberos ライブラリへのリンケージを削除し、ドメイン内のノードを更新してデフォルトの Informatica Kerberos ライブラリを使用するように戻すことができます。

カスタム Kerberos ライブラリの使用

infasetup updateMitKerberosLinkage コマンドを使用して、Informatica ドメイン内のデータベースクライアントおよびアプリケーションサーバーがカスタム Kerberos ライブラリを使用するように設定します。

使用する Kerberos ライブラリが含まれるディレクトリを指定する必要があります。ライブラリを各ノードにコピーすることも、ドメイン内のすべてのノードからアクセスできる共有の場所にコピーすることもできます。

Informatica ドメインで Kerberos 認証を使用する場合、使用するカスタム Kerberos ライブラリのバージョンが、Informatica によってデフォルトで使用される Kerberos ライブラリと同じであることを確認します。

1. カスタム Kerberos ライブラリを Informatica ドメイン内のすべてのノードからアクセスできる場所に配置します。
2. ドメインをシャットダウンします。
3. ドメイン内の各ノードに対して infasetup updateMitKerberosLinkage コマンドを実行します。

以下の表に、infasetup updateMitKerberosLinkage コマンドのオプションと引数を示します。

オプション	引数	説明
-useKeberos -krb	true|false	必須。Informatica ドメインで Kerberos 認証を使用する場合は、この値を true に設定します。true の場合、Informatica プロセスによって、デフォルトの Kerberos ライブラリまたは-mkd オプションで指定されたディレクトリ内のライブラリに対する Kerberos 呼び出しが実行されます。 Informatica ドメインで Kerberos 認証を使用しない場合、この値を false に設定します。false の場合、Informatica ドメインで Kerberos ライブラリがロードされません。データベースクライアントによって、-mkd オプションで指定されたディレクトリ内で指定されたカスタムライブラリに対する Kerberos 呼び出しが実行されます。
-mitKerberosDirectory -mkd	kerberos_library_directory_node_spn	オプション。カスタム Kerberos ライブラリが含まれるディレクトリ。ディレクトリには、ライブラリファイルが含まれている必要があります。シンボリックリンクは使用できません。 -krb オプションが true の場合、使用するカスタム Kerberos ライブラリのバージョンが、Informatica によってデフォルトで使用される Kerberos ライブラリと同じであることを確認します。 同じライブラリにバージョンが複数ある場合は、すべてのバージョンのサイズとチェックサムが同じである必要があります。例えば、ディレクトリに libkr5.so.3 と libkrb5.so など、2 つのバージョンの libkrb5 が含まれる場合、両方のライブラリのファイルサイズおよびチェックサム値が同じである必要があります。 指定されたディレクトリが空の場合、コマンドによって Informatica ドメインからカスタム Kerberos ライブラリがすべて削除されます。 -krb オプションが true であってもライブラリのディレクトリを指定しない場合は、Informatica によってデフォルトの Kerberos ライブラリが使用されます。

4. すべてのノードでこのコマンドを実行した後にドメインを再起動します。

デフォルトの Kerberos ライブラリに戻す

Informatica ドメインのノードで infasetup restoreMitKerberosLinkage コマンドを実行し、Informatica によって使用されるデフォルトの Kerberos ライブラリへのリンケージをリストアします。このコマンドにより、Informatica ドメイン内に存在するカスタム Kerberos ライブラリへのリンケージがすべて削除されます。

1. ドメインをシャットダウンします。
2. ドメイン内の各ノードに対して infasetup restoreMitKerberosLinkage コマンドを実行します。

   このコマンドでは、オプションや引数は使用しません。
3. すべてのノードでこのコマンドを実行した後にドメインを再起動します。

第 5 章

ドメインセキュリティ

この章では、以下の項目について説明します。

ドメインセキュリティの概要

Informatica ドメイン内のオプションを有効にして、ドメイン内のコンポーネント間やドメインとクライアントコンポーネント間に安全な通信を設定することができます。

有効にするオプションを変えて、ドメイン内の特定コンポーネントを保護することもできます。必ずしもすべてのコンポーネントを保護する必要はありません。例えば、ドメイン内のサービス間の通信を保護し、モデルリポジトリサービスとリポジトリデータベースの間の通信は保護しないことにしてもかまいません。

Informatica では、ドメイン内のコンポーネント間の通信プロトコルとして TCP/IP および HTTP を使用しています。ドメインでは、コンポーネント間の通信を保護するために SSL 証明書を使用しています。

Informatica サービスをインストールするときに、ドメイン内のサービスおよび Administrator ツールに対して安全な通信を有効にすることができます。インストール後は、Administrator ツールまたはコマンドラインから、ドメインの安全な通信を設定することができます。

インストール中には、ドメイン内に保存される機密データ（パスワードなど）を暗号化するための暗号化キーをインストーラが生成します。インストーラが暗号化キーの生成に使用するキーワードを、ユーザーが提供することができます。機密データの暗号化キーは、インストール後に変更することができます。暗号化されたデータを更新するには、リポジトリの内容をアップグレードする必要があります。

安全な通信を有効にできる範囲は、次のとおりです。

ドメイン

ドメイン内では、次のコンポーネントに対して安全な通信を有効にするオプションを選択することができます。

- サービスマネージャ、ドメイン内のサービス、および Informatica のクライアントツールとの間。
- ドメインとドメイン環境設定リポジトリの間

- リポジトリとリポジトリデータベースの間
- PowerCenter 統合サービスと DTM プロセスの間

Web **アプリケーションサービス**

アナリストサービスなどの Web アプリケーションサービスとブラウザの間の接続を保護することができます。

ソースおよびターゲット

データ統合サービスおよび PowerCenter 統合サービスと、ソースおよびターゲットのデータベースとの間の安全な通信を有効にすることができます。

データストレージ

Informatica では、ドメイン内にデータを保存するときに、パスワードなどの機密データを暗号化します。Informatica の暗号化キーは、インストール中にユーザーが指定するキーワードに基づいて生成されます。Informatica では、この暗号化キーを使って、ドメイン内に保存される機密データの暗号化および暗号解読を行います。

ドメイン内の通信の保護

［安全な通信］オプションを使用することで、サービス間の接続、およびサービスとドメイン内のサービスマネージャの間の接続を保護することができます。さらに、ワークフローのセキュリティを有効にしてドメイン内に作成するリポジトリにセキュアデータベースを使用することができます。

ドメインを保護した後で、Informatica クライアントアプリケーションをセキュアなドメインと連携するように設定します。

サービスやサービスマネージャに対する安全な通信

ドメイン内の安全な通信はインストール中に設定することができます。インストール後は、Administrator ツールまたはコマンドラインから、ドメインに安全な通信を設定することができます。

Informatica は、ユーザーがドメインの保護に使用できる SSL 証明書を提供します。ただし、プロダクション環境などのより高いレベルのセキュリティが求められるドメインには、カスタム SSL 証明書を提供する必要があります。使用する SSL 証明書の入ったキーストアファイルおよびトラストストアファイルを指定します。

注: Informatica では評価目的での SSL 証明書を提供しています。SSL 証明書の指定がない場合、Informatica では、インストールされたすべての Informatica で同じデフォルトのプライベートキーが使用されます。使用しているドメインのセキュリティが危険にさらされる可能性があります。ドメインに対して高度なセキュリティを確保するために、SSL 証明書を提供してください。提供する証明書は、自己署名したものでも、認証機関（CA）からのものでもかまいません。

ドメインに安全な通信を設定する場合は、次のコンポーネント間の接続を保護します。

- サービスマネージャと、ドメインで実行中のすべてのサービス
- データ統合サービスとモデルリポジトリサービス
- データ統合サービスとワークフロー処理
- PowerCenter 統合サービスと PowerCenter リポジトリサービス
- ドメインのサービスと Informatica クライアントツールおよびコマンドラインプログラム

ドメイン内のセキュアな通信の要件

ドメイン内のセキュアな通信を有効にする前に、次の要件が満たされていることを確認します。

証明書署名要求（CSR）および非公開キーを作成しました。

CSR および非公開キーを作成するにはキーツールまたは OpenSSL を使用できます。

RSA 暗号化を使用する場合、512 ビットを超える暗号化にする必要があります。

署名された SSL 証明書があります。

証明書には、自己署名証明書または CA によって署名された証明書があります。CA によって署名された証明書をお勧めします。

証明書をキーストアにインポートしました。

infa_keystore.pem という名前の PEM 形式のキーストアと、infa_keystore.jks という名前の JKS 形式のキーストアが必要です。

注: JKS 形式のキーストアのパスワードは、SSL 証明書の生成に使用された非公開キーのパスフレーズと同じである必要があります。

証明書をトラストストアにインポートしました。

infa_keystore.pem という名前の PEM 形式のトラストストアと、infa_keystore.jks という名前の JKS 形式のキーストアが必要です。

キーストアとトラストストアは正しいディレクトリにあります。

インストール中にセキュアな通信を有効にする場合、キーストアとトラストストアは、インストーラからアクセスできるディレクトリ内にある必要があります。

インストール後にセキュアな通信を有効にする場合、キーストアとトラストストアは、コマンドラインプログラムからアクセスできるディレクトリ内にある必要があります。

カスタムキーストアおよびトラストストアの作成方法の詳細は、 Informatica How-To Library の記事『How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain』（https://kb.informatica.com/h2l/HowTo%20Library/1/0700-CreateKeystoresAndTruststores-H2L.pdf）を参照してください。

ドメインを保護した後で、Informatica クライアントアプリケーションをセキュアなドメインと連携するように設定します。

コマンドラインでのドメインの安全な通信の有効化

infacmd コマンドと infasetup コマンドを使用してドメインに対する安全な通信を有効にします。安全な通信を有効にした後で、変更を有効にするためにドメインを再起動する必要があります。

SSL 証明書ファイルを使用するには、infasetup コマンドを実行するときにキーストアファイルとトラストストアファイルを指定します。

コマンドラインからセキュアなドメイン通信を設定するには、次のコマンドを実行します。

infacmd isp UpdateDomainOptions

UpdateDomainOptions コマンドを使用して、ドメインに対して安全な通信モードを設定します。

infasetup UpdateGatewayNode

ドメインのゲートウェイノード上のサービスマネージャに対して安全な通信を有効にするには、UpdateGatewayNode コマンドを使用します。ドメインに複数のゲートウェイノードがある場合は、各ゲートウェイノードで UpdateGatewayNode コマンドを実行します。

infasetup UpdateWorkerNode

ドメインの作業ノード上のサービスマネージャに対して安全な通信を有効にするには、UpdateWorkerNode コマンドを使用します。ドメインに複数の作業ノードがある場合は、各作業ノードで UpdateWorkerNode コマンドを実行します。

1. セキュアにすることが必要なドメインが実行中であることを確認します。
2. ドメインを更新します。

   必要なオプションと引数を指定して、以下のコマンドを実行します。

   - Windows: `infacmd isp UpdateDomainOptions`
   - UNIX: `infacmd.sh isp UpdateDomainOptions`

   ドメインに安全な通信を設定するには、infacmd コマンドの実行時に以下のオプションを含めます。

オプション	引数	説明
-DomainOptions -do	option_name=value	ドメインに安全な通信を設定するには、次のオプションを設定します。 TLSMode=True

3. ドメインをシャットダウンする。

   ドメインは、infasetup のコマンドを実行する前にシャットダウンしておく必要があります。
4. 必要なオプションと引数を指定して infasetup を実行します。

   以下のコマンドを入力します。

   - Windows: `infasetup UpdateGatewayNode` または `infasetup UpdateWorkerNode`
   - UNIX: `infasetup.sh UpdateGatewayNode` または `infasetup.sh UpdateWorkerNode`

   ノード上で安全な通信を設定するには、次のオプションを指定してコマンドを実行します。

オプション	引数	説明
-EnableTLS -tls	enable_tls	Informatica ドメインのサービスに安全な通信を設定します。
-NodeKeystore -nk	node_keystore_directory	Informatica からデフォルトの SSL 証明書を使用している場合はオプション。各自の SSL 証明書を使用している場合は必須。キーストアファイルを含めるディレクトリ。Informatica ドメインでは、PEM 形式および Java Keystore（JKS）ファイルの SSL 証明書を必要とします。このディレクトリには PEM および JKS 形式のキーストアファイルが含まれている必要があります。キーストアファイルの名前は、infa_keystore.jks および infa_keystore.pem である必要があります。 複数のノードに対して同じキーストアファイルを使用できます。
-NodeKeystorePass -nkp	node_keystore_password	Informatica からデフォルトの SSL 証明書を使用している場合はオプション。各自の SSL 証明書を使用している場合は必須。infa_keystore.jks ファイルのパスワード。

オプション	引数	説明
-NodeTruststore -nt	node_truststore_directory	Informatica からデフォルトの SSL 証明書を使用している場合はオプション。各自の SSL 証明書を使用している場合は必須。トラストストアファイルが含まれるディレクトリ。Informatica ドメインでは、PEM 形式および Java Keystore (JKS) ファイルの SSL 証明書を必要とします。このディレクトリには PEM および JKS 形式のトラストストアファイルが含まれている必要があります。トラストストアファイルの名前は、infa_truststore.jks および infa_truststore.pem である必要があります。 複数のノードに対して同じトラストストアファイルを使用できます。
-NodeTruststorePass -ntp	node_truststore_password	Informatica からデフォルトの SSL 証明書を使用している場合はオプション。各自の SSL 証明書を使用している場合は必須。infa_truststore.jks ファイルのパスワード。

5. ドメイン内の各ノードに対して infasetup コマンドを実行します。

   ドメインに複数のゲートウェイノードがある場合は、各ゲートウェイノードで infasetup UpdateGatewayNode を実行します。複数の作業ノードがある場合は、各作業ノードで infasetup UpdateWorkerNode を実行します。ドメイン内のすべてのノードに同じキーストアファイルとトラストストアファイルを使用する必要があります。

6. ドメインを再起動します。

ドメイン内のすべてのノードの更新が完了した後、Informatica クライアントツールをホストするマシンを更新する必要があります。Informatica トラストストア環境変数に、SSL 証明書の場所を設定します。

Administrator ツールでのドメインへの通信保護の有効化

Administrator ツールを使用して、ドメインに対する安全な通信を有効にすることができます。Administrator ツールで安全な通信を有効にする場合は、infasetup コマンドを実行してノードを更新する必要もあります。

Administrator ツールで［安全な通信］オプションを有効にする場合は、infasetup コマンドを実行して各ノードの Informatica 構成ファイルを更新する必要もあります。使用する SSL 証明書ファイルを指定するには、infasetup コマンドを実行するときにキーストアファイルとトラストストアファイルを指定します。

各ノード上の Informatica 設定ファイルを更新するには、以下のコマンドを使用します。

infasetup UpdateGatewayNode

ドメインのゲートウェイノード上のサービスマネージャに対して安全な通信を有効にするには、UpdateGatewayNode コマンドを使用します。ドメインに複数のゲートウェイノードがある場合は、各ゲートウェイノードで UpdateGatewayNode コマンドを実行します。

infasetup UpdateWorkerNode

ドメインの作業ノード上のサービスマネージャに対して安全な通信を有効にするには、UpdateWorkerNode コマンドを使用します。ドメインに複数の作業ノードがある場合は、各作業ノードで UpdateWorkerNode コマンドを実行します。

Administrator ツールからセキュアなドメイン通信を有効にするには、以下の手順を実行します。

1. Administrator ツールで、ドメインを選択します。
2. ［コンテンツ］パネルで、**［プロパティ］**ビューをクリックします。
3. **［全般プロパティ］**セクションに移動して、**［編集］**をクリックします。

4. **［全般的なプロパティの編集］**ウィンドウで、**［安全な通信を有効にする］**を選択します。
5. **［OK］**をクリックします。
6. ドメインをシャットダウンする。
   ドメインは、infasetup のコマンドを実行する前にシャットダウンしておく必要があります。
7. 必要なオプションと引数を指定して infasetup を実行します。
   以下のコマンドを入力します。
   - Windows: `infasetup UpdateGatewayNode` または `infasetup UpdateWorkerNode`
   - UNIX: `infasetup.sh UpdateGatewayNode` または `infasetup.sh UpdateWorkerNode`

   ノード上で安全な通信を設定するには、次のオプションを指定してコマンドを実行します。

オプション	引数	説明
-EnableTLS -tls	enable_tls	Informatica ドメインのサービスに安全な通信を設定します。
-NodeKeystore -nk	node_keystore_directory	Informatica からデフォルトの SSL 証明書を使用している場合はオプション。各自の SSL 証明書を使用している場合は必須。キーストアファイルを含めるディレクトリ。Informatica ドメインでは、PEM 形式および Java Keystore（JKS）ファイルの SSL 証明書を必要とします。このディレクトリには PEM および JKS 形式のキーストアファイルが含まれている必要があります。キーストアファイルの名前は、infa_keystore.jks および infa_keystore.pem である必要があります。 複数のノードに対して同じキーストアファイルを使用できます。
-NodeKeystorePass -nkp	node_keystore_password	Informatica からデフォルトの SSL 証明書を使用している場合はオプション。各自の SSL 証明書を使用している場合は必須。infa_keystore.jks ファイルのパスワード。
-NodeTruststore -nt	node_truststore_directory	Informatica からデフォルトの SSL 証明書を使用している場合はオプション。各自の SSL 証明書を使用している場合は必須。トラストストアファイルが含まれるディレクトリ。Informatica ドメインでは、PEM 形式および Java Keystore（JKS）ファイルの SSL 証明書を必要とします。このディレクトリには PEM および JKS 形式のトラストストアファイルが含まれている必要があります。トラストストアファイルの名前は、infa_truststore.jks および infa_truststore.pem である必要があります。 複数のノードに対して同じトラストストアファイルを使用できます。
-NodeTruststorePass -ntp	node_truststore_password	Informatica からデフォルトの SSL 証明書を使用している場合はオプション。各自の SSL 証明書を使用している場合は必須。infa_truststore.jks ファイルのパスワード。

8. ドメイン内の各ノードに対して infasetup コマンドを実行します。

ドメインに複数のゲートウェイノードがある場合は、各ゲートウェイノードで infasetup UpdateGatewayNode を実行します。複数の作業ノードがある場合は、各作業ノードで infasetup UpdateWorkerNode を実行します。ドメイン内のすべてのノードに同じキーストアファイルとトラストストアファイルを使用する必要があります。

9. ドメインを再起動します。

ドメイン内のすべてのノードの更新が完了した後、Informatica クライアントツールをホストするマシンを更新する必要があります。Informatica トラストストア環境変数に、SSL 証明書の場所を設定します。

Informatica クライアントアプリケーションをセキュアなドメインと連携するように設定する

ドメイン内でセキュアな通信を有効にすると、ドメインと、Developer tool などの Informatica クライアントアプリケーションの間の接続も保護されます。環境変数でドメインを保護するために使用するトラストストアファイルの場所とパスワードを指定する必要がある場合もあります。環境変数は、ドメイン内のサービスにアクセスするクライアントアプリケーションをホストするマシンで設定します。

Informatica ドメインを保護するために使用される SSL 証明書は infa_truststore.jks および infa_truststore.pem という名前のトラストストアファイルに格納されています。トラストストアファイルは各クライアントホストで使用できる必要があります。

各クライアントホストで以下の環境変数を設定する必要がある場合もあります。

INFA_TRUSTSTORE

この変数は、infa_truststore.jks および infa_truststore.pem というトラストファイルが格納されているディレクトリに設定します。

INFA_TRUSTSTORE_PASSWORD

この変数は、トラストストアのパスワードに設定します。パスワードは暗号化される必要があります。コマンドラインプログラム pmpasswd を使用して、パスワードを暗号化します。

Informatica は、ユーザーがドメインの保護に使用できる SSL 証明書をデフォルトのトラストストアファイルで提供します。Informatica クライアントをインストールする際、インストーラによって環境変数が設定され、トラストストアファイルはデフォルトで<Informatica installation directory>\clients\shared\security ディレクトリにインストールされます。

デフォルトの Informatica SSL 証明書を使用しており、infa_truststore.jks ファイルと infa_truststore.pem ファイルがデフォルトのディレクトリにある場合、INFA_TRUSTSTORE または INFA_TRUSTSTORE_PASSWORD 環境変数を設定する必要はありません。

INFA_TRUSTSTORE および INFA_TRUSTSTORE_PASSWORD 環境変数は、以下のシナリオで各クライアントホストで設定する必要があります。

カスタム SSL **証明書を使用してドメインを保護する。**

SSL 証明書を提供してドメインを保護するために使用する場合、証明書を infa_truststore.jks および infa_truststore.pem という名前のトラストファイルにインポートし、トラストストアファイルを各クライアントホストにコピーします。ファイルの場所とトラストストアパスワードを指定する必要があります。

デフォルトの Informatica **トラストストアファイルをデフォルトのディレクトリにある独自のトラストストアファイルに置き換える。**

デフォルトの infa_truststore.jks および infa_truststore.pem というトラストストアファイルをデフォルトの Informatica ディレクトリにある独自のトラストストアファイルに置き換える場合、トラストストアパスワードを指定する必要があります。トラストストアファイルはデフォルトのトラストストアファイルと同じ名前である必要があります。

デフォルトの Informatica SSL **証明書を使用するが、トラストストアファイルがデフォルトの** Informatica **ディレクトリにない。**

デフォルトの Informatica SSL 証明書を使用するが、デフォルトの infa_truststore.jks および infa_truststore.pem というトラストストアファイルがデフォルトのディレクトリにない場合、ファイルの場所とトラストストアパスワードを指定する必要があります。

セキュアなドメイン環境設定リポジトリのデータベース

Informatica ドメイン環境設定リポジトリは、設定情報とユーザーアカウントの特権および権限を保存します。Informatica ドメインを作成する場合、ドメイン環境設定リポジトリを作成する必要があります。

ドメイン環境設定リポジトリは、SSL プロトコルで保護されたデータベース上に作成することができます。SSL プロトコルはトラストストアファイルに保存された SSL 証明書を使用します。セキュアデータベースアクセスへのアクセスには、データベースに関する証明書を含んだトラストストアが必要です。

セキュアなドメイン環境設定リポジトリデータベースの作成は、Informatica サービスをインストールしてドメインを作成するときに行うことができます。インストール中のセキュアなドメイン環境設定リポジトリの設定についての詳細は、『Informatica インストールガイド』をご覧ください。

インストール後は、コマンドラインからセキュアなドメイン環境設定リポジトリのデータベースを設定できます。

注: インストール後にセキュアなドメイン環境設定リポジトリのデータベースを設定する前に、ドメインの安全な通信を有効にする必要があります。

セキュアなドメイン環境設定リポジトリの作成に対応したデータベースは、次のとおりです。

- Oracle
- Microsoft SQL Server
- IBM DB2

セキュアなドメイン環境設定リポジトリのデータベースの設定

インストール後に、ドメイン環境設定リポジトリをセキュアデータベースに変更することができます。セキュアなドメイン環境設定リポジトリのデータベースが使用できるのは、ドメインに対し安全な通信を有効にした場合のみです。

ドメイン環境設定リポジトリデータベースを変更する前に、ドメインをシャットダウンする必要があります。ドメイン環境設定リポジトリデータベースのバックアップと、セキュアデータベースへのリストアには、infasetup コマンドを使用します。ドメイン環境設定リポジトリをセキュアデータベースにリストアする場合、セキュアデータベースのセキュリティパラメータを指定します。その後で、ドメイン環境設定リポジトリの情報をゲートウェイノードに追加します。

リポジトリデータベースのバックアップとリストア、およびゲートウェイノードの更新には、以下のコマンドを使用します。

infasetup BackupDomain

ドメイン環境設定リポジトリデータベースからデータをバックアップするには、BackupDomain オプションを使用します。

infasetup RestoreDomain

ドメイン環境設定リポジトリのデータをセキュアデータベースにリストアするには、RestoreDomain オプションを使用します。

infasetup UpdateGatewayNode

ドメインのゲートウェイノードの中のドメイン環境設定リポジトリの設定を更新するには、UpdateGatewayNode オプションを使用します。

ドメイン環境設定リポジトリをセキュアデータベースに変更するには、次の手順を完了します。

1. 安全な通信がドメインに対して有効になっていることを確認します。

   ドメイン環境設定リポジトリにセキュアデータベースを使用できるようにするには、その前にドメインをセキュアにしておく必要があります。

2. ドメインをシャットダウンします。
3. infasetup BackupDomain コマンドを実行し、データベース接続情報を指定します。

   BackupDomain コマンドを実行すると、infasetup が大半のドメイン設定データベーステーブルをユーザー指定のファイル名にバックアップします。

   注: Java メモリエラーで infasetup のバックアップコマンドまたはリストアコマンドが失敗する場合は、infasetup が使用可能なシステムメモリを増やします。システムメモリを増やすには、環境変数 INFA_JAVA_CMD_OPTS の-Xmx の値を設定します。
4. infasetup コマンドがバックアップしない追加のリポジトリテーブルを手動でバックアップするには、データベースバックアップユーティリティを使用します。

   次のテーブルのコンテンツをバックアップします。

   - ISP_RUN_LOG
5. ドメイン環境設定リポジトリをセキュアデータベースにリストアするには、infasetup RestoreDomain コマンドを実行して、データベース接続情報を指定します。

   接続情報に加えて、セキュアデータベースに必要な次のオプションを指定してください。

オプション	引数	説明
-DatabaseTlsEnabled -dbtls	database_tls_enabled	必須。ドメイン環境設定リポジトリのリストア先となるデータベースがセキュアデータベースであるかどうかを示します。このオプションを True に設定します。
-DatabaseTruststoreLocation -dbtl	database_truststore_location	必須。データベースの SSL 証明書を含んだトラストストアファイルのパスとファイル名。
-DatabaseTruststorePassword -dbtp	database_truststore_password	必須。セキュアデータベースに対するデータベーストラストストアファイルのためのパスワード。

   接続文字列で、以下のセキュリティパラメータを含めます。

   EncryptionMethod

   必須。ネットワーク上で送信される際にデータが暗号化されるかどうかを示します。このパラメータは SSL に設定する必要があります。

   ValidateServerCertificate

   オプション。データベースサーバーが送信する証明書を Informatica で検証するかどうかを示します。

   このパラメータを True に設定した場合、Informatica ではデータベースサーバーが送信する証明書を検証します。HostNameInCertificate パラメータを指定すると、Informatica は証明書内のホスト名も検証します。

このパラメータを False に設定した場合、Informatica ではデータベースサーバーが送信する証明書を検証しません。指定するトラストストア情報がすべて無視されます。

デフォルトは True です。

HostNameInCertificate

オプション。セキュアデータベースをホストするマシンのホスト名。ホスト名を指定すると、Informatica は接続文字列に含められたそのホスト名を SSL 証明書内のホスト名と照らして検証します。

cryptoProtocolVersion

必須。セキュアデータベースへの接続に使用する暗号化プロトコルを指定します。データベースサーバーによって使用される暗号化プロトコルに基づいて、`cryptoProtocolVersion=TLSv1.1` または `cryptoProtocolVersion=TLSv1.2` を設定できます。

6. データベースリストアユーティリティを使用して、手動でバックアップしたリポジトリテーブルをリストアします。

   次のテーブルをリストアします。

   - ISP_RUN_LOG

7. セキュアなドメイン環境設定リポジトリの情報でドメイン内のノードを更新するには、infasetup UpdateGatewayNode コマンドを実行して、セキュアデータベース接続情報を指定します。

   ノードオプションに加えて、セキュアデータベースに必要な次のオプションを指定します。

オプション	引数	説明
-DatabaseTlsEnabled -dbtls	database_tls_enabled	必須。ドメイン環境設定リポジトリに使用するデータベースがセキュアデータベースであることを示します。このオプションを True に設定します。
-DatabaseConnectionString -cs	database_connection_string	必須。セキュアデータベースへの接続に使用される接続文字列。接続文字列には、手順 5 で infasetup RestoreDomain コマンドを実行したときに接続文字列に含めたセキュリティパラメータを含める必要があります。
-DatabaseTruststorePassword -dbtp	database_truststore_password	必須。セキュアデータベースに対するデータベーストラストストアファイルのためのパスワード。

   ドメインに複数のゲートウェイノードがある場合は、各ゲートウェイノードで infasetup UpdateGatewayNode を実行します。

8. ドメインを再起動します。

セキュアな PowerCenter リポジトリデータベース

PowerCenter リポジトリサービスを作成するときに、関連する PowerCenter リポジトリを SSL プロトコルで保護されたデータベース上に作成することができます。

PowerCenter リポジトリサービスは、ネイティブ接続を介して PowerCenter リポジトリデータベースに接続します。

セキュアデータベース上に PowerCenter リポジトリを作成するときは、データベースに関するセキュアな接続の情報がデータベースクライアントファイルに含まれているか確かめます。例えば、PowerCenter リポジトリをセキュアな Oracle データベース上に作成する場合、セキュアな接続の情報を使って Oracle データベースのクライアントファイル（tnsnames.ora と sqlnet.ora）を設定します。

セキュアなモデルリポジトリデータベース

モデルリポジトリサービスを作成するときに、関連するモデルリポジトリを SSL プロトコルで保護されたデータベース内に作成することができます。

モデルリポジトリサービスは、JDBC ドライバを介してモデルリポジトリデータベースに接続します。

1. SSL プロトコルで保護されたデータベースを設定します。
2. Administrator ツールで、モデルリポジトリサービスを作成します。
3. **［新しいモデルリポジトリサービス］**ダイアログボックスで、モデルリポジトリサービスの全般プロパティを入力し、**［次へ］**をクリックします。
4. データベースプロパティとモデルリポジトリサービスの JDBC 接続文字列を入力します。

   セキュアデータベースに接続するには、セキュアデータベースのパラメータを**［セキュア JDBC パラメータ］**フィールドに入力します。Informatica は、**［セキュア JDBC パラメータ］**フィールドの値を機密データとして取り扱い、パラメータの文字列を暗号化して保存します。

   以下のリストは、セキュアデータベースのパラメータを示しています。

   EncryptionMethod

   必須。ネットワーク上で送信される際にデータが暗号化されるかどうかを示します。このパラメータは SSL に設定する必要があります。

   ValidateServerCertificate

   オプション。データベースサーバーが送信する証明書を Informatica で検証するかどうかを示します。

   このパラメータを True に設定した場合、Informatica ではデータベースサーバーが送信する証明書を検証します。HostNameInCertificate パラメータを指定すると、Informatica は証明書内のホスト名も検証します。

   このパラメータを False に設定した場合、Informatica ではデータベースサーバーが送信する証明書を検証しません。指定するトラストストア情報がすべて無視されます。

   デフォルトは True です。

   HostNameInCertificate

   オプション。セキュアデータベースをホストするマシンのホスト名。ホスト名を指定すると、Informatica は接続文字列に含められたそのホスト名を SSL 証明書内のホスト名と照らして検証します。

   cryptoProtocolVersion

   必須。セキュアデータベースへの接続に使用する暗号化プロトコルを指定します。データベースサーバーによって使用される暗号化プロトコルに基づいて、`cryptoProtocolVersion=TLSv1.1` または `cryptoProtocolVersion=TLSv1.2` を設定できます。

   TrustStore

   必須。データベースの SSL 証明書を含んだトラストストアファイルのパスとファイル名。
   トラストストアファイルのパスを含めていない場合、Informatica は次のデフォルトディレクトリの中からファイルを探します。`<InformaticaInstallationDirectory>/tomcat/bin`

TrustStorePassword

必須。セキュアデータベースに対するトラストストアファイルのためのパスワード。

注: Informatica は、セキュア JDBC パラメータを JDBC の接続文字列に付加します。セキュア JDBC パラメータを接続文字列に直接含める場合、**［セキュア JDBC パラメータ］**フィールドにはパラメータを入力しないでください。

5. 接続をテストして、セキュアなリポジトリデータベースへの接続が有効であるか確かめてください。
6. モデルリポジトリサービスを作成するプロセスを完了します。

ワークフローとセッションの通信保護

デフォルトでは、ドメインに対し安全な通信オプションを有効にすると、Informatica がデータ統合サービスおよび PowerCenter 統合サービスと DTM プロセスとの間の接続を保護します。

さらに、グリッドで PowerCenter セッションを実行すると、DTM プロセス間のデータ通信を保護するオプションを有効にできます。

PowerCenter セッションで DTM プロセス間のデータ通信の保護を有効にするには、PowerCenter 統合サービスに対して **［データの暗号化を有効にする］**オプションを選択します。

注: DTM プロセスがセキュアモードで実行されているときは、PowerCenter セッションにより多くの CPU およびメモリが必要になります。PowerCenter セッションに対して DTM プロセス間のデータ通信保護を有効にする前に、負荷が増えても問題ないだけのドメインリソースがあるかどうか判断してください。

PowerCenter DTM プロセスに対する通信保護の有効化

グリッド上で実行されている PowerCenter セッション内の DTM プロセス間の接続を保護するには、DTM プロセスでデータの暗号化が有効になるように PowerCenter 統合サービスを設定してください。

1. Administrator ツールのナビゲータで、PowerCenter 統合サービスを選択します。
2. ［コンテンツ］パネルで、［プロパティ］ビューをクリックします。
3. PowerCenter 統合サービスの［プロパティ］セクションに移動して、［編集］をクリックします。
4. **［PowerCenter 統合サービスのプロパティの編集］**ウィンドウで、**［データの暗号化を有効にする］**を選択します。
5. **［OK］**をクリックします。

グリッドで PowerCenter セッションを実行すると、DTM プロセスが他の DTM プロセスと通信を行うときに、暗号化されたデータが送信されます。

Web アプリケーションサービスへのセキュアな接続

Web アプリケーションサービスとブラウザの間で送信されるデータを保護するには、Web アプリケーションサービスとブラウザの間の接続を保護します。

次の接続を保護することができます。

Administrator **ツールへの接続**

Administrator ツールとブラウザの間の接続を保護することができます。

Web **アプリケーションサービスへの接続**

次の Web アプリケーションサービスとブラウザの間の接続を保護することができます。

- アナリストサービス
- Metadata Manager サービス
- Test Data Manager サービス
- Web サービス Hub コンソールサービス

Web アプリケーションサービスへのセキュアな接続の要件

Web アプリケーションサービスへの接続を保護する前に、次の要件が満たされていることを確認します。

証明書署名要求（CSR）および非公開キーを作成しました。

CSR および非公開キーを作成するにはキーツールまたは OpenSSL を使用できます。

RSA 暗号化を使用する場合、512 ビットを超える暗号化にする必要があります。

署名された SSL 証明書があります。

証明書には、自己署名証明書または CA によって署名された証明書があります。CA によって署名された証明書をお勧めします。

証明書を JKS 形式のキーストアにインポートしました。

キーストアに含める証明書は 1 つのみです。Web アプリケーションサービスごとに一意の証明書を使用する場合は、それぞれの証明書に個別のキーストアを作成します。または、共有の証明書およびキーストアを使用することができます。

Administrator ツールに対してインストーラで生成された SSL 証明書を使用する場合、この証明書を JKS 形式のキーストアにインポートする必要はありません。

キーストアはアクセス可能なディレクトリ内にあります。

キーストアは、Administrator ツールおよびコマンドラインプログラムからアクセスできるディレクトリ内にある必要があります。

Administrator ツールへの安全な接続の有効化

インストール後は、コマンドラインから Administrator ツールに安全な接続を設定することができます。

ドメイン内のゲートウェイノードのプロパティを、Informatica Administrator のサービスとブラウザの間の接続が保護されるように更新する必要があります。

安全な接続のプロパティでゲートウェイノードを更新するには、次のコマンドを実行します。`infasetup UpdateGatewayNode`

以下のオプションがあります。

オプション	引数	説明
-HttpsPort -hs	AdminConsole_https_port	Informatica Administrator サービスへのセキュアな接続に使用するポート番号。
-KeystoreFile -kf	AdminConsole_Keystore_File	Informatica Administrator サービスへの HTTPS 接続に使用するキーストアファイルのパスとファイル名。
-KeystorePass -kp	AdminConsole_Keystore_Password	キーストアファイルのパスワード。

ドメイン内に複数のゲートウェイノードがある場合、各ゲートウェイノードでこのコマンドを実行します。

Informatica Web アプリケーションサービス

Web アプリケーションサービスを作成または設定する場合は、セキュアな接続を設定します。各アプリケーションサービスには、HTTPS によるセキュアな接続のための特定のプロパティがあります。

Analyst ツールのセキュリティ

アナリストサービスを作成するときは、セキュアな HTTPS のプロパティを Analyst ツールに設定することができます。

ブラウザとアナリストサービスの間の接続を保護するには、以下のアナリストサービスプロパティを設定してください。

プロパティ	説明
安全な通信を有効にする	これを選択すると、Analyst ツールとアナリストサービスの間の接続保護が有効になります。
HTTPS ポート	Transport Layer Security（TLS）プロトコルが有効なときに Informatica Analyst の Web アプリケーションが実行されるポート番号。HTTP ポート番号と異なるポート番号を使用します。
キーストアファイル	デジタル証明書を含むキーストアファイルが保存されているディレクトリ。
キーストアのパスワード	キーストアファイルのプレーンテキストパスワード。このプロパティが設定されていない場合、アナリストサービスはデフォルトのパスワード「*changeit*」を使用します。
SSL プロトコル	このフィールドは空白にしておくことをお勧めします。有効になる TLS のバージョンはこの値によって決まります。フィールドを空白にしておくと、使用可能な TLS バージョンのうち最上位のバージョンが有効になります。値を入力すると、最上位ではないバージョンの TLS が有効になる可能性があります。動作は、現在の環境の Java バージョンに基づきます。 詳細については、現在お使いの Java バージョンのドキュメントを参照してください。

Web サービス Hub コンソールのセキュリティ

Web サービス Hub サービスを作成する場合、Web サービス Hub のコンソールに対してセキュアな HTTPS のプロパティを設定することができます。

ブラウザと Web サービス Hub サービスの間の接続を保護するには、次の Web サービス Hub サービスプロパティを設定してください。

プロパティ	説明
URLScheme	Web サービス Hub に対して設定するセキュリティプロトコルを示します。 - HTTP。Web サービス Hub を HTTP でのみ実行します。 - HTTPS。Web サービス Hub を HTTPS でのみ実行します。 - HTTP と HTTPS。Web サービス Hub を HTTP モードと HTTPS モードで実行します。
HubPortNumber (https)	HTTPS の Web サービス Hub のポート番号。選択された URL スキームに HTTPS が含まれている場合に表示されます。Web サービス Hub を HTTPS で実行するように選択する場合に必要です。デフォルトは 7343 です。
キーストアファイル	HTTPS 接続に必要なキーと証明書を含むキーストアファイルのパスとファイル名。
キーストアのパスワード	キーストアファイルのパスワード。このプロパティが設定されていない場合、Web サービス Hub は、デフォルトのパスワード「*changeit*」を使用します。

Metadata Manager のセキュリティ

Metadata Manager サービスを作成する場合、Metadata Manager の Web アプリケーションに対してセキュアな HTTPS プロパティを設定することができます。

ブラウザと Metadata Manager サービスの間の接続を保護するには、以下の Metadata Manager サービスプロパティを設定してください。

プロパティ	説明
Secure Sockets Layer を有効にする	Metadata Manager Web アプリケーションに対して安全な接続を設定する場合に選択します。 **注**: このプロパティは Metadata Manager サービスを作成する場合に表示されます。既存の Metadata Manager サービスの接続を保護するには、[URL **スキーム**] 設定プロパティを HTTPS に設定します。
ポート番号	Metadata Manager アプリケーションが実行されるポート番号。デフォルトは 10250 です。
キーストアファイル	Metadata Manager Web アプリケーションに対して安全な接続を設定する場合に必要なキーと証明書を含むキーストアファイル。 **注**: Metadata Manager サービスは RSA 暗号化を使用します。そのため、RSA アルゴリズムで生成されたセキュリティ証明書を使用することをお勧めします。
キーストアのパスワード	キーストアファイルのパスワード。

Informatica ドメイン用の暗号スイート

Informatica ドメイン内で接続を暗号化するときに使用される暗号スイートを設定できます。Informatica ドメインからドメイン外部のリソースへの接続は暗号スイート設定の影響を受けません。

Informatica ドメインの安全な通信または Web アプリケーションサービスへの安全な接続を有効にすると、暗号スイートを使用してトラフィックが暗号化されます。

Informatica では、次のリストに基づいて、使用する暗号スイートの有効リストが作成されます。

ブラックリスト

Informatica ドメインでブロックする暗号スイートのリストです。暗号スイートをブラックリストに追加すると、その暗号スイートは有効リストから削除されます。デフォルトリストにある暗号リストをブラックリストに追加できます。

デフォルトリスト

デフォルトで Informatica ドメインがサポートする暗号スイートのリストです。ホワイトリストまたはブラックリストを設定しない場合、デフォルトリストが有効リストとして使用されます。

詳細については、付録 C,「暗号スイートのデフォルトリスト」 (ページ 253)を参照してください。

ホワイトリスト

Informatica ドメインでサポートする暗号スイートのリストです。暗号スイートをホワイトリストに追加すると、その暗号スイートは有効リストに追加されます。デフォルトリストにある暗号リストはホワイトリストに追加する必要はありません。

有効リストは、ホワイトリストの暗号スイートをデフォルトリストに追加し、ブラックリストの暗号スイートをデフォルトリストから削除することによって作成されます。

有効リストについて、以下のガイドラインを考慮します。

- Web クライアントへの安全な接続にカスタム有効リストを使用するには、Informatica ドメイン内で安全な通信を使用する必要があります。ドメインで安全な通信が使用されていない場合、デフォルトリストが有効リストとして使用されます。
- 有効リストは Informatica ドメイン内の接続のみを対象としています。データソースへの接続では、有効リストは使用されません。
- 有効リストには、TLS v1.1 または 1.2 がサポートする暗号スイートが少なくとも 1 つ含まれている必要があります。
- 有効リストは、Windows、Java Runtime Environment、および OpenSSL に対して有効な暗号スイートである必要があります。

高度な暗号を使用するための Informatica ドメインの設定

高度なセキュリティを実現するために AES-256 を用いる高度な暗号スイートを使用する場合、ドメイン内の各ノードに Java Runtime Environment（JRE）と共にインストールされる Java Cryptography Extension（JCE）ポリシーファイルを強度無制限の JCE ポリシーファイルに置き換える必要があります。強度無制限の JCE ポリシーファイルには暗号強度に対する制約がありません。

1. Java Cryptography Extension（JCE）Unlimited Strength Jurisdiction Policy Files 8 アーカイブをダウンロードします。
2. ドメインをシャットダウンします。
3. ドメインノードで次のディレクトリに移動します。

   `<Informatica installation directory>\java\jre\lib\security\`

4. 以下の JAR ファイルをアーカイブから抽出した JAR ファイルに置き換えます。
   - local_policy.jar
   - US_export_policy.jar
5. ドメインを再起動します。

暗号スイートリストの作成

特定の暗号スイートを使用するように Informatica ドメインを設定するには、サポートする追加の暗号スイートを指定するホワイトリストを作成します。ブロックする暗号スイートを指定するブラックリストを作成することもできます。

ネットワークセキュリティ管理者と協力して、Informatica ドメインに適した暗号スイートを決定します。

暗号スイートのリストはコンマ区切りのリストにする必要があります。リスト内の暗号スイートには Internet Assigned Numbers Authority（IANA）名を使用します。または、Java の正規表現を使用することもできます。

infasetup を使用してホワイトリストおよびブラックリストを設定します。リストはコマンドのパラメータに直接指定することも、コンマ区切りリストを含むプレーンテキストファイルを指定することもできます。

次のサンプルテキストは、2 つの暗号スイートを使用したリストを示しています。

```
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

Informatica ドメインの暗号スイートのホワイトリストとブラックリストは、ドメインを作成するときに設定できます。infasetup を使用して、Informatica ドメイン、ゲートウェイノード、作業ノードを作成します。infasetup コマンドの詳細は、『*Informatica コマンドリファレンス*』に記載されています。

または、既存の Informatica ドメインにホワイトリストとブラックリストを設定できます。

暗号スイートの新しい有効リストを使用した Informatica ドメインの設定

Informatica ドメインで使用する暗号スイートを設定するには、同じホワイトリストとブラックリストを使用して Informatica ドメイン、すべてのゲートウェイノード、すべての作業ノードを更新する必要があります。

注: ブラックリスト、ホワイトリスト、有効リストへの変更は累積されません。コマンドを実行すると、ブラックリスト、デフォルトリスト、ホワイトリストに基づいて新しい有効リストが作成されます。新しい有効リストは以前のリストを上書きします。

暗号スイートの新しい有効リストを使用して既存の Informatica ドメインを設定するには、次の手順を実行します。

1. Informatica ドメインをシャットダウンします。
2. 必要に応じて、infasetup listDomainCiphers コマンドを実行して、ドメインまたはノードがサポートまたはブロックしている暗号スイートのリストを表示します。

   例えば、すべての暗号スイートのリストを表示するには、次のコマンドを実行します。

   ```
   infasetup listDomainCiphers -l ALL -dc true
   ```
3. ゲートウェイノードで infasetup updateDomainCiphers コマンドを実行し、ホワイトリスト、ブラックリスト、またはその両方を指定します。

   例えば、1 つの暗号スイートを有効リストに追加し、2 つの暗号スイートを有効リストから削除するには、次のコマンドを実行します。

   ```
   infasetup updateDomainCiphers -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl
   TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
   ```

4. 各ゲートウェイノードで infasetup updateGatewayNode コマンドを実行し、ホワイトリスト、ブラックリスト、またはその両方を指定します。

   ドメインと同じホワイトリストとブラックリストを使用します。

   例えば、次のコマンドを実行します。

   ```
   infasetup updateGatewayNode -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl
   TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
   ```

5. Informatica ドメインと同じ暗号スイートセットを使用して各作業ノードを更新します。

   ドメインと同じホワイトリストとブラックリストを使用します。

   例えば、次のコマンドを実行します。

   ```
   infasetup updateWorkerNode -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl
   TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
   ```

6. Informatica ドメインを起動します。
7. 必要に応じて、infacmd isp listDomainCiphers コマンドを実行して、ドメインまたはノードが使用する暗号スイートのリストを表示します。

   例えば、ドメインで使用する暗号スイートの有効リストを表示するには、次のコマンドを実行します。

   ```
   infacmd isp listCiphers -l EFFECTIVE -dc true
   ```

セキュアなソースおよびターゲット

Informatica では、接続オブジェクトを使ってソースまたはターゲットとしてリレーショナルデータベースに接続します。SSL 証明書で保護されているリレーショナルデータベースへの接続オブジェクトを作成することができます。

Workflow Manager で PowerCenter の接続オブジェクトを作成します。Developer tool または Administrator ツールで Data Service、Data Quality、または Profiling の接続を作成します。

セキュアなソートまたはターゲットへの接続を作成できるのは、以下のデータベースです。

- Oracle
- Microsoft SQL Server
- IBM DB2

データ統合サービスのソースとターゲット

データ統合サービスがマッピング、データプロファイル、スコアカード、または SQL データサービスを処理できるように接続オブジェクトを作成するときは、SSL プロトコルで保護されたデータベースへの接続を定義することができます。

データ統合サービスが、JDBC ドライバを通じてソースまたはターゲットのデータベースに接続されます。セキュアリポジトリデータベースへの接続を設定する場合は、JDBC 接続文字列の中にセキュア接続パラメータを含める必要があります。

1. SSL プロトコルで保護されたデータベースを、ソースまたはターゲットとして使用するように設定します。
2. Administrator ツールで、接続を作成します。
3. **［新しい接続］**ダイアログボックスで、接続のタイプを選択します。それから **［OK］**をクリックします。

   DB2、Microsoft SQL Server、または Oracle のセキュアなデータベースへの接続を作成することができます。

4. **［新しい接続 - 手順 1/3］**ダイアログボックスで接続のプロパティを入力し、**［次へ］**をクリックします。
5. **［新しい接続 - 手順 2/3］**ページで、データベースへの接続文字列を入力します。

   セキュアデータベースに接続するには、セキュアデータベースのパラメータを**［詳細 JDBC セキュリティオプション］**フィールドに入力します。Informatica は、**［詳細 JDBC セキュリティオプション］**フィールドの値を機密データとして取り扱い、パラメータの文字列を暗号化して保存します。

   以下のリストは、セキュアデータベースのパラメータを示しています。

   EncryptionMethod

   必須。ネットワーク上で送信される際にデータが暗号化されるかどうかを示します。このパラメータは SSL に設定する必要があります。

   ValidateServerCertificate

   オプション。データベースサーバーが送信する証明書を Informatica で検証するかどうかを示します。

   このパラメータを True に設定した場合、Informatica ではデータベースサーバーが送信する証明書を検証します。HostNameInCertificate パラメータを指定すると、Informatica は証明書内のホスト名も検証します。

   このパラメータを False に設定した場合、Informatica ではデータベースサーバーが送信する証明書を検証しません。指定するトラストストア情報がすべて無視されます。

   デフォルトは True です。

   HostNameInCertificate

   オプション。セキュアデータベースをホストするマシンのホスト名。ホスト名を指定すると、Informatica は接続文字列に含められたそのホスト名を SSL 証明書内のホスト名と照らして検証します。

   TrustStore

   必須。データベースの SSL 証明書を含んだトラストストアファイルのパスとファイル名。

   TrustStorePassword

   必須。セキュアデータベースに対するトラストストアファイルのためのパスワード。

   注: Informatica は、セキュア JDBC パラメータを接続文字列に付加します。セキュア JDBC パラメータを接続文字列に直接含める場合、**［詳細 JDBC セキュリティオプション］**フィールド内にはパラメータを入力しないでください。
6. 接続をテストして、セキュアデータベースへの接続が有効であることを確かめます。
7. リレーショナル接続を作成するプロセスを完了します。

PowerCenter のソースとターゲット

PowerCenter セッションに接続オブジェクトを作成するときに、SSL プロトコルで保護されたデータベースへの接続を定義することができます。

ネイティブ接続または ODBC ドライバを通じて PowerCenter のリレーショナルソースとリレーショナルターゲットに接続することができます。

ネイティブ接続でセキュアなリレーショナルソースまたはリレーショナルターゲットに接続する場合、データベースクライアントの中にセキュアデータベースに関する接続情報があることを確認します。例えば、セキュアな Oracle データベース上の PowerCenter のターゲットに接続する場合、セキュアデータベースのための接続情報を使って Oracle データベースクライアントファイル「*tnsnames.ora*」を設定します。

ODBC ドライバを通じてセキュアなリレーショナルソースまたはリレーショナルターゲットに接続する場合は、データベースクライアントの中にセキュアデータベースに関する接続情報があることと、ODBC データソースがセキュアデータベースへの接続を正しく定義していることを確認します。

セキュアなデータストレージ

Informatica は、ドメイン環境設定リポジトリ内にデータを保存する前に、パスワードや安全な接続パラメータのような機密データを暗号化します。Informatica では、機密データの暗号化に使用する暗号化キーを作成するときに、ユーザーが提供するキーワードを使用しています。

インストール時にユーザーがインストーラに対して、ドメインの暗号化キーの生成に使用するキーワードを提供する必要があります。ドメイン内のすべてのノードが、同じ暗号化キーを使用する必要があります。複数のノードにインストールする場合、インストーラはドメイン内のすべてのノードに対して同じ暗号化キーを使用します。インストール時のドメインの暗号化キー生成についての詳細は、『Informatica インストールガイド』をご覧ください。

インストール後は、ドメインの暗号化キーを変更することができます。暗号化キーの生成およびドメインの暗号化キーの変更を行うには、infasetup コマンドを実行します。ドメインの暗号化キーを変更した後は、暗号化されたデータを更新するためにドメイン内のリポジトリの内容をアップグレードしてください。

注: ドメインの名前、暗号化キーのためのキーワード、および暗号化キーファイルは、安全な場所に保管しておく必要があります。ドメイン名、キーワード、暗号化キーは、ドメインの暗号化キーを変更するとき、またはリポジトリを他のドメインに移動するときに必要になります。暗号化キーファイルを紛失すると、暗号化キーを再び生成するためにキーワードが必要になります。キーワードも暗号化キーも紛失してしまうと、ドメインの暗号化キーの変更も、リポジトリの他のドメインへの移動もできなくなります。

UNIX での安全なディレクトリ

Informatica をインストールする場合、インストーラはドメインの暗号化キーファイルなどの限定的なアクセスが必要な Informatica ファイルを保存するディレクトリを作成します。UNIX では、インストーラはディレクトリとディレクトリ内のファイルに対し異なる権限を割り当てます。

デフォルトでは、インストーラは次のディレクトリを Informatica インストールディレクトリに作成し、暗号化キーを保存します。<INFA_HOME>/isp/config/keys

/keys ディレクトリにはノードに対する暗号化キーファイルが含まれます。Kerberos 認証を使用するようにドメインを設定する場合、ディレクトリにも Kerberos キータブファイルが含まれます。

インストール中に、別のディレクトリを暗号化ファイルの保存先に指定することができます。インストーラで、指定されたディレクトリにデフォルトのディレクトリと同じ権限を割り当てます。

/keys ディレクトリとこのディレクトリ内のファイルには以下の権限があります。

ディレクトリ権限

ディレクトリの所有者は、ディレクトリに対する-wx 権限がありますが、r 権限はありません。ディレクトリの所有者は、インストーラの実行に使用されたユーザーアカウントです。この所有者が属するグループにも、ディレクトリに対する-wx 権限がありますが、r 権限はありません。

例えば、ユーザーアカウント *ediqa* はディレクトリを所有し、*infaadmin* グループに属しているとします。*ediqa* ユーザーアカウントおよび *infaadmin* グループには、-wx-wx---権限があります。

ediqa ユーザーアカウントおよび *infaadmin* グループは、ディレクトリ内のファイルの書き込みおよび実行ができます。ディレクトリ内のファイルのリストを表示することはできませんが、特定のファイルを名前で一覧表示できます。

ディレクトリ内のファイル名を知っている場合には、そのファイルをディレクトリから別の場所にコピーできます。ファイル名を知らない場合には、ディレクトリに対する権限を読み取り権限を含むように変更して、ファイルをコピーできるようにする必要があります。コマンド chmod 730 を使用して、ディレクトリおよびサブディレクトリの所有者に読み取り権限を付与できます。

例えば、*siteKey* という名前の暗号化キーファイルをドメイン内の別のノードがアクセスできるようにするには、これを一時ディレクトリにコピーする必要があります。rwx-wx---権限を割り当てるには、

<Informatica インストールディレクトリ>/isp/config ディレクトリでコマンド chmod 730 を実行します。その後、/keys サブディレクトリから別のディレクトリに暗号化キーファイルをコピーできるようになります。

ファイルのコピーが完了したら、ディレクトリの権限を書き込みおよび実行権限に戻すように変更します。コマンド chmod 330 を使用して、読み取り権限を削除できます。

注: ディレクトリおよびファイルへの権限を再帰的に変更する際には、-R オプションを使用しません。ディレクトリおよびディレクトリ内のファイルには、異なる権限があります。

ファイル権限

ディレクトリ内のファイルの所有者には、そのファイルへの rwx 権限があります。ディレクトリ内のファイルの所有者は、インストーラの実行に使用されたユーザーアカウントです。この所有者が属するグループにも、ディレクトリ内のファイルに対する rwx 権限があります。

この所有者およびグループにはファイルへのフルアクセス権があり、ディレクトリ内のファイルを表示または編集できます。

注: ファイルを一覧表示または編集するには、ファイル名を知っている必要があります。

コマンドラインからの暗号化キーの変更

インストール後に、コマンドラインからドメインの暗号化キーを変更することができます。暗号化キーを変更する前にドメインをシャットダウンする必要があります。

infasetup コマンドを使用して暗号化キーを生成し、新しい暗号化キーが使用されるようにドメインを設定します。

以下の infasetup コマンドで、暗号化キーの生成および変更ができます。

generateEncryptionKey

暗号化キーを生成して *sitekey* という名前のファイルにします。暗号化キーのために指定したディレクトリに sitekey という名前のファイルが入っている場合、Informatica がそのファイル名を *siteKey_old* に変更します。

migrateEncryptionKey

Informatica ドメイン内への機密データの保存に使用される暗号化キーを変更します。

ドメインに対する暗号化キーを変更するには、次の手順を完了します。

1. ドメインをシャットダウンします。
2. 暗号化キーを変更する前にドメインのバックアップを作成します。

   暗号化キーを変更したことで問題が発生したときに確実にドメインをリカバリできるようにするために、infasetup コマンドを実行する前にドメインのバックアップを作成します。
3. ドメインの暗号化キーを生成するために、infasetup generateEncryptionKey コマンドを実行します。

暗号化キーの生成に必要な以下のオプションを指定します。

オプション	引数	説明
-keyword -kw	キーワード	暗号化キー生成の基になるベースワードとして使用するテキスト文字列。 キーワードは以下の基準をすべて満たす必要があります。 - 長さが 8〜20 文字である - 大文字を 1 文字以上使用する - 小文字を 1 文字以上使用する - 数字を 1 文字以上使用する - スペースを含まない
-domainName -dn	domain_name	Informatica ドメインの名前。
-encryptionKeyLocation -kl	encryption_key_location	現在の暗号化キーが入ったディレクトリ。暗号化ファイルの名前は *sitekey* です。 Informatica は、現在の *sitekey* ファイルを *sitekey_old* に名称変更し、同じディレクトリ内に *sitekey* という名前の新しいファイルを作り、そこに暗号化キーを生成します。

4. ドメインの暗号化キーを変更するには、infasetup migrateEncryptionKey コマンドを実行して、前の暗号化キーと新しい暗号化キーの場所を指定します。

ドメインの暗号化キーの変更に必要な次のオプションを指定します。

オプション	引数	説明
-LocationOfEncryptionKeys -loc	location_of_encryption_keys	*siteKey_old* という名前の古い暗号化キーファイルと、*siteKey* という名前の新しい暗号化キーファイルが保存されているディレクトリ。 このディレクトリには、古い暗号化キーファイルと新しい暗号化キーファイルが入っている必要があります。前の暗号化キーファイルと新しい暗号化キーファイルが別々のディレクトリに保存されている場合、暗号化キーファイルを同じディレクトリにコピーしてください。 ドメインに複数のノードがある場合、migrateEncryptionKey コマンドを実行するドメインの中のどのノードからでも、このディレクトリにアクセスできるようにしておく必要があります。 **注**: UNIX では、ファイル名 *siteKey_old* は大文字小文字が区別されます。以前の暗号化キーファイルの名前を手動で変更する場合は、大文字小文字が正しく区別されることを確認してください。
-IsDomainMigrated -mig	is_domain_migrated	ドメインが最新の暗号化キーを使用するように更新されているかどうかを示します。 migrateEncryptionKey コマンドを初めて実行するときは、このドメインが以前の暗号化キーを使用することを示すために、このオプションを False に設定します。 2 回目以降、migrateEncryptionKey コマンドを実行してドメイン内の他のノードを更新するときに、このドメインが最新の暗号化キーを使用するように更新されていることを示すために、このオプションを True に設定します。あるいは、このオプションを使わずに migrateEncryptionKey コマンドを実行してもかまいません。 デフォルトは True です。

5. ドメイン内の各ノードに対して infasetup コマンドを実行します。

   ドメインに複数のノードがある場合、各ノードに対して infasetup migrateEncryptionKey を実行します。このコマンドは、作業ノードに対して実行する前に、まずゲートウェイノードに対して実行してください。このコマンドの初回実行が済んだら、以後は IsDomainMigrated オプションを省略してもかまいません。

6. ドメインを再起動します。

   新しい暗号化キーを使用してリポジトリ内の機密データを更新して暗号化するには、ドメイン内のすべてのリポジトリサービスをアップグレードする必要があります。

7. モデルリポジトリサービス、PowerCenter リポジトリサービス、および Metadata Manager サービスをすべてアップグレードします。

モデルリポジトリサービスと PowerCenter リポジトリサービスは、Administrator ツールまたはコマンドプロンプトでアップグレードできます。Metadata Manager サービスは、Administrator ツールでアップグレードできます。

注: Metadata Manager サービスは、アップグレードする前に無効にする必要があります。

Administrator ツールでサービスをアップグレードするには、ヘッダ領域で **［管理］** > **［アップグレード］** を選択します。複数のサービスを選択した場合、Administrator ツールでは適切な順序でアップグレードします。

コマンドプロンプトでサービスをアップグレードするには、以下のコマンドを使用します。

リポジトリサービスタイプ	コマンド
モデルリポジトリサービス	`infacmd mrs UpgradeContents`
PowerCenter リポジトリサービス	`pmrep Upgrade`

アプリケーションサービスとポート

Informatica ドメイン内の Informatica ドメインサービスとアプリケーションサービスには一意のポートがあります。

Informatica ドメイン

以下の表に、設定できるポートを示します。

ポート	説明
サービスマネージャポート	ノードのサービスマネージャが使用するポート番号。 サービスマネージャは、このポートで受信する接続要求をリスンします。クライアントアプリケーションは、このポートを使用してドメインのサービスと通信します。Informatica コマンドラインプログラムは、このポートを使用して、ドメインと通信します。このポートは、SQL データサービスの JDBC/ODBC ドライバ用のポートでもあります。デフォルトは 6006 です。
サービスマネージャのシャットダウンポート	ドメインのサービスマネージャに対するサーバーのシャットダウンを制御するポート番号。サービスマネージャは、このポートでシャットダウンコマンドをリスンします。デフォルトは 6007 です。
Informatica Administrator ポート	Informatica Administrator が使用するポート番号。デフォルトは 6008 です。
Informatica Administrator シャットダウンポート	Informatica Administrator のサーバーシャットダウンを制御するポート番号。Informatica Administrator は、このポートでシャットダウンコマンドをリスンします。デフォルトは 6009 です。
最小ポート番号	このノードで実行するアプリケーションサービスプロセスに割り当てられる動的ポート番号範囲の最小ポート番号。デフォルトは 6014 です。
最大ポート番号	このノードで実行するアプリケーションサービスプロセスに割り当てられる動的ポート番号範囲の最大ポート番号。デフォルトは 6114 です。

アナリストサービス

以下の表に、アナリストサービスに関連付けられたデフォルトポートを一覧表示します。

タイプ	デフォルトポート
アナリストサービス(HTTP)	8085
アナリストサービス (HTTPS)	デフォルトポートはありません。サービスの作成時に必要なポート番号を入力します。
アナリストサービス（ステージングデータベース）	デフォルトポートはありません。データベースポート番号を入力します。

コンテンツ管理サービス

以下の表に、コンテンツ管理サービスに関連付けられたデフォルトポートを一覧表示します。

タイプ	デフォルトポート
コンテンツ管理サービス (HTTP)	8105
コンテンツ管理サービス (HTTPS)	デフォルトポートはありません。サービスの作成時に必要なポート番号を入力します。

データディレクタサービス

以下の表に、データディレクタサービスに関連付けられたデフォルトポートを一覧表示します。

タイプ	デフォルトポート
データディレクタサービス (HTTP)	デフォルトポートはありません。サービスの作成時に必要なポート番号を入力します。
データディレクタサービス (HTTPS)	デフォルトポートはありません。サービスの作成時に必要なポート番号を入力します。

データ統合サービス

以下の表に、データ統合サービスに関連付けられたデフォルトポートを一覧表示します。

タイプ	デフォルトポート
データ統合サービス（HTTP プロキシ）	8085
データ統合サービス (HTTP)	8095
データ統合サービス (HTTPS)	デフォルトポートはありません。サービスの作成時に必要なポート番号を入力します。

タイプ	デフォルトポート
プロファイリングウェアハウスデータベース	デフォルトポートはありません。データベースポート番号を入力します。
ヒューマンタスクデータベース	デフォルトポートはありません。データベースポート番号を入力します。

Metadata Manager サービス

以下の表に、Metadata Manager サービスに関連付けられたデフォルトポートを一覧表示します。

タイプ	デフォルトポート
Metadata Manager サービス (HTTP)	デフォルトは 10250 です。
Metadata Manager サービス (HTTPS)	デフォルトポートはありません。サービスの作成時に必要なポート番号を入力します。

PowerExchange® リスナサービス

DBMOVER ファイルの SVCNODE 文内で指定するポート番号と同じポート番号を使用します。

複数の Listener サービスを定義してノード上で実行する場合、各サービスに対して一意の SVCNODE ポート番号を定義する必要があります。

PowerExchange ロガーサービス

DBMOVER ファイルの SVCNODE 文内で指定するポート番号と同じポート番号を使用します。

複数の Listener サービスを定義してノード上で実行する場合、各サービスに対して一意の SVCNODE ポート番号を定義する必要があります。

Web サービス Hub サービス

以下の表に、Web サービス Hub サービスに関連付けられたデフォルトポートを一覧表示します。

タイプ	デフォルトポート
Web サービス Hub サービス（HTTP）	7333
Web サービス Hub サービス（HTTPS）	7343

第 6 章

Informatica Web アプリケーションへのシングルサインオン

この章では、以下の項目について説明します。

SAML ベースのシングルサインオンの概要

Administrator ツール、Analyst ツール、Monitoring ツール用に Security Assertion Markup Language（SAML）を使用するシングルサインオン（SSO）を設定できます。

Security Assertion Markup Language は、サービスプロバイダと ID プロバイダ間で認証情報と承認情報を交換するための XML ベースのデータ形式です。Informatica ドメインでは、Informatica Web アプリケーションがサービスプロバイダです。ID プロバイダは、Microsoft Active Directory Federation Services（AD FS）2.0 です。このプロバイダは、組織の LDAP または Active Directory ID ストアを使用して、Web アプリケーションユーザーを認証します。

注: SAML ベースのシングルサインオンは、Kerberos 認証を使用するように設定された Informatica ドメインでは使用できません。

SAML ベースのシングルサインオンの認証プロセス

Informatica Web アプリケーションと Active Directory フェデレーションサービスは、認証情報と承認情報を交換して、Informatica ドメインでシングルサインオンを有効にします。

以下の手順は、基本的な SAML ベースのシングルサインオン認証フローを示しています。

1. ユーザーが Informatica Web アプリケーションにログインします。
2. アプリケーションによって SAML 認証要求が AD FS に送信されます。
3. AD FS によって LDAP または Active Directory ID ストアのユーザーアカウント情報に対してユーザーの資格情報が認証されます。

4. AD FS によってユーザーのセッションが作成され、ユーザーに関するセキュリティ関連情報が含まれる SAML アサーショントークンが Web アプリケーションに送信されます。
5. アプリケーションによってアサーションが検証されます。

Web アプリケーションのユーザーエクスペリエンス

ユーザーは、シングルサインオンアカウントが含まれているセキュリティドメイン経由で SAML ベースのシングルサインオンを使用できる Informatica Web アプリケーションにログインします。

Web アプリケーションにログインするときに、ユーザーはアプリケーションログインページでログインするセキュリティドメインを選択します。シングルサインオンを使用できるユーザーは、アカウントに対するシングルサインオンが含まれる LDAP セキュリティドメインを選択します。ユーザーは次に、自分のユーザー名およびパスワードを入力します。資格情報が SAML 認証要求の中で AD FS に送信され、ユーザーが認証されます。

以降の認証は、初期認証中に Web ブラウザで設定されるセッションクッキーを使用して管理されます。認証が完了すると、ユーザーはアプリケーションログインページで LDAP セキュリティドメインを選択して、同じブラウザセッションで SAML ベースのサインオンを使用するように設定されている別の Informatica Web アプリケーションにアクセスできます。ユーザーがユーザー名やパスワードを入力する必要はありません。

認証が完了すると、ユーザーは同じブラウザセッションで実行されているすべての Informatica Web アプリケーションにログインしたままになります。AD FS が永続的なクッキーを発行するように設定されている場合、ユーザーはブラウザを終了して再起動した後もログインしたままになります。

ただし、ユーザーが Informatica Web アプリケーションからログアウトした場合、同じブラウザセッションで実行されている他の Informatica Web アプリケーションからもログアウトされます。

SAML ベースのシングルサインオンを使用できないユーザーは、Web アプリケーションログインページでネイティブセキュリティドメインを選択してから、ネイティブアカウント用のユーザー名およびパスワードを入力します。

SAML ベースのシングルサインオンのセットアップ

SAML ベースのシングルサインオンが使用されるように Active Directory フェデレーションサービス（AD FS）および Informatica ドメインを設定します。

サポートされている Informatica Web アプリケーション用に SAML ベースのシングルサインオンを設定するには、以下のタスクを実行します。

1. Informatica Web アプリケーションのユーザーアカウント用に LDAP セキュリティドメインを作成し、ユーザーを Active Directory からドメインにインポートします。
2. ID プロバイダアサーション署名証明書を AD FS からエクスポートします。
3. ID プロバイダアサーション署名証明書をドメイン内の各ゲートウェイノード上にある Informatica のデフォルトのトラストストアファイルにインポートします。
4. AD FS で Informatica を証明書利用者信頼として追加し、LDAP 属性を AD FS によって発行されたセキュリティトークンで使用される対応タイプにマッピングします。
5. 各 Informatica Web アプリケーションの URL を AD FS に追加します。
6. Informatica ドメイン内の Informatica Web アプリケーションへのシングルサインオンを有効にします。

シングルサインオンを有効にする前に

Windows ネットワークおよび Informatica ドメインゲートウェイノードでシングルサインオンが使用されるように設定されていることを確認します。

以下の要件を検証して、Informatica ドメインでシングルサインオンを使用できることを確認します。

必要なサービスが Windows **ネットワークでデプロイおよび設定されていることを確認します。**

シングルサインオンには以下のサービスが必要です。

- Microsoft Active Directory
- Microsoft Active Directory フェデレーションサービス 2.0

Informatica Web **アプリケーションサービスでセキュアな** HTTPS **接続が使用されることを確認します。**

デフォルトでは、AD FS には Web アプリケーション URL で HTTPS プロトコルが使用される必要があります。

AD FS **ホストと、ドメイン内のすべてのゲートウェイノードのシステムクロックが同期されていることを確認します。**

AD FS によって発行された SAML トークンの有効期間が AD FS ホストのシステムクロックに従って設定されます。AD FS ホストと、ドメイン内のすべてのゲートウェイノードのシステムクロックが同期されていることを確認します。

認証の問題を回避するために、トークンで設定された開始時間または終了時間がゲートウェイノードのシステム時間の 120 秒以内であれば、AD FS によって発行された SAML トークンの有効期間は有効となります。

手順 1. Web アプリケーションのユーザーアカウント用のセキュリティドメインの作成

SAML ベースのシングルサインオンを使用する Web アプリケーションユーザーアカウント用のセキュリティドメインを作成し、各ユーザーの LDAP アカウントを Active Directory からドメインにインポートします。

Administrator ツール、Analyst ツール、Monitoring ツールにアクセスするために SAML ベースのシングルサインオンを使用するすべてのユーザー用に、LDAP をセキュリティドメインにインポートする必要があります。アカウントをドメインにインポートしたら、適切な Informatica ドメインロール、特権、および権限を LDAP セキュリティドメイン内のアカウントに割り当てます。

1. Administrator ツールで、**[ユーザー]** タブをクリックし、**[セキュリティ]** ビューを選択します。
2. **[アクション]** メニューをクリックし、**[LDAP 設定]** を選択します。

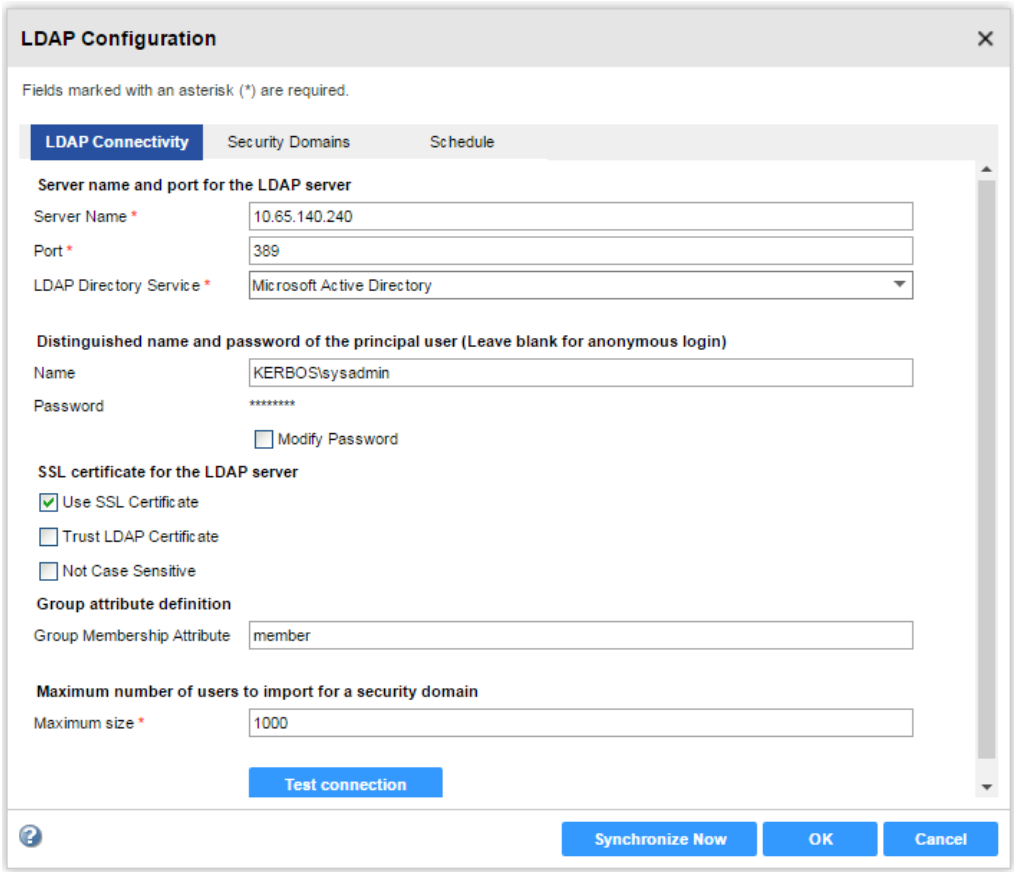
   [LDAP の設定] ダイアログボックスが開きます。
3. **[LDAP の接続方法]** タブをクリックします。
4. Active Directory サーバーの接続プロパティを設定します。

   以下の表に、サーバーの接続プロパティを示します。

プロパティ	説明
サーバー名	Active Directory サーバーのホスト名または IP アドレス。
ポート	サーバのリスニングポート。デフォルト値は 389 です。

プロパティ	説明
LDAP ディレクトリサービス	Microsoft Active Directory を選択。
名前	プリンシパル LDAP ユーザーの識別名（DN）。通常、ユーザ名は、共通名（CN）、組織（O）、および国名（C）により構成されます。Principal User の名前は、ディレクトリへのアクセス権を持つ管理ユーザです。ディレクトリサービス内の他のユーザエントリの読み取り権限を持つユーザを指定します。
パスワード	プリンシパル LDAP ユーザーのパスワード。
SSL 認証の使用	LDAP サーバーがセキュアソケットレイヤー（SSL）プロトコルを使用することを示します。 LDAP サーバーで SSL を使用する場合、Informatica ドメイン内の各ゲートウェイノード上にあるトラストファイルに証明書をインポートする必要があります。また、証明書をデフォルトの Informatica トラストストアにインポートしない場合は、INFA_TRUSTSTORE および INFA_TRUSTSTORE_PASSWORD 環境変数を設定する必要があります。
トラスト LDAP 証明書	サービスマネージャにより、LDAP サーバーの SSL 証明書が信頼できるかどうかが判断されます。 このオプションを選択する場合、サービスマネージャは、SSL 証明書を確認しないで LDAP サーバーに接続します。 このオプションを選択しない場合、サービスマネージャは、LDAP サーバーに接続する前に SSL 証明書が認証機関によって署名されていることを確認します。
大文字と小文字を区別しない	サービスマネージャでグループにユーザーを割り当てるときに識別名属性の大文字と小文字を区別しないことを示す。このオプションは有効にしてください。
グループメンバシップ属性	ユーザを削除するグループの名前。これは、グループのメンバーであるユーザおよびグループの識別名（DN）を含む LDAP グループオブジェクト内の属性です。例えば、*member* または *memberof* です。
最大サイズ	セキュリティドメインにインポートするユーザとグループの最大数。 インポートするユーザがこのプロパティ値を超えた場合、サービスマネージャによってエラーメッセージが生成され、いずれのユーザもインポートされません。インポートするユーザー数が多い場合は、このプロパティに大きい値を設定してください。 デフォルト値は 1000 です。

次の図は、**[LDAP の設定]** ダイアログボックスの［LDAP の接続方法］パネルで設定される LDAP サーバーの接続の詳細を示しています。



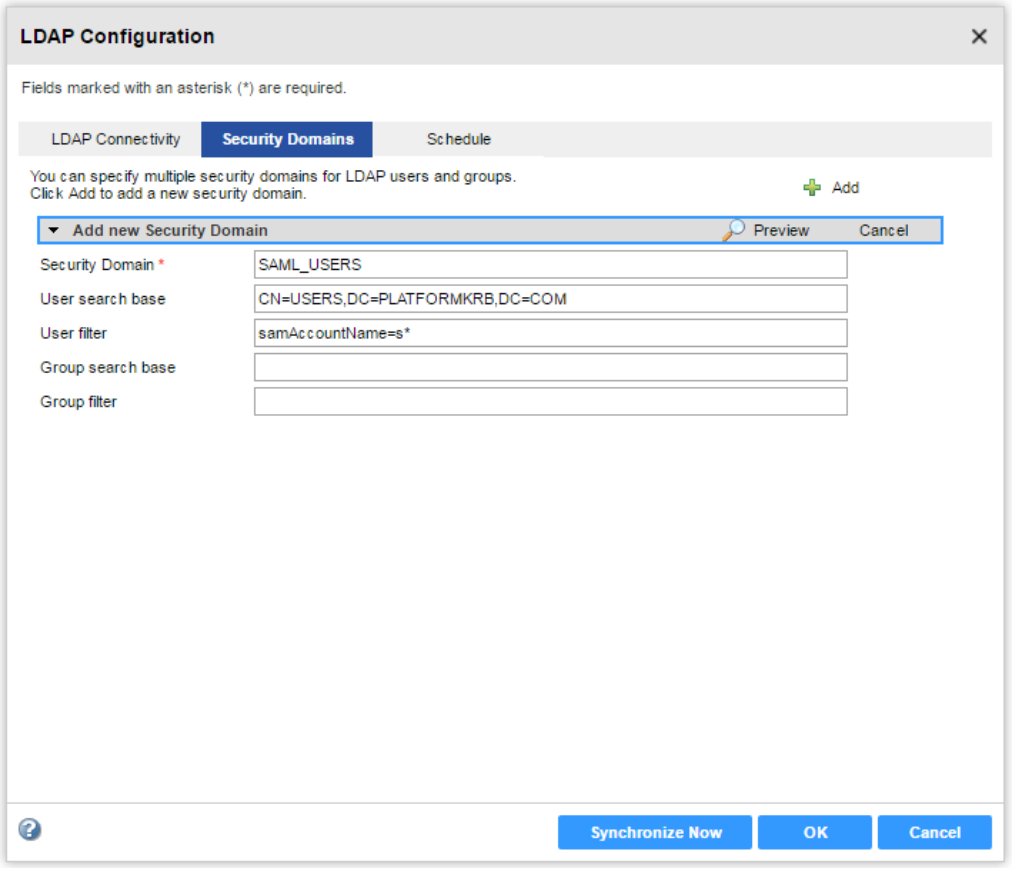
5. **［テスト接続］**をクリックし、Active Directory サーバーへの接続が有効であるか確認します。
6. **［セキュリティドメイン］**タブをクリックします。
7. **［追加］**をクリックしてセキュリティドメインを作成します。
8. セキュリティドメインプロパティを入力します。

   以下の表に、セキュリティドメインプロパティを示します。

プロパティ	説明
セキュリティドメイン	ドメインの名前。この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。名前は 128 文字以内で指定し、以下の特殊文字は使用できません。 , + / < > @ ; \ % ? 名前の最初および最後の文字以外で、ASCII のスペース文字を使用できます。その他のスペース文字は許可されません。
ユーザ検索ベース	LDAP ディレクトリサービス内のユーザ名検索の基点となるエントリの識別名（Distinguished Name：DN）。検索により、オブジェクトの識別名のパスに従ってディレクトリ内のオブジェクトが見つかります。 Active Directory では、ユーザーオブジェクトの識別名は、cn=UserName、ou=OrganizationalUnit、dc=DomainName となり、dc=DomainName により示される一連の相対識別名は、オブジェクトの DNS ドメインを識別します。

プロパティ	説明
ユーザーフィルタ	Active Directory 内のユーザー検索の条件を指定する LDAP クエリ文字列。このフィルタでは、属性タイプ、アサーション値、マッチング基準が指定できます。 Active Directory の場合、クエリ文字列を次の形式にします。 `sAMAccountName=<account>`
グループ検索ベース	Active Directory 内のグループ名検索の基点となるエントリの識別名（DN）。
グループフィルタ	ディレクトリサービス内のグループ検索の基準を指定する LDAP クエリー文字列。

次の図は、**［LDAP の設定］**ダイアログボックスの［セキュリティドメイン］パネルで設定される SAML_USERS という名前の LDAP セキュリティドメインのプロパティを示しています。ユーザーフィルタは「s」で始まるすべてのユーザーをインポートするように設定されています。



9. **［今すぐ同期］**をクリックします。

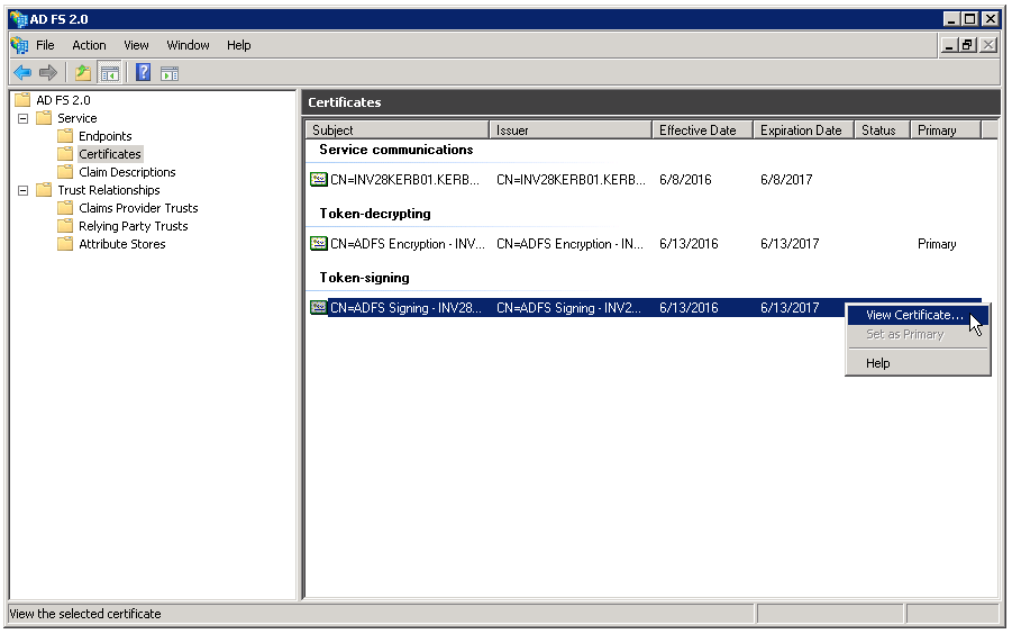
   セキュリティドメインが［ユーザー］ビューに表示されます。
10. ナビゲータでドメインを展開し、インポートされたユーザーアカウントを表示します。
11. 各 Web アプリケーションにアクセスするユーザーアカウントで適切なロール、特権、および権限を設定します。

手順 2.AD FS からの証明書のエクスポート

AD FS からのアサーション署名証明書のエクスポート。

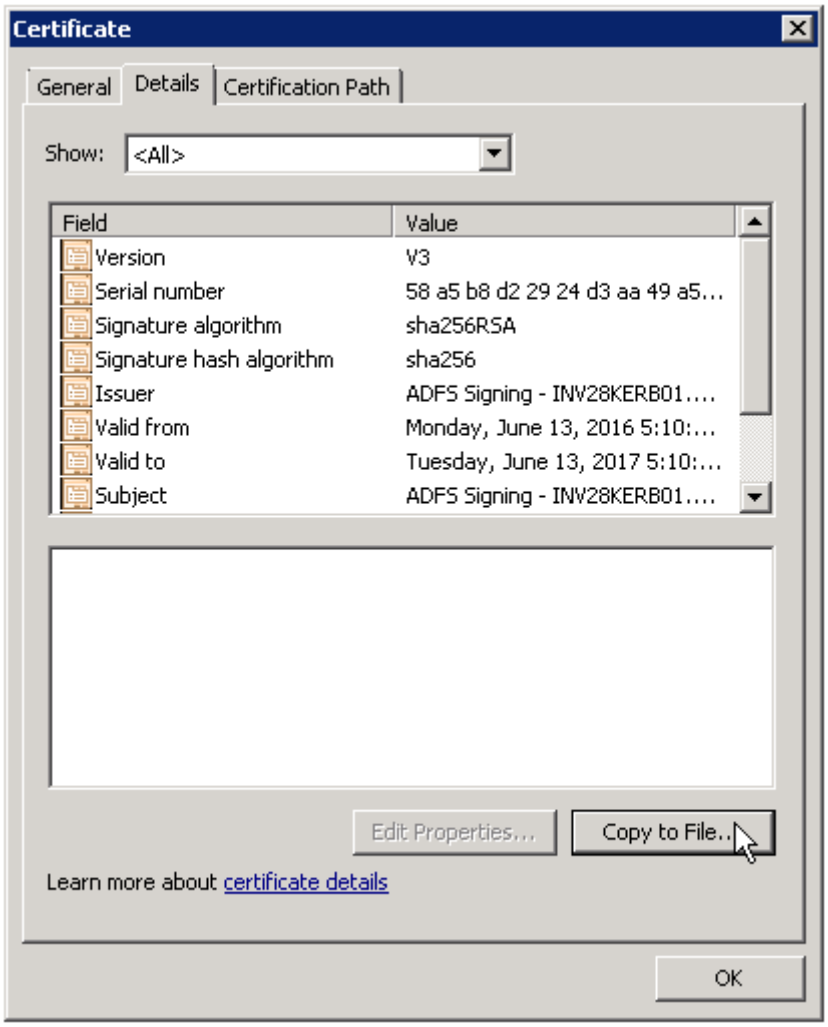
この証明書は、AD FS が Informatica Web アプリケーションに発行する SAML トークン内でアサーションに署名するために使用される標準的な X.509 証明書です。AD FS 用に自己署名 Secure Sockets Layer（SSL）を生成することも、証明機関から証明書を取得して AD FS にインポートすることもできます。

1. AD FS 管理コンソールにログインします。
2. **［サービス］** > **［証明書］**フォルダを展開します。
3. 次の図で示しているように、［証明書］ペインでトークン署名の下の証明書を右クリックし、**［証明書の表示］**を選択します。



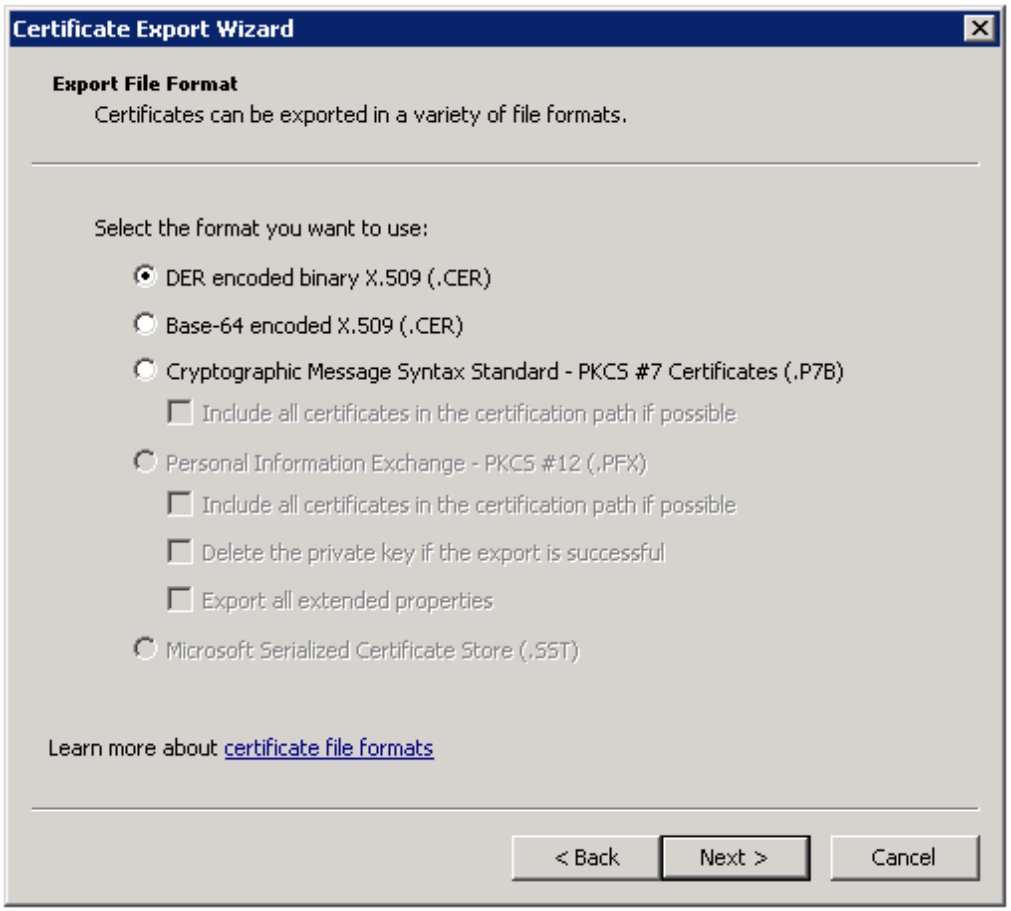
［証明書］ダイアログが表示されます。

4. 次の図で示しているように、**［詳細］**タブをクリックし、**［ファイルにコピー］**をクリックします。



[証明書のエクスポートウィザード] が表示されます。

5. 次の図で示しているように、形式として **[DER encoded binary X.509 (.CER)]** を選択します。



6. **[次へ]** をクリックします。
7. 証明書ファイル名およびエクスポート先の場所を入力し、**[次へ]** をクリックします。
8. **[OK]** をクリックし、**[完了]** をクリックしてエクスポートを完了します。

手順 3. Informatica トラストストアへの証明書のインポート

アサーション署名証明書を Informatica ドメイン内の各ゲートウェイノード上にあるデフォルトの Informatica トラストストアファイルにインポートします。

Java キーツールキーおよび証明書管理ユーティリティを使用して、証明書を Informatica トラストストアファイルにインポートします。デフォルトのトラストストアファイル infa_truststore.jks は、各ノード上の次のディレクトリにインストールされます。

```
<Informatica installation directory>\services\shared\security\
```

1. 証明書を Informatica ドメイン内のゲートウェイノード上にあるローカルフォルダにコピーします。
2. コマンドラインから、ノード上のキーツールユーティリティの場所に移動します。

   ```
   <Informatica installation directory>\java\jre\bin
   ```
3. コマンドラインから、次のコマンドを実行します。

   ```
   keytool -importcert -alias <certificate alias name> -file <certificate path>\<certificate filename> -keystore <Informatica installation directory>\services\shared\security\infa_truststore.jks -storepass <password>
   ```

   Informatica のデフォルトトラストストアのパスワードを含める必要があります。

4. ノードを再起動してください。

手順 4.Active Directory フェデレーションサービスの設定

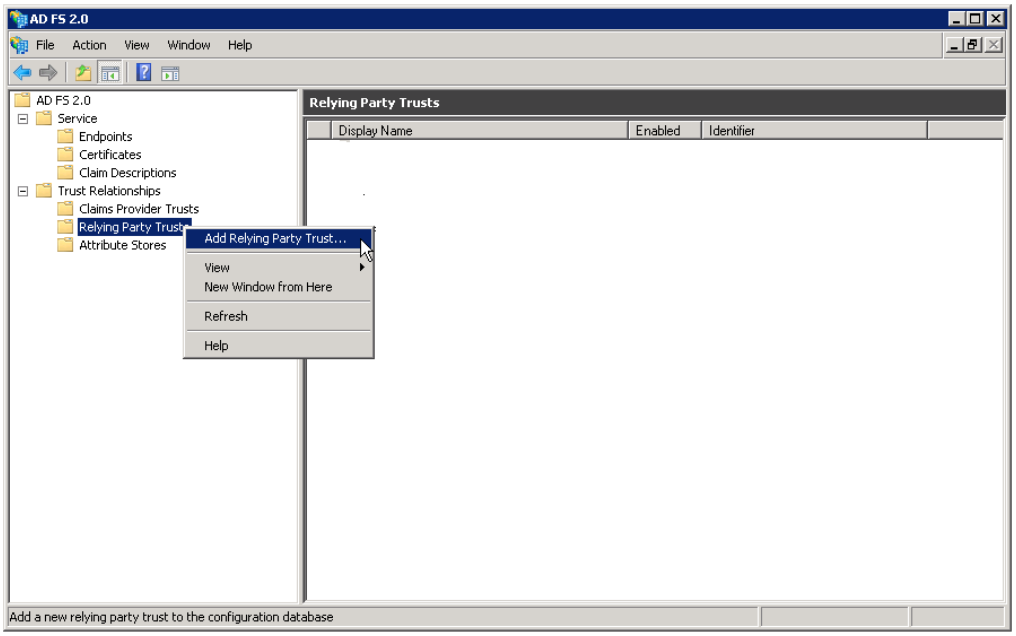
SAML トークンを Informatica Web アプリケーションに発行するように AD FS を設定します。

AD FS 管理コンソールを使用して以下のタスクを実行します。

- AD FS で Informatica を証明書利用者信頼として追加します。証明書利用者信頼の定義により、AD FS は Informatica Web アプリケーションからの認証要求を受け入れることができます。
- ID ストアの LDAP 属性を、AD FS 発行の SAML トークンで使用される対応タイプにマッピングするように、［LDAP 属性を要求として送信］規則を編集します。

注: URL を含めて、AD FS ではすべての文字列で大文字と小文字が区別されます。

1. AD FS 管理コンソールにログインします。
2. **［信頼関係］** > **［証明書利用者信頼］** フォルダを展開します。
3. 次の図で示しているように、**［証明書利用者信頼］** フォルダを右クリックし、**［証明書利用者信頼の追加］** を選択します。

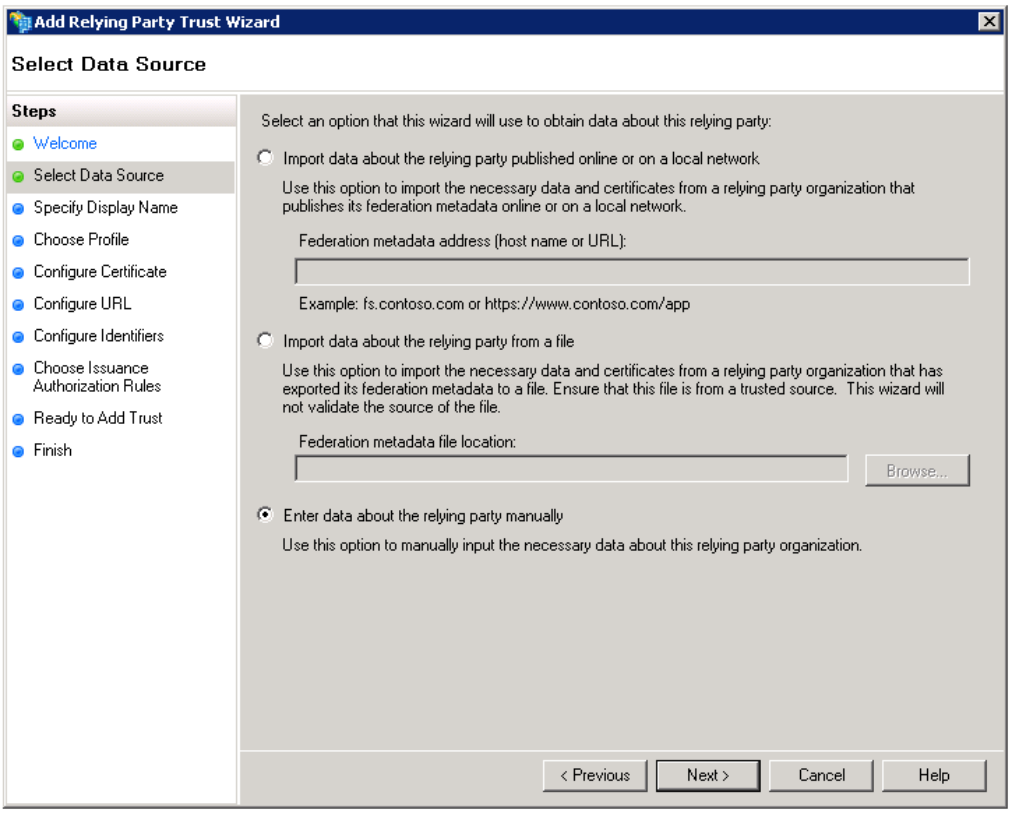


［証明書利用者信頼の追加ウィザード］ が表示されます。

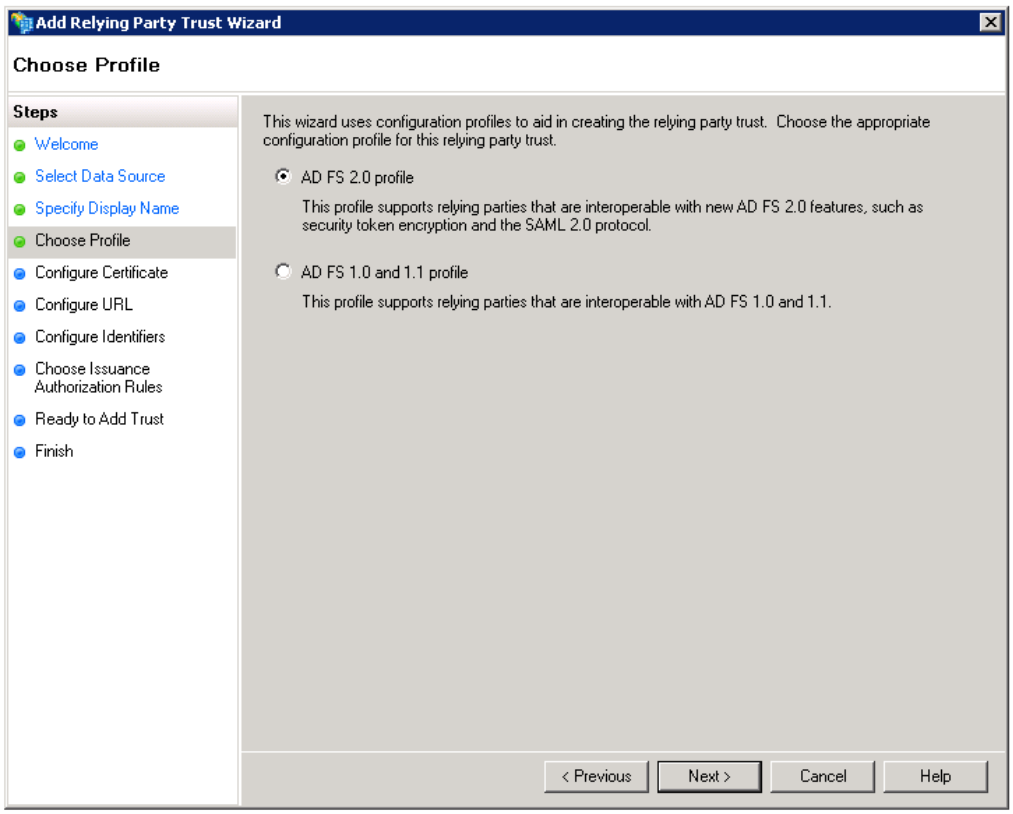
4. **［開始］** をクリックします。

   ［データソースの選択］ パネルが表示されます。

5. 次の図で示しているように、**［証明書利用者についてのデータを手動で入力する］** をクリックします。



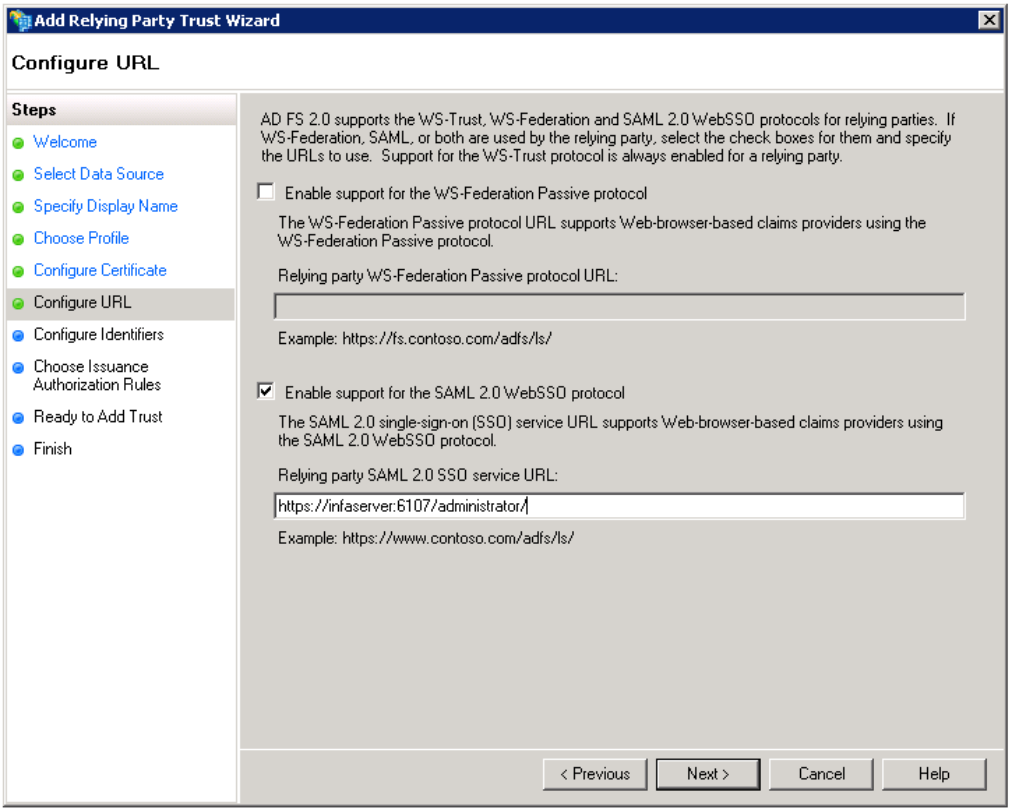
6. **[次へ]** をクリックします。
7. 表示名として「Informatica」と入力し、**[次へ]** をクリックします。
8. 次の図で示しているように、**[AD FS 2.0 プロファイル]** をクリックします。



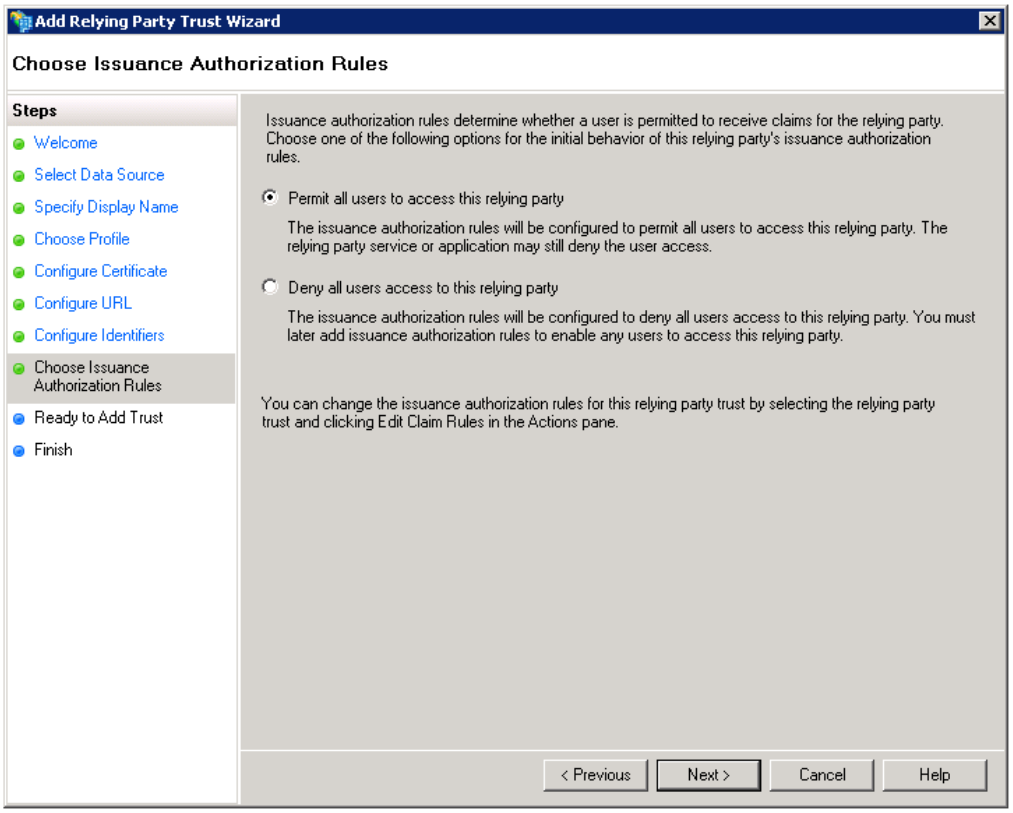
9. **[次へ]** をクリックします。

   このウィザードでは証明書設定パネルはスキップします。

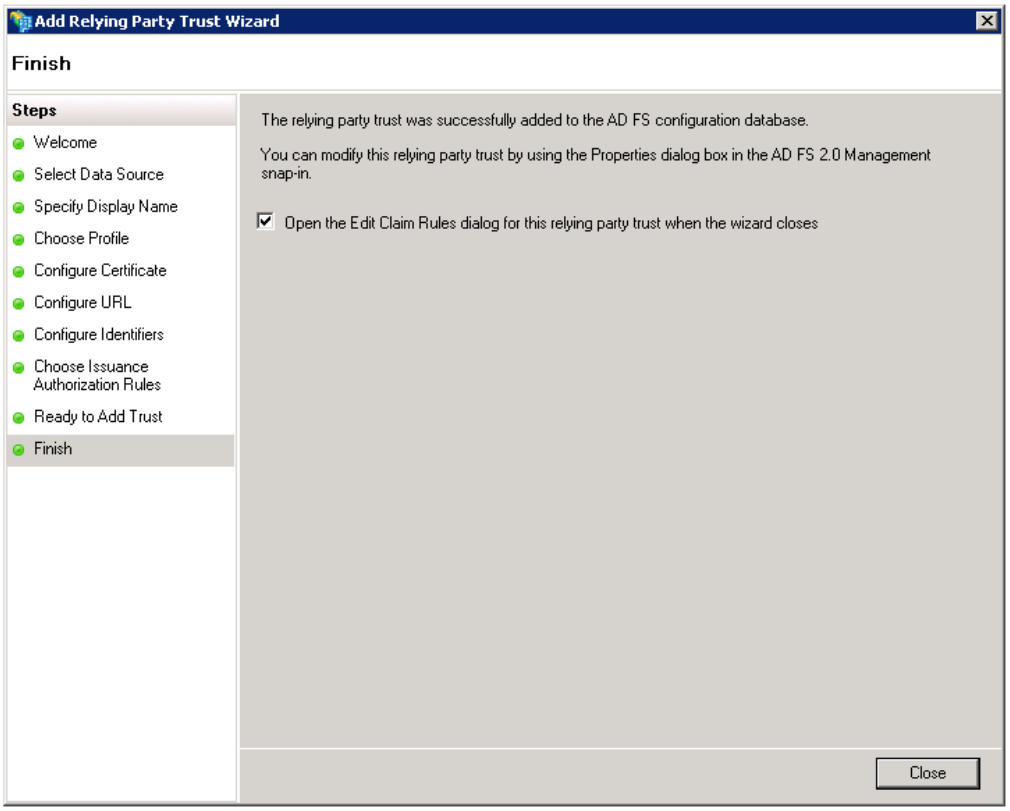
10. 次の図で示しているように、**[SAML WebSSO プロトコルのサポートを有効にする]** にチェックを入れて、Administrator ツールの完全な URL を入力します。



11. **[次へ]** をクリックします。
12. 証明書利用者信頼の ID フィールドに「Informatica」と入力します。**[追加]** をクリックし、**[次へ]** をクリックします。
13. 次の図で示しているように、**[すべてのユーザーに対して証明書利用者へのアクセスを許可する]** を選択します。



14. **[次へ]** をクリックします。
15. 次の図で示しているように、**[ウィザードの終了時にこの証明書利用者信頼の［要求規則の編集］ダイアログを開く]** にチェックを入れます。



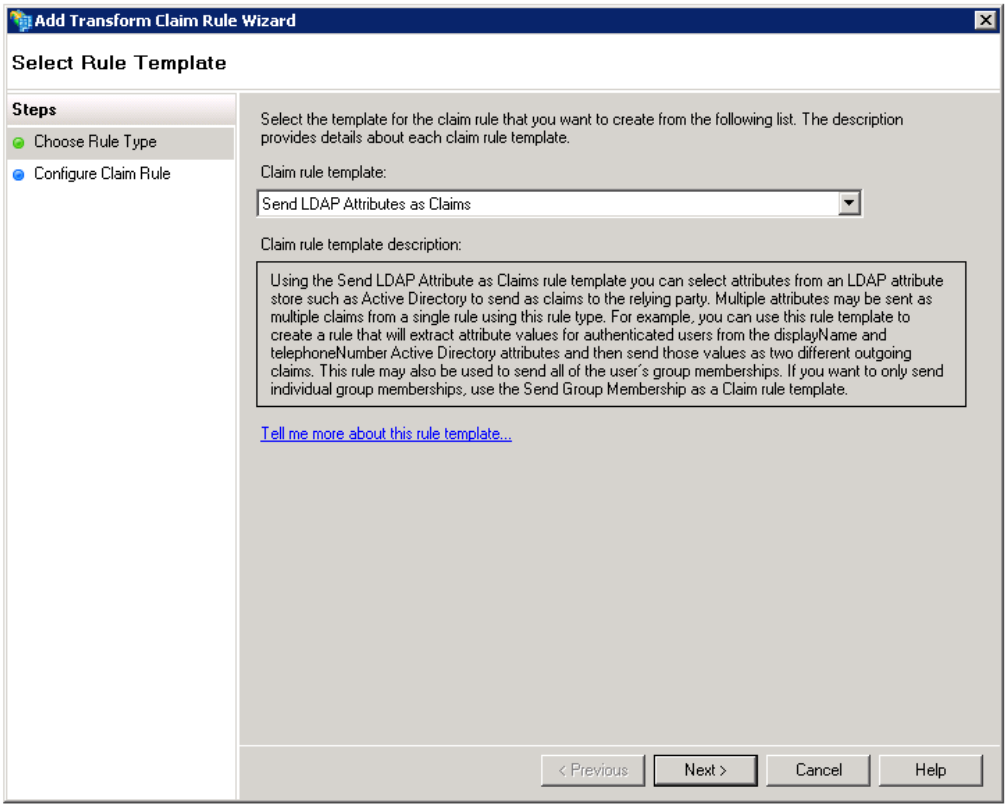
16. **[閉じる]** をクリックします。

    [Informatica の要求規則の編集] ダイアログボックスが表示されます。

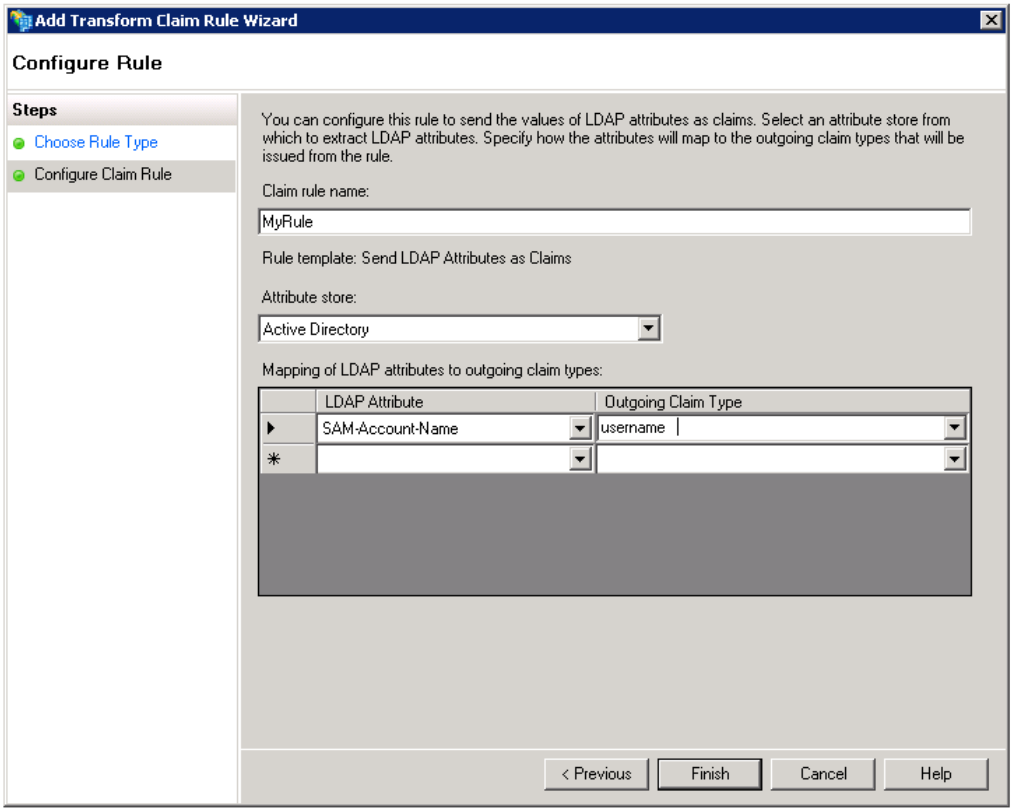
17. **[規則の追加]** をクリックします。

    [変換要求規則の追加ウィザード] が開きます。

18. 次の図で示しているように、メニューから **[LDAP 属性を要求として送信]** を選択します。



19. **[次へ]** をクリックします。
20. 下の図で示しているように、要求規則名として任意の文字列を入力します。



21. **[属性ストア]** メニューから［Active Directory］を選択します。
22. **[LDAP 属性]** メニューから［SAM-Account-Name］を選択します。
23. **[出力方向の要求の種類]** フィールドに「username」と入力します。
24. **[完了]** をクリックし、**[OK]** をクリックしてウィザードを終了します。

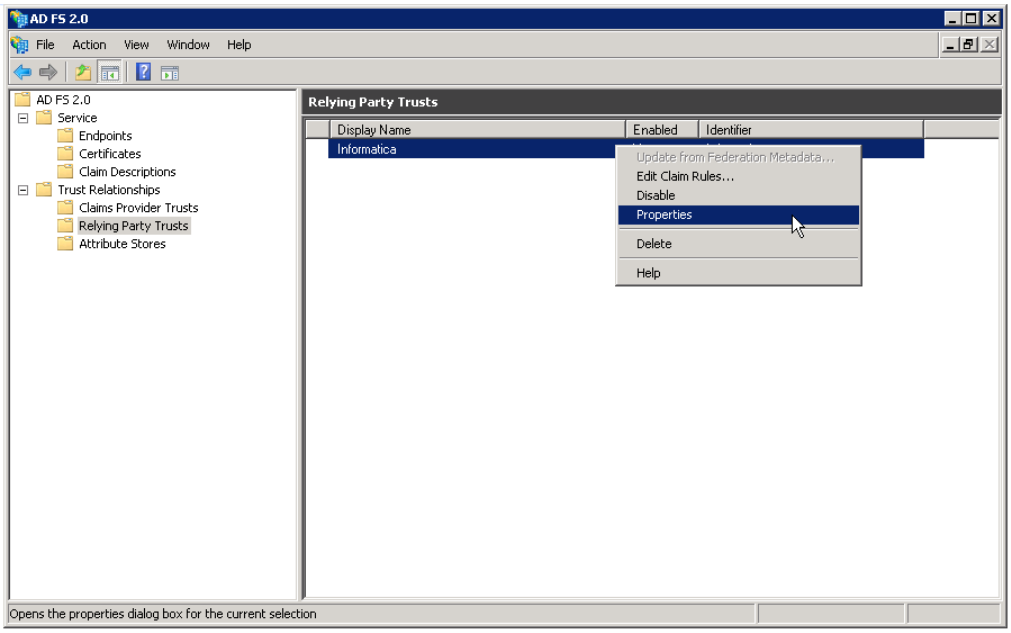
手順 5.AD FS への Informatica Web アプリケーション URL の追加

シングルサインオンを使用する各 Informatica Web アプリケーションの URL を AD FS に追加します。

Informatica Web アプリケーションの URL を入力して、AD FS がアプリケーションによって送信される認証要求を受け入れられるようにします。URL を入力すると、AD FS はユーザーの認証後に SAML トークンをアプリケーションに送信することもできます。

Administrator ツールの URL は AD FS の設定中にすでに入力しているため、追加する必要はありません。

1. AD FS 管理コンソールにログインします。
2. **[信頼関係]** > **[証明書利用者信頼]** フォルダを展開します。
3. 下の図で示しているように、**[Informatica]** エントリを右クリックし、**[プロパティ]** を選択します。

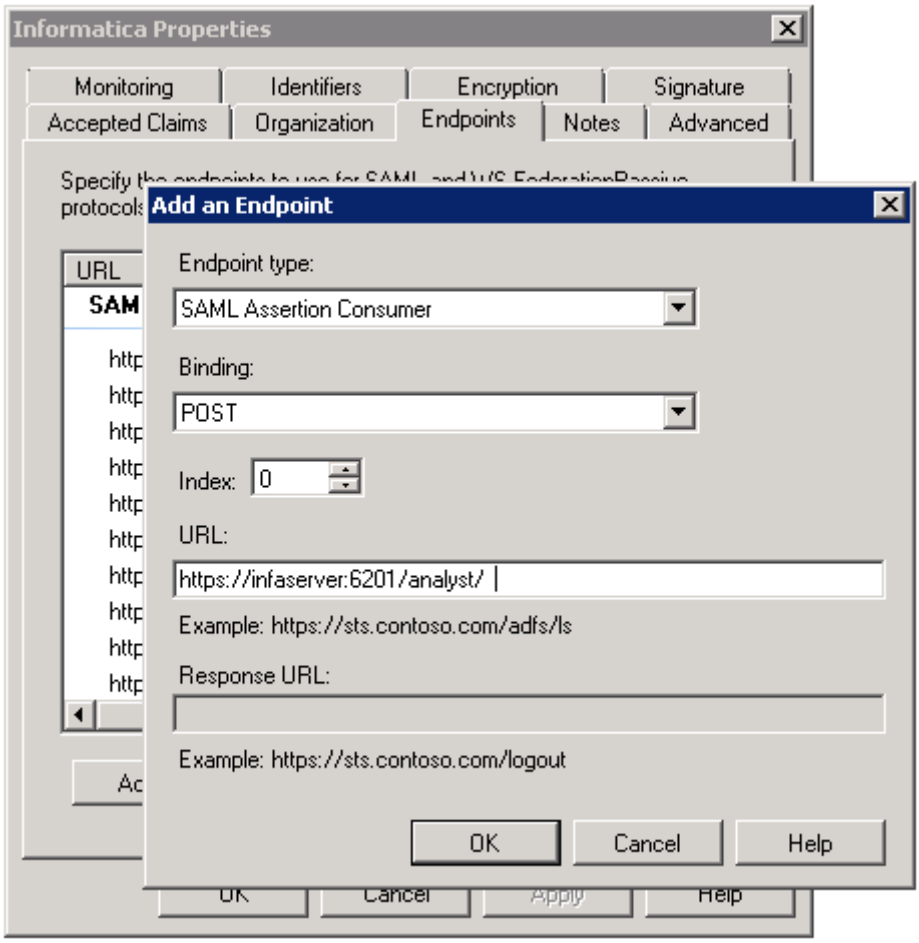


[Informatica のプロパティ] ダイアログボックスが表示されます。

4. **[エンドポイント]** タブをクリックします。

   [エンドポイントの追加] ダイアログボックスが表示されます。

5. 下の図で示しているように、**[エンドポイント]** の種類メニューから **[SAML アサーションコンシューマ]** を選択し、**[バインド]** メニューから **[POST]** を選択します。



6. サポートされる Informatica Web アプリケーションの完全な URL を入力し、**[OK]** をクリックします。

   各 Web アプリケーションでこの手順を繰り返します。

手順 6.SAML ベースのシングルサインオンの有効化

既存の Informatica ドメインで SAML ベースのシングルサインオンを有効にすることも、ドメインをインストールまたは作成するときに有効にすることもできます。

次のいずれかのオプションを選択します。

Informatica **サービスのインストール時にシングルサインオンを有効にする。**

インストールプロセス中にドメインを設定するときに SAML ベースのシングルサインオンを有効にして、ID プロバイダの URL を指定することができます。

既存のドメインでシングルサインオンを有効にする。

infasetup updateSamlConfig コマンドを使用して既存の Informatica ドメインでシングルサインオンを有効にします。ドメイン内の任意のゲートウェイノードでコマンドを実行できます。

ドメインをシャットダウンしてから、コマンドを実行します。

-iu オプションの値として ID プロバイダの URL を指定します。次の例は、コマンドの使用方法を示しています。

```
infasetup updateSamlConfig -saml true -iu https://server.company.com/adfs/ls/
```

ドメインの作成時にシングルサインオンを有効にする。

ドメインを作成するときに infasetup defineDomain コマンドを使用してシングルサインオンを有効にします。

次の例は、コマンドラインの最後の 2 つのオプションとして SAML オプションを示しています。

```
infasetup defineDomain -dn TestDomain -nn TestNode1 -na host1.company.com -cs
"jdbc:informatica:oracle://host:1521;sid=xxxx" -du test_user -dp test_user -dt oracle -rf $HOME/ISP/BIN/
nodeoptions.xml -ld $HOME/ISP/1011/source/logs -mi 10000 -ma 10200 -ad test_admin -pd test_admin -saml
true -iu https://server.company.com/adfs/ls/
```

infasetup コマンドオプション

infasetup updateSamlConfig コマンドで SAML オプションを設定して、ドメインまたはドメイン作成時に infasetup defineDomain コマンドでシングルサインオンを有効にします。

以下の表にオプションおよび引数を示します。

オプション	引数	説明
-EnableSaml -saml	true|false	必須。この値を true に設定すると、Informatica ドメイン内でサポートされている Informatica Web アプリケーションに対して SAML ベースのシングルサインオンが有効になります。 この値を false に設定すると、Informatica ドメイン内でサポートされている Informatica Web アプリケーションに対して SAML ベースの SSO が無効になります。
-IdpUrl -iu	identity_provider_url	-saml オプションが true の場合は必須。ドメインの ID プロバイダの URL を指定します。完全な URL 文字列を指定する必要があります。

infasetup updateSamlConfig コマンドおよび infasetup defineDomain コマンドを使用する手順については、『*Informatica コマンドリファレンス*』を参照してください。

ID プロバイダ URL の取得

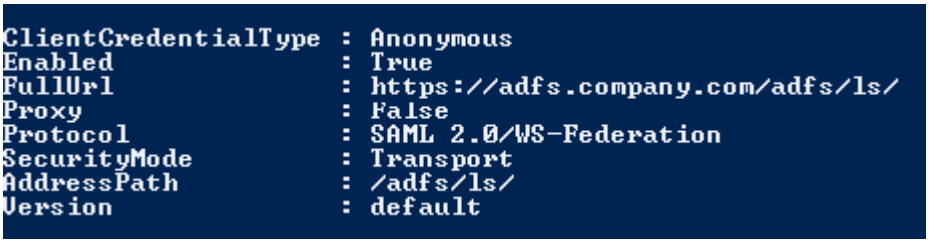
シングルサインオンを有効にするには、AD FS サーバーの SAML 2.0/WS-Federation URL を指定する必要があります。

この URL は、infasetup updateSamlConfig コマンドまたは infasetup defineDomain コマンドを実行するときに-iu オプションの値として指定します。この URL を取得するには AD FS サーバーで Windows PowerShell を使用します。

1. AD FS サーバーで Windows PowerShell コマンドプロンプトウィンドウを開きます。コマンドプロンプトを開くときに［管理者として実行］オプションを選択します。
2. Windows PowerShell コマンドプロンプトで次のコマンドを入力します。

   ```
   Get-ADFSEndpoint
   ```

3. 下の図に示すように、SAML 2.0/WS-Federation プロトコルに対して返された FullUrl 値を見つけます。



第 7 章

Informatica Administrator のセキュリティ管理

この章では、以下の項目について説明します。

Informatica Administrator の使用の概要

Informatica Administrator は、Informatica ドメインおよび Informatica セキュリティの管理に使用するツールです。

Administrator ツールを使用して、以下のタイプのタスクを実行します。

- ドメイン管理タスク。ログ、ドメインオブジェクト、ユーザー権限、およびドメインレポートを管理します。ノード診断を生成してアップロードします。データ統合サービスのジョブおよびアプリケーションを監視します。ドメインオブジェクトには、アプリケーションサービス、ノード、グリッド、フォルダ、データベース接続、オペレーティングシステムのプロファイル、およびライセンスが含まれます。
- ドメイン管理タスク。ログ、ドメインオブジェクトおよびユーザー権限を管理します。データ統合サービスのジョブおよびアプリケーションを監視します。
- ドメイン管理タスク。ログ、ドメインオブジェクトおよびユーザー権限を管理します。
- セキュリティ管理タスク。ユーザー、グループ、ロール、および特権を管理します。

注: PowerCenter Express Personal Edition の場合、セキュリティ機能にアクセスできません。

Administrator ツールには、以下のタブがあります。

- **管理**。ドメインのプロパティおよびドメイン内のオブジェクトを表示および編集します。
- **モニタ**。各データ統合サービスのプロファイルジョブ、スコアカードジョブ、プレビュージョブ、マッピングジョブ、SQL データサービス、Web サービス、およびワークフローのステータスを表示します。
- **モニタ**。各データ統合サービスのプロファイルジョブ、プレビュージョブ、マッピングジョブ、SQL データサービス、Web サービスのステータスを表示します。

- **モニタ**。データ統合サービスのプロファイルジョブ、プレビュージョブ、マッピングジョブ、およびワークフローのステータスを表示します。
- **モニタ**。Ultra Messaging デプロイメントを表示し、監視します。
- **ログ**。ドメインおよびドメイン内のサービスのログイベントを表示します。
- **レポート**。Web サービスレポートまたはライセンス管理レポートを実行します。
- **セキュリティ**。ユーザー、グループ、ロール、および特権を管理します。
- **セキュリティ**。ユーザー、グループ、ロール、および特権を管理します。PowerCenter Express Personal Edition の場合、［セキュリティ］タブへアクセスできません。
- **クラウド**。Informatica Cloud®組織に関する情報を表示します。

Administrator ツールには、以下のヘッダ項目があります。

- **ログアウト**。Administrator ツールからログアウトします。
- **管理**。アカウントを管理します。
- **ヘルプ**。現在のタブのヘルプにアクセスして、Informatica のバージョンを特定します。
- **ヘルプ**。現在のタブのヘルプにアクセスして、Informatica のバージョンを特定し、データの使用ポリシーを設定します。

ユーザーセキュリティ

サービスマネージャおよび一部のアプリケーションサービスは、アプリケーションクライアントのユーザーセキュリティを制御します。アプリケーションクライアントには、Informatica Administrator、Informatica Analyst、Informatica Developer、Metadata Manager および、PowerCenter Client が含まれます。サービスマネージャおよび一部のアプリケーションサービスは、アプリケーションクライアントのユーザーセキュリティを制御します。アプリケーションクライアントには Informatica Administrator および Informatica Developer が含まれます。サービスマネージャおよび一部のアプリケーションサービスは、アプリケーションクライアントのユーザーセキュリティを制御します。アプリケーションクライアントには Informatica Administrator が含まれます。

サービスマネージャおよびアプリケーションサービスは、次の機能を実行することによってユーザーセキュリティを制御します。

暗号化

アプリケーションクライアントにログインする際、サービスマネージャによってパスワードが暗号化されます。

認証

アプリケーションクライアントにログインする際、ユーザー名とパスワードまたはユーザー認証トークンに基づいて、サービスマネージャによってユーザーアカウントが認証されます。

認証

アプリケーションクライアント内のオブジェクトを要求すると、サービスマネージャおよび一部のアプリケーションサービスにより、特権、ロールおよび権限に基づき要求が許可されます。

ドメインおよびアプリケーションサービスへのセキュアな接続には HTTPS も使用できます。以下に示すアプリケーションサービスは、Informatica ドメインとともに HTTPS 接続を提供します。

- データ統合サービス

- アナリストサービス
- コンテンツ管理サービス
- Metadata Manager サービス
- Web Service Hub サービス

ドメインおよびアプリケーションサービスへのセキュアな接続には HTTPS も使用できます。以下に示すアプリケーションサービスは、Informatica ドメインとともに HTTPS 接続をサポートします。

- データ統合サービス
- アナリストサービス

ドメインおよびアプリケーションサービスへのセキュアな接続には HTTPS も使用できます。

暗号化

Informatica ではアプリケーションクライアントから Service Manager に送信されたパスワードが暗号化されます。 Informatica では、複数の 128 ビットキーで AES 暗号化が使用されてパスワードが暗号化され、暗号化されたパスワードがドメイン環境設定データベース内に格納されます。 アプリケーションクライアントから Service Manager に送信されるパスワードを暗号化するように HTTPS を設定します。

認証

Service Manager により、アプリケーションクライアントにログインするユーザーが認証されます。

初めてアプリケーションクライアントにログインするときには、ユーザー名、パスワードおよびセキュリティドメインを入力します。 セキュリティドメインは、Informatica ドメイン内のユーザーアカウントおよびグループのコレクションです。

選択したセキュリティドメインにより、Service Manager が使用する認証方法が決定され、ユーザーアカウントが認証されます。

- ネイティブ。アプリケーションクライアントにネイティブユーザーとしてログインする場合、Service Manager によりドメイン環境設定データベース内のユーザーアカウントに対して、ユーザーのユーザー名とパスワードが認証されます。
- Lightweight Directory Access Protocol（LDAP）。アプリケーションクライアントに LDAP ユーザーとしてログインする場合、Service Manager では認証を行うために、外部の LDAP ディレクトリサービスにユーザーのユーザー名とパスワードが渡されます。

アプリケーションクライアントにネイティブユーザーとしてログインする場合、Service Manager によりドメイン環境設定データベース内のユーザーアカウントに対して、ユーザーのユーザー名とパスワードが認証されます。

アプリケーションクライアントにネイティブユーザーとしてログインする場合、Service Manager によりドメイン環境設定データベース内のユーザーアカウントに対して、ユーザーのユーザー名とパスワードが認証されます。

シングルサインイン

アプリケーションクライアントにログインすると、Service Manager によって、別のアプリケーションクライアントの起動、またはアプリケーションクライアント内の複数のリポジトリへのアクセスが許可されます。 追加のアプリケーションクライアントやリポジトリにログインする必要はありません。

Service Manager により初めてユーザーアカウントが認証されるときに、そのユーザーアカウントに対して暗号化された認証トークンが作成され、その認証トークンがアプリケーションクライアントに返されます。 ユーザー名とパスワードを入力します。Service Manager は、認証トークンを有効期限まで定期的に更新します。

アプリケーションクライアント内の複数のリポジトリにアクセスする際、アプリケーションクライアントによってユーザー認証のために認証トークンが Service Manager に送信されます。

Web アプリケーションのクライアントを別のアプリケーションから起動する際に、アプリケーションクライアントにより、認証トークンが次のアプリケーションクライアントに渡されます。 次の Web アプリケーションクライアントによって、ユーザー認証のために認証トークンがサービスマネージャに送信されます。各 Web アプリケーションクライアントは別々にログアウトする必要があります。 例えば、Administrator ツールから Analyst ツールを開いた場合は、Analyst ツールと Administrator ツールを別々にログアウトする必要があります。

注: Administrator ツール、Analyst ツール、および Monitoring ツールの間でシングルサインオンを使用するには、すべてのノードのホストファイルにそれらの完全修飾ドメイン名を追加する必要があります。

シングルサインオンを使用して、クライアントツールから Web アプリケーションクライアントに接続することはできません。 例えば、Developer tool から Administrator ツールを起動する場合は、Administrator ツールにログインする必要があります。

承認

サービスマネージャにより、ドメインオブジェクトのユーザー要求が許可されます。要求は Administrator ツールから送信されます。 以下のアプリケーションサービスにより、他のオブジェクトへのユーザー要求が認証されます。

- データ統合サービス
- Metadata Manager サービス
- モデルリポジトリサービス
- PowerCenter リポジトリサービス

サービスマネージャにより、ドメインオブジェクトのユーザー要求が許可されます。要求は Administrator ツールから送信されます。以下のアプリケーションサービスにより、他のオブジェクトへのユーザー要求が認証されます。

- データ統合サービス
- モデルリポジトリサービス

ネイティブユーザーとグループを作成、および LDAP ユーザーとグループをインポートした場合、サービスマネージャにより、ドメイン環境設定データベース内の情報は以下のリポジトリに格納されます。

- モデルリポジトリ
- PowerCenter リポジトリ
- Metadata Manager の PowerCenter リポジトリ

以下のようなイベントが発生した場合、サービスマネージャは、リポジトリとドメイン環境設定データベース間のユーザーおよびグループ情報を同期します。

- Metadata Manager サービス、モデルリポジトリサービス、または PowerCenter リポジトリサービスを再起動します。
- ネイティブユーザーまたはグループを、追加または削除する。
- サービスマネージャにより、ドメイン環境設定データベース内の LDAP ユーザーおよびグループのリストが、LDAP ディレクトリサービス内のユーザーのおよびグループのリストとともに同期される。

以下のようなイベントが発生した場合、サービスマネージャは、リポジトリとドメイン環境設定データベース間のユーザーおよびグループ情報を同期します。

- モデルリポジトリサービスを再起動する。

- ネイティブユーザーまたはグループを、追加または削除する。

アプリケーションクライアントのユーザーとグループに権限を割り当てる場合、アプリケーションサービスにより、権限の割り当てが、アプリケーションリポジトリ内のユーザーおよびグループの情報とともに格納されます。

アプリケーションクライアントのオブジェクトを要求した場合、適切なアプリケーションサービスにより、その要求が許可されます。 例えば、Informatica Developer 内のプロジェクトを編集しようとした場合、ユーザーの特権、ロール、権限の割り当てに基づいてモデルリポジトリサービスにより要求が許可されます。

［セキュリティ］タブ

Administrator ツールの［セキュリティ］タブで、Informatica セキュリティを管理します。

［セキュリティ］タブには以下のコンポーネントがあります。

- ［検索］セクション。ユーザー、グループ、またはロールを名前で検索します。
- ナビゲータ。 左側のペインにナビゲータが表示され、グループ、ユーザー、およびロールが示されます。
- コンテンツパネル。 コンテンツパネルには、ナビゲータで選択されたオブジェクトとコンテンツパネルで選択されたタブに基づいて、プロパティおよびオプションが表示されます。
- ［セキュリティアクション］メニュー。グループ、ユーザー、またはロールを作成または削除するためのオプションが含まれます。 LDAP およびオペレーティングシステムのプロファイルを管理できます。 サービスに関する権限を持つユーザーを表示することもできます。

注: PowerCenter Express Personal Edition がある場合、セキュリティタブへのアクセスがありません。

［検索］セクションの使用

［検索］セクションを使用して、ユーザー、グループ、およびロールを名前で検索します。検索では、大文字小文字は区別されません。

1. ［検索］セクションで、ユーザー、グループ、またはロールを検索するかどうかを選択します。
2. 検索対象の名前または名前の一部を入力してください。

   アスタリスク（*）を名前に使用して、検索のワイルドカードとして使用できます。たとえば、“ad*”を入力すると、先頭が“ad”のすべてのオブジェクトを検索します。“*ad”を入力すると、末尾が“ad”のすべてのオブジェクトを検索します。
3. ［移動］をクリックします。

   ［検索結果］セクションが表示され、最大 100 個のオブジェクトが示されます。検索によって 100 個以上のオブジェクトが返された場合は、検索基準を狭めて検索結果を絞ります。
4. ［検索結果］セクションでオブジェクトを選択して、コンテンツパネルにオブジェクトに関する情報を表示します。

セキュリティナビゲータの使用

ナビゲータは、［セキュリティ］タブのコンテンツパネルに表示されます。 ナビゲータでオブジェクトを選択する場合、コンテンツパネルにオブジェクトに関する情報が表示されます。

ナビゲータは、ユーザーが何を表示しているかに基づいて、セキュリティタブに以下のいずれかのセクションを表示します。

- ［グループ］セクショングループを選択して、グループのプロパティ、グループに割り当てられたユーザー、グループに割り当てられたロールおよび特権を表示します。
- ［ユーザー］セクションユーザーを選択して、ユーザーのプロパティ、ユーザーが属するグループ、ユーザーに割り当てられたロールおよび特権を表示します。
- ［ロール］セクションロールを選択して、ロールのプロパティ、ロールが割り当てられたユーザーおよびグループ、ロールに割り当てられた特権を表示します。

作業を実行するために、ナビゲータにはさまざまな方法があります。次のいずれかの方法を使用して、グループ、ユーザー、およびロールを管理できます。

- ［アクション］メニューをクリックします。ナビゲータの各セクションには、グループ、ユーザー、またはロールを管理するための［アクション］メニューが含まれます。ナビゲータでオブジェクトを選択し、［アクション］メニューをクリックして、グループ、ユーザー、またはロールを作成、削除、または移動します。
- オブジェクトを右クリックします。ナビゲータでオブジェクトを右クリックすると、［アクション］メニューに選択可能な作成、削除、および移動オプションが表示されます。
- キーボードショートカットを使用します。キーボードショートカットを使用して、ナビゲータの異なるセクションに移動します。

グループ

グループは、同じ特権、ロール、および権限を持つユーザーおよびグループのコレクションです。

ナビゲータのグループセクションにより、グループがセキュリティドメインフォルダに整理されます。セキュリティドメインは、Informatica ドメイン内のユーザーアカウントおよびグループのコレクションです。ネイティブ認証では、Administrator ツールで作成および管理されるユーザーとグループを含むネイティブセキュリティドメインが使用されます。LDAP 認証では、LDAP ディレクトリサービスからインポートされるユーザーおよびグループを含む LDAP セキュリティドメインが使用されます。

ナビゲータのグループセクションにより、グループがセキュリティドメインフォルダに整理されます。セキュリティドメインは、Informatica ドメイン内のユーザーアカウントおよびグループのコレクションです。ネイティブ認証では、Administrator ツールで作成および管理されるユーザーとグループを含むネイティブセキュリティドメインが使用されます。

ナビゲータのグループセクションにより、グループがセキュリティドメインフォルダに整理されます。セキュリティドメインは、Informatica ドメイン内のユーザーアカウントおよびグループのコレクションです。ネイティブ認証では、Administrator ツールで作成および管理されるユーザーとグループを含むネイティブセキュリティドメインが使用されます。

ナビゲータのグループセクションでセキュリティドメインフォルダを選択する場合、セキュリティドメインに属するすべてのグループがコンテンツパネルに表示されます。 グループを右クリックして［アイテムにナビゲート］を選択し、グループの詳細をコンテンツパネルに表示します。

ナビゲータでグループを選択した場合、コンテンツパネルに以下のタブが表示されます。

- 概要。 グループに割り当てられたグループおよびユーザーの一般的なプロパティを表示します。
- 特権。ドメインのためのグループ、およびドメインのアプリケーションサービスのためのグループに割り当てられた特権とロールを表示します。

ユーザー

Informatica ドメインにアカウントを持つユーザーは、以下のアプリケーションクライアントにログインできます。

- Informatica Administrator
- PowerCenter Client
- Metadata Manager
- Informatica Developer
- Informatica Analyst

Informatica ドメインにアカウントを持つユーザーは、以下のアプリケーションクライアントにログインできます。

- Informatica Administrator
- Informatica Developer

Informatica ドメインにアカウントを持つユーザーは、Informatica Administrator にログインできます。

ナビゲータのユーザーセクションにより、ユーザーがセキュリティドメインフォルダに整理されます。セキュリティドメインは、Informatica ドメイン内のユーザーアカウントおよびグループのコレクションです。 ネイティブ認証では、Administrator ツールで作成および管理されるユーザーとグループを含むネイティブセキュリティドメインが使用されます。LDAP 認証では、LDAP ディレクトリサービスからインポートされるユーザーおよびグループを含む LDAP セキュリティドメインが使用されます。

ナビゲータのユーザーセクションにより、ユーザーがセキュリティドメインフォルダに整理されます。セキュリティドメインは、Informatica ドメイン内のユーザーアカウントおよびグループのコレクションです。

ナビゲータのユーザーセクションにより、ユーザーがセキュリティドメインフォルダに整理されます。セキュリティドメインは、Informatica ドメイン内のユーザーアカウントおよびグループのコレクションです。

ナビゲータのユーザーセクションでセキュリティドメインを選択する場合、コンテンツパネルにセキュリティドメインに属するすべてのユーザーが表示されます。 ユーザーを右クリックして［アイテムにナビゲート］を選択し、ユーザーの詳細をコンテンツパネルに表示します。

ナビゲータでユーザーを選択した場合、コンテンツパネルに以下のタブが表示されます。

- 概要。 ユーザーおよびユーザーが属するすべてのグループの全般的なプロパティを表示します。
- 特権。ドメインのためのユーザー、およびドメインのアプリケーションサービスのためのユーザーに割り当てられた特権とロールを表示します。

ロール

ロールとは、ユーザーまたはグループに割り当てる特権の集合です。ユーザーが実行できるアクションは、特権によって決定されます。 ドメインのためのユーザーとグループ、およびドメイン内のアプリケーションサービスのためのユーザーとグループにロールを割り当てます。

ナビゲータのロールセクションにより、ロールが以下のフォルダに整理されます。

- システム定義のロール。編集または削除できないロールを含みます。管理者ロールは、システム定義のロールです。
- カスタムロール。作成、編集、および削除できるロールを含みます。Administrator ツールには、編集してユーザーおよびグループに割り当てることができる一部のカスタムロールが含まれます。

ナビゲータのロールセクションでフォルダを選択する場合、コンテンツパネルにそのフォルダに属するすべてのロールが表示されます。 ロールを右クリックして［アイテムにナビゲート］を選択し、ロールの詳細をコンテンツパネルに表示します。

ナビゲータでロールを選択した場合、コンテンツパネルに以下のタブが表示されます。

- 概要。 ロールの全般的なプロパティ、およびドメインとアプリケーションサービスに対してロールが割り当てられたユーザーとグループを表示します。
- 特権。ドメインおよびアプリケーションサービスのためのロールに割り当てられた特権を表示します。

パスワード管理

パスワードは、Change Password アプリケーションを使用して変更できます。

Change Password アプリケーションは、Administrator ツールから開くことも、URL: `http://<fully qualified host name>:<port>/passwordchange/`を使用して開くこともできます。

Service Manager は、作業ノードに関連付けられたユーザーパスワードを使用してドメインユーザーを認証します。1 つ以上の作業ノードに関連付けられたユーザーパスワードを変更すると、Service Manager により各作業ノードのパスワードが更新されます。Service Manager では、実行中でないノードを更新できません。実行中でないノードについては、Service Manager はノードが再起動されるときにパスワードを更新します。

注: LDAP ユーザーアカウントの場合は、LDAP ディレクトリサービスでパスワードを変更します。

パスワードの変更

ネイティブユーザーアカウントのパスワードは、いつでも変更できます。 他のユーザーによって作成されたユーザーアカウントの場合は、Administrator ツールに初めてログインするときにパスワードを変更します。

1. Administrator ツールのヘッダー領域で、**［管理］** > **［パスワードの変更］**をクリックします。
   パスワードの変更アプリケーションによって、新しいブラウザウィンドウが開きます。
2. **［パスワード］**ボックスに現在のパスワードを、**［新しいパスワード］**と**［パスワードの確認］**ボックスに新しいパスワードを入力します。
3. **［更新］**をクリックします。

ドメインのセキュリティ管理

Secure Sockets Layer（SSL）プロトコルまたは Transport Layer Security（TLS）プロトコルを使用して他のコンポーネントとの接続を暗号化するように、Informatica ドメインコンポーネントを設定することができます。 ドメインコンポーネントに対して SSL または TLS を有効にすると、安全な通信が確保されます。

安全な通信は以下の範囲で設定できます。

ドメイン内のサービス間

ドメイン内でサービス間の安全な通信を設定できます。

ドメインと外部コンポーネントの間

Informatica ドメインコンポーネントと Web ブラウザまたは Web サービスクライアントの間に、安全な通信を設定できます。

安全な通信を設定する方法は、それぞれ互いに独立しています。 1 つのコンポーネントセットに安全な通信を設定したら、他のセットに安全な通信を設定する必要はありません。

注: セキュアなドメインを非セキュアなドメインに、または非セキュアなドメインをセキュアなドメインに変更する場合は、Developer ツールと PowerCenter Client ツールでドメイン設定を削除し、クライアントでドメインをもう一度設定する必要があります。

ユーザーのセキュリティ管理

ドメイン内のユーザーセキュリティは、特権および権限を使用して管理します。

ドメインオブジェクトに対してユーザーが実行できるアクションは、特権に応じて決定されます。 ドメインオブジェクトに対するユーザーのアクセスレベルは、権限によって定義されます。ドメインオブジェクトには、ドメイン、フォルダ、ノード、グリッド、ライセンス、データベース接続、オペレーティングシステムのプロファイル、およびアプリケーションサービスが含まれます。

ドメインオブジェクトに対してユーザーが実行できるアクションは、特権に応じて決定されます。 ドメインオブジェクトに対するユーザーのアクセスレベルは、権限によって定義されます。ドメインオブジェクトには、ドメイン、ノード、ライセンス、データベース接続、およびアプリケーションサービスが含まれます。

ユーザーが特定のアクションを完了するドメイン特権を持っていても、特定のオブジェクトに対してそのアクションを完了する権限が必要とされる場合もあります。例えば、ユーザーにアプリケーションサービス編集権限を付与する Manage Services ドメイン特権があるとします。ただし、そのユーザーにはアプリケーションサービスに対する権限も必要です。Manage Services のドメイン特権および、Development Repository Service に対する権限はあっても、Production Repository Service に対する権限のないユーザーは、Development Repository Service の編集はできますが、Production Repository Service の編集はできません。

ユーザーが特定のアクションを完了するドメイン特権を持っていても、特定のオブジェクトに対してそのアクションを完了する権限が必要とされる場合もあります。

Administrator ツールにログインするには、Access Informatica Administrator ドメイン特権が必要です。ユーザーは、あるオブジェクトに対する Access Informatica Administrator 特権および権限を持っていても、そのオブジェクトタイプの変更機能を付与するドメイン特権を持っていない場合は、そのオブジェクトを表示することができます。 例えば、ユーザーがあるノードに対する権限を持っていても、ノードおよびグリッド管理の特権を持っていなければ、ノードのプロパティは表示できますが、ノードの設定、シャットダウン、削除を行なうことはできません。

Administrator ツールにログインするには、Access Informatica Administrator ドメイン特権が必要です。ユーザーは、あるオブジェクトに対する Access Informatica Administrator 特権および権限を持っていても、そのオブジェクトタイプの変更機能を付与するドメイン特権を持っていない場合は、そのオブジェクトを表示することができます。

ユーザーがナビゲータで選択されたオブジェクトに対する権限がない場合、オブジェクトに対する権限が拒否されたことを示すメッセージがコンテンツパネルに表示されます。

第 8 章

ユーザーおよびグループ

この章では、以下の項目について説明します。

ユーザーおよびグループの概要ユーザーとグループ

Informatica ドメインでアプリケーションサービスとオブジェクトにアクセスしたり、アプリケーションクライアントを使用したりするには、ユーザーアカウントが必要になります。 実行可能なタスクはユーザーアカウントのタイプおよび PowerCenter Express のライセンスのタイプに依存します。

Informatica ドメインでアプリケーションサービスとオブジェクトにアクセスしたり、アプリケーションクライアントを使用したりするには、ユーザーアカウントが必要になります。

インストール時に、デフォルトの管理者ユーザーアカウントが作成されます。 デフォルトの管理者アカウントを使用して Informatica ドメインにログインし、アプリケーションサービス、ドメインオブジェクト、およびその他のユーザーアカウントを管理します。 インストール後に Informatica ドメインにログインする際に、パスワードを変更して Informatica ドメインとアプリケーションのセキュリティを確保します。

注: PowerCenter Express Personal Edition をインストールする場合、すべての処理にデフォルトの管理者アカウントを使用する必要があります。ユーザーやグループを作成したり権限を管理することはできません。

Informatica でのユーザーアカウント管理には、以下のキーコンポーネントが関係しています。

- ユーザー Informatica ドメインでは、さまざまなタイプのユーザーアカウントを設定できます。ユーザーは自分に割り当てられたロール、特権および権限に応じてタスクを実行することができます。
- 認証。ユーザーがアプリケーションクライアントにログインする際、サービスマネージャは Informatica ドメイン内のユーザーアカウントを認証して、ユーザーがアプリケーションクライアントを使用可能であることを確認します。 Informatica ドメインは、ネイティブまたは LDAP 認証を使用してユーザーを認証できます。 サービスマネージャにより、ユーザーアカウントおよびグループはセキュリティドメイン別に整理されます。ユーザーが属しているセキュリティドメインに基づき認証されます。

- 認証。ユーザーがアプリケーションクライアントにログインする際、サービスマネージャは Informatica ドメイン内のユーザーアカウントを認証して、ユーザーがアプリケーションクライアントを使用可能であることを確認します。
- 認証。ユーザーがアプリケーションクライアントにログインする際、サービスマネージャは Informatica ドメイン内のユーザーアカウントを認証して、ユーザーがアプリケーションクライアントを使用可能であることを確認します。
- グループ。ただし、ユーザーのグループをセットアップし、異なるロール、特権や権限を各グループに割り当てることもできます。Informatica ドメインでそのグループのユーザーが実行できるタスクは、グループに割り当てられたロール、特権、および権限によって決定されます。
- 特権とロール。特権により、ユーザーがアプリケーションクライアントで実行できるアクションが決定されます。 ロールとは、ユーザーおよびグループへの割り当ての可能な特権の集まりです。ドメインのユーザーおよびグループ、ドメイン内のアプリケーションサービスのユーザーおよびグループにロールまたは特権を割り当てます。
- オペレーティングシステムプロファイル。統合サービスを UNIX または Linux 上で実行する場合は、オペレーティングシステムのプロファイルを使用するように統合サービスを設定できます。オペレーティングシステムのプロファイルを使用して、セキュリティの向上やユーザーのランタイム環境の切り離しを行うことができます。Administrator ツールの［セキュリティ］タブで、オペレーティングシステムプロファイルを作成および管理できます。
- アカウントロックアウト。 アカウントロックを設定し、ユーザーが Administrator ツールやその他のアプリケーションクライアント（Developer tool および Analyst ツールなど）で間違ったログイン情報を指定した場合、そのユーザーのアカウントをロックできます。 ユーザーアカウントのロックを解除することもできます。
- アカウントロックアウト。アカウントロックアウトを設定し、ユーザーが Administrator ツールまたは Developer tool で正しくないログイン情報を指定した場合、そのユーザーのアカウントをロックできます。ユーザーアカウントのロックを解除することもできます。
- アカウントロックアウト。ユーザーが Administrator ツールで正しくないログイン情報を指定した場合、そのユーザーのアカウントをロックするようアカウントロックアウトを設定することができます。ユーザーアカウントのロックを解除することもできます。

デフォルトグループ

Informatica ドメインには、インストール時に作成された一連のユーザーグループがあります。

デフォルトでは、インストール後の Informatica ドメインに次のユーザーグループがあります。

- 管理者
- エブリワン
- オペレータ

管理者グループ

Informatica ドメインには、「管理者」という名前の付いたデフォルトのグループが含まれています。インストール中に作成されたデフォルトの管理者アカウントは、このグループに属します。

管理者グループには、ドメインおよびすべてのアプリケーションサービスに対し管理者の権限と特権があります。管理者グループに対してユーザーの追加や削除を行うことができます。管理者グループ内のすべてのユーザーに、インストール中に作成されたデフォルトの管理者と同じ権限および特権が与えられます。

デフォルト管理者アカウントを管理者グループから削除することも、管理者グループを削除することもできません。

エブリワングループ

Informatica ドメインには、「エブリワン」という名前の付いたデフォルトのグループが含まれています。ドメイン内のすべてのユーザーがこのグループに属します。

デフォルトでは、エブリワングループは特権を持ちません。特権、ロール、権限をエブリワングループに割り当てることで、すべてのユーザーに同じアクセス権を付与することができます。

エブリワングループに対して以下のタスクを実行することはできません。

- エブリワングループの編集または削除。
- エブリワングループからのユーザーの追加または削除。
- エブリワングループへのグループの移動。

オペレータグループ

Informatica ドメインには、「オペレータ」という名前の付いたデフォルトのグループが含まれています。

デフォルトでは、オペレータグループにはドメイン内のすべてのオブジェクトに対する権限があります。オペレータロールをオペレータグループに割り当てて、ドメインのオペレータユーザーを管理するために使用できます。

オペレータグループに対して次のタスクを実行できます。

- グループへの特権とロールの割り当て。
- グループからのユーザーの追加または削除。
- グループへのグループの移動。
- グループの編集または削除。

ユーザーアカウントについて

Informatica ドメインには、次のタイプのアカウントがあります。

- デフォルト管理者
- ドメイン管理者
- アプリケーションクライアントの管理者
- ユーザー

Informatica ドメインには、次のタイプのアカウントがあります。

- デフォルト管理者
- ドメイン管理者
- アプリケーションクライアントの管理者
- ユーザー

Informatica ドメインには、デフォルトの管理者アカウントがあります。

デフォルト管理者

Informatica Services をインストールする場合、インストーラによって、ユーザーが提供したユーザー名、およびパスワードでデフォルト管理者が作成されます。 デフォルト管理者アカウントを利用して、最初に Administrator ツールにログインすることができます。

デフォルト管理者にはドメインおよびすべてのアプリケーションサービスの管理者権限および特権があります。

デフォルト管理者が実行可能な作業は以下のとおりです。

- ノード、アプリケーションサービス、管理者およびユーザーアカウントなど、ドメイン内のすべてのオブジェクトを作成、設定、および管理します。
- 他のドメイン管理者およびアプリケーションクライアントの管理者によって作成された、すべてのオブジェクトおよびユーザーアカウントを設定して管理します。
- アプリケーションクライアントにログインします。

ドメイン内の管理者アカウントのユーザー名です。デフォルトの管理者を作成することはできません。デフォルト管理者のユーザー名または特権を無効にしたり、変更することはできません。デフォルト管理者のパスワードは変更できます。

ドメイン管理者

ドメイン管理者はドメインのオブジェクトの作成や管理ができます。

ドメイン管理者は、Administrator ツールにログインして、ドメイン内でアプリケーションサービスを作成し、設定することができます。 ただし、デフォルトでは、ドメイン管理者はアプリケーションクライアントにログインできません。 デフォルト管理者は、ドメイン管理者に対し、アプリケーションクライアント内で、ログインおよび管理タスクを実行できるように、アプリケーションサービスへの、完全な権限および特権を明示的に付与する必要があります。

ドメイン管理者は、Administrator ツールにログインして、ドメイン内でアプリケーションサービスを設定することができます。 ただし、デフォルトでは、ドメイン管理者はアプリケーションクライアントにログインできません。デフォルト管理者は、ドメイン管理者に対し、アプリケーションクライアント内で、ログインおよび管理タスクを実行できるように、アプリケーションサービスへの、完全な権限および特権を明示的に付与する必要があります。

ドメイン管理者を作成する際は、ユーザーにドメインの管理者ロールを割り当てます。

アプリケーションクライアントの管理者

アプリケーションクライアントの管理者は、アプリケーションクライアント内に、オブジェクトを作成して管理することができます。 アプリケーションクライアントの管理者アカウントを作成する必要があります。 管理者特権を制限し、アプリケーションクライアントの安全性を保つには、各アプリケーションクライアントに別々の管理者アカウントを作成します。

デフォルトでは、アプリケーションクライアントの管理者には、ドメインの権限や特権がありません。 ドメインの権限や特権がない場合、アプリケーションクライアントの管理者は、Administrator ツールにログインし、アプリケーションサービスを管理することができません。

以下のアプリケーションクライアントの管理者を設定することができます。

Informatica Analyst **管理者**

Informatica Analyst のすべての権限および特権があります。Informatica Analyst 管理者は、Informatica Analyst にログインし、プロジェクトを作成して管理し、アプリケーションクライアントのすべてのタスクを実行することができます。

Informatica Analyst の管理者を作成するには、ユーザーにアナリストサービスおよび関連付けられたモデルリポジトリサービスの管理者ロールを割り当てます。

Informatica Developer **管理者**

Informatica Developer のすべての権限および特権があります。Informatica Developer 管理者は、Informatica Developer にログインし、プロジェクト、およびプロジェクトのオブジェクトを作成して管理し、アプリケーションクライアントのすべてのタスクを実行することができます。

Informatica Developer 管理者を作成するには、ユーザーにモデルリポジトリサービスの管理者ロールを割り当てます。

Metadata Manager **管理者**

Metadata Manager のすべての権限および特権があります。Metadata Manager 管理者は、Metadata Manager にログインし、Metadata Manager オブジェクトを作成して管理し、アプリケーションクライアントのすべてのタスクを実行することができます。

Metadata Manager の管理者を作成するには、ユーザーに Metadata Manager サービスの管理者ロールを割り当てます。

Test Data **管理者**

Test Data Manager のすべての権限と特権があります。Test Data Manager 管理者は、Test Data Manager にログインし、Test Data Manager オブジェクトを作成して管理し、アプリケーションクライアントですべてのタスクを実行することができます。

Test Data 管理者を作成するには、ユーザーに Test Data Manager サービスの管理者ロールを割り当てます。

PowerCenter Client **管理者**

PowerCenter Client のすべてのオブジェクトに対するすべての権限および特権があります。PowerCenter Client の管理者は、PowerCenter Client にログインし、PowerCenter リポジトリオブジェクトを管理し、PowerCenter Client のすべてのタスクを実行することができます。PowerCenter Client の管理者は、pmrep および pmcmd コマンドラインプログラムのすべてのタスクを実行することもできます。

PowerCenter Client の管理者を作成するには、ユーザーに PowerCenter リポジトリサービスの管理者ロールを割り当てます。

ユーザー

Informatica ドメインにアカウントを持つユーザーは、アプリケーションクライアントでタスクを実行することができます。

通常は、デフォルト管理者またはドメイン管理者がユーザーアカウントを作成および管理して、Informatica ドメイン内でのロール、権限、および特権をユーザーに割り当てます。 ただし、必要なドメイン特権および権限を持つユーザーであれば誰でも、ユーザーアカウントを作成し、ロール、権限、および特権を割り当てることができます。

ユーザーは、自分に割り当てられた特権および権限に基づいたタスクをアプリケーションクライアントで実行することができます。

ユーザーの管理

ネイティブセキュリティドメイン内でユーザーを作成、編集、および削除できます。 LDAP セキュリティドメイン内で、ユーザーアカウントのプロパティを削除または変更できません。LDAP グループへのユーザー割り当てを変更できません。

PowerCenter Express のライセンスのタイプによりユーザーを作成、編集、および削除できます。 次に、ユーザーアカウントにロール、権限、および特権を割り当てることができます。Informatica ドメインでユーザーが実行できるタスクは、ユーザーに割り当てられたロール、権限、および特権によって決定されます。PowerCenter Express Personal Edition がある場合、ユーザーまたはグループを作成できません。すべてのタスクを実行するにはデフォルトの管理者ユーザーを使用する必要があります。

ライセンスタイプに応じて、ユーザーを作成、編集、および削除できます。次に、ユーザーアカウントにロール、権限、および特権を割り当てることができます。Informatica ドメインでユーザーが実行できるタスクは、ユーザーに割り当てられたロール、権限、および特権によって決定されます。

ネイティブセキュリティドメインまたは LDAP セキュリティドメイン内で、ユーザーアカウントにロール、権限、および特権を割り当てることができます。Informatica ドメインでユーザーが実行できるタスクは、ユーザーに割り当てられたロール、権限、および特権によって決定されます。

ユーザーアカウントのロックを解除することもできます。

ネイティブユーザーの作成ユーザーの作成ユーザーの作成

［セキュリティ］タブで、ネイティブユーザーを追加、編集、または削除します。

1. Administrator ツールで、［セキュリティ］タブをクリックします。
2. ［セキュリティアクション］メニュー上で、［ユーザーの作成］をクリックします。
3. ユーザーの詳細を入力します。

プロパティ	説明
ログイン名	ユーザーアカウントのログイン名。ユーザアカウントのログイン名は、所属するセキュリティドメイン内で一意でなくてはなりません。 名前では大文字と小文字が区別されず、128 文字以内であることが必要です。タブ、改行文字、または次の特殊文字は使用できません。 , + " \ < > ; / * % ? & 名前には、先頭と末尾の文字以外に ASCII スペース文字を使用できます。その他のスペース文字は許可されません。
パスワード	ユーザアカウントのパスワードです。パスワードは、1～80 文字の範囲で指定できます。
パスワードの確認	確認するために、パスワードを再度入力してください。パスワードを指定する必要があります。パスワードは、コピーしてペーストすることができません。
完全名（フルネーム）	ユーザアカウントの完全名。完全名に次の特殊文字は使用できません。 < > “
説明	ユーザアカウントの説明。説明は、765 文字を超えることや、以下の特殊文字を含めることはできません。 < > “

プロパティ	説明
電子メール	ユーザのメールアドレス。メールアドレスには、次の特殊文字を使用できません。 < > “ ホスト名:ポート番号のフォーマットでアドレスを入力してください。
電話番号	ユーザの電話番号。電話番号には、次の特殊文字を使用できません。 < > “

4. ［OK］をクリックして、ユーザアカウントを保存します。

   ユーザーアカウント作成後、詳細パネルにはユーザーアカウントのプロパティとユーザーが割り当てられたグループのプロパティが表示されます。

ネイティブユーザーの一般的なプロパティの編集

ネイティブユーザーのログイン名は変更できません。ネイティブユーザーアカウントのパスワードおよび他の詳細は変更できます。

1. Administrator ツールで、［セキュリティ］タブをクリックします。
2. ナビゲータの［ユーザー］セクションで、ネイティブユーザーアカウントを選択し、［編集］をクリックします。
3. パスワードを変更するには、［パスワードの変更］を選択します。

   ［セキュリティ］タブで、［パスワード］フィールドおよび［パスワードの確認］フィールドが取り消されます。
4. 新しいパスワードを入力して確認します。
5. 完全名、説明、メールアドレス、および電話番号には、次の特殊文字を使用できません。
6. ［OK］をクリックして変更を保存します。

ネイティブユーザーのネイティブグループへの割り当て

ネイティブユーザーを［セキュリティ］タブのネイティブグループに割り当てます。

1. Administrator ツールで、［セキュリティ］タブをクリックします。
2. ナビゲータの［ユーザー］セクションで、ネイティブユーザーアカウントを選択し、**［編集］**をクリックします。
3. ［グループ］タブをクリックします。
4. ネイティブユーザーをグループに割り当てるには、［すべてのグループ］カラムでグループ名を選択し、**［追加］**をクリックします。

   ネストされたグループが［すべてのグループ］カラムに表示されない場合は、各グループを展開してネストされたすべてのグループを表示します。

   複数のグループに 1 人のネイティブユーザーを割り当てることができます。Ctrl キーまたは Shift キーを押してフォルダ内の複数のグループを選択します。
5. ネイティブユーザーをグループから削除するには、［割り当てグループ］カラムでグループを選択し、**［削除］**をクリックします。
6. **［OK］**をクリックして、グループ割り当てを保存します。

LDAP ユーザーのネイティブグループへの割り当て

LDAP ユーザーアカウントをネイティブグループに割り当てることができます。LDAP グループへの LDAP ユーザアカウントの割り当ては変更できません。

1. Administrator ツールで、［セキュリティ］タブをクリックします。
2. ナビゲータの［グループ］セクションで、ネイティブグループを選択し、［編集］をクリックします。
3. ［ユーザー］タブをクリックします。
4. LDAP ユーザーをグループに割り当てるには、［すべてのユーザー］カラムで LDAP ユーザーを選択し、［追加］をクリックします。
5. LDAP ユーザーをグループから登録解除するには、［割り当てユーザー］カラムで LDAP ユーザーを選択し、［削除］をクリックします。
6. ［OK］をクリックして、ユーザー割り当てを保存します。

ユーザーアカウントの有効化および無効化

アクティブなアカウントを有するユーザーは、自分の権限と特権に基づき、アプリケーションクライアントにログイン、およびタスクを実行することができます。 ユーザーにアプリケーションクライアントへのアクセスを一時的にさせない場合は、ユーザーのアカウントを無効にすることができます。 ネイティブまたは LDAP セキュリティドメイン内で、ユーザーアカウントを有効、または無効にすることができます。ユーザーアカウントを無効にした場合は、ユーザーはアプリケーションクライアントにログインすることができません。

アクティブなアカウントを有するユーザーは、自分の権限と特権に基づき、アプリケーションクライアントにログイン、およびタスクを実行することができます。 ユーザーにアプリケーションクライアントへのアクセスを一時的にさせない場合は、ユーザーのアカウントを無効にすることができます。ユーザーアカウントを無効にした場合は、ユーザーはアプリケーションクライアントにログインすることができません。

ユーザーアカウントを無効にする際には、ナビゲータのユーザーセクションでユーザーアカウントを選択し、［無効化］をクリックします。無効なユーザーアカウントを選択した場合、［セキュリティ］タブにユーザーアカウントが無効であることを知らせるメッセージが表示されます。 ユーザーアカウントが無効になると、［無効化］ボタンが利用可能になります。ユーザーアカウントを有効化するには、［有効化］をクリックします。

デフォルトの管理者アカウントは無効にできません。

注: Service Manager が LDAP ディレクトリサービスからユーザーアカウントをインポートする場合、ユーザーアカウントが有効であるか無効であるかを示す LDAP 属性はインポートされません。 Service Manager により、すべてのユーザーアカウントは有効なユーザーアカウントとしてインポートされます。ユーザーにアプリケーションクライアントへのアクセスをさせない場合は、Administrator ツール内で LDAP ユーザーのアカウントを無効にします。 LDAP サーバーと続けて同期している間は、ユーザーアカウントは Administrator ツールにおいて、有効または無効状態を維持されます。

ネイティブユーザーの削除

ネイティブユーザーアカウントを削除するには、Navigator の［ユーザー］セクションにあるユーザーアカウント名を右クリックし、［ユーザーの削除］を選択します。 そのユーザーアカウントを削除することを確認します。

デフォルト管理者アカウントは削除できません。Administrator ツールへログインする際は、ユーザーアカウントを削除することはできません。

PowerCenter のユーザーの削除

PowerCenter リポジトリ内のオブジェクトを所有するユーザーを削除した場合、ユーザーがフォルダ、接続オブジェクト、デプロイメントグループ、ラベル、またはクエリに対して持つ所有権が削除されます。 ユーザー

を削除した後、デフォルトの管理者は削除されたユーザーにより所有されていたオブジェクトすべてのオーナーになります。

削除したユーザーにより以前に所有されていた、バージョンされたオブジェクトの履歴を表示した際、削除されたユーザーの名前は、「deleted」という単語のプレフィックスが付いて表示されます。

Metadata Manager のユーザーの削除

ショートカットおよびフォルダを所有するユーザーを削除した場合、Metadata Manager によりそのユーザーの個人フォルダが、デフォルトの管理者が所有する削除済みユーザーという名前の付いたフォルダに移動されます。 削除されたユーザーの個人フォルダには、ユーザーによって作成されたすべてのショートカットとフォルダが含まれています。 共有フォルダはユーザーの削除後も共有が維持されます。

削除済みユーザーフォルダに同一のユーザー名のフォルダが含まれている場合、Metadata Manager により追加されたフォルダに「<username>のコピー（n）」という名前が付けられます。

LDAP ユーザー

Administrator ツールでは、LDAP ユーザーを追加、編集、または削除することはできません。 LDAP ユーザーアカウントは、LDAP ディレクトリサービスで管理する必要があります。

ユーザーアカウントのロック解除

ドメイン管理者はドメインからロックアウトされたユーザーアカウントのロックを解除できます。 ネイティブユーザーの場合、管理者はユーザーがドメインにログインし直す前に、パスワードを変更するようにユーザーに要求できます。

ユーザーは、パスワードがリセットされるときに通知を受け取るため、ドメインで有効な電子メールアドレスを設定しておく必要があります。

そのユーザーが LDAP 認証サーバーからロックアウトされている場合、LDAP の管理者が LDAP サーバー内でそのユーザーアカウントをロック解除する必要があります。

1. Administrator ツールの［**セキュリティ**］タブをクリックします。
2. ［**アカウント管理**］をクリックします。

   以下のように、ロックアウトされたユーザーのリストが［アカウント管理］ページに表示されます。

   ロックアウトされたネイティブユーザー

   ネイティブのセキュリティドメイン内のロックアウトされたユーザーアカウントを表示します。

   ロックアウトされた LDAP **ユーザー**

   LDAP のセキュリティドメイン内のロックアウトされたユーザーアカウントを表示します。
3. ロックを解除するユーザーを選択します。
4. アカウントのロックを解除した後にユーザーの新しいパスワードを生成するには、［**ユーザーのロックを解除してパスワードをリセット**］を選択します。

   ユーザーは電子メールで新しいパスワードを受け取ります。
5. ［**選択したユーザーのロック解除**］ボタンをクリックします。

多数のユーザー用のシステムメモリの増加

Informatica ドメインのリスタート、LDAP ユーザーの同期、および複数回の infacmd および infasetup コマンドにかかる処理時間は、Informatica ドメインのユーザー数と比例して増えます。

ユーザー数は以下のコマンドの処理時間に影響があります。

- infasetup BackupDomain、DeleteDomain、および RestoreDomain
- infacmd isp ExportDomainObjects、ExportUsersandGroups、ImportDomainObjects、および ImportUsersandGroups
- infacmd oie ExportObjects および ImportObjects

ドメイン内のユーザー数が多数の場合は、状況に応じて Informatica サービス、infasetup、および infacmd が使用するシステムメモリを増やす必要があります。最大ヒープサイズを増やすには、以下の環境変数を設定し、メガバイト単位で値を指定します。

- INFA_JAVA_OPTS。Informatica サービスで使用する最大ヒープサイズを決定します。Informatica サービスがインストールされているノードごとに設定します。
- ICMD_JAVA_OPTS。infacmd で使用する最大ヒープサイズを決定します。infacmd を実行するマシンごとに設定します。
- INFA_JAVA_CMD_OPTS。infasetup で使用する最大ヒープサイズを決定します。infasetup を実行するマシンごとに設定します。

例えば、INFA_JAVA_OPTS 環境変数で UNIX に 2048 MB のシステムメモリを設定するには、以下のコマンドを使用します。

```
setenv INFA_JAVA_OPTS "-Xmx2048m"
```

Windows の場合、この環境変数をシステム変数として設定します。

以下の表に、ドメイン内のユーザーとサービスの数に基づく、最大ヒープサイズ設定の最小要件を示します。

ドメインのユーザー数	最大ヒープ サイズ（1〜5 個のサービス）	最大ヒープ サイズ（6〜10 個のサービス）
最大 1,000	512MB（デフォルト）	1024MB
5,000	2048MB	3072MB
10,000	3072MB	5120MB
20,000	5120MB	6144MB
30,000	5120MB	6144MB

注: この表の最大ヒープサイズの設定内容は、ドメイン内のアプリケーションサービスの数に基づいています。

これらの環境変数の設定後は、変更を有効にするためにノードをリスタートします。

ユーザーアクティビティの表示

infacmd isp getUserActivityLog コマンドまたは Administrator ツールの［ログ］タブを使用して、ユーザーアクティビティログを表示します。ユーザーアクティビティログイベントを表示して、ユーザーがサービス、ノード、ユーザー、グループ、またはロールをいつ作成、更新、または削除したかを判断します。

以下のコマンドを実行して、すべてのユーザーのユーザーアクティビティログイベントを表示します。

```
infacmd isp getUserActivityLog -dn domain_name -un user_name -pd password
```

このコマンドには、管理者ロールまたは管理者グループのメンバーシップが必要です。

以下のオプションのフィルタに基づきログイベントを表示できます。

- ユーザー名
- セキュリティドメイン
- 日付と時刻
- 時系列順
- アクティビティコード
- アクティビティテキスト

ログイベントをコマンドラインに表示するか、または以下の形式でファイルに書き込むことができます。

- バイナリ
- テキスト
- XML

ログをバイナリ形式で出力する場合、infacmd isp convertUserActivityLog コマンドを使用して、テキストまたは XML 形式に変換できます。

ユーザーアクティビティログおよび Administrator ツールの［ログ］タブの詳細については、『*Informatica Administrator ガイド*』を参照してください。

ユーザーアクティビティのログフィルタ

1 つ以上のフィルタを使用して、特定のユーザー、日付、またはイベントのログイベントを取得できます。

infacmd isp getUserActivityLog コマンドに以下のパラメータを 1 つ以上使用して、ログイベントをフィルタできます。

ユーザーおよびセキュリティドメイン

オプション。ログイベントを取得する対象のユーザーのリスト。ユーザーが複数の場合はスペースで区切ります。1 つのセキュリティドメインまたはすべてのセキュリティドメインの複数のユーザーのログを表示するには、ワイルドカード記号（*）を使用します。例えば、次の文字列はオプションに対する有効な値です。

```
user:Native
"user:*"
"user*"
"*_users_*"
"*:Native"
```

getUserActivityLog コマンドに以下のパラメータを追加し、ユーザーまたはセキュリティドメインに基づいてログイベントをフィルタします。

```
-usrs <UserName>:<SecurityDomain>
```

例えば、以下のパラメータを追加して、すべてのセキュリティドメインの User1 という名前のユーザーのアクティビティを取得します。

```
-usrs "User1:*"
```

日付と時刻

オプション。ログイベントを表示する日付の範囲。

終了日を開始日より前の日付で入力すると、このコマンドを実行してもログイベントは返されません。

以下のいずれかの形式で日付を入力します。

- MM/dd/yyyy

- MM/dd/yyyy HH:mm:ss
- yyyy-MM-dd
- yyyy-MM-dd HH:mm:ss

getUserActivityLog コマンドに以下のパラメータを追加して、開始日または終了日でログをフィルタします。

-sd *<start_date>* -ed *<end_date>*

例えば、以下のパラメータを追加して、2014 年 1 月 1 日から 2014 年 2 月 3 日までのユーザーアクティビティを取得します。

-sd 01/01/2014 -ed 02/03/2014

アクティビティコード

オプション。アクティビティコードに基づいてログイベントを返します。

複数のアクティビティコードに対するログイベントを取得するには、ワイルドカード記号（*）を使用します。有効なアクティビティコードは以下のとおりです。

- CCM_10437。アクティビティが成功したことを示します。
- CCM_10438。アクティビティが失敗したことを示します。

getUserActivityLog コマンドに以下のパラメータを追加して、アクティビティコードでフィルタします。

-ac *<activity_code>*

例えば、以下のパラメータを追加して、成功したログイベントを取得します。

-ac CCM_10437

ワイルドカード記号を使用する場合、引数を引用符で囲みます。

アクティビティテキスト

オプション。アクティビティテキストで検出された文字列に基づいてログイベントを返します。

getUserActivityLog コマンドに以下のパラメータを追加して、アクティビテテキストでフィルタします。

-atxt *<activity_text>*

複数のイベントに対するログを取得するには、ワイルドカード記号（*）を使用します。例えば、以下のパラメータでは、説明に「Enabling service」という句が含まれるすべてのログイベントが返されます。

-atxt "*Enabling service*"

ワイルドカード記号を使用する場合、引数を引用符で囲みます。

時系列順

オプション。時系列とは逆の順序でログイベントを出力します。このパラメータを指定しないと、コマンドはログイベントを時系列順に表示します。

getUserActivityLog コマンドに以下のパラメータを追加して、最新のイベントを最初に出力します。

-ro true

ユーザーアクティビティのログイベントの書き込みと表示

infacmd isp getUserActivityLog コマンドを使用する際に、ユーザーアクティビティのログイベントをファイルに書き込むか、またはコマンドラインに表示することができます。ユーザーアクティビティのログイベントを、エクスポートされたログイベントファイルの使用方法に基づいた形式で書き込みます。

ログファイルの書き込みと表示

ユーザーアクティビティのログイベントをファイルに書き込むには、出力ファイルパラメータ-lo を指定してコマンドを実行します。

-lo *output_file_name*

出力形式を指定しないと、コマンドはログイベントをテキストファイルに書き込みます。例えば、次のコマンドを実行して、ログイベントを log.txt という名前のファイルに書き込みます。

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -lo log.txt
```

出力形式を指定するには、形式パラメータ-fm を指定してコマンドを実行します。

-fm *output_format_BIN_TEXT_XML*

有効な形式は以下のとおりです。

- Bin（バイナリ）。バイナリ形式でログイベントをバックアップする場合にはバイナリ形式を使用します。Informatica グローバルカスタマサポートにログイベントを送信するには、この形式の使用が必要になる場合があります。
- テキスト。テキストエディタでログイベントを分析する場合は、テキスト形式を使用します。
- XML。XML を使用する外部ツールでログイベントを分析する場合、または XSLT などの XML ツールを使用する場合は、XML 形式を使用します。

出力形式としてテキストまたは XML を指定し、出力ファイルを指定しない場合、コマンドはテキストまたは XML ログをコマンドラインに表示します。

出力形式としてバイナリを指定する場合、出力ファイル名を指定する必要があります。

例えば、次のコマンドを実行して、ログイベントを log.xml という名前のファイルに書き込みます。

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -fm xml -lo log.xml
```

ログファイルの変換

getUserActivity コマンドを使用してログイベントをバイナリファイルに書き込む場合、ファイルをテキストまたは XML 形式に変換できます。

次のコマンドを実行して、取得したバイナリログをテキストまたは XML 形式に変換します。

```
infacmd isp convertUserActivityLogFile -in BIN_input_file_name -fm output_format_TEXT_XML -lo output_file_name
```

例えば、次のコマンドを実行して、log.bin という名前のバイナリ入力ファイルを XML 形式に変換し、それを convertedLog.xml という名前のファイルに出力します。

```
infacmd isp convertUserActivityLogFile -in log.bin -fm XML -lo convertedLog.xml
```

コマンドラインにログを表示するには、出力ファイル名を省略します。

形式を省略すると、コマンドはテキスト形式を使用します。

グループの管理

ネイティブセキュリティドメイン内のグループの作成、編集、削除を行うことができます。

ネイティブのグループまたは LDAP セキュリティドメインにロール、権限、および特権を割り当てることができます。LDAP セキュリティドメイン内で、グループアカウントのプロパティを削除または変更できません。Informatica ドメインでそのグループのユーザーが実行できるタスクは、グループに割り当てられたロール、権限、および特権によって決定されます。

グループにロール、権限、および特権を割り当てることができます。Informatica ドメインでそのグループのユーザーが実行できるタスクは、グループに割り当てられたロール、権限、および特権によって決定されます。

グループにロール、権限、および特権を割り当てることができます。Informatica ドメインでそのグループのユーザーが実行できるタスクは、グループに割り当てられたロール、権限、および特権によって決定されます。

ネイティブグループの追加

［セキュリティ］タブでネイティブグループを追加、編集、または削除します。

ネイティブグループには、ネイティブまたは LDAP ユーザーアカウントを入れることも、他のネイティブグループを入れることもできます。複数レベルのネイティブグループを作成できます。たとえば、Finance グループには AccountsPayable が含まれ、AccountsPayable グループには OfficeSupplies グループが含まれます。Finance グループは、AccountsPayable グループの親グループであり、AccountsPayable グループは OfficeSupplies グループの親グループです。各グループには、他のネイティブグループを入れることができます。

ネイティブグループには、ユーザーアカウントや他のネイティブグループを入れることができます。複数レベルのネイティブグループを作成できます。たとえば、Finance グループには AccountsPayable が含まれ、AccountsPayable グループには OfficeSupplies グループが含まれます。Finance グループは、AccountsPayable グループの親グループであり、AccountsPayable グループは OfficeSupplies グループの親グループです。各グループには、他のネイティブグループを入れることができます。

ネイティブグループには、ユーザーアカウントや他のネイティブグループを入れることができます。複数レベルのネイティブグループを作成できます。たとえば、Finance グループには AccountsPayable が含まれ、AccountsPayable グループには OfficeSupplies グループが含まれます。Finance グループは、AccountsPayable グループの親グループであり、AccountsPayable グループは OfficeSupplies グループの親グループです。各グループには、他のネイティブグループを入れることができます。

1. Administrator ツールで、［セキュリティ］タブをクリックします。
2. ［セキュリティアクション］メニューで、［グループの作成］をクリックします。

3. グループについて、以下の情報を入力します。

プロパティ	説明
Name	グループの名前。名前は、大文字と小文字を区別せず、128 文字を超えることはできません。 タブ、改行文字、または次の特殊文字は使用できません。 , + " \ < > ; / * % ? 名前には、先頭と末尾の文字以外に ASCII スペース文字を使用できます。その他のすべてのスペース文字は許可されません。
親グループ	新しいグループが属しているグループ。ネイティブグループを選択してから［Create Group（グループの作成）］をクリックすると、選択したグループが親グループになります。それ以外の場合、［ネイティブ］と表示され、新しいグループがグループに属していないことを表します。
説明	グループの説明。グループの説明は、765 文字を超えることや、以下の特殊文字を含めることはできません。 < > “

4. ［参照］をクリックして、別の親グループを選択します。

   複数レベルのグループおよびサブグループを作成できます。

5. ［OK］をクリックして、グループを保存します。

ネイティブグループのプロパティの編集

グループを作成した後に、グループの説明、およびグループ内のユーザーのリストを変更できます。グループまたはグループの親の名前は変更できません。グループの親を変更するには、グループを別のグループに移動する必要があります。

1. Administrator ツールで、［セキュリティ］タブをクリックします。
2. ナビゲータの［グループ］セクションで、ネイティブグループを選択し、［編集］をクリックします。
3. グループの説明を変更します。
4. グループ内のユーザのリストを変更するには、［ユーザ］タブを使用します。

   ［ユーザー］タブには、ドメイン内のユーザーのリストと、グループに割り当てられたユーザーのリストが表示されます。

5. ユーザをグループに割り当てるには、［すべてのユーザ］カラム内でユーザアカウントを選択して、［追加］をクリックします。
6. ユーザをグループから削除するには、［Assigned Users（割り当てユーザ）］カラムでユーザアカウントを選択し、［削除］をクリックします。
7. ［OK］をクリックして変更を保存します。

別のネイティブグループへのネイティブグループの移動

ネイティブセキュリティドメイン内のユーザーのグループを整理するため、ネストされたグループを設定して、グループを別のグループに移動できます。

ネイティブグループを別のネイティブグループに移動するには、ナビゲータの［グループ］セクションでネイティブグループの名前を右クリックし、［グループの移動］を選択します。

ネイティブグループの削除

ネイティブグループを削除するには、ナビゲータの［グループ］セクションでグループ名を右クリックし、［グループの削除］を選択します。

グループを削除した場合、グループのユーザーは、グループのメンバシップおよびグループから継承した権限または特権を失います。

グループを削除した場合、Service Manager によりグループに属するグループおよびサブグループすべてが削除されます。

LDAP グループ

Administrator ツールでは、LDAP グループを追加、編集、削除、またはユーザー割り当てを変更することができません。 グループおよびユーザー割り当ては、LDAP ディレクトリサービスで管理する必要があります。

オペレーティングシステムのプロファイルの管理

Administrator ツールの［セキュリティ］タブまたはコマンドラインで、オペレーティングシステムのプロファイルを作成および管理します。オペレーティングシステムのプロファイルを作成、編集、削除できます。デフォルトのオペレーティングシステムのプロファイルの変更や、ユーザーおよびグループへの割り当てが可能です。

オペレーティングシステムのプロファイルを使用するようにデータ統合サービスが設定されている場合、データ統合サービスは、オペレーティングシステムのプロファイルを使用してマッピング、プロファイル、およびワークフローを実行します。オペレーティングシステムのプロファイルを使用するように PowerCenter 統合サービスが設定されている場合、PowerCenter 統合サービスは、オペレーティングシステムのプロファイルを使用してワークフローを実行します。

［セキュリティ］タブの**［オペレーティングシステムプロファイル］**ビューで、オペレーティングシステムのプロファイルを作成、編集、削除します。

オペレーティングシステムのプロファイルを作成するには、次の手順を実行します。

1. オペレーティングシステムのプロファイル名とシステムユーザー名を入力します。
2. 統合サービスを選択して、オペレーティングシステムのプロファイルのプロパティを設定します。
3. 必要に応じて、オペレーティングシステムのプロファイルに権限を割り当てます。

   オペレーティングシステムのプロファイルを作成したら、ユーザーおよびグループをオペレーティングシステムのプロファイルに割り当て、デフォルトのプロファイルをユーザーおよびグループに割り当てることができます。

PowerCenter 統合サービス用のオペレーティングシステムのプロファイルのプロパティ

セッションプロパティおよびパラメータファイル内で設定されたサービスプロセス変数により、オペレーティングシステムのプロファイル設定がオーバーライドされます。

次の表に、PowerCenter 統合サービス用のオペレーティングシステムのプロファイルのプロパティを示します。

プロパティ	説明
名前	オペレーティングシステムプロファイルの読み取り専用の名前。名前は 128 文字を超えることはできません。 空白または次の特殊文字は使用できません。\ / : * ? " < > | [ ] = + ; ,
システムユーザ名	PowerCenter 統合サービスが実行されるマシンに存在するオペレーティングシステムユーザーの読み取り専用の名前。PowerCenter 統合サービスでは、オペレーティングシステムのプロファイル用に定義されたシステムユーザーのシステムアクセスを使用して、ワークフローを実行します。
$PMRootDir	ノードによるルートディレクトリへのアクセス性。これは他のサービスプロセス変数のルートディレクトリです。次の特殊文字は使用できません。 * ? < > " | ,
$PMSessionLogDir	セッションログのディレクトリ。次の特殊文字は使用できません。 * ? < > " | , デフォルトは、$PMRootDir/SessLogs です。
$PMBadFileDir	リジェクトファイルのディレクトリ。次の特殊文字は使用できません。 * ? < > " | , デフォルトは、$PMRootDir/BadFiles です。
$PMCacheDir	インデックスファイルとデータキャッシュファイルのディレクトリ。 キャッシュディレクトリが PowerCenter 統合サービスプロセスへのローカルドライブである場合、パフォーマンスを向上させることができます。キャッシュファイルには、マッピングドライブやマウントドライブを使用しないでください。次の特殊文字は使用できません。 * ? < > " | , デフォルトは、$PMRootDir/Cache です。
$PMTargetFileDir	ターゲットファイルのディレクトリ。次の特殊文字は使用できません。 * ? < > " | , デフォルトは、$PMRootDir/TgtFiles です。
$PMSourceFileDir	ソースファイルのディレクトリ。次の特殊文字は使用できません。 * ? < > " | , デフォルトは、$PMRootDir/SrcFiles です。
$PMExtProcDir	外部プロシージャのディレクトリ。次の特殊文字は使用できません。 * ? < > " | , デフォルトは、$PMRootDir/ExtProc です。
$PMTempDir	一時ファイルのディレクトリ。次の特殊文字は使用できません。 * ? < > " | , デフォルトは、$PMRootDir/Temp です。
$PMLookupFileDir	ルックアップファイルのディレクトリ。次の特殊文字は使用できません。 * ? < > " | , デフォルトは、$PMRootDir/LkpFiles です。

プロパティ	説明
$PMStorageDir	実行時ファイルのディレクトリ。ワークフローリカバリファイルは、PowerCenter 統合サービスプロパティで設定された$PMStorageDir に保存されます。セッションリカバリファイルは、オペレーティングシステムプロファイルで設定された $PMStorageDir に保存されます。次の特殊文字は使用できません。 * ? < > “ \| , デフォルトは、$PMRootDir/Storage です。
環境変数	実行時に統合サービスによって使用される環境変数の名前と値。 オペレーティングシステムのプロファイルのプロパティで、LD_LIBRARY_PATH 環境変数を指定した場合、統合サービスによって LD_LIBRARY_PATH 環境変数にこの変数の値が付加されます。統合サービスは、その LD_LIBRARY_PATH 環境変数の値を使用して、オペレーティングシステムのプロファイルに対して生成された子プロセスの環境変数を設定します。 オペレーティングシステムのプロファイルのプロパティで、LD_LIBRARY_PATH 環境変数を指定していない場合、統合サービスは、その LD_LIBRARY_PATH 環境変数を使用します。

データ統合サービス用のオペレーティングシステムのプロファイルのプロパティ

次の表に、データ統合サービス用のオペレーティングシステムのプロファイルのプロパティを示します。

プロパティ	説明
名前	オペレーティングシステムプロファイルの読み取り専用の名前。名前は 128 文字を超えることはできません。 空白または次の特殊文字は使用できません。\ / : * ? " < > | [ ] = + ; ,
システムユーザー名	データ統合サービスが実行されるシステムに存在するオペレーティングシステムユーザーの読み取り専用の名前。データ統合サービスは、オペレーティングシステムユーザーのシステムアクセスを使用して、マッピング、ワークフロー、およびプロファイリングの各ジョブを実行します。
$DISRootDir	ノードによるルートディレクトリへのアクセス性。これは他のサービスプロセス変数のルートディレクトリです。次の特殊文字は使用できません。 * ? < > " | , [ ]
$DISTempDir	ジョブが実行されるときに作成される一時ファイルのディレクトリ。次の特殊文字は使用できません。 * ? < > " | , [ ] デフォルトは<root directory>/disTemp です。
$DISCacheDir	トランスフォーメーションのインデックスファイルおよびデータキャッシュファイルのディレクトリ。次の特殊文字は使用できません。 * ? < > " | , [ ] デフォルトは<root directory>/cache です。

プロパティ	説明
$DISSourceDir	マッピングで使用されているソースフラットファイルのディレクトリ。次の特殊文字は使用できません。 * ? < > " | , [ ] デフォルトは<root directory>/source です。
$DISTargetDir	マッピングで使用されているターゲットフラットファイルのディレクトリ。次の特殊文字は使用できません。 * ? < > " | , [ ] デフォルトは<root directory>/target です。
$DISRejectedFilesDir	リジェクトファイルのディレクトリ。拒否ファイルには、マッピングの実行中に拒否された行が含まれます。次の特殊文字は使用できません。 * ? < > " | , [ ] デフォルトは<root directory>/reject です。
$DISLogDir	ログのディレクトリ。次の特殊文字は使用できません。 * ? < > " | , [ ] デフォルトは<root directory>/disLogs です。
Hadoop 偽装のプロパティの有効化	データ統合サービスが Hadoop 偽装ユーザーを使用して、Hadoop 環境内でマッピング、ワークフロー、およびプロファイリングジョブを実行することを示します。 デフォルトの Hadoop 偽装ユーザーはログインユーザーです。別の Hadoop 偽装ユーザーを指定するには、**[指定したユーザーを Hadoop 偽装ユーザーとして使用する]** を選択して、ユーザー名を入力します。
環境変数	実行時に統合サービスによって使用される環境変数の名前と値。 オペレーティングシステムのプロファイルのプロパティで、LD_LIBRARY_PATH 環境変数を指定した場合、統合サービスによって LD_LIBRARY_PATH 環境変数にこの変数の値が付加されます。統合サービスは、その LD_LIBRARY_PATH 環境変数の値を使用して、オペレーティングシステムのプロファイルに対して生成された子プロセスの環境変数を設定します。 オペレーティングシステムのプロファイルのプロパティで、LD_LIBRARY_PATH 環境変数を指定していない場合、統合サービスは、その LD_LIBRARY_PATH 環境変数を使用します。 **注**: AIX で、データ統合サービスがオペレーティングシステムのプロファイルを使用して、マッピング、プロファイル、およびワークフローを正常に実行するためには、LD_LIBRARY_PATH 環境変数を INFA_HOME/services/shared/bin に設定する必要があります。
フラットファイルキャッシュディレクトリ	アップロードされたフラットファイルを Analyst ツールが格納するフラットファイルキャッシュのディレクトリ。 アナリストサービスが、オペレーティングシステムのプロファイルを使用するデータ統合サービスに接続する場合、オペレーティングシステムのプロファイルに指定されているオペレーティングシステムユーザーは、このフラットファイルのキャッシュディレクトリにアクセスできる必要があります。参照テーブルまたはフラットファイルソースをインポートすると、Analyst ツールによって、このディレクトリからファイルが使用されて、参照テーブルまたはフラットファイルデータオブジェクトが作成されます。フラットファイルの場所を変更した場合は、アナリストサービスを再起動します。

オペレーティングシステムのプロファイルの作成

セキュリティの向上とランタイムユーザー環境の分離を目的に、オペレーティングシステムのプロファイルを作成し、それをユーザーおよびグループに割り当てます。1 つ以上のオペレーティングシステムのプロファイルを作成できます。PowerCenter 統合サービスでは、オペレーティングシステムのプロファイルを使用してワークフローを実行します。データ統合サービスでは、オペレーティングシステムのプロファイルを使用してマッピング、プロファイル、およびワークフローを実行します。

1. Administrator ツールの **［セキュリティ］** タブをクリックします。
2. ［セキュリティアクション］メニューで、**［オペレーティングシステムプロファイルの作成］** をクリックします。

   ［オペレーティングシステムプロファイルの作成 - 手順 1/3］ ダイアログボックスが表示されます。
3. オペレーティングシステムのプロファイルの次の全般プロパティを入力します。

プロパティ	説明
名前	オペレーティングシステムプロファイルの名前。この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。128 文字を超えたり、@で始めることはできません。また、以下の特殊文字を含むことはできません。 % * + \ / ? ; < > 名前の最初および最後の文字以外で、ASCII のスペース文字を使用できます。その他のスペース文字は許可されません。
システムユーザー名	統合サービスが実行されるマシンに存在するオペレーティングシステムユーザーの名前。統合サービスは、オペレーティングシステムのプロファイル用に定義されたシステムユーザーのシステムアクセスを使用して、ワークフローまたはジョブを実行します。 **注**: オペレーティングシステムプロファイルを作成する場合は、システムユーザー名をルートとして指定したり、uid==0 の非ルートユーザーを使用することはできません。

4. **［次へ］** をクリックします。

   ［オペレーティングシステムプロファイルの設定 - 手順 2/3］ ダイアログボックスが表示されます。
5. オペレーティングシステムのプロファイルを使用する統合サービスの 1 つまたは両方を選択します。
   - PowerCenter 統合サービス
   - データ統合サービス
6. 統合サービス用のオペレーティングシステムのプロファイルのプロパティを設定します。
7. データ統合サービスが Hadoop 環境でマッピング、プロファイル、およびワークフローを実行する場合、次のように Hadoop 偽装のプロパティを設定します。
   a. **［Hadoop 偽装のプロパティの有効化］** を選択します。
   b. Hadoop ジョブを実行する際に、ログインユーザーを使用するか Hadoop 偽装ユーザーを指定するかを選択します。
8. 必要に応じて、環境変数を設定します。
9. オペレーティングシステムのプロファイルを使用するデータ統合サービスにアナリストサービスが接続する場合は、アナリストサービスのプロパティを設定します。
10. **［次へ］** をクリックします。

    ［オペレーティングシステムプロファイルへのユーザー/グループの割り当て - 手順 3/3］ ダイアログボックスが表示されます。

11. **[グループ]** タブで、次のようにグループをオペレーティングシステムのプロファイルに割り当てます。
    a. 特定のグループをオペレーティングシステムのプロファイルに割り当てるには、1 つ以上のグループを選択して、**[追加]** をクリックします。
    b. オペレーティングシステムのプロファイルに利用可能なすべてのグループを割り当てるには、**[すべて追加]** をクリックします。
12. 必要に応じて、オペレーティングシステムのプロファイルをデフォルトのプロファイルとして、1 つ以上のグループに割り当てます。デフォルトのプロファイルを割り当てるには、選択したグループリストにあるグループに対して **[デフォルトのプロファイル]** を選択します。
13. **[ユーザー]** タブで、次のようにユーザーをオペレーティングシステムのプロファイルに割り当てます。
    a. 特定のユーザーをオペレーティングシステムのプロファイルに割り当てるには、1 つ以上のユーザーを選択して、**[追加]** をクリックします。
    b. オペレーティングシステムのプロファイルに利用可能なすべてのユーザーを割り当てるには、**[すべて追加]** をクリックします。
14. 必要に応じて、オペレーティングシステムのプロファイルをデフォルトのプロファイルとして、1 つ以上のユーザーに割り当てます。デフォルトのプロファイルを割り当てるには、選択したユーザーリストにあるユーザーに対して **[デフォルトのプロファイル]** を選択します。
15. **[完了]** をクリックします。

    オペレーティングシステムのプロファイルを作成すると、[詳細] パネルにオペレーティングシステムのプロファイルのプロパティ、およびプロファイルが割り当てられたグループおよびユーザーが表示されます。

オペレーティングシステムのプロファイルの編集

オペレーティングシステムのプロファイルを編集して、オペレーティングシステムのプロファイルのプロパティを変更できます。

オペレーティングシステムプロファイルの作成後は、名前またはシステムユーザー名を変更できません。オペレーティングシステムのプロファイルに指定されているオペレーティングシステムユーザーを使用しない場合は、オペレーティングシステムのプロファイルを削除してください。

1. Administrator ツールの **[セキュリティ]** タブをクリックします。
2. **[オペレーティングシステムプロファイル]** ビューを選択します。
3. オペレーティングシステムのプロファイルを選択します。
4. **[プロパティ]** タブで **[編集]** をクリックします。

   [プロパティの編集] ダイアログボックスが表示されます。
5. 設定する**データ統合サービス**または **PowerCenter 統合サービス**を選択します。
6. 統合サービスのプロパティを編集します。
7. **[OK]** をクリックします。

ユーザーまたはグループへのデフォルトのオペレーティングシステムのプロファイルの割り当て

ユーザーまたはグループが複数のオペレーティングシステムのプロファイルにアクセスできる場合、統合サービスがジョブおよびワークフローの実行に使用するデフォルトのオペレーティングシステムのプロファイルを割り当てます。直接権限のあるオペレーティングシステムのプロファイルをデフォルトのプロファイルとして、ユーザーまたはグループに割り当てることができます。ユーザーまたはグループに割り当てることができるデフォルトのオペレーティングシステムのプロファイルは、1 つのみです。ただし、同じオペレーティングシス

テムのプロファイルをデフォルトのプロファイルとして、複数のユーザーまたはグループに割り当てることができます。

1. ［セキュリティ］タブで**［ユーザー］**または**［グループ］**ビューを選択します。
2. ナビゲータで、ユーザーまたはグループを選択します。
3. ［コンテンツ］パネルで、**［権限］**ビューを選択します。
4. **［オペレーティングシステムプロファイル］**タブをクリックします。
5. **［デフォルトのオペレーティングシステムプロファイルを割り当てまたは変更します］**ボタンをクリックします。

   ［デフォルトのオペレーティングシステムプロファイルを割り当てまたは変更します］ダイアログボックスが表示されます。
6. **［デフォルトのオペレーティングシステムプロファイル］**リストからプロファイルを選択します。または、リストから**［デフォルトのオペレーティングシステムプロファイルを割り当てないでください］**を選択し、ユーザーまたはグループに割り当てられているデフォルトのプロファイルを削除します。
7. **［OK］**をクリックします。

   ［詳細］パネルの**［デフォルトのプロファイル］**カラムには、オペレーティングシステムのプロファイルに対して**［はい（直接）］**と表示されます。

オペレーティングシステムのプロファイルの削除

オペレーティングシステムのプロファイルを削除するには、ナビゲータの［オペレーティングシステムプロファイル］セクションでオペレーティングシステムのプロファイル名を右クリックして、**［プロファイルの削除］**を選択します。

オペレーティングシステムのプロファイルを削除した後、そのオペレーティングシステムのプロファイルが割り当てられていたユーザーとグループに、別のオペレーティングシステムのプロファイルをデフォルトのプロファイルとして割り当てます。PowerCenter 統合サービスがオペレーティングシステムのプロファイルを使用する場合、そのオペレーティングシステムのプロファイルが割り当てられていたリポジトリフォルダとワークフローに、別のオペレーティングシステムのプロファイルを割り当てます。

セキュアなドメインでのオペレーティングシステムのプロファイルに関する作業

セキュアな通信が有効な Informatica ドメインでオペレーティングシステムのプロファイルを使用できます。

セキュアな通信が有効なドメインでオペレーティングシステムのプロファイルを使用する場合、以下の規則とガイドラインに従う必要があります。

- 以下のオペレーティングシステムのプロファイルの環境変数を設定する必要があります。
  INFA_TRUSTSTORE

  セキュアなドメインの SSL 証明書のトラストストアファイルを含むディレクトリに値を設定します。このディレクトリには infa_truststore.pem という名前のトラストストアファイルが含まれている必要があります。

  INFA_TRUSTSTORE_PASSWORD

  カスタムトラストストアを使用する場合は、セキュアドメインのための SSL 証明書が含まれている infa_truststore.pem のパスワードに値を設定します。 パスワードは暗号化される必要があります。pmpasswd というコマンドラインプログラムを使用して、パスワードを暗号化します。

- さらに、PowerCenter 統合サービスが［グリッド上のセッション］オプションを使用する場合は、以下のオペレーティングシステムのプロファイルの環境変数を設定する必要があります。
  INFA_KEYSTORE

  セキュアなドメインの SSL 証明書のキーストアファイルを含むディレクトリに値を設定します。このディレクトリには infa_keystore.pem という名前のキーストアファイルが含まれている必要があります。

Administrator ツールでオペレーティングシステムのプロファイルの環境変数を設定できます。オペレーティングシステムのプロファイルの環境変数を設定するには、**［セキュリティ］** > **［オペレーティングシステムのプロファイル］**をクリックします。オペレーティングシステムのプロファイルのプロパティを編集して環境変数を設定します。

Kerberos 認証を使用したドメイン内のオペレーティングシステムのプロファイルに関する作業

Kerberos 認証を使用して、ネットワーク上で実行する Informatica ドメイン内のオペレーティングシステムのプロファイルを使用できます。

Kerberos 認証を使用してネットワーク上で実行するドメイン内のオペレーティングシステムのプロファイルを使用する場合、以下の規則とガイドラインに従う必要があります。

- オペレーティングシステムのプロファイルのユーザーアカウントは Kerberos 認証に使用される Active Directory サービスのプリンシパルである必要があり、Informatica ドメイン内の LDAP セキュリティドメインにインポートされます。
- ユーザーアカウントにはオペレーティングシステムのプロファイルのユーザーアカウントにアクセス可能な Kerberos の資格情報キャッシュファイルが必要です。オペレーティングシステムのプロファイルの各ユーザーアカウントには、個別の資格情報キャッシュファイルが必要です。
- オペレーティングシステムのプロファイルのユーザーアカウントの資格情報キャッシュファイルは forwardable である必要があります。例えば、*kinit* ユーティリティを使用して資格情報キャッシュファイルを作成する場合、*-f* オプションを指定する必要があります。
- オペレーティングシステムのプロファイルのユーザーアカウントの資格情報キャッシュファイルは、オペレーティングシステムのプロファイルを使用するワークフローを実行するときに使用できる必要があります。
- オペレーティングシステムのプロファイルのユーザーアカウントの資格情報キャッシュファイルには、必ず最新の資格情報が必要です。*cron* などのジョブスケジューラユーティリティを実行して、資格情報キャッシュファイル内のユーザークレデンシャルを定期的に更新することができます。

- 以下のオペレーティングシステムのプロファイルの環境変数を設定する必要があります。
  INFA_OSPI_SECURITY_DOMAIN

  オペレーティングシステムのプロファイルのユーザーアカウントを含むセキュリティドメインの名前に値を設定します。ユーザーアカウントが Kerberos 用のユーザーレルムセキュリティドメインに属している場合、この変数を設定する必要はありません。Kerberos 用のユーザーレルムセキュリティドメインは、Kerberos ユーザーレルムと同じ名前を持つ、インストール中に作成されたセキュリティドメインです。

  KRB5_CONFIG

  Kerberos 設定ファイルのパスとファイル名に値を設定します。Kerberos 設定ファイルの名前は *krb5.conf* です。

  KRB5CCNAME

  オペレーティングシステムのプロファイルのユーザーアカウントの Kerberos 資格情報キャッシュファイルのパスとファイル名に変数を設定します。

  Administrator ツールでオペレーティングシステムのプロファイルの環境変数を設定できます。オペレーティングシステムのプロファイルの環境変数を設定するには、**［セキュリティ］** > **［オペレーティングシステムのプロファイル］**をクリックします。オペレーティングシステムのプロファイルのプロパティを編集して環境変数を設定します。

アカウントロックアウト

Informatica ドメインでのセキュリティを強化するために、管理者は複数回のログインの失敗後にドメインのユーザーアカウント（他の管理者ユーザーを含む）のロックアウトを実行できます。

管理者は、ユーザーアカウントがロックされるまでにそのユーザーが失敗できるログイン試行の回数を指定できます。アカウントがロックアウトされた場合、管理者が Informatica ドメインのアカウントをロック解除することができます。

管理者がユーザーアカウントをロック解除するときに、管理者が［ユーザーのロックを解除してパスワードをリセット］オプションを選択してユーザーのパスワードをリセットすることができます。管理者は、ユーザーがドメインに再度ログインする前にパスワードを変更する必要があることを伝えるための電子メールを、ユーザーに送信することができます。パスワードのリセット時にドメインからユーザーに電子メールを送信するには、そのドメインに対する電子メールサーバーの設定を行います。

ユーザーが Informatica ドメインと LDAP サーバーからロックアウトされた場合、Informatica の管理者は Informatica ドメインのユーザーアカウントをロック解除することができます。ユーザーは LDAP の管理者も LDAP サーバーのユーザーアカウントをロック解除するまで Informatica ドメインにログインできません。

注: Informatica ドメインで Kerberos ネットワーク認証が使用されている場合、ユーザーアカウントに対してロックアウトを設定することはできません。**［アカウント管理］**ビューが Administrator ツールの **［セキュリティ］**タブで使用できません。

アカウントロックアウトの設定

Informatica ドメイン内の複数回ログインに失敗したユーザーアカウントをロックアウトするアカウントロックアウトオプションを選択します。

1. Administrator ツールで、**［セキュリティ］** > **［アカウント管理］**の順にクリックします。
2. **［アカウントロックアウトの設定］**セクションで、**［編集］**をクリックします。

3. 以下のプロパティを設定します。

プロパティ	説明
アカウントのロックアウトを有効にする	指定したログイン失敗回数を超えたら Informatica ドメインのユーザーアカウントをロックアウトします。このオプションのデフォルトでは、管理者ユーザーのアカウントに対してはロックアウトを行いません。管理者ユーザーアカウントのロックアウトを実行するには、**［管理者アカウントロックアウトを有効にする］**オプションを選択する必要があります。
管理者アカウントのロックアウトを有効にする	指定したログイン失敗回数を超えたら Informatica ドメインの管理者ユーザーアカウントをロックアウトします。管理者ユーザーアカウントに対するロックアウトの実行を可能にするには、その前に **［アカウントロックアウトを有効にする］**オプションを選択する必要があります。
ログインの許容最大試行回数	ユーザーアカウントが Informatica ドメインからロックアウトされるまでの許容最大連続ログイン失敗回数を指定します。

アカウントロックアウトの規則とガイドライン

Informatica ユーザーに対するアカウントのロックアウトを実行するときには、次のルールとガイドラインを考慮してください。

- アプリケーションサービスがユーザーアカウントで実行され、入力されたパスワードが誤りの場合、アプリケーションサービスを開始しようとすると、そのユーザーアカウントはロックされます。 データ統合サービス、Web サービス Hub サービス、および PowerCenter 統合サービスは、モデルリポジトリサービスまたは PowerCenter リポジトリサービスでの認証にユーザー名とパスワードを使用する、復元性が高いアプリケーションサービスです。 データ統合サービス、Web サービス Hub サービス、または PowerCenter 統合サービスが、ログインの失敗後に繰り返し再起動を試行する場合、最終的にドメインは関連するユーザーアカウントをロックします。
- LDAP ユーザーアカウントが Informatica ドメインと LDAP 認証サーバーからロックアウトされた場合、Informatica ドメインの管理者は Informatica ドメイン内のユーザーアカウントをロック解除することができます。LDAP サーバー内のユーザーアカウントのロック解除は、LDAP 管理者が行うことができます。
- Informatica ドメイン内と LDAP サーバー内のアカウントのロックアウトを有効にする場合、Informatica ドメイン内と LDAP サーバー内で同じしきい値をログイン失敗回数に設定しておけば、アカウントロックアウトポリシーについての混乱を避けることができます。
- Informatica ドメインでアカウントのロックアウトを有効にしていないにもかかわらずユーザーがロックアウトされた場合、そのユーザーが LDAP サーバーからロックアウトされていないか確認します。

第 9 章

特権およびロール

この章では、以下の項目について説明します。

特権およびロールの概要

特権およびロールがあるユーザーセキュリティを管理します。

PowerCenter Express のライセンスのタイプにより特権およびロールを変更できます。

特権

特権により、ユーザーがアプリケーションクライアントで実行できるアクションが決定されます。Informatica には、以下の特権が含まれます。

- ドメイン特権。ユーザーが Administrator ツール、infacmd および pmrep コマンドラインプログラムを使用して、Informatica ドメイン上で実行できるアクションを決定します。
- ドメイン特権。ユーザーが Administrator ツールを使用して実行できる Informatica ドメインでのアクションを決定します。

- アナリストサービス特権。 ユーザーが Informatica Analyst を使用して実行できるアクションを決定します。
- コンテンツ管理サービス特権。ユーザーが Informatica Developer ツールと Informatica Analyst ツールで参照テーブルを使用して実行できるアクションを決定します。
- データ統合サービス特権。 ユーザーが Administrator ツールおよび infacmd コマンドラインプログラムを使用して実行できるアプリケーションでのアクションを決定します。また、この特権によって、ユーザーがプロファイル結果のドリルダウンおよびエクスポートを実行できるかどうかも決まります。
- データ統合サービス特権。ユーザーが Administrator ツールを使用して実行できるアプリケーションでのアクションを決定します。また、この特権によって、ユーザーがプロファイル結果のドリルダウンおよびエクスポートを実行できるかどうかも決まります。
- Metadata Manager サービス特権。ユーザーが Metadata Manager を使用して実行できるアクションを決定します。
- モデルリポジトリサービス特権。 ユーザーが Informatica Analyst および Informatica Developer を使用して実行できるプロジェクトでのアクションを決定します。
- モデルリポジトリサービス特権。 ユーザーが Informatica Developer を使用して実行できるプロジェクトでのアクションを決定します。
- PowerCenter リポジトリサービス特権。 ユーザーが Repository Manager、Designer、Workflow Manager、Workflow Monitor、pmrep および pmcmd コマンドラインプログラムを使用して実行できる PowerCenter リポジトリアクションを決定します。
- PowerExchange アプリケーションサービス特権。 PowerExchange リスナサービスおよび PowerExchange ロガーサービスで、ユーザーが infacmd pwx コマンドを使用して実行できるアクションを決定します。
- スケジューラサービス特権。ユーザーがスケジューラサービスを使用して実行できるアクションを決定します。
- Test Data Manager サービス特権。Test Data Manager を使用して実行できるタスク（データ検出、データマスキング、データサブセット、およびテストデータ生成）を決定します。

特権により、ユーザーがアプリケーションクライアントで実行できるアクションが決定されます。Informatica には、Administrator ツールを使用してユーザーが実行できるアクションを決定するドメイン特権が含まれます。

アプリケーションサービスのユーザーおよびグループに特権を割り当てます。同一サービスタイプの各アプリケーションサービスのユーザーに対して、さまざまな特権を割り当てることができます。

Administrator ツールの［**セキュリティ**］タブで、ユーザーおよびグループに特権を割り当てます。

Administrator ツールにより、権限がレベル別に整理されます。 特権は、その特権に含まれる特権の下に表示されます。一部の特権は、他の特権を含みます。ユーザーおよびグループに特権を割り当てる場合、Administrator ツールでは、特権に含まれるすべての特権も割り当てられます。

特権グループ

ドメイン特権およびアプリケーションサービス特権は、特権グループに編成されます。特権グループとは、ユーザーアクションを定義する特権を体系的に組織化したものです。例えば、ドメイン特権には次の特権グループが含まれます。

- ツール。Administrator ツールにログインする権限が含まれます。
- セキュリティ管理。ユーザー、グループ、ロールおよび特権を管理する特権を含みます。
- ドメイン管理。ドメイン、フォルダ、ノード、グリッド、ライセンス、およびアプリケーションサービスを管理する特権を含みます。

- ドメイン管理。ドメイン、フォルダ、およびアプリケーションサービスを管理する特権を含みます。
- セキュリティ管理。ユーザー、グループ、ロールおよび特権を管理する特権を含みます。
- ドメイン管理。ドメイン、フォルダ、ノード、グリッド、ライセンス、およびアプリケーションサービスを管理する特権を含みます。
- ツール。Administrator ツールにログインする権限が含まれます。
- 監視。Ultra Messaging デプロイメントを監視して統計を表示する特権を含みます。

ヒント: ユーザーおよびユーザーグループに特権を割り当てる場合、グループ内のすべての特権を割り当てるための特権グループを選択することができます。

ロール

ロールとは、ユーザーまたはグループに割り当てる特権の集合です。組織内の各ユーザーは、デベロッパ、管理者、基本ユーザー、上級ユーザーなどの特定のロールを持ちます。

例えば、PowerCenter デベロッパロールには、デベロッパが実行する PowerCenter リポジトリサービス特権やアクションがすべて含まれます。

ドメインのユーザーとグループ、およびドメイン内のアプリケーションサービスのユーザーとグループにロールを割り当てます。

ヒント: ユーザーをグループに編成し、次にグループにロールと権限を割り当てると、ユーザー管理タスクを簡単にすることができます。例えば、ユーザーの組織内の地位が変更された場合、そのユーザーを別のグループに移動します。新しいユーザーが組織に加わった場合は、そのユーザーをグループに追加します。ユーザーはグループに割り当てられたロールと権限を継承します。特権、ロール、権限を再割り当てする必要はありません。詳細については、Informatica How-To ライブラリに掲載した「https://kb.informatica.com/h2l/HowTo%20Library/1/0236-GroupsAndRolesToManageAccessControl.pdf」という記事を参照してください。

ヒント: ユーザーをグループに編成し、次にグループにロールと権限を割り当てると、ユーザー管理タスクを簡単にすることができます。例えば、ユーザーの組織内の地位が変更された場合、そのユーザーを別のグループに移動します。新しいユーザーが組織に加わった場合は、そのユーザーをグループに追加します。ユーザーはグループに割り当てられたロールと権限を継承します。特権、ロール、権限を再割り当てする必要はありません。

ドメイン特権

ドメイン特権により、ユーザーが Administrator ツール、infacmd および pmrep コマンドラインプログラムを使用して実行できるアクションが決定されます。

ドメイン特権により、Administrator ツールを使用して実行できるアクションが決定されます。

次の表に、各ドメイン特権グループについて示します。

特権グループ	説明
セキュリティ管理	ユーザー、グループ、ロールおよび特権を管理する特権を含みます。
ドメイン管理	ドメイン、フォルダ、ノード、グリッド、ライセンス、アプリケーションサービス、および接続を管理する特権を含みます。

特権グループ	説明
監視	監視統計とレポートを設定し、統合オブジェクトの監視を表示し、監視にアクセスする特権を含みます。
ツール	Administrator ツールにログインする権限が含まれます。
Cloud 管理	Administrator ツールに Informatica Cloud 組織を追加して表示する特権が含まれます。

特権グループ	説明
セキュリティ管理	ユーザー、グループ、ロールおよび特権を管理する特権を含みます。
ドメイン管理	ドメイン、アプリケーションサービス、および接続を管理する特権を含みます。
監視	監視統計とレポートを設定し、統合オブジェクトの監視を表示し、監視にアクセスする特権を含みます。
ツール	Administrator ツールにログインする権限が含まれます。

特権グループ	説明
セキュリティ管理	ユーザー、グループ、ロールおよび特権を管理する特権を含みます。
ドメイン管理	ドメイン、アプリケーションサービス、および接続を管理する特権を含みます。
監視	UM デプロイメントを監視して統計を表示する特権を含みます。
ツール	Administrator ツールにログインする権限が含まれます。

セキュリティ管理特権グループ

ユーザーが実行を許可されるセキュリティ管理アクションは、セキュリティ管理特権グループ内の特権、およびドメイン権限によって規定されます。

一部のセキュリティ管理タスクは、特権や権限によってではなく、管理者ロールによって規定されます。

一部のセキュリティ管理タスクは、特権や権限によってではなく、管理者ロールによって規定されます。管理者は、次の作業を実行できます。

- オペレーティングシステムプロファイルの作成、編集、および削除。
- オペレーティングシステムプロファイルに対する権限の付与。

注: Administrator ツールのセキュリティ管理タスクを完了するには、ユーザーは Access Informatica Administrator の特権も持っている必要があります。

権限とロールの付与特権

権限とロールの付与特権が割り当てられているユーザーは特権とロールをユーザーとグループに割り当てることができます。

次の表に、必要な権限とユーザーが権限とロールの付与特権で実行できるアクションを示します。

権限	説明
ドメインまたはアプリケーションサービス	ユーザーは、以下のアクションを実行できます。 - ドメインまたはアプリケーションサービスのユーザーやグループに対する特権とロールの割り当て。 - ユーザーやグループに割り当てられた特権とロールの編集、および削除。

ユーザー、グループ、およびロールの管理特権

ユーザー、グループ、およびロールの管理特権が割り当てられたユーザーは、LDAP 認証を設定し、ユーザー、グループ、およびロールを管理できます。

ユーザー、グループ、およびロールの管理特権には、権限とロールの付与特権が含まれます。

次の表に、必要な権限とユーザーがユーザー、グループ、およびロールの管理特権で実行できるアクションを示します。

権限	説明
-	ユーザーは、以下のアクションを実行できます。 - ドメインに対して LDAP 認証の設定。 - ユーザー、グループ、およびロールの作成、編集、削除。 - LDAP ユーザーおよびグループのインポート。
オペレーティングシステムのプロファイル	ユーザーは、オペレーティングシステムのプロファイルプロパティを編集できます。

ドメイン管理特権グループ

ユーザーが実行可能なドメイン管理アクションは、ドメイン管理グループの特権とドメインオブジェクトの権限によって異なります。

一部のドメイン管理作業は、特権や権限によってではなく管理者ロールによって規定されます。管理者は、次の作業を実行できます。

- ドメインプロパティの設定。
- ドメインに対する権限の付与。
- ログイベントの管理とパージ。
- ドメインアラートの受信。
- ライセンスレポートの実行
- ユーザーアクティビティログのイベントの表示。
- ドメインをシャットダウンする。
- サービスアップグレードウィザードへのアクセス。

ドメインオブジェクトの特権ではなく権限を割り当てられたユーザーは、ドメイン管理タスクの一部を完了できます。次の表に、ドメインオブジェクト権限が割り当てられているユーザーが実行できるアクションを示します。

権限	説明
ドメイン	ユーザーは以下のアクションを実行できます。 - ドメインプロパティおよびログイベントの表示。 - 監視の設定。
フォルダ	ユーザーはフォルダプロパティを表示できます。
アプリケーションサービス	ユーザーはアプリケーションサービスプロパティとログイベントを表示できます。
ライセンスオブジェクト	ユーザーはライセンスオブジェクトプロパティを表示できます。
グリッド	ユーザーはグリッドプロパティを表示できます。
ノード	ユーザーはノードプロパティを表示できます。
Web サービス Hub	ユーザーは Web サービスレポートを実行できます。

注: Administrator ツールのドメイン管理タスクを完了するには、ユーザーは Informatica Administrator の特権も持っている必要があります。

サービス実行の管理特権

サービス実行の管理特権が割り当てられたユーザーは、アプリケーションサービスを有効および無効にでき、アプリケーションサービスの警告を受け取ります。

次の表に、必要な権限とユーザーがサービス実行の管理特権で実行できるアクションを示します。

権限	説明
アプリケーションサービス	ユーザーは、以下のアクションを実行できます。 - アプリケーションサービスとサービスプロセスの有効化および無効化。Metadata Manager Service の有効化または無効化するには、関連する PowerCenter Integration Service および PowerCenter リポジトリサービスについての権限も必要です。 - アプリケーションサービス警告の受信。

権限	説明
アプリケーションサービス	ユーザーは、以下のアクションを実行できます。 - アプリケーションサービスとサービスプロセスの有効化および無効化。 - アプリケーションサービス警告の受信。

サービスの管理特権

サービスの管理特権が割り当てられたユーザーは、アプリケーションサービスとライセンスオブジェクトの作成、移動、削除、および権限の付与ができます。

サービスの管理特権には、サービス実行の管理特権が含まれます。

次の表に、必要な権限とユーザーがサービスの管理特権で実行できるアクションを示します。

権限	説明
ドメインまたは親フォルダ	ユーザーは、ライセンスオブジェクトを作成できます。
ドメインまたは親フォルダ、アプリケーションサービスが実行されるノードまたはグリッド、ライセンスオブジェクト、および任意の関連アプリケーションサービス	ユーザーは、アプリケーションサービスを作成できます。
アプリケーションサービス	ユーザーは、以下のアクションを実行できます。 - アプリケーションサービスの設定。 - アプリケーションサービスに対する権限の付与。
元のフォルダと宛先フォルダ	ユーザーは、フォルダ間でアプリケーションサービスまたはライセンスオブジェクトを移動できます。
ドメインまたは親フォルダ、およびアプリケーションサービス	ユーザーは、アプリケーションサービスを削除できます。
アナリストサービス	ユーザーは、監査証跡テーブルを作成および削除できます。
Metadata Manager サービス	ユーザーは、以下のアクションを実行できます。 - Metadata Manager リポジトリコンテンツをバックアップします。 - Metadata Manager リポジトリコンテンツを削除します。 - Metadata Manager サービスのコンテンツのアップグレード。 **注:** Metadata Manager リポジトリコンテンツを作成またはリストアするには、ユーザーがデフォルトの管理者グループに属している必要があります。
Metadata Manager サービス PowerCenter リポジトリサービス	ユーザーは、Metadata Manager の PowerCenter リポジトリをリストアできます。
モデルリポジトリサービス	ユーザーは、以下のアクションを実行できます。 - モデルリポジトリコンテンツの作成と削除。 - 検索インデックスの作成、削除、再インデックス。 - **［アクション］**メニューまたはコマンドラインからモデルリポジトリサービスのコンテンツをアップグレードします。ユーザーには、モデルリポジトリサービスでのプロジェクトの作成、編集、削除の特権、プロジェクトでの書込み権限も必要です。
PowerCenter 統合サービス	ユーザーは、セーフモードで PowerCenter 統合サービスを実行できます。

権限	説明
PowerCenter リポジトリサービス	ユーザーは、以下のアクションを実行できます。 - PowerCenter リポジトリのバックアップ、リストア、およびアップグレード。 - PowerCenter リポジトリ用データリネージの設定。 - 別の PowerCenter リポジトリからコンテンツをコピーする。 - ユーザー接続の遮断と PowerCenter リポジトリロックの解放。 - PowerCenter リポジトリコンテンツの作成と削除。 - PowerCenter リポジトリ Manager の再利用可能なメタデータエクステンションの作成、編集、削除。 - PowerCenter リポジトリのバージョン管理の有効化。 - PowerCenter リポジトリドメインの管理。 - PowerCenter リポジトリ Manager のリポジトリレベルでの、オブジェクトバージョンの詳細パージの実行。 - PowerCenter リポジトリのプラグインの登録と登録解除。 - PowerCenter リポジトリの排他モードでの実行。 - PowerCenter リポジトリ通知のユーザーへの送信。 - PowerCenter リポジトリ統計の更新。 - PowerCenter リポジトリサービスのコンテンツのアップグレード。
Test Data Manager サービス	ユーザーは、以下のアクションを実行できます。 - Test Data Manager のリポジトリの内容の作成および削除。 - Test Data Manager サービスの内容のアップグレード。
ライセンスオブジェクト	ユーザーは、以下のアクションを実行できます。 - ライセンスオブジェクトの編集。 - ライセンスオブジェクトに対する権限の付与。
ライセンスオブジェクトとアプリケーションサービス	ユーザーは、ライセンスをアプリケーションサービスに割り当てることができます。
ドメインまたは親フォルダ、およびライセンスオブジェクト	ユーザーは、ライセンスオブジェクトを削除できます。

権限	説明
アプリケーションサービスが実行されているドメイン、および任意の関連アプリケーションサービス	ユーザーは、アプリケーションサービスを作成できます。
アプリケーションサービス	ユーザーは、以下のアクションを実行できます。 - アプリケーションサービスの設定。 - アプリケーションサービスに対する権限の付与。
モデルリポジトリサービス	ユーザーは、以下のアクションを実行できます。 - モデルリポジトリコンテンツの作成と削除。 - 検索インデックスの作成、削除、再インデックス。

ノードとグリッドの管理特権

ノードとグリッドの管理特権が割り当てられたユーザーは、ノードとグリッドの作成、設定、移動、削除、シャットダウン、権限の付与ができます。

次の表に、必要な権限とユーザーがノードとグリッドの管理特権で実行できるアクションを示します。

権限	説明
ドメインまたは親フォルダ	ユーザーはノードを作成できます。
ドメインまたは親フォルダ、およびグリッドに割り当てられたノード	ユーザーはグリッドを作成できます。
ノードまたはグリッド	ユーザーは、以下のアクションを実行できます。 - ノードとグリッドの設定、およびシャットダウン。 - ノードとグリッドに対する権限の付与。
元のフォルダーと宛先フォルダー	ユーザーは、フォルダ間でノードとグリッドを移動できます。
ドメインまたは親フォルダ、およびノードまたはグリッド。	ユーザーは、ノードとグリッドを削除できます。

ドメインフォルダーの管理特権

ドメインフォルダーの管理特権が割り当てられたユーザーは、ドメインフォルダーの作成、編集、移動、削除、および権限の付与ができます。

次の表に、必要な権限とユーザーがドメインフォルダーの管理特権で実行できるアクションを示します。

権限	説明
ドメインまたは親フォルダ	ユーザーは、フォルダを作成できます。
フォルダ	ユーザーは、以下のアクションを実行できます。 - フォルダの編集。 - フォルダーに対する権限の付与。
元のフォルダーと宛先フォルダー	ユーザーは親フォルダ間でフォルダを移動できます。
ドメインまたは親フォルダ、および削除対象フォルダ	ユーザーはフォルダを除できます。

接続の管理特権

接続の管理特権が割り当てられたユーザーは、Administrator ツール、Analyst ツール、Developer ツール、infacmd コマンドラインプログラムで、接続を作成、編集、および削除できます。ユーザーは Developer ツールで接続をコピーして、Administrator ツールおよび infacmd コマンドラインプログラムで接続の権限を付与することができます。

接続の管理特権が割り当てられたユーザーは、Administrator ツール、Developer ツール、infacmd コマンドラインプログラムで、接続を作成、編集、および削除できます。ユーザーは Developer ツールで接続をコピーして、Administrator ツールおよび infacmd コマンドラインプログラムで接続の権限を付与することができます。

接続権限が割り当てられているが、接続の管理特権が割り当てられていないユーザーは、次の接続管理アクションを実行できます。

- パスワードを除くすべての接続メタデータを表示する。接続の読み取り権限が必要です。
- データをプレビューするか、マッピング、スコアカード、またはプロファイルを実行する。接続の実行権限が必要です。
- データをプレビューするか、マッピングまたはプロファイルを実行する。接続の実行権限が必要です。

次の表に、必要な権限とユーザーが接続の管理特権で実行できるアクションを示します。

権限	説明
-	ユーザーは接続を作成できます。
接続での書き込み	ユーザーは、接続を作成、編集、および削除できます。
接続への付与	ユーザーは、接続に関する権限を付与および取り消しできます。

監視特権グループ

監視特権グループの特権によって、監視を表示および設定できるユーザーが決まります。

次の表に、必要な権限とユーザーが監視の管理グループの特権で実行できるアクションを示します。

親特権	特権	権限	説明
監視の管理	監視設定	ドメイン	ユーザーが監視設定を設定できます。
監視の管理	レポート設定と統計設定	ドメイン	ユーザーが監視統計およびレポートを設定できます。
表示	ユーザーが属しているグループのすべてのユーザーのジョブを表示	ドメイン	グループ内のユーザーは、グループ内の他のユーザーによって実行されているジョブを監視できます。ユーザーが複数のグループに属している場合、ユーザーはすべてのグループのジョブを確認できます。
ユーザーが属しているグループのすべてのユーザーのジョブを表示	他のユーザーのジョブの表示	ドメイン	ユーザーが他のユーザーのジョブを表示できます。
表示	統計の表示	ドメイン	ユーザーがサマリ統計ビューおよびドメインオブジェクトの統計を表示できます。 **注**: Kerberos 認証を使用するドメインでは、ユーザーは監視のために設定されたモデルリポジトリサービスの管理者ロールも保持している必要があります。
表示	レポートの表示	ドメイン	ユーザーがドメインオブジェクトのレポートを表示できます。

親特権	特権	権限	説明
監視へのアクセス	Analyst ツールからアクセス	ドメイン	ユーザーが Analyst ツールの［ジョブステータス］ワークスペースにアクセスできます。
監視へのアクセス	Developer tool からアクセス	ドメイン	ユーザーが Developer tool から Monitoring ツールにアクセスできます。
監視へのアクセス	Administrator ツールからアクセス	ドメイン	ユーザーが Administrator ツールの［監視］タブにアクセスできます。
該当なし	ジョブに対するアクションの実行	ドメイン	ユーザーは次のアクションを実行できます。 - ジョブの強制終了。 - マッピングジョブの再発行。 - ジョブのログの表示。

Monitoring ツールにアクセスするのに、ユーザーは Informatica Administrator へのアクセス特権は必要ありません。

ツール特権グループ

どのユーザーが Administrator ツールへのアクセスを許可されるかは、ドメインのツールグループ内での特権によって規定されます。

次の表に、必要な権限とユーザーがツールグループ内の特権で実行できるアクションを示します。

特権	説明
Informatica Administrator へのアクセス	ユーザーは、以下のアクションを実行できます。 - Administrator ツールにログインする。 - Administrator ツールでユーザー自身のユーザーアカウントを管理する。 - ログイベントをエクスポートする。

Administrator ツールでタスクを完了するには、ユーザーに Informatica Administrator へのアクセス特権が必要です。infacmd コマンドを実行したり、Monitoring ツールにアクセスするのに、ユーザーは Informatica Administrator へのアクセス特権は必要ありません。

クラウド管理特権グループ

クラウド管理グループの特権で、Informatica Cloud 組織を表示および設定できるユーザーが決定されます。

次の表に、必要な権限とユーザーがクラウド管理グループの特権で実行できるアクションを示します。

特権	権限	説明
組織の表示	ドメイン	ユーザーは、Informatica Cloud 組織、関連するセキュアエージェント、クラウド接続を確認できます。
組織の管理	ドメイン	ユーザーは、Administrator ツールに Informatica Cloud 組織を追加できます。

アナリストサービスの特権

アナリストサービスの特権により、ライセンスされたユーザーが、Analyst ツールを使用してプロジェクトに対して実行できるアクションが決定されます。

以下の表に、プロジェクトおよびプロジェクト内のオブジェクトの管理に必要な特権および権限を示します。

特権	権限	説明
プロファイルおよびスコアカードの実行	プロジェクトの読み取り。 リレーショナルデータソース接続を実行します。	ユーザーは、ライセンスされたユーザーのプロファイルやスコアカードを Analyst ツールで実行できます。
マッピング仕様にアクセス	プロジェクトの読み取り。	ユーザーは、ライセンスされたユーザーのマッピング仕様に Analyst ツールでアクセスできます。
マッピング仕様の結果のロード	プロジェクトへの書き込み。	ユーザーは、ライセンスされたユーザーのマッピング仕様の結果をテーブルまたはフラットファイルにロードできます。 **注**: この特権を選択すると、デフォルトで**マッピング仕様にアクセス**する特権が付与されます。
グロッサリの管理	-	ユーザーがビジネス用語集を管理できます。
用語集の表示	-	ユーザーが［ライブラリ］ワークスペースのパブリッシュされている Business Glossary アセットを表示できます。これは、［用語集のセキュリティ］ワークスペースの用語集および用語集アセットの読み取り権限を付与することと同等です。
ワークスペースアクセス	-	ユーザーが Analyst ツールで次のワークスペースにアクセスできます。 - **［設計］**ワークスペース - **［検出］**ワークスペース - **［用語集］**ワークスペース - **［スコアカード］**ワークスペース **注**: この特権を選択すると、Analyst ツールのプロジェクトへのアクセスも付与されます。この特権を持っていない場合、そのユーザーがプロジェクトにアクセスするには、**［設計ワークスペース］**、**［検出ワークスペース］**、**［用語集ワークスペース］**、**［スコアカードワークスペース］**特権のいずれかを持っている必要があります。
設計ワークスペース	-	ユーザーが**［設計］**ワークスペースにアクセスできます。
検出ワークスペース	-	ユーザーが**［検出］**ワークスペースにアクセスできます。
用語集のワークスペース	-	ユーザーが**［用語集］**ワークスペースにアクセスできます。
スコアカードのワークスペース	-	ユーザーが**［スコアカード］**ワークスペースにアクセスできます。

コンテンツ管理サービス特権

コンテンツ管理サービス特権により、ライセンスユーザーが参照テーブルで実行できるアクションが決定されます。

以下の表に、参照テーブルの管理に必要な特権および権限の一覧を示します。

特権	権限	説明
参照テーブルの作成	プロジェクトへの書き込み	- Analyst および Developer ツールで参照テーブルを作成します。 - infacmd rtm インポートで参照テーブルを作成します。 - 参照テーブルオブジェクトをモデルリポジトリにインポートします。 - Analyst および Developer ツールで参照テーブルをコピーします。 - プロファイルデータから参照テーブルを作成します。 **注**: 作成特権には、デフォルトで編集特権も付与されます。
参照テーブルデータおよびメタデータの編集	プロジェクトの読み取り	- Developer ツールおよび Analyst ツールで、参照テーブルのデータ値を編集します。 - プロファイルデータを参照テーブルに追加します。 - 参照テーブルで列を追加または削除します。列名、説明、デフォルト値など、参照テーブルのメタデータを変更します。

データ統合サービスの特権

データ統合サービスの特権は、ユーザーが Administrator ツールおよび infacmd コマンドラインプログラムを使用して、アプリケーションに対して実行できるアクションを決定します。また、ユーザーが Analyst ツールおよび Developer tool を使用して、プロファイル結果をドリルダウンしてエクスポートできるかどうかも決定します。

データ統合サービスの特権は、ユーザーが Administrator ツールおよび infacmd コマンドラインプログラムを使用して、アプリケーションに対して実行できるアクションを決定します。また、ユーザーが Developer tool を使用して、プロファイル結果をドリルダウンしてエクスポートできるかどうかも決定します。

次の表に、アプリケーション管理特権グループ内の各特権で実行できるアクションを示します。

特権名	説明
アプリケーションの管理	ユーザーは、以下のアクションを実行できます。 - アプリケーションをファイルにバックアップおよびリストアします。 - データ統合サービスへのアプリケーションのデプロイおよび名前の競合の解決。 - デプロイメント後のアプリケーションの起動。 - アプリケーションの検索。 - アプリケーションでのオブジェクトの開始または停止。 - アプリケーションプロパティの設定。

次の表に、必要な権限とユーザーがプロファイリング管理特権グループの特権で実行できるアクションを示します。

特権名	権限	説明
結果のドリルダウンとエクスポート	プロジェクトの読み取り 実データをドリルダウンするには、リレーショナルデータソース接続の実行も必要	ユーザーは、以下のアクションを実行できます。 - プロファイリング結果のドリルダウン。 - プロファイリング結果のエクスポート。

Metadata Manager Service 特権

ユーザーが Metadata Manager を使って実行できる Metadata Manager アクションは、Metadata Manager Service 特権によって決定されます。

次の表に、Metadata Manager の各特権グループについて説明します。

特権グループ	説明
カタログ	Metadata Manager インターフェイスの［参照］ページでオブジェクトを管理する特権を含みます。
ロード	Metadata Manager インターフェイスの［ロード］ページでオブジェクトを管理する特権を含みます。
モデル	Metadata Manager インターフェイスの［モデル］ページでオブジェクトを管理する特権を含みます。
セキュリティ	Metadata Manager インターフェイスの［セキュリティ］ページでオブジェクトを管理する特権を含みます。

カタログ特権グループ

カタログ特権グループ内の特権によって、Metadata Manager アプリケーションの**［参照］**タブでユーザーが実行できるタスクが決まります。特定のアクションを実行する特権を持つユーザーには、特定のオブジェクト

に対してそのアクションを実行する権限も必要です。Metadata Manager アプリケーションの［**セキュリティ**］タブで権限を設定します。

以下の表に、カタログ特権グループの特権、およびオブジェクトに対するアクションの実行に必要な権限の一覧を示します。

特権	含まれる特権	権限	説明
ショートカットの共有	なし	書き込み	ユーザーは、ショートカットが含まれているフォルダを別のユーザーやグループと共有できます。
系列の表示	なし	読み取り	ユーザーは、以下のアクションを実行できます。 - メタデータオブジェクト、カテゴリ、およびビジネス用語に対するデータリネージ分析の実行。 - PowerCenter Designer からのデータリネージ分析の実行。PowerCenter リポジトリフォルダに対する読み取り権限も必要です。
ビュー関連カタログ	なし	読み取り	ユーザーは、関連カタログを表示できます。
プロファイル結果の表示	なし	読み取り	ユーザーは、リレーショナルソースから抽出されたカタログ内でメタデータオブジェクトのプロファイリング情報を表示できます。
カタログの表示	なし	読み取り	ユーザーは、以下のアクションを実行できます。 - メタデータカタログ内のリソースおよびメタデータオブジェクトの表示。 - メタデータカタログの検索。
リレーションの表示	なし	読み取り	ユーザーは、メタデータオブジェクト、カテゴリ、およびビジネス用語のリレーションを表示できます。
リレーションの管理	リレーションの表示	書き込み	ユーザーは、カスタムのメタデータオブジェクト、カテゴリ、およびビジネス用語のリレーションを作成、編集、削除できます。
コメントの表示	なし	読み取り	ユーザーは、メタデータオブジェクト、カテゴリ、およびビジネス用語のコメントを表示できます。
コメントの転記	コメントの表示	書き込み	ユーザーは、メタデータオブジェクト、カテゴリ、およびビジネス用語のコメントを追加できます。
コメントの削除	- コメントの転記 - コメントの表示	書き込み	ユーザーは、メタデータオブジェクト、カテゴリ、およびビジネス用語のコメントを削除できます。
リンクの表示	なし	読み取り	ユーザーは、メタデータオブジェクト、カテゴリ、およびビジネス用語のリンクを表示できます。
リンクの管理	リンクの表示	書き込み	ユーザーは、メタデータオブジェクト、カテゴリ、およびビジネス用語のリンクを作成、編集、および削除できます。

特権	含まれる特権	権限	説明
用語解説の表示	なし	読み取り	ユーザーは、以下のアクションを実行できます。 - **［ビジネス用語集］**ビューにビジネス用語集を表示。 - ビジネス用語集を検索。
オブジェクトの管理	なし	書き込み	ユーザーは、以下のアクションを実行できます。 - カタログ内のメタデータオブジェクトの編集。 - カスタムメタデータオブジェクトの作成、編集、および削除。ユーザーは View Model（モデルの表示）特権も持つ必要があります。 - カスタムメタデータリソースの作成、編集、および削除。ユーザーは Manage Resource（リソースの管理）特権も持つ必要があります。

ロード特権グループ

ロード特権グループ内の特権によって、Metadata Manager アプリケーションの**［ロード］**タブでユーザーが実行できるタスクが決まります。特定のアクションを実行する特権を持つユーザーには、特定のオブジェクトに対してそのアクションを実行する権限も必要です。Metadata Manager アプリケーションの**［セキュリティ］**タブで権限を設定します。

以下の表に、Metadata Manager ウェアハウス内のリソースのインスタンスの管理に必要な特権と権限の一覧を示します。

特権	含まれる特権	権限	説明
リソースの表示	-	読み取り	ユーザーは、以下のアクションを実行できます。 - Metadata Manager ウェアハウス内のリソースおよびリソースプロパティの表示。 - リソース設定をエクスポートする。 - Metadata Manager エージェントインストーラをダウンロードする。
リソースのロード	リソースの表示	書き込み	ユーザーは、以下のアクションを実行できます。 - Metadata Manager ウェアハウスへのリソースのメタデータのロード。* - データリネージのために接続されたリソース内のオブジェクト間のリンクの作成。 - リソースに対する検索インデックス処理の設定。 - リソース設定をインポートする。
スケジュールの管理	リソースの表示	書き込み	ユーザーは、以下のアクションを実行できます。 - スケジュールを作成し編集する。 - リソースにスケジュールを追加する。
メタデータのパージ	リソースの表示	書き込み	ユーザーは、Metadata Manager ウェアハウスからリソースのメタデータを削除できます。
リソースの管理	- メタデータのパージ - リソースの表示	書き込み	ユーザーは、リソースを作成、編集、および削除できます。
* Business Glossary リソースのメタデータをロードするには、リソースのロード、リソースの管理、モデルの表示の各特権が必要です。			

モデル特権グループ

モデル特権グループ内の特権によって、Metadata Manager アプリケーションの［**モデル**］タブでユーザーが実行できるタスクが決まります。モデルに対する権限を設定することはできません。

以下の表に、モデルの管理に必要な特権の一覧を示します。

特権	含まれる特権	権限	説明
モデルの表示	-	-	ユーザーは、モデルとクラスを開き、モデルとクラスのプロパティを表示できます。クラスの関係および属性の表示。
モデルの管理	モデルの表示	-	ユーザーは、カスタムモデルを作成、編集、および削除できます。パッケージモデルとユニバーサルモデルに属性を追加します。
モデルのエクスポート/インポート	モデルの表示	-	ユーザーは、カスタムモデルをインポートおよびエクスポートできます。変更されたパッケージモデルとユニバーサルモデルをインポートおよびエクスポートします。

セキュリティ特権グループ

セキュリティ特権グループ内の特権によって、Metadata Manager アプリケーションの［**セキュリティ**］タブでユーザーが実行できるタスクが決まります。

デフォルトでは、セキュリティ特権グループのカタログ権限の管理特権は、管理者、または Metadata Manager サービスの管理者ロールを持つユーザーに割り当てられています。 カタログ権限の管理特権は他のユーザーに割り当てることができます。

以下の表に、Metadata Manager セキュリティの管理に必要な特権と権限の一覧を示します。

特権	含まれる特権	権限	説明
カタログ権限の管理	-	フルコントロール	ユーザーは、以下のアクションを実行できます。 - リソース、メタデータオブジェクト、カテゴリ、およびビジネス用語に対する権限のユーザおよびグループへの割り当て。 - リソース、メタデータオブジェクト、カテゴリ、およびビジネス用語に対する権限の編集。

モデルリポジトリサービス特権

モデルリポジトリサービス特権は、ユーザーが Informatica Analyst および Informatica Developer を使用してプロジェクトに対して実行できるアクションを規定します。

モデルリポジトリサービス特権は、ユーザーが Informatica Developer を使用してプロジェクトに対して実行できるアクションを規定します。

モデルリポジトリオブジェクト権限によって、プロジェクトでユーザーがオブジェクトに対して実行できるタスクが決まります。

次の表に、必要な権限と、ユーザーがモデルリポジトリサービス特権で実行できるアクションを示します。

特権	権限	説明
該当なし	プロジェクトの読み取り	ユーザーがプロジェクトおよびプロジェクト内のオブジェクトを表示できます。
該当なし	プロジェクトへの書き込み	ユーザーがプロジェクト内のオブジェクトの作成、編集、および削除を行うことができます。
該当なし	プロジェクトへの付与	ユーザーがプロジェクトの権限をユーザーやグループに付与したり取り消すことができます。
Access Analyst	該当なし	ユーザーが Analyst ツールからモデルリポジトリにアクセスできます。
Developer へのアクセス	該当なし	ユーザーが Developer tool からモデルリポジトリにアクセスできます。
プロジェクトの作成、編集、削除	該当なし	ユーザーがプロジェクトを作成できます。
プロジェクトの作成、編集、削除	プロジェクトへの書き込み	ユーザーは次のアクションを実行できます。 - プロジェクトの編集。 - プロジェクトの削除（ユーザーがプロジェクトを作成していた場合）。 - モデルリポジトリサービスのコンテンツのアップグレード。**[アクション]** メニューまたはコマンドラインからサービスをアップグレードするには、ユーザーにドメインに対するサービスの管理特権、およびモデルリポジトリサービスでの権限も必要です。サービスのアップグレードウィザードを使用してサービスをアップグレードするには、ユーザーにドメインに対する管理者ロールも必要です。
データドメインの管理	該当なし	ユーザーがデータドメイングロッサリ内のデータドメインの作成、編集、および削除を行うことができます。この特権は、**データドメイン管理**特権グループの一部です。
通知の管理	該当なし	ユーザーがスコアカード通知を設定できます。この特権は、**プロファイリング管理**特権グループの一部です。
チームベース開発の管理	該当なし	ユーザーは、モデルリポジトリオブジェクトのロック状態またはロック解除状態を管理できます。モデルリポジトリがバージョン管理システムと統合されている場合、ユーザーはオブジェクトのチェックアウト状態またはチェックイン状態を管理できます。ユーザーは、チェックアウトされたオブジェクトの所有権も管理できます。
セキュリティの詳細の表示	該当なし	ユーザーが次の詳細を表示できます。 - 読み取り権限を持っていないプロジェクトの名前 - エラーメッセージおよび警告メッセージの詳細

特権	権限	説明
該当なし	プロジェクトの読み取り	ユーザーがプロジェクトおよびプロジェクト内のオブジェクトを表示できます。
該当なし	プロジェクトへの書き込み	ユーザーがプロジェクト内のオブジェクトの作成、編集、および削除を行うことができます。

特権	権限	説明
該当なし	プロジェクトへの付与	ユーザーがプロジェクトの権限をユーザーやグループに付与したり取り消すことができます。
Developer へのアクセス	該当なし	ユーザーが Developer tool からモデルリポジトリにアクセスできます。
プロジェクトの作成、編集、削除	該当なし	ユーザーは次のアクションを実行できます。 - プロジェクトの作成。 - モデルリポジトリサービスのアップグレード。
プロジェクトの作成、編集、削除	プロジェクトへの書き込み	ユーザーは次のアクションを実行できます。 - プロジェクトの編集。 - プロジェクトの削除（ユーザーがプロジェクトを作成していた場合）。
セキュリティの詳細の表示	該当なし	ユーザーが次の詳細を表示できます。 - 読み取り権限を持っていないプロジェクトの名前 - エラーメッセージおよび警告メッセージの詳細

PowerCenter リポジトリサービス特権

PowerCenter リポジトリサービス特権によって、ユーザーが PowerCenter Repository Manager、Designer、Workflow Manager、Workflow Monitor、pmrep および pmcmd コマンドラインプログラムを使用して実行できる PowerCenter リポジトリアクションが決定されます。

次の表に、PowerCenter リポジトリサービスの各特権グループについて説明します。

特権グループ	説明
ツール	PowerCenter Client ツールおよびコマンドラインプログラムにアクセスする特権を含みます。
フォルダ	リポジトリフォルダを管理する特権を含みます。
デザインオブジェクト	ビジネスコンポーネント、マッピングパラメータ、マッピング変数、マッピング、マップレット、トランスフォーメーション、およびユーザー定義関数を管理する特権を含みます。
ソースおよびターゲット	キューブ、次元、ソース定義、およびターゲット定義を管理する特権を含みます。
ランタイムオブジェクト	セッション設定オブジェクト、タスク、ワークフロー、ワークレットを管理する特権を含みます。
グローバルオブジェクト	接続オブジェクト、デプロイメントグループ、ラベル、クエリーを管理する特権を含みます。

ユーザーは、Repository Manager で以下のアクションを行うためには、PowerCenter リポジトリサービスで Manage Services ドメイン特権および権限を持つ必要があります。

- PowerCenter リポジトリレベルでオブジェクトバージョンの詳細パージを実行する。

- 再利用可能なメタデータエクステンションを作成、編集、および削除する。

ツール特権グループ

PowerCenter リポジトリサービスのツール特権グループ内の特権によって、ユーザーがアクセスできる PowerCenter Client のツールおよびコマンドラインプログラムが決定されます。

以下の表に、ツールグループ内での特権に対してユーザーが実行できるアクションを一覧表示します。

特権	権限	説明
Designer へのアクセス	-	ユーザーは Designer を使用して PowerCenter リポジトリに接続できます。
リポジトリマネージャへのアクセス	-	ユーザーは、以下のアクションを実行できます。 - Repository Manager を使用して PowerCenter リポジトリへ接続する。 - *pmrep* コマンドを実行する。
Workflow Manager へのアクセス	-	ユーザーは、以下のアクションを実行できます。 - Workflow Manager を使用して PowerCenter リポジトリへ接続する。 - Workflow Manager から PowerCenter 統合サービスを削除する。
Workflow Monitor へのアクセス	-	ユーザーは、以下のアクションを実行できます。 - Workflow Monitor を使用して PowerCenter リポジトリへ接続する。 - Workflow Monitor で PowerCenter 統合サービスへ接続する。

注: PowerCenter 統合サービスがセーフモードで実行されている場合、ユーザーは関連する PowerCenter リポジトリサービスに対する管理者ロールが必要です。

ツール特権グループ内での適切な特権は、PowerCenter Client ツールおよびコマンドラインプログラム内でタスクを完了させるすべてのユーザーのために必要とされています。 例えば、Repository Manager 内にフォルダーを作成するためには、ユーザーはフォルダーの作成の特権、および Repository Manager へのアクセス特権が必要です。

ユーザーは、ツール特権グループ内での特権および PowerCenter リポジトリオブジェクトに対する権限を持っていても、そのオブジェクトタイプを変更する特権は持っていない場合は、オブジェクトに対する一部のアクションは引き続き実行することができます。 例えば、ユーザーは Repository Manager へのアクセス特権、および一部のフォルダーに対する読み取り権限があります。 ユーザーはフォルダー特権グループ内での特権を何も持っていません。ユーザーはフォルダー内のオブジェクトを表示し、フォルダーどうしを比較することができます。

フォルダー特権グループ

フォルダー管理アクションは、フォルダー特権グループ内の特権、PowerCenter リポジトリオブジェクト権限および、ドメインオブジェクト権限によって決定されます。ユーザーは、Repository Manager で、pmrep コマンドラインプログラムを使用して、フォルダー管理アクションを実行します。

一部のフォルダー管理タスクは、特権や権限によってではなく、フォルダー所有権および管理者ロールによって決定されます。PowerCenter リポジトリサービスの管理者ロールが割り当てられたフォルダーの所有者またはユーザーは、以下のフォルダー管理タスクを実行することができます。

- PowerCenter Integration Service でオペレーティングシステムプロファイルが使用される場合、フォルダーにオペレーティングシステムプロファイルを割り当てます。 オペレーティングシステムプロファイルに対する権限が必要です。
- フォルダのオーナーの変更。
- フォルダ権限の設定。
- フォルダの削除。
- 共有するフォルダの指定。
- フォルダ名と説明の編集。

フォルダー権限が割り当てられているが、特権が割り当てられていないユーザーは、一部のフォルダー管理アクションを実行できます。次の表に、フォルダー権限のみが割り当てられているユーザーが実行できるアクションを示します。

権限	説明
フォルダーに対する読み取り	ユーザーは、以下のアクションを実行できます。 - フォルダーの比較。 - フォルダ内のオブジェクトの表示。

注: フォルダーでアクションを実行するには、ユーザーは Access Repository Manager の特権も所有している必要があります。

フォルダーの作成特権

フォルダーの作成特権が割り当てられたユーザーは PowerCenter リポジトリフォルダーを作成できます。

次の表に、必要な権限とユーザーがフォルダーの作成特権で実行できるアクションを示します。

権限	説明
-	ユーザーは、フォルダを作成できます。

フォルダーのコピー特権

フォルダーのコピー特権が割り当てられたユーザーは、PowerCenter リポジトリ内で、または別の PowerCenter リポジトリへファイルをコピーできます。

次の表に、必要な権限とユーザーがフォルダーコピーの特権で実行できるアクションを示します。

権限	説明
フォルダーに対する読み取り	ユーザーは、同じ PowerCenter リポジトリ内、または別の PowerCenter リポジトリにフォルダをコピーできます。ユーザーは、宛先リポジトリでのフォルダー作成特権も持っている必要があります。

フォルダーのバージョン管理

チームベースの開発オプションがある場合、ユーザーに、バージョン管理された PowerCenter リポジトリでのフォルダーのバージョン管理特権を割り当てます。 ユーザーは、フォルダーのステータスの変更、およびフォルダーレベルでのオブジェクトバージョンの詳細パージの実行ができます。

次の表に、必要な権限とユーザーがフォルダーのバージョン管理特権で実行できるアクションを示します。

権限	説明
フォルダに対する読み取りおよび書き込み	ユーザーは、以下のアクションを実行できます。 - フォルダのステータスの変更。 - フォルダレベルでのオブジェクトバージョンの詳細パージの実行。

Design Objects 特権グループ

Design Objects 特権グループ内での特権、および PowerCenter リポジトリオブジェクト権限により、以下のデザインオブジェクト上でユーザーが実行できるアクションが決定されます。

- ビジネスコンポーネント
- マッピングパラメータとマッピング変数。
- マッピング
- マプレット
- トランスフォーメーション
- ユーザー定義関数

権限が割り当てられているが特権が割り当てられていないユーザーは、デザインオブジェクトに対して一部のアクションを実行できます。次の表に、権限のみが割り当てられているユーザーが実行できるアクションを示します。

権限	説明
フォルダーに対する読み取り	ユーザーは、以下のアクションを実行できます。 - デザインオブジェクトの比較。 - デザインオブジェクトをイメージとしてコピー。 - デザインオブジェクトのエクスポート。 - カスタムトランスフォーメーションおよびエクスターナルプロシージャ用コードの生成。 - PowerCenter リポジトリ通知メッセージを受信する。 - デザインオブジェクトに対するデータリネージの実行。ユーザーは、Metadata Manage Service に対するリネージの表示特権と、Metadata Manager カタログのメタデータオブジェクトに対する読み取り権限も必要になります。 - デザインオブジェクトの検索。 - デザインオブジェクト、デザインオブジェクト依存性、およびデザインオブジェクト履歴の表示。
共有フォルダーに対する読み取り 宛先フォルダに対する読み取りおよび書き込み	ユーザーはショートカットを作成できます。

注: デザインオブジェクトに対してアクションを実行するには、ツール特権グループ内での適切な特権も必要です。

デザインオブジェクトの作成、編集、および削除特権

デザインオブジェクトの作成、編集、および削除特権が割り当てられたユーザーは、ビジネスコンポーネント、マッピングパラメータ、マッピング変数、マッピング、マップレット、トランスフォーメーション、ユーザー定義関数を作成、編集、および削除できます。

次の表に、必要な権限とユーザーがデザインオブジェクトの作成、編集、および削除特権で実行できるアクションを示します。

権限	説明
元のフォルダに対する読み取り 宛先フォルダに対する読み取りおよび書き込み	ユーザーは、以下のアクションを実行できます。 - デザインオブジェクトをフォルダー間でコピー。 - デザインオブジェクトを別の PowerCenter リポジトリにコピー。 ユーザーは、接続先リポジトリ内でのデザインオブジェクトの作成、編集および削除の特権も持っている必要があります。
フォルダに対する読み取りおよび書き込み	ユーザーは、以下のアクションを実行できます。 - バージョン管理されているデザインオブジェクトのコメントの変更。 - チェックイン、およびユーザー自身のユーザーアカウントでチェックアウトされたデザインオブジェクトのチェックアウトの取り消し。 - デザインオブジェクトのチェックアウト。 - 同じフォルダ内のデザインオブジェクトのコピーおよび貼り付け。 - データプロファイルの作成、編集および削除、Profile Manager の起動。ユーザーはランタイムオブジェクトの作成、編集および削除の特権も持っている必要があります。 - デザインオブジェクトの作成、編集および削除。 - SAP ABAP プログラムの生成と消去。 - ビジネスコンテンツ統合マッピングの生成。ユーザーはソースとターゲットの作成、編集および削除の特権も持っている必要があります。 - Designer でのデザインオブジェクトのインポート。ユーザーはソースとターゲットの作成、編集および削除の特権も持っている必要があります。 - Repository Manager を使用した、デザインオブジェクトのインポート。ユーザーはランタイムオブジェクトの作成、編集および削除の特権、ソースとターゲットの作成、編集および削除の特権も持っている必要があります。 - 以前のデザインオブジェクトのバージョンへの復帰。 - マッピング、マプレット、およびユーザー定義関数の検証。

デザインオブジェクトのバージョン管理

チームベースの開発オプションがある場合、ユーザーに、バージョン管理された PowerCenter リポジトリでのデザインオブジェクトのバージョン管理特権を割り当てます。 ユーザーは、デザインオブジェクトのバージョンのステータスの変更、リカバリ、消去ができます。さらに、ユーザーはチェックインおよび他のユーザーによって行われたチェックアウトの取り消しもできます。

デザインオブジェクトのバージョン管理特権には、デザインオブジェクトの作成、編集、および削除特権が含まれます。

次の表に、必要な権限とユーザーがデザインオブジェクトのバージョン管理特権で実行できるアクションを示します。

権限	説明
フォルダに対する読み取りおよび書き込み	ユーザーは、以下のアクションを実行できます。 - デザインオブジェクトのステータスの変更。 - チェックイン、および他のユーザーによってチェックアウトされたデザインオブジェクトのチェックアウトの取り消し。 - デザインオブジェクトのバージョンのパージ。 - 削除されたデザインオブジェクトの復旧。

ソースおよびターゲットの特権グループ

ソースおよびターゲットの特権グループ内の特権、および PowerCenter リポジトリオブジェクト権限により、以下のソースおよびターゲットオブジェクト上でユーザーが実行できるアクションが決定されます。

- キューブ
- 次元
- ソース定義
- ターゲット定義

権限が割り当てられているが、特権が割り当てられていないユーザーは、ソースおよびターゲットオブジェクトに対して一部のアクションを実行できます。次の表に、権限のみが割り当てられているユーザーが実行できるアクションを示します。

権限	説明
フォルダーに対する読み取り	ユーザーは、以下のアクションを実行できます。 - ソースオブジェクトとターゲットオブジェクトとの比較。 - ソースオブジェクトとターゲットオブジェクトのエクスポート。 - ソースデータとターゲットデータのプレビュー。 - PowerCenter リポジトリ通知メッセージを受信する。 - ソースオブジェクトおよびターゲットオブジェクトに対するデータリネージの実行。ユーザーは、Metadata Manage Service に対するリネージの表示特権と、Metadata Manager カタログのメタデータオブジェクトに対する読み取り権限も必要になります。 - ソースオブジェクトとターゲットオブジェクトの検索。 - ソースオブジェクトとターゲットオブジェクト、ソースオブジェクトとターゲットオブジェクトの依存性、およびソースオブジェクトとターゲットオブジェクトの履歴の表示。
共有フォルダーに対する読み取り 宛先フォルダに対する読み取りおよび書き込み	ショートカットの作成。

注: ソースオブジェクトとターゲットオブジェクトに対してアクションを実行するには、ツール特権グループ内での適切な特権も必要です。

ソースおよびターゲットの作成、編集、および削除特権

ソースおよびターゲットの作成、編集、および削除特権が割り当てられたユーザーは、キューブ、次元、ソース定義、ターゲット定義を作成、編集、および削除できます。

次の表に、必要な権限とユーザーがソースおよびターゲットの作成、編集、および削除特権で実行できるアクションを示します。

権限	説明
元のフォルダに対する読み取り 宛先フォルダに対する読み取りおよび書き込み	ユーザーは、以下のアクションを実行できます。 - ソースオブジェクトとターゲットオブジェクトを別のフォルダーにコピーする。 - ソースオブジェクトとターゲットオブジェクトを別の PowerCenter リポジトリにコピーする。 ユーザーは、接続先リポジトリ内でのソースおよびターゲットの作成、編集および削除の特権も持っている必要があります。
フォルダに対する読み取りおよび書き込み	ユーザーは、以下のアクションを実行できます。 - バージョン管理されているソースまたはターゲットオブジェクトのコメントの変更。 - チェックイン、およびユーザー自身のユーザーアカウントでチェックアウトされたソースオブジェクトおよびターゲットオブジェクトのチェックアウトの取り消し。 - ソースオブジェクトおよびターゲットオブジェクトのチェックアウト。 - 同じフォルダ内のソースオブジェクトとターゲットオブジェクトのコピーおよび貼り付け。 - ソースオブジェクトとターゲットオブジェクトの作成、編集、および削除。 - SAP 関数のインポート。 - Designer を使用した、ソースオブジェクトとターゲットオブジェクトのインポート。デザインオブジェクトの作成、編集、および削除の特権が必要です。 - Repository Manager を使用した、ソースオブジェクトとターゲットオブジェクトのインポート。ユーザーは、デザインオブジェクトとランタイムオブジェクトに対する作成、編集および削除の特権も持っている必要があります。 - リレーショナルデータベース内にターゲットを作成する SQL の生成、および実行。 - ソースオブジェクトまたはターゲットオブジェクトのバージョンへの復帰。

ソースおよびターゲットのバージョン管理特権

チームベースの開発オプションがある場合、ユーザーに、バージョン管理された PowerCenter リポジトリでのソースおよびターゲットのバージョン管理特権を割り当てます。 ユーザーはソースおよびターゲットオブジェクトのバージョンのステータスの変更、リカバリ、消去ができます。さらに、ユーザーはチェックインおよび他のユーザーによって行われたチェックアウトの取り消しもできます。

ソースおよびターゲットのバージョン管理特権には、ソースおよびターゲットの作成、編集、および削除特権が含まれます。

次の表に、必要な権限とユーザーがソースおよびターゲットのバージョン管理特権で実行できるアクションを示します。

権限	説明
フォルダに対する読み取りおよび書き込み	ユーザーは、以下のアクションを実行できます。 - ソースオブジェクトとターゲットオブジェクトのステータスの変更。 - チェックイン、および他のユーザーによってチェックアウトされたソースオブジェクトおよびターゲットオブジェクトのチェックアウトの取り消し。 - ソースオブジェクトとターゲットオブジェクトのパージ。 - 削除されたソースオブジェクトとターゲットオブジェクトの復旧。

ランタイムオブジェクト特権グループ

ランタイムオブジェクト特権グループ内の特権、PowerCenter リポジトリオブジェクトの権限、およびドメインオブジェクトの権限により、以下のランタイムオブジェクトに対してユーザーが実行できるアクションが決定されます。

- セッション設定オブジェクト
- タスク
- ワークフロー
- ワークレット

ランタイムオブジェクトの一部のタスクは、特権や権限によってではなく管理者ロールによって決定されます。 PowerCenter リポジトリサービスの管理者ロールが割り当てられたユーザーは、Workflow Manager のナビゲータから PowerCenter Integration Service を削除することができます。

権限が割り当てられているが、特権が割り当てられていないユーザーはランタイムオブジェクトに対して一部のアクションを実行できます。次の表に、権限のみが割り当てられているユーザーが実行できるアクションを示します。

権限	説明
フォルダーに対する読み取り	ユーザーは、以下のアクションを実行できます。 - ランタイムオブジェクトの比較。 - ランタイムオブジェクトオブジェクトのエクスポート。 - PowerCenter リポジトリ通知メッセージを受信する。 - ランタイムオブジェクトの検索。 - セッションでの、マッピングパラメータおよびマッピング変数の使用。 - ランタイムオブジェクト、ランタイムオブジェクト依存性、およびランタイムオブジェクト履歴の表示。
フォルダーに対する読み取りおよび実行	ユーザー自身のユーザーアカウントによって開始されたタスクおよびワークフローの停止および強制終了。 PowerCenter Integration Service がセーフモードで実行されている場合、ユーザーは関連する PowerCenter リポジトリサービスに対する管理者ロールが必要です。

注: ランタイムオブジェクトに対して操作を実行するには、ユーザーはツール特権グループ内での適切な特権も必要です。

ランタイムオブジェクトの作成、編集、および削除特権

ランタイムオブジェクトの作成、編集、および削除特権が割り当てられたユーザーは、セッション設定オブジェクト、タスク、ワークフロー、ワークレットを作成、編集、および削除できます。

次の表に、必要な権限とユーザーがランタイムオブジェクトの作成、編集、および削除特権で実行できるアクションを示します。

権限	説明
元のフォルダに対する読み取り 宛先フォルダに対する読み取りおよび書き込み	ユーザーは、以下のアクションを実行できます。 - タスク、ワークフロー、またはワークレットをフォルダー間でコピーする。 - タスク、ワークフロー、またはワークレットを別の PowerCenter リポジトリにコピーする。 ユーザーは、接続先リポジトリ内でのランタイムオブジェクトの作成、編集、および削除の特権も持っている必要があります。
フォルダに対する読み取りおよび書き込み	ユーザーは、以下のアクションを実行できます。 - ワークフローのプロパティで PowerCenter Integration Service をワークフローに割り当てる。 - サービスレベルをワークフローに割り当てる。 - バージョン管理されているランタイムオブジェクトのコメントの変更。 - チェックイン、およびユーザー自身のユーザーアカウントでチェックアウトされたランタイムオブジェクトのチェックアウトの取り消し。 - ランタイムオブジェクトのチェックアウト。 - 同じフォルダ内のタスク、ワークフロー、およびワークレットのコピー、貼り付け。 - データプロファイルの作成、編集および削除、Profile Manager の起動。デザインオブジェクトの作成、編集、および削除の特権が必要です。 - セッション設定オブジェクトの作成、編集、および削除。 - タスク、ワークフロー、およびワークレットの削除と検証。 - Repository Manager を使用した、ランタイムオブジェクトのインポート。ユーザーは、デザインオブジェクトの作成、編集、および削除の特権のほか、ソースとターゲットの作成、編集、および削除の特権も持っている必要があります。 - Workflow Manager を使用した、ランタイムオブジェクトのインポート。 - 以前のオブジェクトのバージョンへの復帰。
フォルダに対する読み取りおよび書き込み 接続オブジェクトに対する読み取り	ユーザーは、以下のアクションを実行できます。 - タスク、ワークフロー、およびワークレットの作成と編集。 - 接続を使用する全セッションのリレーショナルデータベース接続の置換。

ランタイムオブジェクトのバージョン管理特権

チームベースの開発オプションを所有している場合、バージョン管理された PowerCenter リポジトリでユーザーにランタイムオブジェクトのバージョン管理特権を割り当てます。 ユーザーはランタイムオブジェクトのバージョンのステータスの変更、復元、消去ができます。さらに、ユーザーはチェックインおよび他のユーザーによって行われたチェックアウトの取り消しもできます。

ランタイムオブジェクトのバージョン管理特権には、ランタイムオブジェクトの作成、編集、および削除特権が含まれます。

次の表に、必要な権限とユーザーがランタイムオブジェクトのバージョン管理特権で実行できるアクションを示します。

権限	説明
フォルダに対する読み取りおよび書き込み	ユーザーは、以下のアクションを実行できます。 - ランタイムオブジェクトのステータスの変更。 - チェックイン、および他のユーザーによってチェックアウトされたランタイムオブジェクトのチェックアウトの取り消し。 - ランタイムオブジェクトのバージョンのパージ。 - 削除されたランタイムオブジェクトの復旧。

ランタイムオブジェクトのモニタ特権

ランタイムオブジェクトのモニタ特権が割り当てられたユーザーは、Workflow Monitor で、ワークフローおよびタスクを監視できます。

次の表に、必要な権限とユーザーがランタイムオブジェクトのモニタ特権で実行できるアクションを示します。

権限	ユーザーに付与される権限
フォルダーに対する読み取り	ユーザーは、以下のアクションを実行できます。 - Workflow Monitor でのランタイムオブジェクトのプロパティの表示。 - Workflow Monitor での、セッションログおよびワークフローログの表示。 - Workflow Monitor でのパフォーマンス詳細の表示。 PowerCenter Integration Service がセーフモードで実行されている場合、ユーザーは関連する PowerCenter リポジトリサービスに対する管理者ロールが必要です。

ランタイムオブジェクトの実行特権

ランタイムオブジェクトの実行特権が割り当てられているユーザーはタスクとワークフローを起動、コールドスタート、およびリカバリできます。

ランタイムオブジェクトの実行特権には、ランタイムオブジェクトのモニタ特権が含まれます。

次の表に、必要な権限とユーザーがランタイムオブジェクトの実行特権で実行できるアクションを示します。

権限	説明
フォルダーに対する読み取りおよび実行	ユーザーは、[サービス] メニューまたはナビゲータを使用して PowerCenter Integration Service をワークフローに割り当てることができます。
フォルダに対する読み取り、書き込み、および実行 接続オブジェクトに対する読み取りおよび実行	ユーザーは、デバッグ用セッションインスタンスを作成するかまたは既存の再利用可能なセッションを使用して、マッピングをデバッグできます。ユーザーはランタイムオブジェクトを作成、編集および削除する特権も持っている必要があります。 PowerCenter Integration Service がセーフモードで実行されている場合、ユーザーは関連する PowerCenter リポジトリサービスに対する管理者ロールが必要です。

権限	説明
フォルダーに対する読み取りおよび実行 接続オブジェクトに対する読み取りおよび実行	ユーザーは、既存の再利用不可能なセッションを使用してマッピングをデバッグできます。 PowerCenter Integration Service がセーフモードで実行されている場合、ユーザーは関連する PowerCenter リポジトリサービスに対する管理者ロールが必要です。
フォルダーに対する読み取りおよび実行 接続オブジェクトに対する読み取りおよび実行	ユーザーは、以下のアクションを実行できます。 - タスクおよびワークフローのスタート、コールドスタート、およびリスタート。 - ユーザー自身のユーザーアカウントによって開始されたタスクおよびワークフローのリカバリ。 PowerCenter Integration Service でオペレーティングシステムプロファイルが使用されている場合、ユーザーはそのオペレーティングシステムプロファイルに対する権限も必要です。 PowerCenter Integration Service がセーフモードで実行されている場合、ユーザーは関連する PowerCenter リポジトリサービスに対する管理者ロールが必要です。

ランタイムオブジェクトの実行の管理特権

ランタイムオブジェクトの実行の管理特権が割り当てられたユーザーは、ワークフローをスケジュールおよびスケジュール解除できます。さらに、ユーザーは他のユーザーによって開始されたタスクとワークフローを停止、強制終了、およびリカバリすることもできます。

ランタイムオブジェクトの実行の管理特権には、ランタイムオブジェクトの実行特権とランタイムオブジェクトのモニタ特権が含まれます。

次の表に、必要な権限とユーザーがランタイムオブジェクトの実行の管理特権で実行できるアクションを示します。

権限	説明
フォルダーに対する読み取りおよび実行	ユーザーは、ワークフローとセッションログのエントリを削除できます。
フォルダーに対する読み取りおよび実行	ユーザーは、以下のアクションを実行できます。 - 他のユーザーによって開始されたタスクとワークフローの停止、および強制終了。 - 自動的に復旧されたタスクの停止および強制終了。 - ワークフローのスケジュールの解除。 PowerCenter Integration Service がセーフモードで実行されている場合、ユーザーは関連する PowerCenter リポジトリサービスに対する管理者ロールが必要です。

権限	説明
フォルダーに対する読み取りおよび実行 接続オブジェクトに対する読み取りおよび実行	ユーザーは、以下のアクションを実行できます。 - 他のユーザーによって開始されたタスクおよびワークフローの復旧。 - 自動的に復旧されたタスクの復旧。 PowerCenter Integration Service でオペレーティングシステムプロファイルが使用されている場合、ユーザーはそのオペレーティングシステムプロファイルに対する権限も必要です。 PowerCenter Integration Service がセーフモードで実行されている場合、ユーザーは関連する PowerCenter リポジトリサービスに対する管理者ロールが必要です。
フォルダに対する読み取り、書き込み、および実行 接続オブジェクトに対する読み取りおよび実行	ユーザーは、以下のアクションを実行できます。 - ［ワークフロー］-［スケジューラ］メニューからの再利用可能なスケジューラの作成および編集。 - ワークフロープロパティからの再利用不可能なスケジューラの編集。 - ワークフロープロパティからの再利用可能なスケジューラの編集。ユーザーはランタイムオブジェクトの作成、編集および削除の特権も持っている必要があります。 PowerCenter Integration Service でオペレーティングシステムプロファイルが使用されている場合、ユーザーはそのオペレーティングシステムプロファイルに対する権限も必要です。 PowerCenter Integration Service がセーフモードで実行されている場合、ユーザーは関連する PowerCenter リポジトリサービスに対する管理者ロールが必要です。

グローバルオブジェクト特権グループ

グローバルオブジェクト特権グループ内での特権、および PowerCenter リポジトリオブジェクト権限により、以下のグローバルオブジェクト上でユーザーが実行できるアクションが決定されます。

- 接続オブジェクト
- デプロイメントグループ
- ラベル
- クエリ（Q）

グローバルオブジェクト作業は、特権や権限によってではなく、グローバルオブジェクト所有権および管理者ロールによって規定されます。PowerCenter リポジトリサービスに対する管理者ロールを割り当てられたグローバルオブジェクトのオーナーまたはユーザーは、以下のグローバルオブジェクトタスクを実行できます。

- グローバルオブジェクト権限の設定。
- グローバルオブジェクトのオーナーの変更。
- グローバルオブジェクトの削除。

権限が割り当てられているが、特権が割り当てられていないユーザーは、グローバルオブジェクトに対して一部のアクションを実行できます。次の表に、権限のみが割り当てられているユーザーが実行できるアクションを示します。

権限	説明
接続オブジェクトに対する読み取り	ユーザーは接続オブジェクトを表示できます。
デプロイメントグループに対する読み取り	ユーザーはデプロイメントグループを表示できます。

権限	説明
ラベルに対する読み取り	ユーザーはラベルを表示できます。
クエリに対する読み取り	ユーザーはオブジェクトクエリを表示できます。
接続オブジェクトに対する読み取りおよび書き込み	ユーザーは接続オブジェクトを編集できます。
ラベルに対する読み取りおよび書き込み	ユーザーはラベルを編集およびロックできます。
クエリに対する読み取りおよび書き込み	ユーザーは、オブジェクトクエリを編集および検証できます。
クエリに対する読み取りおよび実行	ユーザーはオブジェクトクエリを実行できます。
フォルダーに対する読み取り ラベルに対する読み取りおよび実行	ユーザーは、ラベルの適用とラベル参照の削除を実行できます。

注: グローバルオブジェクトに対してアクションを実行するには、ツール特権グループ内での適切な特権も必要です。

接続の作成特権

接続の作成特権が割り当てられたユーザーは接続オブジェクトを作成できます。

次の表に、必要な権限とユーザーが接続の作成特権で実行できるアクションを示します。

権限	説明
-	ユーザーは、接続オブジェクトを作成およびコピーできます。

デプロイメントグループの管理特権

チームベースの開発オプションがある場合、バージョン管理された PowerCenter リポジトリでのデプロイメントグループの管理特権を割り当てられたユーザーは、デプロイメントグループを作成、編集、コピー、またはロールバックすることができます。 バージョン管理されないリポジトリでは、ユーザーはデプロイメントグループを作成、編集、コピー、およびロールバックできます。

次の表に、必要な権限とユーザーがデプロイメントグループの管理特権で実行できるアクションを示します。

権限	説明
-	ユーザーはデプロイメントグループを作成できます。
デプロイメントグループに対する読み取りおよび書き込み	ユーザーは、以下のアクションを実行できます。 - デプロイメントグループの編集。 - デプロイメントグループからオブジェクトを削除。
元のフォルダに対する読み取り デプロイメントグループに対する読み取りおよび書き込み	ユーザーは、デプロイメントグループにオブジェクトを追加できます。

権限	説明
元のフォルダに対する読み取り 宛先フォルダに対する読み取りおよび書き込み デプロイメントグループに対する読み取りおよび実行	ユーザーはデプロイメントグループをコピーできます。
宛先フォルダに対する読み取りおよび書き込み	ユーザーはデプロイメントグループをロールバックできます。

デプロイメントグループの実行特権

デプロイメントグループの実行特権が割り当てられているユーザーは、ターゲットフォルダーへの書き込み権限がなくても、デプロイメントグループをコピーできます。

次の表に、必要な権限とユーザーがデプロイメントグループの実行特権で実行できるアクションを示します。

権限	説明
元のフォルダーに対する読み取り デプロイメントグループに対する実行	ユーザーはデプロイメントグループをコピーできます。

ラベルの作成特権

チームベース開発オプションがある場合、ラベルの作成権限を割り当てられたユーザーは、バージョン管理された PowerCenter リポジトリでラベルを作成できます。

次の表に、必要な権限とユーザーがラベルの作成特権で実行できるアクションを示します。

権限	説明
-	ユーザーは、ラベルを作成できます。

クエリーの作成特権

クエリーの作成特権が割り当てられたユーザーはオブジェクトクエリーを作成できます。

次の表に、必要な権限とユーザーがクエリーの作成特権で実行できるアクションを示します。

権限	説明
-	ユーザーは、オブジェクトクエリを作成できます。

PowerExchange Listener サービス特権

PowerExchange Listener サービス特権によって、ユーザーが実行できる infacmd pwx コマンドが決定されます。

次の表に、情報コマンド特権グループの PowerExchange Listener サービス特権について説明します。

特権名	説明
listtask	infacmd pwx ListTaskListener コマンドを実行します。

次の表に、管理コマンド特権グループの PowerExchange Listener サービス特権について説明します。

特権名	説明
close	infacmd pwx CloseListener コマンドを実行します。
closeforce	infacmd pwx CloseForceListener コマンドを実行します。
stoptask	infacmd pwx StopTaskListener コマンドを実行します。

PowerExchange ロッガーサービス特権

PowerExchange ロッガーサービス特権によって、ユーザーが実行できる infacmd pwx コマンドが決定されます。

次の表に、情報コマンド特権グループの PowerExchange ロッガーサービス特権について説明します。

特権名	説明
displayall	infacmd pwx DisplayAllLogger コマンドを実行します。
displaycpu	infacmd pwx DisplayCPULogger コマンドを実行します。
displaycheckpoints	infacmd pwx DisplayCheckpointsLogger コマンドを実行します。
displayevents	infacmd pwx DisplayEventsLogger コマンドを実行します。
displaymemory	infacmd pwx DisplayMemoryLogger コマンドを実行します。
displayrecords	infacmd pwx DisplayRecordsLogger コマンドを実行します。
displaystatus	infacmd pwx DisplayStatusLogger コマンドを実行します。

次の表に、管理コマンド特権グループの PowerExchange ロッガーサービス特権について説明します。

特権名	説明
condense	infacmd pwx CondenseLogger コマンドを実行します。
fileswitch	infacmd pwx FileSwitchLogger コマンドを実行します。
shutdown	infacmd pwx ShutDownLogger コマンドを実行します。

スケジューラサービス特権

スケジューラサービス特権によって、ユーザーがスケジュールおよびスケジュールされたジョブに対して実行できるアクションが決まります。

次の表に、スケジューラサービスの特権と必要な権限を示します。

特権	説明	権限が必要な対象
スケジュールの作成	ユーザーがスケジュールを作成できます。スケジュールを作成する場合、ユーザーには、データ統合サービスに対するアプリケーション管理権限も必要です。	- スケジューラサービス - ユーザーがスケジュールするジョブを実行するデータ統合サービス
スケジュールの編集	ユーザーがスケジュールを編集、一時停止、および再開できます。スケジュールを編集する場合、ユーザーには、データ統合サービスに対するアプリケーション管理権限も必要です。	- スケジューラサービス - ユーザーがスケジュールするジョブを実行するデータ統合サービス
スケジュールの削除	ユーザーがスケジュールを削除できます。	スケジューラサービス
スケジュールの表示	ユーザーが**［スケジュール］**ビューおよびスケジュールを表示できます。	スケジューラサービス

Test Data Manager サービスの特権

Test Data Manager サービスの特権は、ユーザーが Test Data Manager を使用して実行できるアクションを決定します。Administrator ツールの**［セキュリティ］**タブで特権を設定します。

以下の表で、Test Data Manager の各特権グループについて説明します。

特権グループ	説明
管理	Informatica Administrator での接続およびロールの作成と管理、ユーザーおよびユーザーグループへの特権の割り当て、リポジトリの管理、ライセンスの追加、ワークフローとプロジェクト属性のセットアップを行う特権が含まれます。 **注**: ユーザーとグループを作成する前に、デフォルトの Informatica Administrator ユーザーは、セキュリティ管理者特権をテストデータ管理者ユーザーに割り当てる必要があります。
データドメイン	この特権により、Test Data Manager でデータドメインを表示および管理することができます。
データマスキング	この特権により、Test Data Manager でマスキングルールとポリシーの割り当てを表示および管理することができます。
データサブセット	この特権により、エンティティ、グループ、テンプレートなどのサブセットオブジェクトを Test Data Manager で表示および管理することができます。
ポリシー	この特権により、Test Data Manager でポリシーを表示および管理することができます。

特権グループ	説明
プロジェクト	この特権により、プロジェクトの表示と管理、メタデータの監査とインポート、プランとワークフローの実行などを Test Data Manager で行うことができます。
ルール	この特権により、Test Data Manager でマスキングルールと生成ルールを表示および管理することができます。
データ生成	この特権により、Test Data Manager でテストデータの生成を表示および管理することができます。

管理特権グループ

管理特権グループの特権は、テストデータ管理者が実行できる管理タスクを決定します。

以下の表に、管理特権グループの特権、およびオブジェクトに対するタスクの実行に必要な権限の一覧を示します。

特権	含まれる特権	権限	説明
設定の管理	-	書き込み	ユーザーは Informatica Administrator と Test Data Manager に対して、次のアクションを実行できます。 - ロールの作成。 - ロールの編集。 - ロールの削除。 - ロールの表示。 - ロールとユーザーの関連付け。 - 特権とユーザーの関連付け。 - ロールとユーザーグループの関連付け。 - 特権とユーザーグループの関連付け。 - ライセンスの追加。 - TDM リポジトリのセットアップ。 - PowerCenter リポジトリのセットアップ。 - データドメインの機密度のセットアップ。 - Test Data Warehouse リポジトリの設定。 - Test Data Warehouse の設定。 - プロジェクトのカスタム属性のセットアップ。 - ワークフロー生成属性のセットアップ。 - Data Discovery の有効化。 - プロファイリングサービスのセットアップ。 - 管理オブジェクトの表示。 - キーワード検索のインデックス処理オプションの設定。
接続の表示	-	読み取り	ユーザーは Test Data Manager で［接続］ページで、次のアクションを実行できます。 - 接続の表示。 - 接続のテスト。
接続の管理	接続の表示	書き込み	ユーザーは Test Data Manager で［接続］ページで、次のアクションを実行できます。 - 接続の作成。 - 接続の編集。 - 接続の削除。 - 接続の表示。 - 接続のテスト。 - Test Data Warehouse リポジトリの設定。 - Test Data Warehouse の設定。

接続特権グループ

接続特権グループの特権によって、ユーザーが TDM Workbench の［接続］ページで実行できるタスクが決まります。次の表に、接続特権グループの特権、およびオブジェクトに対するタスクの実行に必要な権限を示します。

特権	含まれる特権	権限	説明
接続の表示	-	読み取り	ユーザーは TDM Workbench で、接続の表示と接続のテストができます。
接続の管理	接続の表示	書き込み	ユーザーは、TDM Workbench の［接続］ページで、次のアクションを実行できます。 - 接続の作成。 - 接続の編集。 - 接続の削除。 - 接続の表示。 - 接続のテスト。

データドメイン特権グループ

データドメインという特権グループの特権は、Test Data Manager の［ポリシー］ページ内のデータドメインでユーザーが実行できるタスクを決定します。

以下の表に、データドメイン特権グループの特権、およびオブジェクトに対するタスクの実行に必要な権限の一覧を示します。

の特権	含まれる特権	権限	説明
データドメインの表示	-	読み取り	ユーザーは Test Data Manager でデータドメインを確認することができます。
データドメインの管理	データドメインの表示	書き込み	ユーザーは Test Data Manager でデータドメインに対して次のアクションを実行できます。 - データドメインの作成。 - データドメインの編集。 - データドメインの削除。 - データドメインの表示。

データマスキング特権グループ

データマスキングという特権グループの特権は、Test Data Manager の［プロジェクト | 定義 | データマスキング］ビューでユーザーが実行できるタスクを決定します。このビューからテーブルカラムにルールとポリシーを割り当てることができます。

以下の表に、データマスキング特権グループの特権、およびオブジェクトに対するタスクの実行に必要な権限の一覧を示します。

の特権	含まれる特権	権限	説明
データマスキングの表示	-	読み取り	ユーザーは Test Data Manager でデータマスキングの割り当てを確認することができます。
データマスキングの管理	データマスキングの表示	書き込み	ユーザーは、次に挙げるデータマスキング割り当てアクションを Test Data Manager で実行することができます。 - ルールとポリシーの割り当ての追加。 - ルールとポリシーの割り当ての削除。 - ルールプロパティのオーバーライド。 - データマスキング割り当ての表示。

データサブセット特権グループ

データサブセットという特権グループの特権は、Test Data Manager のデータサブセットオブジェクトでユーザーが実行できるタスクを決定します。

以下の表に、Data Subset 特権グループの特権、およびオブジェクトに対するタスクの実行に必要な権限の一覧を示します。

の特権	含まれる特権	権限	説明
データサブセットの表示	-	読み取り	ユーザーは、次に挙げるデータサブセットアクションを Test Data Manager で実行することができます。 - グループの表示。 - テンプレートの表示。 - エンティティの表示。 - 最近のプロジェクトオブジェクトの表示。
データサブセットの管理	データサブセットの表示	書き込み	ユーザーは、次に挙げるデータサブセットアクションを Test Data Manager で実行することができます。 - グループの作成。 - グループの編集。 - グループの削除。 - グループパラメータの追加。 - テンプレートの作成。 - テンプレートの編集。 - テンプレートの削除。 - テンプレートパラメータの追加。 - エンティティの作成。 - エンティティの編集。 - エンティティの削除。 - エンティティ条件の追加。 - リレーションの有効化。 - リレーションの無効化。 - リレーションの編集。 - 変更の確認と実行。 - 変更の確認を完了としてマーク。

ポリシー特権グループ

ポリシーという特権グループの特権は、Test Data Manager でポリシーに対してユーザーが実行できるタスクを決定します。

以下の表に、ポリシー特権グループの特権、およびオブジェクトに対するタスクの実行に必要な権限の一覧を示します。

の特権	含まれる特権	権限	説明
ポリシーの表示	-	読み取り	ユーザーは Test Data Manager でポリシーを確認することができます。
ポリシーの管理	ポリシーの表示	書き込み	ユーザーは、次に挙げるポリシーアクションを Test Data Manager で実行することができます。 - ポリシーの作成。 - ポリシーの編集。 - ポリシーの削除。 - ポリシーの表示。

プロジェクト特権グループ

プロジェクトという特権グループの特権は、Test Data Manager でプロジェクトに対してユーザーが実行できるタスクを決定します。

以下の表に、プロジェクト特権グループの特権、およびオブジェクトに対するタスクの実行に必要な権限の一覧を示します。

特権	含まれる特権	権限	説明
プロジェクトの表示	-	読み取り	ユーザーは Test Data Manager でプロジェクトに対して次のアクションを実行できます。 - プロジェクトの表示。 - プランの表示。 - プラン詳細レポートの表示。 - プラン監査レポートの表示。 - 最近のプロジェクトの表示。 - Test Data Warehouse プランの作成 - Test Data Warehouse プランの管理 - Test Data Warehouse プランの生成 - Test Data Warehouse プランの実行
プロジェクトの管理	プロジェクトの表示	書き込み	ユーザーは Test Data Manager でプロジェクトに対して次のアクションを実行できます。 - プロジェクトの作成。 - プロジェクトの編集。 - プロジェクトの削除。 - プロジェクトの表示。 - ユーザーとプロジェクトの関連付け。 - ユーザーグループとプロジェクトの関連付け。 - ルールとプロジェクトの関連付けと削除。 - ポリシーとプロジェクトの関連付けと削除。 - プランの作成。 - プランの編集。 - プランの削除。 - プランの生成。

特権	含まれる特権	権限	説明
プロジェクトの検出	-	書き込み	ユーザーは Test Data Manager でプロジェクトに対して次の検出アクションを実行できます。 - テーブルの分類。 - 検出を完了としてマーク。 - データドメインとカラムの関連付け。 - カラムを制限ありとしてマーク。 - カラムを機密としてマーク。 - 類似の値を持つカラムを設定。 - 類似の値を持つカラムを削除。 - プライマリキーの追加。 - プライマリキーの削除。 - 論理制約の作成。 - 論理制約の表示。 - 論理制約の編集。 - 論理制約の削除。 - プロジェクトの表示。 - プロファイル済みデータドメインの表示。 - プロファイル済みデータドメインの承認または却下。 - データドメイン分類を完了としてマーク。 - プロファイル済みプライマリキーの表示。 - プロファイル済みプライマリキーの承認または却下。 - プライマリキーの検出を完了としてマーク。 - プロファイル済みエンティティの表示。 - プロファイル済みエンティティの承認または却下。 - エンティティ検出を完了としてマーク。 - プロジェクトリスク分析の表示。 - 最近のプロジェクト機密データ分布の表示。
プロジェクトの生成	-	書き込み	ユーザーは Test Data Manager でワークフローを生成することができます。
プロジェクトの実行	-	書き込み	ユーザーは Test Data Manager でプロジェクトに対して次の実行アクションを行うことができます。 - プランの実行。 - ワークフローの実行。 - ワークフローの停止。 - ワークフローの中断。 - ワークフローのリカバリ。 - プラン実行の表示。
プロジェクトの監視	-	読み取り	ユーザーは Test Data Manager でプロジェクトに対して次の監視アクションを実行できます。 - プロジェクトジョブの監視。 - プロジェクトジョブのログの表示。 - 複数プロジェクトにわたるジョブの監視。 - 複数プロジェクトにわたるジョブのログを表示。

特権	含まれる特権	権限	説明
プロジェクトの監査	-	読み取り	ユーザーは Test Data Manager でプロジェクトとプランに対する最近のアクティビティを確認できます。
メタデータのインポート	-	書き込み	ユーザーは Test Data Manager でプロジェクトに対して次のアクションを実行できます。 - ソースのインポート。 - ソースの削除。

注: プロジェクトの管理特権を持っているユーザーは、少なくとも以下のレベルの権限を持ち、各コンポーネントでプランを作成できる必要があります。

- 管理特権グループから接続を表示する。プラン作成用。
- データサブセット特権グループからデータサブセットを表示する。サブセットコンポーネントでのプラン作成用。
- ルール特権グループからマスキングルールを表示する。マスキングコンポーネントでのプラン作成用。
- ルール特権グループから生成ルールを表示する。生成コンポーネントでのプラン作成用。

ルール特権グループ

ルールという特権グループの特権は、Test Data Manager でデータマスキングルールとデータ生成ルールに対してユーザーが実行できるタスクを決定します。

以下の表に、データマスキング特権グループの特権、およびオブジェクトに対するタスクの実行に必要な権限の一覧を示します。

の特権	含まれる特権	権限	説明
マスキングルールの表示	-	読み取り	ユーザーは Test Data Manager でマスキングルールを確認することができます。
マスキングルールの管理	マスキングルールの表示	書き込み	ユーザーは Test Data Manager でデータマスキングルールに対して次のアクションを実行できます。 - マスキングルールの作成。 - マスキングルールの編集。 - マスキングルールの削除。 - マスキングルールの表示。

の特権	含まれる特権	権限	説明
生成ルールの表示	-	読み取り	ユーザーは Test Data Manager で生成ルールを確認することができます。
生成ルールの管理	生成ルールの表示	書き込み	ユーザーは Test Data Manager でデータ生成ルールに対して次のアクションを実行できます。 - 生成ルールの作成。 - 生成ルールの編集。 - 生成ルールの削除。 - 生成ルールの表示。

データ生成特権グループ

データ生成という特権グループの特権は、ユーザーが Test Data Manager で実行できるテストデータの生成タスクを決定します。

以下の表に、データ生成特権グループの特権、およびオブジェクトに対するタスクの実行に必要な権限の一覧を示します。

の特権	含まれる特権	権限	説明
データ生成の表示	-	読み取り	ユーザーは Test Data Manager でデータ生成ルールの割り当てを確認することができます。
データ生成の管理	データ生成の表示	書き込み	ユーザーは Test Data Manager でデータ生成に対して次に挙げるアクションを実行できます。 - データ生成ルール割り当ての表示 - データ生成ルール割り当ての追加。 - データ生成ルール割り当ての削除。 - データ生成ルール割り当てのオーバーライド。

ロールの管理

ロールとは、ユーザーおよびグループへの割り当ての可能な特権の集まりです。ユーザーによる割り当ての可能なロールには、次の種類があります。

- システム定義。編集または削除ができないロール。
- カスタム。作成、編集、削除ができないロール。

ロールには、ドメインまたはアプリケーションサービスのタイプに応じた特権が含まれます。ドメイン内のアプリケーションサービスごとにドメインのユーザーまたはグループにロールを割り当てます。例えば、PowerCenter リポジトリサービスの特権が含まれるデベロッパロールを作成することができます。 ドメインには、複数の PowerCenter リポジトリサービスを含めることができます。 Development PowerCenter リポジトリサービスのユーザーに、デベロッパロールを割り当てることができます。 Production PowerCenter リポジトリサービスのユーザーに異なるロールを割り当てることができます。

ロールには、ドメインまたはアプリケーションサービスのタイプに応じた特権が含まれます。ドメイン内のアプリケーションサービスごとにドメインのユーザーまたはグループにロールを割り当てます。

ロールには、ドメインまたはアプリケーションサービスのタイプに応じた特権が含まれます。ドメイン内のアプリケーションサービスごとにドメインのユーザーまたはグループにロールを割り当てます。

UMSM には、以下のタイプのロールがあります。

- 管理者。Administrator ツールを管理する特権を持つ、システム定義のロールです。このロールでは、ユーザーアカウントの作成および管理、Ultra Messaging サービスの作成および設定、UMSM コンポーネントの設定、および UM のデプロイメントの実行ができます。
- オペレータ。UM のデプロイメントを監視する特権を持つ、カスタムロールです。

ナビゲータの［ロール］セクションでロールを選択するときは、ドメインおよびアプリケーションサービスのロールを直接割り当てられたユーザおよびグループを、すべて表示することができます。ロールの割り当ては、ユーザ/グループ別またはサービス別に表示することができます。［割り当て］セクションにリストされたユーザまたはグループにナビゲートするには、ユーザまたはグループを右クリックして、［Navigate to Item（アイテムへのナビゲート）］を選択します。

ユーザーはシステム定義ロールおよびカスタムロールを検索することができます。

システム定義のロール

システム定義のロールとは、ユーザーによる編集/削除が許可されていないロールです。管理者ロールは、システム定義のロールです。

ドメイン、アナリストサービス、データ統合サービス、Metadata Manager サービス、モデルリポジトリサービス、または PowerCenter リポジトリサービスのユーザーまたはグループに管理者ロールを割り当てると、そのユーザーまたはグループは、サービスに対するすべての特権を付与されます。管理者ロールでは、権限のチェックが省略されます。 管理者ロールを持つユーザーは、サービスで管理されるすべてのオブジェクトにアクセスすることができます。

ドメイン、データ統合サービス、モデルリポジトリサービスのユーザーまたはグループに管理者ロールを割り当てると、そのユーザーまたはグループは、サービスに対するすべての特権を付与されます。管理者ロールでは、権限のチェックが省略されます。 管理者ロールを持つユーザーは、サービスで管理されるすべてのオブジェクトにアクセスすることができます。

ドメイン、または Ultra Messaging サービスのユーザーまたはグループに管理者ロールを割り当てると、そのユーザーまたはグループは、そのサービスに対するすべての特権を付与されます。管理者ロールでは、権限のチェックが省略されます。 管理者ロールを持つユーザーは、サービスで管理されるすべてのオブジェクトにアクセスすることができます。

管理者ロール

ドメイン、データ統合サービス、または PowerCenter リポジトリサービスのユーザーまたはグループに管理者ロールを割り当てる際、そのユーザーまたはグループは、特権または権限ではなく、管理者ロールによって決定される一部のタスクを実行することができます。

管理者ロールをドメインまたはデータ統合サービスのユーザまたはグループに割り当てると、そのユーザまたはグループは、特権または権限によってではなく管理者ロールによって規定された一部のタスクを完了できます。

管理者ロールをドメインまたは Ultra Messaging サービスのユーザーまたはグループに割り当てると、そのユーザーまたはグループは、特権または権限によってではなく管理者ロールによって規定された一部のタスクを完了できます。

ユーザーまたはグループにドメイン、データ統合サービス、または PowerCenter リポジトリサービスに対するすべての特権を割り当て、その後、そのユーザーまたはグループに、すべてのドメインまたは PowerCenter

リポジトリオブジェクトに対する完全な権限を付与することができます。 ただし、このユーザーまたはグループは、管理者ロールによって決定されているタスクを完了させることはできません。

ユーザーまたはグループにドメインまたはデータ統合サービスに対するすべての特権を割り当て、その後、そのユーザーまたはグループに、すべてのドメインに対する完全な権限を付与することができます。 ただし、このユーザーまたはグループは、管理者ロールによって決定されているタスクを完了させることはできません。

ユーザーまたはグループにドメインまたは Ultra Messaging サービスに対するすべての特権を割り当て、その後、そのユーザーまたはグループに、すべてのドメインオブジェクトに対する完全な権限を付与することができます。ただし、このユーザーまたはグループは、管理者ロールによって決定されているタスクを完了させることはできません。

例えば、ドメインの管理者ロールが割り当てられているユーザーは、Administrator ツールでドメインのプロパティを設定することができます。 ドメインでのすべてのドメイン特権および権限を割り当てられたユーザーは、ドメインプロパティを設定することができません。

以下の表に、ドメイン、データ統合サービス、および PowerCenter リポジトリサービスの管理者ロールによって決定されるタスクを示します。

以下の表に、ドメインまたはデータ統合サービスの管理者ロールによって決定されるタスクを一覧表示します。

以下の表に、ドメインまたは Ultra Messaging サービスの管理者ロールによって決定されるタスクを一覧表示します。

サービス	タスク
ドメイン	- ドメインプロパティの設定。 - オペレーティングシステムプロファイルの作成。 - オペレーティングシステムのプロファイルの削除。 - ドメインおよびオペレーティングシステムのプロファイルに対する権限の付与。 - ログイベントの管理とパージ。 - ドメインアラートの受信。 - ライセンスレポートの実行 - ユーザーアクティビティログのイベントの表示。 - ドメインをシャットダウンする。 - サービスアップグレードウィザードへのアクセス。
データ統合サービス	- ［アクション］メニューによるデータ統合サービスのアップグレード。
PowerCenter リポジトリサービス	- PowerCenter 統合サービスがオペレーティングシステムのプロファイルを使用する場合、オペレーティングシステムのプロファイルをリポジトリフォルダに割り当てる。* - フォルダおよびオブジェクトのオーナーの変更。* - フォルダ権限およびグローバルオブジェクト権限の設定。* - PowerCenter 統合サービスをセーフモードで実行している場合、PowerCenter クライアントから PowerCenter 統合サービスに接続する。 - Workflow Manager のナビゲータから PowerCenter 統合サービスを削除する。 - フォルダやグローバルオブジェクトにアクセスするためのユーザー権限とグループ権限が管理できます。* - 共有するフォルダの指定。* - フォルダの名前および説明の編集。* *PowerCenter リポジトリフォルダのオーナー、またはグローバルオブジェクトのオーナーも、これらのタスクを実行することができる。

サービス	タスク
ドメイン	- ドメインプロパティの設定。 - ドメインに対する権限の付与 - ログイベントの管理とパージ。 - ドメインアラートの受信。 - ユーザーアクティビティログのイベントの表示。

サービス	タスク
ドメイン	- ドメインプロパティの設定。 - ドメインに対する権限の付与 - ログイベントの管理とパージ。 - ドメインアラートの受信。

サービス	タスク
	- ユーザーアクティビティログのイベントの表示。

カスタムロール

カスタムロールとは、ユーザーが編集または削除できるロールです。

デフォルトでは、Administrator ツールには次のカスタムロールが含まれています。

- アナリストサービスのカスタムロール
- Metadata Manager サービスのカスタムロール
- 演算子カスタムロール
- PowerCenter リポジトリサービスのカスタムロール
- Test Data Manager サービスのカスタムロール

これらのロールの権限を編集したり、ロールを削除したりできます。 独自のカスタムロールを作成することもできます。

カスタムロールの作成

カスタムロールを作成するときは、ドメインまたはアプリケーションサービスタイプに対応したロールに特権を割り当てます。ロールには 1 つまたは複数のサービスに対する特権を含めることができます。

1. Administrator ツールで、［セキュリティ］タブをクリックします。
2. ［セキュリティアクション］メニューで、［ロールの作成］をクリックします。
   ［ロールの作成］ダイアログボックスが表示されます。
3. ロールの以下のプロパティを入力します。

プロパティ	説明
Name	ロールの名前。ロールの名前には大文字と小文字の区別があり、128 文字を超えることはできません。 タブ、改行文字、または以下の特殊文字は使用できません。 , + " \ < > ; / * % ? 名前には、先頭と末尾の文字以外に ASCII スペース文字を使用できます。その他のすべてのスペース文字は許可されません。
説明	ロールの説明。説明は、765 文字を超えることや、タブ、改行文字、または以下の特殊文字を含めることはできません。 < > "

4. ［特権］タブをクリックします。
5. ドメインまたはアプリケーションサービスタイプを展開します。
6. ドメインまたはアプリケーションサービスタイプに応じてロールに割り当てる特権を選択します。
7. ［OK］をクリックします。

カスタムロールのプロパティの編集

カスタムロールを編集するときは、ロールのプロパティを変更することができます。ロールの名前は変更することができません。

1. Administrator ツールで、［セキュリティ］タブをクリックします。
2. ナビゲータのロールのセクションで、［ロール］を選択します。
3. ［編集］をクリックします。
4. ロールの説明を変更し、［OK］ をクリックします。

カスタムロールに割り当てられた特権の編集

ユーザーは、ドメイン用のカスタムロール、および各アプリケーションサービスタイプ用のカスタムロールに割り当てられた特権を変更することができます。

1. Administrator ツールで、［セキュリティ］タブをクリックします。
2. ナビゲータの［ロール］セクションで、ロールを選択します。
3. ［特権］タブをクリックします。
4. ［編集］をクリックします。

   ［Edit Roles and Privileges（ロールと特権の編集）］ダイアログボックスが表示されます。
5. ドメインまたはアプリケーションサービスタイプを展開します。
6. ロールに特権を割り当てるには、ドメインまたはアプリケーションサービスタイプに応じたロールを選択します。
7. ロールから特権を削除するには、ドメインまたはアプリケーションサービスタイプに応じた特権を選択解除します。
8. 手順を繰り返して、サービスタイプごとに特権を変更します。
9. ［OK］をクリックします。

カスタムロールの削除

カスタムロールを削除した場合、カスタムロールおよびそれに含まれるすべての特権が、ロールを割り当てたユーザーまたはグループから削除されます。

カスタムロールを削除するには、ナビゲータの［ロール］セクションでロールを右クリックし、［ロールの削除］をクリックします。 ロールを削除するかどうかを確認します。

ユーザーおよびグループへの特権およびロールの割り当て

ユーザーに実行を許可するアクションを確定するには、次のアイテムをユーザーおよびグループに割り当てます。

- 特権。特権により、ユーザーがアプリケーションクライアントで実行可能なアクションが決定されます。
- ロール。ロールとは、特権の集合です。ユーザーまたはグループにロールを割り当てるときは、そのロールに属する特権の集まりを割り当ててください。

ユーザーおよびグループに特権を割り当てる場合は、次に示す規則とガイドラインを使用します。

- ドメインのためのユーザーとグループ、およびドメイン内の次の各アプリケーションサービスのユーザーとグループに特権を割り当てます。

  以下のような状況では、Metadata Manager サービスまたは PowerCenter リポジトリサービスのユーザーおよびグループに特権およびロールを割り当てることはできません。

  •アプリケーションサービスが無効になっている。

  •PowerCenter リポジトリサービスが排他モードで実行中である。
- 同一サービスタイプの各アプリケーションサービスのユーザーまたはグループに対して、様々な特権および権限を割り当てることができます。
- ロールには、ドメインおよび複数のアプリケーションサービスタイプのロールに応じた特権を含めることができます。あるアプリケーションサービスのユーザーまたはグループにロールを割り当てる場合、そのアプリケーションサービスタイプに応じた特権が、ユーザーまたはグループに割り当てられます。

あるユーザーに割り当てられた特権またはロールを変更する場合、変更された特権またはロールは、次にそのユーザーがログインしたときに有効になります。

注: ユーザーは、デフォルトの管理者ユーザーアカウントに割り当てられた特権またはロールを編集することができません。

継承される特権

ユーザーまたはグループにより、以下のオブジェクトから特権が継承されます。

- グループ。 グループに特権を割り当てた場合、グループに属するすべてのサブグループおよびユーザーに権限が継承されます。
- ロール。ユーザーにロールを割り当てた場合、ユーザーはロールに属する特権を継承します。 グループにロールを割り当てると、そのロールに属している特権はグループと全サブグループに継承されると共に、グループの所属ユーザーにも継承されます。サブグループおよびユーザーには、ロールが継承されません。

グループまたはロールから継承された特権は、取り消すことができません。グループまたはロールから継承されない追加の特権は、ユーザーまたはグループに割り当てることができます。

ユーザーまたはグループの［特権］タブには、ユーザーまたはグループに割り当てられているすべてのロールおよび特権がドメイン別/各アプリケーションサービス別に表示されます。ドメインまたはサービスに対して割り当てられた特権を表示する、対象のドメインまたはアプリケーションサービスを選択します。以下の項目をクリックし、割り当てられたロールおよび特権に関する追加情報を表示します。

- 割り当てられたロールの名前。詳細パネルにロールの詳細が表示されます。
- 割り当てられたロールの情報アイコン。そのロールに継承されたすべての特権を強調表示します。

ロールまたはグループから継承される特権には、継承アイコンが表示されます。継承される特権のツールヒントには、ユーザーが特権を継承した特定のロールまたはグループが表示されます。

ナビゲーションによる、特権およびロールのユーザーまたはグループへの割り当て

1. Administrator ツールで、［セキュリティ］タブをクリックします。
2. ナビゲータで、ユーザーまたはグループを選択します。
3. ［特権］タブをクリックします。
4. ［編集］をクリックします。

   ［Edit Roles and Privileges（ロールと特権の編集）］ダイアログボックスが表示されます。
5. ロールを割り当てるには、［ロール］タブでドメインまたはアプリケーションサービスを展開します。

6. ロールを付与するには、ドメインまたはアプリケーションサービスのユーザーまたはグループに割り当てるロールを選択します。

   選択されたドメインまたはアプリケーションサービスタイプの特権を含むロールを、どれでも選択することができます。
7. ロールを取り消すには、ユーザーまたはグループに割り当てられているロールをクリアします。
8. 5 から 7 までの手順を繰り返して、別のサービスのロールを割り当てます。
9. 特権を割り当てるには、[特権] タブをクリックします。
10. ドメインまたはアプリケーションサービスを展開します。
11. 特権を付与するには、ドメインまたはアプリケーションサービスのユーザーまたはグループに割り当てる特権を選択します。
12. 特権を取り消すには、ユーザーまたはグループに割り当てられた特権をクリアします。

    ロールまたはグループから継承された特権は、取り消すことができません。
13. 10 から 12 までの手順を繰り返して、別のサービスの特権を割り当てます。
14. [OK] をクリックします。

サービスの特権を持つユーザーの表示

ドメインまたはアプリケーションサービスに対する特権を持つ、すべてのユーザーを表示することができます。

1. Administrator ツールで、[セキュリティ] タブをクリックします。
2. [セキュリティアクション] メニューで、[サービスユーザー特権] をクリックします。

   [サービス] ダイアログボックスが表示されます。
3. ドメインまたはアプリケーションサービスを選択します。

   詳細パネルに、ドメインまたはアプリケーションサービスに対する特権を持つすべてのユーザーが表示されます。
4. ユーザー名を右クリックして [アイテムにナビゲート] をクリックし、そのユーザーに移動します。

特権およびロールのトラブルシューティング

既存の Metadata Manager サービスまたは PowerCenter リポジトリサービスのユーザーに、特権またはロールを割り当てることができません。

以下の状況では、既存の Metadata Manager サービスまたは PowerCenter リポジトリサービスのユーザーおよびグループに特権およびロールを割り当てることができません。

- アプリケーションサービスが無効になっている。
- PowerCenter リポジトリサービスが排他モードで実行中である。

グループから特権を削除しました。この特権を持つグループのユーザーがまだ存在するのはなぜですか。

ユーザーへの特権の割り当てには、以下の方法のいずれかを使用できます。

- 特権をユーザーに直接割り当てます。
- ユーザーにロールを割り当てます。
- ユーザーが属するグループに特権またはロールを割り当てます。

グループから特権を削除する場合、そのグループに属するユーザーは、特権が直接割り当てられるか、または割り当てられたロールから特権を継承することができます。

すべてのドメインオブジェクトに対するすべてのドメイン特権および権限が割り当てられていますが、Administrator ツールですべてのタスクを完了できるわけではありません。

一部の Administrator ツールのタスクは、特権または権限ではなく管理者ロールによって決定されます。ドメインのすべての特権が割り当てられ、すべてのドメインオブジェクトに対する完全な権限が付与されることはありますが、管理者ロールによって規定されるタスクは完了することができません。

アプリケーションサービスに対して管理者ロールが割り当てられていますが、Administrator ツールでアプリケーションサービスを設定することはできません。

アプリケーションサービスに対して管理者ロールが割り当てられている場合、そのユーザーがアプリケーションクライアントの管理者です。 アプリケーションクライアントの管理者には、アプリケーションクライアント内のすべての権限および特権があります。

ただし、アプリケーションクライアントの管理者は Informatica ドメインに対する権限または特権がありません。 アプリケーションクライアントの管理者は、Administrator ツールにログインして管理者特権を持つアプリケーションクライアントのサービスを管理することはできません。

Administrator ツールでアプリケーションサービスを管理するには、適切なドメイン特権および権限が必要です。

PowerCenter リポジトリサービスに対して管理者ロールが割り当てられていますが、Repository Manager を使用してオブジェクトの詳細パージを行ったり、再利用可能なメタデータエクステンションを作成することはできません。

Repository Manager で以下のアクションを行うためには、Administrator ツールの PowerCenter リポジトリサービスでの Manage Services ドメイン特権および権限を持つ必要があります。

- PowerCenter リポジトリレベルでオブジェクトバージョンの詳細パージを実行する。
- 再利用可能なメタデータエクステンションを作成、編集、および削除する。

自分の特権でアプリケーションクライアント内のオブジェクトを編集できることが示されていますが、メタデータを編集することはできません。

アプリケーションクライアントで必要なオブジェクト権限がない場合があります。特定のアクションを実行する特権があっても、特定のオブジェクトでのアクションを実行するための権限が必要になる場合もあります。

排他モードで実行している新しい PowerCenter リポジトリサービスに接続するための pmrep を使用することができません。

サービスマネージャで、PowerCenter リポジトリ内のユーザーとグループのリストと、ドメイン環境設定データベース内のリストが同期していないことがあります。ユーザーとグループのリストを同期するには、PowerCenter リポジトリサービスを再起動します。

PowerCenter リポジトリサービスのフォルダ特権グループのすべての特権が割り当てられており、フォルダに対する読み取り、書き込み、および実行権限があります。 ただし、フォルダの権限を設定することはできません。

PowerCenter リポジトリサービスに対する管理者ロールが割り当てられたフォルダの所有者またはユーザーのみが、以下のフォルダ管理タスクを実行できます。

- PowerCenter 統合サービスでオペレーティングシステムプロファイルが使用される場合、フォルダにオペレーティングシステムプロファイルを割り当てます。 オペレーティングシステムプロファイルに対する権限が必要です。
- フォルダの所有者の変更。
- フォルダ権限の設定。
- フォルダの削除。
- 共有するフォルダの指定。
- フォルダ名と説明の編集。

Metadata Manager サービスの管理者ロールを割り当てられていますが、Metadata Manager リポジトリを作成したりリストアしたりできません。

Metadata Manager リポジトリを作成またはリストアするには、デフォルトの管理者グループに属している必要があります。デフォルトの管理者グループに属するユーザーは、アプリケーションサービスで管理者ロールを割り当てられているユーザーよりも多くの特権があります。

Metadata Manager サービスのリソースのロード特権を割り当てられていますが、Business Glossary リソースをロードしようとすると、「特権が不十分です」というエラーが表示されます。

Business Glossary リソースをロードするには、リソースのロード、リソースの管理、モデルの表示の各特権が必要です。ロードするビジネス用語集リソースに対する書き込み権限も必要です。

第 10 章

権限

この章では、以下の項目について説明します。

権限の概要

ユーザーセキュリティは、特権および権限を使用して管理します。権限により、ユーザーおよびグループのオブジェクトに対するアクセスレベルが定義されます。

ユーザーは特定のアクションを実行する特権を持っている場合でも、特定のオブジェクトに対してアクションを実行する権限が必要とされる場合もあります。

例えば、ユーザーは Manage Services のドメインの特権および、Production PowerCenter リポジトリサービスではなく、Development PowerCenter リポジトリサービスの権限を持っています。 ユーザーは、Production PowerCenter リポジトリサービスではなく、Development PowerCenter リポジトリサービスの編集または削除を行うことができます。 アプリケーションサービスを管理するには、ユーザーは Manage Services のドメインの特権および、アプリケーションサービスの権限を持っている必要があります。

異なるツールを使用して、以下のオブジェクトの権限を設定します。

異なるツールを使用して、以下のオブジェクトの権限を設定します。

オブジェクトタイプ	ツール	説明
アプリケーションおよびアプリケーションオブジェクト	Administrator ツール	アプリケーションおよびアプリケーションオブジェクト（マッピング、ワークフローなど）に権限を割り当てることができます。
接続オブジェクト	Administrator ツール Analyst ツール Developer tool	Administrator ツール、Analyst ツール、または Developer tool で定義された接続に対する権限を割り当てることができます。これらのツールは接続権限を共有します。

オブジェクトタイプ	ツール	説明
ドメインオブジェクト	Administrator ツール	次のドメインオブジェクトの権限を割り当てることができます: ドメイン、フォルダ、ノード、グリッド、ライセンス、アプリケーションサービス、およびオペレーティングシステムのプロファイル。
Metadata Manager のカタログオブジェクト	Metadata Manager	Metadata Manager のフォルダおよびカタログオブジェクトの権限を割り当てることができます。
モデルリポジトリプロジェクト	Analyst ツール Developer tool	Analyst ツールおよび Developer tool で定義されたプロジェクトの権限を割り当てることができます。これらのツールはプロジェクトの権限を共有します。
PowerCenter リポジトリオブジェクト	PowerCenter Client	PowerCenter フォルダ、デプロイメントグループ、ラベル、クエリおよび接続オブジェクトを割り当てることができます。
SQL データサービスオブジェクト	Administrator ツール	SQL データサービス、仮想スキーマ、仮想テーブルおよび仮想ストアドプロシージャなどの SQL データオブジェクトの権限を割り当てることができます。
Web サービスオブジェクト	Administrator ツール	Web サービスまたは Web サービス操作に対する権限を割り当てることができます。

オブジェクトタイプ	ツール	説明
接続オブジェクト	Administrator ツール Developer tool	Administrator ツール、または Developer tool で定義された接続に対する権限を割り当てることができます。これらのツールは接続権限を共有します。
ドメインオブジェクト	Administrator ツール	次のドメインオブジェクトの権限を割り当てることができます。ドメイン、フォルダ、ノード、およびアプリケーションサービス。
モデルリポジトリプロジェクト	Developer tool	Developer tool で定義されたプロジェクトの権限を割り当てることができます。

Administrator ツールを使用して、ドメインオブジェクトの権限を設定できます。権限は、以下のドメインオブジェクトに割り当てることができます。

- ドメイン
- ノード
- アプリケーションサービス

権限のタイプ

ユーザーおよびグループはドメイン内で以下のタイプの権限を持つことができます。

直接権限

ユーザーまたはグループに直接割り当てられている権限。 ユーザーおよびグループがオブジェクトに対する権限を持つ場合に適切な特権も持つとき、そのオブジェクトに対して管理タスクを実行することができます。直接権限を編集することができます。

継承された権限

ユーザーが継承する権限。 ユーザーがドメインまたはフォルダに対する権限を持つ場合、ドメインまたはフォルダ内のすべてのオブジェクトの権限を継承します。ドメインオブジェクトに対する権限を持っているグループでは、そのグループに属しているサブグループおよびユーザーのすべてに、そのドメインオブジェクトに対する権限が継承されます。例えば、複数のノードを含む Nodes という名前のフォルダを持つドメインがあるとします。フォルダに対するグループ権限を割り当てると、そのグループに属しているサブグループおよびユーザのそれぞれに、フォルダおよびフォルダ内のすべてのノードに対する権限が継承されます。

ユーザーが継承する権限。 ユーザーがドメインに対して権限を持つ場合、ドメイン内のすべてのオブジェクトの権限を継承する。ドメインオブジェクトに対する権限を持っているグループでは、そのグループに属しているサブグループおよびユーザーのすべてに、そのドメインオブジェクトに対する権限が継承されます。

ユーザーが継承する権限。 ユーザーがドメインに対して権限を持つ場合、ドメイン内のすべてのオブジェクトの権限を継承する。ドメインオブジェクトに対する権限を持っているグループでは、そのグループに属しているサブグループおよびユーザーのすべてに、そのドメインオブジェクトに対する権限が継承されます。

継承された権限を取り消すことはできません。また、管理者ロールが割り当てられたユーザーやグループから権限を取り消すこともできません。 管理者ロールでは、権限のチェックが省略されます。 管理者ロールを持つユーザーは、すべてのオブジェクトにアクセスすることができます。

一部のオブジェクトタイプについては、継承された権限を拒否することができます。 権限を拒否するには、ユーザーとグループがすでに持っている可能性のある権限に例外を設定します。

有効な権限

ユーザーまたはグループのすべての権限のスーパーセット。 直接権限および継承された権限が含まれます。

権限の詳細を表示すると、有効な権限の元になる権限を確認できます。 権限の詳細には、ユーザーまたはグループに割り当てられた直接権限、親グループに割り当てられた直接権限、および親オブジェクトから継承された権限が表示されます。 また、権限のチェックを省略する管理者ロールがユーザーまたはグループに割り当てられているかどうかも表示されます。

権限の検索フィルタ

ユーザーまたはグループに対して、権限の割り当て、権限の詳細の表示、あるいは権限の編集を行う際に、検索フィルタを使用してユーザーまたはグループを検索することができます。

ユーザーまたはグループの権限を管理する場合は、次の検索フィルタを使用できます。

セキュリティドメイン

ユーザーまたはグループを検索するセキュリティドメインを選択します。

パターン文字列

ユーザーまたはグループを検索するための文字列を入力します。 検索文字列を含むすべての名前が返されます。 文字列の大文字と小文字は区別されません。例えば、文字列「DA」を指定すると、「iasdaemon」、「daphne」、「DA_AdminGroup」などが返されます。

ユーザーまたはグループのリストをソートすることもできます。 列名を右クリックして、列を昇順または降順にソートします。

ドメインオブジェクト権限

特権および権限を設定して、ドメイン内のユーザーのセキュリティを管理します。 ドメインオブジェクトに対するユーザーのアクセスレベルは、権限によって定義されます。Administrator ツールにログインするには、ユーザーは最低でも 1 つのドメインオブジェクトに対する権限を持っている必要があります。 ユーザーが、あるオブジェクトに対する権限を持っていても、オブジェクトタイプの変更権を付与するドメイン特権を持っていない場合、そのオブジェクトを表示することのみ可能です。

例えば、ユーザーがあるノードに対する権限を持っていても、ノードおよびグリッド管理の特権を持っていなければ、ノードのプロパティは表示できますが、ノードの設定、シャットダウン、削除を行なうことはできません。

次のいずれかのタイプのドメインオブジェクトに対して権限を設定することができます。

ドメインオブジェクトタイプ	権限の説明
ドメイン	Administrator ツールのユーザーは、ドメイン内のすべてのオブジェクトにアクセスすることができます。 ユーザーがドメインに対して権限を持つ場合、ドメイン内のすべてのオブジェクトの権限を継承します。
フォルダ	Administrator ツールのユーザーは、Administrator ツールのフォルダ内のすべてのオブジェクトにアクセスすることができます。 ユーザーがフォルダに対する権限を持つ場合、フォルダ内のすべてのオブジェクトの権限を継承します。
ノード	Administrator ツールのユーザーは、ノードのプロパティを表示および編集することができます。 権限がない場合、ユーザーはアプリケーションサービスの定義時またはグリッドの作成時にノードを使用することができません。
グリッド	Administrator ツールのユーザーは、グリッドのプロパティを表示および編集することができます。 権限がない場合、ユーザーは、データ統合サービスまたは PowerCenter 統合サービスにグリッドを割り当てることができません。
ライセンス	Administrator ツールのユーザーは、ライセンスのプロパティを表示および編集することができます。 権限がない場合、ユーザーは、アプリケーションサービスを作成する際にライセンスを使用することができません。

ドメインオブジェクトタイプ	権限の説明
アプリケーションサービス	Administrator ツールのユーザーは、アプリケーションサービスのプロパティを表示および編集することができます。
オペレーティングシステムプロファイル	オペレーティングシステムのプロファイルに関連付けられている開発者、アナリスト、オペレータは、マッピング、プロファイル、およびワークフローを実行することができます。 PowerCenter のユーザーは、オペレーティングシステムのプロファイルに関連付けられているワークフローを実行することができます。 ワークフローを実行するユーザーに、ワークフローに割り当てられたオペレーティングシステムのプロファイルの権限がない場合、ワークフローは失敗します。

ドメインオブジェクトタイプ	権限の説明
ドメイン	Administrator ツールのユーザーは、ドメイン内のすべてのオブジェクトにアクセスすることができます。 ユーザーがドメインに対して権限を持つ場合、ドメイン内のすべてのオブジェクトの権限を継承します。
ノード	Administrator ツールのユーザーは、ノードのプロパティを表示および編集することができます。
アプリケーションサービス	Administrator ツールのユーザーは、アプリケーションサービスのプロパティを表示および編集することができます。
ライセンス	Administrator ツールのユーザーは、ライセンスのプロパティを表示および編集することができます。

ドメインオブジェクトタイプ	権限の説明
ドメイン	Administrator ツールのユーザーは、ドメイン内のすべてのオブジェクトにアクセスすることができます。 ユーザーがドメインに対して権限を持つ場合、ドメイン内のすべてのオブジェクトの権限を継承します。
ノード	Administrator ツールのユーザーは、ノードのプロパティを表示および編集することができます。
アプリケーションサービス	Administrator ツールのユーザーは、アプリケーションサービスのプロパティを表示および編集することができます。
ライセンス	Administrator ツールのユーザーは、ライセンスのプロパティを表示および編集することができます。

ドメインオブジェクト権限は、以下の方法で管理できます。

- ドメインオブジェクト別に権限を管理します。 ドメインオブジェクトの［権限］ビューを使用して、複数のユーザーまたはグループを対象に、オブジェクトに対する権限の割り当てと編集を行います。
- ユーザーまたはグループ別に権限を管理します。 ［権限の管理］ダイアログボックスを使用して、特定のユーザーまたはグループを対象に、ドメインオブジェクトに対する権限の割り当てと編集を行います。

注: オペレーティングシステムのプロファイルに対する権限は、他のドメインオブジェクトに対する権限とは異なる方法で設定します。

ドメインオブジェクト別の権限

複数のユーザーまたはグループのドメインオブジェクトに対する権限の割り当て、表示、および編集を行うには、ドメインオブジェクトの **[権限]** ビューを使用します。

ドメインオブジェクトに対する権限の割り当て

ドメインオブジェクトに対する権限を割り当てると、ユーザーおよびグループにオブジェクトへのアクセスが付与されます。

1. [管理] タブで **[サービスとノード]** ビューを選択します。
2. ナビゲータで、ドメインオブジェクトを選択します。
3. [コンテンツ] パネルで、**[権限]** ビューを選択します。
4. **[グループ]** タブまたは **[ユーザー]** タブをクリックします。
5. **[アクション]** > **[権限の割り当て]** をクリックします。

   [権限の割り当て] ダイアログボックスに、オブジェクトに対する権限がないすべてのユーザーまたはグループが表示されます。
6. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**[フィルタ]** ボタンをクリックします。
7. ユーザーまたはグループを選択し、**[次へ]** をクリックします。
8. **[許可]** を選択し、**[完了]** をクリックします。

ドメインオブジェクトに対する権限の詳細の表示

権限の詳細を表示すると、有効な権限の元になる権限を確認できます。

1. [管理] タブで **[サービスとノード]** ビューを選択します。
2. ナビゲータで、ドメインオブジェクトを選択します。
3. [コンテンツ] パネルで、**[権限]** ビューを選択します。
4. **[グループ]** タブまたは **[ユーザー]** タブをクリックします。
5. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**[フィルタ]** ボタンをクリックします。
6. ユーザーまたはグループを選択し、**[アクション]** > **[権限の詳細の表示]** をクリックします。

   [権限の詳細] ダイアログボックスが表示されます。 このダイアログボックスには、ユーザーまたはグループに割り当てられた直接権限、親グループに割り当てられた直接権限、および親オブジェクトから継承された権限が表示されます。 また、権限のチェックを省略する管理者ロールがユーザーまたはグループに割り当てられているかどうかも表示されます。
7. **[閉じる]** をクリックします。
8. または、**[権限の編集]** をクリックして直接権限を編集します。

ドメインオブジェクトに対する権限の編集

ユーザーまたはグループのドメインオブジェクトに対する直接権限を編集することができます。 継承された権限や自分自身の権限を取り消すことはできません。

注: オブジェクトに対する直接権限を取り消した後も、ユーザーやグループが親グループまたはオブジェクトから権限を継承している可能性があります。

1. ［管理］タブで **［サービスとノード］** ビューを選択します。
2. ナビゲータで、ドメインオブジェクトを選択します。
3. ［コンテンツ］パネルで、**［権限］** ビューを選択します。
4. **［グループ］** タブまたは **［ユーザー］** タブをクリックします。
5. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**［フィルタ］** ボタンをクリックします。
6. ユーザーまたはグループを選択し、**［アクション］** > **［直接権限の編集］** をクリックします。

   ［直接権限の編集］ ダイアログボックスが表示されます。
7. オブジェクトに対する権限を割り当てるには、**［許可］** を選択します。
8. オブジェクトに対する権限を取り消すには、**［権限を取り消す］** を選択します。

   直接割り当てられた権限か継承された権限かを確認するには、**［権限の詳細の表示］** をクリックします。
9. **［OK］** をクリックします。

ユーザーまたはグループ別の権限

特定のユーザーまたはグループのドメインオブジェクトに対する権限の表示、割り当て、および編集を行うには、ドメインオブジェクトの **［権限の管理］** ダイアログボックスを使用します。

ユーザーまたはグループの権限の詳細の表示

権限の詳細を表示すると、有効な権限の元になる権限を確認できます。

1. Infomatica Administrator のヘッダで、**［管理］** > **［権限］** をクリックします。

   ［権限の管理］ ダイアログボックスが表示されます。
2. **［グループ］** タブまたは **［ユーザー］** タブをクリックします。
3. ユーザーおよびグループを検索するための文字列を入力し、**［フィルタ］** ボタンをクリックします。
4. ユーザーまたはグループを選択します。
5. ドメインオブジェクトを選択し、**［権限の詳細の表示］** ボタンをクリックします。

   ［権限の詳細］ ダイアログボックスが表示されます。 このダイアログボックスには、ユーザーまたはグループに割り当てられた直接権限、親グループに割り当てられた直接権限、および親オブジェクトから継承された権限が表示されます。 また、権限のチェックを省略する管理者ロールがユーザーまたはグループに割り当てられているかどうかも表示されます。
6. **［閉じる］** をクリックします。
7. または、**［権限の編集］** をクリックして直接権限を編集します。

ユーザーまたはグループに対する権限の割り当ておよび編集

ユーザーまたはグループのドメインオブジェクト権限を編集する場合は、権限の割り当て、および既存の直接権限の編集を行うことができます。 継承された権限や自分自身の権限を取り消すことはできません。

注: オブジェクトに対する直接権限を取り消した後も、ユーザーやグループが親グループまたはオブジェクトから権限を継承している可能性があります。

1. Infomatica Administrator のヘッダで、**［管理］** > **［権限］** をクリックします。

   ［権限の管理］ ダイアログボックスが表示されます。
2. **［グループ］** タブまたは **［ユーザー］** タブをクリックします。
3. ユーザーおよびグループを検索するための文字列を入力し、**［フィルタ］** ボタンをクリックします。
4. ユーザーまたはグループを選択します。
5. ドメインオブジェクトを選択し、**［直接権限の編集］** ボタンをクリックします。

   ［直接権限の編集］ ダイアログボックスが表示されます。
6. オブジェクトに対する権限を割り当てるには、**［許可］** を選択します。
7. オブジェクトに対する権限を取り消すには、**［権限を取り消す］** を選択します。

   直接割り当てられた権限か継承された権限かを確認するには、**［権限の詳細の表示］** をクリックします。
8. **［OK］** をクリックします。
9. **［閉じる］** をクリックします。

オペレーティングシステムのプロファイルの権限

Administrator ツールの［セキュリティ］ページで、オペレーティングシステムのプロファイルに対する権限の割り当て、表示、編集を行います。

管理者グループには、すべてのオペレーティングシステムのプロファイルに対する権限があります。

オペレーティングシステムのプロファイルの権限の割り当て

オペレーティングシステムのプロファイルに権限を割り当てると、Informatica ユーザーは、オペレーティングシステムのプロファイルを使用してマッピング、プロファイル、およびワークフローを実行します。 PowerCenter ユーザーは、オペレーティングシステムのプロファイルに割り当てられたワークフローを実行します。

1. **［セキュリティ］** タブで **［オペレーティングシステムプロファイル］** ビューを選択します。
2. オペレーティングシステムのプロファイルを選択し、**［権限］** タブをクリックします。
3. **［グループ］** または **［ユーザー］** ビューを選択し、**［権限の付与］** をクリックします。

   ［ユーザー/グループをオペレーティングシステムプロファイルに割り当てる］ ダイアログボックスに、オペレーティングシステムのプロファイルに対する権限を持たないすべてのユーザーまたはグループが表示されます。
4. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**［フィルタ］** ボタンをクリックします。
5. ユーザーまたはグループを選択し、**［次へ］** をクリックします。
6. **［許可］** を選択し、**［完了］** をクリックします。

オペレーティングシステムのプロファイルに対する権限の詳細の表示

権限の詳細を表示すると、有効な権限の元になる権限を確認できます。

1. **［セキュリティ］** タブで **［オペレーティングシステムプロファイル］** ビューを選択します。

2. オペレーティングシステムのプロファイルを選択し、**[権限]** タブをクリックします。
3. **[グループ]** または **[ユーザー]** ビューを選択します。
4. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**[フィルタ]** ボタンをクリックします。
5. ユーザーまたはグループを選択し、**[権限の詳細の表示]** をクリックします。

   [権限の詳細] ダイアログボックスが表示されます。 このダイアログボックスには、ユーザーまたはグループに割り当てられた直接権限、親グループに割り当てられた直接権限、および親オブジェクトから継承された権限が表示されます。 また、権限のチェックを省略する管理者ロールがユーザーまたはグループに割り当てられているかどうかも表示されます。
6. **[閉じる]** をクリックします。
7. または、**[権限の編集]** をクリックして直接権限を編集します。

オペレーティングシステムのプロファイルに対する権限の編集

オペレーティングシステムプロファイルに対するユーザーまたはグループの直接権限を編集することができます。 継承された権限や自分自身の権限を取り消すことはできません。

注: オブジェクトに対する直接権限を取り消した後も、ユーザーやグループが親グループまたはオブジェクトから権限を継承している可能性があります。

1. **[セキュリティ]** タブで **[オペレーティングシステムプロファイル]** ビューを選択します。
2. オペレーティングシステムのプロファイルを選択し、**[権限]** タブをクリックします。
3. **[グループ]** または **[ユーザー]** ビューを選択します。
4. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**[フィルタ]** ボタンをクリックします。
5. ユーザーまたはグループを選択して、**[直接権限の編集]** をクリックします。

   [直接権限の編集] ダイアログボックスが表示されます。
6. オペレーティングシステムプロファイルに対する権限を割り当てるには、**[許可]** を選択します。
7. オペレーティングシステムプロファイルに対する権限を取り消すには、**[権限を取り消す]** を選択します。

   直接割り当てられた権限か継承された権限かを確認するには、**[権限の詳細の表示]** をクリックします。
8. **[OK]** をクリックします。

接続権限

接続に対する、ユーザーまたはグループのアクセスレベルは、権限によって管理されます。

Analyst ツール、Developer ツール、または Administrator ツールで接続に対する権限を設定することができます。

Developer ツール、または Administrator ツールで接続に対する権限を設定することができます。

1 つのツールでの、ユーザーまたはグループに割り当てられたいかなる接続の権限も、他のツールにも適用されます。 例えば、Developer ツールで、グループ A に接続 A に対する権限を付与します。 グループ A は、Analyst ツールおよび Administrator ツールにおいても、接続 A に対する権限を有しています。

1 つのツールでの、ユーザーまたはグループに割り当てられたいかなる接続の権限も、他のツールにも適用されます。 例えば、Developer ツールで、グループ A に接続 A に対する権限を付与します。 グループ A は、Administrator ツールにおいても、接続 A に対する権限を有しています。

以下の Informatica コンポーネントによって、接続権限が使用されます。

- Administrator ツール。 接続に対する読み込み、書き込み、および実行権限が強制されます。
- Analyst ツール。 接続に対する読み込み、書き込み、および実行権限が強制されます。
- Informatica コマンドラインインタフェース。 接続に対する読み込み、書き込み、付与権限が強制されます。
- Developer ツール。 接続に対する読み込み、書き込み、および実行権限が強制されます。
  SQL データサービスの場合は、Developer ツールによって接続権限が強制されません。 代わりに、データへのアクセスを制限するために、カラムレベルセキュリティ、およびパススルーセキュリティが強制されます。
- データ統合サービス。 ユーザーがデータのプレビュー、マッピング、スコアカード、またはプロファイルを実行しようとする場合、実行権限が強制されます。
- データ統合サービス。ユーザーがデータのプレビュー、マッピングまたはプロファイルの実行をしようとする場合、実行権限が強制されます。

注: プロファイリングウェアハウス、データオブジェクトキャッシュデータベース、またはモデルリポジトリの各接続に対しては、権限を割り当てることはできません。

接続権限のタイプ

次のアクションを実行するために、ユーザーに異なる権限のタイプを割り当てることができます。

アクション	権限のタイプ
接続名、タイプ、説明、接続文字列、ユーザー名など、パスワードを除くすべての接続メタデータを表示する。	読み取り
パスワードを含むすべての接続メタデータを編集する。接続を削除する。書き込み権限を持つユーザーが、読み取り権限を継承する。	書き込み
接続によって定義される基本となるデータソースにある物理データにアクセスする。ユーザーは、データのプレビュー、マッピングの実行、ワークフローマッピングタスクでのマッピングの実行、スコアカードの実行、または接続を使用するプロファイルの実行が可能です。 接続によって定義される基本となるデータソースにある物理データにアクセスする。ユーザーは、データのプレビュー、マッピングの実行、ワークフローマッピングタスクでのマッピングの実行、または接続を使用するプロファイルの実行が可能です。	実行
接続の権限の付与および取り消し。	付与

デフォルトの接続権限

ドメイン管理者には、すべての接続において、すべての権限があります。 接続を作成したユーザーには、その接続の読み取り、書き込み、実行、および権限の付与の権限があります。デフォルトでは、すべてのユーザーに、接続で以下のアクションを実行する権限があります。

- 接続名、タイプ、説明など、基本的な接続メタデータを表示する。
- Developer ツールで、マッピングでの接続を使用する。
- 接続でのオブジェクト上で、Analyst ツールにプロファイルを作成する。

接続の権限の割り当て

接続に対して権限を割り当てて、その接続に対するユーザーまたはグループのアクセスレベルを定義します。

1. ［管理］タブで、**［接続］**ビューを選択します。
2. ナビゲータで、接続を選択します。
3. ［コンテンツ］パネルで、**［権限］**ビューを選択します。
4. **［グループ］**タブまたは**［ユーザー］**タブをクリックします。
5. **［アクション］** > **［権限の割り当て］**をクリックします。

   ［権限の割り当て］ダイアログボックスに、接続に対する権限を持たないすべてのユーザーまたはグループが表示されます。
6. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**［フィルタ］**ボタンをクリックします。
7. ユーザーまたはグループを選択し、**［次へ］**をクリックします。
8. 割り当てるそれぞれの権限タイプについて、**［許可］**を選択します。
9. **［完了］**をクリックします。

接続に対する権限の詳細の表示

権限の詳細を表示すると、有効な権限の元になる権限を確認できます。

1. ［管理］タブで、**［接続］**ビューを選択します。
2. ナビゲータで、接続を選択します。
3. ［コンテンツ］パネルで、**［権限］**ビューを選択します。
4. **［グループ］**タブまたは**［ユーザー］**タブをクリックします。
5. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**［フィルタ］**ボタンをクリックします。
6. ユーザーまたはグループを選択し、**［アクション］** > **［権限の詳細の表示］**をクリックします。

   ［権限の詳細の表示］ダイアログボックスが表示されます。ダイアログボックスには、ユーザーまたはグループに割り当てられている直接権限と、親グループに割り当てられている直接権限が表示されます。また、権限のチェックを省略する管理者ロールがユーザーまたはグループに割り当てられているかどうかも表示されます。
7. **［閉じる］**をクリックします。
8. または、**［権限の編集］**をクリックして直接権限を編集します。

接続に対する権限の編集

ユーザーまたはグループの接続に対する直接権限を編集することができます。 継承された権限や自分自身の権限を取り消すことはできません。

注: オブジェクトに対する直接権限を取り消した後も、ユーザーやグループが親グループまたはオブジェクトから権限を継承している可能性があります。

1. ［管理］タブで、**［接続］**ビューを選択します。
2. ナビゲータで、接続を選択します。
3. ［コンテンツ］パネルで、**［権限］**ビューを選択します。
4. **［グループ］**タブまたは**［ユーザー］**タブをクリックします。
5. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**［フィルタ］**ボタンをクリックします。
6. ユーザーまたはグループを選択し、**［アクション］** > **［直接権限の編集］**をクリックします。

［**直接権限の編集**］ダイアログボックスが表示されます。

7. 権限を許可または取り消します。
   - 権限を割り当てる場合は、［**許可**］を選択します。
   - 特定の権限を 1 つだけ取り消す場合は、［**許可**］の選択を解除します。
   - すべての権限を取り消す場合は、［**権限を取り消す**］を選択します。

   直接割り当てられた権限か継承された権限かを確認するには、［**権限の詳細の表示**］をクリックします。
8. ［**OK**］をクリックします。

アプリケーションとアプリケーションオブジェクトの権限

権限によって、アプリケーションおよびアプリケーションオブジェクト（マッピング、ワークフローなど）に対するユーザーまたはグループのアクセスレベルを制御します。

アプリケーションおよびアプリケーションオブジェクトの権限は、Administrator ツールまたはコマンドラインから設定できます。

アプリケーションとアプリケーションオブジェクトの権限のタイプ

ユーザーおよびグループに、表示権限、付与権限、実行権限を割り当てることができます。

以下の権限をユーザーおよびグループに割り当てることができます。

表示権限

アプリケーションおよびアプリケーションオブジェクトを表示します。

付与権限

アプリケーションおよびアプリケーションオブジェクトに対する権限の付与および取り消しを行います。

実行権限

アプリケーションおよびアプリケーションオブジェクトを実行します。

注: Administrator ツールで、またはコマンドラインから開始、停止、バックアップなどのアプリケーション操作を実行するには、そのアプリケーションに対する実行権限およびアプリケーション管理特権を持っている必要があります。

アプリケーションまたはアプリケーションオブジェクトへの権限の割り当て

アプリケーションまたはアプリケーションオブジェクトに対して権限を割り当てると、アプリケーションまたはアプリケーションオブジェクトに対するユーザーまたはグループのアクセスレベルが定義されます。

1. ［管理］タブで［**サービスとノード**］ビューを選択します。
2. ナビゲータで、データ統合サービスを選択します。
3. ［コンテンツ］パネルで、［**アプリケーション**］ビューを選択します。
4. アプリケーション、マッピング、またはワークフローを選択します。
5. ［詳細］パネルで、［**グループ権限**］ビューまたは［**ユーザー権限**］ビューを選択します。

6. **［権限の割り当て］**ボタンをクリックします。

   ［権限の割り当て］ダイアログボックスに、アプリケーションまたはアプリケーションオブジェクトに対する権限がないすべてのユーザーまたはグループが表示されます。
7. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**［フィルタ］**ボタンをクリックします。
8. ユーザーまたはグループを選択し、**［次へ］**をクリックします。
9. 割り当てるそれぞれの権限タイプについて、**［許可］**を選択します。
10. **［完了］**をクリックします。

アプリケーションまたはアプリケーションオブジェクトに対する権限の詳細の表示

権限の詳細を表示すると、有効な権限の元になる権限を確認できます。

1. ［管理］タブで**［サービスとノード］**ビューを選択します。
2. ナビゲータで、データ統合サービスを選択します。
3. ［コンテンツ］パネルで、**［アプリケーション］**ビューを選択します。
4. アプリケーション、マッピング、またはワークフローを選択します。
5. ［詳細］パネルで、**［グループ権限］**ビューまたは**［ユーザー権限］**ビューを選択します。
6. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**［フィルタ］**ボタンをクリックします。
7. ユーザーまたはグループを選択し、**［権限の詳細の表示］**ボタンをクリックします。

   ［権限の詳細］ダイアログボックスが表示されます。 このダイアログボックスには、ユーザーまたはグループに割り当てられた直接権限、親グループに割り当てられた直接権限、および親オブジェクトから継承された権限が表示されます。 また、権限のチェックを省略する管理者ロールがユーザーまたはグループに割り当てられているかどうかも表示されます。
8. **［閉じる］**をクリックします。
9. または、**［権限の編集］**をクリックして直接権限を編集します。

アプリケーションまたはアプリケーションオブジェクトに対する権限の編集

ユーザーまたはグループのアプリケーションまたはアプリケーションオブジェクトに対する直接権限を編集することができます。継承された権限や自分自身の権限を取り消すことはできません。

注: オブジェクトに対する直接権限を取り消した後も、ユーザーやグループが親グループまたはオブジェクトから権限を継承している可能性があります。

1. ［管理］タブで**［サービスとノード］**ビューを選択します。
2. ナビゲータで、データ統合サービスを選択します。
3. ［コンテンツ］パネルで、**［アプリケーション］**ビューを選択します。
4. アプリケーションまたはアプリケーションオブジェクトを選択します。
5. ［詳細］パネルで、**［グループ権限］**ビューまたは**［ユーザー権限］**ビューを選択します。
6. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**［フィルタ］**ボタンをクリックします。
7. ユーザーまたはグループを選択し、**［直接権限の編集］**ボタンをクリックします。

   ［直接権限の編集］ダイアログボックスが表示されます。
8. 権限を許可または取り消します。

- 権限を割り当てる場合は、**[許可]** を選択します。
- 特定の権限を 1 つだけ取り消す場合は、**[許可]** の選択を解除します。
- すべての権限を取り消す場合は、**[権限を取り消す]** を選択します。

直接割り当てられた権限か継承された権限かを確認するには、**[権限の詳細の表示]** をクリックします。

9. **[OK]** をクリックします。

アプリケーションまたはアプリケーションオブジェクトに対する権限の拒否

アプリケーションおよびアプリケーションオブジェクトに対する権限を明示的に拒否することができます。権限を拒否すると、有効な権限に例外を割り当てることになります。

SQL データサービスの権限

エンドユーザーは、JDBC または ODBC クライアントツールを使用して、SQL データサービスに接続することができます。 接続した後に、ユーザーは SQL データサービス内の仮想テーブルに対して SQL クエリを実行し、または SQL データサービス内の仮想ストアードプロシージャを実行することができます。 権限により、ユーザーが SQL データサービスを持つアクセスレベルが制御されます。

以下の SQL データサービスオブジェクトのユーザーおよびグループに権限を割り当てることができます。

- SQL データサービス
- 仮想テーブル
- 仮想ストアードプロシージャ

SQL データサービスオブジェクトの権限を割り当てる場合、ユーザーまたはグループは、SQL データサービスオブジェクトに属するすべてのオブジェクトの同じ権限を継承します。 例えば、SQL データサービスにユーザーが選択した権限を割り当てます。 ユーザーは、SQL データサービス内のすべての仮想テーブルの選択した権限を継承します。

一部の SQL データサービスオブジェクトのユーザーとグループへの権限を拒否することができます。 権限を拒否する場合、ユーザーとグループが既に持っている可能性のある権限の例外を設定します。 例えば、仮想テーブル内のカラムに権限を割り当てることはできませんが、ユーザーがカラムが含まれる SQL SELECT 文を実行することを拒否することができます。

SQL データサービスの権限のタイプ

以下の権限をユーザーおよびグループに割り当てることができます。

- 権限の付与。 Administrator ツールまたは *infacmd* コマンドラインプログラムを使用して、SQL データサービスオブジェクトの権限を付与および取り消すことができます。
- 実行権限。ユーザーは、JDBC または ODBC クライアントツールを使用して、SQL データサービス内の仮想ストアードプロシージャを実行することができます。
- 権限の選択。 ユーザーは、JDBC または ODBC クライアントツールを使用して、SQL データサービス内の仮想テーブルの SQL SELECT 文を実行することができます。

一部の権限は、すべての SQL データサービスオブジェクトに対して適用されるとは限りません。

以下の表に、各 SQL データサービスオブジェクトに対する権限を示します。

オブジェクト	権限の付与	実行権限	権限の選択
SQL データサービス	SQL データサービスの権限および SQL データサービス内のすべてのオブジェクトを付与および取り消すことができます。	SQL データサービス内のすべての仮想ストアードプロシージャを実行します。	SQL データサービス内のすべての仮想テーブルで SQL SELECT 文を実行します。
仮想テーブル	仮想テーブルの権限を付与および取り消すことができます。	-	仮想テーブルで SQL SELECT 文を実行します。
仮想ストアードプロシージャ	仮想ストアードプロシージャの権限を付与および取り消すことができます。	仮想ストアードプロシージャを実行します。	-

SQL データサービスの権限の割り当て

SQL データサービスオブジェクトに対する権限を割り当てると、オブジェクトに対するユーザーまたはグループのアクセスレベルが定義されます。

1. ［管理］タブで **［サービスとノード］** ビューを選択します。
2. ナビゲータで、Data Integration Service を選択します。
3. ［コンテンツ］パネルで、**［アプリケーション］** ビューを選択します。
4. SQL データサービスオブジェクトを選択します。
5. ［詳細］パネルで、**［グループ権限］** ビューまたは **［ユーザー権限］** ビューを選択します。
6. **［権限の割り当て］** ボタンをクリックします。

   ［権限の割り当て］ ダイアログボックスに、SQL データサービスオブジェクトに対する権限がないすべてのユーザーまたはグループが表示されます。
7. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**［フィルタ］** ボタンをクリックします。
8. ユーザーまたはグループを選択し、**［次へ］** をクリックします。
9. 割り当てるそれぞれの権限タイプについて、**［許可］** を選択します。
10. **［完了］** をクリックします。

SQL データサービスに対する権限の詳細の表示

権限の詳細を表示すると、有効な権限の元になる権限を確認できます。

1. ［管理］タブで **［サービスとノード］** ビューを選択します。
2. ナビゲータで、Data Integration Service を選択します。
3. ［コンテンツ］パネルで、**［アプリケーション］** ビューを選択します。
4. SQL データサービスオブジェクトを選択します。
5. ［詳細］パネルで、**［グループ権限］** ビューまたは **［ユーザー権限］** ビューを選択します。
6. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**［フィルタ］** ボタンをクリックします。
7. ユーザーまたはグループを選択し、**［権限の詳細の表示］** ボタンをクリックします。

   ［権限の詳細］ ダイアログボックスが表示されます。 このダイアログボックスには、ユーザーまたはグループに割り当てられた直接権限、親グループに割り当てられた直接権限、および親オブジェクトから継承

された権限が表示されます。 また、権限のチェックを省略する管理者ロールがユーザーまたはグループに割り当てられているかどうかも表示されます。

8. **［閉じる］**をクリックします。
9. または、**［権限の編集］**をクリックして直接権限を編集します。

SQL データサービスの権限の編集

ユーザーまたはグループの SQL データサービスに対する直接権限を編集することができます。 継承された権限や自分自身の権限を取り消すことはできません。

注: オブジェクトに対する直接権限を取り消した後も、ユーザーやグループが親グループまたはオブジェクトから権限を継承している可能性があります。

1. ［管理］タブで**［サービスとノード］**ビューを選択します。
2. ナビゲータで、Data Integration Service を選択します。
3. ［コンテンツ］パネルで、**［アプリケーション］**ビューを選択します。
4. SQL データサービスオブジェクトを選択します。
5. ［詳細］パネルで、**［グループ権限］**ビューまたは**［ユーザー権限］**ビューを選択します。
6. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**［フィルタ］**ボタンをクリックします。
7. ユーザーまたはグループを選択し、**［直接権限の編集］**ボタンをクリックします。

   ［直接権限の編集］ダイアログボックスが表示されます。
8. 権限を許可または取り消します。
   - 権限を割り当てる場合は、**［許可］**を選択します。
   - 特定の権限を 1 つだけ取り消す場合は、**［許可］**の選択を解除します。
   - すべての権限を取り消す場合は、**［権限を取り消す］**を選択します。

   直接割り当てられた権限か継承された権限かを確認するには、**［権限の詳細の表示］**をクリックします。
9. **［OK］**をクリックします。

SQL データサービスの権限の拒否

一部の SQL データサービスオブジェクトに対する権限を明示的に拒否することができます。 SQL データサービスにおいてオブジェクトに対する権限を拒否する場合、有効な権限に例外を適用しています。

権限を拒否する場合、以下のいずれかの infacmd コマンドを使用します。

- infacmd sql SetStoredProcedurePermissions。 ストアドプロシージャレベルで権限の実行または付与を拒否します。
- infacmd sql SetTablePermissions。 仮想テーブルレベルで権限の選択と付与を拒否します。
- infacmd sql SetColumnPermissions。 カラムレベルで権限の選択を拒否します。

各コマンドには、権限の適用（-ap）と権限の拒否（-dp）を行うオプションがあります。 SetColumnPermissions コマンドには、権限の適用オプションは含まれません。

注: Administrator ツールから、権限を拒否することはできません。

Data Integration Service により、仮想データベースに対して SQL クエリとストアドプロシージャを実行する前に、権限が確認されます。 Data Integration Service により、SQL データサービスレベルで開始するユーザーまたはグループのための権限が検証されます。 SQL データサービス内で親オブジェクトに権限が適用された場合、子オブジェクトは権限を継承します。 Data Integration Service により、カラムレベルで拒否された権限がチェックされます。

カラムレベルセキュリティ

管理者は、SQL データオブジェクトの仮想テーブル内のカラムに対するアクセスを拒否することができます。管理者は、制限されたカラムに対するクエリのためのデータ統合サービスの動作を設定できます。

ユーザーが権限を持たないカラムに対してクエリを行った場合、以下の結果が生じる場合があります。

- クエリがデータの代わりに代替値を返す。 クエリが、結果を返す行ごとに代替値を返します。 クエリによって、カラムの値が代替値に置き換えられます。 クエリにフィルタまたは結合が含まれる場合、代替結果が結果として表示されます。
- 不十分な権限のエラーのためクエリが失敗する。

SQL データサービスのセキュリティの設定の詳細については、Informatica How-To ライブラリの記事「How to Configure Security for SQL Data Services」（https://kb.informatica.com/h2l/HowTo%20Library/1/0266_ConfiguringSecurityForSQLDataServices.pdf）を参照してください。

カラムの制限

カラムレベルのセキュリティを設定する場合、ユーザーが制限されたカラムをクエリで選択したときの動作を決定するカラムオプションを設定します。 制限されたデータをデフォルト値で置き換えることができます。 または、ユーザーが制限されたカラムを選択した場合に、クエリが失敗するようにもできます。

例えば、管理者が Employee テーブルの Salary カラムへのユーザーアクセスを拒否するとします。 管理者は Salary カラムに 100,000 という代替値を設定します。 ユーザーが SQL クエリで salary カラムを選択した場合、Data Integration Service によって各行の Salary カラムに 100,000 が返されます。

infacmd sql UpdateColumnOptions コマンドを実行して、カラムオプションを設定します。 Administrator ツールではカラムオプションを設定することはできません。

infacmd sql UpdateColumnOptions を実行する場合、以下のオプションを入力します。

ColumnOptions.DenyWith=*option*

制限されたカラム値を置き換えるか、クエリが失敗するかどうかを決定します。 カラム値を置き換える場合、NULL 値または定数値のいずれかで値を置き換えるかを選択できます。 以下のいずれかのオプションを入力します。

- ERROR。 SQL クエリで制限されたカラムが選択された場合、クエリが失敗してエラーを返します。
- NULL。 各行の制限されたカラムに NULL 値を返します。
- VALUE。 各行の制限されたカラムある場所に定数値を返します。 定数値は、ColumnOptions.InsufficientPermissionValue オプションで設定します。

ColumnOptions.InsufficientPermissionValue=*value*

制限されたカラムを定数で置き換えます。 デフォルトは空の文字列です。 Data Integration Service でカラムを空の文字列に置き換える場合、そのカラムが数字または日付の場合には、クエリはエラーを返します。 DenyWith オプションに値を設定しない場合、Data Integration Service は InsufficientPermissionValue オプションを無視します。

カラムに代替値を設定するには、以下の構文を使用してコマンドを入力します。

```
infacmd sql UpdateColumnOptions -dn empDomain -sn DISService -un Administrator -pd Adminpass -sqlds
employee_APP.employees_SQL -t Employee -c Salary -o ColumnOptions.DenyWith=VALUE
ColumnOptions.InsufficientPermissionValue=100000
```

制限されたカラムにどちらのオプションも設定しない場合、デフォルトではクエリは失敗しません。 クエリが実行され、Data Integration Service によってそのカラム値が NULL に置き換えられます。

カラムレベルセキュリティの追加

infacmd sql SetColumnPermissions コマンドでカラムレベルセキュリティを設定します。 Administrator ツールから、カラムレベルセキュリティを設定することはできません。

Employee テーブルには、FirstName、LastName、Dept、および Salary というカラムがあります。 あるユーザーに対して、Employee テーブルにアクセスできるようにする一方で、Salary カラムへのアクセスは制限します。

Salary カラムへのユーザーのアクセスを制限するには、Data Integration Service を無効にして、以下のコマンドと同じような infacmd コマンドを入力します。

```
infacmd sql SetColumnPermissions -dn empDomain -sn DISService -un Administrator -pd Adminpass -sqlds
employee_APP.employees -t Employee -c Salary gun -Tom -dp SQL_Select
```

以下の SQL 文は、Salary カラムに NULL を返します。

```
Select * from Employee
Select LastName, Salary from Employee
```

デフォルト動作では NULL 値を返します。

Web サービスの権限

エンドユーザーは、Web サービスクライアントを通じて Web サービス要求の送信および Web サービス応答の受信を行うことができます。 Web サービスに対するユーザーのアクセスレベルは、権限によって制御されます。

ユーザーおよびグループには、以下の Web サービスオブジェクトに対する権限を割り当てることができます。

- Web サービス
- REST Web サービスリソース
- SOAP Web サービス操作

Web サービスオブジェクトに対する権限を割り当てた場合、ユーザーまたはグループはその Web サービスオブジェクトに属するすべてのオブジェクトに対して同じ権限を継承します。 例えば、Web サービスに対する実行権限をユーザーに割り当てたとします。 このユーザーは、Web サービスでの Web サービス操作に対する実行権限を継承します。

Web サービス操作に対するユーザーおよびグループの権限を拒否することができます。 権限を拒否するには、ユーザーとグループがすでに持っている可能性のある権限に例外を設定します。例えば、3 種類の操作がある Web サービスに対する実行権限をユーザーが持っているとします。 この Web サービスに属する Web サービス操作の 1 つについて、ユーザーによる実行を拒否することができます。

Web サービスの権限のタイプ

管理者は Web サービス権限を次のタイプのユーザーおよびグループに割り当てます。

- Web サービスコンシューマ。Web サービスに要求を送信して Web サービスから応答を受信するネイティブドメインユーザー。ユーザーは Web サービスに対する実行権限を持っている必要があります。
- Web サービス管理者。Administrator にログインし、Web サービスプロパティを編集して、権限を他のユーザーに付与できるユーザー。
- Web サービスオペレータ。Administrator にログインし、Web サービスを監視して、Web サービスの開始または停止を実行できるユーザー。

管理者は、以下の権限をユーザーおよびグループに割り当てることができます。

- 付与権限: Administrator ツールまたは *infacmd* コマンドラインプログラムを使用して、Web サービスオブジェクトに対する権限を管理できます。
- 実行権限: Web サービス要求を送信したり Web サービス応答を受信したりできます。

以下の表に、各 SOAP Web サービスオブジェクトの権限を示します。

オブジェクト	権限の付与	実行権限
SOAP Web サービス	Web サービスおよび Web サービス内のすべての Web サービス操作に対する権限を付与および取り消すことができます。	Web サービス内のすべての Web サービス操作について、Web サービス要求を送信したり Web サービス応答を受信したりできます。
SOAP Web サービス操作	Web サービス操作に対する権限を付与、取り消し、および拒否することができます。	Web サービス操作について、Web サービス要求を送信したり Web サービス応答を受信したりできます。

以下の表に、各 REST Web サービスオブジェクトの権限を示します。

オブジェクト	権限の付与	実行権限
REST Web サービス	REST Web サービスおよび Web サービス内のすべての Web サービスリソースに対する権限を付与および取り消すことができます。	REST Web サービス内のすべての Web サービスリソースについて、Web サービス要求を送信したり Web サービス応答を受信したりできます。
REST リソース	REST Web サービスリソースの付与、取り消し、および拒否を行うことができます。	REST Web サービスリソースについて、Web サービス要求を送信したり Web サービス応答を受信したりできます。

Web サービスに対する権限の割り当て

Web サービスオブジェクトに対する権限を割り当てると、オブジェクトに対するユーザーまたはグループのアクセスレベルが定義されます。

1. ［管理］タブで **［サービスとノード］** ビューを選択します。
2. ナビゲータで、Data Integration Service を選択します。
3. ［コンテンツ］パネルで、**［アプリケーション］** ビューを選択します。
4. Web サービスオブジェクトを選択します。
5. ［詳細］パネルで、**［グループ権限］** ビューまたは **［ユーザー権限］** ビューを選択します。
6. **［権限の割り当て］** ボタンをクリックします。

   ［権限の割り当て］ ダイアログボックスに、SQL データサービスオブジェクトに対する権限がないすべてのユーザーまたはグループが表示されます。
7. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**［フィルタ］** ボタンをクリックします。
8. ユーザーまたはグループを選択し、**［次へ］** をクリックします。
9. 割り当てるそれぞれの権限タイプについて、**［許可］** を選択します。
10. **［完了］** をクリックします。

Web サービスに対する権限の詳細の表示

権限の詳細を表示すると、有効な権限の元になる権限を確認できます。

1. ［管理］タブで**［サービスとノード］**ビューを選択します。
2. ナビゲータで、Data Integration Service を選択します。
3. ［コンテンツ］パネルで、**［アプリケーション］**ビューを選択します。
4. Web サービスオブジェクトを選択します。
5. ［詳細］パネルで、**［グループ権限］**ビューまたは**［ユーザー権限］**ビューを選択します。
6. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**［フィルタ］**ボタンをクリックします。
7. ユーザーまたはグループを選択し、**［権限の詳細の表示］**ボタンをクリックします。

   ［権限の詳細］ダイアログボックスが表示されます。 このダイアログボックスには、ユーザーまたはグループに割り当てられた直接権限、親グループに割り当てられた直接権限、および親オブジェクトから継承された権限が表示されます。 また、権限のチェックを省略する管理者ロールがユーザーまたはグループに割り当てられているかどうかも表示されます。
8. **［閉じる］**をクリックします。
9. または、**［権限の編集］**をクリックして直接権限を編集します。

Web サービスに対する権限の編集

ユーザーまたはグループの Web サービスに対する直接権限を編集することができます。 Web サービスオブジェクトに対する権限を編集する際、オブジェクトに対する権限を拒否することもできます。 継承された権限や自分自身の権限を取り消すことはできません。

注: オブジェクトに対する直接権限を取り消した後も、ユーザーやグループが親グループまたはオブジェクトから権限を継承している可能性があります。

1. ［管理］タブで**［サービスとノード］**ビューを選択します。
2. ナビゲータで、Data Integration Service を選択します。
3. ［コンテンツ］パネルで、**［アプリケーション］**ビューを選択します。
4. Web サービスオブジェクトを選択します。
5. ［詳細］パネルで、**［グループ権限］**ビューまたは**［ユーザー権限］**ビューを選択します。
6. ユーザーおよびグループを検索するためのフィルタ条件を入力し、**［フィルタ］**ボタンをクリックします。
7. ユーザーまたはグループを選択し、**［直接権限の編集］**ボタンをクリックします。

   ［直接権限の編集］ダイアログボックスが表示されます。
8. 権限を許可または取り消します。
   - 権限を割り当てる場合は、**［許可］**を選択します。
   - Web サービスオブジェクトに対する権限を拒否する場合は、**［拒否］**を選択します。
   - 特定の権限を 1 つだけ取り消す場合は、**［許可］**の選択を解除します。
   - すべての権限を取り消す場合は、**［権限を取り消す］**を選択します。

   直接割り当てられた権限か継承された権限かを確認するには、**［権限の詳細の表示］**をクリックします。
9. **［OK］**をクリックします。

第 11 章

監査レポート

この章では、以下の項目について説明します。

監査レポートの概要

監査レポートを使用すると、Informatica ドメイン内のユーザーとグループの情報、およびそれらに割り当てられた特権と権限についての情報を表示することができます。

以下の監査レポートが生成できます。

ユーザーの個人情報

ドメイン内のユーザーアカウントについての情報（ユーザーのステータスなど）を表示します。レポート生成対象（ユーザーまたはグループ）を選択することができます。

ユーザーグループの関連付け

ユーザーとユーザーが属するグループに関する情報を表示します。レポート生成対象（ユーザーまたはグループ）を選択することができます。

特権

ドメイン内のユーザーおよびグループに割り当てられた特権についての情報を表示します。レポート生成対象（ユーザーまたはグループ）を選択することができます。

ロール

ドメイン内のユーザーおよびグループに割り当てられたロールの情報を表示します。レポート生成対象にするロールを選択することができます。

ドメインオブジェクト権限

ユーザーおよびグループが権限を持っているドメインオブジェクトの情報を表示します。レポート生成対象（ユーザーまたはグループ）を選択することができます。

監査レポートはさまざまな形式（CSV、テキスト、PDF ファイルなど）で生成できます。レポートは画面上で見ることもできます。

監査レポートは Administrator ツールまたはコマンドラインから生成できます。コマンドラインから監査レポートを実行する場合は、infacmd aud というコマンドラインプログラムを実行します。

ユーザーの個人情報

ユーザーの個人情報レポートには、ドメイン内のユーザーアカウントの連絡先情報とステータスが表示されます。

グループに関してレポートを実行する場合、レポートはユーザーのリストをグループに分けて整理し、グループ名とセキュリティドメインをグループごとに表示します。レポートには、ネストされたグループが個別に表示されます。

ユーザーの個人情報レポートには、以下の情報が表示されます。

ログイン名

ユーザーアカウントのログイン名。

フルネーム

ユーザーアカウントのフルネーム。

セキュリティドメイン

ユーザーが属しているセキュリティドメイン。

説明

ユーザアカウントの説明。

電子メール ID

ユーザーアカウントの電子メールアドレス。

電話番号

ユーザーアカウントの電話番号。

ロックされたアカウント

アカウントがロックされているかどうかを示します。アカウントがロックされていれば「はい」、ロックされていなければ「いいえ」とレポートに表示されます。

無効になっているアカウント

アカウントが無効になっているかどうかを示します。アカウントが無効になっていれば「はい」、有効になっていれば「いいえ」とレポートに表示されます。

ユーザーグループの関連付け

ユーザーグループの関連付けレポートには、ユーザーおよびその関連のグループについての情報が表示されます。

ユーザーに関してこのレポートを実行した場合、レポートにはユーザーのリストと、ユーザーが属するグループが表示されます。

ユーザーグループの関連付けレポートには、以下の情報が表示されます。

ログイン名

ユーザーアカウントのログイン名。

フルネーム

ユーザーアカウントのフルネーム。

セキュリティドメイン

ユーザーアカウントが属しているセキュリティドメイン。

グループ名

ユーザーが属するグループの名前。

グループパス

グループが単一のグループの場合、グループパスにはグループ名が表示されます。グループがネストされたグループの場合、ネストされたグループの階層の中でそのグループのいる位置がグループパスに表示されます。

グループのセキュリティドメイン

ユーザーが属しているグループのセキュリティドメイン。

グループに関してレポートを実行する場合、レポートはユーザーのリストをグループに分けて整理し、グループ名とセキュリティドメインをグループごとに表示します。レポートには、ネストされたグループが個別に表示されます。各グループに関し、グループに属する子グループとユーザーのリストがレポートに表示されます。

ユーザーグループの関連付けレポートには、グループに属するユーザーに関して以下の情報が表示されます。

ログイン名

ユーザーアカウントのログイン名。

フルネーム

ユーザーアカウントのフルネーム。

セキュリティドメイン

ユーザーアカウントが属しているセキュリティドメイン。

ユーザーグループの関連付けレポートには、グループに属する子グループに関して以下の情報が表示されます。

グループ名

グループの名前。

セキュリティドメイン

グループが属しているセキュリティドメイン。

グループパス

グループが単一のグループの場合、グループパスにはグループ名が表示されます。グループがネストされたグループの場合、ネストされたグループの階層の中でそのグループのいる位置がグループパスに表示されます。

特権

特権レポートに、ユーザーとグループ、およびユーザーとグループに割り当てられた特権が表示されます。

ユーザーに関してレポートを実行した場合、ユーザーリストと、各ユーザーに割り当てられた特権がレポートに表示されます。グループのレポートを実行した場合、グループリストと、各グループに割り当てられた特権がレポートに表示されます。

特権レポートには、以下の情報が表示されます。

特権名

特権の名前。

特権パス

特権が入っている特権グループの階層。

オブジェクト名

特権が許可されている対象のオブジェクトの名前。

オブジェクトタイプ

特権が許可されている対象のオブジェクトのタイプ。

ロールの関連付け

ロールの関連付けレポートには、ロールのリストと、ロールが割り当てられているユーザーおよびグループが表示されます。

ロールの関連付けレポートには、以下の情報が表示されます。

ログイン名

ロールが割り当てられているユーザーアカウントのログイン名。ユーザーのリストに対して表示します。

フルネーム

ロールが割り当てられているユーザーアカウントのフルネーム。ユーザーのリストに対して表示します。

グループ名

ロールが割り当てられているグループの名前。グループのリストに対して表示します。

セキュリティドメイン

ユーザーまたはグループが属するセキュリティドメイン。

オブジェクト名

ロールの一連の特権の許可対象となるオブジェクトの名前。

オブジェクトタイプ

ロールの一連の特権の許可対象となるオブジェクトのタイプ。

ドメインオブジェクト権限

ドメインオブジェクト権限のレポートでは、ユーザーとグループ、およびユーザーとグループが権限を持つオブジェクトを表示します。

ユーザーに関してレポートを実行する場合、ユーザーのリスト、およびユーザーが権限を持つオブジェクトがレポートに表示されます。グループのレポートを実行する場合、グループのリスト、およびグループが権限を持つオブジェクトがレポートに表示されます。

ドメインオブジェクト権限のレポートでは、以下の情報が表示されます。

オブジェクト名

ユーザーまたはグループが権限を持つオブジェクトの名前。

オブジェクトタイプ

ユーザーまたはグループが権限を持つオブジェクトのタイプ。

オブジェクトパス

リポジトリ内のオブジェクトの場所。

監査レポートの対象ユーザーの選択

複数のユーザーに対して監査レポートを生成できます。

1. Administrator ツールで、**[セキュリティ]** > **[監査レポート]** をクリックします。
2. **[レポートのタイプを選択]** リストから、実行する監査レポートのタイプを選択します。
3. **[次のレポートを作成]** リストから、**[ユーザー]** を選択して **[実行]** をクリックします。

   [ユーザーの選択] ダイアログボックスが表示されます。デフォルトで **[ユーザー]** アイコンが選択され、使用できるすべてのユーザーが表示されます。リストには、ユーザーのフルネームと、そのユーザーが属するセキュリティドメインが表示されます。
4. **[使用可能なユーザー]** リストから、実行するレポートの対象のユーザーを選択します。

   複数のユーザーを選択するには、Shift キーまたは Ctrl キーを使用します。
5. ユーザーをグループごとに選択するには、**[グループ]** アイコンをクリックします。

   [使用可能なグループ] リストに、ドメイン内のすべてのグループが表示され、**[メンバ]** リストに、グループのメンバであるユーザーが表示されます。**[メンバ]** リストから、レポートの実行対象のユーザーを選択します。複数のグループからユーザーを選択することができます。
6. **[追加]** をクリックします。

   すべてのユーザーに関するレポートを実行するには、**[ユーザー]** アイコンをクリックしてから、ユーザーを選択せずに **[すべて追加]** をクリックします。

   グループ内のすべてのユーザーに関してレポートを実行する場合は、**[グループ]** アイコンをクリックします。グループを選択し、**[メンバ]** リストからユーザーを選択せずに、**[すべて追加]** をクリックします。

   選択されたユーザーが **[選択したユーザー]** リストに移動します。
7. **[レポート出力形式]** リストから、レポートを表示する形式を選択します。

   デフォルトで、レポートが画面に表示されます。

監査レポートを以下の形式のいずれかで表示することもできます。

- テキスト。値を列形式にリストしてテキストファイルとして監査レポートを生成します。
- CSV。値をカンマで区切ってテキストファイルとして監査レポートを生成します。
- PDF。監査レポートを PDF 形式で生成します。レポートを表示するには Acrobat Reader をインストールする必要があります。

8. **［レポートの生成］**をクリックします。

監査レポートの対象グループの選択

複数のグループに対して監査レポートを実行できます。

1. Administrator ツールで、**［セキュリティ］** > **［監査レポート］**をクリックします。
2. **［レポートのタイプを選択］**リストから、実行する監査レポートのタイプを選択します。
3. **［次のレポートを作成］**リストから、**［グループ］**を選択して**［実行］**をクリックします。

   ［グループの選択］ダイアログボックスが表示されます。グループのリストがセキュリティドメインごとの整理して表示されます。
4. **［使用可能なグループ］**リストから、実行するレポートの対象のグループを選択します。

   複数のグループを選択するには、Shift キーまたは Ctrl キーを使用します。
5. **［追加］**をクリックします。

   すべてのグループに関してレポートを実行する場合は、グループを 1 つ選択してから**［すべて追加］**をクリックするという操作は行わないでください。

   選択されたグループが**［選択したグループ］**リストに移動します。
6. **［レポート出力形式］**リストから、レポートを表示する形式を選択します。

   デフォルトで、レポートが画面に表示されます。
   監査レポートを以下の形式のいずれかで実行することもできます。

   - テキスト。値を列形式にリストしてテキストファイルとして監査レポートを生成します。
   - CSV。値をカンマで区切ってテキストファイルとして監査レポートを生成します。
   - PDF。監査レポートを PDF 形式で生成します。レポートを表示するには Acrobat Reader をインストールする必要があります。
7. **［レポートの生成］**をクリックします。

監査レポートの対象ロールの選択

ロールの関連付けレポートを実行するときに、レポート実行の対象になるロールを選択する必要があります。

1. Administrator ツールで、**［セキュリティ］** > **［監査レポート］**をクリックします。
2. **［レポートのタイプを選択］**リストから、**［ロールの関連付け］**レポートを選択します。
3. **［次のレポートを作成］**リストから、**［ロール］**を選択して**［実行］**をクリックします。

［ロールの選択］ダイアログボックスが表示されます。システム定義のロールのリストが、カスタムロールのリストとは別に表示されます。

4. **［使用可能なロール］**リストから、実行するレポートの対象のロールを選択します。

   複数のロールを選択するには、Shift キーまたは Ctrl キーを使用します。

5. **［追加］**をクリックします。

   すべてのロールに関してレポートを実行する場合は、ロールを 1 つ選択してから**［すべて追加］**をクリックするという操作は行わないでください。

   選択されたロールが**［選択したロール］**リストに移動します。

6. **［レポート出力形式］**リストから、レポートを表示する形式を選択します。

   デフォルトで、レポートが画面に表示されます。
   監査レポートを以下の形式のいずれかで実行することもできます。

   - テキスト。値を列形式にリストしてテキストファイルとして監査レポートを生成します。
   - CSV。値をカンマで区切ってテキストファイルとして監査レポートを生成します。
   - PDF。監査レポートを PDF 形式で生成します。レポートを表示するには Acrobat Reader をインストールする必要があります。

7. **［レポートの生成］**をクリックします。

付録 A

コマンドラインの特権および権限

この付録では、以下の項目について説明します。

infacmd as コマンド

infacmd as コマンドを実行するには、ユーザーは一覧表示されているドメイン特権、アナリストサービス特権、ドメインオブジェクト権限のセットの 1 つを持っていることが必要です。

以下の表に、*infacmd as* コマンドに必要な特権と権限を一覧表示します。

infacmd as **コマンド**	**特権グループ**	**特権名**	**権限の対象**
CreateAuditTables	ドメイン管理	サービス管理	アナリストサービスが実行されるドメインまたはノード
CreateService	ドメイン管理	サービス管理	アナリストサービスが実行されるドメインまたはノード
DeleteAuditTables	ドメイン管理	サービス管理	アナリストサービスが実行されるドメインまたはノード
ListServiceOptions	-	-	アナリストサービス
ListServiceProcessOptions	-	-	アナリストサービス
UpdateServiceOptions	ドメイン管理	サービス管理	アナリストサービスが実行されるドメインまたはノード
UpdateServiceProcessOptions	ドメイン管理	サービス管理	アナリストサービスが実行されるドメインまたはノード

infacmd dis コマンド

infacmd dis コマンドを実行するには、ユーザーは一覧表示されているドメイン特権、データ統合サービス特権、ドメインオブジェクト権限のセットの 1 つを持っていることが必要です。

以下の表に、*infacmd dis* コマンドに必要な特権と権限を一覧表示します。

infacmd dis **コマンド**	**特権グループ**	**特権名**	**権限**
BackupApplication	アプリケーション管理	アプリケーションの管理	アプリケーション
CancelDataObjectCacheRefresh	-	-	-
CreateService	ドメイン管理	サービスの管理	データ統合サービスが実行されるドメインまたはノード
DeployApplication	アプリケーション管理	アプリケーションの管理	アプリケーション
ListApplicationObjects	-	-	-
ListApplications	-	-	-
ListComputeOptions	ドメイン管理	サービスの管理	データ統合サービス

infacmd dis コマンド	特権グループ	特権名	権限
ListDataObjectOptions	-	-	-
ListServiceOptions	ドメイン管理	サービスの管理	データ統合サービス
ListServiceProcessOptions	ドメイン管理	サービスの管理	データ統合サービス
PurgeDataObjectCache	-	-	-
RefreshDataObjectCache	-	-	-
RenameApplication	アプリケーション管理	アプリケーションの管理	アプリケーション
RestoreApplication	アプリケーション管理	アプリケーションの管理	アプリケーション
StartApplication	アプリケーション管理	アプリケーションの管理	アプリケーション
StopApplication	アプリケーション管理	アプリケーションの管理	アプリケーション
stopBlazeService	アプリケーション管理	アプリケーションの管理	アプリケーション
UndeployApplication	アプリケーション管理	アプリケーションの管理	アプリケーション
UpdateApplication	アプリケーション管理	アプリケーションの管理	アプリケーション
UpdateApplicationOptions	アプリケーション管理	アプリケーションの管理	アプリケーション
UpdateDataObjectOptions	アプリケーション管理	アプリケーションの管理	-
UpdateComputeOptions	ドメイン管理	サービスの管理	データ統合サービス
UpdateServiceOptions	ドメイン管理	サービスの管理	データ統合サービス
UpdateServiceProcessOptions	ドメイン管理	サービスの管理	データ統合サービス

infacmd es コマンド

次の infacmd es コマンドを実行するには、ユーザーにドメインの管理者ロールが割り当てられている必要があります。

- ListServiceOptions
- UpdateServiceOptions
- UpdateSMTPOptions

infacmd ipc コマンド

infacmd ipc コマンドを実行するには、ユーザーは一覧表示されているモデルリポジトリオブジェクト権限の 1 つを持っていることが必要です。

以下の表に、*infacmd ipc* コマンドに必要な特権と権限を一覧表示します。

infacmd ipc **コマンド**	**特権グループ**	**特権名**	**権限**
ExportToPC	-	-	エクスポートされる参照テーブルを作成するフォルダでの読み取り。
genReuseReportFromPC	ツール	リポジトリマネージャへのアクセス	-

infacmd isp コマンド

infacmd isp コマンドを実行するには、ユーザーは一覧表示されているドメイン特権、サービス特権、ドメインオブジェクト権限、および接続権限のセットの 1 つを持っていることが必要です。

以下のコマンドを実行するには、ユーザーにドメインの管理者ロールが割り当てられている必要があります。

- AddDomainLink
- AssignGroupPermission（ドメインに対して）
- AssignGroupPermission（オペレーティングシステムプロファイルに対して）
- AddServiceLevel
- AssignUserPermission（ドメインに対して）
- AssignUserPermission（オペレーティングシステムプロファイルに対して）
- CreateConnection
- CreateOSProfile
- PurgeLog
- RemoveDomainLink
- RemoveOSProfile
- RemoveServiceLevel
- SwitchToGatewayNode
- SwitchToWorkerNode
- UpdateDomainOptions
- UpdateGatewayInfo
- UpdateServiceLevel
- UpdateSMTPOptions

UpdateGatewayInfo コマンドを実行するには、ユーザーにドメインの管理者ロールが割り当てられている必要があります。

以下の表に、*infacmd isp* コマンドに必要な特権と権限を一覧表示します。

infacmd isp **コマンド**	**特権グループ**	**特権名**	**権限**
GetNodeName	-	-	ノード
UpdateGatewayInfo	-	-	-

infacmd isp **コマンド**	**特権グループ**	**特権名**	**権限**
AddAlertUser（ユーザーアカウント用）	-	-	-
AddAlertUser（他のユーザー用）	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
AddConnectionPermissions	-	-	接続への付与
AddDomainLink	-	-	-
AddDomainNode	ドメイン管理	ノードとグリッドの管理	ドメインとノード
AssignGroupPermission（アプリケーションサービスまたはライセンスオブジェクトに対して）	ドメイン管理	サービスの管理	アプリケーションサービスまたはライセンスオブジェクト
AssignGroupPermission（ドメインに対して）	-	-	-
AssignGroupPermission（フォルダに対して）	ドメイン管理	ドメインフォルダの管理	Folder
AssignGroupPermission（ノードとグリッドに対して）	ドメイン管理	ノードとグリッドの管理	ノードまたはグリッド
AssignGroupPermission（オペレーティングシステムプロファイルに対して）	-	-	-
AddGroupPrivilege	セキュリティ管理	権限とロールの付与	ドメイン、Metadata Manager サービス、モデルリポジトリサービス、または PowerCenter リポジトリサービス
AddLicense	ドメイン管理	サービスの管理	ドメインまたは親フォルダ
AddNodeResource	ドメイン管理	ノードとグリッドの管理	Node

infacmd isp **コマンド**	**特権グループ**	**特権名**	**権限**
AddRolePrivilege	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
AddServiceLevel	-	-	-
AssignUserPermission（アプリケーションサービスまたはライセンスオブジェクトに対して）	ドメイン管理	サービスの管理	アプリケーションサービスまたはライセンスオブジェクト
AssignUserPermission（ドメインに対して）	-	-	-
AssignUserPermission（フォルダに対して）	ドメイン管理	ドメインフォルダの管理	Folder
AssignUserPermission（ノードとグリッドに対して）	ドメイン管理	ノードとグリッドの管理	ノードまたはグリッド
AssignUserPermission（オペレーティングシステムプロファイルに対して）	-	-	-
AssignUserPrivilege	セキュリティ管理	権限とロールの付与	ドメイン、Metadata Manager サービス、モデルリポジトリサービス、または PowerCenter リポジトリサービス
AssignUserToGroup	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
AssignedToLicense	ドメイン管理	サービスの管理	ライセンスオブジェクトとアプリケーションサービス
AssignISTOMMService	ドメイン管理	サービスの管理	Metadata Manager サービス
AssignLicense	ドメイン管理	サービスの管理	ライセンスオブジェクトとアプリケーションサービス
AssignRoleToGroup	セキュリティ管理	権限とロールの付与	ドメイン、Metadata Manager サービス、モデルリポジトリサービス、または PowerCenter リポジトリサービス

infacmd isp コマンド	特権グループ	特権名	権限
AssignRoleToUser	セキュリティ管理	権限とロールの付与	ドメイン、Metadata Manager サービス、モデルリポジトリサービス、または PowerCenter リポジトリサービス
AssignRSToWSHubService	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスおよび Web サービス Hub
ConvertLogFile	-	-	ドメインまたはアプリケーションサービス
CreateFolder	ドメイン管理	ドメインフォルダの管理	ドメインまたは親フォルダ
CreateConnection	-	-	-
CreateGrid	ドメイン管理	ノードとグリッドの管理	ドメインまたは親フォルダ、およびグリッドに割り当てられているノード
CreateGroup	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
CreateIntegrationService	ドメイン管理	サービスの管理	ドメインまたは親フォルダ、PowerCenter 統合サービスが実行されているノードまたはグリッド、ライセンスオブジェクト、および関連する PowerCenter リポジトリサービス
CreateMMService	ドメイン管理	サービスの管理	ドメインまたは親フォルダ、Metadata Manager サービスが実行されているノード、ライセンスオブジェクト、および関連する PowerCenter 統合サービスと PowerCenter リポジトリサービス
CreateOSProfile	-	-	-
CreateRepositoryService	ドメイン管理	サービスの管理	ドメインまたは親フォルダ、PowerCenter リポジトリサービスが実行されているノード、およびライセンスオブジェクト

infacmd isp コマンド	特権グループ	特権名	権限
CreateRole	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
CreateSAPBWService	ドメイン管理	サービスの管理	ドメインまたは親フォルダ、SAP BW サービスが実行されているノードまたはグリッド、ライセンスオブジェクト、および関連する PowerCenter 統合サービス
CreateUser	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
CreateWSHubService	ドメイン管理	サービスの管理	ドメインまたは親フォルダ、Web サービス Hub が実行されているノードまたはグリッド、ライセンスオブジェクト、および関連する PowerCenter リポジトリサービス
DisableNodeResource	ドメイン管理	ノードとグリッドの管理	Node
DisableService（Metadata Manager サービス用）	ドメイン管理	サービス実行の管理	Metadata Manager サービス、および関連する PowerCenter 統合サービスと PowerCenter リポジトリサービス
DisableService（その他のすべてのアプリケーションサービス用）	ドメイン管理	サービス実行の管理	アプリケーションサービス
DisableServiceProcess	ドメイン管理	サービス実行の管理	アプリケーションサービス
DisableUser	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
EditUser	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
EnableNodeResource	ドメイン管理	ノードとグリッドの管理	Node

infacmd isp コマンド	特権グループ	特権名	権限
EnableService（Metadata Manager サービス用）	ドメイン管理	サービス実行の管理	Metadata Manager サービス、および関連する PowerCenter 統合サービスと PowerCenter リポジトリサービス
EnableService(その他のすべてのアプリケーションサービス用）	ドメイン管理	サービス実行の管理	アプリケーションサービス
EnableServiceProcess	ドメイン管理	サービス実行の管理	アプリケーションサービス
EnableUser	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
ExportDomainObjects（ユーザー、グループ、およびロール用）	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
ExportDomainObjects（接続用）	ドメイン管理	接続の管理	接続での読み込み
ExportUsersAndGroups	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
generateHadoopConnectionFromHiveConection	-	-	-
GetFolderInfo	-	-	Folder
GetLastError	-	-	アプリケーションサービス
GetLog	-	-	ドメインまたはアプリケーションサービス
GetNodeName	-	-	Node
GetServiceOption	-	-	アプリケーションサービス
GetServiceProcessOption	-	-	アプリケーションサービス
GetServiceProcessStatus	-	-	アプリケーションサービス
GetServiceStatus	-	-	アプリケーションサービス

infacmd isp コマンド	特権グループ	特権名	権限
GetSessionLog	ランタイムオブジェクト	監視	リポジトリフォルダに対する読み込み
GetWorkflowLog	ランタイムオブジェクト	監視	リポジトリフォルダに対する読み込み
ヘルプ	-	-	-
ImportDomainObjects（ユーザー、グループ、およびロール用）	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
ImportDomainObjects（接続用）	ドメイン管理	接続の管理	接続での書き込み
ImportUsersAndGroups	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
ListAlertUsers	-	-	ドメイン
ListAllGroups	-	-	-
ListAllRoles	-	-	-
ListAllUsers	-	-	-
ListConnectionOptions	-	-	接続での読み込み
ListConnections	-	-	-
ListConnectionPermissions	-	-	-
グループによる ListConnectionPermissions	-	-	-
ユーザーによる ListConnectionPermissions	-	-	-
ListDomainLinks	-	-	ドメイン
ListDomainOptions	-	-	ドメイン
ListFolders	-	-	フォルダ
ListGridNodes	-	-	-
ListGroupsForUser	-	-	ドメイン
ListGroupPermissions	-	-	-

infacmd isp コマンド	特権グループ	特権名	権限
ListGroupPrivilege	セキュリティ管理	権限とロールの付与	ドメイン、Metadata Manager サービス、モデルリポジトリサービス、または PowerCenter リポジトリサービス
ListLDAPConnectivity	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
ListLicenses	-	-	ライセンスオブジェクト
listMonitoringOptions	監視	監視設定	ドメイン
ListNodeOptions	-	-	ノード
ListNodes	-	-	-
ListNodeResources	-	-	ノード
ListPlugins	-	-	-
ListRepositoryLDAPConfiguration	-	-	ドメイン
ListRolePrivileges	-	-	-
ListSecurityDomains	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
ListServiceLevels	-	-	ドメイン
ListServiceNodes	-	-	アプリケーションサービス
ListServicePrivileges	-	-	-
ListServices	-	-	-
ListSMTPOptions	-	-	ドメイン
ListUserPermissions	-	-	-
ListUserPrivilege	セキュリティ管理	権限とロールの付与	ドメイン、Metadata Manager サービス、モデルリポジトリサービス、または PowerCenter リポジトリサービス
MoveFolder	ドメイン管理	ドメインフォルダの管理	元のフォルダと宛先フォルダ

infacmd isp **コマンド**	**特権グループ**	**特権名**	**権限**
MoveObject（アプリケーションサービスまたはライセンスオブジェクト用）	ドメイン管理	サービスの管理	元のフォルダと宛先フォルダ
MoveObject（ノードまたはグリッド用）	ドメイン管理	ノードとグリッドの管理	元のフォルダと宛先フォルダ
Ping	-	-	-
PurgeLog	-	-	-
purgeMonitoringData	監視	監視設定	ドメイン
RemoveAlertUser（ユーザーアカウント用）	-	-	-
RemoveAlertUser（他のユーザー用）	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
RemoveConnection	-	-	接続での書き込み
RemoveConnectionPermissions	-	-	接続への付与
RemoveDomainLink	-	-	-
RemoveFolder	ドメイン管理	ドメインフォルダの管理	ドメインまたは親フォルダ、および削除対象フォルダ
RemoveGrid	ドメイン管理	ノードとグリッドの管理	ドメインまたは親フォルダ、およびグリッド
RemoveGroup	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
RemoveGroupPrivilege	セキュリティ管理	権限とロールの付与	ドメイン、Metadata Manager サービス、モデルリポジトリサービス、または PowerCenter リポジトリサービス
RemoveLicense	ドメイン管理	サービスの管理	ドメインまたは親フォルダ、およびライセンスオブジェクト
RemoveNode	ドメイン管理	ノードとグリッドの管理	ドメインまたは親フォルダ、およびノード

infacmd isp コマンド	特権グループ	特権名	権限
RemoveNodeResource	ドメイン管理	ノードとグリッドの管理	Node
RemoveOSProfile	-	-	-
RemoveRole	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
RemoveRolePrivilege	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
RemoveService	ドメイン管理	サービスの管理	ドメインまたは親フォルダ、およびアプリケーションサービス
RemoveServiceLevel	-	-	-
RemoveUser	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
RemoveUserFromGroup	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
RemoveUserPrivilege	セキュリティ管理	権限とロールの付与	ドメイン、Metadata Manager サービス、モデルリポジトリサービス、または PowerCenter リポジトリサービス
RenameConnection	-	-	接続での書き込み
ResetPassword（ユーザーのユーザーアカウント用）	-	-	-
ResetPassword（他のユーザ用）	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
RunCPUProfile	ドメイン管理	ノードとグリッドの管理	Node
SetConnectionPermission	-	-	接続への付与

infacmd isp コマンド	特権グループ	特権名	権限
SetLDAPConnectivity	セキュリティ管理	ユーザー、グループ、およびロールの管理。	-
SetRepositoryLDAPConfiguration	-	-	ドメイン
ShowLicense	-	-	ライセンスオブジェクト
ShutdownNode	ドメイン管理	ノードとグリッドの管理	Node
SwitchToGatewayNode	-	-	-
SwitchToWorkerNode	-	-	-
UnAssignISMMService	ドメイン管理	サービスの管理	PowerCenter 統合サービスおよび Metadata Manager サービス
UnassignLicense	ドメイン管理	サービスの管理	ライセンスオブジェクトとアプリケーションサービス
UnAssignRoleFromGroup	セキュリティ管理	権限とロールの付与	ドメイン、Metadata Manager サービス、モデルリポジトリサービス、または PowerCenter リポジトリサービス
UnAssignRoleFromUser	セキュリティ管理	権限とロールの付与	ドメイン、Metadata Manager サービス、モデルリポジトリサービス、または PowerCenter リポジトリサービス
UnassignRSWSHubService	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスおよび Web サービス Hub
UnassociateDomainNode	ドメイン管理	ノードとグリッドの管理	Node
UpdateConnection	-	-	接続での書き込み
UpdateDomainOptions	-	-	-
UpdateFolder	ドメイン管理	ドメインフォルダの管理	Folder
UpdateGatewayInfo	-	-	-

infacmd isp コマンド	特権グループ	特権名	権限
UpdateGrid	ドメイン管理	ノードとグリッドの管理	グリッドとノード
UpdateIntegrationService	ドメイン管理	サービスの管理	PowerCenter 統合サービス
UpdateLicense	ドメイン管理	サービスの管理	ライセンスオブジェクト
UpdateMMService	ドメイン管理	サービスの管理	Metadata Manager サービス
updateMonitoringOptions	監視	監視設定	ドメイン
UpdateNodeOptions	ドメイン管理	ノードとグリッドの管理	Node
UpdateNodeRole	ドメイン管理	ノードとグリッドの管理	Node
UpdateOSProfile	セキュリティ管理	ユーザー、グループ、およびロールの管理。	オペレーティングシステムプロファイル
UpdateRepositoryService	ドメイン管理	サービスの管理	PowerCenter リポジトリサービス
UpdateSAPBWService	ドメイン管理	サービスの管理	SAP BW サービス
UpdateServiceLevel	-	-	-
UpdateServiceProcess	ドメイン管理	サービスの管理	PowerCenter 統合サービス PowerCenter 統合サービスに追加された各ノード
UpdateSMTPOptions	-	-	-
UpdateWSHubService	ドメイン管理	サービスの管理	Web サービス Hub

infacmd mrs コマンド

infacmd mrs コマンドを実行するには、ユーザーは一覧表示されているドメイン特権、モデルリポジトリサービス特権、およびモデルリポジトリオブジェクト権限のセットの 1 つを持っていることが必要です。

ユーザーが、所有するオブジェクトに対するロックおよびバージョニング操作に関連する次のコマンドを実行できます。他のユーザーが所有しているオブジェクトに対してコマンドを実行するには、チームベース開発の管理特権が必要となります。

- CheckInObject
- ListCheckedOutObjects
- ListLockedObjects
- UndoCheckout
- UnlockObject

以下の表に、*infacmd mrs* コマンドに必要な特権と権限を一覧表示します。

infacmd mrs **コマンド**	**特権グループ**	**特権名**	**権限**
BackupContents	ドメイン管理	サービス管理	モデルリポジトリサービスが実行されるドメインまたはノード
CheckInObject	ドメイン管理	チームベース開発の管理	モデルリポジトリサービス
CreateContents	ドメイン管理	サービス管理	モデルリポジトリサービスが実行されるドメインまたはノード
CreateFolder	ドメイン管理	Developer tool の場合: - Developer へのアクセス Analyst ツールの場合: - Analyst へのアクセス - 検出ワークスペースへのアクセス	モデルリポジトリサービス
CreateProject	ドメイン管理	プロジェクトの作成、編集、削除	モデルリポジトリサービス
CreateService	ドメイン管理	サービス管理	モデルリポジトリサービスが実行されるドメインまたはノード
DeleteContents	ドメイン管理	サービス管理	モデルリポジトリサービスが実行されるドメインまたはノード
DeleteFolder	ドメイン管理	Developer tool の場合: - Developer へのアクセス Analyst ツールの場合: - Analyst へのアクセス - 検出ワークスペースへのアクセス	モデルリポジトリサービス
DeleteProject	ドメイン管理	プロジェクトの作成、編集、削除	モデルリポジトリサービス

infacmd mrs コマンド	特権グループ	特権名	権限
ListBackupFiles	ドメイン管理	サービス管理	モデルリポジトリサービスが実行されるドメインまたはノード
ListCheckedOutObjects	ドメイン管理	チームベース開発の管理	モデルリポジトリサービス
ListFolders	ドメイン管理	サービス管理	モデルリポジトリサービスが実行されるドメインまたはノード
ListLockedObjects	ドメイン管理	チームベース開発の管理	モデルリポジトリサービス
ListProjects	ドメイン管理	Developer tool の場合: - Developer へのアクセス Analyst ツールの場合: - Analyst へのアクセス - 検出ワークスペースへのアクセス	モデルリポジトリサービスが実行されるドメインまたはノード
ListServiceOptions	-	-	モデルリポジトリサービス
ListServiceProcessOptions	-	-	モデルリポジトリサービス
PopulateVCS	ドメイン管理	チームベース開発の管理	モデルリポジトリサービス
ReassignCheckedOutObject	ドメイン管理	チームベース開発の管理	モデルリポジトリサービス
RebuildDependencyGraph	-	-	モデルリポジトリサービス
RenameFolder	ドメイン管理	Developer tool の場合: - Developer へのアクセス Analyst ツールの場合: - Analyst へのアクセス - 検出ワークスペースへのアクセス	モデルリポジトリサービス
RestoreContents	ドメイン管理	サービス管理	モデルリポジトリサービスが実行されるドメインまたはノード
UndoCheckout	ドメイン管理	チームベース開発の管理	モデルリポジトリサービス
UnlockObject	ドメイン管理	チームベース開発の管理	モデルリポジトリサービス

infacmd mrs コマンド	特権グループ	特権名	権限
UpdateServiceOptions	ドメイン管理	サービス管理	モデルリポジトリサービス
UpdateServiceProcessOptions	ドメイン管理	サービス管理	モデルリポジトリサービス
UpgradeContents	モデルリポジトリサービス管理	サービス管理	モデルリポジトリサービス

infacmd ms コマンド

infacmd ms コマンドを実行するには、記載されているドメインオブジェクト権限のセットのいずれかを持っている必要があります。

以下の表に、*infacmd ms* コマンドに必要な特権と権限を一覧表示します。

infacmd ms コマンド	特権グループ	特権名	権限
GetRequestLog	-	-	-
ListMappings	-	-	-
ListMappingParams	-	-	-
RunMapping	-	-	マッピングで使用される接続オブジェクトに対する実行

infacmd oie コマンド

infacmd oie コマンドを実行するには、ユーザーは一覧表示されているモデルリポジトリオブジェクト権限の 1 つを持っている必要があります。

以下の表に、*infacmd oie* コマンドに必要な権限の一覧を示します。

infacmd oie コマンド	特権グループ	特権名	権限の対象
ExportObjects	-	-	プロジェクトの読み取り
ImportObjects	-	-	プロジェクトへの書き込み

infacmd ps コマンド

infacmd ps コマンドを実行するには、ユーザーは一覧表示されているプロファイリング特権およびドメインオブジェクト権限のセットの 1 つを持っていることが必要です。

以下の表に、*infacmd ps* コマンドに必要な特権と権限を一覧表示します。

infacmd ps **コマンド**	**特権グループ**	**特権名**	**権限の対象**
CreateWH	-	-	-
DropWH	-	-	-
実行	-	-	プロジェクトの読み取り ソース接続オブジェクトの実行
リスト	-	-	プロジェクトの読み取り
パージ	-	-	プロジェクトの読み取りおよび書き込み

infacmd ps **コマンド**	**特権グループ**	**特権名**	**権限の対象**
CreateWH	-	-	-
DropWH	-	-	-

infacmd pwx コマンド

infacmd pwx コマンドを実行するには、ユーザーは一覧表示されている PowerExchange アプリケーションの権限と特権のセットの 1 つを持っていることが必要です。

以下の表に、*infacmd pwx* コマンドに必要な特権と権限を一覧表示します。

infacmd pwx **コマンド**	**特権グループ**	**特権名**	**権限**
CloseForceListener	管理コマンド	closeforce	-
CloseListener	管理コマンド	閉じる	-
CondenseLogger	管理コマンド	圧縮	-
CreateListenerService	ドメイン管理	サービス管理	PowerExchange アプリケーションサービスを実行するドメインまたはノード

infacmd pwx コマンド	特権グループ	特権名	権限
CreateLoggerService	ドメイン管理	サービス管理	PowerExchange アプリケーションサービスを実行するドメインまたはノード
DisplayAllLogger	情報コマンド	displayall	-
DisplayCPULogger	情報コマンド	displaycpu	-
DisplayEventsLogger	情報コマンド	displayevents	-
DisplayMemoryLogger	情報コマンド	displaymemory	-
DisplayRecordsLogger	情報コマンド	displayrecords	-
DisplayStatusLogger	情報コマンド	displaystatus	-
FileSwitchLogger	管理コマンド	fileswitch	-
ListTaskListener	情報コマンド	listtask	-
ShutDownLogger	管理コマンド	shutdown	-
StopTaskListener	管理コマンド	stoptask	-
UpdateListenerService	ドメイン管理	サービス管理	PowerExchange アプリケーションサービスを実行するドメインまたはノード
UpdateLoggerService	ドメイン管理	サービス管理	PowerExchange アプリケーションサービスを実行するドメインまたはノード

infacmd rms コマンド

infacmd rms コマンドを実行するには、記載されているドメイン特権および権限のセットのいずれかを持っている必要があります。

次の表に、*infacmd rms* コマンドに必要な特権と権限を一覧表示します。

infacmd rms コマンド	特権グループ	特権名	権限
ListComputeNodeAttributes	ドメイン管理	-	リソースマネージャサービス
ListServiceOptions	ドメイン管理	-	リソースマネージャサービス

infacmd rms コマンド	特権グループ	特権名	権限
SetComputeNodeAttributes	ドメイン管理	サービスの管理	リソースマネージャサービス
UpdateServiceOptions	ドメイン管理	サービスの管理	リソースマネージャサービス

infacmd rtm コマンド

infacmd rtm コマンドを実行するには、ユーザーが一覧表示されているモデルリポジトリサービス特権およびドメインオブジェクト権限のセットの 1 つを持っている必要があります。

以下の表に、*infacmd rtm* コマンドに必要な特権と権限を一覧表示します。

infacmd rtm コマンド	特権グループ	特権名	権限の対象
Deployimport	-	-	-
Export	-	-	エクスポートされる参照テーブルを含むプロジェクトに対する読み取り
Import	-	-	参照テーブルがインポートされるプロジェクトに対する読み取りと書き込み

infacmd sch コマンド

infacmd sch コマンドを実行するには、記載されている特権および権限のセットのいずれかを持っている必要があります。

次の表に、infacmd sch コマンドに必要な特権と権限を一覧表示します。

infacmd sch コマンド	特権グループ	特権名	権限
CreateSchedule	スケジューラ特権	スケジュールの作成	スケジューラサービス
DeleteSchedule	スケジューラ特権	スケジュールの削除	スケジューラサービス
ListSchedule	スケジューラ特権	スケジュールの表示	スケジューラサービス
ListServiceOptions	ドメイン特権	サービスの管理	スケジューラサービス
ListServiceProcessOptions	ドメイン特権	サービスの管理	スケジューラサービス

infacmd sch コマンド	特権グループ	特権名	権限
PauseAll	スケジューラ特権	スケジュールの編集	スケジューラサービス
PauseSchedule	スケジューラ特権	スケジュールの編集	スケジューラサービス
ResumeAll	スケジューラ特権	スケジュールの編集	スケジューラサービス
ResumeSchedule	スケジューラ特権	スケジュールの編集	スケジューラサービス
UpdateSchedule	スケジューラ特権	スケジュールの編集	スケジューラサービス
UpdateService	ドメイン特権	サービスの管理	スケジューラサービス
UpdateServiceProcess	ドメイン特権	サービスの管理	スケジューラサービス
アップグレード	ドメイン特権	サービスの管理	スケジューラサービス

infacmd sql コマンド

infacmd sql コマンドを実行するには、ユーザーは一覧表示されているドメイン特権、データ統合サービス特権、ドメインオブジェクト権限のセットの 1 つを持っていることが必要です。

以下の表に、*infacmd sql* コマンドに必要な特権と権限を一覧表示します。

infacmd sql コマンド	特権グループ	特権名	権限の対象
ExecuteSQL	-	-	SQL 文にアクセスするオブジェクトに基づく
ListColumnPermissions	-	-	-
ListSQLDataServiceOptions	-	-	-
ListSQLDataServicePermissions	-	-	-
ListSQLDataServices	-	-	-
ListStoredProcedurePermissions	-	-	-
ListTableOptions	-	-	-
ListTablePermissions	-	-	-
PurgeTableCache	-	-	-
RefreshTableCache	-	-	-
RenameSQLDataService	アプリケーション管理	アプリケーションの管理	-

infacmd sql コマンド	特権グループ	特権名	権限の対象
SetColumnPermissions	-	-	オブジェクトに付与
SetSQLDataServicePermissions	-	-	オブジェクトに付与
SetStoredProcedurePermissions	-	-	オブジェクトに付与
SetTablePermissions	-	-	オブジェクトに付与
StartSQLDataService	アプリケーション管理	アプリケーションの管理	-
StopSQLDataService	アプリケーション管理	アプリケーションの管理	-
UpdateColumnOptions	アプリケーション管理	アプリケーションの管理	-
UpdateSQLDataServiceOptions	アプリケーション管理	アプリケーションの管理	-
UpdateTableOptions	アプリケーション管理	アプリケーションの管理	-

infacmd wfs コマンド

infacmd wfs コマンドを実行するには、特権や権限は必要ありません。

pmcmd コマンド

pmcmd コマンドを実行するには、ユーザーは一覧表示されている PowerCenter リポジトリサービス特権および PowerCenter リポジトリオブジェクト権限のセットが必要です。

PowerCenter 統合サービスがセーフモードで実行されている場合、ユーザーは次のコマンドを実行するために、関連する PowerCenter リポジトリサービスに対する管理者ロールが必要です。

- aborttask
- abortworkflow
- getrunningsessionsdetails
- getservicedetails
- getsessionstatistics
- gettaskdetails
- getworkflowdetails
- recoverworkflow

- scheduleworkflow
- starttask
- startworkflow
- stoptask
- stopworkflow
- unscheduleworkflow

以下の表に、*pmcmd* コマンドに必要な特権と権限を一覧表示します。

pmcmd **コマンド**	**特権グループ**	**特権名**	**権限**
aborttask（ユーザー自身のユーザーアカウントによって起動された場合）	-	-	フォルダに対する読み取りおよび実行
aborttask（他のユーザーによって起動された場合）	ランタイムオブジェクト	実行の管理	フォルダに対する読み取りおよび実行
abortworkflow（ユーザー自身のユーザーアカウントによって起動された場合）	-	-	フォルダに対する読み取りおよび実行
abortworkflow（他のユーザーによって起動された場合）	ランタイムオブジェクト	実行の管理	フォルダに対する読み取りおよび実行
connect	-	-	-
disconnect	-	-	-
exit	-	-	-
getrunningsessionsdetails	ランタイムオブジェクト	モニタ(M)	-
getservicedetails	ランタイムオブジェクト	モニタ(M)	フォルダに対する読み込み
getserviceproperties	-	-	-
getsessionstatistics	ランタイムオブジェクト	モニタ(M)	フォルダに対する読み込み
gettaskdetails	ランタイムオブジェクト	モニタ(M)	フォルダに対する読み込み
getworkflowdetails	ランタイムオブジェクト	モニタ(M)	フォルダに対する読み込み
ヘルプ	-	-	-
pingservice	-	-	-

pmcmd コマンド	特権グループ	特権名	権限
recoverworkflow（ユーザー自身のユーザーアカウントによって起動された場合）	ランタイムオブジェクト	実行	フォルダに対する読み取りおよび実行 接続オブジェクトに対する読み取りおよび実行 オペレーティングシステムプロファイルに対する権限（該当する場合）
recoverworkflow（他のユーザーによって起動された場合）	ランタイムオブジェクト	実行の管理	フォルダに対する読み取りおよび実行 接続オブジェクトに対する読み取りおよび実行 オペレーティングシステムプロファイルに対する権限（該当する場合）
scheduleworkflow	ランタイムオブジェクト	実行の管理	フォルダに対する読み取りおよび実行 接続オブジェクトに対する読み取りおよび実行 オペレーティングシステムプロファイルに対する権限（該当する場合）
setfolder	-	-	フォルダに対する読み込み
setnowait	-	-	-
setwait	-	-	-
showsettings	-	-	-
starttask	ランタイムオブジェクト	実行	フォルダに対する読み取りおよび実行 接続オブジェクトに対する読み取りおよび実行 オペレーティングシステムプロファイルに対する権限（該当する場合）
startworkflow	ランタイムオブジェクト	実行	フォルダに対する読み取りおよび実行 接続オブジェクトに対する読み取りおよび実行 オペレーティングシステムプロファイルに対する権限（該当する場合）
stoptask（ユーザー自身のユーザーアカウントによって起動された場合）	-	-	フォルダに対する読み取りおよび実行
stoptask（他のユーザーによって起動された場合）	ランタイムオブジェクト	実行の管理	フォルダに対する読み取りおよび実行

pmcmd コマンド	特権グループ	特権名	権限
stopworkflow（ユーザー自身のユーザーアカウントによって起動された場合）	-	-	フォルダに対する読み取りおよび実行
stopworkflow（他のユーザーによって起動された場合）	ランタイムオブジェクト	実行の管理	フォルダに対する読み取りおよび実行
unscheduleworkflow	ランタイムオブジェクト	実行の管理	フォルダに対する読み取りおよび実行
unsetfolder	-	-	フォルダに対する読み込み
version	-	-	-
waittask	ランタイムオブジェクト	モニタ(M)	フォルダに対する読み込み
waitworkflow	ランタイムオブジェクト	モニタ(M)	フォルダに対する読み込み

pmrep コマンド

ユーザーは以下のコマンド以外で、*pmrep* コマンドを実行するには、Repository Manager へのアクセス特権を有している必要があります。

- 実行
- 作成
- リストア
- アップグレード
- バージョン
- ヘルプ

pmrep コマンドを実行するには、ユーザーは一覧表示されているドメイン特権、PowerCenter リポジトリサービス特権、ドメインオブジェクト権限、および PowerCenter リポジトリオブジェクト権限のセットの 1 つが必要です。

ユーザーは、次のコマンドを実行するために、オブジェクトの所有者であるか、PowerCenter リポジトリサービスの管理者ロールが必要です。

- AssignPermission
- ChangeOwner
- deleteconnection
- deletedeploymentgroup
- deletefolder
- deletelabel

- ModifyFolder（所有者の変更、権限の設定、フォルダー共有化の指定、またはフォルダー名/説明の編集を行う場合）

以下の表に、*pmrep* コマンドに必要な特権と権限を一覧表示します。

pmrep **コマンド**	**特権グループ**	**特権名**	**権限**
AddToDeploymentGroup	グローバルオブジェクト	デプロイメントグループの管理	元のフォルダーに対する読み取り デプロイメントグループに対する読み取りおよび書き込み
ApplyLabel	-	-	フォルダーに対する読み取り ラベルに対する読み取りおよび実行
AssignPermission	-	-	-
BackUp	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスに対する権限
ChangeOwner	-	-	-
CheckIn（ユーザー自身のチェックアウト用）	デザインオブジェクト	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
CheckIn（ユーザー自身のチェックアウト用）	ソースおよびターゲット	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
CheckIn（ユーザー自身のチェックアウト用）	ランタイムオブジェクト	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
CheckIn（その他のユーザーのチェックアウト用）	デザインオブジェクト	バージョンの管理	フォルダーに対する読み取りおよび書き込み
CheckIn（その他のユーザーのチェックアウト用）	ソースおよびターゲット	バージョンの管理	フォルダーに対する読み取りおよび書き込み
CheckIn（その他のユーザーのチェックアウト用）	ランタイムオブジェクト	バージョンの管理	フォルダーに対する読み取りおよび書き込み
CleanUp	-	-	-
ClearDeploymentGroup	グローバルオブジェクト	デプロイメントグループの管理	デプロイメントグループに対する読み取りおよび書き込み
Connect	-	-	-
作成	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスに対する権限
CreateConnection	グローバルオブジェクト	接続の作成	-
CreateDeploymentGroup	グローバルオブジェクト	デプロイメントグループの管理	-

pmrep コマンド	特権グループ	特権名	権限
CreateFolder	フォルダー	作成	-
CreateLabel	グローバルオブジェクト	ラベルの作成	-
削除	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスに対する権限
deleteconnection	-	-	-
deletedeploymentgroup	-	-	-
deletefolder	-	-	-
deletelabel	-	-	-
DeleteObject	デザインオブジェクト	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
DeleteObject	ソースおよびターゲット	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
DeleteObject	ランタイムオブジェクト	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
DeployDeploymentGroup	グローバルオブジェクト	デプロイメントグループの管理	元のフォルダーに対する読み取り 宛先フォルダーに対する読み取りおよび書き込み デプロイメントグループに対する読み取りおよび実行
DeployFolder	フォルダー	元のリポジトリに対するコピー 宛先リポジトリに対する作成	フォルダーに対する読み取り
ExecuteQuery	-	-	クエリーに対する読み取りおよび実行
終了	-	-	-
FindCheckout	-	-	フォルダーに対する読み取り
GetConnectionDetails	-	-	接続オブジェクトに対する読み取り
ヘルプ	-	-	-
KillUserConnection	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスに対する権限
ListConnections	-	-	接続オブジェクトに対する読み取り

pmrep コマンド	特権グループ	特権名	権限
ListObjectDependencies	-	-	フォルダーに対する読み取り
ListObjects	-	-	フォルダーに対する読み取り
ListTablesBySess	-	-	フォルダーに対する読み取り
ListUserConnections	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスに対する権限
ModifyFolder（所有者の変更、権限の設定、フォルダー共有化の指定、またはフォルダー名/説明の編集を行う場合）	-	-	-
ModifyFolder（ステータスを変更する場合）	フォルダー	バージョンの管理	フォルダーに対する読み取りおよび書き込み
Notify	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスに対する権限
ObjectExport	-	-	フォルダーに対する読み取り
objectImport	デザインオブジェクト	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
objectImport	ソースおよびターゲット	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
objectImport	ランタイムオブジェクト	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
PurgeVersion	デザインオブジェクト	バージョンの管理	フォルダーに対する読み取りおよび書き込み クエリー名を指定した場合のクエリーに対する読み取り、書き込み、および実行
PurgeVersion	ソースおよびターゲット	バージョンの管理	フォルダーに対する読み取りおよび書き込み クエリー名を指定した場合のクエリーに対する読み取り、書き込み、および実行
PurgeVersion	ランタイムオブジェクト	バージョンの管理	フォルダーに対する読み取りおよび書き込み クエリー名を指定した場合のクエリーに対する読み取り、書き込み、および実行
PurgeVersion（フォルダーレベルでのオブジェクトのパージ）	フォルダー	バージョンの管理	フォルダーに対する読み取りおよび書き込み

pmrep コマンド	特権グループ	特権名	権限
PurgeVersion（リポジトリレベルでのオブジェクトのパージ）	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスに対する権限
登録	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスに対する権限
RegisterPlugin	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスに対する権限
リストア	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスに対する権限
RollbackDeployment	グローバルオブジェクト	デプロイメントグループの管理	宛先フォルダーに対する読み取りおよび書き込み
実行	-	-	-
ShowConnectionInfo	-	-	-
SwitchConnection	ランタイムオブジェクト	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み 接続オブジェクトに対する読み取り
TruncateLog	ランタイムオブジェクト	実行の管理	フォルダに対する読み取りおよび実行
UndoCheckout（ユーザー自身のチェックアウト用）	デザインオブジェクト	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
UndoCheckout（ユーザー自身のチェックアウト用）	ソースおよびターゲット	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
UndoCheckout（ユーザー自身のチェックアウト用）	ランタイムオブジェクト	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
UndoCheckout（その他のユーザーのチェックアウト用）	デザインオブジェクト	バージョンの管理	フォルダーに対する読み取りおよび書き込み
UndoCheckout（その他のユーザーのチェックアウト用）	ソースおよびターゲット	バージョンの管理	フォルダーに対する読み取りおよび書き込み
UndoCheckout（その他のユーザーのチェックアウト用）	ランタイムオブジェクト	バージョンの管理	フォルダーに対する読み取りおよび書き込み
登録解除	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスに対する権限

pmrep コマンド	特権グループ	特権名	権限
UnregisterPlugin	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスに対する権限
UpdateConnection	-	-	接続オブジェクトに対する読み取りおよび書き込み
UpdateEmailAddr	ランタイムオブジェクト	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
UpdateSeqGenVals	デザインオブジェクト	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
UpdateSrcPrefix	ランタイムオブジェクト	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
UpdateStatistics	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスに対する権限
UpdateTargPrefix	ランタイムオブジェクト	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
アップグレード	ドメイン管理	サービスの管理	PowerCenter リポジトリサービスに対する権限
Validate	デザインオブジェクト	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
Validate	ランタイムオブジェクト	作成、編集、および削除	フォルダーに対する読み取りおよび書き込み
バージョン	-	-	-

付録 B

カスタムロール

この付録では、以下の項目について説明します。

アナリストサービスのカスタムロール

アナリストサービスの Business Glossary Consumer は、カスタムのアナリストサービスロールです。

次の表に、アナリストサービスの Business Glossary Consumer ロールに割り当てられるデフォルトの特権の一覧を示します。

特権グループ	特権名
ワークスペースアクセス	用語集のワークスペース

Metadata Manager サービスのカスタムロール

Metadata Manager サービスのカスタムロールには、Metadata Manager 上級ユーザー、Metadata Manager 基本ユーザー、Metadata Manager 中級ユーザーがあります。

Metadata Manager の上級ユーザ

次の表に、Metadata Manager の上級ユーザーのカスタムロールに割り当てられるデフォルトの特権を一覧表示します。

特権グループ	特権名
カタログ	- ショートカットの共有 - リネージュの表示 - 関連カタログの表示 - レポートの表示 - プロファイル結果の表示 - カタログの表示 - リレーションの表示 - リレーションの管理 - コメントの表示 - コメントの転記 - コメントの削除 - リンクの表示 - リンクの管理 - 用語集の表示 - オブジェクトの管理
ロード	- リソースの表示 - リソースのロード - スケジュールの管理 - メタデータのパージ - リソースの管理
モデル	- モデルの表示 - モデルの管理 - モデルのエクスポート/インポート
セキュリティ	カタログ権限の管理

Metadata Manager の基本ユーザ

次の表に、Metadata Manager の基本ユーザーのカスタムロールに割り当てられるデフォルトの特権を一覧表示します。

特権グループ	特権名
カタログ	- リネージュの表示 - 関連カタログの表示 - カタログの表示 - リレーションの表示 - コメントの表示 - リンクの表示
モデル	モデルの表示

Metadata Manager の中級ユーザ

次の表に、Metadata Manager の中級ユーザーのカスタムロールに割り当てられるデフォルトの特権を一覧表示します。

特権グループ	特権名
カタログ	- リネージュの表示 - 関連カタログの表示 - レポートの表示 - プロファイル結果の表示 - カタログの表示 - リレーションの表示 - コメントの表示 - コメントの転記 - コメントの削除 - リンクの表示 - リンクの管理 - 用語集の表示
ロード	- リソースの表示 - リソースのロード
モデル	モデルの表示

オペレータカスタムロール

オペレータカスタムロールには、アプリケーションサービスの管理、スケジュール、および監視の特権が含まれています。

次の表に、オペレータカスタムロールに割り当てられるデフォルトの特権を一覧表示します。

特権グループ	特権名
アプリケーション管理	アプリケーションの管理
ドメイン管理	サービス実行の管理
モデルリポジトリサービス管理	チームベース開発の管理

特権グループ	特権名
監視	監視特権グループには、次の特権が含まれています。 - 表示: 他のユーザーのジョブの表示 - 表示: 統計の表示 - 表示: レポートの表示 - 監視へのアクセス: Analyst ツールからアクセス - 監視へのアクセス: Developer tool からアクセス - 監視へのアクセス: Administrator ツールからアクセス - ジョブに対するアクションの実行 **注:** Kerberos 認証を使用するドメインでは、ユーザーは監視のために設定されたモデルリポジトリサービスの管理者ロールも保持している必要があります。
スケジューラ	スケジューラ特権グループには次の特権が含まれています。 - スケジュール済みのジョブの管理: スケジュールの作成 - スケジュール済みのジョブの管理: スケジュールの削除 - スケジュール済みのジョブの管理: スケジュールの編集 - スケジュール済みのジョブの管理: スケジュールの表示
ツール	Informatica Administrator へのアクセス

PowerCenter リポジトリサービスのカスタムロール

PowerCenter リポジトリサービスのカスタムロールには、PowerCenter 接続管理者、PowerCenter 開発者、PowerCenter オペレータ、および PowerCenter リポジトリフォルダ管理者があります。

PowerCenter 接続管理者

次の表に、PowerCenter 接続管理者のカスタムロールに割り当てられるデフォルトの特権を一覧表示します。

特権グループ	特権名
ツール	Workflow Manager へのアクセス
グローバルオブジェクト	接続の作成

PowerCenter 開発者

次の表に、PowerCenter 開発者のカスタムロールに割り当てられるデフォルトの特権を一覧表示します。

特権グループ	特権名
ツール	- Designer へのアクセス - Workflow Manager へのアクセス - Workflow Monitor へのアクセス
デザインオブジェクト	- 作成、編集、および削除 - バージョンの管理

特権グループ	特権名
ソースおよびターゲット	- 作成、編集、および削除 - バージョンの管理
ランタイムオブジェクト	- 作成、編集、および削除 - 実行 - バージョンの管理 - モニタ(M)

PowerCenter オペレータ

次の表に、PowerCenter オペレータのカスタムロールに割り当てられるデフォルトの特権を一覧表示します。

特権グループ	特権名
ツール	Workflow Monitor へのアクセス
ランタイムオブジェクト	- 実行 - 実行の管理 - モニタ(M)

PowerCenter リポジトリフォルダ管理者

次の表に、PowerCenter リポジトリフォルダー管理者のカスタムロールに割り当てられるデフォルトの特権を一覧表示します。

特権グループ	特権名
ツール	Repository Manager へのアクセス
フォルダー	- コピー - 作成 - バージョンの管理
グローバルオブジェクト	- デプロイメントグループの管理 - デプロイメントグループの実行 - ラベルの作成 - クエリーの作成

Test Data Manager のカスタムロール

Test Data Manager のカスタムロールには、テストデータ管理者、テストデータ開発者、テストデータプロジェクト DBA、テストデータプロジェクト開発者、テストデータプロジェクト所有者、テストデータリスクマネージャ、テストデータ専門家、テストエンジニアなどがあります。

テストデータ管理者

以下の表に、テストデータ管理者のカスタムロールに割り当てられるデフォルトの特権の一覧を示します。

特権グループ	特権名
プロジェクト	プロジェクトの監査
管理	- 接続の表示 - 接続の管理 - 設定の管理

テストデータ開発者

以下の表に、テストデータ開発者のカスタムロールに割り当てられるデフォルトの特権の一覧を示します。

特権グループ	特権名
ポリシー	- ポリシーの表示 - ポリシーの管理
データドメイン	- データドメインの表示 - データドメインの管理
ルール	- マスキングルールの表示 - マスキングルールの管理 - 生成ルールの表示 - 生成ルールの管理
プロジェクト	プロジェクトの監査

テストデータプロジェクト DBA

以下の表に、テストデータプロジェクト DBA のカスタムロールに割り当てられるデフォルトの特権の一覧を示します。

特権グループ	特権名
プロジェクト	- プロジェクトの表示 - プロジェクトの実行 - プロジェクトの監視 - プロジェクトの監査
管理	- 接続の表示 - 接続の管理
データセット	- データセットの表示 - データセットのデータの表示。

テストデータプロジェクト開発者

以下の表に、テストデータプロジェクト開発者のカスタムロールに割り当てられるデフォルトの特権の一覧を示します。

特権グループ	特権名
ポリシー	ポリシーの表示
ルール	- マスキングルールの表示 - 生成ルールの表示 - 生成ルールの管理
データドメイン	データドメインの表示
プロジェクト	- プロジェクトの表示 - プロジェクトの検出 - プロジェクトの実行 - プロジェクトの監視 - プロジェクトの監査 - メタデータのインポート
データマスキング	- データマスキングの表示 - データマスキングの管理
データサブセット	- Data Subset の表示 - Data Subset の管理
データ生成	- データ生成の表示 - データ生成の管理
管理	- 接続の表示 - 接続の管理
データセット	- データセットの表示 - データセットのデータの表示

テストデータプロジェクト所有者

以下の表に、テストデータプロジェクト所有者のカスタムロールに割り当てられるデフォルトの特権の一覧を示します。

特権グループ	特権名
ポリシー	ポリシーの表示
ルール	- マスキングルールの表示 - 生成ルールの表示 - 生成ルールの管理
データドメイン	データドメインの表示

特権グループ	特権名
プロジェクト	- プロジェクトの表示 - プロジェクトの管理 - プロジェクトの検出 - プロジェクトの実行 - プロジェクトの監視 - プロジェクトの監査 - メタデータのインポート
データマスキング	- データマスキングの表示 - データマスキングの管理
データサブセット	- Data Subset の表示 - Data Subset の管理
データ生成	- データ生成の表示 - データ生成の管理
管理	- 接続の表示 - 接続の管理
データセット	- データセットの表示 - データセットのデータの表示 - データセットの管理 - データセットのデータの管理 - データセットのリセット

テストデータリスク管理者

以下の表に、テストデータリスクマネージャのカスタムロールに割り当てられるデフォルトの特権の一覧を示します。

特権グループ	特権名
ポリシー	ポリシーの表示
ルール	- マスキングルールの表示 - 生成ルールの表示
データドメイン	データドメインの表示
プロジェクト	プロジェクトの監査

テストデータ専門家

以下の表に、テストデータスペシャリストのカスタムロールに割り当てられるデフォルトの特権の一覧を示します。

特権グループ	特権名
ポリシー	ポリシーの表示
ルール	- マスキングルールの表示 - マスキングルールの管理 - 生成ルールの表示 - 生成ルールの管理
データドメイン	- データドメインの表示 - データドメインの管理
プロジェクト	- プロジェクトの表示 - プロジェクトの管理 - プロジェクトの検出 - プロジェクトの実行 - プロジェクトの監視 - プロジェクトの監査 - メタデータのインポート
データマスキング	- データマスキングの表示 - データマスキングの管理
データサブセット	- Data Subset の表示 - Data Subset の管理
データ生成	- データ生成の表示 - データ生成の管理
管理	- 接続の表示 - 接続の管理
データセット	- データセットの表示 - データセットのデータの表示 - データセットの管理 - データセットのデータの管理 - データセットのリセット

テストエンジニア

以下の表に、テストエンジニアのカスタムロールに割り当てられるデフォルトの特権の一覧を示します。

特権グループ	特権名
プロジェクト	- プロジェクトの表示 - プロジェクトの監視
データセット	- データセットの表示 - データセットの管理 - データセットのリセット - データセットのデータの表示 - データセットのデータの管理

付録 C

暗号スイートのデフォルトリスト

Informatica ドメインでは、ドメイン内の安全な通信および安全なクライアント接続のためにデフォルトで次の暗号スイートを使用します。

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256

索引

N

O

P

R

S

T

U

W

あ

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

な

に

ね

の

は

ふ

ま

も

ゆ

ら

ろ

わ