



## Red Hat Enterprise Linux 9

# Installation de la confiance entre IdM et AD

Gestion d'une confiance inter-forêts entre un IdM et un domaine AD



# Red Hat Enterprise Linux 9 Installation de la confiance entre IdM et AD

---

Gestion d'une confiance inter-forêts entre un IdM et un domaine AD

## Notice légale

Copyright © 2023 Red Hat, Inc.

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

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

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

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack<sup>®</sup> Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## Résumé

Red Hat Identity Management (IdM) et Active Directory (AD) gèrent tous deux une variété de services centraux, tels que Kerberos, LDAP, DNS et les services de certificats. Une relation de confiance intègre de manière transparente ces deux environnements en permettant à tous les services centraux d'interagir de manière transparente. Par exemple, une relation de confiance permet aux utilisateurs d'AD de s'authentifier auprès des services de la topologie IdM. La préparation de la confiance nécessite l'utilisation de types de cryptage communs dans IdM et AD, l'ouverture de ports dans le pare-feu et la configuration des paramètres DNS et Kerberos. Si la confiance n'est plus nécessaire, vous pouvez la supprimer.

## Table des matières

RENDRE L'OPEN SOURCE PLUS INCLUSIF .....	4
FOURNIR UN RETOUR D'INFORMATION SUR LA DOCUMENTATION DE RED HAT .....	5
CHAPITRE 1. CONDITIONS PRÉALABLES À L'ÉTABLISSEMENT D'UN TRUST .....	6
CHAPITRE 2. VERSIONS PRISES EN CHARGE DE WINDOWS SERVER .....	7
CHAPITRE 3. FONCTIONNEMENT DE LA FIDUCIE .....	8
CHAPITRE 4. DROITS D'ADMINISTRATION AD .....	9
CHAPITRE 5. ASSURER LA PRISE EN CHARGE DES TYPES DE CHIFFREMENT COURANTS DANS AD ET RHEL .....	10
CHAPITRE 6. PORTS NÉCESSAIRES À LA COMMUNICATION ENTRE IDM ET AD .....	11
CHAPITRE 7. CONFIGURATION DES PARAMÈTRES DNS ET REALM POUR UNE CONFIANCE .....	15
7.1. DOMAINES DNS PRIMAIRES UNIQUES .....	15
7.2. CONFIGURATION D'UNE ZONE DE TRANSFERT DNS DANS L'INTERFACE WEB IDM .....	16
7.3. CONFIGURATION D'UNE ZONE DE TRANSFERT DNS DANS LE CLI .....	19
7.4. CONFIGURATION DE LA REDIRECTION DNS DANS AD .....	20
7.5. VÉRIFICATION DE LA CONFIGURATION DNS .....	21
CHAPITRE 8. CONFIGURATION DES CLIENTS IDM DANS UN DOMAINE DNS ACTIVE DIRECTORY .....	23
8.1. CONFIGURATION D'UN CLIENT IDM SANS AUTHENTIFICATION UNIQUE KERBEROS .....	23
8.2. DEMANDE DE CERTIFICATS SSL SANS AUTHENTIFICATION UNIQUE .....	24
8.3. CONFIGURATION D'UN CLIENT IDM AVEC AUTHENTIFICATION UNIQUE KERBEROS .....	24
8.4. DEMANDE DE CERTIFICATS SSL AVEC L'AUTHENTIFICATION UNIQUE .....	24
CHAPITRE 9. CRÉATION D'UN TRUST .....	26
9.1. PRÉPARATION DU SERVEUR IDM POUR LA CONFIANCE .....	26
9.2. MISE EN PLACE D'UN CONTRAT DE FIDUCIE À L'AIDE DE LA LIGNE DE COMMANDE .....	28
9.3. MISE EN PLACE D'UN ACCORD DE CONFIANCE DANS L'INTERFACE WEB IDM .....	30
9.4. MISE EN PLACE D'UN ACCORD DE CONFIANCE À L'AIDE D'ANSIBLE .....	32
9.5. VÉRIFICATION DE LA CONFIGURATION DE KERBEROS .....	36
9.6. VÉRIFICATION DE LA CONFIGURATION DE LA CONFIANCE SUR IDM .....	36
9.7. VÉRIFICATION DE LA CONFIGURATION DE LA CONFIANCE SUR AD .....	37
9.8. CRÉATION D'UN AGENT FIDUCIAIRE .....	39
9.9. ACTIVATION DU MAPPAGE AUTOMATIQUE DES GROUPES PRIVÉS POUR UNE PLAGE D'ID POSIX SUR LA CLI .....	40
9.10. ACTIVATION DU MAPPAGE AUTOMATIQUE DES GROUPES PRIVÉS POUR UNE PLAGE D'ID POSIX DANS L'IDM WEBUI .....	41
CHAPITRE 10. RÉOLUTION DES PROBLÈMES LIÉS À LA MISE EN PLACE D'UNE FIDUCIE INTER-FORESTIÈRE .....	43
10.1. SÉQUENCE DES ÉVÉNEMENTS LORS DE L'ÉTABLISSEMENT D'UNE CONFIANCE INTER-FORÊTS AVEC AD .....	43
10.2. LISTE DE CONTRÔLE DES CONDITIONS PRÉALABLES À L'ÉTABLISSEMENT D'UNE CONFIANCE AD .....	45
10.3. COLLECTE DES JOURNAUX DE DÉBOGAGE D'UNE TENTATIVE D'ÉTABLISSEMENT D'UNE CONFIANCE AD .....	47
CHAPITRE 11. DÉPANNAGE DE L'ACCÈS DES CLIENTS AUX SERVICES DANS L'AUTRE FORÊT .....	50
11.1. FLUX D'INFORMATIONS LORSQU'UN HÔTE DU DOMAINE RACINE DE LA FORÊT AD DEMANDE DES SERVICES À UN SERVEUR IDM .....	50

11.2. FLUX D'INFORMATIONS LORSQU'UN HÔTE D'UN DOMAINE ENFANT AD DEMANDE DES SERVICES À UN SERVEUR IDM	51
11.3. FLUX D'INFORMATIONS LORSQU'UN CLIENT IDM DEMANDE DES SERVICES À UN SERVEUR AD	52
<b>CHAPITRE 12. SUPPRESSION DE LA CONFIANCE À L'AIDE DE LA LIGNE DE COMMANDE</b>	<b>54</b>
<b>CHAPITRE 13. SUPPRESSION DE LA CONFIANCE À L'AIDE DE L'INTERFACE WEB IDM</b>	<b>55</b>
<b>CHAPITRE 14. SUPPRESSION DE LA CONFIANCE À L'AIDE D'ANSIBLE</b>	<b>57</b>
<b>CHAPITRE 15. SUPPRESSION D'UNE PLAGE D'IDENTIFIANTS APRÈS LA SUPPRESSION D'UNE CONFIANCE DANS AD</b>	<b>59</b>



## 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. CONDITIONS PRÉALABLES À L'ÉTABLISSEMENT D'UN TRUST

Cette documentation a pour but de vous aider à créer une confiance entre votre serveur Identity Management IdM et Active Directory (AD), lorsque les deux serveurs sont situés dans la même forêt.

## Conditions préalables

- Tout d'abord, lisez le document [Planification d'une confiance inter-forêts entre la gestion des identités et Active Directory](#).
- AD est installé avec un contrôleur de domaine.
- Le serveur IdM est installé et fonctionne.  
Pour plus de détails, voir [Installation de la gestion des identités](#).
- Les horloges du serveur AD et du serveur IdM doivent être synchronisées, car Kerberos exige un délai maximum de 5 minutes dans la communication.
- Des noms NetBIOS uniques pour chacun des serveurs placés dans la confiance, car les noms NetBIOS sont essentiels pour identifier le domaine Active Directory.  
Le nom NetBIOS d'un domaine Active Directory ou IdM est généralement la première partie du domaine DNS correspondant. Si le domaine DNS est **ad.example.com**, le nom NetBIOS est généralement **AD**. Il n'est toutefois pas obligatoire. L'important est que le nom NetBIOS ne comporte qu'un seul mot sans point. La longueur maximale d'un nom NetBIOS est de 15 caractères.
- Le protocole IPv6 doit être activé dans le noyau du système IdM.  
Si IPv6 est désactivé, le plug-in CLDAP utilisé par les services IdM ne s'initialise pas.

## CHAPITRE 2. VERSIONS PRISES EN CHARGE DE WINDOWS SERVER

Vous pouvez établir une relation de confiance avec les forêts Active Directory (AD) qui utilisent les niveaux fonctionnels de forêt et de domaine suivants :

- Gamme de niveaux fonctionnels de la forêt : Windows Server 2012 - Windows Server 2016
- Gamme de niveaux fonctionnels du domaine : Windows Server 2012 - Windows Server 2016

Identity Management (IdM) prend en charge l'établissement d'une confiance avec les contrôleurs de domaine Active Directory exécutant les systèmes d'exploitation suivants :

- Windows Server 2022 (RHEL 9.1 et versions ultérieures)
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012



### NOTE

Identity Management (IdM) ne prend pas en charge l'établissement d'une relation de confiance avec Active Directory avec les contrôleurs de domaine Active Directory exécutant Windows Server 2008 R2 ou des versions antérieures. RHEL IdM nécessite le cryptage SMB lors de l'établissement de la relation de confiance, qui n'est pris en charge que par Windows Server 2012 ou une version ultérieure.

## CHAPITRE 3. FONCTIONNEMENT DE LA FIDUCIE

La confiance entre Identity Management IdM et Active Directory (AD) est établie sur la base de la confiance Kerberos inter-royaumes. Cette solution utilise la capacité de Kerberos pour établir la confiance entre différentes sources d'identité. Par conséquent, tous les utilisateurs d'AD peuvent :

- Se connecter pour accéder aux systèmes et ressources Linux.
- Utiliser l'authentification unique (SSO).

Tous les objets IdM sont gérés dans l'IdM de la fiducie.

Tous les objets AD sont gérés dans AD au sein de la fiducie.

Dans les environnements complexes, une seule forêt IdM peut être connectée à plusieurs forêts AD. Cette configuration permet une meilleure séparation des tâches pour les différentes fonctions de l'organisation. Les administrateurs AD peuvent se concentrer sur les utilisateurs et les politiques liées aux utilisateurs, tandis que les administrateurs Linux ont un contrôle total sur l'infrastructure Linux. Dans ce cas, le domaine Linux contrôlé par IdM est analogue à un domaine de ressources AD, mais avec des systèmes Linux.

Du point de vue d'AD, la gestion des identités représente une forêt AD distincte avec un seul domaine AD. Lorsque la confiance entre le domaine racine d'une forêt AD et un domaine IdM est établie, les utilisateurs des domaines de la forêt AD peuvent interagir avec les machines et les services Linux du domaine IdM.



### NOTE

Dans les environnements de confiance, IdM vous permet d'utiliser les vues ID pour configurer les attributs POSIX des utilisateurs AD sur le serveur IdM.

## CHAPITRE 4. DROITS D'ADMINISTRATION AD

Lorsque vous souhaitez établir une relation de confiance entre AD (Active Directory) et IdM (Identity Management), vous devez utiliser un compte d'administrateur AD doté des privilèges AD appropriés.

Un tel administrateur AD doit être membre de l'un des groupes suivants :

- Groupe Enterprise Admin dans la forêt AD
- Groupe d'administrateurs de domaine dans le domaine racine de votre forêt AD

### Ressources supplémentaires

- Pour plus d'informations sur les administrateurs d'entreprise, voir les [administrateurs d'entreprise](#).
- Pour plus d'informations sur les administrateurs de domaine, voir [Admins de domaine](#).
- Pour plus d'informations sur la confiance AD, voir [Comment fonctionne la confiance dans les domaines et les forêts](#).

## CHAPITRE 5. ASSURER LA PRISE EN CHARGE DES TYPES DE CHIFFREMENT COURANTS DANS AD ET RHEL

Par défaut, Identity Management établit une confiance inter-royaumes avec la prise en charge des types de chiffrement Kerberos RC4, AES-128 et AES-256.

Le cryptage RC4 a été déprécié et désactivé par défaut, car il est considéré comme moins sûr que les nouveaux types de cryptage AES-128 et AES-256. En revanche, les informations d'identification des utilisateurs d'Active Directory (AD) et les liens de confiance entre les domaines AD prennent en charge le cryptage RC4 et peuvent ne pas prendre en charge les types de cryptage AES.

En l'absence de types de chiffrement communs, la communication entre IdM et les domaines enfants AD peut ne pas fonctionner, ou certains comptes AD peuvent ne pas être en mesure de s'authentifier. Pour remédier à cette situation, modifiez l'une des configurations suivantes :

### Activer la prise en charge du cryptage AES dans Active Directory (option recommandée)

Pour s'assurer que les trusts entre les domaines AD dans une forêt AD prennent en charge les types de cryptage AES fort, voir l'article Microsoft suivant : [AD DS : Security : Erreur Kerberos "Unsupported etype" lors de l'accès à une ressource dans un domaine de confiance](#)

### Activer la prise en charge de RC4 dans RHEL

Sur chaque contrôleur de confiance IdM, agent de confiance et client où l'authentification contre les contrôleurs de domaine AD a lieu :

- a. Utilisez la commande **update-crypto-polices** pour activer la sous-politique cryptographique **AD-SUPPORT-LEGACY** en plus de la politique cryptographique **DEFAULT**.

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

- b. Redémarrer l'hôte.

### Ressources supplémentaires

- Voir [Utilisation de stratégies cryptographiques à l'échelle du système](#) .
- Voir [Contrôleurs de confiance et agents de confiance](#) .

## CHAPITRE 6. PORTS NÉCESSAIRES À LA COMMUNICATION ENTRE IDM ET AD

Pour permettre la communication entre vos environnements Active Directory (AD) et Identity Management (IdM), ouvrez les ports suivants sur les pare-feu de vos contrôleurs de domaine AD et de vos serveurs IdM.

**Tableau 6.1. Ports requis pour une confiance AD**

Service	Port	Protocol
Résolution des points d'extrémité portmapper	135	TCP
NetBIOS-DGM	138	TCP et UDP
NetBIOS-SSN	139	TCP et UDP
Microsoft-DS	445	TCP et UDP
RPC dynamique	49152-65535	TCP
Catalogue général AD	3268	TCP
LDAP	389	TCP et UDP



### NOTE

Il n'est pas nécessaire que le port TCP 389 soit ouvert sur les serveurs IdM pour la confiance, mais il est nécessaire pour les clients qui communiquent avec le serveur IdM.

Pour ouvrir des ports, vous pouvez utiliser les méthodes suivantes :

- Service FirewallD - vous pouvez activer les ports particuliers ou les services suivants qui incluent les ports :
  - Création d'un trust FreeIPA
  - FreeIPA avec LDAP
  - Kerberos
  - DNS

Pour plus d'informations, voir [Contrôle des ports à l'aide de l'interface CLI](#) .



## NOTE

Si vous utilisez RHEL 8.2 ou une version antérieure, le service **freeipa-trust** Firewalld inclut une plage de ports RPC de **1024-1300**, ce qui est incorrect. Sur RHEL 8.2 et les versions antérieures, vous devez ouvrir manuellement la plage de ports TCP **49152-65535** en plus d'activer le service **freeipa-trust** Firewalld.

Ce problème a été corrigé pour RHEL 8.3 et les versions ultérieures dans le [bogue 1850418 - mise à jour de la définition de freeipa-trust.xml pour inclure la plage RPC dynamique correcte](#).

- La console web RHEL, qui est une interface utilisateur avec des paramètres de pare-feu basés sur le service **firewalld**.

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

Pour plus d'informations sur la configuration du pare-feu via la console web, voir [Activation des services sur le pare-feu à l'aide de la console web](#)



## NOTE

Si vous utilisez RHEL 8.2 ou une version antérieure, le service **FreeIPA Trust Setup** inclut une plage de ports RPC de **1024-1300**, ce qui est incorrect. Sur RHEL 8.2 et les versions antérieures, vous devez ouvrir manuellement la plage de ports TCP **49152-65535** en plus d'activer le service **FreeIPA Trust Setup** dans la console web RHEL.

Ce problème a été corrigé pour RHEL 8.3 et les versions ultérieures dans le [bogue 1850418 - mise à jour de la définition de freeipa-trust.xml pour inclure la plage RPC dynamique correcte](#).

Tableau 6.2. Ports requis par les serveurs IdM dans le cadre d'une confiance

Service	Port	Protocol
Kerberos	88, 464	TCP et UDP



Service	Port	Protocol
LDAP	389	TCP
DNS	53	TCP et UDP

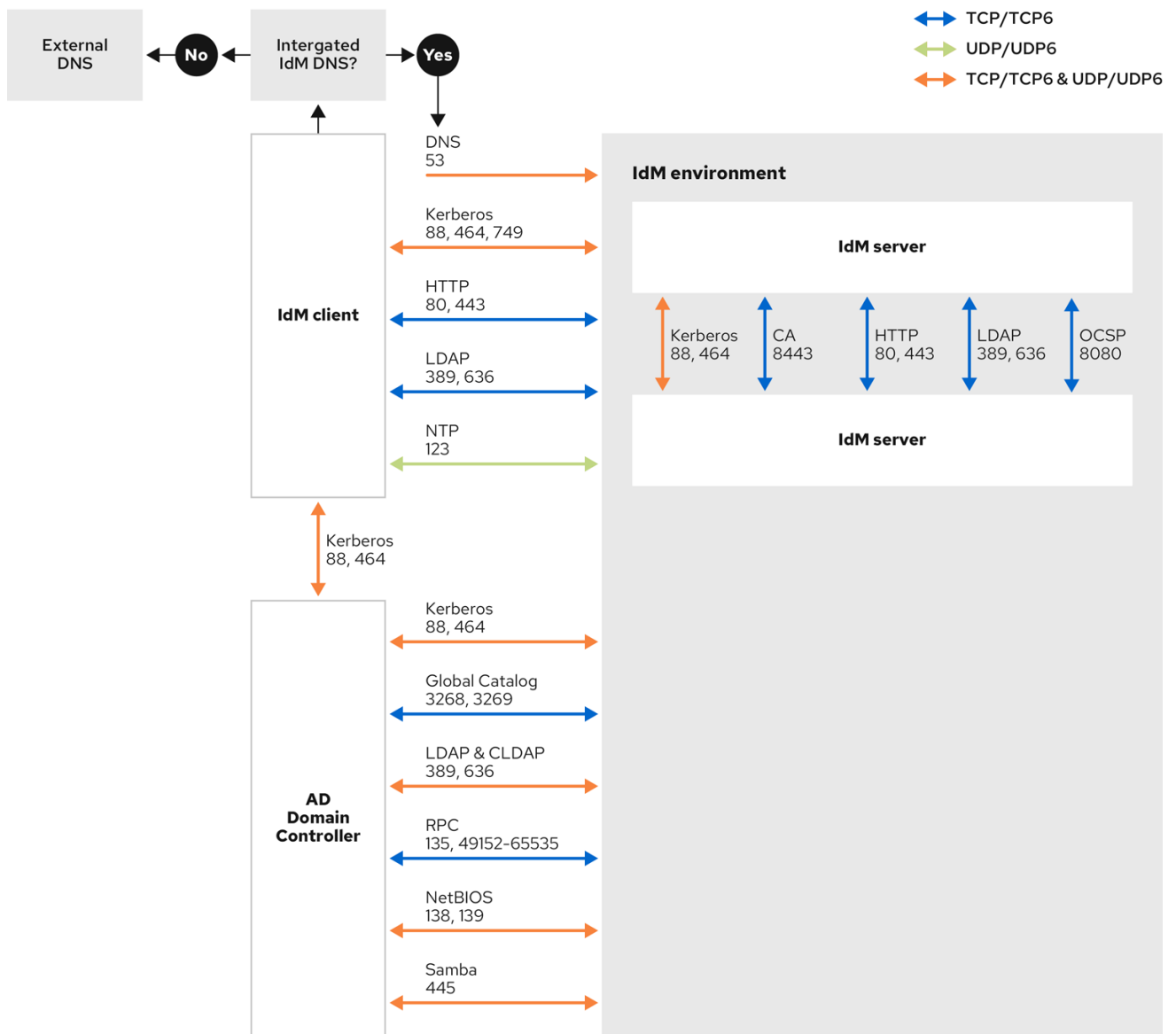
Tableau 6.3. Ports requis par les clients IdM dans une confiance AD

Service	Port	Protocol
Kerberos	88	UDP et TCP

**NOTE**

La bibliothèque **libkrb5** utilise le protocole UDP et revient au protocole TCP si les données envoyées par le centre de distribution de clés (KDC) sont trop volumineuses. Active Directory associe un certificat d'attribut de privilège (PAC) au ticket Kerberos, ce qui augmente la taille du ticket et nécessite l'utilisation du protocole TCP. Afin d'éviter de devoir renvoyer la demande, SSSD dans Red Hat Enterprise Linux 7.4 et les versions ultérieures utilise par défaut le protocole TCP pour l'authentification de l'utilisateur. Si vous souhaitez configurer la taille avant que **libkrb5** n'utilise TCP, définissez **udp\_preference\_limit** dans le fichier **/etc/krb5.conf**. Pour plus de détails, consultez la page de manuel **krb5.conf(5)**.

Le diagramme suivant montre les communications envoyées par les clients IdM, et reçues et répondues par les serveurs IdM et les contrôleurs de domaine AD. Pour définir les ports et protocoles entrants et sortants sur votre pare-feu, Red Hat recommande d'utiliser le service **firewalld**, qui contient déjà des définitions pour les services FreeIPA.



231\_RHEL\_0422

### Ressources supplémentaires

- Pour plus d'informations sur la plage de ports RPC dynamique dans Windows Server 2008 et les versions ultérieures, voir [La plage de ports dynamiques par défaut pour TCP/IP a changé depuis Windows Vista et dans Windows Server 2008.](#)

## CHAPITRE 7. CONFIGURATION DES PARAMÈTRES DNS ET REALM POUR UNE CONFIANCE

Avant de connecter Identity Management (IdM) et Active Directory (AD) dans le cadre d'une confiance, vous devez vous assurer que les serveurs se voient mutuellement et résolvent correctement les noms de domaine. Ce scénario décrit la configuration du DNS pour permettre l'utilisation des noms de domaine entre :

- Un serveur IdM primaire utilisant un serveur DNS et une autorité de certification intégrés.
- Un contrôleur de domaine AD.

Les paramètres DNS sont nécessaires :

- Configuration des zones DNS dans le serveur IdM
- Configuration de la redirection DNS conditionnelle dans AD
- Vérification de l'exactitude de la configuration DNS

### 7.1. DOMAINES DNS PRIMAIRES UNIQUES

Dans Windows, chaque domaine est à la fois un domaine Kerberos et un domaine DNS. Chaque domaine géré par le contrôleur de domaine doit avoir sa propre zone DNS dédiée. Il en va de même lorsque la gestion des identités (IdM) est approuvée par Active Directory (AD) en tant que forêt. AD s'attend à ce que IdM ait son propre domaine DNS. Pour que la configuration de confiance fonctionne, le domaine DNS doit être dédié à l'environnement Linux.

Chaque système doit avoir son propre domaine DNS primaire configuré. Par exemple :

- ***ad.example.com*** pour AD et ***idm.example.com*** pour IdM
- ***example.com*** pour AD et ***idm.example.com*** pour IdM
- ***ad.example.com*** pour AD et ***example.com*** pour IdM

La solution de gestion la plus pratique est un environnement où chaque domaine DNS est géré par des serveurs DNS intégrés, mais il est également possible d'utiliser tout autre serveur DNS conforme aux normes.

#### Les noms de domaines Kerberos sont des versions en majuscules des noms de domaines DNS primaires

Les noms de domaines Kerberos doivent être identiques aux noms de domaines DNS primaires, avec toutes les lettres en majuscules. Par exemple, si les noms de domaine sont ***ad.example.com*** pour AD et ***idm.example.com*** pour IdM, les noms de domaine Kerberos doivent être ***AD.EXAMPLE.COM*** et ***IDM.EXAMPLE.COM***.

#### Enregistrements DNS pouvant être résolus à partir de tous les domaines DNS dans la confiance

Toutes les machines doivent être en mesure de résoudre les enregistrements DNS de tous les domaines DNS impliqués dans la relation de confiance.

#### Domaines IdM et AD DNS

Les systèmes reliés à IdM peuvent être distribués sur plusieurs domaines DNS. Red Hat recommande de déployer les clients IdM dans une zone DNS différente de celles appartenant à Active Directory. Le domaine DNS IdM primaire doit avoir des enregistrements SRV appropriés pour prendre en charge les trusts AD.



## NOTE

Dans certains environnements où il existe des liens de confiance entre IdM et Active Directory, vous pouvez installer un client IdM sur un hôte qui fait partie du domaine DNS d'Active Directory. L'hôte peut alors bénéficier des fonctionnalités Linux de l'IdM. Cette configuration n'est pas recommandée et présente certaines limites. Pour plus de détails, voir [Configuration des clients IdM dans un domaine DNS Active Directory](#) .

Vous pouvez obtenir une liste des enregistrements SRV requis, spécifiques à la configuration de votre système, en exécutant la commande suivante :

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

La liste générée peut par exemple ressembler à ceci :

IPA DNS records:

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

Pour les autres domaines DNS qui font partie du même domaine IdM, il n'est pas nécessaire de configurer les enregistrements SRV lorsque la confiance en AD est configurée. En effet, les contrôleurs de domaine AD n'utilisent pas les enregistrements SRV pour découvrir les KDC, mais basent plutôt la découverte des KDC sur les informations de routage du suffixe de nom pour la confiance.

## 7.2. CONFIGURATION D'UNE ZONE DE TRANSFERT DNS DANS L'INTERFACE WEB IDM

Cette section décrit comment ajouter une zone de transfert DNS au serveur de gestion des identités (IdM) à l'aide de l'interface Web IdM.

Avec les zones de transfert DNS, vous pouvez transférer les requêtes DNS pour une zone spécifique vers un serveur DNS différent. Par exemple, vous pouvez transférer les requêtes DNS pour le domaine Active Directory (AD) vers un serveur DNS AD.

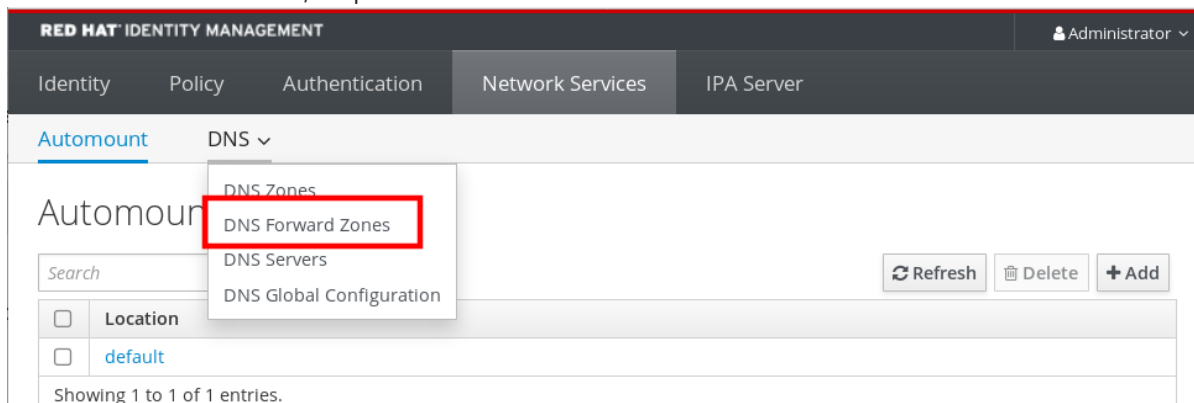
### Conditions préalables

- Accès à l'interface Web IdM avec un compte d'utilisateur disposant de droits d'administrateur.
- Serveur DNS correctement configuré.

### Procédure

1. Se connecter à l'interface Web IdM avec des privilèges d'administrateur. Pour plus de détails, voir [Accès à l'interface web IdM dans un navigateur web](#) .
2. Cliquez sur l'onglet **Network Services**.

3. Cliquez sur l'onglet **DNS**.
4. Dans le menu déroulant, cliquez sur l'élément **DNS Forward Zones**.



5. Cliquez sur le bouton **Add**.
6. Dans la boîte de dialogue **Add DNS forward zone**, ajoutez un nom de zone.
7. Dans la rubrique **Zone forwarders**, cliquez sur le bouton **Add**.
8. Dans le champ **Zone forwarders**, ajoutez l'adresse IP du serveur pour lequel vous souhaitez créer la zone de transfert.
9. Cliquez sur le bouton **Add**.

 The screenshot shows a dialog box titled 'Add DNS forward zone' with a close button (X) in the top right corner. The dialog contains several form fields:
 

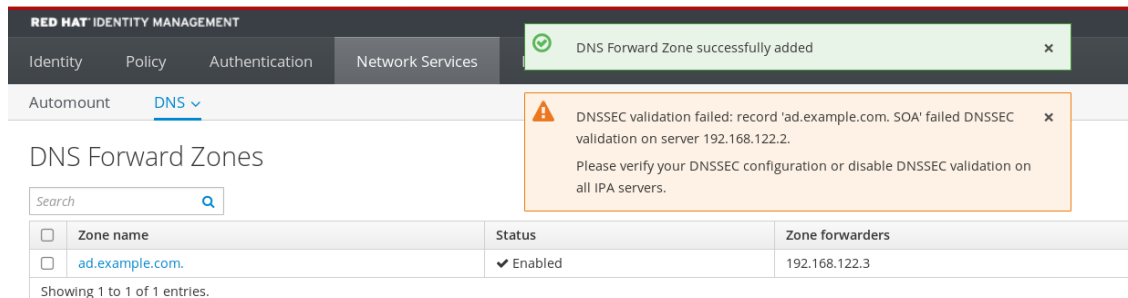
- Zone name \***: A text input field containing 'ad.example.com'.
- Reverse zone**: A radio button that is unselected.
- IP network**: A text input field that is currently empty.
- Zone forwarders \***: A list of text input fields. The first one contains '192.168.122.3' and has an 'Undo' button to its right. The second one is empty and also has an 'Undo' button.
- Add**: A button located below the 'Zone forwarders' list.
- Forward policy**: Three radio buttons: 'Forward first' (selected), 'Forward only', and 'Forwarding disabled'.
- Skip overlap check ⓘ**: A checkbox that is unselected.

 At the bottom left, there is a note: '\* Required field'. At the bottom right, there are four buttons: 'Add', 'Add and Add Another', 'Add and Edit', and 'Cancel'.

La zone transférée a été ajoutée aux paramètres DNS et vous pouvez la vérifier dans les paramètres DNS Forward Zones. L'interface Web vous informe de la réussite de l'opération à l'aide du message contextuel suivant : **DNS Forward Zone successfully added.**

## NOTE

L'interface Web peut afficher un avertissement concernant un échec de validation DNSSEC après l'ajout d'une zone de transfert à la configuration.



The screenshot shows the Red Hat Identity Management web interface. At the top, there is a navigation bar with tabs for Identity, Policy, Authentication, and Network Services. A green notification banner at the top right says "DNS Forward Zone successfully added". Below this, there is a warning banner with a red triangle icon that reads: "DNSSEC validation failed: record 'ad.example.com. SOA' failed DNSSEC validation on server 192.168.122.2. Please verify your DNSSEC configuration or disable DNSSEC validation on all IPA servers." The main content area is titled "DNS Forward Zones" and contains a search bar and a table with one entry:

<input type="checkbox"/>	Zone name	Status	Zone forwarders
<input type="checkbox"/>	ad.example.com.	✓ Enabled	192.168.122.3

Showing 1 to 1 of 1 entries.

DNSSEC (Domain Name System Security Extensions) sécurise les données DNS à l'aide d'une signature numérique afin de protéger le DNS contre les attaques. Ce service est activé par défaut dans le serveur IdM. L'avertissement apparaît car le serveur DNS distant n'utilise pas DNSSEC. Red Hat vous recommande d'activer DNSSEC sur le serveur DNS distant.

Si vous ne pouvez pas activer la validation DNSSEC sur le serveur distant, vous pouvez désactiver DNSSEC dans le serveur IdM :

1. Choisissez le fichier de configuration approprié à modifier :
  - Si votre serveur IdM utilise RHEL 8.0 ou RHEL 8.1, ouvrez le fichier **/etc/named.conf**.
  - Si votre serveur IdM utilise RHEL 8.2 ou une version ultérieure, ouvrez le fichier **/etc/named/ipa-options-ext.conf**.

2. Ajoutez les paramètres DNSSEC suivants :

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

3. Enregistrez et fermez le fichier de configuration.

4. Redémarrez le service DNS :

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

## Verification steps

- Utilisez la commande **nslookup** avec le nom du serveur DNS distant :

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

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

Si vous avez configuré correctement la redirection de domaine, l'adresse IP du serveur DNS distant s'affiche.

## 7.3. CONFIGURATION D'UNE ZONE DE TRANSFERT DNS DANS LE CLI

Cette section décrit comment ajouter une nouvelle zone DNS au serveur de gestion des identités (IdM) à l'aide de l'interface de ligne de commande (CLI).

Avec les zones de transfert DNS, vous pouvez transférer les requêtes DNS pour une zone spécifique vers un serveur DNS différent. Par exemple, vous pouvez transférer les requêtes DNS pour le domaine Active Directory (AD) vers un serveur DNS AD.

### Conditions préalables

- Accès à la CLI avec un compte d'utilisateur disposant de droits d'administrateur.
- Serveur DNS correctement configuré.

### Procédure

- Créez une zone de transfert DNS pour le domaine AD et indiquez l'adresse IP du serveur DNS distant avec l'option **--forwarder**:

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

## NOTE

Vous pouvez voir un avertissement concernant un échec de validation DNSSEC dans les journaux du système `/var/log/messages` après avoir ajouté une nouvelle zone de transfert à la configuration :

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

DNSSEC (Domain Name System Security Extensions) sécurise les données DNS à l'aide d'une signature numérique afin de protéger le DNS contre les attaques. Ce service est activé par défaut dans le serveur IdM. L'avertissement apparaît car le serveur DNS distant n'utilise pas DNSSEC. Red Hat vous recommande d'activer DNSSEC sur le serveur DNS distant.

Si vous ne pouvez pas activer la validation DNSSEC sur le serveur distant, vous pouvez désactiver DNSSEC dans le serveur IdM :

1. Choisissez le fichier de configuration approprié à modifier :
  - Si votre serveur IdM utilise RHEL 8.0 ou RHEL 8.1, ouvrez le fichier `/etc/named.conf`.
  - Si votre serveur IdM utilise RHEL 8.2 ou une version ultérieure, ouvrez le fichier `/etc/named/ipa-options-ext.conf`.

2. Ajoutez les paramètres DNSSEC suivants :

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

3. Enregistrez et fermez le fichier de configuration.
4. Redémarrez le service DNS :

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

### Verification steps

- Utilisez la commande **nslookup** avec le nom du serveur DNS distant :

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

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

Si la redirection de domaine est configurée correctement, la requête **nslookup** affiche une adresse IP du serveur DNS distant.

## 7.4. CONFIGURATION DE LA REDIRECTION DNS DANS AD



Cette section décrit comment configurer une redirection DNS dans Active Directory (AD) pour le serveur de gestion des identités (IdM).

### Conditions préalables

- Serveur Windows avec AD installé.
- Port DNS ouvert sur les deux serveurs.

### Procédure

1. Connectez-vous au serveur Windows.
2. Ouvrir **Server Manager**.
3. Ouvrir **DNS Manager**.
4. Dans **Conditional Forwarders**, ajoutez un nouveau forwarder conditionnel avec :
  - L'adresse IP du serveur IdM
  - Un nom de domaine complet, par exemple, **server.idm.example.com**
5. Sauvegarder les paramètres.

## 7.5. VÉRIFICATION DE LA CONFIGURATION DNS

Avant de configurer la confiance, vérifiez que les serveurs Identity Management (IdM) et Active Directory (AD) peuvent se résoudre et se résoudre mutuellement.

### Conditions préalables

- Vous devez être connecté avec les permissions sudo.

### Procédure

1. Lancez une requête DNS pour les enregistrements de service Kerberos over UDP et LDAP over TCP.

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

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

Les commandes sont censées répertorier tous les serveurs IdM.

2. Lancer une requête DNS pour l'enregistrement TXT avec le nom du domaine Kerberos de l'IdM. La valeur obtenue devrait correspondre au domaine Kerberos spécifié lors de l'installation d'IdM.

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

Si les étapes précédentes n'ont pas permis d'obtenir tous les enregistrements attendus, mettez à jour la configuration DNS avec les enregistrements manquants :

- Si votre environnement IdM utilise un serveur DNS intégré, entrez la commande **ipa dns-update-system-records** sans aucune option pour mettre à jour les enregistrements de votre système :

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

- Si votre environnement IdM n'utilise pas de serveur DNS intégré :
  1. Sur le serveur IdM, exporter les enregistrements DNS IdM dans un fichier :

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

La commande crée un fichier nommé **dns\_records\_file.nsupdate** avec les enregistrements DNS IdM pertinents.

2. Soumettez une demande de mise à jour DNS à votre serveur DNS à l'aide de l'utilitaire **nsupdate** et du fichier **dns\_records\_file.nsupdate**. Pour plus d'informations, voir [Mise à jour des enregistrements DNS externes à l'aide de nsupdate](#) dans la documentation RHEL 7. Vous pouvez également vous référer à la documentation de votre serveur DNS pour l'ajout d'enregistrements DNS.
3. Vérifiez que l'IdM est en mesure de résoudre les enregistrements de service pour AD à l'aide d'une commande qui exécute une requête DNS pour les enregistrements de service Kerberos et LDAP sur TCP :

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

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

## CHAPITRE 8. CONFIGURATION DES CLIENTS IDM DANS UN DOMAINE DNS ACTIVE DIRECTORY

Si vous avez des systèmes clients dans un domaine DNS contrôlé par Active Directory et que vous souhaitez que ces clients puissent rejoindre le serveur IdM pour bénéficier de ses fonctionnalités RHEL, vous pouvez configurer les utilisateurs pour qu'ils accèdent à un client à l'aide d'un nom d'hôte du domaine DNS Active Directory.



### IMPORTANT

Cette configuration n'est pas recommandée et présente certaines limitations. Red Hat recommande de toujours déployer les clients IdM dans une zone DNS différente de celles détenues par Active Directory et d'accéder aux clients IdM via leurs noms d'hôtes IdM.

La configuration du client IdM dépend de la nécessité ou non d'une authentification unique avec Kerberos.

### 8.1. CONFIGURATION D'UN CLIENT IDM SANS AUTHENTIFICATION UNIQUE KERBEROS

L'authentification par mot de passe est la seule méthode d'authentification disponible pour que les utilisateurs puissent accéder aux ressources des clients IdM si ces derniers font partie d'un domaine DNS Active Directory. Cette procédure décrit comment configurer votre client sans authentification unique Kerberos.

#### Procédure

1. Installez le client IdM avec l'option **--domain=IPA\_DNS\_Domain** pour que le démon des services de sécurité du système (SSSD) puisse communiquer avec les serveurs IdM :

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

Cette option désactive la détection automatique des enregistrements SRV pour le domaine DNS Active Directory.

2. Ouvrez le fichier de configuration **/etc/krb5.conf** et localisez le mappage existant pour le domaine Active Directory dans la section **[domain\_realm]**.

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

3. Remplacez les deux lignes par une entrée mettant en correspondance le nom de domaine complet (FQDN) des clients Linux dans la zone DNS Active Directory avec le domaine IdM :

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

En remplaçant le mappage par défaut, vous empêchez Kerberos d'envoyer ses demandes pour le domaine Active Directory au centre de distribution Kerberos (KDC) de l'IdM. Au lieu de cela, Kerberos utilise la découverte automatique par le biais des enregistrements DNS SRV pour localiser le KDC.

## 8.2. DEMANDE DE CERTIFICATS SSL SANS AUTHENTIFICATION UNIQUE

Les services basés sur SSL nécessitent un certificat avec des enregistrements d'extension **dNSName** qui couvrent tous les noms d'hôtes du système, car les enregistrements originaux (A/AAAA) et CNAME doivent figurer dans le certificat. Actuellement, IdM ne délivre des certificats qu'aux objets hôtes de la base de données IdM.

Dans la configuration décrite, sans authentification unique, IdM dispose déjà d'un objet hôte pour le FQDN dans la base de données, et **certmonger** peut demander un certificat en utilisant ce nom.

### Conditions préalables

- Installer et configurer le client IdM en suivant la procédure décrite dans la section [Configuration d'un client IdM sans authentification unique Kerberos](#).

### Procédure

- Utilisez **certmonger** pour demander un certificat en utilisant le FQDN :

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

Le service **certmonger** utilise la clé hôte par défaut stockée dans le fichier **/etc/krb5.keytab** pour s'authentifier auprès de l'autorité de certification (AC) de l'IdM.

## 8.3. CONFIGURATION D'UN CLIENT IDM AVEC AUTHENTIFICATION UNIQUE KERBEROS

Si vous avez besoin d'une authentification unique Kerberos pour accéder aux ressources du client IdM, celui-ci doit se trouver dans le domaine DNS IdM, par exemple **idm-client.idm.example.com**. Vous devez créer un enregistrement CNAME **idm-client.ad.example.com** dans le domaine DNS Active Directory pointant vers l'enregistrement A/AAAA du client IdM.

Pour les serveurs d'application basés sur Kerberos, MIT Kerberos prend en charge une méthode permettant l'acceptation de tout principal basé sur l'hôte disponible dans le keytab de l'application.

### Procédure

- Sur le client IdM, désactivez les contrôles stricts sur le principal Kerberos utilisé pour cibler le serveur Kerberos en définissant l'option suivante dans la section **[libdefaults]** du fichier de configuration **/etc/krb5.conf**:

```
ignore_acceptor_hostname = true
```

## 8.4. DEMANDE DE CERTIFICATS SSL AVEC L'AUTHENTIFICATION UNIQUE

Les services basés sur SSL nécessitent un certificat avec des enregistrements d'extension **dnsName** qui couvrent tous les noms d'hôtes du système, car les enregistrements originaux (A/AAAA) et CNAME doivent figurer dans le certificat. Actuellement, IdM ne délivre des certificats qu'aux objets hôtes de la base de données IdM.

Cette procédure décrit comment créer un objet hôte pour **ipa-client.example.com** dans IdM et s'assurer que l'objet hôte de la machine IdM réelle est capable de gérer cet hôte.

### Conditions préalables

- Vous avez désactivé les contrôles stricts du principal Kerberos utilisé pour cibler le serveur Kerberos, comme indiqué dans la section [Configuration d'un client IdM avec authentification unique Kerberos](#).

### Procédure

1. Créer un nouvel objet hôte sur le serveur IdM :

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

Utilisez l'option **--force**, car le nom d'hôte est un CNAME et non un enregistrement A/AAAA.

2. Sur le serveur IdM, autoriser le nom d'hôte DNS IdM à gérer l'entrée d'hôte Active Directory dans la base de données IdM :

```
[root@idm-server.idm.example.com ~]# ipa host-add-managedby idm-client.ad.example.com \
--hosts=idm-client.idm.example.com
```

3. Vous pouvez maintenant demander un certificat SSL pour votre client IdM avec l'enregistrement d'extension **dnsName** pour son nom d'hôte dans le domaine DNS Active Directory :

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

## CHAPITRE 9. CRÉATION D'UN TRUST

Cette section décrit comment configurer la confiance Identity Management (IdM)/Active Directory (AD) du côté IdM à l'aide de la ligne de commande.

### Conditions préalables

- Le DNS est correctement configuré. Les serveurs IdM et AD doivent être en mesure de résoudre leurs noms respectifs. Pour plus de détails, voir [Configuration des paramètres DNS et Realm pour une confiance](#).
- Les versions prises en charge d'AD et d'IdM sont déployées. Pour plus de détails, voir [Versions prises en charge de Windows Server](#).
- Vous avez obtenu un ticket Kerberos. Pour plus de détails, voir [Utilisation de kinit pour se connecter manuellement à IdM](#).

### 9.1. PRÉPARATION DU SERVEUR IDM POUR LA CONFIANCE

Avant d'établir une confiance avec AD, vous devez préparer le domaine IdM à l'aide de l'utilitaire **ipa-adtrust-install** sur un serveur IdM.



#### NOTE

Tout système sur lequel vous exécutez la commande **ipa-adtrust-install** devient automatiquement un contrôleur de confiance AD. Toutefois, vous ne devez exécuter **ipa-adtrust-install** qu'une seule fois sur un serveur IdM.

### Conditions préalables

- Le serveur IdM est installé.
- Vous devez disposer des privilèges de root pour installer les paquets et redémarrer les services IdM.

### Procédure

1. Installez les paquets nécessaires :

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

2. S'authentifier en tant qu'utilisateur administratif de l'IdM :

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

3. Exécutez l'utilitaire **ipa-adtrust-install**:

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

Les enregistrements de service DNS sont créés automatiquement si IdM a été installé avec un serveur DNS intégré.

Si vous avez installé IdM sans serveur DNS intégré, **ipa-adtrust-install** imprime une liste d'enregistrements de service que vous devez ajouter manuellement au DNS avant de pouvoir continuer.

- Le script vous indique que le site **/etc/samba/smb.conf** existe déjà et qu'il va être réécrit :

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

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

- Le script vous invite à configurer le plug-in **slapi-nis**, un plug-in de compatibilité qui permet aux anciens clients Linux de travailler avec des utilisateurs de confiance :

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

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

- Lorsque vous y êtes invité, entrez le nom NetBIOS du domaine IdM ou appuyez sur **Enter** pour accepter le nom proposé :

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

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

- Vous êtes invité à exécuter la tâche de génération de SID afin de créer un SID pour tous les utilisateurs existants :

```
Voulez-vous exécuter la tâche ipa-sidgen ? [non] : yes
```

Il s'agit d'une tâche gourmande en ressources, donc si vous avez un grand nombre d'utilisateurs, vous pouvez l'exécuter à un autre moment.

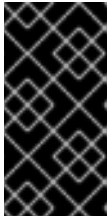
- (Optional)** Par défaut, la plage de ports Dynamic RPC est définie comme **49152-65535** pour Windows Server 2008 et les versions ultérieures. Si vous devez définir une plage de ports Dynamic RPC différente pour votre environnement, configurez Samba pour qu'il utilise d'autres ports et ouvrez ces ports dans les paramètres de votre pare-feu. L'exemple suivant définit la plage de ports à **55000-65000**.

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

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

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

- Assurez-vous que le DNS est correctement configuré, comme décrit dans la section [Vérification de la configuration DNS d'une confiance](#).



## IMPORTANT

Red Hat vous recommande fortement de vérifier la configuration DNS comme décrit dans la section [Vérification de la configuration DNS pour une confiance](#) à chaque fois après l'exécution de **ipa-adtrust-install**, en particulier si IdM ou AD n'utilisent pas de serveurs DNS intégrés.

10. Redémarrez le service **ipa**:

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

11. Utilisez l'utilitaire **smbclient** pour vérifier que Samba répond à l'authentification Kerberos du côté IdM :

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

## 9.2. MISE EN PLACE D'UN CONTRAT DE FIDUCIE À L'AIDE DE LA LIGNE DE COMMANDE

Cette section décrit comment configurer l'accord de confiance à l'aide de la ligne de commande. Le serveur Identity Management (IdM) vous permet de configurer trois types d'accords de confiance :

- **One-way trust**- option par défaut. La confiance à sens unique permet aux utilisateurs et aux groupes Active Directory (AD) d'accéder aux ressources du domaine IdM, mais pas l'inverse. Le domaine IdM fait confiance à la forêt AD, mais la forêt AD ne fait pas confiance au domaine IdM.
- **Two-way trust**- La confiance réciproque permet aux utilisateurs et aux groupes AD d'accéder aux ressources de l'IdM.

Vous devez configurer une confiance à double sens pour des solutions telles que Microsoft SQL Server qui s'attendent à ce que les extensions Microsoft **S4U2Self** et **S4U2Proxy** du protocole Kerberos fonctionnent au-delà d'une limite de confiance. Une application sur un hôte IdM RHEL peut demander à un contrôleur de domaine Active Directory des informations **S4U2Self** ou **S4U2Proxy** sur un utilisateur AD, et une confiance à double sens fournit cette fonctionnalité.

Notez que cette fonctionnalité de confiance bidirectionnelle ne permet pas aux utilisateurs de l'IdM de se connecter aux systèmes Windows, et que la confiance bidirectionnelle dans l'IdM ne donne aux utilisateurs aucun droit supplémentaire par rapport à la solution de confiance unidirectionnelle dans AD.

- Pour créer une confiance réciproque, ajoutez l'option suivante à la commande : **--two-way=true**
- **External trust** - une relation de confiance entre l'IdM et un domaine AD dans différentes forêts. Alors qu'une confiance forestière nécessite toujours l'établissement d'une confiance entre l'IdM et le domaine racine d'une forêt Active Directory, une confiance externe peut être établie entre l'IdM et un domaine à l'intérieur d'une forêt. Cette solution n'est recommandée que s'il n'est pas possible d'établir une confiance forestière entre les domaines racines d'une forêt pour des raisons administratives ou organisationnelles.



- Pour créer la confiance externe, ajoutez l'option suivante à la commande : **--external=true**

Dans cette section, les étapes ci-dessous vous montrent comment créer un contrat de fiducie à sens unique.

### Conditions préalables

- Nom d'utilisateur et mot de passe d'un administrateur Windows.
- Vous avez [préparé le serveur IdM pour la confiance](#) .

### Procédure

- Créez un accord de confiance pour le domaine AD et le domaine IdM à l'aide de la commande **ipa trust-add**:
  - Pour que SSSD génère automatiquement des UID et des GID pour les utilisateurs AD en fonction de leur SID, créez un accord de confiance avec le type de plage d'ID **Active Directory domain**. Il s'agit de la configuration la plus courante.

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

- Si vous avez configuré des attributs POSIX pour vos utilisateurs dans Active Directory (tels que **uidNumber** et **gidNumber**) et que vous souhaitez que SSSD traite ces informations, créez un accord de confiance avec le type de plage d'identifiants **Active Directory domain with POSIX attributes**:

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



### AVERTISSEMENT

Si vous ne spécifiez pas un type de plage d'identifiants lors de la création d'une fiducie, l'IdM tente de sélectionner automatiquement le type de plage approprié en demandant des détails aux contrôleurs de domaine AD dans le domaine racine de la forêt. Si l'IdM ne détecte aucun attribut POSIX, le script d'installation du trust sélectionne la plage d'identifiants **Active Directory domain**.

Si IdM détecte des attributs POSIX dans le domaine racine de la forêt, le script d'installation de la confiance sélectionne la plage d'ID **Active Directory domain with POSIX attributes** et suppose que les UID et les GID sont correctement définis dans AD. Si les attributs POSIX ne sont pas correctement définis dans AD, vous ne pourrez pas résoudre les utilisateurs AD.

Par exemple, si les utilisateurs et les groupes qui ont besoin d'accéder aux systèmes IdM ne font pas partie du domaine racine de la forêt, mais sont plutôt situés dans un domaine enfant du domaine de la forêt, le script d'installation peut ne pas détecter les attributs POSIX définis dans le domaine AD enfant. Dans ce cas, Red Hat vous recommande de choisir explicitement le type de plage d'ID POSIX lors de l'établissement de la confiance.

## 9.3. MISE EN PLACE D'UN ACCORD DE CONFIANCE DANS L'INTERFACE WEB IDM

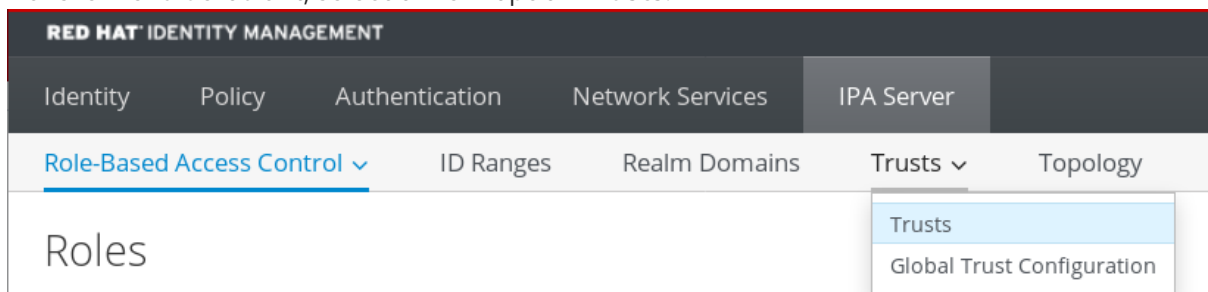
Cette section décrit comment configurer l'accord de confiance entre Identity Management (IdM)/Active Directory (AD) du côté IdM à l'aide de l'interface Web IdM.

### Conditions préalables

- Le DNS est correctement configuré. Les serveurs IdM et AD doivent être en mesure de résoudre les noms des autres.
- Les versions prises en charge d'AD et d'IdM sont déployées.
- Vous avez obtenu un ticket Kerberos.
- Avant de créer une confiance dans l'interface Web, préparez le serveur IdM pour la confiance comme décrit dans : [Préparation du serveur IdM pour la confiance](#) .
- Vous devez être connecté en tant qu'administrateur IdM.

### Procédure

1. Se connecter à l'interface Web IdM avec des privilèges d'administrateur. Pour plus de détails, voir [Accès à l'interface web IdM dans un navigateur web](#) .
2. Dans l'interface Web IdM, cliquez sur l'onglet **IPA Server**.
3. Dans l'onglet **IPA Server**, cliquez sur l'onglet **Trusts**.
4. Dans le menu déroulant, sélectionnez l'option **Trusts**.



5. Cliquez sur le bouton **Add**.
6. Dans la boîte de dialogue **Add Trust**, entrez le nom du domaine Active Directory.
7. Dans les champs **Account** et **Password**, ajoutez les informations d'identification de l'administrateur Active Directory.

8. (Optional) Sélectionnez **Two-way trust**, si vous souhaitez permettre aux utilisateurs et aux groupes AD d'accéder aux ressources dans IdM. Cependant, la confiance bidirectionnelle dans IdM ne donne aux utilisateurs aucun droit supplémentaire par rapport à la solution de confiance unidirectionnelle dans AD. Les deux solutions sont considérées comme aussi sûres l'une que l'autre en raison des paramètres de filtrage SID par défaut de la confiance inter-forêts.
9. (Optional) Sélectionnez **External trust** si vous configurez une confiance avec un domaine AD qui n'est pas le domaine racine d'une forêt AD. Bien qu'une confiance de forêt nécessite toujours l'établissement d'une confiance entre IdM et le domaine racine d'une forêt Active Directory, vous pouvez établir une confiance externe entre IdM et n'importe quel domaine au sein d'une forêt AD.
10. (Optional) Par défaut, le script d'installation de trust tente de détecter le type de plage d'identifiants approprié. Vous pouvez également définir explicitement le type de plage d'identifiants en choisissant l'une des options suivantes :
  - a. Pour que SSSD génère automatiquement des UID et des GID pour les utilisateurs AD en fonction de leur SID, sélectionnez le type de plage d'ID **Active Directory domain**. Il s'agit de la configuration la plus courante.
  - b. Si vous avez configuré des attributs POSIX pour vos utilisateurs dans Active Directory (tels que **uidNumber** et **gidNumber**) et que vous souhaitez que SSSD traite ces informations, sélectionnez le type de plage d'ID **Active Directory domain with POSIX attributes**.

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



## AVERTISSEMENT

Si vous laissez le paramètre **Range type** sur l'option par défaut **Detect**, l'IdM tente de sélectionner automatiquement le type de plage approprié en demandant des détails aux contrôleurs de domaine AD dans le domaine racine de la forêt. Si l'IdM ne détecte aucun attribut POSIX, le script d'installation de la confiance sélectionne la plage d'ID **Active Directory domain**.

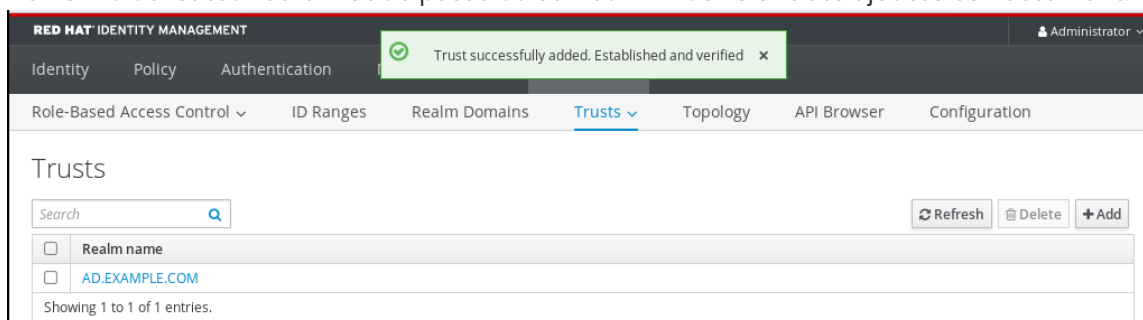
Si IdM détecte des attributs POSIX dans le domaine racine de la forêt, le script d'installation de la confiance sélectionne la plage d'ID **Active Directory domain with POSIX attributes** et suppose que les UID et les GID sont correctement définis dans AD. Si les attributs POSIX ne sont pas correctement définis dans AD, vous ne pourrez pas résoudre les utilisateurs AD.

Par exemple, si les utilisateurs et les groupes qui ont besoin d'accéder aux systèmes IdM ne font pas partie du domaine racine de la forêt, mais sont plutôt situés dans un domaine enfant du domaine de la forêt, le script d'installation peut ne pas détecter les attributs POSIX définis dans le domaine AD enfant. Dans ce cas, Red Hat vous recommande de choisir explicitement le type de plage d'ID POSIX lors de l'établissement de la confiance.

11. Cliquez sur **Add**.

### Verification steps

- Si la confiance a été ajoutée avec succès au serveur IdM, vous pouvez voir la fenêtre pop-up verte dans l'interface Web IdM. Cela signifie que le :
  - Le nom de domaine existe
  - Le nom d'utilisateur et le mot de passe du serveur Windows ont été ajoutés correctement.



Vous pouvez maintenant continuer à tester la connexion de confiance et l'authentification Kerberos.

## 9.4. MISE EN PLACE D'UN ACCORD DE CONFIANCE À L'AIDE D'ANSIBLE

Cette section décrit comment configurer un accord de confiance à sens unique entre Identity Management (IdM) et Active Directory (AD) à l'aide d'un playbook Ansible. Vous pouvez configurer trois types d'accords de confiance :

- **One-way trust**- option par défaut. La confiance à sens unique permet aux utilisateurs et aux groupes Active Directory (AD) d'accéder aux ressources du domaine IdM, mais pas l'inverse. Le domaine IdM fait confiance à la forêt AD, mais la forêt AD ne fait pas confiance au domaine IdM.
- **Two-way trust**- La confiance réciproque permet aux utilisateurs et aux groupes AD d'accéder aux ressources de l'IdM.

Vous devez configurer une confiance à double sens pour des solutions telles que Microsoft SQL Server qui s'attendent à ce que les extensions Microsoft **S4U2Self** et **S4U2Proxy** du protocole Kerberos fonctionnent au-delà d'une limite de confiance. Une application sur un hôte IdM RHEL peut demander à un contrôleur de domaine Active Directory des informations **S4U2Self** ou **S4U2Proxy** sur un utilisateur AD, et une confiance à double sens fournit cette fonctionnalité.

Notez que cette fonctionnalité de confiance bidirectionnelle ne permet pas aux utilisateurs de l'IdM de se connecter aux systèmes Windows, et que la confiance bidirectionnelle dans l'IdM ne donne aux utilisateurs aucun droit supplémentaire par rapport à la solution de confiance unidirectionnelle dans AD.

- Pour créer la confiance réciproque, ajoutez la variable suivante à la tâche du playbook ci-dessous : **two\_way: true**
- **External trust** - une relation de confiance entre l'IdM et un domaine AD dans différentes forêts. Alors qu'une confiance forestière nécessite toujours l'établissement d'une confiance entre l'IdM et le domaine racine d'une forêt Active Directory, une confiance externe peut être établie entre l'IdM et un domaine à l'intérieur d'une forêt. Cette solution n'est recommandée que s'il n'est pas possible d'établir une confiance forestière entre les domaines racines d'une forêt pour des raisons administratives ou organisationnelles.
  - Pour créer la confiance externe, ajoutez la variable suivante à la tâche du playbook ci-dessous : **external: true**

### Conditions préalables

- Nom d'utilisateur et mot de passe d'un administrateur Windows.
- Le mot de passe de l'IdM **admin**.
- Vous avez [préparé le serveur IdM pour la confiance](#) .
- Vous utilisez la version 4.8.7 d'IdM ou une version ultérieure. Pour connaître la version d'IdM installée sur votre serveur, exécutez **ipa --version**.
- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire `~/MyPlaybooks/` vous avez créé un [fichier d'inventaire Ansible](#) avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin\_password**.

- Vous utilisez la version 2.8 ou ultérieure d'Ansible.
- Vous avez installé le paquet `ansible-freeipa`.
- L'exemple suppose que dans le répertoire `~/MyPlaybooks/` vous avez créé un [fichier d'inventaire Ansible](#) avec le nom de domaine complet (FQDN) du serveur IdM sur lequel vous configurez la confiance.

## Procédure

1. Naviguez jusqu'à votre répertoire `~/MyPlaybooks/` répertoire :

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

2. Sélectionnez l'un des scénarios suivants en fonction de votre cas d'utilisation :

- Pour créer un accord de confiance de mappage d'ID, dans lequel SSSD génère automatiquement des UID et des GID pour les utilisateurs et les groupes AD en fonction de leurs SID, créez un playbook **add-trust.yml** avec le contenu suivant :

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

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: ensure the trust is present
    ipatrust:
      ipadmin_password: "{{ ipadmin_password }}"
      realm: ad.example.com
      admin: Administrator
      password: secret_password
      range_type: ipa-ad-trust
      state: present
```

Dans l'exemple :

- **realm** définit la chaîne de nom du domaine AD.
- **admin** définit la chaîne de l'administrateur du domaine AD.
- **password** définit la chaîne de mots de passe de l'administrateur du domaine AD.
- Pour créer un accord de confiance POSIX, dans lequel SSSD traite les attributs POSIX stockés dans AD, tels que **uidNumber** et **gidNumber**, créez un playbook **add-trust.yml** avec le contenu suivant :

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

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: ensure the trust is present
```

```

ipatrust:
  ipaadmin_password: "{{ ipaadmin_password }}"
  realm: ad.example.com
  admin: Administrator
  password: secret_password
  range_type: ipa-ad-trust-posix
  state: present

```

- Pour créer un accord de confiance dans lequel IdM tente de sélectionner automatiquement le type de plage approprié, **ipa-ad-trust** ou **ipa-ad-trust-posix**, en demandant des détails aux contrôleurs de domaine AD dans le domaine racine de la forêt, créez un playbook **add-trust.yml** avec le contenu suivant :

```

---
- name: Playbook to create a trust
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: ensure the trust is present
    ipatrust:
      ipaadmin_password: "{{ ipaadmin_password }}"
      realm: ad.example.com
      admin: Administrator
      password: secret_password
      state: present

```



### AVERTISSEMENT

Si vous ne spécifiez pas de type de plage d'identifiants lors de la création d'un trust et si IdM ne détecte aucun attribut POSIX dans le domaine racine de la forêt AD, le script d'installation du trust sélectionne la plage d'identifiants **Active Directory domain**.

Si IdM détecte des attributs POSIX dans le domaine racine de la forêt, le script d'installation de la confiance sélectionne la plage d'ID **Active Directory domain with POSIX attributes** et suppose que les UID et les GID sont correctement définis dans AD.

Cependant, si les attributs POSIX ne sont pas correctement définis dans AD, vous ne pourrez pas résoudre les utilisateurs AD. Par exemple, si les utilisateurs et les groupes qui ont besoin d'accéder aux systèmes IdM ne font pas partie du domaine racine de la forêt, mais sont plutôt situés dans un domaine enfant du domaine de la forêt, le script d'installation peut ne pas détecter les attributs POSIX définis dans le domaine AD enfant. Dans ce cas, Red Hat vous recommande de choisir explicitement le type de plage d'ID POSIX lors de l'établissement de la confiance.

3. Enregistrer le fichier.

4. Exécutez le playbook Ansible. Spécifiez le fichier du livre de jeu, le fichier contenant le mot de passe protégeant le fichier **secret.yml** et le fichier d'inventaire :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory add-trust.yml
```

### Ressources supplémentaires

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

## 9.5. VÉRIFICATION DE LA CONFIGURATION DE KERBEROS

Pour vérifier la configuration de Kerberos, testez s'il est possible d'obtenir un ticket pour un utilisateur de gestion d'identité (IdM) et si l'utilisateur IdM peut demander des tickets de service.

### Procédure

1. Demander un ticket pour un utilisateur Active Directory (AD) :

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

2. Demande de tickets de service pour un service dans le domaine IdM :

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

Si le ticket de service AD est accordé avec succès, un ticket d'octroi de ticket (TGT) inter-royaumes est listé avec tous les autres tickets demandés. Le TGT est nommé `krbtgt/IPA.DOMAIN@AD.DOMAIN`.

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

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

Le plug-in **localauth** établit une correspondance entre les principaux Kerberos et les noms d'utilisateurs locaux du System Security Services Daemon (SSSD). Cela permet aux utilisateurs AD d'utiliser l'authentification Kerberos et d'accéder aux services Linux, qui prennent directement en charge l'authentification GSSAPI.

## 9.6. VÉRIFICATION DE LA CONFIGURATION DE LA CONFIANCE SUR IDM

Avant de configurer la confiance, vérifiez que les serveurs Identity Management (IdM) et Active Directory (AD) peuvent se résoudre et se résoudre mutuellement.



## Conditions préalables

- Vous devez être connecté avec des privilèges d'administrateur.

## Procédure

1. Exécutez une requête DNS pour les enregistrements de service MS DC Kerberos over UDP et LDAP over TCP.

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

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

Ces commandes dressent la liste de tous les serveurs IdM sur lesquels **ipa-adtrust-install** a été exécuté. La sortie est vide si **ipa-adtrust-install** n'a été exécuté sur aucun serveur IdM, ce qui est généralement le cas avant l'établissement de la première relation de confiance.

2. Lancez une requête DNS pour les enregistrements de service Kerberos et LDAP over TCP afin de vérifier que l'IdM est en mesure de résoudre les enregistrements de service pour AD :

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

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

## 9.7. VÉRIFICATION DE LA CONFIGURATION DE LA CONFIANCE SUR AD

Après avoir configuré la confiance, vérifiez que

- Les services hébergés par Identity Management (IdM) peuvent être résolus à partir du serveur Active Directory (AD).
- Les services AD peuvent être résolus à partir du serveur AD.

## Conditions préalables

- Vous devez être connecté avec des privilèges d'administrateur.

## Procédure

1. Sur le serveur AD, configurez l'utilitaire **nslookup.exe** pour qu'il recherche les enregistrements de service.

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

2. Entrez le nom de domaine pour les enregistrements de service Kerberos sur UDP et LDAP sur TCP.

```

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

```

- Changez le type de service en TXT et lancez une requête DNS pour l'enregistrement TXT avec le nom du royaume IdM Kerberos.

```

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

    "IDM.EXAMPLE.COM"

```

- Exécutez une requête DNS pour les enregistrements de service MS DC Kerberos over UDP et LDAP over TCP.

```

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

```

Active Directory ne s'attend à découvrir que les contrôleurs de domaine qui peuvent répondre aux demandes de protocole spécifiques à AD, tels que les autres contrôleurs de domaine AD et les contrôleurs de confiance IdM. Utilisez l'outil **ipa-adtrust-install** pour promouvoir un serveur IdM en contrôleur de confiance, et vous pouvez vérifier quels serveurs sont des contrôleurs de confiance à l'aide de la commande **ipa server-role-find --role 'AD trust controller'**.

- Vérifiez que les services AD peuvent être résolus à partir du serveur AD.

```

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

```

- Entrez le nom de domaine pour les enregistrements de service Kerberos sur UDP et LDAP sur TCP.

■

```

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

```

## 9.8. CRÉATION D'UN AGENT FIDUCIAIRE

Un agent de confiance est un serveur IdM qui peut effectuer des recherches d'identité auprès des contrôleurs de domaine AD.

Par exemple, si vous créez une réplique d'un serveur IdM qui a un lien de confiance avec Active Directory, vous pouvez configurer la réplique en tant qu'agent de confiance. Le rôle d'agent fiduciaire AD n'est pas automatiquement installé sur un réplica.

### Conditions préalables

- IdM est installé avec une confiance Active Directory.
- The **sssd-tools** package is installed.

### Procédure

1. Sur un contrôleur de confiance existant, exécutez la commande **ipa-adtrust-install --add-agents**:

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

La commande lance une session de configuration interactive et vous invite à fournir les informations nécessaires à la configuration de l'agent.

2. Redémarrer le service IdM sur l'agent de confiance.

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

3. Supprimer toutes les entrées du cache SSSD de l'agent de confiance :

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

4. Vérifiez que le rôle d'agent fiduciaire AD est installé sur la réplique :

```

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

```

### Ressources supplémentaires

- Pour plus d'informations sur l'option **--add-agents**, voir la page de manuel **ipa-adtrust-install(1)**.
- Pour plus d'informations sur les agents de confiance, voir [Contrôleurs et agents de confiance](#) dans le guide Planification de la gestion des identités.

## 9.9. ACTIVATION DU MAPPAGE AUTOMATIQUE DES GROUPES PRIVÉS POUR UNE PLAGE D'ID POSIX SUR LA CLI

Par défaut, SSSD ne mappe pas les groupes privés pour les utilisateurs d'Active Directory (AD) si vous avez établi une confiance POSIX qui repose sur des données POSIX stockées dans AD. Si des utilisateurs AD n'ont pas de groupes primaires configurés, IdM n'est pas en mesure de les résoudre.

Cette procédure explique comment activer le mappage automatique des groupes privés pour une plage d'identifiants en définissant l'option **hybrid** pour le paramètre **auto\_private\_groups** SSSD sur la ligne de commande. En conséquence, IdM est en mesure de résoudre les utilisateurs AD qui n'ont pas de groupes primaires configurés dans AD.

### Conditions préalables

- Vous avez réussi à établir une confiance POSIX inter-forêts entre vos environnements IdM et AD.

### Procédure

1. Affichez toutes les plages d'identification et notez la plage d'identification AD que vous souhaitez modifier.

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

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

2. Ajustez le comportement du groupe privé automatique pour la plage d'ID AD à l'aide de la commande **ipa idrange-mod**.

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

3. Réinitialisez le cache SSSD pour activer le nouveau paramètre.

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

## Ressources supplémentaires

- [Options de mappage automatique des groupes privés pour les utilisateurs AD](#)

## 9.10. ACTIVATION DU MAPPAGE AUTOMATIQUE DES GROUPES PRIVÉS POUR UNE PLAGE D'ID POSIX DANS L'IDM WEBUI

Par défaut, SSSD ne mappe pas les groupes privés pour les utilisateurs d'Active Directory (AD) si vous avez établi une confiance POSIX qui repose sur des données POSIX stockées dans AD. Si des utilisateurs AD n'ont pas de groupes primaires configurés, IdM n'est pas en mesure de les résoudre.

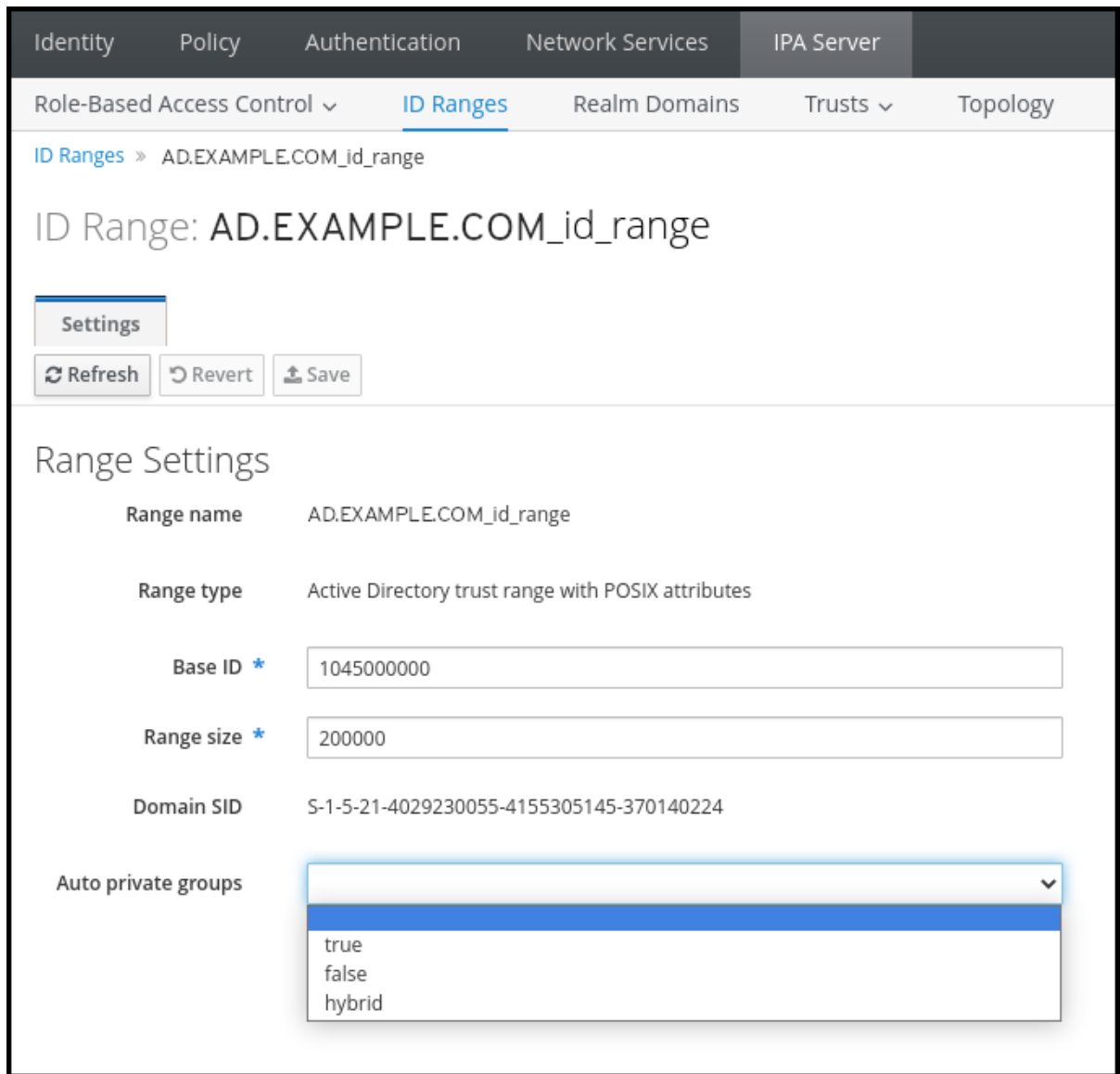
Cette procédure explique comment activer le mappage automatique des groupes privés pour une plage d'identifiants en définissant l'option **hybrid** pour le paramètre **auto\_private\_groups** SSSD dans l'interface Web de gestion des identités (IdM). En conséquence, IdM est capable de résoudre les utilisateurs AD qui n'ont pas de groupes primaires configurés dans AD.

### Conditions préalables

- Vous avez réussi à établir une confiance POSIX inter-forêts entre vos environnements IdM et AD.

### Procédure

1. Connectez-vous à l'interface Web IdM avec votre nom d'utilisateur et votre mot de passe.
2. Ouvrez l'onglet **IPA Server** → **ID Ranges**.
3. Sélectionnez la plage d'identifiants que vous souhaitez modifier, par exemple **AD.EXAMPLE.COM\_id\_range**.
4. Dans le menu déroulant **Auto private groups**, sélectionnez l'option **hybrid**.



The screenshot displays the Red Hat IdM web interface. At the top, there are navigation tabs: Identity, Policy, Authentication, Network Services, IPA Server, and a partially visible one. Below these are sub-tabs: Role-Based Access Control, ID Ranges (selected), Realm Domains, Trusts, and Topology. The breadcrumb path is 'ID Ranges » AD.EXAMPLE.COM\_id\_range'. The main heading is 'ID Range: AD.EXAMPLE.COM\_id\_range'. Below the heading are three buttons: 'Settings' (highlighted), 'Refresh', 'Revert', and 'Save'. The 'Range Settings' section contains the following fields:

- Range name: AD.EXAMPLE.COM\_id\_range
- Range type: Active Directory trust range with POSIX attributes
- Base ID \*: 1045000000
- Range size \*: 200000
- Domain SID: S-1-5-21-4029230055-4155305145-370140224
- Auto private groups: A dropdown menu with options 'true', 'false', and 'hybrid'.

5. Cliquez sur le bouton **Save** pour enregistrer vos modifications.

### Ressources supplémentaires

- [Options de mappage automatique des groupes privés pour les utilisateurs AD](#)

## CHAPITRE 10. RÉOLUTION DES PROBLÈMES LIÉS À LA MISE EN PLACE D'UNE FIDUCIE INTER-FORESTIÈRE

Ce chapitre traite du dépannage du processus de configuration d'une confiance inter-forêts entre votre environnement de gestion des identités (IdM) et une forêt Active Directory (AD).

### 10.1. SÉQUENCE DES ÉVÉNEMENTS LORS DE L'ÉTABLISSEMENT D'UNE CONFIANCE INTER-FORÊTS AVEC AD

Lorsque vous utilisez la commande **ipa trust-add** pour établir une confiance inter-forêts avec un contrôleur de domaine (DC) Active Directory (AD), la commande opère au nom de l'utilisateur qui a lancé la commande et effectue les actions suivantes sur le serveur IdM. Si vous ne parvenez pas à établir une confiance inter-forêts, vous pouvez utiliser cette liste pour vous aider à circonscrire et à résoudre votre problème.

#### Partie 1 : La commande vérifie les réglages et les entrées

1. Vérifiez que le serveur IdM a le rôle **Trust Controller**.
2. Validez les options passées à la commande **ipa trust-add**.
3. Validez la plage d'identifiants associée à un domaine racine de la forêt de confiance. Si vous n'avez pas spécifié le type et les propriétés de la plage d'identifiants en tant qu'options de la commande **ipa trust-add**, ils sont découverts à partir d'Active Directory.

#### Partie 2 : La commande tente d'établir une relation de confiance avec un domaine Active Directory

4. Créer un objet de confiance distinct pour chaque direction de confiance. Chacun des objets est créé des deux côtés (IdM et AD). Si vous établissez une confiance à sens unique, un seul objet est créé de chaque côté.
5. Le serveur IdM utilise la suite Samba pour gérer les capacités de contrôleur de domaine pour Active Directory et crée un objet de confiance sur le PDC AD cible :
  - a. Le serveur IdM établit une connexion sécurisée au partage **IPC\$** sur le DC cible. Depuis RHEL 8.4, la connexion nécessite au moins le protocole SMB3 avec Windows Server 2012 et supérieur pour garantir que la connexion est suffisamment sécurisée avec un cryptage basé sur AES utilisé pour la session.
  - b. Le serveur IdM demande la présence de l'objet de domaine de confiance (TDO) à l'aide d'un appel **LSA QueryTrustedDomainInfoByName**.
  - c. Si le TDO est déjà présent, supprimez-le en appelant **LSA DeleteTrustedDomain**.



#### NOTE

Cet appel échoue si le compte d'utilisateur AD utilisé pour établir la confiance ne dispose pas de tous les privilèges **Enterprise Admin (EA)** ou **Domain Admin (DA)** pour la racine de la forêt, tels que les membres du groupe **Incoming Forest Trust Builders**. Si l'ancien TDO n'est pas automatiquement supprimé, un administrateur AD doit le supprimer manuellement d'AD.

- d. Le serveur IdM crée un nouveau TDO à l'aide d'un appel **LSA CreateTrustedDomainEx2**. Les informations d'identification du TDO sont générées de manière aléatoire à l'aide d'un générateur de mot de passe fourni par Samba, avec 128 caractères aléatoires.
- e. Le nouveau TDO est ensuite modifié par un appel à **LSA SetInformationTrustedDomain** pour s'assurer que les types de chiffrement pris en charge par la confiance sont correctement définis :
  - i. Le type de cryptage **RC4\_HMAC\_MD5** est activé, même si aucune clé RC4 n'est utilisée, en raison de la conception d'Active Directory.
  - ii. **AES128\_CTS\_HMAC\_SHA1\_96** et **AES256\_CTS\_HMAC\_SHA1\_96** sont activés.



#### NOTE

Par défaut, RHEL 9 n'autorise pas le cryptage SHA-1, qui est un algorithme requis par AD. Assurez-vous d'avoir activé la sous-politique cryptographique à l'échelle du système **AD-SUPPORT** pour autoriser le chiffrement SHA-1 dans vos serveurs IdM RHEL 9 pour la communication avec les contrôleurs de domaine AD. Voir <link TBA>.

6. Pour une confiance forestière, vérifiez que les domaines internes à la forêt peuvent être atteints de manière transitive avec un appel **LSA SetInformationTrustedDomain**.
7. Ajouter des informations sur la topologie de confiance de l'autre forêt (IdM dans le cas d'une communication avec AD, AD dans le cas d'une communication avec IdM) à l'aide d'un appel **LSA RSetForestTrustInformation**.





## NOTE

Cette étape peut provoquer un conflit pour l'une des trois raisons suivantes :

1. Un conflit d'espace de noms SID, signalé comme une erreur **LSA\_SID\_DISABLED\_CONFLICT**. Ce conflit ne peut être résolu.
2. Un conflit d'espace de noms NetBIOS, signalé comme une erreur **LSA\_NB\_DISABLED\_CONFLICT**. Ce conflit ne peut être résolu.
3. Un conflit d'espace de noms DNS avec un nom de premier niveau (TLN), signalé comme une erreur **LSA\_TLN\_DISABLED\_CONFLICT**. Le serveur IdM peut résoudre automatiquement un conflit TLN s'il est causé par une autre forêt.

Pour résoudre un conflit TLN, le serveur IdM effectue les étapes suivantes :

1. Récupérer les informations de confiance de la forêt en conflit.
2. Ajouter une entrée d'exclusion pour l'espace de noms IdM DNS à la forêt AD.
3. Définir les informations de confiance pour la forêt sur laquelle nous sommes en conflit.
4. Réessayez d'établir la confiance avec la forêt d'origine.

Le serveur IdM ne peut résoudre ces conflits que si vous avez authentifié la commande **ipa trust-add** avec les privilèges d'un administrateur AD qui peut modifier les trusts de la forêt. Si vous n'avez pas accès à ces privilèges, l'administrateur de la forêt d'origine doit effectuer manuellement les étapes ci-dessus dans la section **Active Directory Domains and Trusts** de l'interface utilisateur Windows.

8. S'il n'existe pas, créez la plage d'ID pour le domaine de confiance.
9. Dans le cas d'une confiance forestière, interrogez les contrôleurs de domaine Active Directory à partir de la racine de la forêt pour obtenir des détails sur la topologie de la forêt. Le serveur IdM utilise ces informations pour créer des plages d'identifiants supplémentaires pour tous les domaines supplémentaires de la forêt approuvée.

### Ressources supplémentaires

- [Contrôleurs et agents de confiance](#)
- [Documents de synthèse](#) (Microsoft)
- [Documents techniques](#) (Microsoft)
- [Comptes et groupes privilégiés dans Active Directory](#) (Microsoft)

## 10.2. LISTE DE CONTRÔLE DES CONDITIONS PRÉALABLES À L'ÉTABLISSEMENT D'UNE CONFIANCE AD

Vous pouvez utiliser la liste de contrôle suivante pour passer en revue les conditions préalables à la création d'une confiance avec un domaine AD.

Tableau 10.1. Tableau

Composant	Configuration	Détails supplémentaires
Versions du produit	Votre domaine Active Directory utilise une version prise en charge de Windows Server.	<a href="#">Versions prises en charge de Windows Server</a>
Privilèges de l'administrateur AD	Le compte d'administration Active Directory doit être membre de l'un des groupes suivants : <ul style="list-style-type: none"> <li>● <b>Enterprise Admin (EA)</b> dans la forêt AD</li> <li>● <b>Domain Admins (DA)</b> dans le domaine racine de votre forêt AD</li> </ul>	
Mise en réseau	La prise en charge d'IPv6 est activée dans le noyau Linux pour tous les serveurs IdM.	<a href="#">Exigences IPv6 pour l'IdM</a>
Date et heure	Assurez-vous que les paramètres de date et d'heure des deux serveurs correspondent.	<a href="#">Exigences en matière de services horaires pour l'IdM</a>
Types de cryptage	Les comptes AD suivants disposent de clés de chiffrement AES : <ul style="list-style-type: none"> <li>● Administrateur AD</li> <li>● Comptes d'utilisateurs AD</li> <li>● Services AD</li> </ul> <p>Si vous avez récemment activé le cryptage AES dans AD, générez de nouvelles clés AES en suivant les étapes suivantes :</p> <ol style="list-style-type: none"> <li>1. Rétablissez les relations de confiance entre tous les domaines AD de votre forêt.</li> <li>2. Modifier les mots de passe de l'administrateur AD, des comptes utilisateurs et des services.</li> </ol>	<ul style="list-style-type: none"> <li>● <a href="#">Prise en charge des types de cryptage dans l'IdM</a></li> <li>● <a href="#">Activation du type de cryptage AES dans Active Directory à l'aide d'un GPO</a></li> </ul>

Composant	Configuration	Détails supplémentaires
Firewall	Vous avez ouvert tous les ports nécessaires sur les serveurs IdM et les contrôleurs de domaine AD pour une communication bidirectionnelle.	<a href="#">Ports nécessaires à la communication entre IdM et AD</a>
DNS	<ul style="list-style-type: none"> <li>● IdM et AD ont chacun un domaine DNS primaire unique.</li> <li>● Les domaines IdM et AD DNS ne se chevauchent pas.</li> <li>● Enregistrements DNS (SRV) appropriés pour les services LDAP et Kerberos.</li> <li>● Vous pouvez résoudre les enregistrements DNS de tous les domaines DNS de la confiance.</li> <li>● Les noms de domaine Kerberos sont les versions en majuscules des noms de domaine DNS primaires. Par exemple, le domaine DNS <b>example.com</b> a un domaine Kerberos correspondant <b>EXAMPLE.COM</b></li> </ul>	<a href="#">Configuration des paramètres DNS et Realm pour une confiance</a>
Topology	Assurez-vous que vous essayez d'établir une confiance avec un serveur IdM que vous avez configuré en tant que contrôleur de confiance.	<a href="#">Contrôleurs et agents de confiance</a>

### 10.3. COLLECTE DES JOURNAUX DE DÉBOGAGE D'UNE TENTATIVE D'ÉTABLISSEMENT D'UNE CONFIANCE AD

Si vous rencontrez des problèmes lors de l'établissement d'une confiance entre un environnement IdM et un domaine AD, suivez les étapes suivantes pour activer la journalisation détaillée des erreurs afin de rassembler les journaux d'une tentative d'établissement d'une confiance. Vous pouvez examiner ces journaux pour vous aider dans vos efforts de dépannage, ou vous pouvez les fournir dans un cas d'assistance technique de Red Hat.

#### Conditions préalables

- Pour redémarrer les services IdM, vous devez disposer des droits d'accès à la racine.

## Procédure

1. Pour activer le débogage du serveur IdM, créez le fichier **/etc/ipa/server.conf** avec le contenu suivant.

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

2. Redémarrez le service **httpd** pour charger la configuration de débogage.

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

3. Arrêtez les services **smb** et **winbind**.

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

4. Définir le niveau de journalisation de débogage pour les services **smb** et **winbind**.

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

5. Pour activer la journalisation de débogage pour le code client Samba utilisé par le cadre IdM, modifiez le fichier de configuration **/usr/share/ipa/smb.conf.empty** pour qu'il contienne le contenu suivant.

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

6. Supprimer les journaux Samba précédents.

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

7. Démarrez les services **smb** et **winbind**.

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

8. Imprimer un horodatage lorsque vous tentez d'établir une confiance avec le mode verbeux activé.

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

9. Consultez les fichiers journaux d'erreurs suivants pour obtenir des informations sur l'échec de la demande :

- a. **/var/log/httpd/error\_log**

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

10. Désactiver le débogage.

```
[root@trust_controller ~]# mv /etc/ipa/server.conf /etc/ipa/server.conf.backup
[root@trust_controller ~]# systemctl restart httpd
```

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

11. (*Optional*) Si vous ne parvenez pas à déterminer la cause du problème d'authentification :

- a. Rassemblez et archivez les fichiers journaux que vous avez récemment générés.

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

- b. Ouvrez un dossier d'assistance technique Red Hat et fournissez l'horodatage et les journaux de débogage de la tentative.

### Ressources supplémentaires

- [IPA - Dépannage AD Trust](#)

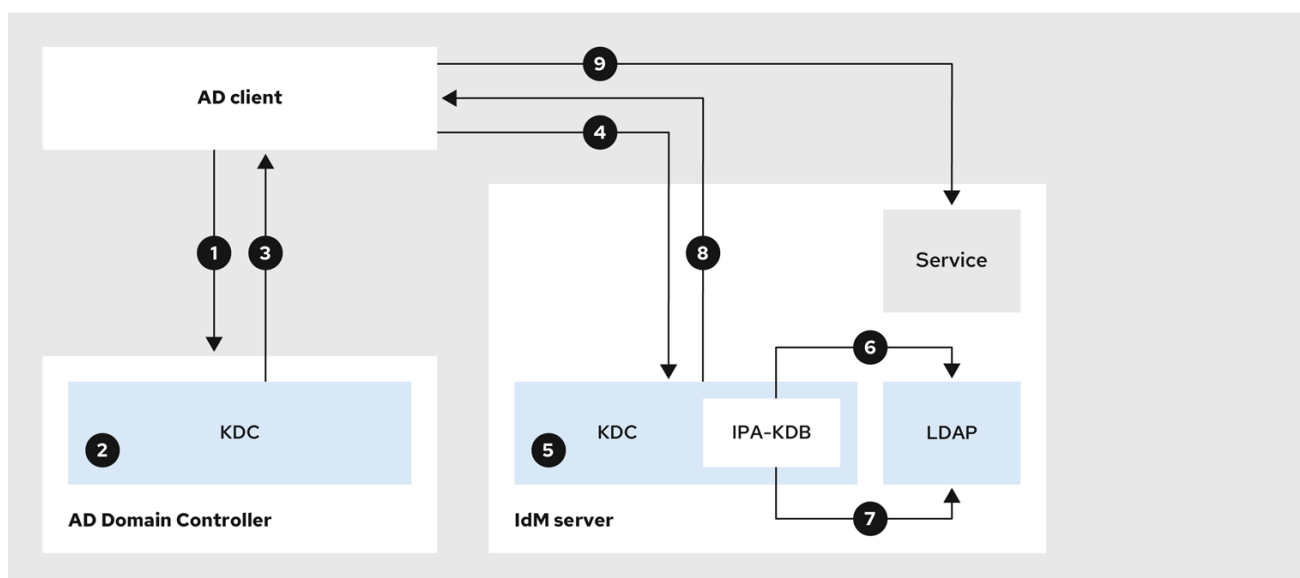
## CHAPITRE 11. DÉPANNAGE DE L'ACCÈS DES CLIENTS AUX SERVICES DANS L'AUTRE FORÊT

Après avoir configuré une confiance entre vos environnements Identity Management (IdM) et Active Directory (AD), vous pouvez rencontrer des problèmes lorsqu'un client d'un domaine n'est pas en mesure d'accéder à un service dans l'autre domaine. Utilisez les diagrammes suivants pour résoudre le problème.

### 11.1. FLUX D'INFORMATIONS LORSQU'UN HÔTE DU DOMAINE RACINE DE LA FORÊT AD DEMANDE DES SERVICES À UN SERVEUR IDM

Le diagramme suivant explique le flux d'informations lorsqu'un client Active Directory (AD) demande un service dans le domaine Identity Management (IdM).

Si vous avez des difficultés à accéder aux services IdM à partir de clients AD, vous pouvez utiliser ces informations pour limiter vos efforts de dépannage et identifier la source du problème.



231\_RHEL\_0422

1. Le client AD contacte le centre de distribution Kerberos AD (KDC) pour effectuer une requête TGS pour le service dans le domaine IdM.
2. Le KDC AD reconnaît que le service appartient au domaine IdM de confiance.
3. Le KDC AD envoie au client un ticket d'attribution de ticket inter-royaumes (TGT), ainsi qu'une référence au KDC IdM de confiance.
4. Le client AD utilise le TGT inter-royaumes pour demander un ticket au KDC IdM.
5. La KDC IdM valide le certificat d'attribut privilégié (MS-PAC) transmis avec le TGT inter-royaumes.
6. Le plugin IPA-KDB peut vérifier l'annuaire LDAP pour voir si des mandants étrangers sont autorisés à obtenir des tickets pour le service demandé.

7. Le plugin IPA-KDB décode le MS-PAC, vérifie et filtre les données. Il effectue des recherches dans le serveur LDAP pour vérifier s'il est nécessaire d'ajouter des informations supplémentaires au MS-PAC, telles que des groupes locaux.
8. Le plugin IPA-KDB encode alors le PAC, le signe, l'attache au ticket de service et l'envoie au client AD.
9. Le client AD peut maintenant contacter le service IdM en utilisant le ticket de service émis par le KDC IdM.

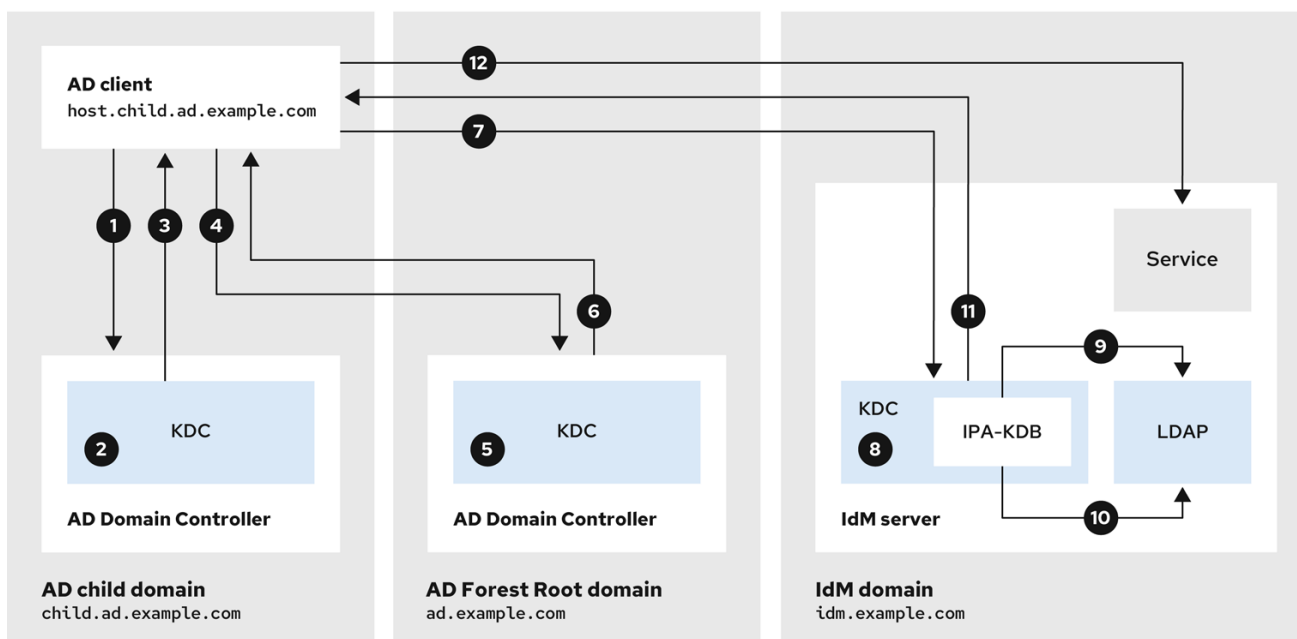
### Ressources supplémentaires

- [Flux d'informations lorsqu'un hôte d'un domaine enfant AD demande des services à un serveur IdM](#)

## 11.2. FLUX D'INFORMATIONS LORSQU'UN HÔTE D'UN DOMAINE ENFANT AD DEMANDE DES SERVICES À UN SERVEUR IDM

Le diagramme suivant explique le flux d'informations lorsqu'un hôte Active Directory (AD) dans un domaine enfant demande un service dans le domaine Identity Management (IdM). Dans ce scénario, le client AD contacte le centre de distribution Kerberos (KDC) du domaine enfant, puis le KDC de la racine de la forêt AD et enfin le KDC IdM pour demander l'accès au service IdM.

Si vous avez des difficultés à accéder aux services IdM à partir de clients AD et que votre client AD appartient à un domaine qui est un domaine enfant de la racine d'une forêt AD, vous pouvez utiliser ces informations pour limiter vos efforts de dépannage et identifier la source du problème.



231\_RHEL\_0422

1. Le client AD contacte le centre de distribution Kerberos AD (KDC) dans son propre domaine pour effectuer une demande de TGS pour le service dans le domaine IdM.
2. Le KDC AD de **child.ad.example.com**, le domaine enfant, reconnaît que le service appartient au domaine IdM de confiance.

3. Le KDC AD du domaine enfant envoie au client un ticket de renvoi pour le domaine racine de la forêt AD **ad.example.com**.
4. Le client AD contacte le KDC dans le domaine racine de la forêt AD pour le service dans le domaine IdM.
5. Le KDC du domaine racine de la forêt reconnaît que le service appartient au domaine IdM de confiance.
6. Le KDC AD envoie au client un ticket d'attribution de ticket inter-royaumes (TGT), ainsi qu'une référence au KDC IdM de confiance.
7. Le client AD utilise le TGT inter-royaumes pour demander un ticket au KDC IdM.
8. La KDC IdM valide le certificat d'attribut privilégié (MS-PAC) transmis avec le TGT inter-royaumes.
9. Le plugin IPA-KDB peut vérifier l'annuaire LDAP pour voir si des mandants étrangers sont autorisés à obtenir des tickets pour le service demandé.
10. Le plugin IPA-KDB décode le MS-PAC, vérifie et filtre les données. Il effectue des recherches dans le serveur LDAP pour vérifier s'il est nécessaire d'ajouter des informations supplémentaires au MS-PAC, telles que des groupes locaux.
11. Le plugin IPA-KDB encode alors le PAC, le signe, l'attache au ticket de service et l'envoie au client AD.
12. Le client AD peut maintenant contacter le service IdM en utilisant le ticket de service émis par le KDC IdM.

### Ressources supplémentaires

- [Flux d'informations lorsqu'un hôte du domaine racine de la forêt AD demande des services à un serveur IdM](#)

## 11.3. FLUX D'INFORMATIONS LORSQU'UN CLIENT IDM DEMANDE DES SERVICES À UN SERVEUR AD

Le diagramme suivant explique le flux d'informations lorsqu'un client Identity Management (IdM) demande un service dans le domaine Active Directory (AD) lorsque vous avez configuré une confiance réciproque entre IdM et AD.

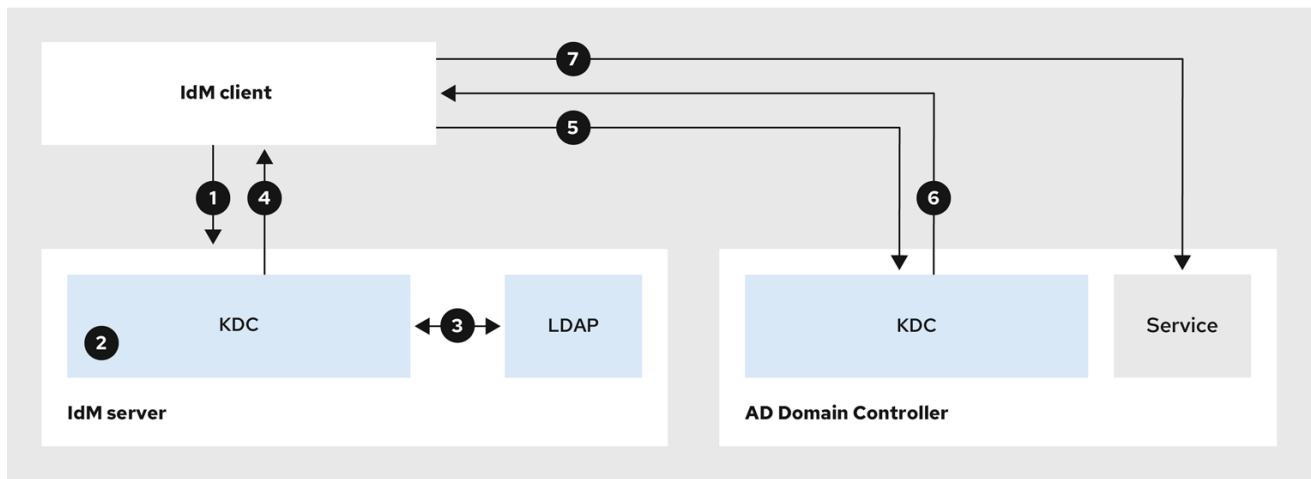
Si vous rencontrez des difficultés pour accéder aux services AD à partir de clients IdM, vous pouvez utiliser ces informations pour limiter vos efforts de dépannage et identifier la source du problème.



### NOTE

Par défaut, IdM établit une confiance unidirectionnelle avec AD, ce qui signifie qu'il n'est pas possible d'émettre des tickets d'attribution de tickets (TGT) inter-royaumes pour des ressources dans une forêt AD. Pour pouvoir demander des tickets à des services de domaines AD de confiance, il faut configurer une confiance bidirectionnelle.





231\_RHEL\_0422

1. Le client IdM demande un ticket d'attribution de ticket (TGT) au centre de distribution Kerberos (KDC) IdM pour le service AD qu'il souhaite contacter.
2. Le KDC IdM reconnaît que le service appartient à la zone AD, vérifie que la zone est connue et approuvée, et que le client est autorisé à demander des services dans cette zone.
3. À l'aide des informations fournies par le serveur d'annuaire IdM sur le principal utilisateur, la KDC IdM crée un TGT inter-royaumes avec un enregistrement de certificat d'attribut privilégié (MS-PAC) sur le principal utilisateur.
4. Le KDC IdM renvoie un TGT inter-royaumes au client IdM.
5. Le client IdM contacte le KDC AD pour demander un ticket pour le service AD, en présentant le TGT inter-royaumes qui contient le MS-PAC fourni par le KDC IdM.
6. Le serveur AD valide et filtre le PAC et renvoie un ticket pour le service AD.
7. Le client IPA peut maintenant contacter le service AD.

### Ressources supplémentaires

- [Fiducies à sens unique et fiducies à double sens](#)

## CHAPITRE 12. SUPPRESSION DE LA CONFIANCE À L'AIDE DE LA LIGNE DE COMMANDE

Cette section décrit comment supprimer la confiance Identity Management (IdM)/Active Directory (AD) du côté IdM à l'aide de l'interface de ligne de commande.

### Conditions préalables

- Vous avez obtenu un ticket Kerberos en tant qu'administrateur IdM. Pour plus de détails, voir [Connexion à IdM dans l'interface Web : Utilisation d'un ticket Kerberos](#).

### Procédure

1. Utilisez la commande **ipa trust-del** pour supprimer la configuration de confiance de l'IdM.

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

```
-----  
Deleted trust "ad_domain_name"  
-----
```

2. Supprimez l'objet de confiance de votre configuration Active Directory.

### NOTE

La suppression de la configuration de la confiance ne supprime pas automatiquement la plage d'identifiants que l'IdM a créée pour les utilisateurs AD. Ainsi, si vous ajoutez à nouveau la confiance, la plage d'identifiants existante est réutilisée. En outre, si les utilisateurs AD ont créé des fichiers sur un client IdM, leurs identifiants POSIX sont conservés dans les métadonnées du fichier.

Pour supprimer toutes les informations relatives à une confiance AD, supprimez la plage d'ID utilisateur AD après avoir supprimé la configuration de la confiance et l'objet de confiance :

```
# ipa idrange-del AD.EXAMPLE.COM_id_range  
# systemctl restart sssd
```

### Verification steps

- Utilisez la commande **ipa trust-show** pour confirmer que la confiance a été supprimée.

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

### Ressources supplémentaires

- [Suppression d'une plage d'identifiants après la suppression d'une confiance dans AD](#)

## CHAPITRE 13. SUPPRESSION DE LA CONFIANCE À L'AIDE DE L'INTERFACE WEB IDM

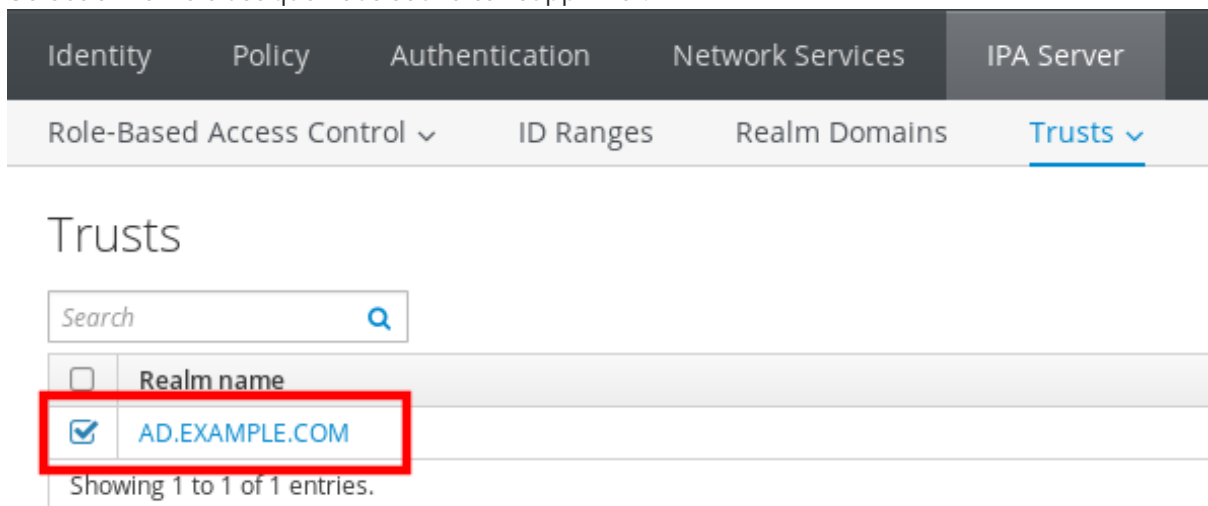
Cette section décrit comment supprimer la confiance entre Identity Management (IdM)/Active Directory (AD) à l'aide de l'interface Web IdM.

### Conditions préalables

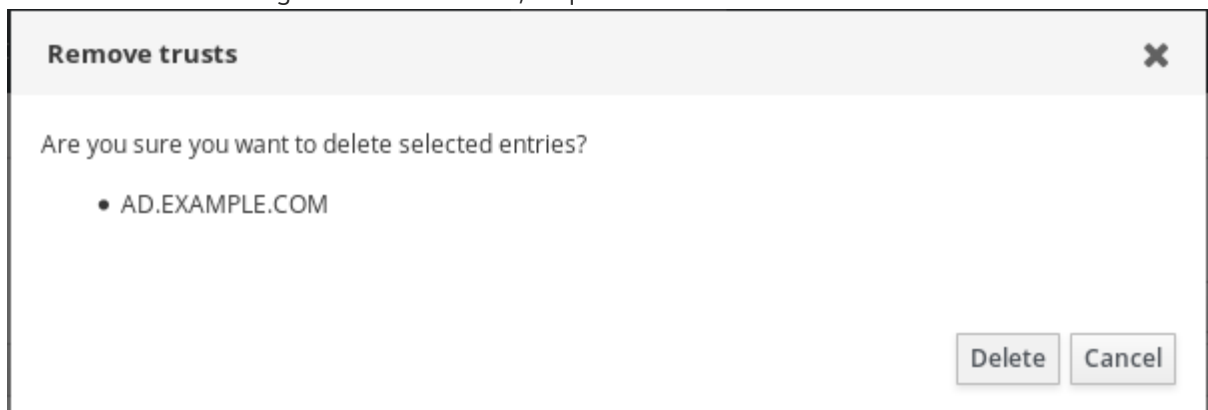
- Vous avez obtenu un ticket Kerberos. Pour plus de détails, voir [Connexion à IdM dans l'interface Web : Utilisation d'un ticket Kerberos](#).

### Procédure

1. Se connecter à l'interface Web IdM avec des privilèges d'administrateur. Pour plus de détails, voir [Accès à l'interface web IdM dans un navigateur web](#).
2. Dans l'interface Web IdM, cliquez sur l'onglet **IPA Server**.
3. Dans l'onglet **IPA Server**, cliquez sur l'onglet **Trusts**.
4. Sélectionnez le trust que vous souhaitez supprimer.



5. Cliquez sur le bouton **Delete**.
6. Dans la boîte de dialogue **Remove trusts**, cliquez sur **Delete**.



7. Supprimez l'objet de confiance de votre configuration Active Directory.



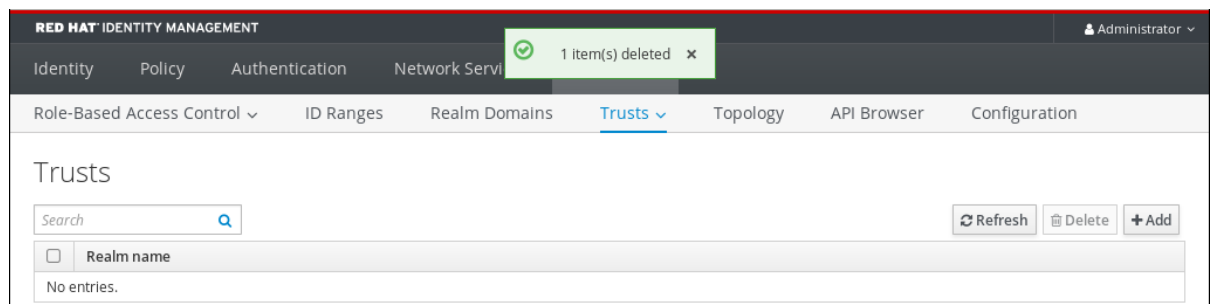
## NOTE

La suppression de la configuration de la confiance ne supprime pas automatiquement la plage d'identifiants que l'IdM a créée pour les utilisateurs AD. Ainsi, si vous ajoutez à nouveau la confiance, la plage d'identifiants existante est réutilisée. En outre, si les utilisateurs AD ont créé des fichiers sur un client IdM, leurs identifiants POSIX sont conservés dans les métadonnées du fichier.

Pour supprimer toutes les informations relatives à une confiance AD, supprimez la plage d'ID utilisateur AD dans l'onglet **ID Ranges** après avoir supprimé la configuration de la confiance et l'objet de confiance.

## Verification steps

- Si la confiance a été supprimée avec succès, l'interface utilisateur Web affiche une fenêtre contextuelle verte avec le texte suivant :



## Ressources supplémentaires

- [Suppression d'une plage d'identifiants après la suppression d'une confiance dans AD](#)

## CHAPITRE 14. SUPPRESSION DE LA CONFIANCE À L'AIDE D'ANSIBLE

Cette section décrit comment supprimer la confiance entre Identity Management (IdM)/Active Directory (AD) du côté IdM à l'aide d'un playbook Ansible.

### Conditions préalables

- Vous avez obtenu un ticket Kerberos en tant qu'administrateur IdM. Pour plus de détails, voir [Connexion à IdM dans l'interface Web : Utilisation d'un ticket Kerberos](#) .
- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire `~/MyPlaybooks/` vous avez créé un [fichier d'inventaire Ansible](#) avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin\_password**.
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquet **ansible-freeipa**.
  - L'exemple suppose que dans le répertoire `~/MyPlaybooks/` vous avez créé un [fichier d'inventaire Ansible](#) avec le nom de domaine complet (FQDN) du serveur IdM sur lequel vous supprimez la confiance.

### Procédure

1. Naviguez jusqu'à votre répertoire `~/MyPlaybooks/` répertoire :

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

2. Créez un playbook **del-trust.yml** avec le contenu suivant :

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

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: ensure the trust is absent
    ipatrust:
      ipaadmin_password: "{{ ipaadmin_password }}"
      realm: ad.example.com
      state: absent
```

Dans l'exemple, **realm** définit la chaîne de nom de la zone AD.

3. Enregistrer le fichier.
4. Exécutez le playbook Ansible. Spécifiez le fichier du livre de jeu, le fichier contenant le mot de passe protégeant le fichier **secret.yml** et le fichier d'inventaire :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory del-trust.yml
```

## NOTE

La suppression de la configuration de la confiance ne supprime pas automatiquement la plage d'identifiants que l'IdM a créée pour les utilisateurs AD. Ainsi, si vous ajoutez à nouveau la confiance, la plage d'identifiants existante est réutilisée. En outre, si les utilisateurs AD ont créé des fichiers sur un client IdM, leurs identifiants POSIX sont conservés dans les métadonnées du fichier.

Pour supprimer toutes les informations relatives à une confiance AD, supprimez la plage d'ID utilisateur AD après avoir supprimé la configuration de la confiance et l'objet de confiance :

```
# ipa idrange-del AD.EXAMPLE.COM_id_range  
# systemctl restart sssd
```

## Verification steps

- Utilisez la commande **ipa trust-show** pour confirmer que la confiance a été supprimée.

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

## Ressources supplémentaires

- [/usr/share/doc/ansible-freeipa/README-trust.md](#)
- [/usr/share/doc/ansible-freeipa/playbooks/trust](#)
- [Suppression d'une plage d'identifiants après la suppression d'une confiance dans AD](#)

## CHAPITRE 15. SUPPRESSION D'UNE PLAGE D'IDENTIFIANTS APRÈS LA SUPPRESSION D'UNE CONFIANCE DANS AD

Si vous avez supprimé la confiance entre vos environnements IdM et Active Directory (AD), il se peut que vous souhaitiez supprimer la plage d'identifiants qui y est associée.



### AVERTISSEMENT

Les identifiants attribués aux plages d'identifiants associées aux domaines de confiance peuvent encore être utilisés pour la propriété des fichiers et des répertoires sur les systèmes inscrits dans IdM.

Si vous supprimez la plage d'identifiants correspondant à un groupe AD que vous avez supprimé, vous ne pourrez pas déterminer la propriété des fichiers et des répertoires appartenant à des utilisateurs AD.

### Conditions préalables

- Vous avez supprimé une confiance dans un environnement AD.

### Procédure

1. Affiche toutes les plages d'identification actuellement utilisées :

```
[root@server ~]# ipa idrange-find
```

2. Identifiez le nom de la plage d'identifiants associée au trust que vous avez supprimé. La première partie du nom de la plage d'identifiants est le nom du trust, par exemple **AD.EXAMPLE.COM\_id\_range**.

3. Retirer la gamme :

```
[root@server ~]# ipa idrange-del AD.EXAMPLE.COM_id_range
```

4. Redémarrez le service SSSD pour supprimer les références à la plage d'identifiants que vous avez supprimée.

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

### Ressources supplémentaires

- Voir [Suppression de la confiance à l'aide de la ligne de commande](#) .
- Voir [Suppression de la confiance à l'aide de l'interface Web IdM](#) .

