



Red Hat Enterprise Linux 9

IdM と AD との間信頼のインストール

IdM ドメインと Active Directory ドメインとの間のフォレスト間の信頼の設定

Red Hat Enterprise Linux 9 IdM と AD との間の信頼のインストール

IdM ドメインと Active Directory ドメインとの間のフォレスト間の信頼の設定

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

法律上の通知

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Installing_trust_between_IdM_and_AD.ent file |.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

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, the Red Hat 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 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

本書は、Identity Management デプロイメントと Active Directory(AD)環境との間で信頼を作成する方法を説明します。

目次

多様性を受け入れるオープンソースの強化	4
RED HAT ドキュメントへのフィードバック (英語のみ)	5
第1章 信頼を確立するための前提条件	6
第2章 サポート対象の WINDOWS SERVER バージョン	7
第3章 信頼の仕組み	8
第4章 AD 管理者権限	9
第5章 AD および RHEL で一般的な暗号化タイプに対応	10
第6章 IDM と AD との間の通信に必要なポート	11
第7章 信頼用の DNS およびレルムの設定の構成	15
7.1. 一意のプライマリー DNS ドメイン	15
7.2. IDM WEB UI での DNS 正引きゾーンの設定	16
7.3. CLI での DNS 正引きゾーンの設定	19
7.4. AD での DNS 転送の設定	20
7.5. DNS 設定の確認	21
第8章 ACTIVE DIRECTORY DNS ドメインで IDM クライアントの設定	23
8.1. KERBEROS シングルサインオンを使用しない IDM クライアントの設定	23
8.2. シングルサインオンなしで SSL 証明書の要求	23
8.3. KERBEROS シングルサインオンで IDM クライアントの設定	24
8.4. シングルサインオンで SSL 証明書の要求	24
第9章 信頼の設定	26
9.1. 信頼用の IDM サーバーの準備	26
9.2. コマンドラインで信頼関係の設定	28
9.3. IDM WEB UI で信頼関係の設定	29
9.4. ANSIBLE を使用した信頼関係の設定	32
9.5. KERBEROS 設定の確認	35
9.6. IDM で信頼設定の確認	35
9.7. AD で信頼設定の確認	36
9.8. 信頼エージェントの作成	38
9.9. CLI での POSIX ID 範囲の自動プライベートグループマッピングの有効化	38
9.10. IDM WEBUI での POSIX ID 範囲の自動プライベートグループマッピングの有効化	39
第10章 フォレスト間の信頼設定に関するトラブルシューティング	41
10.1. AD とのフォレスト間の信頼を確立する際の一連のイベント	41
10.2. AD の信頼を確立するための前提条件のチェックリスト	43
10.3. AD の信頼を確立する試みのデバッグログを収集	45
第11章 他のフォレストのサービスへのクライアントアクセスに関するトラブルシューティング	47
11.1. AD フォレストルートドメイン内のホストが IDM サーバーのサービスをリクエストする場合の情報の流れ	47
11.2. AD 子ドメイン内のホストが IDM サーバーのサービスをリクエストする場合の情報の流れ	48
11.3. IDM クライアントが AD サーバーのサービスをリクエストする場合の情報の流れ	49
第12章 コマンドラインを使用した信頼の削除	51
第13章 IDM WEB UI で信頼の削除	52

第14章 ANSIBLE を使用した信頼の削除 54

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、[弊社](#) の CTO、[Chris Wright](#) の [メッセージ](#) を参照してください。

Identity Management では、以下のような用語の置き換えが含まれます。

- **ブラックリストからブロックリスト**
- **ホワイトリストから許可リスト**
- **スレーブからセカンダリー**
- **単語 マスター は、コンテキストに応じて、より正確な言語に置き換えられます。**
 - **マスターからIdM サーバー**
 - **CA 更新マスターからCA 更新サーバー**
 - **CRL マスターからCRL パブリッシャーサーバー**
 - **マルチマスターからマルチサプライヤー**

RED HAT ドキュメントへのフィードバック (英語のみ)

ご意見ご要望をお聞かせください。ドキュメントの改善点はございませんか。

- 特定の部分についての簡単なコメントをお寄せいただく場合は、以下をご確認ください。
 1. ドキュメントの表示が **Multi-page HTML** 形式になっていて、ドキュメントの右上隅に **Feedback** ボタンがあることを確認してください。
 2. マウスカーソルで、コメントを追加する部分を強調表示します。
 3. そのテキストの下に表示される **Add Feedback** ポップアップをクリックします。
 4. 表示される手順に従ってください。
- Bugzilla を介してフィードバックを送信するには、新しいチケットを作成します。
 1. [Bugzilla](#) の Web サイトに移動します。
 2. Component で **Documentation** を選択します。
 3. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも記入してください。
 4. **Submit Bug** をクリックします。

第1章 信頼を確立するための前提条件

本章では、Identity Management (IdM) サーバーと Active Directory (AD) が同じフォレストにある場合に、両サーバー間に信頼を確立する方法を説明します。

前提条件

- [「Planning a cross-forest trust between Identity Management and Active Directory」](#) を読んで
いる。
- ドメインコントローラーとともに、AD がインストールされている。
- IdM サーバーがインストールされ、実行している。
詳細は、[Installing Identity Management](#) を参照してください。
- Kerberos では、通信に最大 5 分の遅延が必要になるため、AD サーバーおよび IdM サーバーの
両方でクロックが同期されている必要があります。
- NetBIOS 名は、Active Directory ドメインの特定に不可欠であるため、各サーバーで一意的
NetBIOS 名を信頼に配置します。
Active Directory または IdM ドメインの NetBIOS 名は通常、対応する DNS ドメインの最初の
部分になります。DNS ドメインが **ad.example.com** の場合、NetBIOS 名は通常 **AD** になりま
す。ただし、必須ではありません。重要なのは、NetBIOS 名がピリオドなしの 1 つの単語であ
るということです。NetBIOS 名は最長 15 文字です。
- 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。

第2章 サポート対象の WINDOWS SERVER バージョン

Identity Management (IdM) は、Windows Server 2008 R2 以前のバージョンを実行している Active Directory ドメインコントローラーとの間で Active Directory への信頼を確立することに対応していません。RHEL IdM との信頼関係を確立する際に、SMB 暗号化が必要です。これは、Windows Server 2012 以降でのみ対応しています。

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

- フォレストの機能レベルの範囲:Windows Server 2012 – Windows Server 2016
- ドメインの機能レベルの範囲:Windows Server 2012 – Windows Server 2016

Identity Management (IdM) は、以下のオペレーティングシステムを実行している Active Directory ドメインコントローラーとの信頼の確立に対応しています。

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

第3章 信頼の仕組み

Identity Management (IdM) と Active Directory (AD) の間の信頼は、レルム間の Kerberos 信頼で確立されます。このソリューションでは、Kerberos 機能を使用して、異なる ID ソース間で信頼関係を確立します。したがって、すべての AD ユーザーは次のことができます。

- ログインして、Linux システムおよびリソースにアクセスする。
- シングルサインオン (SSO) を使用する。

IdM オブジェクトはすべて、信頼の IdM で管理されます。

AD オブジェクトはすべて、信頼の AD で管理されます。

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

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



注記

信頼環境では、IdM は ID ビューを使用して、IdM サーバーの AD ユーザーの POSIX 属性を設定できます。

第4章 AD 管理者権限

AD (Active Directory) と IdM (Identity Management) との間で信頼を構築する場合は、適切な AD 権限のある AD 管理者アカウントを使用する必要があります。

このような AD 管理者は、以下のいずれかのグループのメンバーである必要があります。

- AD フォレスト内のエンタープライズ管理グループ
- AD フォレスト用のフォレストルートドメインのドメイン管理グループ

関連情報

- エンタープライズ管理の詳細は、[「Enterprise Admins」](#) を参照してください。
- ドメイン管理の詳細は、[「Domain Admins」](#) を参照してください。
- AD 信頼の詳細は、[「How Domain and Forest Trusts Work」](#) を参照してください。

第5章 AD および RHEL で一般的な暗号化タイプに対応

デフォルトでは、Identity Management は RC4、AES-128、および AES-256 の Kerberos 暗号化タイプに対応するレルム間の信頼を確立します。

RC4 暗号化は、新しい暗号化タイプ AES-128 および AES-256 よりも安全ではないと見なされるため、デフォルトで非推奨となり、無効にされています。一方、Active Directory (AD) ユーザーの認証情報と AD ドメイン間の信頼は RC4 暗号化をサポートしており、AES 暗号化タイプに対応していない可能性があります。

一般的な暗号化タイプがないと、IdM と AD 子ドメインとの間の通信が機能しないか、一部の AD アカウントが認証できない可能性があります。この状況を修正するには、以下の設定のいずれかを変更します。

Active Directory での AES 暗号化サポートの有効化（推奨オプション）

AD フォレストの AD ドメイン間の信頼を確保して、強力な AES 暗号化の種類に対応するには、Microsoft の記事を参照してください。[AD DS:セキュリティ:Kerberos "Unsupported etype" error when accessing a resource in a trusted domain](#)

RHEL での RC4 サポートの有効化

AD ドメインコントローラーに対する認証が行われるすべての IdM 信頼コントローラー、信頼エージェント、およびクライアント。

- a. **update-crypto-policies** コマンドを使用して、**DEFAULT** 暗号化ポリシーに加え **AD-SUPPORT** 暗号化サブポリシーを有効にします。

```
[root@host ~]# update-crypto-policies --set DEFAULT:AD-SUPPORT
Setting system policy to DEFAULT:AD-SUPPORT
Note: System-wide crypto policies are applied on application start-up.
It is recommended to restart the system for the change of policies
to fully take place.
```

- b. ホストを再起動します。

関連情報

- [Using system-wide cryptographic policies](#) を参照してください。
- 「[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。

第6章 IDM と AD との間の通信に必要なポート

Active Directory (AD) 環境と Identity Management (IdM) 環境間の通信を有効にするには、AD ドメインコントローラーおよび IdM サーバーのファイアウォールで次のポートを開きます。

表6.1 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プ	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
動的 RPC	49152-65535	TCP
AD グローバルカタログ	3268	TCP
LDAP	389	TCP および UDP



注記

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

ポートを開くには、以下の方法を使用できます。

- Firewalld サービス - 特定ポートを有効にするか、そのポートが含まれる以下のサービスを有効にすることができます。
 - freeipa 信頼の設定
 - LDAP を用いた FreeIPA
 - Kerberos
 - DNS

詳細は「[CLI を使用したポートの制御](#)」を参照してください。



注記

RHEL 8.2 以前を使用している場合、**freeipa-trust** Firewalld サービスには **1024-1300** の RPC ポート範囲が含まれていますが、これは正しくありません。RHEL 8.2 以前では、**freeipa-trust** Firewalld サービスを有効にすることに加えて、TCP ポート範囲 **49152-65535** を手動で開く必要があります。

この問題は、RHEL8.3 以降の [バグ 1850418 - freeipa-trust.xml 定義を更新して正しい動的 RPC 範囲を含める](#) で修正されています。

- RHEL Web コンソール。firewalld サービスに基づくファイアウォール設定を含む UI です。

Service	TCP	UDP
Cockpit	9090	
DHCPv6 Client		546
DNS	53	53
FreeIPA trust setup	135, 138-139, 389, 445, 1024-1300, 3268	138-139, 389, 445
FreeIPA with LDAP	80, 443, 88, 464, 389	88, 464, 123
FreeIPA with LDAPS	80, 443, 88, 464, 636	88, 464, 123
Kerberos	88	88

Web コンソールを使用したファイアウォール設定の詳細は、[Web コンソールを使用したファイアウォールでのサービスの有効化](#) を参照してください。



注記

RHEL 8.2 以前を使用している場合、**FreeIPA Trust Setup** サービスには **1024-1300** の RPC ポート範囲が含まれていますが、これは正しくありません。RHEL 8.2 以前では、RHEL Web コンソールで **FreeIPA Trust Setup** サービスを有効にすることに加えて、TCP ポート範囲 **49152-65535** を手動で開く必要があります。

この問題は、RHEL8.3 以降の [バグ 1850418 - freeipa-trust.xml 定義を更新して正しい動的 RPC 範囲を含める](#) で修正されています。

表6.2 信頼の IdM サーバーに必要なポート

サービス	ポート	プロトコル
Kerberos	88、464	TCP および UDP
LDAP	389	TCP

サービス	ポート	プロトコル
DNS	53	TCP および UDP

表6.3 AD 信頼で IdM クライアントに必要なポート

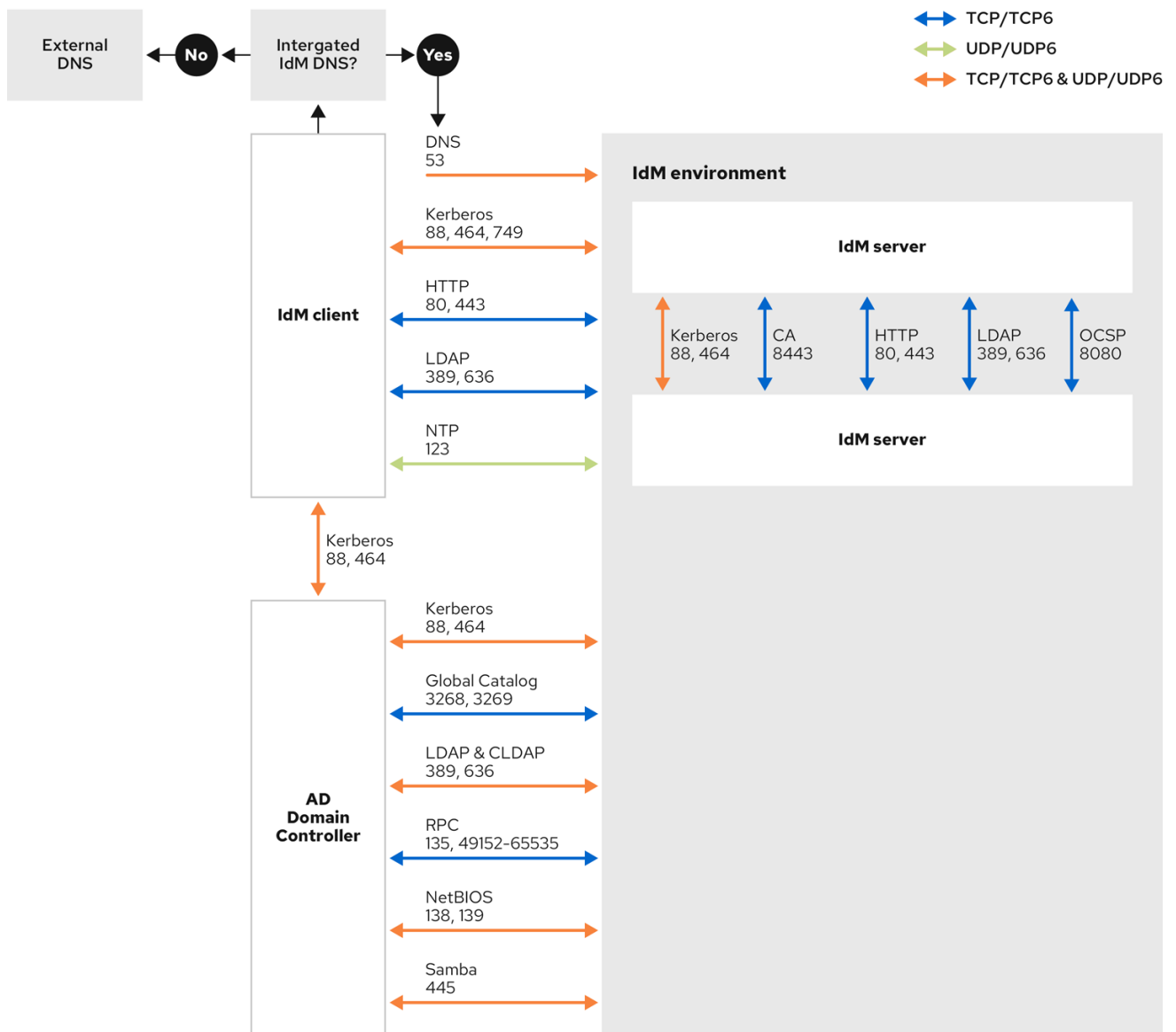
サービス	ポート	プロトコル
Kerberos	88	UDP および TCP



注記

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

次の図は、IdM クライアント、IdM サーバー、および AD ドメインコントローラーが相互に通信するときに使用するポートとプロトコルを示しています。



231_RHEL_0422

関連情報

- Windows Server 2008 以降の Dynamic RPC ポート範囲の詳細は、「[The default dynamic port range for TCP/IP has changed since Windows Vista and in Windows Server 2008](#)」を参照してください。

第7章 信頼用の DNS およびレلمムの設定の構成

信頼で Identity Management (IdM) と Active Directory (AD) を接続する前に、サーバーが相互に認識し、ドメイン名を正しく解決できるようにする必要があります。ここでは、以下の間でドメイン名を使用できるように DNS を設定する方法を説明します。

- 統合 DNS サーバーおよび認証局を使用する 1 台のプライマリー IdM サーバー
- 1 台の AD ドメインコントローラー

DNS 設定には以下が必要です。

- IdM サーバーに DNS ゾーンの設定
- AD での条件付き DNS 転送の設定
- DNS 設定の正確性の確認

7.1. 一意のプライマリー DNS ドメイン

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

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

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

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

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

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

DNS レコードが信頼内の全 DNS ドメインから解決可能である

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

IdM ドメインおよび AD DNS ドメイン

IdM に参加しているシステムは、複数の DNS ドメインに分散できます。Red Hat では、Active Directory が所有するクライアントとは異なる DNS ゾーンに IdM クライアントをデプロイすることを推奨しています。プライマリー IdM DNS ドメインには、AD 信頼に対応するのに適切な SRV レコードが必要です。



注記

IdM と Active Directory との間の信頼がある一部の環境では、Active Directory DNS ドメインの一部であるホストに IdM クライアントをインストールできます。ホストは、これにより、Linux に焦点を合わせた IdM の機能の恩恵を受けることができます。これは推奨される設定ではなく、いくつかの制限があります。詳細は [Active Directory DNS ドメインで IdM クライアントの設定](#) を参照してください。

次のコマンドを実行して、システム設定に必要な固有の SRV レコードの一覧を取得できます。

```
$ ipa dns-update-system-records --dry-run
```

生成される一覧は、たとえば以下ようになります。

IPA DNS records:

```
_kerberos-master._tcp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
_kerberos-master._udp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
_kerberos._tcp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
_kerberos._tcp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
_kerberos.idm.example.com. 86400 IN TXT "IDM.EXAMPLE.COM"
_kpasswd._tcp.idm.example.com. 86400 IN SRV 0 100 464 server.idm.example.com.
_kpasswd._udp.idm.example.com. 86400 IN SRV 0 100 464 server.idm.example.com.
_ldap._tcp.idm.example.com. 86400 IN SRV 0 100 389 server.idm.example.com.
_ipa-ca.idm.example.com. 86400 IN A 192.168.122.2
```

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

7.2. IDM WEB UI での DNS 正引きゾーンの設定

本セクションでは、IdM Web UI を使用して、新しい DNS 正引きゾーンを Identity Management (IdM) サーバーに追加する方法を説明します。

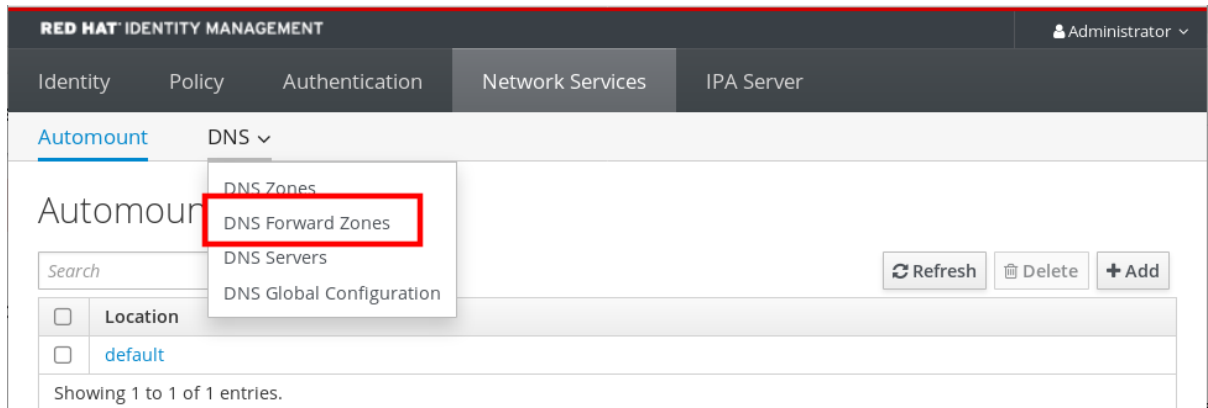
DNS 正引きゾーンを使用すると、特定のゾーンの DNS クエリーを別の DNS サーバーに転送できます。たとえば、Active Directory (AD) ドメインの DNS クエリーを AD DNS サーバーに転送することができます。

前提条件

- 管理者権限のあるユーザーアカウントを使用して IdM Web UI にアクセスする。
- DNS サーバーを正しく設定している。

手順

1. 管理者権限で IdM Web UI にログインします。詳細は「[Web ブラウザーで IdM Web UI へのアクセス](#)」を参照してください。
2. **Network Services** タブをクリックします。
3. **DNS** タブをクリックします。
4. ドロップダウンメニューで、**DNS Forward Zones** 項目をクリックします。



5. **追加** ボタンをクリックします。
6. **Add DNS forward zone** ダイアログボックスにゾーン名を追加します。
7. **Zone forwarders** 項目で、**Add** ボタンをクリックします。
8. **Zone forwarders** フィールドに、新しい正引きゾーンを作成するサーバーの IP アドレスを追加します。
9. **追加** ボタンをクリックします。

The 'Add DNS forward zone' dialog box is shown. It has a title bar with a close button (X). The form contains the following fields and options:

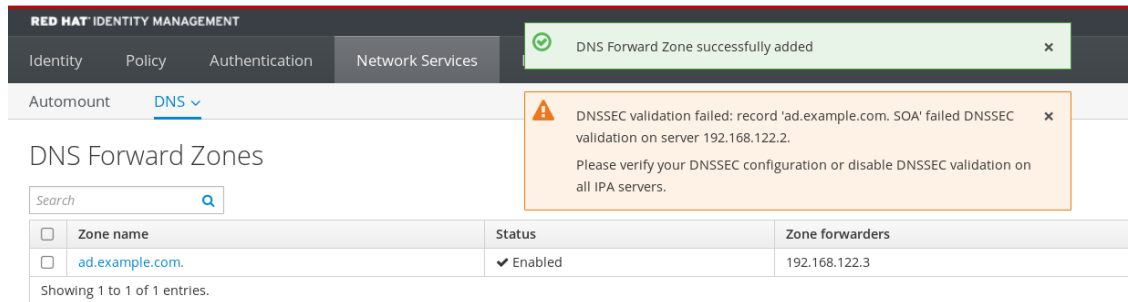
- Zone name ***: Text input field containing 'ad.example.com'.
- Reverse zone**: Radio button (unselected).
- IP network**: Text input field (disabled).
- Zone forwarders ***: Text input field containing '192.168.122.3' with an 'Undo' button to its right. A second empty text input field with an 'Undo' button is below it.
- Add**: Button to add the zone.
- Forward policy**: Radio buttons for 'Forward first' (selected), 'Forward only', and 'Forwarding disabled'.
- Skip overlap check ⓘ**: Unchecked checkbox.
- * Required field**: Text indicating that fields with an asterisk are required.

At the bottom of the dialog, there are four buttons: 'Add', 'Add and Add Another', 'Add and Edit', and 'Cancel'.

正引きゾーンが DNS 設定に追加されており、DNS 正引きゾーン設定で確認できます。Web UI は、ポップアップメッセージで、成功を通知します。**DNS 正引きゾーンが正常に追加されました。**

注記

設定に新しい正引きゾーンを追加した後に、Web UI にDNSSEC 検証の失敗に関する警告が表示される場合があります。



DNSSEC (Domain Name System Security Extensions) は、DNS データをデジタル署名で保護し、攻撃から DNS を保護します。このサービスは、IdM サーバーでデフォルトで有効になっています。リモート DNS サーバーが DNSSEC を使用していないため、警告が表示されます。Red Hat は、リモート DNS サーバーで DNSSEC を有効にすることを推奨します。

リモートサーバーで DNSSEC 検証を有効にできない場合は、IdM サーバーで DNSSEC を無効にすることができます。

1. 編集する適切な設定ファイルを選択します。
 - IdM サーバーが RHEL 8.0 または RHEL 8.1 を使用している場合は、**/etc/named.conf** ファイルを開きます。
 - IdM サーバーが RHEL 8.2 以降を使用している場合は、**/etc/named/ipa-options-ext.conf** ファイルを開きます。

2. 以下の DNSSEC パラメーターを追加します。

```
dnssec-enable no;
dnssec-validation no;
```

3. 設定ファイルを保存して閉じます。
4. DNS サービスを再起動します。

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

検証手順

- **nslookup** コマンドを、リモート DNS サーバーの名前で使用します。

```
$ nslookup ad.example.com
Server:      192.168.122.2
Address:     192.168.122.2#53

No-authoritative answer:
Name:       ad.example.com
Address:    192.168.122.3
```

ドメイン転送が正しく設定されている場合、**nslookup** 要求はリモート DNS サーバーの IP アドレスを表示します。

7.3. CLI での DNS 正引きゾーンの設定

本セクションでは、コマンドラインインターフェース(CLI)を使用して、新しい DNS 正引きゾーンを Identity Management (IdM) サーバーに追加する方法を説明します。

DNS 正引きゾーンを使用すると、特定のゾーンの DNS クエリーを別の DNS サーバーに転送できます。たとえば、Active Directory (AD)ドメインの DNS クエリーを AD DNS サーバーに転送することができます。

前提条件

- 管理者権限のあるユーザーアカウントを使用して CLI にアクセスする。
- DNS サーバーを正しく設定している。

手順

- AD ドメインの DNS 正引きゾーンを作成し、**--forwarder** オプションを使用してリモート DNS サーバーの IP アドレスを指定します。

```
# ipa dnsforwardzone-add ad.example.com --forwarder=192.168.122.3 --forward-policy=first
```

注記

設定に新しい正引きゾーンを追加した後に、`/var/log/messages` システムログに DNSSEC 検証の失敗に関する警告が表示される場合があります。

```
named-pkcs11[2572]: no valid DS resolving 'host.ad.example.com/A/IN':
192.168.100.25#53
```

DNSSEC (Domain Name System Security Extensions) は、DNS データをデジタル署名で保護し、攻撃から DNS を保護します。このサービスは、IdM サーバーでデフォルトで有効になっています。リモート DNS サーバーが DNSSEC を使用していないため、警告が表示されます。Red Hat は、リモート DNS サーバーで DNSSEC を有効にすることを推奨します。

リモートサーバーで DNSSEC 検証を有効にできない場合は、IdM サーバーで DNSSEC を無効にすることができます。

1. 編集する適切な設定ファイルを選択します。
 - IdM サーバーが RHEL 8.0 または RHEL 8.1 を使用している場合は、`/etc/named.conf` ファイルを開きます。
 - IdM サーバーが RHEL 8.2 以降を使用している場合は、`/etc/named/ipa-options-ext.conf` ファイルを開きます。
2. 以下の DNSSEC パラメーターを追加します。

```
dnssec-enable no;
dnssec-validation no;
```

3. 設定ファイルを保存して閉じます。
4. DNS サービスを再起動します。

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

検証手順

- `nslookup` コマンドを、リモート DNS サーバーの名前で使用します。

```
$ nslookup ad.example.com
Server:      192.168.122.2
Address:     192.168.122.2#53

No-authoritative answer:
Name:       ad.example.com
Address:    192.168.122.3
```

ドメイン転送が正しく設定されている場合、`nslookup` 要求はリモート DNS サーバーの IP アドレスを表示します。

7.4. AD での DNS 転送の設定

本セクションでは、Identity Management (IdM) サーバーの Active Directory (AD) に DNS 転送を設定する方法を説明します。

前提条件

- AD を使用する Windows Server がインストールされている。
- 両方のサーバーで DNS ポートが開いている。

手順

1. Windows サーバーにログインします。
2. **Server Manager** を開きます。
3. **DNS Manager** を開きます。
4. **Conditional Forwarders** で、以下を含む新しい条件フォワーダーを追加します。
 - IdM サーバーの IP アドレス
 - **server.idm.example.com** などの完全修飾ドメイン名
5. 設定を保存します。

7.5. DNS 設定の確認

信頼を設定する前に、Identity Management (IdM) サーバーおよび Active Directory (AD) サーバーが自身を解決でき、相互に解決できることを確認します。

前提条件

- `sudo` パーミッションでログインする必要があります。

手順

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

```
[admin@server ~]# dig +short -t SRV _kerberos._udp.idm.example.com.  
0 100 88 server.idm.example.com.
```

```
[admin@server ~]# dig +short -t SRV _ldap._tcp.idm.example.com.  
0 100 389 server.idm.example.com.
```

コマンドは、すべての IdM サーバーを一覧で表示する必要があります。

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

```
[admin@server ~]# dig +short -t TXT _kerberos.idm.example.com.  
"IDM.EXAMPLE.COM"
```

前の手順で想定されるレコードがすべて返されなかった場合は、欠落しているレコードで DNS 設定を更新します。

- IdM 環境で統合 DNS サーバーを使用する場合は、システムレコードを更新するオプションを指定せずに **ipa dns-update-system-records** コマンドを実行します。

```
[admin@server ~]$ ipa dns-update-system-records
```

- IdM 環境で統合 DNS サーバーを使用しない場合は、以下を行います。

1. IdM サーバーで、IdM DNS レコードをファイルにエクスポートします。

```
[admin@server ~]$ ipa dns-update-system-records --dry-run --out  
dns_records_file.nsupdate
```

このコマンドは、関連する IdM DNS レコードで **dns_records_file.nsupdate** という名前のファイルを作成します。

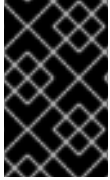
2. **nsupdate** ユーティリティおよび **dns_records_file.nsupdate** ファイルを使用して DNS サーバーに DNS 更新リクエストを送信します。詳細は、RHEL7 ドキュメントの「[nsupdate を使用した外部 DNS レコード更新](#)」を参照してください。または、DNS レコードの追加については、お使いの DNS サーバーのドキュメントを参照してください。
3. IdM が、TCP サービスレコードの Kerberos および LDAP サービスレコードで DNS クエリーを実行するコマンドで、AD のサービスレコードを解決できることを確認します。

```
[admin@server ~]# dig +short -t SRV _kerberos._tcp.dc._msdcs.ad.example.com.  
0 100 88 addc1.ad.example.com.
```

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

第8章 ACTIVE DIRECTORY DNS ドメインで IDM クライアントの設定

Active Directory が制御する DNS ドメインにクライアントシステムがあり、そのクライアントが RHEL 機能の恩恵を受けるために IdM Server に参加できるようにする必要がある場合は、Active Directory DNS ドメインのホスト名を使用してクライアントにアクセスするようにユーザーを設定できます。



重要

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

IdM クライアントの設定は、Kerberos でシングルサインオンを必要とするかどうかによって異なります。

8.1. KERBEROS シングルサインオンを使用しない IDM クライアントの設定

パスワード認証は、IdM クライアントが Active Directory DNS ドメインに存在する場合に、IdM クライアントのリソースにアクセスするためにユーザーが利用できる唯一の認証方法です。この手順では、Kerberos シングルサインオンを使用せずにクライアントを設定する方法を説明します。

手順

1. `--domain=IPA_DNS_Domain` を指定して IdM クライアントをインストールし、SSSD (System Security Services Daemon) が IdM サーバーと通信できるようにします。

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

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

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

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

3. 両方の行を、Active Directory DNS ゾーンの Linux クライアントの完全修飾ドメイン名 (FQDN) を IdM レルムにマッピングするエントリーに置き換えます。

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

デフォルトのマッピングを置き換えても、Kerberos が Active Directory ドメインの要求を IdM Kerberos Distribution Center (KDC) に送信しないようにします。Kerberos は、SRV DNS レコードを介して自動検出を使用して KDC を見つけます。

8.2. シングルサインオンなしで SSL 証明書の要求

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

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

前提条件

- [Kerberos シングルサインオンを使用しない IdM クライアントの設定](#) での手順に従って、IdM クライアントをインストールし、設定します。

手順

- **certmonger** を使用して、FQDN を使用して証明書をリクエストします。

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

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

8.3. KERBEROS シングルサインオンで IDM クライアントの設定

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

Kerberos ベースのアプリケーションサーバーの場合、MIT Kerberos は、アプリケーションのキータブで利用可能なホストベースのプリンシパルの受け入れを可能にする方法をサポートします。

手順

- IdM クライアントでは、**/etc/krb5.conf** 設定ファイルの **[libdefaults]** セクションにある次のオプションを設定して、Kerberos サーバーのターゲットに使用される Kerberos プリンシパルに関する厳格なチェックを無効にします。

```
ignore_acceptor_hostname = true
```

8.4. シングルサインオンで SSL 証明書の要求

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

この手順では、IdM で **ipa-client.example.com** 用のホストオブジェクトを作成し、実際の IdM マシンのホストオブジェクトがこのホストを管理できるようにする方法を説明します。

前提条件

- [Kerberos シングルサインオンで IdM クライアントの設定](#) で説明されているように、Kerberos サーバーのターゲットに使用される Kerberos プリンシパルに関する厳格なチェックを無効にしています。

手順

1. IdM サーバーに新しいホストオブジェクトを作成します。

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

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

2. IdM サーバーで、IdM DNS ホスト名が、IdM データベースの Active Directory 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
```

3. これで、Active Directory DNS ドメイン内のホスト名に **dNSName** 拡張レコードを使用して、IdM クライアントの SSL 証明書を要求できるようになります。

```
[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
```

第9章 信頼の設定

本セクションでは、コマンドラインを使用して、IdM に Identity Management (IdM)/Active Directory (AD) 信頼を設定する方法を説明します。

前提条件

- DNS が正しく設定されている。IdM サーバーおよび AD サーバーはどちらも、相手の名前を解決できる。詳細は「[信頼用の DNS およびレールム設定の構成](#)」を参照してください。
- 対応しているバージョンの AD および IdM がデプロイされている。詳細は「[サポート対象の Windows Server バージョン](#)」を参照してください。
- Kerberos チケットを取得している。詳細は、[Using kinit to log in to IdM manually](#) を参照してください。

9.1. 信頼用の IDM サーバーの準備

AD との信頼を確立する前に、IdM サーバーで **ipa-adtrust-install** ユーティリティを使用して IdM ドメインを準備する必要があります。



注記

ipa-adtrust-install コマンドを自動的に実行するシステムは、AD 信頼コントローラーになります。ただし、**ipa-adtrust-install** は、IdM サーバーで1回のみ実行する必要があります。

前提条件

- IdM サーバーがインストールされている。
- パッケージをインストールし、IdM サービスを再起動するには、root 権限が必要です。

手順

1. 必要なパッケージをインストールします。

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

2. IdM 管理ユーザーとして認証します。

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

3. **ipa-adtrust-install** ユーティリティを実行します。

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

統合 DNS サーバーとともに IdM がインストールされていると、DNS サービスレコードが自動的に作成されます。

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

4. スクリプトにより、`/etc/samba/smb.conf` がすでに存在し、書き換えられることが求められます。

```
WARNING: The smb.conf already exists. Running ipa-adtrust-install will break your existing Samba configuration.
```

```
Do you wish to continue? [no]: yes
```

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

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

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

6. プロンプトが表示されたら、IdM ドメインの NetBIOS 名を入力するか、**Enter** を押して提案された名前を使用します。

```
Trust is configured but no NetBIOS domain name found, setting it now.
Enter the NetBIOS name for the IPA domain.
Only up to 15 uppercase ASCII letters, digits and dashes are allowed.
Example: EXAMPLE.
```

```
NetBIOS domain name [IDM]:
```

7. SID 生成タスクを実行して、既存ユーザーに SID を作成するように求められます。

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

これはリソースを集中的に使用するタスクであるため、ユーザー数が多い場合は別のタイミングで実行できます。

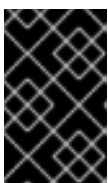
8. (必要に応じて) デフォルトでは、Windows Server 2008 以降では、動的 RPC ポートの範囲は **49152-65535** として定義されます。ご使用の環境に異なる動的 RPC ポート範囲を定義する必要がある場合は、Samba が異なるポートを使用するように設定し、ファイアウォール設定でそのポートを開くように設定します。以下の例では、ポート範囲を **55000-65000** に設定します。

```
[root@ipaserver ~]# net conf setparm global 'rpc server dynamic port range' 55000-65000
```

```
[root@ipaserver ~]# firewall-cmd --add-port=55000-65000/tcp
```

```
[root@ipaserver ~]# firewall-cmd --runtime-to-permanent
```

9. 「[信頼の DNS 設定の確認](#)」に従って、DNS が適切に設定されていることを確認します。



重要

Red Hat では、IdM または AD が統合 DNS サーバーを使用しない場合に、**ipa-adtrust-install** を実行してから [信頼に対する DNS 設定の確認](#) に従って DNS 設定を検証することが強く推奨されます。

10. **ipa** サービスを再起動します。

■

```
[root@ipaserver ~]# ipactl restart
```

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

```
[root@ipaserver ~]# smbclient -L server.idm.example.com -U user_name --use-kerberos=required
lp_load_ex: changing to config backend registry
  Sharename      Type      Comment
  -----
  IPC$           IPC      IPC Service (Samba 4.15.2)
  ...
```

9.2. コマンドラインで信頼関係の設定

本セクションでは、コマンドラインを使用して信頼関係を設定する方法を説明します。

Identity Management (IdM) サーバーには、3 種類の信頼関係を設定できます。

- **一方向の信頼** – デフォルトのオプション。一方向の信頼により、Active Directory (AD) ユーザーおよびグループは IdM のリソースにアクセスできますが、その逆はできません。IdM ドメインは AD フォレストを信頼しますが、AD フォレストは IdM ドメインを信頼しません。

- **双方向の信頼** – 双方向の信頼により、AD ユーザーおよびグループが IdM のリソースにアクセスできるようになります。

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

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

- 双方向の信頼を作成するには、コマンドに **--two-way=true** オプションを追加します。

- **外部信頼** – 異なるフォレストの IdM と AD ドメインとの間の信頼関係です。フォレストの信頼では常に IdM と Active Directory フォレストのルートドメインとの間で信頼関係を確立する必要がありますが、IdM からフォレスト内の任意のドメインへの外部の信頼関係も確立できます。管理上または組織上の理由で、フォレストの root ドメイン間でフォレストの信頼を確立できない場合に限り、これが推奨されます。

- 外部の信頼を作成するには、コマンドに **--external=true** オプションを追加します。

本セクションでは、以下の手順に従って、一方向の信頼関係を作成する方法を説明します。

前提条件

- Windows 管理者のユーザー名およびパスワード
- [信頼用の IdM サーバーの準備ができています。](#)

手順

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

- SSSD が SID に基づいて AD ユーザーの UID および GID を自動的に生成できるようにするには、**Active Directory domain ID** 範囲タイプとの信頼関係を作成します。これが最も一般的な設定です。

```
[root@server ~]# ipa trust-add --type=ad ad.example.com --admin
<ad_admin_username> --password --range-type=ipa-ad-trust
```

- Active Directory でユーザーに POSIX 属性を設定し（`uidNumber`、`gidNumber`など）、SSSD でこの情報を処理する場合は、**Active Directory domain with POSIX attributes ID** 範囲タイプとの信頼関係を作成します。

```
[root@server ~]# ipa trust-add --type=ad ad.example.com --admin
<ad_admin_username> --password --range-type=ipa-ad-trust-posix
```



警告

信頼の作成時に ID 範囲タイプを指定しないと、IdM はフォレストルートドメインの AD ドメインコントローラーから詳細を要求することで、適切な範囲タイプを自動的に選択しようとします。IdM が POSIX 属性を検出しない場合、信頼インストールスクリプトは **Active Directory domain ID** 範囲を選択します。

IdM がフォレストルートドメインの POSIX 属性を検出すると、信頼インストールスクリプトは、**Active Directory domain with POSIX attributes ID** 範囲を選択し、UID および GID が AD に正しく定義されていることを前提とします。POSIX 属性が AD で正しく設定されていない場合は、AD ユーザーを解決できません。

たとえば、IdM システムへのアクセスを必要とするユーザーおよびグループがフォレストルートドメインの一部ではなく、フォレストドメインの子ドメインにある場合は、インストールスクリプトで、子 AD ドメインで定義された POSIX 属性が検出されない場合があります。この場合、Red Hat は、信頼の確立時に POSIX ID 範囲タイプを明示的に選択することを推奨します。

9.3. IDM WEB UI で信頼関係の設定

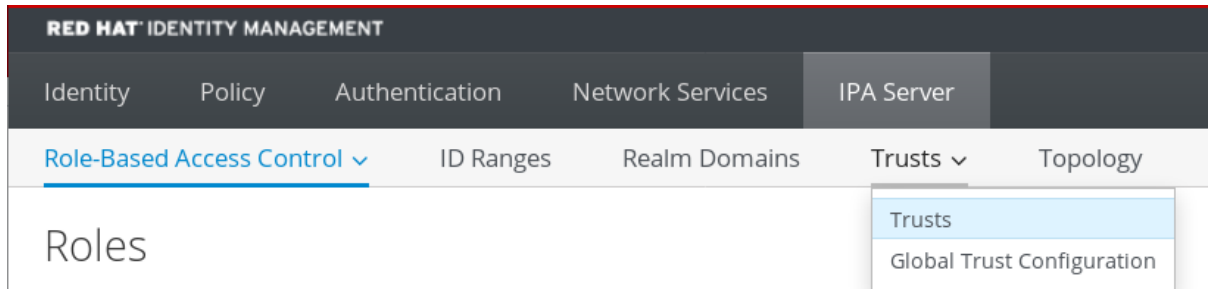
本セクションでは、IdM Web UI を使用して、IdM で Identity Management (IdM) /Active Directory (AD) の信頼関係を設定する方法を説明します。

前提条件

- DNS が正しく設定されている。IdM サーバーおよび AD サーバーはどちらも、相手の名前を解決できる。
- 対応しているバージョンの AD および IdM がデプロイされている。
- Kerberos チケットを取得している。
- Web UI で信頼を作成する前に、以下に従って信頼用に IdM サーバーを準備している。[信頼用の IdM サーバーの準備](#)。
- IdM 管理者としてログインしている。

手順

1. 管理者権限で IdM Web UI にログインします。詳細は「[Web ブラウザーで IdM Web UI へのアクセス](#)」を参照してください。
2. IdM Web UI で、**IPA Server** タブをクリックします。
3. **IPA Server** タブで、**Trusts** タブをクリックします。
4. ドロップダウンメニューで、**Trusts** オプションを選択します。



5. **Add** ボタンをクリックします。
6. **Add Trust** ダイアログボックスで、Active Directory ドメインの名前を入力します。
7. **Account** フィールドおよび **Password** フィールドに、Active Directory 管理者の管理者認証情報を追加します。

8. (オプション) AD ユーザーおよびグループが IdM のリソースにアクセスできるようにする場合は、**Two-way trust** を選択します。ただし、IdM の双方向の信頼では、AD の一方向の信頼ソリューションと比較して、ユーザーに追加の権限が付与されません。デフォルトのフォレスト間信頼の SID フィルタリング設定により、両方のソリューションの安全性は同じであると見なされます。
9. (オプション) AD フォレストのルートドメインではない AD ドメインで信頼を設定する場合は、**External trust** を選択します。フォレストの信頼では常に IdM と Active Directory フォレストのルートドメインとの間で信頼関係を確立する必要がありますが、IdM から AD フォレスト内の任意のドメインへの外部の信頼関係も確立できます。

10. (オプション) デフォルトでは、信頼インストールスクリプトは適切な ID 範囲タイプの検出を試みます。以下のオプションのいずれかを選択して、ID 範囲タイプを明示的に設定することもできます。
- SSSD が SID に基づいて AD ユーザーの UID および GID を自動的に生成するには、**Active Directory domain** ID 範囲タイプを選択します。これが最も一般的な設定です。
 - Active Directory でユーザーに POSIX 属性を設定し (**uidNumber**、**gidNumber**など)、SSSD がこの情報を処理する必要がある場合は、**Active Directory domain with POSIX attributes** ID 範囲タイプを選択します。

<p>Range type</p> <p><input checked="" type="radio"/> Detect</p> <p><input type="radio"/> Active Directory domain</p> <p><input type="radio"/> Active Directory domain with POSIX attributes</p>
--



警告

Range type 設定をデフォルトの **Detect** オプションに残すと、IdM はフォレストルートドメインの AD ドメインコントローラーから詳細を要求することで、適切な範囲タイプを自動的に選択しようとします。IdM が POSIX 属性を検出しない場合、信頼インストールスクリプトは **Active Directory domain** ID 範囲を選択します。

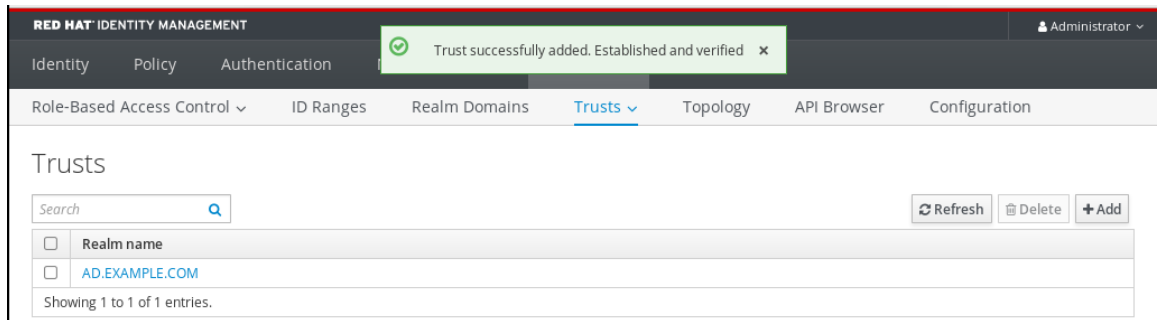
IdM がフォレストルートドメインの POSIX 属性を検出すると、信頼インストールスクリプトは、**Active Directory domain with POSIX attributes** ID 範囲を選択し、UID および GID が AD に正しく定義されていることを前提とします。POSIX 属性が AD で正しく設定されていない場合は、AD ユーザーを解決できません。

たとえば、IdM システムへのアクセスを必要とするユーザーおよびグループがフォレストルートドメインの一部ではなく、フォレストドメインの子ドメインにある場合は、インストールスクリプトで、子 AD ドメインで定義された POSIX 属性が検出されない場合があります。この場合、Red Hat は、信頼の確立時に POSIX ID 範囲タイプを明示的に選択することを推奨します。

11. **Add** をクリックします。

検証手順

- 信頼が IdM サーバーに正常に追加されると、IdM Web UI で緑色のポップアップ画面が表示されます。これは、以下を示しています。
 - ドメイン名が存在する。
 - Windows Server のユーザー名およびパスワードが正しく追加されている。



これで、信頼接続と Kerberos 認証のテストを続行します。

9.4. ANSIBLE を使用した信頼関係の設定

本セクションでは、Ansible Playbook を使用して、Identity Management(IdM)と Active Directory(AD) との間で一方方向の信頼関係を設定する方法を説明します。3 種類の信頼関係を設定できます。

- **一方方向の信頼** – デフォルトのオプション。一方方向の信頼により、Active Directory (AD) ユーザーおよびグループは IdM のリソースにアクセスできますが、その逆はできません。IdM ドメインは AD フォレストを信頼しますが、AD フォレストは IdM ドメインを信頼しません。
- **双方方向の信頼** – 双方方向の信頼により、AD ユーザーおよびグループが IdM のリソースにアクセスできるようになります。
信頼境界を使用して Kerberos プロトコルに **S4U2Self** および **S4U2Proxy** の Microsoft 拡張を必要とする、Microsoft SQL Server などのソリューションに、双方方向の信頼を設定する必要があります。RHEL IdM ホスト上にあるアプリケーションは、AD ユーザーに関する **S4U2Self** または **S4U2Proxy** の情報を Active Directory ドメインコントローラーから要求する場合があります、双方方向の信頼でこの機能が提供されます。

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

- 双方方向の信頼を作成するには、以下の変数を Playbook タスクに追加します：**two_way: true**
- **外部信頼** – 異なるフォレストの IdM と AD ドメインとの間の信頼関係です。フォレストの信頼では常に IdM と Active Directory フォレストのルートドメインとの間で信頼関係を確立する必要がありますが、IdM からフォレスト内の任意のドメインへの外部の信頼関係も確立できます。管理上または組織上の理由で、フォレストの root ドメイン間でフォレストの信頼を確立できない場合に限り、これが推奨されます。
 - 外部信頼を作成するには、以下の変数を **external: true** の Playbook タスクに追加します。

前提条件

- Windows 管理者のユーザー名およびパスワード
- IdM 管理者パスワード。
- [信頼用の IdM サーバーの準備ができています。](#)
- 以下の要件を満たす Ansible コントロールノードを設定している。
 - Ansible バージョン 2.8 以降を使用している。

- `ansible-freeipa` パッケージがインストールされている。
- `~/MyPlaybooks/` ディレクトリーに、信頼を設定する IdM サーバーの完全修飾ドメイン名 (FQDN) で `Ansible インベントリーファイル` を作成している。

手順

1. `~/MyPlaybooks/` ディレクトリーに移動します。

```
$ cd ~/MyPlaybooks/
```

2. ユースケースに基づいて、以下のいずれかのシナリオを選択します。

- SSSD が SID に基づいて AD ユーザーおよびグループの UID および GID を自動的に生成する ID マッピング信頼関係を作成するには、以下の内容で `add-trust.yml` Playbook を作成します。

```
---
- name: Playbook to create a trust
  hosts: ipaserver
  become: true

  tasks:
  - name: ensure the trust is present
    ipatrust:
      ipaadmin_password: SomeADMINpassword
      realm: ad.example.com
      admin: Administrator
      password: secret_password
      range_type: ipa-ad-trust
      state: present
```

この例では以下が設定されています。

- **realm** は、AD レルム名文字列を定義します。
- **admin** は AD ドメイン管理者文字列を定義します。
- **Password** は、AD ドメイン管理者のパスワード文字列を定義します。
- SSSD が AD に保存されている POSIX 属性 (`uidNumber` や `gidNumber` など) を処理する POSIX 信頼関係を作成するには、以下の内容で `add-trust.yml` Playbook を作成します。

```
---
- name: Playbook to create a trust
  hosts: ipaserver
  become: true

  tasks:
  - name: ensure the trust is present
    ipatrust:
      ipaadmin_password: SomeADMINpassword
      realm: ad.example.com
      admin: Administrator
```

```
password: secret_password
range_type: ipa-ad-trust-posix
state: present
```

- フォレストルートドメインの AD ドメインコントローラーからの詳細を要求して、IdM が適切な範囲タイプ **ipa-ad-trust** または **ipa-ad-trust-posix** を選択しようとする信頼関係を作成するには、以下の内容を含む **add-trust.yml** Playbook を作成します。

```
---
- name: Playbook to create a trust
  hosts: ipaserver
  become: true

  tasks:
  - name: ensure the trust is present
    ipatrust:
      ipaadmin_password: SomeADMINpassword
      realm: ad.example.com
      admin: Administrator
      password: secret_password
      state: present
```



警告

信頼の作成時に ID 範囲タイプを指定しない場合で、IdM が AD フォレストルートドメインの POSIX 属性を検出しない場合は、信頼インストールスクリプトで **Active Directory ドメイン ID 範囲** が選択されます。

IdM がフォレストルートドメインの POSIX 属性を検出すると、信頼インストールスクリプトは、**Active Directory domain with POSIX attributes** ID 範囲を選択し、UID および GID が AD に正しく定義されていることを前提とします。

ただし、AD で POSIX 属性が正しく設定されていない場合は、AD ユーザーを解決できません。たとえば、IdM システムへのアクセスを必要とするユーザーおよびグループがフォレストルートドメインの一部ではなく、フォレストドメインの子ドメインにある場合は、インストールスクリプトで、子 AD ドメインで定義された POSIX 属性が検出されない場合があります。この場合、Red Hat は、信頼の確立時に POSIX ID 範囲タイプを明示的に選択することを推奨します。

3. ファイルを保存します。
4. Playbook ファイルとインベントリーファイルを指定して Ansible Playbook を実行します。

```
$ ansible-playbook -v -i inventory add-trust.yml
```

関連情報

- `/usr/share/doc/ansible-freeipa/README-trust.md`

- /usr/share/doc/ansible-freeipa/playbooks/trust

9.5. KERBEROS 設定の確認

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

手順

1. Active Directory (AD) ユーザーのチケットを要求します。

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

2. IdM ドメイン内のサービスのサービスチケットを要求します。

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

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

```
[root@server ~]# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_hRtox00
Default principal: user@AD.EXAMPLE.COM
```

```
Valid starting    Expires          Service principal
03.05.2016 18:31:06 04.05.2016 04:31:01 host/server.idm.example.com@IDM.EXAMPLE.COM
renew until 04.05.2016 18:31:00
03.05.2016 18:31:06 04.05.2016 04:31:01 krbtgt/IDM.EXAMPLE.COM@AD.EXAMPLE.COM
renew until 04.05.2016 18:31:00
03.05.2016 18:31:01 04.05.2016 04:31:01 krbtgt/AD.EXAMPLE.COM@AD.EXAMPLE.COM
renew until 04.05.2016 18:31:00
```

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

9.6. IDM で信頼設定の確認

信頼を設定する前に、Identity Management (IdM) サーバーおよび Active Directory (AD) サーバーが自身を解決でき、相互に解決できることを確認します。

前提条件

- 管理者権限でログインしている。

手順

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

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

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

以下のコマンドは、**ipa-adtrust-install** を実行した IdM サーバーを一覧表示します。**ipa-adtrust-install** が IdM サーバーで実行していない場合、通常は最初の信頼関係を確立する前に出力が空になります。

2. TCP サービスレコード上の Kerberos と LDAP で DNS クエリーを実行して、IdM が AD のサービスレコードを解決できることを確認します。

```
[root@server ~]# dig +short -t SRV _kerberos._tcp.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.
```

9.7. AD で信頼設定の確認

信頼の設定後に、以下を確認します。

- Identity Management (IdM) がホストするサービスが、Active Directory (AD) サーバーから解決できる。
- AD サービスは、AD サーバーで解決できる。

前提条件

- 管理者権限でログインしている。

手順

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

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

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

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


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

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

      "IDM.EXAMPLE.COM"
```

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

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

Active Directory は、その他の AD ドメインコントローラーや IdM 信頼コントローラーなど、AD 固有のプロトコル要求に回答できるドメインコントローラーの検出のみを想定します。**ipa-adtrust-install** ツールを使用して、IdM サーバーを信頼コントローラーに昇格し、どのサーバーが信頼コントローラーであるかを確認するには、**ipa server-role-find --role 'AD trust controller'** コマンドを使用します。

- AD サービスが AD サーバーで解決可能であることを検証します。

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

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

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

9.8. 信頼エージェントの作成

信頼エージェントは、AD ドメインコントローラーに対して ID ルックアップを実行できる IdM サーバーです。

たとえば、Active Directory と信頼できる IdM サーバーのレプリカを作成する場合は、そのレプリカを信頼エージェントとして設定できます。レプリカには、AD 信頼エージェントロールが自動的にインストールされていません。

前提条件

- IdM は、Active Directory 信頼でインストールされます。
- **sssd-tools** パッケージがインストールされている。

手順

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

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

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

2. 信頼エージェントで IdM サービスを再起動します。

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

3. 信頼エージェントの SSSD キャッシュからすべてのエントリを削除します。

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

4. レプリカに AD 信頼エージェントロールがインストールされていることを確認します。

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

関連情報

- **--add-agents** オプションの詳細は、man ページの **ipa-adtrust-install(1)** を参照してください。
- 信頼エージェントの詳細は、『Planning Identity Management』の「[Trust controllers and trust agents](#)」を参照してください。

9.9. CLI での POSIX ID 範囲の自動プライベートグループマッピングの有効化

デフォルトでは、SSSD は、AD に保存されている POSIX データに依存する POSIX 信頼を確立している場合は、Active Directory(AD)ユーザーのプライベートグループをマッピングしません。AD ユーザーにプライマリーグループが設定されていない場合、IdM はこれを解決できません。

この手順では、コマンドラインで **auto_private_groups** SSSD パラメーターに **hybrid** オプションを設定して、ID 範囲の自動プライベートグループマッピングを有効にする方法を説明します。これにより、IdM は、AD にプライマリーグループが設定されていない AD ユーザーを解決できます。

前提条件

- IdM 環境と AD 環境との間で、POSIX フォレスト間の信頼が正常に確立されました。

手順

1. すべての ID 範囲を表示し、変更する AD ID 範囲を書き留めます。

```
[root@server ~]# ipa idrange-find
-----
2 ranges matched
-----
Range name: IDM.EXAMPLE.COM_id_range
First Posix ID of the range: 882200000
Number of IDs in the range: 200000
Range type: local domain range

Range name: AD.EXAMPLE.COM_id_range
First Posix ID of the range: 1337000000
Number of IDs in the range: 200000
Domain SID of the trusted domain: S-1-5-21-4123312420-990666102-3578675309
Range type: Active Directory trust range with POSIX attributes
-----
Number of entries returned 2
-----
```

2. **ipa idrange-mod** コマンドを使用して、AD ID 範囲の自動プライベートグループの動作を調整します。

```
[root@server ~]# ipa idrange-mod --auto-private-groups=hybrid
AD.EXAMPLE.COM_id_range
```

3. SSSD キャッシュをリセットして、新しい設定を有効にします。

```
[root@server ~]# sss_cache -E
```

関連情報

- [Options for automatically mapping private groups for AD users](#)

9.10. IDM WEBUI での POSIX ID 範囲の自動プライベートグループマッピングの有効化

デフォルトでは、SSSD は、AD に保存されている POSIX データに依存する POSIX 信頼を確立している場合は、Active Directory(AD)ユーザーのプライベートグループをマッピングしません。AD ユーザーにプライマリーグループが設定されていない場合、IdM はこれを解決できません。

この手順では、Identity Management(IdM)WebUI の **auto_private_groups** SSSD パラメーターの **hybrid** オプションを設定して、ID 範囲の自動プライベートグループマッピングを有効にする方法を説

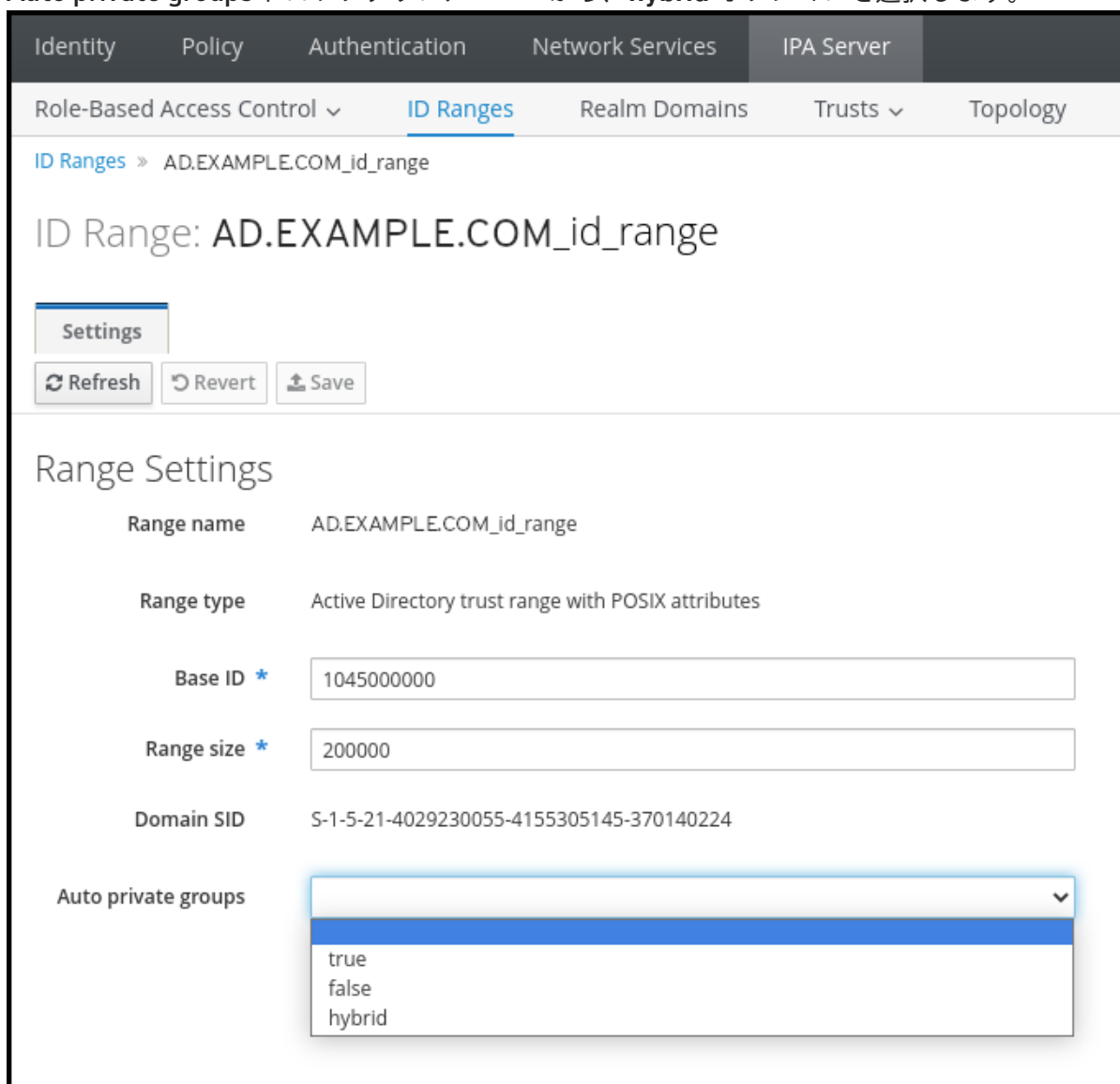
明します。これにより、IdM は、AD にプライマリーグループが設定されていない AD ユーザーを解決できます。

前提条件

- IdM 環境と AD 環境との間で、POSIX フォレスト間の信頼が正常に確立されました。

手順

1. ユーザー名とパスワードを使用して IdM Web UI にログインします。
2. IPA Server → ID Ranges タブを開きます。
3. **AD.EXAMPLE.COM_id_range** など、変更する ID 範囲を選択します。
4. **Auto private groups** ドロップダウンメニューから、**hybrid** オプションを選択します。



5. **Save** ボタンをクリックして変更を保存します。

関連情報

- [Options for automatically mapping private groups for AD users](#)

第10章 フォレスト間の信頼設定に関するトラブルシューティング

この章では、Identity Management (IdM) 環境と Active Directory (AD) フォレストの間で、フォレスト間で信頼を設定するプロセスのトラブルシューティングについて説明します。

10.1. AD とのフォレスト間の信頼を確立する際の一連のイベント

ipa trust-add コマンドを使用して Active Directory(AD)ドメインコントローラー(DC)ドメインコントローラーとのフォレスト間の信頼を確立すると、コマンドは、コマンドを実行するユーザーの代わりに動作し、IdM サーバーで次のアクションを実行します。フォレスト間の信頼を確立する際に問題が発生した場合は、このリストを使用して、問題を絞り込み、トラブルシューティングすることができます。

パート1:コマンドによる設定と入力の確認

1. IdM サーバーに **Trust Controller** のロールがあることを確認します。
2. **ipa trust-add** コマンドに渡されたオプションを確認します。
3. 信頼されたフォレストルートドメインに関連付けられている ID 範囲を確認します。ID 範囲の種類とプロパティを **ipatrust-add** コマンドのオプションとして指定しなかった場合、それらは Active Directory から検出されます。

パート2:コマンドによる Active Directory ドメインへの信頼確立の試行

4. 信頼方向ごとに個別の信頼オブジェクトを作成します。各オブジェクトは両サイド (IdM と AD) で作成されます。一方向の信頼を確立する場合、各サイドに1つのオブジェクトのみが作成されます。
5. IdM サーバーは Samba スイートを使用して Active Directory のドメインコントローラー機能を処理し、ターゲット AD PDC 上に信頼オブジェクトを作成します。
 - a. IdM サーバーは、ターゲット DC の **IPC\$** 共有へのセキュアな接続を確立します。RHEL 8.4 以降、接続には、セッションに使用される AES ベースの暗号化で接続が十分に保護されていることを保証するために、少なくとも WindowsServer2012 以降での SMB3 プロトコルが必要です。
 - b. IdM サーバーは、**LSA QueryTrustedDomainInfoByName** 呼び出しを使用して、信頼されたドメインオブジェクト (TDO) の存在をクエリーします。
 - c. TDO がすでに存在する場合は、**LSA DeleteTrustedDomain** 呼び出しを使用してその TDO を削除します。



注記

信頼の確立に使用される AD ユーザーアカウントに、**Incoming Forest Trust Builders** グループのメンバーなど、フォレストルートに対する完全な **Enterprise Admin (EA)** または **Domain Admin (DA)** 特権がない場合、この呼び出しは失敗します。古い TDO が自動的に削除されない場合、AD 管理者は手動で AD から削除する必要があります。

- d. IdM サーバーは、**LSA CreateTrustedDomainEx2** 呼び出しを使用して新しい TDO を作成します。TDO クレデンシャルは、Samba が提供する 128 文字のランダムなパスワードジェネレーターを使用してランダムに生成されます。

- e. 次に、新しい TDO を **LSA SetInformationTrustedDomain** 呼び出しで変更し、信頼でサポートされている暗号化タイプが適切に設定されていることを確認します。
 - i. Active Directory の設計に基づき、RC4 キーが使用されていない場合でも、**RC4_HMAC_MD5** 暗号化タイプが有効になっている。
 - ii. **AES128_CTS_HMAC_SHA1_96** および **AES256_CTS_HMAC_SHA1_96** 暗号化タイプが有効になっている。



注記

デフォルトでは、RHEL 9 は AD が必要とするアルゴリズムである SHA-1 暗号化を許可していません。**AD-SUPPORT** システム全体の暗号化サブポリシーを有効にして、AD ドメインコントローラーとの通信のために RHEL 9 サーバーで SHA-1 暗号化を許可していることを確認してください。<リンク TBA>を参照してください。

- 6. フォレストの信頼の場合、**LSA SetInformationTrustedDomain** 呼び出しでフォレスト内のドメインに推移的に到達できることを確認します。
- 7. **LSA RSetForestTrustInformation** 呼び出しを使用して、他のフォレスト (AD と通信する場合は IdM、IdM と通信する場合は AD) に関する信頼トポロジー情報を追加します。



注記

この手順により、次の 3 つの理由のいずれかで競合が発生する可能性があります。

1. **LSA_SID_DISABLED_CONFLICT** エラーとして報告される SID namespace の競合。この競合は解決できません。
2. **LSA_NB_DISABLED_CONFLICT** エラーとして報告される NetBIOS namespace の競合。この競合は解決できません。
3. **LSA_TLN_DISABLED_CONFLICT** エラーとして報告される、DNS namespace とトップレベル名 (TLN) の競合。別のフォレストが原因で TLN の競合が発生した場合、IdM サーバーは自動的に解決できます。

TLN の競合を解決するために、IdM サーバーは次の手順を実行します。

1. 競合するフォレストのフォレスト信頼情報を取得します。
2. IdM DNS namespace 間の除外エントリーを AD フォレストに追加します。
3. 競合するフォレストのフォレスト信頼情報を設定します。
4. 元のフォレストへの信頼確立を再試行します。

IdM サーバーは、フォレストの信頼を変更できる AD 管理者の権限で **ipa trust-add** コマンドを認証した場合にのみ、これらの競合を解決できます。これらの権限にアクセスできない場合、元のフォレストの管理者は、Windows UI の **Active Directory Domains and Trusts** セクションで上記の手順を手動で実行する必要があります。

- 8. 存在しない場合は、信頼されたドメインの ID 範囲を作成します。

9. フォレストの信頼については、フォレストのトポロジーの詳細について、フォレストのルートから Active Directory ドメインコントローラーにクエリーします。IdM サーバーはこの情報を使用して、信頼されたフォレストから追加のドメインの追加 ID 範囲を作成します。

関連情報

- [信頼コントローラーおよび信頼エージェント](#)
- [Overview Documents](#) (Microsoft)
- [Technical Documents](#) (Microsoft)
- [Privileged Accounts and Groups in Active Directory](#) (Microsoft)

10.2. AD の信頼を確立するための前提条件のチェックリスト

次のチェックリストを使用して、AD ドメインとの信頼を作成するための前提条件を確認できます。

表10.1 テーブル

コンポーネント	設定	詳細
製品バージョン	Active Directory ドメインは、サポートされているバージョンの Windows Server を使用していません。	サポート対象の Windows Server バージョン
AD 管理者権限	Active Directory 管理アカウントは、次のいずれかのグループのメンバーです。 <ul style="list-style-type: none"> ● AD フォレストの Enterprise Admin (EA) グループ ● AD フォレスト用のフォレストルートドメインの Domain Admins (DA) グループ 	
ネットワーキング	IPv6 サポートは、すべての IdM サーバーの Linux カーネルで有効になっています。	IdM における IPv6 要件
日付と時刻	両方のサーバーの日付と時刻の設定が一致していることを確認します。	IdM のタイムサービス要件

コンポーネント	設定	詳細
暗号化タイプ	<p>次の AD アカウントに AES 暗号化キーがあります。</p> <ul style="list-style-type: none"> ● AD 管理者 ● AD ユーザーアカウント ● AD サービス <p>最近 AD で AES 暗号化を有効にした場合は、次の手順で新しい AES キーを生成します。</p> <ol style="list-style-type: none"> 1. フォレスト内の AD ドメイン間の信頼関係を再確立します。 2. AD 管理者、ユーザーアカウント、およびサービスのパスワードを変更します。 	<ul style="list-style-type: none"> ● IdM における暗号化タイプのサポート ● GPO を使用した Active Directory で AES 暗号化タイプの有効化
ファイアウォール	<p>双方向通信のために、IdM サーバーと AD ドメインコントローラーで必要なすべてのポートを開いています。</p>	<p>IdM と AD との間の通信に必要なポート</p>
DNS	<ul style="list-style-type: none"> ● IdM と AD には、それぞれ固有のプライマリー DNS ドメインがあります。 ● IdM ドメインと AD DNS ドメインは重複していません。 ● LDAP および Kerberos サービスの適切な DNS サービス (SRV) レコード。 ● 信頼内のすべての DNS ドメインから DNS レコードを解決できます。 ● Kerberos レルム名は、プライマリー DNS ドメイン名を大文字にしたものです。たとえば、DNS ドメイン example.com には、対応する Kerberos レルム EXAMPLE.COM があります。 	<p>信頼用の DNS およびレルムの設定の構成</p>

コンポーネント	設定	詳細
トポロジー	信頼コントローラーとして設定した IdM サーバーとの信頼を確立しようとしていることを確認します。	信頼コントローラーおよび信頼エージェント

10.3. AD の信頼を確立する試みのデバッグログを収集

IdM 環境と AD ドメイン間の信頼確立で問題が発生した場合は、次の手順を使用して詳細なエラーログを有効にし、信頼を確立する試みのログを収集できるようにします。これらのログを確認してトラブルシューティング作業に役立てたり、Red Hat テクニカルサポートケースで提供したりできます。

前提条件

- IdM サービスを再起動するには root 権限が必要です。

手順

1. IdM サーバーのデバッグを有効にするには、次の内容でファイル `/etc/ipa/server.conf` を作成します。

```
[global]
debug=True
```

2. **httpd** サービスを再起動して、デバッグ設定をロードします。

```
[root@trust_controller ~]# systemctl restart httpd
```

3. **smb** および **winbind** サービスを停止します。

```
[root@trust_controller ~]# systemctl stop smb winbind
```

4. **smb** および **winbind** サービスのデバッグログレベルを設定します。

```
[root@trust_controller ~]# net conf setparm global 'log level' 100
```

5. IdM フレームワークで使用される Samba クライアントコードのデバッグログを有効にするには、`/usr/share/ipa/smb.conf.empty` 設定ファイルを編集して次の内容にします。

```
[global]
log level = 100
```

6. 以前の Samba ログを削除します。

```
[root@trust_controller ~]# rm /var/log/samba/log.*
```

7. **smb** サービスおよび **winbind** サービスを起動します。

```
[root@trust_controller ~]# systemctl start smb winbind
```

8. 詳細モードを有効にして信頼の確率を試みる際に、タイムスタンプを出力します。

```
[root@trust_controller ~]# date; ipa -vvv trust-add --type=ad ad.example.com
```

9. 失敗したリクエストについては、次のエラーログファイルを確認してください。

- a. `/var/log/httpd/error_log`

- b. `/var/log/samba/log.*`

10. デバッグを無効にします。

```
[root@trust_controller ~]# mv /etc/ipa/server.conf /etc/ipa/server.conf.backup
[root@trust_controller ~]# systemctl restart httpd
[root@trust_controller ~]# systemctl stop smb winbind
[root@trust_controller ~]# net conf setparm global 'log level' 0
[root@trust_controller ~]# mv /usr/share/ipa/smb.conf.empty
/usr/share/ipa/smb.conf.empty.backup
[root@trust_controller ~]# systemctl start smb winbind
```

11. (オプション) 認証問題の原因を判断できない場合は、以下を行います。

- a. 最近生成したログファイルを収集してアーカイブします。

```
[root@trust_controller ~]# tar -xvzf debugging-trust.tar /var/log/httpd/error_log
/var/log/samba/log.*
```

- b. Red Hat テクニカルサポートケースを開き、試行からのタイムスタンプとデバッグログを提供します。

関連情報

- [IPA - AD Trust Troubleshooting](#)

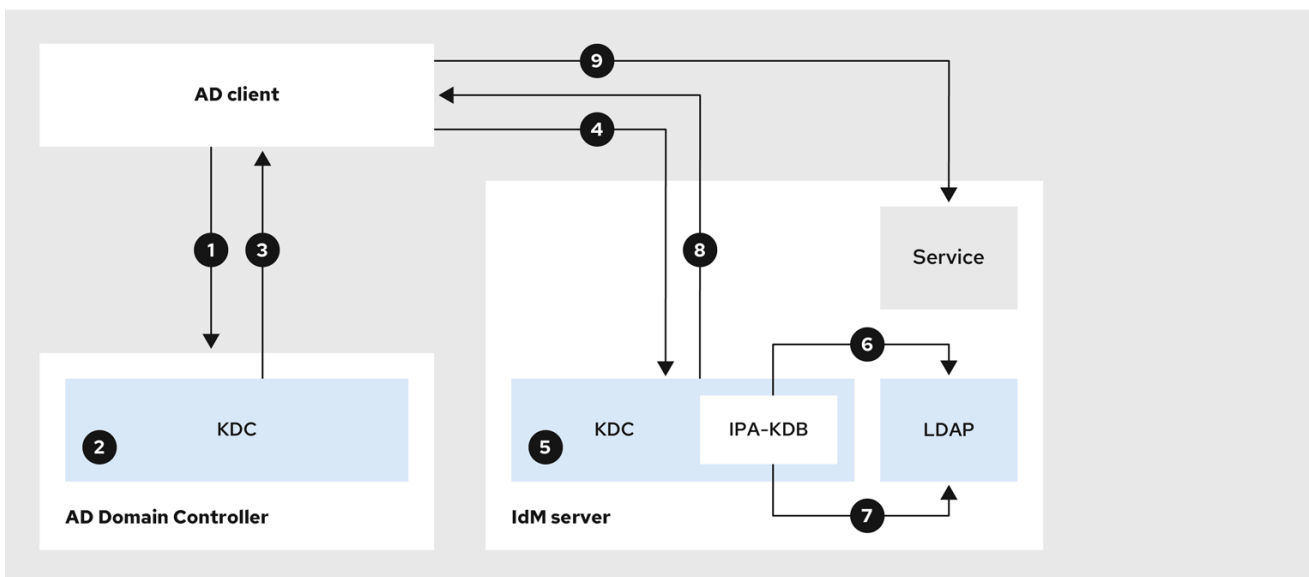
第11章 他のフォレストのサービスへのクライアントアクセスに関するトラブルシューティング

Identity Management (IdM) 環境と Active Directory (AD) 環境の間に信頼を設定した後、一方のドメインのクライアントがもう一方のドメインのサービスにアクセスできないという問題が発生する場合があります。次の図を使用して、問題のトラブルシューティングを行ってください。

11.1. AD フォレストルートドメイン内のホストが IDM サーバーのサービスをリクエストする場合の情報の流れ

次の図は、Active Directory (AD) クライアントが Identity Management (IdM) ドメインのサービスをリクエストする際の情報の流れを説明しています。

AD クライアントから IdM サービスにアクセスする際に問題が発生した場合は、この情報を使用してトラブルシューティングの作業を絞り込み、問題の原因を特定できます。



231_RHEL_0422

1. AD クライアントは AD Kerberos Distribution Center (KDC) に接続して、IdM ドメインのサービスに対して TGS リクエストを実行します。
2. AD KDC は、サービスが信頼された IdM ドメインに属していることを認識します。
3. AD KDC は、信頼された IdM KDC への参照とともに、クライアントにレルム間のチケット保証チケット (TGT) を送信します。
4. AD クライアントは、レルム間 TGT を使用して IdM KDC へのチケットをリクエストします。
5. IdM KDC は、クロスレルム TGT で送信される特権属性証明書 (MS-PAC) を検証します。
6. IPA-KDB プラグインは、LDAP ディレクトリーをチェックして、外部プリンシパルがリクエストされたサービスのチケットを取得できるかどうかを確認する場合があります。
7. IPA-KDB プラグインは、MS-PAC をデコードし、データを検証およびフィルタリングします。LDAP サーバーで検索を行い、ローカルグループなどの追加情報で MS-PAC を拡張する必要があるかどうかを確認します。

8. 次に、IPA-KDB プラグインは PAC をエンコードして署名し、サービスチケットに添付して AD クライアントに送信します。
9. AD クライアントは、IdM KDC によって発行されたサービスチケットを使用して IdM サービスに接続できるようになります。

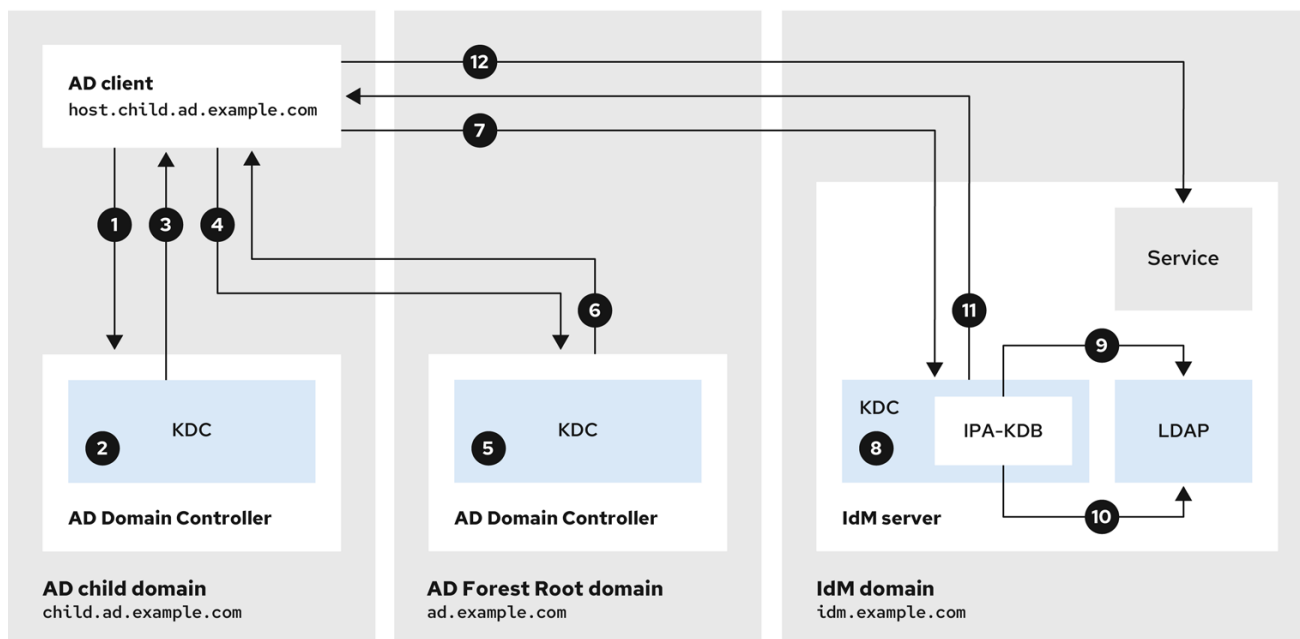
関連情報

- [Flow of information when a host in an AD child domain requests services from an IdM server](#)

11.2. AD 子ドメイン内のホストが IDM サーバーのサービスをリクエストする場合の情報の流れ

次の図は、子ドメイン内の Active Directory (AD) ホストが Identity Management (IdM) ドメインのサービスをリクエストする際の情報の流れを説明しています。このシナリオでは、AD クライアントは子ドメインの Kerberos Distribution Center (KDC) に接続し、次に AD フォレストルートの KDC に接続し、最後に IdM KDC に接続して IdM サービスへのアクセスをリクエストします。

AD クライアントから IdM サービスにアクセスする際に問題が発生し、AD クライアントが AD フォレストルートの子ドメインであるドメインに属する場合、この情報を使用してトラブルシューティングの作業を絞り込み、問題の原因を特定できます。



231_RHEL_0422

1. AD クライアントは 独自ドメイン内の AD Kerberos Distribution Center (KDC) に接続して、IdM ドメインのサービスに対して TGS リクエストを実行します。
2. 子ドメインである **child.ad.example.com** 内の AD KDC は、サービスが信頼された IdM ドメインに属していることを認識します。
3. 子ドメイン内の AD KDC は、AD フォレストルートドメイン **ad.example.com** の参照チケットをクライアントに送信します。
4. AD クライアントは、IdM ドメインのサービスについて、AD フォレストルートドメインの KDC に接続します。

5. フォレストルートドメインの KDC は、サービスが信頼された IdM ドメインに属していることを認識します。
6. AD KDC は、信頼された IdM KDC への参照とともに、クライアントにレルム間のチケット保証チケット (TGT) を送信します。
7. AD クライアントは、レルム間 TGT を使用して IdM KDC へのチケットをリクエストします。
8. IdM KDC は、クロスレルム TGT で送信される特権属性証明書 (MS-PAC) を検証します。
9. IPA-KDB プラグインは、LDAP ディレクトリーをチェックして、外部プリンシパルがリクエストされたサービスのチケットを取得できるかどうかを確認する場合があります。
10. IPA-KDB プラグインは、MS-PAC をデコードし、データを検証およびフィルタリングします。LDAP サーバーで検索を行い、ローカルグループなどの追加情報で MS-PAC を拡張する必要があるかどうかを確認します。
11. 次に、IPA-KDB プラグインは PAC をエンコードして署名し、サービスチケットに添付して AD クライアントに送信します。
12. AD クライアントは、IdM KDC によって発行されたサービスチケットを使用して IdM サービスに接続できるようになります。

関連情報

- [AD フォレストルートドメイン内のホストが IdM サーバーのサービスをリクエストする場合の情報の流れ](#)

11.3. IDM クライアントが AD サーバーのサービスをリクエストする場合の情報の流れ

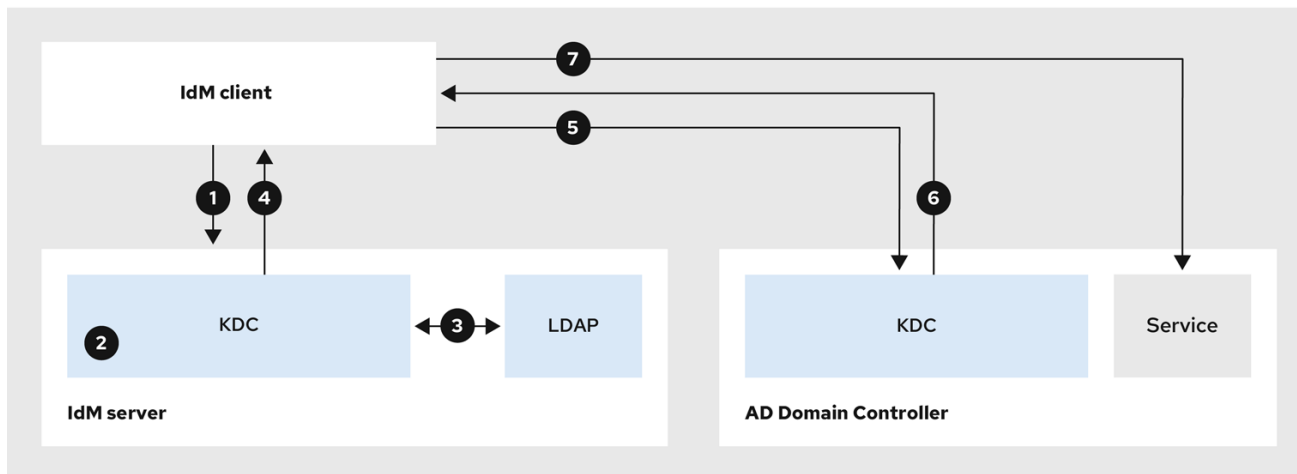
次の図は、Identity Management (IdM) と Active Directory (AD) の間に双方向の信頼を設定した場合に、IdM クライアントが AD ドメインでサービスをリクエストする場合の情報の流れを説明しています。

IdM クライアントから AD サービスにアクセスする際に問題が発生した場合は、この情報を使用してトラブルシューティングの取り組みを絞り込み、問題の原因を特定できます。



注記

デフォルトでは、IdM は AD への一方向の信頼を確立します。つまり、AD フォレスト内のリソースに対してレルム間のチケット保証チケット (TGT) を発行することはできません。信頼された AD ドメインからサービスへのチケットをリクエストできるようにするには、双方向の信頼を設定します。



231_RHEL_0422

1. IdM クライアントは、接続する AD サービスの IdM Kerberos Distribution Center (KDC) にチケット保証チケット (TGT) を要求します。
2. IdM KDC は、サービスが AD レルムに属していることを認識し、レルムが既知で信頼されていること、およびクライアントがそのレルムからサービスをリクエストできることを確認します。
3. IdM Directory Server からのユーザープリンシパルに関する情報を使用して、IdM KDC は、ユーザープリンシパルに関する特権属性証明書 (MS-PAC) レコードを使用してレルム間 TGT を作成します。
4. IdM KDC は、レルム間 TGT を IdM クライアントに送り返します。
5. IdM クライアントは AD KDC に接続して、AD サービスのチケットをリクエストし、IdM KDC によって提供される MS-PAC を含むレルム間 TGT を提示します。
6. AD サーバーは PAC を検証およびフィルタリングし、AD サービスのチケットを返します。
7. これで、IPA クライアントは AD サービスに接続できます。

関連情報

- [一方向および双方向の信頼](#)

第12章 コマンドラインを使用した信頼の削除

本セクションでは、コマンドラインインターフェースを使用して、IdM に Identity Management (IdM)/Active Directory (AD) 信頼を削除する方法を説明します。

前提条件

- IdM 管理者として Kerberos チケットを取得している。詳細は、[Logging in to IdM in the Web UI:Using a Kerberos ticket](#) を参照してください。

手順

1. **ipa trust-del** コマンドを使用して、IdM から信頼設定を削除します。

```
[root@server ~]# ipa trust-del ad_domain_name
-----
Deleted trust "ad_domain_name"
-----
```

2. Active Directory 設定から信頼オブジェクトを削除します。

検証手順

- **ipa trust-show** を実行して、信頼が削除されたことを確認します。

```
[root@server ~]# ipa trust-show ad.example.com
ipa: ERROR: ad.example.com: trust not found
```

第13章 IDM WEB UI で信頼の削除

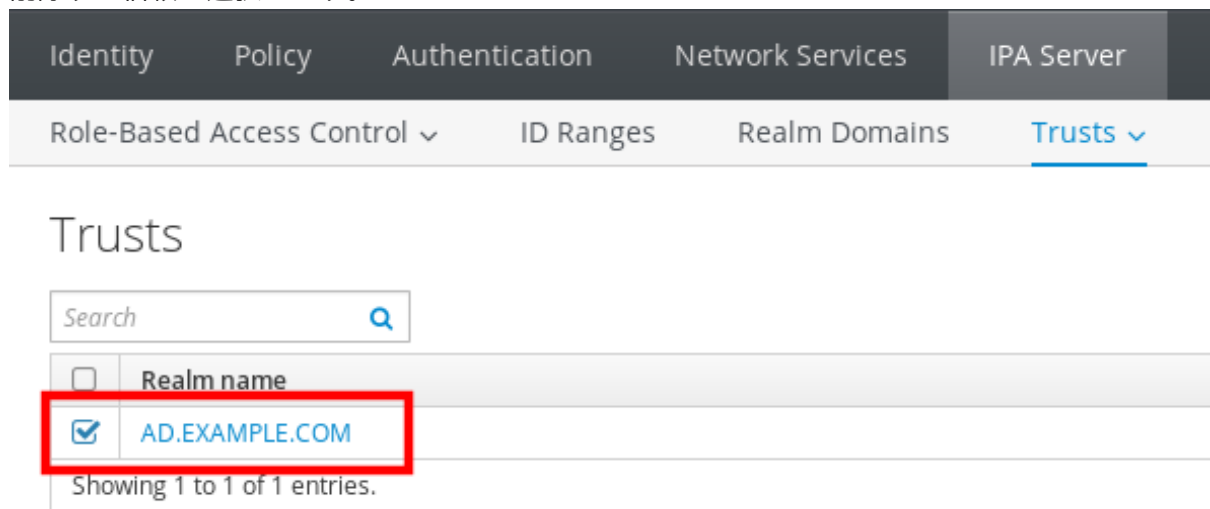
本セクションでは、IdM Web UI を使用して、Identity Management (IdM)/Active Directory (AD) の信頼を削除する方法を説明します。

前提条件

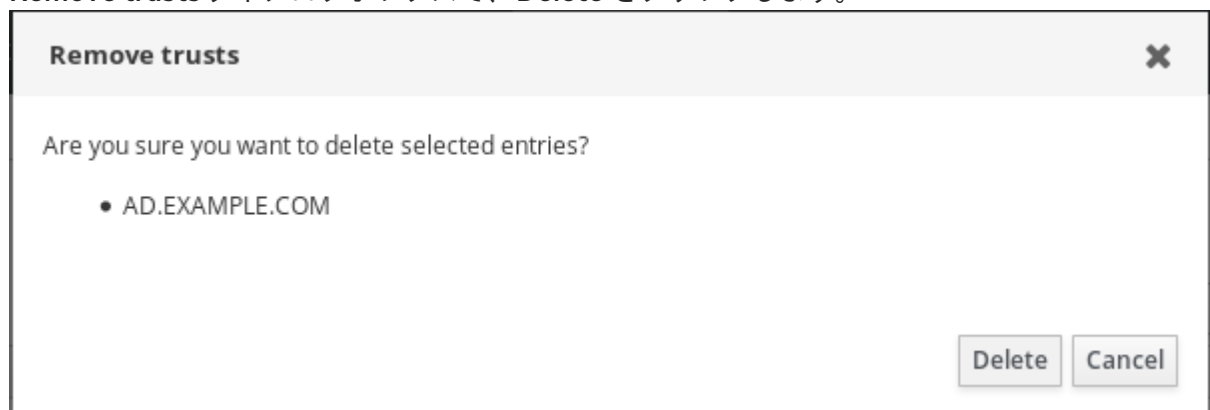
- Kerberos チケットを取得している。詳細は、[Logging in to IdM in the Web UI:Using a Kerberos ticket](#) を参照してください。

手順

1. 管理者権限で IdM Web UI にログインします。詳細は「[Web ブラウザーで IdM Web UI へのアクセス](#)」を参照してください。
2. IdM Web UI で、**IPA Server** タブをクリックします。
3. **IPA Server** タブで、**Trusts** タブをクリックします。
4. 削除する信頼を選択します。



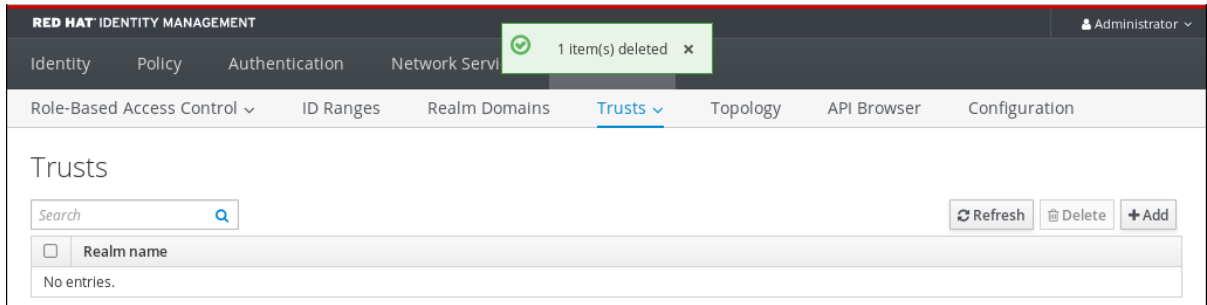
5. **Delete** ボタンをクリックします。
6. **Remove trusts** ダイアログボックスで、**Delete** をクリックします。



7. Active Directory 設定から信頼オブジェクトを削除します。

検証手順

- 信頼が正常に削除されていると、Web UI はテキストが付いた緑色のポップアップを表示します。



第14章 ANSIBLE を使用した信頼の削除

本セクションでは、Ansible Playbook を使用して、IdM で Identity Management(IdM)/Active Directory(AD)信頼を削除する方法を説明します。

前提条件

- IdM 管理者として Kerberos チケットを取得している。詳細は、[Logging in to IdM in the Web UI:Using a Kerberos ticket](#) を参照してください。
- 以下の要件を満たす Ansible コントロールノードを設定している。
 - Ansible バージョン 2.8 以降を使用している。
 - `ansible-freeipa` パッケージがインストールされている。
 - `~/MyPlaybooks/` ディレクトリーに、信頼を削除する IdM サーバーの完全修飾ドメイン名 (FQDN) で `Ansible インベントリーファイル` を作成している。

手順

1. `~/MyPlaybooks/` ディレクトリーに移動します。

```
$ cd ~/MyPlaybooks/
```

2. 以下の内容を含む `del-trust.yml` Playbook を作成します。

```
---
- name: Playbook to delete trust
  hosts: ipaserver
  become: true

  tasks:
    - name: ensure the trust is absent
      ipatrust:
        ipaadmin_password: SomeADMINpassword
        realm: ad.example.com
        state: absent
```

この例では、`realm` は AD レルム名の文字列を定義します。

3. ファイルを保存します。
4. Playbook ファイルとインベントリーファイルを指定して Ansible Playbook を実行します。

```
$ ansible-playbook -v -i inventory del-trust.yml
```

検証手順

- `ipa trust-show` を実行して、信頼が削除されたことを確認します。

```
[root@server ~]# ipa trust-show ad.example.com
ipa: ERROR: ad.example.com: trust not found
```

関連情報

- `/usr/share/doc/ansible-freeipa/README-trust.md`
- `/usr/share/doc/ansible-freeipa/playbooks/trust`