Red Hat Enterprise Linux 9

Identity Management サービスへのアクセス

IdM へのログインとそのサービスの管理

Last Updated: 2024-06-26

Red Hat Enterprise Linux 9 Identity Management サービスへのアクセス

IdM へのログインとそのサービスの管理

法律上の通知

概要

Red Hat Identity Management (IdM) で管理タスクを実行する前に、サービスにログインする必要があります。コマンドラインまたは IdM Web UI を使用してログインする場合は、IdM の認証方法として Kerberos およびワンタイムパスワードを使用できます。

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 コマンドラインから IDENTITY MANAGEMENT へのログイン

Identity Management (IdM) では、Kerberos プロトコルを使用してシングルサインオンに対応します。シングルサインオンとは、ユーザーが正しいユーザー名およびパスワードを一度だけ入力すれば、システムが認証情報を再度求めることなく、IdM サービスにアクセスできるという機能です。

重要

IdM では、ユーザーが、対応する Kerberos プリンシパル名を使用して IdM クライアントマシンのデスクトップ環境にログインすると、SSSD (System Security Services Daemon) が、そのユーザーの TGT (Ticket-Granting Ticket) を自動的に取得します。これは、ログインしてから、**kinit** ユーティリティーを使用して IdM リソースにアクセスする必要がなくなることを意味します。

Kerberos 認証情報キャッシュを削除している場合、または Kerberos TGT の有効期限が切れている場合に IdM リソースにアクセスするには、手動で Kerberos チケットを要求する必要があります。以下のセクションでは、IdM で Kerberos を使用している場合の基本的なユーザー操作を説明します。

1.1. KINIT による IDM への手動ログイン

kinit ユーティリティーを使用して Identity Management (IdM) 環境に対して手動で認証するには、次の手順に従います。**kinit** ユーティリティーは、IdM ユーザーの代わりに Kerberos の TGT (Ticket-Granting Ticket) を取得して、キャッシュに格納します。

注記

この手順は、最初の Kerberos TGT を破棄したか、有効期限が切れている場合にのみ使用します。ローカルマシンに、IdM ユーザーとしてログインすると、IdM に自動的にログインします。これは、ログイン後に IdM リソースにアクセスするのに **kinit** ユーティリティーを使用する必要がないことを示しています。

手順

1. IdM にログインします。

   - ローカルシステムに現在ログインしているユーザーのユーザー名で、(ユーザー名を指定せずに) **kinit** を使用します。たとえば、ローカルシステムにログインしているユーザーが **example_user** の場合は、次のコマンドを実行します。

     ```
     [example_user@server ~]$ kinit
     Password for example_user@EXAMPLE.COM:
     [example_user@server ~]$
     ```

     ローカルユーザーのユーザー名と、IdM のユーザーエントリーが一致しないと、認証に失敗します。

     ```
     [example_user@server ~]$ kinit
     kinit: Client 'example_user@EXAMPLE.COM' not found in Kerberos database while
     getting initial credentials
     ```

- ローカルユーザー名に対応しない Kerberos プリンシパルを使用して、**kinit** ユーティリティーに必要なユーザー名を渡します。たとえば、**admin** ユーザーとしてログインするには、次のコマンドを実行します。

```
[example_user@server ~]$ kinit admin
Password for admin@EXAMPLE.COM:
[example_user@server ~]$
```

2. 必要に応じて、ログインが成功したことを確認するには、**klist** ユーティリティーを使用して、キャッシュした TGT を表示します。以下の例では、キャッシュに **example_user** プリンシパルのチケットが含まれています。これは、このホストでは IdM サービスにアクセスするのは、**example_user** にのみ許可されていることを示しています。

```
$ klist
Ticket cache: KEYRING:persistent:0:0
Default principal: example_user@EXAMPLE.COM

Valid starting       Expires              Service principal
11/10/2019 08:35:45  11/10/2019 18:35:45  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

1.2. アクティブなユーザーの KERBEROS チケットの破棄

ユーザーのアクティブな Kerberos チケットを含む認証情報キャッシュをクリアするには、次の手順に従います。

手順

1. Kerberos チケットを破棄するには、次のコマンドを実行します。

```
[example_user@server ~]$ kdestroy
```

2. 必要に応じて、Kerberos チケットが破棄されたことを確認するには、次のコマンドを実行します。

```
[example_user@server ~]$ klist
klist: Credentials cache keyring 'persistent:0:0' not found
```

1.3. KERBEROS 認証用の外部システムの設定

Identity Management (IdM) ユーザーが Kerberos 認証情報を使用して外部システムから IdM にログインできるように外部システムを設定するには、この手順に従います。

外部システムの Kerberos 認証を有効にすることは、インフラストラクチャーに、複数のレルムまたは重複ドメインが含まれている場合に特に便利です。また、**ipa-client-install** を実行してシステムを IdM ドメインに登録していない場合にも便利です。

IdM ドメインのメンバーではないシステムから IdM への Kerberos 認証を有効にするには、IdM 固有の Kerberos 設定ファイルを外部システムに定義します。

前提条件

- 外部システムに **krb5-workstation** パッケージがインストールされている。

パッケージがインストールされているかどうかを確認するには、次の CLI コマンドを使用します。

```
# dnf list installed krb5-workstation
Installed Packages
krb5-workstation.x86_64    1.16.1-19.el8    @BaseOS
```

手順

1. IdM サーバーから外部システムに **/etc/krb5.conf** ファイルをコピーします。以下に例を示します。

```
# scp /etc/krb5.conf root@externalsystem.example.com:/etc/krb5_ipa.conf
```

警告

外部マシンにある既存の **krb5.conf** ファイルは上書きしないでください。

2. 外部システムで、コピーした IdM の Kerberos 設定ファイルを使用するように、端末セッションを設定します。

```
$ export KRB5_CONFIG=/etc/krb5_ipa.conf
```

KRB5_CONFIG 変数は、ログアウトまで一時的に存在します。ログアウト時に削除されないように、この変数のファイル名を変えてエクスポートします。

3. **/etc/krb5.conf.d/** ディレクトリーの Kerberos 設定部分を、外部システムにコピーします。

外部システムのユーザーが、**kinit** ユーティリティーを使用して IdM サーバーで認証できるようになりました。

1.4. 関連情報

- **krb5.conf(5)** の man ページ
- **kinit(1)** の man ページ
- **klist(1)** の man ページ
- **kdestroy(1)** の man ページ

第2章 IDENTITY MANAGEMENT サービスの表示、開始、および停止

Identity Management (IdM) 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。IdM サーバーでさまざまなサービスが実行していますが、中でも注目すべきは Directory Server、Certificate Authority (CA)、DNS、および Kerberos です。

2.1. IDM サービス

IdM サーバーおよびクライアントにインストールして実行できるサービスには、さまざまなものがあります。

IdM サーバーがホストするサービスのリスト

以下のサービスの多くは、IdM サーバーへのインストールが必須というわけではありません。たとえば、認証局 (CA) や DNS サーバーなどのサービスは、IdM ドメイン内にない外部サーバーにインストールできます。

Kerberos

krb5kdc サービスおよび **kadmin** サービス

IdM は、シングルサインオンに対応する **Kerberos** プロトコルを使用します。Kerberos では、正しいユーザー名とパスワードを一度提示するだけで済み、システムから認証情報を再度求められることなく IdM サービスにアクセスできます。

Kerberos は 2 つの部分に分類されます。

- **krb5kdc** サービス。Kerberos 認証サービスおよびキー配布センター (KDC) デーモンです。
- **kadmin** サービス。Kerberos V5 データベース管理プログラムです。

IdM で Kerberos を使用して認証する方法は、コマンドラインからの Identity Management へのログイン および Web UI で IdM にログイン: Kerberos チケットの使用 を参照してください。

LDAP ディレクトリーサーバー

dirsrv サービス

IdM の **LDAP ディレクトリーサーバー** インスタンスは、 Kerberos、ユーザーアカウント、ホストエントリー、サービス、ポリシー、DNS などの情報をはじめとした、IdM 情報をすべて保存します。LDAP ディレクトリーサーバーインスタンスは、Red Hat Directory Server と同じテクノロジーをベースにしています。ただし、IdM 固有のタスクに合わせて調整されます。

認証局

pki-tomcatd サービス

統合 **認証局 (CA)** は、Red Hat Certificate System と同じテクノロジーをベースにしています。**pki** は、Certificate System サービスにアクセスするコマンドラインインターフェイスです。

必要な証明書をすべて単独で作成して提供する場合は、統合 CA なしでサーバーをインストールすることもできます。

詳細は、CA サービスの計画 を参照してください。

DNS (Domain Name System)

named サービス

IdM は、動的サービス検出に **DNS** を使用します。IdM クライアントのインストールユーティリティーは、DNS からの情報を使用して、クライアントマシンを自動的に設定できます。クライアントを IdM ドメインに登録したら、クライアントは DNS を使用してドメイン内の IdM サーバーおよびサービスを検索します。Red Hat Enterprise Linux の DNS (Domain Name System) プロトコルの **BIND** (Berkeley Internet Name Domain) 実装には、**名前付き** の DNS サーバーが含まれています。 **named-pkcs11** は、PKCS#11 暗号化標準に対するネイティブサポートありで構築された BIND DNS サーバーのバージョンです。

詳細は、DNS サービスとホスト名の計画 を参照してください。

Apache HTTP サーバー

httpd サービス

Apache HTTP Web サーバー には、IdM Web UI があり、認証局とその他の IdM サービスの間の通信も管理します。

Samba / Winbind

SMB サービスおよび **winbind** サービス

Samba は、Red Hat Enterprise Linux に、Common Internet File System (CIFS) プロトコルとも呼ばれる Server Message Block (SMB) プロトコルを実装します。smb サービス経由で SMB プロトコルを使用すると、ファイル共有や共有プリンターなどのサーバーのリソースにアクセスできます。Active Directory (AD) 環境で信頼を設定している場合には、'Winbind' サービスが IdM サーバーと AD サーバー間の通信を管理します。

ワンタイムパスワード (OTP) 認証

ipa-otpd サービス

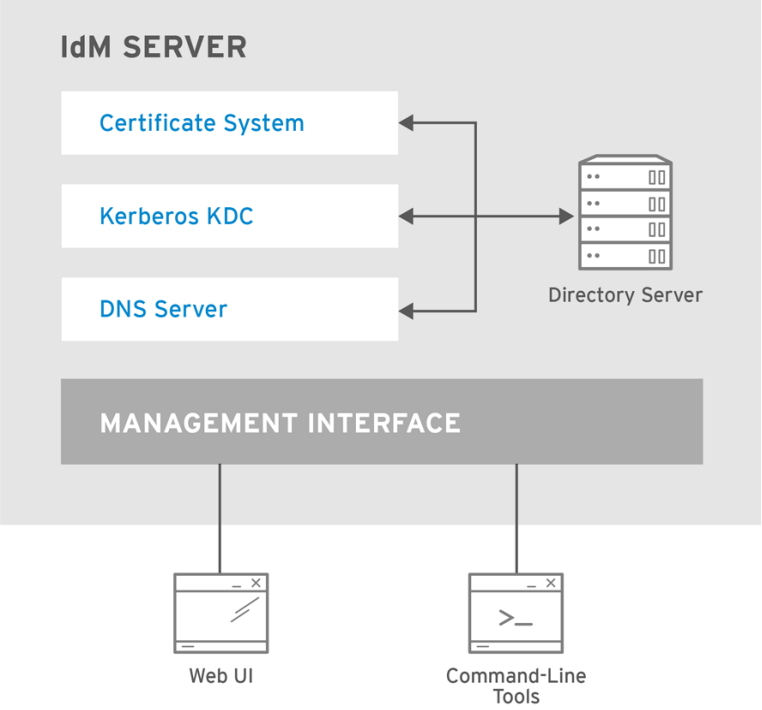
ワンタイムパスワード (OTP) は、2 要素認証の一部として、認証トークンがセッション 1 回だけ使用できるように生成するパスワードです。OTP 認証は、**ipa-otpd** サービスを介して Red Hat Enterprise Linux に実装されています。

詳細は、ワンタイムパスワードを使用した Identity Management Web UI へのログイン を参照してください。

OpenDNSSEC

ipa-dnskeysyncd サービス

OpenDNSSEC は、DNSSEC (DNS Security Extensions) キーおよびゾーンの署名の記録プロセスを自動化する DNS マネージャーです。**ipa-dnskeysyncd** サービスは、IdM Directory Server と OpenDNSSEC との間の同期を管理します。



IdM クライアントがホストするサービスのリスト

- System Security Services Daemon: **sssd** サービス

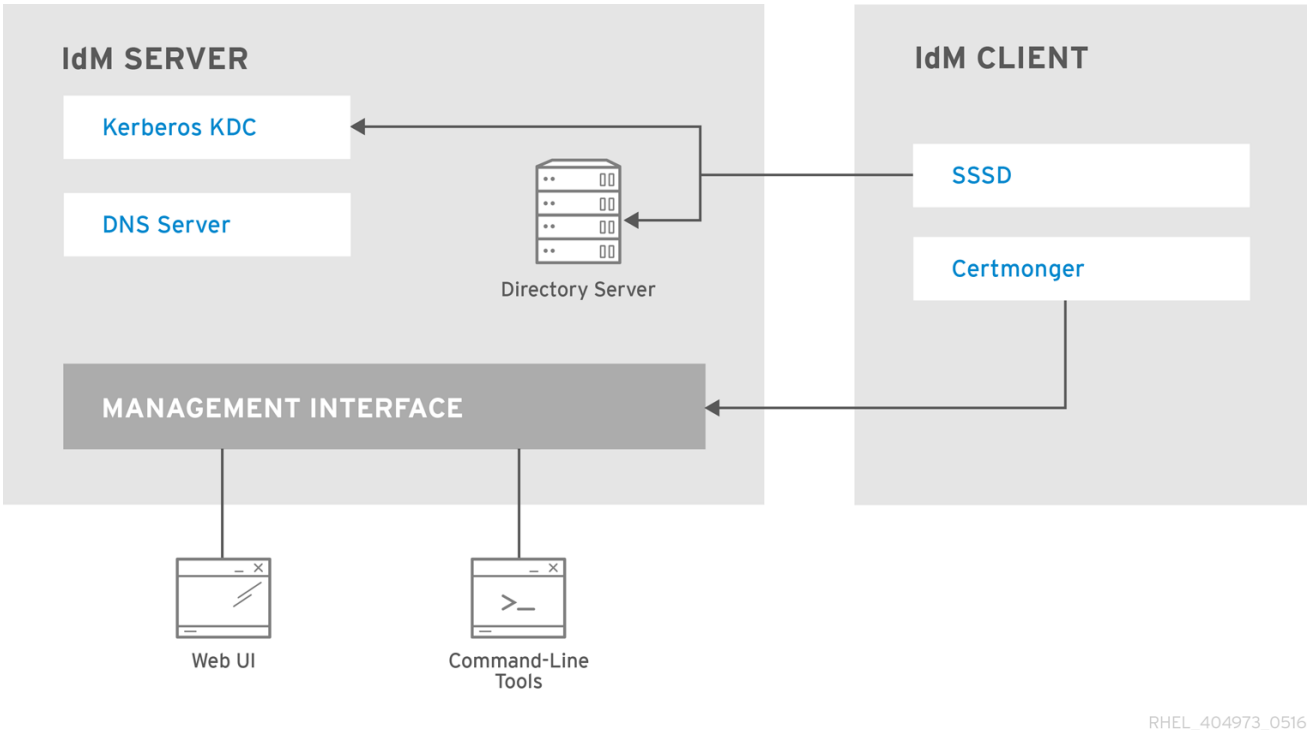
SSSD (**System Security Services Daemon**) は、ユーザー認証およびキャッシュ認証情報を管理するクライアント側のアプリケーションです。キャッシュを使用すると、IdM サーバーが利用できなくなったり、クライアントがオフラインになったりした場合に、ローカルシステムが通常の認証操作を継続できるようになります。

詳細は SSSD とその利点について を参照してください。

- certmonger: **certmonger** サービス

certmonger サービスは、クライアント上の証明書を監視、更新します。このサービスは、システム上のサービスに対して新しい証明書を要求できます。

詳細は、certmonger でサービスの IdM 証明書の取得 を参照してください。



2.2. IDM サービスの状態の表示

IdM サーバーに設定されている IdM サービスの状態を表示するには、**ipactl status** コマンドを実行します。

```
[root@server ~]# ipactl status
Directory Service: RUNNING
krb5kdc Service: RUNNING
kadmin Service: RUNNING
named Service: RUNNING
httpd Service: RUNNING
pki-tomcatd Service: RUNNING
smb Service: RUNNING
winbind Service: RUNNING
ipa-otpd Service: RUNNING
ipa-dnskeysyncd Service: RUNNING
ipa: INFO: The ipactl command was successful
```

サーバーの **ipactl status** コマンドの出力は、IdM 設定により異なります。たとえば、IdM デプロイメントに DNS サーバーが含まれていない場合は、**named** サービスがリストに表示されません。

注記

IdM の Web UI を使用して、特定の IdM サーバーで実行しているすべての IdM サービスの状態を表示することはできません。Kerberos に対応し、複数のサーバーで実行しているサービスは、IdM の Web UI の **Identity → Services** タブで表示できます。

サーバー全体、または個々のサービスのみを起動または停止できます。

IdM サーバー全体を起動、停止、または再起動する場合は、以下を参照してください。

- Identity Management サーバー全体の起動と停止

個々の IdM サービスを起動、停止、または再起動する場合は、以下を参照してください。

- 個々の Identity Management サービスの開始および停止

IdM ソフトウェアのバージョンを表示するには、次を参照してください。

- IdM ソフトウェアのバージョンを表示する方法

2.3. IDENTITY MANAGEMENT サーバー全体の起動と停止

ipa systemd サービスを使用して、IdM サーバー全体を、インストールしたすべてのサービスを停止、起動、または再起動します。**systemctl** ユーティリティーを使用して **ipa** systemd サービスを制御すると、すべてのサービスが適切な順序で停止、開始、または再起動されます。**ipa** systemd サービスは、IdM サービスを起動する前に RHEL IdM 設定もアップグレードし、IdM サービスの管理時に適切な SELinux コンテキストを使用します。**systemctl ipa** コマンドを実行するには、有効な Kerberos チケットは必要ありません。

ipa systemd service コマンド

IdM サーバー全体を起動するには、次のコマンドを実行します。

```
# systemctl start ipa
```

IdM サーバー全体を停止するには、次のコマンドを実行します。

```
# systemctl stop ipa
```

IdM サーバー全体を再起動するには、次のコマンドを実行します。

```
# systemctl restart ipa
```

IdM を設定するすべてのサービスのステータスを表示するには、**ipactl** ユーティリティーを使用します。

```
# ipactl status
```

重要

- IdM サービスは、**ipactl** ユーティリティーで、起動、停止、または再起動しないでください。代わりに **systemctl ipa** コマンドを使用して、予測可能な環境で **ipactl** ユーティリティーを呼び出します。
- **ipactl** コマンドは、IdM の Web UI では使用できません。

2.4. 個々の IDENTITY MANAGEMENT サービスの開始および停止

IdM 設定ファイルを手動で変更することは推奨されていません。ただし、特定の状況では、管理者が特定のサービスを手動で設定する必要があります。このような場合は、**systemctl** ユーティリティーを使用して、個々の IdM サービスを停止、開始、または再開します。

たとえば、その他の IdM サービスを変更せずに、Directory Server の挙動をカスタマイズした場合は、**systemctl** を使用します。

```
# systemctl restart dirsrv@REALM-NAME.service
```

また、Active Directory と IdM の信頼を最初にデプロイする場合は、**/etc/sssd/sssd.conf** ファイルを変更して、以下を追加します。

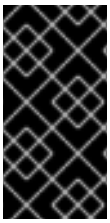
- リモートサーバーのレイテンシーが長い環境で、タイムアウト設定オプションを調整するための特定のパラメーター
- Active Directory サイトのアフィニティーを調整するための特定のパラメーター
- グローバルの IdM 設定では提供されない特定の設定オプションのオーバーライド

/etc/sssd/sssd.conf ファイルに加えた変更を適用する場合は、次のコマンドを実行します。

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

System Security Services Daemon (SSSD) は、設定を自動的に再読み込みまたは再適用しないため、**systemctl restart sssd.service** を実行する必要があります。

変更が、IdM の ID 範囲に影響を及ぼす場合は、サーバーを完全に再起動することが推奨されます。



重要

複数の IdM ドメインサービスを再起動するには、常に **systemctl restart ipa** を使用します。IdM サーバーにインストールされているサービス間での依存関係により、サービスを開始および停止する順番は極めて重要です。**ipa** systemd サービスは、サービスが適切な順序で開始および停止されるようにします。

便利な systemctl コマンド

特定の IdM サービスを開始するには、次のコマンドを実行します。

```
# systemctl start name.service
```

特定の IdM サービスを停止するには、次のコマンドを実行します。

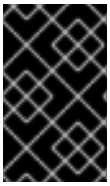
```
# systemctl stop name.service
```

特定の IdM サービスを再開するには、次のコマンドを実行します。

```
# systemctl restart name.service
```

特定の IdM サービスの状態を表示するには、次のコマンドを実行します。

```
# systemctl status name.service
```



重要

IdM の Web UI を使用して、IdM サーバーで実行している個々のサービスを開始または停止することはできません。Web UI で可能なのは、**Identity → Services** に移動してサービスを選択し、Kerberos に対応する設定を修正することです。

関連情報

- Identity Management サーバー全体の起動と停止

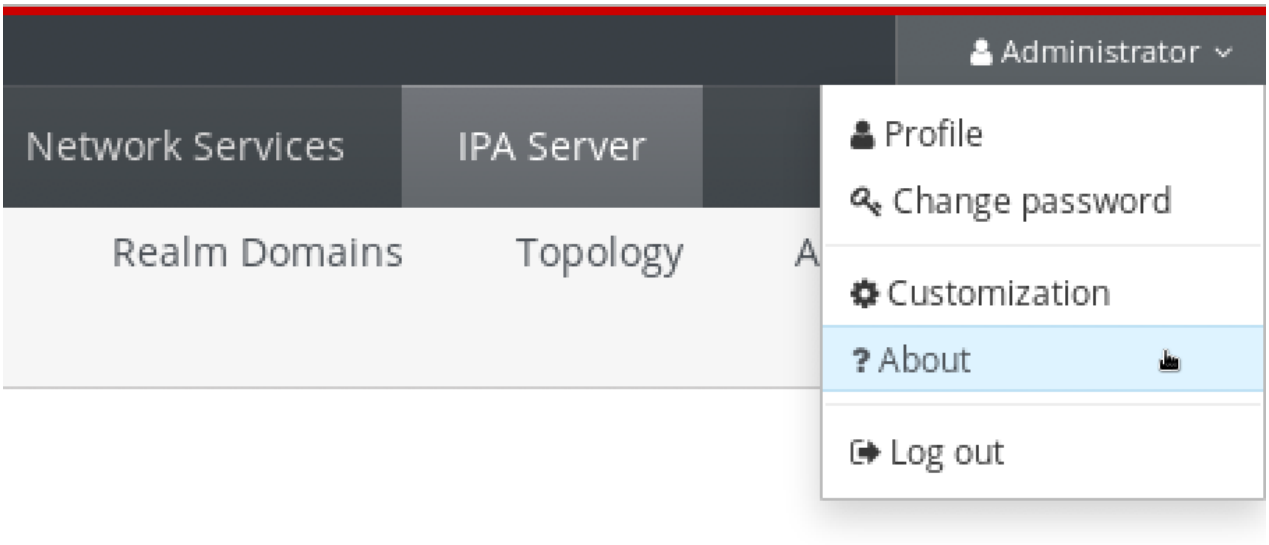
2.5. IDM ソフトウェアのバージョンを表示する方法

IdM バージョン番号は次の方法で表示できます。

- IdM WebUI
- **ipa** コマンド
- **rpm** コマンド

WebUI を介したバージョンの表示

IdM WebUI では、右上のユーザー名メニューから **About** を選択して、ソフトウェアバージョンを表示できます。



ipa コマンドによるバージョンの表示

コマンドラインから、**ipa --version** コマンドを使用します。

```
[root@server ~]# ipa --version
VERSION: 4.8.0, API_VERSION: 2.233
```

rpm コマンドによるバージョンの表示

IdM サービスが適切に動作していない場合は、**rpm** ユーティリティーを使用して、現在インストールされている **ipa-server** パッケージのバージョン番号を確認できます。

```
[root@server ~]# rpm -q ipa-server
ipa-server-4.8.0-11.module+el8.1.0+4247+9f3fd721.x86_64
```

第3章 IDM コマンドラインユーティリティーの概要

Identity Management (IdM) コマンドラインユーティリティーの基本的な使用方法を説明します。

前提条件

- IdM サーバーをインストールしていて、アクセス可能である。
  詳細は、Identity Management のインストール を参照してください。
- IPA コマンドラインインターフェイスを使用する場合は、有効な Kerberos チケットを使用して IdM に対してを認証している。

3.1. IPA コマンドラインインターフェイスとは

IPA コマンドラインインターフェイス (CLI) は、Identity Management (IdM) の管理向けの基本的なコマンドラインインターフェイスです。

新しいユーザーを追加するための **ipa user-add** コマンドなど、IdM を管理するための多くのサブコマンドがサポートされています。

IPA CLI では以下を行うことができます。

- ネットワーク内のユーザー、グループ、ホスト、その他のオブジェクトを追加、管理、または削除する。
- 証明書を管理する。
- エントリーを検索する。
- オブジェクトを表示し、オブジェクトリストを表示する。
- アクセス権を設定する。
- 正しいコマンド構文でヘルプを取得する。

3.2. IPA のヘルプとは

IPA ヘルプは、IdM サーバー用の組み込みドキュメントシステムです。

IPA コマンドラインインターフェイス (CLI) は、読み込んだ IdM プラグインモジュールから、利用可能なヘルプトピックを生成します。IPA ヘルプユーティリティーを使用するには、以下が必要です。

- IdM サーバーがインストールされ、実行している。
- 有効な Kerberos チケットで認証されている。

オプションを指定せずに **ipa help** コマンドを実行すると、基本的なヘルプの使用方法と、最も一般的なコマンドの例が表示されます。

さまざまな **ipa help** のユースケースに対して、次のオプションを使用できます。

```
$ ipa help [TOPIC | COMMAND | topics | commands]
```

- **[]** - 括弧は、すべてのパラメーターが任意であることを示しており、**ipa help** のみを入力すれば、コマンドが実行できます。

- | - パイプ文字は **または** の意味になります。したがって、基本的な **ipa help** コマンドを使用して、**TOPIC**、**COMMAND**、**topics** または **commands** を指定できます。
  - **topics** – コマンド **ipa help topics** を実行して、IPA ヘルプでカバーされている **user**、**cert**、**server** などのトピックのリストを表示できます。
  - **TOPIC** – 大文字の TOPIC は変数になります。したがって、特定のトピック (**ipa help user** など) を指定できます。
  - **commands** – コマンド **ipa help commands** を入力して、**user-add**、**ca-enable**、**server-show** などの IPA ヘルプでカバーされているコマンドのリストを表示できます。
  - **COMMAND** – 大文字の COMMAND は変数になります。したがって、**ipa help user-add** などの特定のコマンドを指定できます。

3.3. IPA ヘルプトピックの使用

次の手順では、コマンドラインインターフェイスで IPA ヘルプを使用する方法について説明します。

手順

1. 端末を開き、IdM サーバーに接続します。
2. ヘルプに記載されているトピックのリストを表示するには、**ipa help topics** を実行します。

```
$ ipa help topics
```

3. トピックの 1 つを選択し、**ipa help [topic_name]** のパターンに従ってコマンドを作成します。**topic_name** 文字列の代わりに、前の手順でリストしたトピックの 1 つを追加します。この例では、**user** トピックを使用します。

```
$ ipa help user
```

4. IPA ヘルプの出力が長すぎるため、テキスト全体を表示できない場合は、以下の構文を使用します。

```
$ ipa help user | less
```

スクロールダウンすれば、ヘルプ全体を表示できます

IPA CLI は、**ユーザー** トピックのヘルプページを表示します。概要を読むと、トピックのコマンドを使用するパターンに関して、多くの例を確認できます。

3.4. IPA HELP コマンドの使用

次の手順では、コマンドラインインターフェイスで IPA help コマンドを作成する方法について説明します。

手順

1. 端末を開き、IdM サーバーに接続します。
2. ヘルプで使用できるコマンドのリストを表示するには、**ipa help commands** コマンドを実行します。

```
$ ipa help commands
```

3. コマンドの1つを選択し、**ipa help <COMMAND>** のパターンに従ってヘルプコマンドを作成します。**<COMMAND>** 文字列の代わりに、前の手順でリストしたコマンドの1つを追加します。

```
$ ipa help user-add
```

関連情報

- **ipa** の man ページ

3.5. IPA コマンドの構造

IPA CLI は、以下のタイプのコマンドを区別します。

- **組み込みコマンド** – 組み込みコマンドはすべて、IdM サーバーで利用できます。
- **プラグインにより提供されたコマンド**

IPA コマンドの構造を使用すると、さまざまなタイプのオブジェクトを管理できます。以下に例を示します。

- ユーザー
- ホスト
- DNS レコード
- 証明書

その他にも多数あります。

このようなほとんどのオブジェクトでは、IPA CLI に、以下を行うためのコマンドが含まれます。

- 追加 (**add**)
- 修正 (**mod**)
- 削除 (**del**)
- 検索 (**find**)
- 表示 (**show**)

コマンドの構造は次のとおりです。

ipa user-add、**ipa user-mod**、**ipa user-del**、**ipa user-find**、**ipa user-show**

ipa host-add、**ipa host-mod**、**ipa host-del**、**ipa host-find**、**ipa host-show**

ipa dnsrecord-add、**ipa dnsrecord-mod**、**ipa dnsrecord-del**、**ipa dnsrecord-find**、**ipa dnrecord-show**

ipa user-add [options] でユーザーを作成できます。**[options]** は任意です。**ipa user-add** コマンドのみを使用する場合、スクリプトは、詳細を1つずつ要求します。

既存のオブジェクトを変更するには、オブジェクトを定義する必要があります。そのため、コマンドには、オブジェクト **ipa user-mod USER_NAME [options]** も含まれます。

3.6. IPA コマンドを使用した IDM へのユーザーアカウントの追加

以下の手順では、コマンドラインを使用して Identity Management (IdM) データベースに新しいユーザーを追加する方法について説明します。

前提条件

- IdM サーバーにユーザーアカウントを追加するには、管理者権限が必要です。

手順

1. 端末を開き、IdM サーバーに接続します。
2. 新しいユーザーを追加するコマンドを入力します。

   ```
   $ ipa user-add
   ```

   このコマンドは、ユーザーアカウントの作成に必要な基本データの提供を求めるスクリプトを実行します。
3. **First name:** フィールドに、新規ユーザーの名前を入力して、**Enter** キーを押します。
4. **Last name:** フィールドに、新規ユーザーの苗字を入力し、**Enter** キーを押します。
5. **User login [suggested user name]:**にユーザー名を入力します。または、提案されたユーザー名を使用する場合は、**Enter** キーを押します。
   ユーザー名は、IdM データベース全体で一意にする必要があります。そのユーザー名がすでに存在するためにエラーが発生した場合は、**ipa user-add** コマンドでそのプロセスを再度実行し、別の一意のユーザー名を使用します。

ユーザー名を追加すると、ユーザーアカウントが IdM データベースに追加され、IPA コマンドラインインターフェイス (CLI) は以下の出力を出力します。

```
----------------------
Added user "euser"
----------------------
User login: euser
First name: Example
Last name: User
Full name: Example User
Display name: Example User
Initials: EU
Home directory: /home/euser
GECOS: Example User
Login shell: /bin/sh
Principal name: euser@IDM.EXAMPLE.COM
Principal alias: euser@IDM.EXAMPLE.COM
Email address: euser@idm.example.com
UID: 427200006
GID: 427200006
```

```
Password: False
Member of groups: ipausers
Kerberos keys available: False
```

注記

デフォルトでは、ユーザーアカウントにユーザーパスワードは設定されていません。ユーザーアカウントの作成中にパスワードを追加するには、次の構文で **ipa user-add** コマンドを使用します。

```
$ ipa user-add --first=Example --last=User --password
```

次に、IPA CLI は、ユーザー名とパスワードを追加または確認するように要求します。

ユーザーがすでに作成されている場合は、**ipa user-mod** コマンドでパスワードを追加できます。

関連情報

- パラメーターの詳細は、**ipa help user-add** コマンドを実行してください。

3.7. IPA コマンドで IDM のユーザーアカウントの変更

各ユーザーアカウントの多くのパラメーターを変更できます。たとえば、新しいパスワードをユーザーに追加できます。

基本的なコマンド構文は **user-add** 構文とは異なります。たとえば、パスワードを追加するなど、変更を実行する既存のユーザーアカウントを定義する必要があるためです。

前提条件

- ユーザーアカウントを変更するには、管理者権限が必要です。

手順

1. 端末を開き、IdM サーバーに接続します。
2. **ipa user-mod** コマンドを入力し、変更するユーザーと、パスワードを追加するための **--password** などのオプションを指定します。

   ```
   $ ipa user-mod euser --password
   ```

   このコマンドは、新しいパスワードを追加できるスクリプトを実行します。
3. 新しいパスワードを入力し、**Enter** キーを押します。

IPA CLI は次の出力を出力します。

```
----------------------
Modified user "euser"
----------------------
User login: euser
First name: Example
Last name: User
```

```
Home directory: /home/euser
Principal name: euser@IDM.EXAMPLE.COM
Principal alias: euser@IDM.EXAMPLE.COM
Email address: euser@idm.example.com
UID: 427200006
GID: 427200006
Password: True
Member of groups: ipausers
Kerberos keys available: True
```

これでユーザーパスワードがアカウントに対して設定され、ユーザーが IdM にログインできます。

関連情報

- パラメーターの詳細は、**ipa help user-mod** コマンドを実行してください。

3.8. IDM ユーティリティーに値をリスト形式で提供する方法

Identity Management (IdM) は、多値属性の値をリスト形式で保存します。

IdM は、多値リストを提供する次の方法に対応します。

- 同じコマンド呼び出しで、同じコマンドライン引数を複数回指定します。

```
$ ipa permission-add --right=read --permissions=write --permissions=delete ...
```

- または、リストを中括弧で囲むこともできます。この場合、シェルはデプロイメントを実行します。

```
$ ipa permission-add --right={read,write,delete} ...
```

上記の例では、パーミッションをオブジェクトに追加する **permission-add** コマンドを表示します。この例では、このオブジェクトについては触れていません。**...** の代わりに、権限を追加するオブジェクトーを追加する必要があります。

このような多値属性をコマンド行から更新すると、IdM は、前の値リストを新しいリストで完全に上書きします。したがって、多値属性を更新するときは、追加する 1 つの値だけでなく、新しいリスト全体を指定する必要があります。

たとえば、上記のコマンドでは、パーミッションのリストには、読み取り、書き込み、および削除が含まれます。**permission-mod** コマンドでリストを更新する場合は、すべての値を追加する必要があります。すべての値を追加しないと、追加されていない値は削除されます。

例 1: - **ipa permission-mod** コマンドは、以前に追加した権限をすべて更新します。

```
$ ipa permission-mod --right=read --right=write --right=delete ...
```

または

```
$ ipa permission-mod --right={read,write,delete} ...
```

例 2 - **ipa permission-mod** コマンドは、コマンドに含まれないため、**--right=delete** 引数を削除します。

```
$ ipa permission-mod --right=read --right=write ...
```

または

```
$ ipa permission-mod --right={read,write} ...
```

3.9. IDM ユーティリティーで特殊文字を使用する方法

特殊文字を含むコマンドライン引数を **ipa** コマンドに渡す場合は、この文字をバックスラッシュ (\) でエスケープします。たとえば、一般的な特殊文字には、山かっこ (< および >)、アンパサンド (&)、アスタリスク (*)、またはバーティカルバー (|) があります。

たとえば、アスタリスク (*) をエスケープするには、次のコマンドを実行します。

```
$ ipa certprofile-show certificate_profile --out=exported\*profile.cfg
```

シェルが特殊文字を正しく解析できないため、エスケープしていない特殊文字をコマンドに含めると、予想通りに機能しなくなります。

第4章 コマンドラインから IDENTITY MANAGEMENT エントリーの検索

次のセクションでは、オブジェクトの検索または表示に役立つ IPA コマンドの使用方法を説明します。

4.1. IDM エントリーのリスト表示の概要

ipa *-find コマンドを使用すると、特定のタイプの IdM エントリーを検索できます。

すべての **find** コマンドを表示するには、次の ipa help コマンドを使用します。

```
$ ipa help commands | grep find
```

特定のユーザーが IdM データベースに含まれているかどうかの確認が必要になる場合があります。次のコマンドを使用すると、ユーザーをリスト表示できます。

```
$ ipa user-find
```

指定の属性にキーワードが含まれるユーザーグループのリストを表示するには、次のコマンドを実行します。

```
$ ipa group-find keyword
```

たとえば、**ipa group-find admin** コマンドは、名前または説明に文字列 **admin** が含まれるグループのリストを表示します。

```
----------------
3 groups matched
----------------
  Group name: admins
  Description: Account administrators group
  GID: 427200002

  Group name: editors
  Description: Limited admins who can edit other users
  GID: 427200002

  Group name: trust admins
  Description: Trusts administrators group
```

ユーザーグループの検索の際には、特定のユーザーを含むグループに検索結果を絞り込むことも可能です。

```
$ ipa group-find --user=user_name
```

また、特定のユーザーを含まないグループを検索するには、次のコマンドを実行します。

```
$ ipa group-find --no-user=user_name
```

4.2. 特定のエントリーの詳細の表示

ipa *-show コマンドを使用して、特定の IdM エントリーの詳細を表示します。

手順

- ホスト **server.example.com** に関する詳細を表示します。

```
$ ipa host-show server.example.com

Host name: server.example.com
Principal name: host/server.example.com@EXAMPLE.COM
...
```

4.3. 検索サイズおよび時間制限の調整

IdM ユーザーのリストを要求するなど、一部のクエリーでは、エントリー数が大量に返される場合があります。この検索操作を調整して、**ipa user-find** などの **ipa *-find** コマンドの実行時や、Web UI で対応するリストを表示する際に、全体的なサーバーのパフォーマンスを向上できます。

検索サイズ制限

クライアントの CLI または IdM Web UI にアクセスするブラウザーからサーバーに送信されるリクエストで返される最大エントリー数を定義します。
デフォルト - 100 エントリー

検索時間の制限

検索の実行までにサーバーが待機する最大時間 (秒) を定義します。検索がこの制限に到達したら、サーバーは検索を停止し、停止するまでの期間に検出されたエントリーを返します。
デフォルト - 2 秒

この値が **-1** に設定されていると、IdM は、検索時に制限を適用しません。

重要

検索のサイズや時間制限を高く設定しすぎると、サーバーのパフォーマンスに影響を及ぼすことがあります。

4.3.1. コマンドラインで検索サイズおよび時間制限の調整

以下の手順では、コマンドラインで検索サイズと時間制限を調整する方法について説明します。

- グローバル
- 特定のエントリーの場合

手順

1. 現在の検索時間およびサイズ制限を CLI で表示するには、**ipa config-show** コマンドを使用します。

```
$ ipa config-show

Search time limit: 2
Search size limit: 100
```

2. すべてのクエリーに対して **グローバルに** 制限を調整するには、**ipa config-mod** コマンドを使用して、**--searchrecordslimit** および **--searchtimelimit** のオプションを追加します。以下に例を示します。

```
$ ipa config-mod --searchrecordslimit=500 --searchtimelimit=5
```

3. 特定のクエリーに対してのみ **一時的に** 制限を調整するには、コマンドに **--sizelimit** または **--timelimit** オプションを追加してください。以下に例を示します。

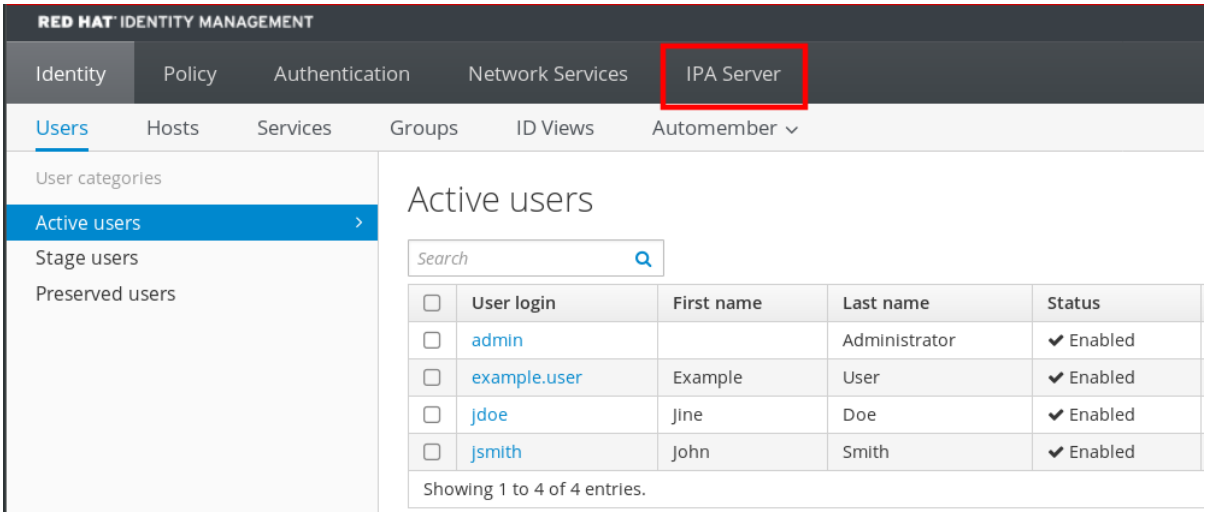
```
$ ipa user-find --sizelimit=200 --timelimit=120
```

4.3.2. Web UI で検索サイズおよび時間制限の調整

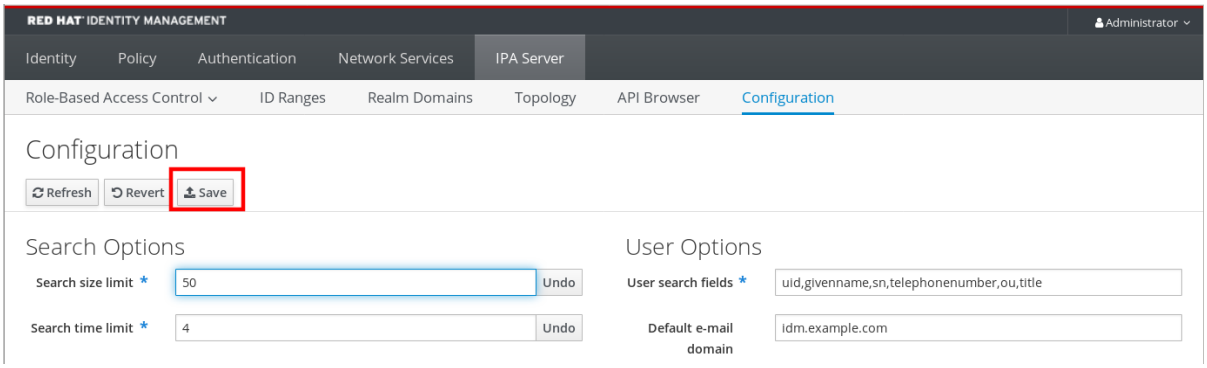
以下の手順では、IdM Web UI でグローバル検索のサイズと時間制限を調整する方法について説明します。

手順

1. IdM Web UI にログインします。
2. **IPA Server** をクリックします。



3. **IPA Server** タブで、**Configuration** をクリックします。
4. **Search Options** エリアに必要な値を設定します。
デフォルト値は以下の通りです。
   - 検索サイズの制限 - 100 エントリー
   - 検索時間の制限 - 2 秒
5. ページ上部にある **Save** をクリックします。


RED HAT IDENTITY MANAGEMENT
Administrator
Identity
Policy
Authentication
Network Services
IPA Server
Role-Based Access Control
ID Ranges
Realm Domains
Topology
API Browser
Configuration
Configuration
Refresh
Revert
Save
Search Options
Search size limit *
50
Undo
Search time limit *
4
Undo
User Options
User search fields *
uid,givenname,sn,telephonenumber,ou,title
Default e-mail domain
idm.example.com

第5章 WEB ブラウザーで IDM WEB UI へのアクセス

IdM (Identity Management) Web UI は、IdM 管理用の Web アプリケーションであり、IdM コマンドラインインターフェイス (CLI) のグラフィカルな代替手段です。

5.1. IDM WEB UI とは

IdM (Identity Management) Web UI は、IdM 管理用の Web アプリケーションです。IdM Web UI には、以下のユーザーとしてアクセスできます。

- **IdM ユーザー** - IdM サーバーでユーザーに付与されている権限に応じて制限されている一連の操作。基本的に、アクティブな IdM ユーザーは IdM サーバーにログインして自身のアカウントを設定できます。その他のユーザーまたは IdM サーバーの設定は変更できません。
- **管理者** - IdM サーバーへのフルアクセス権
- **Active Directory ユーザー** - ユーザーに付与されている権限に応じた一連の操作Active Directory ユーザーが Identity Management の管理可能に詳細は IdM を管理する AD ユーザーの有効化 を参照してください。

5.2. WEB UI へのアクセスに対応している WEB ブラウザー

Identity Management (IdM) は、Web UI への接続に、以下のブラウザーをサポートします。

- Mozilla Firefox 38 以降
- Google Chrome 46 以降

注記

ブラウザーで TLS v1.3 を使用しようとすると、スマートカードで IdM Web UI にアクセスできなくなる場合があります。

```
[ssl:error] [pid 125757:tid 140436077168384] [client 999.999.999.999:99999] AH:
verify client post handshake
[ssl:error] [pid 125757:tid 140436077168384] [client 999.999.999.999:99999]
AH10158: cannot perform post-handshake authentication
[ssl:error] [pid 125757:tid 140436077168384] SSL Library Error: error:14268117:SSL
routines:SSL_verify_client_post_handshake:extension not received
```

これは、最新バージョンのブラウザーで TLS Post-Handshake Authentication (PHA) がデフォルトで有効になっていないか、PHA をサポートしていないためです。スマートカード認証で IdM Web UI にアクセスする場合など、Web サイトの一部にのみ TLS クライアント証明書を必要とする場合は、PHA が必要です。

Mozilla Firefox 68 以降でこの問題を解決するには、TLS PHA を有効にします。

1. アドレスバーに **about:config** と入力して、Mozilla Firefox 設定メニューにアクセスします。
2. 検索バーに **security.tls.enable_post_handshake_auth** と入力します。
3. トグルボタンをクリックして、パラメーターを true に設定します。

現在 PHA をサポートしていない Chrome でこの問題を解決するには、TLS v1.3 を無効にします。

1. **/etc/httpd/conf.d/ssl.conf** 設定ファイルを開きます。
2. **-TLSv1.3** を **SSLProtocol** オプションに追加します。

```
SSLProtocol all -TLSv1 -TLSv1.1 -TLSv1.3
```

3. **httpd** サービスを再起動します。

```
service httpd restart
```

IdM は **ssl.conf** ファイルを管理するため、パッケージの更新時にそのコンテンツが上書きされる可能性があることに注意してください。IdM パッケージの更新後に、カスタム設定を確認します。

5.3. WEB UI へのアクセス

次の手順では、パスワードを使用して、IdM (Identity Management) Web UI に最初にログインする方法を説明します。

最初のログイン後に、IdM サーバーを認証するように設定できます。

- Kerberos チケット
  詳細は、Kerberos authentication in Identity Management を参照してください。
- スマートカード
  詳細は、スマートカード認証用の IdM サーバーの設定 を参照してください。

- ワンタイムパスワード (OTP) - パスワードと組み合わせることができ、Kerberos 認証に利用されます。
  詳細は、One time password (OTP) authentication in Identity Management を参照してください。

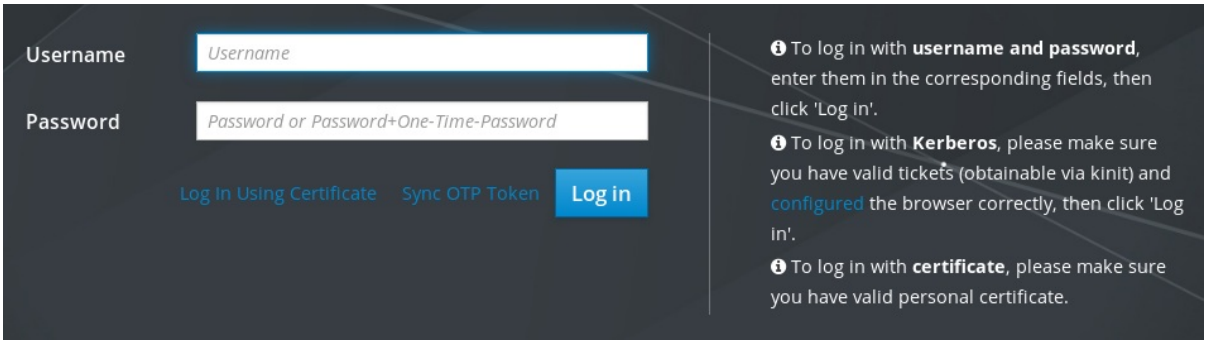
手順

1. ブラウザーのアドレスバーに、IdM サーバーの URL を入力します。名前は次の例のようになります。

   ```
   https://server.example.com
   ```

   server.example.com を、IdM サーバーの DNS 名に変更するだけです。

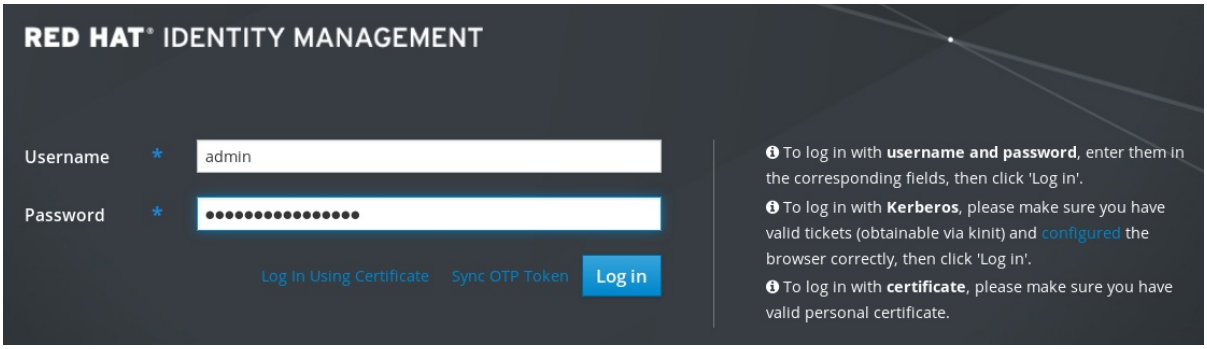
   これで、ブラウザーに IdM Web UI ログイン画面が開きます。



   - サーバーが応答しない、またはログイン画面が開かない場合は、接続している IdM サーバーの DNS 設定を確認してください。
   - 自己署名証明書を使用する場合は、ブラウザーに警告が表示されます。証明書を確認し、セキュリティー例外を許可して、ログインを続行します。
     セキュリティーの例外を回避するために、認証局が署名した証明書をインストールします。

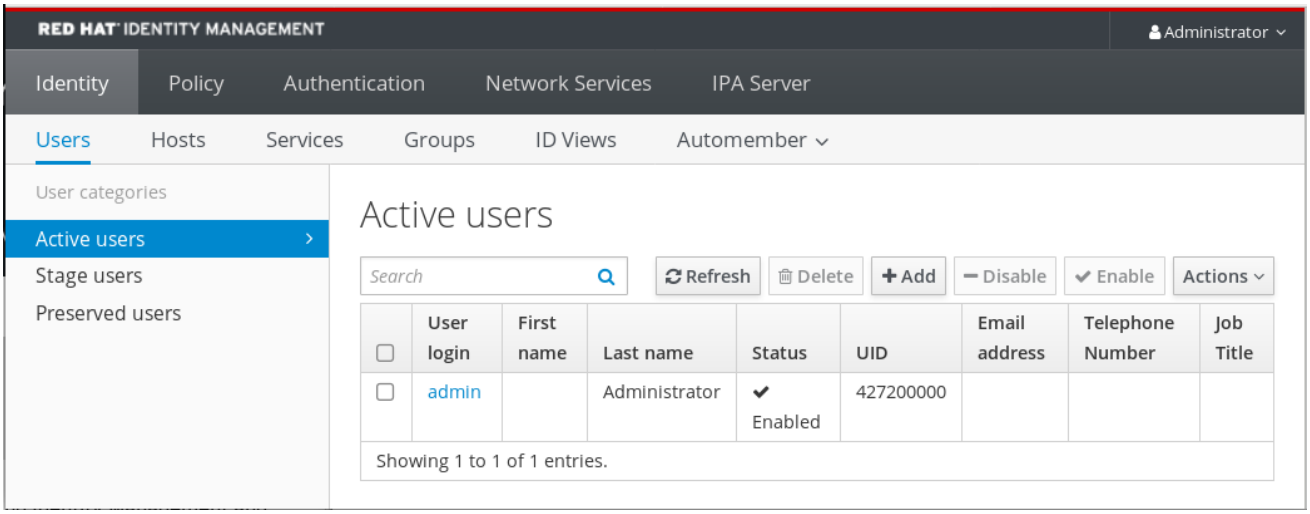
2. Web UI ログイン画面で、IdM サーバーのインストール時に追加した管理者アカウントの認証情報を入力します。
   詳細は Identity Management サーバーのインストール: 統合 DNS と統合 CA の場合 を参照してください。

   IdM サーバーに、個人アカウントの認証情報がすでに入力されている場合は、それを入力できます。



3. **Log in** をクリックします。

ログインに成功したら、IdM サーバーの設定を開始できます。


RED HAT IDENTITY MANAGEMENT
Administrator
Identity
Policy
Authentication
Network Services
IPA Server
Users
Hosts
Services
Groups
ID Views
Automember
User categories
Active users
Stage users
Preserved users
Active users
Search
Refresh
Delete
Add
Disable
Enable
Actions
User login
First name
Last name
Status
UID
Email address
Telephone Number
Job Title
admin
Administrator
Enabled
427200000
Showing 1 to 1 of 1 entries.

第6章 WEB UI で IDM にログイン: KERBEROS チケットの使用

IdM Web UI への Kerberos ログインと、Kerberos 認証を使用した IdM へのアクセスを有効にするように環境を設定する方法について詳しく説明します。

前提条件

- ネットワーク環境にインストールしている IdM サーバー
  詳細は、Red Hat Enterprise Linux 9 の Identity Management のインストール を参照してください。

6.1. IDENTITY MANAGEMENT における KERBEROS 認証

Identity Management (IdM) は、シングルサインオンに対応する Kerberos プロトコルを使用します。シングルサインオン認証により、ユーザーが正しいユーザー名およびパスワードを一度入力すれば、再度システムに認証情報を求められることなく、Identity Management サービスにアクセスできます。

DNS および証明書の設定が適切に設定されている場合は、インストール直後に、IdM サーバーが Kerberos 認証を提供します。詳細は、Identity Management のインストール を参照してください。

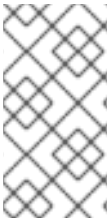
ホストで Kerberos 認証を使用するには、以下をインストールします。

- IdM クライアント
  詳細は Identity Management クライアントをインストールするためのシステムの準備 を参照してください。

- krb5conf パッケージ

6.2. KINIT による IDM への手動ログイン

kinit ユーティリティーを使用して Identity Management (IdM) 環境に対して手動で認証するには、次の手順に従います。**kinit** ユーティリティーは、IdM ユーザーの代わりに Kerberos の TGT (Ticket-Granting Ticket) を取得して、キャッシュに格納します。



注記

この手順は、最初の Kerberos TGT を破棄したか、有効期限が切れている場合にのみ使用します。ローカルマシンに、IdM ユーザーとしてログインすると、IdM に自動的にログインします。これは、ログイン後に IdM リソースにアクセスするのに **kinit** ユーティリティーを使用する必要がないことを示しています。

手順

1. IdM にログインします。

   - ローカルシステムに現在ログインしているユーザーのユーザー名で、(ユーザー名を指定せずに) **kinit** を使用します。たとえば、ローカルシステムにログインしているユーザーが **example_user** の場合は、次のコマンドを実行します。

     ```
     [example_user@server ~]$ kinit
     Password for example_user@EXAMPLE.COM:
     [example_user@server ~]$
     ```

ローカルユーザーのユーザー名と、IdM のユーザーエントリーが一致しないと、認証に失敗します。

```
[example_user@server ~]$ kinit
kinit: Client 'example_user@EXAMPLE.COM' not found in Kerberos database while
getting initial credentials
```

- ローカルユーザー名に対応しない Kerberos プリンシパルを使用して、**kinit** ユーティリティーに必要なユーザー名を渡します。たとえば、**admin** ユーザーとしてログインするには、次のコマンドを実行します。

```
[example_user@server ~]$ kinit admin
Password for admin@EXAMPLE.COM:
[example_user@server ~]$
```

2. 必要に応じて、ログインが成功したことを確認するには、**klist** ユーティリティーを使用して、キャッシュした TGT を表示します。以下の例では、キャッシュに **example_user** プリンシパルのチケットが含まれています。これは、このホストでは IdM サービスにアクセスするのは、**example_user** にのみ許可されていることを示しています。

```
$ klist
Ticket cache: KEYRING:persistent:0:0
Default principal: example_user@EXAMPLE.COM

Valid starting       Expires              Service principal
11/10/2019 08:35:45  11/10/2019 18:35:45  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

6.3. KERBEROS 認証用のブラウザーの設定

Kerberos チケットによる認証を有効にするには、ブラウザーの設定が必要になることもあります。

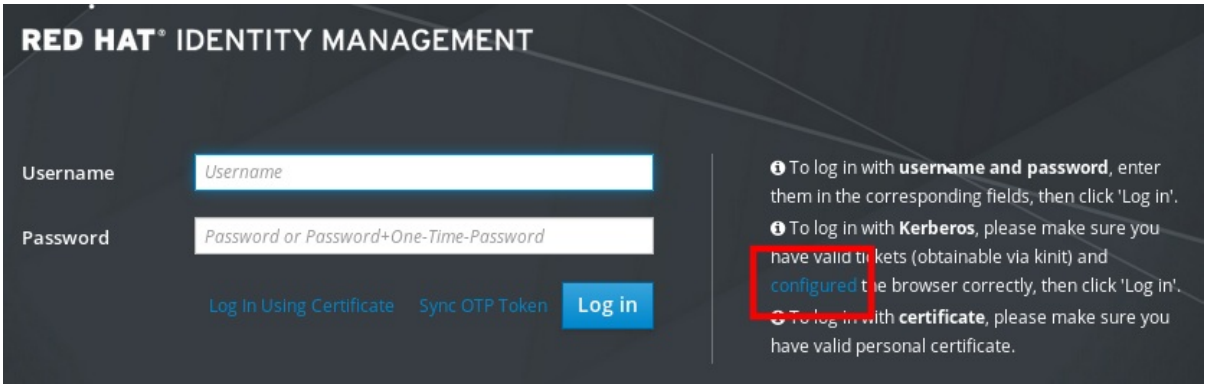
以下の手順は、IdM ドメインにアクセスする Kerberos ネゴシエーションに対応するのに役に立ちます。

Kerberos に対応する方法はブラウザーによって異なるため、異なる設定が必要です。IdM Web UI には、次のブラウザーに関するガイドラインが含まれています。

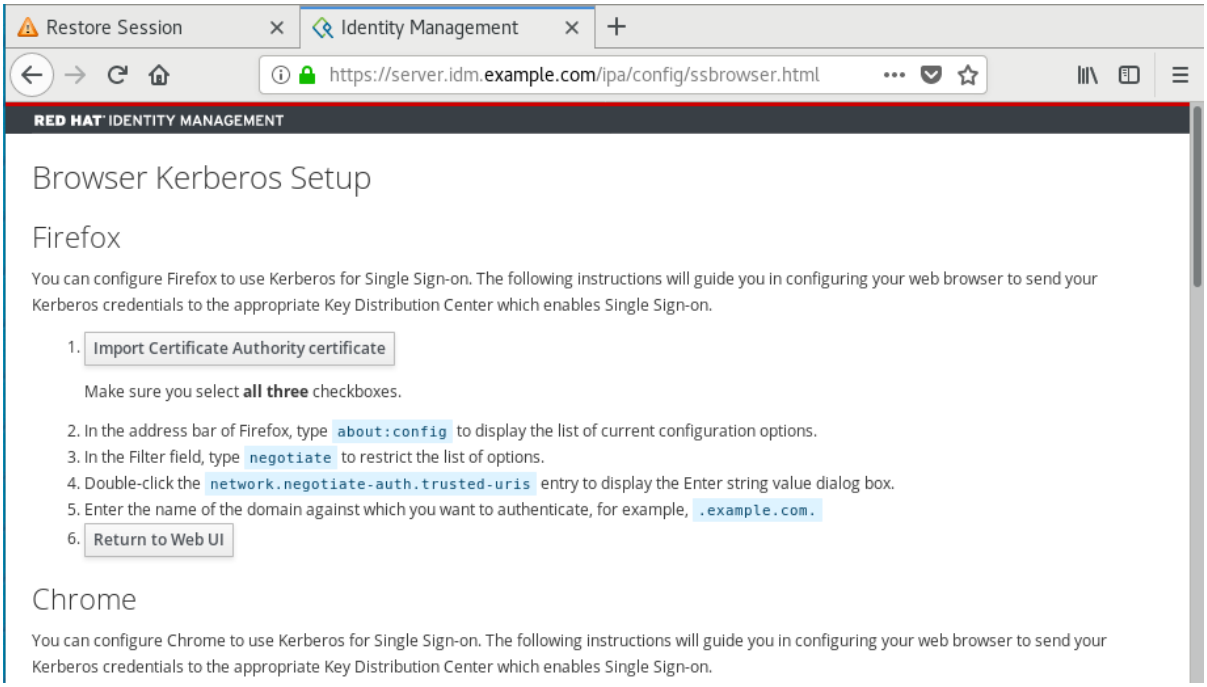
- Firefox
- Chrome

手順

1. Web ブラウザーで、WebUI ログインダイアログを開きます。
2. Web UI のログイン画面で、ブラウザー設定のリンクをクリックします。



3. 設定ページの手順に従います。



設定が完了したら、IdM Web UI に戻り、**ログイン** をクリックします。

6.4. KERBEROS チケットで WEB UI へのログイン

Kerberos Ticket-Granting Ticket (TGT) を使用して IdM Web UI にログインするには、次の手順に従います。

TGT は、事前定義された時間で有効期限が切れます。デフォルトの時間間隔は 24 時間で、IdM Web UI でそれを変更できます。

期限が切れたら、チケットを更新する必要があります。

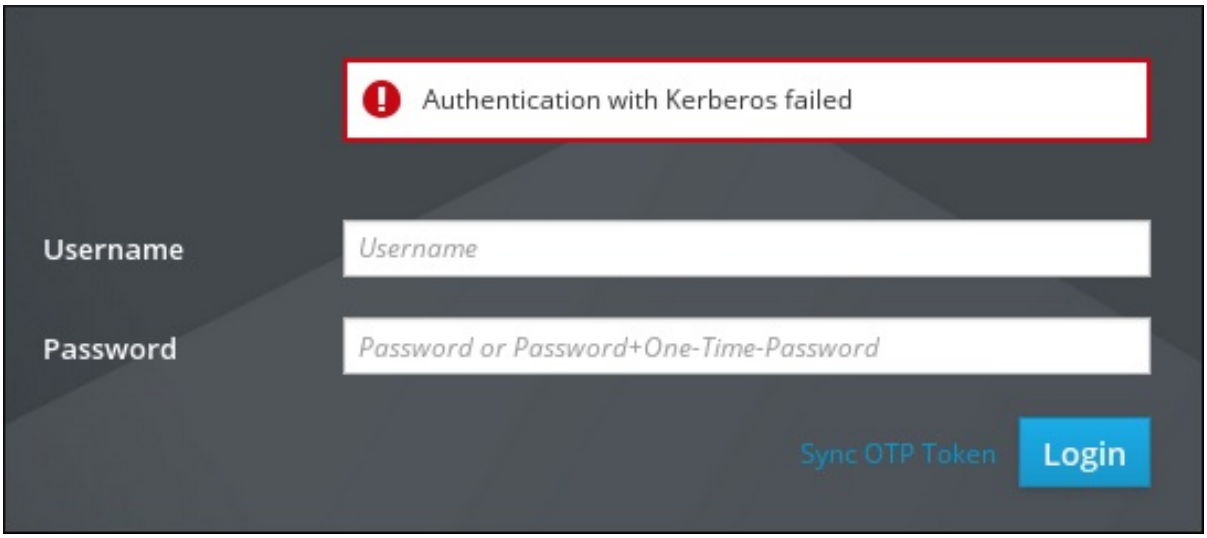
- kinit コマンドの使用
- Web UI ログインダイアログで、IdM ログイン認証情報を使用

手順

- IdM Web UI を開きます。
  Kerberos 認証が正しく機能し、有効なチケットがある場合は、自動的に認証されて Web UI が開きます。

チケットの有効期限が切れている場合は、最初に認証情報を使用して認証する必要があります。ただし、次からはログインダイアログを開かずに IdM Web UI が自動的に開きます。

エラーメッセージ **Authentication with Kerberos failed** が表示された場合は、ブラウザーが Kerberos 認証用に設定されていることを確認してください。Kerberos 認証用のブラウザーの設定 を参照してください。



6.5. KERBEROS 認証用の外部システムの設定

Identity Management (IdM) ユーザーが Kerberos 認証情報を使用して外部システムから IdM にログインできるように外部システムを設定するには、この手順に従います。

外部システムの Kerberos 認証を有効にすることは、インフラストラクチャーに、複数のレルムまたは重複ドメインが含まれている場合に特に便利です。また、**ipa-client-install** を実行してシステムを IdM ドメインに登録していない場合にも便利です。

IdM ドメインのメンバーではないシステムから IdM への Kerberos 認証を有効にするには、IdM 固有の Kerberos 設定ファイルを外部システムに定義します。

前提条件

- 外部システムに **krb5-workstation** パッケージがインストールされている。
  パッケージがインストールされているかどうかを確認するには、次の CLI コマンドを使用します。

```
# dnf list installed krb5-workstation
Installed Packages
krb5-workstation.x86_64    1.16.1-19.el8    @BaseOS
```

手順

1. IdM サーバーから外部システムに **/etc/krb5.conf** ファイルをコピーします。以下に例を示します。

```
# scp /etc/krb5.conf root@externalsystem.example.com:/etc/krb5_ipa.conf
```

警告

外部マシンにある既存の **krb5.conf** ファイルは上書きしないでください。

2. 外部システムで、コピーした IdM の Kerberos 設定ファイルを使用するように、端末セッションを設定します。

```
$ export KRB5_CONFIG=/etc/krb5_ipa.conf
```

KRB5_CONFIG 変数は、ログアウトまで一時的に存在します。ログアウト時に削除されないように、この変数のファイル名を変えてエクスポートします。

3. **/etc/krb5.conf.d/** ディレクトリーの Kerberos 設定部分を、外部システムにコピーします。

4. Kerberos 認証用のブラウザーの設定 の説明に従って、外部システムでブラウザーを設定します。

外部システムのユーザーが、**kinit** ユーティリティーを使用して IdM サーバーで認証できるようになりました。

6.6. ACTIVE DIRECTORY ユーザーの WEB UI ログイン

Active Directory ユーザーに対して Web UI ログインを有効にするには、**デフォルトの信頼ビュー** で、Active Directory の各ユーザーに対して ID のオーバーライドを定義します。以下に例を示します。

```
[admin@server ~]$ ipa idoverrideuser-add 'Default Trust View' ad_user@ad.example.com
```

関連情報

- Active Directory ユーザーの ID ビューの使用

第7章 ワンタイムパスワードを使用した IDENTITY MANAGEMENT WEB UI へのログイン

IdM Web UI へのアクセスは、いくつかの方法を使用して保護できます。基本的なものはパスワード認証です。

パスワード認証のセキュリティーを向上させるために、2 つ目の手順を追加して、自動生成ワンタイムパスワード (OTP) を要求できます。最も一般的な使用方法は、ユーザーアカウントに関連付けられたパスワードと、ハードウェアまたはソフトウェアのトークンにより生成された期限付きワンタイムパスワードを組み合わせることです。

以下のセクションでは、次のことができます。

- IdM で OTP 認証がどう機能するかを理解する。
- IdM サーバーで OTP 認証を設定する。
- IdM で OTP バリデーション用に RADIUS サーバーを設定する。
- OTP トークンを作成し、そのトークンを、電話の FreeOTP アプリと同期する。
- ユーザーパスワードとワンタイムパスワードの組み合わせて、IdM Web UI に対して認証する。
- Web UI でトークンを再同期する。
- OTP ユーザーまたは RADIUS ユーザーとして IdM チケット許可チケットを取得する

7.1. 前提条件

- Web ブラウザーで IdM Web UI へのアクセス

7.2. IDENTITY MANAGEMENT におけるワンタイムパスワード (OTP) 認証

ワンタイムパスワードにより、認証セキュリティーに関する手順が追加されます。認証では、自身のパスワードと、自動生成されたワンタイムパスワードが使用されます。

ワンタイムパスワードを生成するには、ハードウェアまたはソフトウェアのトークンを使用できます。IdM は、ソフトウェアトークンとハードウェアトークンの両方をサポートします。

Identity Management は、以下にある、2 つの標準 OTP メカニズムに対応しています。

- HMAC ベースのワンタイムパスワード (HOTP) アルゴリズムは、カウンターに基づいています。HMAC は、Hashed Message Authentication Code (ハッシュメッセージ認証コード) を表しています。
- 時間ベースのワンタイムパスワード (TOTP) アルゴリズムは、時間ベースの移動要素に対応する HOTP の拡張機能です。

重要

IdM は、Active Directory 信頼ユーザーの OTP ログインに対応していません。

7.3. WEB UI でのワンタイムパスワードの有効化

Identity Management (IdM) 管理者は、IdM ユーザーに対して 2 要素認証 (2FA) をシステム全体でまたは個別に有効にすることができます。ユーザーは、コマンドラインまたは Web UI ログインダイアログの専用フィールドで、通常のパスワードの後にワンタイムパスワード (OTP) を入力します。これらのパスワードの間にはスペースを入れません。

2FA を有効にしても、2FA が強制されるわけではありません。LDAP バインドに基づくログインを使用する場合、IdM ユーザーはパスワードを入力するだけで認証できます。ただし、**krb5** ベースのログインを使用する場合は、2FA が強制されます。Red Hat は今後のリリースで設定オプションを提供して、管理者が次のいずれかを選択できるようにする予定です。

- ユーザーが独自のトークンを設定できるようにします。この場合、**krb5** ベースのログインでは 2FA が強制されますが、LDAP バインドでは依然として強制されません。
- ユーザーが独自のトークンを設定できないようにします。この場合、2FA は LDAP バインドと **krb5** ベースのログインの両方で強制されます。

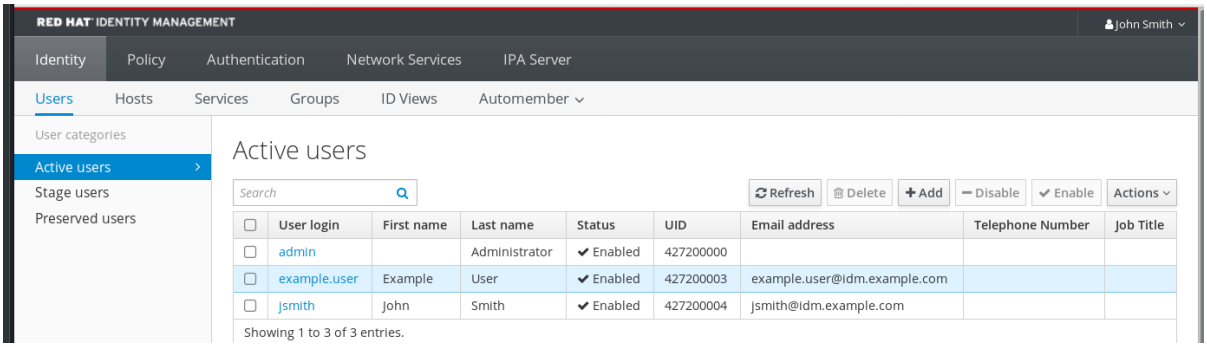
IdM Web UI を使用して、個々の **example.user** IdM ユーザーに対して 2FA を有効にするには、以下の手順を完了します。

前提条件

- 管理者権限

手順

1. IdM **admin** 権限を使用して IdM Web UI にログインします。
2. **Identity → Users → Active users**タブを開きます。



3. **example.user** を選択してユーザー設定を開きます。
4. **User authentication types** で、**Two factor authentication (password + OTP)** を選択します。
5. **Save** をクリックします。

この時点で、IdM ユーザーに対して OTP 認証が有効になります。

次に、管理者権限を持つユーザーまたは **example.user** が、**example.user** アカウントに新しいトークン ID を割り当てる必要があります。

7.4. IDM での OTP バリデーション用の RADIUS サーバー設定

プロプライエタリーのワンタイムパスワード (OTP) ソリューションから Identity Management (IdM) ネイティブの OTP ソリューションへの大規模なデプロイメントの移行を可能にするために、IdM では、ユーザーのサブセットに対して OTP バリデーションをサードパーティーの RADIUS サーバーにオフ

ロードすることができます。管理者は、各プロキシーが単一の RADIUS サーバーのみを参照できる RADIUS プロキシーのセットを作成します。複数のサーバーに対応する必要がある場合は、複数の RADIUS サーバーを参照する仮想 IP ソリューションを作成することが推奨されます。

このようなソリューションは、**keepalived** デーモンなどを使用して、RHEL IdM の外部でビルドする必要があります。次に、管理者はこれらのプロキシーセットのいずれかをユーザーに割り当てます。ユーザーが RADIUS プロキシーが設定されている限り、IdM は他のすべての認証メカニズムをバイパスします。

注記

IdM は、サードパーティーシステムのトークンに対するトークン管理または同期のサポートを提供しません。

OTP バリデーション用に RADIUS サーバーを設定し、プロキシーサーバーにユーザーを追加する手順を実行します。

前提条件

- radius ユーザー認証方法が有効になっている。詳細は、Web UI でのワンタイムパスワードの有効化 を参照してください。

手順

1. RADIUS プロキシーを追加します。

```
$ ipa radiusproxy-add proxy_name --secret secret
```

このコマンドは、必要な情報を挿入するように求められます。

RADIUS プロキシーの設定には、クライアントとサーバーとの間の共通のシークレットを使用して認証情報をラップする必要があります。**--secret** パラメーターにこのシークレットを指定します。

2. 追加したプロキシーにユーザーを割り当てます。

```
ipa user-mod radiususer --radius=proxy_name
```

3. 必要に応じて、RADIUS に送信するユーザー名を設定します。

```
ipa user-mod radiususer --radius-username=radius_user
```

これにより、RADIUS プロキシーサーバーがユーザーの OTP 認証の処理を開始します。

ユーザーが IdM ネイティブ OTP システムに移行する準備ができたら、ユーザーの RADIUS プロキシー割り当てを削除するだけです。

7.4.1. 低速ネットワークで RADIUS サーバーを実行する場合の KDC タイムアウト値の変更

低速ネットワークで RADIUS プロキシーを実行している場合などの特定の状況では、ユーザーがトークンを入力するのを待機している間に接続がタイムアウトして、RADIUS サーバーが応答する前に Identity Management (IdM) Kerberos Distribution Center (KDC) が接続を閉じます。

KDC のタイムアウト設定を変更するには、以下を実行します。

1. **/var/kerberos/krb5kdc/kdc.conf** ファイルの **[otp]** セクションで **timeout** パラメーターの値を変更します。たとえば、タイムアウトを **120** 秒に設定するには、以下のようにします。

```
[otp]
DEFAULT = {
  timeout = 120
  ...
}
```

2. **krb5kdc** サービスを再起動します。

```
# systemctl restart krb5kdc
```

関連情報

- ナレッジベース記事 How to configure FreeRADIUS authentication in FIPS mode

7.5. WEB UI での OTP トークンの追加

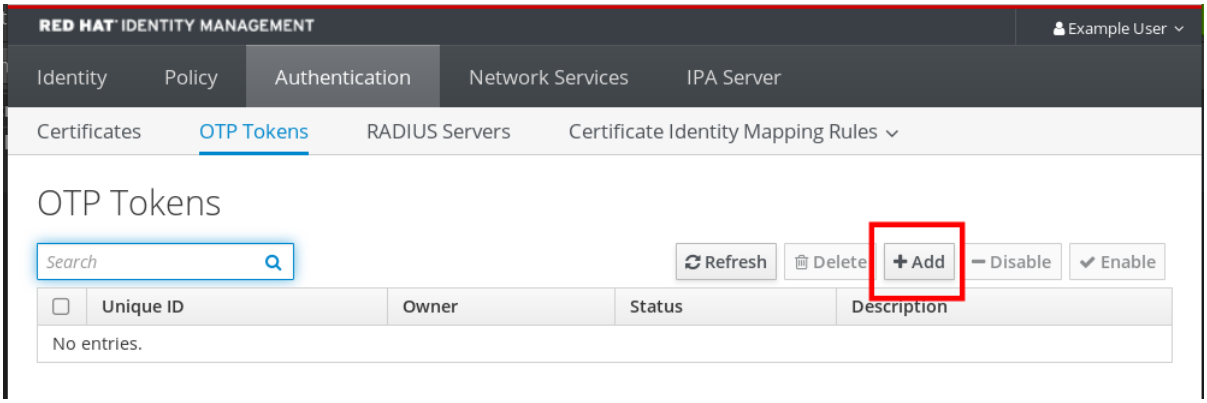
次のセクションは、IdM Web UI およびソフトウェアトークンジェネレーターに、トークンを追加するのに役立ちます。

前提条件

- IdM サーバーでアクティブなユーザーアカウント。
- 管理者が、IdM Web UI の特定のユーザーアカウントに対して OTP を有効にしている。
- FreeOTP などの OTP トークンを生成するソフトウェアデバイス。

手順

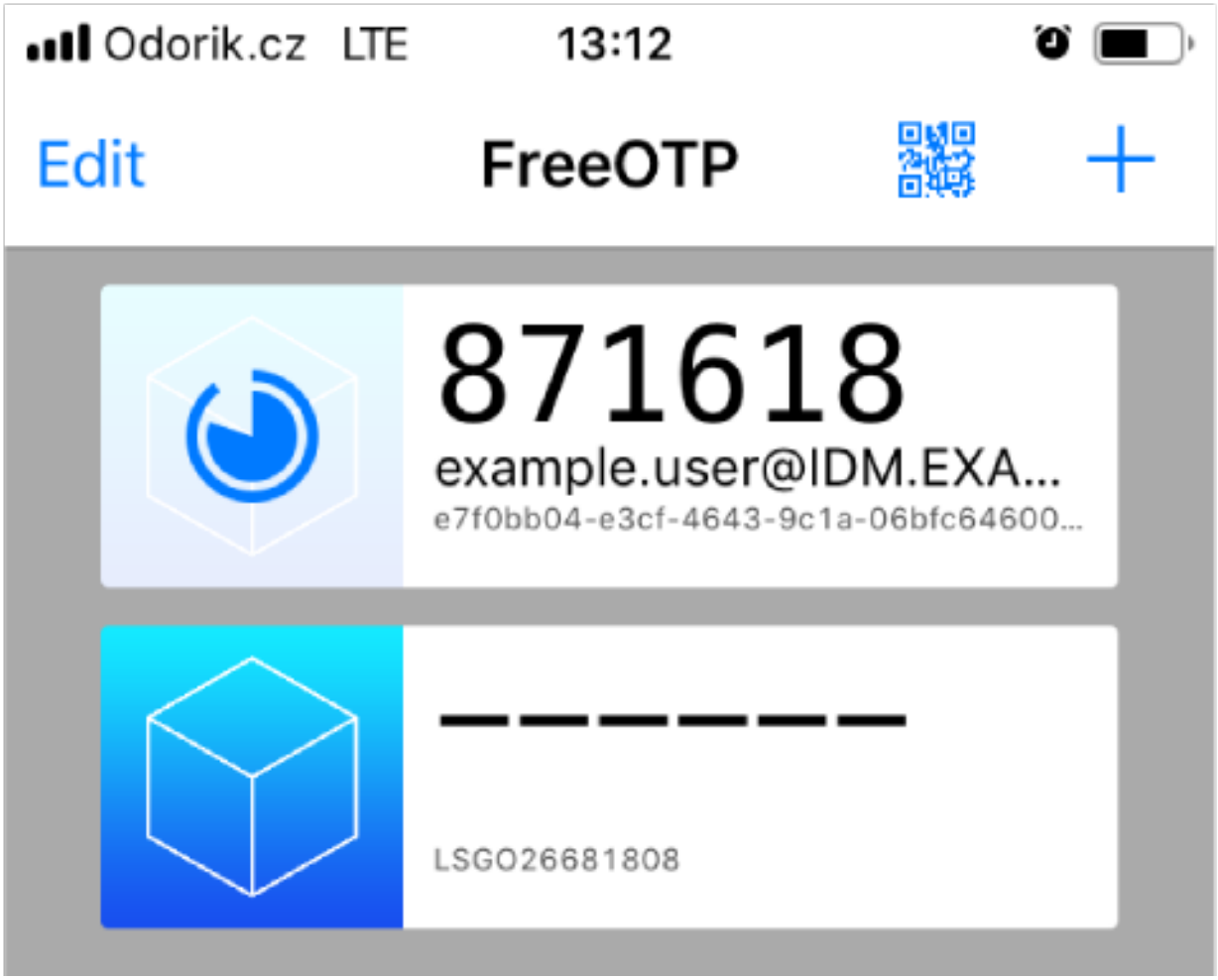
1. ユーザー名とパスワードを使用して IdM Web UI にログインします。
2. **Authentication → OTP Tokens**タブを開いて、携帯電話でトークンを作成します。
3. **Add** をクリックします。



4. **Add OTP token** ダイアログボックスに何も入力せず、**Add** をクリックします。
この段階で、IdM サーバーはデフォルトパラメーターを使用してトークンを作成し、QR コード付きページを開きます。

5. QR コードを携帯電話にコピーします。
6. **OK** をクリックして QR コードを閉じます。

これで、ワンタイムパスワードを生成して、IdM Web UI にログインできるようになりました。



7.6. ワンタイムパスワードで WEB UI にログイン

ワンタイムパスワード (OTP) を使用して IdM Web UI に初めてログインする際には、この手順に従います。

前提条件

- OTP 認証を使用しているユーザーアカウントに対して、Identity Management サーバーで OTP 設定が有効になっている。管理者およびユーザー自身が、OTP を有効にできる。
  OTP 設定を有効にする場合は、Web UI でワンタイムパスワードの有効化 を参照してください。
- 設定された OTP トークンを生成するハードウェアまたはソフトウェアのデバイス

手順

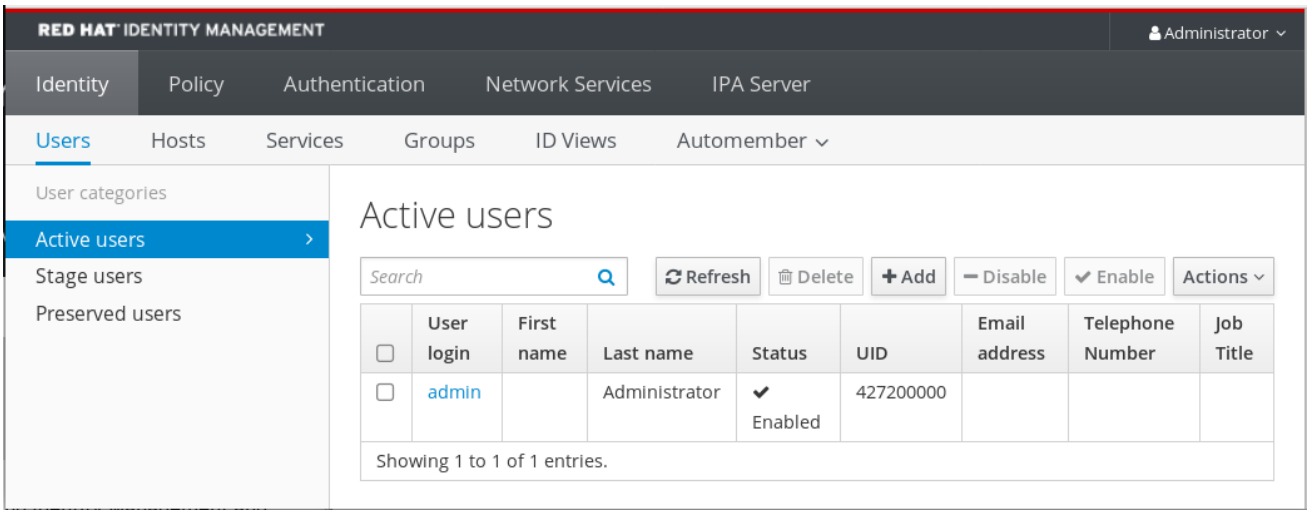
1. Identity Management ログイン画面で、自身のユーザー名、または IdM サーバー管理者アカウントのユーザー名を入力します。
2. 上記で入力したユーザーのパスワードを追加します。

3. デバイスでワンタイムパスワードを生成します。
4. パスワードの直後にワンタイムパスワードを入力します (空白文字は追加しない)。
5. **Log in** をクリックします。
   認証に失敗した場合は、OTP トークンを同期します。

   CA が自己署名証明書を使用する場合は、ブラウザーに警告が表示されます。証明書を確認し、セキュリティー例外を許可して、ログインを続行します。

   IdM Web UI が開かない場合は、Identity Management サーバーの DNS 設定を確認してください。

ログインが成功すると、IdM Web UI が表示されます。



7.7. WEB UI で OTP トークンの同期

OTP (ワンタイムパスワード) でのログインに失敗した場合、OTP トークンは正しく同期しません。

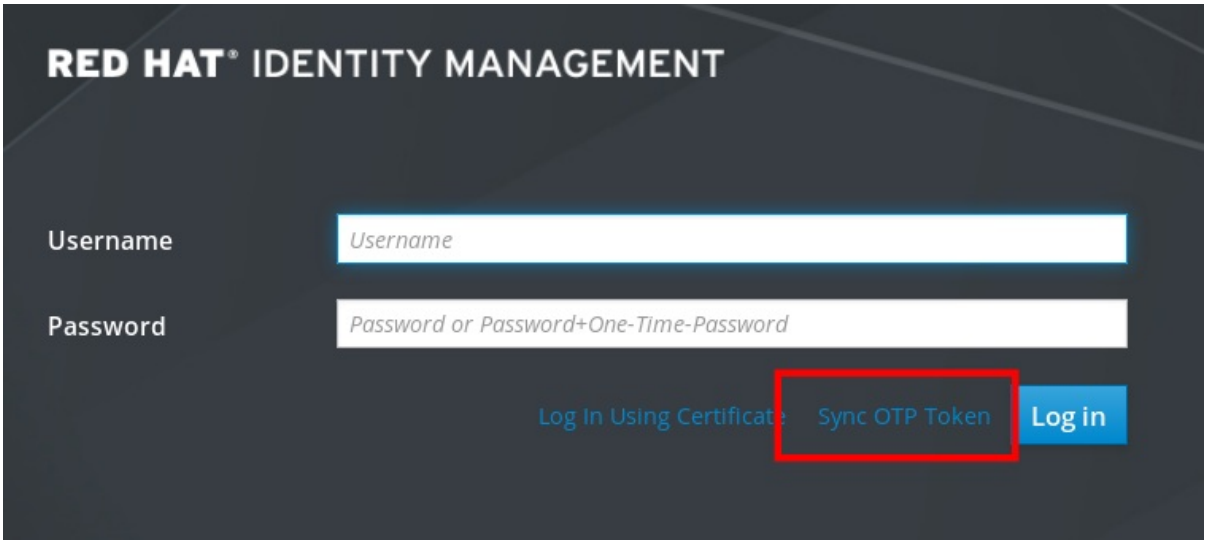
以下のテキストは、トークンの再同期を説明します。

前提条件

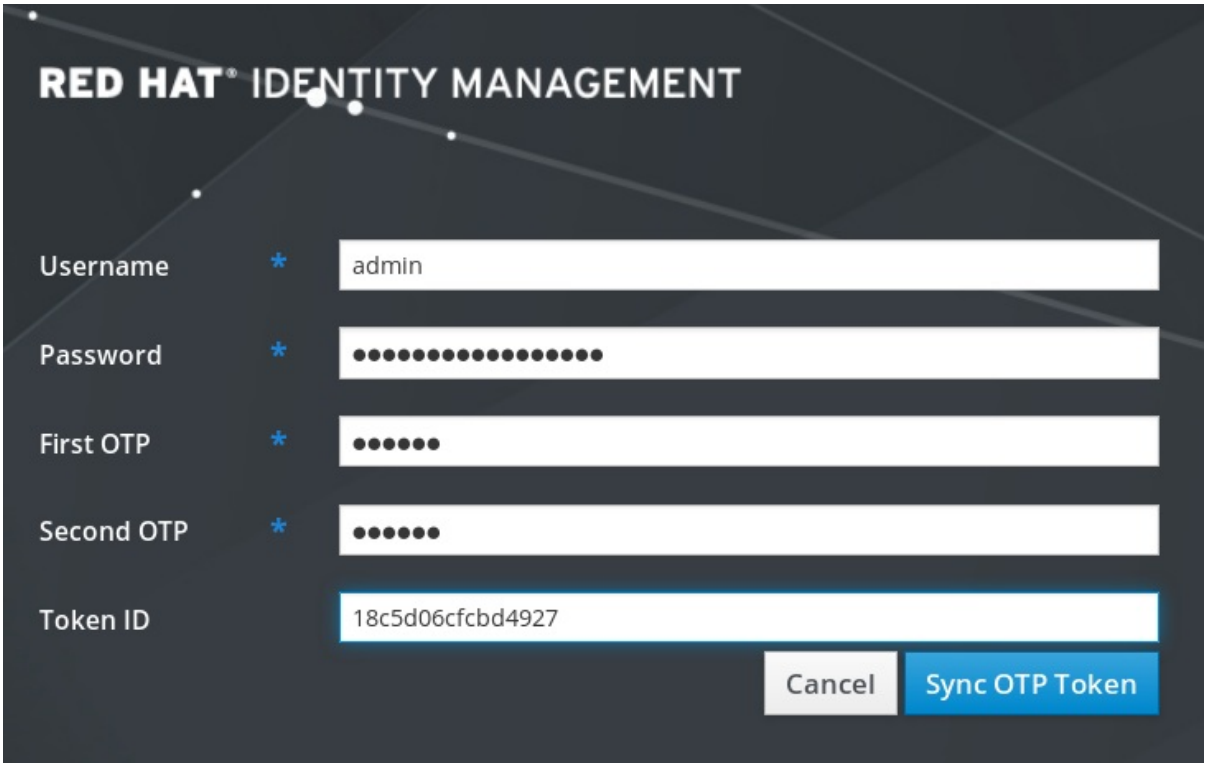
- ログイン画面を開いている。
- 設定した OTP トークンを生成するデバイス。

手順

1. IdM Web UI ログイン画面で、**Sync OTP Token** をクリックします。



2. ログイン画面で、ユーザー名と、Identity Management パスワードを入力します。
3. ワンタイムパスワードを生成し、**First OTP** フィールドに入力します。
4. ワンタイムパスワードをもう一度生成し、**Second OTP** フィールドに入力します。
5. 必要に応じて、トークン ID を入力してします。



6. **Sync OTP Token**をクリックします。

同期に成功したら、IdM サーバーにログインできます。

7.8. 期限切れパスワードの変更

Identity Management の管理者は、ユーザーが次回ログインする時にパスワードを変更するように強制できます。これを設定すると、パスワードを変更しないと IdM Web UI にログインできなくなります。

パスワードの有効期限は、Web UI に初めてログインしたときに発生する可能性があります。

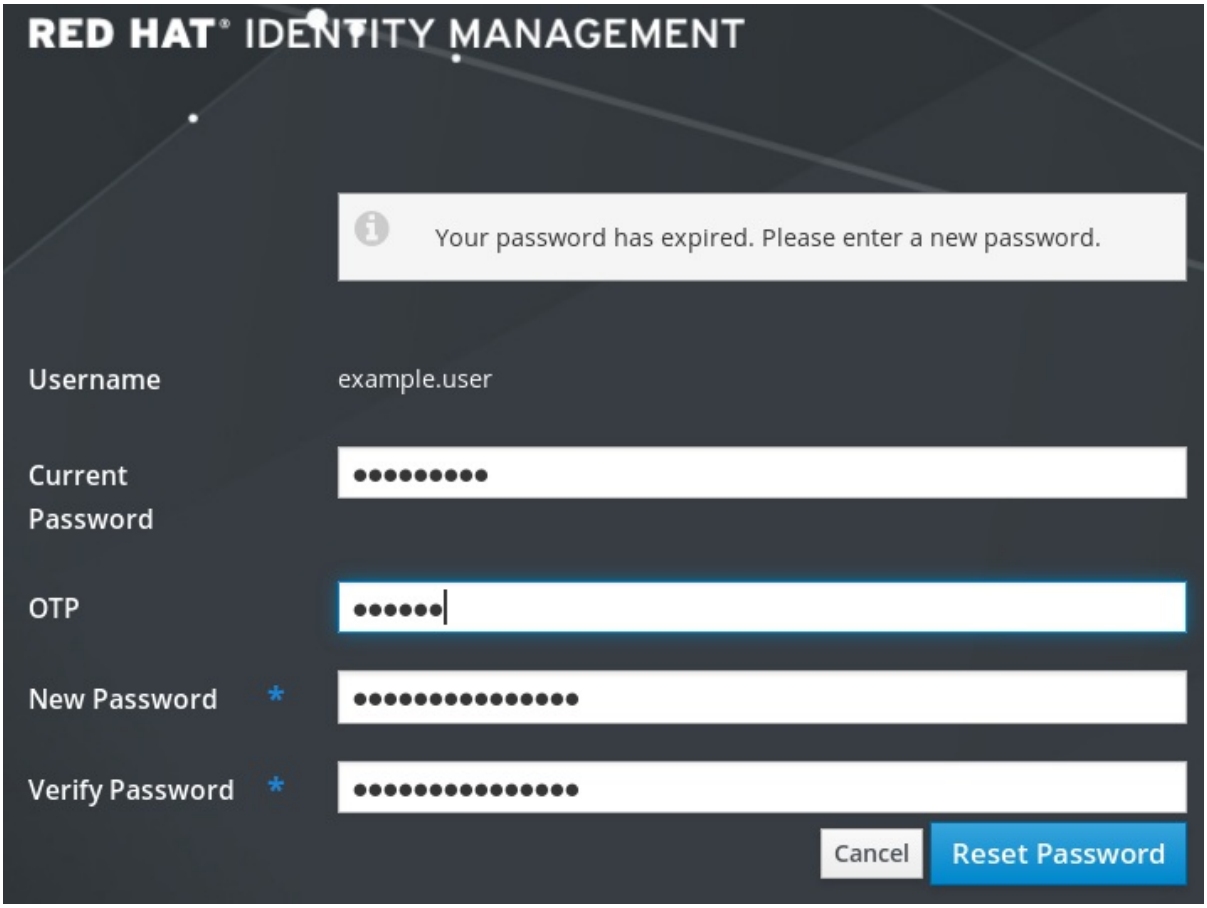
有効期限のパスワードのダイアログが表示されたら、手順の指示に従ってください。

前提条件

- ログイン画面を開いている。
- IdM サーバーへのアクティブなアカウント。

手順

1. パスワード有効期限のログイン画面に、ユーザー名を入力します。
2. 上記で入力したユーザーのパスワードを追加します。
3. ワンタイムパスワード認証を使用する場合は、OTP フィールドにワンタイムパスワードを生成します。
   OTP 認証を有効にしていない場合は、このフィールドを空白のままにします。
4. 確認のために新しいパスワードを 2 回入力します。
5. **Reset Password** をクリックします。



パスワード変更が成功すると、通常のログインダイアログが表示されます。新しいパスワードでログインします。

7.9. OTP または RADIUS ユーザーとして IDM チケット許可チケットを取得する

OTP ユーザーとして Kerberos TGT (Ticket-granting ticket) を取得するには、匿名の Kerberos チケットを要求し、Secure Tunneling (FAST) チャネルを介したフレキシブル認証を有効にして、Kerberos クライアントと Kerberos ディストリビューションセンター (KDC) 間のセキュアな接続を提供します。

前提条件

- IdM クライアントと IdM サーバーが RHEL 9.1 以降を使用している。
- IdM クライアントと IdM サーバーが SSSD 2.7.0 以降を使用している。
- 必要なユーザーアカウントに対して OTP が有効になっている。

手順

1. 次のコマンドを実行して認証情報キャッシュを初期化します。

```
[root@client ~]# kinit -n @IDM.EXAMPLE.COM -c FILE:armor.ccache
```

このコマンドは、新しい Kerberos チケットを要求するたびに指定する必要がある **armor.ccache** ファイルを作成することに注意してください。

2. 次のコマンドを実行して Kerberos チケットを要求します。

```
[root@client ~]# kinit -T FILE:armor.ccache <username>@IDM.EXAMPLE.COM
Enter your OTP Token Value.
```

検証

- Kerberos チケット情報を表示します。

```
[root@client ~]# klist -C
Ticket cache: KCM:0:58420
Default principal: <username>@IDM.EXAMPLE.COM

Valid starting     Expires            Service principal
05/09/22 07:48:23  05/10/22 07:03:07  krbtgt/IDM.EXAMPLE.COM@IDM.EXAMPLE.COM
config: fast_avail(krbtgt/IDM.EXAMPLE.COM@IDM.EXAMPLE.COM) = yes
08/17/2022 20:22:45  08/18/2022 20:22:43
krbtgt/IDM.EXAMPLE.COM@IDM.EXAMPLE.COM
config: pa_type(krbtgt/IDM.EXAMPLE.COM@IDM.EXAMPLE.COM) = 141
```

pa_type = 141 は OTP/RADIUS 認証を示します。

第8章 IDENTITY MANAGEMENT のセキュリティー設定

Identity Management のセキュリティー関連機能について詳しく説明します。

8.1. IDENTITY MANAGEMENT がデフォルトのセキュリティー設定を適用する方法

デフォルトでは、Identity Management (IdM) はシステム全体の暗号化ポリシーを使用します。このポリシーの利点は、個々の IdM コンポーネントを手動で強化する必要がないことです。

重要

Red Hat は、システム全体の暗号化ポリシーを使用することが推奨されます。個々のセキュリティー設定を変更すると、IdM のコンポーネントが破損する可能性があります。

関連情報

- **crypto-policies(7)** man ページを参照してください。

8.2. IDENTITY MANAGEMENT の匿名 LDAP バインド

デフォルトでは、Identity Management (IdM) LDAP サーバーへの匿名バインドが有効になっています。匿名バインドは、特定の設定またはディレクトリー値を公開できます。ただし、**reald** などの一部のユーティリティーや古い RHEL クライアントでは、クライアントの登録時にドメイン設定を検出する匿名バインドを有効にする必要があります。

関連情報

- 匿名バインドの無効化

8.3. 匿名バインドの無効化

LDAP ツールを使用して **nsslapd-allow-anonymous-access** 属性をリセットすることで、Identity Management (IdM) 389 Directory Server インスタンスで匿名バインドを無効にできます。

以下は **nsslapd-allow-anonymous-access** 属性の有効な値です。

- **on**: すべての匿名バインドを許可します (デフォルト)。
- **Rootdse**: root の DSE 情報についてのみ匿名バインドを許可します。
- **off**: 匿名バインドを拒否します。

Red Hat では、属性を **off** に設定して匿名バインドを完全に拒否すると、外部クライアントによるサーバー設定のチェックもブロックするため、この設定は推奨していません。LDAP および web クライアントはドメインクライアントに限られるわけではないため、こうしたクライアントは匿名で接続を行ってルートの DSE ファイルを読み取り接続情報を取得します。

nsslapd-allow-anonymous-access 属性の値を **rootdse** に変更すると、ディレクトリーデータにアクセスせずにルート DSE およびサーバー設定へのアクセスを許可します。

警告

特定のクライアントは、匿名バインドを使用して IdM 設定を検出します。また、compat ツリーは、認証を使用していない従来のクライアントでは機能しない可能性があります。この手順は、クライアントが匿名バインドを必要としない場合にのみ実行します。

前提条件

- Directory Manager として認証して LDAP サーバーに書き込むことができる。
- **root** ユーザーとして認証して IdM サービスを再起動できる。

手順

1. **nsslapd-allow-anonymous-access** 属性を **rootdse** に変更します。

```
$ ldapmodify -x -D "cn=Directory Manager" -W -h server.example.com -p 389
Enter LDAP Password:
dn: cn=config
changetype: modify
replace: nsslapd-allow-anonymous-access
nsslapd-allow-anonymous-access: rootdse

modifying entry "cn=config"
```

2. 389 Directory Server インスタンスを再起動して、新しい設定を読み込みます。

```
# systemctl restart dirsrv.target
```

検証

- **nsslapd-allow-anonymous-access** 属性の値を表示します。

```
$ ldapsearch -x -D "cn=Directory Manager" -b cn=config -W -h server.example.com  -p 389
nsslapd-allow-anonymous-access | grep nsslapd-allow-anonymous-access
Enter LDAP Password:
# requesting: nsslapd-allow-anonymous-access
nsslapd-allow-anonymous-access: rootdse
```

関連情報

- Directory Server 11 ドキュメントの nsslapd-allow-anonymous-access
- Identity Management の匿名 LDAP バインド

第9章 IDM ログファイルおよびディレクトリー

以下のセクションを使用して、Identity Management (IdM) の個々のコンポーネントを監視、分析、およびトラブルシューティングします。

- LDAP
- Apache Web Server
- Certificate System
- Kerberos
- DNS
- custodia

さらに、IdM サーバーおよびクライアント の監視、分析、トラブルシューティングを行い、IdM サーバーの監査ロギングの有効化 ができます。

9.1. IDM サーバーおよびクライアントのログファイルおよびディレクトリー

以下の表は、Identity Management (IdM) サーバーおよびクライアントが情報のログ記録に使用するディレクトリーおよびファイルを示しています。インストールエラーのトラブルシューティングには、ファイルおよびディレクトリーを使用できます。

ディレクトリーまたはファイル	説明
/var/log/ipaserver-install.log	IdM サーバーのインストールログ。
/var/log/ipareplica-install.log	IdM レプリカのインストールログ
/var/log/ipaclient-install.log	IdM クライアントのインストールログ
/var/log/sssd/	SSSD のログファイル。sssd.conf ファイル または sssctl コマンド で SSSD の詳細ロギングを有効化できます。
~/.ipa/log/cli.log	**ipa** ユーティリティーによる応答、リモートプロシージャーコール (RPC) で返されるエラーのログファイル。ツールを実行する **実効ユーザー** のホームディレクトリーに作成されます。このユーザーは、IdM ユーザープリンシパルとはユーザー名が異なる可能性があります。(これは、**ipa** コマンドの実行を試みて失敗する前にチケット保証チケット (TGT) 取得した IdM ユーザーです。)たとえば、**root** でシステムにログインし、IdM **管理者** の TGT を取得している場合は、エラーが **/root/.ipa/log/cli.log** ファイルに記録されます。
/etc/logrotate.d/	DNS、SSSD、Apache、Tomcat、および Kerberos のログローテーションのポリシー

ディレクトリーまたはファイル	説明
/etc/pki/pki-tomcat/logging.properties	このリンクは、**/usr/share/pki/server/conf/logging.properties** でデフォルトの認証局ロギング設定を参照します。

関連情報

- IdM サーバーのインストールに関するトラブルシューティング
- IdM クライアントのインストールに関するトラブルシューティング
- IdM レプリカのインストールに関するトラブルシューティング
- IdM で SSSD を使用した認証のトラブルシューティング

9.2. DIRECTORY SERVER のログファイル

以下の表は、Identity Management (IdM) Directory Server (DS) インスタンスが情報をログ記録に使用するディレクトリーおよびファイルを示しています。DS 関連の問題のトラブルシューティングには、ファイルおよびディレクトリーを使用できます。

表9.1 Directory Server のログファイル

ディレクトリーまたはファイル	説明
/var/log/dirsrv/slapd-REALM_NAME/	IdM サーバーが使用する DS インスタンスに関連付けられたログファイル。ここに記録されるほとんどの運用データは、サーバーとレプリカの相互作用に関連しています。
/var/log/dirsrv/slapd-REALM_NAME/audit	DS 設定で監査を有効にした場合のすべての DS 操作の監査証跡が含まれます。 **注記** IdM API がアクセスを記録する Apache エラーログを監査することもできます。ただし、LDAP 経由で直接変更できるため、Red Hat は監査目的でより包括的な **/var/log/dirsrv/slapd-REALM_NAME/audit** ログを有効にすることを推奨します。
/var/log/dirsrv/slapd-REALM_NAME/access	ドメイン DS インスタンスの試行したアクセスに関する詳細情報が含まれています。
/var/log/dirsrv/slapd-REALM_NAME/errors	ドメイン DS インスタンスの失敗した操作に関する詳細情報が含まれます。

関連情報

- サーバーおよびデータベースアクティビティーの監視

- ログファイルのリファレンス

9.3. IDM サーバーでの監査ロギングの有効化

監査目的で Identity Management (IdM) サーバーでのロギングを有効にするには、次の手順に従います。詳細なログを使用すると、データの監視、問題のトラブルシューティング、ネットワーク上の疑わしいアクティビティーを確認できます。

注記

特に値が大きい場合など、多くの LDAP 変更がログに記録されている場合、LDAP サービスが遅くなることがあります。

前提条件

- Directory Manager のパスワード

手順

1. LDAP サーバーにバインドします。

```
$ ldapmodify -D "cn=Directory Manager" -W << EOF
```

2. [Enter] を押します。
3. 作成するすべての変更を指定します。以下に例を示します。

```
dn: cn=config
changetype: modify
replace: nsslapd-auditlog-logging-enabled
nsslapd-auditlog-logging-enabled: on
-
replace:nsslapd-auditlog
nsslapd-auditlog: /var/log/dirsrv/slapd-REALM_NAME/audit
-
replace:nsslapd-auditlog-mode
nsslapd-auditlog-mode: 600
-
replace:nsslapd-auditlog-maxlogsize
nsslapd-auditlog-maxlogsize: 100
-
replace:nsslapd-auditlog-logrotationtime
nsslapd-auditlog-logrotationtime: 1
-
replace:nsslapd-auditlog-logrotationtimeunit
nsslapd-auditlog-logrotationtimeunit: day
```

4. 新しい行で **EOF** を入力して、**ldapmodify** コマンドの最後を示します。
5. [Enter] を 2 回押します。
6. 監査ロギングを有効にする他のすべての IdM サーバーで直前の手順を繰り返します。

検証

- **/var/log/dirsrv/slapd-REALM_NAME/audit** ファイルを開きます。

```
389-Directory/1.4.3.231 B2021.322.1803
server.idm.example.com:636 (/etc/dirsrv/slapd-IDM-EXAMPLE-COM)

time: 20220607102705
dn: cn=config
result: 0
changetype: modify
replace: nsslapd-auditlog-logging-enabled
nsslapd-auditlog-logging-enabled: on
[...]
```

ファイルが空ではない場合には、監査が有効になっていることが分かります。

重要

システムは、変更を行うエントリーのバインドされた LDAP 識別名 (DN) をログに記録します。このため、ログを後処理する必要がある場合があります。たとえば、IdM Directory Server では、レコードを変更する AD ユーザーの ID を表す ID オーバーライド DN になります。

```
$ modifiersName: ipaanchoruuid=:sid:s-1-5-21-19610888-1443184010-
1631745340-279100,cn=default trust
view,cn=views,cn=accounts,dc=idma,dc=idm,dc=example,dc=com
```

SID ユーザーがある場合は、**pysss_nss_idmap.getnamebysid** Python コマンドを使用して AD ユーザーを検索します。

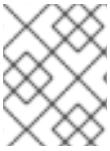
```
>>> import pysss_nss_idmap
>>> pysss_nss_idmap.getnamebysid('S-1-5-21-1273159419-3736181166-
4190138427-500'))
{'S-1-5-21-1273159419-3736181166-4190138427-500': {'name':
'administrator@ad.vm', 'type': 3}}
```

関連情報

- Red Hat Directory Server ドキュメントの Core サーバー設定属性 の監査ログ設定オプション
- IPA/IDM サーバーおよびレプリカサーバーの KCS で監査ロギングを有効にする方法
- Directory Server のログファイル

9.4. IDM サーバーでのエラーログの変更

特定の種類のエラーに関するデバッグ情報を取得するには、次の手順に従います。この例では、エラーログレベルを 8192 に設定して、レプリケーションに関する詳細なエラーログを取得することに重点を置いています。異なるタイプの情報を記録するには、Red Hat Directory Server ドキュメントの Error Log Logging Levels の表から別の番号を選択します。



注記

特に値が大きい場合に、LDAP サービスが多数のタイプをログに記録すると、処理が遅くなる可能性があります。

前提条件

- Directory Manager のパスワード。

手順

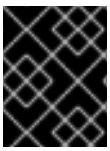
1. LDAP サーバーにバインドします。

```
$ ldapmodify -x -D "cn=directory manager" -w <password>
```

2. [Enter] を押します。
3. 変更する変更を指定します。たとえば、レプリケーションに関連するログのみを収集するには、以下を実行します。

```
dn: cn=config
changetype: modify
add: nsslapd-errorlog-level
nsslapd-errorlog-level: 8192
```

4. [Enter] を 2 回押して、**ldapmodify** 命令の最後を示します。これにより、**modifying entry "cn=config"** メッセージが表示されます。
5. [Ctrl+C] を押して **ldapmodify** コマンドを終了します。
6. レプリケーションエラーに関する詳細なログを収集する他のすべての IdM サーバーで直前の手順を繰り返します。



重要

トラブルシューティングが完了したら、**nsslapd-errorlog-level** を 0 に戻し、パフォーマンスの問題を防ぎます。

関連情報

- Directory Server エラーログレベル

9.5. IDM APACHE サーバーのログファイル

以下の表は、Identity Management (IdM) Apache Server が情報をログに記録するために使用するディレクトリーおよびファイルを示しています。

表9.2 Apache サーバーのログファイル

ディレクトリーまたはファイル	説明
/var/log/httpd/	Apache Web サーバーのログファイル。

ディレクトリーまたはファイル	説明
/var/log/httpd/access_log	これは、Apache サーバーの標準的なアクセスログおよびエラーログです。IdM Web UI および RPC コマンドラインインターフェイスは Apache を使用するため、IdM 固有のメッセージは Apache メッセージとともに記録されます。アクセスログは、主にユーザープリンシパルと使用される URI のみをログに記録します。多くの場合、これは RPC エンドポイントです。エラーログには IdM サーバーログが含まれます。
/var/log/httpd/error_log	

関連情報

- Apache ドキュメントの ログファイル

9.6. IDM の CERTIFICATE SYSTEM のログファイル

以下の表は、Identity Management (IdM) Certificate System が情報のログ記録に使用するディレクトリーおよびファイルを示しています。

表9.3 Certificate System のログファイル

ディレクトリーまたはファイル	説明
/var/log/pki/pki-ca-spawn.time_of_installation.log	IdM 認証局 (CA) のインストールログ。
/var/log/pki/pki-kra-spawn.time_of_installation.log	IdM Key Recovery Authority (KRA) のインストールログ。
/var/log/pki/pki-tomcat/	PKI 操作ログのトップレベルディレクトリー。CA ログおよび KRA ログが含まれます。
/var/log/pki/pki-tomcat/ca/	証明書の操作に関連するログを含むディレクトリー。IdM では、このログは証明書を使用するサービスプリンシパル、ホスト、およびその他のエンティティーに使用されます。
/var/log/pki/pki-tomcat/kra	KRA に関連するログを含むディレクトリー。
/var/log/messages	証明書のエラーメッセージがその他のシステムメッセージに含まれます。

関連情報

- Red Hat Certificate System **管理ガイド** の サブシステムのログの設定

9.7. IDM の KERBEROS ログファイル

以下の表は、Kerberos が Identity Management (IdM) に情報をログに記録するために使用するディレクトリーおよびファイルを示しています。

表9.4 Kerberos ログファイル

ディレクトリーまたはファイル	説明
/var/log/krb5kdc.log	これは、Kerberos KDC サーバーの主なログファイルです。
/var/log/kadmind.log	Kerberos 管理システムサーバーの主なログファイルです。
これらのファイルの場所は **krb5.conf** ファイルで設定されます。システムによっては異なる場合があります。	

9.8. IDM の DNS ログファイル

以下の表は、DNS が Identity Management (IdM) に情報をログに記録するために使用するディレクトリーおよびファイルを示しています。

表9.5 DNS ログファイル

ディレクトリーまたはファイル	説明
/var/log/messages	DNS エラーメッセージおよびその他のシステムメッセージが含まれます。このファイルの DNS ロギングは、デフォルトでは有効になりません。これを有効にするには、**# /usr/sbin/rndc querylog** コマンドを実行します。このコマンドを実行すると、次の行が **var/log/messages** に追加されます。 **Jun 26 17:37:33 r8server named-pkcs11[1445]: received control channel command 'querylog'** **Jun 26 17:37:33 r8server named-pkcs11[1445]: query logging is now on** ロギングを無効にするには、コマンドを再度実行します。

9.9. IDM の CUSTODIA ログファイル

以下の表は、Custodia が Identity Management (IdM) に情報をログに記録するために使用するディレクトリーおよびファイルを示しています。

表9.6 Custodia ログファイル

ディレクトリーまたはファイル	説明
/var/log/custodia/	Custodia サービスのログファイルディレクトリー。

9.10. 関連情報

- ログファイルの表示**journalctl** を使用すると、**systemd** ユニットファイルのログ出力を表示できます。