Red Hat Enterprise Linux 9

RHEL システムと Windows Active Directory を直接統合

RHEL ホストを AD に参加させ、AD のリソースにアクセスする

Last Updated: 2024-06-26

Red Hat Enterprise Linux 9 RHEL システムと Windows Active Directory を直接統合

RHEL ホストを AD に参加させ、AD のリソースにアクセスする

法律上の通知

概要

管理者は、System Security Services Daemon (SSSD) または Samba Winbind サービスを使用して、Red Hat Enterprise Linux (RHEL) ホストを Active Directory (AD) ドメインに参加させ、AD リソースにアクセスできます。または、マネージドサービスアカウント (MSA) を使用して、ドメインを統合せずに AD リソースにアクセスすることもできます。

目次

RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに関するご意見やご感想をお寄せください。また、改善点があればお知らせください。

Jira からのフィードバック送信 (アカウントが必要)

1. Jira の Web サイトにログインします。
2. 上部のナビゲーションバーで **Create** をクリックします。
3. **Summary** フィールドにわかりやすいタイトルを入力します。
4. **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追加してください。
5. ダイアログの下部にある **Create** をクリックします。

第1章 SSSD を使用して RHEL システムを AD に直接接続

RHEL 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 つ目のコンポーネントは SSSD と呼ばれ、中央の ID および認証ソースと相互作用します。2 つ目のコンポーネントは **realmd** と呼ばれ、利用可能なドメインを検出し、SSSD がドメインに接続するように基盤となる RHEL システムサービスを設定します。

本セクションでは、SSSD (System Security Services Daemon) を使用して、RHEL システムを Active Directory (AD) に接続する方法を説明します。

- SSSD を使用した直接統合の概要
- 直接統合でサポートされる Windows プラットフォーム
- AD に直接接続
- AD プロバイダーが動的 DNS 更新を処理する方法
- AD プロバイダーの動的 DNS 設定の変更
- AD プロバイダーが信頼されるドメインを処理する方法
- SSSD を使用した Active Directory サイトの自動検出のオーバーライド
- realm コマンド

1.1. SSSD を使用した直接統合の概要

オフラインのログインを許可するために、SSSD を使用して、ユーザーキャッシュを備えた共通のフレームワークを介して、ユーザーディレクトリーにアクセスして認証および認可を行います。SSSD は高度な設定が可能で、PAM (Pluggable Authentication Module) と NSS (Name Switch Service) の統合と、ローカルユーザーと、中央サーバーから取得した拡張ユーザーデータを保存するデータベースを提供します。SSSD は、RHEL システムを以下のいずれかの ID サーバーに接続するのに推奨されるコンポーネントです。

- Active Directory
- RHEL の ID 管理 (IdM)
- あらゆる汎用 LDAP または Kerberos サーバー

注記

SSSD との直接統合は、デフォルトで 1 つの AD フォレスト内でのみ機能します。

SSSD が AD と Linux システムを直接統合するように設定する最も便利な方法は、**realmd** サービスを使用することです。これにより、呼び出し元はネットワーク認証およびドメインメンバーシップを標準的な方法で設定できます。**realmd** サービスは、アクセス可能なドメインおよびレルムに関する情報を自動的に検出し、ドメインまたはレルムに参加するのに高度な設定を必要としません。

SSSD は、AD との直接統合および間接統合の両方に使用でき、ある統合アプローチから別の統合アプローチに切り替えることができます。直接統合は、RHEL システムを AD 環境に導入する簡単な方法です。ただし、RHEL システムの共有が増えると、デプロイメントは通常、ホストベースのアクセス制御、sudo、SELinux ユーザーマッピングなどの ID 関連のポリシーをより集中管理する必要があります。最初に、ローカル設定ファイルで、RHEL システムのこのような設定を維持できます。ただし、シ

ステムの数が増えると、Red Hat Satellite などのプロビジョニングシステムでは、設定ファイルの配布と管理が簡単になります。直接統合がスケーリングされない場合は、間接統合を検討する必要があります。直接統合 (RHEL クライアントは AD ドメインにあります) から間接統合 (AD と信頼関係がある IdM) への移行の詳細は、Moving RHEL clients from AD domain to IdM Server を参照してください。

重要

IdM が FIPS モードの場合、IdM-AD 統合は機能しません。これは、AD は RC4 または AES HMAC-SHA1 暗号化の使用しかサポートしない一方で、FIPS モードの RHEL 9 は、デフォルトでは AES HMAC-SHA2 しか許可しないためです。RHEL 9 で AES HMAC-SHA1 の使用を有効にするには、**# update-crypto-policies --set FIPS:AD-SUPPORT** と入力してください。

IdM は、より制限の厳しい **FIPS:OSPP** 暗号化ポリシーはサポートしていません。このポリシーは、Common Criteria で評価されたシステムでしか使用できません。

どのタイプの統合がユースケースに適合するかに関する詳細は、直接統合と間接統合を決定するためのガイドライン を参照してください。

関連情報

- man ページの **realm(8)**
- man ページの **sssd-ad(5)**
- man ページの **sssd(8)**

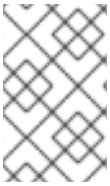
1.2. 直接統合でサポートされる WINDOWS プラットフォーム

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

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

直接統合は、以下のサポート対象のオペレーティングシステムでテストされています。

- Windows Server 2022 (RHEL 9.1 以降)
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2



注記

Windows Server 2019 および Windows Server 2022 では、新しい機能レベルは導入されていません。Windows Server 2019 および Windows Server 2022 で使用される最高の機能レベルは、Windows Server 2016 です。

1.3. AD に直接接続

System Security Services Daemon (SSSD) は、Red Hat Enterprise Linux (RHEL) システムを Active Directory (AD) に接続するために推奨されるコンポーネントです。本セクションでは、SSSD のデフォルトである ID マッピングを使用するか、POSIX 属性を使用して、AD と直接統合する方法を説明します。

- AD との統合オプション: ID マッピングまたは POSIX 属性の使用
- SSSD を使用した AD ドメインの検出および参加
- Active Directory で定義された POSIX 属性を使用した AD への接続
- SSSD を使用したさまざまな AD フォレストでの複数ドメインへの接続

IMPORTANT

システムを AD に参加させる前に、基本的な事前チェック手順: 'adcli'、'realm'、および 'net' コマンドを使用した RHEL による Active Directory への参加 の手順に従って、システムが正しく設定されていることを確認してください。

1.3.1. AD との統合オプション: ID マッピングまたは POSIX 属性の使用

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

- Linux では、**ユーザー ID** (UID) と **グループ ID** (GID) が使用されます。**基本的なシステム設定** の ユーザーアカウントおよびグループアカウントの管理 を参照してください。Linux の UID および GID は、POSIX 標準に準拠します。
- Windows は、**セキュリティー ID** (SID) を使用します。

重要

RHEL システムを AD に接続すると、AD のユーザー名とパスワードを使用して認証できます。名前の重複が原因で競合が生じ、認証プロセスが中断される可能性があるため、Windows ユーザーと同じ名前の Linux ユーザーを作成しないでください。

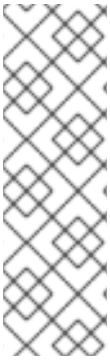
RHEL システムに対して AD ユーザーとして認証するには、UID と GID が割り当てられている必要があります。SSSD は、ID マッピングまたは POSIX 属性のいずれかを使用して AD と統合するオプションを提供します。デフォルトでは、ID マッピングを使用します。

AD ユーザー用に新規 UID および GID を自動的に生成

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

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

SSSD を使用した AD ドメインの検出および参加 を参照してください。



注記

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

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

AD で定義されている POSIX 属性の使用

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

上記の ID マッピングを使用すると、SSSD は新しい UID と GID を作成し、AD で定義された値を上書きします。AD 定義の値を維持するには、SSSD で ID マッピングを無効にする必要があります。

Active Directory で定義された POSIX 属性を使用した AD への接続 を参照してください。

1.3.2. SSSD を使用した AD ドメインの検出および参加

この手順に従って、AD ドメインを検出し、SSSD を使用して RHEL システムをそのドメインに接続します。

前提条件

- AD ドメインコントローラーの以下のポートが開いており、RHEL ホストからアクセス可能であることを確認します。

表1.1 SSSD を使用した Linux システムの AD への直接統合に必要なポート

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

サービス	ポート	プロトコル	備考
NTP	123	UDP	任意

- DNS に AD ドメインコントローラーサーバーが使用されていることを確認します。
- 両方のシステムのシステム時刻が同期していることを確認します。これにより、Kerberos が正常に機能できるようになります。

手順

1. 以下のパッケージをインストールします。

```
# dnf install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli krb5-workstation
```

2. 特定のドメインの情報を表示するには、**realm detect** を実行して、検出するドメイン名を追加します。

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

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

注記

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

3. **realm join** コマンドを使用して、ローカルの RHEL システムを設定します。 **realmd** スイートは、必要なすべての設定ファイルを自動的に編集します。たとえば、**ad.example.com** ドメインの場合は、次のコマンドを実行します。

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

検証手順

- 管理者ユーザーなど、AD ユーザーの詳細を表示します。

```
# getent passwd administrator@ad.example.com
administrator@ad.example.com:*:1450400500:1450400513:Administrator:/home/administrator
@ad.example.com:/bin/bash
```

関連情報

- man ページの **realm(8)** を参照してください。
- man ページの **nmcli(1)** を参照してください。

1.3.3. Active Directory で定義された POSIX 属性を使用した AD への接続

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

前提条件

- RHEL ホストの以下のポートが開放され、AD ドメインコントローラーからアクセスできることを確認している。

  表1.2 SSSD を使用した Linux システムの AD への直接統合に必要なポート

サービス	ポート	プロトコル	備考
DNS	53	UDP および TCP	
LDAP	389	UDP および TCP	
Kerberos	88	UDP および TCP	
Kerberos	464	UDP および TCP	パスワードを設定または変更するために、kadmin により使用されます。
LDAP グローバルカタログ	3268	TCP	**id_provider = ad** オプションが使用されている場合
NTP	123	UDP	任意

- DNS に AD ドメインコントローラーサーバーが使用されていることを確認します。
- 両方のシステムのシステム時刻が同期していることを確認します。これにより、Kerberos が正常に機能できるようになります。

手順

1. 以下のパッケージをインストールします。

```
# dnf install realmd oddjob oddjob-mkhomedir sssd adcli krb5-workstation
```

2. **realm join** コマンドに **--automatic-id-mapping=no** オプションを付けて実行して、ローカルの RHEL システムで ID マッピングを無効にします。**realmd** スイートは、必要な設定ファイルをすべて自動的に編集します。たとえば、**ad.example.com** ドメインの場合は、次のコマンドを実行します。

```
# realm join --automatic-id-mapping=no ad.example.com
```

3. ドメインに参加している場合は、SSSD で ID マッピングを手動で無効にできます。
   a. **/etc/sssd/sssd.conf** ファイルを開きます。
   b. AD ドメインセクションで、**ldap_id_mapping = false** 設定を追加します。
   c. SSSD キャッシュを削除します。

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

   d. SSSD を再起動します。

```
systemctl restart sssd
```

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

注記

AD のユーザーに関連する POSIX 属性 (**uidNumber**、**gidNumber**、**unixHomeDirectory**、および **loginShell**) を設定する必要があります。

検証手順

- 管理者ユーザーなど、AD ユーザーの詳細を表示します。

```
# getent passwd administrator@ad.example.com
administrator@ad.example.com:*:10000:10000:Administrator:/home/Administrator:/bin/bash
```

関連情報

- ID マッピングおよび **ldap_id_mapping** パラメーターの詳細は、man ページの **sssd-ldap(8)** を参照してください。

1.3.4. SSSD を使用したさまざまな AD フォレストでの複数ドメインへの接続

Active Directory (AD) Managed Service Account (MSA) を使用して、信頼関係のないさまざまなフォレストの AD ドメインにアクセスできます。

Accessing AD with a Managed Service Account を参照してください。

1.4. AD プロバイダーが動的 DNS 更新を処理する方法

Active Directory (AD) は、アクティブではないレコードをタイムアウト (**aging**) および削除 (**scavenging**) して、DNS レコードをアクティブに管理します。

デフォルトでは、SSSD サービスは、RHEL クライアントの DNS レコードを以下の間隔で更新します。

- アイデンティティープロバイダーがオンラインになるタイミング。
- RHEL システムが再起動したタイミング。
- **/etc/sssd/sssd.conf** 設定ファイルの **dyndns_refresh_interval** オプションで指定される間隔。デフォルト値は **86400** 秒 (24 時間) です。

注記

dyndns_refresh_interval オプションを DHCP リースと同じ間隔に設定すると、IP リースの更新後に DNS レコードを更新できます。

SSSD は、Kerberos/GSSAPI for DNS (GSS-TSIG) を使用して動的 DNS 更新を AD サーバーに送信します。そのため、必要な操作は、AD へのセキュアな接続を有効にするだけです。

関連情報

- man ページの **sssd-ad(5)**

1.5. AD プロバイダーの動的 DNS 設定の変更

System Security Services Daemon (SSSD) サービスは、AD 環境に参加している Red Hat Enterprise Linux (RHEL) クライアントの DNS レコードをデフォルトの間隔で更新します。次の手順で、これらの間隔を調整します。

前提条件

- RHEL ホストが SSSD サービスを使用して Active Directory 環境に追加している。
- **/etc/sssd/sssd.conf** 設定ファイルを編集するには、**root** パーミッションが必要です。

手順

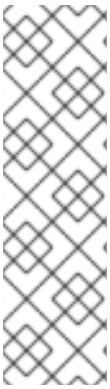
1. テキストエディターで **/etc/sssd/sssd.conf** 設定ファイルを開きます。
2. AD ドメインの **[domain]** セクションに以下のオプションを追加して、DNS レコードの更新間隔を 12 時間に設定し、PTR レコードの更新を無効にして DNS レコード Time To Live (TTL) を 1 時間に設定します。

```
[domain/ad.example.com]
id_provider = ad
...
dyndns_refresh_interval = 43200
dyndns_update_ptr = false
dyndns_ttl = 3600
```

3. **/etc/sssd/sssd.conf** 設定ファイルを保存して閉じます。

4. SSSD サービスを再起動して、設定の変更を読み込みます。

```
[root@client ~]# systemctl restart sssd
```



注記

sssd.conf ファイルの **dyndns_update** オプションを **false** に設定すると、動的 DNS 更新を無効にできます。

```
[domain/ad.example.com]
id_provider = ad
...

dyndns_update = false
```

関連情報

- AD プロバイダーが動的 DNS 更新を処理する方法
- man ページの **の sssd-ad(5)**

1.6. AD プロバイダーが信頼されるドメインを処理する方法

/etc/sssd/sssd.conf 設定ファイルで **id_provider = ad** オプションを設定すると、SSSD は信頼できるドメインを次のように処理します。

- SSSD は、AD フォレストのドメインを 1 つだけサポートします。SSSD が複数のフォレストから複数のドメインにアクセスする必要がある場合は、SSSD の代わりに信頼 (推奨) または **winbindd** サービスで IPA を使用することを検討してください。
- デフォルトでは、SSSD はフォレスト内のすべてのドメインを検出し、信頼されるドメイン内のオブジェクトの要求が到達すると、SSSD はこれを解決しようとします。
  信頼できるドメインに到達できない、または地理的に離れているために遅くなる場合は、**/etc/sssd/sssd.conf** に **ad_enabled_domains** パラメーターを設定して、どの信頼ドメインから SSSD がオブジェクトを解決するかを制限できます。
- デフォルトでは、完全修飾ユーザー名を使用して信頼されるドメインのユーザーを解決する必要があります。

関連情報

- man ページの **sssd.conf(5)**

1.7. SSSD を使用した ACTIVE DIRECTORY サイトの自動検出のオーバーライド

Active Directory (AD) フォレストは非常に大きくなる可能性があり、多数の異なるドメインコントローラー、ドメイン、子ドメイン、および物理サイトがあります。AD は **サイト** の概念を使用して、ドメインコントローラーの物理的な場所を特定します。これにより、クライアントが地理的に最も近いドメインコントローラーに接続できるため、クライアントのパフォーマンスが向上します。

本セクションでは、SSSD が自動検出を使用して接続先である AD サイトを見つけ、自動検出を上書きし、サイトを手動で指定する方法を説明します。

1.7.1. SSSD が AD サイトの自動検出を処理する方法

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

1. SSSD は SRV クエリーを実行して、ドメイン内のドメインコントローラー (DC) を検索します。SSSD は、SSSD 設定ファイルの **dns_discovery_domain** オプションまたは **ad_domain** オプションから検出ドメインを読み取ります。

2. SSSD は Connection-Less LDAP (CLDAP) を 3 つのバッチでこの DC に ping し、多数の DC に ping 送信しないようにし、到達不可能な DC のタイムアウトを回避します。SSSD がこれらのバッチのいずれかでサイトとフォレスト情報を受け取ると、残りのバッチはスキップされます。

3. SSSD は、サイト固有およびバックアップサーバーのリストを作成して保存します。

1.7.2. AD サイトの自動検出の上書き

自動検出プロセスを上書きするには、**/etc/sssd/sssd.conf** ファイルの **[domain]** セクションに **ad_site** オプションを追加して、クライアントが接続する AD サイトを指定します。この例では、クライアントが **ExampleSite** AD サイトに接続するように設定します。

前提条件

- SSSD サービスを使用して、RHEL ホストを Active Directory 環境に追加している。
- **root** ユーザーとして認証できるため、**/etc/sssd/sssd.conf** 設定ファイルを編集できます。

手順

1. テキストエディターで **/etc/sssd/sssd.conf** ファイルを開きます。
2. AD ドメインの **[domain]** セクションに **ad_site** オプションを追加します。

```
[domain/ad.example.com]
id_provider = ad
...
ad_site = ExampleSite
```

3. **/etc/sssd/sssd.conf** 設定ファイルを保存して閉じます。
4. SSSD サービスを再起動して、設定の変更を読み込みます。

```
# systemctl restart sssd
```

1.8. REALM コマンド

realmd システムの主要なタスク領域は、以下の 2 つになります。

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

realmd では、コマンドラインツールの **realm** を使用してコマンドを実行します。ほとんどの **realm** コマンドでは、ユーティリティーが実行するアクションと、アクションを実行するドメインやユーザーアカウントなどのエンティティーを指定する必要があります。

表1.3 realmd コマンド

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

関連情報

- man ページの **realm(8)**

第2章 SAMBA WINBIND を使用して RHEL システムを AD に直接接続

RHEL システムを 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 Samba Winbind は AD のアイデンティティーおよび認証ソースと対話し、もう 1 つのコンポーネントである **realmd** は利用可能なドメインを検出し、基盤となる RHEL システムサービス (この場合は Samba Winbind) が AD ドメインに接続するように設定します。

本セクションでは、Samba Winbind を使用して RHEL システムを Active Directory (AD) に接続する方法を説明します。

- Samba Winbind を使用した直接統合の概要
- 直接統合でサポートされる Windows プラットフォーム
- RHEL システムの AD ドメインへの参加
- realm コマンド

2.1. SAMBA WINBIND を使用した直接統合の概要

Samba Winbind は、Linux システムで Windows クライアントをエミュレートし、AD サーバーと通信します。

realmd サービスを使用すると、以下を実行して Samba Winbind を設定できます。

- ネットワーク認証およびドメインメンバーシップの標準的な設定。
- アクセス可能なドメインおよびレルムに関する情報を自動的に検出します。
- ドメインまたはレルムに参加するために高度な設定を必要としません。

以下の点に留意してください。

- マルチフォレストの AD 設定における Winbind との直接統合は、双方向の信頼が必要になります。
- **idmap_ad** プラグインがリモートフォレストユーザーを正常に処理するには、リモートフォレストがローカルフォレストを信頼する必要があります。

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

winbindd を使用すると、追加のソフトウェアをインストールしなくてもディレクトリーとプリンターを共有する設定が強化されます。詳細は、さまざまな種類のサーバーのデプロイメントの Samba をサーバーとして使用 を参照してください。

関連情報

- man ページの **realmd** を参照してください。
- man ページの **winbindd** を参照してください。

2.2. 直接統合でサポートされる WINDOWS プラットフォーム

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

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

直接統合は、以下のサポート対象のオペレーティングシステムでテストされています。

- Windows Server 2022 (RHEL 9.1 以降)
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

注記

Windows Server 2019 および Windows Server 2022 では、新しい機能レベルは導入されていません。Windows Server 2019 および Windows Server 2022 で使用される最高の機能レベルは、Windows Server 2016 です。

2.3. RHEL システムの AD ドメインへの参加

Samba Winbind は、Red Hat Enterprise Linux (RHEL) システムを Active Directory (AD) に接続するための System Security Services Daemon (SSSD) の代替手段です。**realmd** を使用して Samba Winbind を設定することで、RHEL システムを AD ドメインに参加させることができます。

手順

1. AD で Kerberos 認証に非推奨の RC4 暗号化タイプが必要な場合は、RHEL でこの暗号のサポートを有効にします。

```
# update-crypto-policies --set DEFAULT:AD-SUPPORT
```

2. 以下のパッケージをインストールします。

```
# dnf install realmd oddjob-mkhomedir oddjob samba-winbind-clients \
      samba-winbind samba-common-tools samba-winbind-krb5-locator
```

3. ドメインメンバーでディレクトリーまたはプリンターを共有するには、**samba** パッケージをインストールします。

```
# dnf install samba
```

4. 既存の Samba 設定ファイル **/etc/samba/smb.conf** をバックアップします。

```
# mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
```

5. ドメインに参加します。たとえば、ドメイン **ad.example.com** に参加するには、以下のコマンドを実行します。

```
# realm join --membership-software=samba --client-software=winbind ad.example.com
```

上記のコマンドを使用すると、**realm** ユーティリティーが自動的に以下を実行します。

- **ad.example.com** ドメインのメンバーシップに **/etc/samba/smb.conf** ファイルを作成します。
- ユーザーおよびグループの検索用の **winbind** モジュールを、**/etc/nsswitch.conf** ファイルに追加します。
- **/etc/pam.d/** ディレクトリーの PAM (プラグ可能な認証モジュール) 設定ファイルを更新します。
- **winbind** サービスを起動し、システムの起動時にサービスを起動できるようにします。

6. 必要に応じて、**/etc/samba/smb.conf** ファイルの別の ID マッピングバックエンド、またはカスタマイズした ID マッピングを設定します。

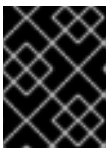
詳細は、SambaID マッピングの理解と設定 を参照してください。

1. **/etc/krb5.conf** ファイルを編集し、以下のセクションを追加します。

```
[plugins]
  localauth = {
    module = winbind:/usr/lib64/samba/krb5/winbind_krb5_localauth.so
    enable_only = winbind
  }
```

2. **winbind** サービスが稼働していることを確認します。

```
# systemctl status winbind
...
  Active: active (running) since Tue 2018-11-06 19:10:40 CET; 15s ago
```



重要

Samba がドメインのユーザーおよびグループの情報をクエリーできるようにするには、**smb** を起動する前に **winbind** サービスを実行する必要があります。

3. **samba** パッケージをインストールしてディレクトリーおよびプリンターを共有している場合は、**smb** サービスを有効化して開始します。

```
# systemctl enable --now smb
```

検証手順

1. AD ドメインの AD 管理者アカウントなど、AD ユーザーの詳細を表示します。

```
# getent passwd "AD\administrator"
AD\administrator:*:10000:10000::/home/administrator@AD:/bin/bash
```

2. AD ドメイン内のドメインユーザーグループのメンバーをクエリーします。

```
# getent group "AD\Domain Users"
  AD\domain users:x:10000:user1,user2
```

3. オプションで、ファイルやディレクトリーに権限を設定する際に、ドメインのユーザーおよびグループを使用できることを確認します。たとえば、**/srv/samba/example.txt** ファイルの所有者を **AD\administrator** に設定し、グループを **AD\Domain Users** に設定するには、以下のコマンドを実行します。

```
# chown "AD\administrator":"AD\Domain Users" /srv/samba/example.txt
```

4. Kerberos 認証が期待どおりに機能することを確認します。

   a. AD ドメインメンバーで、**administrator@AD.EXAMPLE.COM** プリンシパルのチケットを取得します。

```
# kinit administrator@AD.EXAMPLE.COM
```

   b. キャッシュされた Kerberos チケットを表示します。

```
# klist
Ticket cache: KCM:0
Default principal: administrator@AD.EXAMPLE.COM

Valid starting       Expires              Service principal
01.11.2018 10:00:00  01.11.2018 20:00:00
krbtgt/AD.EXAMPLE.COM@AD.EXAMPLE.COM
        renew until 08.11.2018 05:00:00
```

5. 利用可能なドメインの表示:

```
# wbinfo --all-domains
BUILTIN
SAMBA-SERVER
AD
```

関連情報

- 非推奨の RC4 暗号化を使用しない場合は、AD で AES 暗号化タイプを有効にすることができます。詳細は、以下を参照してください。
- GPO を使用した Active Directory で AES 暗号化タイプの有効化
- **realm(8)** man ページ

2.4. REALM コマンド

realmd システムの主要なタスク領域は、以下の 2 つになります。

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

realmd では、コマンドラインツールの **realm** を使用してコマンドを実行します。ほとんどの **realm** コマンドでは、ユーティリティーが実行するアクションと、アクションを実行するドメインやユーザーアカウントなどのエンティティーを指定する必要があります。

表2.1 realmd コマンド

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

関連情報

- man ページの **realm(8)**

第3章 RHEL システムロールを使用した RHEL システムと AD の直接統合

ad_integration システムロールを使用すると、Red Hat Ansible Automation Platform を使用して RHEL システムと Active Directory (AD) の直接統合を自動化できます。

3.1. AD_INTEGRATION RHEL システムロール

ad_integration システムロールを使用すると、RHEL システムを Active Directory (AD) に直接接続できます。

ロールは次のコンポーネントを使用します。

- 中央の ID および認証ソースと対話するための SSSD
- 使用可能な AD ドメインを検出し、基盤となる RHEL システムサービス (この場合は SSSD) を設定して、選択した AD ドメインに接続する **realmd**

注記

ad_integration ロールは、Identity Management (IdM) 環境を使用せずに直接 AD 統合を使用するデプロイメント用です。IdM 環境の場合は、**ansible-freeipa** ロールを使用します。

関連情報

- **/usr/share/ansible/roles/rhel-system-roles.ad_integration/README.md** ファイル
- **/usr/share/doc/rhel-system-roles/ad_integration/** ディレクトリー
- SSSD を使用して RHEL システムを AD に直接接続

第4章 AD への直接接続の管理

System Security Services Daemon (SSSD) または Samba Winbind を使用して、Red Hat Enterprise Linux (RHEL) システムを Active Directory (AD) に接続できます。このセクションでは、RHEL システムがすでに AD クライアントとして設定されている場合に、AD への接続を変更および管理する方法について説明します。

前提条件

- SSSD または Samba Winbind を使用して、RHEL システムを Active Directory ドメインに接続している。

4.1. デフォルトの KERBEROS ホストのキータブの更新間隔を変更

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

デフォルトの更新間隔は 30 日です。デフォルトを変更するには、以下の手順に従います。

手順

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

```
ad_maximum_machine_account_password_age = value_in_days
```

2. SSSD を再起動します。

```
# systemctl restart sssd
```

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

関連情報

- **adcli(8)**
- **sssd.conf(5)**
- SSSD サービスが 'Failed to initialize credentials using keytab [MEMORY:/etc/krb5.keytab]: Preauthentication failed.' というエラーで失敗します。

4.2. AD ドメインからの RHEL システムの削除

Active Directory (AD) に直接統合されている Red Hat Enterprise Linux (RHEL) システムを AD ドメインから直接削除するするには、次の手順に従います。

前提条件

- System Security Services Daemon (SSSD) または Samba Winbind を使用して、RHEL システムを AD に接続しました。

手順

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

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

注記

クライアントがドメインを離れると、AD はアカウントを削除せず、ローカルクライアント設定のみを削除します。AD アカウントを削除するには、**--remove** オプションを指定してコマンドを実行します。最初は認証情報なしで接続を試行しますが、有効な Kerberos チケットを持っていない場合は、ユーザーパスワードの入力を求められます。Active Directory からアカウントを削除する権限が必要です。

2. **realm leave** コマンドに **-U** オプションを付けて実行し、システムを ID ドメインから削除する別のユーザーを指定します。
デフォルトでは、**realm leave** コマンドはデフォルトの管理者として実行されます。AD の場合は、管理者アカウントは **Administrator** と呼ばれます。ドメインに参加するために別のユーザーを使用していた場合は、そのユーザーとして削除を実行しないといけない場合があります。

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

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

検証手順

- ドメインが設定されていないことを確認します。

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

関連情報

- man ページの **realm(8)** を参照してください。

4.3. SSSD でドメイン解決順序を設定して、AD ユーザーの短縮名を解決する手順

デフォルトでは、**ad_username@ad.example.com** および **group@ad.example.com** など完全修飾ユーザー名を指定して、SSSD サービスで AD に接続された RHEL ホスト上にある Active Directory (AD) ユーザーおよびグループを解決する必要があります。

この手順では、SSSD 設定でドメイン解決の順序を設定し、**ad_username** などの短縮名を使用して AD ユーザーおよびグループを解決できるようにします。この設定例では、以下の順序でユーザーおよびグループを検索します。

1. Active Directory (AD) 子ドメイン **subdomain2.ad.example.com**
2. AD 子ドメイン **subdomain1.ad.example.com**
3. AD root ドメイン **ad.example.com**

前提条件

- SSSD サービスを使用して、RHEL ホストを直接 AD に接続している。

手順

1. テキストエディターで **/etc/sssd/sssd.conf** ファイルを開きます。
2. このファイルの **[sssd]** セクションに **domain_resolution_order** オプションを設定します。

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

3. ファイルを保存してから閉じます。
4. SSSD サービスを再起動して、新しい設定を読み込みます。

```
[root@ad-client ~]# systemctl restart sssd
```

検証手順

- 短縮名だけを使用して、最初のドメインからユーザー情報を取得できることを確認します。

```
[root@ad-client ~]# id <user_from_subdomain2>
uid=1916901142(user_from_subdomain2) gid=1916900513(domain users)
groups=1916900513(domain users)
```

4.4. ドメインユーザーのログインパーミッションの管理

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

ドメインがクライアント側のアクセス制御を適用する場合は、**realmd** を使用して、そのドメインのユーザーの基本的なアクセスルールである allow または deny を設定できます。

注記

アクセスルールは、システムにあるすべてのサービスへのアクセスを許可または拒否します。特定のシステムリソースまたはドメインに、より具体的なアクセスルールを設定する必要があります。

4.4.1. ドメイン内でユーザーのアクセス権を有効化

デフォルトでは、Active Directory (AD) ユーザーのログインポリシーは AD ドメイン自体で定義されています。このデフォルトの動作をオーバーライドし、AD ドメイン内のユーザーがアクセスできるように RHEL ホストを設定するには、次の手順に従います。

重要

デフォルトですべてへのアクセスを許可し、レルム許可 **-x** を使用して特定のユーザーにのみアクセスを拒否することは推奨しません。Red Hat では、代わりに、すべてのユーザーに対してデフォルトのアクセス禁止ポリシーを維持し、レルム許可を使用して選択したユーザーのアクセスのみを許可することが推奨されます。

前提条件

- RHEL システムが Active Directory ドメインのメンバーである。

手順

1. すべてのユーザーにアクセス権を付与します。

```
# realm permit --all
```

2. 特定のユーザーにアクセス権を付与します。

```
$ realm permit aduser01@example.com
$ realm permit 'AD.EXAMPLE.COM\aduser01'
```

現在、アクセスを許可できるのはプライマリードメインのユーザーのみで、信頼できるドメインのユーザーには許可できません。これは、ユーザーログインにドメイン名を含める必要があり、SSSD は、現在、**realmd** に利用可能な子ドメインに関する情報を提供できないためです。

検証手順

1. SSH を使用して、**aduser01@example.com** ユーザーとしてサーバーにログインします。

```
$ ssh aduser01@example.com@server_name
[aduser01@example.com@server_name ~]$
```

2. ssh コマンドをもう一度使用して、**aduser02@example.com** ユーザーと同じサーバーにアクセスします。

```
$ ssh aduser02@example.com@server_name
Authentication failed.
```

aduser02@example.com ユーザーがシステムへのアクセスを拒否する方法に注目してください。**aduser01@example.com** ユーザーにのみ、システムにログインするパーミッションを付与してい

ます。指定したログインポリシーが原因で、その Active Directory ドメインの他のユーザーはすべて拒否されます。

注記

sssd.conf ファイルで **use_fully_qualified_names** を true に設定すると、すべての要求で完全修飾ドメイン名を使用する必要があります。ただし、**use_fully_qualified_names** を false に設定すると、要求で完全修飾名を使用できますが、出力には簡略化されたバージョンのみが表示されます。

関連情報

- man ページの **realm(8)** を参照してください。

4.4.2. ドメイン内でユーザーのアクセス権を拒否

デフォルトでは、Active Directory (AD) ユーザーのログインポリシーは AD ドメイン自体で定義されています。このデフォルトの動作をオーバーライドし、AD ドメイン内のユーザーへのアクセスを拒否するように RHEL ホストを設定するには、次の手順に従います。

重要

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

前提条件

- RHEL システムが Active Directory ドメインのメンバーである。

手順

1. ドメイン内のすべてのユーザーへのアクセスを拒否します。

```
# realm deny --all
```

このコマンドは、**realm** アカウントがローカルマシンにログインできないようにします。**realm permit** を使用して、ログインを特定アカウントに制限します。

2. ドメインユーザーの **login-policy** が **deny-any-login** に設定されていることを確認します。

```
[root@replica1 ~]# realm list
example.net
  type: kerberos
  realm-name: EXAMPLE.NET
  domain-name: example.net
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
```

```
required-package: sssd
required-package: adcli
required-package: samba-common-tools
login-formats: %U@example.net
login-policy: deny-any-login
```

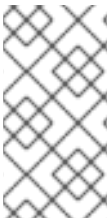
3. **-x** オプションを使用して特定のユーザーへのアクセスを拒否します。

```
$ realm permit -x 'AD.EXAMPLE.COM\aduser02'
```

検証手順

- SSH を使用して、**aduser01@example.net** ユーザーとしてサーバーにログインします。

```
$ ssh aduser01@example.net@server_name
Authentication failed.
```



注記

sssd.conf ファイルで **use_fully_qualified_names** を true に設定すると、すべての要求で完全修飾ドメイン名を使用する必要があります。ただし、**use_fully_qualified_names** を false に設定すると、要求で完全修飾名を使用できますが、出力には簡略化されたバージョンのみが表示されます。

関連情報

- man ページの **realm(8)** を参照してください。

4.5. RHEL でのグループポリシーアクセス制御の適用

Group Policy Object (GPO) は、AD 環境のコンピューターおよびユーザーに適用可能な Microsoft Active Directory (AD) に保存されているアクセス制御設定の集合です。管理者は、AD で GPO を指定することで、AD に参加している Windows クライアントと Red Hat Enterprise Linux (RHEL) ホストの両方が許可するログインポリシーを定義できます。

以下のセクションでは、環境で GPO を管理する方法を説明します。

- SSSD が GPO アクセス制御ルールを解釈する方法
- SSSD がサポートする GPO 設定のリスト
- GPO 強制を制御する SSSD オプションのリスト
- GPO アクセス制御モードの変更
- RHEL ホストの GPO の作成と設定

4.5.1. SSSD が GPO アクセス制御ルールを解釈する方法

デフォルトでは、SSSD は Active Directory (AD) ドメインコントローラーからグループポリシーオブジェクト (GPO) を取得し、ユーザーが AD に参加している特定の RHEL ホストにログインできるかどうかを判断します。

SSSD は AD **Windows Logon Rights** を Pluggable Authentication Module (PAM) サービス名にマッピングし、GNU/Linux 環境でこれらのパーミッションを強制します。

AD 管理者として、**セキュリティーフィルター**にリストすることで、GPO ルールのスコープを特定のユーザー、グループ、またはホストに制限できます。

ホストによるフィルタリングの制限

SSSD の古いバージョンは、AD GPO セキュリティーフィルター内のホストを評価しません。

- **RHEL 8.3.0 以降:** SSSD は、セキュリティーフィルター内のユーザー、グループ、およびホストをサポートします。
- **8.3.0 よりも古い RHEL バージョン:** SSSD はホストエントリーを無視し、セキュリティーフィルターでユーザーおよびグループのみをサポートします。
  SSSD が GPO ベースのアクセス制御を特定のホストに適用するようにするには、AD ドメインで新しい組織単位 (OU) を作成し、システムを新しい OU に移動してから GPO をこの OU にリンクします。

グループ別フィルタリングの制限

SSSD は現在、セキュリティー識別子 (SID) **S-1-5-32-544** を持つ **Administrators** など、Active Directory の組み込みグループをサポートしていません。Red Hat は、RHEL ホストを対象とする AD GPO で AD の組み込みグループを使用することを推奨しています。

関連情報

- Windows GPO オプションとそれに対応する SSSD オプションのリストは、SSSD がサポートする GPO 設定のリスト を参照してください。

4.5.2. SSSD がサポートする GPO 設定のリスト

以下の表は、Windows の **グループポリシー管理エディター** で指定される Active Directory GPO オプションに対応する SSSD オプションを示しています。

表4.1 SSSD が取得した GPO アクセス制御オプション

GPO オプション	対応する sssd.conf オプション
ローカルでのログオンの許可 ローカルでのログオンの拒否	**ad_gpo_map_interactive**
リモートデスクトップサービスを介したログオンの許可 リモートデスクトップサービスを介したログオンの拒否	**ad_gpo_map_remote_interactive**
ネットワークからこのコンピューターへのアクセス ネットワークからこのコンピューターへのアクセスを拒否	**ad_gpo_map_network**
バッチジョブとしてのログオンの許可 バッチジョブとしてのログオンの拒否	**ad_gpo_map_batch**

GPO オプション	対応する sssd.conf オプション
サービスとしてのログオンの許可 サービスとしてのログオンの拒否	**ad_gpo_map_service**

関連情報

- GPO オプションにマップする PAM (プラグ可能な認証モジュール) サービスなど、この **sssd.conf** 設定の詳細は、**sssd-ad(5)** の man ページを参照してください。

4.5.3. GPO 強制を制御する SSSD オプションのリスト

次の SSSD オプションを設定して、GPO ルールの範囲を制限できます。

ad_gpo_access_control オプション

/etc/sssd/sssd.conf ファイルに **ad_gpo_access_control** オプションを設定して、GPO ベースのアクセス制御が動作する 3 種類のモードを選択できます。

表4.2 ad_gpo_access_control の値の表

ad_gpo_access_control の値	動作
enforcing	GPO ベースのアクセス制御ルールが評価され、適用されます。 **これは RHEL 8 のデフォルト設定です。**
permissive	GPO ベースのアクセス制御ルールは評価されますが、**強制**されません。**syslog** メッセージは、アクセスが拒否される度に記録されます。これは、RHEL 7 ではデフォルトの設定です。 このモードは、ユーザーがログインを継続できるように、ポリシーの調整をテストするのに適しています。
disabled	GPO ベースのアクセス制御ルールは、評価も強制もされません。

ad_gpo_implicit_deny オプション

ad_gpo_implicit_deny オプションは、デフォルトで **False** に設定されます。このデフォルトの状態では、適用可能な GPO が見つからない場合にユーザーがアクセスが許可されます。このオプションを **True** に設定する場合は、GPO ルールを使用したユーザーアクセスを明示的に許可する必要があります。

この機能を使用してセキュリティーを強化することはできますが、アクセスを意図せずに拒否しないように注意してください。Red Hat は、**ad_gpo_access_control** が **permissive** に設定されている間に、この機能をテストすることを推奨します。

以下の表では、AD サーバー側で定義したログイン権限と **ad_gpo_implicit_deny** の値に基づいてユーザーがアクセスを許可または拒否されるタイミングを表しています。

表4.3 ad_gpo_implicit_deny が False (デフォルト) に設定されているログイン動作

allow-rules	deny-rules	結果
なし	なし	すべてのユーザーが許可
なし	あり	deny-rules でないユーザーのみが許可
あり	なし	allow-rules のユーザーのみを許可
あり	あり	allow-rules のユーザーのみが許可されますが、拒否ルールでは許可されません

表4.4 ad_gpo_implicit_deny が True に設定されているログイン動作

allow-rules	deny-rules	結果
なし	なし	すべてのユーザーを拒否
なし	あり	すべてのユーザーを拒否
あり	なし	allow-rules のユーザーのみを許可
あり	あり	allow-rules のユーザーのみが許可されますが、拒否ルールでは許可されません

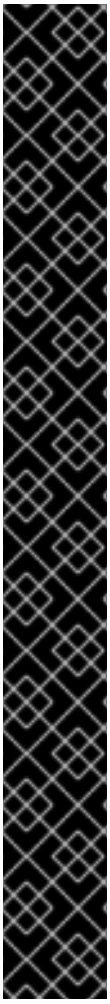
関連情報

- SSSD で GPO 強制モードを変更する手順は、GPO アクセス制御モードの変更 を参照してください。
- さまざまな GPO モードの詳細は、**sssd-ad(5)** man ページの **ad_gpo_access_control** のエントリーを参照してください。

4.5.4. GPO アクセス制御モードの変更

この手順では、GPO ベースのアクセス制御ルールが Active Directory (AD) 環境に参加している RHEL ホストでどのように評価されるかを変更します。

この例では、テスト目的で GPO 操作モードを **Enforcing** (デフォルト) から **Permissive** に変更します。



重要

以下のエラーが表示された場合には、GPO ベースのアクセス制御により Active Directory ユーザーはログインできません。

- **/var/log/secure**:

```
Oct 31 03:00:13 client1 sshd[124914]: pam_sss(sshd:account): Access denied for user aduser1: 6 (Permission denied)
Oct 31 03:00:13 client1 sshd[124914]: Failed password for aduser1 from 127.0.0.1 port 60509 ssh2
Oct 31 03:00:13 client1 sshd[124914]: fatal: Access denied for user aduser1 by PAM account configuration [preauth]
```

- **/var/log/sssd/sssd__example.com_.log**:

```
(Sat Oct 31 03:00:13 2020) [sssd[be[example.com]]] [ad_gpo_perform_hbac_processing] (0x0040): GPO access check failed: [1432158236](Host Access Denied)
(Sat Oct 31 03:00:13 2020) [sssd[be[example.com]]] [ad_gpo_cse_done] (0x0040): HBAC processing failed: [1432158236](Host Access Denied}
(Sat Oct 31 03:00:13 2020) [sssd[be[example.com]]] [ad_gpo_access_done] (0x0040): GPO-based access control failed.
```

これが望ましくない動作の場合は、AD で正しい GPO 設定のトラブルシューティング中に、この手順で説明されているように、**ad_gpo_access_control** を **Permissive** に設定できます。

前提条件

- SSSD を使用して RHEL ホストを AD 環境に追加している。
- **/etc/sssd/sssd.conf** 設定ファイルの編集には、**root** 権限が必要になります。

手順

1. SSSD サービスを停止します。

```
[root@server ~]# systemctl stop sssd
```

2. テキストエディターで **/etc/sssd/sssd.conf** ファイルを開きます。
3. AD ドメインの **domain** セクションで、**ad_gpo_access_control** を **Permissive** に設定します。

```
[domain/example.com]
ad_gpo_access_control=permissive
...
```

4. **/etc/sssd/sssd.conf** ファイルを保存します。
5. SSSD サービスを再起動して、設定の変更を読み込みます。

```
[root@server ~]# systemctl restart sssd
```

関連情報

- さまざまな GPO アクセス制御モードのリストは、GPO の適用を制御する SSSD オプションのリスト を参照してください。

4.5.5. AD GUI での RHEL ホストの GPO の作成および設定

Group Policy Object (GPO) は、AD 環境のコンピューターおよびユーザーに適用可能な Microsoft Active Directory (AD) に保存されているアクセス制御設定の集合です。次の手順では、AD グラフィカルユーザーインターフェイス (GUI) に GPO を作成して、AD ドメインに直接統合されている RHEL ホストへのログオンアクセスを制御します。

前提条件

- SSSD を使用して RHEL ホストを AD 環境に追加している。
- GUI を使用して AD に変更を加えるための AD 管理者権限がある。

手順

1. **Active Directory ユーザーおよびコンピューター** 内で、新しい GPO に関連付ける組織単位 (OU) を作成します。
   a. ドメインを右クリックします。
   b. **New** を選択ます。
   c. **Organizational Unit** を選択します。
2. Active Directory に参加しているときに) RHEL ホストを表す Computer オブジェクトの名前をクリックし、新しい OU にドラッグします。独自の OU に RHEL ホストがあると、GPO はこのホストをターゲットとします。
3. **Group Policy Management Editor** で、作成した OU の GPO を新規作成します。
   a. **Forest** をデプロイメントします。
   b. **Domain** をデプロイメントします。
   c. ドメインをデプロイメントします。
   d. 新しい OU をダブルクリックします。
   e. **Create a GPO in this domain** を選択します。
4. **Allow SSH access** または **Allow Console/GUI access** など、新規 GPO の名前を指定して **OK** をクリックします。
5. 新規 GPO を編集します。
   a. **Group Policy Management** エディター内で OU を選択します。
   b. 右クリックして **Edit** を選択します。
   c. **User Queuing Assignment** を選択します。
   d. **Computer Configuration** を選択します

e. **Policies** を選択します。

f. **Windows Settings** を選択します。

g. **セキュリティー設定** を選択します。

h. **Local Policies** を選択します。

i. **User Queuing Assignment** を選択します。

6. ログインパーミッションを割り当てます。

a. **Allow log on locally** をダブルクリックしてローカルコンソール/GUI アクセスを付与します。

b. **Allow log on through Remote Desktop Services** をダブルクリックして、SSH アクセスを付与します。

7. これらのポリシーのいずれかにアクセスするユーザーをポリシー自体に追加します。

a. **Add User or Group** をクリックします。

b. 空白フィールドにユーザー名を入力します。

c. **OK** をクリックします。

関連情報

- Group Policy Objects の詳細は、Microsoft ドキュメントの Group Policy Objects を参照してください。

4.5.6. 関連情報

- RHEL ホストを Active Directory 環境にジョインする方法は、SSSD を使用した RHEL システムを AD に直接接続 を参照してください。

第5章 MANAGED SERVICE ACCOUNT を使用した AD へのアクセス

Active Directory (AD) Managed Service Accounts (MSA) を使用すると、特定のコンピューターに対応するアカウントを AD で作成できます。MSA を使用すると、RHEL ホストを AD ドメインに参加させずに、AD リソースに特定のユーザープリンシパルとして接続できます。

このセクションでは、以下のトピックについて説明します。

- Managed Service Account の利点
- RHEL ホスト用の Managed Service Account の設定
- Managed Service Account のパスワードの更新
- Managed Service Account の仕様
- adcli create-msa コマンドのオプション

5.1. MANAGED SERVICE ACCOUNT の利点

RHEL ホストが Active Directory (AD) ドメインに参加せずにこれにアクセスできるようにする場合は、Managed Service Account (MSA) を使用してそのドメインにアクセスできます。MSA は、特定のコンピューターに対応する AD のアカウントです。これを使用すると、特定のユーザープリンシパルとして AD リソースに接続できます。

たとえば、AD ドメイン **production.example.com** が、**lab.example.com** AD ドメインと一方向の信頼関係を持つ場合は、以下の条件が適用されます。

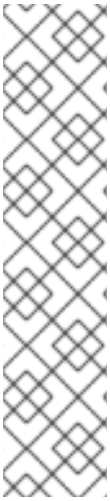
- **lab** ドメインは、**production** ドメインのユーザーとホストを信頼します。
- **production** ドメインは、**lab** ドメインのユーザーとホストを **信頼しません**。

つまり、**client.lab.example.com** などの **lab** ドメインに参加しているホストは、信頼を介して **production** ドメインからリソースにアクセスできないことを意味します。

client.lab.example.com ホストの例外を作成する場合は、**adcli** ユーティリティーを使用して、**production.example.com** ドメイン内の **client** ホストの MSA を作成できます。MSA の Kerberos プリンシパルを使用して認証することにより、**client** ホストから **production** ドメインで安全な LDAP 検索を実行できます。

5.2. RHEL ホスト用の MANAGED SERVICE ACCOUNT の設定

この手順では、**lab.example.com** Active Directory (AD) ドメインからホスト用の MSA (Managed Service Account) を作成し、**production.example.com** AD ドメインにアクセスして認証できるように SSSD を設定します。



注記

RHEL ホストから AD リソースにアクセスする必要がある場合、Red Hat では、**realm** コマンドを使用して RHEL ホストを AD ドメインに参加させることを推奨しています。Connecting RHEL systems directly to AD using SSSD を参照してください。

以下の条件のいずれかが当てはまる場合に限り、この手順を実行します。

- RHEL ホストを AD ドメインに参加させることはできませんが、AD でそのホストのアカウントを作成する必要があります。
- RHEL ホストを AD ドメインに参加させており、一方向の信頼など、参加しているドメインのホストの認証情報が無効な別の AD ドメインにアクセスする必要があります。

前提条件

- RHEL ホストの以下のポートが開放され、AD ドメインコントローラーからアクセスできることを確認している。

サービス	ポート	プロトコル
DNS	53	TCP、UDP
LDAP	389	TCP、UDP
LDAPS (オプション)	636	TCP、UDP
Kerberos	88	TCP、UDP

- **production.example.com** ドメインに MSA を作成する権限を持つ AD 管理者のパスワードがある。
- **adcli** コマンドを実行し、**/etc/sssd/sssd.conf** 設定ファイルを変更するために必要な root 権限がある。
- **(任意) klist** 診断ユーティリティーを含む **krb5-workstation** パッケージがインストールされている。

手順

1. **production.example.com** AD ドメインにホスト用の MSA を作成します。

```
[root@client ~]# adcli create-msa --domain=production.example.com
```

2. 作成された Kerberos キータブから MSA に関する情報を表示します。MSA の名前を書き留めておきます。

```
[root@client ~]# klist -k /etc/krb5.keytab.production.example.com
Keytab name: FILE:/etc/krb5.keytab.production.example.com
KVNO Principal
```

```
---- ------------------------------------------------------------
   2 CLIENT!S3A$@PRODUCTION.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
   2 CLIENT!S3A$@PRODUCTION.EXAMPLE.COM (aes128-cts-hmac-sha1-96)
```

3. **/etc/sssd/sssd.conf** ファイルを開き、適切な SSSD ドメイン設定を選択して追加します。

   - MSA が**別のフォレストの AD ドメイン** に対応する場合は、**[domain/<name_of_domain>]** という名前の新しいドメインセクションを作成し、MSA とキータブに関する情報を入力します。最も重要なオプションは、**ldap_sasl_authid**、**ldap_krb5_keytab**、および **krb5_keytab** です。

     ```
     [domain/production.example.com]
     ldap_sasl_authid = CLIENT!S3A$@PRODUCTION.EXAMPLE.COM
     ldap_krb5_keytab = /etc/krb5.keytab.production.example.com
     krb5_keytab = /etc/krb5.keytab.production.example.com
     ad_domain = production.example.com
     krb5_realm = PRODUCTION.EXAMPLE.COM
     access_provider = ad
     ...
     ```

   - MSA が**ローカルフォレストの AD ドメイン** に対応する場合は、**[domain/root.example.com/sub-domain.example.com]** 形式で新しいサブドメインセクションを作成し、MSA とキータブに関する情報を入力します。最も重要なオプションは、**ldap_sasl_authid**、**ldap_krb5_keytab**、および **krb5_keytab** です。

     ```
     [domain/ad.example.com/production.example.com]
     ldap_sasl_authid = CLIENT!S3A$@PRODUCTION.EXAMPLE.COM
     ldap_krb5_keytab = /etc/krb5.keytab.production.example.com
     krb5_keytab = /etc/krb5.keytab.production.example.com
     ad_domain = production.example.com
     krb5_realm = PRODUCTION.EXAMPLE.COM
     access_provider = ad
     ...
     ```

検証手順

- MSA として Kerberos TGT (Ticket-granting ticket) を取得できることを確認します。

  ```
  [root@client ~]# kinit -k -t /etc/krb5.keytab.production.example.com 'CLIENT!S3A$'
  [root@client ~]# klist
  Ticket cache: KCM:0:54655
  Default principal: CLIENT!S3A$@PRODUCTION.EXAMPLE.COM

  Valid starting       Expires              Service principal
  11/22/2021 15:48:03  11/23/2021 15:48:03
  krbtgt/PRODUCTION.EXAMPLE.COM@PRODUCTION.EXAMPLE.COM
  ```

- AD で、Managed Service Accounts Organizational Unit (OU) にホストの MSA があることを確認します。

関連情報

- SSSD を使用して RHEL システムを AD に直接接続

5.3. MANAGED SERVICE ACCOUNT のパスワードの更新

Managed Service Accounts (MSA) には、Active Directory (AD) が自動的に管理する複雑なパスワードがあります。デフォルトでは、System Services Security Daemon (SSSD) は、MSA パスワードが 30 日を超えると Kerberos キータブでこれを自動的に更新します。これにより、AD ではパスワードを最新の状態に維持できます。この手順では、MSA のパスワードを手動で更新する方法を説明します。

前提条件

- production.example.com AD ドメインにホストの MSA を作成している。
- **(任意) klist** 診断ユーティリティーを含む **krb5-workstation** パッケージがインストールされている。

手順

1. **(任意)** Kerberos キータブで、MSA の現在の Key Version Number (KVNO) を表示します。現在の KVNO は 2 です。

```
[root@client ~]# klist -k /etc/krb5.keytab.production.example.com
Keytab name: FILE:/etc/krb5.keytab.production.example.com
KVNO Principal
---- --------------------------------------------------------------
   2 CLIENT!S3A$@PRODUCTION.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
   2 CLIENT!S3A$@PRODUCTION.EXAMPLE.COM (aes128-cts-hmac-sha1-96)
```

2. **production.example.com** AD ドメイン内の MSA のパスワードを更新します。

```
[root@client ~]# adcli update --domain=production.example.com --host-
keytab=/etc/krb5.keytab.production.example.com --computer-password-lifetime=0
```

検証手順

- Kerberos キータブで、KVNO が増加していることを確認します。

```
[root@client ~]# klist -k /etc/krb5.keytab.production.example.com
Keytab name: FILE:/etc/krb5.keytab.production.example.com
KVNO Principal
---- --------------------------------------------------------------
   3 CLIENT!S3A$@PRODUCTION.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
   3 CLIENT!S3A$@PRODUCTION.EXAMPLE.COM (aes128-cts-hmac-sha1-96)
```

5.4. MANAGED SERVICE ACCOUNT の仕様

adcli ユーティリティーが作成する MSA (Managed Service Account) の仕様は次のとおりです。

- 追加のサービスプリンシパル名 (SPN) を持つことはできません。
- デフォルトでは、MSA の Kerberos プリンシパルは、**/etc/krb5.keytab.production.example.com** のように、**<default_keytab_location>.<Active_Directory_domain>** という名前の Kerberos キータブに保存されます。
- MSA の名前は 20 文字以内に制限されています。最後の 4 文字は、**!** の文字を区切り文字として使用して、指定した短いホスト名に追加された、数字と大文字および小文字の ASCII 範囲か

らの 3 つのランダムな文字の接尾辞です。たとえば、**myhost** という短い名前のホストは、次の仕様の MSA を受け取ります。

仕様	値
共通名 (CN) 属性	**myhost!A2c**
NetBIOS 名	**myhost!A2c$**
sAMAccountName	**myhost!A2c$**
production.example.com AD ドメイン内の Kerberos プリンシパル	**myhost!A2c$@PRODUCTION.EXAMPLE.COM**

5.5. ADCLI CREATE-MSA コマンドのオプション

adcli ユーティリティーに渡すことができるグローバルオプションのほかに、MSA (Managed Service Accounts) の処理方法を制御する以下のオプションを指定できます。

-N, --computer-name

Active Directory (AD) ドメインで作成される MSA の短縮名 (ドットなし)。名前を指定しない場合、**-host-fqdn** の最初の部分、またはそのデフォルトがランダムな接尾辞とともに使用されます。

-O, --domain-ou=OU=<path_to_OU>

MSA を作成する組織ユニット (OU) の完全な識別名。この値を指定しないと、MSA がデフォルトの場所の **OU=CN=Managed Service Accounts,DC=EXAMPLE,DC=COM** に作成されます。

-H, --host-fqdn=host

ローカルマシンの完全修飾 DNS ドメイン名を上書きします。このオプションを指定しない場合は、ローカルマシンのホスト名が使用されます。

-K, --host-keytab=<path_to_keytab>

MSA 認証情報を保存するホストのキータブのパス。この値を指定しない場合は、デフォルトの場所の **/etc/krb5.keytab** が使用され、**/etc/krb5.keytab.domain.example.com** のように小文字の Active Directory ドメイン名が接尾辞として追加されます。

--use-ldaps

セキュア LDAP (LDAPS) チャネルを介して MSA を作成します。

--verbose

MSA の作成時に、詳細情報を出力します。

--show-details

MSA の作成後に、その MSA に関する情報を出力します。

--show-password

MSA の作成後、MSA パスワードを出力します。