Red Hat Enterprise Linux 9

Planification de la gestion de l'identité

Planification de l'infrastructure et de l'intégration des services d'un environnement IdM

Last Updated: 2024-01-18

Red Hat Enterprise Linux 9 Planification de la gestion de l'identité

Planification de l'infrastructure et de l'intégration des services d'un environnement IdM

Notice légale

Résumé

Red Hat Identity Management (IdM) offre un moyen centralisé et unifié de gérer les magasins d'identité, l'authentification et les politiques d'autorisation. Pour une intégration réussie de l'IdM dans votre environnement, renseignez-vous sur les composants de l'IdM et planifiez l'installation. Par exemple, planifiez une topologie de réplication pour le basculement et l'équilibrage de charge, l'intégration dans Active Directory (AD), la structure des zones DNS et de l'autorité de certification (CA), ainsi que les scénarios de sauvegarde et de récupération.

Table des matières

RENDRE L'OPEN SOURCE PLUS INCLUSIF

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

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

- ***block list*** remplace *blacklist*
- ***allow list*** remplace *whitelist*
- ***secondary*** remplace *slave*
- Le mot *master* sera remplacé par des termes 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**.

gestion de l'identité de planification :parent-context-of-overview-of-planning-idm-and-access-control : gestion de l'identité de planification gestion de l'identité de planification

CHAPITRE 1. APERÇU DE LA PLANIFICATION DE L'IDM ET DU CONTRÔLE D'ACCÈS DANS RHEL

Les sections suivantes fournissent une vue d'ensemble des options de gestion des identités (IdM) et de contrôle d'accès dans Red Hat Enterprise Linux. Après avoir lu ces sections, vous serez en mesure d'aborder la phase de planification de votre environnement.

1.1. INTRODUCTION À L'IDM

Ce module explique l'objectif de la gestion d'identité (IdM) dans Red Hat Enterprise Linux. Il fournit également des informations de base sur le domaine IdM, y compris les machines client et serveur qui font partie du domaine.

L'objectif de l'IdM dans Red Hat Enterprise Linux

IdM dans Red Hat Enterprise Linux fournit un moyen centralisé et unifié de gérer les magasins d'identité, l'authentification, les politiques et les politiques d'autorisation dans un domaine basé sur Linux. IdM réduit considérablement la charge administrative liée à la gestion individuelle de différents services et à l'utilisation de différents outils sur différentes machines.

IdM est l'une des rares solutions logicielles centralisées d'identité, de politique et d'autorisation à prendre en charge :

- Fonctionnalités avancées des environnements de systèmes d'exploitation Linux
- Unifier de grands groupes de machines Linux
- Intégration native avec Active Directory

IdM crée un domaine basé sur Linux et contrôlé par Linux :

- L'IdM s'appuie sur des outils et des protocoles Linux natifs existants. Il possède ses propres processus et sa propre configuration, mais ses technologies sous-jacentes sont bien établies sur les systèmes Linux et sont reconnues par les administrateurs Linux.
- Les serveurs et les clients IdM sont des machines Red Hat Enterprise Linux. Les clients IdM peuvent également être d'autres distributions Linux et UNIX si elles prennent en charge les protocoles standard. Un client Windows ne peut pas être membre du domaine IdM, mais les utilisateurs connectés à des systèmes Windows gérés par Active Directory (AD) peuvent se connecter à des clients Linux ou accéder à des services gérés par IdM. Pour ce faire, on établit une confiance inter-forêts entre les domaines AD et IdM.

Gestion des identités et des politiques sur plusieurs serveurs Linux

Without IdM: Chaque serveur est administré séparément. Tous les mots de passe sont enregistrés sur les machines locales. L'administrateur informatique gère les utilisateurs sur chaque machine, définit les politiques d'authentification et d'autorisation séparément et conserve les mots de passe locaux. Cependant, les utilisateurs ont souvent recours à d'autres solutions centralisées, par exemple l'intégration directe avec AD. Les systèmes peuvent être directement intégrés à AD à l'aide de plusieurs solutions différentes :

- Anciens outils Linux (dont l'utilisation n'est pas recommandée)
- Solution basée sur Samba winbind (recommandée pour des cas d'utilisation spécifiques)
- Solution basée sur un logiciel tiers (nécessite généralement une licence d'un autre fournisseur)

- Solution basée sur SSSD (native Linux et recommandée pour la majorité des cas d'utilisation)

With IdM: L'administrateur informatique peut :

- Conserver les identités dans un lieu central : le serveur IdM
- Appliquer des politiques de manière uniforme à plusieurs machines en même temps
- Définir différents niveaux d'accès pour les utilisateurs en utilisant le contrôle d'accès basé sur l'hôte, la délégation et d'autres règles
- Gestion centralisée des règles d'escalade des privilèges
- Définir le mode de montage des répertoires personnels

SSO d'entreprise

Dans le cas d'IdM Enterprise, l'authentification unique (SSO) est mise en œuvre à l'aide du protocole Kerberos. Ce protocole est populaire au niveau de l'infrastructure et permet l'authentification unique avec des services tels que SSH, LDAP, NFS, CUPS ou DNS. Les services web utilisant différentes piles web (Apache, EAP, Django et autres) peuvent également être activés pour utiliser Kerberos pour le SSO. Toutefois, la pratique montre que l'utilisation d'OpenID Connect ou de SAML pour le SSO est plus pratique pour les applications web. Pour faire le lien entre les deux couches, il est recommandé de déployer un fournisseur d'identité (IdP) capable de convertir l'authentification Kerberos en ticket OpenID Connect ou en assertion SAML. La technologie SSO de Red Hat basée sur le projet open source Keycloak est un exemple d'un tel IdP

Without IdM: Les utilisateurs se connectent au système et sont invités à entrer un mot de passe chaque fois qu'ils accèdent à un service ou à une application. Ces mots de passe peuvent être différents et les utilisateurs doivent se rappeler quel identifiant utiliser pour quelle application.

With IdM: Une fois que les utilisateurs se sont connectés au système, ils peuvent accéder à de nombreux services et applications sans qu'on leur demande à plusieurs reprises leurs informations d'identification. Cela permet de :

- Améliorer la convivialité
- Réduire le risque que les mots de passe soient écrits ou stockés de manière non sécurisée
- Augmenter la productivité des utilisateurs

Gestion d'un environnement mixte Linux et Windows

Without IdM: Les systèmes Windows sont gérés dans une forêt AD, mais les équipes de développement, de production et autres disposent de nombreux systèmes Linux. Les systèmes Linux sont exclus de l'environnement AD.

With IdM: L'administrateur informatique peut :

- Gérer les systèmes Linux à l'aide d'outils Linux natifs
- Intégrer les systèmes Linux dans les environnements gérés de manière centralisée par Active Directory, ce qui permet de conserver une base de données centralisée des utilisateurs.
- Déployer facilement de nouveaux systèmes Linux à grande échelle ou selon les besoins.
- Réagir rapidement aux besoins de l'entreprise et prendre des décisions relatives à la gestion de l'infrastructure Linux sans dépendre d'autres équipes, ce qui permet d'éviter les retards.

Comparaison entre l'IdM et un annuaire LDAP standard

Un annuaire LDAP standard, tel que Red Hat Directory Server, est un annuaire polyvalent : il peut être personnalisé pour répondre à un large éventail de cas d'utilisation.

- Schéma : un schéma flexible qui peut être personnalisé pour un large éventail d'entrées, telles que les utilisateurs, les machines, les entités du réseau, l'équipement physique ou les bâtiments.
- Généralement utilisé comme : un répertoire d'arrière-plan pour stocker des données pour d'autres applications, telles que les applications commerciales qui fournissent des services sur Internet.

L'IdM a un objectif spécifique : gérer les identités internes, au sein de l'entreprise, ainsi que les politiques d'authentification et d'autorisation liées à ces identités.

- Schéma : un schéma spécifique qui définit un ensemble particulier d'entrées pertinentes pour son objectif, telles que les entrées pour les identités des utilisateurs ou des machines.
- Généralement utilisé comme : serveur d'identité et d'authentification pour gérer les identités dans les limites d'une entreprise ou d'un projet.

La technologie sous-jacente du serveur d'annuaire est la même pour Red Hat Directory Server et IdM. Cependant, IdM est optimisé pour gérer les identités au sein de l'entreprise. Cela limite son extensibilité générale, mais apporte également certains avantages : une configuration plus simple, une meilleure automatisation de la gestion des ressources et une efficacité accrue dans la gestion des identités de l'entreprise.

Ressources supplémentaires

- Identity Management or Red Hat Directory Server - Which One Should I Use ? sur le blog de Red Hat Enterprise Linux
- Article de la base de connaissances sur les protocoles standard
- Documentation produit pour Red Hat Enterprise Linux 9

1.2. SCÉNARIOS COURANTS POUR LES CLIENTS DE LA GESTION DE L'IDENTITÉ ET LEURS SOLUTIONS

Vous trouverez ci-dessous des exemples de cas d'utilisation courants en matière de gestion des identités et de contrôle d'accès dans les environnements Linux et Windows, ainsi que leurs solutions.

Scénario 1

Situation

Vous êtes administrateur Windows dans votre entreprise.
Outre les systèmes Windows, vous devez également administrer plusieurs systèmes Linux.

Comme vous ne pouvez déléguer le contrôle d'aucune partie de votre environnement à un administrateur Linux, vous devez gérer tous les contrôles de sécurité dans Active Directory (AD).

Solution

Integrate your Linux hosts to AD directly
Si vous souhaitez que les règles **sudo** soient définies de manière centralisée dans un serveur LDAP, vous devez implémenter une extension de schéma dans le contrôleur de domaine AD (DC). Si vous

n'êtes pas autorisé à implémenter cette extension, envisagez d'installer Identity Management (IdM) - voir le scénario 3 ci-dessous. Comme IdM contient déjà l'extension de schéma, vous pouvez gérer les règles **sudo** directement dans IdM.

Autres conseils si vous prévoyez d'avoir besoin de plus de compétences Linux à l'avenir

Entrez en contact avec la communauté Linux pour voir comment les autres gèrent les identités : utilisateurs, hôtes et services.
Rechercher les meilleures pratiques.

Familiarisez-vous avec Linux :

- Utilisez la console web RHEL dans la mesure du possible.
- Utilisez autant que possible des commandes simples sur la ligne de commande.
- Assister à un cours d'administration de système Red Hat.

Scénario 2

Situation

Vous êtes administrateur Linux dans votre entreprise.
Vos utilisateurs Linux ont besoin de différents niveaux d'accès aux ressources de l'entreprise.

Vous avez besoin d'un contrôle d'accès centralisé et rigoureux de vos machines Linux.

Solution

Installez IdM et migrez vos utilisateurs vers ce système.

Autres conseils si vous prévoyez de développer votre entreprise à l'avenir

Après avoir installé IdM, configurez le contrôle d'accès basé sur l'hôte et les règles sudo. Ces règles sont nécessaires pour maintenir les meilleures pratiques de sécurité en matière d'accès limité et de moindre privilège.
Pour atteindre vos objectifs de sécurité, développez une stratégie cohérente de gestion des identités et des accès (IAM) qui utilise des protocoles pour sécuriser à la fois l'infrastructure et les couches applicatives.

Scénario 3

Situation

Vous êtes administrateur Linux dans votre entreprise et vous devez intégrer vos systèmes Linux aux serveurs Windows de l'entreprise. Vous souhaitez rester le seul responsable du contrôle d'accès à vos systèmes Linux.
Différents utilisateurs ont besoin de différents niveaux d'accès aux systèmes Linux, mais ils résident tous dans AD.

Solution

Les contrôles AD n'étant pas assez robustes, vous devez configurer le contrôle d'accès aux systèmes Linux du côté Linux. Installez IdM et établissez une confiance IdM-AD.

Autres conseils pour renforcer la sécurité de votre environnement

Après avoir installé IdM, configurez le contrôle d'accès basé sur l'hôte et les règles sudo. Ces règles sont nécessaires pour maintenir les meilleures pratiques de sécurité en matière d'accès limité et de moindre privilège.
Pour atteindre vos objectifs de sécurité, développez une stratégie cohérente de gestion des identités et des accès (IAM) qui utilise des protocoles pour sécuriser à la fois l'infrastructure et les couches applicatives.

Scénario 4

Situation

En tant qu'administrateur de sécurité, vous devez gérer les identités et les accès dans tous vos environnements, y compris tous vos produits Red Hat. Vous devez gérer toutes vos identités en un seul endroit et maintenir des contrôles d'accès sur l'ensemble de vos plates-formes, nuages et produits.

Solution

Intégrer IdM, Red Hat Single Sign-On, Red Hat Satellite, Red Hat Ansible Tower et d'autres produits Red Hat.

Scénario 5

Situation

En tant qu'administrateur de sécurité et de système dans un environnement du ministère de la défense (DoD) ou de la communauté du renseignement (IC), vous êtes tenu d'utiliser l'authentification par carte à puce ou RSA. Vous devez utiliser des certificats PIV ou des jetons RSA.

Solution

1. Configurer le mappage des certificats dans IdM.
2. Assurez-vous que la délégation GSSAPI est activée si une confiance IdM-AD est présente.
3. Configurer l'utilisation de la configuration radius dans IdM pour les jetons RSA.
4. Configurer les serveurs et les clients Id M pour l'authentification par carte à puce.

Ressources supplémentaires

- Utilisez Ansible pour automatiser vos tâches IdM afin de réduire le temps et la complexité de la configuration du client et de limiter les erreurs.
- Étudier l'approche de la confiance zéro dans la conception des architectures de sécurité.

1.3. INTRODUCTION AUX SERVEURS ET CLIENTS IDM

Le domaine de la gestion des identités (IdM) comprend les types de systèmes suivants :

Clients IdM

Les clients IdM sont des systèmes Red Hat Enterprise Linux enrôlés avec les serveurs et configurés pour utiliser les services IdM sur ces serveurs.
Les clients interagissent avec les serveurs IdM pour accéder aux services qu'ils fournissent. Par exemple, les clients utilisent le protocole Kerberos pour s'authentifier et obtenir des tickets pour l'authentification unique de l'entreprise (SSO), utilisent LDAP pour obtenir des informations sur

l'identité et la politique, utilisent DNS pour détecter où se trouvent les serveurs et les services et comment s'y connecter.

Serveurs IdM

Les serveurs IdM sont des systèmes Red Hat Enterprise Linux qui répondent aux demandes d'identité, d'authentification et d'autorisation au sein d'un domaine IdM. Dans la plupart des déploiements, une autorité de certification (AC) intégrée est également installée avec le serveur IdM.
Les serveurs IdM sont les dépositaires centraux des informations relatives à l'identité et à la politique. Les serveurs IdM peuvent également héberger les services optionnels utilisés par les membres du domaine :

- Autorité de certification (AC)
- Autorité de recouvrement des clés (ARK)
- DNS
- Contrôleur de confiance Active Directory (AD)
- Agent de confiance Active Directory (AD)

Les serveurs IdM sont également des clients IdM intégrés. En tant que clients inscrits avec eux-mêmes, les serveurs fournissent les mêmes fonctionnalités que les autres clients.

Pour fournir des services à un grand nombre de clients, ainsi que pour assurer la redondance et la disponibilité, IdM permet le déploiement sur plusieurs serveurs IdM dans un seul domaine. Il est possible de déployer jusqu'à 60 serveurs. C'est le nombre maximum de serveurs IdM, également appelés répliques, qui est actuellement pris en charge dans le domaine IdM. Les serveurs IdM fournissent différents services au client. Tous les serveurs ne doivent pas nécessairement fournir tous les services possibles. Certains composants du serveur, comme Kerberos et LDAP, sont toujours disponibles sur chaque serveur. D'autres services comme CA, DNS, Trust Controller ou Vault sont optionnels. Cela signifie que les différents serveurs jouent généralement des rôles différents dans le déploiement.

Si votre topologie IdM contient une AC intégrée, un serveur joue le rôle de serveur d'édition de la liste de révocation des certificats (CRL) et un serveur joue le rôle de serveur de renouvellement de l'AC .

Par défaut, le premier serveur CA installé remplit ces deux rôles, mais vous pouvez attribuer ces rôles à des serveurs distincts.

AVERTISSEMENT

Le site *CA renewal server* est essentiel pour votre déploiement IdM, car il s'agit du seul système du domaine responsable du suivi des certificats et des clés du sous-système CA. Pour plus d'informations sur la reprise après un sinistre affectant votre déploiement IdM, reportez-vous à la section Reprise après sinistre avec Identity Management.

Pour assurer la redondance et l'équilibrage de la charge, les administrateurs créent des serveurs supplémentaires en créant une réplique (*replica*) d'un serveur existant. Lors de la création d'une

réplique, IdM clone la configuration du serveur existant. Une réplique partage avec le serveur initial sa configuration de base, y compris les informations internes sur les utilisateurs, les systèmes, les certificats et les politiques configurées.

NOTE

Une réplique et le serveur à partir duquel elle a été créée sont fonctionnellement identiques, à l'exception des rôles *CA renewal* et *CRL publisher*. Par conséquent, les termes ***server*** et ***replica*** sont utilisés ici de manière interchangeable en fonction du contexte.

1.4. IDM ET CONTRÔLE D'ACCÈS DANS RHEL : CENTRAL OU LOCAL

Dans Red Hat Enterprise Linux, vous pouvez gérer les identités et les politiques de contrôle d'accès à l'aide d'outils centralisés pour un domaine entier de systèmes, ou à l'aide d'outils locaux pour un seul système.

Gestion des identités et des politiques sur plusieurs serveurs Red Hat Enterprise Linux : Avec et sans IdM

Grâce à la gestion des identités (IdM), l'administrateur informatique peut :

- Conserver les identités et les mécanismes de regroupement en un lieu central : le serveur IdM
- Gestion centralisée de différents types d'informations d'identification telles que les mots de passe, les certificats PKI, les jetons OTP ou les clés SSH
- Appliquer des politiques de manière uniforme à plusieurs machines en même temps
- Gérer les attributs POSIX et autres pour les utilisateurs externes d'Active Directory
- Définir différents niveaux d'accès pour les utilisateurs en utilisant le contrôle d'accès basé sur l'hôte, la délégation et d'autres règles
- Gestion centralisée des règles d'escalade des privilèges (sudo) et du contrôle d'accès obligatoire (SELinux user mapping)
- Maintenir l'infrastructure centrale de l'ICP et la réserve de secrets
- Définir le mode de montage des répertoires personnels

Sans IdM :

- Chaque serveur est administré séparément.
- Tous les mots de passe sont enregistrés sur les machines locales.
- L'administrateur informatique gère les utilisateurs sur chaque machine, définit des politiques d'authentification et d'autorisation distinctes et conserve les mots de passe locaux.

1.5. TERMINOLOGIE DE L'IDM

Forêt Active Directory

Une forêt Active Directory (AD) est un ensemble d'une ou plusieurs arborescences de domaines qui partagent un catalogue global, un schéma d'annuaire, une structure logique et une configuration

d'annuaire communs. La forêt représente la limite de sécurité à l'intérieur de laquelle les utilisateurs, les ordinateurs, les groupes et d'autres objets sont accessibles. Pour plus d'informations, voir le document Microsoft sur les forêts.

Catalogue global Active Directory

Le catalogue global est une fonctionnalité d'Active Directory (AD) qui permet à un contrôleur de domaine de fournir des informations sur n'importe quel objet de la forêt, que l'objet soit ou non membre du domaine du contrôleur de domaine. Les contrôleurs de domaine dont la fonction de catalogue global est activée sont appelés serveurs de catalogue global. Le catalogue global fournit un catalogue consultable de tous les objets de chaque domaine d'un Active Directory Domain Services (AD DS) multi-domaines.

Identifiant de sécurité Active Directory

Un identifiant de sécurité (SID) est un numéro d'identification unique attribué à un objet dans Active Directory, tel qu'un utilisateur, un groupe ou un hôte. C'est l'équivalent fonctionnel des UID et des GID sous Linux.

Jeu Ansible

Les jeux Ansible sont les éléments constitutifs des playbooks Ansible. L'objectif d'un play est de faire correspondre un groupe d'hôtes à des rôles bien définis, représentés par des tâches Ansible.

Playbook Ansible

Un cahier de jeu Ansible est un fichier qui contient une ou plusieurs séquences Ansible. Pour plus d'informations, voir la documentation officielle d'Ansible sur les playbooks .

Tâche Ansible

Les tâches Ansible sont des unités d'action dans Ansible. Une pièce Ansible peut contenir plusieurs tâches. L'objectif de chaque tâche est d'exécuter un module, avec des arguments très spécifiques. Une tâche Ansible est un ensemble d'instructions permettant d'atteindre un état défini, dans ses grandes lignes, par un rôle ou un module Ansible spécifique, et affiné par les variables de ce rôle ou de ce module. Pour plus d'informations, consultez la documentation officielle sur les tâches Ansible .

Serveur web Apache

Le serveur HTTP Apache, appelé familièrement Apache, est une application de serveur web multiplateforme libre et gratuite, publiée selon les termes de la licence Apache 2.0. Apache a joué un rôle clé dans la croissance initiale du World Wide Web et est actuellement le principal serveur HTTP. Le nom de son processus est **httpd**, qui est l'abréviation de *HTTP daemon*. Red Hat Identity Management (IdM) utilise le serveur Web Apache pour afficher l'interface Web IdM et pour coordonner la communication entre les composants, tels que le serveur de répertoire et l'autorité de certification.

Certificat

Un certificat est un document électronique utilisé pour identifier une personne, un serveur, une entreprise ou une autre entité et pour associer cette identité à une clé publique. Comme un permis de conduire ou un passeport, un certificat fournit une preuve généralement reconnue de l'identité d'une personne. La cryptographie à clé publique utilise des certificats pour résoudre le problème de l'usurpation d'identité.

Autorités de certification (AC) dans l'IdM

Une entité qui émet des certificats numériques. Dans Red Hat Identity Management, l'autorité de certification primaire est **ipa**, l'autorité de certification IdM. Le certificat de l'autorité de certification **ipa** est l'un des types suivants :

- Autosigné. Dans ce cas, l'autorité de certification **ipa** est l'autorité de certification racine.
- Signature externe. Dans ce cas, l'autorité de certification **ipa** est subordonnée à l'autorité de certification externe.

Dans IdM, vous pouvez également créer plusieurs **sub-CAs**. Les sous-CA sont des AC IdM dont les certificats sont de l'un des types suivants :

- Signé par l'AC **ipa**.
- Signé par n'importe quelle AC intermédiaire entre elle-même et l'AC **ipa**. Le certificat d'une sous-AC ne peut pas être auto-signé.

Voir aussi Planification des services de l'AC.

Confiance dans les forêts

Une confiance établit une relation d'accès entre deux domaines Kerberos, permettant aux utilisateurs et aux services d'un domaine d'accéder aux ressources d'un autre domaine.
Avec une confiance inter-forêts entre le domaine racine d'une forêt Active Directory (AD) et un domaine IdM, les utilisateurs des domaines de la forêt AD peuvent interagir avec les machines et les services Linux du domaine IdM. Du point de vue d'AD, la gestion des identités représente une forêt AD distincte avec un seul domaine AD. Pour plus d'informations, voir Comment fonctionne la confiance.

Serveur d'annuaire

Un serveur d'annuaire centralise les informations relatives à l'identité des utilisateurs et aux applications. Il fournit un registre indépendant du système d'exploitation, basé sur le réseau, pour stocker les paramètres des applications, les profils des utilisateurs, les données des groupes, les politiques et les informations de contrôle d'accès. Chaque ressource du réseau est considérée comme un objet par le serveur d'annuaire. Les informations relatives à une ressource particulière sont stockées sous la forme d'une collection d'attributs associés à cette ressource ou à cet objet. Red Hat Directory Server est conforme aux normes LDAP.

Enregistrements DNS PTR

Les enregistrements DNS de pointeurs (PTR) permettent de résoudre l'adresse IP d'un hôte en fonction d'un nom de domaine ou d'un nom d'hôte. Les enregistrements PTR sont l'opposé des enregistrements DNS A et AAAA, qui résolvent les noms d'hôtes en adresses IP. Les enregistrements DNS PTR permettent d'effectuer des recherches DNS inversées. Les enregistrements PTR sont stockés sur le serveur DNS.

Enregistrements DNS SRV

Un enregistrement de service DNS (SRV) définit le nom d'hôte, le numéro de port, le protocole de transport, la priorité et le poids d'un service disponible dans un domaine. Vous pouvez utiliser les enregistrements SRV pour localiser les serveurs IdM et les répliques.

Contrôleur de domaine (DC)

Un contrôleur de domaine (DC) est un hôte qui répond aux demandes d'authentification de sécurité au sein d'un domaine et qui contrôle l'accès aux ressources de ce domaine. Les serveurs IdM fonctionnent comme des DC pour le domaine IdM. Un DC authentifie les utilisateurs, stocke les informations relatives aux comptes utilisateurs et applique la politique de sécurité d'un domaine. Lorsqu'un utilisateur se connecte à un domaine, le DC authentifie et valide ses informations d'identification et autorise ou refuse l'accès.

Nom de domaine complet

Un nom de domaine pleinement qualifié (FQDN) est un nom de domaine qui spécifie l'emplacement exact d'un hôte dans la hiérarchie du système de noms de domaine (DNS). Un appareil portant le nom d'hôte **myhost** dans le domaine parent **example.com** possède le FQDN **myhost.example.com**. Le FQDN distingue de manière unique le dispositif de tout autre hôte appelé **myhost** dans d'autres domaines.

Si vous installez un client IdM sur l'hôte **machine1** en utilisant l'autodécouverte DNS et que vos enregistrements DNS sont correctement configurés, le FQDN de **machine1** est tout ce dont vous avez besoin. Pour plus d'informations, voir Nom d'hôte et exigences DNS pour IdM .

GSSAPI

L'interface de programme d'application du service de sécurité générique (GSSAPI, ou GSS-API) permet aux développeurs d'abstraire la manière dont leurs applications protègent les données envoyées à des applications homologues. Les fournisseurs de services de sécurité peuvent fournir des implémentations GSSAPI d'appels de procédure communs sous forme de bibliothèques avec leur logiciel de sécurité. Ces bibliothèques présentent une interface compatible avec la GSSAPI aux auteurs d'applications qui peuvent écrire leur application pour utiliser uniquement la GSSAPI indépendante du fournisseur. Grâce à cette flexibilité, les développeurs n'ont pas à adapter leurs implémentations de sécurité à une plate-forme, un mécanisme de sécurité, un type de protection ou un protocole de transport particuliers.
Kerberos est l'implémentation dominante du mécanisme GSSAPI, ce qui permet aux implémentations Red Hat Enterprise Linux et Microsoft Windows Active Directory Kerberos d'être compatibles au niveau de l'API.

Réplique cachée

Une réplique cachée est une réplique IdM dont tous les services fonctionnent et sont disponibles, mais dont les rôles de serveur sont désactivés, et que les clients ne peuvent pas découvrir parce qu'elle n'a pas d'enregistrements SRV dans le DNS.
Les répliques cachées sont principalement conçues pour des services tels que les sauvegardes, l'importation et l'exportation en masse, ou les actions qui nécessitent l'arrêt des services IdM. Étant donné qu'aucun client n'utilise un réplica caché, les administrateurs peuvent arrêter temporairement les services sur cet hôte sans affecter aucun client. Pour plus d'informations, voir Le mode réplique cachée.

Serveur HTTP

Voir serveur web.

Cartographie des identifiants

SSSD peut utiliser le SID d'un utilisateur AD pour générer algorithmiquement des ID POSIX dans un processus appelé *ID mapping*. Le mappage d'ID crée une correspondance entre les SID dans AD et les ID sur Linux.

- Lorsque SSSD détecte un nouveau domaine AD, il lui attribue une plage d'identifiants disponibles. Par conséquent, chaque domaine AD dispose de la même plage d'identifiants sur chaque machine cliente SSSD.
- Lorsqu'un utilisateur AD se connecte pour la première fois à une machine cliente SSSD, SSSD crée une entrée pour l'utilisateur dans le cache SSSD, y compris un UID basé sur le SID de l'utilisateur et la plage d'ID pour ce domaine.
- Étant donné que les identifiants d'un utilisateur AD sont générés de manière cohérente à partir du même SID, l'utilisateur possède les mêmes UID et GID lorsqu'il se connecte à n'importe quel système Red Hat Enterprise Linux.

Plages d'identification

Une plage d'ID est une plage de numéros d'ID attribués à la topologie IdM ou à un réplica spécifique. Vous pouvez utiliser les plages d'ID pour spécifier la plage valide d'UID et de GID pour les nouveaux utilisateurs, hôtes et groupes. Les plages d'ID sont utilisées pour éviter les conflits de numéros d'ID. Il existe deux types distincts de plages d'ID dans IdM :

- *IdM ID range*

Utilisez cette plage d'ID pour définir les UID et les GID des utilisateurs et des groupes dans l'ensemble de la topologie IdM. L'installation du premier serveur IdM crée la plage d'ID IdM. Vous ne pouvez pas modifier la plage d'ID IdM après l'avoir créée. Toutefois, vous pouvez créer une plage d'ID IdM supplémentaire, par exemple lorsque la plage d'origine est presque épuisée.

- *Distributed Numeric Assignment (DNA) ID range*
  Cette plage d'ID permet de définir les UID et les GID qu'un réplica utilise lors de la création de nouveaux utilisateurs. L'ajout d'un nouvel utilisateur ou d'une nouvelle entrée d'hôte à un réplica IdM pour la première fois attribue une plage d'ID DNA à ce réplica. Un administrateur peut modifier la plage d'ID DNA, mais la nouvelle définition doit s'inscrire dans une plage d'ID IdM existante.

  Notez que la plage IdM et la plage DNA correspondent, mais qu'elles ne sont pas interconnectées. Si vous modifiez l'une des plages, veillez à modifier l'autre pour qu'elle corresponde.

Pour plus d'informations, voir Plages d'identification.

Vues de l'ID

Les vues ID vous permettent de spécifier de nouvelles valeurs pour les attributs des utilisateurs ou des groupes POSIX, et de définir sur quel(s) hôte(s) client(s) les nouvelles valeurs s'appliqueront. Par exemple, vous pouvez utiliser les vues ID pour :

- Définir des valeurs d'attributs différentes pour des environnements différents.
- Remplacer une valeur d'attribut générée précédemment par une valeur différente.

Dans une configuration de confiance IdM-AD, le site **Default Trust View** est une vue d'identification appliquée aux utilisateurs et aux groupes AD. En utilisant **Default Trust View**, vous pouvez définir des attributs POSIX personnalisés pour les utilisateurs et les groupes AD, remplaçant ainsi les valeurs définies dans AD.

Pour plus d'informations, voir Utilisation d'une vue ID pour remplacer une valeur d'attribut utilisateur sur un client IdM.

Serveur CA IdM

Serveur IdM sur lequel le service d'autorité de certification IdM est installé et fonctionne.
Noms alternatifs : **CA server**

Déploiement de l'IdM

Terme désignant l'ensemble de votre installation IdM. Vous pouvez décrire votre déploiement IdM en répondant aux questions suivantes :

- Votre déploiement IdM est-il un déploiement de test ou un déploiement de production ?
  - Combien de serveurs IdM avez-vous ?
- Votre déploiement IdM contient-il une autorité de certification intégrée ?
  - Dans l'affirmative, l'autorité de certification intégrée est-elle auto-signée ou signée de l'extérieur ?
  - Si c'est le cas, sur quels serveurs le rôle CA est-il disponible ? Sur quels serveurs le rôle KRA est-il disponible ?

- Votre déploiement IdM contient-il un DNS intégré?
  - Si c'est le cas, sur quels serveurs le rôle DNS est-il disponible ?
- Votre déploiement IdM fait-il l'objet d'un accord de confiance avec une forêt AD?
  - Si c'est le cas, sur quels serveurs le rôle de contrôleur de confiance AD ou d'agent de confiance AD est-il disponible ?

Serveur IdM et répliques

Pour installer le premier serveur d'un déploiement IdM, vous devez utiliser la commande **ipa-server-install**.
Les administrateurs peuvent alors utiliser la commande **ipa-replica-install** pour installer **replicas** en plus du premier serveur installé. Par défaut, l'installation d'une réplique crée un accord de réplication avec le serveur IdM à partir duquel elle a été créée, ce qui permet de recevoir et d'envoyer des mises à jour au reste d'IdM.

Il n'y a pas de différence fonctionnelle entre le premier serveur installé et une réplique. Les deux sont des serveurs IdM en lecture/écriture entièrement fonctionnels.

Noms obsolètes : **master server**

Serveur de renouvellement de l'AC IdM

Si votre topologie IdM contient une autorité de certification (CA) intégrée, un serveur joue le rôle unique de serveur de renouvellement de la CA . Ce serveur assure la maintenance et le renouvellement des certificats du système IdM.
Par défaut, le premier serveur CA que vous installez remplit ce rôle, mais vous pouvez configurer n'importe quel serveur CA pour qu'il devienne le serveur de renouvellement CA. Dans un déploiement sans autorité de certification intégrée, il n'y a pas de serveur de renouvellement de l'autorité de certification.

Noms obsolètes : **master CA**

Serveur d'édition de CRL IdM

Si votre topologie IdM contient une autorité de certification (CA) intégrée, un serveur joue le rôle unique de serveur éditeur de liste de révocation de certificats (CRL) . Ce serveur est responsable de la maintenance de la CRL.
Par défaut, le serveur qui joue le rôle de **CA renewal server** joue également ce rôle, mais vous pouvez configurer n'importe quel serveur d'autorité de certification pour qu'il devienne le serveur d'édition de CRL. Dans un déploiement sans autorité de certification intégrée, il n'y a pas de serveur éditeur de CRL.

Topologie de l'IdM

Un terme qui se réfère à la structure de votre solution IdM , en particulier les accords de réplication entre et au sein des centres de données individuels et des clusters.

Indicateurs d'authentification Kerberos

Les indicateurs d'authentification sont attachés aux tickets Kerberos et représentent la méthode d'authentification initiale utilisée pour acquérir un ticket :

- **otp** pour l'authentification à deux facteurs (mot de passe à usage unique)
- **radius** pour l'authentification RADIUS (Remote Authentication Dial-In User Service) (généralement pour l'authentification 802.1x)

- **pkinit** pour la cryptographie à clé publique pour l'authentification initiale dans Kerberos (PKINIT), la carte à puce ou l'authentification par certificat
- **hardened** pour les mots de passe renforcés contre les tentatives de force brute

Pour plus d'informations, voir les indicateurs d'authentification Kerberos.

Protocole d'accord Kerberos

Alors que le mot de passe est la méthode d'authentification par défaut pour un utilisateur, les keytabs sont la méthode d'authentification par défaut pour les hôtes et les services. Un keytab Kerberos est un fichier qui contient une liste des principaux Kerberos et de leurs clés de chiffrement associées, de sorte qu'un service peut récupérer sa propre clé Kerberos et vérifier l'identité d'un utilisateur.
Par exemple, chaque client IdM possède un fichier **/etc/krb5.keytab** qui contient des informations sur le principal **host**, qui représente la machine du client dans le domaine Kerberos.

Principal Kerberos

Des principes Kerberos uniques identifient chaque utilisateur, chaque service et chaque hôte dans un domaine Kerberos :

Entité	Convention d'appellation	Exemple :
Utilisateurs	**identifier@REALM**	**admin@EXAMPLE.COM**
Services	**service/fully-qualified-hostname@REALM**	**http/server.example.com@EXAMPLE.COM**
Hosts	**host/fully-qualified-hostname@REALM**	**host/client.example.com@EXAMPLE.COM**

Protocole Kerberos

Kerberos est un protocole d'authentification réseau qui fournit une authentification forte pour les applications client et serveur en utilisant la cryptographie à clé secrète. IdM et Active Directory utilisent Kerberos pour authentifier les utilisateurs, les hôtes et les services.

Domaine Kerberos

Un domaine Kerberos englobe tous les mandants gérés par un centre de distribution de clés Kerberos (KDC). Dans un déploiement IdM, le domaine Kerberos comprend tous les utilisateurs, hôtes et services IdM.

Politiques de ticket Kerberos

Le Centre de distribution de clés Kerberos (KDC) applique le contrôle d'accès aux tickets par le biais de stratégies de connexion et gère la durée des tickets Kerberos par le biais de stratégies de cycle de vie des tickets. Par exemple, la durée de vie globale par défaut des tickets est d'un jour, et l'âge maximum de renouvellement global par défaut est d'une semaine.
Pour plus d'informations, voir Types de politiques de ticket IdM Kerberos .

Centre de distribution des clés (KDC)

Le centre de distribution de clés Kerberos (KDC) est un service qui joue le rôle d'autorité centrale de confiance gérant les informations relatives aux justificatifs Kerberos. Le KDC émet des tickets Kerberos et garantit l'authenticité des données provenant des entités du réseau IdM.
Pour plus d'informations, voir Le rôle du KDC IdM.

LDAP

Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole d'application ouvert, indépendant des fournisseurs, qui permet d'accéder à des services d'information d'annuaire distribués sur un réseau et de les gérer. Une partie de cette spécification est un arbre d'informations d'annuaire (DIT), qui représente les données dans une structure hiérarchique arborescente composée des noms distinctifs (DN) des entrées du service d'annuaire. LDAP est une version "allégée" du protocole d'accès à l'annuaire (DAP) décrit par la norme ISO X.500 pour les services d'annuaire en réseau.

Sous-CA léger

Dans l'IdM, une sous-CA légère est une autorité de certification (AC) dont le certificat est signé par une AC racine de l'IdM ou par l'une des AC qui lui sont subordonnées. Une AC secondaire légère émet des certificats uniquement dans un but spécifique, par exemple pour sécuriser une connexion VPN ou HTTP.
Pour plus d'informations, voir Restreindre une application à un sous-ensemble de certificats .

Politique en matière de mot de passe

Une politique de mot de passe est un ensemble de conditions auxquelles les mots de passe d'un groupe d'utilisateurs IdM particulier doivent satisfaire. Les conditions peuvent inclure les paramètres suivants :

- La longueur du mot de passe
- Le nombre de classes de caractères utilisées
- Durée de vie maximale d'un mot de passe.

Pour plus d'informations, voir Qu'est-ce qu'une politique de mot de passe ?

Attributs POSIX

Les attributs POSIX sont des attributs utilisateur permettant de maintenir la compatibilité entre les systèmes d'exploitation.
Dans un environnement Red Hat Identity Management, les attributs POSIX pour les utilisateurs incluent :

- **cn**le nom de l'utilisateur
- **uid**le nom du compte (login)
- **uidNumber**un numéro d'utilisateur (UID)
- **gidNumber**le numéro de groupe primaire (GID)
- **homeDirectory**le répertoire personnel de l'utilisateur

Dans un environnement Red Hat Identity Management, les attributs POSIX pour les groupes incluent :

- **cn**, le nom du groupe
- **gidNumber**le numéro de groupe (GID)

Ces attributs identifient les utilisateurs et les groupes comme des entités distinctes.

Accord de réplication

Un accord de réplication est un accord entre deux serveurs IdM dans le même déploiement IdM. L'accord de réplication garantit que les données et la configuration sont répliquées en permanence entre les deux serveurs.
IdM utilise deux types d'accords de réplication : les accords *domain replication*, qui répliquent les informations relatives à l'identité, et les accords *certificate replication*, qui répliquent les informations relatives au certificat.

Pour plus d'informations, voir :

- Accords de réplication
- Déterminer le nombre approprié de répliques
- Connexion des répliques dans une topologie
- Exemples de topologie de réplique

Carte à puce

Une carte à puce est un dispositif amovible ou une carte utilisée pour contrôler l'accès à une ressource. Il peut s'agir de cartes de crédit en plastique dotées d'un circuit intégré (CI), de petits dispositifs USB tels que Yubikey ou d'autres dispositifs similaires. Les cartes à puce peuvent fournir une authentification en permettant aux utilisateurs de connecter une carte à puce à un ordinateur hôte, et le logiciel sur cet ordinateur hôte interagit avec le matériel clé stocké sur la carte à puce pour authentifier l'utilisateur.

SSSD

Le System Security Services Daemon (SSSD) est un service système qui gère l'authentification et l'autorisation des utilisateurs sur un hôte RHEL. En option, SSSD conserve un cache des identités et des informations d'identification des utilisateurs récupérées auprès de fournisseurs distants pour l'authentification hors ligne. Pour plus d'informations, voir Comprendre SSSD et ses avantages .

Backend SSSD

Un backend SSSD, souvent également appelé fournisseur de données, est un processus enfant SSSD qui gère et crée le cache SSSD. Ce processus communique avec un serveur LDAP, effectue différentes recherches et stocke les résultats dans le cache. Il effectue également l'authentification en ligne par LDAP ou Kerberos et applique une politique d'accès et de mot de passe à l'utilisateur qui se connecte.

Ticket-granting ticket (TGT)

Après s'être authentifié auprès d'un centre de distribution de clés Kerberos (KDC), un utilisateur reçoit un ticket d'accès (TGT), qui est un ensemble temporaire d'informations d'identification pouvant être utilisées pour demander des tickets d'accès à d'autres services, tels que les sites web et le courrier électronique.
L'utilisation d'un TGT pour demander un accès supplémentaire permet à l'utilisateur de bénéficier d'une ouverture de session unique, puisqu'il ne doit s'authentifier qu'une seule fois pour accéder à plusieurs services. Les TGT sont renouvelables et les politiques de tickets Kerberos déterminent les limites de renouvellement des tickets et le contrôle d'accès.

Pour plus d'informations, voir Gestion des politiques de tickets Kerberos .

Serveur web

Un serveur web est un logiciel informatique et un matériel sous-jacent qui accepte les demandes de contenu web, telles que des pages, des images ou des applications. Un agent utilisateur, tel qu'un navigateur web, demande une ressource spécifique en utilisant HTTP, le protocole réseau utilisé pour distribuer le contenu web, ou sa variante sécurisée HTTPS. Le serveur web répond avec le contenu

de cette ressource ou un message d'erreur. Le serveur web peut également accepter et stocker des ressources envoyées par l'agent utilisateur. Red Hat Identity Management (IdM) utilise le serveur Web Apache pour afficher l'interface Web IdM et pour coordonner la communication entre les composants, tels que le serveur de répertoire et l'autorité de certification (CA). Voir Serveur web Apache.

Glossaires supplémentaires

Si vous ne parvenez pas à trouver un terme relatif à la gestion de l'identité dans ce glossaire, consultez les glossaires du serveur d'annuaire et du système de certificats :

- Serveur d'annuaire 11 Glossaire
- Glossaire du système de certification 9

1.6. RESSOURCES SUPPLÉMENTAIRES

- Pour obtenir des informations générales sur Red Hat IdM, consultez la page du produit Red Hat Identity Management sur le portail client de Red Hat.

CHAPITRE 2. BASCULEMENT, ÉQUILIBRAGE DE LA CHARGE ET HAUTE DISPONIBILITÉ DANS L'IDM

La gestion des identités (IdM) intègre des mécanismes de basculement pour les clients IdM, ainsi que des fonctions d'équilibrage de la charge et de haute disponibilité pour les serveurs IdM.

2.1. CAPACITÉ DE BASCULEMENT CÔTÉ CLIENT

- Par défaut, le service **SSSD** d'un client IdM est configuré pour utiliser les enregistrements de ressources de service (SRV) du DNS afin de déterminer automatiquement le meilleur serveur IdM auquel se connecter. Ce comportement est contrôlé par l'option **_srv_** dans le paramètre **ipa_server** du fichier **/etc/sssd/sssd.conf**:

  ```
  [root@client ~]# cat /etc/sssd/sssd.conf

  [domain/example.com]
  id_provider = ipa
  ipa_server = _srv_, server.example.com
  ...
  ```

  Si un serveur IdM est hors ligne, le service SSSD du client IdM se connecte à un autre serveur IdM qu'il a automatiquement découvert.

- Si vous préférez éviter les recherches DNS pour des raisons de performance, supprimez l'entrée **_srv_** du paramètre **ipa_server** et indiquez les serveurs IdM auxquels le client doit se connecter, par ordre de préférence :

  ```
  [root@client ~]# cat /etc/sssd/sssd.conf

  [domain/example.com]
  id_provider = ipa
  ipa_server = server1.example.com, server2.example.com
  ...
  ```

2.2. ÉQUILIBRAGE DE LA CHARGE CÔTÉ SERVEUR ET DISPONIBILITÉ DES SERVICES

L'installation de plusieurs répliques IdM permet d'équilibrer la charge et d'assurer la haute disponibilité de l'IdM :

- Si vous disposez d'un réseau géographiquement dispersé, vous pouvez raccourcir le chemin entre les clients IdM et le serveur accessible le plus proche en configurant plusieurs répliques IdM par centre de données.

- Red Hat prend en charge les environnements comportant jusqu'à 60 répliques.

- Le mécanisme de réplication de l'IdM assure une disponibilité active/active des services : les services de toutes les répliques de l'IdM sont disponibles en même temps.

NOTE

Red Hat recommande de ne pas combiner IdM et d'autres logiciels d'équilibrage de charge ou de haute disponibilité (HA).

De nombreuses solutions tierces de haute disponibilité supposent des scénarios actifs/passifs et provoquent des interruptions de service inutiles pour la disponibilité de l'IdM. D'autres solutions utilisent des IP virtuelles ou un seul nom d'hôte par service groupé. Toutes ces méthodes ne fonctionnent généralement pas bien avec le type de disponibilité de service fourni par la solution IdM. Elles s'intègrent également très mal à Kerberos, ce qui réduit la sécurité et la stabilité globales du déploiement.

CHAPITRE 3. PLANIFICATION DE LA TOPOLOGIE DU RÉPLICA

Les sections suivantes fournissent des conseils pour déterminer la topologie de réplique appropriée à votre cas d'utilisation.

3.1. DES SERVEURS RÉPLIQUES MULTIPLES COMME SOLUTION DE HAUTE PERFORMANCE ET DE REPRISE APRÈS SINISTRE

La fonctionnalité continue et la haute disponibilité des services de gestion des identités (IdM) sont vitales pour les utilisateurs qui accèdent aux ressources. L'une des solutions intégrées pour assurer une fonctionnalité continue et une haute disponibilité de l'infrastructure de gestion des identités grâce à l'équilibrage de la charge est la réplication de l'annuaire central en créant des serveurs répliques du premier serveur.

IdM permet de placer des serveurs supplémentaires dans des centres de données géographiquement dispersés afin de refléter la structure organisationnelle de votre entreprise. De cette manière, le chemin entre les clients IdM et le serveur accessible le plus proche est raccourci. En outre, le fait de disposer de plusieurs serveurs permet de répartir la charge et de s'adapter à un plus grand nombre de clients.

La maintenance de plusieurs serveurs IdM redondants et leur réplication mutuelle est également un mécanisme de sauvegarde courant qui permet d'atténuer ou de prévenir la perte d'un serveur. Par exemple, si un serveur tombe en panne, les autres serveurs continuent à fournir des services au domaine. Vous pouvez également récupérer le serveur perdu en créant une nouvelle réplique basée sur l'un des serveurs restants.

3.2. INTRODUCTION AUX SERVEURS ET CLIENTS IDM

Le domaine de la gestion des identités (IdM) comprend les types de systèmes suivants :

Clients IdM

Les clients IdM sont des systèmes Red Hat Enterprise Linux enrôlés avec les serveurs et configurés pour utiliser les services IdM sur ces serveurs.
Les clients interagissent avec les serveurs IdM pour accéder aux services qu'ils fournissent. Par exemple, les clients utilisent le protocole Kerberos pour s'authentifier et obtenir des tickets pour l'authentification unique de l'entreprise (SSO), utilisent LDAP pour obtenir des informations sur l'identité et la politique, utilisent DNS pour détecter où se trouvent les serveurs et les services et comment s'y connecter.

Serveurs IdM

Les serveurs IdM sont des systèmes Red Hat Enterprise Linux qui répondent aux demandes d'identité, d'authentification et d'autorisation au sein d'un domaine IdM. Dans la plupart des déploiements, une autorité de certification (AC) intégrée est également installée avec le serveur IdM.
Les serveurs IdM sont les dépositaires centraux des informations relatives à l'identité et à la politique.
Les serveurs IdM peuvent également héberger les services optionnels utilisés par les membres du domaine :

- Autorité de certification (AC)
- Autorité de recouvrement des clés (ARK)
- DNS
- Contrôleur de confiance Active Directory (AD)

- Agent de confiance Active Directory (AD)

Les serveurs IdM sont également des clients IdM intégrés. En tant que clients inscrits avec eux-mêmes, les serveurs fournissent les mêmes fonctionnalités que les autres clients.

Pour fournir des services à un grand nombre de clients, ainsi que pour assurer la redondance et la disponibilité, IdM permet le déploiement sur plusieurs serveurs IdM dans un seul domaine. Il est possible de déployer jusqu'à 60 serveurs. C'est le nombre maximum de serveurs IdM, également appelés répliques, qui est actuellement pris en charge dans le domaine IdM. Les serveurs IdM fournissent différents services au client. Tous les serveurs ne doivent pas nécessairement fournir tous les services possibles. Certains composants du serveur, comme Kerberos et LDAP, sont toujours disponibles sur chaque serveur. D'autres services comme CA, DNS, Trust Controller ou Vault sont optionnels. Cela signifie que les différents serveurs jouent généralement des rôles différents dans le déploiement.

Si votre topologie IdM contient une AC intégrée, un serveur joue le rôle de serveur d'édition de la liste de révocation des certificats (CRL) et un serveur joue le rôle de serveur de renouvellement de l'AC .

Par défaut, le premier serveur CA installé remplit ces deux rôles, mais vous pouvez attribuer ces rôles à des serveurs distincts.

AVERTISSEMENT

Le site *CA renewal server* est essentiel pour votre déploiement IdM, car il s'agit du seul système du domaine responsable du suivi des certificats et des clés du sous-système CA. Pour plus d'informations sur la reprise après un sinistre affectant votre déploiement IdM, reportez-vous à la section Reprise après sinistre avec Identity Management.

Pour assurer la redondance et l'équilibrage de la charge, les administrateurs créent des serveurs supplémentaires en créant une réplique (*replica*) d'un serveur existant. Lors de la création d'une réplique, IdM clone la configuration du serveur existant. Une réplique partage avec le serveur initial sa configuration de base, y compris les informations internes sur les utilisateurs, les systèmes, les certificats et les politiques configurées.

NOTE

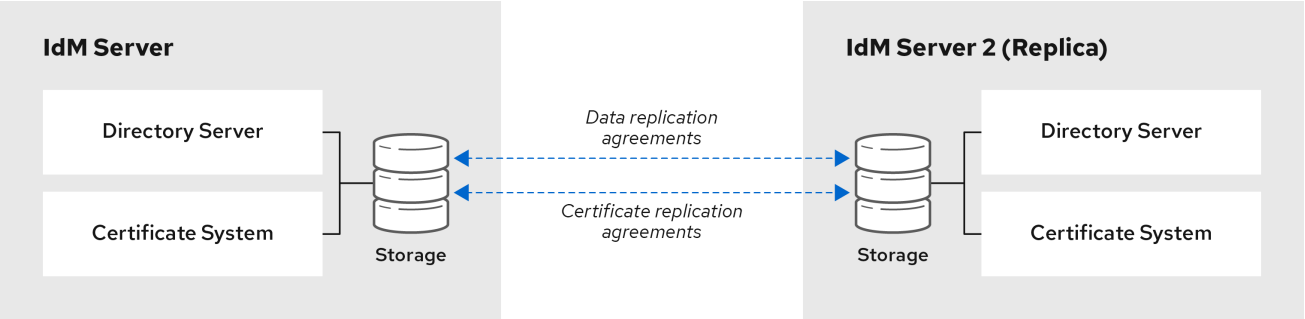
Une réplique et le serveur à partir duquel elle a été créée sont fonctionnellement identiques, à l'exception des rôles *CA renewal* et *CRL publisher*. Par conséquent, les termes ***server*** et ***replica*** sont utilisés ici de manière interchangeable en fonction du contexte.

3.3. ACCORDS DE RÉPLICATION ENTRE LES RÉPLIQUES DE L'IDM

Lorsqu'un administrateur crée une réplique basée sur un serveur existant, Identity Management (IdM) crée un *replication agreement* entre le serveur initial et la réplique. L'accord de réplication garantit que les données et la configuration sont répliquées en permanence entre les deux serveurs.

IdM utilise *multiple read/write replica replication* . Dans cette configuration, toutes les répliques liées par un accord de réplication reçoivent et fournissent des mises à jour et sont donc considérées comme des fournisseurs et des consommateurs. Les accords de réplication sont toujours bilatéraux.

Figure 3.1. Accords sur les serveurs et les répliques



IdM utilise deux types d'accords de réplication :

Accords de réplication de domaine

Ces accords reproduisent les informations relatives à l'identité.

Accords de réplication de certificats

Ces accords reproduisent les informations du certificat.

Les deux canaux de réplication sont indépendants. Deux serveurs peuvent avoir un ou les deux types d'accords de réplication configurés entre eux. Par exemple, lorsque le serveur A et le serveur B n'ont configuré qu'un accord de réplication de domaine, seules les informations relatives à l'identité sont répliquées entre eux, et non les informations relatives au certificat.

3.4. LIGNES DIRECTRICES POUR DÉTERMINER LE NOMBRE APPROPRIÉ DE RÉPLIQUES IDM DANS UNE TOPOLOGIE

Mettre en place au moins deux répliques dans chaque centre de données (ce n'est pas une obligation absolue)

Un centre de données peut être, par exemple, un bureau principal ou un emplacement géographique.

Mettre en place un nombre suffisant de serveurs pour servir vos clients

Un serveur de gestion d'identité (IdM) peut fournir des services à 2000 - 3000 clients. Cela suppose que les clients interrogent les serveurs plusieurs fois par jour, mais pas, par exemple, toutes les minutes. Si vous prévoyez des requêtes plus fréquentes, prévoyez plus de serveurs.

Mettre en place un nombre suffisant de répliques de l'autorité de certification (CA)

Seules les répliques sur lesquelles le rôle d'autorité de certification est installé peuvent répliquer les données des certificats. Si vous utilisez l'autorité de certification IdM, assurez-vous que votre environnement dispose d'au moins deux répliques d'autorité de certification avec des accords de réplication de certificats entre elles.

Configurer un maximum de 60 répliques dans un seul domaine IdM

Red Hat prend en charge les environnements comportant jusqu'à 60 répliques.

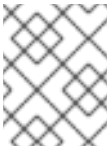
3.5. LIGNES DIRECTRICES POUR LA CONNEXION DES RÉPLIQUES IDM DANS UNE TOPOLOGIE

Connecter chaque réplique à au moins deux autres répliques

La configuration d'accords de réplication supplémentaires garantit que les informations sont répliquées non seulement entre le réplica initial et le premier serveur que vous avez installé, mais aussi entre les autres réplicas.

Connecter une réplique à un maximum de quatre autres répliques (ce n'est pas une exigence absolue)

Un grand nombre d'accords de réplication par serveur n'apporte pas d'avantages significatifs. Une réplique réceptrice ne peut être mise à jour que par une seule autre réplique à la fois et, pendant ce temps, les autres accords de réplication sont inactifs. Plus de quatre accords de réplication par réplique signifient généralement un gaspillage de ressources.



NOTE

Cette recommandation s'applique aux accords de réplication de certificats et de domaines.

Il existe deux exceptions à la limite de quatre accords de réplication par réplique :

- Vous voulez des chemins de basculement si certaines répliques ne sont pas en ligne ou ne répondent pas.
- Dans les déploiements plus importants, vous souhaitez disposer de liens directs supplémentaires entre des nœuds spécifiques.

La configuration d'un nombre élevé d'accords de réplication peut avoir un impact négatif sur les performances globales : lorsque plusieurs accords de réplication dans la topologie envoient des mises à jour, certaines répliques peuvent subir une forte contention sur le fichier de la base de données changelog entre les mises à jour entrantes et les mises à jour sortantes.

Si vous décidez d'utiliser davantage d'accords de réplication par réplique, assurez-vous que vous ne rencontrez pas de problèmes de réplication et de latence. Notez toutefois que les grandes distances et le nombre élevé de nœuds intermédiaires peuvent également entraîner des problèmes de latence.

Connecter les répliques d'un centre de données entre elles

Cela permet d'assurer la réplication du domaine au sein du centre de données.

Connecter chaque centre de données à au moins deux autres centres de données

Cela garantit la réplication du domaine entre les centres de données.

Connecter les centres de données en utilisant au moins une paire d'accords de réplication

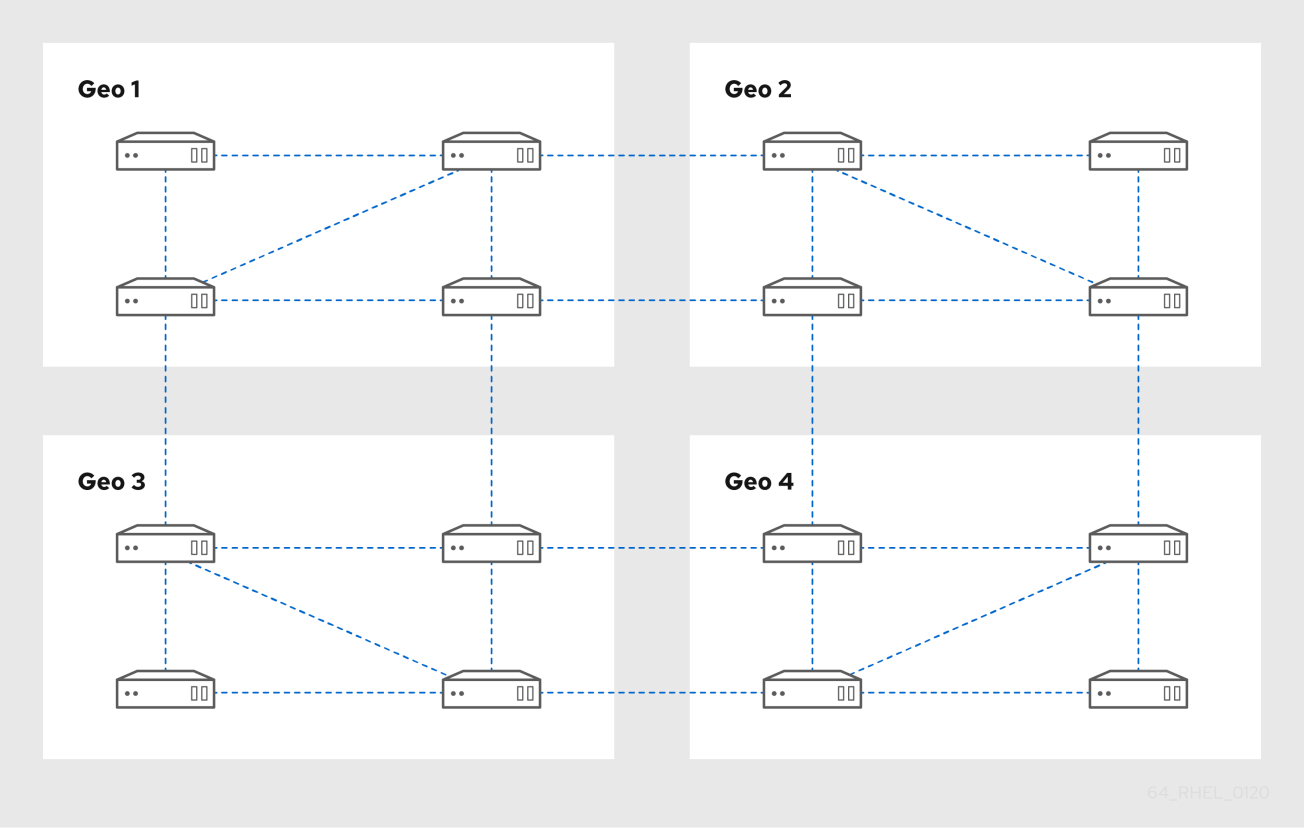
Si les centres de données A et B ont un accord de réplication de A1 à B1, le fait d'avoir un accord de réplication de A2 à B2 garantit que si l'un des serveurs est en panne, la réplication peut se poursuivre entre les deux centres de données.

3.6. EXEMPLES DE TOPOLOGIE DE RÉPLIQUE

Les figures ci-dessous montrent des exemples de topologies de gestion d'identité (IdM) basées sur les lignes directrices pour la création d'une topologie fiable.

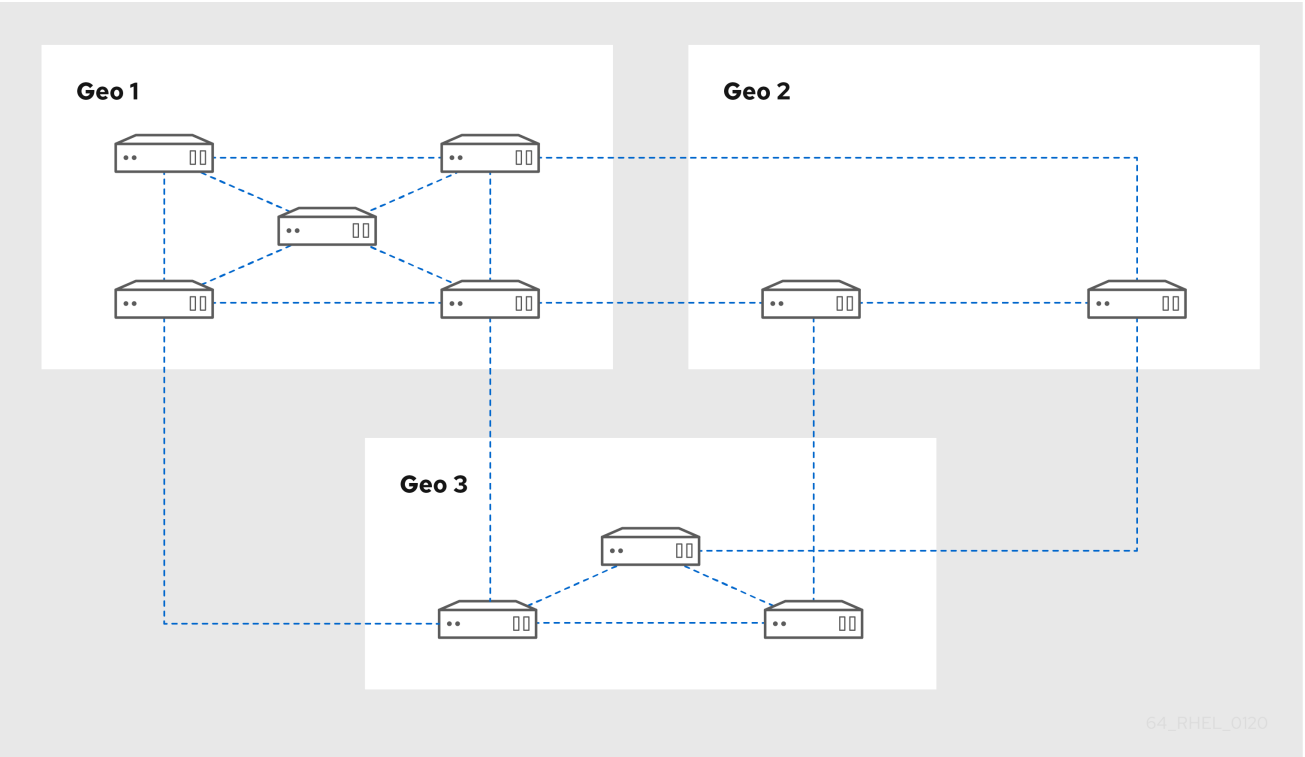
Topologie de réplication L'exemple 1 montre quatre centres de données, chacun avec quatre serveurs. Les serveurs sont reliés par des accords de réplication.

Figure 3.2. Exemple de topologie répliquée 1



Topologie de réplication L'exemple 2 montre trois centres de données, chacun avec un nombre différent de serveurs. Les serveurs sont reliés par des accords de réplication.

Figure 3.3. Exemple de topologie répliquée 2



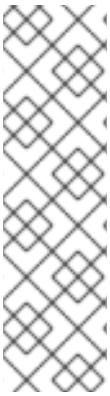
3.7. LE MODE RÉPLIQUE CACHÉ

Par défaut, lorsque vous configurez un réplica, le programme d'installation crée automatiquement des enregistrements de ressources de service (SRV) dans le DNS. Ces enregistrements permettent aux clients de découvrir automatiquement le réplica et ses services. Un réplica caché est un serveur IdM dont tous les services sont en cours d'exécution et disponibles. Cependant, il n'a pas d'enregistrements SRV dans le DNS et les rôles de serveur LDAP ne sont pas activés. Par conséquent, les clients ne peuvent pas utiliser la découverte de services pour détecter ces répliques cachées.

NOTE

La fonction de réplique cachée, introduite dans RHEL 8.1 en tant qu'aperçu technologique, est entièrement prise en charge à partir de RHEL 8.2.

Les répliques cachées sont principalement conçues pour des services dédiés qui pourraient autrement perturber les clients. Par exemple, une sauvegarde complète d'IdM nécessite l'arrêt de tous les services IdM sur le serveur. Comme aucun client n'utilise une réplique cachée, les administrateurs peuvent arrêter temporairement les services sur cet hôte sans affecter aucun client.



NOTE

- La restauration d'une sauvegarde à partir d'un réplica caché sur un nouvel hôte aboutit toujours à un réplica non caché (normal).
- Tous les rôles de serveur utilisés dans un cluster, en particulier le rôle d'autorité de certification si l'autorité de certification intégrée est utilisée, doivent être installés sur le réplica caché pour que la sauvegarde puisse restaurer ces services.
- Pour plus d'informations sur la création et l'utilisation des sauvegardes d'IdM, voir Sauvegarde et restauration d'IdM.

D'autres cas d'utilisation incluent des opérations à forte charge sur l'API IdM ou le serveur LDAP, telles qu'une importation de masse ou des requêtes approfondies. Pour installer un réplica en tant que réplique cachée, passez le paramètre **--hidden-replica** à la commande **ipa-replica-install**.

Pour plus de détails sur l'installation d'un réplica, voir Installation d'un réplica de gestion des identités .

Vous pouvez également modifier l'état d'un réplica existant. Pour plus d'informations, voir Démotion ou promotion des répliques cachées.

CHAPITRE 4. PLANIFICATION DES SERVICES DNS ET DES NOMS D'HÔTES

La gestion des identités (IdM) offre différents types de configurations DNS dans le serveur IdM. Les sections suivantes les décrivent et donnent des conseils sur la manière de déterminer celle qui convient le mieux à votre cas d'utilisation.

4.1. SERVICES DNS DISPONIBLES DANS UN SERVEUR IDM

Vous pouvez installer un serveur de gestion des identités (IdM) avec ou sans DNS intégré.

Tableau 4.1. Comparaison de l'IdM avec DNS intégré et sans DNS intégré

	Avec DNS intégré	Sans DNS intégré
Vue d'ensemble :	IdM gère son propre service DNS pour le domaine IdM.	IdM utilise les services DNS fournis par un serveur DNS externe.
Limites :	Le serveur DNS intégré fourni par IdM ne prend en charge que les fonctions liées au déploiement et à la maintenance d'IdM. Il ne prend pas en charge certaines fonctions DNS avancées. Il n'est pas conçu pour être utilisé comme serveur DNS polyvalent.	Le DNS n'est pas intégré aux outils natifs de l'IdM. Par exemple, IdM ne met pas à jour les enregistrements DNS automatiquement après un changement de topologie.
Fonctionne le mieux pour :	Utilisation de base dans le cadre du déploiement de l'IdM. Lorsque le serveur IdM gère le DNS, celui-ci est étroitement intégré aux outils IdM natifs, ce qui permet d'automatiser certaines tâches de gestion des enregistrements DNS.	Environnements dans lesquels des fonctions DNS avancées dépassant la portée du DNS IdM sont nécessaires. Environnements dotés d'une infrastructure DNS bien établie et pour lesquels vous souhaitez continuer à utiliser un serveur DNS externe.

Même si un serveur Identity Management est utilisé comme serveur DNS primaire, d'autres serveurs DNS externes peuvent encore être utilisés comme serveurs secondaires. Par exemple, si votre environnement utilise déjà un autre serveur DNS, tel qu'un serveur DNS intégré à Active Directory (AD), vous pouvez déléguer uniquement le domaine primaire IdM au DNS intégré à IdM. Il n'est pas nécessaire de migrer les zones DNS vers le DNS IdM.

NOTE

Si vous devez émettre des certificats pour des clients IdM ayant une adresse IP dans l'extension Subject Alternative Name (SAN), vous devez utiliser le service DNS intégré IdM.

4.2. LIGNES DIRECTRICES POUR LA PLANIFICATION DU NOM DE DOMAINE DNS ET DU NOM DE DOMAINE KERBEROS

Lors de l'installation du premier serveur de gestion des identités (IdM), le programme d'installation demande le nom DNS primaire du domaine IdM et le nom du domaine Kerberos. Les lignes directrices de cette section peuvent vous aider à définir les noms correctement.

AVERTISSEMENT

Vous ne pourrez pas modifier le nom du domaine primaire IdM et le nom du domaine Kerberos une fois que le serveur est déjà installé. Ne vous attendez pas à pouvoir passer d'un environnement de test à un environnement de production en changeant les noms, par exemple de ***lab.example.com*** à ***production.example.com***.

Un domaine DNS distinct pour les enregistrements de service

Veillez à ce que le site *primary DNS domain* utilisé pour IdM ne soit partagé avec aucun autre système. Cela permet d'éviter les conflits au niveau du DNS.

Délégation correcte du nom de domaine DNS

Assurez-vous que vous disposez d'une délégation valide dans l'arborescence DNS publique pour le domaine DNS. N'utilisez pas un nom de domaine qui ne vous est pas délégué, même sur un réseau privé.

Domaine DNS multi-label

N'utilisez pas de noms de domaine à étiquette unique, par exemple **.company**. Le domaine IdM doit être composé d'un ou plusieurs sous-domaines et d'un domaine de premier niveau, par exemple **example.com** ou **company.example.com**.

Un nom de domaine Kerberos unique

Assurez-vous que le nom du domaine n'est pas en conflit avec un autre nom de domaine Kerberos existant, tel qu'un nom utilisé par Active Directory (AD).

Nom du domaine Kerberos en tant que version majuscule du nom DNS primaire

Envisagez de définir le nom de domaine comme une version en majuscules (***EXAMPLE.COM***) du nom de domaine DNS primaire (***example.com***).

AVERTISSEMENT

Si vous ne définissez pas le nom de domaine Kerberos comme étant la version en majuscules du nom DNS primaire, vous ne pourrez pas utiliser les trusts AD.

Remarques supplémentaires sur la planification du nom de domaine DNS et du nom de domaine Kerberos

- Un déploiement IdM représente toujours un royaume Kerberos.
- Vous pouvez joindre des clients IdM à partir de plusieurs domaines DNS distincts (***example.com***, ***example.net***, ***example.org***) à un seul royaume Kerberos (***EXAMPLE.COM***).

- Les clients IdM ne doivent pas nécessairement se trouver dans le domaine DNS primaire. Par exemple, si le domaine IdM est ***idm.example.com***les clients peuvent se trouver dans le domaine ***clients.example.com*** mais une correspondance claire doit être configurée entre le domaine DNS et le domaine Kerberos.

NOTE

La méthode standard pour créer la correspondance est d'utiliser les enregistrements DNS **_kerberos** TXT. Le DNS intégré de l'IdM ajoute ces enregistrements automatiquement.

Planification de la transmission DNS

- Si vous souhaitez utiliser un seul transitaire pour l'ensemble de votre déploiement IdM, configurez un **global forwarder**.

- Si votre entreprise est répartie sur plusieurs sites dans des régions géographiquement éloignées, les transitaires mondiaux peuvent s'avérer peu pratiques. Configurez **per-server forwarders**.

- Si votre entreprise dispose d'un réseau DNS interne qui n'est pas résolvable depuis l'internet public, configurez un **forward zone** et un **zone forwarders** pour que les hôtes du domaine IdM puissent résoudre les hôtes de cet autre réseau DNS interne.

CHAPITRE 5. PLANIFICATION DES SERVICES DE L'AC

La gestion des identités (IdM) dans Red Hat Enterprise Linux fournit différents types de configurations d'autorité de certification (CA). Les sections suivantes décrivent différents scénarios et fournissent des conseils pour vous aider à déterminer la configuration la mieux adaptée à votre cas d'utilisation.

CA sujet DN

Le nom distinctif (DN) du sujet de l'autorité de certification (CA) est le nom de l'autorité de certification. Il doit être globalement unique dans l'infrastructure de l'autorité de certification de la gestion des identités (IdM) et ne peut pas être modifié après l'installation. Si vous avez besoin que l'autorité de certification IdM soit signée de manière externe, vous devrez peut-être consulter l'administrateur de l'autorité de certification externe pour connaître la forme que doit prendre le Subject DN de l'autorité de certification IdM.

5.1. SERVICES CA DISPONIBLES DANS UN SERVEUR IDM

Vous pouvez installer un serveur de gestion des identités (IdM) avec une autorité de certification (AC) IdM intégrée ou sans AC.

Tableau 5.1. Comparaison de la gestion de l'identité avec une autorité de certification intégrée et sans autorité de certification

CA intégré	Sans CA

	CA intégré	Sans CA
Vue d'ensemble :	IdM utilise son propre service d'infrastructure à clé publique (PKI) avec *CA signing certificate* pour créer et signer les certificats dans le domaine IdM. ● Si l'autorité de certification racine est l'autorité de certification intégrée, l'IdM utilise un certificat d'autorité de certification auto-signé. ● Si l'autorité de certification racine est une autorité de certification externe, l'autorité de certification intégrée de l'IdM est subordonnée à l'autorité de certification externe. Le certificat d'autorité de certification utilisé par IdM est signé par l'autorité de certification externe, mais tous les certificats du domaine IdM sont émis par l'instance du système de certification intégré. ● L'autorité de certification intégrée est également en mesure d'émettre des certificats pour les utilisateurs, les hôtes ou les services. L'autorité de certification externe peut être une autorité de certification d'entreprise ou une autorité de certification tierce.	IdM ne met pas en place sa propre autorité de certification, mais utilise des certificats d'hôte signés par une autorité de certification externe. L'installation d'un serveur sans autorité de certification nécessite de demander les certificats suivants à une autorité tierce : ● Un certificat de serveur LDAP ● Un certificat de serveur Apache ● Un certificat PKINIT ● Chaîne complète des certificats de l'autorité de certification qui a émis les certificats des serveurs LDAP et Apache

	CA intégré	Sans CA
Limites :	Si l'autorité de certification intégrée est subordonnée à une autorité de certification externe, les certificats émis dans le domaine IdM sont potentiellement soumis à des restrictions fixées par l'autorité de certification externe pour divers attributs de certificat, tels que • La période de validité. • Contraintes relatives aux noms de sujets pouvant figurer sur les certificats délivrés par l'autorité de certification IDM ou ses subordonnés . • Contraintes sur la possibilité pour l'autorité de certification IDM de délivrer elle-même des certificats d'autorités de certification subordonnées, ou sur le degré de "profondeur" de la chaîne de certificats subordonnés.	La gestion des certificats en dehors de l'IdM entraîne un grand nombre d'activités supplémentaires, telles que : • La création, le téléchargement et le renouvellement des certificats sont des opérations manuelles. • Le service **certmonger** ne suit pas les certificats IPA (serveur LDAP, serveur Apache et certificats PKINIT) et ne vous avertit pas lorsque les certificats sont sur le point d'expirer. Les administrateurs doivent configurer manuellement des notifications pour les certificats émis en externe ou définir des demandes de suivi pour ces certificats s'ils veulent que **certmonger** les suive.
Fonctionne le mieux pour :	Les environnements qui vous permettent de créer et d'utiliser votre propre infrastructure de certificats.	Très rares cas où les restrictions de l'infrastructure ne permettent pas d'installer les services de certificats intégrés au serveur.

NOTE

Il est possible de passer de l'autorité de certification auto-signée à une autorité de certification externe, ou l'inverse, et de changer l'autorité de certification externe qui délivre le certificat de l'autorité de certification IdM, même après l'installation. Il est également possible de configurer une autorité de certification intégrée même après une installation sans autorité de certification. Pour plus de détails, voir Installation d'un serveur IdM : Avec DNS intégré, sans AC.

5.2. LIGNES DIRECTRICES POUR LA DISTRIBUTION DES SERVICES DE L'AC

Les étapes suivantes fournissent des lignes directrices pour la distribution des services de l'autorité de certification (AC).

Procédure

1. Installez les services CA sur plusieurs serveurs de la topologie.
   Les répliques configurées sans autorité de certification transmettent toutes les demandes d'opérations de certificat aux serveurs d'autorité de certification de votre topologie.

AVERTISSEMENT

Si vous perdez tous les serveurs dotés d'une autorité de certification, vous perdrez toute la configuration de l'autorité de certification sans aucune chance de récupération. Dans ce cas, vous devez mettre en place une nouvelle autorité de certification et émettre et installer de nouveaux certificats.

2. Maintenez un nombre suffisant de serveurs d'autorité de certification pour traiter les demandes d'autorité de certification dans votre déploiement.

Le tableau suivant contient des recommandations sur le nombre approprié de serveurs d'autorité de certification :

Tableau 5.2. Lignes directrices pour la mise en place d'un nombre approprié de serveurs d'autorité de certification

Description du déploiement	Nombre suggéré de serveurs d'autorité de certification
Un déploiement avec un très grand nombre de certificats émis	Trois ou quatre serveurs d'autorité de certification
Un déploiement avec des problèmes de bande passante ou de disponibilité entre plusieurs régions	Un serveur CA par région, avec un minimum de trois serveurs au total pour le déploiement
Tous les autres déploiements	Deux serveurs d'autorité de certification

CHAPITRE 6. INTÉGRATION DE LA PLANIFICATION AVEC AD

Les sections suivantes présentent les options d'intégration de Red Hat Enterprise Linux avec Active Directory (AD).

6.1. INTÉGRATION DIRECTE DES SYSTÈMES LINUX DANS ACTIVE DIRECTORY

Dans l'intégration directe, les systèmes Linux sont connectés directement à Active Directory (AD). Les types d'intégration suivants sont possibles :

Intégration avec le démon des services de sécurité du système (SSSD)

SSSD peut connecter un système Linux à différents systèmes d'identité et d'authentification : AD, Identity Management (IdM), ou un serveur générique LDAP ou Kerberos.
Exigences notables pour l'intégration avec SSSD :

- Lors de l'intégration avec AD, SSSD ne fonctionne par défaut qu'au sein d'une seule forêt AD. Pour une installation multi-forêts, configurez l'énumération manuelle des domaines.
- Les forêts AD distantes doivent faire confiance à la forêt locale pour que le plug-in **idmap_ad** gère correctement les utilisateurs des forêts distantes.

SSSD prend en charge l'intégration directe et indirecte. Il permet également de passer d'une approche d'intégration à l'autre sans coûts de migration importants.

Intégration avec Samba Winbind

Le composant Winbind de la suite Samba émule un client Windows sur un système Linux et communique avec les serveurs AD.
Exigences notables pour l'intégration avec Samba Winbind :

- L'intégration directe avec Winbind dans une configuration AD multi-forêts nécessite des trusts bidirectionnels.
- Un chemin bidirectionnel doit exister entre le domaine local d'un système Linux et le domaine d'un utilisateur dans une forêt AD distante pour permettre au plug-in **idmap_ad** de disposer d'informations complètes sur l'utilisateur à partir du domaine AD distant.

Recommendations

- SSSD répond à la plupart des cas d'utilisation pour l'intégration d'AD et fournit une solution robuste en tant que passerelle générique entre un système client et différents types de fournisseurs d'identité et d'authentification - AD, IdM, Kerberos et LDAP.
- Il est recommandé de déployer Winbind sur les serveurs membres du domaine AD sur lesquels vous prévoyez de déployer Samba FS.

6.2. INTÉGRATION INDIRECTE DES SYSTÈMES LINUX DANS ACTIVE DIRECTORY PAR LE BIAIS DE LA GESTION DES IDENTITÉS

Dans l'intégration indirecte, les systèmes Linux sont d'abord connectés à un serveur central qui est ensuite connecté à Active Directory (AD). L'intégration indirecte permet à l'administrateur de gérer les systèmes et les politiques Linux de manière centralisée, tandis que les utilisateurs d'AD peuvent accéder de manière transparente aux systèmes et aux services Linux.

Intégration basée sur la confiance entre les forêts avec AD

Le serveur de gestion des identités (IdM) fait office de serveur central pour contrôler les systèmes Linux. Une confiance Kerberos inter-royaumes est établie avec AD, ce qui permet aux utilisateurs d'AD de se connecter pour accéder aux systèmes et aux ressources Linux. IdM se présente à AD comme une forêt distincte et tire parti de la confiance au niveau de la forêt prise en charge par AD. Lors de l'utilisation d'une fiducie :

- Les utilisateurs AD peuvent accéder aux ressources IdM.
- Les serveurs et les clients IdM peuvent résoudre les identités des utilisateurs et des groupes AD.
- Les utilisateurs et les groupes AD accèdent à l'IdM dans les conditions définies par l'IdM, comme le contrôle d'accès basé sur l'hôte.
- Les utilisateurs et les groupes AD continuent d'être gérés du côté AD.

Intégration basée sur la synchronisation

Cette approche est basée sur l'outil WinSync. Un accord de réplication WinSync synchronise les comptes d'utilisateurs d'AD vers IdM.

AVERTISSEMENT

WinSync n'est plus activement développé dans Red Hat Enterprise Linux 8. La solution préférée pour l'intégration indirecte est la confiance inter-forêts.

Les limites de l'intégration basée sur la synchronisation sont les suivantes :

- Les groupes ne sont pas synchronisés entre IdM et AD.
- Les utilisateurs sont dupliqués dans AD et IdM.
- WinSync ne prend en charge qu'un seul domaine AD.
- Un seul contrôleur de domaine dans AD peut être utilisé pour synchroniser les données avec une instance d'IdM.
- Les mots de passe des utilisateurs doivent être synchronisés, ce qui nécessite l'installation du composant PassSync sur tous les contrôleurs de domaine du domaine AD.
- Après avoir configuré la synchronisation, tous les utilisateurs AD doivent modifier manuellement leurs mots de passe avant que PassSync ne puisse les synchroniser.

6.3. LIGNES DIRECTRICES POUR DÉCIDER DE L'INTÉGRATION DIRECTE OU INDIRECTE

Les lignes directrices de cette section peuvent vous aider à décider quel type d'intégration correspond à votre cas d'utilisation.

Nombre de systèmes à connecter à Active Directory

Connecter moins de 30 à 50 systèmes (ce n'est pas une limite absolue)

Si vous connectez moins de 30 à 50 systèmes, envisagez l'intégration directe. L'intégration indirecte risque d'entraîner des frais généraux inutiles.

Connecter plus de 30 à 50 systèmes (pas de limite stricte)

Si vous connectez plus de 30 à 50 systèmes, envisagez une intégration indirecte avec la gestion des identités. Cette approche vous permet de bénéficier d'une gestion centralisée des systèmes Linux.

Gérer un petit nombre de systèmes Linux, mais s'attendre à ce que ce nombre augmente rapidement

Dans ce cas, il convient d'envisager une intégration indirecte pour éviter de devoir migrer l'environnement ultérieurement.

Fréquence de déploiement de nouveaux systèmes et leur type

Déployer des systèmes "bare metal" de manière irrégulière

Si vous déployez rarement de nouveaux systèmes et qu'il s'agit généralement de systèmes "bare metal", envisagez l'intégration directe. Dans ce cas, l'intégration directe est généralement la plus simple et la plus facile.

Déploiement fréquent de systèmes virtuels

Si vous déployez souvent de nouveaux systèmes et qu'il s'agit généralement de systèmes virtuels approvisionnés à la demande, envisagez l'intégration indirecte. Avec l'intégration indirecte, vous pouvez utiliser un serveur central pour gérer les nouveaux systèmes de manière dynamique et les intégrer à des outils d'orchestration, tels que Red Hat Satellite.

Active Directory est le fournisseur d'authentification requis

Vos politiques internes prévoient-elles que tous les utilisateurs doivent s'authentifier auprès d'Active Directory ?

Vous pouvez choisir une intégration directe ou indirecte. Si vous utilisez l'intégration indirecte avec une confiance entre Identity Management et Active Directory, les utilisateurs qui accèdent aux systèmes Linux s'authentifient auprès d'Active Directory. Les politiques qui existent dans Active Directory sont exécutées et appliquées lors de l'authentification.

CHAPITRE 7. PLANIFICATION D'UNE CONFIANCE INTER-FORÊTS ENTRE IDM ET AD

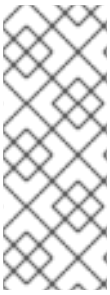
Active Directory (AD) et Identity Management (IdM) sont deux environnements alternatifs qui gèrent une variété de services de base, tels que Kerberos, LDAP, DNS et les services de certificats. Une relation *cross-forest trust* intègre de manière transparente ces deux environnements divers en permettant à tous les services de base d'interagir de manière transparente. Les sections suivantes fournissent des conseils sur la manière de planifier et de concevoir un déploiement de confiance inter-forêts.

7.1. CONFIANCE INTER-FORÊTS ET EXTERNE ENTRE IDM ET AD

Une confiance inter-forêts entre IdM et AD

Dans un environnement Active Directory (AD) pur, une confiance inter-forêts relie deux domaines racines de forêt AD distincts. Lorsque vous créez une confiance inter-forêts entre AD et IdM, le domaine IdM se présente à AD comme une forêt distincte avec un seul domaine. Une relation de confiance est alors établie entre le domaine racine de la forêt AD et le domaine IdM. Par conséquent, les utilisateurs de la forêt AD peuvent accéder aux ressources du domaine IdM.

IdM peut établir une confiance avec une forêt AD ou plusieurs forêts non liées.



NOTE

Deux domaines Kerberos distincts peuvent être connectés sur le site *cross-realm trust*. Toutefois, un domaine Kerberos ne concerne que l'authentification, et non les autres services et protocoles impliqués dans les opérations d'identité et d'autorisation. Par conséquent, l'établissement d'une confiance inter-royaumes Kerberos n'est pas suffisant pour permettre aux utilisateurs d'un royaume d'accéder aux ressources d'un autre royaume.

Une confiance externe vers un domaine AD

Une confiance externe est une relation de confiance entre l'IdM et un domaine Active Directory. Alors qu'une confiance de forêt nécessite toujours l'établissement d'une confiance entre IdM et le domaine racine d'une forêt Active Directory, une confiance externe peut être établie entre IdM et n'importe quel domaine au sein d'une forêt.

7.2. CONTRÔLEURS ET AGENTS DE CONFIANCE

La gestion des identités (IdM) fournit les types suivants de serveurs IdM qui prennent en charge la confiance dans Active Directory (AD) :

Contrôleurs de confiance

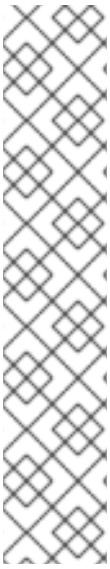
Serveurs IdM qui peuvent effectuer des recherches d'identité auprès des contrôleurs de domaine AD. Ils exécutent également la suite Samba afin d'établir la confiance avec AD. Les contrôleurs de domaine AD contactent les contrôleurs de confiance lorsqu'ils établissent et vérifient la confiance avec AD. Les machines inscrites à AD communiquent avec les contrôleurs de confiance IdM pour les demandes d'authentification Kerberos.
Le premier contrôleur de confiance est créé lorsque vous configurez la confiance. Si vous disposez de plusieurs contrôleurs de domaine répartis sur différents sites géographiques, utilisez la commande **ipa-adtrust-install** pour désigner les serveurs RHEL IdM comme contrôleurs de confiance sur ces sites.

Les contrôleurs de confiance exécutent plus de services en contact avec le réseau que les agents de confiance et présentent donc une plus grande surface d'attaque pour les intrus potentiels.

Agents de confiance

Serveurs IdM capables de résoudre les recherches d'identité effectuées par les clients RHEL IdM auprès des contrôleurs de domaine AD. Contrairement aux contrôleurs de confiance, les agents de confiance ne peuvent pas traiter les demandes d'authentification Kerberos.

Outre les agents de confiance et les contrôleurs, le domaine IdM peut également inclure des serveurs IdM standard. Toutefois, ces serveurs ne communiquent pas avec AD. Par conséquent, les clients qui communiquent avec ces serveurs standard ne peuvent pas résoudre les utilisateurs et les groupes AD, ni authentifier et autoriser les utilisateurs AD.



NOTE

Un serveur IdM n'est pas configuré pour jouer le rôle de contrôleur ou d'agent fiduciaire, sauf si l'une des actions suivantes a été effectuée :

- Vous avez installé le serveur ou le réplica avec les commandes **ipa-server-install** ou **ipa-replica-install** avec l'option **--setup-ad**.
- Vous avez exécuté la commande **ipa-adtrust-install** sur le serveur IdM pour configurer le rôle de contrôleur de confiance.
- Vous avez exécuté la commande **ipa-adtrust-install --add-agents** sur un contrôleur de confiance pour désigner un autre réplica IdM comme agent de confiance.
  Par défaut, les serveurs IdM ne peuvent pas résoudre les utilisateurs et les groupes des domaines de confiance sans ces opérations.

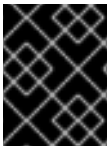
Tableau 7.1. Comparaison des capacités des contrôleurs de confiance et des agents de confiance

Capacité	Agent fiduciaire	Contrôleur de confiance
Résoudre les utilisateurs et les groupes AD	Oui	Oui
Inscrire les clients IdM qui exécutent des services accessibles aux utilisateurs des forêts AD de confiance	Oui	Oui
Ajouter, modifier ou supprimer des contrats de fiducie	Non	Oui
Attribuer le rôle d'agent de confiance à un serveur IdM	Non	Oui

Lors de la planification du déploiement des contrôleurs de confiance et des agents de confiance, il convient de tenir compte des lignes directrices suivantes :

- Configurer au moins deux contrôleurs de confiance par déploiement IdM.
- Configurez au moins deux contrôleurs de confiance dans chaque centre de données.

Si vous souhaitez créer des contrôleurs de confiance supplémentaires ou si un contrôleur de confiance existant échoue, créez un nouveau contrôleur de confiance en promouvant un agent de confiance ou un serveur standard. Pour ce faire, utilisez l'utilitaire **ipa-adtrust-install** sur le serveur IdM.



IMPORTANT

Vous ne pouvez pas transformer un contrôleur de confiance existant en agent de confiance.

7.3. FIDUCIES À SENS UNIQUE ET FIDUCIES À DOUBLE SENS

Dans un sens, la gestion des identités (IdM) fait confiance à Active Directory (AD), mais AD ne fait pas confiance à IdM. Les utilisateurs d'AD peuvent accéder aux ressources du domaine IdM, mais les utilisateurs d'IdM ne peuvent pas accéder aux ressources du domaine AD. Le serveur IdM se connecte à AD à l'aide d'un compte spécial et lit les informations d'identité qui sont ensuite transmises aux clients IdM par LDAP.

Dans le cas d'une confiance à double sens, les utilisateurs de l'IdM peuvent s'authentifier auprès d'AD et les utilisateurs d'AD peuvent s'authentifier auprès de l'IdM. Les utilisateurs d'AD peuvent s'authentifier et accéder aux ressources du domaine IdM, comme dans le cas d'une confiance à sens unique. Les utilisateurs IdM peuvent s'authentifier mais ne peuvent pas accéder à la plupart des ressources du domaine AD. Ils ne peuvent accéder qu'aux services Kerberisés des forêts AD qui ne nécessitent pas de contrôle d'accès.

Pour pouvoir accorder l'accès aux ressources AD, IdM doit mettre en œuvre le service Global Catalog. Ce service n'existe pas encore dans la version actuelle du serveur IdM. Pour cette raison, une confiance bidirectionnelle entre IdM et AD est presque équivalente, d'un point de vue fonctionnel, à une confiance unidirectionnelle entre IdM et AD.

7.4. KERBEROS FAST POUR LES DOMAINES DE CONFIANCE

Kerberos Flexible Authentication Secure Tunneling (FAST) est également appelé blindage Kerberos dans un environnement Active Directory (AD). Kerberos FAST fournit une couche de sécurité supplémentaire pour la communication Kerberos entre les clients et le centre de distribution de clés (KDC). Dans IdM, les KDC sont exécutés sur les serveurs IdM et FAST est activé par défaut. L'authentification à deux facteurs (2FA) dans IdM nécessite également l'activation de FAST.

Dans AD, l'armure Kerberos est désactivée par défaut sur les contrôleurs de domaine AD (DC). Vous pouvez l'activer sur le contrôleur de domaine à l'adresse **Tools>Group Policy Management>Default Domain Controller Policy**:

- Cliquez avec le bouton droit de la souris sur **Default Domain Controller Policy** et sélectionnez **edit**. Naviguez jusqu'à **Computer Configuration>Policies>Administrative Templates>System>KDC** et double-cliquez sur **KDC support for claims, compound authentication, and Kerberos armoring**.

Une fois que vous avez activé la prise en charge du KDC pour les réclamations, le paramètre de stratégie permet les options suivantes :

- \Pas de soutien
- "Supported" (supprimé)
- \Toujours fournir des demandes d'indemnisation
- \Échec des demandes d'authentification non blindées

Kerberos FAST est implémenté dans les bibliothèques Kerberos des clients IdM. Vous pouvez configurer les clients IdM pour qu'ils utilisent FAST pour tous les domaines de confiance qui annoncent FAST ou pour qu'ils n'utilisent pas du tout Kerberos FAST. Si vous activez le blindage Kerberos dans la forêt AD

de confiance, le client IdM utilise Kerberos FAST par défaut. FAST établit un tunnel sécurisé à l'aide d'une clé cryptographique. Pour protéger la connexion aux contrôleurs de domaine d'un domaine de confiance, Kerberos FAST doit obtenir un Ticket Granting Ticket (TGT) du domaine de confiance, car ces clés ne sont valables qu'à l'intérieur du domaine Kerberos. Kerberos FAST utilise les clés Kerberos des hôtes du client IdM pour demander le TGT inter-royaumes avec l'aide des serveurs IdM. Cela ne fonctionne que si la forêt AD fait confiance au domaine IdM, ce qui signifie qu'une confiance réciproque est nécessaire.

Si les politiques AD exigent l'application de l'utilisation de Kerberos FAST, vous devez établir une confiance réciproque entre le domaine IdM et la forêt AD. Vous devez planifier cette opération avant d'établir la connexion, car l'IdM et AD doivent tous deux disposer d'enregistrements sur la direction et le type de confiance.

Si vous avez déjà établi une confiance à sens unique, exécutez la commande **ipa trust-add … --two-way=true** pour supprimer l'accord de confiance existant et créer une confiance à double sens. Cette opération nécessite l'utilisation d'informations d'identification administratives. Comme l'IdM tente de supprimer l'accord de confiance existant du côté AD, il a besoin d'autorisations d'administrateur pour l'accès à AD. Si vous établissez la confiance initiale en utilisant un secret partagé plutôt qu'un compte administratif AD, la confiance est recréée dans les deux sens et les objets de domaine approuvés ne sont modifiés que du côté de l'IdM. Les administrateurs Windows doivent répéter la même procédure en utilisant l'interface utilisateur Windows pour choisir une confiance bidirectionnelle et utiliser le même secret partagé pour recréer la confiance.

Si l'utilisation d'une confiance bidirectionnelle n'est pas possible, vous devez désactiver Kerberos FAST sur tous les clients IdM. Les utilisateurs de la forêt AD de confiance peuvent s'authentifier avec un mot de passe ou une carte à puce directe. Pour désactiver Kerberos FAST, ajoutez le paramètre suivant au fichier **sssd.conf** dans la section **[domain]**:

```
krb5_use_fast = jamais
```

Remarque : il n'est pas nécessaire d'utiliser cette option lorsque l'authentification est basée sur les clés ssh, l'authentification GSSAPI ou SSH avec des cartes à puce à partir de clients Windows distants. Ces méthodes n'utilisent pas Kerberos FAST car le client IdM ne doit pas communiquer avec un DC. En outre, après avoir désactivé FAST sur le client IdM, la fonction d'authentification à deux facteurs IdM est également indisponible.

7.5. POSIX ET MAPPAGE D'ID TYPES DE PLAGES D'ID POUR LES UTILISATEURS AD

La gestion des identités (IdM) applique des règles de contrôle d'accès basées sur l'ID utilisateur POSIX (UID) et l'ID de groupe (GID) d'un utilisateur. Les utilisateurs d'Active Directory (AD), cependant, sont identifiés par des identifiants de sécurité (SID). Les administrateurs AD peuvent configurer AD pour stocker des attributs POSIX pour vos utilisateurs et groupes AD, tels que **uidNumber**, **gidNumber**, **unixHomeDirectory**, ou **loginShell**.

Vous pouvez configurer une confiance inter-forêts pour référencer ces informations en établissant une confiance avec la plage d'ID **ipa-ad-trust-posix**:

```
[server ~]# ipa trust-add --type=ad ad.example.com --admin administrator --password  --range-type=ipa-ad-trust-posix
```

Si vous ne stockez pas d'attributs POSIX dans AD, le System Security Services Daemon (SSSD) peut mapper de manière cohérente un UID unique basé sur le SID d'un utilisateur dans un processus appelé **ID mapping**. Vous pouvez explicitement choisir ce comportement en créant une confiance avec la plage d'ID **ipa-ad-trust**:

```
[server ~]# ipa trust-add --type=ad ad.example.com --admin administrator --password  --range-type=ipa-ad-trust
```

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.

Ressources supplémentaires

- Options de mappage automatique des groupes privés pour les utilisateurs AD

7.6. OPTIONS DE MAPPAGE AUTOMATIQUE DES GROUPES PRIVÉS POUR LES UTILISATEURS AD : FIDUCIES POSIX

Dans un environnement Linux, chaque utilisateur dispose d'un groupe d'utilisateurs principal. Red Hat Enterprise Linux (RHEL) utilise un schéma de groupe privé d'utilisateurs (UPG) : un UPG porte le même nom que l'utilisateur pour lequel il a été créé et cet utilisateur est le seul membre de l'UPG.

Si vous avez attribué des UID à vos utilisateurs AD, mais que les GID n'ont pas été ajoutés, vous pouvez configurer SSSD pour qu'il crée automatiquement des groupes privés pour les utilisateurs en fonction de leur UID en ajustant le paramètre auto_private_groups pour cette plage d'ID.

Par défaut, l'option auto_private_groups est définie sur false pour les plages d'ID **ipa-ad-trust-posix** utilisées dans une confiance POSIX. Avec cette configuration, SSSD récupère les adresses **uidNumber** et **gidNumber** de chaque entrée d'utilisateur AD.

auto_private_groups = false

SSSD attribue la valeur **uidNumber** à l'UID de l'utilisateur et la valeur **gidNumber** au GID de l'utilisateur. Un groupe avec ce GID doit exister dans AD, sinon vous ne pourrez pas résoudre cet utilisateur. Le tableau suivant indique si vous pourrez résoudre les utilisateurs AD en fonction des différentes configurations AD.

Tableau 7.2. Comportement de SSSD lorsque la variable auto_private_groups est définie sur

false pour une plage d'ID POSIX

Configuration des utilisateurs dans AD	Sortie de **id username**
L'entrée utilisateur AD a : • **uidNumber** = 4000 • **gidNumber** n'est pas défini • Aucun groupe dans AD avec **gidNumber** = 4000.	SSSD ne peut pas résoudre l'utilisateur.
L'entrée utilisateur AD a : • **uidNumber** = 4000 • **gidNumber** = 4000 • Aucun groupe dans AD avec **gidNumber** = 4000.	SSSD ne peut pas résoudre l'utilisateur.
L'entrée utilisateur AD a : • **uidNumber** = 4000 • **gidNumber** = 4000 • AD a un groupe avec **gidNumber** = 4000.	**# id aduser@AD-DOMAIN.COMuid=4000(aduser@ad-domain.com) gid=4000(adgroup@ad-domain.com) groups=4000(adgroup@ad-domain.com), …**

Si un utilisateur AD n'a pas de groupe primaire configuré dans AD, ou si son adresse **gidNumber** ne correspond pas à un groupe existant, le serveur IdM n'est pas en mesure de résoudre cet utilisateur correctement car il ne peut pas rechercher tous les groupes auxquels l'utilisateur appartient. Pour contourner ce problème, vous pouvez activer le mappage automatique des groupes privés dans SSSD en définissant l'option **auto_private_groups** sur **true** ou **hybrid**:

auto_private_groups = true

SSSD crée toujours un groupe privé dont l'adresse **gidNumber** correspond à l'adresse **uidNumber** de l'entrée de l'utilisateur AD.

Tableau 7.3. Comportement de SSSD lorsque la variable auto_private_groups est définie sur true pour une plage d'ID POSIX

Configuration des utilisateurs dans AD	Sortie de **id username**
L'entrée utilisateur AD a : • **uidNumber** = 4000 • **gidNumber** n'est pas défini • AD n'a pas de groupe avec GID=4000.	**# id aduser@AD-DOMAIN.COMuid=4000(aduser@ad-domain.com) gid=4000(aduser@ad-domain.com) groups=4000(aduser@ad-domain.com), …**
L'entrée utilisateur AD a : • **uidNumber** = 4000 • **gidNumber** = 5000 • AD n'a pas de groupe avec **gidNumber** = 5000.	**# id aduser@AD-DOMAIN.COMuid=4000(aduser@ad-domain.com) gid=4000(aduser@ad-domain.com) groups=4000(aduser@ad-domain.com), …**
L'entrée utilisateur AD a : • **uidNumber** = 4000 • **gidNumber** = 4000 • AD n'a pas de groupe avec **gidNumber** = 4000.	**# id aduser@AD-DOMAIN.COMuid=4000(aduser@ad-domain.com) gid=4000(aduser@ad-domain.com) groups=4000(aduser@ad-domain.com), …**
L'entrée utilisateur AD a : • **uidNumber** = 4000 • **gidNumber** = 5000 • AD a un groupe avec **gidNumber** = 5000.	**# id aduser@AD-DOMAIN.COMuid=4000(aduser@ad-domain.com) gid=4000(aduser@ad-domain.com) groups=4000(aduser@ad-domain.com), …**

auto_private_groups = hybrid

Si la valeur **uidNumber** correspond à **gidNumber**, mais qu'il n'y a pas de groupe avec cette valeur **gidNumber**, SSSD affecte un groupe privé comme groupe d'utilisateurs principal de l'utilisateur avec une valeur **gidNumber** qui correspond à **uidNumber**. Si les valeurs **uidNumber** et **gidNumber** diffèrent, et qu'il y a un groupe avec cette valeur **gidNumber**, SSSD utilise la valeur de **gidNumber**.

Tableau 7.4. Comportement de SSSD lorsque la variable auto_private_groups est définie sur hybrid pour une plage d'ID POSIX

Configuration des utilisateurs dans AD	Sortie de **id username**
Entrée utilisateur AD avec : • **uidNumber** = 4000 • **gidNumber** n'est pas défini • AD n'a pas de groupe avec **gidNumber** = 4000.	SSSD ne peut pas résoudre l'utilisateur.
Entrée utilisateur AD avec : • **uidNumber** = 4000 • **gidNumber** = 5000 • AD n'a pas de groupe avec **gidNumber** = 5000.	SSSD ne peut pas résoudre l'utilisateur.
Entrée utilisateur AD avec : • **uidNumber** = 4000 • **gidNumber** = 4000 • AD n'a pas de groupe avec **gidNumber** = 4000.	**# id aduser@AD-DOMAIN.COMuid=4000(aduser@ad-domain.com) gid=4000(aduser@ad-domain.com) groups=4000(aduser@ad-domain.com), …**
Entrée utilisateur AD avec : • **uidNumber** = 4000 • **gidNumber** = 5000 • AD a un groupe avec **gidNumber** = 5000.	**# id aduser@AD-DOMAIN.COMuid=4000(aduser@ad-domain.com) gid=5000(aduser@ad-domain.com) groups=5000(adgroup@ad-domain.com), …**

Ressources supplémentaires

- POSIX et mappage d'ID Types de plages d'ID pour les utilisateurs AD
- Activation du mappage automatique des groupes privés pour une plage d'ID POSIX sur la CLI
- Activation du mappage automatique des groupes privés pour une plage d'ID POSIX dans l'IdM WebUI

7.7. OPTIONS DE MAPPAGE AUTOMATIQUE DES GROUPES PRIVÉS POUR LES UTILISATEURS AD : FIDUCIES DE MAPPAGE D'ID

Dans un environnement Linux, chaque utilisateur dispose d'un groupe d'utilisateurs principal. Red Hat Enterprise Linux (RHEL) utilise un schéma de groupe privé d'utilisateurs (UPG) : un UPG porte le même nom que l'utilisateur pour lequel il a été créé et cet utilisateur est le seul membre de l'UPG.

Si vous avez attribué des UID à vos utilisateurs AD, mais que les GID n'ont pas été ajoutés, vous pouvez configurer SSSD pour qu'il crée automatiquement des groupes privés pour les utilisateurs en fonction de leur UID en ajustant le paramètre auto_private_groups pour cette plage d'ID.

Par défaut, l'option **auto_private_groups** est définie sur **true** pour les plages d'identifiants **ipa-ad-trust** utilisées dans une confiance de mappage d'identifiants. Avec cette configuration, SSSD calcule l'UID et le GID d'un utilisateur AD en fonction de son identifiant de sécurité (SID). SSSD ignore tous les attributs POSIX dans AD, tels que **uidNumber**, **gidNumber**, et ignore également l'option **primaryGroupID**.

auto_private_groups = true

SSSD crée toujours un groupe privé dont le GID correspond à l'UID, qui est basé sur le SID de l'utilisateur AD.

Tableau 7.5. Comportement de SSSD lorsque la variable auto_private_groups est définie sur true pour une plage d'ID mapping

Configuration des utilisateurs dans AD	Sortie de id username
Entrée utilisateur AD où : • Le SID correspond à 7000 • **primaryGroupID** cartes jusqu'à 8000	**# id aduser@AD-DOMAIN.COMuid=7000(aduser@ad-domain.com) gid=7000(aduser@ad-domain.com) groups=7000(aduser@ad-domain.com), 8000(adgroup@ad-domain.com), …**

auto_private_groups = false

Si vous donnez à l'option **auto_private_groups** la valeur **false**, SSSD utilise le numéro **primaryGroupID** défini dans l'entrée AD comme numéro GID. La valeur par défaut de **primaryGroupID** correspond au groupe **Domain Users** dans AD.

Tableau 7.6. Comportement de SSSD lorsque la variable auto_private_groups est définie sur false pour une plage d'ID mapping

Configuration des utilisateurs dans AD	Sortie de id username
Entrée utilisateur AD où : • Le SID correspond à 7000 • **primaryGroupID** cartes jusqu'à 8000	**# id aduser@AD-DOMAIN.COMuid=7000(aduser@ad-domain.com) gid=8000(adgroup@ad-domain.com) groups=8000(adgroup@ad-domain.com), …**

Ressources supplémentaires

- POSIX et mappage d'ID Types de plages d'ID pour les utilisateurs AD

7.8. 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

7.9. 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.

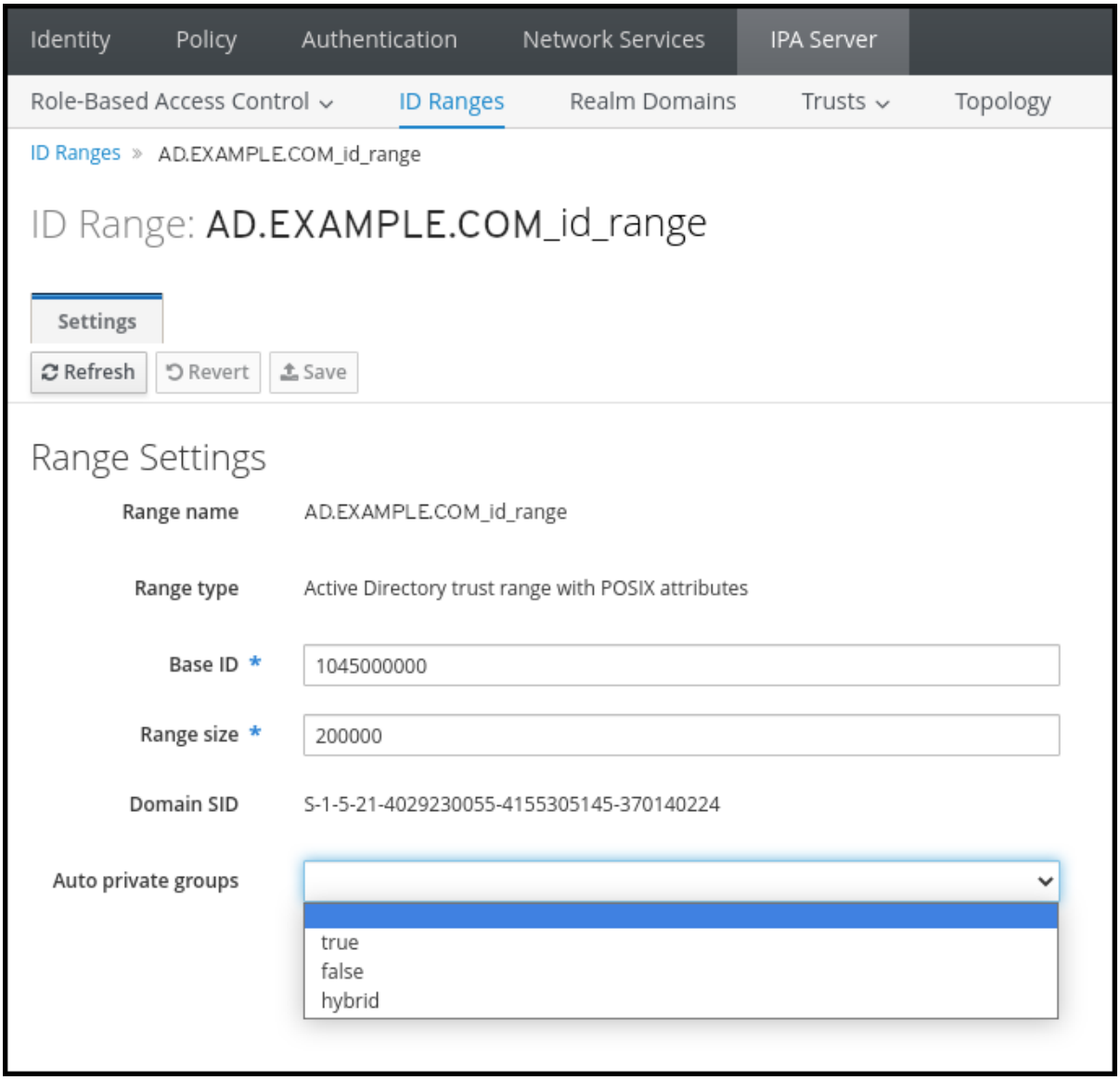
Cette procédure explique comment activer le mappage automatique des groupes privés pour une plage d'identifiants en définissant l'option **hybrid** pour le paramètre **auto_private_groups** SSSD dans l'interface Web de gestion des identités (IdM). En conséquence, IdM est capable de résoudre les utilisateurs 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**.



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

Ressources supplémentaires

- Options de mappage automatique des groupes privés pour les utilisateurs AD

7.10. GROUPES EXTERNES NON-POSIX ET MAPPAGE DES SID

La gestion des identités (IdM) utilise LDAP pour gérer les groupes. Les entrées d'Active Directory (AD) ne sont pas synchronisées ou copiées dans IdM, ce qui signifie que les utilisateurs et les groupes AD n'ont pas d'objets LDAP dans le serveur LDAP et qu'ils ne peuvent donc pas être utilisés directement pour exprimer l'appartenance à un groupe dans le LDAP IdM. Pour cette raison, les administrateurs de l'IdM doivent créer des groupes externes non-POSIX, référencés comme des objets LDAP IdM normaux pour indiquer l'appartenance à un groupe pour les utilisateurs et les groupes AD dans l'IdM.

Les identifiants de sécurité (SID) des groupes externes non-POSIX sont traités par SSSD, qui fait correspondre les SID des groupes dans Active Directory aux groupes POSIX dans IdM. Dans Active Directory, les SID sont associés à des noms d'utilisateurs. Lorsqu'un nom d'utilisateur AD est utilisé pour accéder aux ressources IdM, SSSD utilise le SID de l'utilisateur pour établir une information complète sur l'appartenance de l'utilisateur à un groupe dans le domaine IdM.

7.11. LIGNES DIRECTRICES POUR LA MISE EN PLACE DE DNS POUR UNE CONFIANCE IDM-AD

Ces lignes directrices peuvent vous aider à obtenir la bonne configuration DNS pour établir une confiance inter-forêts entre Identity Management (IdM) et Active Directory (AD).

Domaines DNS primaires uniques

Assurez-vous que AD et IdM ont leurs propres domaines DNS primaires configurés. Par exemple :

- ***ad.example.com*** pour AD et ***idm.example.com*** pour IdM
- ***example.com*** pour AD et ***idm.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 vous pouvez également utiliser n'importe quel autre serveur DNS conforme aux normes.

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 .

Enregistrements SRV appropriés

S'assurer que le domaine DNS primaire de l'IdM dispose des enregistrements SRV appropriés pour prendre en charge les trusts AD.
Pour les autres domaines DNS qui font partie du même domaine IdM, il n'est pas nécessaire de configurer les enregistrements SRV lors de l'établissement de la confiance avec AD. En effet, les contrôleurs de domaine AD n'utilisent pas les enregistrements SRV pour découvrir les centres de distribution de clés Kerberos (KDC), mais basent plutôt la découverte des KDC sur les informations de routage des suffixes de noms pour la confiance.

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

Assurez-vous que toutes les machines peuvent résoudre les enregistrements DNS de tous les domaines DNS impliqués dans la relation de confiance :

- Lors de la configuration du DNS IdM, suivez les instructions décrites dans Installation d'un serveur IdM avec une autorité de certification externe.
- Si vous utilisez IdM sans DNS intégré, suivez les instructions décrites dans Installation d'un serveur IdM sans DNS intégré.

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

Assurez-vous que les noms de domaines Kerberos sont 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***.

7.12. LIGNES DIRECTRICES POUR LA CONFIGURATION DES NOMS NETBIOS

Le nom NetBIOS est généralement la composante la plus à gauche du nom de domaine. Par exemple, le nom NetBIOS est la composante la plus à gauche du nom de domaine :

- Dans le nom de domaine ***linux.example.com*** le nom NetBIOS est **linux**.
- Dans le nom de domaine ***example.com*** le nom NetBIOS est **example**.

Noms NetBIOS différents pour les domaines Identity Management (IdM) et Active Directory (AD)

Assurez-vous que les domaines IdM et AD ont des noms NetBIOS différents.
Le nom NetBIOS est essentiel pour identifier le domaine AD. Si le domaine IdM se trouve dans un sous-domaine du DNS AD, le nom NetBIOS est également essentiel pour identifier le domaine et les services IdM.

Limite de caractères pour les noms NetBIOS

La longueur maximale d'un nom NetBIOS est de 15 caractères.

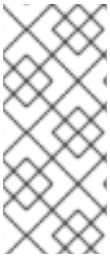
7.13. VERSIONS PRISES EN CHARGE DE WINDOWS SERVER

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.

7.14. DÉCOUVERTE DU SERVEUR AD ET AFFINITÉ

La configuration de la découverte et de l'affinité des serveurs affecte les serveurs Active Directory (AD) avec lesquels un client Identity Management (IdM) communique. Cette section donne un aperçu du fonctionnement de la découverte et de l'affinité dans un environnement où la confiance entre IdM et AD s'étend d'une forêt à l'autre.

Configurer les clients de manière à ce qu'ils préfèrent les serveurs situés dans la même zone géographique permet d'éviter les décalages temporels et autres problèmes qui surviennent lorsque les clients contactent les serveurs d'un autre centre de données distant. Pour vous assurer que les clients communiquent avec les serveurs locaux, vous devez veiller à ce que :

- Les clients communiquent avec les serveurs IdM locaux via LDAP et Kerberos
- Les clients communiquent avec les serveurs AD locaux via Kerberos
- Les clients intégrés aux serveurs IdM communiquent avec les serveurs AD locaux via LDAP et Kerberos

Options de configuration de LDAP et Kerberos sur le client IdM pour la communication avec les serveurs IdM locaux

Lors de l'utilisation d'IdM avec DNS intégré

Par défaut, les clients utilisent la recherche automatique de services basée sur les enregistrements DNS. Dans cette configuration, vous pouvez également utiliser la fonction *DNS locations* pour configurer la recherche de services basée sur le DNS.
Pour remplacer la recherche automatique, vous pouvez désactiver la découverte du DNS de l'une des manières suivantes :

- Pendant l'installation du client IdM, en fournissant les paramètres de basculement à partir de la ligne de commande
- Après l'installation du client, en modifiant la configuration du System Security Services Daemon (SSSD)

En cas d'utilisation d'IdM sans DNS intégré

Vous devez configurer explicitement les clients de l'une des manières suivantes :

- Pendant l'installation du client IdM, en fournissant les paramètres de basculement à partir de la ligne de commande
- Après l'installation du client en modifiant la configuration SSSD

Options de configuration de Kerberos sur le client IdM pour la communication avec les serveurs AD locaux

Les clients IdM ne sont pas en mesure de découvrir automatiquement les serveurs AD avec lesquels ils doivent communiquer. Pour spécifier manuellement les serveurs AD, modifiez le fichier **krb5.conf**:

- Ajouter les informations relatives à la zone AD
- Liste explicite des serveurs AD avec lesquels communiquer

Par exemple :

```
[realms]
```

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

Options de configuration des clients intégrés sur les serveurs IdM pour la communication avec les serveurs AD locaux via Kerberos et LDAP

Le client intégré à un serveur IdM fonctionne également comme un client du serveur AD. Il peut découvrir et utiliser automatiquement le site AD approprié.

Lorsque le client intégré effectue la découverte, il peut d'abord découvrir un serveur AD à distance. Si la tentative de contact avec le serveur distant prend trop de temps, le client peut interrompre l'opération sans établir la connexion. Utilisez l'option **dns_resolver_timeout** du fichier **sssd.conf** sur le client pour augmenter la durée pendant laquelle le client attend une réponse du résolveur DNS. Voir la page de manuel *sssd.conf(5)* pour plus de détails.

Une fois que le client intégré a été configuré pour communiquer avec les serveurs AD locaux, le SSSD se souvient du site AD auquel le client intégré appartient. Grâce à cela, le SSSD envoie normalement un ping LDAP directement à un contrôleur de domaine local pour rafraîchir ses informations sur le site. Si le site n'existe plus ou si le client a entre-temps été assigné à un autre site, le SSSD commence à demander des enregistrements SRV dans la forêt et passe par tout un processus d'autodécouverte.

En utilisant *trusted domain sections* dans **sssd.conf**, vous pouvez également remplacer explicitement certaines des informations qui sont découvertes automatiquement par défaut.

7.15. OPÉRATIONS EFFECTUÉES LORS DE L'INTÉGRATION INDIRECTE DE IDM À AD

Cette section détaille les opérations et les demandes effectuées lors de l'intégration indirecte d'IdM à AD.

Lisez le tableau pour connaître les opérations et les demandes effectuées lors de la création d'une confiance entre Identity Management (IdM) et Active Directory (AD), du contrôleur de confiance IdM vers les contrôleurs de domaine AD.

Tableau 7.7. Opérations effectuées à partir d'un contrôleur de confiance IdM vers les contrôleurs de domaine AD

Fonctionnement	Protocole utilisé	Objectif
Résolution DNS par rapport aux résolveurs DNS AD configurés sur un contrôleur de confiance IdM	DNS	Pour découvrir les adresses IP des contrôleurs de domaine AD
Requêtes vers le port UDP/UDP6 389 d'un AD DC	LDAP sans connexion (CLDAP)	Pour effectuer la découverte d'un AD DC
Requêtes vers les ports TCP/TCP6 389 et 3268 sur un AD DC	LDAP	Pour interroger les informations sur les utilisateurs et les groupes AD
Requêtes vers les ports TCP/TCP6 389 et 3268 sur un AD DC	DCE RPC et SMB	Mettre en place et soutenir un système de confiance inter-forêts pour AD

Fonctionnement	Protocole utilisé	Objectif
Requêtes vers les ports TCP/TCP6 135, 139, 445 sur un AD DC	DCE RPC et SMB	Mettre en place et soutenir un système de confiance inter-forêts pour AD
Requêtes adressées à des ports ouverts dynamiquement sur un AD DC selon les instructions du contrôleur de domaine Active Directory, probablement dans la plage 49152-65535 (TCP/TCP6)	DCE RPC et SMB	Pour répondre aux demandes de DCE RPC End-point mapper (port 135 TCP/TCP6)
Requêtes vers les ports 88 (TCP/TCP6 et UDP/UDP6), 464 (TCP/TCP6 et UDP/UDP6) et 749 (TCP/TCP6) sur un AD DC	Kerberos	Obtenir un ticket Kerberos ; modifier un mot de passe Kerberos ; administrer Kerberos à distance

Lisez le tableau pour connaître les opérations et les requêtes effectuées lors de la création d'une confiance IdM to AD du contrôleur de domaine AD vers les contrôleurs de confiance IdM.

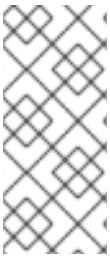
Tableau 7.8. Opérations effectuées à partir d'un contrôleur de domaine AD vers les contrôleurs de confiance IdM

Fonctionnement	Protocole utilisé	Objectif
Résolution DNS par rapport aux résolveurs DNS IdM configurés sur un contrôleur de domaine AD	DNS	Pour découvrir les adresses IP des contrôleurs de confiance IdM
Demandes adressées au port UDP/UDP6 389 d'un contrôleur de confiance IdM	CLDAP	Pour effectuer la découverte du contrôleur de confiance IdM
Requêtes adressées aux ports TCP/TCP6 135, 139, 445 d'un contrôleur de confiance IdM	DCE RPC et SMB	Pour vérifier la confiance entre les forêts et AD
Requêtes adressées à des ports ouverts dynamiquement sur un contrôleur de confiance IdM, selon les instructions de ce dernier, probablement dans la plage 49152-65535 (TCP/TCP6)	DCE RPC et SMB	Pour répondre aux demandes de DCE RPC End-point mapper (port 135 TCP/TCP6)
Demandes adressées aux ports 88 (TCP/TCP6 et UDP/UDP6), 464 (TCP/TCP6 et UDP/UDP6) et 749 (TCP/TCP6) d'un contrôleur de confiance IdM	Kerberos	Obtenir un ticket Kerberos ; modifier un mot de passe Kerberos ; administrer Kerberos à distance

CHAPITRE 8. SAUVEGARDE ET RESTAURATION DE L'IDM

Red Hat Enterprise Linux Identity Management fournit une solution pour sauvegarder et restaurer manuellement le système IdM. Cela peut s'avérer nécessaire après une perte de données.

Pendant la sauvegarde, le système crée un répertoire contenant des informations sur votre configuration IdM et le stocke. Lors de la restauration, vous pouvez utiliser ce répertoire de sauvegarde pour rétablir votre configuration IdM d'origine.



NOTE

Les fonctions de sauvegarde et de restauration de l'IdM sont conçues pour aider à prévenir la perte de données. Pour atténuer l'impact de la perte d'un serveur et assurer la continuité des opérations en fournissant des serveurs alternatifs aux clients, assurez-vous d'avoir une topologie de réplication conforme à Atténuer la perte de serveur avec la réplication.

8.1. TYPES DE SAUVEGARDE IDM

L'utilitaire **ipa-backup** vous permet de créer deux types de sauvegardes :

Sauvegarde complète du serveur

- **Contains** tous les fichiers de configuration du serveur liés à l'IdM et les données LDAP dans les fichiers LDAP Data Interchange Format (LDIF)
- Les services IdM doivent être accessibles à l'adresse **offline**.
- **Suitable for** reconstruire un déploiement IdM à partir de zéro.

Sauvegarde des données uniquement

- **Contains** Données LDAP dans les fichiers LDIF et le journal des modifications de la réplication
- Les services IdM peuvent être **online or offline**.
- **Suitable for** rétablir les données de l'IdM dans un état antérieur

8.2. CONVENTIONS D'APPELLATION POUR LES FICHIERS DE SAUVEGARDE IDM

Par défaut, IdM stocke les sauvegardes sous forme d'archives **.tar** dans des sous-répertoires du répertoire **/var/lib/ipa/backup/**.

Les archives et les sous-répertoires suivent les conventions de dénomination suivantes :

Sauvegarde complète du serveur

Une archive nommée **ipa-full.tar** dans un répertoire nommé **ipa-full-*<YEAR-MM-DD-HH-MM-SS>***avec l'heure spécifiée en heure GMT.

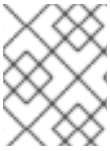
```
[root@server ~]# ll /var/lib/ipa/backup/ipa-full-2021-01-29-12-11-46
total 3056
```

```
-rw-r--r--. 1 root root     158 Jan 29 12:11 header
-rw-r--r--. 1 root root 3121511 Jan 29 12:11 ipa-full.tar
```

Sauvegarde des données uniquement

Une archive nommée **ipa-data.tar** dans un répertoire nommé **ipa-data-*<YEAR-MM-DD-HH-MM-SS>***avec l'heure spécifiée en heure GMT.

```
[root@server ~]# ll /var/lib/ipa/backup/ipa-data-2021-01-29-12-14-23
total 1072
-rw-r--r--. 1 root root     158 Jan 29 12:14 header
-rw-r--r--. 1 root root 1090388 Jan 29 12:14 ipa-data.tar
```



NOTE

La désinstallation d'un serveur IdM ne supprime pas automatiquement les fichiers de sauvegarde.

8.3. ÉLÉMENTS À PRENDRE EN COMPTE LORS DE LA CRÉATION D'UNE SAUVEGARDE

Cette section décrit les comportements importants et les limites de la commande **ipa-backup**.

- Par défaut, l'utilitaire **ipa-backup** fonctionne en mode déconnecté, ce qui arrête tous les services IdM. L'utilitaire redémarre automatiquement les services IdM une fois la sauvegarde terminée.
- Une sauvegarde complète du serveur doit être exécutée sur **always** avec les services IdM hors ligne, mais une sauvegarde des données uniquement peut être effectuée avec les services en ligne.
- Par défaut, l'utilitaire **ipa-backup** crée des sauvegardes sur le système de fichiers contenant le répertoire **/var/lib/ipa/backup/**. Red Hat recommande de créer régulièrement des sauvegardes sur un système de fichiers distinct du système de fichiers de production utilisé par IdM et d'archiver les sauvegardes sur un support fixe, tel qu'une bande ou un stockage optique.
- Pensez à effectuer des sauvegardes sur des répliques cachées. Les services IdM peuvent être arrêtés sur des répliques cachées sans affecter les clients IdM.
- L'utilitaire **ipa-backup** vérifie si tous les services utilisés dans votre cluster IdM, tels qu'une autorité de certification (CA), un système de noms de domaine (DNS) et un agent de récupération des clés (KRA), sont installés sur le serveur sur lequel vous exécutez la sauvegarde. Si tous ces services ne sont pas installés sur le serveur, l'utilitaire **ipa-backup** sort avec un avertissement, car les sauvegardes effectuées sur cet hôte ne seraient pas suffisantes pour une restauration complète du cluster.
  Par exemple, si votre déploiement IdM utilise une autorité de certification (CA) intégrée, une sauvegarde exécutée sur une réplique non-CA ne capturera pas les données de la CA. Red Hat recommande de vérifier que la réplique sur laquelle vous effectuez une sauvegarde **ipa-backup** dispose de tous les services IdM utilisés dans le cluster.

  Vous pouvez contourner la vérification du rôle du serveur IdM à l'aide de la commande **ipa-backup --disable-role-check**, mais la sauvegarde résultante ne contiendra pas toutes les données nécessaires à la restauration complète d'IdM.

8.4. CRÉATION D'UNE SAUVEGARDE IDM

Cette section décrit comment créer une sauvegarde complète du serveur et des données uniquement en mode hors ligne et en ligne à l'aide de la commande **ipa-backup**.

Conditions préalables

- Vous devez disposer des privilèges **root** pour exécuter l'utilitaire **ipa-backup**.

Procédure

- Pour créer une sauvegarde complète du serveur en mode hors ligne, utilisez l'utilitaire **ipa-backup** sans options supplémentaires.

```
[root@server ~]# ipa-backup
Preparing backup on server.example.com
Stopping IPA services
Backing up ipaca in EXAMPLE-COM to LDIF
Backing up userRoot in EXAMPLE-COM to LDIF
Backing up EXAMPLE-COM
Backing up files
Starting IPA service
Backed up to /var/lib/ipa/backup/ipa-full-2020-01-14-11-26-06
The ipa-backup command was successful
```

- Pour créer une sauvegarde hors ligne des données uniquement, spécifiez l'option **--data**.

```
[root@server ~]# ipa-backup --data
```

- Pour créer une sauvegarde complète du serveur qui inclut les fichiers journaux IdM, utilisez l'option **--logs**.

```
[root@server ~]# ipa-backup --logs
```

- Pour créer une sauvegarde de données uniquement lorsque les services IdM sont en cours d'exécution, spécifiez les options **--data** et **--online**.

```
[root@server ~]# ipa-backup --data --online
```

NOTE

Si la sauvegarde échoue en raison d'un manque d'espace dans le répertoire **/tmp**, utilisez la variable d'environnement **TMPDIR** pour modifier la destination des fichiers temporaires créés par le processus de sauvegarde :

```
[root@server ~]# TMPDIR=/new/location ipa-backup
```

Pour plus de détails, voir La commande ipa-backup ne se termine pas .

Étapes de la vérification

- Le répertoire de sauvegarde contient une archive avec la sauvegarde.

```
[root@server ~]# ls /var/lib/ipa/backup/ipa-full-2020-01-14-11-26-06
header  ipa-full.tar
```

8.5. CRÉATION D'UNE SAUVEGARDE DE L'IDM CHIFFRÉE PAR GPG2

Vous pouvez créer des sauvegardes cryptées en utilisant le cryptage GNU Privacy Guard (GPG). La procédure suivante crée une sauvegarde IdM et la crypte à l'aide d'une clé GPG2.

Conditions préalables

- Vous avez créé une clé GPG2. Voir Création d'une clé GPG2.

Procédure

- Créez une sauvegarde chiffrée par GPG en spécifiant l'option **--gpg**.

```
[root@server ~]# ipa-backup --gpg
Preparing backup on server.example.com
Stopping IPA services
Backing up ipaca in EXAMPLE-COM to LDIF
Backing up userRoot in EXAMPLE-COM to LDIF
Backing up EXAMPLE-COM
Backing up files
Starting IPA service
Encrypting /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00/ipa-full.tar
Backed up to /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00
The ipa-backup command was successful
```

Étapes de la vérification

- Assurez-vous que le répertoire de sauvegarde contient une archive cryptée avec une extension de fichier **.gpg**.

```
[root@server ~]# ls /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00
header  ipa-full.tar.gpg
```

Ressources supplémentaires

- Création d'une sauvegarde.

8.6. CRÉATION D'UNE CLÉ GPG2

La procédure suivante décrit comment générer une clé GPG2 à utiliser avec les utilitaires de cryptage.

Conditions préalables

- Vous avez besoin des privilèges de **root**.

Procédure

1. Installer et configurer l'utilitaire **pinentry**.

```
[root@server ~]# dnf install pinentry
[root@server ~]# mkdir ~/.gnupg -m 700
[root@server ~]# echo "pinentry-program /usr/bin/pinentry-curses" >> ~/.gnupg/gpg-agent.conf
```

2. Créez un fichier **key-input** utilisé pour générer une paire de clés GPG avec les détails de votre choix. Par exemple :

```
[root@server ~]# cat >key-input <<EOF
%echo Generating a standard key
Key-Type: RSA
Key-Length: 2048
Name-Real: GPG User
Name-Comment: first key
Name-Email: root@example.com
Expire-Date: 0
%commit
%echo Finished creating standard key
EOF
```

3. *(Optional)* Par défaut, GPG2 stocke son trousseau de clés dans le fichier **~/.gnupg**. Pour utiliser un emplacement de trousseau personnalisé, définissez la variable d'environnement **GNUPGHOME** dans un répertoire accessible uniquement par root.

```
[root@server ~]# export GNUPGHOME=/root/backup

[root@server ~]# mkdir -p $GNUPGHOME -m 700
```

4. Générer une nouvelle clé GPG2 basée sur le contenu du fichier **key-input**.

```
[root@server ~]# gpg2 --batch --gen-key key-input
```

5. Saisissez une phrase de passe pour protéger la clé GPG2. Cette phrase d'authentification permet d'accéder à la clé privée pour le décryptage.

```
┌──────────────────────────────────────────────────────┐
│ Please enter the passphrase to                       │
│ protect your new key                                 │
│                                                      │
│ Passphrase: <passphrase>                             │
│                                                      │
│  <OK>                    <Cancel>                    │
└──────────────────────────────────────────────────────┘
```

6. Confirmez la phrase d'authentification correcte en la saisissant à nouveau.

```
┌──────────────────────────────────────────────────────┐
│ Please re-enter this passphrase                      │
│                                                      │
│ Passphrase: <passphrase>                             │
│                                                      │
│  <OK>                    <Cancel>                    │
└──────────────────────────────────────────────────────┘
```

7. Vérifiez que la nouvelle clé GPG2 a été créée avec succès.

```
gpg: keybox '/root/backup/pubring.kbx' created
gpg: Generating a standard key
gpg: /root/backup/trustdb.gpg: trustdb created
gpg: key BF28FFA302EF4557 marked as ultimately trusted
gpg: directory '/root/backup/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/backup/openpgp-
revocs.d/8F6FCF10C80359D5A05AED67BF28FFA302EF4557.rev'
gpg: Finished creating standard key
```

Étapes de la vérification

- Liste des clés GPG sur le serveur.

```
[root@server ~]# gpg2 --list-secret-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
/root/backup/pubring.kbx
------------------------
sec   rsa2048 2020-01-13 [SCEA]
      8F6FCF10C80359D5A05AED67BF28FFA302EF4557
uid           [ultimate] GPG User (first key) <root@example.com>
```

Ressources supplémentaires

- GNU Privacy Guard

8.7. QUAND RESTAURER À PARTIR D'UNE SAUVEGARDE IDM

Vous pouvez répondre à plusieurs scénarios de désastre en restaurant à partir d'une sauvegarde IdM :

- **Undesirable changes were made to the LDAP content** Des entrées ont été modifiées ou supprimées, la réplication a effectué ces changements tout au long du déploiement et vous souhaitez revenir sur ces modifications. La restauration d'une sauvegarde de données uniquement permet de rétablir l'état antérieur des entrées LDAP sans affecter la configuration IdM elle-même.

- **Total Infrastructure Loss, or loss of all CA instances** Si un sinistre endommage toutes les répliques d'autorité de certification, le déploiement a perdu la capacité de se reconstruire en déployant des serveurs supplémentaires. Dans ce cas, il faut restaurer une sauvegarde d'une réplique d'autorité de certification et construire de nouvelles répliques à partir de celle-ci.

- **An upgrade on an isolated server failed** Le système d'exploitation reste fonctionnel, mais les données IdM sont corrompues, c'est pourquoi vous souhaitez restaurer le système IdM dans un état de bon fonctionnement connu. Red Hat recommande de travailler avec le support technique pour diagnostiquer et résoudre le problème. Si ces efforts échouent, restaurez à partir d'une sauvegarde complète du serveur.

IMPORTANT

La solution préférée en cas de défaillance matérielle ou de mise à niveau consiste à reconstruire le serveur perdu à partir d'un réplica. Pour plus d'informations, voir Récupération d'un serveur unique avec réplication .

8.8. CONSIDÉRATIONS À PRENDRE EN COMPTE LORS DE LA RESTAURATION À PARTIR D'UNE SAUVEGARDE IDM

Si vous disposez d'une sauvegarde créée avec l'utilitaire **ipa-backup**, vous pouvez restaurer votre serveur IdM ou le contenu LDAP dans l'état où ils se trouvaient lorsque la sauvegarde a été effectuée.

Voici les principales considérations à prendre en compte lors de la restauration d'une sauvegarde IdM :

- Vous ne pouvez restaurer une sauvegarde que sur un serveur dont la configuration correspond à celle du serveur sur lequel la sauvegarde a été créée à l'origine. Le serveur **must** a :
  - Le même nom d'hôte
  - La même adresse IP
  - La même version du logiciel IdM
- Si un serveur IdM parmi d'autres est restauré, le serveur restauré devient la seule source d'information pour IdM. Tous les autres serveurs **must** sont réinitialisés à partir du serveur restauré.
- Étant donné que toutes les données créées après la dernière sauvegarde seront perdues, n'utilisez pas la solution de sauvegarde et de restauration pour la maintenance normale du système.
- Si un serveur est perdu, Red Hat recommande de reconstruire le serveur en le réinstallant en tant que réplique, au lieu de le restaurer à partir d'une sauvegarde. La création d'une nouvelle réplique préserve les données de l'environnement de travail actuel. Pour plus d'informations, voir Préparation à la perte d'un serveur avec la réplication .
- Les fonctions de sauvegarde et de restauration ne peuvent être gérées qu'à partir de la ligne de commande et ne sont pas disponibles dans l'interface web de l'IdM.
- Vous ne pouvez pas restaurer des fichiers de sauvegarde situés dans les répertoires **/tmp** ou **/var/tmp**. Le serveur d'annuaire IdM utilise un répertoire **PrivateTmp** et ne peut pas accéder aux répertoires **/tmp** ou **/var/tmp** généralement disponibles pour le système d'exploitation.

ASTUCE

La restauration à partir d'une sauvegarde nécessite les mêmes versions de logiciels (RPM) sur l'hôte cible que celles qui ont été installées lorsque la sauvegarde a été effectuée. Pour cette raison, Red Hat recommande de restaurer à partir d'un instantané de machine virtuelle plutôt qu'à partir d'une sauvegarde. Pour plus d'informations, voir Récupérer des données perdues avec des snapshots de VM .

8.9. RESTAURATION D'UN SERVEUR IDM À PARTIR D'UNE SAUVEGARDE

La procédure suivante décrit la restauration d'un serveur IdM ou de ses données LDAP à partir d'une sauvegarde IdM.

Figure 8.1. Topologie de réplication utilisée dans cet exemple

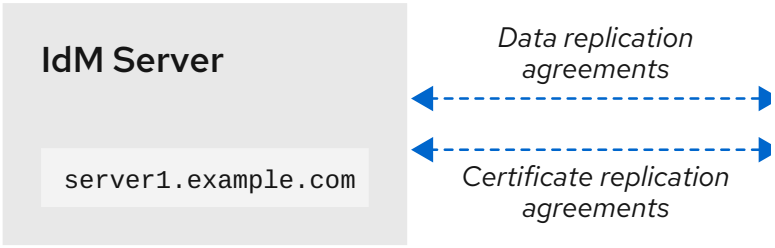


Tableau 8.1. Conventions de dénomination des serveurs utilisées dans cet exemple

Nom d'hôte du serveur	Fonction
server1.example.com	Le serveur qui doit être restauré à partir de la sauvegarde.
caReplica2.example.com	Une réplique de l'autorité de certification (CA) connectée à l'hôte **server1.example.com**.
replica3.example.com	Une réplique connectée à l'hôte **caReplica2.example.com**.

Conditions préalables

- Vous avez généré une sauvegarde complète du serveur ou des données uniquement du serveur IdM à l'aide de l'utilitaire **ipa-backup**. Voir Création d'une sauvegarde.
- Vos fichiers de sauvegarde ne se trouvent pas dans les répertoires **/tmp** ou **/var/tmp**.
- Avant d'effectuer une restauration complète du serveur à partir d'une sauvegarde complète du serveur, désinstallez IdM du serveur et réinstallez IdM en utilisant la même configuration de serveur qu'auparavant.

Procédure

1. Utilisez l'utilitaire **ipa-restore** pour restaurer un serveur complet ou une sauvegarde de données uniquement.
   - Si le répertoire de sauvegarde se trouve dans l'emplacement par défaut **/var/lib/ipa/backup/**, saisissez uniquement le nom du répertoire :

     ```
     [root@server1 ~]# ipa-restore ipa-full-2020-01-14-12-02-32
     ```

   - Si le répertoire de sauvegarde ne se trouve pas à l'emplacement par défaut, saisissez son chemin d'accès complet :

     ```
     [root@server1 ~]# ipa-restore /mybackups/ipa-data-2020-02-01-05-30-00
     ```

NOTE

L'utilitaire **ipa-restore** détecte automatiquement le type de sauvegarde que le répertoire contient et effectue le même type de restauration par défaut. Pour effectuer une restauration de données uniquement à partir d'une sauvegarde complète du serveur, ajoutez l'option **--data** à la commande **ipa-restore**:

```
[root@server1 ~]# ipa-restore --data ipa-full-2020-01-14-12-02-32
```

2. Saisissez le mot de passe du gestionnaire de répertoire.

```
Mot de passe du gestionnaire d'annuaire (maître existant) :
```

3. Entrez **yes** pour confirmer l'écrasement des données actuelles par la sauvegarde.

```
Preparing restore from /var/lib/ipa/backup/ipa-full-2020-01-14-12-02-32 on
server1.example.com
Performing FULL restore from FULL backup
Temporary setting umask to 022
Restoring data will overwrite existing live data. Continue to restore? [no]: yes
```

4. L'utilitaire **ipa-restore** désactive la réplication sur tous les serveurs disponibles :

```
Each master will individually need to be re-initialized or
re-created from this one. The replication agreements on
masters running IPA 3.1 or earlier will need to be manually
re-enabled. See the man page for details.
Disabling all replication.
Disabling replication agreement on server1.example.com to caReplica2.example.com
Disabling CA replication agreement on server1.example.com to caReplica2.example.com
Disabling replication agreement on caReplica2.example.com to server1.example.com
Disabling replication agreement on caReplica2.example.com to replica3.example.com
Disabling CA replication agreement on caReplica2.example.com to server1.example.com
Disabling replication agreement on replica3.example.com to caReplica2.example.com
```

L'utilitaire arrête ensuite les services IdM, restaure la sauvegarde et redémarre les services :

```
Stopping IPA services
Systemwide CA database updated.
Restoring files
Systemwide CA database updated.
Restoring from userRoot in EXAMPLE-COM
Restoring from ipaca in EXAMPLE-COM
Restarting GSS-proxy
Starting IPA services
Restarting SSSD
Restarting oddjobd
Restoring umask to 18
The ipa-restore command was successful
```

5. Réinitialiser toutes les répliques connectées au serveur restauré :

a. Listez tous les segments de topologie de réplication pour le suffixe **domain**, en prenant note des segments de topologie impliquant le serveur restauré.

```
[root@server1 ~]# ipa topologysegment-find domain
-----------------
2 segments matched
-----------------
  Segment name: server1.example.com-to-caReplica2.example.com
  Left node: server1.example.com
  Right node: caReplica2.example.com
  Connectivity: both

  Segment name: caReplica2.example.com-to-replica3.example.com
  Left node: caReplica2.example.com
  Right node: replica3.example.com
  Connectivity: both
----------------------------
Number of entries returned 2
----------------------------
```

b. Réinitialisez le suffixe **domain** pour tous les segments de la topologie avec le serveur restauré.
Dans cet exemple, il s'agit de réinitialiser **caReplica2** avec des données provenant de **server1**.

```
[root@caReplica2 ~]# ipa-replica-manage re-initialize --from=server1.example.com
Update in progress, 2 seconds elapsed
Update succeeded
```

c. En ce qui concerne les données relatives à l'autorité de certification, dressez la liste de tous les segments de la topologie de réplication pour le suffixe **ca**.

```
[root@server1 ~]# ipa topologysegment-find ca
-----------------
1 segment matched
-----------------
  Segment name: server1.example.com-to-caReplica2.example.com
  Left node: server1.example.com
  Right node: caReplica2.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------
```

d. Réinitialisez toutes les répliques de CA connectées au serveur restauré.
Dans cet exemple, nous effectuons une réinitialisation de **csreplica** à partir de **caReplica2** avec des données provenant de **server1**.

```
[root@caReplica2 ~]# ipa-csreplica-manage re-initialize --
from=server1.example.com
Directory Manager password:

Update in progress, 3 seconds elapsed
Update succeeded
```

6. Continuez à vous déplacer vers l'extérieur dans la topologie de réplication, en réinitialisant les répliques successives, jusqu'à ce que tous les serveurs aient été mis à jour avec les données du serveur restauré **server1.example.com**.
   Dans cet exemple, il suffit de réinitialiser le suffixe **domain** sur **replica3** avec les données de **caReplica2**:

```
[root@replica3 ~]# ipa-replica-manage re-initialize --from=caReplica2.example.com
Directory Manager password:

Update in progress, 3 seconds elapsed
Update succeeded
```

7. Vider le cache de SSSD sur chaque serveur pour éviter les problèmes d'authentification dus à des données non valides :

   a. Arrêtez le service SSSD :

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

   b. Supprimer tout le contenu mis en cache du SSSD :

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

   c. Démarrez le service SSSD :

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

   d. Redémarrer le serveur.

Ressources supplémentaires

- La page de manuel **ipa-restore (1)** couvre également en détail la manière de gérer les scénarios de réplication complexes lors de la restauration.

8.10. RESTAURATION À PARTIR D'UNE SAUVEGARDE CRYPTÉE

Cette procédure permet de restaurer un serveur IdM à partir d'une sauvegarde IdM cryptée. L'utilitaire **ipa-restore** détecte automatiquement si une sauvegarde IdM est cryptée et la restaure à l'aide du trousseau de clés racine GPG2.

Conditions préalables

- Une sauvegarde IdM chiffrée par GPG. Voir Création de sauvegardes IdM cryptées .
- Le mot de passe du gestionnaire de répertoire LDAP
- La phrase de passe utilisée lors de la création de la clé GPG

Procédure

1. Si vous avez utilisé un emplacement de trousseau personnalisé lors de la création des clés GPG2, assurez-vous que la variable d'environnement **$GNUPGHOME** est définie sur ce répertoire. Voir Création d'une clé GPG2 .

```
[root@server ~]# echo $GNUPGHOME
/root/backup
```

2. Indiquez à l'utilitaire **ipa-restore** l'emplacement du répertoire de sauvegarde.

```
[root@server ~]# ipa-restore ipa-full-2020-01-13-18-30-54
```

   a. Saisissez le mot de passe du gestionnaire de répertoire.

```
Mot de passe du gestionnaire d'annuaire (maître existant) :
```

   b. Saisissez la phrase de passe que vous avez utilisée lors de la création de la clé GPG.

```
┌──────────────────────────────────────────────────────────────────────┐
│ Please enter the passphrase to unlock the OpenPGP secret key:        │
│ "GPG User (first key) <root@example.com>"                            │
│ 2048-bit RSA key, ID BF28FFA302EF4557,                               │
│ created 2020-01-13.                                                  │
│                                                                      │
│                                                                      │
│ Passphrase: <passphrase>                                             │
│                                                                      │
│       <OK>                              <Cancel>                     │
└──────────────────────────────────────────────────────────────────────┘
```

3. Réinitialisez toutes les répliques connectées au serveur restauré. Voir Restauration d'un serveur IdM à partir d'une sauvegarde.

CHAPITRE 9. SAUVEGARDE ET RESTAURATION DES SERVEURS IDM À L'AIDE DE PLAYBOOKS ANSIBLE

En utilisant le rôle Ansible **ipabackup**, vous pouvez automatiser la sauvegarde d'un serveur IdM, le transfert des fichiers de sauvegarde entre les serveurs et votre contrôleur Ansible, et la restauration d'un serveur IdM à partir d'une sauvegarde.

9.1. UTILISER ANSIBLE POUR CRÉER UNE SAUVEGARDE D'UN SERVEUR IDM

La procédure suivante décrit comment utiliser le rôle ipabackup dans un playbook Ansible pour créer une sauvegarde d'un serveur IdM et la stocker sur le serveur IdM.

Conditions préalables

- 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 paquetage **ansible-freeipa**.
  - Vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM sur lequel vous configurez ces options.
  - Votre fichier d'inventaire Ansible est situé dans le répertoire ~/**MyPlaybooks**/.

Procédure

1. Naviguez jusqu'au répertoire ~/**MyPlaybooks**/:

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

2. Faites une copie du fichier **backup-server.yml** situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/backup-server.yml backup-my-server.yml
```

3. Ouvrez le fichier **backup-my-server.yml** Ansible playbook pour l'éditer.
4. Adaptez le fichier en fixant la variable **hosts** à un groupe d'hôtes de votre fichier d'inventaire. Dans cet exemple, il s'agit du groupe d'hôtes **ipaserver**:

```
---
```

```
- name: Playbook to backup IPA server
  hosts: ipaserver
  become: true

  roles:
  - role: ipabackup
    state: present
```

5. Enregistrer le fichier.
6. Exécutez le playbook Ansible, en spécifiant le fichier d'inventaire et le fichier du playbook :

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory
backup-my-server.yml
```

Verification steps

1. Connectez-vous au serveur IdM que vous avez sauvegardé.
2. Vérifiez que la sauvegarde se trouve dans le répertoire **/var/lib/ipa/backup**.

```
[root@server ~]# ls /var/lib/ipa/backup/
ipa-full-2021-04-30-13-12-00
```

Ressources supplémentaires

- Pour plus d'exemples de playbooks Ansible qui utilisent le rôle **ipabackup**, voir :
  - Le fichier **README.md** dans le répertoire **/usr/share/doc/ansible-freeipa/roles/ipabackup**.
  - Le répertoire **/usr/share/doc/ansible-freeipa/playbooks/**.

9.2. UTILISER ANSIBLE POUR CRÉER UNE SAUVEGARDE D'UN SERVEUR IDM SUR VOTRE CONTRÔLEUR ANSIBLE

La procédure suivante décrit comment utiliser le rôle **ipabackup** dans un playbook Ansible pour créer une sauvegarde d'un serveur IdM et la transférer automatiquement sur votre contrôleur Ansible. Le nom de votre fichier de sauvegarde commence par le nom d'hôte du serveur IdM.

Conditions préalables

- 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 paquetage **ansible-freeipa**.
- Vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM sur lequel vous configurez ces options.
- Votre fichier d'inventaire Ansible est situé dans le répertoire ~/**MyPlaybooks**/.

Procédure

1. Pour stocker les sauvegardes, créez un sous-répertoire dans votre répertoire personnel sur le contrôleur Ansible.

```
$ mkdir ~/ipabackups
```

2. Naviguez jusqu'au répertoire ~/**MyPlaybooks**/:

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

3. Faites une copie du fichier **backup-server-to-controller.yml** situé dans le répertoire /**usr**/**share**/**doc**/**ansible-freeipa**/**playbooks**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/backup-server-to-controller.yml backup-my-server-to-my-controller.yml
```

4. Ouvrez le fichier **backup-my-server-to-my-controller.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes :
   a. Définissez la variable **hosts** sur un groupe d'hôtes de votre fichier d'inventaire. Dans cet exemple, il s'agit du groupe d'hôtes **ipaserver**.
   b. *(Optional)* Pour conserver une copie de la sauvegarde sur le serveur IdM, décommentez la ligne suivante :

```
# ipabackup_keep_on_server: yes
```

6. Par défaut, les sauvegardes sont stockées dans le répertoire de travail actuel du contrôleur Ansible. Pour spécifier le répertoire de sauvegarde que vous avez créé à l'étape 1, ajoutez la variable **ipabackup_controller_path** et définissez-la sur le répertoire /**home**/**user**/**ipabackups**.

```
---
- name: Playbook to backup IPA server to controller
  hosts: ipaserver
  become: true
  vars:
    ipabackup_to_controller: yes
    # ipabackup_keep_on_server: yes
    ipabackup_controller_path: /home/user/ipabackups

  roles:
  - role: ipabackup
    state: present
```

7. Enregistrer le fichier.
8. Exécutez le playbook Ansible, en spécifiant le fichier d'inventaire et le fichier du playbook :

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory
backup-my-server-to-my-controller.yml
```

Verification steps

- Vérifiez que la sauvegarde se trouve dans le répertoire **/home/user/ipabackups** de votre contrôleur Ansible :

```
[user@controller ~]$ ls /home/user/ipabackups
server.idm.example.com_ipa-full-2021-04-30-13-12-00
```

Ressources supplémentaires

- Pour plus d'exemples de playbooks Ansible qui utilisent le rôle **ipabackup**, voir :
  - Le fichier **README.md** dans le répertoire **/usr/share/doc/ansible-freeipa/roles/ipabackup**.
  - Le répertoire **/usr/share/doc/ansible-freeipa/playbooks/**.

9.3. UTILISER ANSIBLE POUR COPIER UNE SAUVEGARDE D'UN SERVEUR IDM SUR VOTRE CONTRÔLEUR ANSIBLE

La procédure suivante décrit comment utiliser un playbook Ansible pour copier une sauvegarde d'un serveur IdM depuis le serveur IdM vers votre contrôleur Ansible.

Conditions préalables

- 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 paquetage **ansible-freeipa**.
  - Vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM sur lequel vous configurez ces options.
  - Votre fichier d'inventaire Ansible est situé dans le répertoire ~/**MyPlaybooks**/.

Procédure

1. Pour stocker les sauvegardes, créez un sous-répertoire dans votre répertoire personnel sur le contrôleur Ansible.

```
$ mkdir ~/ipabackups
```

2. Naviguez jusqu'au répertoire ~/**MyPlaybooks**/:

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

3. Faites une copie du fichier **copy-backup-from-server.yml** situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/copy-backup-from-server.yml copy-backup-from-my-server-to-my-controller.yml
```

4. Ouvrez le fichier **copy-my-backup-from-my-server-to-my-controller.yml** pour le modifier.

5. Adaptez le fichier en définissant les variables suivantes :

   a. Définissez la variable **hosts** sur un groupe d'hôtes de votre fichier d'inventaire. Dans cet exemple, il s'agit du groupe d'hôtes **ipaserver**.

   b. Définissez la variable **ipabackup_name** avec le nom de **ipabackup** sur votre serveur IdM à copier dans votre contrôleur Ansible.

   c. Par défaut, les sauvegardes sont stockées dans le répertoire de travail actuel du contrôleur Ansible. Pour spécifier le répertoire que vous avez créé à l'étape 1, ajoutez la variable **ipabackup_controller_path** et définissez-la sur le répertoire **/home/user/ipabackups**.

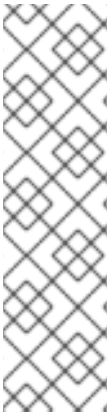
```
---
- name: Playbook to copy backup from IPA server
  hosts: ipaserver
  become: true
  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00
    ipabackup_to_controller: yes
    ipabackup_controller_path: /home/user/ipabackups

  roles:
  - role: ipabackup
    state: present
```

6. Enregistrer le fichier.

7. Exécutez le playbook Ansible, en spécifiant le fichier d'inventaire et le fichier du playbook :

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory copy-backup-from-my-server-to-my-controller.yml
```



NOTE

Pour copier les sauvegardes de **all** IdM sur votre contrôleur, définissez la variable **ipabackup_name** dans Ansible playbook à **all**:

```
vars:
  ipabackup_name: all
  ipabackup_to_controller: yes
```

Pour un exemple, voir le playbook Ansible **copy-all-backups-from-server.yml** dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks**.

Verification steps

- Vérifiez que votre sauvegarde se trouve dans le répertoire **/home/user/ipabackups** sur votre contrôleur Ansible :

```
[user@controller ~]$ ls /home/user/ipabackups
server.idm.example.com_ipa-full-2021-04-30-13-12-00
```

Ressources supplémentaires

- Le fichier **README.md** dans le répertoire **/usr/share/doc/ansible-freeipa/roles/ipabackup**.
- Le répertoire **/usr/share/doc/ansible-freeipa/playbooks/**.

9.4. UTILISATION D'ANSIBLE POUR COPIER UNE SAUVEGARDE D'UN SERVEUR IDM DEPUIS VOTRE CONTRÔLEUR ANSIBLE VERS LE SERVEUR IDM

La procédure suivante décrit comment utiliser un playbook Ansible pour copier une sauvegarde d'un serveur IdM depuis votre contrôleur Ansible vers le serveur IdM.

Conditions préalables

- 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 paquetage **ansible-freeipa**.
  - Vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM sur lequel vous configurez ces options.

- Votre fichier d'inventaire Ansible est situé dans le répertoire ~/**MyPlaybooks**/.

Procédure

1. Naviguez jusqu'au répertoire ~/**MyPlaybooks**/:

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

2. Faites une copie du fichier **copy-backup-from-controller.yml** situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/copy-backup-from-controller.yml copy-backup-from-my-controller-to-my-server.yml
```

3. Ouvrez le fichier **copy-my-backup-from-my-controller-to-my-server.yml** pour le modifier.

4. Adaptez le fichier en définissant les variables suivantes :

   a. Définissez la variable **hosts** sur un groupe d'hôtes de votre fichier d'inventaire. Dans cet exemple, il s'agit du groupe d'hôtes **ipaserver**.

   b. Définissez la variable **ipabackup_name** avec le nom de **ipabackup** sur votre contrôleur Ansible à copier sur le serveur IdM.

```
---
- name: Playbook to copy a backup from controller to the IPA server
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: server.idm.example.com_ipa-full-2021-04-30-13-12-00
    ipabackup_from_controller: yes

  roles:
  - role: ipabackup
    state: copied
```

5. Enregistrer le fichier.

6. Exécutez le playbook Ansible, en spécifiant le fichier d'inventaire et le fichier du playbook :

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory copy-backup-from-my-controller-to-my-server.yml
```

Ressources supplémentaires

- Le fichier **README.md** dans le répertoire **/usr/share/doc/ansible-freeipa/roles/ipabackup**.
- Le répertoire **/usr/share/doc/ansible-freeipa/playbooks/**.

9.5. UTILISER ANSIBLE POUR SUPPRIMER UNE SAUVEGARDE D'UN SERVEUR IDM

La procédure suivante décrit comment utiliser un playbook Ansible pour supprimer une sauvegarde d'un serveur IdM.

Conditions préalables

- 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 paquetage **ansible-freeipa**.
  - Vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM sur lequel vous configurez ces options.
  - Votre fichier d'inventaire Ansible est situé dans le répertoire ~/**MyPlaybooks**/.

Procédure

1. Naviguez jusqu'au répertoire ~/MyPlaybooks/ :

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

2. Faites une copie du fichier **remove-backup-from-server.yml** situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/remove-backup-from-server.yml remove-backup-from-my-server.yml
```

3. Ouvrez le fichier **remove-backup-from-my-server.yml** pour le modifier.
4. Adaptez le fichier en définissant les variables suivantes :
   a. Définissez la variable **hosts** sur un groupe d'hôtes de votre fichier d'inventaire. Dans cet exemple, il s'agit du groupe d'hôtes **ipaserver**.
   b. Attribuez à la variable **ipabackup_name** le nom du site **ipabackup** à supprimer de votre serveur IdM.

```
---
- name: Playbook to remove backup from IPA server
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00
```

```
roles:
- role: ipabackup
  state: absent
```

5. Enregistrer le fichier.

6. Exécutez le playbook Ansible, en spécifiant le fichier d'inventaire et le fichier du playbook :

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory
remove-backup-from-my-server.yml
```

NOTE

Pour supprimer les sauvegardes **all** IdM du serveur IdM, définissez la variable **ipabackup_name** dans le carnet de commande Ansible à **all**:

```
vars:
  ipabackup_name: all
```

Pour un exemple, voir le playbook Ansible **remove-all-backups-from-server.yml** dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks**.

Ressources supplémentaires

- Le fichier **README.md** dans le répertoire **/usr/share/doc/ansible-freeipa/roles/ipabackup**.
- Le répertoire **/usr/share/doc/ansible-freeipa/playbooks/**.

9.6. UTILISER ANSIBLE POUR RESTAURER UN SERVEUR IDM À PARTIR D'UNE SAUVEGARDE STOCKÉE SUR LE SERVEUR

La procédure suivante décrit comment utiliser un playbook Ansible pour restaurer un serveur IdM à partir d'une sauvegarde stockée sur cet hôte.

Conditions préalables

- 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 paquetage **ansible-freeipa**.

- Vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM sur lequel vous configurez ces options.
- Votre fichier d'inventaire Ansible est situé dans le répertoire ~/**MyPlaybooks**/.

- Vous connaissez le mot de passe du gestionnaire de répertoire LDAP.

Procédure

1. Naviguez jusqu'au répertoire ~/**MyPlaybooks**/:

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

2. Faites une copie du fichier **restore-server.yml** situé dans le répertoire /**usr**/**share**/**doc**/**ansible-freeipa**/**playbooks**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/restore-server.yml restore-my-server.yml
```

3. Ouvrez le fichier **restore-my-server.yml** Ansible playbook pour l'éditer.
4. Adaptez le fichier en définissant les variables suivantes :
   a. Définissez la variable **hosts** sur un groupe d'hôtes de votre fichier d'inventaire. Dans cet exemple, il s'agit du groupe d'hôtes **ipaserver**.
   b. Attribuez à la variable **ipabackup_name** le nom du site **ipabackup** à restaurer.
   c. Définissez la variable **ipabackup_password** avec le mot de passe du gestionnaire d'annuaire LDAP.

```
---
- name: Playbook to restore an IPA server
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00
    ipabackup_password: <your_LDAP_DM_password>

  roles:
  - role: ipabackup
    state: restored
```

5. Enregistrer le fichier.
6. Exécutez le playbook Ansible en spécifiant le fichier d'inventaire et le fichier du playbook :

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory
restore-my-server.yml
```

Ressources supplémentaires

- Le fichier **README.md** dans le répertoire /**usr**/**share**/**doc**/**ansible-freeipa**/**roles**/**ipabackup**.
- Le répertoire /**usr**/**share**/**doc**/**ansible-freeipa**/**playbooks**/.

9.7. UTILISER ANSIBLE POUR RESTAURER UN SERVEUR IDM À PARTIR D'UNE SAUVEGARDE STOCKÉE SUR VOTRE CONTRÔLEUR ANSIBLE

La procédure suivante décrit comment utiliser un playbook Ansible pour restaurer un serveur IdM à partir d'une sauvegarde stockée sur votre contrôleur Ansible.

Conditions préalables

- 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 paquetage **ansible-freeipa**.
  - Vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM sur lequel vous configurez ces options.
  - Votre fichier d'inventaire Ansible est situé dans le répertoire ~/**MyPlaybooks**/.
- Vous connaissez le mot de passe du gestionnaire de répertoire LDAP.

Procédure

1. Naviguez jusqu'au répertoire ~/**MyPlaybooks**/:

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

2. Faites une copie du fichier **restore-server-from-controller.yml** situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/restore-server-from-controller.yml restore-my-server-from-my-controller.yml
```

3. Ouvrez le fichier **restore-my-server-from-my-controller.yml** pour le modifier.
4. Adaptez le fichier en définissant les variables suivantes :
   a. Définissez la variable **hosts** sur un groupe d'hôtes de votre fichier d'inventaire. Dans cet exemple, il s'agit du groupe d'hôtes **ipaserver**.
   b. Attribuez à la variable **ipabackup_name** le nom du site **ipabackup** à restaurer.
   c. Définissez la variable **ipabackup_password** avec le mot de passe du gestionnaire d'annuaire LDAP.

```
---
- name: Playbook to restore IPA server from controller
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: server.idm.example.com_ipa-full-2021-04-30-13-12-00
    ipabackup_password: <your_LDAP_DM_password>
    ipabackup_from_controller: yes

  roles:
  - role: ipabackup
    state: restored
```

5. Enregistrer le fichier.

6. Exécutez le playbook Ansible, en spécifiant le fichier d'inventaire et le fichier du playbook :

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory
restore-my-server-from-my-controller.yml
```

Ressources supplémentaires

- Le fichier **README.md** dans le répertoire **/usr/share/doc/ansible-freeipa/roles/ipabackup**.
- Le répertoire **/usr/share/doc/ansible-freeipa/playbooks/**.

CHAPITRE 10. INTÉGRATION DE L'IDM AVEC D'AUTRES PRODUITS RED HAT

Cette section fournit des liens vers la documentation d'autres produits Red Hat qui s'intègrent à IdM. Vous pouvez configurer ces produits pour permettre aux utilisateurs de l'IdM d'accéder à leurs services.

Plate-forme d'automatisation Ansible

Configuration de l'authentification LDAP

OpenShift Container Platform

Configuration d'un fournisseur d'identité LDAP

Plate-forme OpenStack

Intégration d'OpenStack Identity (keystone) avec Red Hat Identity Manager (IdM)

Satellite

Utilisation de Red Hat Identity Management

Signature unique

Intégration de SSSD et de FreeIPA Identity Management

Virtualisation

Configuration d'un fournisseur LDAP externe

CHAPITRE 11. CONFIGURATION DE L'AUTHENTIFICATION UNIQUE POUR LA CONSOLE WEB RHEL 9 DANS LE DOMAINE IDM

Apprenez à utiliser l'authentification unique (SSO) fournie par Identity Management (IdM) dans la console web RHEL 9.

Avantages :

- Les administrateurs de domaines IdM peuvent utiliser la console web RHEL 9 pour gérer les machines locales.
- Les utilisateurs disposant d'un ticket Kerberos dans le domaine IdM n'ont pas besoin de fournir d'identifiants de connexion pour accéder à la console web.
- Tous les hôtes connus du domaine IdM sont accessibles via SSH à partir de l'instance locale de la console web RHEL 9.
- La configuration du certificat n'est pas nécessaire. Le serveur web de la console bascule automatiquement sur un certificat émis par l'autorité de certification IdM et accepté par les navigateurs.

Ce chapitre couvre les étapes suivantes pour configurer le SSO pour la connexion à la console web RHEL :

1. Ajouter des machines au domaine IdM à l'aide de la console web RHEL 9.
   Pour plus d'informations, voir Joindre un système RHEL 9 à un domaine IdM à l'aide de la console Web.
2. Si vous souhaitez utiliser Kerberos pour l'authentification, vous devez obtenir un ticket Kerberos sur votre machine.
   Pour plus d'informations, voir Connexion à la console web à l'aide de l'authentification Kerberos .
3. Permet aux administrateurs du serveur IdM d'exécuter n'importe quelle commande sur n'importe quel hôte.
   Pour plus de détails, voir Activation de l'accès sudo aux administrateurs de domaine sur le serveur IdM

Conditions préalables

- La console web RHEL installée sur les systèmes RHEL 9.
  Pour plus de détails, voir Installation de la console web.
- Client IdM installé sur les systèmes dotés de la console web RHEL.
  Pour plus de détails, voir l'installation du client IdM.

11.1. JOINDRE UN SYSTÈME RHEL 9 À UN DOMAINE IDM À L'AIDE DE LA CONSOLE WEB

Vous pouvez utiliser la console Web pour joindre le système Red Hat Enterprise Linux 9 au domaine Identity Management (IdM).

Conditions préalables

- Le domaine IdM est en cours d'exécution et accessible à partir du client que vous souhaitez rejoindre.
- Vous disposez des informations d'identification de l'administrateur du domaine IdM.

Procédure

1. Connectez-vous à la console web RHEL.
   Pour plus de détails, voir Connexion à la console web .
2. Dans le champ **Configuration** de l'onglet **Overview**, cliquez sur **Join Domain**.
3. Dans la boîte de dialogue **Join a Domain**, entrez le nom d'hôte du serveur IdM dans le champ **Domain Address**.
4. Dans le champ **Domain administrator name**, entrez le nom d'utilisateur du compte d'administration IdM.
5. Dans le site **Domain administrator password**, ajoutez un mot de passe.
6. Cliquez sur **Join**.

Verification steps

1. Si la console web RHEL 9 n'a pas affiché d'erreur, le système a été joint au domaine IdM et vous pouvez voir le nom du domaine dans l'écran **System**.
2. Pour vérifier que l'utilisateur est membre du domaine, cliquez sur la page Terminal et tapez la commande **id**:

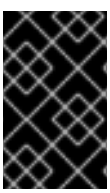
```
$ id
euid=548800004(example_user) gid=548800004(example_user)
groups=548800004(example_user) context=unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023
```

Ressources supplémentaires

- Planification de la gestion de l'identité
- Installation de la gestion des identités
- Gestion des utilisateurs, des groupes, des hôtes et des règles de contrôle d'accès de l'IdM

11.2. SE CONNECTER À LA CONSOLE WEB EN UTILISANT L'AUTHENTIFICATION KERBEROS

La procédure suivante décrit les étapes à suivre pour configurer le système RHEL 9 afin d'utiliser l'authentification Kerberos.



IMPORTANT

Avec SSO, vous n'avez généralement pas de privilèges administratifs dans la console web. Cela ne fonctionne que si vous avez configuré sudo sans mot de passe. La console web ne demande pas de mot de passe sudo de manière interactive.

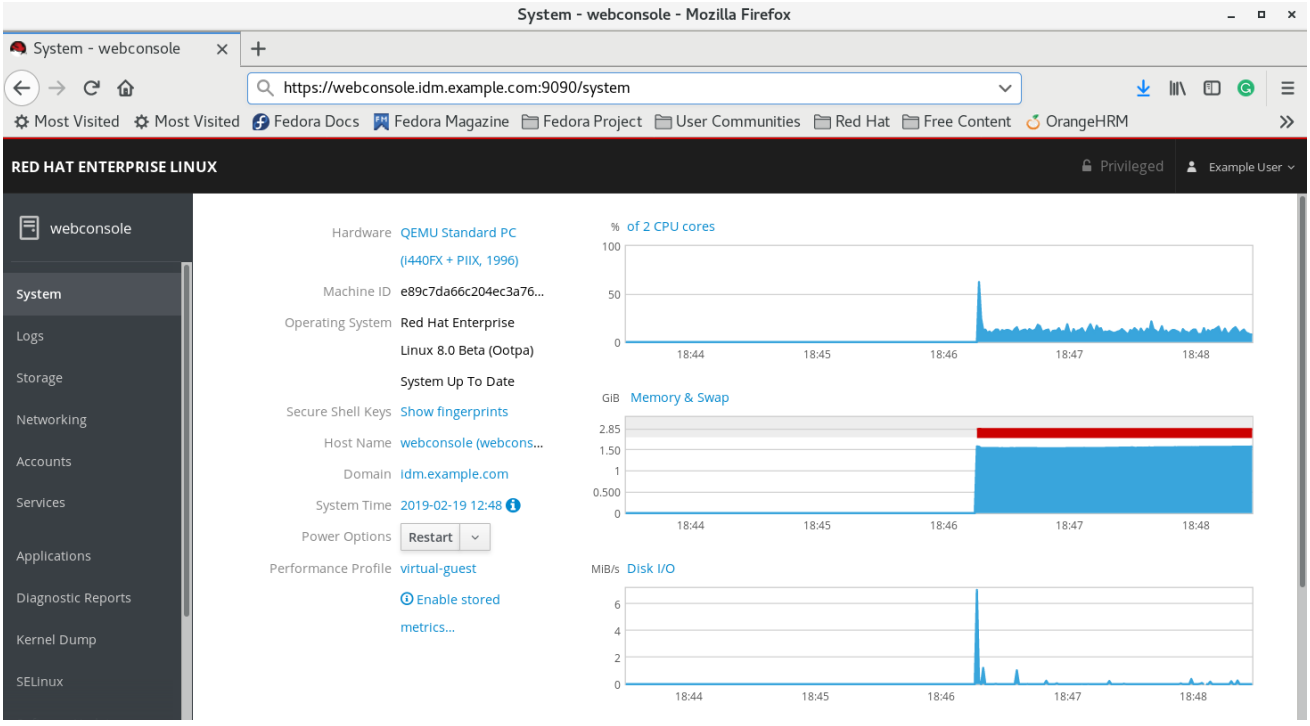
Conditions préalables

- Le domaine IdM fonctionne et est accessible dans l'environnement de votre entreprise. Pour plus d'informations, voir Joindre un système RHEL 9 à un domaine IdM à l'aide de la console Web.
- Activez le service **cockpit.socket** sur les systèmes distants auxquels vous souhaitez vous connecter et les gérer à l'aide de la console Web RHEL. Pour plus de détails, voir Installation de la console web .
- Si le système n'utilise pas de ticket Kerberos géré par le client SSSD, essayez de demander manuellement le ticket à l'aide de l'utilitaire **kinit**.

Procédure

Connectez-vous à la console web RHEL avec l'adresse suivante : **https://dns_name:9090**.

À ce stade, vous êtes connecté avec succès à la console web RHEL et vous pouvez commencer la configuration.



11.3. ACTIVATION DE L'ACCÈS SUDO AUX ADMINISTRATEURS DE DOMAINE SUR LE SERVEUR IDM

La procédure suivante décrit les étapes à suivre pour permettre aux administrateurs de domaine d'exécuter n'importe quelle commande sur n'importe quel hôte du domaine Identity Management (IdM).

Pour ce faire, activez l'accès sudo au groupe d'utilisateurs **admins** créé automatiquement lors de l'installation du serveur IdM.

Tous les utilisateurs ajoutés au groupe **admins** auront un accès sudo si vous exécutez le script **ipa-advise** sur le groupe.

Conditions préalables

- Le serveur utilise IdM 4.7.1 ou une version ultérieure.

Procédure

1. Se connecter au serveur IdM.
2. Exécutez le script ipa-advise :

```
$ ipa-advise enable-admins-sudo | sh -ex
```

Si la console n'affiche pas d'erreur, le groupe **admins** dispose des droits d'administration sur toutes les machines du domaine IdM.

CHAPITRE 12. SUPPORT RFC POUR LE SERVEUR D'ANNUAIRE IDM

Le composant Serveur d'annuaire de la gestion des identités (IdM) prend en charge de nombreuses demandes de commentaires (RFC) relatives à LDAP. Pour plus d'informations, voir Prise en charge des RFC par le serveur d'annuaire.

Ressources supplémentaires

- Guide de déploiement de Directory Server 11