



Red Hat Enterprise Linux 7

Windows 統合ガイド

Linux システムの Active Directory 環境との統合

Red Hat Enterprise Linux 7 Windows 統合ガイド

Linux システムの Active Directory 環境との統合

Filip Hanzelka
Red Hat Customer Content Services
fhanzelk@redhat.com

Lucie Maňásková
Red Hat Customer Content Services
lmanasko@redhat.com

Aneta Šteflová Petrová
Red Hat Customer Content Services

Marc Muehlfeld
Red Hat Customer Content Services

Tomáš Čapek
Red Hat Customer Content Services

Ella Deon Ballard
Red Hat Customer Content Services

法律上の通知

Copyright © 2018 Red Hat, Inc.

This document is licensed by Red Hat under the [Creative Commons Attribution-ShareAlike 3.0 Unported License](https://creativecommons.org/licenses/by-sa/3.0/). If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

概要

このドキュメントは、プレビュー版として提供されています。本書は作成中で、大きな変更が加えられる可能性があります。本書に含まれる情報は、不完全なものとし、慎重に使用するようになっています。異種の IT 環境には、シームレスな通信が必要な各種のドメインやオペレーティングシステムが含まれています。Red Hat Enterprise Linux は、Linux を Microsoft Windows の Active Directory (AD) に緊密に統合するための複数の方法を提供します。この統合は、複数のユーザー、グループ、サービス、またはシステムを含む複数の異なるドメインオブジェクトに対して実行できます。本書では、軽量 AD パススルー認証から本格的な Kerberos で信頼できるレムまでのさまざまな統合シナリオについても説明します。Red Hat Enterprise Linux Identity Management に関する他の機能およびサービスについての資料は、本ガイドのほかに以下のガイドがあります。Linux ドメイン ID、認証、およびポリシーガイドでは、Linux ベースのドメイン内における認証および承認ポリシーに加え、ID ストアを集中管理するソリューションである Red Hat Identity Management について説明しています。システムレベルの認証ガイドでは、authconfigユーティリティーや System Security Services Daemon (SSSD) サービス、プラグ可能な認証モジュール (PAM) フレー

ムワーク、Kerberos、certmonger ユーティリティー、アプリケーション用のシングルサインオン (SSO) など、ローカルシステム上で認証設定に使用可能な異なるアプリケーションやサービスについて説明しています。

目次

第1章 ACTIVE DIRECTORY と LINUX 環境の統合方法	4
1.1. WINDOWS 統合の定義	4
1.2. 直接的な統合	5
1.3. 間接的な統合	6
パート I. 単一の LINUX システムの ACTIVE DIRECTORY ドメインへの追加	8
第2章 SSSD のアイデンティティプロバイダーとしての ACTIVE DIRECTORY の使用	9
2.1. SSSD 用の AD プロバイダーの設定	9
2.2. KERBEROS ホストキータブの自動更新	13
2.3. ダイナミック DNS 更新の有効化	13
2.4. SSSD での範囲取得検索の使用	14
2.5. グループポリシーオブジェクトのアクセス制御	14
2.6. 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	16
2.7. SSSD クライアントおよび ACTIVE DIRECTORY DNS サイトの自動検出	17
第3章 REALMD を使用した ACTIVE DIRECTORY ドメインへの接続	19
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	19
3.2. REALMD 使用の前提条件	19
3.3. REALMD コマンド	19
3.4. ID ドメインの検出および参加	20
3.5. ID ドメインからのシステムの削除	24
3.6. ドメインの一覧表示	24
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	25
3.8. デフォルトユーザー設定の変更	26
3.9. ACTIVE DIRECTORY ドメインエントリーの追加設定	26
第4章 ACTIVE DIRECTORY 統合での SAMBA の使用	28
4.1. ドメインユーザー認証での WINBINDD の使用	28
4.2. SSSD および WINBIND での SMB 共有の使用	28
4.3. その他のリソース	30
パート II. LINUX ドメインと ACTIVE DIRECTORY ドメインの統合: フォレスト間信頼	31
第5章 ACTIVE DIRECTORY および IDENTITY MANAGEMENT によるフォレスト間の信頼作成	32
5.1. フォレスト間の信頼について	32
5.2. フォレスト間の信頼作成	40
5.3. フォレスト間信頼環境の管理および設定	58
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	73
5.5. 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	75
5.6. レガシー LINUX クライアントでの ACTIVE DIRECTORY 信頼	76
パート III. LINUX ドメインと ACTIVE DIRECTORY ドメインの統合: 同期	80
第6章 ACTIVE DIRECTORY と IDENTITY MANAGEMENT ユーザーの同期	81
6.1. サポートされる WINDOWS プラットフォーム	81
6.2. ACTIVE DIRECTORY および IDENTITY MANAGEMENT について	81
6.3. 同期された属性について	84
6.4. 同期用の ACTIVE DIRECTORY の設定	87
6.5. 同期合意の管理	88
6.6. パスワード同期の管理	95

第7章 同期から信頼への既存環境の移行	101
7.1. IPA-WINSYNC-MIGRATE を使用した同期から信頼への自動移行	101
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	102
第8章 ACTIVE DIRECTORY 環境での ID ビューの使用	104
8.1. ACTIVE DIRECTORY のデフォルト信頼ビュー	104
8.2. ID 競合の解決	106
8.3. ID ビューを使った AD ユーザー属性の定義	106
8.4. NIS ドメインの IDM への移行	106
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	107
付録A 改訂履歴	110

第1章 ACTIVE DIRECTORY と LINUX 環境の統合方法

IT 環境にはそれぞれの構造があり、IT 環境内のシステムは目的別に配置されます。2 つの別々のインフラストラクチャーを統合するには、それぞれの環境のインフラストラクチャーの目的を判断し、それらがどのように、またどこで相互に作用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 環境間で必要とされる相互作用により、異なるものになります。個々の Linux システムを Windows ドメインに登録する、Linux ドメインを Windows ドメインのピアに設定する、またはこれらの環境間で情報をコピーする、などが挙げられます。

Windows ドメインと Linux システム間にはいくつかの接点があります。これらの接点では、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) の識別とその識別に使用されるサービスが主に実行されます。

ユーザー識別子および認証

- ユーザーアカウントが置かれる場所: Windows (AD ドメイン) 上で実行される中央の認証システムか、または Linux 上で実行される中央のアイデンティティおよび認証サーバーか?
- Linux システムのユーザーの認証方法: ローカル Linux 認証システムか、または Window 上で実行される中央認証システムか?
- ユーザーのグループメンバーシップの設定方法: グループメンバーシップの判別方法は?
- ユーザーの認証方法: ユーザー名/パスワードのペア、Kerberos チケット、証明書、またはこれらのメソッドの組み合わせが使用されるのか?
- Linux マシンのサービスへのアクセスに必要な POSIX 属性の保存方法: これらの属性は Windows ドメインで設定されるか、Linux システムでローカルに設定されるか、または動的にマップされるか (UID/GID 番号と Windows SID)?
- どのユーザーがどのリソースにアクセスするか: Windows で定義されたユーザーは Linux リソースにアクセスできるか? Linux で定義されたユーザーは Windows リソースにアクセスできるか?

ほとんど環境では、Active Directory ドメインがユーザー情報の中央ハブになります。Linux システムが認証要求のためにユーザー情報にアクセスするには何らかの経路が必要になります。ここでは、そのユーザー情報を取得する方法にはどのようなものがあり、そのユーザー情報のうち、外部システムが利用できる情報はどの程度あるかという点を考えることができます。また、Linux システム (POSIX 属性) および Linux ユーザー (特定のアプリケーション管理者) に必要な情報とその情報が管理される方法との間には一定のバランスが必要です。

ホストおよびサービスプリンシパル

- どのリソースがアクセスされるか?
- どの認証プロトコルが必要か?
- Kerberos チケットはどのように取得されるか? SSL 証明書はどのように要求され、検証されるか?
- ユーザーは単一ドメイン、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 設定をどのように行うか？
- 単一 DNS ドメインがあるか？複数のサブドメインがあるか？
- システムのホスト名はどのように解決されるか？
- サービス検出はどのように設定されるか？

セキュリティポリシー

- アクセス制御の指示が設定される場所は？
- 各ドメインに設定される管理者は？

変更管理

- システムがドメインに追加される頻度はどの程度か？
- DNS サービスなど、Windows 統合の関連要素についての基礎的な設定が変更される場合、それらの変更はどのように伝播されるか？
- 設定はドメイン関連のツールまたはプロビジョニングシステムで維持されるか？
- 統合パスには Windows サーバー上のアプリケーションまたは設定が追加が必要か？

ドメイン内の統合される要素と同様に、その統合がどのように維持されるかも重要な点になります。環境内に頻繁に更新されるシステムが多数含まれる場合には、手作業に大きく依存する特定の統合方法は保守の面で機能しない可能性があります。

以下のセクションでは、Windows との統合についての主要なシナリオを概略します。直接的な統合では、Linux システムは Active Directory に追加の中継なしに接続されます。一方、間接的な統合ではアイデンティティサーバーが使用されます。このサーバーは Linux システムを中央で管理し、その環境全体をサーバー対サーバーレベルで Active Directory に接続します。

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、中央のアイデンティティおよび認証ソース (この場合は AD) と対話します。もう 1 つのコンポーネントは、利用可能なドメインを検出し、正しい認証ソースを使用するように 1 つ目のコンポーネントを設定します。情報を取得し、AD に対して認証を実行するために使用できるオプションは複数あります。それらには以下が含まれます。

ネイティブ LDAP と 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** が含まれます。PAM 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ロードされるので、それらは実行環境に直接影響を与えます。キャッシュやオフラインサポート、またはアクセス資格情報の保護などがない場合は、NSS および PAM 用に基本的な LDAP および Kerberos モジュールを使用することは、機能的に制限があるために推奨されません。

Samba Winbind

Samba Winbind の使用は、Linux システムを AD に接続する従来の方法でした。Winbind は Linux システム上で Windows クライアントをエミュレートし、AD サーバーに通信できます。System Security Services Daemon (SSSD) の最新バージョンでは Samba Winbind と SSSD 間に機能的な

キャップはなくなり、SSSD は Winbind の置き換えとして使用できるようになりました。Winbind を依然として使用する必要があるケースも稀にありますが、一般的には Winbind が第一のオプションとして使用されることはなくなりました。

以下の点に留意してください。

- マルチフォレスト 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フレームワークから、リモートのアイデンティティおよび認証リソースにアクセスすることです。SSSD は詳細な設定が可能で、PAM および NSS 統合を提供するだけでなく、中央サーバーから取得されるコアおよび拡張ユーザーデータと共にローカルユーザーを保存するデータベースを提供します。SSSD は、Active Directory、Red Hat Enterprise Linux の Identity Management (IdM)、または汎用的な LDAP または Kerberos サーバーのいずれでも、ユーザーが選択するアイデンティティサーバーに Linux システムを接続する際に推奨されるコンポーネントです。

以下の点に留意してください。

- SSSD との直接統合は、デフォルトでは単一の AD フォレスト内でのみ機能します。マルチフォレスト環境では、以下のナレッジベースソリューションを参考にして手動でドメイン列挙を設定します: [Joining SSSD to domains in different forests](#)。
- **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 に切り替える主な理由には、SSSD が直接的な統合および間接的な統合の両方に利用でき、多額の移行コストなしにある統合アプローチを別の統合アプローチに切り替えることができる点があります。Linux システムを AD に直接的に統合するために SSSD または Winbind を設定する際の最も便利な方法として、**realmd** サービスを使用することができます。このサービスを使用することにより、呼び出し元は、標準的な方法でネットワークの認証およびドメインのメンバーシップを設定することができます。**realmd** サービスは、アクセス可能なドメインおよびレルムについての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ために詳細な設定を必要としません。

直接的な統合は、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 システムのシェアが拡大すると、通常デプロイメントにおいてホストベースのアクセス制御、sudo、または SELinux ユーザーのマッピングなどのアイデンティティ関連のポリシーをより効果的に一元管理する必要が生じます。最初は Linux システムのこれらの分野の設定はローカル設定ファイルで維持することができますが、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を使用する方が、設定ファイルの配信と管理をより簡単に行うことができます。ただし、この方法では設定ファイルを変更してからファイルを配信することによるオーバーヘッドが生じます。直接的な統合における拡張が予想されない場合は、次のセクションで説明する間接的な統合を検討するとよいでしょう。

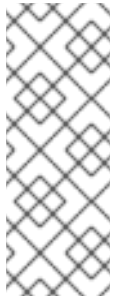
1.3. 間接的な統合

間接的な統合の主な利点は、Active Directory (AD) ドメインのユーザーが Linux システムおよびサービスに透過的にアクセスできるようにすると共に、Linux システムとそれらのシステムに関するポリシーを一元的に管理できる点にあります。この間接的な統合には、以下のような 2 つの異なるアプローチがあります。

信頼ベースのソリューション

推奨されるアプローチとしては、Red Hat Enterprise Linux の Identity Management (IdM) を Linux システムを制御する中央サーバーとして利用し、AD とのクロスレルム Kerberos 信頼を設定し、AD のユーザーがログオンおよび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できるようにする方法があります。このソリューションでは、Kerberos 機能を使用して異なるアイデンティティソース間の信頼を設定します。IdM は自らを別個のフォレストとして AD に表示し、AD でサポートされるフォレストレベルの信頼の利点を活用します。

複雑な環境では、単一の IdM フォレストは複数の AD フォレストに接続することができます。このセットアップにより、組織内の異なる業務/機能をより効果的に分離することができます。AD 管理者はユーザーおよびユーザー関連のポリシーに焦点を当て、Linux 管理者は Linux インフラストラクチャーを全面的に管理します。このケースでは、IdM で制御される Linux レルムは AD リソースドメインまたはレルムに類似しますが、Linux システムがこれに組み込まれています。



注記

Windows では、すべてのドメインが Kerberos レルムであると同時に DNS ドメインになります。ドメインコントローラーで管理されるすべてのドメインには、独自の専用 DNS ゾーンが設定されている必要があります。IdM がフォレストとして AD によって信頼される場合にも同じことが当てはまります。AD は IdM に独自の DNS ドメインがあることを期待します。信頼のセットアップが機能するには、DNS ドメインを Linux 環境の専用ドメインとして設定する必要があります。

信頼環境では、IdM により *ID views* を使用して、IdM サーバー上の AD ユーザーの POSIX 属性を設定できる点に注意してください。詳細は以下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

これは信頼ベースソリューションの代替ソリューションで、IdM または Red Hat Directory Server (RHDS) でも利用できるユーザー同期機能を使用します。ユーザーアカウント (RHDS の場合はグループアカウントも含む) を AD から IdM または RHDS に同期させることができますが、反対方向ではできません。ただし、ユーザー同期には以下のような制約があります。

- ユーザーの重複
- パスワード同期の必要性。これには AD ドメインのすべてのドメインコントローラーで特殊なコンポーネントが必要になります。
- パスワード取得が可能になるには、全ユーザーが最初にパスワードを手動で変更する必要があります。
- 同期は単一ドメインにのみ対応。
- 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 内で 1 つのドメインコントローラーのみが使用可能。

統合シナリオによってはユーザーの同期オプションしか選択できない場合がありますが、一般的には同期アプローチがクロスレルムの信頼ベース統合よりも奨励されることはありません。

パート I. 単一の **LINUX** システムの **ACTIVE DIRECTORY** ドメインへの追加

第2章 SSSD のアイデンティティプロバイダーとしての ACTIVE DIRECTORY の使用

System Security Services Daemon (SSSD) は、リモートの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。SSSD は、ローカルシステム (SSSD *client*) と外部のバックエンドシステム (*domain*) を接続します。これにより、SSSD クライアントが SSSD プロバイダーを使用して、アイデンティティと認証リモートサービスにアクセスできます。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、Kerberos レalm などがあります。

SSSD は、AD 統合のアイデンティティ管理サービスとして使用する場合には、NIS または Winbind などのサービスの代わりとなります。本章では、SSSD が AD とどのように連携するのかを説明します。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. SSSD 用の AD プロバイダーの設定

AD プロバイダーを使用すると、SSSD が LDAP のアイデンティティプロバイダーと Kerberos 認証プロバイダーを使用し、AD 環境の最適化を図ることができます。

2.1.1. 統合オプションの概要

Linux と Windows のシステムは、ユーザーやグループに異なる識別子を使用します。

- Linux は、ユーザー ID (UID) および グループ ID (GID) を使用します。『システム管理者のガイド』の『[ユーザーとグループの管理](#)』を参照してください。Linux UID と 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。

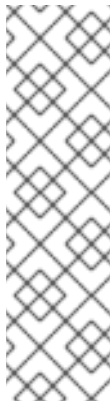
AD ユーザーなど、Red Hat Enterprise Linux システムに対して認証を行うユーザーには、必ず UID と GID を割り当てる必要があります。この目的で、SSSD は以下の統合オプションを提供します。

AD ユーザーに対する新規 UID と GID の自動生成

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で POSIX ID をアルゴリズム的に生成できます。ID マッピングにより、AD の SID と Linux の ID 間のマッピングを作成します。

- SSSD により新しい AD ドメインが検出されると、この新規ドメインに利用可能な ID 範囲を割り当てます。そのため、すべての SSSD クライアントマシンの各 AD ドメインには同じ ID 範囲が設定されます。
- 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 により、ユーザーの SID やそのドメインの ID 範囲をベースにした UID など、ユーザーのエントリーが SSSD キャッシュに作成されます。
- AD ユーザーの ID は、同じ SID をもとに、一貫したかたちで生成されるので、ユーザーはどの Red Hat Enterprise Linux システムにログインする場合も同じ UID と GID を使用します。

『[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 にマッピングする場合には、マッピングは一貫性が保たれますが、一部のクライアントが異なるソフトウェアを使用する場合には、以下のいずれかを選択してください。

- 同じマッピングアルゴリズムが全クライアントで使用されていることを確認します。
- [AD に定義されている 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 に定義されている POSIX 属性の使用

AD は、`uidNumber`、`gidNumber`、`unixHomeDirectory`、または `loginShell` などの POSIX 属性を作成して保存します。

[AD ユーザーに対する新規 UID と GID の自動生成](#) で説明されている ID マッピングを使用する場合には、SSSD は新しい UID および GID を作成し、AD で定義されている値を上書きします。AD で定義された値を保持するには、SSSD の ID マッピングを無効にします。

「[SSSD が AD で定義されている POSIX 属性を使用するように設定](#)」を参照してください。

2.1.2. 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 システムの両方が正しく設定されていることを確認してください。

- 名前解決の設定を確認します。特に、DNS SRV レコードを検証します。たとえば、`ad.example.com` という名前のドメインの場合には、以下を実行してください。
 - DNS SRV の LDAP レコードを検証します。

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

- AD レコードを検証します。

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

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

- 両システムのシステム時刻が同期されていることを確認します。これで、Kerberos が正しく機能できるようになります。
- Linux システムとすべての AD ドメインコントローラー両方で [必要とされるポート](#) を、Linux システムから AD ドメインコントローラー、AD ドメインコントローラーから Linux システムの両方向で開放します。

表2.1 SSSD を使用して Linux と AD を直接統合するのに必要なポート

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	パスワードの設定や変更には 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 オプションを使用する場合
NTP	123	UDP	オプション

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 *realm* を使用した Active Directory ドメインへの接続](#)を参照してください。**realm** スイートは、自動的に必要な設定すべてを編集します。以下に例を示します。

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

realm を使用しない場合には、手動でシステムを設定できます。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: ユーザーのホームディレクトリーおよびシェルの設定

pam_ouddjob_mkhome ライブラリーは、ユーザーが Linux システムに初回ログインした時に、自動的にホームディレクトリーを作成します。デフォルトでは、SSSD は AD アイデンティティ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 クライアントでディレクトリーの形式をカスタマイズするには、以下を実行します。

1. **/etc/sss/sss.conf** ファイルを開きます。
2. **[domain]** セクションで、以下のオプションのいずれかを使用します。
 - **fallback_homedir** は、フォールバックするホームディレクトリー形式を設定し、ホームディレクトリーが AD に定義されていない場合のみ使用されます。
 - **override_homedir** はホームディレクトリーを設定して、AD に定義されているホームディレクトリーを常に上書きします。

たとえば、**/home/domain_name/user_name** の形式を常に使用するようにします。

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


詳細は、`sssd.conf(5)` man ページを参照してください。

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

1. `/etc/sss/sss.conf` ファイルを開きます。
2. 以下のオプションを使用して、必要なユーザーシェルの設定を定義します。
 - **shell_fallback** はフォールバック値を設定し、シェルが AD で定義されていない場合にのみ使用されます。
 - **override_shell** は、AD で定義したシェルの常に上書き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、許可するシェルまたはブラックリストに追加するシェルの一覧を設定します。

詳細は、`sssd.conf(5)` man ページを参照してください。

新規設定の読み込み

- 設定ファイルを変更した後に SSSD を再起動します。

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

その他のリソース

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

2.1.3. SSSD が AD で定義されている POSIX 属性を使用するように設定

注記

以前のリリースでは、ユーザーアカウントに POSIX 属性を提供するために *UNIX のアイデンティティ管理* 拡張が提供されていました。この拡張は、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 のアイデンティティ管理を使用してきた場合には、よくある質問の回答については [このナレッジ記事](#) を参照してください。

Unix のアイデンティティ管理および *Unix* のサービス パッケージに関する以前の手順については、以下の Red Hat ナレッジアーティクルを参照してください。

- [POSIX 属性を使用した Active Directory ドメインの設定](#)
- [LDAP ドメインとしての Active Directory の設定](#)

推奨情報

最適なパフォーマンスを実現するためには、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には、SSSD は LDAP ポート上にある個別のドメインコントローラーに直接接続します。

AD ドメインへの Linux システムの参加

「[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](#)」の手順に従うようにしてください。

SSSD での ID マッピングの無効化

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



注記

`realm` ユーティリティーを使用してドメインと結合し、`--automatic-id-mapping=no` スイッチを追加した場合には、`realm` ユーティリティーにより SSSD は `ldap_id_mapping = false` ですでに設定されています。

3. 以前にデフォルトの ID マッピング設定が指定されたユーザーを要求した場合には、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 からの POSIX 属性を使用します。

2.2. KERBEROS ホストキータブの自動更新

SSSD は、`adcli` がインストールされている場合には、AD 環境にある Kerberos ホストの keytab ファイルを自動的に更新します。このデーモンは、マシンのアカウントのパスワードが設定値よりも古い場合に、必要に応じてこ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、以下を実行します。

1. `/etc/sss/sss.conf` ファイルで、AD プロバイダーに対して以下のパラメーターを追加します。

```
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 keytab 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。

2.3. ダイナミック DNS 更新の有効化

AD は、そのクライアントが DNS レコードを自動的に更新することを許可します。さらに、AD は DNS レコードをアクティブに維持し、非アクティブなレコードのタイムアウトおよび削除などを実行し、これらのレコードの更新状態を維持できます。DNS の削除機能については AD 側ではデフォルトで有効で

はありません。

SSSD は、DNS レコードを更新して Linux システムが Windows クライアントを模倣できるようにします。さらにレコードが非アクティブとマークされて DNS レコードから削除されることを防ぎます。動的 DNS 更新が有効にされると、クライアントの DNS レコードが以下のタイミングで更新されます。

- アイデンティティプロバイダーがオンラインになる時点 (常時)
- Linux システムが再起動する時点 (常時)
- 指定された間隔 (任意の設定)。デフォルトでは、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 リースと同じ間隔を設定することができます。このように設定した場合には、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、DNS の Kerberos/GSSAPI (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ることを意味します。

動的 DNS 設定は各ドメインに対して設定されます。以下が例になります。

```
[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に関する詳細は、`sssd-ad(5)` man ページを参照してください。

2.4. SSSD での範囲取得検索の使用

SSSD は、AD の **範囲取得**を使用した検索機能をサポートします。範囲取得検索に関する詳細は、[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にカスタムのフィルターを設定する場合には、非常に大規模なグループには、これらのフィルターは正しく機能しない可能性があります。

2.5. グループポリシーオブジェクトのアクセス制御

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、名前と値のペアなどのポリシー設定の集合で、これらはドメインコントローラー (DC) に保存され、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されます。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。

2.5.1. SSSD と GPO アクセス制御の連携

SSSD が GPO のアクセス制御を適用できるように設定するには、SSSD はホストシステムと AD ユーザーに適用可能な GPO を取得します。取得した GPO 設定をもとに、SSSD は、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 と Windows クライアントが AD ドメインコントローラーで集約的に受け入れるログインポリシーを定義できるようになります。



重要

セキュリティフィルタリングは、セキュリティフィルターにリストすることで、GPO アクセス制御の範囲を特定のユーザー、グループまたはホストにさらに絞り込むことができる機能です。ただし、SSSD はそのセキュリティフィルター内のユーザーおよびグループしかサポートしません。SSSD は、このセキュリティフィルターのホストのエントリーを無視します。

SSSD が GPO アクセス制御が特定のシステムに適用されるようにするには、AD ドメインに新規の OU を作成し、OU にこのシステムを移動して、GPO をこの OU にリンクします。

2.5.2. SSSD がサポートする GPO 設定

表2.2 SSSD が取得する GPOアクセス制御オプション

GPO オプション [a]	対応の <code>sssd.conf</code> オプション [b]
ローカルでのログインを許可します ローカルでのログインを拒否します。	<code>ad_gpo_map_interactive</code>
リモートデスクトップサービスを使ったログオンを許可します リモートデスクトップサービスを使ったログオンを拒否します	<code>ad_gpo_map_remote_interactive</code>
ネットワークから対象のコンピューターにアクセスします ネットワークから対象のコンピューターへのアクセスを拒否します	<code>ad_gpo_map_network</code>
バッチジョブとしてログオンを許可します バッチジョブとしてログオンを拒否します	<code>ad_gpo_map_batch</code>
サービスとしてログオンを許可します サービスとしてログオンを拒否します	<code>ad_gpo_map_service</code>
[a] Windows のグループポリシーマネージャーで指定されています。	
[b] これらのオプションに関する詳細および、デフォルトで GPO オプションがマッピングされている、プラグ可能な認証モジュール (PAM) サービスについては、 <code>sssd-ad(5) man</code> ページを参照してください。	

2.5.3. SSSD 用の GPO ベースのアクセス制御設定

GPO ベースのアクセス制御は、`/etc/sss/sss.conf` ファイルで設定します。**`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。アクセスが拒否されると、**`syslog`** メッセージが記録されます。これが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を使用して **`ad_gpo_access_control`** を **`enforcing`** モードに設定する前に、**`ad_gpo_access_control`** を **`permissive`** モードに設定してログを検証することが推奨されます。**`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 **`sss.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`** では、どの PAM サービスを特定の Windows ログイン権限にマッピングするかを設定します。

PAM サービスを、固有の GPO 設定にマッピングされている PAM サービスのデフォルトリストに追加するか、リスト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、対話ログインにマッピングされた PAM サービスの一覧 (ローカルでのログインを許可および拒否する GPO 設定) から **`su`** サービスを削除するには、以下を実行します。

```
ad_gpo_map_interactive = -su
```

- **`ad_gpo_cache_timeout`** オプションでは、後続のアクセス制御リクエストが DC から新たに取得するのではなく、キャッシュに保存されているファイルを再利用可能な間隔を指定します。

利用可能な GPO パラメーターの詳細一覧とその説明およびデフォルト値については、`sss-ad(5) man` ページを参照してください。

2.5.4. その他のリソース

- SSSD と GPO を連携させるように設定する方法は、Red Hat ナレッジベースの [「Configure SSSD to respect Active Directory SSH or Console/GUI GPO」](#) を参照してください。

2.6. 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、取得した全 AD ユーザーにユーザーのプライベートグループを自動的に作成し、GID の番号がすでに使用済みでない限り、GID がユーザーの UID と一致す

るようにします。競合を回避するには、ユーザー UID と同じ GID を持つグループがサーバー上に存在しないようにします。

GID は、AD に格納されていないので、AD ユーザーはグループの機能の利点を活用でき、LSAP データベースに必要な空のグループが含まれないようにします。

2.6.1. AD ユーザー用にユーザーのプライベートグループの自動作成を有効化する手順

AD ユーザー用にユーザーのプライベートグループの自動作成を有効化します。

1. `/etc/sss/sss.conf` ファイルを編集して、`[domain/LDAP]` セクションに以下を追加します。

```
auto_private_groups = true
```

2. sssd サービスを再起動して、sss データベースを削除します。

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

この手順を実行した後に、すべての AD ユーザーには UID と同じ GID が割り当てられています。

```
# 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)
```

2.6.2. AD ユーザー用のユーザーのプライベートグループの自動作成を無効化する手順

AD ユーザー用にユーザーのプライベートグループの自動作成を無効化します。

1. `/etc/sss/sss.conf` ファイルを編集して、`[domain/LDAP]` セクションに以下を追加します。

```
auto_private_groups = false
```

2. sssd サービスを再起動して、sss データベースを削除します。

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

この手順を実行した後は、全 AD ユーザーには、全体で同一の GID が割り当てられます。

```
# 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)
```

2.7. 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、多数の異なるドメインコントローラー、ドメイン、サブドメイン、物理

サイトなどで構成され、非常に大規模になる可能性があります。Active Directory は、サイトというコンセプトを使用し、ドメインコントローラーの物理的なロケーションを特定します。これにより、クライアントが、地理的に近いドメインコントローラーに接続できるようになり、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 サイトを検出氏、最寄りのドメインコントローラーに接続します。このプロセスは、以下の手順で構成されます。

1. SSSD は、AD フォレストの DNS サーバーからの SRV レコードにクエリーを送信します。返されるレコードには、フォレスト内の DC 名が含まれています。
2. SSSD は、これらの各 DC に LDAP の ping を送信します。DC が設定した間隔内に応答しない場合には、要求がタイムアウトし、SSSD は次の DC に LDAP の ping を送信します。接続に成功すると、応答には、SSSD クライアントが所属する AD サイトに関する情報が含まれます。
3. SSSD は次に、DNS サーバーからの SRV レコードにクエリーを送信し、所属するサイト内の DC を特定し、そのうちの 1 つに接続します。



注記

SSSD は、デフォルトで所属する AD サイトを記憶します。このように、SSSD は自動検出プロセス時にこのサイト内の DC に直接 LDAP の Ping を送信して、サイト情報を更新することができます。その結果、通常タイムアウトが発生しないので、自動検出の手順は非常に高速になります。

このサイトが存在しないか、クライアントが別のサイトに割り当てられている場合には、SSSD はフォレスト内の SRV レコードにクエリの送信を開始し、再度今プロセス全体を繰り返します。

自動検出を無効にするには `/etc/sss/sss.conf` ファイルの `[domain]` セクションの **`ad_site`** オプションを使用して、クライアントを接続する AD サイトを指定します。

その他のリソース

- **`ad_site`** に関する詳細は、`sss-ad(5) man` ページを参照してください。
- Identity Management と Active Directory の間に信頼関係がある環境については、[「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。

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、アイデンティティドメインを検出してドメインに参加し、直接のドメイン統合を達成する明確で簡単な方法を提供します。SSSD や Winbind といった基礎となる Linux システムサービスがドメインに接続できるように設定します。

[2章SSSD のアイデンティティプロバイダーとしての Active Directory の使用](#)では、システムセキュリティサービスデーモン (SSSD) をローカルシステムおよび Active Directory でバックエンドのアイデンティティプロバイダーとして使用する方法を説明しています。このためにシステムを適切に設定することは、複雑なタスクになります。それぞれの使用可能なアイデンティティプロバイダーおよび SSSD 自体には数多くの異なる設定パラメーターがあります。また、すべてのドメイン情報は事前に利用可能にしておく必要があり、その後に SSSD がローカルシステムをAD に統合できるよう SSSD 設定で適切にフォーマットされる必要があります。

realmd はこの設定を単純化します。利用可能な AD および Identity Management ドメインを識別する検索を実行し、システムをドメインに参加させるとともに、指定された ID ドメインに接続してユーザーアクセスを管理するために必要となるクライアントサービスを設定します。また、SSSD は基礎となるサービスとして複数のドメインをサポートするため、**realmd** も複数のドメインを検出し、サポートすることができます。

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に対応しています。

- Microsoft Active Directory
- Red Hat Enterprise Linux Identity Management

realmd は、以下のドメインクライアントに対応しています。

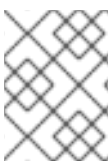
- Red Hat Enterprise Linux Identity Management および Microsoft Active Directory の SSSD
- Microsoft Active Directory の Winbind

3.2. REALMD 使用の前提条件

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** のパッケージがインストール済みであることを確認してください。これらは **realmd** を使用するシステムの管理に必要となります。



注記

「[ID ドメインの検出および参加](#)」での説明にあるように、**realmd** を使用してインストールするパッケージを確認できます。

3.3. REALMD コマンド

realmd システムには、以下の 2 つの主要タスクがあります。

- ドメインにおけるシステム登録の管理
- ドメインユーザーのローカルシステムリソースへのアクセス設定

realm の中心となるのは **realm** というユーティリティです。**realm** のほとんどのコマンドでは、実行するアクションと、ドメインやユーザーアカウントなどのアクションの実行対象となるエンティティを指定する必要があります。

```
realm command arguments
```

例:

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

表3.1 realm コマンド

コマンド	説明
Realm コマンド	
discover	ネットワーク上のドメインの検出スキャンを実行します。
join	システムを指定されたドメインに追加します。
leave	指定されたドメインからシステムを削除します。
list	システム用に設定されたすべてのドメイン、または検出され、設定されたすべてのドメインを一覧表示します。
ログインコマンド	
permit	設定されたドメイン内の指定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	設定されたドメイン内の指定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制限します。

realm コマンドについての詳細は、**realm(8)** man ページを参照してください。

3.4. ID ドメインの検出および参加

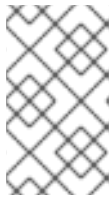
realm discover コマンドは完全なドメイン設定と、システムをドメインに登録するためにインストールが必要となるパッケージの一覧を返します。

realm join コマンドは、ローカルシステムのサービスと ID ドメイン内のエントリーの両方を設定することにより、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ようになります。

1. 指定されたドメインについて検出スキャンを実行します。

2. システムがドメインに参加するために必要となるパッケージを自動的にインストールします。

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では **PackageKit** スイートが実行中である必要があることに注意してください。



注記

PackageKit が無効な場合は、システムが不足しているパッケージを要求します。このため、それらのパッケージを **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. ディレクトリー内にシステムのアカунツエントリーが作成されて、ドメインに参加します。
4. **/etc/krb5.keytab** ホストキータブファイルを作成します。
5. SSSD 内でドメインを設定し、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に対してドメインユーザーを有効にします。

ドメインの検出

realm discover コマンドをオプションなしで実行すると、デフォルトの DNS ドメインについての情報が表示されます。これは、Dynamic Host Configuration Protocol (DHCP) で割り当てられるドメインになります。

```
# 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
```

特定のドメインを検出するように実行することも可能で、その場合は以下のように **realm discover** に検出するドメイン名を追記します。

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

すると **realmd** システムは DNS SRV ルックアップを使っ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見つけます。



注記

realm discover コマンドの使用には NetworkManager が実行中である必要があります。特に NetworkManager の D-Bus インターフェースに依存しています。システムが NetworkManager を使用していない場合は、**realm discover** コマンドで常にドメイン名を指定してください。

realmd システムは、Active Directory と Identity Management の両方のドメインを検出します。環境内に両方のドメインがある場合は、以下のように **--server-software** オプションを使用することで検出結果を特定のサーバータイプにしぼることができます。

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

検出結果で返される属性の 1 つに **login-policy** があります。これは、参加の完了後にすぐにドメインユーザー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** コマンドで手動で許可することができます。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 コマンドについての詳細は、`realm(8) man` ページを参照してください。

ドメインへの参加



重要

Active Directory ドメインでは、一意のコンピューター名を使用する必要がある点に注意してください。NetBIOS コンピューター名と、DNS ホスト名は一意に定義し、それぞれが対応するようにしてください。

システムを ID ドメインに参加させるには、以下のように **realm join** コマンドで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**、IdM の場合は、**admin** と呼ばれます。別のユーザーで接続するには、**-U** オプションを使用します。

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

このコマンドでは最初に認証情報なしで接続を試行しますが、必要に応じてパスワードが要求されます。

Kerberos が Linux システム上で適切に設定されている場合、参加は認証用の Kerberos チケットで実行することもできます。Kerberos プリンシパルを選択する場合は、**-U** オプションを使用します。

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

realm join コマンドではいくつか他のオプションも受け付けます。**realm join** コマンドについての詳細は、`realm(8) 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サンプル手順

1. **realm discover** コマンドを実行してドメインについての情報を表示します。

```
# 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** コマンドでドメイン名を渡します。システムが要求する場合は、管理者パスワードを入力します。

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

ドメインの検出や参加時には、**realmd** が DNS SRV レコードをチェックすることに留意してください。

- **Identity_ldap._tcp.domain.example.com.Management** レコードの場合は
- **Active_ldap._tcp.dc._msdcs.domain.example.com.Directory** レコードの場合は

レコードは AD 設定時にデフォルトで作成され、サービス検出で見つけることができるようになります。

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たかどうかをテストするには、そのドメインからユーザーとしてログインし、ユーザー情報が正常に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からユーザー情報を表示します。

```
# 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、同じユーザーでログインします。

```
# 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** でユーザーのホームディレクトリーがプリントされることを確認します。

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

4. **id** を実行して、最初のステップの **id user@domain_name** コマンドと同じ情報がプリントされ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
```

ドメインへの参加が成功したことをテストする際には、**kinit** ユーティリティーも有効です。このユーティリティーを使用するには **krb5-workstation** パッケージがインストールされている必要があります。

3.5. ID ドメインからのシステムの削除

システムを ID ドメインから削除するには、**realm leave** コマンドを使用します。このコマンドは、SSSD と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、この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** になります。IdM の場合は、**admin** になります。ドメインへの参加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する必要がある場合があります。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'
```

このコマンドでは最初に認証情報なしで接続を試行しますが、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いなくなっても、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ないことに注意してください。削除されるのは、ローカルクライアントの設定のみです。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 コマンドについての詳細は、**realm(8) 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、システムのすべての設定済みドメイン、およびそのドメインの詳細およびデフォルトの設定を一覧表示します。この内容は、すでにシステム設定内にあるドメインの場合のみ、**realm discovery** コマンドで返される情報と同じものになります。

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

realm list が受け付ける重要なオプションは以下の通りです。

--all

--all オプションを使用すると、設定済みおよび未設定の両方の検出されたドメインすべてを一覧表示します。

--name-only

--name-only オプションを使用すると、表示結果がドメイン名のみとなり、設定の詳細は表示されません。

realm list コマンドについての詳細は、**realm(8) 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、ドメイン内で定義されたログインポリシーがドメインユーザーに適用されます。このデフォルト動作は、クライアント側のアクセス制御の使用で無効になります。クライアント側の制御を使用すると、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** システムを使ってそのドメインにおけるユーザーの基本的な allow or deny アクセスルールを設定することができます。このアクセスルールはシステム上の全サービスに対する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。特定のアクセスルールは、特定のシステムリソースもしくはドメインで設定する必要があります。

アクセス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にアクセスを拒否します。このコマンドは **--all** オプションと使用します。

realm permit

realm permit コマンドは、以下を可能にします。

- **--all** オプションを使用して全ユーザーにアクセスを付与します。

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

- 以下のように指定したユーザーにアクセスを付与します。

```
$ 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にアクセスを拒否します。

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

現時点では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有効で、信頼されるドメインのユーザーには有効ではありません。ユーザーログインにはドメイン名を含める必要がありますが、SSSD は現時点では **realmd** に利用可能なサブドメインの情報を提供できないためです。



重要

一部のユーザーのアクセスを拒否してその他のユーザーにアクセスを許可するよりも、特定のユーザーやグループのみアクセスを許可する方がより安全な方法になります。つまり、デフォルトで全員にアクセスを許可して、かつ **realm permit -x** で指定されたユーザーにアクセスを拒否するというやり方は推奨されません。Red Hat で推奨しているのは、デフォルトで全ユーザーにアクセスを拒否し、**realm permit** で選択したユーザーにのみアクセスを許可するという方法です。

realm deny および **realm permit** コマンドについての詳細は、**realm(8) man** ページを参照してください。

3.8. デフォルト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や shell POSIX 属性の変更に対応しています。例えば、POSIX 属性が Windows のユーザーアカウントで設定されていなかったり、これらの属性がローカルシステム上の他のユーザーの POSIX 属性と異なる場合などにこれが必要になることがあります。



重要

本セクションに記載の設定変更が可能なのは、**realm join** コマンドを実行していない場合のみになります。システムが既に参加している場合は、デフォルトのホームディレクトリーと shell は **/etc/sss/sssd.conf** に記載の「[オプション: ユーザーのホームディレクトリーおよびシェルの設定](#)」ファイルで変更します。

デフォルトのホームディレクトリーと shell POSIX 属性を上書きするには、**[users]** ファイルの **/etc/realmd.conf** セクションで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が明示的に設定され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テンプレートを設定します。一般的な形式は **/home/%d/%u** となり、ここでの **%d** はドメイン名、**%u** はユーザー名になります。

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。サポートされるシステムシェルを受け付けます。

例:

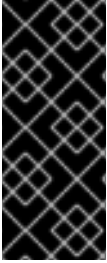
```
[users]
default-home = /home/%u
default-shell = /bin/bash
```

これらのオプションについての詳細は、**realmd.conf(5)** 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

個別ドメインのカスタム設定は、**/etc/realmd.conf** 設定ファイルで定義することができます。各ドメインには、独自の設定セクションを設けることができ、このセクション名はドメイン名に一致する必要があります。例を示します。

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



重要

本セクションに記載の設定変更が可能なのは、**realm join** コマンドを実行していない場合のみになります。システムが既に参加している場合は、これらの設定を変更しても反映されません。そのような場合は、「[ID ドメインからのシステムの削除](#)」にあるように一旦ドメインを離れ、「[ドメインへの参加](#)」の説明に従って再度参加します。参加にはドメイン管理者の認証情報が必要にな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** の対応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、システムを指定されたサブツリーに追加しています。

```
[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
```

同様の設定は **realm join** にある「[ドメインへの参加](#)」コマンドで最初にシステムをドメインに参加させる際にも以下のようにセットアップすることができます。

```
# 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](#)」では、**/etc/realmd.conf** のドメインのデフォルトセクションで設定可能な最重要オプションを一覧表示しています。利用可能な設定オプションについての完全一覧は、**realmd.conf(5)** 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ためのディレクトリーの場所を設定します。これは、root エントリーに関連する完全 DN または RDN にすることができます。サブツリーは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 の属性値を提供された 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、またはマッピングを無効にして Active Directory で設定済みの POSIX 属性を使用するかを設定します。

第4章 ACTIVE DIRECTORY 統合での SAMBA の使用

Samba は、Red Hat Enterprise Linux で Server Message Block (SMB) プロトコルを実装します。SMB プロトコルを使用して、ファイル共有や共有プリンターなど、サーバー上のリソースにアクセスします。

Samba を使用して、ドメインコントローラー (DC) にアクセスする Active Directory (AD) ドメインユーザーを認証できます。さらに、Samba を使用してネットワーク上の他の SMB クライアントに、プリンターやローカルディレクトリーを共有できます。

4.1. ドメインユーザー認証での WINBINDD の使用

Samba の **winbindd** サービスでは、Name Service Switch (NSS) へのインターフェースを提供し、ドメインユーザーがローカルシステムにログインする時に 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することなしにディレクトリーを共有するなど設定を強化するという利点があります。詳しい情報は、『[Red Hat システム管理者ガイド](#)』を参照してください。

4.1.1. AD ドメインへの参加

AD ドメインに参加し、**winbind** サービスを使用する場合には、**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 および PAM などの設定ファイルを自動的に更新します。

詳細情報と例については、『[Red Hat システム管理者ガイド](#)』の『「ドメインメンバーとしての Samba の設定」』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

このセクションでは、SSSD クライアントを使用して、Common Internet File System (CIFS) と呼ばれる Server Message Block (SMB) プロトコルをベースにした共有にアクセスして、完全に利用する方法を説明します。



注記

Red Hat Enterprise Linux 7.1 より前のバージョンでは、Winbind のみがこの機能を提供していました。Red Hat Enterprise Linux 7.1 以降のバージョンでは、SMB 共有へのアクセスに Winbind と SSSD を並行して実行する必要がなくなりました。たとえば、アクセス制御リスト (ACL) には SSSD クライアント上に Winbind を配置する必要がなくなりました。



重要

SSSD は Winbind が提供するすべてのサービスをサポートするわけではありません。たとえば、SSSD は NT LAN Manager (NTLM) または NetBIOS 名前ルックアップを使用した認証はサポートしません。これらのサービスが必要な場合には、Winbind を使用してください。Identity Management ドメインでは、Kerberos 認証および DNS 名前ルックアップが同じ目的で提供されている点に注意してください。

4.2.1. SSSD と SMB との連携方法

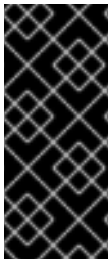
SMB ファイル共有プロトコルは、Windows マシンで幅広く使用されています。Identity Management と Active Directory の間のトラストが設定されている Red Hat Enterprise Linux の環境では、SSSD により、標準の Linux ファイルシステムのように、SMB をシームレスに使用できます。

SMB 共有にアクセスするには、システムは Windows の SID を Linux の POSIX UID と GID に変換する機能が必要です。SSSD クライアントは、SID から ID または SID から名前のアルゴリズムを使用して、この ID マッピングを可能にします。

4.2.2. SMB 共有に SSSD または Winbind を使用するかどうかの判断

SSSD クライアントの多くでは、SSSD の使用を推奨します。

- Identity Management クライアントは、デフォルトで SSSD を使用して、Active Directory ユーザーを UNIX ユーザーにマッピングします。SMB ID マッピングに、SSSD の代わりに Winbind を使用すると、マッピングで整合性が取れなくなります。
- Active Directory が直接統合されている環境では、クライアントが一般的な Active Directory ユーザーマッピングに SSSD を使用しますが、このような環境で SSSD の代わりに、SMB ID マッピングの Winbind を使用すると、マッピングに一貫性がなくなる可能性があります。



重要

SSSD は Winbind が提供するすべてのサービスをサポートするわけではありません。たとえば、SSSD は NT LAN Manager (NTLM) または NetBIOS 名前ルックアップを使用した認証はサポートしません。これらのサービスが必要な場合には、Winbind を使用してください。Identity Management ドメインでは、Kerberos 認証および DNS 名前ルックアップが同じ目的で提供されている点に注意してください。

4.2.3. SSSD クライアントからの SMB 共有のアクセス

Samba ドメインに所属する全 SSSD クライアントから SMB 共有にアクセスできます。

システムが SMB 共有へのアクセスに SSSD を使用することを確認するには、**alternatives** ユーティリティを使用します。このユーティリティは、現在使用するライブラリーを表示します。以下の例では、このシステムは、SSSD ライブラリーを使用します。

```
# alternatives --list | grep -E cifs\|libwbclient
cifs-idmap-plugin          auto          /usr/lib64/cifs-utils/cifs_idmap_sss.so
libwbclient.so.0.11-64    auto          /usr/lib64/sss/modules/libwbclient.so.0.11.0
```

4.2.4. SMB 共有アクセス用の SSSD と Winbind 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する Winbind プラグインと、SSSD の間でどのように切り替えるかを説明しています。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 パッケージをインストールする必要があります。お使いのマシンに cifs-utils がインストールされていることを確認するには、以下を実行します。

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

1. **オプション:** SSSD クライアントから SMB 共有にアクセスするのに SSSD または Winbind のいずれを使用しているかを確認します。

```
# alternatives --display cifs-idmap-plugin
cifs-idmap-plugin - status is auto.
```

```
link currently points to /usr/lib/cifs-utils/cifs_idmap_sss.so
/usr/lib/cifs-utils/cifs_idmap_sss.so - priority 20
/usr/lib/cifs-utils/idmapwb.so - priority 10
Current `best' version is /usr/lib/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、このプラグインはデフォルトで Winbind プラグイン (**idmapwb.so**) よりも優先されます。

2. Winbind プラグインに切り替える前に、Winbind がシステムで実行されていることを確認します。

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

SSSD プラグインに切り替える前に、SSSD がシステムで実行されていることを確認します。

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

3. 異なる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、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/lib/cifs-
utils/idmapwb.so
```

4.3. その他のリソース

Samba の詳細は、[『Red Hat システム管理者ガイド』](#)の適切な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: フォレスト間信頼

第5章 ACTIVE DIRECTORY および IDENTITY MANAGEMENT によるフォレスト間の信頼作成

本章では、Active Directory と Active Directory Identity Management の間のクロスフォレストトラストの作成について説明します。アイデンティティ管理および Active Directory 環境を間接的に統合する方法で推奨の方法が 2 つあり、クロスフォレストトラストは、そのうちの 1 つとです。もう 1 つの方法が同期です。お使いの環境でどちらの方法を選択するといったのが不明な場合には、「[間接的な統合](#)」を確認してください。

Kerberos は **信頼**という概念を実装しています。信頼では、ある 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、2 つの別個のレルム間の関係を作成する機能があります。これは、**レルム間の信頼**と呼ばれています。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になります。

Red Hat Identity Management は、IdM ドメインと Active Directory ドメイン間のフォレスト間の信頼設定に対応しています。

5.1. フォレスト間の信頼について

Kerberos レルムが関与するのは認証のみです。他のサービスやプロトコルが、Kerberos レルム内のマシンで実行中のリソースについての識別や承認を補完します。

このため、Kerberos レルム間の信頼を確立するだけでは、ある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。通信の別の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 および Identity Management の両方が、Kerberos、LDAP、DNS、または証明書サービスなどの各種のコアサービスを管理します。これら 2 つの異なる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 の信頼、フォレスト、およびフォレスト間の信頼

Kerberos レルム間の信頼は、Active Directory の環境間の認証で重要な役割を果たします。信頼される AD ドメインでユーザーおよびグループ名を解決するすべてのアクティビティは、アクセス方法に関係なく認証が必要になります。つまり、LDAP プロトコルを使用する場合でも、Server Message Block (SMB) プロトコルの他に分散コンピューティング環境/リモートプロシージャコール (DCE/RPC) の一部とする場合でもです。2 つの異なる Active Directory ドメイン間でのアクセスを組織する際には多くのプロトコルが関わってくるため、信頼の関係は *Active Directory 信頼* という一般的な名前になります。

複数の AD ドメインは、1 つの *Active Directory forest* 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 フォレストの一部とすることはできないため、常に別個のフォレストとみなされます。

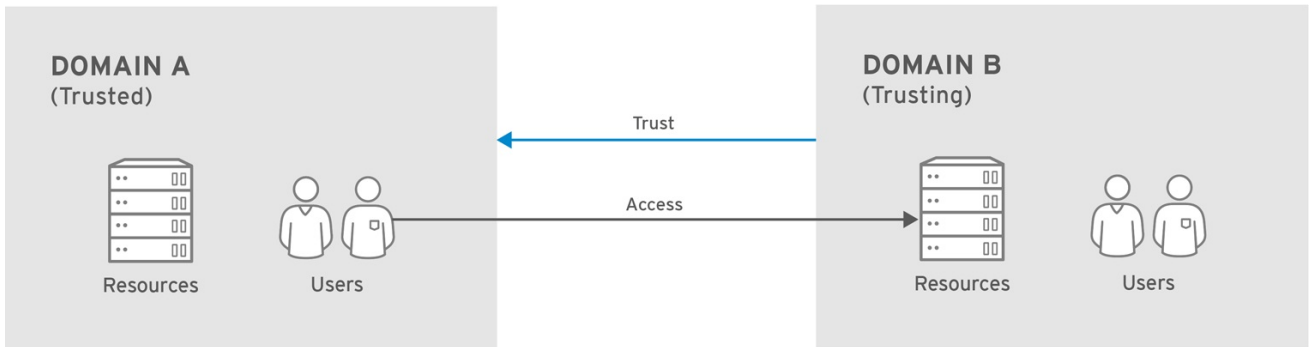
2 つの別個のフォレスト root ドメイン間で信頼関係が確立され、異なる AD フォレストからユーザーやサービスが通信できるようになると、この信頼は *Active Directory フォレスト間の信頼* と呼ばれるようになります。

信頼のフローと一方向の信頼

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 環境は複雑になり得るので、サブドメイン、root ドメイン、またはフォレスト間には複数の異なるタイプの Active Directory 信頼や

その配置が存在することになります。信頼は、あるドメインから別のドメインへのパスです。アイデンティティおよび情報がドメイン間で移動することは **信頼のフロー** 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、信頼する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、ユーザーは信頼する側のドメインのリソースにアクセスできますが、信頼する側のドメインのユーザーは、信頼されるドメインのリソースにアクセスすることはできないという一方向のみの信頼のフローになります。図5.1「一方向の信頼」では、ドメイン A はドメイン B から信頼されていますが、ドメイン B はドメイン A から信頼されていません。



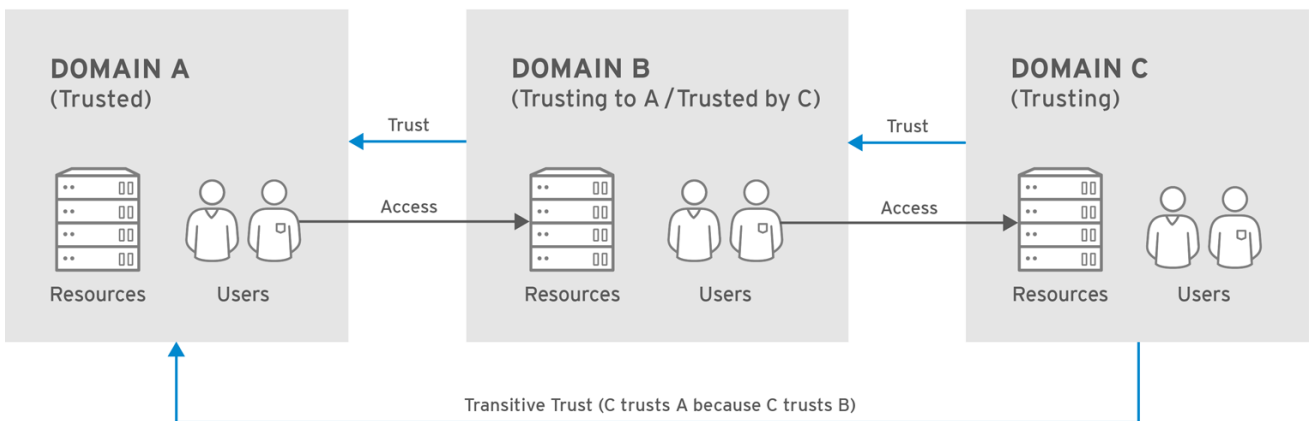
RHEL_404973_0516

図5.1 一方向の信頼

IdM を使用すると、管理者は一方向および双方向の両方の信頼を設定できます。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

信頼は **推移的** とすることが可能で、その場合、1 つ目のドメインが別のドメインを信頼し、この 2 つ目のドメインが信頼している他のドメインも 1 つ目のドメインが信頼することになります。



RHEL_404973_0516

図5.2 推移的な信頼

信頼は **非推移的** にすることもできます。この場合、信頼関係は明示的に含まれるドメインに限定されます。

Active Directory と Identity Management における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双方向で、デフォルトで推移的となっています。

2 つの AD フォレスト間の信頼は 2 つのフォレスト root ドメイン間の信頼なので、双方向にも一方向に

もすることができます。フォレスト間の信頼の推移性は明示的なものです。つまり、フォレストの root ドメインにつながっている AD フォレスト内のドメイン信頼は、フォレスト間の信頼で推移的になります。ただし、別個のフォレスト間信頼は非推移的になります。ある AD フォレスト root ドメインと別の AD フォレスト root ドメイン間では、明示的なフォレスト信頼を確立する必要があります。

AD の観点からは、Identity Management は単一の 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 root ドメインと IdM ドメイン間でフォレスト間信頼が確立されると、AD フォレスト ドメインからのユーザーは IdM ドメインからの Linux マシンやサービスと対話できるようになります。

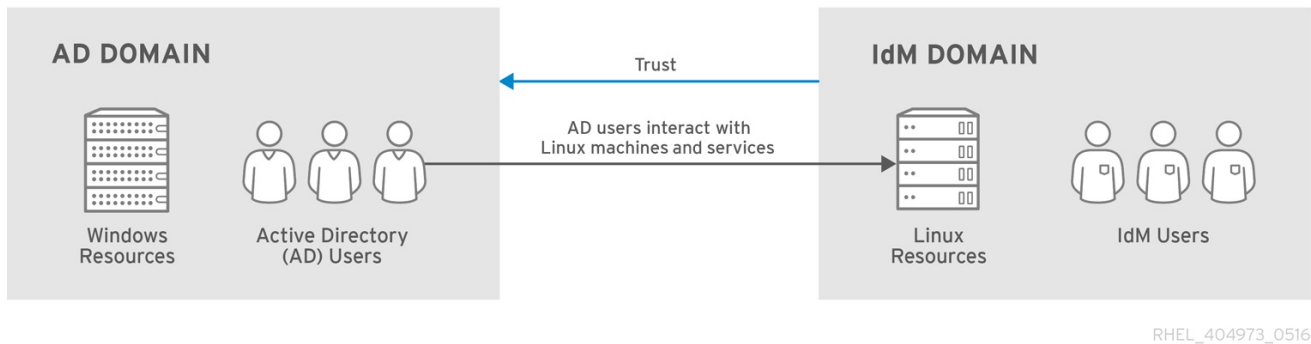


図5.3 信頼の方向

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 のオブジェクトについての情報が含まれます。自身のドメイン内にあるオブジェクトの完全コピーが保存されます。Active Directory フォレスト内の他のドメインのオブジェクトからは、最も一般的に検索される属性のコピーの一部のみがグローバルカタログに保存されます。また、グループの一部のタイプのみが特定のスコープ内で有効になり、これはグローバルカタログの一部とならない可能性があります。

フォレスト間信頼のコンテキストは、単一ドメインのものよりも広くなることに注意してください。このため、信頼されるフォレストからのサーバー-ローカルもしくはドメイン-ローカルのセキュリティーグループメンバーシップの一部は、IdM サーバーに認識されない可能性があります。

グローバルカタログと POSIX 属性

Active Directory はデフォルトでは POSIX 属性を複製しません。Red Hat では、AD で定義される POSIX 属性を使用する必要がある場合は、グローバルカタログサービスに属性を複製することを強く推奨しています。

5.1.3. IdM における信頼アーキテクチャー

Identity Management 側では、IdM サーバーは Active Directory アイデンティティーを認識し、かつアクセス制御の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) にはユーザーについての必要な情報が含まれます。これには、ユーザーのセキュリティー 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 チケット上の PAC 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 は、Active Directory 上の ID 検索を実行し、認可のためにユーザーおよびグループセキュリティー識別子 (SID) を取得します。さらに 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 および 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、an IdM ポリシーおよびアクセスのために IdM グループと関連付けます。



注記

SELinux、sudo、およびホストベースのアクセス制御など、Linux ドメイン管理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 側で設定されるいずれのアクセス制御ルールも IdM では評価または使用されます。関連する Active Directory 設定はグループメンバーシップのみになります。

異なる **Active Directory** フォレストとの信頼

IdM は複数の異なる AD フォレストとの信頼関係の一部に組み込むこともできます。信頼が確立されると、同じコマンドと手順で他のフォレストとの信頼を後で追加することができます。IdM は複数のまったく無関係のフォレストを同時に信頼できるため、関連性のない AD フォレストのユーザーが同じ共有済みの IdM ドメイン内のリソースにアクセスできます。

5.1.3.1. Active Directory PAC および IdM チケット

Active Directory 内のグループ情報は、*特権属性証明書* (MS-PAC または PAC) のデータセット内の識別子リストに保存されます。PAC には、グループメンバーシップや新たな認証情報などの各種の認証情報が含まれます。また、これには、Active Directory ドメイン内のユーザーおよびグループの *セキュリティ識別子* (SID) も含まれます。SID は、Active Directory ユーザーおよびグループの作成時にそれらに割り当てられる識別子です。信頼環境では、グループのメンバーは名前や DN ではなく、SID で識別されます。

PAC は、Active Directory ユーザー向けにエンティティを Windows ドメイン内の他の Windows クライアントおよびサーバーに特定する方法として、Kerberos サービスリクエストチケットに埋め込まれています。IdM は PAC 内のグループ情報を Active Directory グループにマッピングし、その後に対応する IdM グループにマッピングすることでアクセスを決定します。

Active Directory ユーザーが IdM リソース上のサービスのチケットをリクエストすると、以下のプロセスが実行されます。

1. サービスのリクエストにはユーザーの PAC が含まれます。IdM KDC は、Active Directory グループ一覧と IdM グループ内のメンバーシップを比較して PAC を分析します。
2. MS-PAC 内で定義されている Kerberos プリンシパルの SID の場合、IdM KDC が IdM LDAP で定義されている外部のグループメンバーシップを評価します。SID の新たな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。この拡張された MS-PAC は IdM KDC で署名されます。
3. IdM KDC で署名された更新済み PAC のあるサービスチケットがユーザーに返されます。IdM に既知の AD グループに属するユーザーは、これでサービスチケットの MS-PAC コンテンツをベースにした IdM クライアント上で実行している SSSD に認識されます。これにより、IdM クライアントによるグループメンバーシップを検索するアイデンティティトラフィックを抑制することができます。

IdM クライアントがサービスチケットを評価する際には、以下のプロセスが発生します。

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が PAC データを SSSD PAC レスポンダーに送信します。

2. PAC レスポンダーが PAC 内のグループ SID を確認し、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、新規サービスがアクセスされるたびに複数の TGT と各ユーザーのチケットを保存します。
3. 確認されたグループに所属するユーザーは、IdM 側にある必要なサービスにアクセスできるようになります。

5.1.3.2. Active Directory ユーザーと Identity Management グループ

Active Directory のユーザーとグループを管理する際には、個別の AD ユーザーと AD グループ全体を Identity Management グループに追加することができます。

IdM グループを AD ユーザー向けに設定する詳細な方法は、[「IdM ユーザー用の Active Directory 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 内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 の識別名 (DN) を指定することで表記されます。AD エントリーは IdM と同期されたりコピーされたりしないので、AD ユーザーとグループは IdM LDAP 内に LDAP オブジェクトがないことになります。このため、IdM LDAP 内のグループメンバーシップの表記にこれらは直接使用できません。

この理由のために、IdM は *非 POSIX 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 への参照を文字列として含むプロキシ LDAP オブジェクトです。非 POSIX 外部グループは、IdM 内の 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示する際に通常の 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 で処理されます。SSSD は、AD ユーザーが所属するグループの SID を IdM の POSIX グループにマップします。AD 側の SID は、ユーザー名に関連付けられています。ユーザー名を使用して IdM リソースにアクセスすると、IdM 内の SSSD がそのユーザー名を SID に解決し、AD 内のその SID の情報を検索します。これについては [「Active Directory PAC および IdM チケット」](#) で説明しています。

ID の範囲

Linux でユーザーが作成されると、ユーザー ID 番号が割り当てられ、さらにそのユーザーの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の ID 番号はユーザー ID 番号と同じものになります。Linux 環境ではこれによって競合は発生しませんが、Windows では、セキュリティ ID 番号はドメイン内の各オブジェクトで一意である必要があります。

信頼される AD ユーザーは、Linux システムで UID および GID 番号が必要になります。この UID/GID 番号は IdM で生成できますが、AD エントリーに UID/GID 番号がすでに割り当てられている場合は、異なる番号を割り当てると競合が生じます。このような競合を避けるために、AD で定義された POSIX 属性 (UID/GID 番号および好みのログインシェルを含む) を使用することができます。



注記

AD は、フォレスト内の全オブジェクトの情報のサブセットを *グローバルカタログ* に保存します。この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全エントリーが含まれます。AD 定義の POSIX 属性を使用する場合は、Red Hat では、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ています。

信頼が作成されると IdM は使用する ID 範囲を自動的に検出し、信頼に追加される AD ドメイン用に一意の ID 範囲を作成します。これは以下のオプションのいずれかを `ipa trust-add` コマンドに渡すことで手動で選択することもできます。

ipa-ad-trust

この範囲のオプションは、SID をベースに IdM がアルゴリズムで生成した ID に使用します。

IdM が SID-to-POSIX ID マッピングを使用して SID を生成している場合は、AD および IdM ユーザーおよびグループの ID 範囲は一意で、重複しない ID 範囲が利用可能になっている必要があります。

ipa-ad-trust-posix

この範囲のオプションは、AD エントリー内の POSIX 属性で定義された ID に使用されます。

IdM は、**uidNumber** および **gidNumber**などを含む POSIX 属性を 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取得します。AD ドメインが適切に管理されており、かつ ID の競合がなければ、この方法で生成された ID 番号は一意のものになります。この場合、ID の検証や範囲は必要ありません。

例:

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

他の ID 範囲でのトラストの再作成

作成したトラストの ID 範囲が使用しているデプロイメントに適さない場合には、他の **--range-type** オプションを使用してトラストを再作成します。

1. 現在使用している ID 範囲をすべて表示します。

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

ipa trust-add コマンドで作成した ID 範囲名を、リストの中から特定します。ID 範囲名の最初の部分は、トラストの名前 (*name_of_the_trust_id_range*) です。例: *ad.example.com*。

2. (オプション) トラストの作成時に、どの **--range-type** オプション (**ipa-ad-trust** または **ipa-ad-trust-posix**) を使用したか分からない場合には、以下のコマンドを使用してオプションを特定します。

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

タイプをメモし、ステップ 5 で新しいトラストには、もう一方のタイプを選択します。

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. トラストを削除します。

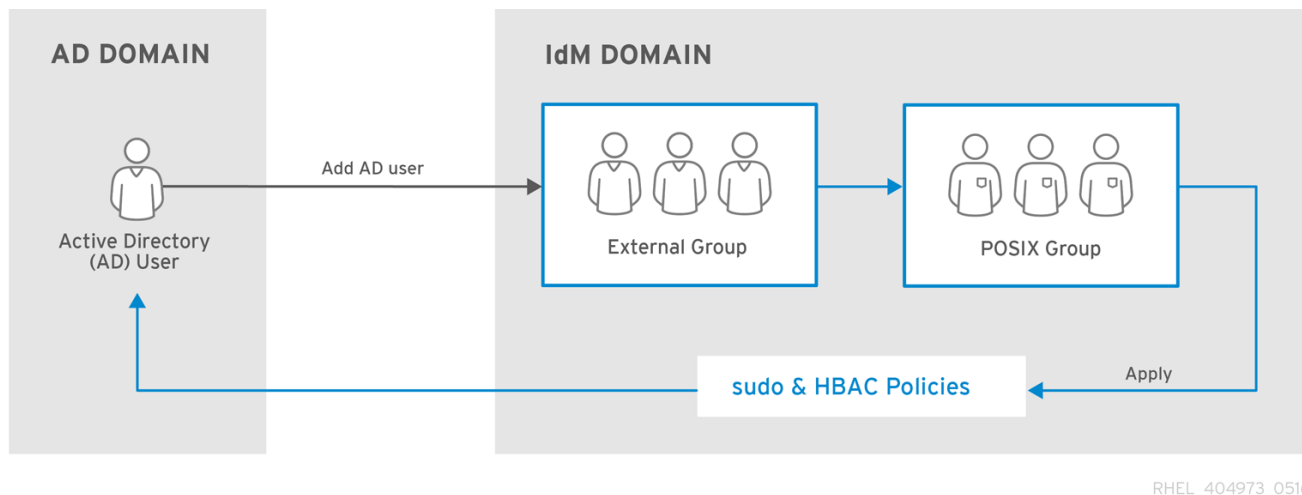
```
[root@ipaserver ~]# ipa trust-del name_of_the_trust
```

5. 正しい **--range-type** オプションで新規トラストを作成します。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 ユーザーと 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 およびネットグループなどのいくつかの IdM ポリシー定義では、ポリシー適用方法の特定でユーザーグループに依存します。



RHEL_404973_0516

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

Active Directory ユーザーは IdM ドメインには外部という位置付けになりますが、IdM があるように「[Active Directory ユーザーと Identity Management グループ](#)」グループが外部グループとして設定されていれば、これらのユーザーは IdM グループのグループメンバーとして追加できます。この場合、ドメインリソースにアクセスする際には、sudo、ホストベースのアクセス制御、および他のポリシーは外部 POSIX に適用され、最終的には AD ユーザーに適用されます。

チケットの PAC にあるユーザー SID は Active Directory アイデンティティに対して解決されます。つまり、完全修飾ユーザー名または SID を使用してユーザーをグループメンバーとして追加できることになります。

5.1.4. 一方向および双方向の信頼

IdM は IdM 内のサービスへの接続を確立できるエンティティが AD に限定されるか、もしくは IdM エンティティも含めることができるかによって、2つのタイプの信頼関係をサポートします。

一方向の信頼

一方向の信頼では、AD ユーザーとグループは IdM 内のリソースにアクセスできますが、その逆は可能ではありません。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、信頼の作成におけるデフォルトのモードです。

双方向の信頼

双方向の信頼では、AD ユーザーとグループは IdM 内のリソースにアクセスできます。IdM の双方向信頼では、AD における一方向の信頼ソリューションと比較した場合、ユーザーに新たな権限が与えられるわけではありません。デフォルトのフォレスト間信頼のフィルター設定により、両方のソリューションの安全性は同等なものと考えられます。

一方向および双方向の信頼に関する詳細情報は、「[信頼関係のアーキテクチャー](#)」を参照してください。

信頼を確立した後は、タイプを修正することはできません。異なるタイプの信頼が必要な場合は、**ipa trust-add** コマンドを再度実行してください。これにより既存の信頼を削除し、新規の信頼を確立することができます。

5.1.5. Active Directory への外部の信頼

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 root ドメイン間の信頼確立を必要としますが、フォレスト内では外部の信頼をどのドメインに対しても確立できます。

外部の信頼は非推移的です。このため、他の Active Directory ドメインからのユーザーおよびグループには IdM リソースへのアクセスはありません。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 に対する信頼をサポートする、以下のタイプの IdM サーバーがあります。

信頼エージェント

Active Directory ドメインコントローラーに対してアイデンティティ検索を実行可能な IdM サーバー

信頼コントローラー

Samba スイートも実行する信頼エージェントの機能を持つ 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、検証する場合には信頼コントローラーに問い合わせます。

最初の信頼コントローラーは、「[信頼向けに IdM サーバーを準備する](#)」で記載されているように信頼の設定時に作成されます。

信頼コントローラーは信頼エージェントと比較するとネットワークに接続されているサービスを多く実行するので、侵入者が攻撃できる範囲が大きくなります。

信頼エージェントとコントローラーに加え、IdM ドメインには、標準の IdM サーバーも含めることができます。ただし、これらのサーバーは Active Directory と通信しないので、標準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許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

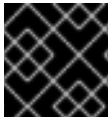
機能	信頼エージェント	信頼コントローラー
Active Directory ユーザーとグループの解決	はい	はい
IdM クライアントを登録して、信頼済みの Active Directory フォレストからのユーザーがアクセスできるサービスを実行します	はい	はい
信頼を管理します（たとえば、信頼合意の追加）	いいえ	はい

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。

- 最低でもアイデンティティ管理のデプロイメントごとに、信頼コントローラーは 2 台設定してください。

- 最低でも各データセンターごとに信頼コントローラーは 2 台設定してください。

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標準サーバーをプロモートして、新規信頼コントローラーを作成してください。これには、「[信頼向けに IdM サーバーを準備する](#)」で記載されているように、IdMサーバーの **ipa-adtrust-install** ユーティリティを使用してください。



重要

信頼エージェント上の既存の信頼コントローラーはダウングレードできません。

その他のリソース

- 信頼コントローラーの追加については、「[信頼の作成](#)」に記載されています。
- 信頼エージェントの追加については、「[信頼エージェントの設定](#)」に記載されています。

5.2. フォレスト間の信頼作成

5.2.1. 環境およびマシン要件

信頼関係を設定する前に、Active Directory と Identity Management の両方のサーバー、マシン、および環境が本セクション記載の要件および設定を満たしていることを確認してください。

5.2.1.1. サポートされる Windows プラットフォーム

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、信頼関係を確立することができます。

- フォレスト機能レベルの範囲: Windows Server 2008 - Windows Server 2016 R2
- ドメイン機能レベルの範囲: Windows Server 2008 - Windows Server 2016 R2

以下のオペレーティングシステムは、上記の機能レベルを用いた信頼確立においサポートされ、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 では、信頼確立のサポートはありません。

5.2.1.2. DNS およびレルム設定

信頼関係を確立するには、Active Directory と Identity Management で以下の特定の 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

各システムは、一意のプライマリー DNS ドメインを設定する必要があります。例えば、

- AD の場合は **ad.example.com**、IdM の場合は **idm.example.com**
- AD の場合は **example.com**、IdM の場合は **idm.example.com**



注記

IdM の **example.com** や、AD の **ad.example.com** など、IdM ドメインが AD ドメインの親ドメインの場合には、バグがあるため ([BZ#1421869](#) で追跡)、IdM は正しく機能しません。

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、標準準拠の DNS サーバーであればいずれのものでも使用できます。

AD または IdM では、アイデンティティ管理目的でプライマリー DNS ドメインを別のシステムと共有することはできません。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](#) のホスト名および DNS 設定要件のセクションを参照してください。

Kerberos レルム名をプライマリー DNS ドメイン名の大文字バージョンとする

Kerberos レルム名はプライマリー DNS ドメイン名と同一のものにし、すべて大文字にする必要があります。例えば、AD のドメイン名が **ad.example.com**、IdM のドメイン名が **idm.example.com** である場合、Kerberos レルム名は **AD.EXAMPLE.COM** および **IDM.EXAMPLE.COM** とします。

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こと

信頼関係内で関連するすべての DNS ドメインからの DNS レコードをすべてのマシンが解決可能である必要があります。

- IdM DNS を設定する際には、[Linux ドメイン ID、認証、およびポリシーガイド](#) の [IdM ドメイン内での DNS サービスの設定](#) および『DNS 転送の管理』セクションに記載の指示に従います。
- 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 なしでサーバーをインストールする』セクションにある指示に従ってください。

IdM と AD DNS ドメイン間で重複しないこと

IdM に参加したマシンは複数の DNS ドメインに分配することができます。IdM クライアントを含んでいる DNS ドメインは、AD に参加しているマシンを含んでいる DNS ドメインと重複することはできません。AD 信頼をサポートするには、プライマリー IdM DNS ドメインに適切な SRV レコードがある必要があります。

\$ ipa dns-update-system-records --dry-run コマンドを実行して、お使いのシステム設定に固有の必須 SRV レコード一覧を取得できます。

生成されたリストは、以下のような形式になっています。

```
$ 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 レルムの一部である他の DNS ドメインでは、AD への信頼設定時に 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 レコードを使用せず、KDC の検索には信頼の名前サフィックス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 と Active Directory サーバーが自身を解決し、また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しても期待される結果が表示されない場合は、コマンドが実行されたホストの DNS 設定を調べます。このホスト設定が正しい場合は、親から子ドメインへの DNS 委任が正しく設定されていることを確認します。

AD は DNS 検索の結果をキャッシュするので、DNS 内の変更は直ちには見えない場合があることに注意してください。**ipconfig /flushdns** コマンドを実行するとキャッシュが削除できます。

IdM でホストされているサービスが信頼確立に使用される IdM ドメインサーバーから解決可能であることを確認する

1. TCP サービスレコードに対する LDAP と UDP による Kerberos の DNS クエリを実行します。

```
[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.
```

このコマンドでは、全 IdM サーバーが一覧表示されるはずですが。

2. IdM Kerberos レルム名で TXT レコードの DNS クエリを実行します。取得される値は、IdM インストール時に指定した Kerberos レルムと一致することが期待されます。

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

3. **ipa-adtrust-install** にあるように「**信頼向けに IdM サーバーを準備する**」ユーティリティを実行した後、TCP サービスレコードに対する LDAP と UDP による MS DC Kerberos の DNS クエリを実行します。

```
[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.
```

このコマンドでは、**ipa-adtrust-install** を実行した全 IdM サーバーが一覧表示されるはずですが。**ipa-adtrust-install** を IdM サーバーで実行していない場合は、出力は空白になることに留意してください。最初の信頼関係を確立していない場合は、これはよくあることです。

IdM が AD のサービスレコードを解決可能であることを確認する

TCP サービスレコードに対する LDAP と UDP による Kerberos の DNS クエリを実行します。

```
[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.
```

このコマンドでは、AD ドメインコントローラーの名前が返されるはずですが、

IdM でホストされているサービスが AD サーバーから解決可能であることを確認する

1. AD サーバーでサービスレコードを検索する **nslookup.exe** ユーティリティーをセットアップします。

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

2. TCP サービスレコードに対する LDAP と UDP による Kerberos の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
```

予測される出力には **IdM でホストされているサービスが信頼確立に使用される IdM ドメインサーバーから解決可能であることを確認する** で表示される IdM サーバーと同じものが含まれます。

3. サービスタイプを TXT に変更し、IdM Kerberos レルム名を使って TXT レコードの DNS クエリを実行します。

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

      "IPA.EXAMPLE.COM"
```

出力は **IdM でホストされているサービスが信頼確立に使用される IdM ドメインサーバーから解決可能であることを確認する** で表示される値と同じものが含まれるはずですが、

4. **ipa-adtrust-install** にあるように「[信頼向けに IdM サーバーを準備する](#)」ユーティリティを実行した後、TCP サービスレコードに対する LDAP と UDP による MS DC Kerberos の DNS クエリを実行します。

```
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
```

このコマンドでは、**ipa-adtrust-install** ユーティリティを実行した全 IdM サーバーが一覧表示されるはずですが、**ipa-adtrust-install** を IdM サーバーで実行していない場合は、出力は空白になることに留意してください。最初の信頼関係を確立していない場合は、これはよくあることです。

AD サービスが AD サーバーから解決可能であることを確認する

1. AD サーバーでサービスレコードを検索する **nslookup.exe** ユーティリティをセットアップします。

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

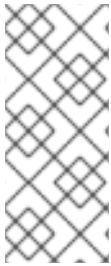
2. TCP サービスレコードに対する LDAP と UDP による Kerberos のドメイン名を入力します。

```
> _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
```

予測される出力には **IdM が AD のサービスレコードを解決可能であることを確認する** で表示される AD サーバーと同じものが含まれます。

5.2.1.3. NetBIOS 名

NetBIOS 名は AD ドメインの特定に必須のもので、IdM ドメインが Active Directory DNS のサブドメイン内にある場合は、IdM ドメインとサービスの特定に必須のものです。IdM ドメインと Active Directory ドメインでは、NetBIOS 名は別のものである必要があります。



注記

NetBIOS 名は通常、ドメイン名の左端の要素になります。例えば、ドメイン名が **linux.example.com** であれば NetBIOS 名は **linux** になり、ドメイン名が **example.com** であれば NetBIOS 名は **example** になります。

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 サーバーとの通信を可能にするには、以下のポート要件を満たす必要があります。

- [AD 信頼に必要なポート](#) と [AD 信頼内の IdM サーバーに必要なポート](#) を IdM サーバーと全 AD ドメインコントローラーで開きます。これらは、IdM サーバーから AD ドメインコントローラーおよびその逆の両方向で開きます。
- [AD 信頼内の IdM クライアントに必要なポート](#) を信頼される AD フォレストの全 AD ドメインコントローラーで開きます。IdM クライアント上では、ポートが発信方向で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](#) の『クライアントインストールの前提条件』を参照してください)。

表5.2 AD 信頼に必要なポート

サービス	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] TCP ポート 389 は信頼のためには IdM サーバー上で開く必要はありませんが、クライアントが IdM サーバーと通信するために必要になります。		

表5.3 信頼内の IdM サーバーに必要なポート

サービス	ポート	プロトコル	備考
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 信頼内の IdM クライアントに必要なポート

サービス	ポート	プロトコル	備考
Kerberos	88	UDP および TCP	KDC (キー配布センター) プロキシを設定済みの場合は、このポートは必要ありません。その場合、IdM クライアントは Kerberos リクエストを IdM サーバー経由で送信します。

その他のリソース

- 必要なポートを開く方法に関しては、[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. 時計の設定

Active Directory サーバーと IdM サーバーの両方の時計が同期している必要があります。

5.2.1.7. サポートされるユーザー名の形式

IdM はローカル SSSD クライアント内でユーザー名マッピングを実行します。SSSD がサポートするデフォルトのユーザー名形式は、**name@domain** です。Active Directory は **username**、**username@DOMAIN.NAME**、および **DOMAIN\username** といったいくつかの異なる形式をサポートします。

ユーザー名と所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る正規表現を使用します。この正規表現は IdM バックエンドおよび AD バックエンドで使用され、上記の形式すべてをサポートします。

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

5.2.2. 信頼の作成

以下のセクションでは、各種の設定シナリオにおける信頼の作成について説明しています。「[コマンドラインからの信頼作成](#)」には、コマンドラインから信頼を設定する完全な手順が含まれています。他のシナリオでは、基本的な設定シナリオとは別のステップを説明し、他のすべてのステップの基本的な手順を紹介しています。

信頼の作成後には「[フォレスト間の信頼のインストール後の検討事項](#)」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作成

IdM と Active Directory Kerberos レalm間での信頼関係の作成には以下を実行します。

1. 「[信頼向けに IdM サーバーを準備する](#)」にあるように、信頼向けに IdM サーバーを準備します。
2. 「[信頼合意の作成](#)」にあるように、信頼の合意を作成します。
3. 「[Kerberos 設定の確認](#)」にあるように、Kerberos 設定を確認します。

5.2.2.1.1. 信頼向けに IdM サーバーを準備する

AD との信頼関係向けに 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、および 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. IdM サーバーで信頼サービスを有効に設定します。

- a. **ipa-adtrust-install** ユーティリティを実行します。このユーティリティは AD 信頼に必要な DNS サービスレコードを追加します。これらのレコードは、IdM が統合 DNS サーバーでインストールされた場合に自動的に作成されます。

IdM が統合 DNS なしでインストールされた場合は、**ipa-adtrust-install** はこの後の手順を進める前に手動で DNS に追加する必要があるサービスレコード一覧をプリントします。



重要

Red Hat では、「[DNS 設定の確認](#)」の説明にあるように、**ipa-adtrust-install** の実行後は毎回 DNS 設定を確認することを強く推奨します。IdM もしくは AD が統合 DNS サーバーを使用しない場合は特にこれが該当します。

- b. このスクリプトは、古い Linux クライアントが信頼されるユーザーと作業可能にする互換性プラグインである **slapi-nis** プラグインの設定を以下のように求めます。

```
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. ディレクトリーの初回作成時には少なくとも 1 人のユーザー (IdM 管理者) が存在します。SID 生成タスクでは既存ユーザー向けに SID を作成し、信頼環境をサポートします。これはリソース集約型タスクです。ユーザー数が多い場合は、これは別個に実行できます。

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

3. 「DNS およびレルム設定」にあるように、DNS が正常に設定されていることを確認します。
4. **smb** デーモンを起動し、**smbclient** ユーティリティを使って Samba が IdM 側から Kerberos 認証に応答していることを確認します。

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

[root@ipaserver ~]# smbclient -L ipaserver.ipa.example.com -k
lp_load_ex: changing to config backend registry
Domain=[IDM] OS=[Windows 6.1] Server=[Samba 4.2.10]
  Sharename      Type            Comment
  -----
IPC$             IPC             IPC Service (Samba 4.2.10)
Domain=[IDM] OS=[Windows 6.1] Server=[Samba 4.2.10]
  Server          Comment
  -----
Workgroup         Master
  -----
```

5.2.2.1.2. 信頼合意の作成

コマンドで Active**ipa trust-add**Directory ドメインと IdM ドメインの信頼合意を作成します。

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

ipa trust-add は、デフォルトで一方向の信頼を設定します。双方向の信頼を確立するには、**--two-way=true** オプションを渡します。詳細は、「[一方向および双方向の信頼](#)」を参照してください。

外部の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 への外部の信頼](#)」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認します。

```
[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、また IdM ユーザーがサービスチケットをリクエストできるかをテストします。

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リクエストします。

```
[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リクエストします。

```
[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リクエストします。

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

AD サービスチケットが正常に付与されると、レルム間のチケット保証チケット (TGT) にリクエストされた他のチケットすべてが記載されます。この TGT は **krbtgt/AD.DOMAIN@IPA.DOMAIN** という名前になります。

```
[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 側からの一方方向の信頼を確認するには、以下を実行します。

1. Active Directory ユーザーのチケットをリクエストします。

```
[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リクエストします。

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

AD サービスチケットが正常に付与されると、レルム間のチケット保証チケット (TGT) にリクエストされた他のチケットすべてが記載されます。この TGT は **krbtgt/IPA.DOMAIN@AD.DOMAIN** という名前になります。

```
[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 プラグインが 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 認証を直接サポートする Linux サービスにアクセスできるようになります。



注記

このプラグインについての詳細は、[「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. 共有シークレットでの双方向の信頼の作成

共有シークレットとは信頼されたピアに対して既知のパスワードで、他のドメインはこれを使ってこの信頼に参加できます。Active Directory 内の双方向の信頼は、共有シークレットで設定できます。AD 内では、共有シークレットは信頼の設定内に *信頼される側のドメインオブジェクト (TDO)* として保存されます。

IdM は、AD 管理者認証情報の代わりに共有シークレットを使用した双方向の信頼の作成をサポートしています。この方法で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 側で信頼を手動で確認する必要があります。



注記

共有シークレットは、双方向の信頼を作成するためにだけ使用できます。一方向の信頼を確立するには、管理者の認証情報を使用します。

Windows Server 2012、2012 R2 または 2016 で、共有シークレットを使用して双方向の信頼を作成するには、以下を行います。

1. [「信頼向けに IdM サーバーを準備する」](#) にあるように、信頼向けに IdM サーバーを準備します。

2. **Active Directory Domains and Trusts** コンソールで信頼を設定します。具体的には、以下を行います。

- 新規の信頼を作成します。
- 信頼に、**idm.example.com**などの IdM ドメイン名を指定します。
- 信頼の **forest** タイプであることを指定します。
- 信頼の **two-way** タイプであることを指定します。
- **forest-wide** の認証であることを指定します。
- **Trust Password** を設定します。



注記

IdM 内で信頼を設定する際には、同じパスワードを使用する必要があります。

着信の信頼の確認を求められたら、**No** を選択します。

3. 「**信頼合意の作成**」にあるように、信頼の合意を作成します。**ipa trust-add** コマンドでは、**--type** および **--trust-secret** オプションを使用し、**--two-way=True** オプションは使用しないでください。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
```


4. **ipa trust-show** コマンドを使用して、IdM サーバー上で信頼関係が確立されてことを確認します。

```
[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
```



注記

ipa trust-show コマンドの実行前に、**ipa trust-fetch-domains ad_domain** コマンドを実行して Common Internet File System (CIFS) チケット保証チケットを取得する必要がある場合があります。

5. 「[Kerberos 設定の確認](#)」にあるように、Kerberos 設定を確認します。

5.2.2.3. 既存の IdM インスタンス上での信頼の作成

既存の IdM インスタンスで信頼を設定する場合は、IdM サーバーとそのドメイン内のエントリーについての特定のセッティングは設定済みになっています。ただし、Active Directory ドメインの DNS 設定では、Active Directory SID をすべての既存の IdM ユーザーおよびグループに割り当てる設定にする必要があります。

1. 「[信頼向けに IdM サーバーを準備する](#)」にあるように、信頼向けに IdM サーバーを準備します。
2. 「[信頼合意の作成](#)」にあるように、信頼の合意を作成します。
3. 各 IdM ユーザーに SID を生成します。



注記

ipa-adtrust-install ユーティリティを使用した信頼の確立時に SID が生成されている場合は、このステップを実行しないでください。

- a. バックエンドの LDAP ディレクトリーで、**ipa-sidgen-task** 操作を実行して、各エントリーごとに、SID を含む、新しい **ipaNTSecurityIdentifier** 属性を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. このタスクが正常に完了すると、SID 生成タスク (**Sidgen task**) がステータスゼロ (0) で終了したというメッセージがエラーログに記録されます。

```
[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](#)」にあるように、Kerberos 設定を確認します。

5.2.2.4. 2 つ目の信頼の追加

1 つ以上の信頼合意が設定されている IdM サーバーに新たな信頼を追加する際は、信頼関連のパッケージのインストールや SID の設定といった一般的な IdM 信頼設定の一部が不要になります。新たな信頼を追加するには、DNS を設定し、信頼合意を確立することのみが必要になります。

1. 「[DNS およびレルム設定](#)」にあるように、DNS が正常に設定されていることを確認します。
2. 「[信頼合意の作成](#)」にあるように、信頼の合意を作成します。

5.2.2.5. Web UI 内での信頼の作成

Web UI 内で信頼を作成する前に、信頼用の IdM サーバーを用意します。この信頼設定はコマンドラインから実行すると最も容易で、「[信頼向けに IdM サーバーを準備する](#)」で説明されています。

初期設定が完了したら、信頼合意を IdM web UI で追加します。

1. IdM web UI を開きます。

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

2. **IPA Server** メインタブを開いてから、**Trusts** サブタブを選択します。
3. **Trusts** サブタブで **Add** をクリックし、新規信頼設定ウィンドウを開きます。
4. 信頼についての必須情報を入力します。

- a. **Domain** フィールドに AD ドメイン名を記入します。

- b. 信頼を双方向にするには、**Two-way trust** チェックボックスを選択します。信頼を一方向にするには、**Two-way trust** を選択しないでください。

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. 別のフォレストにある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 への外部の信頼](#)」を参照してください。

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

- AD 管理者のユーザー名とパスワードを使って信頼を確立する場合は、**Administrative account** を選択して必要な認証情報を入力します。
- 共有パスワードを使って信頼を確立する場合は、**Pre-shared password** を選択して信頼パスワードを入力します。

e. 信頼の ID 設定を定義します。

- **Range type** オプションでは、ID 範囲のタイプを選択できます。IdM が自動的に使用する ID 範囲のタイプを検出するには、**Detect** を選択します。
- ID 範囲の最初の 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。これらのオプションを指定しないと、IdM は ID 範囲のデフォルト値を使用します。

ID 範囲についての詳細は、[「ID の範囲」](#) を参照してください。

Add Trust [X]

Domain * [Text Field]

Two-way trust ⓘ ☐

External trust ⓘ ☐

Establish using

☒ Administrative account

Account * [Text Field]

Password * [Text Field]

☐ Pre-shared password

Password [Text Field]

Verify Password [Text Field]

Range type

☒ Detect

☐ Active Directory domain

☐ Active Directory domain with POSIX attributes

Base ID [Text Field]

Range size [Text Field]

* Required field

[Add] [Add and Add Another] [Add and Edit] [Cancel]

図5.5 Web UI での信頼の追加

5. **Add** をクリックして新規の信頼を保存します。

この後に「[Kerberos 設定の確認](#)」にあるように、Kerberos 設定を確認します。

5.2.3. フォレスト間の信頼のインストール後の検討事項

5.2.3.1. Active Directory 信頼における動作の潜在的問題

5.2.3.1.1. Active Directory ユーザーと IdM 管理

現在、IdM Web UI にログイン後は、Active Directory (AD) ユーザーおよび管理者には、セルフサービスページのみが表示されます。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 ドメインアイデンティティ認証およびポリシーガイド](#)』の対応するセクションを参照してください。

また、AD ユーザーは現時点で自身の ID 上書きを管理することはできません。ID の上書きの追加および管理が可能なのは、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 および資格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い場合は、SSSD によりローカルシステムはこれまでに正常にログインしたことのあるユーザーの ID を参照することができます。

SSSD はユーザー一覧をローカルで保持するため、バックエンドでなされた変更は SSSD をオフラインで実行するクライアントに直には認識されない可能性があります。そのようなクライアントでは、IdM リソースにログインしたことがあるユーザーでハッシュ化されたパスワードが SSSD キャッシュに保存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いても再度ログインすることができます。

上記の条件が満たされる場合は、ユーザー ID が SSSD にキャッシュされ、AD でユーザーアカウントが削除されても 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 ユーザーログオンを AD ドメインコントローラーに対して確認できるようになるまで続きます。

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は AD ドメインコントローラーに対して確認されます。これにより、削除された AD ユーザーのログインが許可されなくなります。

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、クライアントプリンシパルを以下の識別子に対して以下の順でサーバープリンシパルに対して一致させるよう試行します。

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もしくはレルム名をベースとし、認証情報キャッシュのコレクションが使用される場合は、AD ユーザーとしてバインドする際に予期しない動作が発生する場合があります。これは、Active Directory ユーザーのレルム名が 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** ユーティリティを使用してチケットを取得し、SSH を使って an IdM リソースに接続すると、プリンシパルはこのリソースチケットに選択されません。an IdM プリンシパルがリソースのレルム名と一致することから、IdM プリンシパルが使用されます。

例えば、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 ユーザーが Kerberos チケット (**admin** など) も持っている場合、IdM デフォルトプリンシパルと共に別の an IdM 認証情報キャッシュも存在することになります。その IdM デフォルトプリンシパルは、Active Directory ユーザーが SSH を使用してリソースに接続する場合にホストチケットに選択されます。

```
[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 リソースのレルムに一致するために実行されます。

5.2.3.1.4. グループ SID の解決

Kerberos チケットの失効

net getlocalsid または **net getdomainsid** などの、Samba サービスから SID を取得するためのコマンドを実行すると、Kerberos キャッシュから既存の admin チケットが削除されます。



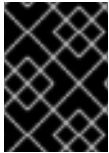
注記

Active**net getlocalsid**Directory 信頼を使用するために **getdomainsid** や といった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 グループに関連付けられていることを確認することはできません。

Active Directory ユーザーの (リモート) **Active Directory** グループメンバーシップを表示できない



重要

IdM サーバーおよびクライアントが Red Hat Enterprise Linux 7.1 またはそれ以降で実行される場合は、この問題は発生しないことに留意してください。

id ユーティリティーを使うと、Linux システムユーザーのローカルグループの関連付けが表示できます。ただし、Samba ツールでは **ActiveIdDirectory** ユーザーの Active Directory グループメンバーシップは表示できますが、**id** ではこれは表示されません。

この問題を回避するには、**ssh** ユーティリティーを使って指定された AD ユーザーとして an IdM クライアントマシンにログインします。この AD ユーザーログインが最初に成功すると、**id** では AD グループメンバーシップを検出して表示します。

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

5.2.3.2. 信頼エージェントの設定

通常の IdM マスターが信頼エージェントとして動作するようにするには、以下の設定を行います。

1. 信頼コントローラー上で **ipa-adtrust-install --add-agents** コマンドを実行します。これで対話式的設定セッションになり、エージェント設定に必要な情報の入力が必要になります。

--add-agents オプションについての詳細情報は、**ipa-adtrust-install(1)** man ページを参照してください。
2. LDAP サービスを再起動します。

信頼エージェントについての詳細は、「[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。

5.3. フォレスト間信頼環境の管理および設定

5.3.1. 信頼され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) を使ったログインに対応しています。UPN は認証に使用するユーザー名の代わりとなるもので、**username@KERBEROS-REALM** という形式になっています。Active Directory フォレストでは、追加の UPN 接尾辞を設定することができます。これらのエンタープライズプリンシパル名は、デフォルトの UPN の代替ログインとして使用できます。

例えば、ある企業で Kerberos レalm **AD.EXAMPLE.COM** を使っているとする、ユーザーのデフォルトの UPN は **user@ad.example.com** になります。しかし、企業ではユーザーが **user@example.com** といったメールアドレスを使用してログインできるようにする場合がよくあります。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、ユーザーアカウントのプロパティーでこの新たな接尾辞を設定します。

信頼された AD フォレストで UPN 接尾辞を追加したり削除する場合は、IdM マスター上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、代替 UPN がフェッチされたことを確認します。

```

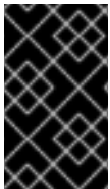
[root@ipaserver ~]# ipa trust-show
Realm-Name: ad.example.com
  Realm-Name: ad.example.com
  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
  Trust direction: Two-way trust
  Trust type: Active Directory domain
  UPN suffixes: example.com

```

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

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

IdM と Active Directory 間の信頼がある一部の環境では、ユーザーが IdM DNS ドメインからのホスト名を使用して Active Directory クライアントにアクセスする設定が可能な一方、クライアント自体は IdM に参加して Linux にフォーカスした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、一定の制限があります。Red Hat では、IdM が所有している DNS ゾーンとは別のゾーンに Active Directory クライアントをデプロイし、IdM ホスト名で IdM クライアントにアクセスすることを常に推奨しています。

5.3.2.1. IdM クライアントへの Kerberos シングルサインオンが不要

IdM DNS ドメインでの Active Directory クライアントの構成では、この IdM ホスト上のリソースにアクセスするには、パスワード認証のみが利用可能になっています。このシナリオ向けにクライアントを設定するには、以下を実行します。

1. クライアント上の System Security Service Daemon (SSSD) が IdM サーバーと通信できることを確認するために、IdM オプションを使って **--domain=IPA_DNS_Domain** クライアントをインストールします。

```

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

```

このオプションを使用すると、Active Directory DNS ドメインの SRV レコードの自動検出が無効になります。

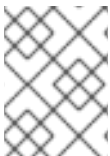
2. Active Directory 設定ファイル内の **[domain_realm]** セクションで **/etc/krb5.conf** ドメインの既存のマッピングを見つけます。


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

この両方の行を以下のような Active Directory DNS ゾーン内の Linux クライアントの完全修飾ドメイン名 (FQDN) から IdM レルムへのマッピングエントリで置き換えます。

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

デフォルトのマッピングを置換することで、Kerberos が Active Directory ドメインのリクエストを IdM Kerberos Distribution Center (KDC) に送信できなくなります。Kerberos は代わりに SRV DNS レコードによる自動検出を使用して KDC を見つけます。追加されたホストの **idm-client.ad.example.com** に対してのみ、IdM KDC は設定されます。



注記

IdM が所有する DNS ゾーン内にないクライアント上のリソースに対しての認証は、ユーザー名とパスワードを使用する方法のみになります。

SSL 証明書の処理

SSL ベースのサービスは、すべてのシステムホスト名をカバーしている dNSName 拡張子レコードがある証明書を必要とします。これは、オリジナル (A/AAAA) レコードと CNAME レルムの両方が証明書内にある必要があるためです。現時点では、IdM は IdM データベース内のホストオブジェクトにのみ証明書を発行します。

シングルサインオンが利用できない設定では、IdM はすでにデータベースに FQDN のホストオブジェクトがあり、**certmonger** がこの名前の証明書をリクエストできます。

```
[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 Certificate Authority (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

IdM クライアント上のリソースへのアクセスに Kerberos シングルサインオンが必要な場合は、このクライアントが例えば IdM などの **idm-client.idm.example.com** DNS ドメイン内にある必要があります。CNAME レコード **idm-client.ad.example.com** を Active Directory DNS ドメイン内に作成し、IdM クライアントの A/AAAA レコードを指す必要があります。

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キータブ内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ています。Kerberos サーバーのターゲットにどの Kerberos プリンシパルを使用したかを厳密にチェックすることを無効にするには、以下のオプションを **[libdefaults]** 設定ファイルの **/etc/krb5.conf** セクションに設定します。

```
ignore_acceptor_hostname = true
```

SSL 証明書の処理

SSL ベースのサービスは、すべてのシステムホスト名をカバーしている dNSName 拡張子レコードがある証明書が必要です。これは、オリジナル (A/AAAA) レコードと CNAME レルムの両方が証明書内にある必要があるためです。現時点では、IdM は IdM データベース内のホストオブジェクトにのみ証明書を発行します。

シングルサインオンが利用できない設定では、IdM はすでにデータベースに FQDN のホストオブジェクトがあり、**certmonger** がこの名前の証明書をリクエストできます。

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
```

ホスト名が A/AAAA レコードではなく CNAME であることから、**--force** オプションを使用します。

2. IdM DNS ホスト名が Active Directory データベースの IdM ホストエントリ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 ドメイン内のホスト名に対して dNSName 拡張子レコードのある SSL 証明書をリクエストすることができます。

```
[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. IdM ユーザー用の Active Directory グループの作成

ユーザーグループは、アクセス権限、ホストベースのアクセス制御、sudo ルールおよび IdM ユーザーの他の制御を設定するために必要です。これらのグループは、アクセスを制限するだけでなく、IdM ドメインリソースへのアクセスを付与する際のベースになります。

AD ユーザーと AD グループの両方を直接 IdM ユーザーグループに追加することができます。これを行うには、まず AD ユーザーまたはグループを 非 POSIX IdM 外部グループに追加し、その後にローカルの IdM POSIX グループに追加します。すると、POSIX グループを使用して AD ユーザーのユーザーおよびロール管理ができるようになります。この IdM 内の非 POSIX グループの処理についての原則は、「[Active Directory ユーザーと Identity Management グループ](#)」で説明しています。



注記

AD ユーザーグループを IdM 外部グループのメンバーとして追加することもできます。これにより、ユーザーおよびグループ管理を単一の AD レルム内で維持し、Windows ユーザー向けのポリシー定義が容易になる場合があります。

1. **これはオプションです。** IdM レルムで IdM ユーザー管理に使用する AD ドメインのグループを作成または選択します。複数のグループを使用して、側の異なるグループに追加することができます。
2. IdM オプションを Active Directory に追加して、**--external** ユーザー用に **ipa group-add** ドメインの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ことを示します。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
```

3. IdM ポリシーの管理用に新規の IdM POSIX グループを作成するか既存のものを選択します。例えば、新規グループを作成するには、以下を実行します。

```
[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** や **DOMAIN\username** などのその完全修飾名で識別されます。その後、AD のアイデンティティが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。

例えば 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 POSIX IdM グループにメンバーとして追加します。以下が例になります。

```
[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

信頼の管理には、グローバル信頼設定、Kerberos 信頼設定、DNS レルム設定、Active Directory ユーザーへの ID 範囲の割り当てなど多数の分野が関わってきます。

5.3.4.1. グローバル信頼設定の編集

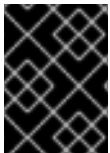
ipa-adtrust-install は、IdM ドメインとの信頼作成に必要な Active Directory ドメインのバックグラウンド情報を自動的に設定します。

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): 自動生成され、変更できません。
- ドメイン GUID: 自動生成され、変更できません。
- Kerberos ドメイン名: 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: 変更可能です。
- 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

NetBIOS 名の変更は多くの場合、すべての既存の信頼の再確立を必要とするため、Red Hat ではこの属性の変更は推奨していません。

ユーティリティを実行すると、Active**ipa-adtrust-install**Directory トポロジー内で互換性のある NetBIOS 名が IdM サーバー向けに設定されます。これを後で変更するには、**ipa-adtrust-install** オプションを使用して **--netbios-name** を再度実行し、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、PAC レコードが IdM ユーザーの Kerberos チケットに追加されます。MS-PAC レコードには、IdM が所属するグループのセキュリティー ID (SID) が含まれています。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と、*Default SMB Group*に定義されたセキュリティー ID 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場合も、同じ論理が Samba スイートで適用されます。

Default SMB Group は、**ipa-adtrust-install** ユーティリティが自動作成するフォールバックのグループです。デフォルトグループは削除することはできませんが、グローバル信頼設定を使用して別

の IdM グループを指定し、これを 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ことができます。

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 でデフォルトグループを設定するには、以下の手順に従います。

1. IdM web UI を開きます。

<https://ipaserver.example.com>

2. **IPA Server** メインタブから **Trusts** サブタブを選択し、**Global Configuration** セクションを開きます。
3. IdMFallback primary group ドロップダウンリストの全 グループから新規グループを選択します。

The screenshot shows the 'Global Trust Configuration' page in the IdM web UI. The 'Trusts' tab is active. Under the 'Options' section, several configuration fields are visible: Domain (ipa.test), Security Identifier (S-1-5-21-1951046116-856800292-3600857858), NetBIOS name (IPA), and Domain GUID (d07ea95b-feff-402a-9fba-0f92890d0cf7). At the bottom, the 'Fallback primary group' is set to 'Default SMB Group', which is highlighted by a red rectangular box.

図5.6 Windows ユーザーのデフォルトグループの設定

4. **Save** をクリックして新規設定を保存します。

5.3.4.2. 信頼ドメインの検出、有効化、および無効化

信頼が推移的ということは、信頼パスはドメインのチェーンをたどることになります。これについては、「[信頼関係のアーキテクチャー](#)」で詳述しています。

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、そのサブドメインおよび信頼される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、Windows ユーザーがフォレスト内の任意の場所から IdM リソースへアクセスを試行する際に、このトポロジに従います。各ドメインおよびサブドメインは **信頼設定**の trust domainIdM になります。各ドメインは、信頼サブツリーのそれぞれのエントリー **cn=subdomain,cn=trust_name,cn=ad,cn=trusts,dc=example,dc=com** に保存されます。

IdM は、信頼が最初に設定される際に完全な Active Directory トポロジの検出およびそのマッピングを試行します。ただし、場合によってはそのトポロジを手動で取得することが必要であるか、またはそれが望ましい場合があります。これは **trust-fetch-domains** コマンドで実行されます。

```
[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際には、AD フォレストのトポロジを手動で取得する必要があります。**ipa trust-add ad.domain --trust-secret** コマンドを実行した後に AD Domains and Trusts ツールでフォレスト信頼プロパティを使用し、AD 側での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 は使用可能になる信頼についての情報を受信します。

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

たとえば、特定サブ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. DNS レルムの表示および管理

信頼が設定される際に、Active Directory DNS 設定は IdM DNS 設定に追加され、それぞれのレルムは特別な **レルムドメイン** として追加されます。各ドメインは、**cn=Realm Domains,cn=ipa,cn=etc,dc=example,dc=com** ディレクトリーの IdM サブツリーに保存されます。

これらのレルムドメインは自動的に追加されるため、通常 DNS ゾーンを追加したり、変更したりする必要はありません。(IdM で設定されるすべての DNS ゾーンの一覧ではなく) 設定されたレルムドメインの一覧は、**realmdomains-show** コマンドを使用して表示することができます

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

単一レルムドメインを設定に追加する必要がある場合は、**--add-domain** オプションを使用して実行できます。

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

単一ドメインは **--del-domain** オプションを使用して削除することができます。

ドメインの一覧に対して複数の変更が行われる場合、**--domain** オプションを使用して一覧自体を変更し、置き換えることができます。

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

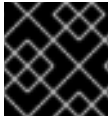
信頼を最初に設定する際に作成する ID 範囲は、「[ID の範囲](#)」で説明しています。後で ID 範囲を追加するには、以下のオプションを付けて **ipa idrange-add** コマンドを実行します。

- **--base-id** オプションは POSIX 範囲のベース ID を設定します。これが最初の番号になります。
- **--range-size** オプションは範囲のサイズを設定します。
- **--rid-base** オプションは RID の開始番号を設定します。これは SID の右端にある番号です。この値は、ベース ID に追加して競合を避ける範囲を表します。

- **--dom-sid** オプションはドメイン SID を設定します。これは、信頼に対して複数のドメインが設定される場合があるからです。

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 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. 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。例えば、シングルサインオンを使用して AD クライアントから IdM (AD) アカウントで Active Directory クライアントにログインする場合は、Kerberos TGT フラグ **OK_AS_DELEGATE** が必要になります。

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『Kerberos Flags for Services and Hosts』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が Active Directory によって送り返され、Kerberos チケットに組み込まれます。

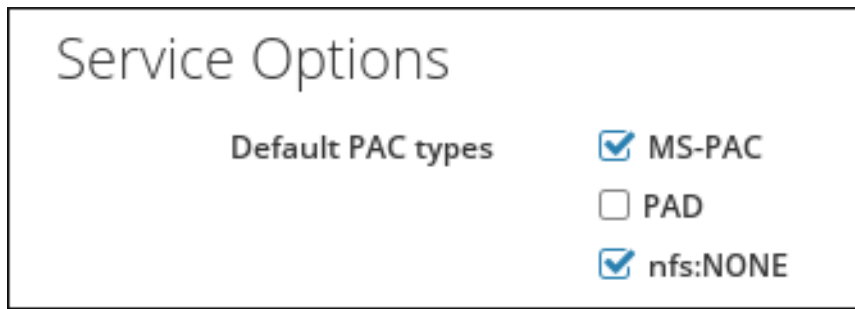
Active Directory のグループ情報は、Active Directory privileged access certificates または **MS-PAC** と呼ばれる特殊なデータセットとしてユーザーの各 Kerberos チケットの識別子の一覧に保存されます。PAC のグループ情報は Active Directory グループにマップされてから、対応する IdM グループにマップされ、アクセスの判別が行われます。

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、認証リクエストに対して 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。



Service Options

Default PAC types

☒ MS-PAC

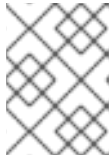
☐ PAD

☒ nfs:NONE

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して構いません。この機能はまだ IdM では利用可能になっていません。

5. 変更を保存するには、ページの上にある **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。

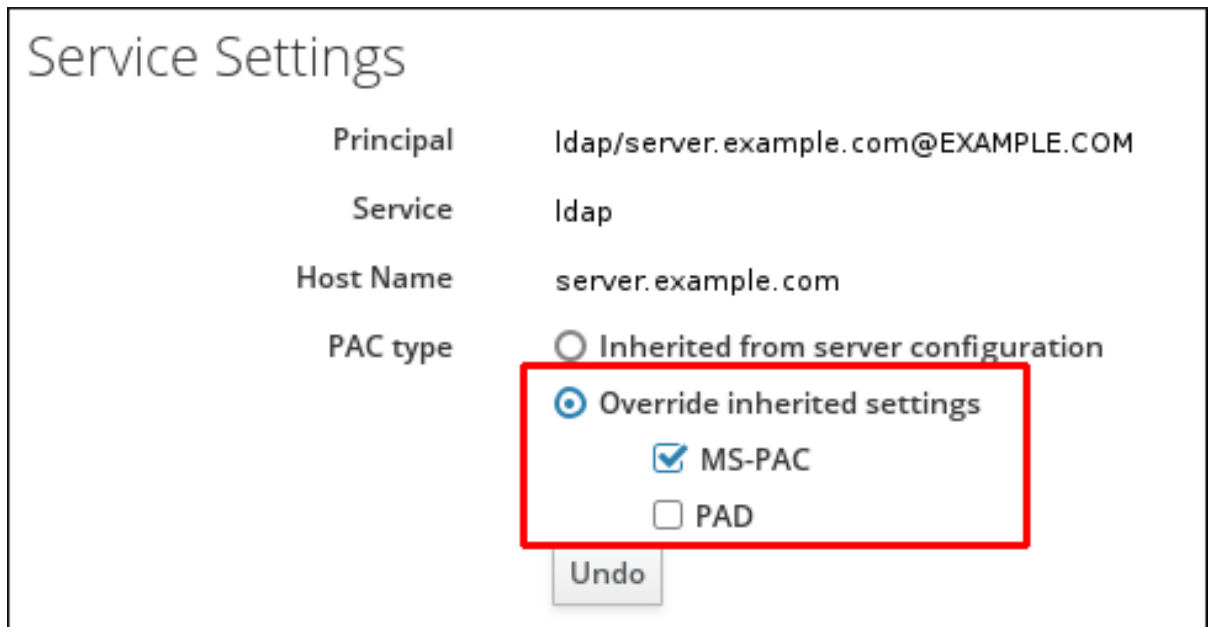
コマンドラインから PAC 設定を変更するには、**ipa service-mod** コマンドに **--pac-type** オプションを付けて実行します。このコマンドに関する詳細情報は、このコマンドに **--help** オプションを付けて実行してください。

```
$ 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。



Service Settings

Principal ldap/server.example.com@EXAMPLE.COM

Service ldap

Host Name server.example.com

PAC type

☐ Inherited from server configuration

☒ Override inherited settings

☒ MS-PAC

☐ PAD

Undo

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して構いません。この機能はまだ IdM では利用可能になっていません。

4. 変更を保存するには、ページの上にある **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 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 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。

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には、IdM サーバー上にある `/etc/sss/sssd.conf` ファイルの **[domain]** セクション内の **subdomain_homedir** オプションが **%o** に設定されている必要があります。**%o** の値は、ID プロバイダーから取得してホームディレクトリーを表します。例を示します。

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

AD 管理者が AD 側で **loginShell** や **unixHomeDirectory** を変更した場合は、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は、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. Active Directory リソースのために IdM マシンから SSH を使用

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 資格情報を使用して、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. 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 からの 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。**sss**d 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。

Red Hat Enterprise Linux 7.1 およびそれ以降のシステムにおける AD ユーザーの Kerberos 認証

Red Hat Enterprise Linux 7.1 およびそれ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 のあるシステムでは、`/etc/krb5.conf` ファイルの **auth_to_local** オプションを設定したり、**.k5login** ファイルに Kerberos プリンシパルを記載する必要がありません。**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

localauth プラグインがないシステムでは、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** ファイル内で **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で **.k5login** ファイルにユーザー Kerberos プリンシパルを記載します。

/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 レルムを名前で識別し、**auth_to_local** を 2 行追加して Kerberos プリンシパル名マッピングを定義します。
 - 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。
 - 2 つ目では、**DEFAULT** の値を標準 Unix ユーザー名に設定します。

例:

```
[realms]
IDM = {
    ....
    auth_to_local = RULE:[1:$1@$0]
    (^.*@ADDOMAIN$)s/@ADDOMAIN/@adomain/
    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は、SSH アクセスに使用するユーザー名は以下の基準を満たす必要があります。

- 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。例えば、**user** と **User** は文字の大きさが異なるので、別のユーザー名とみなされます。

auth_to_local の設定に関する詳細情報は、**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 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。

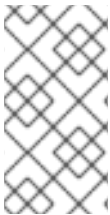
.k5login 設定を使用して Kerberos 認証を設定する場合は、SSH アクセスに使用しするユーザー名は **ad_user@ad_domain** の形式を取る必要があります。

.k5login ファイルの設定に関する詳細情報は、**.k5login(5) 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alm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、Apache サーバーが IdM Kerberos レalmに接続する方法を定義する以下のようなパラメーターがあります。

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 サーバーキータブの場所を指定します。これは必須です。

KrbServiceName

KrbServiceName オプションはキータブで使用する Kerberos サービス名を設定します (HTTP)。これは推奨オプションです。

KrbMethodK5Passwd および **KrbMethodNegotiate**

KrbMethodK5Passwd Kerberos メソッドオプションは、有効なユーザーの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シングルサインオン (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 または共通名) を完全修飾ユーザー名 (**user@REALM.COM** 形式) にマップできるようにします。

このオプションの使用は強く推奨されます。ドメイン名/ログイン名のマッピングがないと、web ログインにはドメインユーザーとは異なるユーザーアカウントが表示され、ユーザーには予測しないデータが表示されてしまいます。

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>
```

5.4. 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/sss/sss.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について説明します。

留意事項

- お使いの SSSD クライアントが直接 Active Directory ドメインに結合されている場合には、全クライアントで以下の手順を実行してください。
- お使いの SSSD クライアントが Active Directory との信頼関係がある Identity Management ドメインにある場合には、Identity Management サーバーで以下の手順を実行します。

手順

1. 信頼されたドメインの **sss.conf** に別の **[domain]** セクションがあることを確認します。信頼されたドメインの見出しは、以下のテンプレートに従うようにしてください。

```
[domain/main_domain/trusted_domain]
```

例:

```
[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、全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に関する詳細は、**sssd-ldap(5) 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には、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** の一般の **[domain]** セクションで、**debug_level** オプションを **10** 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/sss/** 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。

その他のリソース

- **sssd.conf** の信頼されたドメインセクションで使用可能なオプション一覧については、**sssd.conf(5) man** ページの **Trusted domain section** を参照してください。

5.5. 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。

5.5.1. 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/sss/sss.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について説明します。

留意事項

- お使いの SSSD クライアントが直接 Active Directory ドメインに結合されている場合には、全クライアントで以下の手順を実行してください。

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。

- お使いの SSSD クライアントが Active Directory との信頼関係がある Identity Management ドメインにある場合には、Identity Management サーバーで以下の手順を実行します。

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 7.4 の時点では、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. 信頼されたドメインの `sss.conf` に別の `[domain]` セクションがあることを確認します。信頼されたドメインの見出しは、以下のテンプレートに従うようにしてください。

```
[domain/main_domain/trusted_domain]
```

例:

```
[domain/idm.example.com/ad.example.com]
```

2. `sss.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リストします。

`ad_server` オプションと任意で Active Directory サーバーに `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に関する詳細は、`sss-ad(5) man` ページを参照してください。

例:

```
[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からの 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には、以下の手順で問題を解決します。

1. **sssd.conf** の一般の **[domain]** セクションで、**debug_level** オプションを **10** に設定します。
2. **/var/log/sss/** で SSSD ログを毛丸入して、どのサーバーに SSSD が問い合わせたかを確認します。

その他のリソース

- **sssd.conf** の信頼されたドメインセクションで使用可能なオプション一覧については、**sssd.conf(5)** man ページの **Trusted domain section** を参照してください。

5.6. 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 を使った 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 を使って 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 およびそれ以降
- Red Hat Enterprise Linux 6.0 – 6.3



重要

SSSD バージョン 1.9 およびそれ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 およびそれ以降は AD を使った IdM フォレスト間信頼にネイティブサポートを提供するので、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 を使用した信頼関係内にある IdM サーバーのドメインに参加すると、**compat LDAP** ツリーが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が、この **compat** ツリーでは、AD ユーザーは一定数の IdM サービスに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

5.6.1. 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 用の `ipa-server` パッケージと IdM 信頼アドオン用の `ipa-server-trust-ad` パッケージがインストール済みであること。
- **`ipa-server-install`** ユーティリティを実行して 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。

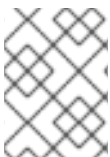
これまでに **`ipa-adtrust-install`** を **`--enable-compat`** オプションなしで実行している場合は、**`--enable-compat`** オプションを追加して再度実行してください。

- **`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`** サービスを有効にして AD ユーザーの認証を許可します。

`allow_all` コマンドを使用すると、コマンドラインから **`ipa hbacrule-show`** の現行ステータスを直接決定できます。このルールが無効になっている場合は、出力に **`Enabled: FALSE`** が表示されます。

```
[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『Configuring Host-Based Access Control』を参照してください。

IdM サーバー上で **`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 IdM マスターへのアクセスを付与する HBAC ルールを追加します。HBAC サービスおよびルールの追加については、[Linux ドメイン ID、認証、およびポリシーガイド](#) で説

明しています。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。

5.6.2. ipa-adviser ユーティリティーを使用したクライアント側の設定

ipa-adviser 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-adviser が設定指示を提供可能なすべてのシナリオを一覧表示するには、**ipa-adviser** をオプションなしで実行します。これで利用可能な全設定指示のセットの名前と各セットの実行内容、推奨される実行時期がプリントされます。

```
[root@server ~]# ipa-adviser
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-adviser** ユーティリティーを実行します。

```
[root@server ~]# ipa-adviser 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-adviser 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-adviser 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。

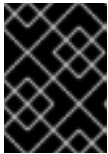
```
[root@server ~]# chmod +x setup_script.sh
```

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. クライアント上でスクリプトを実行します。

```
[root@client ~]# ./setup_script.sh
```



重要

クライアント上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読み、注意深く見なおしてください。

クライアントを手動で設定するには、**ipa-adviser** で表示される指示をコマンドラインから実行します。

パート III. LINUX ドメインと **ACTIVE DIRECTORY** ドメインの統合: 同期

第6章 ACTIVE DIRECTORY と IDENTITY MANAGEMENT ユーザーの同期

本章では、Active Directory と Red Hat Enterprise Linux Identity Management の間の同期について説明します。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。推奨されるもう1つの方法がクロスフォレストのトラストですが、これに関する詳細は、[5章Active Directory および Identity Management によるフォレスト間の信頼作成](#)を参照してください。お使いの環境でどちらの方法を選択するといいいのか不明な場合には、「[間接的な統合](#)」を確認してください。

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 サーバーのディレクトリーデータに接続およびそれを取得するため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. サポートされる 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。

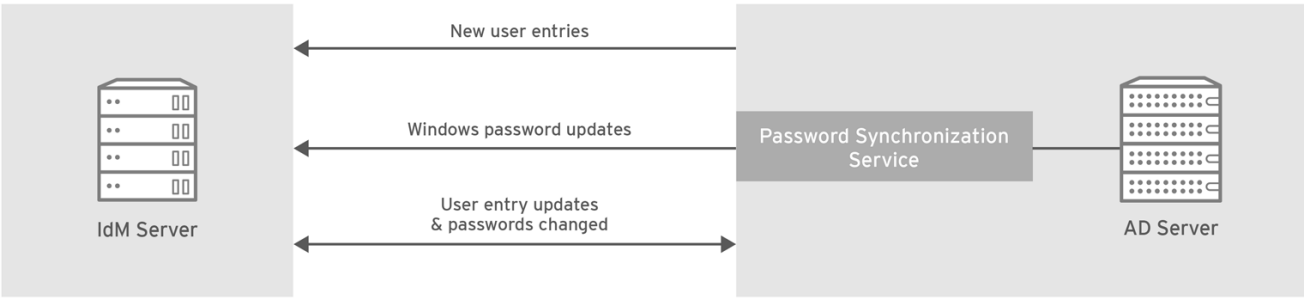
6.2. ACTIVE DIRECTORY および IDENTITY MANAGEMENTについて

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。

AD-IDM SYNC PROCESS



RHEL_404973_0516

図6.1 Active Directory および IdM の同期

同期は an 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ため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
<ul style="list-style-type: none">● ユーザーのサブツリー (cn=Users, \$SUFFIX)● 接続情報<ul style="list-style-type: none">○ Active Directory 管理者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	<ul style="list-style-type: none">● 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 ドメインと 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避けるには、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、同期は 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設定されます。Identity Management サーバーはスループットを 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。

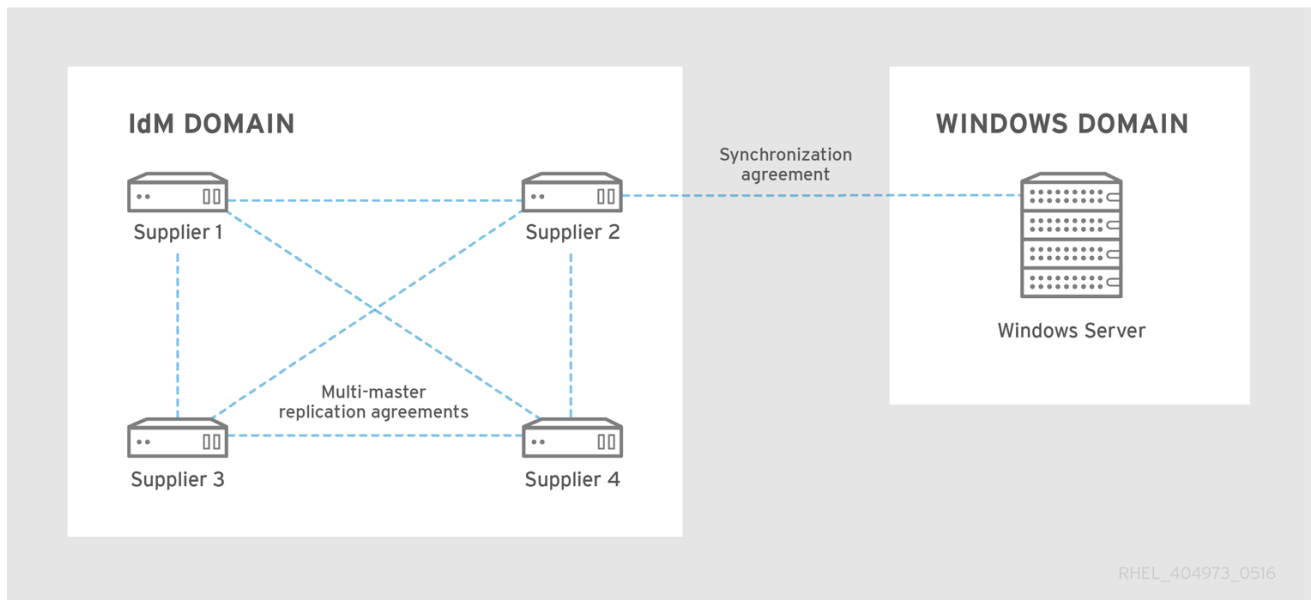


図6.2 同期トポロジー

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=meTowinserver.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。
  - また、同期は 1 つの Active Directory ドメインコントローラーでしか設定できません。
  - 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 (Active Directory から IdM および IdM から Active Directory の両方向) で行われますが、アカウントの作成は、Active Directory から Identity Management の一方向でのみ行われます。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。このような場合には、同期プロセスは、Active Directory の `sAMAccountName` 属性ではなく、IdM の `uid` 属性と同じ値のアカウントを検索使用とします。IdM `ntUserDomainId` 属性が Active Directory `objectGUID` の値に設定されます。これらの属性は、グローバルで一意的かつ不変の値で、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。**

パスワード同期クライアントがインストールされている場合には、IdM と Active Directory の両方のハッシュ化形式で保存されている既存のパスワードについては、暗号化を解除したり、同



期したりすることができないため、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。これらの属性は、IdM によって、IPA ドメイン内で使用されますが、適切な Active Directory ユーザーエントリーに同期し直されるわけではありません。

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することができます。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. 同期された属性について

Identity Management は IdM と Active Directory 間のユーザーエントリーのサブセットを同期します。Identity Management または Active Directory にあるエントリーの他の属性は、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 LDAP スキーマと、Identity Management で使用される 389 Directory Server 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<sup>[1]</sup>
- physicalDeliveryOfficeName
- 説明
- 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 間でマップされるユーザスキーマ**

| Identity Management | Active Directory   |
|---------------------|--------------------|
| cn[a]               | name               |
| nsAccountLock       | userAccountControl |
| ntUserDomainId      | sAMAccountName     |
| ntUserHomeDir       | homeDirectory      |
| ntUserScriptPath    | scriptPath         |
| ntUserLastLogon     | lastLogon          |
| ntUserLastLogoff    | lastLogoff         |

| Identity Management                                                                                                                                                                                                                     | Active Directory |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| ntUserAcctExpires                                                                                                                                                                                                                       | accountExpires   |
| ntUserCodePage                                                                                                                                                                                                                          | codePage         |
| ntUserLogonHours                                                                                                                                                                                                                        | logonHours       |
| ntUserMaxStorage                                                                                                                                                                                                                        | maxStorage       |
| ntUserProfile                                                                                                                                                                                                                           | profilePath      |
| ntUserParms                                                                                                                                                                                                                             | userParameters   |
| ntUserWorkstations                                                                                                                                                                                                                      | userWorkstations |
| <p>[a] <b>cn</b> は、Identity Management から Active Directory に同期される場合には、<b>cn</b> から <b>cn</b> に直接マッピングされます。Active Directory から同期する場合には、<b>cn</b> は Active Directory の <b>name</b> 属性から Identity Management の <b>cn</b> 属性にマッピングされます。</p> |                  |

### 6.3.1. Identity Management と Active Directory 間のユーザスキーマの相違点

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 で編集す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) 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 **streetAddress** 属性を使用します。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 および Identity Management が **streetAddress** および **street** 属性を使用する方法には 2 つの重要な相違点があります。

- 389 Directory Server では、**streetAddress** は **street** のエイリアスです。Active Directory にも **street** 属性がありますが、**streetAddress** のエイリアスではなく、別の属性で個別の値を保持することができます。
- Active Directory は **streetAddress** と **street** を単一値の属性として定義しますが、389 Directory Server は RFC 4519 に指定されているように **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。

- 同期プロセスでは、Active Directory エントリーの **streetAddress** を Identity Management の **street** にマッピングします。競合を避けるために、**street** 属性は Active Directory では使用しないようにしてください。
- Identity Management **street** 属性値 1 つのみが 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 **street** 属性値が新しい Active Directory の値に置き換えられます。

#### 6.3.1.3. initials 属性についての制約

**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 Server 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トリミングされます。

#### 6.3.1.4. surname (sn) 属性の要求

Active Directory では、surname 属性なしに **person** エントリーを作成できますが、RFC 4519 では **person** オブジェクトクラスに surname 属性が必要とされており、この定義が Directory Server で使用されます。

Active Directory **person** エントリーが surname 属性なしで作成される場合には、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** と **gidNumber** 属性値が含まれる場合には、WinSync はこの値を Identity Management には同期せず、Identity Management に新しい UID と GID の値を作成します。

そのため、**uidNumber** と **gidNumber** の値は Active Directory と Identity Management では異なります。

## 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おり、同期合意 (「[同期合意の作成](#)」) の設定だけが必要です。ただし、Active Directory では、Identity Management サーバーが接続できる方法で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** 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 証明局の設定

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することができます。

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、構成手順は、Microsoft のドキュメント ([http://technet.microsoft.com/en-us/library/cc772393\(v=WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc772393(v=WS.10).aspx)) に記載されています。

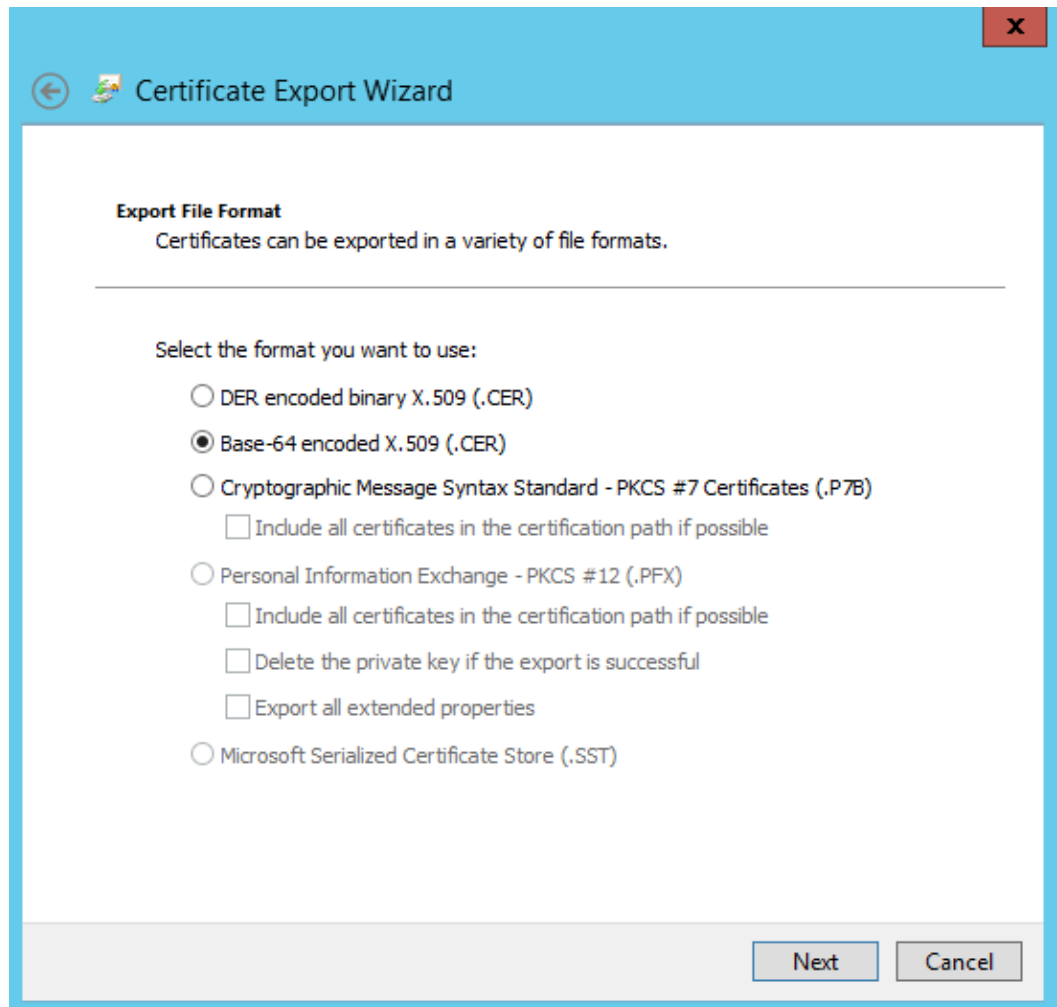
## 6.5. 同期合意の管理

### 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** を作成するので、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には、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、以下の手順を実行します。
    - i. Windows サーバー上の 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** を入力して **OK** をクリックします。
      - C. ローカルの証明局の名前を右クリックして、**プロパティ** を選択します。
      - D. **全般** タブの **CA 証明局** でエクスポートする証明書を選択し、**s s 証明書の表示** 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. **次へ** をクリックしてから、**base-64** でエンコードされた **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。**次へ** をクリックして証明書をエクスポートしてから、**完了** 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 証明書が外部の CA で署名されている場合は、以下の手順を実行します。
- 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。ユーザーアカウントと一緒にパスワードも同期する場合、**--passsync** オプションも使用して、パスワードの同期に使用するパスワードを設定します。

**--binddn** 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と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て属性を同期します。
- **--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。
  - CA 証明書が自己署名されている場合: Active Directory CA 証明書。
  - Active Directory CA が外部の CA で署名されている場合: 外部の CA 証明書。
- **--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. これはオプションです。「**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には、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の変更を取り込み、Active Directory と IdM 間でこれらの変更を同期します。つまり、その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。

パスワード同期クライアントがインストールされている場合には、IdM と Active Directory の両方のハッシュ化形式で保存されている既存のパスワードについては、暗号化を解除したり、同期したりすることができないため、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、同期中の同期プロセスで、ユーザーアカウント属性を処理する方法についての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、デフォルトでは、アカウントのロックアウト属性は IdM と Active Directory 間で同期されますが、**ipaWinSyncAcctDisable** 属性を編集して無効にできます (この変更により、アカウントは Active Directory で無効にされている場合にも IdM ではアクティブな状態になり、その逆の場合も同じになります)。

```
[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**)

- **ipaWinSyncNewUserOCAAttr**: 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 ユーザーが Active Directory ドメインから同期される



場合に AD ユーザーに追加する特定の値で追加の属性を設定します。この属性が複数値の属性の場合は、これを複数回設定でき、同期プロセスは値のすべてをエントリーに追加します。

例: **ipaWinSyncUserAttr: attributeName attributeValue**



#### 注記

これにより、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エントリーの値は Active Directory エントリーの同期時に使用されます。

- **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、一致する IdM ユーザーが自動的に編集され、同期されます。

使用可能な値: **true | false**

an IdM ユーザーに、既存の Active Directory ユーザーの **sAMAccountName** と同一の **uid** パラメーターがある場合には、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、同期サービスに対して、**ntUser** および **ntUserDomainId** を IdM ユーザーエントリーに自動的に追加し、同期されるように指示します。

### 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することができます。たとえば、**to\_ad** は、アカウントロックアウト属性が IdM に設定される場合に、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。

使用可能な値: **both** (デフォルト)、**to\_ad**、**to\_ds**、**none**

- **ipaWinSyncInactivatedFilter:** 非アクティブ化された (無効にされた) 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。その後、エントリーのグループ名がユーザーアカウントの **gidNumber** の検索に使用されます。

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。その後、エントリーのグループ名がユーザーアカウントの **gidNumber** の検索に使用されます。

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alm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

同期契約を作成すると、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的に設定されます。IdMの場合は、デフォルトは **cn=users, cn=accounts, \$SUFFIX** となり、Active Directoryの場合は、デフォルトは **CN=Users, \$SUFFIX** となります。

Active Directory サブツリーの値は、**--win-subtree** オプションを使用して同期合意が作成される場合はデフォルト以外の値に設定できます。この合意の作成後に、**ldapmodify** コマンドを使用し、同期合意エントリー内の **nsds7WindowsReplicaSubtree** 値を編集して 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。この検索により、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=nsds7WindowsReplicaSubtree 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 の変更は Identity Management に対して行われ、Identity Management のエントリーの変更は Active Directory に対して同期されます。これは本質的に平等な複数マスター関係であり、Active Directory と Identity Management はどちらも同期におけるピアであり、どちらもデータマスターになります。

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、複数マスターの関係 (ピアサーバーが平等) からマスター対コンシューマーの関係に同期関係が変更されます。

これには、同期合意で **oneWaySync** パラメーターを設定します。許容値は、**fromWindows** (Active Directory から Identity Management への同期) および **toWindows** (Identity Management から Active Directory への同期) です。

たとえば、Active Directory から Identity Management に変更を同期するには、以下を実行します。

```
[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=map
ping tree,cn=config
changetype: modify
add: oneWaySync
oneWaySync: fromWindows
```

### 重要

一方向の同期を有効にしても、一方向で同期された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。たとえば一方向の同期は、Active Directory から Identity Management の方向に設定されるため、Active Directory は (基本的には) データマスターになります。エントリーが Identity Management で変更されるか、または削除される場合に、Identity Management 情報は異なりますが、その情報および変更は Active Directory に移行されることはありません。次の同期更新時に、編集内容は Directory Server で上書きされ、エントリーを削除していても再び追加されます。

## 6.5.5. 同期合意の削除

同期は、とサーバーのIdM接続を解除するActive Directory、同期合意の削除によって停止することができます。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
```

- Active Directory サーバーデータベースから IdM 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 契約のエラー

#### Active Directory サーバーに接続できないために、同期合意の作成に失敗する

同期合意における最も一般的なエラーの 1 つは、IdM サーバーが Active Directory サーバーに接続できないことです。

```
"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ためパスワードが同期されないというエラーが出る

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す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 の両方にあるパスワードは通常のユーザー同期プロセスの一部として組み込まれ

てはいません。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の変更を取り込み、Active Directory と IdM 間でこれらの変更を同期します。つまり、その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。

パスワード同期クライアントがインストールされている場合には、IdM と Active Directory の両方のハッシュ化形式で保存されている既存のパスワードについては、暗号化を解除したり、同期したりすることができないため、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 で実行されていること。



#### 注記

Enterprise Root Mode で Microsoft 証明書システムをインストールします。次に Active Directory はその SSL サーバー証明書を取得するために自動的に登録されます。

- パスワード同期サービスが各 Active Directory ドメインコントローラーでインストールされていること。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。
- IdM と Active Directory 側でパスワードポリシーが同様に設定されていること。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以下を実行します。

```
> dsquery * -scope base -attr pwdProperties
pwdProperties
1
```

**pwdProperties** が **1** に設定されていれば、そのドメインのパスワード複雑性が有効になっています。

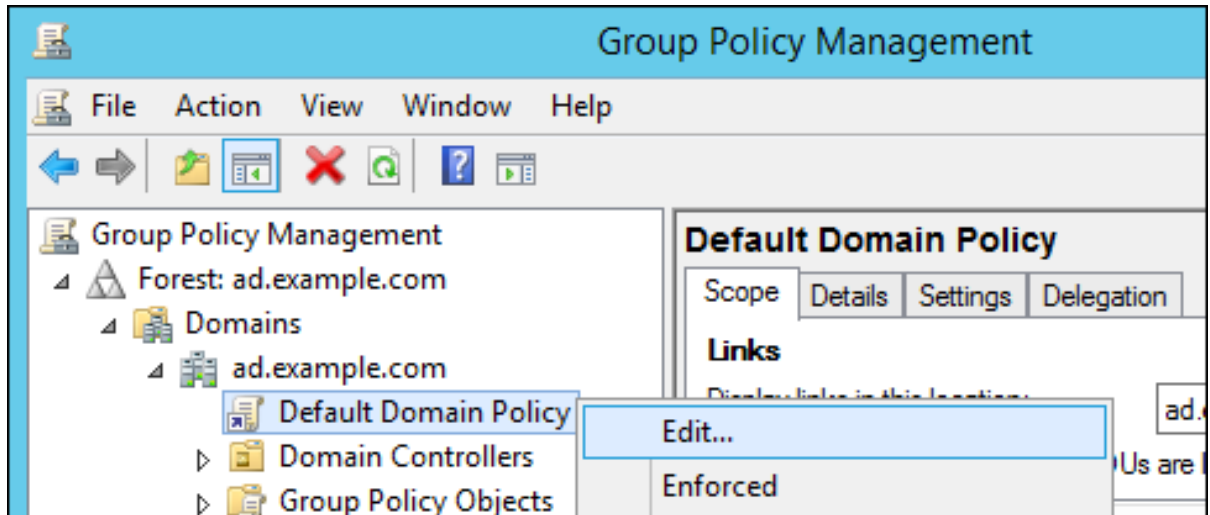


#### 注記

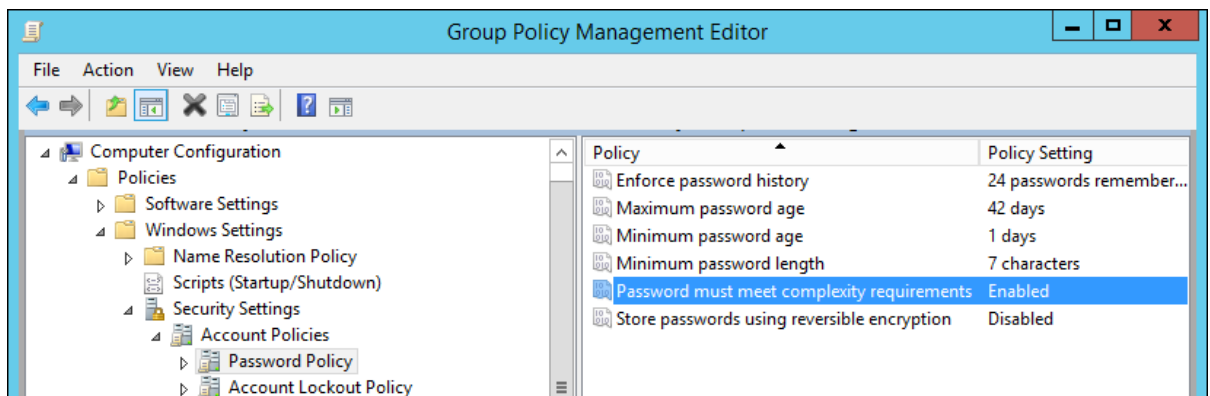
グループポリシーが Organizational Units (ou) の逸脱パスワード設定を定義しているかどうか不明な場合は、グループポリシーの管理者に問い合わせてください。

ドメイン全体に対して Active Directory パスワードの複雑性設定を有効にするには、以下の手順に従います。

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. **PassSync.msi** ファイルを Active Directory マシンにダウンロードします。
  1. カスタマーポータルにログインします。
  2. 左上の **ダウンロード** リンクをクリックします。

### 3. Red Hat Enterprise Linux を選択します。

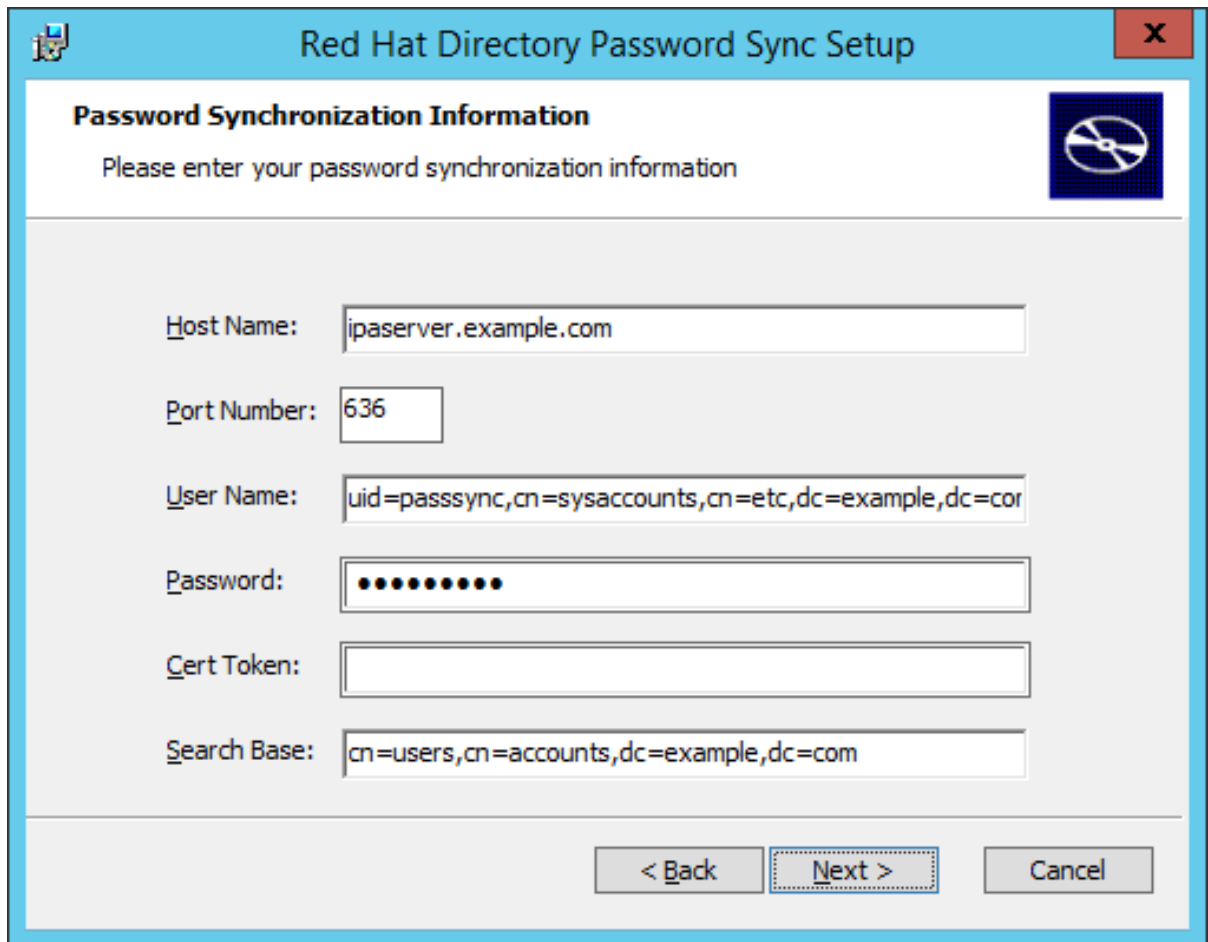
4. Red Hat Enterprise Linux 6 または Red Hat Enterprise Linux 7 のバージョンとアーキテクチャーを選択します。
5. 「今すぐダウンロードする」 ボタンをクリックして **PassSync Installer** をダウンロードします。



#### 注記

Red Hat Enterprise Linux アーキテクチャーの種類を問わず、利用できる 2 つの PassSync パッケージがあります。1 つは 32-bit Windows サーバー用で、もう 1 つは 64-bit 用です。お使いの Windows プラットフォームに適したパッケージを選択するようにしてください。

2. Password Synchronization MSI ファイルをダブルクリックして、これを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. 以下の情報を入力し、IdM サーバーへの接続を設定します。
  - 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 マシンに接続するために IdM が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るパスワード。
  - IdM サーバー上の People サブツリーの検索ベース。Active Directory サーバーは、IdM またはレプリケーション操作の場合と同様に **ldapsearch** サーバーに接続します。そのため、IdM サブツリーのどこでユーザーアカウントを検索できるかを認識する必要があります。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。



**Red Hat Directory Password Sync Setup**

**Password Synchronization Information**

Please enter your password synchronization information

Host Name:

Port Number:

User Name:

Password:

Cert Token:

Search Base:

< Back    Next >    Cancel

**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。

1. 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。
2. IdM CA 証明書を Active Directory サーバーにコピーします。
3. 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。以下が例になります。

```
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、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の変更を取り込み、Active Directory と IdM 間でこれらの変更を同期します。つまり、その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。

パスワード同期クライアントがインストールされている場合には、IdM と Active Directory の両方のハッシュ化形式で保存されている既存のパスワードについては、暗号化を解除したり、同期したりすることができないため、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、例えば、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検証、有効にする方法については、[「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。

---

[1] **cn** は他の同期属性とは異なる処理がされます。Identity Management から Active Directory に同期される場合には、**cn** から **cn** に直接同期されますが、Active Directory から Identity Management の場合は、**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。

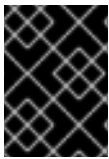
## 第7章 同期から信頼への既存環境の移行

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) 信頼をベースと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について説明しています。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** ユーティリティは、Red Hat Enterprise Linux 7.2 およびそれ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 を使った移行の仕組み

**ipa-winsync-migrate** ユーティリティは、同期済みユーザーすべてを AD フォレストから移行します。この間、既存の Winsync 環境は維持され、これが AD 信頼に送信されます。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、Winsync 内のオリジナル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、ユーザーアカウントのローカルコピーすべてが削除されます。

### 7.1.2. ipa-winsync-migrate を使用した移行方法

作業開始前に、以下を実行してください。

- **ipa-backup** ユーティリティーを使って 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『Backing Up and Restoring Identity Management』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 による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alm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についての詳細は、ipa-winsync-migrate(1) 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についての詳細は、[5章Active Directory および Identity Management による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 view 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、「[ホスト毎にユーザーアカウントで異なる属性値を定義する](#)」を参照してください。



#### 注記

ID ビューを管理できるのは IdM ユーザーのみで、AD ユーザーは管理できません。

4. 元の同期したユーザーまたはグループ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については、[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 ユーザーもしくはグループ属性の新規の値を指定でき、どのクライアントホストに新たな値を適用するかを定義することができます。

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事で、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 ビュー機能について説明します。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 ビューを使った 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。

デフォルト信頼ビューを使うことで、AD ユーザーおよびグループのカスタム POSIX 属性を定義することができ、AD で定義された値を上書きします。

表8.1 デフォルト信頼ビューの適用

|      | AD 内の値  | デフォルト信頼ビュー |   | 結果      |
|------|---------|------------|---|---------|
| ログイン | 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ので、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は、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は、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 内の値  | デフォルト信頼ビュー | ホスト固有のビュー |   | 結果      |
|------|---------|------------|-----------|---|---------|
| ログイン | 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 オーバーライド位

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) に拘わらず、デフォルト信頼ビューからの ID オーバーライドを常に適用します。

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。例えば、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 ビューを使った 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。

例えば、Linux-Windows の混合環境を管理していて、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で AD ポリシーがこれを許可しない場合は、ID ビューを使っ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 ツリーを使って認証する場合、新規の値が認証プロセスで使用されます。



### 注記

ID ビューを管理できるのは IdM ユーザーのみで、AD ユーザーは管理できません。

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. 新規 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「異なるホスト上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。

## 8.4. NIS ドメインの IDM への移行

Linux 環境を管理していて、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管理ソリューションに移行する場合は、ID ビューを使ってホスト固有の 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。詳細は以下を参照してください。
  - [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、「[ホスト毎にユーザーアカウントで異なる属性値を定義する](#)」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』に従い、「[LinuxのドメインID、認証、およびポリシーガイドのインストールとアンインストール](#)」をします。
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について説明します。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

**domain resolution order** オプションを使用してドメイン一覧の検索順を指定し、特定のユーザー名に一致するアイテムを返すことができます。以下のいずれかにオプションを設定できます。

- サーバー上の設定方法は、以下を参照してください。
  - 「[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](#)」
- クライアント上の設定方法は、「[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 トラスト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。

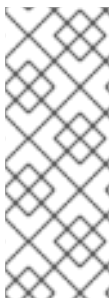
特定のクライアントからすると、上記の 3 つの場所の内、複数箇所に **domain resolution order** オプションを設定できます。クライアントが 3 つの場所を参照する順番は、以下のとおりです。

1. ローカルの **sssd.conf** 設定
2. ID ビューの設定
3. グローバルの 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、クライアントでしか、ドメイン解決の順番を設定できません。





## 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 **default\_domain\_suffix** オプションが含まれており、このオプションで指定していないドメインに要求を送信する場合

## 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には、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、複数のサブ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.exa
mple.com
...
```

このような方法でドメイン解決順を設定した場合には、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、ショートネームだけ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、*server.idm.example.com* のサブドメインサーバーで、*subdomain1.ad.example.com* よりも、*subdomain2.ad.example.com* サブドメインからのログインがはるかに多く検出されているにもかかわらず、グローバル解決順では、*subdomain2.ad.example.com* よりも先に、*subdomain1.ad.example.com* サブドメインユーザーのデータベースを試すように記述されています。特定のサーバーに別の順番を設定するには、特定のビューに対してドメイン解決順を設定します。

1. **domain resolution order** オプションセットで 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. 以下のように、クライアントにこのビューを適用します。

```
$ 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 に接続する場合には、クライアントにドメイン解決順を設定します。

たとえば、`/etc/sss/sss.conf` ファイルの `[sss]` セクションで、`domain_resolution_order` オプションを設定します。

```
domain_resolution_order = subdomain1.ad.example.com,
subdomain2.ad.example.com
```

`domain_resolution_order` オプションの詳細情報は、`sss.conf(5)` man ページを参照してください。

## 付録A 改訂履歴

|                                                                                                       |                        |                               |
|-------------------------------------------------------------------------------------------------------|------------------------|-------------------------------|
| <b>改訂 7.0-46.1</b><br>翻訳ファイルを XML ソースバージョン 7.0-46 と同期                                                 | <b>Thu Sep 20 2018</b> | <b>Ludek Janda</b>            |
| <b>改訂 7.0-46</b><br>7.6 GA 公開用ドキュメントの準備                                                               | <b>Mon Oct 29 2018</b> | <b>Filip Hanzelka</b>         |
| <b>改訂 7.0-45</b><br>『SMB 共有アクセス用の SSSD と Winbind の切り替え』の追加                                            | <b>Mon Jun 25 2018</b> | <b>Filip Hanzelka</b>         |
| <b>改訂 7.0-44</b><br>7.5 GA 公開用ドキュメントの準備                                                               | <b>Thu Apr 5 2018</b>  | <b>Filip Hanzelka</b>         |
| <b>改訂 7.0-43</b><br>『SSSD がサポートする GPO 設定』の更新                                                          | <b>Wed Feb 28 2018</b> | <b>Filip Hanzelka</b>         |
| <b>改訂 7.0-42</b><br>『共有シークレットでの双方向の信頼作成』を更新                                                           | <b>Mon Feb 12 2018</b> | <b>Aneta Šteflová Petrová</b> |
| <b>改訂 7.0-41</b><br>数カ所を若干修正                                                                          | <b>Mon Jan 29 2018</b> | <b>Aneta Šteflová Petrová</b> |
| <b>改訂 7.0-40</b><br>数カ所を若干修正                                                                          | <b>Fri Dec 15 2017</b> | <b>Aneta Šteflová Petrová</b> |
| <b>改訂 7.0-39</b><br>『Active Directory 統合での Samba の使用』の更新                                              | <b>Mon Dec 6 2017</b>  | <b>Aneta Šteflová Petrová</b> |
| <b>改訂 7.0-38</b><br>信頼用の『DNS およびレルムの設定』の更新                                                            | <b>Mon Dec 4 2017</b>  | <b>Aneta Šteflová Petrová</b> |
| <b>改訂 7.0-37</b><br>『共有シークレットでの双方向の信頼作成』を更新                                                           | <b>Mon Nov 20 2017</b> | <b>Aneta Šteflová Petrová</b> |
| <b>改訂 7.0-36</b><br>数カ所を若干修正                                                                          | <b>Mon Nov 6 2017</b>  | <b>Aneta Šteflová Petrová</b> |
| <b>改訂 7.0-35</b><br>『Active Directory エントリおよび 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 | <b>Mon Oct 23 2017</b> | <b>Aneta Šteflová Petrová</b> |
| <b>改訂 7.0-34</b><br>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                                | <b>Mon Oct 9 2017</b>  | <b>Aneta Šteflová Petrová</b> |
| <b>改訂 7.0-33</b><br>SSSD の章の自動検出セクションを更新。信頼ドメインの設定に関する 2 セクションを追加                                     | <b>Tue Sep 26 2017</b> | <b>Aneta Šteflová Petrová</b> |
| <b>改訂 7.0-32</b><br>7.4 GA 公開用ドキュメントバージョン                                                             | <b>Tue Jul 18 2017</b> | <b>Aneta Šteflová Petrová</b> |
| <b>改訂 7.0-31</b><br>セキュリティ ID マッピングについて若干修正                                                           | <b>Tue May 23 2017</b> | <b>Aneta Šteflová Petrová</b> |
| <b>改訂 7.0-30</b><br>Windows 統合定義についてのマイナーな修正。                                                         | <b>Mon Apr 24 2017</b> | <b>Aneta Šteflová Petrová</b> |

|                                                                                                                           |                        |                               |
|---------------------------------------------------------------------------------------------------------------------------|------------------------|-------------------------------|
| <b>改訂 7.0-29</b>                                                                                                          | <b>Mon Apr 10 2017</b> | <b>Aneta Šteflová Petrová</b> |
| 直接的な統合の更新。                                                                                                                |                        |                               |
| <b>改訂 7.0-28</b>                                                                                                          | <b>Mon Mar 27 2017</b> | <b>Aneta Šteflová Petrová</b> |
| 「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として 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。無効だったリンクを修正。他のマイナーな更新。 |                        |                               |
| <b>改訂 7.0-27</b>                                                                                                          | <b>Mon Feb 27 2017</b> | <b>Aneta Šteflová Petrová</b> |
| 信頼のポート要件を更新。信頼および同期に関するマイナーな再構築。他のマイナーな更新。                                                                                |                        |                               |
| <b>改訂 7.0-26</b>                                                                                                          | <b>Wed Nov 23 2016</b> | <b>Aneta Šteflová Petrová</b> |
| ipa-winsync-migrate を追加。信頼、SSSD、および同期の各章でマイナーな修正。                                                                         |                        |                               |
| <b>改訂 7.0-25</b>                                                                                                          | <b>Tue Oct 18 2016</b> | <b>Aneta Šteflová Petrová</b> |
| 7.3 GA 公開用バージョン                                                                                                           |                        |                               |
| <b>改訂 7.0-24</b>                                                                                                          | <b>Thu Jul 28 2016</b> | <b>Marc Muehlfeld</b>         |
| 図を更新、サービスおよびホストの Kerberos フラグを追加、他のマイナーな修正。                                                                               |                        |                               |
| <b>改訂 7.0-23</b>                                                                                                          | <b>Thu Jun 09 2016</b> | <b>Marc Muehlfeld</b>         |
| 同期の章を更新。Kerberos の章を削除。他のマイナーな修正。                                                                                         |                        |                               |
| <b>改訂 7.0-22</b>                                                                                                          | <b>Tue Feb 09 2016</b> | <b>Aneta Petrová</b>          |
| realmd を更新、index を削除、ID ビューの一部を Linux ドメイン ID ガイドに移動、他のマイナーな更新。                                                           |                        |                               |
| <b>改訂 7.0-21</b>                                                                                                          | <b>Fri Nov 13 2015</b> | <b>Aneta Petrová</b>          |
| 7.2 GA リリース向けのバージョンにマイナーな更新                                                                                               |                        |                               |
| <b>改訂 7.0-20</b>                                                                                                          | <b>Thu Nov 12 2015</b> | <b>Aneta Petrová</b>          |
| 7.2 GA リリース向けのバージョン                                                                                                       |                        |                               |
| <b>改訂 7.0-19</b>                                                                                                          | <b>Fri Sep 18 2015</b> | <b>Tomáš Čapek</b>            |
| スプラッシュページに並び替え順序を更新。                                                                                                      |                        |                               |
| <b>改訂 7.0-18</b>                                                                                                          | <b>Thu Sep 10 2015</b> | <b>Aneta Petrová</b>          |
| 出力形式を更新。                                                                                                                  |                        |                               |
| <b>改訂 7.0-17</b>                                                                                                          | <b>Mon Jul 27 2015</b> | <b>Aneta Petrová</b>          |
| GPO ベースのアクセス制御を追加、多数の他のマイナーな変更。                                                                                           |                        |                               |
| <b>改訂 7.0-16</b>                                                                                                          | <b>Thu Apr 02 2015</b> | <b>Tomáš Čapek</b>            |
| ipa-adviser を追加、SSSD を使った CIFS 共有を拡大、UNIX 拡張のアイデンティティ管理の警告                                                                |                        |                               |
| <b>改訂 7.0-15</b>                                                                                                          | <b>Fri Mar 13 2015</b> | <b>Tomáš Čapek</b>            |
| 7.1 向けの最終変更を含む同期更新。                                                                                                       |                        |                               |
| <b>改訂 7.0-13</b>                                                                                                          | <b>Wed Feb 25 2015</b> | <b>Tomáš Čapek</b>            |
| 7.1 GA リリース用バージョン。                                                                                                        |                        |                               |
| <b>改訂 7.0-11</b>                                                                                                          | <b>Fri Dec 05 2014</b> | <b>Tomáš Čapek</b>            |
| スプラッシュページでの分類順序を更新して再構築。                                                                                                  |                        |                               |
| <b>改訂 7.0-7</b>                                                                                                           | <b>Mon Sep 15 2014</b> | <b>Tomáš Čapek</b>            |
| 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。                                                                                       |                        |                               |
| <b>改訂 7.0-5</b>                                                                                                           | <b>June 27, 2014</b>   | <b>Ella Deon Ballard</b>      |
| Samba+Kerberos+Winbind の各章を改善。                                                                                            |                        |                               |

**改訂 7.0-4**

Kerberos レルムの章を追加。

**June 13, 2014**

**Ella Deon Ballard**

**改訂 7.0-3**

初期リリース。

**June 11, 2014**

**Ella Deon Ballard**