# Red Hat Enterprise Linux 9

## Accès aux services de gestion de l'identité

Se connecter à l'IdM et gérer ses services

Last Updated: 2024-02-18

# Red Hat Enterprise Linux 9 Accès aux services de gestion de l'identité

Se connecter à l'IdM et gérer ses services

## Notice légale



## Résumé

Avant de pouvoir effectuer des tâches d'administration dans Red Hat Identity Management (IdM), vous devez vous connecter au service. Vous pouvez utiliser Kerberos et des mots de passe à usage unique comme méthodes d'authentification dans IdM lorsque vous vous connectez à l'aide de la ligne de commande ou de l'interface Web IdM.

# Table des matières

# RENDRE L'OPEN SOURCE PLUS INCLUSIF

Red Hat s'engage à remplacer les termes problématiques dans son code, sa documentation et ses propriétés Web. Nous commençons par ces quatre termes : master, slave, blacklist et whitelist. En raison de l'ampleur de cette entreprise, ces changements seront mis en œuvre progressivement au cours de plusieurs versions à venir. Pour plus de détails, voir le message de notre directeur technique Chris Wright.

Dans le domaine de la gestion de l'identité, les remplacements terminologiques prévus sont les suivants :

- ***block list*** remplace *blacklist*
- ***allow list*** remplace *whitelist*
- ***secondary*** remplace *slave*
- Le mot *master* est remplacé par un langage plus précis, en fonction du contexte :
  - ***IdM server*** remplace *IdM master*
  - ***CA renewal server*** remplace *CA renewal master*
  - ***CRL publisher server*** remplace *CRL master*
  - ***multi-supplier*** remplace *multi-master*

# FOURNIR UN RETOUR D'INFORMATION SUR LA DOCUMENTATION DE RED HAT

Nous apprécions vos commentaires sur notre documentation. Faites-nous savoir comment nous pouvons l'améliorer.

**Soumettre des commentaires sur des passages spécifiques**

1. Consultez la documentation au format **Multi-page HTML** et assurez-vous que le bouton **Feedback** apparaît dans le coin supérieur droit après le chargement complet de la page.
2. Utilisez votre curseur pour mettre en évidence la partie du texte que vous souhaitez commenter.
3. Cliquez sur le bouton **Add Feedback** qui apparaît près du texte en surbrillance.
4. Ajoutez vos commentaires et cliquez sur **Submit**.

**Soumettre des commentaires via Bugzilla (compte requis)**

1. Connectez-vous au site Web de Bugzilla.
2. Sélectionnez la version correcte dans le menu **Version**.
3. Saisissez un titre descriptif dans le champ **Summary**.
4. Saisissez votre suggestion d'amélioration dans le champ **Description**. Incluez des liens vers les parties pertinentes de la documentation.
5. Cliquez sur **Submit Bug**.

# CHAPITRE 1. SE CONNECTER À LA GESTION DES IDENTITÉS À PARTIR DE LA LIGNE DE COMMANDE

La gestion des identités (IdM) utilise le protocole Kerberos pour prendre en charge l'authentification unique. L'authentification unique signifie que l'utilisateur ne saisit qu'une seule fois le nom d'utilisateur et le mot de passe corrects, puis accède aux services IdM sans que le système ne lui demande à nouveau ses informations d'identification.

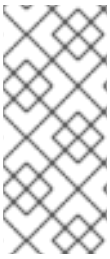
IMPORTANT

Dans l'IdM, le System Security Services Daemon (SSSD) obtient automatiquement un ticket d'attribution de ticket (TGT) pour un utilisateur après que celui-ci s'est connecté avec succès à l'environnement de bureau sur une machine cliente IdM avec le nom de principal Kerberos correspondant. Cela signifie qu'après s'être connecté, l'utilisateur n'est pas obligé d'utiliser l'utilitaire **kinit** pour accéder aux ressources IdM.

Si vous avez effacé votre cache de justificatifs Kerberos ou si votre TGT Kerberos a expiré, vous devez demander manuellement un ticket Kerberos pour accéder aux ressources de l'IdM. Les sections suivantes présentent les opérations de base de l'utilisateur lors de l'utilisation de Kerberos dans IdM.

## 1.1. UTILISATION DE KINIT POUR SE CONNECTER MANUELLEMENT À IDM

Cette procédure décrit l'utilisation de l'utilitaire **kinit** pour s'authentifier manuellement auprès d'un environnement de gestion des identités (IdM). L'utilitaire **kinit** obtient et met en cache un ticket Kerberos (TGT) au nom d'un utilisateur IdM.



NOTE

N'utilisez cette procédure que si vous avez détruit votre TGT Kerberos initial ou s'il a expiré. En tant qu'utilisateur IdM, lorsque vous vous connectez à votre machine locale, vous vous connectez aussi automatiquement à IdM. Cela signifie qu'après vous être connecté, vous n'avez pas besoin d'utiliser l'utilitaire **kinit** pour accéder aux ressources IdM.

**Procédure**

1. Pour se connecter à l'IdM

   - sous le nom d'utilisateur de l'utilisateur actuellement connecté sur le système local, utilisez **kinit** sans spécifier de nom d'utilisateur. Par exemple, si vous êtes connecté en tant que **example_user** sur le système local :

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

     Si le nom d'utilisateur de l'utilisateur local ne correspond à aucune entrée d'utilisateur dans IdM, la tentative d'authentification échoue :

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

- en utilisant un principal Kerberos qui ne correspond pas à votre nom d'utilisateur local, transmettez le nom d'utilisateur requis à l'utilitaire **kinit**. Par exemple, pour vous connecter en tant qu'utilisateur **admin**:

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

2. En option, pour vérifier que la connexion a réussi, utilisez l'utilitaire **klist** pour afficher le TGT mis en cache. Dans l'exemple suivant, le cache contient un ticket pour le principal **example_user**, ce qui signifie que sur cet hôte particulier, seul **example_user** est actuellement autorisé à accéder aux services IdM :

```
$ 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. DESTRUCTION DU TICKET KERBEROS ACTIF D'UN UTILISATEUR

Cette section explique comment effacer le cache des informations d'identification qui contient le ticket Kerberos actif de l'utilisateur.

**Procédure**

1. Pour détruire votre ticket Kerberos :

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

2. Optionnellement, pour vérifier que le ticket Kerberos a été détruit :

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

## 1.3. CONFIGURATION D'UN SYSTÈME EXTERNE POUR L'AUTHENTIFICATION KERBEROS

Cette section décrit comment configurer un système externe pour que les utilisateurs de la gestion des identités (IdM) puissent se connecter à l'IdM à partir du système externe à l'aide de leurs informations d'identification Kerberos.

L'activation de l'authentification Kerberos sur les systèmes externes est particulièrement utile lorsque votre infrastructure comprend plusieurs royaumes ou domaines qui se chevauchent. Elle est également utile si le système n'a été enrôlé dans aucun domaine IdM par le biais de **ipa-client-install**.

Pour permettre l'authentification Kerberos à l'IdM à partir d'un système qui n'est pas membre du domaine IdM, définissez un fichier de configuration Kerberos spécifique à l'IdM sur le système externe.

**Conditions préalables**

- Le paquet **krb5-workstation** est installé sur le système externe.
  Pour savoir si le paquet est installé, utilisez la commande CLI suivante :

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

**Procédure**

1. Copiez le fichier **/etc/krb5.conf** du serveur IdM vers le système externe. Par exemple :

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

AVERTISSEMENT

N'écrasez pas le fichier **krb5.conf** existant sur le système externe.

2. Sur le système externe, configurez la session de terminal pour qu'elle utilise le fichier de configuration IdM Kerberos copié :

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

   La variable **KRB5_CONFIG** n'existe que temporairement, jusqu'à ce que vous vous déconnectiez. Pour éviter cette perte, exportez la variable avec un nom de fichier différent.

3. Copiez les extraits de configuration Kerberos du répertoire **/etc/krb5.conf.d/** vers le système externe.

Les utilisateurs du système externe peuvent désormais utiliser l'utilitaire **kinit** pour s'authentifier auprès du serveur IdM.

## 1.4. RESSOURCES SUPPLÉMENTAIRES

- La page de manuel **krb5.conf(5)**.
- La page de manuel **kinit(1)**.
- La page de manuel **klist(1)**.
- La page de manuel **kdestroy(1)**.

# CHAPITRE 2. VISUALISATION, DÉMARRAGE ET ARRÊT DES SERVICES DE GESTION DES IDENTITÉS

Les serveurs de gestion d'identité (IdM) sont des systèmes Red Hat Enterprise Linux qui fonctionnent comme des contrôleurs de domaine (DC). Un certain nombre de services différents sont exécutés sur les serveurs IdM, notamment le serveur d'annuaire, l'autorité de certification (CA), le DNS et Kerberos.

## 2.1. LES SERVICES IDM

Cette section décrit les services qui peuvent être installés et exécutés sur les serveurs et les clients IdM.

### Liste des services hébergés par les serveurs IdM

La plupart des services suivants ne doivent pas obligatoirement être installés sur le serveur IdM. Par exemple, vous pouvez installer des services tels qu'une autorité de certification (CA) ou un serveur DNS sur un serveur externe en dehors du domaine IdM.

**Kerberos**

les services **krb5kdc** et **kadmin**

IdM utilise le protocole **Kerberos** pour prendre en charge l'authentification unique. Avec Kerberos, les utilisateurs ne doivent présenter qu'une seule fois le nom d'utilisateur et le mot de passe corrects et peuvent accéder aux services IdM sans que le système ne leur demande à nouveau leurs informations d'identification.

Kerberos est divisé en deux parties :

- Le service **krb5kdc** est le service d'authentification Kerberos et le démon du centre de distribution de clés (KDC).
- Le service **kadmin** est le programme d'administration de la base de données Kerberos.

Pour plus d'informations sur l'authentification à l'aide de Kerberos dans IdM, voir Connexion à Identity Management à partir de la ligne de commande et Connexion à IdM dans l'interface Web : Utilisation d'un ticket Kerberos.

**Serveur d'annuaire LDAP**

le service **dirsrv**

L'instance IdM **LDAP directory server** stocke toutes les informations IdM, telles que les informations relatives à Kerberos, aux comptes d'utilisateurs, aux entrées d'hôtes, aux services, aux politiques, au DNS, etc. L'instance du serveur d'annuaire LDAP est basée sur la même technologie que Red Hat Directory Server. Cependant, elle est adaptée aux tâches spécifiques à l'IdM.

**Autorité de certification**

le service **pki-tomcatd**

Le site intégré **certificate authority (CA)** est basé sur la même technologie que le système de certification Red Hat. **pki** est l'interface de ligne de commande pour accéder aux services du système de certification.

Vous pouvez également installer le serveur sans l'autorité de certification intégrée si vous créez et fournissez tous les certificats requis de manière indépendante.

Pour plus d'informations, voir Planification des services de l'AC.

**Système de noms de domaine (DNS)**

le service **named**

IdM utilise **DNS** pour la découverte dynamique de services. L'utilitaire d'installation du client IdM peut utiliser les informations du DNS pour configurer automatiquement la machine cliente. Une fois que le client est inscrit dans le domaine IdM, il utilise le DNS pour localiser les serveurs et les services IdM dans le domaine. L'implémentation **BIND** (Berkeley Internet Name Domain) des protocoles DNS (Domain Name System) dans Red Hat Enterprise Linux inclut le serveur DNS **named**. **named-pkcs11** est une version du serveur DNS BIND construite avec une prise en charge native de la norme cryptographique PKCS#11.

Pour plus d'informations, voir Planification des services DNS et des noms d'hôtes .

**Serveur HTTP Apache**

le service **httpd**

Le site **Apache HTTP web server** fournit l'interface Web IdM et gère également la communication entre l'autorité de certification et les autres services IdM.

**Samba / Winbind**

**smb** et **winbind** services

Samba met en œuvre le protocole Server Message Block (SMB), également connu sous le nom de protocole Common Internet File System (CIFS), dans Red Hat Enterprise Linux. Via le service smb, le protocole SMB vous permet d'accéder aux ressources d'un serveur, telles que les partages de fichiers et les imprimantes partagées. Si vous avez configuré un Trust avec un environnement Active Directory (AD), le service "Winbind" gère la communication entre les serveurs IdM et les serveurs AD.

**Authentification par mot de passe à usage unique (OTP)**

les services **ipa-otpd**

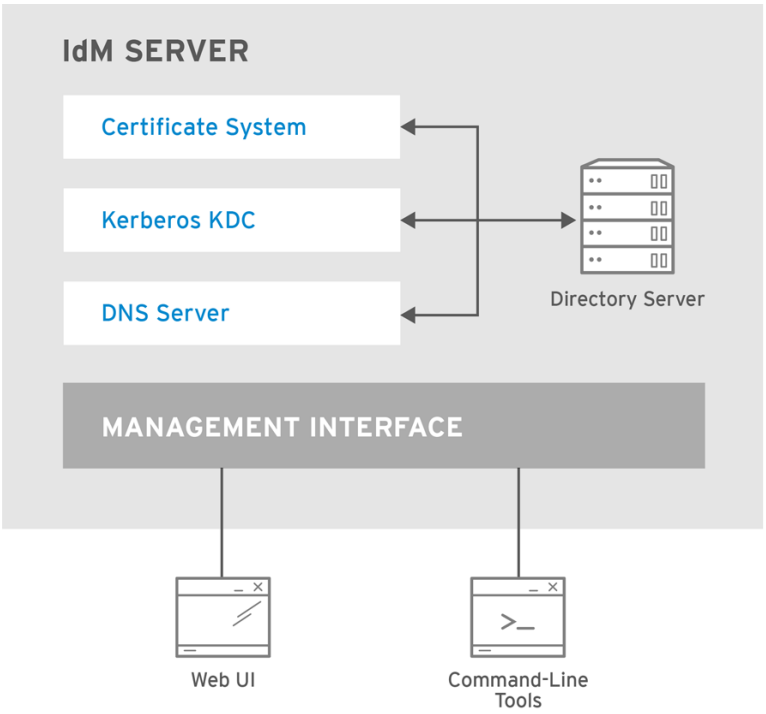
Les mots de passe à usage unique (OTP) sont des mots de passe générés par un jeton d'authentification pour une seule session, dans le cadre de l'authentification à deux facteurs. L'authentification OTP est mise en œuvre dans Red Hat Enterprise Linux via le service **ipa-otpd**.

Pour plus d'informations, voir Connexion à l'interface Web de gestion des identités à l'aide de mots de passe à usage unique.

**OpenDNSSEC**

le service **ipa-dnskeysyncd**

**OpenDNSSEC** est un gestionnaire DNS qui automatise le processus de suivi des clés DNSSEC (DNS security extensions) et la signature des zones. Le service **ipa-dnskeysyncd** gère la synchronisation entre le serveur d'annuaire IdM et OpenDNSSEC.




**Liste des services hébergés par les clients IdM**

- **System Security Services Daemon**: le service **sssd**

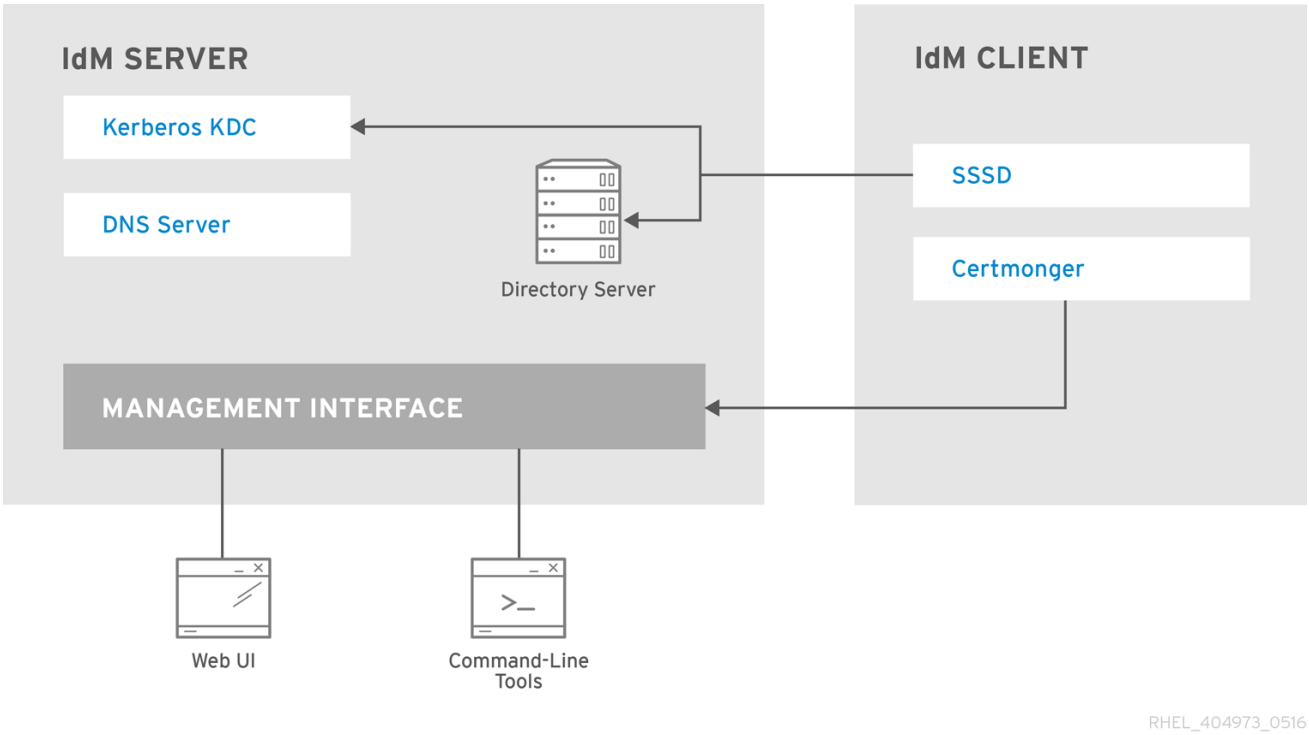
Le site **System Security Services Daemon** (SSSD) est l'application côté client qui gère l'authentification des utilisateurs et la mise en cache des informations d'identification. La mise en cache permet au système local de poursuivre les opérations d'authentification normales si le serveur IdM devient indisponible ou si le client se déconnecte.

Pour plus d'informations, voir Comprendre le SSSD et ses avantages .

- **Certmonger**: le service **certmonger**

Le service **certmonger** surveille et renouvelle les certificats sur le client. Il peut demander de nouveaux certificats pour les services du système.

Pour plus d'informations, voir Obtention d'un certificat IdM pour un service à l'aide de certmonger .

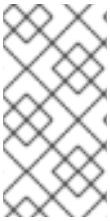



## 2.2. VISUALISATION DE L'ÉTAT DES SERVICES IDM

Pour afficher l'état des services IdM configurés sur votre serveur IdM, exécutez la commande **ipactl status**:

```
[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
```

Le résultat de la commande **ipactl status** sur votre serveur dépend de votre configuration IdM. Par exemple, si un déploiement IdM n'inclut pas de serveur DNS, le service **named** ne figure pas dans la liste.



NOTE

Vous ne pouvez pas utiliser l'interface web IdM pour visualiser l'état de tous les services IdM fonctionnant sur un serveur IdM particulier. Les services Kerberized fonctionnant sur différents serveurs peuvent être visualisés dans l'onglet **Identity → Services** de l'interface web IdM.

Vous pouvez démarrer ou arrêter l'ensemble du serveur, ou seulement un service individuel.

Pour démarrer, arrêter ou redémarrer l'ensemble du serveur IdM, voir :

- Démarrage et arrêt de l'ensemble du serveur de gestion des identités

Pour démarrer, arrêter ou redémarrer un service IdM individuel, voir :

- Démarrage et arrêt d'un service individuel de gestion des identités

Pour afficher la version du logiciel IdM, voir :

- Méthodes d'affichage de la version du logiciel IdM

## 2.3. DÉMARRAGE ET ARRÊT DE L'ENSEMBLE DU SERVEUR DE GESTION DES IDENTITÉS

Utilisez le service **ipa** systemd pour arrêter, démarrer ou redémarrer l'ensemble du serveur IdM ainsi que tous les services installés. L'utilisation de l'utilitaire **systemctl** pour contrôler le service **ipa** systemd garantit que tous les services sont arrêtés, démarrés ou redémarrés dans l'ordre approprié. Le service **ipa** systemd met également à jour la configuration RHEL IdM avant de démarrer les services IdM et utilise les contextes SELinux appropriés lors de l'administration des services IdM. Il n'est pas nécessaire d'avoir un ticket Kerberos valide pour exécuter les commandes **systemctl ipa**.

### ipa commandes du service systemd

Pour démarrer l'ensemble du serveur IdM :

```
# systemctl start ipa
```

Pour arrêter l'ensemble du serveur IdM :

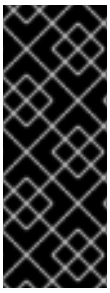
```
# systemctl stop ipa
```

Pour redémarrer l'ensemble du serveur IdM :

```
# systemctl restart ipa
```

Pour afficher l'état de tous les services qui composent IdM, utilisez l'utilitaire **ipactl**:

```
# ipactl status
```



IMPORTANT

- N'utilisez pas directement l'utilitaire **ipactl** pour démarrer, arrêter ou redémarrer les services IdM. Utilisez plutôt les commandes **systemctl ipa**, qui appellent l'utilitaire **ipactl** dans un environnement prévisible.
- Vous ne pouvez pas utiliser l'interface web IdM pour exécuter les commandes **ipactl**.

## 2.4. DÉMARRAGE ET ARRÊT D'UN SERVICE INDIVIDUEL DE GESTION DES IDENTITÉS

Il n'est généralement pas recommandé de modifier manuellement les fichiers de configuration de l'IdM. Cependant, certaines situations exigent qu'un administrateur effectue une configuration manuelle de services spécifiques. Dans ce cas, utilisez l'utilitaire **systemctl** pour arrêter, démarrer ou redémarrer un

service IdM individuel.

Par exemple, utilisez **systemctl** après avoir personnalisé le comportement du serveur d'annuaire, sans modifier les autres services IdM :

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

De plus, lors du déploiement initial d'une confiance IdM avec Active Directory, modifiez le fichier **/etc/sssd/sssd.conf** en ajoutant :

- des paramètres spécifiques pour ajuster les options de configuration du délai d'attente dans un environnement où les serveurs distants ont un temps de latence élevé
- paramètres spécifiques pour régler l'affinité de site Active Directory
- les dérogations pour certaines options de configuration qui ne sont pas fournies par les paramètres globaux de l'IdM

Pour appliquer les modifications que vous avez apportées au fichier **/etc/sssd/sssd.conf**:

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

L'exécution de **systemctl restart sssd.service** est nécessaire car le System Security Services Daemon (SSSD) ne relit pas ou n'applique pas automatiquement sa configuration.

Notez que pour les changements qui affectent les plages d'identité IdM, un redémarrage complet du serveur est recommandé.

IMPORTANT

Pour redémarrer plusieurs services du domaine IdM, utilisez toujours **systemctl restart ipa**. En raison des dépendances entre les services installés avec le serveur IdM, l'ordre dans lequel ils sont démarrés et arrêtés est critique. Le service **ipa** systemd veille à ce que les services soient démarrés et arrêtés dans l'ordre approprié.

### Commandes utiles systemctl

Pour démarrer un service IdM particulier :

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

Pour arrêter un service IdM particulier :

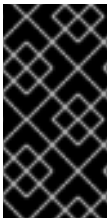
```
# systemctl stop name.service
```

Pour redémarrer un service IdM particulier :

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

Pour consulter l'état d'un service IdM particulier :

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



**IMPORTANT**

Vous ne pouvez pas utiliser l'interface web IdM pour démarrer ou arrêter les services individuels fonctionnant sur les serveurs IdM. Vous ne pouvez utiliser l'interface web que pour modifier les paramètres d'un service Kerberized en naviguant vers **Identity → Services** et en sélectionnant le service.

**Ressources supplémentaires**

- Démarrage et arrêt de l'ensemble du serveur de gestion des identités

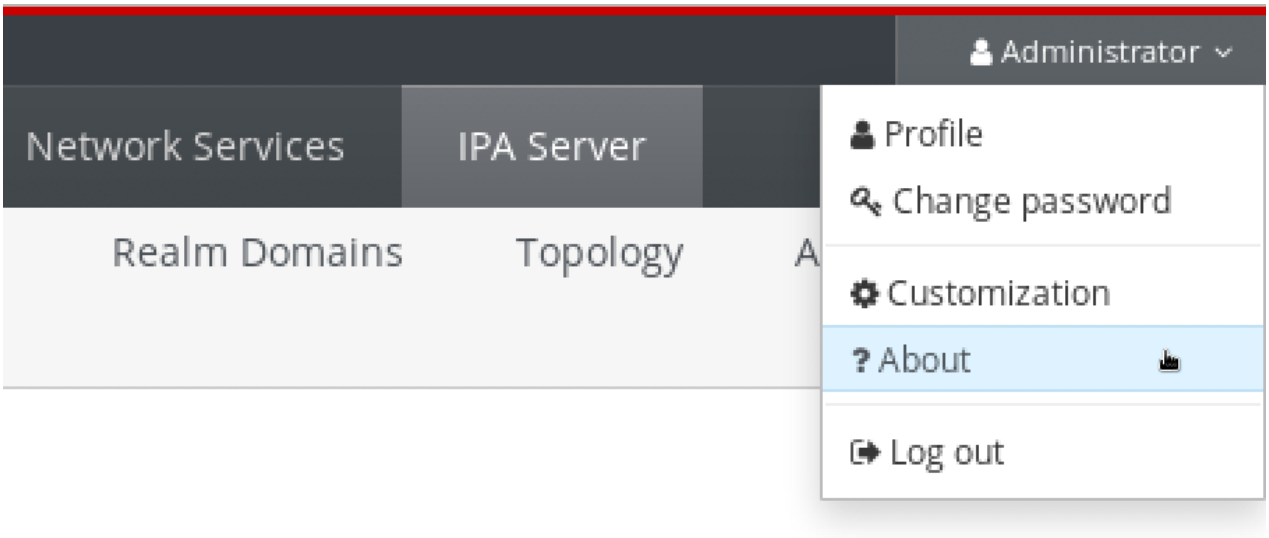
## 2.5. MÉTHODES D'AFFICHAGE DE LA VERSION DU LOGICIEL IDM

Vous pouvez afficher le numéro de version de l'IdM avec :

- l'interface Web de l'IdM
- **ipa** commandes
- **rpm** commandes

**Affichage de la version via l'interface WebUI**

Dans l'IdM WebUI, la version du logiciel peut être affichée en choisissant **About** dans le menu du nom d'utilisateur en haut à droite.




**Affichage de la version avec les commandesipa**

À partir de la ligne de commande, utilisez la commande **ipa --version**.

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

**Affichage de la version avec les commandesrpm**

Si les services IdM ne fonctionnent pas correctement, vous pouvez utiliser l'utilitaire **rpm** pour déterminer le numéro de version du paquetage **ipa-server** actuellement installé.

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

# CHAPITRE 3. INTRODUCTION AUX UTILITAIRES DE LA LIGNE DE COMMANDE IDM

Les sections suivantes décrivent les bases de l'utilisation des utilitaires de ligne de commande de la gestion des identités (IdM).

**Conditions préalables**

- Serveur IdM installé et accessible.
  Pour plus de détails, voir Installation de la gestion des identités .
- Pour utiliser l'interface de ligne de commande de l'IPA, authentifiez-vous auprès de l'IdM à l'aide d'un ticket Kerberos valide.

## 3.1. QU'EST-CE QUE L'INTERFACE DE LIGNE DE COMMANDE DE L'IPA ?

L'interface de ligne de commande (CLI) de l'IPA est l'interface de ligne de commande de base pour l'administration de la gestion des identités (IdM).

Il prend en charge de nombreuses sous-commandes pour la gestion de l'IdM, telles que la commande **ipa user-add** pour ajouter un nouvel utilisateur.

L'interface CLI de l'IPA vous permet de

- Ajouter, gérer ou supprimer des utilisateurs, des groupes, des hôtes et d'autres objets dans le réseau.
- Gérer les certificats.
- Entrées de recherche.
- Afficher et répertorier des objets.
- Définir les droits d'accès.
- Obtenir de l'aide sur la syntaxe correcte de la commande.

## 3.2. QU'EST-CE QUE L'AIDE IPA ?

L'aide IPA est un système de documentation intégré au serveur IdM.

L'interface de ligne de commande (CLI) IPA génère les rubriques d'aide disponibles à partir des modules d'extension IdM chargés. Pour utiliser l'utilitaire d'aide de l'IPA, vous devez :

- Un serveur IdM doit être installé et fonctionner.
- Être authentifié par un ticket Kerberos valide.

La saisie de la commande **ipa help** sans options affiche des informations sur l'utilisation de l'aide de base et les exemples de commandes les plus courants.

Vous pouvez utiliser les options suivantes pour les différents cas d'utilisation de **ipa help**:

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

- **[]**- Les parenthèses signifient que tous les paramètres sont facultatifs et que vous pouvez écrire seulement **ipa help** pour que la commande soit exécutée.
- |- Le caractère "pipe" signifie **or**. Par conséquent, vous pouvez spécifier un **TOPIC**, un **COMMAND**, ou un **topics**, ou un **commands**, avec la commande de base **ipa help**:
  - **topics**- Vous pouvez exécuter la commande **ipa help topics** pour afficher une liste de sujets couverts par l'aide IPA, tels que **user**, **cert**, **server** et bien d'autres.
  - **TOPIC**- Le **TOPIC** avec des lettres majuscules est une variable. Vous pouvez donc spécifier un sujet particulier, par exemple **ipa help user**.
  - **commands**- Vous pouvez entrer la commande **ipa help commands** pour afficher une liste de commandes couvertes par l'aide IPA, par exemple, **user-add**, **ca-enable**, **server-show** et bien d'autres.
  - **COMMAND**- Le **COMMAND** avec des lettres majuscules est une variable. Vous pouvez donc spécifier une commande particulière, par exemple **ipa help user-add**.

## 3.3. UTILISATION DES RUBRIQUES D'AIDE DE L'IPA

La procédure suivante décrit comment utiliser l'aide IPA dans l'interface de ligne de commande.

**Procédure**

1. Ouvrez un terminal et connectez-vous au serveur IdM.
2. Saisissez **ipa help topics** pour afficher une liste des sujets couverts par l'aide.

   ```
   $ ipa help topics
   ```

3. Sélectionnez l'un des sujets et créez une commande selon le modèle suivant : **ipa help *[topic_name]***. À la place de la chaîne **topic_name**, ajoutez l'un des thèmes énumérés à l'étape précédente.
   Dans l'exemple, nous utilisons le sujet suivant : **user**

   ```
   $ ipa help user
   ```

4. Si l'aide IPA est trop longue et que vous ne pouvez pas voir l'intégralité du texte, utilisez la syntaxe suivante :

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

   Vous pouvez ensuite faire défiler la page et lire l'intégralité de l'aide.

L'interface de programmation IPA affiche une page d'aide pour la rubrique **user**. Après avoir lu l'aperçu, vous pouvez voir de nombreux exemples avec des modèles pour travailler avec les commandes de la rubrique.

## 3.4. UTILISATION DES COMMANDES D'AIDE DE L'IPA

La procédure suivante décrit comment créer des commandes d'aide IPA dans l'interface de ligne de commande.

**Procédure**

1. Ouvrez un terminal et connectez-vous au serveur IdM.
2. Saisissez **ipa help commands** pour afficher la liste des commandes couvertes par l'aide.

```
$ ipa help commands
```

3. Sélectionnez l'une des commandes et créez une commande d'aide selon le modèle suivant : **ipa help *<COMMAND>***. À la place de la chaîne **<COMMAND>**, ajoutez l'une des commandes énumérées à l'étape précédente.

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

**Ressources supplémentaires**

- La page de manuel **ipa**.

## 3.5. STRUCTURE DES COMMANDES IPA

L'interface de programmation IPA distingue les types de commandes suivants :

- **Built-in commands**- Les commandes intégrées sont toutes disponibles dans le serveur IdM.
- **Plug-in provided commands**

La structure des commandes IPA permet de gérer différents types d'objets. Par exemple :

- Utilisateurs,
- Hôtes,
- Enregistrements DNS,
- Certificats,

et bien d'autres.

Pour la plupart de ces objets, l'interface CLI de l'IPA comprend des commandes pour :

- Ajouter (**add**)
- Modifier (**mod**)
- Supprimer (**del**)
- Recherche (**find**)
- Affichage (**show**)

Les commandes ont la structure suivante :

**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**

Vous pouvez créer un utilisateur à l'aide de la commande **ipa user-add [options]**, où **[options]** est facultatif. Si vous n'utilisez que la commande **ipa user-add**, le script vous demande les détails un par un.

Pour modifier un objet existant, vous devez définir l'objet, c'est pourquoi la commande comprend également un objet : **ipa user-mod USER_NAME [options]**.

## 3.6. UTILISATION D'UNE COMMANDE IPA POUR AJOUTER UN COMPTE D'UTILISATEUR À IDM

La procédure suivante décrit comment ajouter un nouvel utilisateur à la base de données Identity Management (IdM) à l'aide de la ligne de commande.

**Conditions préalables**

- Vous devez disposer de privilèges d'administrateur pour ajouter des comptes d'utilisateurs au serveur IdM.

**Procédure**

1. Ouvrez un terminal et connectez-vous au serveur IdM.
2. Entrez la commande pour ajouter un nouvel utilisateur :

   ```
   $ ipa user-add
   ```

   La commande exécute un script qui vous invite à fournir les données de base nécessaires à la création d'un compte utilisateur.
3. Dans le champ **First name:**, entrez le prénom du nouvel utilisateur et appuyez sur la touche **Enter**.
4. Dans le champ **Last name:**, entrez le nom de famille du nouvel utilisateur et appuyez sur la touche **Enter**.
5. Dans le champ **User login [suggested user name]:** entrez le nom d'utilisateur ou appuyez simplement sur la touche **Enter** pour accepter le nom d'utilisateur proposé.
   Le nom d'utilisateur doit être unique pour toute la base de données IdM. Si une erreur survient parce que ce nom d'utilisateur existe déjà, répétez le processus avec la commande **ipa user-add** et utilisez un nom d'utilisateur différent et unique.

Une fois le nom d'utilisateur ajouté, le compte d'utilisateur est ajouté à la base de données IdM et l'interface de ligne de commande (CLI) de l'API affiche la sortie suivante :

```
----------------------
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
```

NOTE

Par défaut, aucun mot de passe n'est défini pour le compte d'utilisateur. Pour ajouter un mot de passe lors de la création d'un compte utilisateur, utilisez la commande **ipa user-add** avec la syntaxe suivante :

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

L'interface CLI de l'IPA vous invite ensuite à ajouter ou à confirmer un nom d'utilisateur et un mot de passe.

Si l'utilisateur a déjà été créé, vous pouvez ajouter le mot de passe à l'aide de la commande **ipa user-mod**.

**Ressources supplémentaires**

- Exécutez la commande **ipa help user-add** pour plus d'informations sur les paramètres.

## 3.7. UTILISATION D'UNE COMMANDE IPA POUR MODIFIER UN COMPTE D'UTILISATEUR DANS IDM

Vous pouvez modifier de nombreux paramètres pour chaque compte d'utilisateur. Par exemple, vous pouvez ajouter un nouveau mot de passe à l'utilisateur.

La syntaxe de la commande de base est différente de celle de **user-add** car vous devez définir le compte d'utilisateur existant pour lequel vous souhaitez effectuer des modifications, par exemple, ajouter un mot de passe.

**Conditions préalables**

- Vous devez disposer des droits d'administrateur pour modifier les comptes d'utilisateurs.

**Procédure**

1. Ouvrez un terminal et connectez-vous au serveur IdM.
2. Entrez la commande **ipa user-mod**, indiquez l'utilisateur à modifier et les options éventuelles, telles que **--password** pour l'ajout d'un mot de passe :

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

La commande lance un script dans lequel vous pouvez ajouter le nouveau mot de passe.

3. Saisissez le nouveau mot de passe et appuyez sur la touche **Enter**.

L'interface de programmation de l'IPA affiche la sortie suivante :

```
----------------------
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
```

Le mot de passe de l'utilisateur est maintenant défini pour le compte et l'utilisateur peut se connecter à IdM.

**Ressources supplémentaires**

- Exécutez la commande **ipa help user-mod** pour plus d'informations sur les paramètres.

## 3.8. COMMENT FOURNIR UNE LISTE DE VALEURS AUX UTILITAIRES IDM ?

La gestion de l'identité (IdM) stocke les valeurs des attributs à valeurs multiples dans des listes.

L'IdM prend en charge les méthodes suivantes pour fournir des listes à valeurs multiples :

- Utilisation du même argument de ligne de commande plusieurs fois dans la même invocation de commande :

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

- Vous pouvez également placer la liste entre accolades, auquel cas l'interpréteur de commandes procède à l'expansion :

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

Les exemples ci-dessus montrent une commande **permission-add** qui ajoute des autorisations à un objet. L'objet n'est pas mentionné dans l'exemple. Au lieu de **...** vous devez ajouter l'objet pour lequel vous souhaitez ajouter des autorisations.

Lorsque vous mettez à jour de tels attributs à valeurs multiples à partir de la ligne de commande, l'IdM écrase complètement la liste précédente de valeurs par une nouvelle liste. Par conséquent, lorsque vous mettez à jour un attribut à valeurs multiples, vous devez spécifier l'ensemble de la nouvelle liste, et non pas une seule valeur que vous souhaitez ajouter.

Par exemple, dans la commande ci-dessus, la liste des autorisations comprend la lecture, l'écriture et la suppression. Lorsque vous décidez de mettre à jour la liste avec la commande **permission-mod** vous devez ajouter toutes les valeurs, sinon celles qui ne sont pas mentionnées seront supprimées.

**Example 1:**- La commande **ipa permission-mod** met à jour toutes les autorisations précédemment ajoutées.

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

ou

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

**Example 2**- La commande **ipa permission-mod** supprime l'argument **--right=delete** car il n'est pas inclus dans la commande :

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

ou

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

## 3.9. COMMENT UTILISER LES CARACTÈRES SPÉCIAUX AVEC LES UTILITAIRES IDM ?

Lorsque vous transmettez aux commandes **ipa** des arguments de ligne de commande comprenant des caractères spéciaux, échappez ces caractères à l'aide d'une barre oblique inverse (\N). Par exemple, les caractères spéciaux courants sont les crochets (< et >), l'esperluette (&), l'astérisque (*) ou la barre verticale (|).

Par exemple, pour échapper à un astérisque (*) :

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

Les commandes contenant des caractères spéciaux non encapsulés ne fonctionnent pas comme prévu, car l'interpréteur de commandes ne peut pas analyser correctement ces caractères.

# CHAPITRE 4. RECHERCHE D'ENTRÉES DE GESTION D'IDENTITÉ À PARTIR DE LA LIGNE DE COMMANDE

Les sections suivantes décrivent comment utiliser les commandes IPA, qui permettent de rechercher ou d'afficher des objets.

## 4.1. APERÇU DE LA LISTE DES ENTRÉES IDM

Cette section décrit les commandes **ipa *-find**, qui peuvent vous aider à rechercher un type particulier d'entrées IdM.

Pour obtenir la liste de toutes les commandes **find**, utilisez la commande ipa help suivante :

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

Il se peut que vous deviez vérifier si un utilisateur particulier est inclus dans la base de données IdM. Vous pouvez alors dresser la liste de tous les utilisateurs à l'aide de la commande suivante :

```
$ ipa user-find
```

Pour dresser la liste des groupes d'utilisateurs dont les attributs spécifiés contiennent un mot-clé :

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

Par exemple, la commande **ipa group-find *admin*** répertorie tous les groupes dont le nom ou la description comprend la chaîne **admin**:

```
----------------
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
```

Lors de la recherche de groupes d'utilisateurs, vous pouvez également limiter les résultats de la recherche aux groupes qui contiennent un utilisateur particulier :

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

Pour rechercher les groupes qui ne contiennent pas un utilisateur particulier :

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

## 4.2. AFFICHER LES DÉTAILS D'UNE ENTRÉE PARTICULIÈRE

Utilisez la commande **ipa *-show** pour afficher les détails d'une entrée IdM particulière.

**Procédure**

- Pour afficher les détails d'un hôte nommé *server.example.com*:

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

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

## 4.3. RÉGLAGE DE LA TAILLE ET DE LA DURÉE DE LA RECHERCHE

Certaines requêtes, telles que la demande d'une liste d'utilisateurs IdM, peuvent renvoyer un très grand nombre d'entrées. En réglant ces opérations de recherche, vous pouvez améliorer les performances globales du serveur lors de l'exécution des commandes **ipa *-find**, telles que **ipa user-find**, et lors de l'affichage des listes correspondantes dans l'interface Web.

**Limite de la taille de la recherche**

Définit le nombre maximum d'entrées renvoyées pour une requête envoyée au serveur à partir de l'interface CLI d'un client ou d'un navigateur accédant à l'interface Web IdM.
Valeur par défaut : 100 entrées.

**Limite de temps de recherche**

Définit la durée maximale (en secondes) pendant laquelle le serveur attend que les recherches s'exécutent. Lorsque la recherche atteint cette limite, le serveur l'arrête et renvoie les entrées découvertes pendant cette période.
Valeur par défaut : 2 secondes.

Si vous définissez les valeurs sur **-1**, l'IdM n'appliquera aucune limite lors de la recherche.

IMPORTANT

Le fait de fixer des limites de taille ou de durée de recherche trop élevées peut avoir un impact négatif sur les performances du serveur.

### 4.3.1. Ajuster la taille de la recherche et la limite de temps dans la ligne de commande

La procédure suivante décrit le réglage des limites de taille et de temps de recherche dans la ligne de commande :

- Au niveau mondial
- Pour une entrée spécifique

**Procédure**

1. Pour afficher le temps de recherche actuel et les limites de taille dans l'interface CLI, utilisez la commande **ipa config-show**:

```
$ ipa config-show
```

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

2. Pour ajuster les limites **globally** pour toutes les requêtes, utilisez la commande **ipa config-mod** et ajoutez les options **--searchrecordslimit** et **--searchtimelimit**. Par exemple :

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

3. Pour que **temporarily** ajuste les limites uniquement pour une requête spécifique, ajoutez les options **--sizelimit** ou **--timelimit** à la commande. Par exemple :

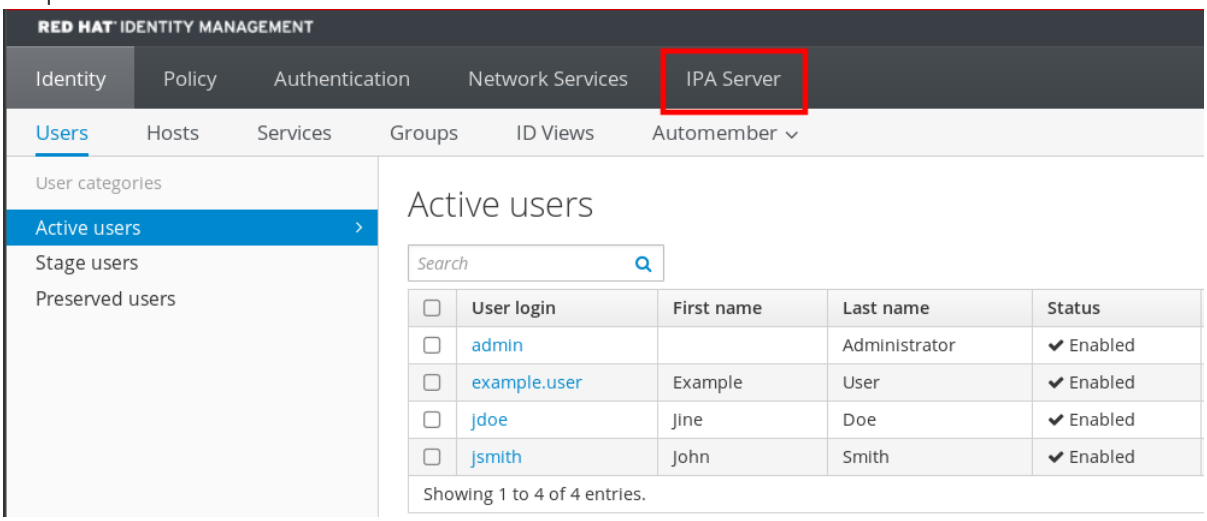
```
$ ipa user-find --sizelimit=200 --timelimit=120
```

### 4.3.2. Ajuster la taille de la recherche et la limite de temps dans l'interface Web

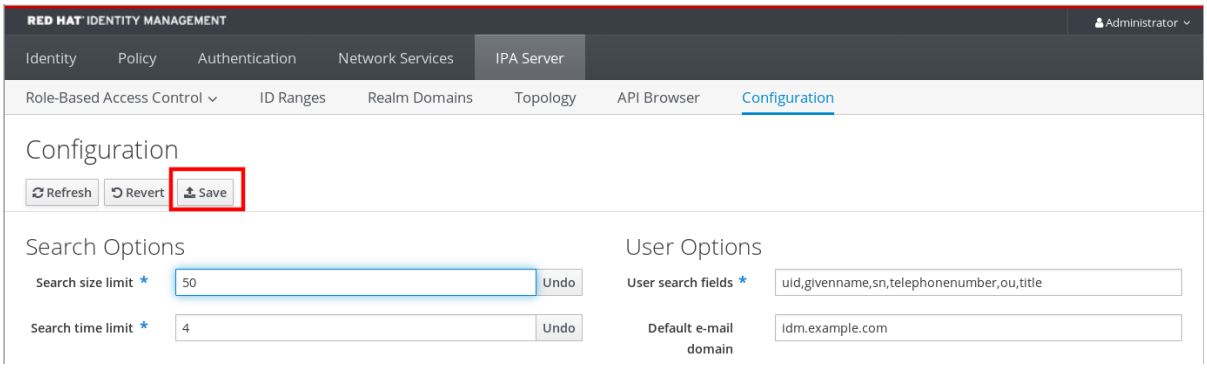
La procédure suivante décrit le réglage des limites de taille et de temps de la recherche globale dans l'interface Web IdM.

**Procédure**

1. Connectez-vous à l'interface Web IdM.
2. Cliquez sur **IPA Server**.




3. Dans l'onglet **IPA Server**, cliquez sur **Configuration**.
4. Réglez les valeurs requises dans la zone **Search Options**.
   Les valeurs par défaut sont les suivantes :
   - Limite de la taille de la recherche : 100 entrées
   - Limite de temps de recherche : 2 secondes
5. Cliquez sur **Save** en haut de la page.


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

# CHAPITRE 5. ACCÈS À L'INTERFACE WEB IDM DANS UN NAVIGATEUR WEB

Les sections suivantes donnent un aperçu de l'interface Web IdM (Identity Management) et décrivent comment y accéder.

## 5.1. QU'EST-CE QUE L'INTERFACE WEB IDM ?

L'interface web IdM (Identity Management) est une application web pour l'administration IdM, une alternative graphique aux outils de ligne de commande IdM.

Vous pouvez accéder à l'interface Web IdM en tant que :

- **IdM users:** Un ensemble limité d'opérations dépendant des autorisations accordées à l'utilisateur dans le serveur IdM. En principe, les utilisateurs IdM actifs peuvent se connecter au serveur IdM et configurer leur propre compte. Ils ne peuvent pas modifier les paramètres d'autres utilisateurs ou les paramètres du serveur IdM.
- **Administrators:** Droits d'accès complets au serveur IdM.
- **Active Directory users:** Un ensemble d'opérations dépendant des permissions accordées à l'utilisateur. Les utilisateurs d'Active Directory peuvent désormais être administrateurs de la gestion des identités. Pour plus de détails, voir Permettre aux utilisateurs AD d'administrer IdM .

## 5.2. NAVIGATEURS WEB PRIS EN CHARGE POUR ACCÉDER À L'INTERFACE WEB

La gestion des identités (IdM) prend en charge les navigateurs suivants pour la connexion à l'interface Web :

- Mozilla Firefox 38 et versions ultérieures
- Google Chrome 46 et versions ultérieures

NOTE

Vous pouvez rencontrer des problèmes pour accéder à l'interface Web IdM avec une carte à puce si votre navigateur tente d'utiliser TLS v1.3 :

```
[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
```

En effet, les versions les plus récentes des navigateurs n'ont pas activé par défaut l'authentification post-handshake TLS (PHA) ou ne la prennent pas en charge. La PHA est nécessaire pour exiger un certificat client TLS pour une partie seulement d'un site web, par exemple lors de l'accès à l'interface web de l'IdM avec une authentification par carte à puce.

Pour résoudre ce problème avec Mozilla Firefox 68 et les versions ultérieures, activez TLS PHA :

1. Saisissez **about:config** dans la barre d'adresse pour accéder au menu des préférences de Mozilla Firefox.
2. Saisissez **security.tls.enable_post_handshake_auth** dans la barre de recherche.
3. Cliquez sur le bouton de basculement pour définir le paramètre comme vrai.

Pour résoudre ce problème avec Chrome, qui ne prend actuellement pas en charge la PHA, désactivez TLS v1.3 :

1. Ouvrez le fichier de configuration **/etc/httpd/conf.d/ssl.conf**.
2. Ajouter **-TLSv1.3** à l'option **SSLProtocol**:

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

3. Redémarrez le service **httpd**:

```
service httpd restart
```

Notez que l'IdM gère le fichier **ssl.conf** et peut écraser son contenu lors de la mise à jour des paquets. Vérifiez les paramètres personnalisés après la mise à jour des paquets IdM.

## 5.3. ACCÈS À L'INTERFACE WEB

La procédure suivante décrit la première connexion à l'interface Web IdM (Identity Management) avec un mot de passe.

Après la première connexion, vous pouvez configurer votre serveur IdM pour vous authentifier :

- Ticket Kerberos
  Pour plus de détails, voir l'authentification Kerberos dans la gestion des identités .

- Carte à puce
  Pour plus de détails, voir Configuration du serveur IdM pour l'authentification par carte à puce .

- Mot de passe à usage unique (OTP) - il peut être combiné avec le mot de passe et l'authentification Kerberos.
  Pour plus de détails, voir l'authentification par mot de passe à usage unique (OTP) dans la gestion des identités.

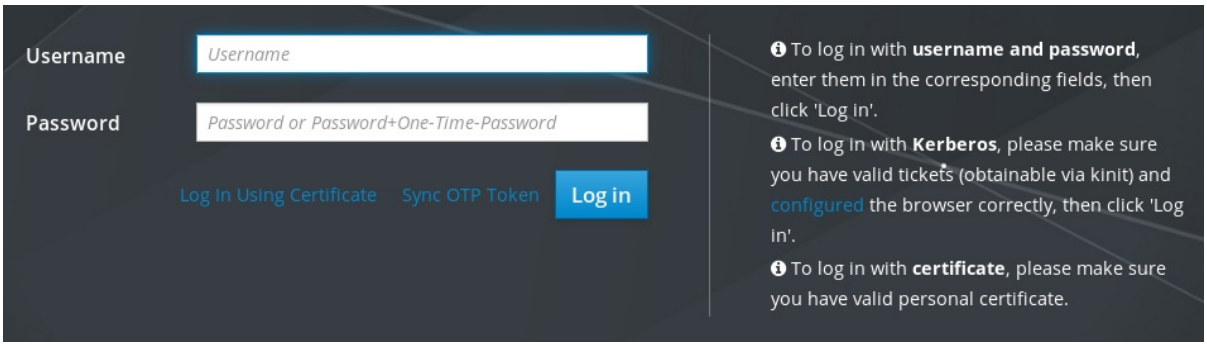
**Procédure**

1. Tapez l'URL du serveur IdM dans la barre d'adresse du navigateur. Le nom ressemblera à l'exemple suivant :

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

   Il vous suffit de remplacer **server.example.com** par le nom DNS de votre serveur IdM.

   Cela ouvre l'écran de connexion de l'IdM Web UI dans votre navigateur.

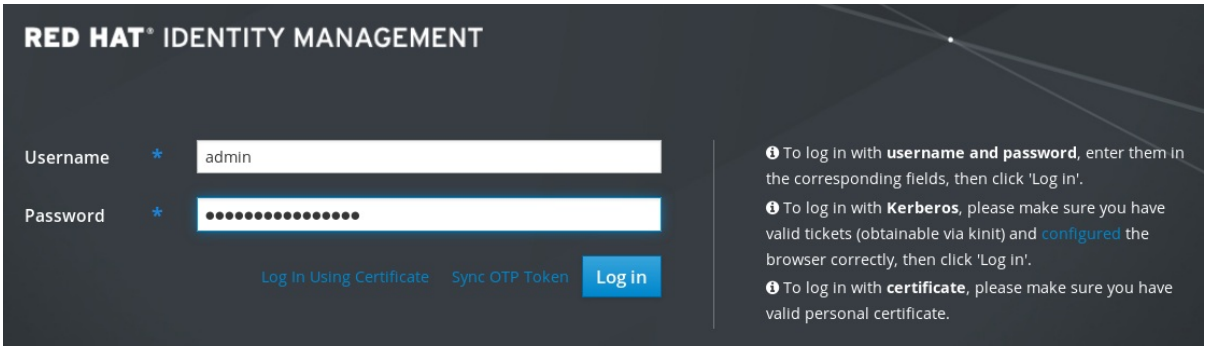



   - Si le serveur ne répond pas ou si l'écran de connexion ne s'ouvre pas, vérifiez les paramètres DNS du serveur IdM auquel vous vous connectez.

   - Si vous utilisez un certificat auto-signé, le navigateur émet un avertissement. Vérifiez le certificat et acceptez l'exception de sécurité pour procéder à la connexion.
     Pour éviter les exceptions de sécurité, installez un certificat signé par une autorité de certification.

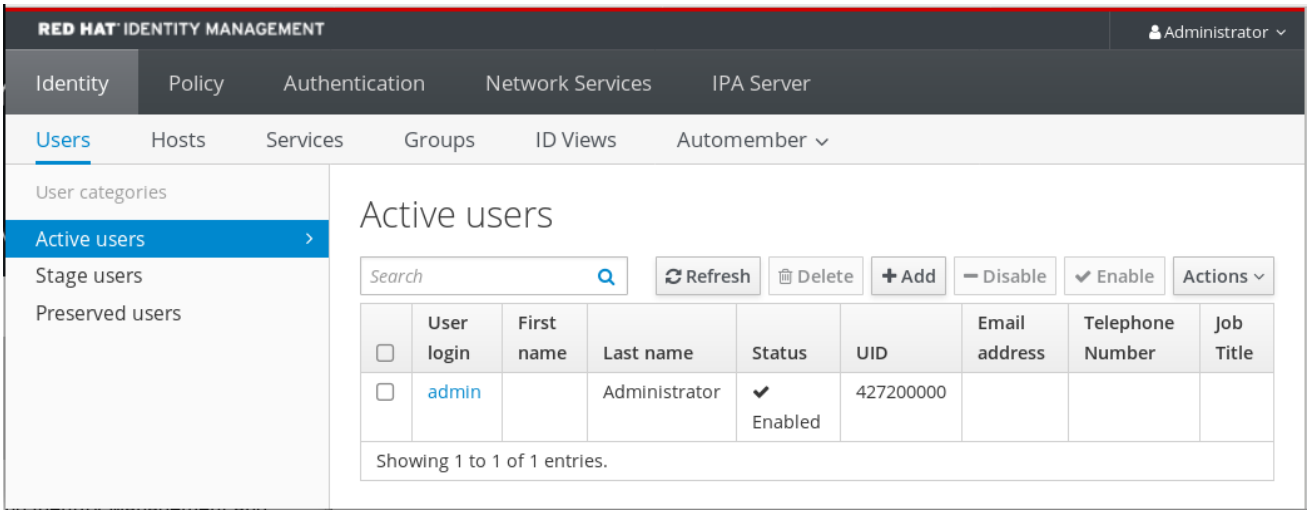
2. Sur l'écran de connexion de l'interface Web, entrez les informations d'identification du compte administrateur que vous avez ajouté lors de l'installation du serveur IdM.
   Pour plus de détails, voir Installation d'un serveur de gestion des identités : Avec DNS intégré, avec CA intégrée.

   Vous pouvez également saisir les informations d'identification de votre compte personnel si elles sont déjà saisies dans le serveur IdM.



3. Cliquez sur **Connexion**.

Une fois la connexion réussie, vous pouvez commencer à configurer le serveur IdM.



# CHAPITRE 6. SE CONNECTER À IDM DANS L'INTERFACE WEB : UTILISATION D'UN TICKET KERBEROS

Les sections suivantes décrivent la configuration initiale de votre environnement pour permettre la connexion Kerberos à l'interface Web de l'IdM et l'accès à l'IdM à l'aide de l'authentification Kerberos.

**Conditions préalables**

- Serveur IdM installé dans votre environnement réseau
  Pour plus de détails, voir Installer la gestion des identités dans Red Hat Enterprise Linux 9

## 6.1. AUTHENTIFICATION KERBEROS DANS LA GESTION DES IDENTITÉS

La gestion des identités (IdM) utilise le protocole Kerberos pour prendre en charge l'authentification unique. L'authentification unique vous permet de ne fournir qu'une seule fois le nom d'utilisateur et le mot de passe corrects, et vous pouvez ensuite accéder aux services de gestion des identités sans que le système ne vous demande à nouveau vos informations d'identification.

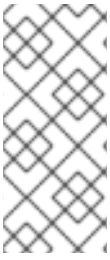
Le serveur IdM fournit l'authentification Kerberos immédiatement après l'installation si les paramètres DNS et de certificat ont été configurés correctement. Pour plus de détails, voir Installation de la gestion des identités.

Pour utiliser l'authentification Kerberos sur les hôtes, installez :

- le client IdM
  Pour plus de détails, voir Préparation du système pour l'installation du client Identity Management.
- le paquet krb5conf

## 6.2. UTILISATION DE KINIT POUR SE CONNECTER MANUELLEMENT À IDM

Cette procédure décrit l'utilisation de l'utilitaire **kinit** pour s'authentifier manuellement auprès d'un environnement de gestion des identités (IdM). L'utilitaire **kinit** obtient et met en cache un ticket Kerberos (TGT) au nom d'un utilisateur IdM.



**NOTE**

N'utilisez cette procédure que si vous avez détruit votre TGT Kerberos initial ou s'il a expiré. En tant qu'utilisateur IdM, lorsque vous vous connectez à votre machine locale, vous vous connectez aussi automatiquement à IdM. Cela signifie qu'après vous être connecté, vous n'avez pas besoin d'utiliser l'utilitaire **kinit** pour accéder aux ressources IdM.

**Procédure**

1. Pour se connecter à l'IdM
   - sous le nom d'utilisateur de l'utilisateur actuellement connecté sur le système local, utilisez **kinit** sans spécifier de nom d'utilisateur. Par exemple, si vous êtes connecté en tant que **example_user** sur le système local :

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

Si le nom d'utilisateur de l'utilisateur local ne correspond à aucune entrée d'utilisateur dans IdM, la tentative d'authentification échoue :

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

- en utilisant un principal Kerberos qui ne correspond pas à votre nom d'utilisateur local, transmettez le nom d'utilisateur requis à l'utilitaire **kinit**. Par exemple, pour vous connecter en tant qu'utilisateur **admin**:

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

2. En option, pour vérifier que la connexion a réussi, utilisez l'utilitaire **klist** pour afficher le TGT mis en cache. Dans l'exemple suivant, le cache contient un ticket pour le principal **example_user**, ce qui signifie que sur cet hôte particulier, seul **example_user** est actuellement autorisé à accéder aux services IdM :

```
$ 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. CONFIGURATION DU NAVIGATEUR POUR L'AUTHENTIFICATION KERBEROS

Pour activer l'authentification avec un ticket Kerberos, il peut être nécessaire de configurer le navigateur.

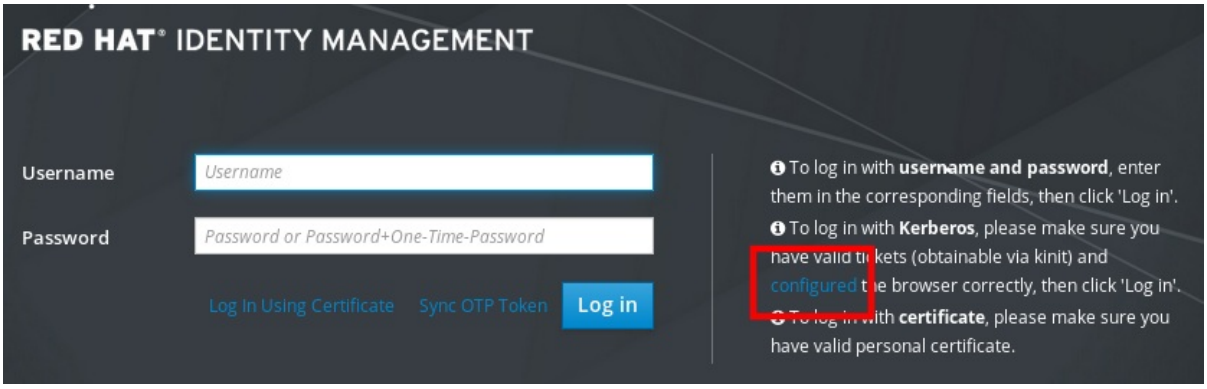
Les étapes suivantes vous aident à prendre en charge la négociation Kerberos pour l'accès au domaine IdM.

Chaque navigateur prend en charge Kerberos de manière différente et nécessite une configuration différente. L'interface Web de l'IdM comprend des instructions pour les navigateurs suivants :

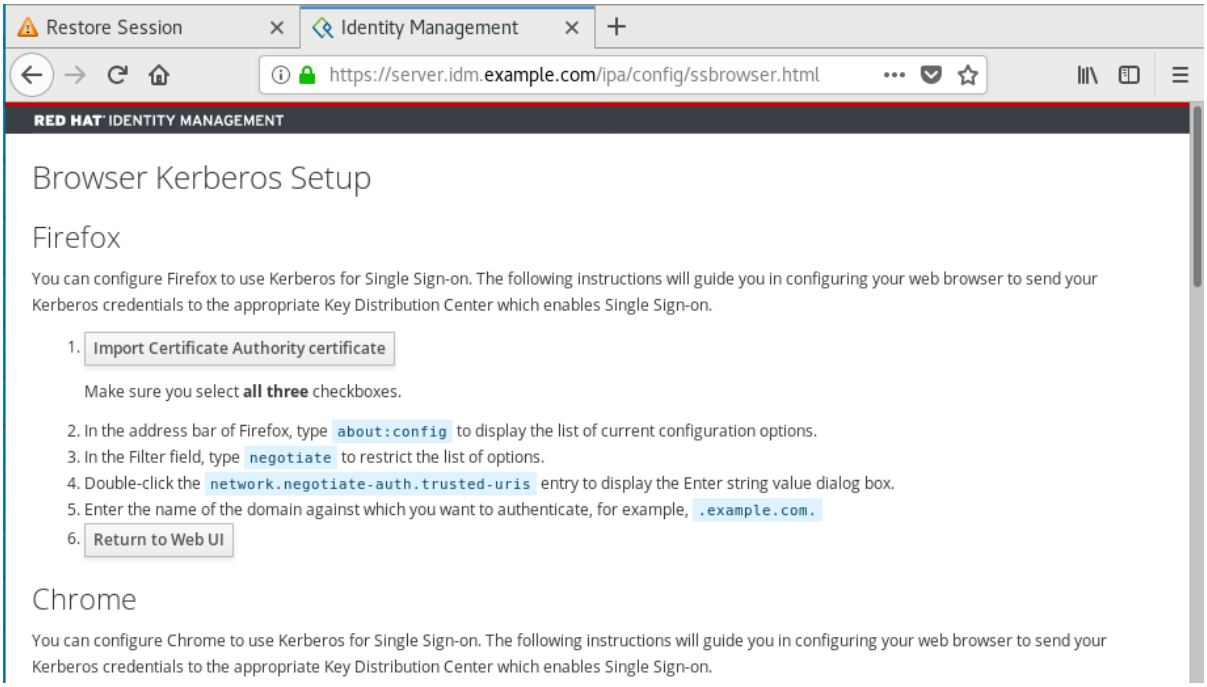
- Firefox
- Chrome

**Procédure**

1. Ouvrez la boîte de dialogue de connexion de l'IdM Web UI dans votre navigateur web.
2. Cliquez sur le lien de configuration du navigateur dans l'écran de connexion de l'interface Web.




3. Suivez les étapes de la page de configuration.




Après la configuration, retournez à l'interface Web IdM et cliquez sur **Log in**.

## 6.4. CONNEXION À L'INTERFACE WEB À L'AIDE D'UN TICKET KERBEROS

Cette procédure décrit la connexion à l'interface Web IdM à l'aide d'un ticket Kerberos (TGT).

Le TGT expire à une heure prédéfinie. L'intervalle de temps par défaut est de 24 heures et vous pouvez le modifier dans l'interface Web IdM.

À l'expiration de l'intervalle de temps, vous devez renouveler le billet :

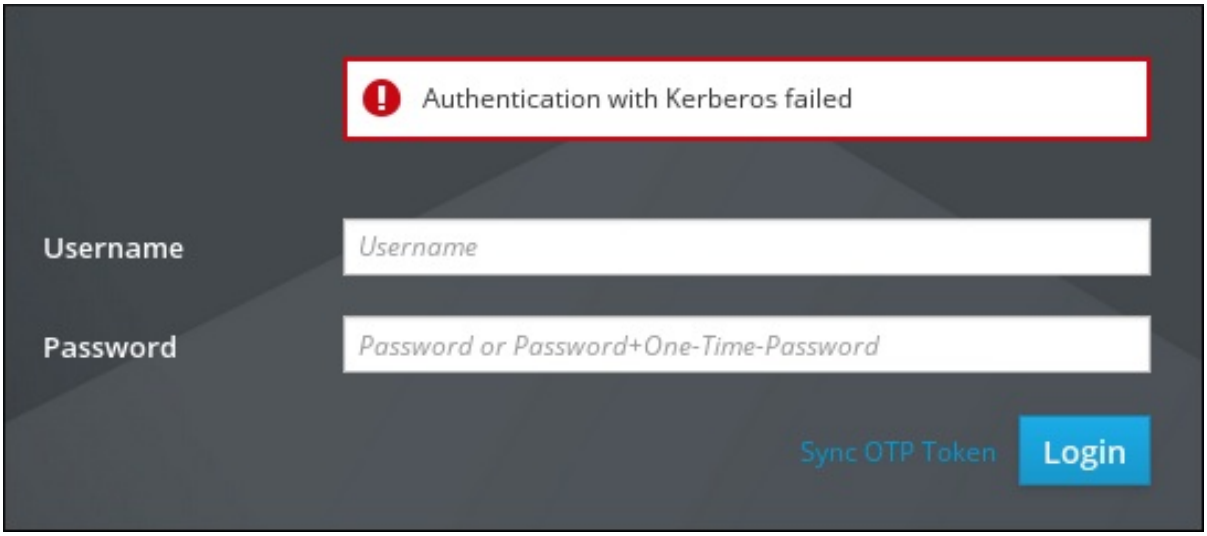
- En utilisant la commande kinit.
- Utilisation des identifiants de connexion IdM dans la boîte de dialogue de connexion de l'interface Web.

**Procédure**

- Ouvrez l'interface Web IdM.
  Si l'authentification Kerberos fonctionne correctement et que vous disposez d'un ticket valide, vous serez automatiquement authentifié et l'interface Web s'ouvrira.

Si le ticket est expiré, il est nécessaire de s'authentifier d'abord avec des informations d'identification. Cependant, la prochaine fois, l'interface Web de l'IdM s'ouvrira automatiquement sans ouvrir la boîte de dialogue de connexion.

Si le message d'erreur **Authentication with Kerberos failed** s'affiche, vérifiez que votre navigateur est configuré pour l'authentification Kerberos. Voir Configuration du navigateur pour l'authentification Kerberos.




## 6.5. CONFIGURATION D'UN SYSTÈME EXTERNE POUR L'AUTHENTIFICATION KERBEROS

Cette section décrit comment configurer un système externe pour que les utilisateurs de la gestion des identités (IdM) puissent se connecter à l'IdM à partir du système externe à l'aide de leurs informations d'identification Kerberos.

L'activation de l'authentification Kerberos sur les systèmes externes est particulièrement utile lorsque votre infrastructure comprend plusieurs royaumes ou domaines qui se chevauchent. Elle est également utile si le système n'a été enrôlé dans aucun domaine IdM par le biais de **ipa-client-install**.

Pour permettre l'authentification Kerberos à l'IdM à partir d'un système qui n'est pas membre du domaine IdM, définissez un fichier de configuration Kerberos spécifique à l'IdM sur le système externe.

### Conditions préalables

- Le paquet **krb5-workstation** est installé sur le système externe.
  Pour savoir si le paquet est installé, utilisez la commande CLI suivante :

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

### Procédure

1. Copiez le fichier **/etc/krb5.conf** du serveur IdM vers le système externe. Par exemple :

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

AVERTISSEMENT

N'écrasez pas le fichier **krb5.conf** existant sur le système externe.

2. Sur le système externe, configurez la session de terminal pour qu'elle utilise le fichier de configuration IdM Kerberos copié :

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

   La variable **KRB5_CONFIG** n'existe que temporairement, jusqu'à ce que vous vous déconnectiez. Pour éviter cette perte, exportez la variable avec un nom de fichier différent.

3. Copiez les extraits de configuration Kerberos du répertoire **/etc/krb5.conf.d/** vers le système externe.

4. Configurez le navigateur sur le système externe, comme décrit dans la section Configuration du navigateur pour l'authentification Kerberos.

Les utilisateurs du système externe peuvent désormais utiliser l'utilitaire **kinit** pour s'authentifier auprès du serveur IdM.

## 6.6. CONNEXION À L'INTERFACE WEB POUR LES UTILISATEURS D'ACTIVE DIRECTORY

Pour activer la connexion à l'interface Web pour les utilisateurs d'Active Directory, définissez un remplacement d'ID pour chaque utilisateur d'Active Directory sur le site **Default Trust View**. Par exemple :

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

**Ressources supplémentaires**

- Utilisation des vues d'identification pour les utilisateurs d'Active Directory

# CHAPITRE 7. CONNEXION À L'INTERFACE WEB DE GESTION DES IDENTITÉS À L'AIDE DE MOTS DE PASSE À USAGE UNIQUE

L'accès à l'interface Web de l'IdM peut être sécurisé par plusieurs méthodes. La méthode de base est l'authentification par mot de passe.

Pour renforcer la sécurité de l'authentification par mot de passe, vous pouvez ajouter une deuxième étape et exiger des mots de passe à usage unique (OTP) générés automatiquement. L'utilisation la plus courante consiste à combiner un mot de passe lié au compte utilisateur et un mot de passe à usage unique limité dans le temps généré par un jeton matériel ou logiciel.

Les sections suivantes vous aideront à :

- Comprendre le fonctionnement de l'authentification OTP dans l'IdM.
- Configurer l'authentification OTP sur le serveur IdM.
- Créez des jetons OTP et synchronisez-les avec l'application FreeOTP de votre téléphone.
- S'authentifier auprès de l'interface Web de l'IdM avec la combinaison du mot de passe de l'utilisateur et du mot de passe à usage unique.
- Re-synchroniser les tokens dans l'interface web.

## 7.1. CONDITIONS PRÉALABLES

- Accès à l'interface web IdM dans un navigateur web

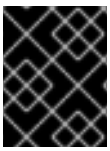
## 7.2. L'AUTHENTIFICATION PAR MOT DE PASSE À USAGE UNIQUE (OTP) DANS LA GESTION DE L'IDENTITÉ

Les mots de passe à usage unique apportent une étape supplémentaire à la sécurité de votre authentification. L'authentification utilise votre mot de passe et un mot de passe à usage unique généré automatiquement.

Pour générer des mots de passe à usage unique, vous pouvez utiliser un jeton matériel ou logiciel. IdM prend en charge les jetons matériels et logiciels.

La gestion de l'identité prend en charge les deux mécanismes OTP standard suivants :

- L'algorithme HMAC-Based One-Time Password (HOTP) est basé sur un compteur. HMAC signifie Hashed Message Authentication Code (code d'authentification des messages hachés).
- L'algorithme TOTP (Time-Based One-Time Password) est une extension de l'algorithme HOTP qui prend en charge le facteur de déplacement basé sur le temps.



**IMPORTANT**

L'IdM ne prend pas en charge les connexions OTP pour les utilisateurs de l'Active Directory.

## 7.3. ACTIVATION DU MOT DE PASSE À USAGE UNIQUE DANS L'INTERFACE WEB

L'interface Web IdM vous permet de configurer un dispositif matériel ou logiciel pour générer des mots de passe à usage unique.

Le mot de passe à usage unique est saisi juste après le mot de passe habituel dans le champ prévu à cet effet dans la boîte de dialogue de connexion.

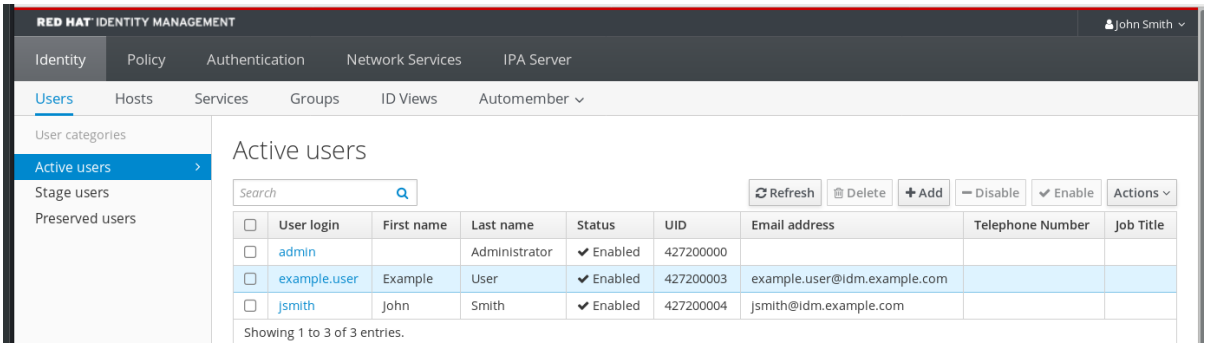
Seuls les administrateurs peuvent activer l'authentification OTP dans les paramètres de l'utilisateur.

### Conditions préalables

- Privilèges d'administration

### Procédure

1. Connectez-vous à l'interface Web IdM avec votre nom d'utilisateur et votre mot de passe.
2. Ouvrez l'onglet **Identity → Users → Active users**




3. Cliquez sur votre nom d'utilisateur pour ouvrir les paramètres de l'utilisateur.
4. Dans le site **User authentication types**, sélectionnez **Two factor authentication (password OTP)**.
5. Cliquez sur **Save**.

À ce stade, l'authentification OTP est activée sur le serveur IdM.

Maintenant, vous ou les utilisateurs eux-mêmes doivent attribuer un nouvel identifiant de jeton au compte d'utilisateur.

## 7.4. AJOUT DE JETONS OTP DANS L'INTERFACE WEB

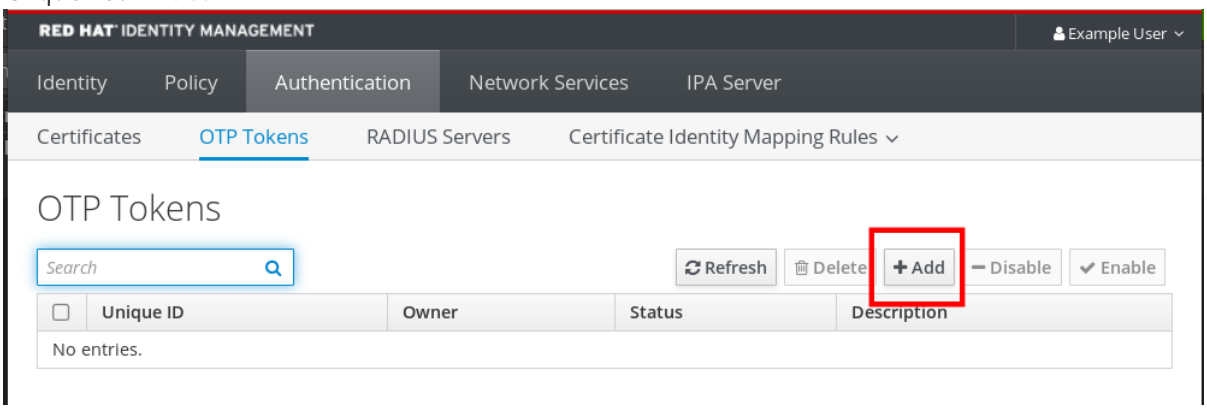
La section suivante vous aide à ajouter des jetons à l'interface Web IdM et au générateur de jetons de votre logiciel.

### Conditions préalables

- Compte d'utilisateur actif sur le serveur IdM.
- L'administrateur a activé l'OTP pour le compte d'utilisateur en question dans l'interface Web de l'IdM.
- Un dispositif logiciel générant des jetons OTP, par exemple FreeOTP.

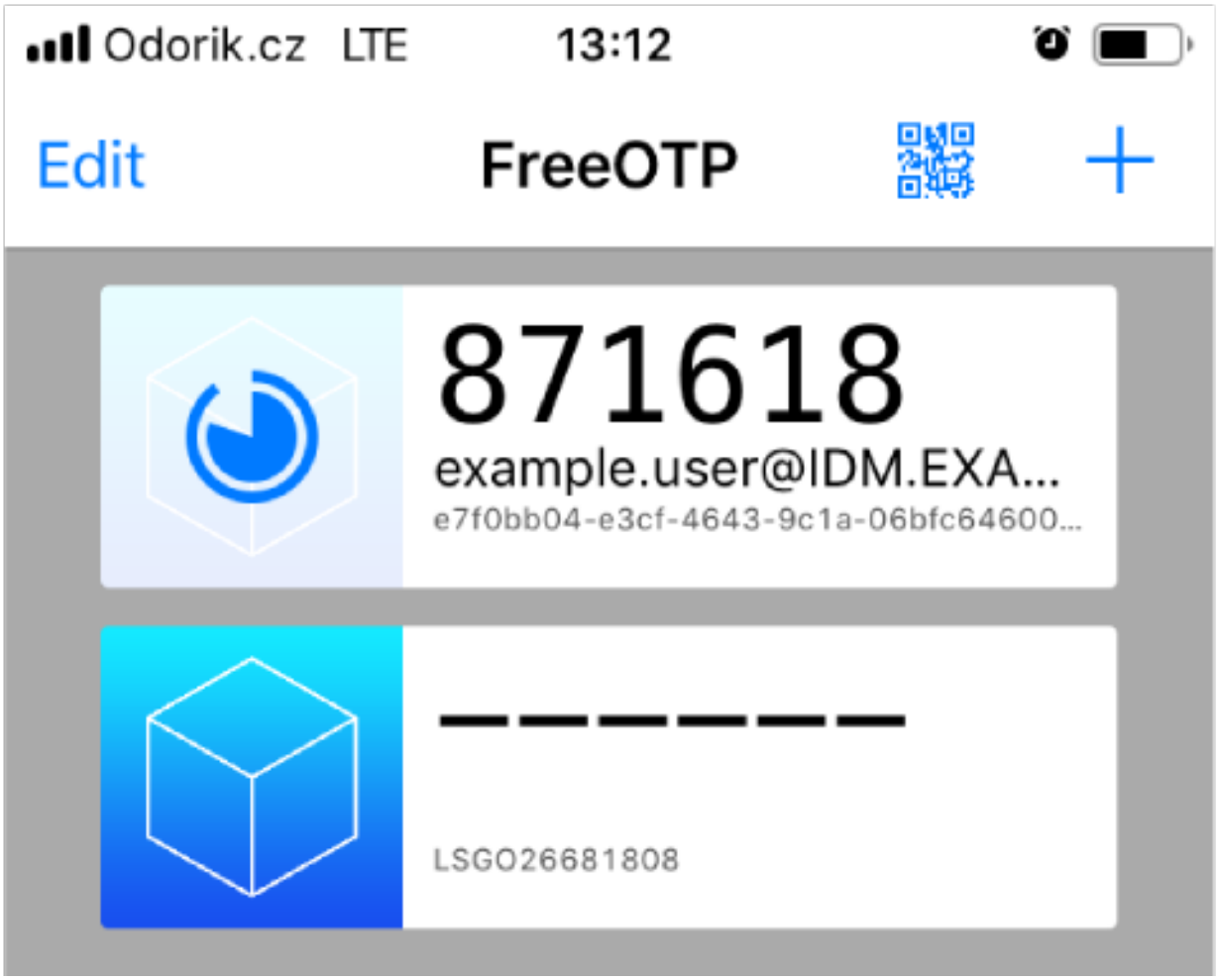
**Procédure**

1. Connectez-vous à l'interface Web IdM avec votre nom d'utilisateur et votre mot de passe.
2. Pour créer le token dans votre téléphone portable, ouvrez l'onglet **Authentication → OTP Tokens**.
3. Cliquez sur **Add**.




4. Dans la boîte de dialogue **Add OTP token**, ne remplissez rien et cliquez sur **Add**.
   À ce stade, le serveur IdM crée un jeton avec des paramètres par défaut sur le serveur et ouvre une page avec un code QR.
5. Copiez le code QR sur votre téléphone portable.
6. Cliquez sur **OK** pour fermer le code QR.

Vous pouvez maintenant générer des mots de passe à usage unique et vous connecter avec eux à l'interface Web de l'IdM.




## 7.5. CONNEXION À L'INTERFACE WEB AVEC UN MOT DE PASSE UNIQUE

Cette procédure décrit la première connexion à l'interface Web IdM à l'aide d'un mot de passe à usage unique (OTP).

**Conditions préalables**

- La configuration OTP est activée sur le serveur de gestion des identités pour le compte utilisateur que vous utilisez pour l'authentification OTP. Les administrateurs ainsi que les utilisateurs eux-mêmes peuvent activer l'OTP.
  Pour activer la configuration OTP, voir Activation du mot de passe à usage unique dans l'interface Web.
- Dispositif matériel ou logiciel générant des jetons OTP configurés.

**Procédure**

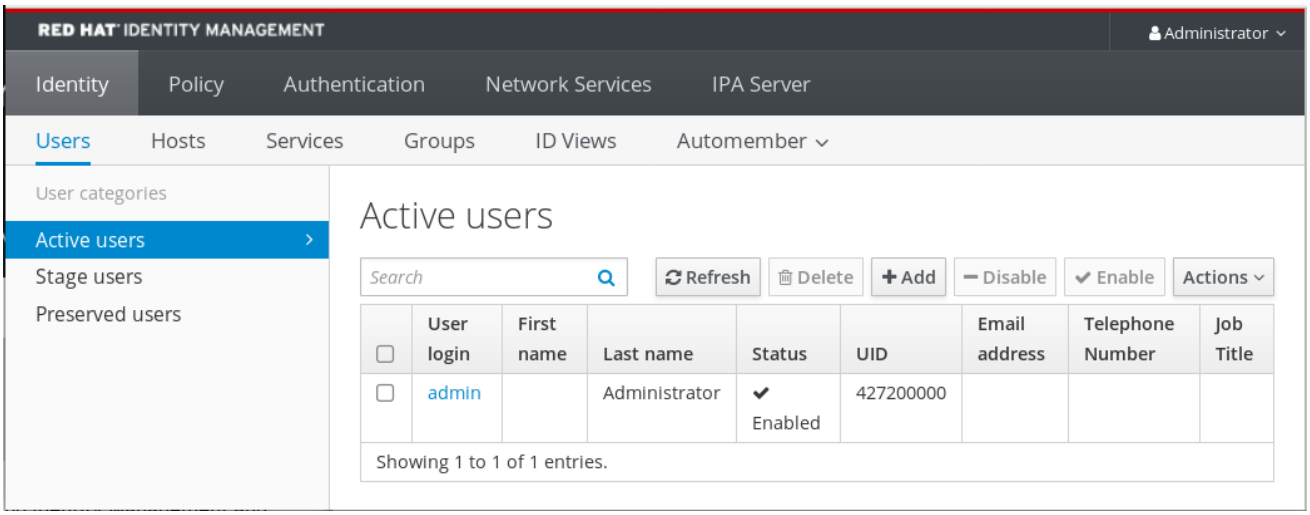
1. Dans l'écran de connexion de la gestion des identités, saisissez votre nom d'utilisateur ou le nom d'utilisateur du compte administrateur du serveur IdM.
2. Ajoutez le mot de passe pour le nom d'utilisateur saisi ci-dessus.
3. Générez un mot de passe à usage unique sur votre appareil.
4. Entrez le mot de passe à usage unique juste après le mot de passe (sans espace).

5. Cliquez sur **Log in**.
   Si l'authentification échoue, synchroniser les jetons OTP.

   Si votre autorité de certification utilise un certificat auto-signé, le navigateur émet un avertissement. Vérifiez le certificat et acceptez l'exception de sécurité pour procéder à la connexion.

   Si l'interface Web IdM ne s'ouvre pas, vérifiez la configuration DNS de votre serveur de gestion des identités.

Une fois la connexion réussie, l'interface Web IdM s'affiche.




## 7.6. SYNCHRONISATION DES JETONS OTP À L'AIDE DE L'INTERFACE WEB

Si la connexion avec OTP (One Time Password) échoue, les jetons OTP ne sont pas synchronisés correctement.

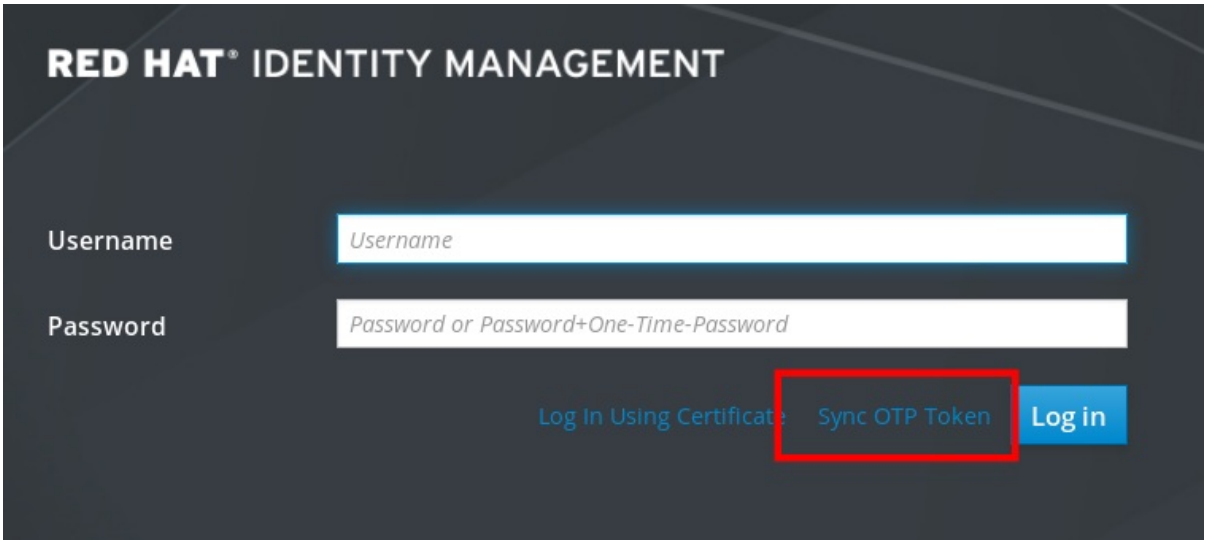
Le texte suivant décrit la resynchronisation des jetons.

### Conditions préalables

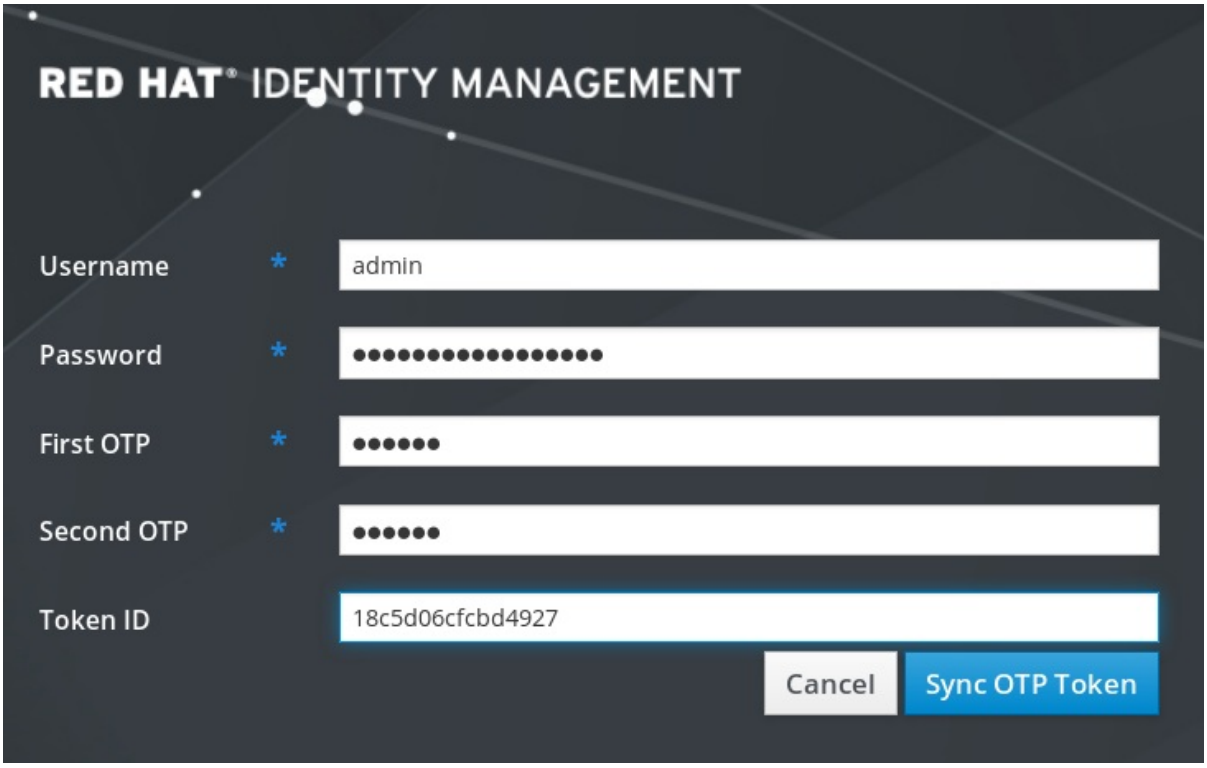
- Un écran de connexion s'est ouvert.
- Dispositif de génération de jetons OTP configuré.

### Procédure

1. Sur l'écran de connexion de l'IdM Web UI, cliquez sur **Sync OTP Token**




2. Dans l'écran de connexion, entrez votre nom d'utilisateur et le mot de passe de gestion de l'identité.
3. Générer un mot de passe à usage unique et le saisir dans le champ **First OTP**.
4. Générez un autre mot de passe à usage unique et saisissez-le dans le champ **Second OTP**.
5. Si vous le souhaitez, vous pouvez saisir l'identifiant du jeton.




6. Cliquez sur **Sync OTP Token**.

Une fois la synchronisation réussie, vous pouvez vous connecter au serveur IdM.

## 7.7. MODIFIER LES MOTS DE PASSE EXPIRÉS

Les administrateurs de la gestion des identités peuvent vous obliger à changer votre mot de passe lors de votre prochaine connexion. Cela signifie que vous ne pouvez pas vous connecter à l'interface Web IdM tant que vous n'avez pas changé votre mot de passe.

L'expiration du mot de passe peut se produire lors de la première connexion à l'interface Web.

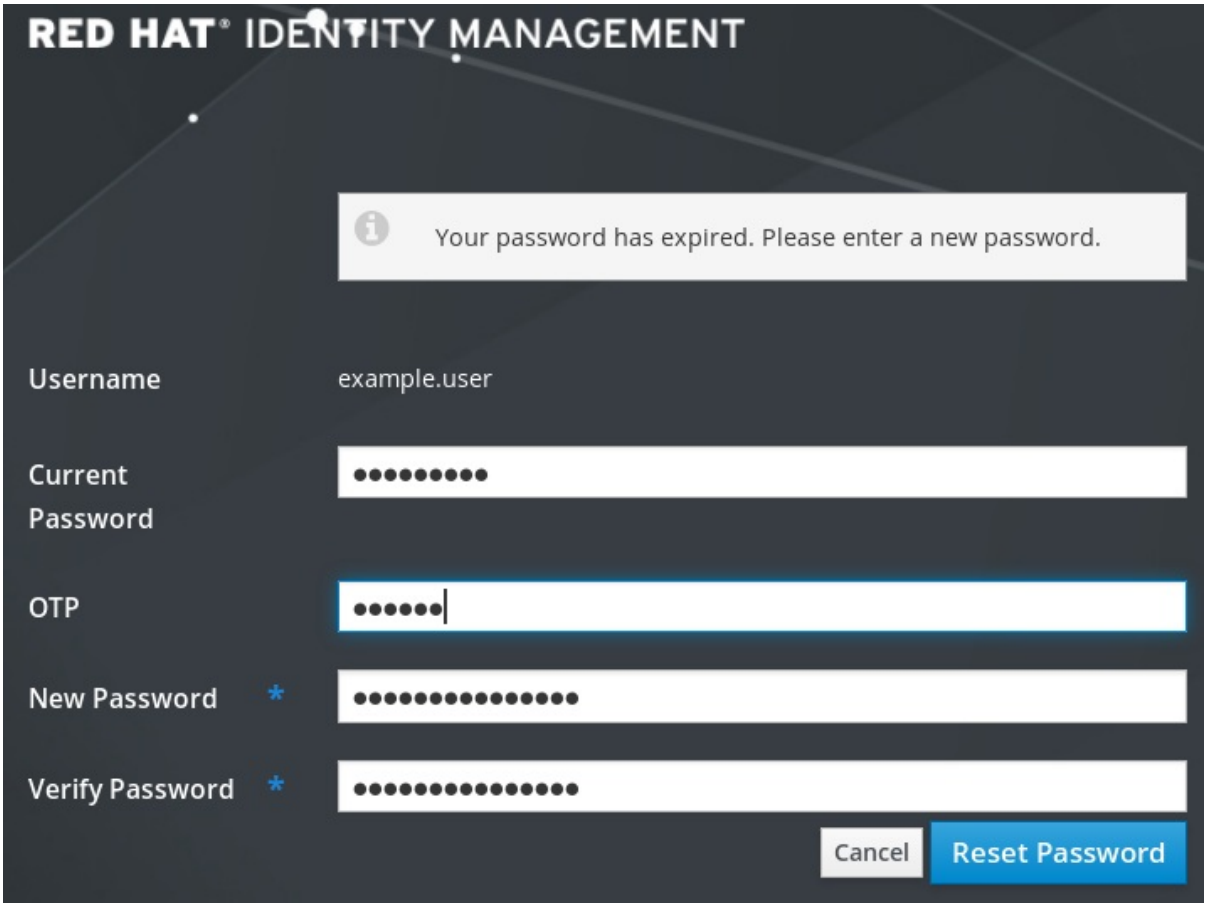
Si la boîte de dialogue d'expiration du mot de passe apparaît, suivez les instructions de la procédure.

**Conditions préalables**

- Un écran de connexion s'est ouvert.
- Compte actif du serveur IdM.

**Procédure**

1. Dans l'écran de connexion relatif à l'expiration du mot de passe, saisissez le nom d'utilisateur.
2. Ajoutez le mot de passe pour le nom d'utilisateur saisi ci-dessus.
3. Dans le champ OTP, générez un mot de passe à usage unique, si vous utilisez l'authentification par mot de passe à usage unique.
   Si vous n'avez pas activé l'authentification OTP, laissez le champ vide.
4. Saisissez le nouveau mot de passe deux fois pour vérification.
5. Cliquez sur **Reset Password**.




Une fois le changement de mot de passe effectué avec succès, la boîte de dialogue de connexion habituelle s'affiche. Connectez-vous avec le nouveau mot de passe.

# CHAPITRE 8. PARAMÈTRES DE SÉCURITÉ DE LA GESTION DES IDENTITÉS

Cette section décrit les caractéristiques de la gestion des identités liées à la sécurité.

## 8.1. COMMENT LA GESTION DES IDENTITÉS APPLIQUE LES PARAMÈTRES DE SÉCURITÉ PAR DÉFAUT

Par défaut, la gestion des identités (IdM) utilise la politique de cryptage du système. L'avantage de cette politique est qu'il n'est pas nécessaire de renforcer manuellement les composants individuels de l'IdM.

**IMPORTANT**

Red Hat vous recommande d'utiliser la politique de cryptage à l'échelle du système. La modification des paramètres de sécurité individuels peut briser les composants de l'IdM.

**Ressources supplémentaires**

- Voir la page de manuel **crypto-policies(7)**.

## 8.2. LIAISONS LDAP ANONYMES DANS LA GESTION DE L'IDENTITÉ

Par défaut, les liaisons anonymes avec le serveur LDAP de gestion des identités (IdM) sont activées. Les liaisons anonymes peuvent exposer certains paramètres de configuration ou valeurs de répertoire. Toutefois, certains utilitaires, tels que **realmd**, ou d'anciens clients RHEL exigent que les liaisons anonymes soient activées pour découvrir les paramètres du domaine lors de l'inscription d'un client.

**Ressources supplémentaires**

- Désactivation des liens anonymes

## 8.3. DÉSACTIVATION DES LIENS ANONYMES

Vous pouvez désactiver les liaisons anonymes sur l'instance du serveur d'annuaire Identity Management (IdM) 389 en utilisant les outils LDAP pour réinitialiser l'attribut **nsslapd-allow-anonymous-access**.

Ce sont les valeurs valides pour l'attribut **nsslapd-allow-anonymous-access**:

- **on**: autorise toutes les liaisons anonymes (par défaut)
- **rootdse**: autorise les liens anonymes uniquement pour les informations sur le DSE racine
- **off**: interdit les liaisons anonymes

Red Hat ne recommande pas d'interdire complètement les connexions anonymes en définissant l'attribut sur **off**, car cela empêche également les clients externes de vérifier la configuration du serveur. Les clients LDAP et Web ne sont pas nécessairement des clients de domaine, ils se connectent donc de manière anonyme pour lire le fichier DSE racine afin d'obtenir des informations de connexion.

En remplaçant la valeur de l'attribut **nsslapd-allow-anonymous-access** par **rootdse**, vous autorisez l'accès au DSE racine et à la configuration du serveur sans aucun accès aux données du répertoire.

**AVERTISSEMENT**

Certains clients s'appuient sur des liaisons anonymes pour découvrir les paramètres IdM. En outre, l'arbre de compatibilité peut s'interrompre pour les anciens clients qui n'utilisent pas l'authentification. N'effectuez cette procédure que si vos clients n'ont pas besoin de liaisons anonymes.

**Conditions préalables**

- Vous pouvez vous authentifier en tant que gestionnaire de répertoire pour écrire sur le serveur LDAP.
- Vous pouvez vous authentifier en tant qu'utilisateur **root** pour redémarrer les services IdM.

**Procédure**

1. Modifier l'attribut **nsslapd-allow-anonymous-access** en **rootdse**.

```
$ 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. Redémarrez l'instance du 389 Directory Server pour charger le nouveau paramètre.

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

**Vérification**

- Affiche la valeur de l'attribut **nsslapd-allow-anonymous-access**.

```
$ 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
```

**Ressources supplémentaires**

- nsslapd-allow-anonymous-access dans la documentation de Directory Server 11
- Liaisons LDAP anonymes dans la gestion de l'identité

# CHAPITRE 9. FICHIERS JOURNAUX ET RÉPERTOIRES DE L'IDM

Les sections suivantes permettent de surveiller, d'analyser et de dépanner les différents composants de la gestion des identités (IdM) :

- LDAP
- Serveur web Apache
- Système de certificats
- Kerberos
- DNS
- Custodia

En outre, vous pouvez surveiller, analyser et dépanner le serveur et le client IdM et activer la journalisation d'audit sur un serveur IdM.

## 9.1. FICHIERS JOURNAUX ET RÉPERTOIRES DU SERVEUR ET DU CLIENT IDM

Le tableau suivant présente les répertoires et les fichiers que le serveur et le client Identity Management (IdM) utilisent pour enregistrer des informations. Vous pouvez utiliser les fichiers et les répertoires pour résoudre les erreurs d'installation.

| Répertoire ou fichier | Description |
|---|---|
| **/var/log/ipaserver-install.log** | Le journal d'installation du serveur IdM. |
| **/var/log/ipareplica-install.log** | Le journal d'installation de la réplique IdM. |
| **/var/log/ipaclient-install.log** | Le journal d'installation du client IdM. |
| **/var/log/sssd/** | Fichiers journaux pour SSSD. Vous pouvez activer la journalisation détaillée pour SSSD dans le fichier sssd.conf ou avec la commande sssctl. |
| **~/.ipa/log/cli.log** | Fichier journal des erreurs renvoyées par les appels de procédure à distance (RPC) et les réponses de l'utilitaire **ipa**. Il est créé dans le répertoire personnel de l'utilisateur **effective user** qui exécute les outils. Cet utilisateur peut avoir un nom d'utilisateur différent de celui de l'utilisateur IdM principal, c'est-à-dire l'utilisateur IdM dont le ticket d'octroi de ticket (TGT) a été obtenu avant d'essayer d'exécuter les commandes **ipa** qui ont échoué. Par exemple, si vous êtes connecté au système en tant que **root** et que vous avez obtenu le TGT de l'IdM**admin**, les erreurs sont enregistrées dans le fichier **/root/.ipa/log/cli.log**. |

| Répertoire ou fichier | Description |
|---|---|
| **/etc/logrotate.d/** | Les politiques de rotation des journaux pour DNS, SSSD, Apache, Tomcat et Kerberos. |
| **/etc/pki/pki-tomcat/logging.properties** | Ce lien renvoie à la configuration par défaut de la journalisation de l'autorité de certification à l'adresse **/usr/share/pki/server/conf/logging.properties**. |

**Ressources supplémentaires**

- Dépannage de l'installation du serveur IdM
- Dépannage de l'installation du client IdM
- Dépannage de l'installation des répliques IdM
- Dépannage de l'authentification avec SSSD dans IdM

## 9.2. FICHIERS JOURNAUX DU SERVEUR D'ANNUAIRE

Le tableau suivant présente les répertoires et les fichiers que l'instance de Directory Server (DS) de Identity Management (IdM) utilise pour enregistrer des informations. Vous pouvez utiliser les fichiers et les répertoires pour résoudre les problèmes liés à DS.

**Tableau 9.1. Fichiers journaux du serveur d'annuaire**

| Répertoire ou fichier | Description |
|---|---|
| **/var/log/dirsrv/slapd-*REALM_NAME*/** | Fichiers journaux associés à l'instance DS utilisée par le serveur IdM. La plupart des données opérationnelles enregistrées ici sont liées aux interactions entre le serveur et la réplique. |
| **/var/log/dirsrv/slapd-*REALM_NAME*/audit** | Contient les pistes d'audit de toutes les opérations DS lorsque l'audit est activé dans la configuration DS.<br><br>**NOTE**<br><br>Vous pouvez également auditer les journaux d'erreurs d'Apache, où l'API IdM enregistre l'accès. Cependant, étant donné que des modifications peuvent également être effectuées directement via LDAP, Red Hat recommande d'activer le journal **/var/log/dirsrv/slapd-REALM_NAME/audit**, plus complet, à des fins d'audit. |
| **/var/log/dirsrv/slapd-*REALM_NAME*/access** | Contient des informations détaillées sur les tentatives d'accès à l'instance DS du domaine. |

| Répertoire ou fichier | Description |
|---|---|
| **/var/log/dirsrv/slapd-*REALM_NAME*/errors** | Contient des informations détaillées sur les opérations qui ont échoué pour l'instance de Domain DS. |

**Ressources supplémentaires**

- Surveillance de l'activité du serveur et de la base de données
- Référence du fichier journal

## 9.3. ACTIVATION DE LA JOURNALISATION D'AUDIT SUR UN SERVEUR IDM

Cette procédure décrit comment activer la journalisation sur un serveur de gestion des identités (IdM) à des fins d'audit. Les journaux détaillés permettent de contrôler les données, de résoudre les problèmes et d'examiner les activités suspectes sur le réseau.

NOTE

Le service LDAP peut devenir plus lent si de nombreuses modifications LDAP sont enregistrées, en particulier si les valeurs sont importantes.

**Conditions préalables**

- Le mot de passe du gestionnaire de répertoire

**Procédure**

1. Liaison avec le serveur LDAP :

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

2. Appuyez sur [Enter].
3. Spécifiez toutes les modifications que vous souhaitez apporter, par exemple :

```
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. Indiquez la fin de la commande **ldapmodify** en entrant **EOF** sur une nouvelle ligne.
5. Appuyez deux fois sur [Enter].
6. Répétez les étapes précédentes sur tous les autres serveurs IdM sur lesquels vous souhaitez activer la journalisation des audits.

### Vérification

- Ouvrez le fichier **/var/log/dirsrv/slapd-REALM_NAME/audit**:

```
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
[...]
```

Le fait que le fichier ne soit plus vide confirme que l'audit est activé.

**IMPORTANT**

Le système enregistre le nom distinctif LDAP lié (DN) de l'entrée qui effectue une modification. C'est pourquoi il peut être nécessaire de post-traiter le journal. Par exemple, dans le serveur d'annuaire IdM, c'est un ID override DN qui représente l'identité d'un utilisateur AD qui a modifié un enregistrement :

```
$ 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
```

Utilisez la commande Python **pysss_nss_idmap.getnamebysid** pour rechercher un utilisateur AD si vous disposez du SID de l'utilisateur :

```
>>> 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}}
```

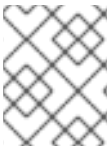
### Ressources supplémentaires

- Fichiers journaux du serveur d'annuaire

- Comment activer la journalisation des audits dans la solution KCS du serveur IPA/IDM et des serveurs de réplique?

## 9.4. MODIFIER LA JOURNALISATION DES ERREURS SUR UN SERVEUR IDM

Cette procédure décrit comment obtenir des informations de débogage sur des types d'erreurs spécifiques. L'exemple se concentre sur l'obtention de journaux d'erreurs détaillés sur la réplication en définissant le niveau du journal d'erreurs sur 8192. Pour enregistrer un autre type d'informations, sélectionnez un autre numéro dans le tableau de la section Niveaux de journalisation du journal des erreurs dans la documentation de Red Hat Directory Server.



NOTE

Le service LDAP peut devenir plus lent si de nombreux types d'erreurs LDAP sont enregistrés, en particulier si les valeurs sont importantes.

**Conditions préalables**

- Le mot de passe du gestionnaire de répertoire.

**Procédure**

1. Liaison avec le serveur LDAP :

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

2. Appuyez sur [Enter].

3. Spécifiez les modifications que vous souhaitez apporter. Par exemple, pour collecter uniquement les journaux liés à la réplication :

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

4. Appuyez deux fois sur [Enter] pour indiquer la fin de l'instruction **ldapmodify**. Le message **modifying entry "cn=config"** s'affiche.

5. Appuyez sur [Ctrl C] pour quitter la commande **ldapmodify**.

6. Répétez les étapes précédentes sur tous les autres serveurs IdM sur lesquels vous souhaitez collecter des journaux détaillés sur les erreurs de réplication.

IMPORTANT

Une fois le dépannage terminé, remettez **nsslapd-errorlog-level** à 0 pour éviter les problèmes de performance.

**Ressources supplémentaires**

- Niveaux de journalisation des erreurs du serveur d'annuaire

## 9.5. LES FICHIERS JOURNAUX DU SERVEUR APACHE DE L'IDM

Le tableau suivant présente les répertoires et les fichiers que le serveur Apache Identity Management (IdM) utilise pour enregistrer des informations.

**Tableau 9.2. Fichiers journaux du serveur Apache**

| Répertoire ou fichier | Description |
|---|---|
| **/var/log/httpd/** | Fichiers journaux du serveur web Apache. |
| **/var/log/httpd/access_log** | Journaux d'accès et d'erreur standard pour les serveurs Apache. Les messages spécifiques à l'IdM sont enregistrés avec les messages Apache, car l'interface web de l'IdM et l'interface de ligne de commande RPC utilisent Apache. Les journaux d'accès enregistrent principalement le principal utilisateur et l'URI utilisé, qui est souvent un point de terminaison RPC. Les journaux d'erreurs contiennent les journaux du serveur IdM. |
| **/var/log/httpd/error_log** | |

**Ressources supplémentaires**

- Fichiers journaux dans la documentation Apache

## 9.6. FICHIERS JOURNAUX DU SYSTÈME DE CERTIFICATION DANS L'IDM

Le tableau suivant présente les répertoires et les fichiers que le système de certificats de gestion des identités (IdM) utilise pour enregistrer des informations.

**Tableau 9.3. Fichiers journaux du système de certification**

| Répertoire ou fichier | Description |
|---|---|
| **/var/log/pki/pki-ca-spawn.*time_of_installation*.log** | Le journal d'installation de l'autorité de certification IdM. |
| **/var/log/pki/pki-kra-spawn.*time_of_installation*.log** | Le journal d'installation de l'autorité de récupération des clés (KRA) de l'IdM. |
| **/var/log/pki/pki-tomcat/** | Répertoire de premier niveau pour les journaux des opérations de l'ICP. Contient les journaux de l'AC et de l'ARK. |
| **/var/log/pki/pki-tomcat/ca/** | Répertoire contenant les journaux relatifs aux opérations de certification. Dans l'IdM, ces journaux sont utilisés pour les mandants de service, les hôtes et les autres entités qui utilisent des certificats. |
| **/var/log/pki/pki-tomcat/kra** | Répertoire contenant les journaux relatifs à l'ARK. |

| Répertoire ou fichier | Description |
|---|---|
| **/var/log/messages** | Inclut les messages d'erreur concernant les certificats parmi d'autres messages du système. |

**Ressources supplémentaires**

- Configuration des journaux de sous-systèmes dans le système de certification Red Hat *Administration Guide*

## 9.7. FICHIERS JOURNAUX KERBEROS DANS IDM

Le tableau suivant présente les répertoires et les fichiers que Kerberos utilise pour enregistrer des informations dans la gestion des identités (IdM).

**Tableau 9.4. Fichiers journaux Kerberos**

| Répertoire ou fichier | Description |
|---|---|
| **/var/log/krb5kdc.log** | Fichier journal principal du serveur Kerberos KDC. |
| **/var/log/kadmind.log** | Fichier journal principal du serveur d'administration Kerberos. |
| L'emplacement de ces fichiers est configuré dans le fichier **krb5.conf**. Ils peuvent être différents sur certains systèmes. | |

## 9.8. FICHIERS JOURNAUX DNS DANS L'IDM

Le tableau suivant présente les répertoires et les fichiers que DNS utilise pour enregistrer les informations dans Identity Management (IdM).

**Tableau 9.5. Fichiers journaux DNS**

| Répertoire ou fichier | Description |
|---|---|
| **/var/log/messages** | Comprend les messages d'erreur DNS et d'autres messages système. La journalisation DNS dans ce fichier n'est pas activée par défaut. Pour l'activer, entrez la commande **# /usr/sbin/rndc querylog**. La commande a pour effet d'ajouter les lignes suivantes à **var/log/messages**:<br><br>**Jun 26 17:37:33 r8server named-pkcs11[1445]: received control channel command 'querylog'**<br><br>**Jun 26 17:37:33 r8server named-pkcs11[1445]: query logging is now on**<br><br>Pour désactiver la journalisation, exécutez à nouveau la commande. |

## 9.9. FICHIERS JOURNAUX DE CUSTODIA DANS L'IDM

Le tableau suivant présente les répertoires et les fichiers que Custodia utilise pour enregistrer les informations dans Identity Management (IdM).

**Tableau 9.6. Fichiers journaux de Custodia**

| Répertoire ou fichier | Description |
|---|---|
| **/var/log/custodia/** | Répertoire du fichier journal pour le service Custodia. |

## 9.10. RESSOURCES SUPPLÉMENTAIRES

- Visualisation des fichiers journaux. Vous pouvez utiliser **journalctl** pour visualiser la sortie de la journalisation des fichiers de l'unité **systemd**.