Red Hat Enterprise Linux 8

Identity Management の計画

Identity Management の計画およびアクセス制御設定のガイド

Last Updated: 2019-04-26

Red Hat Enterprise Linux 8 Identity Management の計画

Identity Management の計画およびアクセス制御設定のガイド

法律上の通知

Copyright © 2019 Red Hat, Inc.

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, 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

本書は、Red Hat Enterprise Linux 8 で Identity Management サービスを計画する方法を説明します。本バージョンのドキュメントには、厳選されたユーザーストーリーが含まれています。

目次

第1章 RED HAT ENTERPRISE LINUX における ID 管理およびアクセス制御の計画の概要

本セクションでは、Red Hat Enterprise Linux でID 管理およびアクセス制御のオプションの概要を説明します。本セクションを読むことで、お使いの環境に合わせた計画の準備が行えます。

1.1. IDENTITY MANAGEMENT の概要

本モジュールでは、Red Hat Enterprise Linux における ID 管理の目的を説明します。また、Identity Management ドメイン (およびこのドメインに含まれるクライアントおよびサーバーのマシン) に関する基本的な情報も提供します。

Red Hat Enterprise Linux における Identity Management の目的

Red Hat Enterprise Linux の Identity Management (IdM) は、Linux ベースのドメイン内で ID ストア、認証ポリシー、および認可ポリシーを一元管理する方法を提供します。IdM は、異なるサービスを個別に管理するオーバーヘッドと、異なるマシンで異なるツールを使用するオーバーヘッドを大幅に削減します。

IdM は、以下に対応する数少ない集中型 ID、ポリシー、および認証ソフトウェアです。

- Linux オペレーティングシステム環境の高度な機能
- Linux マシンの大規模なグループの一元化
- Active Directory とのネイティブな統合

IdM は、Linux ベースおよび Linux 制御のドメインを作成します。

- IdM は、既存のネイティブ Linux ツールとプロトコルを基盤とします。独自のプロセスと設定がありますが、その基礎となるテクノロジーは Linux システム上で十分に確立されおり、Linux 管理者から信頼されています。
- IdM サーバーおよびクライアントは Red Hat Enterprise Linux マシンです。IdM クライアントは、標準プロトコルに対応してさえいれば別の Linux および UNIX のディストリビューションにすることもできます。Windows クライアントは IdM ドメインのメンバーにはなれませんが、Active Directory (AD) が管理する Windows システムにログインしているユーザーは、Linux クライアントに接続したり、IdM が管理するサーバーにアクセスしたりできます。これは、AD ドメインと IdM ドメインとの間に、フォレスト間の信頼関係を確立することで実現します。

複数の Linux サーバーにおけるアイデンティティーおよびポリシーの管理

IdM を使用しない場合 - 各サーバーが個別に管理され、パスワードはすべてローカルマシンに保存されます。IT 管理者は各マシンでユーザーを管理し、個別に認証ポリシーおよび認可ポリシーを設定し、ローカルのパスワードを維持しますが、多くの場合は、その他の集中型ソリューション (たとえば Active Directory (AD) との直接統合) に依存しています。システムは、複数のソリューションを使用して AD と直接統合できます。

- レガシーの Linux ツール (使用は推奨されません)
- Samba winbind に基づくソリューション (特定のユースケースでのみ推奨)
- サードパーティー製ソフトウェアに基づくソリューション (通常は、他のベンダーへのライセンスが必要)
- SSSD に基づくソリューション (ネイティブ Linux と、ほとんどのユースケースに推奨)

IdM を使用する場合 - IT 管理者は以下が可能になります。

- 一か所でアイデンティティーの管理 - IdM サーバー
- 複数のマシンに同時にポリシーを均一に適用
- ホストベースのアクセス制御、委任、および他のルールを使用してユーザーに異なるアクセスレベルを設定
- 権限昇格ルールの一元管理
- ホームディレクトリーのマウント方法の定義

エンタープライズシングルサインオン

企業で Identity Management を利用している場合、SSO (シングルサインオン) は Kerberos プロトコルを使用して実装されます。このプロトコルは、インフラストラクチャーレベルで一般的であり、SSH、LDAP、NFS、CUPS、DNS などのサービスで SSO を有効にします。別の Web スタック (Apache、EAP、Django など) を使用した Web サービスでも、SSO に Kerberos を使用できますが、実際には、Web アプリケーションには SSO を元にした OpenID Connect または SAML を使用する方が便利です。2 つの層をブリッジするには、Kerberos 認証を OpenID Connect チケットまたは SAML アサーションに変換できる Identity Provider (IdP) ソリューションをデプロイすることが推奨されます。Red Hat SSO テクノロジーは、IdP などの Keycloak オープンソースプロジェクトに基づいています。

IdM を使用しない場合 - ユーザーはシステムにログインし、サービスやアプリケーションにアクセスする度にパスワードを求められます。これらのパスワードは異なる場合もあり、ユーザーはアプリケーションごとに使用する認証情報を覚えている必要があります。

IdM を使用する場合 - ユーザーはシステムにログインすると、認証情報を繰り返し聞かれることなく、複数のサービスやアプリケーションにアクセスできます。これにより、以下が可能になります。

- ユーザビリティーの向上
- パスワードを書き留めたり安全でない場所に保存したりするセキュリティーリスクの低減
- ユーザーの生産性向上

Linux と Windows の混合環境の管理

IdM を使用しない場合 - Windows システムは Active Directory フォレストで管理されますが、開発環境、実稼働環境、および他のチームには多くの Linux システムがあり、これらの Linux システムは Active Directory 環境から除外されます。

IdM を使用する場合 - IT 管理者は以下が可能になります。

- ネイティブの Linux ツールを使用して Linux システムを管理する
- Active Directory により一元管理されている環境に Linux システムを統合して、一元管理されたユーザーストアを保護する
- 規模に応じて、または必要に応じて、新しい Linux システムを簡単にデプロイする
- 他のチームに依存することなく遅延を回避しながら、ビジネスニーズに迅速に対応し、Linux インフラストラクチャーの管理に関連する決定を下す

Identity Management と標準 LDAP ディレクトリーの比較

Red Hat Directory Server などの標準 LDAP ディレクトリーは汎用ディレクトリーで、幅広いユースケースに適用するようにカスタマイズできます。

- スキーマー - ユーザー、マシン、ネットワークエンティティー、物理的設備、建物といった非常に幅広いエントリー用にカスタマイズ可能な柔軟性のあるスキーマー
- 典型的な使用例 - インターネット上でサービスを提供するビジネスアプリケーションなど、他のアプリケーションのデータを保存するバックエンドのディレクトリー

Identity Management (IdM) には、企業内 ID と、その ID に関連する認証および認可ポリシーを管理するという特定の目的があります。

- スキーマー - ユーザーやマシンの ID のエントリーといった特定の目的に関連するエントリーセットを定義する特定のスキーマ
- 典型的な使用例 - 企業やプロジェクトの境界内におけるアイデンティティーを管理する ID および認証サーバー

Red Hat Directory Server と IdM では、基礎となるディレクトリーサーバーのテクノロジーは同じです。ただし、IdM は企業内の ID 管理用に最適化されています。これにより全般的な拡張性は制限されますが、シンプルな設定、リソース管理の自動化の改善、企業の ID 管理における効率性の向上などの利点がもたらされます。

関連資料

- Red Hat Enterprise Linux Blog のブログ投稿「Identity Management or Red Hat Directory Server – Which One Should I Use?」
- 標準プロトコルに関するナレッジベースアーティクル
- Red Hat Enterprise Linux 7.3 Beta リリースノート

1.2. IDENTITY MANAGEMENT サーバーおよびクライアントの概要

Identity Management ドメインには、以下のタイプのシステムが含まれます。

Identity Management サーバー

Identity Management サーバーは、ドメインコントローラー (DC) として機能する Red Hat Enterprise Linux システムです。ほとんどのデプロイメントでは、IdM サーバーとともに統合認証局 (CA) がインストールされます。
サーバーは、ID 情報およびポリシー情報の中央リポジトリーで、ドメインメンバーが使用するサービスをホストします。

Identity Management クライアント

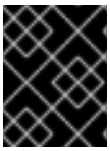
Identity Management クライアントは、サーバーに登録され、そのサーバーで Identity Management サービスを使用するように設定された Red Hat Enterprise Linux システムです。
クライアントは Identity Management サーバーと対話して、そのサーバーが提供するサービスにアクセスします。たとえば、クライアントは、Kerberos プロトコルを使用して認証を実行し、企業の SSO のチケットを取得し、LDAP を使用して ID 情報およびポリシー情報を取得し、DNS を使用してサーバーとサービスの場所と、その接続方法を検出します。

Identity Management サーバーの中には、Identity Management クライアントも組み込まれています。クライアントが自身に登録されるため、サーバーは、他のクライアントと同じ機能を提供します。

冗長性と可用性だけでなく、多数のクライアントにサービスを提供するため、Identity Management では 1 つのドメイン内に複数の IdM サーバーをデプロイできます。最大 60 台のサーバーをデプロイでき

ます。これは、IdM ドメインで現在サポートされている、レプリカとも呼ばれる IdM サーバーの最大数です。Identity Management サーバーは、クライアントにさまざまなサービスを提供します。すべてのサーバーが、可能なサービスをすべて提供する必要があるわけではありません。Kerberos や LDAP などの一部のサーバーコンポーネントは、常にすべてのサーバーで利用できますが、その他のサービス (認証局 (CA)、DNS、Trust Controller、Vault など) は必要に応じて使用します。つまり、デプロイメントでは、通常、サーバーにより役割が異なります。

ドメインを作成するためにインストールした最初のサーバーは **マスターサーバー** になります。Identity Management トポロジーに統合認証局 (CA) が含まれている場合、このサーバーは **CRL 生成マスター** および **CA 更新マスター** になります。これは、ドメイン内で CA サブシステム証明書およびキーの追跡と、証明書失効リスト (CRL) を処理する唯一のシステムです。



重要

トポロジー内では、CRL 生成マスターの役割を担うのは 1 台のサーバーに限定されるため、重要です。

管理者は、冗長性および負荷分散のために、既存のサーバー (マスターサーバーまたは別のレプリカ) の **レプリカ** を作成することで、追加サーバーを作成します。レプリカの作成時、Identity Management は既存サーバーの設定を複製します。レプリカは、ユーザー、システム、証明書、設定されたポリシーなど、そのコア設定を初期サーバーと共有します。

注記

レプリカと、そのレプリカを作成したサーバーは、CRL 生成マスターの役割を除き機能的に同じです。そのため、ここでは **サーバー** と **レプリカ** という用語を、文脈に応じて同じ意味で使用します。

1.3. RED HAT ENTERPRISE LINUX における ID 管理およびアクセス制御: 中央対ローカル

Red Hat Enterprise Linux では、システムのドメイン全体に集中型のツールを使用するか、1 台のシステムにローカルのツールを使用して、ID およびアクセス制御ポリシーを管理できます。

複数の Red Hat Enterprise Linux サーバーでの、ID およびポリシーの管理 (Identity Management の使用にかかわらず)

IT 管理者は、Identity Management で以下が可能になります。

- ID とグループ化メカニズムを一か所 (Identity Management サーバー) で管理
- パスワード、PKI 証明書、OTP トークン、SSH 鍵などのさまざまな種類の認証情報を一元管理
- 複数のマシンに同時にポリシーを均一に適用
- 外部の Active Directory ユーザー用に、POSIX およびその他の属性を管理
- ホストベースのアクセス制御、委任、および他のルールを使用してユーザーに異なるアクセスレベルを設定
- 特権昇格規則 (sudo) と必須アクセス制御 (SELinux ユーザーマッピング) の一元管理
- 中央の PKI インフラストラクチャーおよび秘密ストアの維持
- ホームディレクトリーのマウント方法の定義

ID 管理を使用しないと、以下のようになります。

- 各サーバーは別々に管理
- パスワードはすべて、ローカルマシンに保存
- IT 管理者は、すべてのマシンでユーザーを管理し、認証および認可ポリシーを別々に設定し、ローカルパスワードを維持

1.4. 関連資料

- Red Hat Identity Management に関する一般的な情報は、Red Hat カスタマーポータルの Red Hat Identity Management 製品ページ を参照してください。

第2章 レプリカトポロジーの計画

以下のセクションでは、ユースケースに適したレプリカトポロジーを決定するヒントを紹介します。

2.1. 高性能および災害復旧のソリューションとなる複数のレプリカサーバー

Identity Management サービスの継続的な機能および高可用性は、リソースにアクセスするユーザーに不可欠です。ロードバランスを介して Identity Management インフラストラクチャーの継続的な機能および高可用性を実現する組み込みソリューションの 1 つは、マスターサーバーのレプリカサーバーを作成して中央ディレクトリーを複製することです。

Identity Management を使用すると、企業の組織構造を反映するために、地理的に分散したデータセンターに追加のサーバーを配置できます。このようにして、Identity Management クライアントと、一番近くにある、アクセス可能なサーバーとの間のパスが短くなります。さらに、複数のサーバーを持つことで、負荷を分散し、より多くのクライアントに拡張できます。

複数の冗長な Identity Management サーバーを維持し、それらを違いに複製させることも、サーバーの損失を軽減または防止するための一般的なバックアップメカニズムです。たとえば、1 台のサーバーに障害が発生しても、その他のサーバーがドメインにサービスを提供し続けます。残りのサーバーの 1 つに基づいて新しいレプリカを作成し、失われたサーバーを回復することもできます。

2.2. IDENTITY MANAGEMENT サーバーおよびクライアント

Identity Management ドメインには、以下のタイプのシステムが含まれます。

Identity Management サーバー

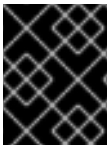
Identity Management サーバーは、ドメインコントローラー (DC) として機能する Red Hat Enterprise Linux システムです。ほとんどのデプロイメントでは、IdM サーバーとともに統合認証局 (CA) がインストールされます。
サーバーは、ID 情報およびポリシー情報の中央リポジトリーで、ドメインメンバーが使用するサービスをホストします。

Identity Management サーバーの中には、Identity Management クライアントも組み込まれています。クライアントが自身に登録されるため、サーバーは、他のクライアントと同じ機能を提供します。

Identity Management クライアント

Identity Management クライアントは、サーバーに登録され、そのサーバーで Identity Management サービスを使用するように設定された Red Hat Enterprise Linux システムです。
クライアントは、ドメイン内のリソースにアクセスするために、Identity Management サーバーと対話します。たとえば、クライアントは、サーバーに設定した Kerberos ドメインに属し、サーバーが発行する証明書およびチケットを受け取り、認証および認可に、その他の集中サービスを使用します。

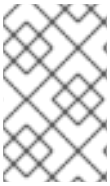
ドメインを作成するためにインストールした最初のサーバーは **マスターサーバー** になります。Identity Management トポロジーに統合認証局 (CA) が含まれている場合、このサーバーは **CRL 生成マスター** および **CA 更新マスター** になります。これは、CA サブシステム認証およびキーの追跡と、証明書失効リスト (CRL) の生成を担当するドメイン内の唯一のシステムです。



重要

トポロジー内では、CRL 生成マスターの役割を担うのは 1 台のサーバーに限定されるため、重要です。

管理者は、冗長性および負荷分散のために、既存のサーバー (マスターサーバーまたは別のレプリカ) の **レプリカ** を作成することで、追加サーバーを作成します。レプリカの作成時、Identity Management は既存サーバーの設定を複製します。レプリカは、ユーザー、システム、証明書、設定されたポリシーなど、そのコア設定を初期サーバーと共有します。



注記

レプリカと、そのレプリカを作成したサーバーは、CRL 生成マスターの役割を除き機能的に同じです。そのため、ここでは **サーバー** と **レプリカ** という用語を、文脈に応じて同じ意味で使用します。

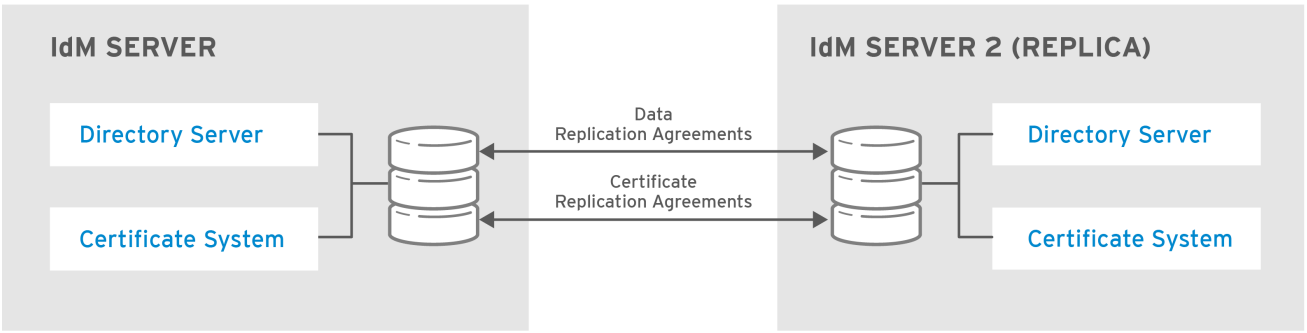
2.3. レプリカ合意

管理者が、既存のサーバーに基づいてレプリカを作成すると、Identity Management は、初期サーバーとレプリカとの間に **replication agreement** を作成します。レプリカ合意は、データと設定が 2 台のサーバー間で継続的に複製されることを保証します。

レプリカ合意は常に双方向のものです。1 台目のサーバーから 2 台目のサーバーにデータが複製されるだけでなく、2 台目のサーバーから 1 台目のサーバーにもデータが複製されます。

Identity Management は **マルチマスターレプリケーション** を使用します。マルチマスターレプリケーションでは、レプリカ合意に参加している全レプリカが更新を受け取るため、データマスターと見なされます。

図2.1 サーバーとレプリカ合意



Identity Management は、2 種類のレプリカ合意を使用します。

ドメインのレプリカ合意
: これにより、識別情報が複製されます。

証明書のレプリカ合意
: これにより、識別情報が複製されます。

両方の複製チャンネルは独立しています。2 台のサーバー間で、一方または両方の種類のレプリカ合意を設定できます。たとえば、サーバー A とサーバー B にドメインレプリカ合意のみが構成されている場合は、証明書情報ではなく ID 情報だけが複製されます。

2.4. 適切なレプリカ数の決定

各データセンターに少なくとも 2 つのレプリカを設定 (必須要件ではありません)
: データセンターは、たとえば、本社または地理的な位置 (領域) にできます。

クライアントにサービスを提供するために十分な数のサーバーを設定

1 台の Identity Management サーバーで 2000 ~ 3000 クライアントにサービスを提供できます。ここでは、クライアントがサーバーに対して 1 日に複数回クエリーすることを想定していますが、毎分ではないことを想定しています。より頻繁なクエリーが予想される場合は、より多くのサーバーを計画してください。

1 つの Identity Management ドメインに最大 60 台のレプリカを設定

Red Hat は、レプリカが最大 60 台含まれる環境をサポートしています。

2.5. トポロジー内でレプリカの接続

1 台のレプリカを少なくとも 2 つのレプリカに接続

追加のレプリカ合意を設定すると、初期レプリカとマスターサーバーとの間だけでなく、他のレプリカ間でも情報が複製されます。

レプリカを、その他のレプリカ (最大 4 つ) に接続 (必須要件ではありません)

サーバーごとに多数のレプリカ合意を行っても、それ以上に大きな利点はありません。1 つのコンシューマーレプリカを一度に更新できるのは、1 つのレプリカだけです。一方、他のレプリカ合意はアイドル状態です。
レプリカ合意を設定しすぎると、全体的なパフォーマンスに悪い影響を及ぼす可能性もあります。

データセンター内のレプリカを互いに接続

これにより、データセンター間のドメインレプリケーションが保証されます。

各データセンターを少なくとも 2 つの他のデータセンターに接続

これにより、データセンター間のドメインレプリケーションが保証されます。

少なくとも一対のレプリカ合意を使用してデータセンターを接続

データセンター A および B に、A1 から B1 までのレプリカ合意がある場合は、いずれかのサーバーがダウンしても、2 つのデータセンター間のレプリケーションは継続します。

2.6. レプリカトポロジーの例

以下の図は、信頼できるトポロジーを作成するガイドラインに基づく Identity Management トポロジーの例を示しています。

図2.2「レプリカトポロジーの例 1」 には 4 つのデータセンターがあり、各データセンターに 4 つのサーバーがあります。このサーバーは、レプリカ合意に接続しています。

図2.2 レプリカトポロジーの例 1

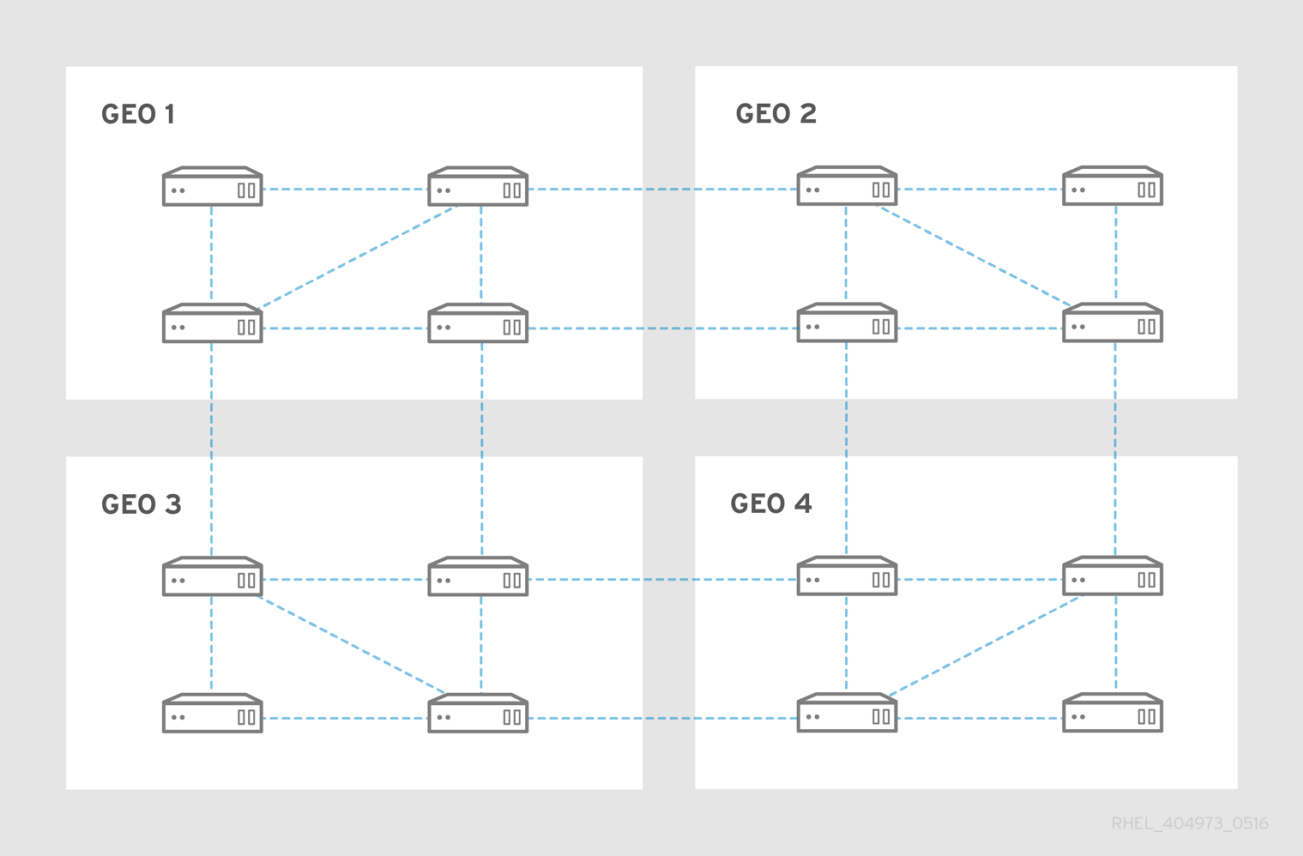
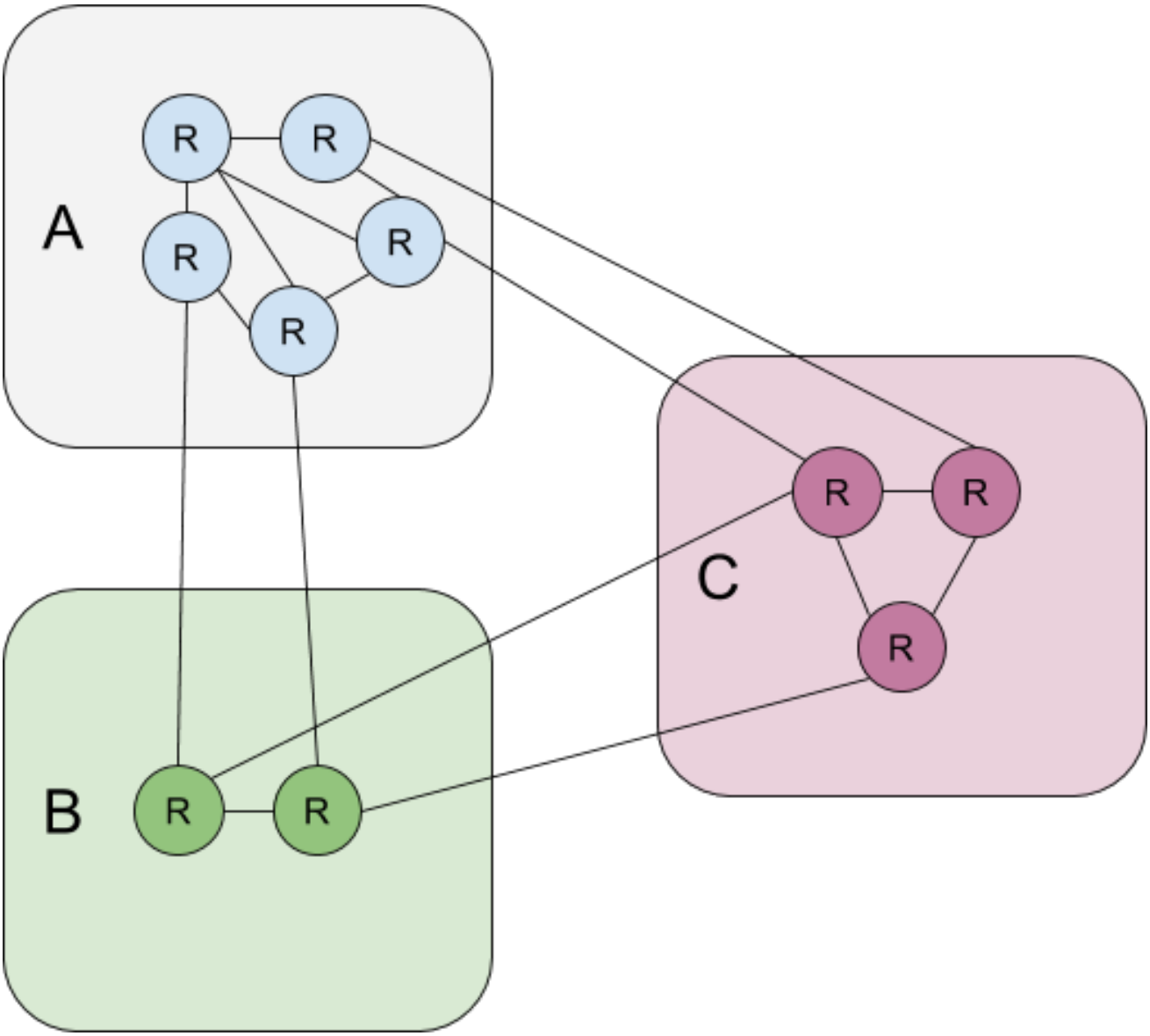


図2.3「レプリカトポロジーの例 2」 には、所有するサーバー数が異なる 3 つのデータセンターが表示されます。サーバーは、レプリカ合意に接続しています。

図2.3 レプリカトポロジーの例 2



第3章 ACTIVE DIRECTORY を使用した統合の計画

以下のセクションでは、Red Hat Enterprise Linux と Active Directory を統合するためのオプションを紹介します。

- 直接統合の概要は「直接的な統合」を参照してください。
- 間接統合の概要は「間接的な統合」を参照してください。
- どちらを選択するかは「間接統合と直接統合の間の決定」を参照してください。

3.1. 直接的な統合

直接統合では、Linux システムは、Active Directory に直接接続されています。次の種類の統合が可能です。

System Security Services Daemon (SSSD) との統合

SSSD は、Linux システムをさまざまな ID および認証ストア (Active Directory、Identity Management、もしくは汎用の LDAP サーバーまたは Kerberos サーバー) に接続できます。
SSSD の統合に関する重要な要件

- Active Directory と統合すると、SSSD は、デフォルトで 1 つの AD フォレスト内でのみ機能します。マルチフォレストを設定する場合は、ドメインのエミュレーションを手動で設定します。
- **`idmap_ad`** プラグインがリモートフォレストユーザーを正常に処理するには、リモートの Active Directory 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。

SSSD は、直接統合と間接統合の両方に対応します。また、莫大な移行コストをかけずに、ある統合アプローチから別のアプローチへ切り替えることもできます。

Samba Winbind との統合

Samba スイートの Winbind コンポーネントは、Linux システム上で Windows クライアントをエミュレートし、Active Directory サーバーと通信します。
Samba Winbind の統合に関する重要な要件

- マルチフォレスト Active Directory 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。
- リモートの Active Directory ドメインユーザーに関する完全な情報を **`idmap_ad`** プラグインで使用できるようにするには、Linux システムのローカルドメインから、ユーザーが所属するリモートの Active Directory フォレスト内ドメインへの双方向パスが存在する必要があります。

推奨情報

- SSSD は、AD 統合のほとんどのユースケースに対応し、クライアントシステムとさまざまなタイプの ID および認証プロバイダー (AD、IdM、Kerberos、および LDAP) との間の汎用ゲートウェイとして堅牢なソリューションを提供します。
- Samba FS をデプロイする予定の AD ドメインメンバーサーバーへのデプロイには、Winbind が推奨されます。

3.2. 間接的な統合

間接統合により、Linux システムが最初に中央サーバーに接続し、次に中央サーバーが Active Directory に接続します。間接統合により、管理者は Linux システムとポリシーを一元管理でき、Active Directory のユーザーは透過的に Linux システムとサービスにアクセスできます。

Active Directory を使用したフォレスト間の信頼に基づく統合

Identity Management サーバーは、Linux システムを制御する中央サーバーとして機能します。Active Directory を使用したレルム間 Kerberos 信頼が確立され、Active Directory のユーザーが Linux システムおよびリソースにログインしてアクセスできるようになります。Identity Management は、それ自体を別のフォレストとして Active Directory に提示し、Active Directory で対応しているフォレストレベルの信頼を利用します。
信頼を使用すると、以下が可能になります。

- Active Directory ユーザーは、Identity Management リソースにアクセスできます。
- Identity Management サーバーおよびクライアントは、Active Directory ユーザーおよびグループの ID を解決できます。
- Active Directory ユーザーおよびグループは、ホストベースのアクセス制御など、Identity Management が定義する条件下で Identity Management にアクセスします。
- Active Directory ユーザーおよびグループの管理は、引き続き Active Directory で行います。

同期に基づく統合

このアプローチは WinSync ツールに基づいています。WinSync レプリカ合意は、Active Directory から Identity Management へユーザーアカウントを同期します。

警告

WinSync は、Red Hat Enterprise Linux 8 で積極的に開発されなくなりました。間接統合に推奨されるソリューションはフォレスト間の信頼です。

同期に基づく統合の制限は次のとおりです。

- Identity Management から Active Directory へのグループの同期がされません。
- Active Directory と Identity Management でユーザーが重複します。
- WinSync は、1 つの Active Directory ドメインのみをサポートします。
- Identity Management 内の 1 つのインスタンスへのデータ同期には、Active Directory 内の 1 つのドメインコントローラーのみが使用できます。
- ユーザーパスワードを同期する必要があります。そのためには、PassSync コンポーネントを Active Directory ドメイン内のすべての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。
- すべての Active Directory ユーザーは、同期を構成してから手動でパスワードを変更しないと、PassSync を同期できません。

3.3. 間接統合と直接統合の間の決定

本セクションのガイドラインは、どのタイプの統合がユースケースに合うかを判断するのに役に立ちます。

Active Directory に接続するシステムの数

30~50 台未満のシステムを接続 (必須要件ではない)

30~50 台未満のシステムを接続する場合は、直接統合を検討してください。間接統合により、不要なオーバーヘッドが発生する可能性があります。

30-50 台を超えるシステムを接続 (必須制限ではない)

30~50 台を超えるシステムを接続する場合は、Identity Management を使用した間接統合を検討してください。このアプローチでは、Linux システムの集中管理から恩恵を受けることができます。

管理する Linux システムの数は少ないが、今後急増する見込み

このシナリオでは、間接的な統合を検討し、後で環境を移行しなくても済むようにします。

新しいシステムをデプロイする頻度とその種類

ベアメタルシステムの不規則なデプロイメント

新しいシステムをデプロイすることがほとんどなく、通常はベアメタルシステムをデプロイする場合は、直接統合を検討してください。そのような場合、直接統合は、通常、最も単純で簡単です。

仮想システムの頻繁なデプロイメント

新しいシステムを頻繁にデプロイし、それが通常オンデマンドでプロビジョニングされた仮想システムである場合は、間接統合を検討してください。間接統合では、中央サーバーを使用して新しいシステムを動的に管理し、Red Hat Satellite などのオーケストレーションツールと統合できます。

Active Directory が必須の認証プロバイダーである

すべてのユーザーが Active Directory に対して認証を行う必要があると、内部ポリシーに記載していますか?

直接統合または間接統合のいずれかを選択できます。Identity Management と Active Directory との間の信頼を使用して間接統合を使用する場合、Linux システムにアクセスするユーザーは、Active Directory に対して認証を行います。Active Directory に存在するポリシーは、認証中に実行され適用されます。

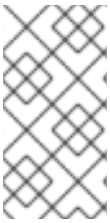
第4章 IDENTITY MANAGEMENT 環境と ACTIVE DIRECTORY との間の信頼関係の計画

Active Directory および Identity Management は、Kerberos、LDAP、DNS、証明書サービスなどのさまざまなコアサービスを管理する 2 つの代替環境です。**フォレスト間の信頼** 関係は、すべてのコアサービスがシームレスに対話できるようにすることで、その 2 つの異なる環境を透過的に統合します。次のセクションでは、フォレスト間の信頼のデプロイメントを計画して設計する方法のヒントを紹介します。

4.1. IDENTITY MANAGEMENT 環境と ACTIVE DIRECTORY との間のフォレスト間の信頼

純粋な Active Directory 環境では、フォレスト間の信頼は、2 つの別々の Active Directory フォレストルートドメインを接続します。Active Directory と Identity Management との間にフォレスト間の信頼関係を作成すると、Identity Management ドメインは、それ自体を 1 つのドメインを持つ独立したフォレストとして Active Directory に提示します。その後、Active Directory フォレストのルートドメインと Identity Management ドメインの間に信頼関係が確立されるため、Active Directory フォレストのユーザーは、Identity Management ドメインのリソースにアクセスできます。

Identity Management は、1 つの Active Directory フォレスト、または関連のない複数のフォレストとの信頼関係を確立できます。



注記

cross-realm trust で、2 つの Kerberos レルムを接続できます。ただし、Kerberos レルムは認証にのみ関係し、識別および認可操作に関連するその他のサービスおよびプロトコルには関係しません。したがって、Kerberos のレルム間の信頼を確立しても、あるレルムのユーザーが別のレルムのリソースにアクセスできるようにするには不十分です。

Active Directory ドメインへの外部の信頼
外部の信頼は、Identity Management と Active Directory 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 Identity Management 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、Identity Management 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。

4.2. 信頼コントローラーおよび信頼エージェント

Identity Management には、Active Directory への信頼をサポートする、以下のタイプの Identity Management 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で ID 検索が実行可能な Identity Management 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。Active Directory ドメインコントローラーは、Active Directory への信頼を確立して検証する際に信頼コントローラーに問い合わせます。信頼を設定すると、最初の信頼コントローラーが作成されます。

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向け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。

Identity Management ドメインには、信頼エージェントと信頼コントローラーだけでなく、標準の

Identity Management サーバーも追加できます。ただし、これらのサーバーは Active Directory と通信しないため、標準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 ユーザーの認証および認可を行うことができません。

表4.1 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 のユーザーおよびグループの解決	はい	はい
Identity Management クライアントを登録して、信頼済みの Active Directory フォレストのユーザーがアクセスできるサービスの実行	はい	はい
信頼の管理 (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。

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

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昇格して、信頼コントローラーを新規作成してください。これには、Identity Management サーバーの **ipa-adtrust-install** ユーティリティーを使用してください。

重要

既存の信頼コントローラーを信頼エージェントにダウングレードすることはできません。

4.3. 一方向および双方向の信頼

一方向の信頼関係では、Identity Management (IdM) は Active Directory (AD) を信頼しますが、AD は IdM を信頼しません。AD ユーザーは IdM ドメイン内のリソースにアクセスできますが、IdM のユーザーは AD ドメインのリソースにアクセスできません。IdM サーバーは、特別なアカウントを使用して AD に接続し、ID 情報を読み取り、それを LDAP 経由で IdM クライアントに配信します。

双方向の信頼では、IdM ユーザーは AD に対して認証でき、AD ユーザーは IdM に対して認証できます。一方向の信頼の場合と同様、AD ユーザーは IdM ドメイン内のリソースに対して認証およびアクセスできます。IdM ユーザーは認証できますが、AD のほとんどのリソースにアクセスすることはできません。IdM ユーザーは、アクセス制御チェックを必要としない、AD フォレスト内の Kerbers 対応サービスにのみアクセスできます。

AD リソースへのアクセスを許可できるようにするには、IdM は Global Catalog サービスを実装する必要があります。IdM サーバーの現在のバージョンにはこのサービスがありません。そのため、IdM と AD との間の双方向の信頼は、IdM と AD との間の一方向の信頼とほぼ機能的に同等です。

4.4. 非 POSIX の外部グループおよびセキュリティー ID マッピング

Identity Management は、グループ管理に LDAP を使用します。Active Directory エントリーは、Identity Management に同期またはコピーされません。つまり、Active Directory ユーザーおよびグループには、LDAP サーバーに LDAP オブジェクトがないため、Identity Management LDAP のグループメンバーシップを表現するために直接使用することはできません。このため、Identity Management の管理者は、非 POSIX 外部グループを作成する必要があります。これは、通常の Identity Management の LDAP オブジェクトで、Identity Management の中で Active Directory ユーザーおよびグループが IdM のグループに所属していることを表現するために使われます。

非 POSIX の外部グループのセキュリティー ID (SID) は SSSD により処理され、Active Directory のグループの SID を、Identity Management の POSIX グループにマップします。Active Directory では、SID はユーザー名に関連付けられています。Active Directory のユーザー名を使用して Identity Management リソースにアクセスする場合、SSSD はユーザーの SID を使用して、Identity Management ドメイン内のユーザーの完全なグループメンバーシップ情報を構築します。

4.5. DNS のセットアップ

このガイドラインは、Identity Management と Active Directory との間でフォレスト間の信頼を確立するために正しい DNS 構成を実現するのに役に立ちます。

一意のプライマリー DNS ドメイン

Active Directory と Identity Management の両方に、固有のプライマリーの DNS ドメインが設定されているのを確認します。以下に例を示します。

- **`ad.example.com`** (Active Directory の場合) および **`idm.example.com`** (Identity Management の場合)
- **`example.com`** (Active Directory の場合) および **`idm.example.com`** (Identity Management 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、標準に準拠した DNS サーバーも使用できます。

Identity Management ドメインと Active Directory DNS ドメインとの間に重複がない

Identity Management 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。Identity Management クライアントを含む DNS ドメインが、Active Directory に参加しているシステムを含む DNS ドメインと重複しないようにします。

適切な SRV レコード

プライマリー Identity Management DNS ドメインに、Active Directory 信頼をサポートするのに適切な SRV レコードがあることを確認してください。

同じ IdM レルムにあるその他の DNS ドメインでは、Active Directory への信頼設定時に SRV レコードを設定する必要がありません。これは、Active Directory ドメインコントローラーが、Kerberos の鍵配布センター (KDC) の検索に SRV レコードを使用せず、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 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

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。

- Identity Management DNS を設定する場合は「Installing an IdM server with an external CA」を参照してください。
- 統合 DNS を使用しない Identity Management を使用している場合は「Installing an IdM server without integrated DNS」の手順を参照してください。

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

Kerberos レルム名は、プライマリー DNS ドメイン名と同じで、すべて大文字になります。たとえば、Active Directory のドメイン名が **ad.example.com** で、Identity Management のドメイン名が **idm.example.com** の場合、Kerberos レルムは **AD.EXAMPLE.COM** および **IDM.EXAMPLE.COM** となります。

4.6. NETBIOS 名

NetBIOS 名は通常、ドメイン名の一番左の部分です。以下に例を示します。

- ドメイン名 **linux.example.com** の NetBIOS 名は **linux** です。
- ドメイン名 **example.com** の NetBIOS 名は **example** です。

Identity Management ドメインと Active Directory ドメインで異なる NetBIOS 名

Identity Management ドメインと Active Directory ドメインが異なる NetBIOS 名を持つようにします。
NetBIOS 名は Active Directory ドメインの識別に必要なもので、Identity Management ドメインが Active Directory DNS のサブドメイン内にある場合は、Identity Management ドメインとサービスの特定に NetBIOS 名も重要になります。

NetBIOS 名の文字制限

NetBIOS 名は最長 15 文字です。

4.7. ACTIVE DIRECTORY サーバーの検出およびアフィニティーを構成

サーバー検出とアフィニティー設定は、Identity Management クライアントが通信する Active Directory サーバーに影響を及ぼします。本セクションは、Identity Management と Active Directory との間でフォレスト間の信頼関係がある環境で、検出とアフィニティーがどのように機能するかを説明します。

地理的に同じ場所にあるサーバーを優先するようにクライアントを設定すると、クライアントが別のリモートデータセンターからサーバーにアクセスするときに発生するタイムラグなどの問題を防ぐことができます。クライアントが確実にローカルサーバーと通信するようにするには、次のことを確認する必要があります。

- クライアントは、LDAP および Kerberos を介して、ローカルの Identity Management サーバーと通信します。
- クライアントは、Kerberos を介してローカルの Active Directory サーバーと通信します。
- Identity Management サーバーの組み込みクライアントは、LDAP と Kerberos を介してローカルの Active Directory サーバーと通信します。

ローカルの Identity Management サーバーと通信するために、Identity Management クライアントで LDAP と Kerberos を設定するためのオプション

統合 DNS で Identity Management を使用する場合

デフォルトでは、クライアントは DNS レコードに基づいて自動サービスルックアップを使用します。この設定では、**DNS の場所** 機能を使用して、DNS ベースのサービス検出を設定することもできます。
自動検索を無効にするには、以下の方法で DNS 検出を無効にします。

- Identity Management クライアントのインストール中に、コマンドラインからフェイルオーバーのパラメーターを指定

- クライアントをインストールした後、System Security Services Daemon の設定を変更

統合 DNS を使用せずに Identity Management を使用する場合

次のいずれかの方法でクライアントを明示的に設定する必要があります。

- Identity Management クライアントのインストール中に、コマンドラインからフェイルオーバーのパラメーターを指定
- クライアントをインストールした後、System Security Services Daemon の設定を変更

ローカルの Active Directory サーバーと通信するために、Identity Management クライアントで Kerberos を構成するためのオプション

Identity Management クライアントは、どの Active Directory サーバーと通信するかを自動的に検出できません。Active Directory サーバーを手動で指定するには、**krb5.conf** ファイルを変更します。

- Active Directory レルム情報を追加します。
- 以下を使用して、通信する Active Directory サーバーを明示的に指定します。

以下に例を示します。

```
[realms]
AD.EXAMPLE.COM = {
kdc = server1.ad.example.com
kdc = server2.ad.example.com
}
```

Kerberos および LDAP を介したローカルの Active Directory サーバーとの通信用に、Identity Management サーバーで組み込みクライアントを設定するためのオプション

Identity Management サーバー上の組み込みクライアントは、Active Directory サーバーのクライアントとしても機能します。適切な Active Directory サイトを自動的に検出して使用できます。

組み込みクライアントが検出を実行すると、リモートの場所にある Active Directory サーバーを最初に検出する可能性があります。リモートサーバーへの接続試行に時間がかかりすぎると、クライアントは接続を確立せずに操作を停止することがあります。クライアント上の **sssd.conf** ファイルの **dns_resolver_timeout** オプションを使用して、クライアントが DNS リゾルバーからの応答を待つ時間を長くします。詳細は man ページの **sssd.conf(5)** を参照してください。

埋め込みクライアントがローカルの Active Directory サーバーと通信するように設定すると、システムセキュリティサービスデーモン (SSSD) は、組み込みクライアントが属する Active Directory サイトを覚えるため、SSSD は通常、ローカルドメインコントローラーに直接 LDAP ping を送信し、そのサイト情報を更新します。そのサイトが存在しなくなったか、クライアントが別のサイトに割り当てられた場合は、SSSD がフォレスト内の SRV レコードのクエリーを開始し、自動検出の全プロセスを実行します。

sssd.conf の **信頼されるドメインセクション** を使用して、デフォルトで自動的に検出される情報の一部を明示的に上書きすることもできます。

4.8. ACTIVE DIRECTORY との IDENTITY MANAGEMENT への間接統合中に実行される操作

表4.2「Identity Management 信頼コントローラーから Active Directory ドメインコントローラーへの操作」 は、Identity Management 信頼コントローラーから Active Directory ドメインコントローラーに向

けた、Identity Management から Active Directory への信頼の作成時に実行される操作およびリクエストを示します。

表4.2 Identity Management 信頼コントローラーから Active Directory ドメインコントローラーへの操作

操作	使用プロトコル	目的
Identity Management 信頼コントローラーに設定された Active Directory の DNS リゾルバーに対する DNS 解決	DNS	Active Directory ドメインコントローラーの IP アドレスを検出する
Active Directory DC における UDP/UDP6 ポート 389 へのリクエスト	非コネクション型 LDAP (CLDAP)	Active Directory DC 検出を実行する
Active Directory DC における TCP/TCP6 ポート 389 および 3268 へのリクエスト	LDAP	Active Directory ユーザーおよびグループ情報をクエリーする
Active Directory DC における TCP/TCP6 ポート 389 および 3268 へのリクエスト	DCE RPC および SMB	Active Directory にフォレスト間の信頼を設定およびサポートする
Active Directory DC における TCP/TCP6 ポート 135、139、445 へのリクエスト	DCE RPC および SMB	Active Directory にフォレスト間の信頼を設定およびサポートする
Active Directory ドメインコントローラーの指示に従って、Active Directory DC で動的に開かれたポートへのリクエスト (おそらく 49152~65535 (TCP/TCP6) の範囲)	DCE RPC および SMB	DCE RPC エンドポイントマッパー (ポート 135 TCP/TCP6) による要求に応答する
Active Directory DC におけるポート 88 (TCP/TCP6 および UDP/UDP6)、464 (TCP/TCP6 および UDP/UDP6)、749 (TCP/TCP6) へのリクエスト	Kerberos	Kerberos チケットを取得する、Kerberos パスワードを変更する、Kerberos をリモートで管理する

表4.2「Identity Management 信頼コントローラーから Active Directory ドメインコントローラーへの操作」 は、Active Directory ドメインコントローラーから Identity Management 信頼コントローラーにむけた、Identity Management から Active Directory への信頼の 作成時に実行される操作とリクエストを示します。

表4.3 Active Directory ドメインコントローラーから Identity Management 信頼コントローラーへの操作

操作	使用プロトコル	目的
Active Directory ドメインコントローラーに設定した Identity Management DNS リゾルバーに対する DNS 解決	DNS	Identity Management 信頼コントローラーの IP アドレスを検出する

操作	使用プロトコル	目的
Identity Management 信頼コントローラーにおける UDP/UDP6 ポート 389 へのリクエスト	非コネクション型 LDAP (CLDAP)	Identity Management 信頼コントローラー検出を実行する
Identity Management 信頼コントローラーにおける TCP/TCP6 ポート 135、139、445 へのリクエスト	DCE RPC および SMB	Active Directory へのフォレスト間の信頼を確認する
Identity Management 信頼コントローラーの指示に従い、Identity Management 信頼コントローラー上で動的に開いたポートへのリクエスト (範囲はおそらく 49152-65535 (TCP/TCP6))	DCE RPC および SMB	DCE RPC エンドポイントマッパー (ポート 135 TCP/TCP6) による要求に応答する
Identity Management 信頼コントローラーにおけるポート 88 (TCP/TCP6 および UDP/UDP6)、464 (TCP/TCP6 and UDP/UDP6)、および 749 (TCP/TCP6) へのリクエスト	Kerberos	Kerberos チケットを取得する、Kerberos パスワードを変更する、Kerberos をリモートで管理する