Red Hat Enterprise Linux 7

Windows 統合ガイド

Active Directory 環境との Linux システムの統合

Last Updated: 2023-04-05

Red Hat Enterprise Linux 7 Windows 統合ガイド

Active Directory 環境との Linux システムの統合

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

概要

多くの場合、異種 IT 環境には、シームレスに通信するのに必要なさまざまなドメインやオペレーティングシステムが含まれます。Red Hat Enterprise Linux は、Microsoft Windows で Active Directory (AD) と Linux ドメインを密接に統合する複数の方法を提供します。統合は、ユーザー、グループ、サービス、またはシステムが含まれる異なるドメインオブジェクトで可能です。本ガイドでは、軽量 AD パススルー認証から本格的な Kerberos の信頼できるレルムまで、さまざまな統合シナリオも説明します。 本ガイドに加えて、Red Hat Enterprise Linux Identity Management に関するその他の機能およびサービスについては、以下のガイドを参照してください。 Linux ドメイン ID、認証、およびポリシーガイド には、Linux ベースのドメインで ID ストアと認証および承認

ポリシーを管理する集中化され統一された方法を提供するソリューションである Red Hat Identity Management が記載されています。 システムレベルの認証ガイド では、authconfig ユーティリティー、System Security Services Daemon (SSSD) サービス、Pluggable Authentication Module(PAM) フレームワーク、Kerberos、certmonger ユーティリティー、およびアプリケーションのシングルサインオン (SSO) など、ローカルシステムにおける認証の設定に使用できるアプリケーションおよびサービスについて説明します。

目次

第1章 ACTIVE DIRECTORY と LINUX 環境を統合する方法

IT 環境には構造があります。環境内のシステムは、目的に合わせて設定されます。2 つの別個のインフラストラクチャーを統合するには、これらの環境の目的を評価し、どのように対話するかを理解する必要があります。

1.1. WINDOWS 統合の定義

Windows 統合は、Linux 環境と Windows 環境の必要な対話によって、非常に異なることが必要になる場合があります。これは、個別の Linux システムが Windows ドメインに登録されている場合は、Linux ドメインが Windows ドメインへのピアとして設定されていて、単に情報が環境間でコピーされることを意味します。

Windows ドメインと Linux システム間の通信には、いくつかの接点があります。それぞれは、異なるドメインオブジェクト (ユーザー、グループ、システム、サービス) を特定することと、その ID で使用されるサービスを特定します。

ユーザー ID および認証

- ユーザーアカウントの場所: Windows (AD ドメイン) で実行している中央認証システムまたは Linux で実行している中央 ID および認証サーバー
- Linux システムで認証する方法: ローカルの Linux 認証システムまたは Windows で実行している中央認証システム経由
- グループメンバーシップはユーザーに対してどのように設定されていますか。そのグループメンバーシップはどのように決定されますか。
- ユーザーは、ユーザー名/パスワードのペア、Kerberos チケット、証明書、またはメソッドの組み合わせを使用して認証しますか。
- Linux マシンのサービスにアクセスするには、POSIX 属性が必要です。これらの属性の保存方法: Windows ドメインに設定、Linux システムにローカルに設定、または動的にマップされますか (UID/GID 番号および Windows SID の場合)。
- どのユーザーにどのリソースにアクセスしますか。Windows が定義するユーザーは Linux リソースにアクセスしますか。Linux 定義のユーザーは Windows リソースにアクセスしますか。

ほとんどの環境では、Active Directory ドメインはユーザー情報の中心となるハブです。つまり、Linux システムが認証要求のためにそのユーザー情報にアクセスするために何らかの方法が必要になります。ユーザー情報を取得する 方法 と、外部システムで利用できる情報の量が実際の質問になります。また、Linux システム (POSIX 属性) および Linux ユーザー (アプリケーション管理者) の情報と、その情報の管理方法のバランスを取る必要があります。

ホストおよびサービスプリンシパル

- アクセスするリソース
- 必要な認証プロトコル
- Kerberos チケットの取得方法SSL 証明書をリクエストまたは検証する方法
- ユーザーは 1 つのドメイン、または Linux ドメインと Windows ドメインの両方にアクセスする必要があるか

DNS ドメイン、クエリー、および名前解決

- DNS 設定の対象
- DNS ドメインが 1 つ必要ですか。サブドメインは存在しますか。
- システムのホスト名が解決される方法
- サービス検出の設定方法

セキュリティーポリシー

- アクセス制御命令はどこに設定されているか
- 各ドメインにどの管理者が設定されているか

管理の変更

- システムがドメインに追加される頻度
- たとえば、Windows 統合に関連する基礎となる設定が変更された (DNS サービスなど) 場合に、これらの変更が伝播される方法
- ドメイン関連のツールやプロビジョニングシステムで維持される設定
- 統合パスには Windows サーバーで追加のアプリケーションまたは設定が必要か

ドメインのどの要素が統合されているかと同様に、統合が維持されるかは重要となります。特定の統合機器で行う手動設定が非常に多いにもかかわらず、環境に頻繁に更新されるシステムが多数ある場合は、その 1 つの機器は、メンテナーンスの観点からその環境では機能しない可能性があります。

以下のセクションでは、Windows と統合するための主なシナリオの概要を説明します。直接統合では、Linux システムは、追加の中間なしで Active Directory に接続されます。一方、間接統合には、Linux システムを一元管理し、環境全体をサーバー間レベルの Active Directory に接続する ID サーバーが含まれます。

1.2. 直接的な統合

Linux システムを Active Directory (AD) に接続するには、2 つのコンポーネントが必要です。1 つのコンポーネントは中央の ID および認証ソースと対話します。この場合は AD です。他のコンポーネントは利用可能なドメインを検出し、最初のコンポーネントが適切な ID ソースに対応するように設定します。情報を取得したり、AD に対して認証を実行するのに使用するオプションを使用できます。以下の特徴があります。

ネイティブ **LDAP**、**Kerberos PAM**、および **NSS** モジュール

これらのモジュールには、**nss_ldap**、**pam_ldap**、および **pam_krb5** があります。PAM モジュールおよび NSS モジュールはすべてのアプリケーションプロセスに読み込まれるため、実行環境に直接影響を及ぼします。キャッシュやオフラインサポート、またはアクセス認証情報の保護が十分でない場合、NSS および PAM に基本的な LDAP モジュールおよび Kerberos モジュールの使用は、一部の機能により推奨されません。

Samba Winbind

Samba Winbind は、Linux システムを AD に接続する従来の方法でした。winbind は、Linux システムで Windows クライアントをエミュレートし、AD サーバーと通信できます。

以下の点に留意してください。

- Samba をドメインメンバーとして設定する場合は、Winbind サービスが実行している必要があります。
- マルチフォレストの AD 設定における Winbind との直接統合は、双方向の信頼が必要になります。
- **idmap_ad** プラグインがリモートフォレストユーザーを正常に処理するには、リモートフォレストがローカルフォレストを信頼する必要があります。

System Security Services Daemon (SSSD)

SSSD の主な機能は、システムにキャッシュおよびオフラインサポートを提供する共通のフレームワークを介してリモートアイデンティティーおよび認証リソースにアクセスすることです。SSSD は高度な設定が可能で、ローカルユーザーを保存する PAM および NSS 統合およびデータベースと、中央サーバーから取得したコアユーザーおよび拡張ユーザーのデータを提供します。SSSD は、Linux システムを任意の ID サーバーに接続するのに推奨されるコンポーネントです。Red Hat Enterprise Linux の Active Directory、Identity Management (IdM)、または汎用の LDAP または Kerberos サーバーです。

以下の点に留意してください。

- SSSD との直接統合は、デフォルトで 1 つの AD フォレスト内でのみ機能します。
- **idmap_ad** プラグインがリモートフォレストユーザーを正常に処理するには、リモートフォレストがローカルフォレストを信頼する必要があります。

Winbind から SSSD への移行の主な理由は、SSSD を直接統合と間接統合の両方に使用することができるという主な理由は、移行コストが大きくならず、ある統合アプローチから別の別のアプローチに切り替えることを可能にすることです。Linux システムを AD に直接統合するために、SSSD または Winbind を設定する最も便利な方法は、**realmd** サービスを使用することです。これにより、呼び出し元はネットワーク認証およびドメインメンバーシップを標準的な方法で設定できます。**realmd** サービスは、アクセス可能なドメインおよびレルムに関する情報を自動的に検出し、ドメインまたはレルムに参加するのに高度な設定を必要としません。

直接統合は、Linux システムを AD 環境に導入する簡単な方法です。ただし、Linux システムの共有が増えると、デプロイメントは通常、ホストベースのアクセス制御、sudo、SELinux ユーザーマッピングなどの ID 関連のポリシーをより集中管理する必要性を確認します。はじめに、Linux システムのこのような側面の設定は、ローカル設定ファイルで維持できます。ただし、システムの数が増えると、Red Hat Satellite などのプロビジョニングシステムでは、設定ファイルの配布と管理が簡単になります。この方法では、設定ファイルを変更して、配布するオーバーヘッドを作成します。直接統合がスケーリングされない場合は、次のセクションで説明する間接統合を検討するより有益です。

1.2.1. 直接統合でサポートされる Windows プラットフォーム

Linux マシンと、以下のフォレストおよびドメインの機能レベルを使用する Active Directory フォレストを直接統合できます。

- フォレスト機能レベルの範囲 - Windows Server 2008 ~ Windows Server 2016[1]
- ドメイン機能レベルの範囲: Windows Server 2008 - Windows Server 2016[1]

直接統合は、上記の機能レベルを使用して、以下のサポート対象のオペレーティングシステムでテストされています。

- Windows Server 2019

- Windows Server 2016
- Windows Server 2012 R2

1.3. 間接的な統合

間接統合の主な利点は、Active Directory (AD) ドメインのユーザーが透過的に Linux システムおよびサービスにアクセスできるようにする一方で、そのシステムに関連する Linux システムおよびポリシーを管理することです。間接統合には、以下の 2 つの方法があります。

信頼ベースのソリューション

推奨のアプローチとして、Red Hat Enterprise Linux で Identity Management (IdM) を中央サーバーとして利用して Linux システムを制御し、AD でレルム間の Kerberos 信頼を確立し、AD からユーザーがログオンしてシングルサインオンを使用して、Linux システムおよびリソースにアクセスするのが推奨される方法です。このソリューションでは、Kerberos 機能を使用して、異なる ID ソース間で信頼関係を確立します。IdM は、それ自体を別のフォレストとして AD に提示し、AD で対応しているフォレストレベルの信頼を利用します。

複雑な環境では、1 つの IdM フォレストを、複数の AD フォレストに接続できます。この設定により、組織のさまざまな機能の作業を、より適切に分離できます。Linux 管理者は Linux インフラストラクチャーを完全に制御できますが、AD 管理者はユーザーと、ユーザーに関連するポリシーに集中できます。このような場合、IdM が制御する Linux レルムは、AD リソースドメインまたはレルムに似ていますが、Linux システムが含まれています。

注記

Windows では、すべてのドメインが Kerberos レルムと DNS ドメインを同時に設定します。ドメインコントローラーが管理するすべてのドメインには、独自の専用 DNS ゾーンが必要です。IdM がフォレストとして AD に信頼される場合も同様です。AD は、IdM に独自の DNS ドメインがあることを想定します。信頼の設定を機能させるには、DNS ドメインを Linux 環境専用にする必要があります。

信頼環境では、IdM は *ID ビュー* を使用して、IdM サーバーの AD ユーザーの POSIX 属性を設定できることに注意してください。詳細は、次を参照してください。

- *8章Active Directory 環境での ID ビューの使用*
- 『システムレベルの認証ガイド』 の SSSD クライアント側のビュー

同期ベースのソリューション

信頼ベースのソリューションの代わりとして、IdM または Red Hat Directory Server (RHDS) で使用可能なユーザー同期機能を利用することです。これにより、ユーザーアカウント (および RHDS ではグループアカウントも) を AD から IdM または RHDS と同期できますが、逆方向にはなりません。ユーザー同期には、以下を含む特定の制限があります。

- ユーザーの重複
- AD ドメインのすべてのドメインコントローラーに特別なコンポーネントが必要なパスワードを同期する必要があります。
- パスワードを取得できるようにするには、まずユーザーを手動で変更する必要があります。
- 同期が 1 つのドメインのみに対応

- IdM 、または RHDS の 1 つのインスタンスへのデータ同期には、AD のドメインコントローラーを 1 つだけ使用できます。

統合のシナリオでは、ユーザー同期が唯一の利用可能なオプションである場合もありますが、一般的には同期アプローチの使用は推奨されず、レルム間の信頼ベースの統合が優先されます。

---

[1] Windows Server 2019 では、新しい機能レベルが導入されていません。Windows Server 2019 が使用する機能レベルで最も高いものは Windows Server 2016 です。

パート I. ACTIVE DIRECTORY ドメインへの LINUX システムを 1 つ追加

このパートでは、System Security Services Daemon (**SSSD**) が Active Directory (**AD**) ドメインと連携する方法、**realmd** システムを使用して直接ドメイン統合を実現する方法、最後に **AD** 統合に **Samba** を使用する方法について説明します。

第2章 ACTIVE DIRECTORY を SSSD のアイデンティティープロバイダーとして使用

システムセキュリティーサービスデーモン (System Security Services Daemon: SSSD) は、リモートディレクトリーと認証メカニズムにアクセスするシステムサービスです。ローカルシステム (SSSD *クライアント*) を外部のバックエンドシステム (*ドメイン*) に接続します。これにより、SSSD クライアントに SSSD プロバイダーを使用した ID および認証のリモートサービスへのアクセスが提供されます。たとえば、これらのリモートサービスには、LDAP ディレクトリー、Identity Management (IdM) または Active Directory (AD) ドメイン、または Kerberos レルムが含まれます。

AD 統合のアイデンティティー管理サービスとして使用すると、SSSD は NIS や Winbind などのサービスの代わりに使用することができます。本章では、SSSD が AD でどのように機能するかを説明します。SSSD の詳細は、『システムレベルの認証ガイド』 を参照してください。

2.1. AD プロバイダーが信頼されるドメインを処理する方法

本セクションでは、**/etc/sssd/sssd.conf** ファイルで **id_provider = ad** を設定すると、SSSD が信頼されるドメインを処理する方法を説明します。

- SSSD は、1 つの Active Directory フォレストのドメインのみをサポートします。SSSD が複数のフォレストから複数のドメインにアクセスする必要がある場合は、SSSD の代わりに信頼 (推奨) または **winbindd** サービスで IdM を使用することを検討してください。
- デフォルトでは、SSSD はフォレスト内のすべてのドメインを検出し、信頼されるドメイン内のオブジェクトの要求が到達すると、SSSD はこれを解決しようとします。

  信頼できるドメインに到達できない、または地理的に離れているために遅くなる場合は、**/etc/sssd/sssd.conf** に ***ad_enabled_domains*** パラメーターを設定して、どの信頼ドメインから SSSD がオブジェクトを解決するかを制限できます。
- デフォルトでは、完全修飾ユーザー名を使用して信頼されるドメインのユーザーを解決する必要があります。

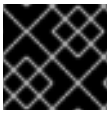
2.2. SSSD 向けの AD プロバイダーの設定

AD プロバイダーにより、SSSD は AD 環境の最適化を使用して LDAP アイデンティティープロバイダーと Kerberos 認証プロバイダーを使用できます。

2.2.1. 統合オプションの概要

Linux システムおよび Windows システムは、ユーザーおよびグループに異なる識別子を使用します。

- Linux では、*ユーザー ID* (UID) と *グループ ID* (GID) が使用されます。『システム管理者ガイド』 の ユーザーおよびグループの管理 を参照してください。Linux の UID および GID は、POSIX 標準に準拠します。
- Windows は、*セキュリティー ID* (SID) を使用します。



重要

Windows と Active Directory で同じユーザー名を使用しないでください。

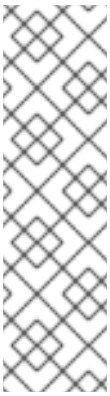
AD ユーザーなど、Red Hat Enterprise Linux システムに対して認証を行うユーザーに UID と GID が割り当てられている必要があります。このため、SSSD は以下の統合オプションを提供します。

AD ユーザー用に新規 UID および GID を自動的に生成

SSSD は、AD ユーザーの SID を使用して、*ID マッピング* と呼ばれるプロセスにおいてアルゴリズムで POSIX ID を生成できます。ID マッピングは、AD の SID と Linux の ID との間にマップを作成します。

- SSSD が新しい AD ドメインを検出すると、利用可能な ID の範囲を新しいドメインに割り当てます。したがって、各 AD ドメインは、すべての SSSD クライアントマシンで同じ ID 範囲を持ちます。
- AD ユーザーが SSSD クライアントマシンに初めてログインすると、SSSD は、ユーザーの SID およびそのドメインの ID 範囲を基にした UID など、SSSD キャッシュにユーザーのエントリーを作成します。
- AD ユーザーの ID は、同じ SID から一貫した方法で生成されるため、Red Hat Enterprise Linux システムにログインする場合は、そのユーザーに同じ UID と GID が使用されます。

「SSSD のプロバイダーとして ID マッピングを使用した AD ドメインの設定」 を参照してください。



注記

全クライアントシステムが SSSD を使用して SID を Linux ID にマッピングすると、マッピングは一貫性を維持します。一部のクライアントが別のソフトウェアを使用する場合は、以下のいずれかを選択します。

- すべてのクライアントで同じマッピングアルゴリズムが使用されていることを確認します。
- AD で定義されている POSIX 属性の使用 で説明されているように、明示的な POSIX 属性を使用します。

AD で定義されている POSIX 属性の使用

AD は、***uidNumber***、***gidNumber***、***unixHomeDirectory***、***loginShell*** などの POSIX 属性を作成して保存できます。

AD ユーザー用に新規 UID および GID を自動的に生成 で説明した ID マッピングを使用すると、SSSD は新しい UID と GID を作成し、AD で定義された値を上書きします。AD 定義の値を維持するには、SSSD で ID マッピングを無効にする必要があります。

「AD で定義された POSIX 属性を定義するように SSSD の設定」 を参照してください。

2.2.2. SSSD のプロバイダーとして ID マッピングを使用した AD ドメインの設定

前提条件

AD システムと Linux システムの両方が適切に設定されていることを確認します。

- 名前解決の設定を確認します。特に、DNS SRV レコードを確認します。たとえば、**ad.example.com** ドメインの場合は、次のコマンドを実行します。
  - DNS SRV LDAP レコードを確認するには、次のコマンドを実行します。

```
# dig -t SRV _ldap._tcp.ad.example.com
```

- AD レコードを確認するには、次のコマンドを実行します。

```
# dig -t SRV _ldap._tcp.dc._msdcs.ad.example.com
```

後で SSSD を特定の AD ドメインコントローラーに接続する場合は、DNS SRV レコードを検証する必要はありません。

- 両方のシステムのシステム時刻が同期していることを確認します。これにより、Kerberos が正常に機能できるようになります。
- AD ドメインコントローラーの以下のポートが開いており、RHEL ホストからアクセス可能であることを確認します。

表2.1 SSSD を使用した Linux システムの AD への直接統合に必要なポート

サービス	ポート	プロトコル	備考
DNS	53	UDP および TCP	
LDAP	389	UDP および TCP	
Kerberos	88	UDP および TCP	
Kerberos	464	UDP および TCP	パスワードを設定または変更するために、kadmin により使用されます。
LDAP グローバルカタログ	3268	TCP	**id_provider = ad** オプションが使用されている場合
NTP	123	UDP	オプション
Samba	445	UDP および TCP	AD グループポリシーオブジェクト (GPO) の場合

ローカルシステムの設定

Red Hat は、**realm join** コマンドを使用してシステムを設定することを推奨します。3章*realmd を使用した Active Directory ドメインへの接続* を参照してください。**realmd** スイートは、必要な設定ファイルをすべて自動的に編集します。以下に例を示します。

```
# realm join ad.example.com
```

realmd を使用しない場合は、システムを手動で設定できます。Red Hat ナレッジベースの Manually Connecting an SSSD Client to an Active Directory Domainを参照してください。

オプション: ユーザーホームディレクトリーおよびシェルの設定

pam_oddjob_mkhomedir.so ライブラリーは、ユーザーが Linux システムを最初にログインする際にホームディレクトリーを自動的に作成します。デフォルトでは、SSSD は AD アイデンティティープロバイダーからホームディレクトリーの形式を取得します。Linux クライアントのディレクトリー形式をカスタマイズするには、以下を実行します。

1. **/etc/sssd/sssd.conf** ファイルを開きます。
2. **[domain]** セクションで、以下のいずれかのオプションを使用します。
   - ***fallback_homedir*** は、ホームディレクトリーが AD で定義されていない場合のみ使用されるフォールバックホームディレクトリー形式を設定します。
   - ***override_homedir*** は、AD で定義されたホームディレクトリーを常に上書きするホームディレクトリーテンプレートを設定します。

   たとえば、常に **/home/*domain_name*/*user_name*** の形式を使用する場合は、次を使用します。

   ```
   [domain/EXAMPLE]
   [... file truncated ...]
   override_homedir = /home/%d/%u
   ```

   詳細は sssd.conf(5) の man ページを参照してください。

デフォルトでは、SSSD は AD で設定された ***loginShell*** パラメーターからユーザーシェルの情報を取得します。Linux クライアントでユーザーシェル設定をカスタマイズするには、以下を実行します。

1. **/etc/sssd/sssd.conf** ファイルを開きます。
2. 次のオプションを使用して、必要なユーザーシェル設定を定義します。
   - ***shell_fallback*** はフォールバック値を設定します。これは、AD でシェルが定義されていない場合にのみ使用されます。
   - ***override_shell*** は、AD で定義されたシェルを常にオーバーライドする値を設定します
   - ***default_shell*** はデフォルトのシェル値を設定します
   - ***allowed_shells*** および ***vetoed_shells*** は、許可されたシェルまたはブラックリストに登録されたシェルのリストを設定します

   詳細は sssd.conf(5) の man ページを参照してください。

新しい設定を読み込みします。

- 設定ファイルの変更後に SSSD を再起動します。

  ```
  # systemctl restart sssd.service
  ```

関連情報

- LDAP および Kerberos プロバイダーのその他の設定オプションについては、sssd-ldap(5) および sssd-krb5(5) の man ページを参照してください。
- AD プロバイダーのその他の設定オプションは、sssd-ad(5) の man ページを参照してください。

2.2.3. AD で定義された POSIX 属性を定義するように SSSD の設定

注記

以前は、*UNIX 拡張機能の Identity Management* を使用して、ユーザーアカウントに POSIX 属性を提供できました。拡張機能は非推奨になりました。詳細は、Microsoft Developer Network を参照してください。

UNIX 向けの Identity Management を使用している場合は、こちらのナレッジベースの記事 で、よくある質問への回答について参照してください。

Unix および *Services for Unix* パッケージの Identity Management を参照する以前の手順は、以下の Red Hat ナレッジベース記事を参照してください。

- Configuring an Active Directory Domain with POSIX Attributes
- Configuring Active Directory as an LDAP Domain

推奨事項
最適なパフォーマンスを得るには、POSIX 属性を AD グローバルカタログに公開します。POSIX 属性がグローバルカタログにない場合、SSSD は LDAP ポート上の個々のドメインコントローラーに直接接続します。

Linux システムの AD ドメインへの参加
「SSSD のプロバイダーとして ID マッピングを使用した AD ドメインの設定」 に記載の手順を行います。

SSSD で ID マッピングを無効化

1. **/etc/sssd/sssd.conf** ファイルを開きます。
2. AD ドメインセクションで、***ldap_id_mapping = false*** 設定を追加します。

注記

realm ユーティリティーを使用してドメインに参加し、**--automatic-id-mapping=no** スイッチを追加すると、**realm** ユーティリティーが **ldap_id_mapping = false** で SSSD を設定しています。

3. デフォルト ID マッピング設定を持つユーザーを要求する場合は、SSSD キャッシュを削除します。

```
rm -f /var/lib/sss/db/*
```

SSSD は、ローカルで作成するのではなく、AD の POSIX 属性を使用するようになりました。

関連情報
ID マッピングと ***ldap_id_mapping*** パラメーターの詳細は、sssd-ldap(8)man ページを参照してください。

2.3. KERBEROS ホストの自動キータブの更新

SSSD は、adcli パッケージがインストールされていると、AD 環境で Kerberos ホストキータブファイルを自動的に更新します。デーモンは、マシンアカウントのパスワードが設定されている値よりも古いかどうかを毎日確認し、必要に応じてそのパスワードを更新します。

デフォルトの更新間隔は 30 日です。デフォルトを変更するには、以下を行います。

1. 以下のパラメーターを **/etc/sssd/sssd.conf** ファイルの AD プロバイダーに追加します。

```
ad_maximum_machine_account_password_age = value_in_days
```

2. SSSD を再起動します。

```
# systemctl restart sssd
```

Kerberos ホストのキータブの自動更新を無効にするには、***ad_maximum_machine_account_password_age = 0*** を設定します。

2.4. ダイナミック DNS 更新の有効化

AD により、クライアントは DNS レコードを自動的に更新できます。AD はまた、DNS レコードをアクティブに維持して、非アクティブなレコードのタイムアウト (エージング) や削除 (スカベンジング) など、DNS レコードが更新されていることを確認します。DNS スカベンジングは、AD 側ではデフォルトで有効になっていません。

SSSD により、Linux システムは DNS レコードを更新して Windows クライアントを省略できます。これにより、レコードに非アクティブとしてマークされ、DNS レコードから削除されるのを防ぐこともできます。動的 DNS 更新を有効にすると、クライアントの DNS レコードが更新されます。

- アイデンティティープロバイダーがオンラインになる (常に)
- Linux システムの再起動時 (常に)
- 指定した間隔 (任意の設定) では、デフォルトで、AD プロバイダーは 24 時間ごとに DNS レコードを更新します。

  この動作は、DHCP リースと同じ間隔に設定できます。この場合、Linux クライアントはリースの更新後に更新されます。

DNS 更新は、Kerberos/GSSAPI for DNS (GSS-TSIG) を使用して AD サーバーに送信されます。これは、セキュアな接続のみを有効にする必要があります。

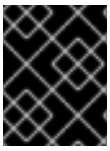
動的 DNS 設定は、各ドメインに設定されます。以下に例を示します。

```
[domain/ad.example.com]
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad

ldap_schema = ad

dyndns_update = true
dyndns_refresh_interval = 43200
dyndns_update_ptr = true
dyndns_ttl = 3600
```

これらのオプションの詳細は、sssd-ad(5) の man ページを参照してください。

2.5. SSSD での RANGE RETRIEVAL SEARCH の使用

SSSD は、AD の *範囲検索を使用した検索* 機能をサポートします。範囲検索の詳細は、Microsoft Developer Network を参照してください。



重要

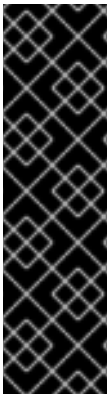
グループまたは検索ベースでカスタムフィルターを設定すると、フィルターは非常に大きなグループでは機能しない可能性があります。

2.6. グループポリシーオブジェクトアクセス制御

グループポリシーは Microsoft Windows の機能の 1 つで、Active Directory (AD) 環境におけるユーザーおよびコンピューターのポリシーを管理者が 1 か所で管理できるようにします。*グループポリシーオブジェクト* (GPO) は、ドメインコントローラー (DC) に保存されているポリシー設定の集合で、コンピューターやユーザーなどのポリシーターゲットに適用できます。AD 環境におけるコンピューターベースのアクセス制御の管理には、Windows *ログオン権限* に関連する GPO ポリシー設定が一般的に使用されます。

2.6.1. GPO アクセス制御を使用した SSSD の仕組み

GPO アクセス制御を適用するように SSSD を設定すると、SSSD はホストシステムおよび AD ユーザーに適用される GPO を取得します。SSSD は、取得した GPO 設定に基づいて、ユーザーが特定のホストにログインできるかどうかを判断します。これにより、管理者は、Linux および Windows クライアントの両方が AD ドメインコントローラーに集中的に有効にするログインポリシーを定義できます。



重要

セキュリティーフィルターリングは、セキュリティーフィルターにリストすることで GPO アクセス制御のスコープを特定のユーザー、グループ、またはホストに制限できる機能です。ただし、SSSD は、セキュリティーフィルター内のユーザーおよびグループのみをサポートします。SSSD は、セキュリティーフィルター内のホストエントリーを無視します。

SSSD が GPO アクセス制御を特定のシステムに適用するようにするには、AD ドメインで新しい OU を作成し、システムを OU に移動してから GPO をこの OU にリンクします。

2.6.2. SSSD がサポートする GPO 設定

表2.2 SSSD が取得した GPO アクセス制御オプション

GPO オプション [a]	対応する sssd.conf オプション [b]
ローカルでのログオンの許可 ローカルでのログオン拒否	***ad_gpo_map_interactive***
リモートデスクトップサービスを介したログオンの許可 リモートデスクトップサービスを介したログオンの拒否	***ad_gpo_map_remote_interactive***

GPO オプション [a]	対応する sssd.conf オプション [b]
ネットワークからこのコンピューターへのアクセス ネットワークからこのコンピューターへのアクセスを拒否	***ad_gpo_map_network***
バッチジョブとしてのログオンの許可 バッチジョブとしてのログオンの拒否	***ad_gpo_map_batch***
サービスとしてのログオンの許可 サービスとしてのログオンの拒否	***ad_gpo_map_service***

[a] Windows の Group Policy Management Editor に指定されているとおりです。

[b] このオプションの詳細と、GPO オプションがデフォルトでマッピングされるプラグ可能な認証モジュール (PAM) サービスの一覧は、sssd-ad(5) の man ページを参照してください。

2.6.3. SSSD の GPO ベースのアクセス制御の設定

GPO ベースのアクセス制御は **/etc/sssd/sssd.conf** ファイルで設定できます。***ad_gpo_access_control*** オプションは、GPO ベースのアクセス制御を実行するモードを指定します。以下の値を使用できます。

ad_gpo_access_control = permissive

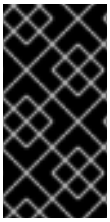
permissive の場合は、GPO ベースのアクセス制御は評価されますが、強制されません。**syslog** メッセージは、アクセスが拒否される度に復元されます。これはデフォルト設定です。

ad_gpo_access_control = enforcing

enforcing の場合は、GPO ベースのアクセス制御は評価され、強制されます。

ad_gpo_access_control = disabled

disabled の場合は、GPO ベースのアクセス制御は評価も強制もされません。



重要

GPO ベースのアクセス制御の使用を開始し、***ad_gpo_access_control*** を強制モードに設定する前に、***ad_gpo_access_control*** が許可モードに設定されていることを確認し、ログを調べることをお勧めします。**syslog** メッセージを見直すことで現行の GPO 設定をテスト、調節してからその後で enforcing モードに設定することができます。

GPO ベースのアクセス制御に関連する以下のパラメーターも **sssd.conf** ファイルで指定することができます。

- ***ad_gpo_map_**** オプションと ***ad_gpo_default_right*** オプションは、どの PAM サービスが特定の Windows ログオン権限にマップされるかを設定します。

  PAM サービスを、特定の GPO 設定にマッピングされた PAM サービスのデフォルトリストに追加するか、一覧からサービスを削除するには、**ad_gpo_map_*** オプションを使用します。たとえば、インタラクティブなログインにマッピングされた PAM サービスの一覧から **su** サービ

スを削除する (GPO 設定のローカルでのログオンの許可、およびローカルでのログオンの拒否) には、以下を行います。

```
ad_gpo_map_interactive = -su
```

- ***ad_gpo_cache_timeout*** オプションは、後続のアクセス制御要求が DC から新たにファイルを取得するのではなく、キャッシュに保存されたファイルを再利用できる間隔を指定します。

使用できる GPO パラメーターの詳細なリストと、その説明およびデフォルト値は、sssd-ad(5) の man ページを参照してください。

2.6.4. 関連情報

- GPO と連携する SSSD の設定に関する詳細は、Red Hat ナレッジベースのConfigure SSSD to respect Active Directory SSH or Console/GUI GPOsを参照してください。

2.7. SSSD を使用したユーザープライベートグループの自動作成

AD に直接統合された SSSD クライアントは、取得したすべての AD ユーザーに対してユーザープライベートグループを自動的に作成し、GID 番号がすでに取得されていない限り、その GID がユーザーの UID と一致することを保証します。競合を回避するには、ユーザーの UID と同じ GID を持つグループがサーバーに存在することを確認します。

GID は AD に保存されていません。これにより、AD ユーザーがグループ機能を活用しますが、LDAP データベースには不要な空のグループが含まれていません。

2.7.1. AD ユーザー用のユーザープライベートグループの自動作成のアクティブ化

AD ユーザー用のユーザープライベートグループの自動作成を有効にするには、以下を実行します。

1. **/etc/sssd/sssd.conf** ファイルを編集し、**[domain/LDAP]** セクションに追加します。

```
auto_private_groups = true
```

2. sssd サービスを再起動して、sssd データベースを削除します。

```
# service sssd stop ; rm -rf /var/lib/sss/db/* ; service sssd start
```

この手順を実行すると、すべての AD ユーザーに UID と同じ GID があります。

```
# id ad_user1
uid=121298(ad_user1) gid=121298(ad_user1) groups=121298(ad_user1),10000(Group1)
# id ad_user2
uid=121299(ad_user2) gid=121299(ad_user2) groups=121299(ad_user2),10000(Group1)
```

2.7.2. AD ユーザー用のユーザープライベートグループの自動作成の無効化

AD ユーザー用のユーザープライベートグループの自動作成を無効にするには、次のコマンドを実行します。

1. **/etc/sssd/sssd.conf** ファイルを編集し、**[domain/LDAP]** セクションに追加します。

```
auto_private_groups = false
```

2. sssd サービスを再起動して、sssd データベースを削除します。

```
# service sssd stop ; rm -rf /var/lib/sss/db/* ; service sssd start
```

この手順を実行すると、すべての AD ユーザーが同じ汎用 GID を持ちます。

```
# id ad_user1
uid=121298(ad_user1) gid=10000(group1) groups=10000(Group1)
# id ad_user2
uid=121299(ad_user2) gid=10000(group1) groups=10000(Group1)
```

2.8. SSSD クライアントおよび ACTIVE DIRECTORY DNS サイトの自動検出

Active Directory フォレストは、さまざまなドメインコントローラー、ドメインおよび子ドメイン、ならびに物理サイトで非常に大きくなる可能性があります。Active Directory はサイトの概念を使用して、ドメインコントローラーの物理的な場所を特定します。これにより、クライアントが地理的に最も近いドメインコントローラーに接続できるため、クライアントのパフォーマンスが向上します。

デフォルトでは、SSSD クライアントは自動検出を使用して AD サイトを検索し、最寄りのドメインコントローラーに接続します。プロセスは以下の手順で設定されます。

1. SSSD は、AD フォレストの DNS サーバーから SRV レコードをクエリーします。返されたレコードには、フォレストに DC の名前が含まれます。

2. SSSD は、これらの各 DC に LDAP ping を送信します。DC が設定された間隔内に応答しない場合、要求はタイムアウトになり、SSSD は LDAP ping を次の要求に送信します。接続に成功すると、応答には SSSD クライアントが属する AD サイトに関する情報が含まれます。

3. SSSD は DNS サーバーから SRV レコードをクエリーし、所属するサイト内の DC を見つけ、それらのいずれかに接続します。

注記

SSSD は、デフォルトでそれが属する AD サイトを覚えます。これにより、SSSD は自動検出プロセスで、このサイトの DC に LDAP ping を直接送信して、サイト情報を更新できます。そのため、通常タイムアウトが発生しないため、自動検出の手順が非常に高速になります。

そのサイトが存在しなくなったか、クライアントが別のサイトに割り当てられた場合は、SSSD がフォレスト内の SRV レコードのクエリーを開始し、自動検出の全プロセスを実行します。

自動検出を無効にするには、**/etc/ssd/ssd.conf** ファイルの domain セクションで ***ad_site*** オプションを使用して、クライアントの接続先である AD サイトを指定します。

関連情報

- ***ad_site* の** 詳細は、sssd-ad(5) man ページを参照してください。
- Identity Management と Active Directory との間の信頼がある環境では、「Identity Management または SSSD を、信頼された Active Directory ドメインの中から選択された Active Directory サーバーやサイトに制限する手順」 を参照してください。

2.9. SSSD のトラブルシューティング

SSSD のトラブルシューティングの詳細は、『システムレベルの認証ガイド』 の付録 『SSSD のトラブルシューティング』 を参照してください。

第3章 REALMD を使用した ACTIVE DIRECTORY ドメインへの接続

realmd システムは、直接ドメインを統合するために ID ドメインを検出および参加するための明確で簡単な方法を提供します。SSSD や Winbind などの基礎となる Linux システムサービスを設定し、ドメインに接続します。

2章Active Directory を SSSD のアイデンティティープロバイダーとして使用 は、ローカルシステムで System Security Services Daemon (SSSD) を使用し、Active Directory をバックエンドアイデンティティープロバイダーとして使用する方法を説明します。これに対してシステムが適切に設定されていることを確認することは、複雑なタスクになる可能性があります。考えられる ID プロバイダーごとおよび SSSD 自体に対して、さまざまな設定パラメーターがあります。さらに、すべてのドメイン情報を事前に使用でき、SSSD がローカルシステムを AD と統合できるように、SSSD 設定で適切にフォーマットする必要があります。

realmd システムは、その設定を簡素化します。検出検索を実行して、利用可能な AD ドメインおよび Identity Management ドメインを特定し、システムをドメインに参加させ、指定のアイデンティティードメインへの接続およびユーザーアクセスを管理するのに使用するクライアントサービスを設定できます。また、基礎となるサービスの SSSD が複数のドメインをサポートするため、**realmd** は複数のドメインを検出およびサポートすることもできます。

3.1. サポートされるドメインタイプおよびクライアント

realmd システムは、以下のドメインタイプをサポートします。

- Microsoft Active Directory
- Red Hat Enterprise Linux Identity Management

realmd では、以下のドメインクライアントがサポートされます。

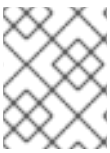
- Red Hat Enterprise Linux Identity Management および Microsoft Active Directory の両方の SSSD
- Microsoft Active Directory の場合は winbind

3.2. REALMDを使用するための前提条件

realmd システムを使用するには、realmd パッケージをインストールします。

```
# yum install realmd
```

さらに、oddjob、oddjob-mkhomedir、sssd、および adcli パッケージがインストールされていることを確認してください。これらのパッケージは、**realmd** を使用してシステムを管理するために必要です。



注記

「Identity ドメインの検出および参加」 で説明しているように、**realmd** を使用してインストールするパッケージを探すことができます。

3.3. REALMD コマンド

realmd システムの主要なタスク領域は、以下の 2 つになります。

- ドメインでのシステム登録の管理
- ローカルシステムリソースへのアクセスが許可されるドメインユーザーの設定

realmd において中心となるユーティリティーは **realm** と呼ばれます。ほとんどの **realm** コマンドでは、ユーティリティーが実行するアクションと、アクションを実行するドメインやユーザーアカウントなどのエンティティーを指定する必要があります。

```
realm command arguments
```

以下に例を示します。

```
realm join ad.example.com
realm permit user_name
```

表3.1 realmd コマンド

コマンド	説明
レルムコマンド	
discover	ネットワーク上にあるドメインの検出スキャンを実行します。
join	指定したドメインにシステムを追加します。
leave	指定したドメインからシステムを削除します。
list	システムに設定したすべてのドメイン、または検出され設定されているすべてのドメインを表示します。
ログインコマンド	
permit	設定されているドメイン内の特定のユーザーまたはすべてのユーザーによるローカルシステムへのアクセスを有効にします。
deny	設定されているドメイン内の特定のユーザーまたはすべてのユーザーがローカルシステムにアクセスするのを制限します。

realm コマンドの詳細は、realm(8) の man ページを参照してください。

3.4. IDENTITY ドメインの検出および参加

realm discover コマンドは、完全なドメイン設定と、システムをドメインに登録するために必要なパッケージの一覧を返します。

realm join コマンドは、ローカルシステムサービスと、ID ドメインのエントリーの両方を設定し、指定されたドメインで使用するローカルマシンを設定します。**realm join** が実行するプロセスは、以下の手順に従います。

1. 指定されたドメインの検出スキャンの実行

2. システムをドメインに参加させるのに必要なパッケージの自動インストール

   これには、SSSD および PAM ホームディレクトリーのジョブパッケージが含まれます。パッケージの自動インストールには、**PackageKit** スイートを実行する必要があることに注意してください。

注記

PackageKit が無効になっていると、システムは足りないパッケージの入力を求められます。また、**yum** ユーティリティーを使用して手動でインストールする必要があります。

3. ディレクトリーにシステムのアカウントエントリーを作成してドメインに参加させる。

4. ホストキータブファイル **/etc/krb5.keytab** の作成

5. SSSD でドメインを設定して、サービスを再起動します。

6. PAM 設定および **/etc/nsswitch.conf** ファイルで、システムサービスのドメインユーザーの有効化

ドメインの検出

オプションなしで実行すると、**realm discover** コマンドは、DHCP (Dynamic Host Configuration Protocol) を介して割り当てられたドメインであるデフォルトの DNS ドメインに関する情報を表示します。

```
# realm discover
ad.example.com
  type: kerberos
  realm-name: AD.EXAMPLE.COM
  domain-name: ad.example.com
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common
```

特定のドメインの検出を実行することもできます。これを行うには、**realm detect** を実行して、検出するドメイン名を追加します。

```
# realm discover ad.example.com
```

realmd システムは DNS SRV ルックアップを使用して、このドメイン内のドメインコントローラーを自動的に検索します。

注記

realm discover コマンドでは、NetworkManager を実行する必要があります。特に、NetworkManager の D-Bus インターフェイスにより異なります。システムが NetworkManager を使用しない場合は、必ず **realm discover** コマンドでドメイン名を指定します。

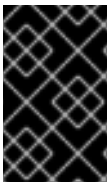
realmd システムは、Active Directory ドメインと Identity Management ドメインの両方を検出できます。両方のドメインが環境に存在する場合は、特定タイプのサーバーに検出結果を絞り込むには **--server-software** オプションを使用します。以下に例を示します。

```
# realm discover --server-software=active-directory
```

検出検索で返される属性の 1 つは **login-policy** で、参加が完了するとすぐにドメインユーザーがログインできるかどうかを示します。ログインがデフォルトで許可されていない場合は、**realm permit** コマンドを使用すると手動で許可できます。詳細は 「ドメインユーザーのログインパーミッションの管理」を参照してください。

realm discover コマンドの詳細は、realm(8) の man ページを参照してください。

ドメインの参加



重要

Active Directory ドメインには、一意のコンピューター名を使用する必要があることに注意してください。NetBIOS コンピューター名と DNS ホスト名の両方を一意に定義し、相互に対応させる必要があります。

システムを ID ドメインに参加させるには、**realm join** コマンドを使用して、ドメイン名を指定します。

```
# realm join ad.example.com
realm: Joined ad.example.com domain
```

デフォルトでは、参加はドメイン管理者として実行されます。AD の場合は、管理者アカウントは **Administrator** と呼ばれ、IdM の場合は **admin** と呼ばれます。別のユーザーとして接続するには、**-U** オプションを使用します。

```
# realm join ad.example.com -U user
```

コマンドは最初に認証情報なしで接続を試みますが、必要に応じてパスワードが要求されます。

Kerberos を Linux システムに適切に設定している場合は、認証のために Kerberos チケットに参加させることもできます。Kerberos プリンシパルを選択するには、**-U** オプションを使用します。

```
# kinit user
  # realm join ad.example.com -U user
```

realm join コマンドは、他にいくつかの設定オプションを受け入れます。**realm join** コマンドの詳細は、realm(8) の man ページを参照してください。

例3.1 システムをドメインに登録する手順の例

1. **realm discover** コマンドを実行して、ドメインに関する情報を表示します。

```
# realm discover ad.example.com
ad.example.com
  type: kerberos
  realm-name: AD.EXAMPLE.COM
  domain-name: ad.example.com
```

```
configured: no
server-software: active-directory
client-software: sssd
```

2. **realm join** コマンドを実行し、ドメイン名をコマンドに渡します。システムから要求された場合は、管理者パスワードを入力します。

```
# realm join ad.example.com
Password for Administrator: password
```

ドメインを検出または参加すると、**realmd** は DNS SRV レコードを確認します。

- Identity Management レコードの場合は **_ldap._tcp.domain.example.com.**
- Active Directory レコードの場合は **_LDAP._tcp.dc._msdcs.domain.example.com.**

AD が設定されている場合に、レコードがデフォルトで作成されます。これにより、サービス検出で検索が可能になります。

ドメイン参加後のシステム設定のテスト

システムがドメインに正常に登録されているかどうかをテストするには、ドメインのユーザーとしてログインし、ユーザー情報が正しく表示されることを確認します。

1. **id *user@domain_name*** コマンドを実行して、ドメインのユーザーに関する情報を表示します。

```
# id user@ad.example.com
uid=1348601103(user@ad.example.com) gid=1348600513(domain
group@ad.example.com) groups=1348600513(domain group@ad.example.com)
```

2. **ssh** ユーティリティーを使用して、同じユーザーとしてログインします。

```
# ssh -l user@ad.example.com linux-client.ad.example.com
user@ad.example.com@linux-client.ad.example.com's password:
Creating home directory for user@ad.example.com.
```

3. **pwd** ユーティリティーがユーザーのホームディレクトリーを出力することを確認します。

```
$ pwd
/home/ad.example.com/user
```

4. **id** ユーティリティーが最初の手順の **id *user@domain_name*** コマンドと同じ情報を出力することを確認します。

```
$ id
uid=1348601103(user@ad.example.com) gid=1348600513(domain
group@ad.example.com) groups=1348600513(domain group@ad.example.com)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

kinit ユーティリティーは、ドメインの参加が成功したかどうかをテストする場合にも役に立ちます。ユーティリティーを使用するには、krb5-workstation パッケージをインストールする必要があることに注意してください。

3.5. IDENTITY ドメインからのシステムの削除

realm leave コマンドを使用して、ID ドメインからシステムを削除します。このコマンドは、SSSD およびローカルシステムからドメイン設定を削除します。

```
# realm leave ad.example.com
```

デフォルトでは、削除はデフォルトの管理者として実行されます。AD の場合は、管理者アカウントは **Administrator** と呼ばれ、IdM の場合は **admin** と呼ばれます。ドメインに参加するために別のユーザーを使用していた場合は、そのユーザーとして削除を実行しないといけない場合があります。別のユーザーを指定するには、**-U** オプションを使用します。

```
# realm leave ad.example.com -U 'AD.EXAMPLE.COM\user'
```

コマンドは最初に認証情報なしで接続を試みますが、必要に応じてパスワードが要求されます。

クライアントがドメインから離れると、コンピューターアカウントはディレクトリーから削除されず、ローカルクライアント設定のみが削除されます。コンピューターアカウントを削除する場合は、**--remove** オプションを指定してコマンドを実行します。

realm leave コマンドの詳細は、realm(8) の man ページを参照してください。

3.6. ドメインの一覧表示

realm list コマンドは、システムに設定されたすべてのドメインと、そのドメインの完全な詳細とデフォルト設定を一覧表示します。これは、**realm discovery** コマンドによって返された情報と同じですが、システム設定にすでにあるドメインに対してのみ返されます。

```
# realm list --all --name-only
ad.example.com
```

realm list で使用できる最も注目すべきオプションは、以下のとおりです。

--all

--all オプションは、すべての検出されたドメイン (設定済みおよび未設定の両方) を一覧表示します。

--name-only

--name-only オプションは、結果をドメイン名に制限し、ドメイン設定の詳細を表示しません。

realm list コマンドの詳細は、realm(8) の man ページを参照してください。

3.7. ドメインユーザーのログインパーミッションの管理

デフォルトでは、*ドメイン側のアクセス制御* が適用されます。これは、ドメインユーザーのログインポリシーがドメイン自体で定義されていることを意味します。*クライアント側のアクセス制御* を使用できるように、このデフォルトの動作は上書きできます。クライアント側のアクセス制御では、ログインパーミッションはローカルポリシーでのみ定義されます。

ドメインがクライアント側のアクセス制御を適用する場合は、**realmd** システムを使用して、そのドメインのユーザーの基本的なアクセスルールである allow または deny を設定できます。このアクセスルールは、システム上の全サービスへのアクセスを許可または拒否することに注意してください。特定

のシステムリソースまたはドメインに、より具体的なアクセスルールを設定する必要があります。

アクセス制御ルールを設定するには、以下の 2 つのコマンドを使用します。

realm deny

realm deny コマンドは、単にドメイン内のすべてのユーザーへのアクセスを拒否します。**--all** オプションを指定して、このコマンドを使用します。

realm permit

realm permit コマンドは以下を実行するために使用できます。

- 以下のように **--all** オプションを使用して、すべてのユーザーへのアクセスを付与します。

```
$ realm permit --all
```

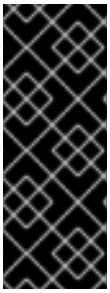
- 指定したユーザーにアクセス権を付与します。以下に例を示します。

```
$ realm permit user@example.com
$ realm permit 'AD.EXAMPLE.COM\user'
```

- **-x** オプションを使用して、指定したユーザーへのアクセスを拒否します。以下に例を示します。

```
$ realm permit -x 'AD.EXAMPLE.COM\user'
```

現在、アクセスの許可はプライマリードメインのユーザーに対してのみ機能し、信頼されたドメインのユーザーに対しては機能しないことに注意してください。これは、ユーザーログインにドメイン名を含める必要があるためです。現在、SSSD は **realmd** に利用可能な子ドメインに関する情報を提供できないためです。



重要

明確に選択したユーザーまたはグループのアクセスのみを許可する方が、一部のユーザーへのアクセスを拒否して、他のすべてのユーザーにアクセスを許可するよりも安全です。したがって、デフォルトで全ユーザーにアクセスを許可し、**realm permit -x** を使用して特定のユーザーのみを拒否することは推奨されません。Red Hat では、代わりに、すべてのユーザーに対してデフォルトのアクセス禁止ポリシーを維持し、**realm permit** を使用して選択したユーザーのアクセスのみを許可することが推奨されます。

realm deny コマンドおよび **realm permit** コマンドの詳細は、realm(8) の man ページを参照してください。

3.8. デフォルトのユーザー設定の変更

realmd システムは、デフォルトのユーザーホームディレクトリーおよびシェル POSIX 属性の変更に対応します。たとえば、これは、一部の POSIX 属性が Windows ユーザーアカウントに設定されていない場合や、これらの属性がローカルシステムの他のユーザーの POSIX 属性と異なる場合に必要となる場合があります。

重要

本セクションで説明されているように設定を変更することは、**realm join** コマンドがまだ実行していない場合のみ有効です。システムがすでに参加している場合は、「オプション: ユーザーホームディレクトリーおよびシェルの設定」 の説明に従って、**/etc/sssd/sssd.conf** ファイルで、デフォルトのホームディレクトリーとシェルを変更します。

デフォルトのホームディレクトリーおよびシェル POSIX 属性を上書きするには、**/etc/realmd.conf** ファイルの **[users]** セクションに以下のオプションを指定します。

default-home

default-home オプションは、ホームディレクトリーを明示的に設定していないアカウントのホームディレクトリーを作成するためのテンプレートを設定します。一般的な形式は **/home/%d/%u** です。ここで、**%d** はドメイン名で、**%u** はユーザー名です。

default-shell

default-shell オプションは、デフォルトのユーザーシェルを定義します。対応しているシステムシェルを受け付けます。

以下に例を示します。

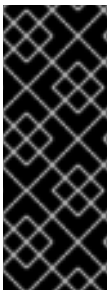
```
[users]
default-home = /home/%u
default-shell = /bin/bash
```

オプションの詳細は、realmd.conf(5) の man ページを参照してください。

3.9. ACTIVE DIRECTORY ドメインエントリーの追加設定

各ドメインのカスタム設定は、**/etc/realmd.conf** ファイルで定義できます。各ドメインには独自の設定セクションを指定できます。セクションの名前はドメイン名と一致する必要があります。以下に例を示します。

```
[ad.example.com]
attribute = value
attribute = value
```



重要

本セクションで説明されているように設定を変更することは、**realm join** コマンドがまだ実行していない場合のみ有効です。システムがすでに参加している場合は、これらの設定を変更しても効果はありません。このような場合は、「Identity ドメインからのシステムの削除」 で説明されているようにドメインから離れて再度参加する必要があります (「ドメインの参加」 を参照)。参加には、ドメイン管理者の認証情報が必要であることに注意してください。

ドメインの設定を変更するには、**/etc/realmd.conf** の該当するセクションを編集します。以下の例では、**ad.example.com** ドメインの ID マッピングを無効にし、ホストプリンシパルを設定して、システムを指定のサブツリーに追加します。

```
[ad.example.com]
computer-ou = ou=Linux Computers,DC=domain,DC=example,DC=com
user-principal = host/linux-client@AD.EXAMPLE.COM
automatic-id-mapping = no
```

「ドメインの参加」 で説明されている **realm join** コマンドを使用して、最初にシステムをドメインに参加したときに同じ設定を設定することもできます。

```
# realm join --computer-ou="ou=Linux Computers,dc=domain,dc=com" --automatic-id-mapping=no --user-principal=host/linux-client@AD.EXAMPLE.COM
```

表3.2「レルム設定オプション」 は、**/etc/realmd.conf** のドメイン default セクションで設定できる最も注目すべきオプションを一覧表示します。利用可能な設定オプションの詳細は、realmd.conf(5) の man ページを参照してください。

表3.2 レルム設定オプション

オプション	説明
computer-ou	コンピューターアカウントをドメインに追加するディレクトリーの場所を設定します。これは、ルートエントリーに対する完全な DN または RDN です。サブツリーがすでに存在している必要があります。
user-principal	コンピューターアカウントの **userPrincipalName** 属性の値を、指定した Kerberos プリンシパルに設定します。
automatic-id-mapping	動的 ID マッピングを有効にするか、マッピングを無効にし、Active Directory で設定された POSIX 属性を使用するかどうかを設定します。

第4章 ACTIVE DIRECTORY 統合での SAMBA の使用

Samba は、Red Hat Enterprise Linux にサーバーメッセージブロック (SMB) プロトコルを実装します。SMB プロトコルは、ファイル共有、共有プリンターなど、サーバーのリソースにアクセスするのに使用されます。

Samba を使用して、Active Directory (AD) ドメインユーザーをドメインコントローラー (DC) に認証できます。また、Samba を使用して、プリンターやローカルディレクトリーを、ネットワーク内の他の SMB クライアントと共有できます。

4.1. WINBINDD を使用したドメインユーザーへの認証

Samba の **winbindd** サービスは、Name Service Switch (NSS) のインターフェイスを提供し、ローカルシステムにログインする際にドメインユーザーが AD に対して認証できるようにします。

winbindd を使用すると、追加のソフトウェアをインストールしなくてもディレクトリーとプリンターを共有する設定が強化されます。詳細は、Red Hat システム管理者のガイド の Samba を参照してください。

4.1.1. AD ドメインの参加

AD ドメインに参加して **Winbind** サービスを使用する場合は、**realm join --client-software=winbind *domain_name*** コマンドを使用します。**realm** ユーティリティーは、Samba、Kerberos、PAM などの設定ファイルを自動的に更新します。

詳細と例については、Red Hat システム管理者のガイド の 『Samba をドメインメンバーとしてセットアップ』 セクションを参照してください。

4.2. SSSD および WINBIND での SMB 共有の使用

本セクションでは、SSSD クライアントを使用して、Server Message Block (SMB) プロトコル (Common Internet File System (CIFS) プロトコルとしても知られる) プロトコルに基づいて共有にアクセスして完全に使用する方法を説明します。

重要

IdM または Active Directory ドメインのクライアントとして SSSD を使用するのは特定の制限があります。Red Hat では、SSSD を Winbind の ID マッピングプラグインとして使用することは推奨されません。詳細は 「What is the support status for Samba file server running on IdM clients or directly enrolled AD clients where SSSD is used as the client daemon」 を参照してください。

SSSD は Winbind が提供するすべてのサービスをサポートしません。たとえば、SSSD は、NT LAN Manager (NTLM) または NetBIOS 名ルックアップを使用した認証をサポートしません。これらのサービスが必要な場合は Winbind を使用します。Identity Management ドメインでは、Kerberos 認証と DNS 名の検索は同じ目的で使用できることに注意してください。

4.2.1. SMB での SSSD の仕組み

SMB のファイル共有プロトコルは、Windows マシンで広く使用されます。Identity Management と Active Directory との間の信頼がある Red Hat Enterprise Linux 環境では、SSSD は、標準の Linux ファイルシステムであるかのように SMB をシームレスに使用できます。

SMB 共有にアクセスするには、システムは Windows SID を Linux POSIX UID および GID に変換できる必要があります。SSSD クライアントは、SID-to-ID または SID-to-name アルゴリズムを使用します。これにより、この ID マッピングが有効になります。

4.2.2. SMB 共有アクセスでの SSSD と Winbind 間の切り替え

この手順では、SSSD クライアントから SMB 共有にアクセスするために使用される SSSD プラグインと Winbind プラグインを切り替える方法を説明します。Winbind が SMB 共有にアクセスできるようにするには、クライアントに cifs-utils パッケージがインストールされている必要があります。cifs-utils がマシンにインストールされていることを確認するには:

```
$ rpm -q cifs-utils
```

1. オプション。現在 SSSD または Winbind を使用して SSSD クライアントから SMB 共有にアクセスするかどうかを確認してください。

   ```
   # alternatives --display cifs-idmap-plugin
   cifs-idmap-plugin - status is auto.
    link currently points to /usr/lib64/cifs-utils/cifs_idmap_sss.so
   /usr/lib64/cifs-utils/cifs_idmap_sss.so - priority 20
   /usr/lib64/cifs-utils/idmapwb.so - priority 10
   Current `best' version is /usr/lib64/cifs-utils/cifs_idmap_sss.so.
   ```

   SSSD プラグイン (**cifs_idmap_sss.so**) がインストールされている場合は、デフォルトで Winbind プラグイン (**idmapwb.so**) よりも優先度が高くなります。

2. Winbind プラグインに切り替える前に、Winbind がシステムで実行していることを確認してください。

   ```
   # systemctl is-active winbind.service
   active
   ```

   SSSD プラグインに切り替える前に、SSSD がシステムで実行していることを確認してください。

   ```
   # systemctl is-active sssd.service
   active
   ```

3. 別のプラグインに切り替えるには、**alternatives --set cifs-idmap-plugin** コマンドを使用して、必要なプラグインへのパスを指定します。たとえば Winbind に切り替えるには、以下を実行します。

   ```
   # alternatives --set cifs-idmap-plugin /usr/lib64/cifs-utils/idmapwb.so
   ```

注記

RHEL 7 の i686 などの 32 ビットバージョンのプラットフォームは、**/usr/lib64/cifs-utils/**の代わりに **usr/lib/cifs-utils/** ディレクトリーを使用します。

4.3. 関連情報

Samba の詳細は、Red Hat システム管理者のガイド の該当するセクションを参照してください。

パート II. LINUX ドメインと ACTIVE DIRECTORY ドメインの統合: フォレスト間の信頼

このパートでは、フォレスト間の信頼環境を作成、設定、および管理することによって、**Linux** ドメイン を **Active Directory** ドメインと統合するための推奨される方法について説明します。

第5章 ACTIVE DIRECTORY および IDENTITY MANAGEMENT を使用したフォレスト間の信頼作成

本章では、Active Directory と Identity Management との間でフォレスト間の信頼関係を作成する方法を説明します。フォレスト間の信頼は、Identity Management 環境と Active Directory (AD) 環境を間接的に統合するための 2 つの方法が推奨されます。他の方法は同期です。お使いの環境に選択する方法が不明な場合は、「間接的な統合」 を参照してください。

Kerberos は *信頼* という概念を実装しています。信頼では、Kerberos レルムからのプリンシパルが別の Kerberos レルムのサービスにチケットを要求できます。プリンシパルはこのチケットを使って、別のレルムに属するマシン上のリソースに対して認証を行うことができます。

Kerberos には、*レルム間の信頼* と呼ばれる、2 つのレルム間の関係を作成する機能があります。この信頼の一部となっているレルムは、共有のチケットとキーのペアを使用します。1 つのレルムのメンバーが両方のレルムのメンバーとして認識されるようなります。

Red Hat Identity Management では、IdM ドメインと Active Directory ドメインとの間にフォレスト間の信頼の設定をサポートしています。

5.1. フォレスト間の信頼の概要

Kerberos レルムは認証にのみ関係します。その他のサービスおよびプロトコルは、Kerberos レルムのマシンで実行しているリソースの ID および承認を補完します。

このため、Kerberos レルム間の信頼を確立するだけでは、レルムのユーザーが別のレルムにあるリソースにアクセスするには不十分になります。別の通信レベルでのサポートも必要になってきます。

5.1.1. 信頼関係のアーキテクチャー

Active Directory と Identity Management の両方が、Kerberos、LDAP、DNS、証明書サービスなどのさまざまなコアサービスを管理します。この 2 つの環境を透過的に統合するには、すべてのコアサービスが相互にシームレスに対話する必要があります。

Active Directory 信頼、フォレスト、およびフォレスト間信頼
Kerberos レルム間の信頼は、Active Directory 環境間の認証で重要なロールを果たします。信頼される AD ドメインのユーザー名およびグループ名を解決するすべてのアクティビティーには、アクセスの実行方法に関係なく認証が必要です。LDAP プロトコルを使用するか、Server Message Block (SMB) プロトコルの上層にある Distributed Computing Environment/Remote Procedure Calls (DCE/RPC) の一部として認証する必要があります。2 つの異なる Active Directory ドメイン間でアクセスを編成するプロトコルが多いため、信頼関係にはより汎用的な名前 *Active Directory 信頼* があります。

複数の AD ドメインは、1 つの *Active Directory フォレスト* にまとめることができます。このフォレストの root ドメインは、フォレスト内で作成される最初のドメインになります。Identity Management ドメインは既存の AD フォレストに含めることができないため、常に別個のフォレストとみなされます。

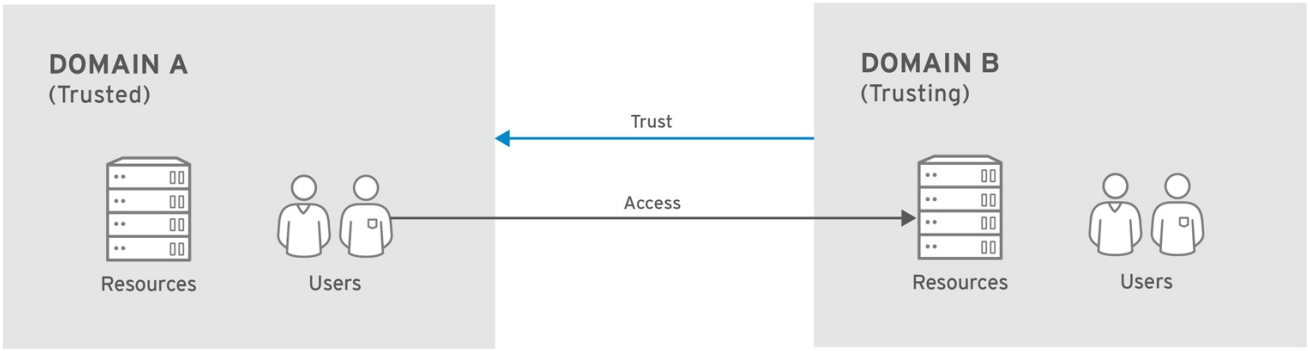
2 つのフォレストルートドメイン間で信頼関係が確立されると、異なる AD フォレストからのユーザーとサービスが通信できるように、*Active Directory のフォレスト間の信頼* と呼ばれます。

信頼フローおよび一方向信頼
信頼は、2 つのドメイン間のアクセス関係を確立します。Active Directory 環境は複雑となるため、子ドメイン、ルートドメイン、フォレスト間など、Active Directory 信頼のタイプや配置が異なります。信頼は、あるドメインから別のドメインへのパスです。アイデンティティーおよび情報をドメイン間で移動する方法は、*信頼フロー* と呼ばれます。

信頼されるドメイン にはユーザーが含まれ、*信頼ドメイン* はリソースへのアクセスを許可します。一

方向の信頼では、信頼フローは一方向のみです。ユーザーは信頼ドメインのリソースにアクセスできますが、信頼しているドメインのユーザーは、信頼できるドメインのリソースにアクセスできません。図5.1「一方向信頼」 では、ドメイン A はドメイン B によって信頼されますが、ドメイン B はドメイン A によって信頼されません。

図5.1 一方向信頼

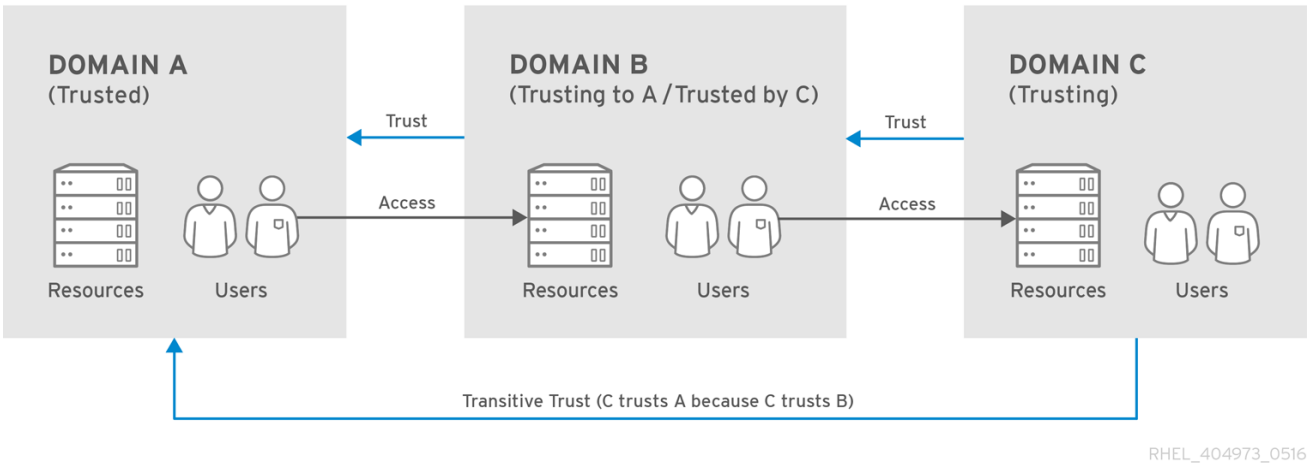


IdM を使用すると、管理者は一方向と双方向の信頼の両方を設定できます。詳細は 「一方向および双方向の信頼」 を参照してください。

推移的および非推移的な信頼

ドメインが別のドメインとその 2 番目のドメインによって信頼されている他のドメインを信頼するように、信頼は *推移的* である可能性があります。

図5.2 推移的な信頼



信頼は *トランザクション以外のもの* でもあるため、信頼は明示的に含まれるドメインのみに制限されます。

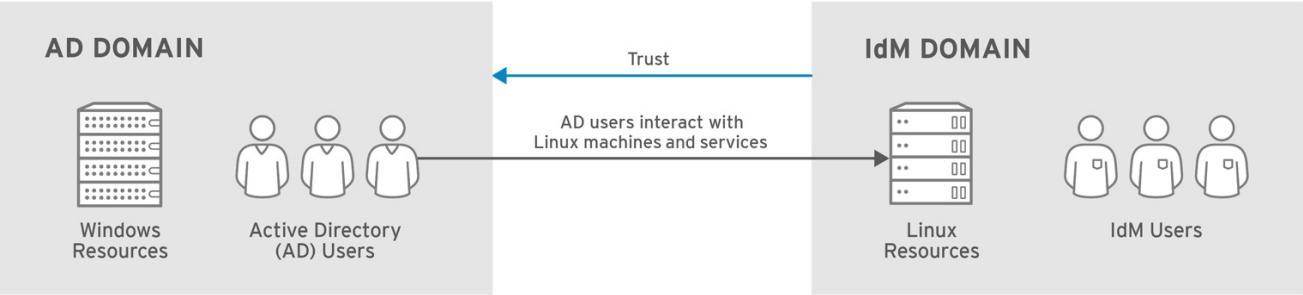
Active Directory および Identity Management のフォレスト間の信頼

Active Directory フォレスト内では、ドメイン間の信頼関係は通常、デフォルトでは双方向で推移的です。

2 つの AD フォレスト間の信頼は 2 つのフォレストルートドメイン間の信頼であるため、双方向または一方向になります。フォレスト間の信頼の遷移は明示的なものです。フォレストのルートドメインを発生する AD フォレスト内のドメイン信頼は、フォレスト間の信頼を推移します。ただし、個別のフォレスト間の信頼は推移的ではありません。明示的なフォレスト間の信頼は、AD フォレストのルートドメイン間で、別の AD フォレストルートドメインに対して確立する必要があります。

AD の観点から観ると、Identity Management は、1 つの AD ドメインを持つ個別の AD フォレストを表します。AD フォレストの root ドメインと IdM ドメインとの間にフォレスト間の信頼が確立されると、AD フォレストドメインのユーザーは、IdM ドメインの Linux マシンおよびサービスと相互作用できます。

図5.3 信頼の方向



5.1.2. Active Directory セキュリティーオブジェクトおよび信頼

Active Directory グローバルカタログ
グローバルカタログには、Active Directory のオブジェクトに関する情報が含まれます。これは、オブジェクトの完全なコピーを独自のドメインに格納します。Active Directory フォレストの他のドメインのオブジェクトから、一般的に検索される属性の一部コピーのみがグローバルカタログに保存されます。さらに、一部のグループは特定のスコープ内でのみ有効であり、グローバルカタログの一部ではない可能性があります。

フォレスト間の信頼コンテキストは、1 つのドメインよりも広いことに注意してください。そのため、信頼できるフォレストからのこれらのサーバーローカルまたはドメインローカルセキュリティーグループメンバーシップの一部は、IdM サーバーには表示されないことがあります。

グローバルカタログおよび POSIX 属性
Active Directory は、デフォルト設定で POSIX 属性を複製しません。AD に定義されている POSIX 属性を使用する必要がある場合は、それらをグローバルカタログサービスに複製することが強く推奨されます。

5.1.3. IdM の信頼アーキテクチャー

Identity Management 側で、IdM サーバーは Active Directory アイデンティティーを認識し、アクセス制御のためにグループメンバーシップを適切に処理する必要があります。Microsoft PAC (MS-PAC、Privilege Account Certificate) には、ユーザーに必要な情報、セキュリティー ID、ドメインユーザー名、およびグループメンバーシップが含まれます。Identity Management には、Kerberos チケットの PAC 内のデータを分析する 2 つのコンポーネントがあります。

- SSSD: Active Directory でアイデンティティールックアップを実行し、承認のためにユーザーおよびグループのセキュリティー識別子 (SID) を取得します。SSSD は、ユーザー、グループ、およびユーザーのチケット情報をキャッシュし、Kerberos ドメインと DNS ドメインをマップします。

- Identity Management (Linux ドメイン管理) は、Active Directory ユーザーを IdM ポリシーおよびアクセス用の IdM グループに関連付けます。

注記

SELinux、sudo、ホストベースのアクセス制御など、Linux ドメイン管理用のアクセス制御ルールおよびポリシーは、Identity Management で定義され、適用されます。Active Directory 側で設定されたアクセス制御ルールは、IdM によって評価または使用されません。関連する唯一の Active Directory 設定は、グループメンバーシップです。

さまざまな Active Directory フォレストとの信頼

IdM は、さまざまな AD フォレストとの信頼関係に含まれることもできます。信頼を確立したら、同じコマンドおよび手順に従って、他のフォレストを使用した追加の信頼を追加できます。IdM は、完全に関連性のない複数のフォレストを同時に信頼できるため、ユーザーは同じ共有 IdM ドメインのリソースに、関係のない AD フォレストによるリソースへのアクセスが可能になります。

5.1.3.1. Active Directory PAC および IdM チケット

Active Directory のグループ情報は、*Privilege Attribute Certificate* (MS-PAC または PAC) データセットの識別子一覧に保存されます。PAC には、グループメンバーシップや追加の認証情報情報などのさまざまな認可情報が含まれます。また、Active Directory ドメインにユーザーおよびグループの *セキュリティー識別子* (SID) も含まれます。SID は、作成時に Active Directory ユーザーおよびグループに割り当てられた識別子です。信頼環境では、グループメンバーは名前または DN ではなく SID で識別されます。

PAC は、Windows ドメイン内の他の Windows クライアントおよびサーバーに対してエンティティーを識別する方法として、Active Directory ユーザーの Kerberos サービス要求チケットに組み込まれています。IdM は、PAC のグループ情報を Active Directory グループにマッピングしてから、対応する IdM グループにマッピングして、アクセスを決定します。

Active Directory ユーザーが IdM リソースのサービスのチケットを要求すると、プロセスは以下のようになります。

1. サービスの要求には、ユーザーの PAC が含まれます。IdM Kerberos Distribution Centre (KDC) は、Active Directory グループの一覧と IdM グループのメンバーシップを比較して、PAC を分析します。

2. MS-PAC で定義された Kerberos プリンシパルの SID の場合、IdM KDC は、IdM LDAP で定義された外部グループメンバーシップを評価します。SID で追加のマッピングが利用可能な場合、MS-PAC レコードは、SID が属する IdM グループの他の SID で拡張されます。結果として得られる MS-PAC は、IdM KDC によって署名されます。

3. サービスチケットは、IdM KDC が署名した更新された PAC のユーザーに戻ります。IdM ドメイン認識されている AD グループに属するユーザーは、サービスチケットの MS-PAC コンテンツに基づいて、IdM クライアントで実行している SSSD が認識できるようになりました。これにより、IdM クライアントがグループメンバーシップを検出するために ID トラフィックを減らすことができます。

IdM クライアントがサービスチケットを評価すると、プロセスには以下の手順が含まれます。

1. 評価プロセスで使用される Kerberos クライアントライブラリーは、PAC データを SSSD PAC レスポンダーに送信します。

2. PAC レスポンダーは、PAC のグループ SID を検証し、そのユーザーを SSSD キャッシュ内の対応するグループに追加します。SSSD は、新規サービスにアクセスするために、各ユーザーの複数の TGT およびチケットを保存します。

3. 検証済みグループに属するユーザーは、IdM 側で必要なサービスにアクセスできるようになりました。

5.1.3.2. Active Directory ユーザーおよび Identity Management グループ

Active Directory ユーザーおよびグループを管理する場合は、個別の AD ユーザーおよびグループをすべて Identity Management グループに追加できます。

AD ユーザーに IdM グループを設定する方法は、「Active Directory ユーザーの IdM グループの作成」を参照してください。

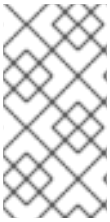
非 POSIX の外部グループおよび SID マッピング
IdM LDAP のグループメンバーシップは、グループのメンバーである LDAP オブジェクトの識別名 (DN) を指定して表現されます。AD エントリーは、IdM に同期またはコピーされません。つまり、AD ユーザーおよびグループには IdM LDAP に LDAP オブジェクトがありません。そのため、IdM LDAP でグループメンバーシップを表現するために直接使用できません。

このため、IdM は *POSIX 以外の外部グループ* を作成します。これは、AD ユーザーおよびグループの SID への参照を含む LDAP オブジェクトを文字列として作成します。次に、POSIX 以外の外部グループは、IdM の AD ユーザーおよびグループのグループメンバーシップを表現するために通常の IdM LDAP オブジェクトとして参照されます。

非 POSIX 外部グループの SID は SSSD により処理されます。SSSD は、AD ユーザーが IdM の POSIX グループに属するグループの SID をマッピングします。AD 側の SID はユーザー名に関連付けられます。ユーザー名を使用して IdM リソースにアクセスする場合、IdM の SSSD はそのユーザー名を SID に解決し、「Active Directory PAC および IdM チケット」 で説明されているように、AD ドメインでその SID の情報を検索します。

ID 範囲
Linux でユーザーを作成すると、ユーザー ID 番号が割り当てられます。さらに、ユーザーにプライベートグループが作成されます。プライベートグループ ID 番号は、ユーザー ID 番号と同じです。Linux 環境では、競合を作成しません。ただし、Windows では、ドメインのすべてのオブジェクトに対して、セキュリティー ID 番号が一意でなければなりません。

信頼できる AD ユーザーには、Linux システムで UID および GID の番号が必要です。この UID および GID の番号を IdM で生成できますが、AD エントリーに UID と GID の番号がすでに割り当てられている場合は、異なる数値を割り当てると競合が作成されます。このような競合を回避するには、UID および GID の番号や推奨ログインシェルなど、AD 定義 POSIX 属性を使用できます。



注記

AD は、*グローバルカタログ* でフォレスト内のすべてのオブジェクトの情報のサブセットを保存します。グローバルカタログには、フォレスト内のすべてのドメインのすべてのエントリーが含まれます。AD 定義 POSIX 属性を使用する場合、Red Hat は、最初に属性をグローバルカタログに複製することを強く推奨します。

信頼が作成されると、IdM は使用する ID 範囲の種類を自動的に検出し、信頼に追加される AD ドメインに一意の ID 範囲を作成します。以下のオプションのいずれかを **ipa trust-add** コマンドに指定することで、手動で選択することもできます。

ipa-ad-trust
この範囲オプションは、SID に基づいて IdM が生成した ID アルゴリズムに使用されます。

IdM が SID-to-POSIX ID マッピングを使用して SID を生成する場合は、AD および IdM のユーザーおよびグループの ID 範囲が一意で、オーバーライピングしていない ID 範囲が利用可能である必要があります。

ipa-ad-trust-posix

この範囲オプションは、AD エントリーの POSIX 属性で定義される ID に使用されます。

IdM は、AD のグローバルカタログまたはディレクトリーコントローラーから、***uidNumber*** および ***gidNumber*** を含む POSIX 属性を取得します。AD ドメインが正しく管理され、ID の競合なしに管理されている場合は、この方法で生成された ID 番号は一意です。この場合、ID の検証や ID 範囲は必要ありません。

以下に例を示します。

```
[root@ipaserver ~]# ipa trust-add name_of_the_trust --range-type=ipa-ad-trust-posix
```

他の **ID** 範囲での信頼の再作成
作成された信頼の ID 範囲がデプロイメントに適していない場合は、別の **--range-type** オプションを使用して信頼を再作成できます。

1. 現在使用中のすべての ID 範囲を表示します。

   ```
   [root@ipaserver ~]# ipa idrange-find
   ```

   一覧で、**ipa trust-add** コマンドで作成された ID 範囲の名前を特定します。ID 範囲の名前の最初の部分は信頼の名前 *name_of_the_trust*_id_range (例: *ad.example.com*) です。

2. (任意手順) 信頼の作成時に使用する **--range-type** オプション、**ipa-ad-trust** または **ipa-ad-trust-posix** が分からない場合は、オプションを特定します。

   ```
   [root@ipaserver ~]# ipa idrange-show name_of_the_trust_id_range
   ```

   ステップ 5 の新しい信頼の逆タイプを選択できるように、そのタイプを書き留めます。

3. **ipa trust-add** コマンドで作成された範囲を削除します。

   ```
   [root@ipaserver ~]# ipa idrange-del name_of_the_trust_id_range
   ```

4. 信頼を削除します。

   ```
   [root@ipaserver ~]# ipa trust-del name_of_the_trust
   ```

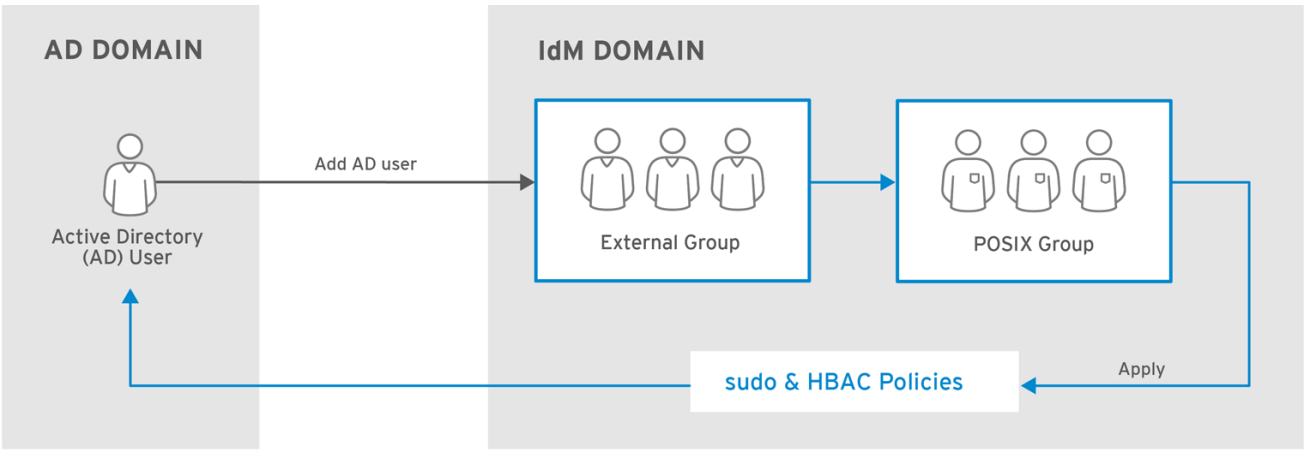
5. 正しい **--range-type** オプションを使用して、新たな信頼を作成します。以下に例を示します。

   ```
   [root@ipaserver ~]# ipa trust-add name_of_the_trust --range-type=ipa-ad-trust
   ```

5.1.3.3. Active Directory ユーザーおよび IdM ポリシーおよび設定

SELinux、ホストベースのアクセス制御、sudo、netgroup などの複数の IdM ポリシー定義が、ユーザーグループに依存してポリシーの適用方法を特定します。

図5.4 Active Directory ユーザーおよび IdM グループおよびポリシー



Active Directory ユーザーは IdM ドメインに外部ですが、「Active Directory ユーザーおよび Identity Management グループ」 で説明されている外部グループとして設定されている限り、これらのグループが IdM グループにグループメンバーとして追加することができます。このような場合は、sudo、ホストベースのアクセス制御、およびその他のポリシーは外部 POSIX グループに適用され、最終的に IdM ドメインリソースにアクセスする際に最終的に AD ユーザーに適用されます。

チケットの PAC のユーザー SID は、AD アイデンティティーに解決されます。つまり、Active Directory ユーザーは、完全修飾ユーザー名または SID を使用してグループメンバーとして追加できます。

5.1.4. 一方向および双方向の信頼

IdM は、IdM でサービスへの接続を確立できるエンティティーが AD のみに制限されるか、または IdM エンティティーも含めるかどうかによって、2 種類の信頼関係がサポートされます。

一方向の信頼

一方向の信頼により、AD ユーザーおよびグループは IdM のリソースにアクセスできますが、その逆はできません。IdM ドメインは AD フォレストを信頼しますが、AD フォレストは IdM ドメインを信頼しません。

一方向の信頼は、信頼を作成するデフォルトのモードです。

双方向の信頼

双方向の信頼により、AD ユーザーおよびグループは IdM のリソースにアクセスできるようになります。信頼境界を使用して Kerberos プロトコルに S4U2Self および S4U2Proxy の Microsoft 拡張を必要とする、Microsoft SQL Server などのソリューションに、双方向の信頼を設定する必要があります。RHEL IdM ホスト上にあるアプリケーションは、AD ユーザーに関する S4U2Self または S4U2Proxy の情報を Active Directory ドメインコントローラーから要求する場合があり、双方向の信頼でこの機能が提供されます。

この双方向の信頼機能では、IdM ユーザーは Windows システムにログインできないだけでなく、IdM の双方向信頼では、AD の一方向信頼ソリューションと比較して、権限が追加でユーザーに付与されるわけではありません。

一方向および双方向の信頼に関する一般的な情報は、「信頼関係のアーキテクチャー」 を参照してください。

信頼を確立した後には、そのタイプを変更することができません。別の信頼タイプが必要な場合は、**ipa trust-add** コマンドを再度実行します。これを実行すると、既存の信頼を削除して、新しい信頼を確立できます。

5.1.5. Active Directory への外部信頼

外部の信頼は、異なるフォレストにあるドメイン間の信頼関係です。フォレストの信頼は常に Active Directory フォレストのルートドメイン間で信頼を確立する必要がありますが、フォレスト内のドメインには外部の信頼を確立できます。

外部の信頼は推移的ではありません。このため、他の Active Directory ドメインのユーザーおよびグループは、IdM リソースにアクセスできません。詳細は 「推移的および非推移的な信頼」 を参照してください。

5.1.6. 信頼コントローラーおよび信頼エージェント

IdM には、Active Directory への信頼をサポートする、次のタイプの IdM サーバーがあります。

信頼コントローラー

信頼を制御し、Active Directory ドメインコントローラー (DC) に対して ID 検索を実行できる IdM サーバー。Active Directory ドメインコントローラーは、Active Directory への信頼を確立して検証する際に信頼コントローラーに問い合わせます。信頼を設定すると、最初の信頼コントローラーが作成されます。

IdM サーバーを信頼コントローラーとして設定する方法は、「信頼の作成」 を参照してください。

信頼コントローラーは、信頼エージェントと比較して、ネットワークに直接接続するサービスの実行量が多いため、潜在的な侵入者に対してより大きな攻撃対象領域を提示します。

信頼エージェント

Active Directory ドメインコントローラーで ID 検索が実行可能な IdM サーバー。

IdM サーバーを信頼エージェントとして設定する方法は、「信頼用の IdM サーバーの準備」 を参照してください。

IdM ドメインには、信頼コントローラーおよびエージェントの他に、ロールなしでレプリカを含めることもできます。ただし、このサーバーは Active Directory と通信しません。したがって、これらのサーバーと通信するクライアントは、Active Directory ユーザーおよびグループを解決できず、Active Directory ユーザーを認証および認可することができません。

表5.1 信頼コントローラーおよび信頼エージェントが提供する機能の比較

機能	信頼コントローラー	信頼エージェント
Active Directory のユーザーおよびグループの解決	はい	はい
信頼された Active Directory フォレストのユーザーがアクセスできるサービスを実行する IdM クライアントを登録	はい	はい
信頼の管理 (たとえば、信頼関係の追加)	はい	いいえ

信頼コントローラーと信頼エージェントのデプロイメントを計画する時に、以下のガイドラインを考慮してください。

- Identity Management のデプロイメントごとに、信頼コントローラーを少なくとも 2 台は設定してください。
- 各データセンターごとに、信頼コントローラーを少なくとも 2 台設定する。

追加の信頼コントローラーを作成する場合や、既存の信頼コントローラーが失敗した場合には、信頼エージェントまたはレプリカを昇格して、信頼コントローラーを新規作成してください。これには、「信頼用の IdM サーバーの準備」 の説明に従って、IdM サーバーの **ipa-adtrust-install** ユーティリティーを使用します。

重要

既存の信頼コントローラーを信頼エージェントにダウングレードすることはできません。インストール後は、信頼コントローラーサーバーのロールはトポロジーから削除できません。

5.2. フォレスト間の信頼の作成

5.2.1. 環境およびマシンの要件

信頼関係を設定する前に、Active Directory サーバーと、Identity Management サーバー、マシン、および環境の両方がこのセクションに記載されている要件を満たすことを確認してください。

5.2.1.1. サポート対象の Windows プラットフォーム

以下のフォレストとドメイン機能レベルを使用する Active Directory フォレストとの信頼関係を確立できます。

- フォレスト機能レベルの範囲 - Windows Server 2008 ~ Windows Server 2016
- ドメイン機能レベルの範囲 - Windows Server 2008 ~ Windows Server 2016

次のオペレーティングシステムは、前述の機能レベルを使用して信頼を確立するためにサポートおよびテストされています。

- Windows Server 2012 R2
- Windows Server 2016

以前のバージョンの Windows Server は、信頼確立ではサポートされません。

5.2.1.2. DNS およびレルムの設定

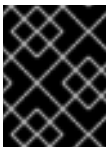
信頼を確立するには、Active Directory と Identity Management に特定の DNS 設定が必要になります。

一意のプライマリー **DNS** ドメイン

各システムには、独自の固有プライマリー DNS ドメインが設定されている必要があります。以下に例を示します。

- **ad.example.com** (AD の場合) および **idm.example.com** (IdM の場合)
- **example.com** (AD の場合) および **idm.example.com** (IdM の場合)

- **ad.example.com** (AD の場合) および **example.com** (IdM の場合)



重要

IdM ドメインが AD ドメインの親ドメインである場合、IdM サーバーは Red Hat Enterprise Linux 7.5 以降で実行する必要があります。

最も便利な管理ソリューションは、各 DNS ドメインが統合 DNS サーバーで管理されている環境ですが、規格に準拠した DNS サーバーも使用できます。

AD または IdM が、ID 管理用の別のシステムとプライマリー DNS ドメインを共有することはできません。詳細は、 Linux ドメイン ID、認証、およびポリシーガイド のホスト名および DNS 設定要件を参照してください。

Kerberos レルム名は、プライマリー DNS ドメイン名を大文字にしたもの

Kerberos レルム名は、プライマリー DNS ドメイン名と同じで、すべて大文字にする必要があります。たとえば、AD のドメイン名が **ad.example.com** で、IdM のドメイン名が **idm.example.com** の場合、Kerberos レルム名は **AD.EXAMPLE.COM** および **IDM.EXAMPLE.COM** になります。

DNS レコードが信頼内の全 DNS ドメインから解決可能である

すべてのマシンが、信頼関係内で関連するすべての DNS ドメインの DNS レコードを解決できるようにする必要があります。

- IdM DNS を設定する場合は、『Linux ドメイン ID、認証、およびポリシーガイド』 で、IdM ドメイン内の DNS サービスの設定に関するセクション および DNS 転送の管理に関するセクション で説明されている手順に従ってください。
- 統合 DNS なしで IdM を使用している場合は、『Linux ドメイン ID、認証、およびポリシーガイド』 の 統合 DNS なしでサーバーインストールを説明しているセクション で説明されている手順に従います。

IdM ドメインと AD DNS ドメインとの間に重複がない

IdM に参加しているシステムは、複数の DNS ドメインに分散できます。IdM クライアントを含む DNS ドメインは、AD に参加しているマシンを含む DNS ドメインと重複できません。プライマリー IdM DNS ドメインには、AD 信頼に対応するのに適切な SRV レコードが必要です。

注記

IdM と Active Directory との間の信頼がある一部の環境では、Active Directory DNS ドメインの一部であるホストに IdM クライアントをインストールできます。ホストは、これにより、Linux に焦点を合わせた IdM の機能の恩恵を受けることができます。これは推奨される設定ではなく、いくつかの制限があります。Red Hat は、Active Directory が所有する DNS ゾーンとは異なる DNS ゾーンに常に IdM クライアントを展開し、IdM ホスト名を介して IdM クライアントにアクセスすることをお勧めします。

$ ipa dns-update-system-records --dry-run コマンドを実行して、システム設定に必要な固有の SRV レコードの一覧を取得できます。

生成される一覧は、たとえば以下のようになります。

```
$ ipa dns-update-system-records --dry-run
 IPA DNS records:
```

```
_kerberos-master._tcp.example.com. 86400 IN SRV 0 100 88 server.example.com.
_kerberos-master._udp.example.com. 86400 IN SRV 0 100 88 server.example.com.
_kerberos._tcp.example.com. 86400 IN SRV 0 100 88 server.example.com.
_kerberos._udp.example.com. 86400 IN SRV 0 100 88 server.example.com.
_kerberos.example.com. 86400 IN TXT "EXAMPLE.COM"
_kpasswd._tcp.example.com. 86400 IN SRV 0 100 464 server.example.com.
_kpasswd._udp.example.com. 86400 IN SRV 0 100 464 server.example.com.
_ldap._tcp.example.com. 86400 IN SRV 0 100 389 server.example.com.
_ntp._udp.example.com. 86400 IN SRV 0 100 123 server.example.com.
```

同じ IdM レルムにあるその他の DNS ドメインでは、AD への信頼を設定する際に SRV レコードを設定する必要はありません。これは、AD ドメインコントローラーが、KDC の検索に SRV レコードではなく、信頼の名前接尾辞のルーティング情報を使用するためです。

DNS 設定の確認

信頼を設定する前に、Identity Management サーバーおよび Active Directory サーバーが自身と解決でき、そして相互に解決できることを確認します。

以下のコマンドを実行すると想定された結果が表示されない場合は、コマンドを実行しているホストで DNS 設定を確認します。ホスト設定が適切であれば、親から子ドメインへの DNS 委譲が正しく設定されていることを確認してください。

AD は DNS ルックアップの結果をキャッシュするため、DNS の変更は即座に表示されないことがあります。現在のキャッシュは、**ipconfig /flushdns** コマンドを実行して削除できます。

IdM がホストするサービスが信頼を確立するために使用される **IdM** ドメインサーバーから解決可能であることを確認します

1. UDP サービスレコードの Kerberos、および TCP サービスレコード上の LDAP に、DNS クエリーを実行します。

```
[root@ipaserver ~]# dig +short -t SRV _kerberos._udp.ipa.example.com.
0 100 88 ipamaster1.ipa.example.com.

[root@ipaserver ~]# dig +short -t SRV _ldap._tcp.ipa.example.com.
0 100 389 ipamaster1.ipa.example.com.
```

   コマンドは、すべての IdM サーバーを一覧で表示する必要があります。

2. IdM Kerberos レルム名を使用して、TXT レコードに DNS クエリーを実行します。取得した値は、IdM のインストール時に指定した Kerberos レルムと一致することが予想されます。

```
[root@ipaserver ~]# dig +short -t TXT _kerberos.ipa.example.com.
IPA.EXAMPLE.COM
```

3. 「信頼用の IdM サーバーの準備」 で説明されているように、**ipa-adtrust-install** ユーティリティーの実行後に、UDP サービスレコード上の MS DC Kerberos、および TCP サービスレコード上の LDAP に DNS クエリーを実行します。

```
[root@ipaserver ~]# dig +short -t SRV _kerberos._udp.dc._msdcs.ipa.example.com.
0 100 88 ipamaster1.ipa.example.com.

[root@ipaserver ~]# dig +short -t SRV _ldap._tcp.dc._msdcs.ipa.example.com.
0 100 389 ipamaster1.ipa.example.com.
```

コマンドは、**ipa-adtrust-install** が実行している IdM サーバーの一覧を表示することが期待されます。**ipa-adtrust-install** が IdM サーバーで実行していない場合、通常は最初の信頼関係を確立する前に出力が空になることに注意してください。

IdM が AD のサービスレコードを解決できることを確認します。

UDP サービスレコードの Kerberos、および TCP サービスレコード上の LDAP に、DNS クエリーを実行します。

```
[root@ipaserver ~]# dig +short -t SRV _kerberos._udp.dc._msdcs.ad.example.com.
0 100 88 addc1.ad.example.com.

[root@ipaserver ~]# dig +short -t SRV _ldap._tcp.dc._msdcs.ad.example.com.
0 100 389 addc1.ad.example.com.
```

これらのコマンドは、AD ドメインコントローラーの名前を返す必要があります。

IdM がホストするサービスが AD サーバーで解決可能であることを確認します

1. AD サーバーに、サービスレコードを検索する **nslookup.exe** ユーティリティーを設定します。

```
C:\>nslookup.exe
> set type=SRV
```

2. UDP サービスレコード上の Kerberos、および TCP サービスレコード上の LDAP に、ドメイン名を入力します。

```
> _kerberos._udp.ipa.example.com.
_kerberos._udp.ipa.example.com.       SRV service location:
    priority              = 0
    weight                = 100
    port                  = 88
    svr hostname   = ipamaster1.ipa.example.com
> _ldap._tcp.ipa.example.com
_ldap._tcp.ipa.example.com       SRV service location:
    priority              = 0
    weight                = 100
    port                  = 389
    svr hostname   = ipamaster1.ipa.example.com
```

予期される出力には、IdM がホストするサービスが信頼を確立するために使用される IdM ドメインサーバーから解決可能であることを確認します で表示される IdM サーバーと同じセットが表示されます。

3. サービスの種類を TXT に変更し、IdM Kerberos レルム名で TXT レコードに DNS クエリーを実行します。

```
C:\>nslookup.exe
> set type=TXT
> _kerberos.ipa.example.com.
_kerberos.ipa.example.com.       text =

    "IPA.EXAMPLE.COM"
```

出力には、IdM がホストするサービスが信頼を確立するために使用される IdM ドメインサーバーから解決可能であることを確認します に表示される値と同じ値が含まれることが予想されます。

4. 「信頼用の IdM サーバーの準備」 で説明されているように、**ipa-adtrust-install** ユーティリティーの実行後に、UDP サービスレコード上の MS DC Kerberos、および TCP サービスレコード上の LDAP に DNS クエリーを実行します。

```
C:\>nslookup.exe
> set type=SRV
> _kerberos._udp.dc._msdcs.ipa.example.com.
_kerberos._udp.dc._msdcs.ipa.example.com.       SRV service location:
    priority = 0
    weight = 100
    port = 88
    svr hostname = ipamaster1.ipa.example.com
> _ldap._tcp.dc._msdcs.ipa.example.com.
_ldap._tcp.dc._msdcs.ipa.example.com.       SRV service location:
    priority = 0
    weight = 100
    port = 389
    svr hostname = ipamaster1.ipa.example.com
```

このコマンドは、**ipa-adtrust-install** ユーティリティーが実行した IdM サーバーの一覧を表示することが期待されます。**ipa-adtrust-install** が IdM サーバーで実行していない場合、通常は最初の信頼関係を確立する前に出力が空になることに注意してください。

AD サービスが **AD** サーバーで解決可能であることを検証します。

1. AD サーバーに、サービスレコードを検索する **nslookup.exe** ユーティリティーを設定します。

```
C:\>nslookup.exe
> set type=SRV
```

2. UDP サービスレコード上の Kerberos、および TCP サービスレコード上の LDAP に、ドメイン名を入力します。

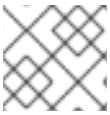
```
> _kerberos._udp.dc._msdcs.ad.example.com.
_kerberos._udp.dc._msdcs.ad.example.com.  SRV service location:
    priority = 0
    weight = 100
    port = 88
    svr hostname = addc1.ad.example.com
> _ldap._tcp.dc._msdcs.ad.example.com.
_ldap._tcp.dc._msdcs.ad.example.com.  SRV service location:
    priority = 0
    weight = 100
    port = 389
    svr hostname = addc1.ad.example.com
```

予期される出力には、IdM が AD のサービスレコードを解決できることを確認します。 で表示されるのと同じ AD サーバーのセットが含まれます。

5.2.1.3. NetBIOS 名

NetBIOS 名は、Active Directory (AD) ドメインを識別するために重要であり、IdM に AD で設定された信頼がある場合は、IdM ドメインとサービスを識別するために重要です。結果として、IdM ドメインには、フォレストの信頼を確立する AD ドメインで使用されている NetBIOS 名とは異なる NetBIOS 名を使用する必要があります。

Active Directory または IdM ドメインの NetBIOS 名は通常、対応する DNS ドメインの左端のコンポーネントです。たとえば、DNS ドメインが **ad.example.com** の場合、NetBIOS 名は通常 **AD** になります。



注記

NetBIOS 名は最長 15 文字です。

5.2.1.4. ファイアウォールおよびポート

AD ドメインコントローラーと IdM サーバーとの間の通信を有効にするには、以下のポート要件を満たしていることを確認してください。

- AD トラストに必要なポート と、AD トラスト内の IdM サーバーが必要とするポート を、IdM サーバーとすべての AD ドメインコントローラーで、IdM サーバーから AD ドメインコントローラーへと、AD ドメインコントローラーから IdM サーバーへの両方向で開きます。
- 信頼された AD フォレストのすべての AD ドメインコントローラーで、AD の信頼で IdM クライアントで必要なポート を開きます。IdM クライアントで、ポートが送信方向に開いていることを確認します (『Linux ドメイン ID、認証、およびポリシーガイド』 に クライアントをインストールするための前提条件を参照)。

表5.2 AD 信頼に必要なポート

Service	ポート	プロトコル
エンドポイント解決ポートマッパー	135	TCP
NetBIOS-DGM	138	TCP および UDP
NetBIOS-SSN	139	TCP および UDP
Microsoft-DS	445	TCP および UDP
エンドポイントマッパーリスナーの範囲	1024 ~ 1300	TCP
AD グローバルカタログ	3268	TCP
LDAP	389	TCP [a] および UDP

[a] 信頼のために IdM サーバーで TCP ポートの 389 を開く必要はありませんが、IdM サーバーと通信しているクライアントに必要です。

表5.3 信頼の IdM サーバーで必要なポート

Service	ポート	プロトコル
Kerberos	『Linux ドメイン ID、認証、およびポリシーガイド』 の ポート要件 を参照してください。	
LDAP		
DNS		

表5.4 AD 信頼で IdM クライアントに必要なポート

Service	ポート	プロトコル	備考
Kerberos	88	UDP および TCP	**libkrb5** ライブラリーは UDP を使用し、KDC (Kerberos Distribution Center) から送信されるデータが大きすぎると、TCP プロトコルにフォールバックします。Active Directory は、PAC (Privilege Attribute Certificate) を Kerberos チケットに割り当てます。これによりサイズが増加し、TCP プロトコルを使用する必要があります。要求のフォールバックと再送信を回避するため、デフォルトでは、Red Hat Enterprise Linux 7.4 以降の SSSD ではユーザー認証に TCP が使用されます。**libkrb5** が TCP を使用する前のサイズを設定するには、**/etc/krb.5.conf** ファイルに ***udp_preference_limit*** を設定してください。詳細は krb5.conf(5) の man ページを参照してください。

関連情報

- 必要なポートを開く方法は、『Linux ドメイン ID、認証、およびポリシーガイド』 の ポート要件 を参照してください。

5.2.1.5. IPv6 設定

IdM システムでは、カーネル内で IPv6 プロトコルが有効になっている必要があります。IPv6 が無効になっていると、IdM サービスが使用する CLDAP プラグインが初期化に失敗します。

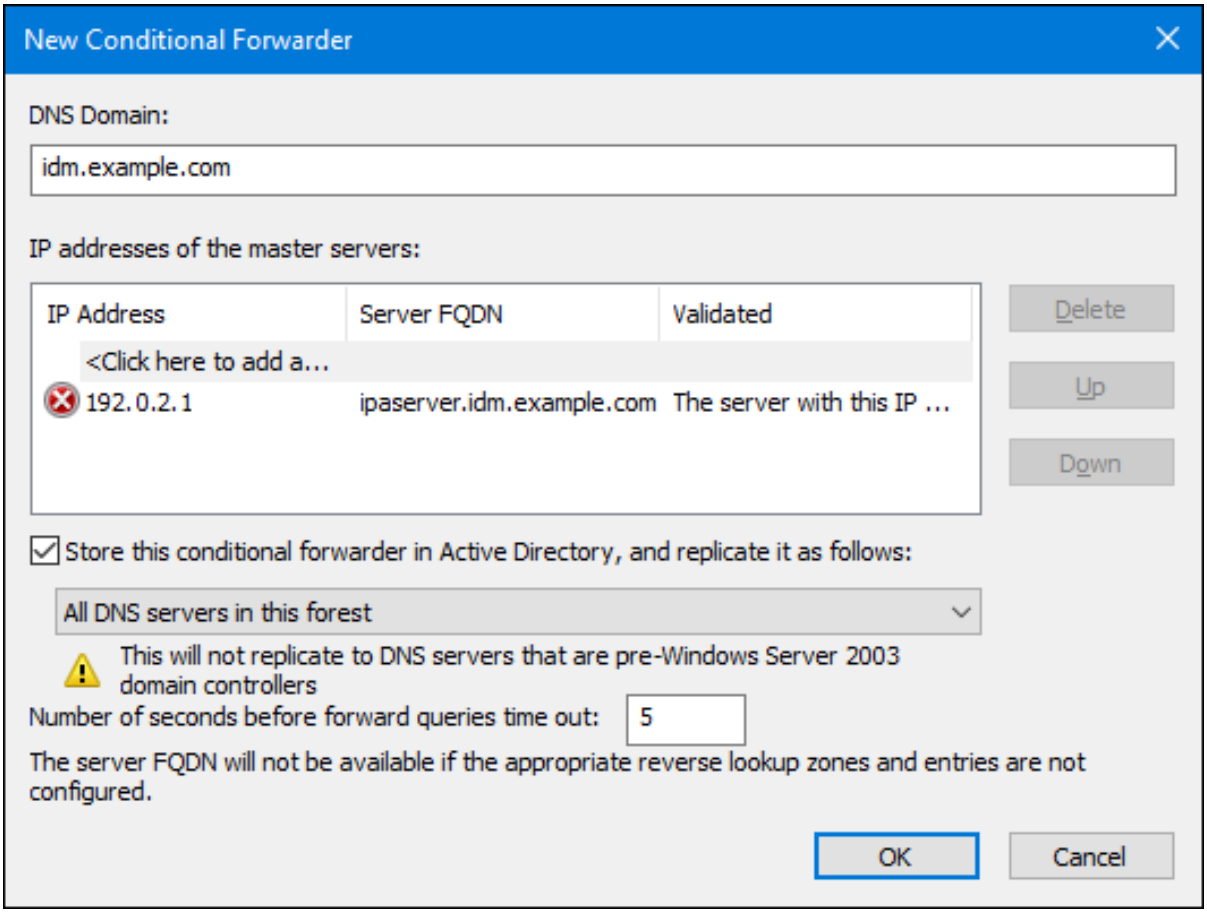
5.2.1.6. クロック設定

Active Directory サーバーおよび IdM サーバーの両方で、クロックが同期されている必要があります。

5.2.1.7. AD での IdM ドメインへの条件付きフォワーダーの作成

AD DNS サーバーを準備して、IdM ドメインのクエリーを IdM DNS サーバーに転送します。

1. Windows AD ドメインコントローラーで、Active Directory (AD) **DNS** コンソールを開きます。
2. **Conditional Forwarders** を右クリックし、**New Conditional Forwarder** を選択します。
3. IdM DNS ドメイン名および IdM DNS サーバーの IP アドレスを入力します。
4. **Store this conditional forwarder in Active Directory, and replicate it as follows** を選択し、環境に一致するレプリケーション設定を選択します。
5. **OK** をクリックします。



6. AD ドメインコントローラー (DC) が IdM ドメインの DNS エントリーを解決できるようにするには、コマンドプロンプトを開いて以下を入力します。

```
C:\> nslookup server.idm.example.com
```

コマンドが IdM サーバーの IP アドレスを返すと、条件フォワーダーが正しく機能しています。

5.2.1.8. IdM での AD ドメインの正引きゾーンの作成

IdM DNS サーバーを準備して、AD ドメインのクエリーを AD DNS サーバーに転送します。

1. IdM サーバーで、AD DNS ドメインの正引きゾーンエントリーを作成します。IdM で DNS 正引きゾーンを作成する方法の詳細については、『Linux ドメイン ID、認証、およびポリシーガイド』 の 『正引きゾーンの設定』 セクションを参照してください。

2. AD DNS サーバーが DNSSEC をサポートしていない場合は、IdM サーバーで DNSSEC 検証を無効にします。

   a. **/etc/named.conf** ファイルを編集し、***dnssec-validation*** パラメーターを **no** に設定します。

   ```
   dnssec-validation no;
   ```

   b. **named-pkcs11** サービスを再起動します。

   ```
   # systemctl restart named-pkcs11
   ```

3. IdM サーバーが AD ドメインの DNS エントリーを解決できるようにするには、次のコマンドを実行します。

```
# host server.ad.example.com
```

コマンドが AD DC の IP アドレスを返すと、正引きゾーンは正しく機能します。

5.2.1.9. サポートされるユーザー名の形式

IdM は、ローカルの SSSD クライアントでユーザー名マッピングを実行します。SSSD がサポートする信頼されるドメインのユーザーのデフォルトの出力ユーザー名の形式は **user_name@domain** です。Active Directory は、**user_name**、**user_name@DOMAIN_NAME**、および **DOMAIN_NAME\user_name** のさまざまな名前形式をサポートします。

ユーザーは、ユーザー名 (**user_name**) または完全修飾ユーザー名 (**user_name@domain_name**) のいずれかを使用してシステムに対して認証することもできます。

警告

同じユーザー名が複数のドメインに存在する場合の競合を避けるために、完全修飾ユーザー名を使用することが推奨されます。

ユーザーがドメインなしでユーザー名のみを指定した場合、SSSD は **/etc/sssd/sssd.conf** ファイルで設定されたすべてのドメインと信頼されたドメインでアカウントを検索します。「IdM クライアントでのドメイン解決順の設定」 で説明されているように、ドメインの解決順序を設定すると、SSSD は定義された順序でユーザーを検索します。いずれの場合も、SSSD は、見つかった最初のエントリーを使用します。同じユーザー名が複数のドメインに存在し、最初に見つかったエントリーが予期されたものではない場合、これは問題や混乱を引き起こす可能性があります。

デフォルトでは、SSSD はユーザー名を常に完全修飾形式で表示します。形式の変更に関する詳細は、「SSSD が表示するユーザー名の形式の変更」 を参照してください。

ユーザー名とそのユーザー名が属するドメインを特定するために、SSSD は ***re_expression*** オプションで定義された正規表現を使用します。IdM バックエンドまたは AD バックエンドには正規表現を使用し、上記のすべての形式をサポートします。

```
re_expression = (((?P<domain>[^\\]+)\\(?P<name>.+$))|((?P<name>[^@]+)@(?P<domain>.+$))|(^(?P<name>[^@\\]+)$))
```

5.2.2. 信頼の作成

以下のセクションでは、さまざまな設定シナリオでの信頼の作成を説明します。「コマンドラインからの信頼の作成」 は、コマンドラインから信頼を設定する全手順を説明します。これ以降のセクションでは、この基本設定シナリオとは異なる手順を説明し、他のすべてのステップの基本手順を参照します。

注記

既存の信頼環境でレプリカを設定すると、レプリカは信頼コントローラーとして自動的に設定されません。レプリカを追加の信頼コントローラーとして設定するには、本セクションの手順に従います。

信頼を作成したら、「フォレスト間の信頼に関するインストール後の考慮事項」 を参照してください。

5.2.2.1. コマンドラインからの信頼の作成

IdM と Active Directory Kerberos レルム間に信頼関係を作成するには、以下の手順を行います。

1. 信頼用の IdM サーバーの準備 (「信頼用の IdM サーバーの準備」 を参照)
2. 信頼関係の作成 (「信頼関係の作成」 を参照)
3. Kerberos 設定の確認 (「Kerberos 設定の確認」 を参照)

5.2.2.1.1. 信頼用の IdM サーバーの準備

AD と信頼関係に IdM サーバーを設定するには、以下の手順に従います。

1. 必要な IdM、信頼、Samba パッケージをインストールします。

```
[root@ipaserver ]# yum install ipa-server ipa-server-trust-ad samba-client
```

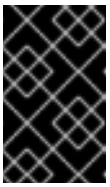
2. 信頼サービスを有効にするように IdM サーバーを設定します。**ipa-replica-install --setup-adtrust** コマンドを使用してサーバーをインストールした場合は、この手順を省略できます。

   a. **ipa-adtrust-install** ユーティリティーを実行します。

   ```
   [root@ipaserver ]# ipa-adtrust-install
   ```

   このユーティリティーは、AD 信頼に必要な DNS サービスレコードを追加します。統合 DNS サーバーとともに IdM がインストールされていると、サービスレコードが自動的に作成されます。

   IdM が統合 DNS サーバーなしでインストールされると、**ipa-adtrust-install** は、続行する前に DNS に手動で追加する必要があるサービスレコードのリストを出力します。

   重要

   Red Hat は、特に IdM または AD が統合 DNS サーバーを使用しない場合に、**ipa-adtrust-install** を実行するたびに 「DNS 設定の確認」 で説明されている DNS 設定を確認することを強く推奨します。

   b. このスクリプトは、従来の Linux クライアントが信頼できるユーザーと連携できるようにする互換性プラグインである **slapi-nis** プラグインを設定するように求めるプロンプトを表示します。

   ```
   Do you want to enable support for trusted domains in Schema Compatibility plugin?
   This will allow clients older than SSSD 1.9 and non-Linux clients to work with trusted
   users.
   ```

```
Enable trusted domains support in slapi-nis? [no]: y
```

c. ディレクトリーを最初にインストールする際に、少なくとも 1 人のユーザー (IdM 管理者) が存在します。SID 生成タスクは、信頼環境をサポートするように既存ユーザーの SID を作成できます。これはリソース集約型タスクであり、多くのユーザーの場合、これは個別に実行できます。

```
Do you want to run the ipa-sidgen task? [no]: yes
```

3. 「DNS およびレルムの設定」 の説明に従って、DNS が適切に設定されていることを確認します。

4. **smb** サービスを起動します。

```
[root@ipaserver ~]# systemctl start smb
```

5. 必要に応じて、システムの起動時に **smb** サービスが自動的に起動するようにします。

```
[root@ipaserver ~]# systemctl enable smb
```

6. **smbclient** ユーティリティーを使用して、Samba が IdM からの Kerberos 認証に応答することを確認します。

```
[root@ipaserver ~]# smbclient -L ipaserver.ipa.example.com -k
lp_load_ex: changing to config backend registry

 Sharename       Type      Comment
 ---------       ----      -------
 IPC$            IPC       IPC Service (Samba 4.9.1)
Reconnecting with SMB1 for workgroup listing.

 Server               Comment
 ---------            -------

 Workgroup            Master
 ---------            -------
```

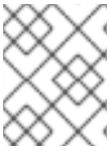
5.2.2.1.2. 信頼関係の作成

ipa trust-add コマンドを使用して、Active Directory ドメインと IdM ドメインに信頼関係を作成します。

```
# ipa trust-add --type=type ad_domain_name --admin ad_admin_username --password
```

ipa trust-add コマンドは、デフォルトで一方向の信頼を設定します。RHEL 7 で双方向の信頼を確立することはできません。

外部信頼を確立するには、**--external=true** オプションを **ipa trust-add** コマンドに渡します。詳細は 「Active Directory への外部信頼」 を参照してください。



注記

ipa trust-add コマンドは、デフォルトでサーバーを信頼コントローラーとして設定します。詳細は 「信頼コントローラーおよび信頼エージェント」 を参照してください。

以下の例では、**--two-way=true** オプションを使用して双方向の信頼を確立します。

```
[root@ipaserver ~]# ipa trust-add --type=ad ad.example.com --admin Administrator --password --
two-way=true
Active Directory domain administrator's password:
----------------------------------------------------------
Added Active Directory trust for realm "ad.example.com"
----------------------------------------------------------
  Realm-Name: ad.example.com
  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
  SID blacklist incoming: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-1-5-7, S-1-5-6, S-1-5-5, S-1-5-4, S-1-
5-9, S-1-5-8, S-1-5-17, S-1-5-16, S-1-5-15, S-1-5-14, S-1-5-13, S-1-5-12, S-1-5-11, S-1-5-10, S-1-3,
S-1-2, S-1-1, S-1-0, S-1-5-19,
                      S-1-5-18
  SID blacklist outgoing: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-1-5-7, S-1-5-6, S-1-5-5, S-1-5-4, S-1-
5-9, S-1-5-8, S-1-5-17, S-1-5-16, S-1-5-15, S-1-5-14, S-1-5-13, S-1-5-12, S-1-5-11, S-1-5-10, S-1-3,
S-1-2, S-1-1, S-1-0, S-1-5-19,
                      S-1-5-18
  Trust direction: Two-way trust
  Trust type: Active Directory domain
  Trust status: Established and verified
```

5.2.2.1.3. Kerberos 設定の確認

Kerberos 設定を確認するには、IdM ユーザーのチケットを取得できるかどうか、および IdM ユーザーがサービスチケットを要求できるかどうかを検証します。

双方向の信頼を確認するには、以下を実行します。

1. IdM ユーザーのチケットを要求します。

   ```
   [root@ipaserver ~]# kinit user
   ```

2. IdM ドメイン内のサービスのサービスチケットを要求します。

   ```
   [root@ipaserver ~]# kvno -S host ipaserver.example.com
   ```

3. AD ドメイン内のサービスのサービスチケットを要求します。

   ```
   [root@ipaserver ~]# kvno -S cifs adserver.example.com
   ```

   AD サービスチケットが正常に許可されると、その他の要求されたすべてのチケットと共に記載されたレルム間の TGT (Ticket-Granting Ticket) があります。TGT の名前は、**krbtgt/*AD.DOMAIN@IPA.DOMAIN*** です。

   ```
   [root@ipaserver ]# klist
   Ticket cache: FILE:/tmp/krb5cc_0
   ```

```
Default principal: user@IPA.DOMAIN

Valid starting     Expires            Service principal
06/15/12 12:13:04  06/16/12 12:12:55  krbtgt/IPA.DOMAIN@IPA.DOMAIN
06/15/12 12:13:13  06/16/12 12:12:55  host/ipaserver.ipa.example.com@IPA.DOMAIN
06/15/12 12:13:23 06/16/12 12:12:55 krbtgt/AD.DOMAIN@IPA.DOMAIN
06/15/12 12:14:58  06/15/12 22:14:58  cifs/adserver.ad.example.com@AD.DOMAIN
```

IdM 側から一方向の信頼を確認するには、次のコマンドを実行します。

1. Active Directory ユーザーのチケットを要求します。

```
[root@ipaserver ~]# kinit user@AD.DOMAIN
```

2. IdM ドメイン内のサービスのサービスチケットを要求します。

```
[root@ipaserver ~]# kvno -S host ipaserver.example.com
```

AD サービスチケットが正常に許可されると、その他の要求されたすべてのチケットと共に記載されたレルム間の TGT (Ticket-Granting Ticket) があります。TGT の名前は、**krbtgt/*IPA.DOMAIN@AD.DOMAIN*** です。

```
[root@ipaserver ]# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_hRtox00
Default principal: user@AD.DOMAIN

Valid starting       Expires              Service principal
03.05.2016 18:31:06  04.05.2016 04:31:01  host/ipaserver.ipa.example.com@IPA.DOMAIN
 renew until 04.05.2016 18:31:00
03.05.2016 18:31:06 04.05.2016 04:31:01 krbtgt/IPA.DOMAIN@AD.DOMAIN
 renew until 04.05.2016 18:31:00
03.05.2016 18:31:01  04.05.2016 04:31:01  krbtgt/AD.DOMAIN@AD.DOMAIN
 renew until 04.05.2016 18:31:00
```

localauth プラグインは、Kerberos プリンシパルをローカルの SSSD ユーザー名にマッピングします。これにより、AD ユーザーは Kerberos 認証を使用し、GSSAPI 認証に対応する Linux サービスに直接アクセスできます。

注記

プラグインの詳細は、「パスワードなしでの SSH の使用」 を参照してください。

5.2.2.2. 共有シークレットを使用した信頼の作成

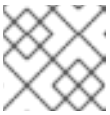
共有シークレットは、信頼できるピアが認識するパスワードで、他のドメインが信頼に参加するために使用できます。共有シークレットは、Active Directory (AD) 内で一方向と双方向の信頼の両方を設定できます。AD では、共有シークレットは信頼設定内に *信頼できるドメインオブジェクト* (TDO) として保存されます。

IdM は、AD 管理者の認証情報の代わりに、共有シークレットを使用して一方向または双方向の信頼を作成します。このような信頼を設定するには、管理者が AD に共有シークレットを作成し、AD 側で信頼を手動で検証する必要があります。

5.2.2.2.1. 共有シークレットを使用した 2 つの信頼の作成

Microsoft Windows Server 2012、2012 R2、または 2016 で共有シークレットとの双方向の信頼を作成するには、以下を実行します。

1. 「信頼用の IdM サーバーの準備」 の説明に従って、信頼用に IdM サーバーを準備します。
2. IdM ホストおよび AD ホストが、両方のドメインを解決できない DNS サーバーを使用する場合は、DNS ゾーンの転送を設定します。
   a. AD DNS サーバーを準備して、IdM ドメインのクエリーを IdM DNS サーバーに転送します。詳細は 「AD での IdM ドメインへの条件付きフォワーダーの作成」 を参照してください。
   b. AD ドメインのクエリーを AD DNS サーバーに転送するため、IdM DNS サーバーを準備します。詳細は 「IdM での AD ドメインの正引きゾーンの作成」 を参照してください。
3. **Active Directory** ドメインおよび信頼 コンソールで信頼を設定します。特に以下が含まれます。
   - 新しい信頼を作成します。
   - IdM ドメイン名 (例: **idm.example.com**) に信頼を付与します。
   - これは、信頼の フォレスト タイプであることを指定します。
   - これは **2** 方向 の信頼タイプであることを指定します。
   - これは、フォレスト全体 の認証であることを指定します。
   - 信頼パスワード を設定します。

   注記

   IdM で信頼を設定する場合は、同じパスワードを使用する必要があります。

   受信トラストを確認するように求められたら、**No** を選択します。
4. 「信頼関係の作成」 で説明されているように、信頼関係を作成します。**ipa trust-add** コマンドの実行時に、**--type** オプション、**--trust-secret** オプション、および **--two-way=True** オプションを使用し、**--admin** オプションを省略します。以下に例を示します。

```
[root@ipaserver ~]# ipa trust-add --type=ad ad.example.com --trust-secret --two-way=True
Shared secret for the trust:
----------------------------------------------------
Added Active Directory trust for realm "ad.example.com"
----------------------------------------------------
  Realm-Name: ad.example.com
  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
  SID blacklist incoming: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-1-5-7, S-1-5-6,
                          S-1-5-5, S-1-5-4, S-1-5-9, S-1-5-8, S-1-5-17, S-1-5-16,
                          S-1-5-15, S-1-5-14, S-1-5-13, S-1-5-12, S-1-5-11,
                          S-1-5-10, S-1-3, S-1-2, S-1-1, S-1-0, S-1-5-19, S-1-5-18
  SID blacklist outgoing: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-1-5-7, S-1-5-6,
                          S-1-5-5, S-1-5-4, S-1-5-9, S-1-5-8, S-1-5-17, S-1-5-16,
```

```
                S-1-5-15, S-1-5-14, S-1-5-13, S-1-5-12, S-1-5-11,
                S-1-5-10, S-1-3, S-1-2, S-1-1, S-1-0, S-1-5-19, S-1-5-18
Trust direction: Trusting forest
Trust type: Active Directory domain
Trust status: Waiting for confirmation by remote side
```

5. ドメインの一覧を取得します。

```
[root@ipaserver ~]# ipa trust-fetch-domains ad_domain
```

6. IdM サーバーで、**ipa trust-show** コマンドを使用して信頼関係が確立されていることを確認します。

```
[root@ipaserver ~]# ipa trust-show ad.example.com

  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
  Trust direction: Trusting forest
  Trust type: Active Directory domain
```

7. 必要に応じて、信頼されたドメインを検索します。

```
[root@ipaserver ~]# ipa trustdomain-find ad.example.com
Domain name: ad.example.com
Domain NetBIOS name: AD
Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
Domain enabled: True
```

8. 「Kerberos 設定の確認」 の説明に従って、Kerberos 設定を確認します。

5.2.2.2.2. 共有シークレットを使用した一方向信頼の作成

Microsoft Windows Server 2012、2012 R2、または 2016 で共有のシークレットを使用して一方向の信頼を作成するには、以下を実行します。

1. 「信頼用の IdM サーバーの準備」 の説明に従って、信頼用に IdM サーバーを準備します。
2. IdM ホストおよび AD ホストが、両方のドメインを解決できない DNS サーバーを使用する場合は、DNS ゾーンの転送を設定します。
   a. AD DNS サーバーを準備して、IdM ドメインのクエリーを IdM DNS サーバーに転送します。詳細は 「AD での IdM ドメインへの条件付きフォワーダーの作成」 を参照してください。
   b. AD ドメインのクエリーを AD DNS サーバーに転送するため、IdM DNS サーバーを準備します。詳細は 「IdM での AD ドメインの正引きゾーンの作成」 を参照してください。
3. **Active Directory** ドメインおよび信頼 コンソールで信頼を設定します。
   a. ドメイン名を右クリックし、**Properties** を選択します。
   b. **Trusts** タブで、**New Trust** をクリックします。
   c. IdM ドメイン名を入力し、**Next** をクリックします。

d. **Forest trust** を選択し、**Next** をクリックします。

e. **One-way: incoming** を選択し、**Next** をクリックします。

f. **This domain only** を選択し、**Next** をクリックします。

g. 共有シークレット (信頼パスワード) を入力し、**Next** をクリックします。

h. 設定を確認し、**Next** をクリックします。

i. 受信信頼を確認するかどうかをシステムが尋ねる場合には、**No, do not confirm the incoming trust** を選択し、**Next** をクリックします。

j. **Finish** をクリックします。

4. 信頼関係を作成します。

```
[root@ipaserver ~]# ipa trust-add --type=ad --trust-secret ad.example.com
Shared secret for the trust: password
----------------------------------------------------------
Added Active Directory trust for realm "ad.example.com"
----------------------------------------------------------
  Realm name: ad.example.com
  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-1762709870-351891212-3141221786
  Trust direction: Trusting forest
  Trust type: Active Directory domain
  Trust status: Waiting for confirmation by remote side
```

AD ドメインおよび信頼コンソールに設定した共有シークレットを入力します。

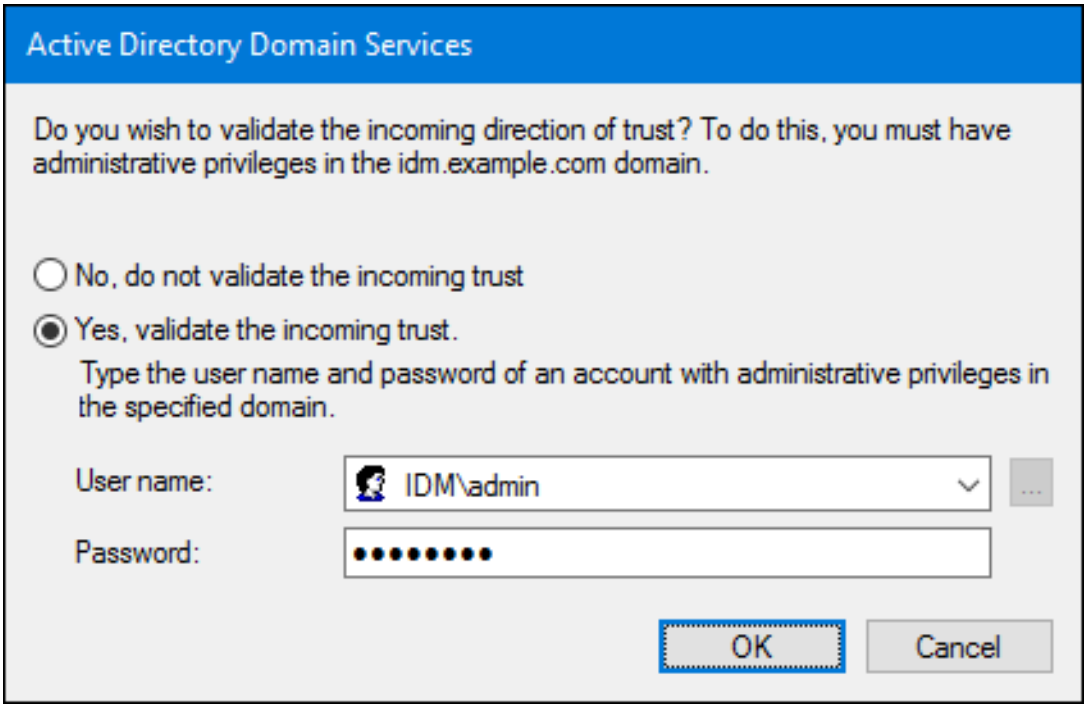
5. **Active Directory Domains and Trusts** コンソールで信頼を検証します。

a. ドメイン名を右クリックし、**Properties** を選択します。

b. **Trusts** タブで、**Domains that trust this domain (incoming trusts) pane** のドメインを選択し **Properties** をクリックします。

c. **Validate** ボタンをクリックします。

d. **Yes, validate the incoming trust** を選択し、IdM *admin* ユーザーの認証情報を入力します。



6. 信頼済みドメインの一覧を更新します。

```
[root@ipaserver ~]# ipa trust-fetch-domains ad.example.com
--------------------------------------------------------------------------------
List of trust domains successfully refreshed. Use trustdomain-find command to list them.
--------------------------------------------------------------------------------
----------------------------
Number of entries returned 0
----------------------------
```

7. 信頼済みドメインを一覧表示します。

```
[root@ipaserver ~]# ipa trustdomain-find ad.example.com
  Domain name: ad.example.com
  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-1762709870-351891212-3141221786
  Domain enabled: True
----------------------------
Number of entries returned 1
----------------------------
```

8. 必要に応じて、IdM サーバーが AD ドメインからユーザー情報を取得できることを確認します。

```
[root@ipaserver ~]# getent passwd administrator@ad.example.com
administrator@ad.example.com:*:610600500:610600500:Administrator:/home/ad.example.com/administrator:
```

5.2.2.3. ID マッピングの確認

ID マッピングを確認するには、次のコマンドを実行します。

1. Windows Active Directory ドメインコントローラー (DC) で以下のコマンドを実行して、最高の ID を一覧表示します。

```
C:\> dcdiag /v /test:ridmanager /s:ad.example.com
...
Available RID Pool for the Domain is 1600 to 1073741823
...
```

2. IdM サーバーの ID 範囲を一覧表示します。

```
[root@ipaserver ~]# ipa idrange-find
----------------
1 range matched
----------------
  Range name: AD.EXAMPLE.COM_id_range
  First Posix ID of the range: 610600000
  Number of IDs in the range: 200000
  First RID of the corresponding RID range: 0
  Domain SID of the trusted domain: S-1-5-21-796215754-1239681026-23416912
  Range type: Active Directory domain range
----------------------------
Number of entries returned 1
----------------------------
```

後の手順で最初の POSIX ID 値が必要です。

3. Active Directory DC で、セキュリティー識別子 (SID) またはユーザーを表示します。たとえば、管理者 の SID を表示するには、次のコマンドを実行します。

```
C:\> wmic useraccount where name="administrator" get sid
S-1-5-21-796215754-1239681026-23416912-500
```

SID の最後の部分は、相対識別子 (RID) です。次の手順では、ユーザーの RID が必要です。

注記

RID がデフォルトの ID 範囲 (200000) より大きい場合は、**ipa idrange-mod** コマンドを使用して範囲を拡張します。以下に例を示します。

```
# ipa idrange-mod --range-size=1000000 AD.EXAMPLE.COM_id_range
```

4. IdM サーバーで同じユーザーのユーザー ID を表示します。

```
[root@ipaserver ~]# id ad\\administrator
uid=610600500(administrator@ad.example.com)...
```

5. 最初の POSIX ID 値 (610600000) を RID (500) に追加する場合、IdM サーバー (610600500) で表示されるユーザー ID と一致する必要があります。

5.2.2.4. 既存の IdM インスタンスへの信頼の作成

既存の IdM インスタンスに信頼を設定する場合は、IdM サーバーおよびそのドメインのエントリーに対する特定の設定がすでに設定されています。ただし、Active Directory ドメインの DNS 設定を設定し、Active Directory SID を、既存のすべての IdM ユーザーおよびグループに割り当てる必要があります。

1. 「信頼用の IdM サーバーの準備」 の説明に従って、信頼用に IdM サーバーを準備します。

2. 「信頼関係の作成」 で説明されているように、信頼関係を作成します。

3. IdM ユーザーごとに SID を生成します。

注記

信頼を確立するために **ipa-adtrust-install** ユーティリティーを使用したときに SID が生成されている場合は、この手順を実行しないでください。

a. バックエンド LDAP ディレクトリーで **ipa-sidgen-task** 操作を実行することにより、SID を含む新しい ***ipaNTSecurityIdentifier*** 属性を各エントリーに自動的に追加します。

```
[root@ipaserver ]# ldapmodify -x -H ldap://ipaserver.ipa.example.com:389 -D
"cn=directory manager" -w password

dn: cn=sidgen,cn=ipa-sidgen-task,cn=tasks,cn=config
changetype: add
objectClass: top
objectClass: extensibleObject
cn: sidgen
nsslapd-basedn: dc=ipadomain,dc=com
delay: 0

adding new entry "cn=sidgen,cn=ipa-sidgen-task,cn=tasks,cn=config"
```

b. タスクが正常に完了したら、SID 生成タスク (**Sidgen** タスク) がゼロ (0) のステータスで終了したエラーログにメッセージが記録されます。

```
[root@ipaserver ]# grep "sidgen_task_thread" /var/log/dirsrv/slapd-IDM-EXAMPLE-
COM/errors
[20/Jul/2012:18:17:16 +051800] sidgen_task_thread - [file ipa_sidgen_task.c, line 191]:
Sidgen task starts ...
[20/Jul/2012:18:17:16 +051800] sidgen_task_thread - [file ipa_sidgen_task.c, line 196]:
Sidgen task finished [0].
```

4. 「Kerberos 設定の確認」 の説明に従って、Kerberos 設定を確認します。

5.2.2.5. 2 番目の信頼の追加

すでに信頼関係が設定されている IdM サーバーに信頼を追加する場合は、信頼関連のパッケージのインストールや SID の設定など、一般的な IdM 信頼設定は不要になりました。信頼を追加するには、DNS を設定し、信頼関係を確立する必要があります。

1. 「DNS およびレルムの設定」 の説明に従って、DNS が適切に設定されていることを確認します。

2. 「信頼関係の作成」 で説明されているように、信頼関係を作成します。

5.2.2.6. Web UI で信頼の作成

Web UI で信頼を作成する前に、信頼用に IdM サーバーを準備してください。この信頼設定は、「信頼用の IdM サーバーの準備」 で説明されているようにコマンドラインから実行する最も簡単な方法です。

初期設定を設定すると、IdM Web UI に信頼関係を追加できます。

1. IdM Web UI を開きます。

   https://*ipaserver.example.com*

2. **IPA Server** メインタブを開き、**Trusts** サブタブを選択します。

3. **Trusts** サブタブの **Add** をクリックして、新しい信頼設定ウィンドウを開きます。

4. 信頼に必要な情報を入力します。

   a. **Domain** フィールドに AD ドメイン名を指定します。

   b. 信頼を双方向に設定するには、**Two-way trust** チェックボックスを選択します。信頼を一方向として設定する場合は、**Two-way trust** は選択されていません。

      一方向および双方向の信頼に関する詳細情報は、「一方向および双方向の信頼」 を参照してください。

   c. 別のフォレストでドメインへの外部の信頼を確立するには、**External Trust** チェックボックスを選択します。

      詳細は、「Active Directory への外部信頼」 を参照してください。

   d. **Establish using** セクションは、信頼の確立方法を定義します。

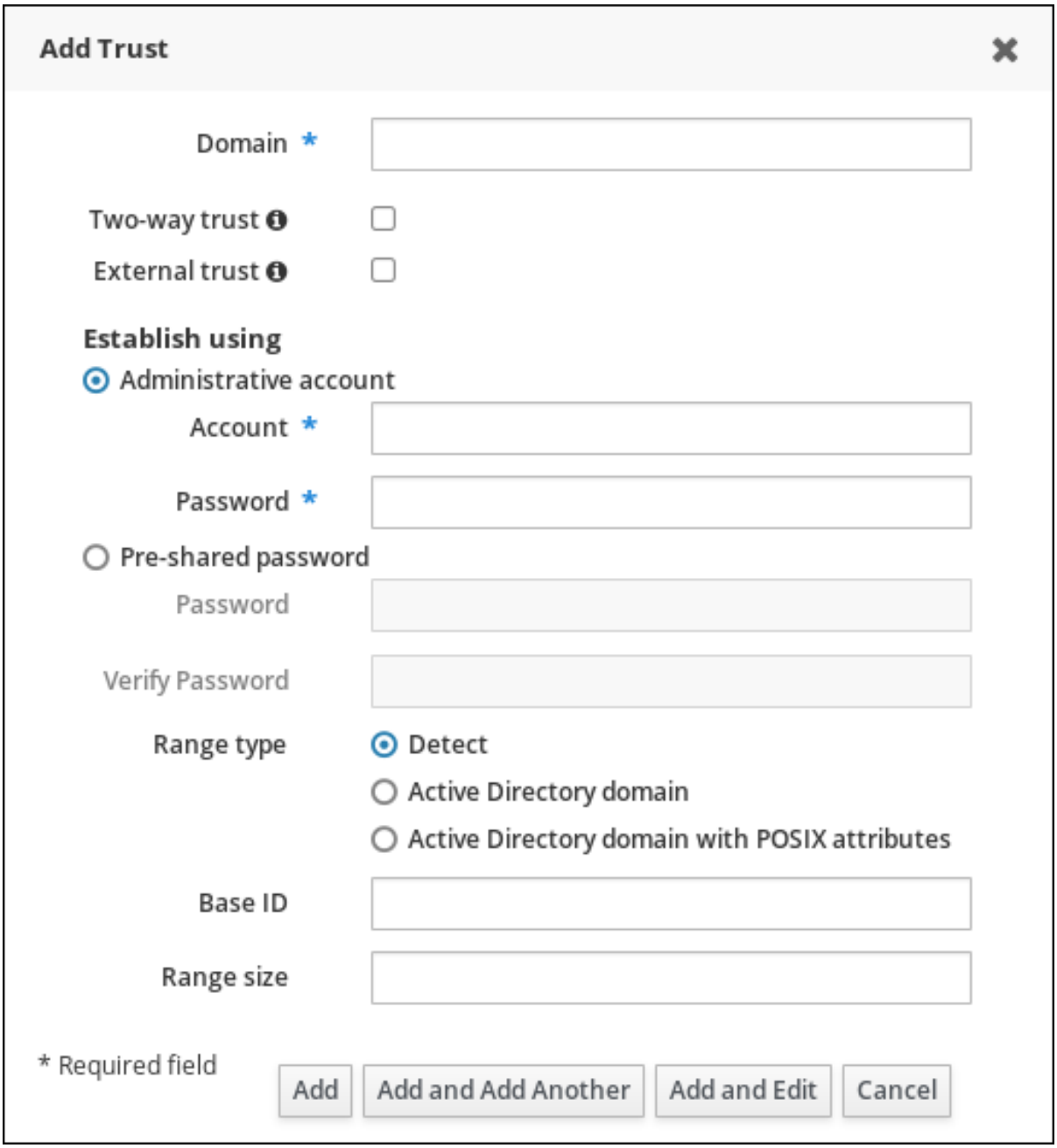
      - AD 管理者のユーザー名およびパスワードを使用して信頼を確立するには、**Administrative account** を選択して必要な認証情報を指定します。
      - 共有パスワードで信頼を確立するには、**Pre-shared password** を選択して、信頼パスワードを指定します。

   e. 信頼の ID 設定を定義します。

      - **Range type** オプションでは、ID 範囲タイプを選択できます。IdM が、使用する ID 範囲の種類を自動的に検出させるには、**Detect** を選択します。
      - ID 範囲の開始 ID を定義するには、**Base ID** フィールドを使用します。ID 範囲のサイズを定義するには、**Range size** フィールドを使用します。IdM で ID 範囲のデフォルト値を使用する場合は、このオプションを指定しないでください。

      ID 範囲の詳細は、「ID 範囲」 を参照してください。

図5.5 Web UI で信頼の追加



5. **Add** をクリックして、新しい信頼を保存します。

その後、「Kerberos 設定の確認」 の説明に従って Kerberos 設定を確認します。

5.2.3. フォレスト間の信頼に関するインストール後の考慮事項

5.2.3.1. Active Directory 信頼で潜在的な動作の問題

5.2.3.1.1. Active Directory ユーザーおよび IdM の管理

現在、Active Directory (AD) ユーザーおよび管理者は、IdM Web UI にログインした後にそのセルフサービスページのみを確認できます。AD 管理者は、IdM Web UI の管理者ビューにアクセスできません。詳細は、『Linux Domain Identity、Authentication、and Policy Guide 』 の Authenticating to IdM Web UI as an AD User のセクションを参照してください。

また、現在、AD ユーザーは独自の ID オーバーライドを管理できません。ID オーバーライドを追加および管理できるのは、IdM ユーザーのみです。

5.2.3.1.2. 削除された Active Directory ユーザーの認証

デフォルトでは、すべての IdM クライアントは SSSD サービスを使用して、ユーザー ID および認証情報をキャッシュします。IdM または AD バックエンドプロバイダーが一時的に利用できなくなると、SSSD により、ローカルシステムが、正常にログインしたユーザーのアイデンティティーを参照できます。

SSSD はユーザーの一覧をローカルに維持するため、バックエンドで加えられた変更は SSSD をオフラインで実行しているクライアントに即座に表示されないことがあります。このようなクライアントでは、IdM リソースにログインし、ハッシュ化されたパスワードが SSSD キャッシュに格納されているユーザーは、AD でユーザーアカウントが削除されても再度ログインできます。

上記の条件が満たされると、ユーザー ID が SSSD にキャッシュされ、ユーザーアカウントが AD から削除された場合でも、AD ユーザーは IdM リソースにログインできます。この問題は、SSSD がオンラインになり、AD ドメインコントローラーに対して AD ユーザーログオンを検証できるまで持続します。

クライアントシステムが SSSD をオンラインで実行している場合は、ユーザーが提供するパスワードが AD ドメインコントローラーにより検証されます。これにより、削除した AD ユーザーがログインできなくなります。

5.2.3.1.3. 認証情報キャッシュコレクションおよび Active Directory プリンシパルの選択

Kerberos 認証情報キャッシュは、次の識別子に基づいて、クライアントプリンシパルとサーバープリンシパルを以下の順序で照合しようとします。

1. サービス名
2. ホスト名
3. レルム名

クライアントとサーバーのマッピングがホスト名または実際の名前および認証情報のキャッシュコレクションが使用されると、AD ユーザーとしてバインディングで予期しない動作が発生する可能性があります。これは、Active Directory ユーザーのレルム名は IdM システムのレルム名とは異なるためです。

AD ユーザーが **kinit** ユーティリティーを使用してチケットを取得し、SSH を使用して IdM リソースに接続すると、リソースチケットにプリンシパルが選択されません。IdM プリンシパルはリソースのレルム名と一致するため、IdM プリンシパルが使用されます。

たとえば、AD ユーザーが **Administrator** で、ドメインが **ADEXAMPLE.ADREALM** の場合、プリンシパルは **Administrator@ADEXAMPLE.ADREALM** になります。

```
[root@server ~]# kinit Administrator@ADEXAMPLE.ADREALM
Password for Administrator@ADEXAMPLE.ADREALM:
[root@server ~]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: Administrator@ADEXAMPLE.ADREALM

Valid starting       Expires              Service principal
27.11.2015 11:25:23  27.11.2015 21:25:23
krbtgt/ADEXAMPLE.ADREALM@ADEXAMPLE.ADREALM
 renew until 28.11.2015 11:25:16
```

これは、Active Directory チケットキャッシュのデフォルトプリンシパルとして設定されます。ただし、IdM ユーザーに Kerberos チケット (**admin** など) がある場合は、IdM のデフォルトプリンシパルに別の IdM 認証情報キャッシュがあります。Active Directory ユーザーが SSH を使用してリソースに接続する場合は、その IdM デフォルトプリンシパルがホストチケットに対して選択されます。

```
[root@vm-197 ~]# ssh -l Administrator@adexample.adrealm ipaclient.example.com
Administrator@adexample.adrealm@ipaclient.example.com's password:

[root@vm-197 ~]# klist -A
Ticket cache: KEYRING:persistent:0:0
Default principal: Administrator@ADEXAMPLE.ADREALM

Valid starting       Expires              Service principal
27.11.2015 11:25:23  27.11.2015 21:25:23
krbtgt/ADEXAMPLE.ADREALM@ADEXAMPLE.ADREALM
 renew until 28.11.2015 11:25:16

Ticket cache: KEYRING:persistent:0:0
Default principal: admin@EXAMPLE.COM >>>>> IdM user

Valid starting       Expires              Service principal
27.11.2015 11:25:18  28.11.2015 11:25:16  krbtgt/EXAMPLE.COM@EXAMPLE.COM
27.11.2015 11:25:48 28.11.2015 11:25:16 host/ipaclient.example.com@EXAMPLE.COM >>>>> host
principal
```

これは、IdM プリンシパルのレルム名が IdM リソースのレルムと一致するためです。

5.2.3.1.4. グループ SID の解決

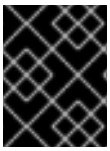
Kerberos チケットの損失
コマンドを実行して、Samba サービス (**net getlocalsid**、**net getdomainsid** など) から SID を取得し、既存の admin チケットを Kerberos キャッシュから削除します。

注記

Active Directory 信頼を使用するには、**net getlocalsid**、net **getdomainsid** などのコマンドを実行する必要はありません。

ユーザーのグループメンバーシップを確認できない
特定の信頼されるユーザーが特定の IdM グループ、外部、または POSIX に関連付けられていることを確認できません。

Active Directory ユーザー用に、リモート Active Directory グループメンバーを表示できません。



重要

IdM サーバーおよびクライアントが Red Hat Enterprise Linux 7.1 以降で実行している場合は、この問題が発生しなくなりました。

id ユーティリティーを使用すると、Linux システムユーザーのローカルグループの関連付けを表示できます。ただし、Samba ツールが表示されていても、**id** は Active Directory ユーザーの Active Directory グループのメンバーシップは表示されません。

これを回避するには、**ssh** ユーティリティーを使用して、指定の AD ユーザーとして IdM クライアントマシンにログインできます。AD ユーザーが初めてログインすると、**id** 検索は AD グループメンバーシップを検出し、表示します。

```
[root@ipaserver ~]# id ADDOMAIN\user
uid=1921801107(user@ad.example.com) gid=1921801107(user@ad.example.com)
groups=1921801107(user@ad.example.com),129600004(ad_users),1921800513(domain
users@ad.example.com)
```

5.2.3.2. 信頼エージェントの設定

信頼環境で新しいレプリカを設定した後に、レプリカには **AD** 信頼エージェントロール が自動的にインストールされません。レプリカを信頼エージェントとして設定するには、以下を実行します。

1. 既存の信頼コントローラーで、**ipa-adtrust-install --add-agents** コマンドを実行します。

   ```
   [root@existing_trust_controller]# ipa-adtrust-install --add-agents
   ```

   このコマンドは、対話型設定セッションを開始し、エージェントの設定に必要な情報の入力を求めます。

   --add-agents オプションの詳細は、ipa-adtrust-install(1) の man ページを参照してください。

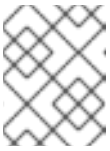
2. 新しいレプリカでは、次を実行します。

   a. IdM サービスを再起動します。

   ```
   [root@new_trust_controller]# ipactl restart
   ```

   b. SSSD キャッシュからエントリーをすべて削除します。

   ```
   [root@new_trust_controller]# sssctl cache-remove
   ```

   注記

   sssctl コマンドを使用するには、sssd-tools パッケージをインストールする必要があります。

   c. 必要に応じて、レプリカに **AD** 信頼エージェント ロールがインストールされていることを確認します。

   ```
   [root@new_trust_controller]# ipa server-show new_replica.idm.example.com
   ...
   Enabled server roles: CA server, NTP server, AD trust agent
   ```

5.3. フォレスト間の信頼環境の管理および設定

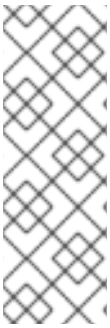
5.3.1. 信頼されているドメイン環境でのユーザープリンシパル名

IdM は、ユーザープリンシパル名 (UPN) を使用したログインをサポートします。UPN は、認証するユーザー名の代替で、形式は **username@KERBEROS-REALM** です。Active Directory フォレストで

は、追加の UPN 接尾辞を設定できます。これらのエンタープライズプリンシパル名は、別のログインをデフォルトの UPN に提供するために使用されます。

たとえば、ある会社が **AD.EXAMPLE.COM** Kerberos レルムを使用する場合に、ユーザーのデフォルトの UPN は **user@ad.example.com** です。ただし、多くの場合、ユーザーが **user@example.com** などのメールアドレスを使用してログインできるようにする必要があります。この場合、管理者は追加の UPN 接尾辞 **example.com** を Active Directory フォレストに追加し、ユーザーのアカウントプロパティーに新しい接尾辞を設定します。

UPN 接尾辞は、AD フォレストルートで定義された場合に IdM にだけ表示されます。AD 管理者は、**Active Directory Domain and Trust** ユーティリティーまたは **PowerShell** コマンドラインツールで UPN を定義できます。



注記

Red Hat は、ユーザーへの UPN 接尾辞の設定には、**Active Directory Domain and Trust** ユーティリティーなどのエラー検証を実行するツールを使用することを推奨します。

Active Directory ではこのような操作は検証されないため、**ldapmodify** コマンドを使用してユーザーの **userPrincipalName** 属性を設定するなど、低レベルの変更で UPN を設定することを推奨します。

信頼できる AD フォレストで UPN 接尾辞を追加または削除する場合は、IdM マスターで信頼されるフォレストの情報を更新する必要があります。

```
[root@ipaserver ~]# ipa trust-fetch-domains
Realm-Name: ad.example.com
--------------------------------
No new trust domains were found
--------------------------------
----------------------------
Number of entries returned 0
----------------------------
```

以下を実行して、別の UPN がフェッチされたことを確認します。

```
[root@ipaserver ~]# ipa trust-show
Realm-Name: ad.example.com
  Realm-Name: ad.example.com
  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
  Trust direction: Two-way trust
  Trust type: Active Directory domain
  UPN suffixes: example.com
```

ドメインの UPN 接尾辞は、**cn=*trusted_domain_name*,cn=ad,cn=trusts,dc=idm,dc=example,dc=com** サブツリーの複数値の **ipaNTAdditionalSuffixes** 属性に保存されます。

5.3.2. Active Directory DNS ドメインの IdM クライアント

IdM と Active Directory との間の信頼がある一部の環境では、Active Directory DNS ドメインの一部であるホストに IdM クライアントをインストールできます。ホストは、これにより、Linux に焦点を合わせた IdM の機能の恩恵を受けることができます。

重要

これは推奨される設定ではなく、いくつかの制限があります。Red Hat は、Active Directory が所有する DNS ゾーンとは異なる DNS ゾーンに常に IdM クライアントを展開し、IdM ホスト名を介して IdM クライアントにアクセスすることをお勧めします。

5.3.2.1. IdM クライアントへの Kerberos シングルサインオンは必要ない

Active Directory DNS ドメインに設定された IdM クライアントでは、この IdM ホストのリソースにアクセスするためのパスワード認証のみが利用できます。このシナリオにクライアントを設定するには、以下を実行します。

1. クライアントの System Security Service Daemon (SSSD) が IdM サーバーと通信できるようにするには、IdM クライアントを **--domain=*IPA_DNS_Domain*** オプションを使用してインストールします。

```
[root@idm-client.ad.example.com ~]# ipa-client-install --domain=idm.example.com
```

このオプションは、Active Directory DNS ドメインの SRV レコードの自動検出を無効にします。

2. **/etc/krb5.conf** 設定ファイルの **[domain_realm]** セクションで、Active Directory ドメインの既存のマッピングを見つけます。

```
.ad.example.com = IDM.EXAMPLE.COM
ad.example.com = IDM.EXAMPLE.COM
```

両方の行を、Active Directory DNS ゾーンの Linux クライアントの完全修飾ドメイン名 (FQDN) の IdM レルムへのマッピングエントリーに置き換えます。

```
idm-client.ad.example.com = IDM.EXAMPLE.COM
```

デフォルトのマッピングを置き換えても、Kerberos が Active Directory ドメインの要求を IdM Kerberos Distribution Center (KDC) に送信しないようにします。Kerberos は、SRV DNS レコードを介して自動検出を使用して KDC を見つけます。追加されたホスト **idm-client.ad.example.com** に対してのみ、IdM KDC が設定されます。

注記

IdM が所有する DNS ゾーンにないクライアントのリソースに対して認証することは、ユーザー名とパスワードを使用するだけで済みます。

SSL 証明書の処理
SSL ベースのサービスでは、元 (A/AAAA) のレコードと CNAME レコードの両方が証明書に含まれている必要があるため、すべてのシステムホスト名に対応する dNSName 拡張レコードを持つ証明書が必要です。現在、IdM は、IdM データベース内のオブジェクトをホストする証明書のみを発行します。

シングルサインオンが利用できない説明されたセットアップでは、IdM は、データベースに FQDN のホストオブジェクトをすでに持っており、**certmonger** はこの名前の証明書を要求できます。

■

```
[root@idm-client.ad.example.com ~]# ipa-getcert request -r \
    -f /etc/httpd/alias/server.crt \
    -k /etc/httpd/alias/server.key \
    -N CN=ipa-client.ad.example.com \
    -D ipa-client.ad.example.com \
    -K host/idm-client.ad.example.com@IDM.EXAMPLE.COM \
    -U id-kp-serverAuth
```

certmonger サービスは、**/etc/krb5.keytab** ファイルに保存されているデフォルトのホストキーを使用して、IdM 認証局 (CA) に対して認証を行います。

5.3.2.2. IdM クライアントへの Kerberos シングルサインオンが必要です。

IdM クライアントのリソースにアクセスするために Kerberos シングルサインオンが必要な場合、クライアントは **idm-client.idm.example.com** などの IdM DNS ドメイン内になければなりません。IdM クライアントの A/AAAA レコードを参照する Active Directory DNS ドメインで CNAME レコード **idm-client.ad.example.com** を作成する必要があります。

Kerberos ベースのアプリケーションサーバーの場合、MIT Kerberos は、アプリケーションのキータブで利用可能なホストベースのプリンシパルの受け入れを可能にする方法をサポートします。Kerberos サーバーの対象に使用していた Kerberos プリンシパルに関する厳密なチェックを無効にするには、**/etc/krb5.conf** 設定ファイルの **[libdefaults]** セクションに以下のオプションを設定します。

```
ignore_acceptor_hostname = true
```

SSL 証明書の処理
SSL ベースのサービスでは、元 (A/AAAA) のレコードと CNAME レコードの両方が証明書に含まれている必要があるため、すべてのシステムホスト名に対応する dNSName 拡張レコードを持つ証明書が必要です。現在、IdM は、IdM データベース内のオブジェクトをホストする証明書のみを発行します。

シングルサインオンが利用できない説明されたセットアップでは、IdM は、データベースに FQDN のホストオブジェクトをすでに持っており、**certmonger** はこの名前の証明書を要求できます。

1. 新規ホストオブジェクトを作成します。

   ```
   [root@idm-server.idm.example.com ~]# ipa host-add idm-client.ad.example.com --force
   ```

   ホスト名は CNAME であり、A/AAAA レコードではないため、**--force** オプションを使用します。

2. IdM DNS ホスト名が、IdM データベースの Active Directory ホストエントリーを管理できるようにします。

   ```
   [root@idm-server.idm.example.com ~]# ipa host-add-managedby idm-client.ad.example.com
   \
       --hosts=idm-client.idm.example.com
   ```

この設定では、IdM クライアントは、Active Directory DNS ドメイン内でホスト名に対して dNSName 拡張レコードで SSL 証明書を要求できます。

```
[root@idm-client.idm.example.com ~]# ipa-getcert request -r \
    -f /etc/httpd/alias/server.crt \
    -k /etc/httpd/alias/server.key \
    -N CN=`hostname --fqdn` \
```

```
-D `hostname --fqdn` \
-D idm-client.ad.example.com \
-K host/idm-client.idm.example.com@IDM.EXAMPLE.COM \
-U id-kp-serverAuth
```

5.3.3. Active Directory ユーザーの IdM グループの作成

ユーザーグループは、アクセスパーミッション、ホストベースのアクセス制御、sudo ルール、および IdM ユーザーのその他の制御を設定する必要があります。このグループは、IdM ドメインリソースへのアクセスを許可し、アクセスを制限するものです。

AD ユーザーおよび AD グループの両方を IdM ユーザーグループに直接追加できます。これには、最初に、非 POSIX IdM 外部グループに AD ユーザーまたはグループを追加し、次にローカルの IdM POSIX グループに追加します。これにより、POSIX グループは、AD ユーザーのユーザーおよびロールの管理に使用できます。IdM で非 POSIX グループを処理する原則は、「Active Directory ユーザーおよび Identity Management グループ」 で説明されています。

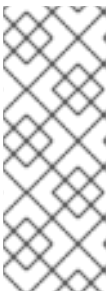
注記

AD ユーザーグループを、IdM 外部グループにメンバーとして追加することもできます。これにより、1 つの AD レルムにユーザーおよびグループの管理を維持することで、Windows ユーザーのポリシーの定義が容易になります。

1. 任意。IdM レルムで AD ユーザーを管理するのに使用する AD ドメインでグループを作成するか、または選択します。IdM 側で複数のグループを使用でき、別のグループに追加できます。

2. **--external** オプションを **ipa group-add** コマンドに追加して、Active Directory ユーザーの IdM ドメインに外部グループを作成します。**--external** オプションは、このグループに IdM ドメイン外からのメンバーが含まれるように指定します。以下に例を示します。

```
[root@ipaserver ~]# ipa group-add --desc='AD users external map' ad_users_external --
external
-------------------------------
Added group "ad_users_external"
-------------------------------
  Group name: ad_users_external
  Description: AD users external map
```



注記

外部グループは、ユーザーのプライマリーグループではなく、ユーザーの追加のグループにリンクする必要があります。Active Directory はグループの ***member*** 属性にグループメンバーを保存し、IdM はこの属性を使用してメンバーを解決します。ただし、Active Directory はユーザーのプライマリーグループをユーザーのエントリーの ***primaryGroupID*** 属性に保存しますが、これは解決されません。

3. 新しい IdM POSIX グループを作成するか、IdM ポリシーを管理する既存のものを選択します。たとえば、新規グループを作成するには、次のコマンドを実行します。

```
[root@ipaserver ~]# ipa group-add --desc='AD users' ad_users
----------------------
Added group "ad_users"
```

```
----------------------
  Group name: ad_users
  Description: AD users
  GID: 129600004
```

4. AD ユーザーまたはグループを外部メンバーとして IdM 外部グループに追加します。AD メンバーは、**DOMAIN\group_name**、**DOMAIN\username** などの完全修飾名で識別されます。AD アイデンティティーは、ユーザーまたはグループの Active Directory SID にマッピングされます。

   たとえば、AD グループの場合は、以下のようになります。

```
[root@ipaserver ~]# ipa group-add-member ad_users_external --external "AD\Domain
Users"
 [member user]:
 [member group]:
  Group name: ad_users_external
  Description: AD users external map
  External member: S-1-5-21-3655990580-1375374850-1633065477-513
SID_DOM_GROUP (2)
-------------------------
Number of members added 1
-------------------------
```

5. 外部 IdM グループをメンバーとして POSIX IdM グループに追加します。以下に例を示します。

```
[root@ipaserver ~]# ipa group-add-member ad_users --groups ad_users_external
  Group name: ad_users
  Description: AD users
  GID: 129600004
  Member groups: ad_users_external
-------------------------
Number of members added 1
-------------------------
```

5.3.4. 信頼の維持

信頼管理には、グローバルな信頼設定、Kerberos 信頼設定、DNS レルム設定、Active Directory ユーザーへの ID 範囲割り当てなど、複数の領域が関係します。

5.3.4.1. グローバル信頼設定の編集

ipa-adtrust-install ユーティリティーは、Active Directory ドメインへの信頼の作成に必要な IdM ドメインのバックグラウンド情報を自動的に設定します。

グローバル信頼設定には、以下の 5 つの属性が含まれます。

- Windows スタイルのセキュリティー ID (SID)。この属性は自動生成され、修正できません。
- ドメイン GUID。この属性は自動生成され、変更できません。
- Kerberos ドメイン名。この属性は IdM 設定から取得され、変更できません。
- IdM ユーザーを追加するデフォルトのグループ。この属性は変更できます。

- NetBIOS 名。この属性を変更することは推奨されません。

信頼設定は **cn=*domain*,cn=ad,cn=etc,dc=example,dc=com** サブツリーに保存されます。

5.3.4.1.1. NetBIOS 名の変更

重要

ほとんどの場合で NetBIOS 名を変更すると、既存の信頼をすべて再確立する必要があります。したがって、Red Hat は、属性を変更しないことを推奨します。

ipa-adtrust-install ユーティリティーを実行するときに、Active Directory トポロジーと互換性がある NetBIOS 名は、IdM サーバーに対して設定されます。後で変更するには、**ipa-adtrust-install** を再度実行し、**--netbios-name** オプションを使用して新しい NetBIOS 名を指定します。

```
[root@ipaserver ]# ipa-adtrust-install --netbios-name=NEWBIOSNAME
```

5.3.4.1.2. Windows ユーザーのデフォルトグループの変更

Identity Management が Active Directory フォレストを信頼するように設定すると、IdM ユーザーの Kerberos チケットに MS-PAC レコードが追加されます。MS-PAC レコードには、IdM ユーザーが属するグループのセキュリティー識別子 (SID) が含まれます。IdM ユーザーのプライマリーグループに SID が割り当てられていない場合は、*Default SMB グループ* に定義されたセキュリティー識別子の値が使用されます。AD ドメインコントローラーが IdM 信頼コントローラーからユーザー情報を要求すると、同じロジックが Samba スイートによって適用されます。

Default SMB グループは、**ipa-adtrust-install** ユーティリティーが自動作成されるフォールバックグループです。デフォルトのグループは削除できませんが、グローバル信頼設定を使用して、IdM ユーザーのプライマリーグループのフォールバックとして使用する別の IdM グループを指定できます。

コマンドラインからデフォルトグループを設定するには、**ipa trustconfig-mod** コマンドを使用します。

```
[root@server ~]# kinit admin
[root@server ~]# ipa trustconfig-mod --fallback-primary-group="Example Windows Group"
```

IdM Web UI からデフォルトグループを設定するには、以下を実行します。

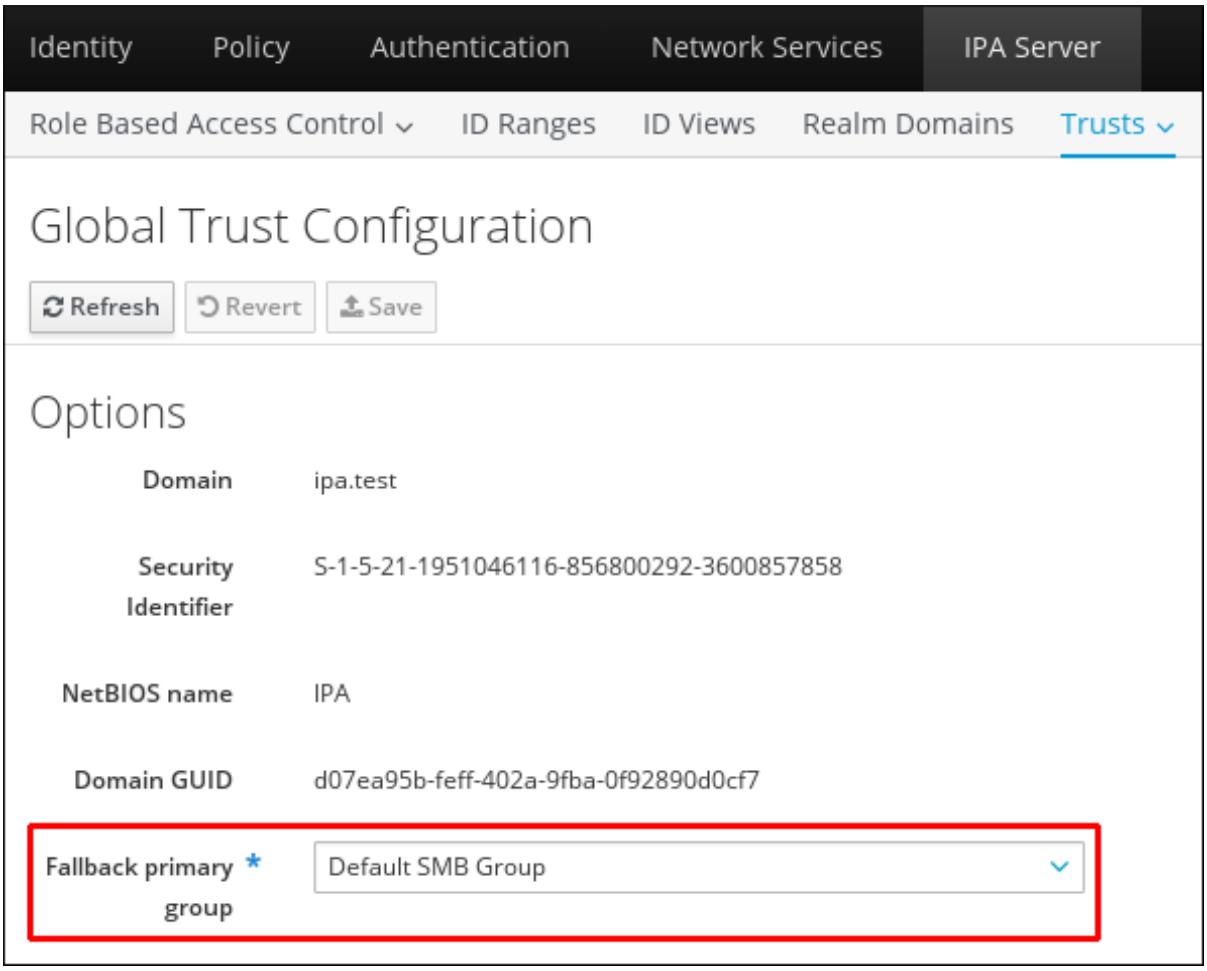
1. IdM Web UI を開きます。

   ```
   https://ipaserver.example.com
   ```

2. **IPA Server** メインタブで **Trusts** サブタブを選択し、**Global Configuration** セクションを開きます。

3. **Fallback primary group** ドロップダウンリストのすべての IdM グループから、新しいグループを選択します。

図5.6 Windows ユーザーのデフォルトグループの設定



4. **Save** をクリックして、新しい設定を保存します。

5.3.4.2. 信頼ドメインの検出、有効化、および無効化

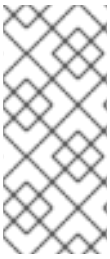
推移の信頼とは、信頼パスがドメインのチェーンを実行できることを示しています。詳細は、「信頼関係のアーキテクチャー」 を参照してください。

IdM にはフォレスト内の root ドメインとの間に信頼があり、推移性により、その子ドメイン、および同じフォレストのその他のドメインはすべてその信頼に暗黙的に組み込まれます。IdM は、フォレスト内の任意の場所に、IdM リソースへのアクセスを試みる Windows ユーザーとしてトポロジーが続きます。各ドメインおよび子ドメインは、IdM 信頼設定の 信頼ドメイン です。各ドメインは、信頼サブツリーの **cn=*subdomain*,cn=*trust_name*,cn=ad,cn=trusts,dc=example,dc=com** の独自のエントリーに保存されます。

信頼が最初に設定されている場合、IdM は完全な Active Directory トポロジーを検出およびマップしようとしますが、そのトポロジーを手動で取得するのにメリットがある場合もあります。これは、**trust-fetch-domains** コマンドで行われます。

```
[root@ipaserver ~]# kinit admin
[root@ipaserver ~]# ipa trust-fetch-domains ad.example.com
----------------------------------------
List of trust domains successfully refreshed
----------------------------------------
  Realm name: test.ad.example.com
  Domain NetBIOS name: TEST
  Domain Security Identifier: S-1-5-21-87535643-5658642561-5780864324
```

```
  Realm name: users.ad.example.com
  Domain NetBIOS name: USERS
  Domain Security Identifier: S-1-5-21-91314187-2404433721-1858927112

  Realm name: prod.ad.example.com
  Domain NetBIOS name: PROD
  Domain Security Identifier: S-1-5-21-46580863-3346886432-4578854233
----------------------------
Number of entries returned 3
----------------------------
```



注記

共有シークレットで信頼を追加する場合は、AD フォレストのトポロジーを手動で取得する必要があります。**ipa trust-add ad.domain --trust-secret** コマンドを実行すると、AD ドメインおよび Trusts ツールのフォレスト信頼プロパティーを使用して、AD 側で着信信頼を検証します。次に、**ipa trust-fetch-domains ad.domain** コマンドを実行します。IdM は信頼に関する情報を受け取り、その信頼に関する情報を利用できます。

トポロジーが取得されると (自動検出または手動検出)、IdM 信頼設定内で、そのトポロジーの個別のドメインおよび子ドメインを有効にしたり、無効にしたり、または完全に削除したりできます。

たとえば、特定の子ドメインのユーザーが IdM リソースを使用できないようにするには、その信頼ドメインを無効にします。

```
[root@ipaserver ~]# kinit admin
[root@ipaserver ~]# ipa trustdomain-disable test.ad.example.com
----------------------------------------
Disabled trust domain "test.ad.example.com"
----------------------------------------
```

その信頼ドメインは、**trustdomain-enable** コマンドを使用して再度有効にできます。

ドメインがトポロジーから永久的に削除される必要がある場合、IdM 信頼設定からこれを削除することができます。

```
[root@ipaserver ~]# kinit admin
[root@ipaserver ~]# ipa trustdomain-del prod.ad.example.com
------------------------------------------------------------------
Removed information about the trusted domain " "prod.ad.example.com"
------------------------------------------------------------------
```

5.3.4.3. IdM Kerberos レルムに関連付けられたドメインの表示および管理

IdM Kerberos レルムに関連するドメインは、IdM ディレクトリーで **cn=Realm Domains,cn=ipa,cn=etc,dc=example,dc=com** サブツリーに保存されています。Active Directory で信頼を確立すると、ドメインの一覧は IdM で使用されます。IdM で管理されるドメインの一覧を把握すると、AD ドメインコントローラーが、どの認証が IdM KDC にルーティングされることを要求しているかを把握できます。IdM レルムで関連するように設定されているドメインの一覧は、**realmdomains-show** コマンドを使用して表記できます。

```
[root@ipaserver ~]# kinit admin
[root@ipaserver ~]# ipa realmdomains-show
Domain: ipa.example.org, ipa.example.com, example.com
```

統合 DNS のある IdM 設定の場合は、以下を行います。

- **ipa dnszone-add** コマンドを使用して新規 DNS ゾーンが IdM に追加されると、ドメイン一覧にドメイン一覧が自動的に追加されます。**ipa realmdomains-show** を実行すると、IdM KDC が管理するドメインの一覧で新しいドメインが表示されます。

  ```
  # kinit admin
  # ipa dnszone-add ipa2.example.com
  # ipa realmdomains-show
  Domain: ipa.example.org, ipa.example.com, example.com, ipa2.example.com
  ```

  IdM Kerberos レルムに関連付けられたドメインの削除や、その他の修正も自動的に行われます。

統合 DNS のない IdM 設定の場合は、以下を行います。

- IdM Kerberos レルムの一部となっている DNS ゾーンが追加される場合は、IdM KDC の制御下にあるドメインの IdM 一覧に新規ドメインを手動で追加する必要があります。**--add-domain** オプションを指定した **ipa realmdomains-mod** コマンドを使用して、新しいドメインを追加します。

  ```
  [root@ipaserver ~]# kinit admin
  [root@ipaserver ~]# ipa realmdomains-mod --add-domain=ipa2.example.com
  Domain: ipa.example.org, ipa.example.com, example.com, ipa2.example.com
  ```

  DNS ゾーンが削除された場合は、IdM Kerberos レルムに関連付けられたドメインも手動で削除する必要があります。

  ```
  [root@ipaserver ~]# kinit admin
  [root@ipaserver ~]# ipa realmdomains-mod --del-domain=ipa2.example.com
  Domain: ipa.example.org, ipa.example.com, example.com
  ```

  ドメインのリストに複数の変更を加える必要がある場合は、**--domain** オプションを使用して、リスト自体を変更および置換できます。

  ```
  [root@ipaserver ~]# ipa realmdomains-mod --domain={ipa.example.org,ipa2.example.com}
  ```

5.3.4.4. 推移的な信頼における UID および GID 番号範囲の追加

信頼を最初に設定する際に作成する ID 範囲は、「ID 範囲」 で説明しています。後で ID 範囲を追加するには、以下のオプションを付けて **ipa idrange-add** コマンドを実行します。

- **--base-id** オプションは、開始番号である POSIX 範囲のベース ID を設定します

- **--range-size** オプションは、IdM が使用する POSIX ID 範囲のサイズを設定します。IdM は、信頼できる AD ドメイン内のユーザーとグループの RID を POSIX ID にマップします。**--range-size** オプションは、IdM が作成する ID の最大数を定義します。AD は、作成するユーザーとグループごとに新しい RID を使用します。ユーザーまたはグループを削除した場合、AD は今後の AD エントリーに RID を再利用しません。したがって、範囲は、IdM が既存の各 AD ユーザーとグループ、および将来作成するものに ID を割り当てるのに十分な大きさである必要があ

ります。たとえば、管理者が 50000 人の AD ユーザーのうち 20000 人を削除し、その間に 10000 人の新しいアカウントを作成する場合、範囲は少なくとも 60000 に設定する必要があります。ただし、範囲にも十分な予約があることが重要になります。大規模な環境では、デフォルト (200000) 範囲のサイズが十分ではないことが予想されます。**--range-size** を高い値に設定します。

- **--rid-base** オプションは、SID の右端の番号である RID の開始番号を設定します。この値は、競合を防ぐためにベース ID に追加する範囲を表します
- 信頼用に複数のドメインを設定できるため、**--dom-sid** オプションはドメイン SID を設定します。

以下の例ではベース ID が 1,200,000、RID が 1,000 です。追加される ID 番号は 1,201,000 になります。

```
[root@server ~]$ kinit admin
[root@server ~]$ ipa idrange-add --base-id=1200000 --range-size=200000 --rid-base=0 --dom-sid=S-1-5-21-123-456-789 trusted_dom_range
```

重要

手動で定義した ID 範囲が IdM の使用する ID 範囲と重複しないようにしてください。

5.3.4.5. DNA ID 範囲の手動調整

場合によっては、既存のレプリカの DNA (Distributed Numeric Assignment) の ID 範囲を手動で調整する必要があります。たとえば、機能していないレプリカに割り当てられた DNA I D 範囲を回復したり、ID が不足している範囲を拡張したりします。

DNA ID 範囲を手動で調整する場合は、新たに調整した範囲が IdM ID 範囲に含まれていることを確認してください。これは、**ipa idrange-find** コマンドを使用して確認できます。新たに調整した範囲が IdM ID 範囲に含まれていない場合、コマンドは失敗します。

機能していないレプリカから DNA ID 範囲を復元するには、**ipa-replica-manage dnarange-show** コマンドを使用して、現在割り当てられている DNA 範囲を表示します。現在、デッキ上の DNA 範囲が割り当てられている場合は、**ipa-replica-manage dnanextrange-show** コマンドを使用します。

重要

重複数 ID 範囲を作成しないでください。サーバーまたはレプリカに割り当てた ID 範囲のいずれかが重複すると、この 2 つのサーバーにより、異なるエントリーに同じ ID 値を割り当てる可能性があります。

指定のサーバーの現在の DNA ID 範囲を定義するには、**ipa-replica-manage dnarange-set** コマンドを使用します。

```
# ipa-replica-manage dnarange-set masterA.example.com 1250-1499
```

指定のサーバーの次の DNA ID 範囲を定義するには、**ipa-replica-manage dnanextrange-set** コマンドを使用します。

```
# ipa-replica-manage dnanextrange-set masterB.example.com 1500-5000
```

5.3.4.6. サービスおよびホスト向けの Kerberos フラグ

信頼されるドメイン内のサービスやホストにアクセスするには、Kerberos チケット保証チケット (TGT) に特別なフラグが必要となる場合があります。たとえば、AD クライアントから Active Directory (AD) アカウントを持つ IdM クライアントにシングルサインオンを使用してログインする場合は、Kerberos TGT フラグ **OK_AS_DELEGATE** が必要です。

Kerberos フラグの設定に関する詳細情報は、『Linux ドメイン ID、認証、およびポリシーガイド』 の サービスおよびホスト向けの Kerberos フラグ を参照してください。

5.3.5. サービスの PAC タイプの設定

IdM リソースについては、Active Directory ユーザーがサービスのチケットを要求する場合に IdM はその要求を Active Directory に転送して、ユーザー情報を取得します。ユーザーの Active Directory グループ割り当てに関連付けられたアクセスデータには、Active Directory により戻され、Kerberos チケットに組み込まれているアクセスデータです。

Active Directory のグループ情報は、**privileged access certificates** または MS-PAC と呼ばれる特殊なデータセットとして Active Directory ユーザーの各 Kerberos チケットの識別子の一覧に保存されます。アクセスを決定するには、PAC のグループ情報を Active Directory グループにマップしてから、対応する IdM グループにマップする必要があります。

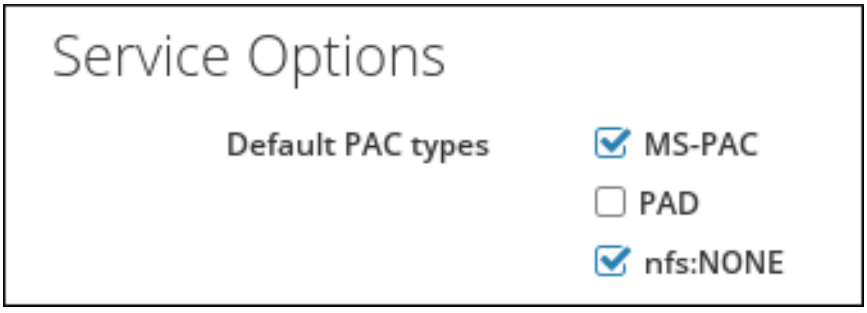
IdM サービスは、ドメインサービスに対するユーザー認証の初回試行時に、認証要求に対して PAC を生成するように設定できます。

5.3.5.1. デフォルト PAC タイプの設定

IdM サーバー設定は、サービスについてデフォルトで生成される PAC タイプを定義します。グローバル設定は、特定サービスのローカル設定を変更して上書きできます。

1. **IPA Server** タブを開きます。
2. **Configuration** サブタブを選択します。
3. **Service Options** 領域にスクロールします。

   図5.7 **Service Options** 領域



4. PAC を使用するには、**MS-PAC** チェックボックスを選択します。これで AD サービスで使用可能な証明書が追加されます。チェックボックスが選択されないと、PAC は Kerberos チケットに追加されません。

   nfs:NONE チェックボックスを選択すると、MS-PAC レコードは NFS サーバーに対して発行されたサービスチケットに追加されません。

注記

PAD チェックボックスは無視できます。この機能は、IdM ではまだ利用できません。

5. 変更を保存するには、ページの上部にある **Update** リンクをクリックします。

5.3.5.2. サービスの PAC タイプの設定

グローバルポリシーは、サービスに明示的な設定がない場合にサービスに使用する PAC タイプを設定します。ただし、グローバル設定はローカルサービス設定で上書きされる可能性があります。

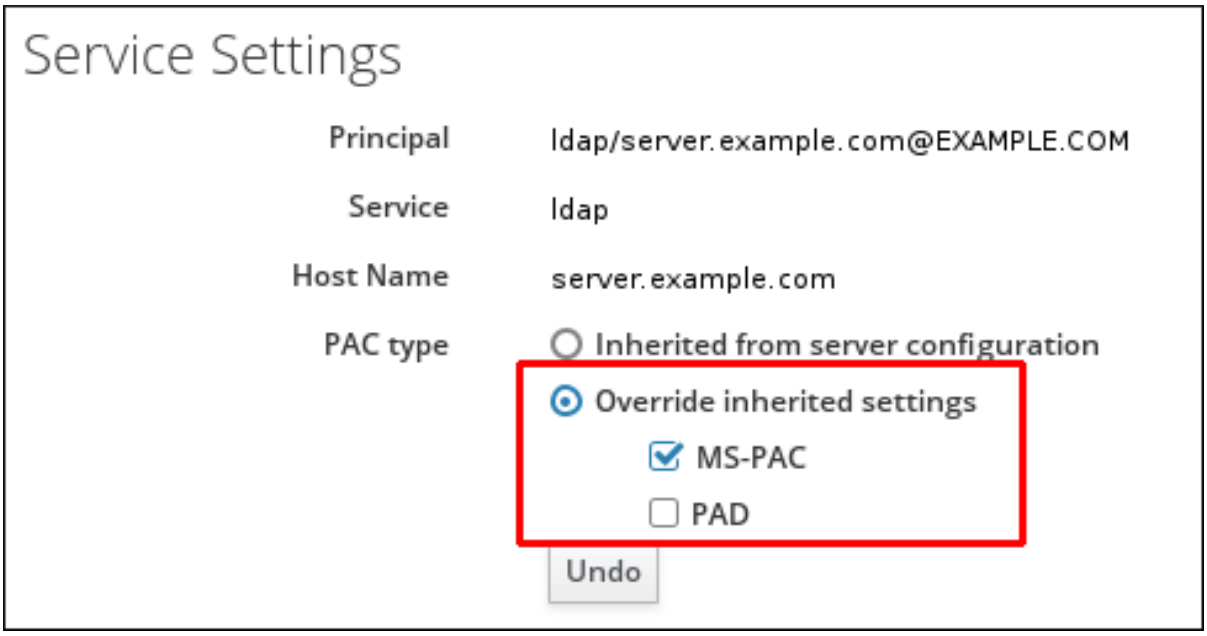
コマンドラインから PAC 設定を変更するには、**--pac-type** オプションを指定して **ipa service-mod** コマンドを使用します。コマンドの使用方法については、**--help** オプションを追加して実行してください。

```
$ ipa service-mod --help
Usage: ipa [global-options] service-mod PRINCIPAL [options]

Modify an existing IPA service.
Options:
-h, --help            show this help message and exit
...
```

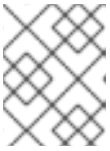
Web UI で PAC 設定を変更するには、以下の手順に従います。

1. **Identity** タブを開き、**Services** サブタブを選択します。
2. 編集するサービスの名前をクリックします。
3. **Service Settings** 領域で **Override inherited settings** オプションを選択し、**MS-PAC** チェックボックスを選択して AD サービスが使用可能な証明書を追加します。

図5.8 **Service Settings** 領域



チェックボックスが選択されない場合、PAC は Kerberos チケットに追加されません。



注記

PAD チェックボックスは無視できます。この機能は、IdM ではまだ利用できません。

4. 変更を保存するには、ページの上部にある **Update** リンクをクリックします。

5.3.6. Active Directory で定義された POSIX 属性の使用

5.3.6.1. Active Directory ユーザーの UID 属性および GID 属性の定義

Windows 管理者がユーザーの POSIX UID と GID 属性を手動で定義する場合は、ユーザーに同じ GID を使用して IdM サーバー上に一致するグループを作成してください。

このグループを作成することで、ユーザーがプライマリーユーザーグループに関連付けられます。このグループが存在しないと、IdM サーバーはユーザーが所属するすべてのグループを探すことができません。

5.3.6.2. ログインシェルとホームディレクトリー属性の送信

重要

この機能を活用するには、Red Hat Enterprise Linux 7.1 移行をベースにした IdM にクライアントが登録されている必要があります。

SSSD は、以下の属性値を IdM との信頼関係にある Active Directory サーバーから読み取ることができます。

- **loginShell** 属性。これは AD ユーザーのシェルを指定します。
- **unixHomeDirectory** 属性。これは AD ユーザーのホームディレクトリーを指定します。

これらの属性を使用して AD サーバー上でカスタムシェルやホームディレクトリーの値を定義する場合、このカスタム値は AD ユーザー向けに IdM クライアントに表示されます。このため、AD 側と IdM 側の両方で同一のユーザーシェルが AD ユーザーに表示されます。

なお、AD ユーザーのホームディレクトリーを IdM クライアントに表示するためには、IdM サーバーの **/etc/ssd/ssd.conf** ファイルの **domain** セクションの ***subdomain_homedir*** オプションに **%o** を設定する必要があります。**%o** 値は、アイデンティティープロバイダーから取得したホームディレクトリーを表します。以下に例を示します。

```
[domain/example.com]
subdomain_homedir = %o
```

AD 管理者が AD 側で **loginShell** や **unixHomeDirectory** を変更した場合、この変更は IdM 側で自動的に反映されます。属性が AD サーバーで定義されていない場合、SSSD はテンプレートのデフォルト値を使用します。このデフォルト値は IdM クライアントにも表示されます。

5.3.7. IdM リソースの Active Directory マシンからの SSH の使用

信頼が設定されると、Active Directory ユーザーは SSH およびそれらの AD 認証情報を使用して、IdM ホスト上のマシン、サービスおよびファイルにアクセスすることができます。

5.3.7.1. キャッシュに関する考慮事項

IdM クライアントは、ユーザー属性を取得するために、Active Directory ドメインコントローラー (DC) に直接接続しません。代わりに、クライアントはこの情報をキャッシュする IdM サーバーに接続します。このため、Active Directory でユーザーを無効にすると、IdM データベースでユーザーの期限が切れるまで、ユーザーは SSH 鍵認証を使用して IdM クライアントに認証することができます。

IdM は以下の状況でユーザーのレコードを更新します。

- エントリーは自動的に期限切れになりました。
- **sss_cache** ユーティリティーを使用して、キャッシュ内のユーザーのエントリーを手動で失効させます。

```
# sss_cache --user user_name
```

- **kinit** ユーティリティーまたは Web UI を使用して IdM サーバーへのユーザー認証を行います。

5.3.7.2. パスワードなしでの SSH の使用

ローカル認証用の **localauth** Kerberos プラグインは、Kerberos プリンシパルが自動的にローカルの SSSD ユーザー名にマッピングされるようにします。この **localauth** を使うことで、信頼される AD ドメインの Windows ユーザーは Kerberos を使用したログイン時にパスワードが求められず、パスワードなしで SSH を使用できるようになります。

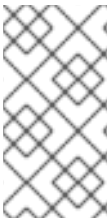
このプラグインは、複数のレルムや信頼にわたって信頼性のあるマッピングメカニズムを提供します。**sssd** が Kerberos ライブラリーに接続してプリンシパルを POSIX ID にマッピングする際には、SSSD プラグインは IdM で定義された信頼合意に従ってこれらをマッピングします。

特定の状況では、SSH bastion ホストを使用してその他の Red Hat Enterprise Linux マシンにアクセスします。デフォルトで Kerberos を使用して bastion ホスト上の SSH に対する認証を行う場合、Kerberos チケットを転送して、Kerberos を使用して他の Red Hat Enterprise Linux ホストへ認証することはできません。このような転送認証を有効にするには、**OK_AS_DELEGATE** Kerberos フラグを bastions ホストプリンシパルに追加します。

```
# ipa host-mod bastion_host.idm.example.com --ok-as-delegate=true
```

Red Hat Enterprise Linux 7.1 以降のシステムでの AD ユーザーの Kerberos 認証
Red Hat Enterprise Linux 7.1 以降のシステムでは、SSSD は **localauth** Kerberos プラグインを自動設定します。

SSSD は、**user@AD.DOMAIN**、**ad.domain\user**、および **AD\user** 形式でのユーザー名を許可します。



注記

localauth を使用するシステムでは、**/etc/krb5.conf** ファイルで ***auth_to_local*** オプションを設定したり、**.k5login** ファイルで Kerberos プリンシパルをリストアップする必要はありません。**localauth** プラグインにより、パスワードなしのログインに使用されていたこの設定は不要になります。

AD ユーザーの Kerberos 認証の手動設定
システムに **localauth** プラグインがない場合は、ユーザーが適切な Kerberos チケットを取得した場合でも、SSH は Active Directory ドメインユーザーのユーザーパスワードを要求します。

このような状況で Active Directory ユーザーが認証に Kerberos を使用できるようにするには、**/etc/krb5.conf** ファイルに ***auth_to_local*** オプションを設定するか、ユーザーのホームディレクトリーの **.k5login** ファイルにユーザーの Kerberos プリンシパルをリストアップします。

/etc/krb5.conf の設定

以下の手順では、Kerberos 設定ファイルにレルムマッピングを設定する方法を説明しています。

1. **/etc/krb5.conf** ファイルを開きます。
2. **realms** セクションで IdM レルムを名前で特定し、Kerberos プリンシパル名のマッピングを定義するために ***auth_to_local*** 行を 2 行追加します。
   - 1 つ目のルールでは、異なる Active Directory ユーザー名形式と特定の Active Directory ドメインをマッピングするルールを定義します。
   - 他のルールで、標準の Unix ユーザー名に **DEFAULT** の値を設定します。

   以下に例を示します。

```
[realms]
IDM = {
....
auth_to_local = RULE:[1:$1@$0](^.*@ADDOMAIN$)s/@ADDOMAIN/@addomain/
auth_to_local = DEFAULT
}
```

3. KDC サービスを再起動します。

```
[root@server ~]# systemctl restart krb5kdc.service
```

auth_to_local オプションを使用して Kerberos 認証を設定する場合、SSH アクセスに使用するユーザー名は次の条件を満たす必要があることに注意してください。

- ユーザー名が **ad_user@ad_domain** 形式になっていること。
- ドメイン名が小文字であること。
- ユーザー名の大文字/小文字が Active Directory 内のユーザー名と一致していること。たとえば、**user** と **User** は、大文字と小文字で異なるので、別のユーザー名とみなされます。

auth_to_local の設定は、krb5.conf(5) man ページを参照してください。

.k5login の設定

以下の手順では、システムがローカルユーザー名の Kerberos プリンシパル名を見つける設定を行います。

1. ユーザーのホームディレクトリーに **.k5login** ファイルを作成します。
2. 作成したファイルにユーザーが使用する Kerberos プリンシパルを記載します。

認証しているユーザーが既存の Kerberos チケットのプリンシパルと一致する場合、ユーザーはパスワードを求められることなく、そのチケットを使用してログインできます。

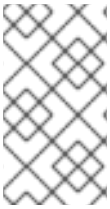
.k5login 設定を使用して Kerberos 認証を設定する場合は、SSH アクセスに使用するユーザー名は **ad_user@ad_domain** の形式を取る必要があります。

.k5login ファイルの設定に関する詳細は、.k5login(5) の man ページを参照してください。

これらのいずれの設定を行うことで、AD ユーザーが Kerberos を使用してログインできるようになります。

5.3.8. Kerberos 対応 Web アプリケーションでの信頼の使用

既存の Web アプリケーションは、信頼される Active Directory および IdM Kerberos レルムを参照する Kerberos 認証を使用するように設定できます。完全な Kerberos 設定ディレクティブについては Configuration page for the mod_auth_kerb module を参照してください。



注記

Apache アプリケーション設定を変更した後に、Apache サービスを再起動します。

```
[root@ipaserver ~]# systemctl restart httpd.service
```

たとえば Apache サーバーの場合は、Apache サーバーが IdM Kerberos レルムに接続する方法を定義する以下のようなオプションがあります。

KrbAuthRealms

KrbAuthRealms オプションは、アプリケーションの場所を IdM ドメインの名前に指定します。これは必須です。

Krb5Keytab

Krb5Keytab オプションは、IdM サーバーのキータブの場所を提供します。これは必須です。

KrbServiceName

KrbServiceName オプションは、キータブ (HTTP) に使用される Kerberos サービス名を設定します。これは推奨されるオプションです。

KrbMethodK5Passwd および ***KrbMethodNegotiate***

KrbMethodK5Passwd Kerberos メソッドオプションは、有効なユーザーに対してパスワードベースの認証を有効にします。***KrbMethodNegotiate*** オプションは、有効な Kerberos チケットが利用可能な場合に Single Sign-On (SSO) を有効にします。

ユーザーが多い場合は、これらのオプションの使用が推奨されます。

KrbLocalUserMapping

KrbLocalUserMapping オプションは、通常の Web ログイン (通常はアカウントの UID またはコモンネーム) を完全修飾ユーザー名 (フォーマットは **user@REALM.COM**) にマッピングすることを可能にします。

このオプションの使用は強く推奨されます。ドメイン名/ログイン名マッピングがないと、Web ログインはドメインユーザーとは別のユーザーアカウントになるよう見えます。つまり、ユーザーは予想されるデータを表示できません。

サポートされるユーザー名形式の詳細については、「サポートされるユーザー名の形式」 を参照してください。

例5.1 Apache Web アプリケーションの Kerberos 設定

```
<Location "/mywebapp">
  AuthType Kerberos
  AuthName "IPA Kerberos authentication"
  KrbMethodNegotiate on
  KrbMethodK5Passwd on
  KrbServiceName HTTP
  KrbAuthRealms IDM_DOMAIN
  Krb5Keytab /etc/httpd/conf/ipa.keytab
  KrbLocalUserMapping on
  KrbSaveCredentials off
  Require valid-user
</Location>
```

5.3.9. Active Directory Kerberos 通信用の Kerberos Distribution Center プロキシーとしての IdM サーバーの設定

特定の状況では、ネットワークの制限またはファイアウォールルールにより、Identity Management (IdM) クライアントが Active Directory (AD) ドメインコントローラー上のポート 88 に Kerberos トラフィックを送信できなくなります。このソリューションは、たとえば Identity Management サーバーで Kerberos プロキシーを設定して、IdM クライアントから AD にトラフィックを中継します。

1. IdM クライアントで、Active Directory レルムを **/etc/krb5.conf** ファイルの [realms] セクションに追加します。**kdc** パラメーターおよび **kpasswd_server** パラメーターを、IdM サーバーの完全修飾ドメイン名 (その後に続く **/KdcProxy**) を参照するように設定します。

```
AD.EXAMPLE.COM = {
        kdc = https://server.idm.example.com/KdcProxy
        kpasswd_server = https://server.idm.example.com/KdcProxy
    }
```

2. IdM クライアントで、前の手順の **/etc/krb5.conf** 指定を上書きする可能性のある **/var/lib/sss/pubconf/kdcinfo.*** ファイルの作成を無効にします。**/etc/sssd/sssd.conf** ファイルを編集し、**krb5_use_kdcinfo** を **False** に設定します。

```
[domain/example.com]
krb5_use_kdcinfo = False
```

3. IdM サーバーで、**/etc/ipa/kdcproxy/kdcproxy.conf** ファイルで **use_dns** オプションを **true** に設定し、DNS サービス (SRV) レコードを使用して以下と通信するための AD サーバーを検索します。

```
use_dns = true
```

また、DNS SRV レコードを使用しない場合は、明示的な AD サーバーを **/etc/krb5.conf** ファイルの [realms] セクションに追加します。

```
AD.EXAMPLE.COM = {
        kdc = ad-server.ad.example.com
        kpasswd_server = ad-server.ad.example.com
    }
```

注記

この手順の 2 と 3 を実行するには、Ansible スクリプトなどのスクリプトを実行します。これは、複数のシステムで変更を行う場合などに特に便利です。

4. IdM サーバーで IPA サービスを再起動します。

```
# ipactl restart
```

5. この手順が成功したことを確認するには、IdM クライアントで以下のコマンドを実行します。

```
# rm /var/lib/sss/pubconf/kdcinfo*
# kinit ad_user@AD.EXAMPLE.COM
Password for ad_user@AD.EXAMPLE.COM:
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: ad_user@AD.EXAMPLE.COM

Valid starting     Expires            Service principal
[... output truncated ...]
```

5.4. 信頼された ACTIVE DIRECTORY ドメインのユーザーおよびグループの LDAP 検索ベースを変更する手順

管理者は、信頼された Active Directory ドメインのユーザーやグループごとに異なる検索ベースを設定することができます。たとえば、SSSD クライアントシステムに対して、アクティブな Active Directory ユーザーとグループだけが表示されるように、ユーザーをアクティブでない組織単位からフィルターリングできるようになります。

5.4.1. 前提条件

- ユーザーが所属する全グループを SSSD が解決しないように、Active Directory 側の **tokenGroups** 属性のサポートを無効にすることを検討してください。

  tokenGroups が有効な場合には、属性に、SID のフラットリストが含まれるため、SSSD はユーザーが所属する全グループを解決します。この属性に関する詳細は、Microsoft Developer Network の Token-Groups attribute を参照してください。

5.4.2. 検索を制限する LDAP 検索ベースの設定

以下の手順は、**/etc/sssd/sssd.conf** ファイルを編集して、固有のサブツリーに、SSSD の検索を制限する方法を説明します。

留意事項

- SSSD クライアントが Active Directory ドメインに直接参加している場合は、すべてのクライアントでこの手順を実行します。

- SSSD クライアントが Active Directory を使用する信頼にある Identity Management ドメインにある場合は、Identity Management サーバーでこの手順のみを実行します。

手順

1. 信頼できるドメインには、**sssd.conf** に別の **[domain]** セクションがあることを確認します。信頼されるドメインセクションの見出しは、以下のテンプレートに従います。

```
[domain/main_domain/trusted_domain]
```

以下に例を示します。

```
[domain/idm.example.com/ad.example.com]
```

2. **sssd.conf** ファイルを編集して、特定の組織単位 (OU) に検索ベースを制限します。たとえば、***ldap_search_base*** オプションは、すべてのタイプのオブジェクトの検索ベースを変更します。

```
[domain/idm.example.com/ad.example.com]
ldap_search_base = ou=finance,dc=ad,dc=example,dc=com
```

ldap_user_search_base、***ldap_group_search_base***、***ldap_netgroup_search_base***、および ***ldap_service_search_base*** オプションも使用できます。これらのオプションの詳細は、sssd-ldap(5) の man ページを参照してください。

3. SSSD を再起動します。

```
# systemctl restart sssd.service
```

4. 確認するには、SSSD クライアント上の複数の Active Directory ユーザーを解決します。たとえば、ユーザーの検索ベースとグループの検索ベースへの変更をテストするには、以下を実行します。

```
# getent passwd ad_user@ad.example.com
# getent group ad_group@ad.example.com
```

SSSD が正しく設定されている場合は、設定した検索ベースからのオブジェクトだけを解決できます。

他の検索ドメインからのユーザーを解決できる場合は、SSSD ログを確認して、問題のトラブルシューティングを行います。

1. SSSD キャッシュを失効させます。

```
# sss_cache --everything
```

2. **sssd.conf** の一般的な **[domain]** セクションで、***debug_level*** オプションを **9** に設定します。

3. ユーザーを解決するためのコマンドを繰り返します。

4. **/var/log/sssd/** の SSSD ログで、**sdap_get_generic_*** 関数からのメッセージを探します。この関数は、ユーザー検索に使用したフィルターおよび検索ベースをログに記録します。

関連情報

- **sssd.conf** の信頼できるドメインセクションで使用できるオプションの一覧は、sssd.conf(5) の man ページの **TRUSTED DOMAIN SECTION** を参照してください。

5.5. SSSD が表示するユーザー名の形式の変更

デフォルトでは、SSSD はユーザー名を表示する際に **user_name@domain_name** 形式を使用します。この形式を変更する前に、「サポートされるユーザー名の形式」 でデフォルト値の理由を確認してください。

SSSD がドメインなしでユーザー名のみを表示するように設定するには、以下を行います。

1. 次のエントリーを **/etc/sssd/sssd.conf** ファイルのドメインのセクションに追加します。

```
full_name_format = %1$s
```

2. SSSD を再起動します。

```
# systemctl restart sssd
```

5.6. IDENTITY MANAGEMENT または SSSD を、信頼された ACTIVE DIRECTORY ドメインの中から選択された ACTIVE DIRECTORY サーバーやサイトに制限する手順

管理者は、信頼された Active Directory ドメイン内の Active Directory サーバーとサイトの自動検出を無効にして、代わりに、手動でサーバー、サイト、またはその両方を表示し、SSSD が通信する Active Directory サーバーの一覧に絞り込む事ができます。たとえば、こうすることで、アクセスできないサイトへの問い合わせを回避できます。

5.6.1. SSSD が特定の Active Directory サーバーに問い合わせするための設定

以下の手順では、**/etc/sssd/sssd.conf** ファイルを編集して、SSSD が接続する Active Directory サーバーを手動で設定する方法を説明します。

留意事項

- SSSD クライアントが Active Directory ドメインに直接参加している場合は、すべてのクライアントでこの手順を実行します。

  この設定では、Active Directory ドメインコントローラー (DC) またはサイトを制限することで、SSSD が特定のサーバーまたはサイトに接続して認証されるように設定します。

- SSSD クライアントが Active Directory を使用する信頼にある Identity Management ドメインにある場合は、Identity Management サーバーでこの手順のみを実行します。

  この設定では、Active Directory DC またはサイトを制限しても、Identity Management クライアントが特定のサーバーまたはサイトに接続して認証されるようには設定されません。信頼された Active Directory ユーザーおよびグループは、Identity Management サーバーを使用して解決されますが、認証は、直接 Active Directory DC に対して行われます。Red Hat Enterprise Linux 7.6 および sssd-1.16.2-5.el7 以降 では、***ad_server*** および ***ad_site*** オプションを使用して、IdM クライアントで SSSD を特定の AD サーバーまたはサイトを使用するように設定できます。Red Hat Enterprise Linux 7 の以前のバージョンでは、クライアント上の **/etc/krb5.conf** ファイルで、必要とされる Active Directory DC を定義して、認証を制限することができます。

手順

1. 信頼できるドメインには、**sssd.conf** に別の **[domain]** セクションがあることを確認します。信頼されるドメインセクションの見出しは、以下のテンプレートに従います。

```
[domain/main_domain/trusted_domain]
```

以下に例を示します。

```
[domain/idm.example.com/ad.example.com]
```

2. **sssd.conf** ファイルを編集して、SSSD を接続する Active Directory サーバーまたはサイトのホスト名を一覧表示します。

   Active Directory Server の ***ad_server*** オプションと、必要に応じて ***ad_server_backup*** オプションを使用します。Active Directory サイトには ***ad_site*** オプションを使用します。これらのオプションの詳細は、sssd-ad(5) の man ページを参照してください。

   以下に例を示します。

```
[domain/idm.example.com/ad.example.com]
ad_server = dc1.ad.example.com
```

3. SSSD を再起動します。

```
# systemctl restart sssd.service
```

4. 確認するには、SSSD クライアントで、設定したサーバーまたはサイトの Active Directory ユーザーとして解決または認証を行います。以下に例を示します。

```
# id ad_user@ad.example.com
```

ユーザーの解決や認証ができない場合は、以下の手順で問題を解決します。

1. **sssd.conf** の一般的な **[domain]** セクションで、***debug_level*** オプションを **9** に設定します。
2. **/var/log/sssd/** で SSSD ログを調査して、どのサーバーに SSSD が問い合わせたかを確認します。

関連情報

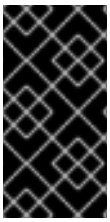
- **sssd.conf** の信頼できるドメインセクションで使用できるオプションの一覧は、sssd.conf(5) の man ページの **TRUSTED DOMAIN SECTION** を参照してください。

5.7. レガシー LINUX クライアントでの ACTIVE DIRECTORY 信頼

バージョン 1.8 以前の SSSD で Red Hat Enterprise Linux を実行している Linux クライアント (*レガシークライアント*) は、Active Directory を使用した IdM フォレスト間信頼にネイティブのサポートを提供しません。このため、IdM サーバーが提供するサービスに AD ユーザーがアクセスできるようにするには、レガシー Linux クライアントと IdM サーバーを適切に設定する必要があります。

バージョン 1.9 以降の SSSD を使用して IdM サーバーと通信することで LDAP 情報を取得する代わりに、レガシークライアントは **nss_ldap**、**nss-pam-ldapd**、またはバージョン 1.8 以前の SSSD などの他のユーティリティーを使用します。以下のバージョンの Red Hat Enterprise Linux を稼働しているクライアントは SSSD 1.9 を使用しないため、レガシークライアントとみなされます。

- Red Hat Enterprise Linux 5.7 以降
- Red Hat Enterprise Linux 6.0 ~ 6.3



重要

SSSD バージョン 1.9 以降を実行しているクライアントはレガシークライアントとはみなされないため、本セクションに記載の設定は使用しないでください。SSSD 1.9 以降は AD を使用した IdM フォレスト間信頼にネイティブサポートを提供するため、AD ユーザーは追加設定なしで IdM クライアント上のサービスに適切にアクセスできます。

レガシークライアントが AD と信頼関係で IdM サーバーのドメインに参加させると、*compat LDAP ツリー*は、必要なユーザーおよびグループデータを AD ユーザーに提供します。ただし、compat ツリーを使用すると、AD ユーザーは限られた数の IdM サービスしかアクセスできません。

レガシークライアントでは以下のサービスにアクセス できません。

- Kerberos 認証
- ホストベースのアクセス制御 (HBAC)
- SELinux ユーザーマッピング
- **sudo** ルール

レガシークライアントにおいても以下のサービスにはアクセスが 提供されます。

- 情報検索
- パスワード認証

5.7.1. レガシークライアントでの AD 信頼向けのサーバー側設定

IdM サーバーが以下の設定要件を満たすようにしてください。

- IdM の ipa-server パッケージと IdM 信頼アドオンの ipa-server-trust-ad パッケージがインストールされています。
- **ipa-server-install** ユーティリティーを実行して IdM サーバーが設定されていること。
- **ipa-adtrust-install --enable-compat** コマンドが実行済みで、IdM サーバーが AD ドメインとの信頼をサポートしており、compat LDAP ツリーが利用可能であること。

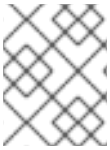
  過去に **--enable-compat** オプションを指定せずに **ipa-adtrust-install** をすでに実行している場合は、再度 **--enable-compat** を追加します。
- **ipa trust-add *ad.example.org*** コマンドを実行して AD 信頼が確立されていること。

ホストベースのアクセス制御 (HBAC) の **allow_all** ルールが無効になっている場合は、IdM サーバー上で **system-auth** サーバーを有効にして AD ユーザーの認証を許可します。

ipa hbacrule-show コマンドを使用すると、コマンドラインから **allow_all** の現行ステータスを直接決定できます。ルールが無効化されると、**Enabled: FALSE** が出力に表示されます。

```
[user@server ~]$ kinit admin
[user@server ~]$ ipa hbacrule-show allow_all
  Rule name: allow_all
  User category: all
  Host category: all
```

```
Service category: all
Description: Allow all users to access any host from any host
Enabled: FALSE
```



注記

HBAC ルールの有効化/無効化に関する情報は、『Linux ドメイン ID、認証、およびポリシーガイド』 の ホストベースのアクセス制御の設定 を参照してください。

IdM サーバーで **system-auth** を有効にするには、**system-auth** という名前の HBAC サービスを作成し、このサービスを使用して HBAC ルールを追加して IdM マスターへのアクセスを付与します。HBAC サービスとルールの追加については、『Linux Domain Identity、Authentication、and Policy Guide 』 の Configuring Host-Based Access Control セクションで説明されています。HBAC サービスは PAM サービス名であることに注意してください。新規 PAM サービスを追加する場合は、同一名の HBAC サービスを作成し、HBAC ルールでこのサービスへのアクセスを付与します。

5.7.2. ipa-advise ユーティリティーを使用したクライアント側の設定

ipa-advise ユーティリティーは、AD 信頼向けにレガシークライアントを設定する方法の指示を提供します。

ipa-advise が設定指示を提供可能なシナリオ一覧を表示するには、**ipa-advise** をオプションなしで実行します。**ipa-advise** を実行すると、使用可能なすべての設定命令セットの名前が、各セットの機能と、使用が推奨されるタイミングの説明とともに出力されます。

```
[root@server ~]# ipa-advise
config-redhat-nss-ldap  : Instructions for configuring a system
    with nss-ldap as a IPA client.
    This set of instructions is targeted
    for platforms that include the
    authconfig utility, which are all
    Red Hat based platforms.
config-redhat-nss-pam-ldapd : Instructions for configuring a system
(...)
```

特定セットの指示を表示するには、指示をパラメーターとして **ipa-advise** ユーティリティーを実行します。

```
[root@server ~]# ipa-advise config-redhat-nss-ldap
#!/bin/sh
# ----------------------------------------------------------------------
# Instructions for configuring a system with nss-ldap as a IPA client.
# This set of instructions is targeted for platforms that include the
# authconfig utility, which are all Red Hat based platforms.
# ----------------------------------------------------------------------
# Schema Compatibility plugin has not been configured on this server. To
# configure it, run "ipa-adtrust-install --enable-compat"
# Install required packages via yum
yum install -y wget openssl nss_ldap authconfig

# NOTE: IPA certificate uses the SHA-256 hash function. SHA-256 was
# introduced in RHEL5.2. Therefore, clients older than RHEL5.2 will not
# be able to interoperate with IPA server 3.x.
# Please note that this script assumes /etc/openldap/cacerts as the
```

```
# default CA certificate location. If this value is different on your
# system the script needs to be modified accordingly.
# Download the CA certificate of the IPA server
mkdir -p -m 755 /etc/openldap/cacerts
wget http://idm.example.com/ipa/config/ca.crt -O /etc/openldap/cacerts/ca.crt
(...)
```

ipa-advise ユーティリティーを使用して Linux クライアントを設定するには、表示された指示をシェルスクリプトとして実行するか、指示を手動で実行します。

シェルスクリプトとして実行するには、以下の手順に従います。

1. スクリプトファイルを作成します。

```
[root@server ~]# ipa-advise config-redhat-nss-ldap > setup_script.sh
```

2. **chmod** ユーティリティーを使用して、実行パーミッションをファイルに追加します。

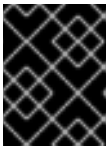
```
[root@server ~]# chmod +x setup_script.sh
```

3. **scp** ユーティリティーを使用してスクリプトをクライアントにコピーします。

```
[root@server ~]# scp setup_script.sh root@client
```

4. クライアントでスクリプトを実行します。

```
[root@client ~]# ./setup_script.sh
```



重要

クライアントでスクリプトを実行する前に、必ずスクリプトファイルを注意深く読んで確認してください。

クライアントを手動で設定するには、**ipa-advise** で表示される指示をコマンドラインから実行します。

5.8. フォレスト間の信頼のトラブルシューティング

本セクションでは、フォレスト間の信頼の環境で発生する問題とその解決方法を説明します。

5.8.1. ipa-extdom プラグインのトラブルシューティング

Active Directory (AD) への信頼のある IdM ドメイン内の IdM のクライアントは、AD から直接ユーザーおよびグループに関する情報を受け取れません。さらに、IdM は、IdM マスターで実行している Directory Server に AD ユーザーに関する情報を保存しません。代わりに、IdM サーバーは **ipa-extdom** を使用して、AD ユーザーおよびグループに関する情報を受け取り、要求元のクライアントに転送します。

ipa-extdom プラグインの設定タイムアウトの設定

ipa-extdom プラグインは、AD ユーザーのデータに要求を SSSD に送信します。ただし、リクエストされているすべてのデータが SSSD のキャッシュ内にすでに存在するわけではありません。この場合、SSSD は AD ドメインコントローラー (DC) からデータを要求します。これは、特定の操作に時間がか

かる場合があります。設定のタイムアウト値は、プラグインが接続をキャンセルしてタイムアウトエラーを呼び出し元に返す前に、**ipa-extdom** プラグインが SSSD の応答を待機する時間をミリ秒単位で定義します。

デフォルトでは、設定のタイムアウトは **10000** ミリ秒 (10 秒) です。

- 設定する値が小さすぎる (例: **500** ミリ秒) と、SSSD に応答するのに十分な時間がない可能性があり、要求は常にタイムアウトを返します。
- 設定する値が大きすぎる (例: **30000** ミリ秒 (30 秒)) と、1 つの要求が、この期間、SSSD への接続をブロックする可能性があります。一度に SSSD に接続できるのは 1 つのスレッドであるため、プラグインからの他のリクエストはすべて待機する必要があります。
- IdM クライアントで多くの要求が送信されると、それは Directory Server 用に設定されたすべての利用可能なワーカーをブロックできます。そのため、サーバーはいずれかの種類の要求に対応できない可能性があります。

以下の状況で設定のタイムアウトを変更します。

- AD ユーザーおよびグループに関する情報を要求する際に、独自の検索タイムアウトが発生する前に IdM クライアントが頻繁にタイムアウトエラーを受け取ると、設定のタイムアウト値が小さすぎます。
- IdM サーバーで Directory Server がロックされていることが多く、**pstack** ユーティリティーは、この時点で多数またはすべてのワーカースレッドが **ipa-extdom** 要求を処理していることを報告する場合は、値が大きすぎます。

たとえば、設定値を **20000** ミリ秒 (20 秒) に設定するには、以下を入力します。

```
# ldapmodify -D "cn=directory manager" -W
dn: cn=ipa_extdom_extop,cn=plugins,cn=config

changetype: modify
replace: ipaExtdomMaxNssTimeout
ipaExtdomMaxNssTimeout: 20000
```

NSS 呼び出しに使用する ipa-extdom プラグインバッファーの最大サイズの設定

ipa-extdom プラグインは、SSSD からのデータを要求する通常の NSS (name service switch) 呼び出しと同じ API を使用する呼び出しを使用します。この呼び出しは、SSSD が要求するデータを格納するバッファーを使用します。バッファーが小さすぎると、SSSD は **ERANGE** エラーを返し、プラグインはより大きなバッファーで要求を再試行します。IdM マスタの Directory Server の **cn=ipa_extdom_extop,cn=plugins,cn=config** エントリーの ***ipaExtdomMaxNssBufSize*** 属性は、バッファーの最大サイズをバイトで定義しています。

デフォルトでは、バッファーは **134217728** バイト (128 MB) です。たとえば、グループに非常に多くのメンバーがあり、すべての名前がバッファーに収まらず、IPA クライアントがグループを解決できない場合にのみ、値を増やしてください。

たとえば、バッファーを **268435456** バイト (256 MB) に設定するには、以下を入力します。

```
# ldapmodify -D "cn=directory manager" -W

dn: cn=ipa_extdom_extop,cn=plugins,cn=config
changetype: modify
replace: ipaExtdomMaxNssBufSize
ipaExtdomMaxNssBufSize: 268435456
```

パート III. LINUX ドメインと ACTIVE DIRECTORY ドメインの統合: 同期

このパートでは、**Active Directory** と **Identity Management** ユーザーを同期する方法、既存の環境を同期から信頼に移行する方法、および **Active Directory** 環境で **ID** ビュー を使用する方法について説明します。

第6章 ACTIVE DIRECTORY ユーザーおよび IDENTITY MANAGEMENT ユーザーの同期

本章では、Active Directory と Red Hat Enterprise Linux Identity Management の同期を説明します。2 つの環境を間接的に統合する方法が 2 種類ありますが、同期はその内の 1 つとなっています。もう 1 つの推奨される方法であるフォレスト間信頼の詳細は、*5章Active Directory および Identity Management を使用したフォレスト間の信頼作成* を参照してください。お使いの環境に選択する方法が不明な場合は、「間接的な統合」 を参照してください。

Identity Management は、同期 によって Active Directory ドメインに保存されるユーザーデータと IdM ドメインに保存されるユーザーデータを組み合わせます。パスワードなどの重要なユーザー属性はサービス間でコピーされ、同期されます。

エントリーの同期は、Windows サーバーに接続してそこからディレクトリーデータを取得するのにフックを使用するレプリケーションと同様のプロセスで実行されます。

パスワードの同期は、Windows サーバーにインストールされ、Identity Management サーバーと通信する Windows サービスで実行されます。

6.1. サポート対象の WINDOWS プラットフォーム

同期は、以下のフォレストやドメイン機能レベルを使用する Active Directory フォレストでサポートされます。

- フォレスト機能レベルの範囲 - Windows Server 2008 ~ Windows Server 2012 R2
- ドメイン機能レベルの範囲 - Windows Server 2008 ~ Windows Server 2012 R2

前述の機能レベルを使用した同期を明示的にサポートし、テストしているオペレーティングシステムは、以下のとおりです。

- Windows Server 2012 R2
- Windows Server 2016

PassSync 1.1.5 およびそれ以降は、サポートされる Windows Server バージョンすべてと互換性があります。

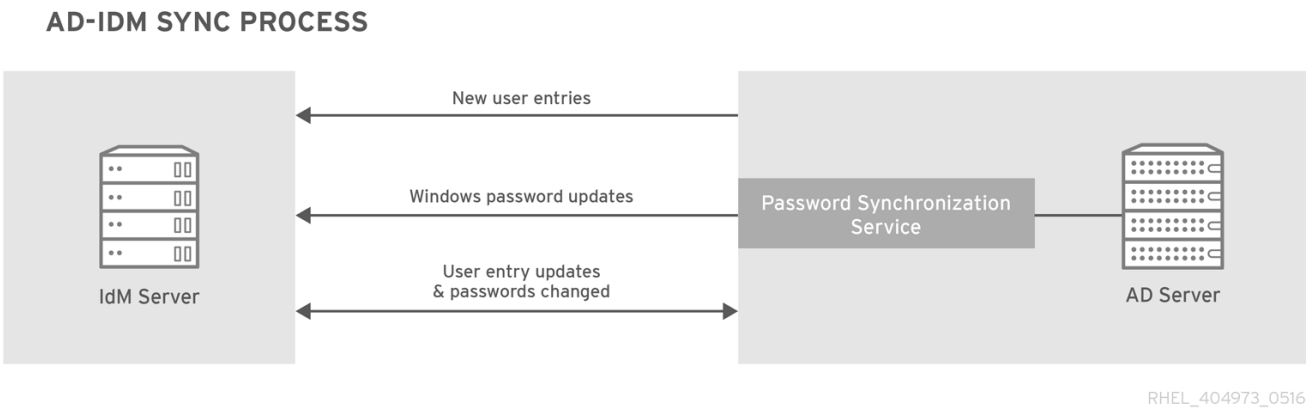
6.2. ACTIVE DIRECTORY および IDENTITY MANAGEMENT の概要

IdM ドメイン内では、情報はデータマスター (サーバーとレプリカ) 間で信頼性と予測性のある方法でコピーされ、複数のサーバーとレプリカ間で共有されます。このプロセスを レプリケーション といいます。

同様のプロセスは、IdM ドメインと Microsoft Active Directory ドメイン間でデータを共有するために使用できます。これが 同期 です。

同期は、Active Directory と Identity Management の間で、ユーザーデータをコピーするプロセスのことです。ユーザーは Active Directory および Identity Management の間で同期され、ディレクトリー同期 (DirSync) LDAP サーバー拡張制御を使用して、変更のあったオブジェクトをディレクトリーから検索します。

図6.1 Active Directory および IdM の同期



同期は、IdM サーバーと Active Directory ドメインコントローラー間の 合意 で定義されます。この合意は、アカウント属性の処理方法を定義するほか、同期するサブツリーなど同期可能なユーザーエントリーを識別するのに必要なすべての情報を定義します。同期合意は、デフォルト値で作成されますが、特定ドメインのニーズに合わせて調整が可能です。2 つのサーバーで同期が行われる場合に、この 2 つのサーバーは ピアと呼ばれます。

表6.1 同期合意内の情報

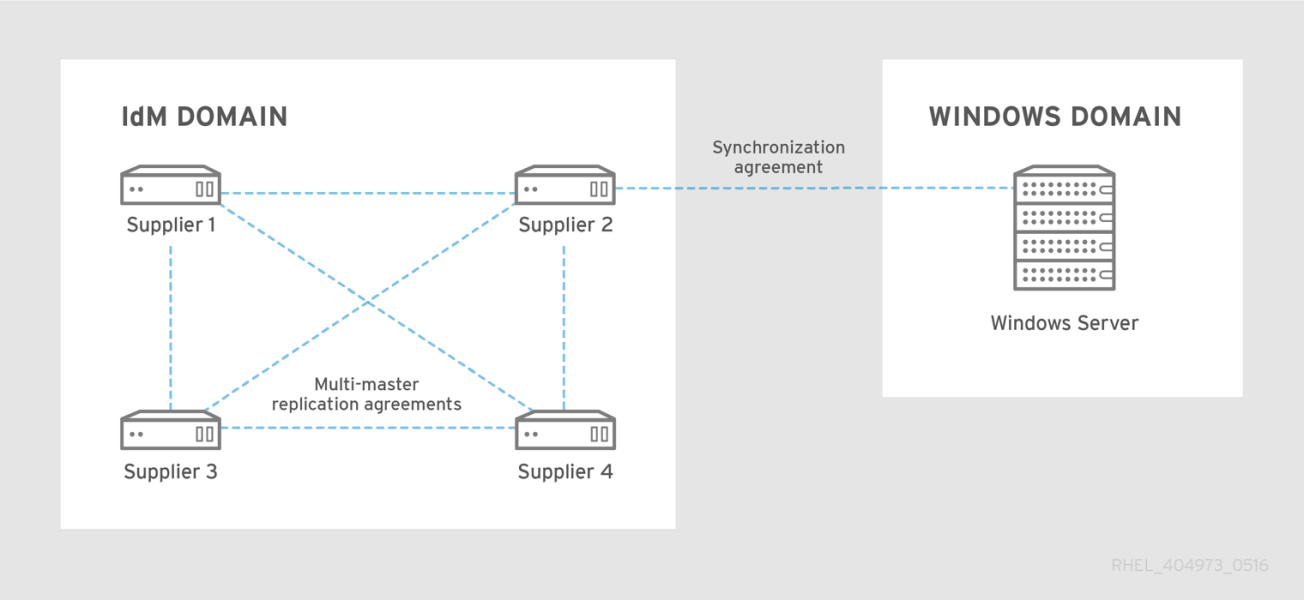
Windows 情報	IdM 情報
● ユーザーのサブツリー (**cn=Users,$SUFFIX**) ● 接続情報 ○ Active Directory 管理者のユーザー名およびパスワード ○ パスワード同期サービスのパスワード ○ CA 証明書	● ユーザーのサブツリー (**ou=People,$SUFFIX**)

同期は通常、双方向 で行われます。情報は、IdM と Windows ドメイン間で送受信され、このプロセスは IdM サーバーとレプリカが情報を共有する方法によく似ています。相違点は新規のユーザーエントリーで、Windows ドメインから IdM ドメインの方向でのみ、追加が可能です。同期は、1 方向のみで行われるように設定することもできます。これは 一方向 の同期と呼ばれます。

データ競合のリスクを回避するには、1 つのディレクトリーのみからユーザーエントリーを追加、または削除する必要があります。このディレクトリーは通常、IT 環境の主要な ID ストアである Windows ディレクトリーであり、新規のアカウントまたはアカウント削除は Identity Management ピアに同期されます。いずれのディレクトリーもエントリーを変更できます。

次に 1 つの Identity Management サーバーと 1 つの Active Directory ドメインコントローラーの間で同期が設定されます。Identity Management サーバーは IdM ドメイン全体に伝播し、ドメインコントローラーは変更を Windows ドメイン全体に伝播します。

図6.2 同期トポロジー



IdM 同期には、以下のような主要な機能があります。

- 同期操作は 5 分ごとに実行されます。この頻度を変更するには、Active Directory ピア DN の **winSyncInterval** 属性を設定します。

  cn=meTo*winserver.ad.example.com*,cn=replica,cn=*dc\3Didm\,dc\3Dexample\,dc\3Dcom*,cn=mapping tree,cn=config

- 同期が設定できるのは、Active Directory ドメイン 1 つのみとなっています。
- 同期が設定できるのは、Active Directory ドメイン **1** つ のみとなっています。
- ユーザー情報のみが同期され、グループ情報は同期されません。
- ユーザー属性とパスワードの両方を同期することができます。
- 変更は双方向ですが (Active Directory から IdM、IdM から Active Directory の両方)、アカウントの作成は、Active Directory から Identity Management への一方向のみになります。新しいアカウントが Active Directory に作成されると、自動的に IdM に対して同期されます。ただし、ユーザーアカウントを IdM で作成した場合には、同期の前に Active Directory にも作成する必要があります。このような場合、同期プロセスは、Active Directory の**sAMAccountName** 属性ではなく、IdM の **uid** 属性と同じ値を持つ一致するアカウントを見つけようとします。一致が見つかると、IdM **ntUserDomainId** 属性は Active Directory の **objectGUID** 値に設定されます。これらの属性は、グローバルで一意かつ不変の値で、移動または名前の変更があった場合でもエントリーはそのまま同期されます。
- アカウントロック情報はデフォルトで同期され、1 つのドメインで無効にされているユーザーアカウントは他方のドメインでも無効にされます。
- パスワードの変更は即時に有効になります。ユーザーパスワードが 1 つのピアで追加または変更される場合、その変更は他のピアサーバーに即時に伝播します。

  パスワード同期クライアントは、新規パスワードまたはパスワード更新を同期します。

  IdM および Active Directory の両方にハッシュ化されたフォームに格納されている既存のパスワードは、Password Synchronization クライアントのインストール時に復号または同期できません。そのため、既存のパスワードは同期されません。ピアサーバー間の同期を開始するに

は、ユーザーパスワードを変更する必要があります。

- 合意は 1 つしか使用できませんが、PassSync サービスは各 Active Directory サーバーにインストールする必要があります。

Active Directory ユーザーが IdM に同期される場合に、特定の属性 (Kerberos および POSIX 属性を含む) では IPA 属性がユーザーエントリーに自動的に追加されます。この属性は、ドメイン内で IdM が使用します。対応する Active Directory ユーザーエントリーには、同期されません。

同期プロセスの一環で、同期データの一部が変更される可能性があります。たとえば、IdM ドメインに同期する場合に、特定の属性を自動的に Active Directory ユーザーアカウントに追加できます。このような属性の変更は、同期合意の一部として定義します。これについては、「ユーザーアカウント属性の同期動作の変更」で説明されています。

6.3. 同期された属性の概要

Identity Management は、IdM と Active Directory ユーザーエントリーの間で、ユーザー属性のサブセットを同期します。エントリーに含まれる他の属性は、Identity Management または Active Directory のどちらにある場合でも、同期時に無視されます。

注記

ほとんどの POSIX 属性は同期されません。

Active Directory の LDAP スキーマと、Identity Management で使用される 389 Directory Server の LDAP スキーマ間には、スキーマは大きな異なりますが、属性は同じものが多数あります。このようなの属性は、Active Directory と IdM ユーザーエントリー間で同期されるだけで、属性名や値の形式には変更が加えられません。

Identity Management および Windows サーバーで同一のユーザースキーマ

- cn[2]
- physicalDeliveryOfficeName
- description
- postOfficeBox
- destinationIndicator
- postalAddress
- facsimileTelephoneNumber
- postalCode
- givenname
- registeredAddress
- homePhone
- sn

- homePostalAddress
- st
- initials
- street
- l
- telephoneNumber
- mail
- teletexTerminalIdentifier
- mobile
- telexNumber
- o
- title
- ou
- userCertificate
- pager
- x121Address

一部の属性には異なる名前が使用されていますが、IdM (389 Directory Server を使用) と Active Directory の間には直接的な対応関係があります。このような属性は、同期プロセスで マッピングされます 。

表6.2 Identity Management と Active Directory との間でマッピングされるユーザースキーマ

ID 管理	Active Directory
cn[a]	name
nsAccountLock	userAccountControl
ntUserDomainId	sAMAccountName
ntUserHomeDir	homeDirectory
ntUserScriptPath	scriptPath
ntUserLastLogon	lastLogon
ntUserLastLogoff	lastLogoff

ID 管理	Active Directory
ntUserAcctExpires	accountExpires
ntUserCodePage	codePage
ntUserLogonHours	logonHours
ntUserMaxStorage	maxStorage
ntUserProfile	profilePath
ntUserParms	userParameters
ntUserWorkstations	userWorkstations

[a] ***cn*** は、Identity Management から Active Directory に同期するときに直接 (***cn*** から ***cn*** に) マップされます。Active Directory から同期する場合、***cn*** は Active Directory の ***name*** 属性から Identity Management の ***cn*** 属性にマップされます。

6.3.1. Identity Management と Active Directory との間のユーザースキーマの相違点

属性が Active Directory と IdM の間で正常に同期される場合でも、Active Directory および Identity Management が基となる X.500 オブジェクトクラスを定義する方法には依然として違いがあり場合があります。この定義方法の相違点により、LDAP サービスが違うと、データの処理方法が異なる可能性があります。

このセクションでは、Active Directory および Identity Management のドメイン間で同期可能な属性を処理する方法に、Active Directory と Identity Management ではどのような違いがあるのかを説明します。

6.3.1.1. cn 属性の値

389 Directory Server では、***cn*** 属性に複数の値を設定できますが、Active Directory ではこの属性には単一の値しか設定できません。Identity Management の ***cn*** 属性が同期されると、単一の値のみが Active Directory ピアに送信されます。

これを同期との関連で見ると、***cn*** 値が Active Directory エントリーに追加され、その値が Identity Management の ***cn*** の値のいずれでもない場合には、Identity Management の ***cn*** 値はすべて単一の Active Directory 値で上書きされる可能性があります。

もう 1 つの重要な相違点として、Active Directory では ***cn*** 属性をその命名属性として使用するのに対し、Identity Management は ***uid*** を使用する点があります。つまり、***cn*** 属性が Identity Management で編集される可能性がある場合には、エントリーの名前が完全に (および間違って) 変更されてしまう可能性があります。

6.3.1.2. street および streetAddress の値

Active Directory は、ユーザーの住所に属性 ***streetAddress*** を使用します。これは、389 Directory Server が ***street*** 属性を使用する方法に相当します。Active Directory と Identity Management がそれぞれ ***streetAddress*** と ***street*** 属性を使用する方法には、2 つの重要な違いがあります。

- 389 Directory Server では、***streetAddress*** は ***street*** の別名です。Active Directory にも ***street*** 属性がありますが、これは独立した値を保持できる別個の属性であり、***streetAddress*** のエイリアスではありません。

- RFC 4519 で指定されているように、Active Directory は ***streetAddress*** と ***street*** の両方を単一値の属性として定義しますが、389 Directory Server は ***street*** を複数値の属性として定義します。

389 Directory Server および Active Directory が ***streetAddress*** および ***street*** 属性を処理する方法が異なるため、Active Directory と Identity Management で address 属性を設定する場合には以下の 2 つのルールに従う必要があります。

- 同期プロセスは、Active Directory エントリーの ***streetAddress*** を Identity Management の ***street*** にマップします。競合を避けるため、Active Directory では ***street*** 属性は使用しないでください。

- Identity Management の ***street*** 属性値は 1 つだけ、Active Directory に同期されます。***streetAddress*** 属性が Active Directory で変更され、新しい値が Identity Management に存在しない場合には、Identity Management のすべての ***street*** 属性値が新しい単一の Active Directory の値に置き換えられます。

6.3.1.3. initials 属性の制約

initials 属性の場合には、Active Directory は最大長 6 文字の制限を課しますが、389 Directory Serve には長さ制限がありません。Identity Management に 7 文字以上の ***initials*** 属性が 追加されると、この値は Active Directory エントリーとの同期時にカットされます。

6.3.1.4. surname (sn) 属性の要求

Active Directory では、surname 属性なしで **person** エントリーを作成できます。ただし、RFC 4519 では、**person** オブジェクトクラスには surname 属性が必要と定義されていますが、これは、Directory Server で使用される定義です。

Active Directory の **person** エントリーが surname 属性なしで作成される場合、このエントリーは、オブジェクトクラス違反で失敗するため、IdM には同期されません。

6.3.2. Active Directory エントリーおよび POSIX 属性

Windows ユーザーアカウントに ***uidNumber*** および ***gidNumber*** 属性の値が含まれている場合、WinSync はこれらの値を Identity Management に同期しません。代わりに、Identity Management に新しい UID および GID の値が作成されます。

その結果、***uidNumber*** と ***gidNumber*** の値は、Active Directory と Identity Management で異なります。

6.4. 同期用の ACTIVE DIRECTORY の設定

IdM では、ユーザーアカウントの同期が有効になっています。同期合意の設定だけが必要となります (「同期合意の作成」)。ただし、Active Directory は、Identity Management サーバーが接続できるように設定する必要があります。

6.4.1. 同期用の Active Directory ユーザーの作成

Windows サーバーでは、IdM サーバーが Active Directory ドメインに接続するために使用するユーザーを作成する必要があります。

Active Directory でのユーザー作成プロセスは、Windows サーバーの文書 (http://technet.microsoft.com/en-us/library/cc732336.aspx) で説明されています。新規のユーザーアカウントには適切な権限を設定する必要があります。

- 同期用のユーザーアカウントには、同期先の Active Directory サブツリーに対して ディレクトリーに加えられた変更を複製する 権限を付与します。同期用のユーザーが同期操作を行うには、レプリケーターの権限が必要です。

  レプリケーターの権限は、http://support.microsoft.com/kb/303972 で説明されています。

- 同期ユーザーを **Account Operators** グループおよび **Enterprise Read-only Domain Controllers** グループのメンバーとして追加します。このユーザーは、**Domain Admins** グループに所属する必要はありません。

6.4.2. Active Directory 認証局の設定

Identity Management サーバーは、セキュアな接続を使用して Active Directory サーバーに接続します。この接続には、Active Directory サーバーで利用可能な CA 証明書または CA 証明書チェーンがあることが条件となります。これらの証明書を Identity Management セキュリティーデータベースにインポートして、Windows サーバーを、信頼されるピアとなるように設定できます。

これは技術的には (Active Directory に対して) 外部の CA で実行できますが、大半のデプロイでは Active Directory で利用可能な証明書サービスを使用する必要があります。

Active Directory での証明書サービスの設定、設定手順は、Microsoft のドキュメント (http://technet.microsoft.com/en-us/library/cc772393(v=WS.10).aspx) に記載されています。

6.5. 同期合意の管理

6.5.1. 同期合意の作成

同期合意は、Active Directory ドメインへの 接続 を作成するため、IdM サーバー上では **ipa-replica-manage connect** コマンドを使用して作成します。Active Directory に対して暗号化された接続を確立するため、IdM は Windows CA 証明書を信頼する必要があります。

1. root 証明局 (CA) の証明書は IdM サーバーにコピーします。

   a. Active Directory CA 証明書が自己署名されている場合は、以下を実行します。

      i. Windows サーバーで Active Directory CA 証明書をエクスポートします。

         A. **Super key**+**R** のキーボードの組み合わせを押して、実行 ダイアログを開きます。

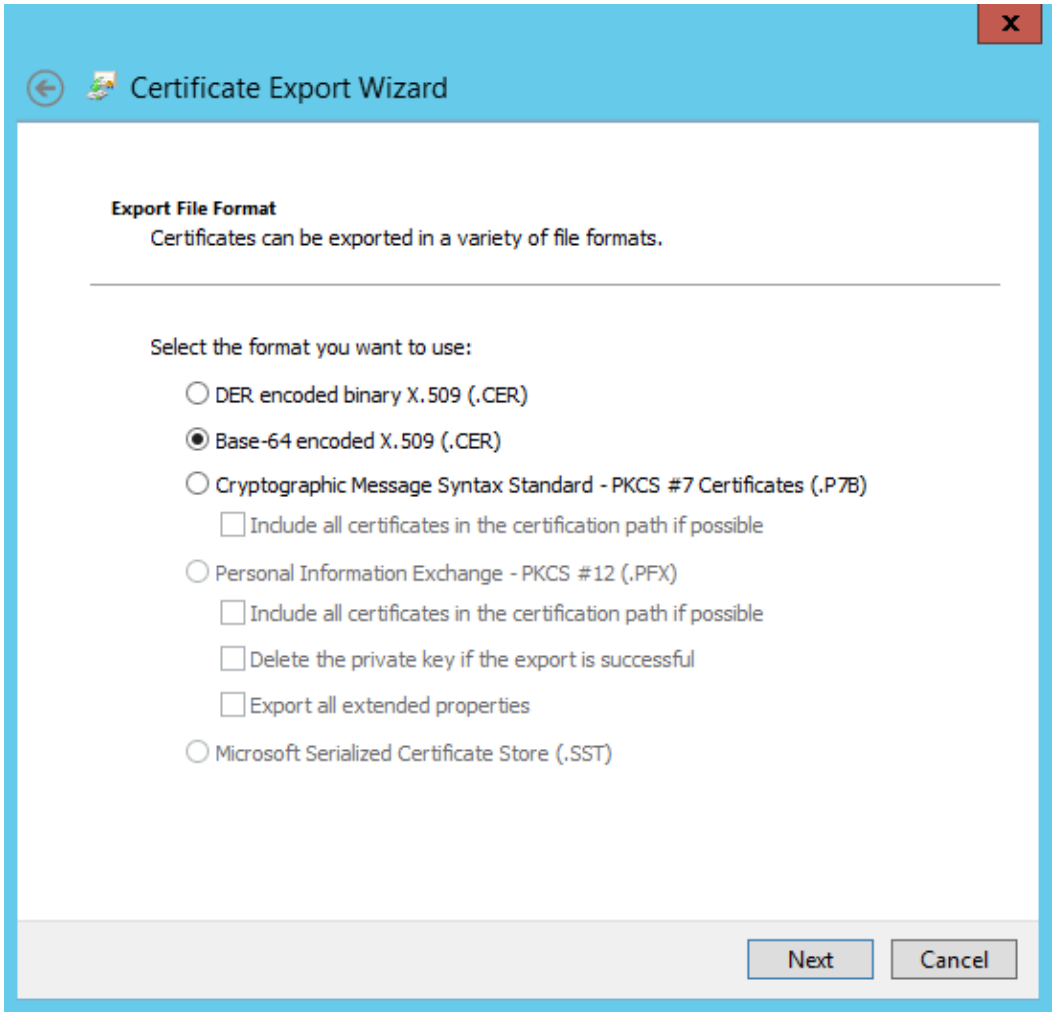
         B. **certsrv.msc** と入力し、**OK** をクリックします。

         C. ローカルの認証局の名前を右クリックし、**Properties** を選択します。

         D. 全般 タブで、**CA certificates** フィールドでエクスポートする証明書を選択し、**View Certificate** をクリックします。

         E. 詳細 タブで、 ファイルにコピー をクリックして 証明書のエクスポートウィザードを起動します。

         F. **Next** をクリックしてから、**Base-64 encoded X.509 (.CER)** を選択します。



G. エクスポートされたファイルに適切なディレクトリーおよびファイル名を指定します。**Next** をクリックして証明書をエクスポートし、**Finish** をクリックします。

H. エクスポートされた証明書を IdM サーバーマシンにコピーします。

b. Active Directory CA 証明書が外部 CA により署名されている場合は、以下を行います。

i. どの証明書が CA root 証明書かを見つけるには、証明書チェーンを表示します。

```
# openssl s_client -connect adserver.example.com:636
CONNECTED(00000003)
depth=1 C = US, O = Demo Company, OU = IT, CN = Demo CA-28
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/O=Demo Company/OU=IT/CN=adserver.example.com
   i:/C=US/O=Demo Company/OU=IT/CN=Demo CA-1
 1 s:/C=US/O=Demo Company/OU=IT/CN=Demo CA-1
   i:/C=US/O=Demo Company/OU=IT/CN=Demo Root CA 2
```

上記の例では、Active Directory サーバーの CA 証明書は、**CN=Demo Root CA 2** で署名された **CN=Demo CA-1** で署名されています。つまり、**CN=Demo Root CA 2** が root CA であることが分かります。

ii. CA 証明書を IdM サーバーにコピーします。

2. IdM サーバー上の既存の Kerberos 資格情報を削除します。

```
$ kdestroy
```

3. **ipa-replica-manage** コマンドを使用して Windows 同期合意を作成します。これには、**--winsync** オプションが必要です。パスワードとユーザーアカウントを同期する場合は、**--passsync** オプションも使用して、パスワード同期に使用するパスワードを設定します。

   --binddn オプションおよび **--bindpw** オプションを指定すると、IdM が Active Directory サーバーへの接続に使用する Active Directory サーバー上のシステムアカウントにユーザー名およびパスワードを設定します。

```
$ ipa-replica-manage connect --winsync \
 --binddn cn=administrator,cn=users,dc=example,dc=com \
 --bindpw Windows-secret \
 --passsync secretpwd \
 --cacert /etc/openldap/cacerts/windows.cer \
 adserver.example.com -v
```

   - **--winsync**: Windows の同期合意として指定します。
   - **--bindDN**: IdM は、Active Directory アカウントのこの DN を使用してリモートディレクトリーにバインドし、属性を同期します。
   - **--bindpw**: 同期アカウントのパスワード。
   - **--cacert**: 以下への完全パスおよびファイル名。
     - Active Directory CA 証明書 (CA が自己署名されている場合)
     - 外部 CA 証明書 (Active Directory CA が外部 CA によって署名されている場合)
   - **--win-subtree**: 同期するユーザーが含まれる Windows ディレクトリーサブツリーの DN。デフォルト値は **cn=Users,$SUFFIX** です。
   - **AD_server_name**: Active Directory ドメインコントローラーの完全修飾ドメイン名 (FQDN)。

4. プロンプトが出されたら、Directory Manager のパスワードを入力します。

5. 任意。「パスワード同期のセットアップ」 に説明されているようにパスワードの同期を設定します。パスワード同期クライアントがない場合、ユーザー属性はピアサーバー間で同期されますが、パスワードは同期されません。

注記

パスワード同期クライアントはパスワード変更を取得し、Active Directory と IdM との間で同期します。これは、新しいパスワードまたはパスワードの更新を同期することを意味します。

IdM および Active Directory の両方にハッシュ化されたフォームに格納されている既存のパスワードは、Password Synchronization クライアントのインストール時に復号または同期できません。そのため、既存のパスワードは同期されません。ピアサーバー間の同期を開始するには、ユーザーパスワードを変更する必要があります。

6.5.2. ユーザーアカウント属性の同期動作の変更

同期合意が作成されると、同期プロセスでのユーザーアカウント属性の処理方法に関して特定のデフォルト動作が定義されます。動作のタイプには、ロックアウト属性の処理方法や異なる DN 形式の処理方法などが含まれます。この動作は、同期合意を編集することで変更できます。

同期合意は LDAP サーバーの特殊なプラグインエントリーとして存在し、それぞれの属性動作は LDAP 属性から設定されます。同期の動作を変更するには、**ldapmodify** コマンドを使用して LDAP サーバーエントリーを直接変更します。

たとえば、アカウントのロックアウト属性はデフォルトで IdM と Active Directory の間で同期されますが、これは ***ipaWinSyncAcctDisable*** 属性を編集することで無効にすることができます。(この属性を変更すると、Active Directory でアカウントが無効な場合でも、IdM で引き続き有効な状態となり、その逆も同様になります)。

```
[jsmith@ipaserver ~]$ ldapmodify -x -D "cn=directory manager" -w password

dn: cn=ipa-winsync,cn=plugins,cn=config
changetype: modify
replace: ipaWinSyncAcctDisable
ipaWinSyncAcctDisable: none

modifying entry "cn=ipa-winsync,cn=plugins,cn=config"
```

以下は、同期設定属性の概要です。

一般ユーザーアカウントのパラメーター

- **ipaWinSyncNewEntryFilter**: 新規ユーザーエントリーに追加するオブジェクトクラスの一覧を含むエントリーの検索に使用する検索フィルターを設定します。

  デフォルト値: **(cn=ipaConfig)**

- **ipaWinSyncNewUserOCAttr**: 新規ユーザーエントリーに追加するオブジェクトクラスの一覧が実際に含まれる設定エントリーの属性を設定します。

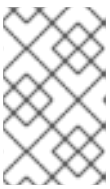
  デフォルト値: **ipauserobjectclasses**

- **ipaWinSyncHomeDirAttr**: POSIX ホームディレクトリーのデフォルトの場所を含むエントリー内の属性を識別します。

  デフォルト値: **ipaHomesRootDir**

- **ipaWinSyncUserAttr**: Active Directory ユーザーを Active Directory ドメインから同期する時に、特定の値で別の属性を設定して AD ユーザーに追加します。複数値の属性の場合は、属性を複数回設定でき、同期プロセスで、値のすべてがエントリーに追加されます。

  例: **ipaWinSyncUserAttr: attributeName attributeValue**



注記

エントリーに属性が存在しない場合に属性値のみが設定されます。属性が存在する場合は、Active Directory エントリーの同期時にエントリーの値が使用されます。

- **ipaWinSyncForceSync**: 既存の AD ユーザーに一致する既存の IdM ユーザーが強制的に同期されるかどうかを設定します。**true** に設定すると、このような IdM ユーザーは自動的に編集され、同期されます。

  使用できる値: **true** | **false**

  IdM ユーザーアカウントに既存の Active Directory ユーザーの ***sAMAccountName*** と同じ ***uid*** パラメーターがある場合、そのアカウントはデフォルトでは 同期されません。この属性は、***ntUser*** および ***ntUserDomainId*** を IdM ユーザーエントリーに自動的に追加するように同期サービスに指示し、それらを同期できるようにします。

ユーザーアカウントのロックパラメーター

- **ipaWinSyncAcctDisable**: アカウントロックアウト属性を同期する方法を設定します。有効にするアカウントロックアウト設定を制御できます。たとえば、**to_ad** は、アカウントロックアウト属性が IdM に設定されると、その値が Active Directory に対して同期され、ローカルの Active Directory 値を上書きすることを意味します。デフォルトでは、アカウントロックアウト属性は両方のドメインから同期されます。

  設定可能な値: **both** (デフォルト)、**to_ad**、**to_ds**、**none**

- **ipaWinSyncInactivatedFilter**: 非アクティブになった (無効になった) ユーザーを保持するために使用されるグループの DN 検索用のフィルターを設定します。これは、ほとんどの実装では変更する必要はありません。

  デフォルト値: **(&(cn=inactivated)(objectclass=groupOfNames))**

グループのパラメーター

- **ipaWinSyncDefaultGroupAttr**: ユーザーのデフォルトグループを確認するために参照する新規ユーザーアカウントの属性を設定します。次に、エントリー内のグループ名を使用して、ユーザーアカウントの ***gidNumber*** を検索します。

  デフォルト値: **ipaDefaultPrimaryGroup**

- **ipaWinSyncDefaultGroupFilter**: ユーザーのデフォルトグループを確認するために参照する新規ユーザーアカウントの属性を設定します。次に、エントリー内のグループ名を使用して、ユーザーアカウントの ***gidNumber*** を検索します。

  デフォルト値: **ipaDefaultPrimaryGroup**

レルムのパラメーター

- **ipaWinSyncRealmAttr**: レルムエントリーにレルム名を含む属性を設定します。

  デフォルト値: ***cn***

- **ipaWinSyncRealmFilter**: IdM レルム名を含むエントリーの検索に使用する検索フィルターを設定します。

  デフォルト値: **(objectclass=krbRealmContainer)**

6.5.3. 同期された Windows サブツリーの変更

同期合意を作成すると、同期されたユーザーデータベースとして使用する 2 つのサブツリーが自動設定されます。IdM の場合、デフォルトは **cn=users,cn=accounts,$SUFFIX** となり、Active Directory の場合、デフォルトは **CN=Users,$SUFFIX** となります。

--win-subtree オプションを使用して同期合意が作成されると、Active Directory サブツリーの値はデフォルト以外の値に設定できます。契約が作成された後、**ldapmodify** コマンドを使用して、同期契約エントリーの ***nsds7WindowsReplicaSubtree*** 値を編集することにより、Active Directory サブツリーを変更できます。

1. **ldapsearch** を使用して同期合意の名前を取得します。この検索では、エントリー全体ではなく、***dn*** および ***nsds7WindowsReplicaSubtree*** 属性の値のみが返されます。

```
[jsmith@ipaserver ~]$ ldapsearch -xLLL -D "cn=directory manager" -w password -p 389 -h
ipaserver.example.com -b cn=config objectclass=nsdswindowsreplicationagreement dn
nsds7WindowsReplicaSubtree

dn:
cn=meToWindowsBox.example.com,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
tree,cn=config
nsds7WindowsReplicaSubtree: cn=users,dc=example,dc=com

... 8< ...
```

2. 同期合意を変更します。

```
[jsmith@ipaserver ~]$ ldapmodify -x -D "cn=directory manager" -W -p 389 -h
ipaserver.example.com <<EOF
 dn:
cn=meToWindowsBox.example.com,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
tree,cn=config
 changetype: modify
 replace: nsds7WindowsReplicaSubtree
 nsds7WindowsReplicaSubtree: cn=alternateusers,dc=example,dc=com
 EOF

 modifying entry
"cn=meToWindowsBox.example.com,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
tree,cn=config"
```

新規のサブツリー設定は即時に有効になります。同期操作が実行中の場合は、現在の操作が完了するとすぐに有効になります。

6.5.4. 一方向の同期の設定

デフォルトでは、すべての変更および削除は双方向で行われます。Active Directory の変更が Identity Management に同期され、Identity Management のエントリーへの変更が Active Directory に同期されます。基本的にこれは、同等のマルチマスターの関係で、Active Directory と Identity Management はどちらも同期時は同等のピアであり、データマスターでもあります。

ただし一部のデータ構造または IT デザインでは、一方のドメインのみをデータマスターとし、他方のドメインでは更新を受け入れられるようにする必要があります。この場合には、マルチマスターの関係 (ピアサーバーが同等) からマスター対コンシュマーの関係に同期関係が変更されます。

これは、同期契約で ***oneWaySync*** パラメーターを設定することによって行われます。使用可能な値は、***fromWindows*** (Active Directory から Identity Management への同期) と ***toWindows*** (Identity Management から Active Directory への同期) です。

たとえば、Active Directory から Identity Management への変更を同期するには、次のコマンドを実行します。

```
[jsmith@ipaserver ~]$ ldapmodify -x -D "cn=directory manager" -w password -p 389 -h
ipaserver.example.com

dn: cn=meToWindowsBox.example.com,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
tree,cn=config
changetype: modify
add: oneWaySync
oneWaySync: fromWindows
```

重要

一方向の同期を有効にしても、同期されていないサーバー上の変更を自動的に回避する訳ではないため、これにより、同期更新間における同期ピア間の不整合が生じる可能性があります。たとえば、一方向同期は Active Directory から Identity Management に送信されるように設定されるので、(基本的には) Active Directory がデータマスターになります。Identity Management でエントリーを変更または削除すると、Identity Management の情報が異なるため、その変更は Active Directory に引き継がれなくなります。次の同期更新時に、編集内容は Directory Server で上書きされ、削除済みのエントリーが再追加されます。

6.5.5. 同期合意の削除

同期を停止するには、同期合意を削除し、IdM と Active Directory サーバーの接続を 切断 します。同期合意を作成する場合とは逆に、同期合意の削除では **ipa-replica-manage disconnect** コマンドおよび Active Directory サーバーのホスト名が使用されます。

1. 同期合意を削除します。

```
# ipa-replica-manage disconnect adserver.ad.example.com
```

2. IdM ディレクトリー証明書データベース内の証明書を一覧表示します。

```
# certutil -L -d /etc/dirsrv/slapd-IDM-EXAMPLE-COM/
Certificate Nickname                    Trust Attributes
                                        SSL,S/MIME,JAR/XPI

IDM.EXAMPLE.COM IPA CA                  CT,C,C
CN=adserver,DC=ad,DC=example,DC=com     C,,
Server-Cert                             u,u,u
```

3. IdM サーバーのデータベースから Active Directory CA 証明書を削除します。

```
# certutil -D -d /etc/dirsrv/slapd-IDM-EXAMPLE-COM/ -n
"CN=adserver,DC=ad,DC=example,DC=com"
```

6.5.6. Winsync 合意のエラー

Active Directory サーバーに接続できないため、同期合意の作成に失敗します。

同期合意での最も一般的なエラーの 1 つとして、IdM サーバーが Active Directory サーバーに接続できない点が挙げられます。

```
"Update failed! Status: [81  - LDAP error: Can't contact LDAP server]
```

これは、合意の作成時に正しくない Active Directory CA 証明書が指定される場合に生じる可能性があります。これにより、IdM LDAP データベース (**/etc/dirsrv/slapd-DOMAIN/** ディレクトリー内) に **Imported CA** という名前で重複した証明書が作成されます。これは、**certutil** を使用して確認できます。

```
$ certutil -L -d /etc/dirsrv/slapd-DOMAIN/

Certificate Nickname                                         Trust Attributes
SSL,S/MIME,JAR/XPI

CA certificate                                               CTu,u,Cu
Imported CA                                                  CT,,C
Server-Cert                                                  u,u,u
Imported CA                                                  CT,,C
```

この問題を解決するには、証明書データベースから CA 証明書を削除します。

```
# certutil -d /etc/dirsrv/slapd-DOMAIN-NAME -D -n "Imported CA"
```

エントリーが存在することを示すため、パスワードが同期されていないことを示すエラーがあります。

ユーザーデータベースの一部のエントリーについて、エントリーがすでに存在するためにパスワードはリセットされないという情報のエラーメッセージが表示される可能性があります。

```
"Windows PassSync entry exists, not resetting password"
```

これはエラーではありません。このメッセージは、適用除外ユーザー、パスワード同期ユーザーが変更されていない場合に生じます。パスワード同期ユーザーは、IdM でパスワードを変更するためにサービスで使用される操作上のユーザーです。

6.6. パスワード同期の管理

ユーザーエントリーの同期は、同期合意で設定されます。ただし、Active Directory と Identity Management の両方のパスワードは、通常のユーザー同期プロセスに含まれません。ユーザーアカウントの作成またはパスワードの変更時にパスワードを取り込み、同期された更新でそのパスワード情報を転送できるようにするには、別のクライアントが Active Directory サーバー上にインストールされる必要があります。

注記

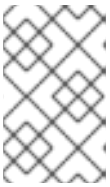
パスワード同期クライアントはパスワード変更を取得し、Active Directory と IdM との間で同期します。これは、新しいパスワードまたはパスワードの更新を同期することを意味します。

IdM および Active Directory の両方にハッシュ化されたフォームに格納されている既存のパスワードは、Password Synchronization クライアントのインストール時に復号または同期できません。そのため、既存のパスワードは同期されません。ピアサーバー間の同期を開始するには、ユーザーパスワードを変更する必要があります。

6.6.1. パスワード同期のための Windows Server のセットアップ

パスワードの同期には、以下の点が必要になります。

- Active Directory が SSL で実行されている必要があります。



注記

エンタープライズルートモードで Microsoft Certificate System をインストールします。Active Directory は自動的に登録され、SSL サーバー証明書を取得します。

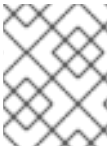
- パスワード同期サービスは、各 Active Directory ドメインコントローラーにインストールする必要があります。Windows からのパスワードを同期するには、PassSync サービスが暗号化されていないパスワードにアクセスし、安全な IdM 接続上でこれを同期する必要があります。ユーザーはパスワードを各ドメインコントローラー上で変更することができるため、PassSync サービスを各ドメインコントローラーにインストールする必要があります。

- パスワードポリシーは、IdM および Active Directory 側で同様に設定する必要があります。同期先で更新済みパスワードを受け取る際には、ソース上のポリシーに対してのみ検証が行われます。同期先での再検証は行われません。

Active Directory パスワードの複雑性ポリシーが有効になっていることを確認するには、Active Directory ドメインコントローラーで実行します。

```
> dsquery * -scope base -attr pwdProperties
  pwdProperties
  1
```

属性 **pwdProperties** の値が **1** に設定されている場合は、パスワードの複雑さポリシーがドメインに対して有効になります。

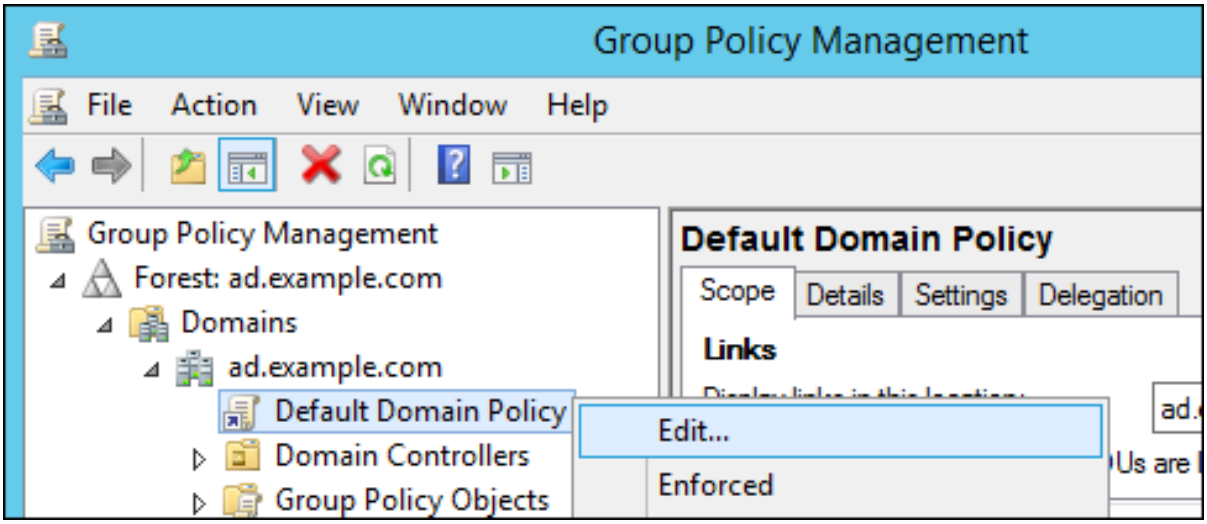


注記

グループポリシーで Organizational Units (ou) の逸脱したパスワード設定が定義されているかどうかわからない場合は、グループポリシー管理者に問い合わせてください。

ドメイン全体で Active Directory パスワードの複雑性設定を有効にするには、以下を実行します。

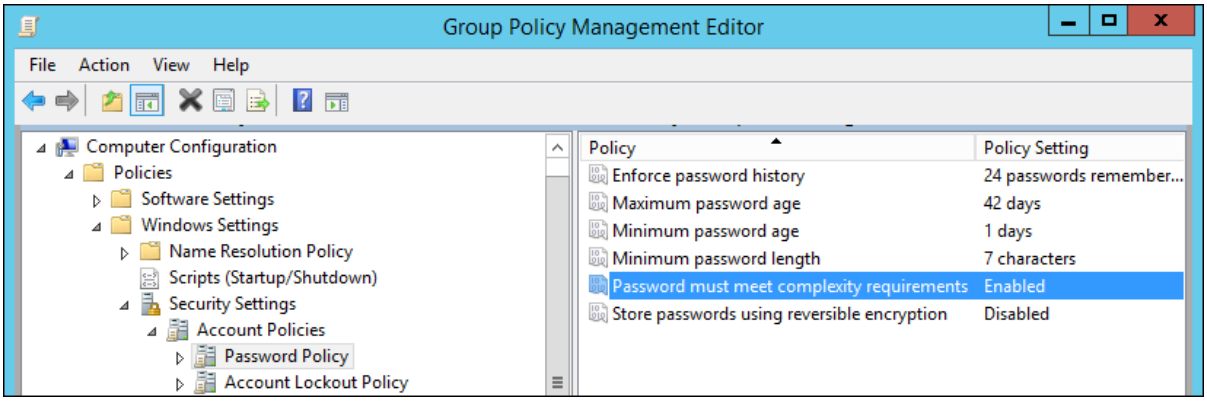
1. コマンドラインから **gpmc.msc** を実行します。
2. **Group Policy Management** を選択します。
3. **Forest:** ***ad.example.com*** → **Domains** → ***ad.example.com*** を開きます。
4. **Default Domain Policy** エントリーを右クリックして、**Edit** を選択します。



5. **Group Policy Management Editor** が自動的に開きます。

6. **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Account Policies** → **Password Policy** を開きます。

7. **Password must meet complexity requirements** オプションを有効にし、保存します。



6.6.2. パスワード同期のセットアップ

Windows パスワードを同期するために、Active Directory ドメインのすべてのドメインコントローラーにパスワード同期サービスをインストールします。

1. **RedHat-PassSync-*.msi** ファイルを Active Directory ドメインコントローラーにダウンロードします。

   a. カスタマーポータルにログインします。

   b. ページ上部の **Downloads** をクリックします。

   c. 製品リストから **Red Hat Enterprise Linux** を選択します。

   d. Red Hat Enterprise Linux 6 または Red Hat Enterprise Linux 7 およびアーキテクチャーの最新版を選択します。

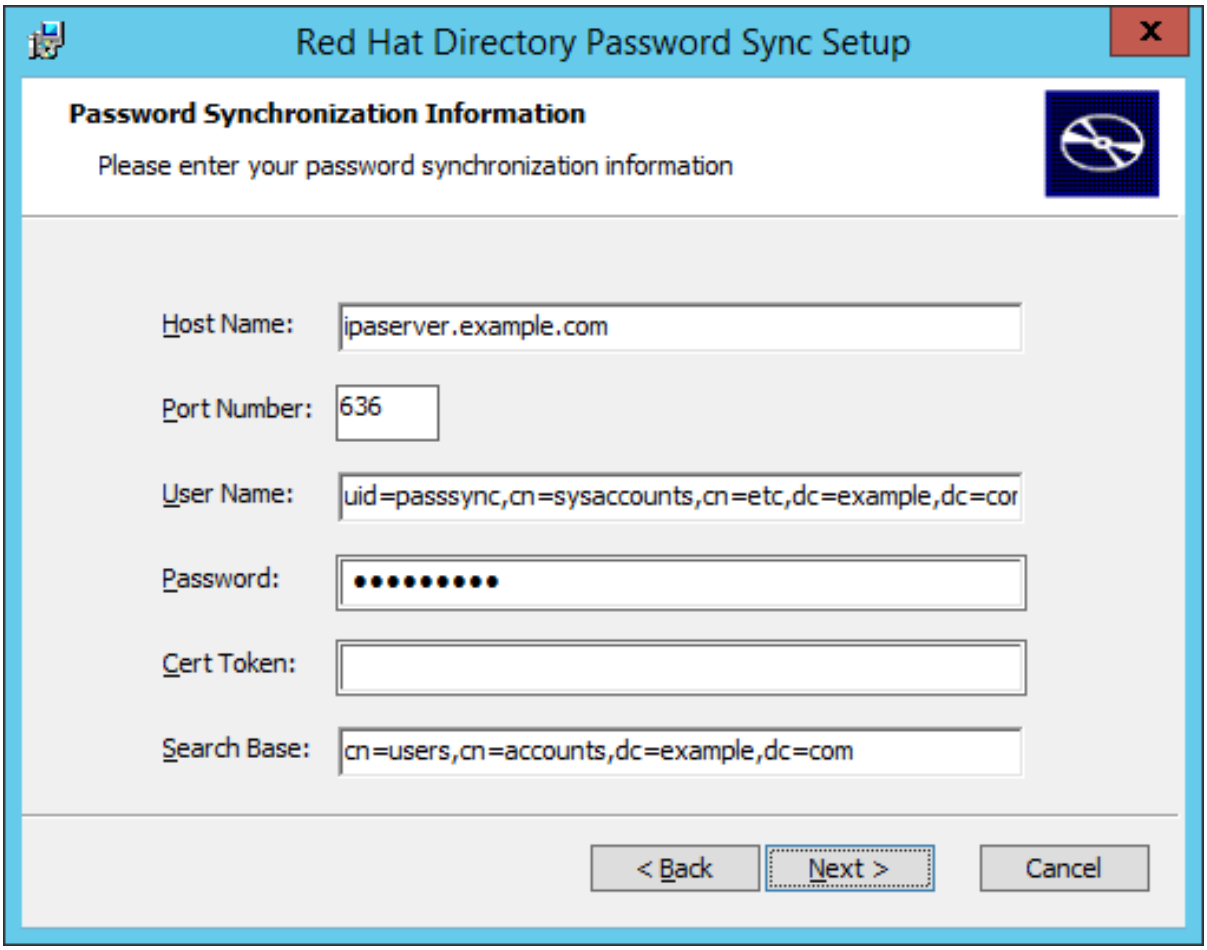
   e. Active Directory ドメインコントローラーのアーキテクチャー用に **WinSync installer** をダウンロードするには、 **Download Now** ボタンをクリックします。

2. **MSI** ファイルをダブルクリックしてインストールします。

3. **Password Synchronrization Setup** 画面が表示されます。**Next** を押して、インストールを開始します。

4. IdM サーバーへの接続を確立するための情報を入力します。

   - ホスト名およびセキュアなポート番号を含む IdM サーバー接続情報。
   - Active Directory が IdM マシンへの接続に使用するシステムユーザーのユーザー名。このアカウントは、同期が IdM サーバー上に設定される場合に自動的に設定されます。デフォルトのアカウントは **uid=passsync,cn=sysaccounts,cn=etc,dc=example,dc=com** です。
   - 同期合意の作成時に **--passsync** オプションに設定されたパスワード。
   - IdM サーバーの people サブツリーの検索ベース。Active Directory サーバーは、**ldapsearch** またはレプリケーション操作と似た IdM サーバーに接続するため、IdM サブツリーでユーザーアカウントを検索する場所を知っている必要があります。ユーザーサブツリーは **cn=users,cn=accounts,dc=example,dc=com** です。
   - 証明書トークンはこの時点では使用されないため、このフィールドは空白にする必要があります。



   Next を押してから **Finish** を押し、Password Synchronization をインストールします。

5. IdM サーバーの CA 証明書を PassSync 証明書ストアにインポートします。

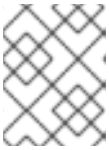
   a. IdM サーバーの CA 証明書を **http://ipa.example.com/ipa/config/ca.crt** からダウンロードします。

   b. IdM CA 証明書を Active Directory サーバーにコピーします。

c. IdM CA 証明書をパスワード同期データベースにインストールします。以下に例を示します。

```
cd "C:\Program Files\Red Hat Directory Password Synchronization"

certutil.exe -d . -A -n "IPASERVER.EXAMPLE.COM IPA CA" -t CT,, -a -i ipaca.crt
```

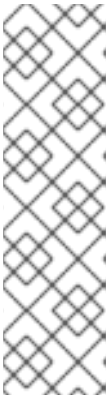
6. Windows マシンを再起動して、Password Synchronization を開始します。



注記

Windows マシンは再起動されている必要があります。再起動しないと **PasswordHook.dll** は有効にされず、パスワードの同期は機能しません。

7. 既存のアカウントのパスワードを同期する必要がある場合は、ユーザーパスワードをリセットします。



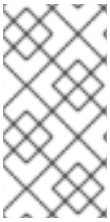
注記

パスワード同期クライアントはパスワード変更を取得し、Active Directory と IdM との間で同期します。これは、新しいパスワードまたはパスワードの更新を同期することを意味します。

IdM および Active Directory の両方にハッシュ化されたフォームに格納されている既存のパスワードは、Password Synchronization クライアントのインストール時に復号または同期できません。そのため、既存のパスワードは同期されません。ピアサーバー間の同期を開始するには、ユーザーパスワードを変更する必要があります。

パスワード同期アプリケーションのインストール時におけるパスワード同期の初回の試行は、Directory Server と Active Directory 同期ピア間の SSL 接続により常に失敗します。証明書およびキーデータベースを作成するためのツールは **.msi** でインストールされます。

パスワード同期クライアントは、IdM **admin** グループのメンバーのパスワードは同期できません。これは、たとえば、パスワード同期エージェントや低レベルのユーザー管理者によるトップレベルの管理者のパスワードを変更できないようにするためのものです。



注記

パスワードは、同期ソースにおいてパスワードポリシーに対して一致するかについてのみ検証されます。Active Directory パスワードの複雑性ポリシーを確認し、有効にするには、「パスワード同期のための Windows Server のセットアップ」 を参照してください。

[2] ***cn*** は、他の同期属性とは異なる扱いを受けます。Identity Management から Active Directory に同期時には、直接 (***cn*** から ***cn*** へ) マッピングされます。ただし、Active Directory から Identity Management に同期する場合には、***cn*** は、Windows の ***name*** 属性から Identity Management の ***cn*** 属性にマッピングされます。

第7章 同期から信頼への既存環境の移行

同期 および *信頼*は、間接的な統合で使用可能な 2 つのアプローチです。同期は一般的に推奨されず、Red Hat では Active Directory (AD) 信頼を基にしたアプローチを推奨しています。詳細は 「間接的な統合」 を参照してください。

本章では、既存の同期ベースの設定を AD 信頼に移行する方法を説明しています。以下の移行オプションは IdM で利用可能です。

- 「**ipa-winsync-migrate** を使用した同期から信頼への自動移行」
- 「ID ビューを使用した同期から信頼への手動での移行」

7.1. IPA-WINSYNC-MIGRATE を使用した同期から信頼への自動移行

重要

ipa-winsync-migrate ユーティリティーは、Red Hat Enterprise Linux 7.2 以降を稼働中のシステムでのみ利用可能です。

7.1.1. ipa-winsync-migrate を使用した移行の仕組み

ipa-winsync-migrate ユーティリティーは、Winsync 環境の既存の設定を保持し、それを AD トラストに転送しながら、同期されたすべてのユーザーを AD フォレストから移行します。Winsync 合意で作成された各 AD ユーザーには、**ipa-winsync-migrate** がデフォルト信頼ビュー内に ID 上書きを作成します (「Active Directory のデフォルト信頼ビュー」 を参照)。

移行完了後には、以下のようになります。

- AD ユーザーの ID 上書きには、Winsync 内の元のエントリーから以下の属性がコピーされます。
  - ログイン名 (**uid**)
  - UID 番号 (**uidnumber**)
  - GID 番号 (**gidnumber**)
  - ホームディレクトリー (**homedirectory**)
  - GECOS エントリー (**gecos**)
- AD 信頼内のユーザーアカウントは、以下を含む IdM 内の元の設定を保持します。
  - POSIX 属性
  - ユーザーグループ
  - ロールベースのアクセス制御ルール
  - ホストベースのアクセス制御ルール
  - SELinux メンバーシップ
  - **sudo** ルール

- 新規 AD ユーザーが外部 IdM グループのメンバーとして追加されます。
- 元の Winsync レプリケーション合意、元の同期済みユーザーアカウント、およびユーザーアカウントのローカルコピーがすべて削除されます。

7.1.2. ipa-winsync-migrate を使用した移行方法

作業を開始する前に:

- **ipa-backup** ユーティリティーを使用する IdM 設定をバックアップする。『Linux ドメイン ID、認証、およびポリシーガイド』 の Identity Management のバックアップと復元 を参照してください。

  理由: 移行は、IdM 設定および多くのユーザーアカウントに多大な影響を及ぼします。バックアップを作成することで、必要な場合は元の設定を復元することができます。

移行は、以下の手順で実行します。

1. 同期されたドメインで信頼を作成します。*5章Active Directory および Identity Management を使用したフォレスト間の信頼作成* を参照してください。
2. **ipa-winsync-migrate** を実行して、AD レルムと、AD ドメインコントローラーのホスト名を指定してください。

   ```
   # ipa-winsync-migrate --realm example.com --server ad.example.com
   ```

   ipa-winsync-migrate が作成した上書き内で競合が発生した場合は、この競合についての情報が表示されますが、移行は継続されます。
3. AD サーバーからのパスワード同期サービスをアンインストールします。これにより、AD ドメインコントローラーから同期合意が削除されます。

このユーティリティーの詳細は、ipa-winsync-migrate(1) の man ページを参照してください。

7.2. ID ビューを使用した同期から信頼への手動での移行

ID ビューを使用すると、AD が以前に AD ユーザー向けに生成した POSIX 属性を手動で変更できます。

1. 元の同期したユーザーまたはグループエントリーのバックアップを作成します。
2. 同期されたドメインで信頼を作成します。信頼を作成する方法の詳細は、*5章Active Directory およびIdentity Management を使用したフォレスト間の信頼作成* を参照してください。
3. 同期されたすべてのユーザーまたはグループについては、IdM で生成される UID および GID を保持するために以下のいずれかを実行します。
   - 特定のホストに適用される ID ビューを個別に作成し、ユーザー ID 上書きをビューに追加する。
   - デフォルト信頼ビューでユーザー ID 上書きを作成する。

   詳細は、異なるホストのユーザーアカウントに対する異なる属性値の定義 を参照してください。

注記

ID ビューは、IdM ユーザーのみが管理できます。AD ユーザーはできません。

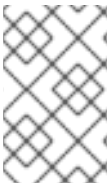
4. 元の同期したユーザーまたはグループのエントリーを削除します。

Active Directory 環境における ID ビューの全般的な情報は、*8章Active Directory 環境での ID ビューの使用* を参照してください。

第8章 ACTIVE DIRECTORY 環境での ID ビューの使用

ID ビューを使用すると、POSIX ユーザーまたはグループ属性に新しい値を指定でき、新しい値が適用されるクライアントホストを 1 つまたは複数定義できます。

Identity Management (IdM) 以外の統合システムでは、IdM で使用されているアルゴリズムとは別のアルゴリズムに基づいて UID や GID の値が生成されることがあります。以前に生成された値を上書きして IdM で使用される値に準拠したものにすることで、別の統合システムのメンバーであったクライアントが IdM に完全に統合できるようになります。



注記

本章では、Active Directory (AD) 関連の ID ビュー機能を説明します。ID ビューの一般的な情報については、Linux ドメイン ID、認証、およびポリシーガイド を参照してください。

AD 環境内では、以下の目的で ID ビューを使用することができます。

POSIX 属性や SSH ログイン詳細といった AD ユーザー属性の上書き

詳細は 「ID ビューを使用した AD ユーザー属性の定義」 を参照してください。

同期ベースから信頼ベースの統合への移行

詳細は 「ID ビューを使用した同期から信頼への手動での移行」 を参照してください。

IdM ユーザー属性のホストごとのグループ上書きの実行

詳細は 「NIS ドメインの IdM への移行」 を参照してください。

8.1. ACTIVE DIRECTORY のデフォルト信頼ビュー

8.1.1. デフォルト信頼ビューとは

デフォルト信頼ビューは、信頼ベースの設定で、AD ユーザーおよびグループに常に適用されるデフォルトの ID ビューです。これは、**ipa-adtrust-install** を使用して信頼を確立すると自動で作成され、削除することはできません。

Default Trust View を使用すると、AD ユーザーおよびグループのカスタム POSIX 属性を定義できます。これにより、AD で定義された値を上書きできます。

表8.1 デフォルト信頼ビューの適用

	AD の値	デフォルトの信頼ビュー		結果
Login	ad_user	ad_user	→	ad_user
UID	111	222	→	222
GID	111	(値なし)	→	111

注記

デフォルト信頼ビューは AD ユーザーおよびグループの上書きのみを受け入れ、IdM ユーザーおよびグループの上書きは受け入れません。IdM サーバーおよびクライアント上で適用されるため、Active Directory ユーザーおよびグループの上書きのみが必要になります。

8.1.2. 他の ID ビューによるデフォルト信頼ビューの上書き

ホストに適用される別の ID ビューがデフォルト信頼ビューの属性値を上書きすると、IdM はデフォルト信頼ビューの上にホスト固有の ID ビューからの値を適用します。

- ホスト固有の ID ビューで属性が定義されている場合、IdM はこのビューからの値を適用します。
- ホスト固有の ID ビューで属性が定義されていない場合、IdM はデフォルト信頼ビューからの値を適用します。

デフォルト信頼ビューは、AD ユーザーおよびグループの他に、IdM サーバーおよびレプリカにも常に適用されます。これらには別の ID ビューを割り当てることはできません。常にデフォルト信頼ビューからの値が適用されます。

表8.2 デフォルト信頼ビューの上にホスト固有の **ID** ビューを適用する

	AD の値	デフォルトの信頼ビュー	ホスト固有のビュー		結果
Login	ad_user	ad_user	(値なし)	→	ad_user
UID	111	222	333	→	333
GID	111	(値なし)	333	→	333

8.1.3. クライアントのバージョンに基づいたクライアントでの ID 上書き

IdM マスターは、IdM クライアントの値の取得方法 (SSSD の使用またはスキーマ互換性ツリーの要求) にかかわらず、デフォルト信頼ビューからの ID 上書きを常に適用します。

ただし、ホスト固有の ID ビューから ID オーバーライドの利用には制限があります。

レガシークライアント: **RHEL 6.3** 以前 **(SSSD 1.8** 以前**)**

このクライアントは、固有の ID ビューを要求して適用することができます。

レガシークライアントでホスト固有の ID ビューを使用するには、クライアントのベース DN を **cn=*id_view_name*,cn=views,cn=compat,dc=*example*,dc=*com*** に変更します。

RHEL 6.4 から **7.0 (SSSD 1.9** から **1.11)**

このクライアントでのホスト固有の ID ビューはサポートされていません。

RHEL 7.1 以降 **(SSSD 1.12** 以降**)**

完全サポート

8.2. ID 競合の解決

IdM は *ID の範囲* を使用して、異なるドメインからの POSIX ID の競合を回避します。ID の範囲に関する詳細は、『Linux ドメイン ID、認証、およびポリシーガイド』 の ID の範囲 を参照してください。

IdM は他の種類の ID 範囲との重複を許可する必要があるため、ID ビューの POSIX ID は特別な範囲タイプを使用しません。たとえば、同期で作成された AD ユーザーは、IdM ユーザーと同じ ID 範囲からの POSIX ID を持つことになります。

POSIX ID は、IdM 側の ID ビューで手動で管理されます。このため、ID の競合が発生すると、競合している ID を変更することでこれを解決することができます。

8.3. ID ビューを使用した AD ユーザー属性の定義

ID ビューでは、AD で定義されるユーザー属性値を変更できます。属性の完全な一覧については、ID ビューで上書き可能な属性 を参照してください。

たとえば、Linux-Windows の混合環境を管理しており、AD ユーザーの POSIX 属性や SSH ログイン属性を手動で定義したい場合に AD ポリシーがこれを許可しない場合は、ID ビューを使用して属性値を上書きすることができます。AD ユーザーが SSSD を実行中のクライアントに対して認証する場合、もしくは compat LDAP ツリーを使用して認証する場合は、新規の値が認証プロセスで使用されます。

注記

ID ビューは、IdM ユーザーのみが管理できます。AD ユーザーはできません。

属性値を上書きするプロセスは、以下のようになります。

1. 新しい ID ビューを作成します。
2. ID ビューにユーザー ID 上書きを追加し、必要な属性値を指定します。
3. ID ビューを特定のホストに適用します。

これらの手順を実行する方法は、『Linux ドメイン ID、認証、およびポリシーガイド』 の ホストごとにユーザーアカウントで異なる属性値を定義 を参照してください。

8.4. NIS ドメインの IDM への移行

Linux 環境を管理しており、異なる UID や GID がある各種の NIS ドメインを最新のアイデンティティー管理ソリューションに移行する場合は、ID ビューを使用してホスト固有の UID および GID を既存ホスト向けに設定し、既存ファイルおよびディレクトリーのパーミッション変更を防ぐことができます。

移行プロセスは、以下のようになります。

1. IdM ドメインにユーザーおよびグループを作成します。詳細は以下参照
   - stage または Active ユーザーの追加
   - ユーザーグループの追加と削除
2. ID ビューを既存ホストに使用して、ユーザー作成中に IdM が生成した ID を上書きします。
   1. 個別の ID ビューを作成します。

2. ユーザーおよびグループの ID 上書きを ID ビューに追加します。

3. ID ビューを特定のホストに割り当てます。

詳細は、異なるホストのユーザーアカウントに対する異なる属性値の定義 を参照してください。

3. 『Linux ドメイン ID、認証、およびポリシーガイド』 の Identity Management クライアントのインストールおよびアンインストール

4. NIS ドメインの使用を停止します。

8.5. ショートネームを使用したユーザーやグループの解決/認証に対する設定オプション

このセクションでは、**user_name@domain** や **domain\user_name** の完全修飾名形式ではなく、略式のユーザーまたはグループ名を使用して、Active Directory (AD) 環境のユーザーやグループを解決し、認証できるような設定オプションを説明します。これは、以下のいずれかで設定できます。

- AD を信頼するアイデンティティ管理 (IdM)
- SSSD で AD が連携された Red Hat Enterprise Linux

8.5.1. ドメイン解決の概要

ドメイン解決順序 オプションを使用して、ドメインのリストを検索して特定のユーザー名に一致するものを返す順序を指定できます。このオプションを設定できます。

- サーバー上では以下の設定になります。参照:
  - 「ドメイン解決順のグローバル設定」
  - 「ID ビューのドメイン解決順の設定」
- クライアント上では以下の設定になります。「IdM クライアントでのドメイン解決順の設定」を参照してください。

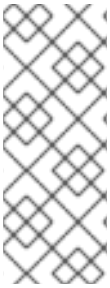
Active Directory 信頼を使用する環境では、サーバーベースのオプションを 1 つまたは両方適用することが推奨されます。

特定のクライアントの観点から見ると、**domain resolution order** オプションは、上記の 3 つの場所の中から複数の場所に設定できます。クライアントが 3 つの場所を参照する順番は、以下のとおりです。

1. ローカルの **sssd.conf** 設定
2. ID ビューの設定
3. グローバル IdM 設定

最初に検出されたドメイン解決の順番のみが使用されます。

Red Hat Enterprise Linux が直接 AD に統合されている環境では、クライアントにのみドメイン解決順序を設定できます。



注記

以下の場合には、修飾名を使用する必要があります。

- ユーザー名が複数のドメインに存在する場合
- SSSD 設定には **default_domain_suffix** オプションが含まれ、そのオプションを指定せずにドメインに対して要求を行う場合

8.5.2. Identity Managment サーバー上でのドメイン解決順の設定

ドメインまたはサブドメイン内の多数のクライアントが同じドメイン解決順を使用する場合は、サーバーベースの設定を選択します。

8.5.2.1. ドメイン解決順のグローバル設定

トラスト内の全クライアントにこのドメイン解決順を設定するにはこのオプションを選択します。これには、**ipa config-mod** コマンドを使用します。たとえば、複数の子ドメインを使用する AD フォレストを信頼する IdM ドメインでは、以下を実行します。

```
$ ipa config-mod --domain-resolution-
order='idm.example.com:ad.example.com:subdomain1.ad.example.com:subdomain2.ad.example.com
'
Maximum username length: 32
Home directory base: /home
...
Domain Resolution Order:
idm.example.com:ad.example.com:subdomain1.ad.example.com:subdomain2.ad.example.com
...
```

このような方法でドメイン解決順を設定した場合は、IdM ドメイン、信頼済みの AD フォレストのどちらからのユーザーであっても、ショートネームのみを使用してログインできます。

8.5.2.2. ID ビューのドメイン解決順の設定

このオプションを選択して、特定のドメイン内にあるクライアントに設定を適用します。

たとえば、サブドメインサーバー *server.idm.example.com* で、*subdomain1.ad.example.com* からよりも、*subdomain2.ad.example.com* サブドメインからのログインの方がはるかに多く検出されます。ただし、グローバルな解決順序の状態では、ユーザー名の解決時に、*subdomain2.ad.example.com* の前に *subdomain1.ad.example.com* サブドメインのユーザーデータベースが試行されます。特定のサーバーに別の順序を設定するには、特定のビューのドメイン解決順序を設定します。

1. **domain resolution order** オプションを指定して ID ビューを作成します。

```
$ ipa idview-add example_view --desc "ID view for custom shortname resolution on
server.idm.example.com" --domain-resolution-order
subdomain2.ad.example.com:subdomain1.ad.example.com
---------------------------------
Added ID View "example_view"
---------------------------------
ID View Name: example_view
Description: ID view for custom shortname resolution on server.idm.example.com
Domain Resolution Order: subdomain2.ad.example.com:subdomain1.ad.example.com
```

2. クライアントにビューを適用します。以下に例を示します。

```
$ ipa idview-apply example_view --hosts server.idm.example.com
-----------------------------------
Applied ID View "example_view"
-----------------------------------
hosts: server.idm.example.com
-------------------------------------------
Number of hosts the ID View was applied to: 1
-------------------------------------------
```

ID ビューの詳細情報は、*8章Active Directory 環境での ID ビューの使用* を参照してください。

8.5.3. IdM クライアントでのドメイン解決順の設定

少数のクライアントに設定する場合や、クライアントを直接 AD に接続する場合は、クライアントにドメイン解決順を設定します。

/etc/sssd/sssd.conf ファイルの [sssd] セクションで、 **domain_resolution_order** オプションを設定します。以下に例を示します。

```
domain_resolution_order = subdomain1.ad.example.com, subdomain2.ad.example.com
```

domain_resolution_order オプションの設定に関する詳細は、sssd.conf(5) の man ページを参照してください。

付録A 更新履歴

改訂番号はこのマニュアルの編集に関するものであり、Red Hat Enterprise Linux の バージョン番号とは関係ありません。

改訂 7.0-51 Thu Mar 4 2021 Florian Delehaye
本ガイドの 7.9 GA バージョン。DNA ID 範囲を手動で調整するための新しいセクションを追加。

改訂 7.0-50 Wed May 27 2020 Florian Delehaye
いくつかの修正および更新。

改訂 7.0-49 Tue Aug 06 2019 Marc Muehlfeld
7.7 GA 公開用ドキュメントバージョン

改訂 7.0-48 Wed Jun 05 2019 Marc Muehlfeld
『トラストエージェントの設定』 を更新し、『AD プロバイダーが信頼ドメインを処理する方法』 と 『SSSD によって表示されるユーザー名の形式の変更』 を追加。

改訂 7.0-47 Tue Apr 08 2019 Marc Muehlfeld
いくつかの若干の修正と更新。

改訂 7.0-46 Mon Oct 29 2018 Filip Hanzelka
7.6 GA 公開用ドキュメントの準備。

改訂 7.0-45 Mon Jun 25 2018 Filip Hanzelka
『SMB 共有アクセス用の SSSD と Winbind の切り替え』 の追加。

改訂 7.0-44 Thu Apr 5 2018 Filip Hanzelka
7.5 GA 公開用ドキュメントの準備。

改訂 7.0-43 Wed Feb 28 2018 Filip Hanzelka
『SSSD がサポートする GPO 設定』 の更新。

改訂 7.0-42 Mon Feb 12 2018 Aneta Šteflová Petrová
『共有シークレットを使用した双方向の信頼の作成』 の更新。

改訂 7.0-41 Mon Jan 29 2018 Aneta Šteflová Petrová
若干の修正。

改訂 7.0-40 Fri Dec 15 2017 Aneta Šteflová Petrová
若干の修正。

改訂 7.0-39 Mon Dec 6 2017 Aneta Šteflová Petrová
『Active Directory 統合での Samba の使用』 の更新。

改訂 7.0-38 Mon Dec 4 2017 Aneta Šteflová Petrová
信頼用の 『DNS およびレルムの設定』 の更新。

改訂 7.0-37 Mon Nov 20 2017 Aneta Šteflová Petrová
『共有シークレットを使用した双方向の信頼の作成』 の更新。

改訂 7.0-36 Mon Nov 6 2017 Aneta Šteflová Petrová
若干の修正。

改訂 7.0-35 Mon Oct 23 2017 Aneta Šteflová Petrová

『Active Directory エントリーおよび POSIX 属性』 および 『SSSD のプロバイダーとしての ID マッピングでの AD ドメインの設定』 の更新。

改訂 7.0-34 Mon Oct 9 2017 Aneta Šteflová Petrová
『短い名前を使用するための設定オプション』 の追加。『信頼コントローラーおよび信頼エージェント』 の更新。

改訂 7.0-33 Tue Sep 26 2017 Aneta Šteflová Petrová
SSSD の章の自動検出セクションの更新。信頼ドメインの設定に関する 2 セクションの追加。

改訂 7.0-32 Tue Jul 18 2017 Aneta Šteflová Petrová
7.4 GA 公開用ドキュメントバージョン

改訂 7.0-31 Tue May 23 2017 Aneta Šteflová Petrová
セキュリティー ID マッピングに関する若干の修正。

改訂 7.0-30 Mon Apr 24 2017 Aneta Šteflová Petrová
Windows 統合定義に関する若干の修正。

改訂 7.0-29 Mon Apr 10 2017 Aneta Šteflová Petrová
直接的な統合の更新。

改訂 7.0-28 Mon Mar 27 2017 Aneta Šteflová Petrová
ユーザーが他のユーザーのパスワードを正常に変更することを許可をパスワードリセットの有効化に変更して Linux ドメイン ID ガイドに移動。信頼に対応する Windows プラットフォームを更新。無効になっていたリンクを修正。その他の若干の更新。

改訂 7.0-27 Mon Feb 27 2017 Aneta Šteflová Petrová
信頼のポート要件を更新。信頼および同期に関する若干の再構築。その他の若干の更新。

改訂 7.0-26 Wed Nov 23 2016 Aneta Šteflová Petrová
ipa-winsync-migrate を追加。信頼、SSSD、および同期の各章で若干の修正。

改訂 7.0-25 Tue Oct 18 2016 Aneta Šteflová Petrová
7.3 GA リリースのバージョン。

改訂 7.0-24 Thu Jul 28 2016 Marc Muehlfeld
図を更新、サービスおよびホストの Kerberos フラグを追加、その他の若干の修正。

改訂 7.0-23 Thu Jun 09 2016 Marc Muehlfeld
同期の章の更新。Kerberos の章の削除。その他の若干の修正。

改訂 7.0-22 Tue Feb 09 2016 Aneta Petrová
realmd の更新、index の削除、ID ビューの一部を Linux ドメイン ID ガイドに移動、その他の若干の更新。

改訂 7.0-21 Fri Nov 13 2015 Aneta Petrová
7.2 GA リリース向けのバージョンに若干の更新。

改訂 7.0-20 Thu Nov 12 2015 Aneta Petrová
7.2 GA リリース向けのバージョン。

改訂 7.0-19 Fri Sep 18 2015 Tomáš Čapek
スプラッシュページに並び替え順序の更新。

改訂 7.0-18 Thu Sep 10 2015 Aneta Petrová
出力形式の更新。

改訂 7.0-17 Mon Jul 27 2015 Aneta Petrová

GPO ベースのアクセス制御の追加、その他の多くの若干の変更。

改訂 7.0-16 **Thu Apr 02 2015** **Tomáš Čapek**
ipa-advise を追加、SSSD を使用した CIFS 共有を拡大、UNIX 拡張のアイデンティティー管理の警告。

改訂 7.0-15 **Fri Mar 13 2015** **Tomáš Čapek**
7.1 向けの最終変更を含む非同期更新。

改訂 7.0-13 **Wed Feb 25 2015** **Tomáš Čapek**
7.1 GA リリース向けバージョン。

改訂 7.0-11 **Fri Dec 05 2014** **Tomáš Čapek**
スプラッシュページでの分類順序を更新して再構築。

改訂 7.0-7 **Mon Sep 15 2014** **Tomáš Čapek**
セクション 5.3 信頼の作成をコンテンツの更新のために一時的に削除。

改訂 7.0-5 **June 27, 2014** **Ella Deon Ballard**
Samba+Kerberos+Winbind の各章の改善。

改訂 7.0-4 **June 13, 2014** **Ella Deon Ballard**
Kerberos レルムの章の追加。

改訂 7.0-3 **June 11, 2014** **Ella Deon Ballard**
初期リリース。