Red Hat Enterprise Linux 9

Installation de la gestion des identités

Méthodes d'installation des serveurs et clients IdM

Last Updated: 2024-02-20

Red Hat Enterprise Linux 9 Installation de la gestion des identités

Méthodes d'installation des serveurs et clients IdM

Notice légale

Résumé

En fonction de votre environnement, vous pouvez installer Red Hat Identity Management (IdM) pour fournir des services DNS et d'autorité de certification (CA), ou vous configurez IdM pour utiliser une infrastructure DNS et CA existante. Vous pouvez installer les serveurs IdM, les répliques et les clients manuellement ou à l'aide des Playbooks Ansible. En outre, vous pouvez utiliser un fichier Kickstart pour joindre automatiquement un client à un domaine IdM pendant l'installation du système.

Table des matières

RENDRE L'OPEN SOURCE PLUS INCLUSIF 6

FOURNIR UN RETOUR D'INFORMATION SUR LA DOCUMENTATION DE RED HAT 7

CHAPITRE 1. PRÉPARATION DU SYSTÈME POUR L'INSTALLATION DU SERVEUR IDM 8
1.1. CONDITIONS PRÉALABLES 8
1.2. RECOMMANDATIONS EN MATIÈRE DE MATÉRIEL 8
1.3. EXIGENCES DE CONFIGURATION PERSONNALISÉE POUR IDM 8
1.4. EXIGENCES EN MATIÈRE DE SERVICES HORAIRES POUR L'IDM 11
1.5. EXIGENCES EN MATIÈRE DE NOM D'HÔTE ET DE DNS POUR L'IDM 13
1.6. EXIGENCES EN MATIÈRE DE PORT POUR L'IDM 16
1.7. OUVERTURE DES PORTS NÉCESSAIRES À L'IDM 17
1.8. INSTALLATION DES PAQUETS REQUIS POUR UN SERVEUR IDM 18
1.9. DÉFINITION DU MASQUE DE CRÉATION DU MODE DE FICHIER CORRECT POUR L'INSTALLATION DE L'IDM 19
1.10. VEILLER À CE QUE LES RÈGLES FAPOLICYD NE BLOQUENT PAS L'INSTALLATION DE L'IDM 19
1.11. OPTIONS POUR LES COMMANDES D'INSTALLATION DE L'IDM 20

CHAPITRE 2. INSTALLATION D'UN SERVEUR IDM : AVEC DNS INTÉGRÉ, AVEC UNE AUTORITÉ DE CERTIFICATION INTÉGRÉE COMME AUTORITÉ DE CERTIFICATION RACINE 23
2.1. INSTALLATION INTERACTIVE 23
2.2. INSTALLATION NON INTERACTIVE 25

CHAPITRE 3. INSTALLATION D'UN SERVEUR IDM : AVEC DNS INTÉGRÉ, AVEC UNE AUTORITÉ DE CERTIFICATION EXTERNE COMME AUTORITÉ DE CERTIFICATION RACINE 27
3.1. INSTALLATION INTERACTIVE 27
3.2. DÉPANNAGE : L'INSTALLATION DE L'AUTORITÉ DE CERTIFICATION EXTERNE ÉCHOUE 31

CHAPITRE 4. INSTALLATION D'UN SERVEUR IDM : AVEC DNS INTÉGRÉ, SANS CA 32
4.1. CERTIFICATS REQUIS POUR L'INSTALLATION D'UN SERVEUR IDM SANS AUTORITÉ DE CERTIFICATION 32
4.2. INSTALLATION INTERACTIVE 34

CHAPITRE 5. INSTALLATION D'UN SERVEUR IDM : SANS DNS INTÉGRÉ, AVEC UNE AUTORITÉ DE CERTIFICATION INTÉGRÉE COMME AUTORITÉ DE CERTIFICATION RACINE 37
5.1. INSTALLATION INTERACTIVE 37
5.2. INSTALLATION NON INTERACTIVE 38
5.3. ENREGISTREMENTS DNS DE L'IDM POUR LES SYSTÈMES DNS EXTERNES 39

CHAPITRE 6. INSTALLATION D'UN SERVEUR IDM : SANS DNS INTÉGRÉ, AVEC UNE AUTORITÉ DE CERTIFICATION EXTERNE COMME AUTORITÉ DE CERTIFICATION RACINE 41
6.1. OPTIONS UTILISÉES LORS DE L'INSTALLATION D'UNE AUTORITÉ DE CERTIFICATION IDM AVEC UNE AUTORITÉ DE CERTIFICATION EXTERNE EN TANT QU'AUTORITÉ DE CERTIFICATION RACINE 41
6.2. INSTALLATION INTERACTIVE 42
6.3. INSTALLATION NON INTERACTIVE 45
6.4. ENREGISTREMENTS DNS DE L'IDM POUR LES SYSTÈMES DNS EXTERNES 47

CHAPITRE 7. INSTALLATION D'UN SERVEUR IDM OU D'UN RÉPLICA AVEC DES PARAMÈTRES DE BASE DE DONNÉES PERSONNALISÉS À PARTIR D'UN FICHIER LDIF 48

CHAPITRE 8. DÉPANNAGE DE L'INSTALLATION DU SERVEUR IDM 49
8.1. EXAMEN DES JOURNAUX D'ERREUR DE L'INSTALLATION DU SERVEUR IDM 49
8.2. EXAMEN DES ERREURS D'INSTALLATION DE L'AUTORITÉ DE CERTIFICATION IDM 50
8.3. SUPPRESSION D'UNE INSTALLATION PARTIELLE DU SERVEUR IDM 51
8.4. RESSOURCES SUPPLÉMENTAIRES 52

CHAPITRE 9. DÉSINSTALLATION D'UN SERVEUR IDM 54

CHAPITRE 10. RENOMMER UN SERVEUR IDM 57

CHAPITRE 11. MISE À JOUR ET RÉTROGRADATION DE L'IDM 58
11.1. MISE À JOUR DES PAQUETS IDM 58
11.2. RÉTROGRADATION DES PAQUETS IDM 58
11.3. RESSOURCES SUPPLÉMENTAIRES 58

CHAPITRE 12. PRÉPARATION DU SYSTÈME POUR L'INSTALLATION DU CLIENT IDM 59
12.1. EXIGENCES DNS POUR LES CLIENTS IDM 59
12.2. EXIGENCES EN MATIÈRE DE PORT POUR LES CLIENTS IDM 59
12.3. EXIGENCES IPV6 POUR LES CLIENTS IDM 59
12.4. INSTALLATION DES PAQUETS REQUIS POUR UN CLIENT IDM 60

CHAPITRE 13. INSTALLATION D'UN CLIENT IDM 61
13.1. CONDITIONS PRÉALABLES 61
13.2. INSTALLATION D'UN CLIENT À L'AIDE DES INFORMATIONS D'IDENTIFICATION DE L'UTILISATEUR : INSTALLATION INTERACTIVE 61
13.3. INSTALLATION D'UN CLIENT À L'AIDE D'UN MOT DE PASSE À USAGE UNIQUE : INSTALLATION INTERACTIVE 63
13.4. INSTALLATION D'UN CLIENT : INSTALLATION NON INTERACTIVE 65
13.5. SUPPRESSION DE LA CONFIGURATION PRÉ-IDM APRÈS L'INSTALLATION D'UN CLIENT 66
13.6. TEST D'UN CLIENT IDM 66
13.7. CONNEXIONS EFFECTUÉES LORS DE L'INSTALLATION D'UN CLIENT IDM 67
13.8. LES COMMUNICATIONS DU CLIENT IDM AVEC LE SERVEUR PENDANT LE DÉPLOIEMENT POST-INSTALLATION 68
13.9. MODÈLES DE COMMUNICATION SSSD 68
13.10. MODÈLES DE COMMUNICATION DE CERTMONGER 70

CHAPITRE 14. INSTALLATION D'UN CLIENT IDM AVEC KICKSTART 72
14.1. INSTALLATION D'UN CLIENT AVEC KICKSTART 72
14.2. FICHIER DE DÉMARRAGE POUR L'INSTALLATION DU CLIENT 72
14.3. TEST D'UN CLIENT IDM 73

CHAPITRE 15. DÉPANNAGE DE L'INSTALLATION DU CLIENT IDM 74
15.1. EXAMEN DES ERREURS D'INSTALLATION DU CLIENT IDM 74
15.2. RÉSOLUTION DES PROBLÈMES SI L'INSTALLATION DU CLIENT NE PARVIENT PAS À METTRE À JOUR LES ENREGISTREMENTS DNS 74
15.3. RÉSOLUTION DES PROBLÈMES SI L'INSTALLATION DU CLIENT NE PARVIENT PAS À REJOINDRE LA ZONE KERBEROS IDM 75
15.4. RESSOURCES SUPPLÉMENTAIRES 76

CHAPITRE 16. RÉINSCRIPTION D'UN CLIENT IDM 77
16.1. RÉINSCRIPTION DU CLIENT À L'IDM 77
16.2. RÉINSCRIPTION D'UN CLIENT À L'AIDE DES INFORMATIONS D'IDENTIFICATION DE L'UTILISATEUR : RÉINSCRIPTION INTERACTIVE 77
16.3. RÉINSCRIPTION D'UN CLIENT À L'AIDE DE LA BASE DE DONNÉES DU CLIENT : RÉINSCRIPTION NON INTERACTIVE 78
16.4. TEST D'UN CLIENT IDM 78

CHAPITRE 17. DÉSINSTALLATION D'UN CLIENT IDM 80
17.1. DÉSINSTALLATION D'UN CLIENT IDM 80
17.2. DÉSINSTALLATION D'UN CLIENT IDM : ÉTAPES SUPPLÉMENTAIRES APRÈS PLUSIEURS INSTALLATIONS ANTÉRIEURES 81

CHAPITRE 18. RENOMMER LES SYSTÈMES CLIENTS IDM 83

18.1. PRÉPARATION D'UN CLIENT IDM POUR SON RENOMMAGE 83
18.2. DÉSINSTALLATION D'UN CLIENT IDM 84
18.3. DÉSINSTALLATION D'UN CLIENT IDM : ÉTAPES SUPPLÉMENTAIRES APRÈS PLUSIEURS INSTALLATIONS ANTÉRIEURES 85
18.4. RENOMMER LE SYSTÈME HÔTE 86
18.5. RÉINSTALLATION D'UN CLIENT IDM 86
18.6. RÉAJUSTEMENT DES SERVICES, RE-GÉNÉRATION DES CERTIFICATS ET RÉAJUSTEMENT DES GROUPES D'HÔTES 86

CHAPITRE 19. PRÉPARATION DU SYSTÈME POUR L'INSTALLATION D'UNE RÉPLIQUE IDM 87
19.1. EXIGENCES RELATIVES À LA VERSION RÉPLIQUÉE 87
19.2. MÉTHODES D'AFFICHAGE DE LA VERSION DU LOGICIEL IDM 87
19.3. ASSURER LA CONFORMITÉ FIPS D'UNE RÉPLIQUE RHEL 9 REJOIGNANT UN ENVIRONNEMENT IDM RHEL 8 88
19.4. AUTORISER L'INSTALLATION D'UNE RÉPLIQUE SUR UN CLIENT IDM 89
19.5. AUTORISER L'INSTALLATION D'UNE RÉPLIQUE SUR UN SYSTÈME QUI N'EST PAS ENRÔLÉ DANS IDM 90

CHAPITRE 20. INSTALLATION D'UNE RÉPLIQUE IDM 92
20.1. INSTALLATION D'UNE RÉPLIQUE IDM AVEC DNS INTÉGRÉ ET UNE AUTORITÉ DE CERTIFICATION 92
20.2. INSTALLATION D'UNE RÉPLIQUE IDM AVEC DNS INTÉGRÉ ET SANS AUTORITÉ DE CERTIFICATION 94
20.3. INSTALLATION D'UNE RÉPLIQUE IDM SANS DNS INTÉGRÉ ET AVEC UNE AC 94
20.4. INSTALLATION D'UNE RÉPLIQUE IDM SANS DNS INTÉGRÉ ET SANS AUTORITÉ DE CERTIFICATION 95
20.5. INSTALLATION D'UNE RÉPLIQUE CACHÉE DE L'IDM 96
20.6. TEST D'UNE RÉPLIQUE IDM 97
20.7. CONNEXIONS EFFECTUÉES LORS DE L'INSTALLATION D'UNE RÉPLIQUE IDM 97

CHAPITRE 21. DÉPANNAGE DE L'INSTALLATION DES RÉPLIQUES IDM 99
21.1. FICHIERS JOURNAUX DES ERREURS D'INSTALLATION DE LA RÉPLIQUE IDM 99
21.2. EXAMEN DES ERREURS D'INSTALLATION DES RÉPLIQUES IDM 99
21.3. FICHIERS JOURNAUX DES ERREURS D'INSTALLATION DE L'AUTORITÉ DE CERTIFICATION IDM 101
21.4. EXAMEN DES ERREURS D'INSTALLATION DE L'AUTORITÉ DE CERTIFICATION IDM 102
21.5. SUPPRESSION D'UNE INSTALLATION PARTIELLE DE RÉPLIQUE IDM 102
21.6. RÉSOUDRE LES ERREURS LIÉES AUX INFORMATIONS D'IDENTIFICATION NON VALIDES 104
21.7. RESSOURCES SUPPLÉMENTAIRES 105

CHAPITRE 22. DÉSINSTALLATION D'UNE RÉPLIQUE IDM 106

CHAPITRE 23. GESTION DE LA TOPOLOGIE DE RÉPLICATION 107
23.1. EXPLICATION DES ACCORDS DE RÉPLICATION, DES SUFFIXES DE TOPOLOGIE ET DES SEGMENTS DE TOPOLOGIE 107
23.2. UTILISATION DU GRAPHE TOPOLOGIQUE POUR GÉRER LA TOPOLOGIE DE RÉPLICATION 110
23.3. CONFIGURATION DE LA RÉPLICATION ENTRE DEUX SERVEURS À L'AIDE DE L'INTERFACE WEB 113
23.4. ARRÊT DE LA RÉPLICATION ENTRE DEUX SERVEURS À L'AIDE DE L'INTERFACE WEB 114
23.5. CONFIGURATION DE LA RÉPLICATION ENTRE DEUX SERVEURS À L'AIDE DU CLI 115
23.6. ARRÊT DE LA RÉPLICATION ENTRE DEUX SERVEURS À L'AIDE DE LA CLI 116
23.7. SUPPRESSION D'UN SERVEUR DE LA TOPOLOGIE À L'AIDE DE L'INTERFACE WEB 117
23.8. SUPPRESSION D'UN SERVEUR DE LA TOPOLOGIE À L'AIDE DE LA CLI 118
23.9. VISUALISATION DES RÔLES DE SERVEUR SUR UN SERVEUR IDM À L'AIDE DE L'INTERFACE WEB 119
23.10. VISUALISATION DES RÔLES DE SERVEUR SUR UN SERVEUR IDM À L'AIDE DE LA CLI 119
23.11. PROMOUVOIR UN RÉPLICA EN TANT QUE SERVEUR DE RENOUVELLEMENT DE L'AUTORITÉ DE CERTIFICATION ET SERVEUR D'ÉDITION DE CRL 120
23.12. RÉTROGRADER OU PROMOUVOIR DES RÉPLIQUES CACHÉES 121

CHAPITRE 24. INSTALLATION ET EXÉCUTION DE L'OUTIL IDM HEALTHCHECK 122
24.1. CONTRÔLE DE SANTÉ DANS L'IDM 122
24.2. INSTALLATION DE IDM HEALTHCHECK 123
24.3. EXÉCUTION DU CONTRÔLE DE SANTÉ DE L'IDM 123
24.4. RESSOURCES SUPPLÉMENTAIRES 123

CHAPITRE 25. INSTALLATION D'UN SERVEUR DE GESTION DES IDENTITÉS À L'AIDE D'UN PLAYBOOK ANSIBLE 125
25.1. ANSIBLE ET SES AVANTAGES POUR L'INSTALLATION D'IDM 125
25.2. INSTALLATION DU PAQUET ANSIBLE-FREEIPA 125
25.3. EMPLACEMENT DES RÔLES ANSIBLE DANS LE SYSTÈME DE FICHIERS 126
25.4. PARAMÉTRAGE D'UN DÉPLOIEMENT AVEC UN DNS INTÉGRÉ ET UNE AC INTÉGRÉE EN TANT QU'AC RACINE 127
25.5. PARAMÉTRAGE D'UN DÉPLOIEMENT AVEC DNS EXTERNE ET UNE AUTORITÉ DE CERTIFICATION INTÉGRÉE EN TANT QU'AUTORITÉ DE CERTIFICATION RACINE 130
25.6. DÉPLOIEMENT D'UN SERVEUR IDM AVEC UNE AUTORITÉ DE CERTIFICATION INTÉGRÉE EN TANT QU'AUTORITÉ DE CERTIFICATION RACINE À L'AIDE D'UN PLAYBOOK ANSIBLE 132
25.7. PARAMÉTRAGE D'UN DÉPLOIEMENT AVEC UN DNS INTÉGRÉ ET UNE AUTORITÉ DE CERTIFICATION EXTERNE COMME AUTORITÉ DE CERTIFICATION RACINE 133
25.8. PARAMÉTRAGE D'UN DÉPLOIEMENT AVEC DNS EXTERNE ET UNE AUTORITÉ DE CERTIFICATION EXTERNE EN TANT QU'AUTORITÉ DE CERTIFICATION RACINE 137
25.9. DÉPLOIEMENT D'UN SERVEUR IDM AVEC UNE AUTORITÉ DE CERTIFICATION EXTERNE EN TANT QU'AUTORITÉ DE CERTIFICATION RACINE À L'AIDE D'UN PLAYBOOK ANSIBLE 139

CHAPITRE 26. INSTALLATION D'UNE RÉPLIQUE DE GESTION DES IDENTITÉS À L'AIDE D'UN PLAYBOOK ANSIBLE 142
26.1. SPÉCIFICATION DES VARIABLES DE BASE, DE SERVEUR ET DE CLIENT POUR L'INSTALLATION DE LA RÉPLIQUE IDM 142
26.2. SPÉCIFICATION DES INFORMATIONS D'IDENTIFICATION POUR L'INSTALLATION DE LA RÉPLIQUE IDM À L'AIDE D'UN PLAYBOOK ANSIBLE 146
26.3. DÉPLOIEMENT D'UNE RÉPLIQUE IDM À L'AIDE D'UN PLAYBOOK ANSIBLE 148

CHAPITRE 27. INSTALLATION D'UN CLIENT DE GESTION DES IDENTITÉS À L'AIDE D'UN PLAYBOOK ANSIBLE 149
27.1. DÉFINITION DES PARAMÈTRES DU FICHIER D'INVENTAIRE POUR LE MODE D'INSTALLATION DU CLIENT D'AUTODÉCOUVERTE 149
27.2. DÉFINITION DES PARAMÈTRES DU FICHIER D'INVENTAIRE LORSQUE L'AUTODÉCOUVERTE N'EST PAS POSSIBLE LORS DE L'INSTALLATION DU CLIENT 152
27.3. VÉRIFICATION DES PARAMÈTRES DANS LE FICHIER INSTALL-CLIENT.YML 154
27.4. OPTIONS D'AUTORISATION POUR L'INSCRIPTION D'UN CLIENT IDM À L'AIDE D'UN PLAYBOOK ANSIBLE 154
27.5. DÉPLOIEMENT D'UN CLIENT IDM À L'AIDE D'UN PLAYBOOK ANSIBLE 156
27.6. TEST D'UN CLIENT DE GESTION D'IDENTITÉ APRÈS L'INSTALLATION D'ANSIBLE 157
27.7. DÉSINSTALLATION D'UN CLIENT IDM À L'AIDE D'UN PLAYBOOK ANSIBLE 157

RENDRE L'OPEN SOURCE PLUS INCLUSIF

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

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

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

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

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

Soumettre des commentaires sur des passages spécifiques

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

Soumettre des commentaires via Bugzilla (compte requis)

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

CHAPITRE 1. PRÉPARATION DU SYSTÈME POUR L'INSTALLATION DU SERVEUR IDM

Les sections suivantes énumèrent les conditions requises pour l'installation d'un serveur de gestion des identités (IdM). Avant l'installation, assurez-vous que votre système répond à ces exigences.

1.1. CONDITIONS PRÉALABLES

- Vous devez disposer des privilèges **root** pour installer un serveur de gestion des identités (IdM) sur votre hôte.

1.2. RECOMMANDATIONS EN MATIÈRE DE MATÉRIEL

La mémoire vive est la caractéristique matérielle la plus importante à dimensionner correctement. Assurez-vous que votre système dispose de suffisamment de mémoire vive. Les exigences typiques en matière de RAM sont les suivantes

- Pour 10 000 utilisateurs et 100 groupes : au moins 4 Go de RAM et 4 Go d'espace de pagination
- Pour 100 000 utilisateurs et 50 000 groupes : au moins 16 Go de RAM et 4 Go d'espace d'échange

Pour les déploiements plus importants, il est plus efficace d'augmenter la mémoire vive que l'espace disque, car une grande partie des données est stockée dans la mémoire cache. En général, l'augmentation de la mémoire vive permet d'obtenir de meilleures performances pour les déploiements plus importants grâce à la mise en cache.

NOTE

Une entrée utilisateur de base ou une entrée hôte simple avec un certificat a une taille d'environ 5 à 10 kB.

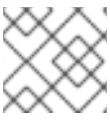
1.3. EXIGENCES DE CONFIGURATION PERSONNALISÉE POUR IDM

Installer un serveur de gestion des identités (IdM) sur un système propre sans aucune configuration personnalisée pour des services tels que DNS, Kerberos, Apache ou Directory Server.

L'installation du serveur IdM écrase les fichiers système pour configurer le domaine IdM. IdM sauvegarde les fichiers système originaux sur **/var/lib/ipa/sysrestore/**. Lorsqu'un serveur IdM est désinstallé à la fin de son cycle de vie, ces fichiers sont restaurés.

1.3.1. Exigences IPv6 pour l'IdM

Le protocole IPv6 doit être activé dans le noyau du système IdM. Si IPv6 est désactivé, le plug-in CLDAP utilisé par les services IdM ne s'initialise pas.



NOTE

Il n'est pas nécessaire d'activer IPv6 sur le réseau.

1.3.2. Prise en charge des types de cryptage dans l'IdM

Red Hat Enterprise Linux (RHEL) utilise la version 5 du protocole Kerberos, qui prend en charge des types de chiffrement tels que Advanced Encryption Standard (AES), Camellia et Data Encryption Standard (DES).

Liste des types de cryptage pris en charge

Alors que les bibliothèques Kerberos sur les serveurs et les clients IdM peuvent supporter plus de types de cryptage, le Centre de Distribution Kerberos IdM (KDC) ne supporte que les types de cryptage suivants :

- **aes256-cts:normal**
- **aes256-cts:special** (par défaut)
- **aes128-cts:normal**
- **aes128-cts:special** (par défaut)
- **aes128-sha2:normal**
- **aes128-sha2:special**
- **aes256-sha2:normal**
- **aes256-sha2:special**
- **camellia128-cts-cmac:normal**
- **camellia128-cts-cmac:special**
- **camellia256-cts-cmac:normal**
- **camellia256-cts-cmac:special**

Les types de cryptage RC4 sont désactivés par défaut

Les types de chiffrement RC4 suivants ont été désactivés par défaut dans RHEL 9, car ils sont considérés comme moins sûrs que les nouveaux types de chiffrement AES-128 et AES-256 :

- **arcfour-hmac:normal**
- **arcfour-hmac:special**

Pour plus d'informations sur l'activation manuelle de la prise en charge de RC4 à des fins de compatibilité avec les anciens environnements Active Directory, voir Assurer la prise en charge des types de chiffrement courants dans AD et RHEL.

La prise en charge du cryptage DES et 3DES a été supprimée

Pour des raisons de sécurité, la prise en charge de l'algorithme DES a été abandonnée dans RHEL 7. Les types de chiffrement Single-DES (DES) et Triple-DES (3DES) ont été supprimés dans RHEL 8 et ne sont pas utilisés dans RHEL 9.

1.3.3. Prise en charge des politiques cryptographiques à l'échelle du système dans l'IdM

IdM utilise la politique cryptographique du système **DEFAULT**. Cette politique offre des paramètres sécurisés pour les modèles de menace actuels. Elle autorise les protocoles TLS 1.2 et 1.3, ainsi que les

protocoles IKEv2 et SSH2. Les clés RSA et les paramètres Diffie-Hellman sont acceptés s'ils ont une longueur d'au moins 2048 bits. Cette politique n'autorise pas les algorithmes DES, 3DES, RC4, DSA, TLS v1.0 et d'autres algorithmes plus faibles.

NOTE

Vous ne pouvez pas installer un serveur IdM tout en utilisant la politique cryptographique du système **FUTURE**. Lors de l'installation d'un serveur IdM, assurez-vous que vous utilisez la politique cryptographique du système **DEFAULT**.

Ressources complémentaires

- Politiques cryptographiques à l'échelle du système

1.3.4. Conformité FIPS

Vous pouvez installer un nouveau serveur IdM ou un réplica sur un système dont le mode FIPS (Federal Information Processing Standard) est activé.

Pour installer IdM avec FIPS, il faut d'abord activer le mode FIPS sur l'hôte, puis installer IdM. Le script d'installation de l'IdM détecte si le mode FIPS est activé et configure l'IdM pour qu'il n'utilise que des types de chiffrement conformes à la norme FIPS 140-3 :

- **aes128-sha2:normal**
- **aes128-sha2:special**
- **aes256-sha2:normal**
- **aes256-sha2:special**

Pour qu'un environnement IdM soit conforme aux normes FIPS, les répliques IdM de **all** doivent avoir le mode FIPS activé.

Red Hat recommande d'activer également FIPS dans les clients IdM, en particulier si vous êtes susceptible de promouvoir ces clients vers des répliques IdM. En fin de compte, c'est aux administrateurs de déterminer comment ils répondent aux exigences FIPS ; Red Hat n'applique pas les critères FIPS.

Prise en charge de la confiance inter-forêts avec le mode FIPS activé

Pour établir une confiance inter-forêts avec un domaine Active Directory (AD) lorsque le mode FIPS est activé, vous devez vous authentifier avec un compte administratif AD. Vous ne pouvez pas établir de confiance à l'aide d'un secret partagé lorsque le mode FIPS est activé.

IMPORTANT

L'authentification RADIUS n'est pas conforme aux normes FIPS. N'installez pas IdM sur un serveur dont le mode FIPS est activé si vous avez besoin d'une authentification RADIUS.

Ressources complémentaires

- Pour activer le mode FIPS dans le système d'exploitation RHEL, voir Passer le système en mode FIPS dans le guide *Security Hardening*.

- Pour plus de détails sur la norme FIPS 140-2, voir les exigences de sécurité pour les modules cryptographiques sur le site web du National Institute of Standards and Technology (NIST).

1.4. EXIGENCES EN MATIÈRE DE SERVICES HORAIRES POUR L'IDM

Les sections suivantes traitent de l'utilisation de **chronyd** pour maintenir vos hôtes IdM synchronisés avec une source de temps centrale :

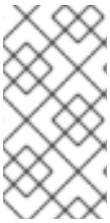
1.4.1. Comment IdM utilise chronyd pour la synchronisation

Cette section traite de l'utilisation de **chronyd** pour maintenir vos hôtes IdM synchronisés avec une source de temps centrale.

Kerberos, le mécanisme d'authentification sous-jacent à IdM, utilise des horodateurs dans le cadre de son protocole. L'authentification Kerberos échoue si l'heure système d'un client IdM diffère de plus de cinq minutes de l'heure système du centre de distribution de clés (KDC).

Pour garantir que les serveurs et les clients IdM restent synchronisés avec une source de temps centrale, les scripts d'installation IdM configurent automatiquement le logiciel client NTP (Network Time Protocol) sur le site **chronyd**.

Si vous ne fournissez aucune option NTP à la commande d'installation de l'IdM, le programme d'installation recherche les enregistrements de service DNS (SRV) de **_ntp._udp** qui pointent vers le serveur NTP de votre réseau et configure **chrony** avec cette adresse IP. Si vous ne disposez pas d'enregistrements SRV pour **_ntp._udp**, **chronyd** utilise la configuration fournie avec le paquet **chrony**.



NOTE

Étant donné que **ntpd** a été abandonné au profit de **chronyd** dans RHEL 8, les serveurs IdM ne sont plus configurés en tant que serveurs NTP (Network Time Protocol) et sont uniquement configurés en tant que clients NTP. Le rôle de serveur IdM de RHEL 7 **NTP Server** a également été supprimé dans RHEL 8.

Ressources supplémentaires

- Mise en œuvre du NTP
- Utilisation de la suite Chrony pour configurer NTP

1.4.2. Liste des options de configuration NTP pour les commandes d'installation IdM

Cette section traite de l'utilisation de **chronyd** pour maintenir vos hôtes IdM synchronisés avec une source de temps centrale.

Vous pouvez spécifier les options suivantes avec n'importe quelle commande d'installation de l'IdM (**ipa-server-install**, **ipa-replica-install**, **ipa-client-install**) pour configurer le logiciel client **chronyd** pendant l'installation.

Tableau 1.1. Liste des options de configuration NTP pour les commandes d'installation IdM

Option	Comportement
--ntp-server	Utilisez-le pour spécifier un serveur NTP. Vous pouvez l'utiliser plusieurs fois pour spécifier plusieurs serveurs.

Option	Comportement
--ntp-pool	Utilisez-le pour spécifier un groupe de plusieurs serveurs NTP résolus sous un seul nom d'hôte.
-N, **--no-ntp**	Ne configurez pas, ne démarrez pas et n'activez pas **chronyd**.

Ressources supplémentaires

- Mise en œuvre du NTP
- Utilisation de la suite Chrony pour configurer NTP

1.4.3. S'assurer que l'IdM peut référencer votre serveur de temps NTP

Cette procédure permet de vérifier que vous avez mis en place les configurations nécessaires pour que l'IdM puisse se synchroniser avec votre serveur de temps NTP (Network Time Protocol).

Conditions préalables

- Vous avez configuré un serveur de temps NTP dans votre environnement. Dans cet exemple, le nom d'hôte du serveur de temps précédemment configuré est **ntpserver.example.com**.

Procédure

1. Effectuez une recherche d'enregistrement de service DNS (SRV) pour les serveurs NTP dans votre environnement.

```
[user@server ~]$ dig +short -t SRV _ntp._udp.example.com
0 100 123 ntpserver.example.com.
```

2. Si la recherche précédente **dig** ne renvoie pas votre serveur de temps, ajoutez un enregistrement SRV **_ntp._udp** qui pointe vers votre serveur de temps sur le port **123**. Ce processus dépend de votre solution DNS.

Verification steps

- Vérifiez que le DNS renvoie une entrée pour votre serveur de temps sur le port **123** lorsque vous effectuez une recherche sur les enregistrements SRV **_ntp._udp**.

```
[user@server ~]$ dig +short -t SRV _ntp._udp.example.com
0 100 123 ntpserver.example.com.
```

Ressources supplémentaires

- Mise en œuvre du NTP
- Utilisation de la suite Chrony pour configurer NTP

1.4.4. Ressources supplémentaires

- Mise en œuvre du NTP
- Utilisation de la suite Chrony pour configurer NTP

1.5. EXIGENCES EN MATIÈRE DE NOM D'HÔTE ET DE DNS POUR L'IDM

Cette section énumère les exigences en matière de nom d'hôte et de DNS pour les systèmes serveur et réplica. Elle indique également comment vérifier que les systèmes répondent à ces exigences.

Les exigences de cette section s'appliquent à tous les serveurs de gestion des identités (IdM), qu'ils soient ou non dotés d'un DNS intégré.

AVERTISSEMENT

Les enregistrements DNS sont essentiels pour presque toutes les fonctions du domaine IdM, y compris l'exécution des services d'annuaire LDAP, Kerberos et l'intégration d'Active Directory. Soyez extrêmement prudent et assurez-vous que

- Vous disposez d'un service DNS testé et fonctionnel
- Le service est correctement configuré

Cette exigence s'applique aux serveurs IdM avec **and** sans DNS intégré.

Vérifier le nom d'hôte du serveur

Le nom d'hôte doit être un nom de domaine entièrement qualifié, tel que ***server.idm.example.com***.

IMPORTANT

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**.

Le nom de domaine pleinement qualifié doit remplir les conditions suivantes :

- Il s'agit d'un nom DNS valide, ce qui signifie que seuls les chiffres, les caractères alphabétiques et les traits d'union (-) sont autorisés. D'autres caractères, tels que les underscores (_), dans le nom d'hôte provoquent des échecs DNS.
- Il s'agit de lettres minuscules. Aucune majuscule n'est autorisée.
- Elle ne se résout pas à l'adresse de bouclage. Il doit être résolu à l'adresse IP publique du système, et non à **127.0.0.1**.

Pour vérifier le nom d'hôte, utilisez l'utilitaire **hostname** sur le système où vous souhaitez effectuer l'installation :

```
# hostname
server.idm.example.com
```

La sortie de **hostname** ne doit pas être **localhost** ou **localhost6**.

Vérifier la configuration du DNS en aval et en amont

1. Obtenir l'adresse IP du serveur.

   a. La commande **ip addr show** affiche les adresses IPv4 et IPv6. Dans l'exemple suivant, l'adresse IPv6 pertinente est **2001:DB8::1111** car sa portée est globale :

```
[root@server ~]# ip addr show
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP group default qlen 1000
 link/ether 00:1a:4a:10:4e:33 brd ff:ff:ff:ff:ff:ff
 inet 192.0.2.1/24 brd 192.0.2.255 scope global dynamic eth0
  valid_lft 106694sec preferred_lft 106694sec
 inet6 2001:DB8::1111/32 scope global dynamic
   valid_lft 2591521sec preferred_lft 604321sec
 inet6 fe80::56ee:75ff:fe2b:def6/64 scope link
        valid_lft forever preferred_lft forever
...
```

2. Vérifiez la configuration du DNS de transmission à l'aide de l'utilitaire **dig**.

   a. Exécutez la commande **dig short *server.idm.example.com* A**. L'adresse IPv4 renvoyée doit correspondre à l'adresse IP renvoyée par **ip addr show**:

```
[root@server ~]# dig +short server.idm.example.com A
192.0.2.1
```

   b. Exécutez la commande **dig short *server.idm.example.com* AAAA**. Si elle renvoie une adresse, elle doit correspondre à l'adresse IPv6 renvoyée par **ip addr show**:

```
[root@server ~]# dig +short server.idm.example.com AAAA
2001:DB8::1111
```

NOTE

Si **dig** ne renvoie aucun résultat pour l'enregistrement AAAA, cela ne signifie pas que la configuration est incorrecte. L'absence de résultat signifie simplement qu'aucune adresse IPv6 n'est configurée dans le DNS pour le système. Si vous n'avez pas l'intention d'utiliser le protocole IPv6 dans votre réseau, vous pouvez poursuivre l'installation dans cette situation.

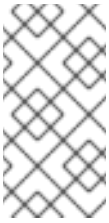
3. Vérifiez la configuration du DNS inverse (enregistrements PTR). Utilisez l'utilitaire **dig** et ajoutez l'adresse IP.
   Si les commandes ci-dessous affichent un nom d'hôte différent ou aucun nom d'hôte, la configuration du reverse DNS est incorrecte.

   a. Exécutez la commande **dig short -x *IPv4_address***. La sortie doit afficher le nom d'hôte du serveur. Par exemple :

```
[root@server ~]# dig +short -x 192.0.2.1
server.idm.example.com
```

b. Si la commande **dig short -x *server.idm.example.com* AAAA** de l'étape précédente a renvoyé une adresse IPv6, utilisez **dig** pour interroger également l'adresse IPv6. La sortie doit afficher le nom d'hôte du serveur. Par exemple :

```
[root@server ~]# dig +short -x 2001:DB8::1111
server.idm.example.com
```



NOTE

Si l'étape précédente **dig short *server.idm.example.com* AAAA** à l'étape précédente n'a pas affiché d'adresse IPv6, l'interrogation de l'enregistrement AAAA n'aboutit à rien. Dans ce cas, il s'agit d'un comportement normal qui n'indique pas une configuration incorrecte.

AVERTISSEMENT

Si une recherche DNS inversée (enregistrement PTR) renvoie plusieurs noms d'hôte, **httpd** et d'autres logiciels associés à IdM peuvent avoir un comportement imprévisible. Red Hat recommande fortement de configurer un seul enregistrement PTR par IP.

Vérifier la conformité aux normes des transitaires DNS (requis uniquement pour le DNS intégré)

Assurez-vous que tous les transitaires DNS que vous souhaitez utiliser avec le serveur DNS IdM sont conformes aux normes Extension Mechanisms for DNS (EDNS0) et DNS Security Extensions (DNSSEC). Pour ce faire, inspectez la sortie de la commande suivante pour chaque transitaire séparément :

```
$ dig dnssec @IP_address_of_the_DNS_forwarder . SOA
```

La sortie attendue affichée par la commande contient les informations suivantes :

- statut : **NOERROR**
- drapeaux : **ra**
- Drapeaux EDNS : **do**
- L'enregistrement **RRSIG** doit être présent dans la section **ANSWER**

Si l'un de ces éléments est absent de la sortie, consultez la documentation de votre transitaire DNS et vérifiez que EDNS0 et DNSSEC sont pris en charge et activés. Dans les dernières versions du serveur BIND, l'option **dnssec-enable yes;** doit être définie dans le fichier **/etc/named.conf**.

Exemple de résultat escompté produit par **dig**:

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48655
```

```
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096

;; ANSWER SECTION:
. 31679 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2015100701 1800 900 604800 86400
. 31679 IN RRSIG SOA 8 0 86400 20151017170000 20151007160000 62530 . GNVz7SQs [...]
```

Vérifier le fichier /etc/hosts

Vérifiez que le fichier **/etc/hosts** remplit l'une des conditions suivantes :

- Le fichier ne contient pas d'entrée pour l'hôte. Il répertorie uniquement les entrées IPv4 et IPv6 localhost de l'hôte.
- Le fichier contient une entrée pour l'hôte et remplit toutes les conditions suivantes :
  - Les deux premières entrées sont les entrées IPv4 et IPv6 localhost.
  - L'entrée suivante spécifie l'adresse IPv4 et le nom d'hôte du serveur IdM.
  - Le site **FQDN** du serveur IdM précède le nom court du serveur IdM.
  - Le nom d'hôte du serveur IdM ne fait pas partie de l'entrée localhost.

  Voici un exemple de fichier **/etc/hosts** correctement configuré :

```
127.0.0.1   localhost localhost.localdomain \
localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain \
localhost6 localhost6.localdomain6
192.0.2.1 server.idm.example.com server
2001:DB8::1111 server.idm.example.com server
```

1.6. EXIGENCES EN MATIÈRE DE PORT POUR L'IDM

Identity Management (IdM) utilise plusieurs ports pour communiquer avec ses services. Ces ports doivent être ouverts et disponibles pour les connexions entrantes vers le serveur IdM pour que ce dernier fonctionne. Ils ne doivent pas être utilisés par un autre service ou bloqués par un pare-feu.

Tableau 1.2. Ports IdM

Service	Ports	Protocol
HTTP/HTTPS	80, 443	TCP
LDAP/LDAPS	389, 636	TCP
Kerberos	88, 464	TCP et UDP
DNS	53	TCP et UDP (en option)

NOTE

IdM utilise les ports 80 et 389. Il s'agit d'une pratique sûre en raison des garanties suivantes :

- L'IdM redirige normalement les demandes qui arrivent sur le port 80 vers le port 443. Le port 80 (HTTP) n'est utilisé que pour fournir des réponses OCSP (Online Certificate Status Protocol) et des listes de révocation de certificats (CRL). Les deux sont signés numériquement et donc protégés contre les attaques de type "man-in-the-middle".
- Le port 389 (LDAP) utilise STARTTLS et Generic Security Services API (GSSAPI) pour le cryptage.

En outre, les ports 8080, 8443 et 749 doivent être libres car ils sont utilisés en interne. N'ouvrez pas ces ports et laissez-les plutôt bloqués par un pare-feu.

Tableau 1.3. firewalld services

Nom du service	Pour plus de détails, voir :
freeipa-ldap	**/usr/lib/firewalld/services/freeipa-ldap.xml**
freeipa-ldaps	**/usr/lib/firewalld/services/freeipa-ldaps.xml**
dns	**/usr/lib/firewalld/services/dns.xml**

1.7. OUVERTURE DES PORTS NÉCESSAIRES À L'IDM

Procédure

1. Vérifiez que le service **firewalld** est en cours d'exécution.
   - Pour savoir si **firewalld** est en cours d'exécution :

     ```
     # systemctl status firewalld.service
     ```

   - Pour démarrer **firewalld** et le configurer pour qu'il démarre automatiquement au démarrage du système :

     ```
     # systemctl start firewalld.service
     # systemctl enable firewalld.service
     ```

2. Ouvrez les ports requis à l'aide de l'utilitaire **firewall-cmd**. Choisissez l'une des options suivantes :
   a. Ajoutez les ports individuels au pare-feu à l'aide de la commande **firewall-cmd --add-port**. Par exemple, pour ouvrir les ports dans la zone par défaut :

      ```
      # firewall-cmd --permanent --add-port=
      {80/tcp,443/tcp,389/tcp,636/tcp,88/tcp,88/udp,464/tcp,464/udp,53/tcp,53/udp}
      ```

b. Ajoutez les services **firewalld** au pare-feu en utilisant la commande **firewall-cmd --add-service**. Par exemple, pour ouvrir les ports dans la zone par défaut :

```
# firewall-cmd --permanent --add-service={freeipa-ldap,freeipa-ldaps,dns}
```

Pour plus de détails sur l'utilisation de **firewall-cmd** pour ouvrir des ports sur un système, voir la page de manuel **firewall-cmd**(1).

3. Rechargez la configuration de **firewall-cmd** pour vous assurer que les modifications sont prises en compte immédiatement :

```
# firewall-cmd --reload
```

Notez que le rechargement de **firewalld** sur un système en production peut entraîner des délais de connexion DNS. Si nécessaire, pour éviter le risque de dépassement de délai et pour rendre les modifications persistantes sur le système en cours d'exécution, utilisez l'option **--runtime-to-permanent** de la commande **firewall-cmd**, par exemple :

```
# firewall-cmd --runtime-to-permanent
```

4. **Optional.** Pour vérifier que les ports sont disponibles dès maintenant, utilisez les utilitaires **nc**, **telnet**, ou **nmap** pour vous connecter à un port ou effectuer un balayage des ports.

NOTE

Notez que vous devez également ouvrir des pare-feu basés sur le réseau pour le trafic entrant et sortant.

1.8. INSTALLATION DES PAQUETS REQUIS POUR UN SERVEUR IDM

La procédure suivante montre comment télécharger les paquets nécessaires à la mise en place de l'environnement IdM de votre choix.

Conditions préalables

- Vous venez d'installer un système RHEL.
- Vous avez mis à disposition les référentiels requis :
  - Si votre système RHEL n'est pas exécuté dans le nuage, vous avez enregistré votre système auprès du Gestionnaire d'abonnements Red Hat (RHSM). Pour plus de détails, voir Enregistrement, attachement et suppression d'abonnements dans la ligne de commande du Gestionnaire d'abonnements. Vous avez également activé les référentiels **BaseOS** et **AppStream** utilisés par IdM :

```
# subscription-manager repos --enable=rhel-9-for-x86_64-baseos-rpms
# subscription-manager repos --enable=rhel-9-for-x86_64-appstream-rpms
```

Pour plus de détails sur l'activation et la désactivation de référentiels spécifiques à l'aide du RHSM, voir Configuration des options dans le Gestionnaire d'abonnements Red Hat .

  - Si votre système RHEL est exécuté dans le nuage, sautez l'enregistrement. Les dépôts requis sont déjà disponibles via l'infrastructure de mise à jour de Red Hat (RHUI).

Procédure

- Choisissez l'une des options suivantes, en fonction de vos besoins en matière d'IdM :
  - Pour télécharger les paquets nécessaires à l'installation d'un serveur IdM sans DNS intégré :

```
# dnf install ipa-server
```

  - Pour télécharger les paquets nécessaires à l'installation d'un serveur IdM avec DNS intégré :

```
# dnf install ipa-server ipa-server-dns
```

  - Pour télécharger les paquets nécessaires à l'installation d'un serveur IdM ayant un accord de confiance avec Active Directory :

```
# dnf install ipa-server ipa-server-trust-ad samba-client
```

1.9. DÉFINITION DU MASQUE DE CRÉATION DU MODE DE FICHIER CORRECT POUR L'INSTALLATION DE L'IDM

Le processus d'installation de la gestion de l'identité (IdM) exige que le masque de création de mode de fichier (**umask**) soit défini sur **0022** pour le compte **root**. Cela permet aux utilisateurs autres que **root** de lire les fichiers créés pendant l'installation. Si le compte **umask** est différent, l'installation d'un serveur IdM affichera un avertissement. Si vous poursuivez l'installation, certaines fonctions du serveur ne fonctionneront pas correctement. Par exemple, vous ne pourrez pas installer un réplica IdM à partir de ce serveur. Après l'installation, vous pouvez rétablir la valeur initiale de **umask**.

Conditions préalables

- Vous avez des privilèges **root**.

Procédure

1. (Facultatif) Affichage de l'adresse actuelle **umask**:

```
# umask
0027
```

2. Réglez le site **umask** sur **0022**:

```
# umask 0022
```

3. (Facultatif) Une fois l'installation de l'IdM terminée, remettez le site **umask** à sa valeur d'origine :

```
# umask 0027
```

1.10. VEILLER À CE QUE LES RÈGLES FAPOLICYD NE BLOQUENT PAS L'INSTALLATION DE L'IDM

Si vous utilisez le cadre logiciel **fapolicyd** sur votre hôte RHEL pour contrôler l'exécution des applications sur la base d'une politique définie par l'utilisateur, l'installation du serveur Identity Management (IdM) peut échouer. Étant donné que l'installation et l'exploitation nécessitent le

programme Java pour se dérouler correctement, assurez-vous que Java et les classes Java ne sont pas bloqués par des règles **fapolicyd**.

Pour plus d'informations, voir les restrictions fapolicy causant des échecs de l'installation IdM dans la solution KCS.

1.11. OPTIONS POUR LES COMMANDES D'INSTALLATION DE L'IDM

Les commandes telles que **ipa-server-install**, **ipa-replica-install**, **ipa-dns-install** et **ipa-ca-install** disposent de nombreuses options que vous pouvez utiliser pour fournir des informations supplémentaires pour une installation interactive. Vous pouvez également utiliser ces options pour programmer une installation sans surveillance.

Les tableaux suivants présentent certaines des options les plus courantes pour différents composants. Les options d'un composant spécifique sont partagées par plusieurs commandes. Par exemple, vous pouvez utiliser l'option **--ca-subject** avec les commandes **ipa-ca-install** et **ipa-server-install**.

Pour une liste exhaustive des options, voir les pages de manuel **ipa-server-install(1)**, **ipa-replica-install(1)**, **ipa-dns-install(1)** et **ipa-ca-install(1)**.

Tableau 1.4. Options générales : disponibles pour ipa-server-install et ipa-replica-install

Argument	Description
-d, **--debug**	Active la journalisation de débogage pour une sortie plus verbeuse.
-U, **--unattended**	Active une session d'installation sans surveillance qui ne demande pas d'entrée de la part de l'utilisateur.
--hostname=*server.idm.example.com*	Le nom de domaine complet de la machine du serveur IdM. Seuls les chiffres, les caractères alphabétiques minuscules et les traits d'union (-) sont autorisés.
--ip-address *127.0.0.1*	Spécifie l'adresse IP du serveur. Cette option n'accepte que les adresses IP associées à l'interface locale.
--dirsrv-config-file *<LDIF_file_name>*	Chemin d'accès à un fichier LDIF utilisé pour modifier la configuration de l'instance du serveur d'annuaire.
-n *example.com*	Le nom du domaine du serveur LDAP à utiliser pour le domaine IdM. Ce nom est généralement basé sur le nom d'hôte du serveur IdM.
-p *<directory_manager_password>*	Le mot de passe du superutilisateur, **cn=Directory Manager**, pour le service LDAP.
-a *<ipa_admin_password>*	Le mot de passe du compte administrateur de **admin** IdM pour l'authentification au domaine Kerberos. Pour **ipa-replica-install**, utilisez plutôt **-w**.

Argument	Description
-r *<KERBEROS_REALM_NAME>*	Le nom du domaine Kerberos à créer pour le domaine IdM en majuscules, tel que **EXAMPLE.COM**. Pour **ipa-replica-install**, il s'agit du nom d'un domaine Kerberos d'un déploiement IdM existant.
--setup-dns	Indique au script d'installation de configurer un service DNS dans le domaine IdM.
--setup-ca	Installer et configurer une autorité de certification sur ce réplica. Si une autorité de certification n'est pas configurée, les opérations de certificat sont transmises à un autre réplica sur lequel une autorité de certification est installée. Pour **ipa-server-install**, une autorité de certification est installée par défaut et vous n'avez pas besoin d'utiliser cette option.

Tableau 1.5. Options CA : disponibles pour **ipa-ca-install** et **ipa-server-install**

Argument	Description
--random-serial-numbers	Active les numéros de série aléatoires version 3 (RSNv3) pour l'autorité de certification IdM. Lorsque cette option est activée, l'autorité de certification génère des numéros de série entièrement aléatoires pour les certificats et les demandes dans l'ICP sans gestion de la plage. **IMPORTANT:** RSNv3 n'est pris en charge que pour les nouvelles installations d'AC IdM. Si elle est activée, il est nécessaire d'utiliser RSNv3 pour tous les services PKI.
--ca-subject=*<SUBJECT>*	Spécifie le nom distinctif du sujet du certificat de l'autorité de certification (par défaut : CN=Autorité de certification,O=REALM.NAME). Les noms distinctifs relatifs (RDN) sont classés dans l'ordre LDAP, en commençant par le RDN le plus spécifique.
--subject-base=*<SUBJECT>*	Spécifie la base du sujet pour les certificats émis par IdM (par défaut O=REALM.NAME). Les noms distinctifs relatifs (RDN) sont classés dans l'ordre LDAP, en commençant par le RDN le plus spécifique.
--external-ca	Génère une demande de signature de certificat à signer par une autorité de certification externe.
--ca-signing-algorithm=*<ALGORITHM>*	Spécifie l'algorithme de signature du certificat de l'autorité de certification IdM. Les valeurs possibles sont SHA1withRSA, SHA256withRSA, SHA512withRSA. La valeur par défaut est SHA256withRSA. Utilisez cette option avec **--external-ca** si l'autorité de certification externe ne prend pas en charge l'algorithme de signature par défaut.

Tableau 1.6. Options DNS : disponibles pour **ipa-dns-install**, ou pour **ipa-server-install** et **ipa-replica-install** lors de l'utilisation de **--setup-dns**

Argument	Description
--forwarder=*192.0.2.1*	Spécifie un transitaire DNS à utiliser avec le service DNS. Pour spécifier plus d'un transitaire, utilisez cette option plusieurs fois.
--no-forwarders	Utilise des serveurs racine avec le service DNS au lieu de forwarders.
--no-reverse	Ne crée pas de zone DNS inversée lors de la configuration du domaine DNS. Si une zone DNS inverse est déjà configurée, c'est cette zone DNS inverse existante qui est utilisée. Si cette option n'est pas utilisée, la valeur par défaut est **true**. Cette option demande au script d'installation de configurer le DNS inverse.

Ressources supplémentaires

- **ipa-server-install(1)** page de manuel
- **ipa-replica-install(1)** page de manuel
- **ipa-dns-install(1)** page de manuel
- **ipa-ca-install(1)** page de manuel

CHAPITRE 2. INSTALLATION D'UN SERVEUR IDM : AVEC DNS INTÉGRÉ, AVEC UNE AUTORITÉ DE CERTIFICATION INTÉGRÉE COMME AUTORITÉ DE CERTIFICATION RACINE

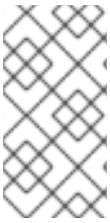
L'installation d'un nouveau serveur de gestion des identités (IdM) avec DNS intégré présente les avantages suivants :

- Vous pouvez automatiser une grande partie de la maintenance et de la gestion des enregistrements DNS à l'aide d'outils IdM natifs. Par exemple, les enregistrements DNS SRV sont automatiquement créés lors de l'installation et sont ensuite automatiquement mis à jour.
- Vous pouvez avoir une connexion stable avec le reste de l'Internet en configurant des redirections globales lors de l'installation du serveur IdM. Les redirections globales sont également utiles pour les trusts avec Active Directory.
- Vous pouvez configurer une zone DNS inverse pour éviter que les courriels de votre domaine soient considérés comme du spam par les serveurs de messagerie en dehors du domaine IdM.

L'installation d'IdM avec DNS intégré présente certaines limites :

- IdM DNS n'est pas conçu pour être utilisé comme un serveur DNS polyvalent. Certaines fonctions DNS avancées ne sont pas prises en charge.

Ce chapitre décrit comment installer un nouveau serveur IdM avec une autorité de certification (AC) intégrée en tant qu'AC racine.



NOTE

La configuration par défaut de la commande **ipa-server-install** est une autorité de certification intégrée en tant qu'autorité de certification racine. Si aucune option d'autorité de certification, par exemple **--external-ca** ou **--ca-less**, n'est spécifiée, le serveur IdM est installé avec une autorité de certification intégrée.

2.1. INSTALLATION INTERACTIVE

Pendant l'installation interactive à l'aide de l'utilitaire **ipa-server-install** il vous est demandé de fournir la configuration de base du système, par exemple le domaine, le mot de passe de l'administrateur et le mot de passe du gestionnaire de répertoire.

Le script d'installation **ipa-server-install** crée un fichier journal à l'adresse **/var/log/ipaserver-install.log**. Si l'installation échoue, le journal peut vous aider à identifier le problème.

Procédure

1. Exécutez l'utilitaire **ipa-server-install**.

```
# ipa-server-install
```

2. Le script invite à configurer un service DNS intégré. Saisissez **yes**.

```
Voulez-vous configurer le DNS intégré (BIND) ? [non] : yes
```

3. Le script demande plusieurs paramètres obligatoires et propose des valeurs par défaut recommandées entre parenthèses.

   - Pour accepter une valeur par défaut, appuyez sur **Entrée**.
   - Pour fournir une valeur personnalisée, saisissez la valeur requise.

   ```
   Server host name [server.idm.example.com]:
   Please confirm the domain name [idm.example.com]:
   Please provide a realm name [IDM.EXAMPLE.COM]:
   ```

   AVERTISSEMENT

   Planifiez ces noms avec soin. Vous ne pourrez pas les modifier une fois l'installation terminée.

4. Saisissez les mots de passe du superutilisateur du serveur d'annuaire (**cn=Directory Manager**) et du compte utilisateur du système d'administration Identity Management (IdM) (**admin**).

   ```
   Directory Manager password:
   IPA admin password:
   ```

5. Le script demande d'indiquer les redirections DNS par serveur.

   ```
   Do you want to configure DNS forwarders? [yes]:
   ```

   - Pour configurer les forwarders DNS par serveur, entrez **yes**, puis suivez les instructions de la ligne de commande. Le processus d'installation ajoutera les adresses IP des transitaires au LDAP de l'IdM.
     - Pour les paramètres par défaut de la politique de transfert, voir la description de **--forward-policy** dans la page de manuel **ipa-dns-install**(1).
   - Si vous ne souhaitez pas utiliser la redirection DNS, entrez **no**.
     En l'absence de redirecteurs DNS, les hôtes de votre domaine IdM ne pourront pas résoudre les noms provenant d'autres domaines DNS internes de votre infrastructure. Les hôtes n'auront plus que les serveurs DNS publics pour résoudre leurs requêtes DNS.

6. Le script demande de vérifier si des enregistrements DNS inverses (PTR) pour les adresses IP associées au serveur doivent être configurés.

   ```
   Do you want to search for missing reverse zones? [yes]:
   ```

   Si vous exécutez la recherche et que des zones inversées manquantes sont découvertes, le script vous demande s'il faut créer les zones inversées en même temps que les enregistrements PTR.

   ```
   Do you want to create reverse zone for IP 192.0.2.1 [yes]:
   Please specify the reverse zone name [2.0.192.in-addr.arpa.]:
   Using reverse zone(s) 2.0.192.in-addr.arpa.
   ```

–

NOTE

L'utilisation d'IdM pour gérer les zones inversées est facultative. Vous pouvez utiliser un service DNS externe à cette fin.

7. Entrez **yes** pour confirmer la configuration du serveur.

```
Continuer à configurer le système avec ces valeurs ? [no] : yes
```

8. Le script d'installation configure maintenant le serveur. Attendez la fin de l'opération.

9. Une fois le script d'installation terminé, mettez à jour vos enregistrements DNS de la manière suivante :

   a. Ajouter la délégation DNS du domaine parent au domaine DNS IdM. Par exemple, si le domaine DNS IdM est ***idm.example.com***ajoutez un enregistrement de serveur de noms (NS) au domaine parent **example.com**.

   IMPORTANT

   Répétez cette étape chaque fois qu'un serveur DNS IdM est installé.

   b. Ajoutez un enregistrement de service **_ntp._udp** (SRV) pour votre serveur de temps à votre DNS IdM. La présence de l'enregistrement SRV pour le serveur de temps du serveur IdM nouvellement installé dans le DNS IdM garantit que les futures installations de répliques et de clients sont automatiquement configurées pour se synchroniser avec le serveur de temps utilisé par ce serveur IdM primaire.

2.2. INSTALLATION NON INTERACTIVE

Le script d'installation **ipa-server-install** crée un fichier journal à l'adresse **/var/log/ipaserver-install.log**. Si l'installation échoue, le journal peut vous aider à identifier le problème.

Procédure

1. Exécutez l'utilitaire **ipa-server-install** avec les options nécessaires pour fournir toutes les informations requises. Les options minimales requises pour une installation non interactive sont les suivantes :

   - **--realm** pour fournir le nom du domaine Kerberos
   - **--ds-password** pour fournir le mot de passe du gestionnaire de répertoire (DM), le super utilisateur du serveur de répertoire
   - **--admin-password** pour fournir le mot de passe de **admin**, l'administrateur de la gestion des identités (IdM)
   - **--unattended** pour laisser le processus d'installation sélectionner les options par défaut pour le nom d'hôte et le nom de domaine

   Pour installer un serveur avec DNS intégré, ajoutez également ces options :

   - **--setup-dns** pour configurer le DNS intégré

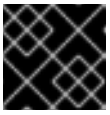
- **--forwarder** ou **--no-forwarders**, selon que vous souhaitez ou non configurer des serveurs DNS
- **--auto-reverse** ou **--no-reverse**, selon que l'on souhaite configurer la détection automatique des zones DNS inversées qui doivent être créées dans le DNS IdM ou qu'il n'y ait pas de détection automatique des zones inversées

Par exemple :

```
# ipa-server-install --realm IDM.EXAMPLE.COM --ds-password DM_password --admin-password admin_password --unattended --setup-dns --forwarder 192.0.2.1 --no-reverse
```

2. Une fois le script d'installation terminé, mettez à jour vos enregistrements DNS de la manière suivante :

   a. Ajouter la délégation DNS du domaine parent au domaine DNS IdM. Par exemple, si le domaine DNS IdM est ***idm.example.com***ajoutez un enregistrement de serveur de noms (NS) au domaine parent **example.com**.

   IMPORTANT

   Répétez cette étape chaque fois qu'un serveur DNS IdM est installé.

   b. Ajoutez un enregistrement de service **_ntp._udp** (SRV) pour votre serveur de temps à votre DNS IdM. La présence de l'enregistrement SRV pour le serveur de temps du serveur IdM nouvellement installé dans le DNS IdM garantit que les futures installations de répliques et de clients sont automatiquement configurées pour se synchroniser avec le serveur de temps utilisé par ce serveur IdM primaire.

Ressources supplémentaires

- Pour obtenir la liste complète des options acceptées par **ipa-server-install**, exécutez la commande **ipa-server-install --help**.

CHAPITRE 3. INSTALLATION D'UN SERVEUR IDM : AVEC DNS INTÉGRÉ, AVEC UNE AUTORITÉ DE CERTIFICATION EXTERNE COMME AUTORITÉ DE CERTIFICATION RACINE

L'installation d'un nouveau serveur de gestion des identités (IdM) avec DNS intégré présente les avantages suivants :

- Vous pouvez automatiser une grande partie de la maintenance et de la gestion des enregistrements DNS à l'aide d'outils IdM natifs. Par exemple, les enregistrements DNS SRV sont automatiquement créés lors de l'installation et sont ensuite automatiquement mis à jour.
- Vous pouvez avoir une connexion stable avec le reste de l'Internet en configurant des redirections globales lors de l'installation du serveur IdM. Les redirections globales sont également utiles pour les trusts avec Active Directory.
- Vous pouvez configurer une zone DNS inverse pour éviter que les courriels de votre domaine soient considérés comme du spam par les serveurs de messagerie en dehors du domaine IdM.

L'installation d'IdM avec DNS intégré présente certaines limites :

- IdM DNS n'est pas conçu pour être utilisé comme un serveur DNS polyvalent. Certaines fonctions DNS avancées ne sont pas prises en charge.

Ce chapitre décrit comment installer un nouveau serveur IdM avec une autorité de certification (AC) externe en tant qu'AC racine.

3.1. INSTALLATION INTERACTIVE

Pendant l'installation interactive à l'aide de l'utilitaire **ipa-server-install** il vous est demandé de fournir la configuration de base du système, par exemple le domaine, le mot de passe de l'administrateur et le mot de passe du gestionnaire de répertoire.

Le script d'installation **ipa-server-install** crée un fichier journal à l'adresse **/var/log/ipaserver-install.log**. Si l'installation échoue, le journal peut vous aider à identifier le problème.

Cette procédure décrit comment installer un serveur :

- avec DNS intégré
- avec une autorité de certification (AC) externe en tant qu'AC racine

Conditions préalables

- Vous avez déterminé le type d'autorité de certification externe à spécifier avec l'option **--external-ca-type**. Voir la page de manuel **ipa-server-install**(1) pour plus de détails.
- Si vous utilisez une autorité de certification Microsoft Certificate Services (MS CS CA) comme autorité de certification externe : vous avez déterminé le profil ou le modèle de certificat à spécifier avec l'option **--external-ca-profile**. Par défaut, le modèle **SubCA** est utilisé.
  Pour plus d'informations sur les options **--external-ca-type** et **--external-ca-profile**, voir Options utilisées lors de l'installation d'une autorité de certification IdM avec une autorité de certification externe en tant qu'autorité de certification racine.

Procédure

1. Exécutez l'utilitaire **ipa-server-install** avec l'option **--external-ca**.

```
# ipa-server-install --external-ca
```

   - Si vous utilisez l'autorité de certification Microsoft Certificate Services (MS CS), utilisez également l'option **--external-ca-type** et, éventuellement, l'option **--external-ca-profile**:

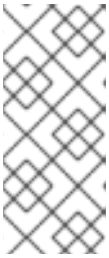
```
[root@server ~]# ipa-server-install --external-ca --external-ca-type=ms-cs --
external-ca-profile=<oid>/<name>/default
```

   - Si vous n'utilisez pas MS CS pour générer le certificat de signature de votre AC IdM, aucune autre option n'est nécessaire :

```
# ipa-server-install --external-ca
```

2. Le script demande de configurer un service DNS intégré. Saisissez **yes** ou **no**. Dans cette procédure, nous installons un serveur avec DNS intégré.

```
Voulez-vous configurer le DNS intégré (BIND) ? [non] : yes
```



NOTE

Si vous souhaitez installer un serveur sans DNS intégré, le script d'installation ne vous demandera pas de configurer le DNS comme décrit dans les étapes ci-dessous. Voir Chapitre 5, *Installation d'un serveur IdM : Sans DNS intégré, avec une autorité de certification intégrée comme autorité de certification racine* pour plus de détails sur les étapes de l'installation d'un serveur sans DNS.

3. Le script demande plusieurs paramètres obligatoires et propose des valeurs par défaut recommandées entre parenthèses.

   - Pour accepter une valeur par défaut, appuyez sur **Entrée**.
   - Pour fournir une valeur personnalisée, saisissez la valeur requise.

```
Server host name [server.idm.example.com]:
Please confirm the domain name [idm.example.com]:
Please provide a realm name [IDM.EXAMPLE.COM]:
```

AVERTISSEMENT

Planifiez ces noms avec soin. Vous ne pourrez pas les modifier une fois l'installation terminée.

4. Saisissez les mots de passe du superutilisateur du serveur d'annuaire (**cn=Directory Manager**) et du compte utilisateur du système d'administration Identity Management (IdM) (**admin**).

```
Directory Manager password:
IPA admin password:
```

5. Le script demande d'indiquer les redirections DNS par serveur.

```
Do you want to configure DNS forwarders? [yes]:
```

- Pour configurer les forwarders DNS par serveur, entrez **yes**, puis suivez les instructions de la ligne de commande. Le processus d'installation ajoutera les adresses IP des transitaires au LDAP de l'IdM.
  - Pour les paramètres par défaut de la politique de transfert, voir la description de **--forward-policy** dans la page de manuel **ipa-dns-install**(1).
- Si vous ne souhaitez pas utiliser la redirection DNS, entrez **no**.
  En l'absence de redirecteurs DNS, les hôtes de votre domaine IdM ne pourront pas résoudre les noms provenant d'autres domaines DNS internes de votre infrastructure. Les hôtes n'auront plus que les serveurs DNS publics pour résoudre leurs requêtes DNS.

6. Le script demande de vérifier si des enregistrements DNS inverses (PTR) pour les adresses IP associées au serveur doivent être configurés.

```
Do you want to search for missing reverse zones? [yes]:
```

Si vous exécutez la recherche et que des zones inversées manquantes sont découvertes, le script vous demande s'il faut créer les zones inversées en même temps que les enregistrements PTR.

```
Do you want to create reverse zone for IP 192.0.2.1 [yes]:
Please specify the reverse zone name [2.0.192.in-addr.arpa.]:
Using reverse zone(s) 2.0.192.in-addr.arpa.
```

NOTE

L'utilisation d'IdM pour gérer les zones inversées est facultative. Vous pouvez utiliser un service DNS externe à cette fin.

7. Entrez **yes** pour confirmer la configuration du serveur.

```
Continuer à configurer le système avec ces valeurs ? [no] : yes
```

8. Lors de la configuration de l'instance du système de certification, l'utilitaire imprime l'emplacement de la demande de signature du certificat (CSR) : **/root/ipa.csr**:

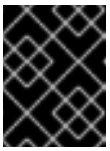
```
...

Configuring certificate server (pki-tomcatd): Estimated time 3 minutes 30 seconds
  [1/8]: creating certificate server user
  [2/8]: configuring certificate server instance
The next step is to get /root/ipa.csr signed by your CA and re-run /sbin/ipa-server-install as:
/sbin/ipa-server-install --external-cert-file=/path/to/signed_certificate --external-cert-
file=/path/to/external_ca_certificate
```

Lorsque cela se produit :

a. Soumettre le CSR situé dans **/root/ipa.csr** à l'autorité de certification externe. La procédure diffère selon le service utilisé comme autorité de certification externe.

b. Récupérer le certificat émis et la chaîne de certificats de l'autorité de certification émettrice dans un blob codé en base 64 (soit un fichier PEM, soit un certificat Base_64 d'une autorité de certification Windows). Là encore, la procédure diffère d'un service de certification à l'autre. En général, un lien de téléchargement sur une page web ou dans l'e-mail de notification permet à l'administrateur de télécharger tous les certificats requis.



IMPORTANT

Veillez à obtenir la chaîne de certificats complète de l'autorité de certification, et pas seulement le certificat de l'autorité de certification.

c. Exécutez à nouveau **ipa-server-install**, en spécifiant cette fois les emplacements et les noms du certificat d'autorité de certification nouvellement émis et des fichiers de la chaîne d'autorité de certification. Par exemple :

```
# ipa-server-install --external-cert-file=/tmp/servercert20170601.pem --external-cert-file=/tmp/cacert.pem
```

9. Le script d'installation configure maintenant le serveur. Attendez la fin de l'opération.

10. Une fois le script d'installation terminé, mettez à jour vos enregistrements DNS de la manière suivante :

a. Ajouter la délégation DNS du domaine parent au domaine DNS IdM. Par exemple, si le domaine DNS IdM est ***idm.example.com***ajoutez un enregistrement de serveur de noms (NS) au domaine parent **example.com**.

IMPORTANT

Répétez cette étape chaque fois qu'un serveur DNS IdM est installé.

b. Ajoutez un enregistrement de service **_ntp._udp** (SRV) pour votre serveur de temps à votre DNS IdM. La présence de l'enregistrement SRV pour le serveur de temps du serveur IdM nouvellement installé dans le DNS IdM garantit que les futures installations de répliques et de clients sont automatiquement configurées pour se synchroniser avec le serveur de temps utilisé par ce serveur IdM primaire.

NOTE

La commande **ipa-server-install --external-ca** peut parfois échouer avec l'erreur suivante :

```
ipa         : CRITICAL failed to configure ca instance Command '/usr/sbin/pkispawn -s CA -f /tmp/configuration_file' returned non-zero exit status 1
Configuration of CA failed
```

Ce problème survient lorsque les variables d'environnement ***_proxy** sont définies. Pour résoudre le problème, voir Dépannage: L'installation de l'autorité de certification externe échoue.

3.2. DÉPANNAGE : L'INSTALLATION DE L'AUTORITÉ DE CERTIFICATION EXTERNE ÉCHOUE

La commande **ipa-server-install --external-ca** échoue avec l'erreur suivante :

```
ipa        : CRITICAL failed to configure ca instance Command '/usr/sbin/pkispawn -s CA -f
/tmp/configuration_file' returned non-zero exit status 1
Configuration of CA failed
```

La commande **env|grep proxy** affiche des variables telles que les suivantes :

```
# env|grep proxy
http_proxy=http://example.com:8080
ftp_proxy=http://example.com:8080
https_proxy=http://example.com:8080
```

Ce que cela signifie :

Les variables environnementales ***_proxy** empêchent l'installation du serveur.

Pour résoudre le problème :

1. Utilisez le script shell suivant pour désactiver les variables d'environnement ***_proxy**:

   ```
   # for i in ftp http https; do unset ${i}_proxy; done
   ```

2. Exécutez l'utilitaire **pkidestroy** pour supprimer l'installation infructueuse du sous-système d'autorité de certification (CA) :

   ```
   # pkidestroy -s CA -i pki-tomcat; rm -rf /var/log/pki/pki-tomcat /etc/sysconfig/pki-
   tomcat /etc/sysconfig/pki/tomcat/pki-tomcat /var/lib/pki/pki-tomcat /etc/pki/pki-tomcat
   /root/ipa.csr
   ```

3. Supprimer l'installation du serveur de gestion des identités (IdM) qui a échoué :

   ```
   # ipa-server-install --uninstall
   ```

4. Réessayer d'exécuter **ipa-server-install --external-ca**.

CHAPITRE 4. INSTALLATION D'UN SERVEUR IDM : AVEC DNS INTÉGRÉ, SANS CA

L'installation d'un nouveau serveur de gestion des identités (IdM) avec DNS intégré présente les avantages suivants :

- Vous pouvez automatiser une grande partie de la maintenance et de la gestion des enregistrements DNS à l'aide d'outils IdM natifs. Par exemple, les enregistrements DNS SRV sont automatiquement créés lors de l'installation et sont ensuite automatiquement mis à jour.
- Vous pouvez avoir une connexion stable avec le reste de l'Internet en configurant des redirections globales lors de l'installation du serveur IdM. Les redirections globales sont également utiles pour les trusts avec Active Directory.
- Vous pouvez configurer une zone DNS inverse pour éviter que les courriels de votre domaine soient considérés comme du spam par les serveurs de messagerie en dehors du domaine IdM.

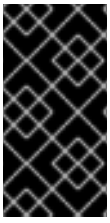
L'installation d'IdM avec DNS intégré présente certaines limites :

- IdM DNS n'est pas conçu pour être utilisé comme un serveur DNS polyvalent. Certaines fonctions DNS avancées ne sont pas prises en charge.

Ce chapitre décrit comment installer un nouveau serveur IdM sans autorité de certification (AC).

4.1. CERTIFICATS REQUIS POUR L'INSTALLATION D'UN SERVEUR IDM SANS AUTORITÉ DE CERTIFICATION

Cette section répertorie les certificats requis pour installer un serveur de gestion d'identité (IdM) sans autorité de certification (CA) et les options de ligne de commande utilisées pour fournir ces certificats à l'utilitaire **ipa-server-install**.



IMPORTANT

Vous ne pouvez pas installer un serveur ou un réplica à l'aide de certificats de serveur tiers auto-signés, car les fichiers de certificats importés doivent contenir la chaîne complète des certificats de l'autorité de certification qui a émis les certificats des serveurs LDAP et Apache.

Le certificat et la clé privée du serveur LDAP

- **--dirsrv-cert-file** pour les fichiers de certificat et de clé privée pour le certificat du serveur LDAP
- **--dirsrv-pin** pour le mot de passe permettant d'accéder à la clé privée dans les fichiers spécifiés dans la rubrique **--dirsrv-cert-file**

Le certificat et la clé privée du serveur Apache

- **--http-cert-file** pour les fichiers de certificat et de clé privée pour le certificat du serveur Apache
- **--http-pin** pour le mot de passe permettant d'accéder à la clé privée dans les fichiers spécifiés dans la rubrique **--http-cert-file**

La chaîne complète des certificats de l'autorité de certification qui a émis les certificats des serveurs LDAP et Apache

- **--dirsrv-cert-file** et **--http-cert-file** pour les fichiers de certificats contenant la chaîne complète de certificats de l'autorité de certification ou une partie de celle-ci

Vous pouvez fournir les fichiers spécifiés dans les options **--dirsrv-cert-file** et **--http-cert-file** dans les formats suivants :

- Certificat codé en PEM (Privacy-Enhanced Mail) (RFC 7468). Notez que le programme d'installation de la gestion de l'identité accepte les objets concaténés codés PEM.
- Règles de codage distinguées (DER)
- Objets de la chaîne de certificats PKCS #7
- Objets de clé privée PKCS #8
- Archives PKCS #12

Vous pouvez spécifier les options **--dirsrv-cert-file** et **--http-cert-file** plusieurs fois pour spécifier plusieurs fichiers.

Les fichiers de certificats pour compléter la chaîne complète de certificats de l'autorité de certification (non nécessaire dans certains environnements)

- **--ca-cert-file** pour le ou les fichiers contenant le certificat de l'autorité de certification qui a émis les certificats LDAP, Apache Server et Kerberos KDC. Utilisez cette option si le certificat de l'autorité de certification n'est pas présent dans les fichiers de certificats fournis par les autres options.

Les fichiers fournis à l'aide de **--dirsrv-cert-file** et **--http-cert-file**, combinés au fichier fourni à l'aide de **--ca-cert-file**, doivent contenir la chaîne complète des certificats de l'autorité de certification qui a émis les certificats des serveurs LDAP et Apache.

Le certificat PKINIT et la clé privée du centre de distribution de clés Kerberos (KDC)

- Si vous disposez d'un certificat PKINIT, utilisez les 2 options suivantes :
  - **--pkinit-cert-file** pour le certificat SSL et la clé privée du Kerberos KDC
  - **--pkinit-pin** pour le mot de passe permettant d'accéder à la clé privée du Kerberos KDC dans les fichiers spécifiés dans la section **--pkinit-cert-file**
- Si vous ne disposez pas d'un certificat PKINIT et que vous souhaitez configurer le serveur IdM avec un KDC local doté d'un certificat auto-signé, utilisez l'option suivante :
  - **--no-pkinit** pour désactiver les étapes d'installation de pkinit

Ressources supplémentaires

- Pour plus de détails sur les formats de fichiers de certificats acceptés par ces options, voir la page de manuel **ipa-server-install**(1).

- Pour plus de détails sur les extensions PKINIT requises pour créer un certificat PKINIT RHEL IdM, voir Certificat KDC RHEL IdM PKINIT et extensions .

4.2. INSTALLATION INTERACTIVE

Pendant l'installation interactive à l'aide de l'utilitaire **ipa-server-install** il vous est demandé de fournir la configuration de base du système, par exemple le domaine, le mot de passe de l'administrateur et le mot de passe du gestionnaire de répertoire.

Le script d'installation **ipa-server-install** crée un fichier journal à l'adresse **/var/log/ipaserver-install.log**. Si l'installation échoue, le journal peut vous aider à identifier le problème.

Procédure

1. Exécutez l'utilitaire **ipa-server-install** et fournissez tous les certificats requis. Par exemple :

```
[root@server ~]# ipa-server-install \
    --http-cert-file /tmp/server.crt \
    --http-cert-file /tmp/server.key \
    --http-pin secret \
    --dirsrv-cert-file /tmp/server.crt \
    --dirsrv-cert-file /tmp/server.key \
    --dirsrv-pin secret \
    --ca-cert-file ca.crt
```

   Voir Certificats requis pour l'installation d'un serveur IdM sans autorité de certification pour plus de détails sur les certificats fournis.

2. Le script demande de configurer un service DNS intégré. Saisissez **yes** ou **no**. Dans cette procédure, nous installons un serveur avec DNS intégré.

```
Voulez-vous configurer le DNS intégré (BIND) ? [non] : yes
```

NOTE

Si vous souhaitez installer un serveur sans DNS intégré, le script d'installation ne vous demandera pas de configurer le DNS comme décrit dans les étapes ci-dessous. Voir Installation d'un serveur IdM : Sans DNS intégré, avec une autorité de certification intégrée comme autorité de certification racine pour plus de détails sur les étapes de l'installation d'un serveur sans DNS.

3. Le script demande plusieurs paramètres obligatoires et propose des valeurs par défaut recommandées entre parenthèses.

   - Pour accepter une valeur par défaut, appuyez sur **Entrée**.
   - Pour fournir une valeur personnalisée, saisissez la valeur requise.

```
Server host name [server.idm.example.com]:
Please confirm the domain name [idm.example.com]:
Please provide a realm name [IDM.EXAMPLE.COM]:
```

AVERTISSEMENT

Planifiez ces noms avec soin. Vous ne pourrez pas les modifier une fois l'installation terminée.

4. Saisissez les mots de passe du superutilisateur du serveur d'annuaire (**cn=Directory Manager**) et du compte utilisateur du système d'administration Identity Management (IdM) (**admin**).

```
Directory Manager password:
IPA admin password:
```

5. Le script demande d'indiquer les redirections DNS par serveur.

```
Do you want to configure DNS forwarders? [yes]:
```

- Pour configurer les forwarders DNS par serveur, entrez **yes**, puis suivez les instructions de la ligne de commande. Le processus d'installation ajoutera les adresses IP des transitaires au LDAP de l'IdM.
  - Pour les paramètres par défaut de la politique de transfert, voir la description de **--forward-policy** dans la page de manuel **ipa-dns-install**(1).
- Si vous ne souhaitez pas utiliser la redirection DNS, entrez **no**.
  En l'absence de redirecteurs DNS, les hôtes de votre domaine IdM ne pourront pas résoudre les noms provenant d'autres domaines DNS internes de votre infrastructure. Les hôtes n'auront plus que les serveurs DNS publics pour résoudre leurs requêtes DNS.

6. Le script demande de vérifier si des enregistrements DNS inverses (PTR) pour les adresses IP associées au serveur doivent être configurés.

```
Do you want to search for missing reverse zones? [yes]:
```

Si vous exécutez la recherche et que des zones inversées manquantes sont découvertes, le script vous demande s'il faut créer les zones inversées en même temps que les enregistrements PTR.

```
Do you want to create reverse zone for IP 192.0.2.1 [yes]:
Please specify the reverse zone name [2.0.192.in-addr.arpa.]:
Using reverse zone(s) 2.0.192.in-addr.arpa.
```

NOTE

L'utilisation d'IdM pour gérer les zones inversées est facultative. Vous pouvez utiliser un service DNS externe à cette fin.

7. Entrez **yes** pour confirmer la configuration du serveur.

```
Continuer à configurer le système avec ces valeurs ? [no] : yes
```

8. Le script d'installation configure maintenant le serveur. Attendez la fin de l'opération.

9. Une fois le script d'installation terminé, mettez à jour vos enregistrements DNS de la manière suivante :

   a. Ajouter la délégation DNS du domaine parent au domaine DNS IdM. Par exemple, si le domaine DNS IdM est ***idm.example.com***ajoutez un enregistrement de serveur de noms (NS) au domaine parent **example.com**.

   IMPORTANT

   Répétez cette étape chaque fois qu'un serveur DNS IdM est installé.

   b. Ajoutez un enregistrement de service **_ntp._udp** (SRV) pour votre serveur de temps à votre DNS IdM. La présence de l'enregistrement SRV pour le serveur de temps du serveur IdM nouvellement installé dans le DNS IdM garantit que les futures installations de répliques et de clients sont automatiquement configurées pour se synchroniser avec le serveur de temps utilisé par ce serveur IdM primaire.

CHAPITRE 5. INSTALLATION D'UN SERVEUR IDM : SANS DNS INTÉGRÉ, AVEC UNE AUTORITÉ DE CERTIFICATION INTÉGRÉE COMME AUTORITÉ DE CERTIFICATION RACINE

Ce chapitre décrit comment installer un nouveau serveur de gestion des identités (IdM) sans DNS intégré.

NOTE

Red Hat recommande fortement d'installer le DNS intégré à l'IdM pour une utilisation de base dans le cadre du déploiement de l'IdM : Lorsque le serveur IdM gère également le DNS, il existe une intégration étroite entre le DNS et les outils IdM natifs, ce qui permet d'automatiser une partie de la gestion des enregistrements DNS.

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

5.1. INSTALLATION INTERACTIVE

Pendant l'installation interactive à l'aide de l'utilitaire **ipa-server-install** il vous est demandé de fournir la configuration de base du système, par exemple le domaine, le mot de passe de l'administrateur et le mot de passe du gestionnaire de répertoire.

Le script d'installation **ipa-server-install** crée un fichier journal à l'adresse **/var/log/ipaserver-install.log**. Si l'installation échoue, le journal peut vous aider à identifier le problème.

Cette procédure permet d'installer un serveur :

- Sans DNS intégré
- Avec l'autorité de certification (AC) de la gestion intégrée des identités (IdM) en tant qu'AC racine, qui est la configuration par défaut de l'AC

Procédure

1. Exécutez l'utilitaire **ipa-server-install**.

```
# ipa-server-install
```

2. Le script invite à configurer un service DNS intégré. Appuyez sur **Entrée** pour sélectionner l'option par défaut **no**.

```
Do you want to configure integrated DNS (BIND)? [no]:
```

3. Le script demande plusieurs paramètres obligatoires et propose des valeurs par défaut recommandées entre parenthèses.
   - Pour accepter une valeur par défaut, appuyez sur **Entrée**.
   - Pour fournir une valeur personnalisée, saisissez la valeur requise.

```
Server host name [server.idm.example.com]:
Please confirm the domain name [idm.example.com]:
Please provide a realm name [IDM.EXAMPLE.COM]:
```

AVERTISSEMENT

Planifiez ces noms avec soin. Vous ne pourrez pas les modifier une fois l'installation terminée.

4. Saisissez les mots de passe du superutilisateur du serveur d'annuaire (**cn=Directory Manager**) et du compte utilisateur du système d'administration IdM (**admin**).

```
Directory Manager password:
IPA admin password:
```

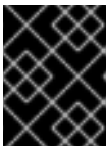
5. Entrez **yes** pour confirmer la configuration du serveur.

```
Continuer à configurer le système avec ces valeurs ? [no] : yes
```

6. Le script d'installation configure maintenant le serveur. Attendez la fin de l'opération.

7. Le script d'installation produit un fichier contenant des enregistrements de ressources DNS : **the /tmp/ipa.system.records.UFRPto.db** dans l'exemple ci-dessous. Ajoutez ces enregistrements aux serveurs DNS externes existants. Le processus de mise à jour des enregistrements DNS varie en fonction de la solution DNS utilisée.

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```



IMPORTANT

L'installation du serveur n'est pas terminée tant que vous n'avez pas ajouté les enregistrements DNS aux serveurs DNS existants.

Ressources supplémentaires

- Pour plus d'informations sur les enregistrements de ressources DNS que vous devez ajouter à votre système DNS, voir Enregistrements DNS IdM pour les systèmes DNS externes .

5.2. INSTALLATION NON INTERACTIVE

Cette procédure permet d'installer un serveur sans DNS intégré ou avec une autorité de certification (AC) de gestion d'identité (IdM) intégrée en tant qu'AC racine, ce qui correspond à la configuration par défaut de l'AC.

NOTE

Le script d'installation **ipa-server-install** crée un fichier journal à l'adresse **/var/log/ipaserver-install.log**. Si l'installation échoue, le journal peut vous aider à identifier le problème.

Procédure

1. Lancer l'utilitaire **ipa-server-install** avec les options permettant de fournir toutes les informations requises. Les options minimales requises pour une installation non interactive sont les suivantes :

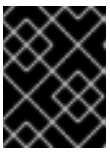
   - **--realm** pour fournir le nom du domaine Kerberos
   - **--ds-password** pour fournir le mot de passe du gestionnaire de répertoire (DM), le super utilisateur du serveur de répertoire
   - **--admin-password** de fournir le mot de passe pour **admin**, l'administrateur IdM
   - **--unattended** pour laisser le processus d'installation sélectionner les options par défaut pour le nom d'hôte et le nom de domaine

   Par exemple :

   ```
   # ipa-server-install --realm IDM.EXAMPLE.COM --ds-password DM_password --admin-password admin_password --unattended
   ```

2. Le script d'installation produit un fichier contenant des enregistrements de ressources DNS : **the /tmp/ipa.system.records.UFRPto.db** dans l'exemple ci-dessous. Ajoutez ces enregistrements aux serveurs DNS externes existants. Le processus de mise à jour des enregistrements DNS varie en fonction de la solution DNS utilisée.

   ```
   ...
   Restarting the KDC
   Please add records in this file to your DNS system:
   /tmp/ipa.system.records.UFRBto.db
   Restarting the web server
   ...
   ```



IMPORTANT

L'installation du serveur n'est pas terminée tant que vous n'avez pas ajouté les enregistrements DNS aux serveurs DNS existants.

Ressources supplémentaires

- Pour plus d'informations sur les enregistrements de ressources DNS que vous devez ajouter à votre système DNS, voir Enregistrements DNS IdM pour les systèmes DNS externes .
- Pour obtenir la liste complète des options acceptées par **ipa-server-install**, exécutez la commande **ipa-server-install --help**.

5.3. ENREGISTREMENTS DNS DE L'IDM POUR LES SYSTÈMES DNS EXTERNES

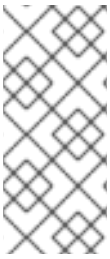
Après avoir installé un serveur IdM sans DNS intégré, vous devez ajouter des enregistrements de ressources DNS LDAP et Kerberos pour le serveur IdM à votre système DNS externe.

Le script d'installation de **ipa-server-install** génère un fichier contenant la liste des enregistrements de ressources DNS avec un nom de fichier au format **/tmp/ipa.system.records.*<random_characters>*.db** et imprime les instructions pour ajouter ces enregistrements :

```
Veuillez ajouter les enregistrements de ce fichier à votre système DNS :
/tmp/ipa.system.records.6zdjqxh3.db
```

Voici un exemple du contenu du fichier :

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



NOTE

Après avoir ajouté les enregistrements de ressources DNS LDAP et Kerberos pour le serveur IdM à votre système DNS, assurez-vous que les outils de gestion DNS n'ont pas ajouté d'enregistrements PTR pour **ipa-ca**. La présence d'enregistrements PTR pour **ipa-ca** dans votre système DNS pourrait faire échouer les installations ultérieures de répliques IdM.

CHAPITRE 6. INSTALLATION D'UN SERVEUR IDM : SANS DNS INTÉGRÉ, AVEC UNE AUTORITÉ DE CERTIFICATION EXTERNE COMME AUTORITÉ DE CERTIFICATION RACINE

Ce chapitre décrit comment installer un nouveau serveur de gestion des identités (IdM), sans DNS intégré, qui utilise une autorité de certification externe comme autorité de certification racine.

NOTE

Red Hat recommande fortement d'installer le DNS intégré à l'IdM pour une utilisation de base dans le cadre du déploiement de l'IdM : Lorsque le serveur IdM gère également le DNS, il existe une intégration étroite entre le DNS et les outils IdM natifs, ce qui permet d'automatiser une partie de la gestion des enregistrements DNS.

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

6.1. OPTIONS UTILISÉES LORS DE L'INSTALLATION D'UNE AUTORITÉ DE CERTIFICATION IDM AVEC UNE AUTORITÉ DE CERTIFICATION EXTERNE EN TANT QU'AUTORITÉ DE CERTIFICATION RACINE

Vous pouvez installer une autorité de certification (AC) Identity Management IdM avec une AC externe en tant qu'AC racine si l'une des conditions suivantes s'applique :

- Vous installez un nouveau serveur IdM ou une nouvelle réplique à l'aide de la commande **ipa-server-install**.
- Vous installez le composant CA dans un serveur IdM existant à l'aide de la commande **ipa-ca-install**.

Cette section décrit les options des deux commandes que vous pouvez utiliser pour créer une demande de signature de certificat (CSR) lors de l'installation d'une autorité de certification IdM avec une autorité de certification externe en tant qu'autorité de certification racine.

--external-ca-type=*TYPE*

Type de l'AC externe. Les valeurs possibles sont ***generic*** et ***ms-cs***. La valeur par défaut est ***generic***. Utilisez ***ms-cs*** pour inclure un nom de modèle requis par Microsoft Certificate Services (MS CS) dans la RSC générée. Pour utiliser un profil autre que celui par défaut, utilisez l'option **--external-ca-profile** en conjonction avec **--external-ca-type=ms-cs**.

--profil-ca-externe=*PROFILE_SPEC*

Spécifiez le profil ou le modèle de certificat que vous souhaitez que MS CS applique lors de l'émission du certificat pour votre autorité de certification IdM.
Notez que l'option **--external-ca-profile** ne peut être utilisée que si **--external-ca-type** est ms-cs.

Vous pouvez identifier le modèle MS CS de l'une des manières suivantes :

- ***<oid>:<majorVersion>[:<minorVersion>]***. Vous pouvez spécifier un modèle de certificat par son identifiant d'objet (OID) et sa version majeure. Vous pouvez également spécifier la version mineure.
- ***<name>***. Vous pouvez spécifier un modèle de certificat par son nom. Le nom ne peut pas contenir de caractères **:** et ne peut pas être un OID, sinon la syntaxe du spécificateur de modèle basé sur l'OID est prioritaire.

- ***default***. Si vous utilisez ce spécificateur, le nom du modèle ***SubCA*** est utilisé.

Dans certains scénarios, l'administrateur Active Directory (AD) peut utiliser le modèle **Subordinate Certification Authority** (SCA), qui est un modèle intégré dans AD CS, pour créer un modèle unique afin de mieux répondre aux besoins de l'organisation. Le nouveau modèle peut, par exemple, avoir une période de validité et des extensions personnalisées. L'identifiant d'objet (OID) associé se trouve dans la console AD **Certificates Template**.

Si l'administrateur AD a désactivé le modèle original intégré, vous devez spécifier l'OID ou le nom du nouveau modèle lorsque vous demandez un certificat pour votre autorité de certification IdM. Demandez à votre administrateur AD de vous fournir le nom ou l'OID du nouveau modèle.

Si le modèle SCA AD CS d'origine est toujours activé, vous pouvez l'utiliser en spécifiant **--external-ca-type=ms-cs** sans utiliser en plus l'option **--external-ca-profile**. Dans ce cas, le profil de l'autorité de certification externe **subCA** est utilisé, qui est le modèle IdM par défaut correspondant au modèle SCA AD CS.

6.2. INSTALLATION INTERACTIVE

Pendant l'installation interactive à l'aide de l'utilitaire **ipa-server-install** il vous est demandé de fournir la configuration de base du système, par exemple le domaine, le mot de passe de l'administrateur et le mot de passe du gestionnaire de répertoire.

Le script d'installation **ipa-server-install** crée un fichier journal à l'adresse **/var/log/ipaserver-install.log**. Si l'installation échoue, le journal peut vous aider à identifier le problème.

Cette procédure décrit comment installer un serveur :

- Sans DNS intégré
- Avec une autorité de certification (AC) externe en tant qu'AC racine

Conditions préalables

- Vous avez déterminé le type d'autorité de certification externe à spécifier avec l'option **--external-ca-type**. Voir la page de manuel **ipa-server-install**(1) pour plus de détails.
- Si vous utilisez une autorité de certification Microsoft Certificate Services (MS CS CA) comme autorité de certification externe : vous avez déterminé le profil ou le modèle de certificat à spécifier avec l'option **--external-ca-profile**. Par défaut, le modèle **SubCA** est utilisé.
  Pour plus d'informations sur les options **--external-ca-type** et **--external-ca-profile**, voir Options utilisées lors de l'installation d'une autorité de certification IdM avec une autorité de certification externe en tant qu'autorité de certification racine.

Procédure

1. Exécutez l'utilitaire **ipa-server-install** avec l'option **--external-ca**.
   - Si vous utilisez l'autorité de certification Microsoft Certificate Services (MS CS), utilisez également l'option **--external-ca-type** et, éventuellement, l'option **--external-ca-profile**:

     ```
     [root@server ~]# ipa-server-install --external-ca --external-ca-type=ms-cs --external-ca-profile=<oid>/<name>/default
     ```

- Si vous n'utilisez pas MS CS pour générer le certificat de signature de votre AC IdM, aucune autre option n'est nécessaire :

```
# ipa-server-install --external-ca
```

2. Le script invite à configurer un service DNS intégré. Appuyez sur **Entrée** pour sélectionner l'option par défaut **no**.

```
Do you want to configure integrated DNS (BIND)? [no]:
```

3. Le script demande plusieurs paramètres obligatoires et propose des valeurs par défaut recommandées entre parenthèses.

- Pour accepter une valeur par défaut, appuyez sur **Entrée**.
- Pour fournir une valeur personnalisée, saisissez la valeur requise.

```
Server host name [server.idm.example.com]:
Please confirm the domain name [idm.example.com]:
Please provide a realm name [IDM.EXAMPLE.COM]:
```

AVERTISSEMENT

Planifiez ces noms avec soin. Vous ne pourrez pas les modifier une fois l'installation terminée.

4. Saisissez les mots de passe du superutilisateur du serveur d'annuaire (**cn=Directory Manager**) et du compte utilisateur du système d'administration IdM (**admin**).

```
Directory Manager password:
IPA admin password:
```

5. Entrez **yes** pour confirmer la configuration du serveur.

```
Continuer à configurer le système avec ces valeurs ? [no] : yes
```

6. Lors de la configuration de l'instance du système de certification, l'utilitaire imprime l'emplacement de la demande de signature du certificat (CSR) : **/root/ipa.csr**:

```
...

Configuring certificate server (pki-tomcatd): Estimated time 3 minutes 30 seconds
  [1/8]: creating certificate server user
  [2/8]: configuring certificate server instance
The next step is to get /root/ipa.csr signed by your CA and re-run /sbin/ipa-server-install as:
/sbin/ipa-server-install --external-cert-file=/path/to/signed_certificate --external-cert-
file=/path/to/external_ca_certificate
```

Lorsque cela se produit :

a. Soumettre le CSR situé dans **/root/ipa.csr** à l'autorité de certification externe. La procédure diffère selon le service utilisé comme autorité de certification externe.

b. Récupérer le certificat émis et la chaîne de certificats de l'autorité de certification émettrice dans un blob codé en base 64 (soit un fichier PEM, soit un certificat Base_64 d'une autorité de certification Windows). Là encore, la procédure diffère d'un service de certification à l'autre. En général, un lien de téléchargement sur une page web ou dans l'e-mail de notification permet à l'administrateur de télécharger tous les certificats requis.

IMPORTANT

Veillez à obtenir la chaîne de certificats complète de l'autorité de certification, et pas seulement le certificat de l'autorité de certification.

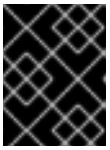
c. Exécutez à nouveau **ipa-server-install**, en spécifiant cette fois les emplacements et les noms du certificat d'autorité de certification nouvellement émis et des fichiers de la chaîne d'autorité de certification. Par exemple :

```
# ipa-server-install --external-cert-file=/tmp/servercert20170601.pem --external-cert-file=/tmp/cacert.pem
```

7. Le script d'installation configure maintenant le serveur. Attendez la fin de l'opération.

8. Le script d'installation produit un fichier contenant des enregistrements de ressources DNS : **the /tmp/ipa.system.records.UFRPto.db** dans l'exemple ci-dessous. Ajoutez ces enregistrements aux serveurs DNS externes existants. Le processus de mise à jour des enregistrements DNS varie en fonction de la solution DNS utilisée.

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```



IMPORTANT

L'installation du serveur n'est pas terminée tant que vous n'avez pas ajouté les enregistrements DNS aux serveurs DNS existants.

Ressources supplémentaires

- Pour plus d'informations sur les enregistrements de ressources DNS que vous devez ajouter à votre système DNS, voir Enregistrements DNS IdM pour les systèmes DNS externes .
- La commande **ipa-server-install --external-ca** peut parfois échouer avec l'erreur suivante :

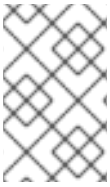
```
ipa         : CRITICAL failed to configure ca instance Command '/usr/sbin/pkispawn -s CA -f /tmp/pass:quotes[configuration_file]' returned non-zero exit status 1
Configuration of CA failed
```

Ce problème survient lorsque les variables d'environnement ***_proxy** sont définies. Pour résoudre le problème, voir Dépannage: L'installation de l'autorité de certification externe échoue.

6.3. INSTALLATION NON INTERACTIVE

Cette procédure permet d'installer un serveur :

- Sans DNS intégré
- avec une autorité de certification (AC) externe en tant qu'AC racine



NOTE

Le script d'installation **ipa-server-install** crée un fichier journal à l'adresse **/var/log/ipaserver-install.log**. Si l'installation échoue, le journal peut vous aider à identifier le problème.

Conditions préalables

- Vous avez déterminé le type d'autorité de certification externe à spécifier avec l'option **--external-ca-type**. Voir la page de manuel **ipa-server-install**(1) pour plus de détails.
- Si vous utilisez une autorité de certification Microsoft Certificate Services (MS CS CA) comme autorité de certification externe : vous avez déterminé le profil ou le modèle de certificat à spécifier avec l'option **--external-ca-profile**. Par défaut, le modèle **SubCA** est utilisé.
  Pour plus d'informations sur les options **--external-ca-type** et **--external-ca-profile**, voir Options utilisées lors de l'installation d'une autorité de certification IdM avec une autorité de certification externe en tant qu'autorité de certification racine.

Procédure

1. Lancer l'utilitaire **ipa-server-install** avec les options nécessaires pour fournir toutes les informations requises. Les options minimales requises pour l'installation non interactive d'un serveur IdM avec une autorité de certification externe en tant qu'autorité de certification racine sont les suivantes :
   - **--external-ca** pour spécifier qu'une autorité de certification externe est l'autorité de certification racine
   - **--realm** pour fournir le nom du domaine Kerberos
   - **--ds-password** pour fournir le mot de passe du gestionnaire de répertoire (DM), le super utilisateur du serveur de répertoire
   - **--admin-password** de fournir le mot de passe pour **admin**, l'administrateur IdM
   - **--unattended** pour laisser le processus d'installation sélectionner les options par défaut pour le nom d'hôte et le nom de domaine
     Par exemple :

     ```
     # ipa-server-install --external-ca --realm IDM.EXAMPLE.COM --ds-password
     DM_password --admin-password admin_password --unattended
     ```

   Si vous utilisez une autorité de certification Microsoft Certificate Services (MS CS), utilisez également l'option **--external-ca-type** et, éventuellement, l'option **--external-ca-profile**. Pour plus d'informations, voir Options utilisées lors de l'installation d'une autorité de certification IdM avec une autorité de certification externe en tant qu'autorité de certification racine.

2. Lors de la configuration de l'instance du système de certification, l'utilitaire imprime l'emplacement de la demande de signature du certificat (CSR) : **/root/ipa.csr**:

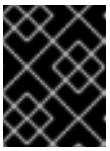
```
...

Configuring certificate server (pki-tomcatd). Estimated time: 3 minutes
  [1/11]: configuring certificate server instance
The next step is to get /root/ipa.csr signed by your CA and re-run /usr/sbin/ipa-server-install
as:
/usr/sbin/ipa-server-install --external-cert-file=/path/to/signed_certificate --external-cert-
file=/path/to/external_ca_certificate
The ipa-server-install command was successful
```

   Lorsque cela se produit :

   a. Soumettre le CSR situé dans **/root/ipa.csr** à l'autorité de certification externe. La procédure diffère selon le service utilisé comme autorité de certification externe.

   b. Récupérer le certificat émis et la chaîne de certificats de l'autorité de certification émettrice dans un blob codé en base 64 (soit un fichier PEM, soit un certificat Base_64 d'une autorité de certification Windows). Là encore, la procédure diffère d'un service de certification à l'autre. En général, un lien de téléchargement sur une page web ou dans l'e-mail de notification permet à l'administrateur de télécharger tous les certificats requis.



IMPORTANT

Veillez à obtenir la chaîne de certificats complète de l'autorité de certification, et pas seulement le certificat de l'autorité de certification.

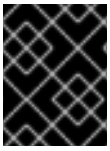
   c. Exécutez à nouveau **ipa-server-install**, en spécifiant cette fois les emplacements et les noms du certificat d'autorité de certification nouvellement émis et des fichiers de la chaîne d'autorité de certification. Par exemple :

```
# ipa-server-install --external-cert-file=/tmp/servercert20170601.pem --external-cert-
file=/tmp/cacert.pem --realm IDM.EXAMPLE.COM --ds-password DM_password --
admin-password admin_password --unattended
```

3. Le script d'installation configure maintenant le serveur. Attendez la fin de l'opération.

4. Le script d'installation produit un fichier contenant des enregistrements de ressources DNS : le fichier **/tmp/ipa.system.records.UFRPto.db** dans l'exemple ci-dessous. Ajoutez ces enregistrements aux serveurs DNS externes existants. Le processus de mise à jour des enregistrements DNS varie en fonction de la solution DNS utilisée.

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```



IMPORTANT

L'installation du serveur n'est pas terminée tant que vous n'avez pas ajouté les enregistrements DNS aux serveurs DNS existants.

Ressources supplémentaires

- Pour plus d'informations sur les enregistrements de ressources DNS que vous devez ajouter à votre système DNS, voir Enregistrements DNS IdM pour les systèmes DNS externes .

6.4. ENREGISTREMENTS DNS DE L'IDM POUR LES SYSTÈMES DNS EXTERNES

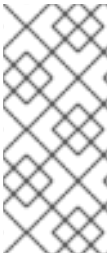
Après avoir installé un serveur IdM sans DNS intégré, vous devez ajouter des enregistrements de ressources DNS LDAP et Kerberos pour le serveur IdM à votre système DNS externe.

Le script d'installation de **ipa-server-install** génère un fichier contenant la liste des enregistrements de ressources DNS avec un nom de fichier au format **/tmp/ipa.system.records.*<random_characters>*.db** et imprime les instructions pour ajouter ces enregistrements :

```
Veuillez ajouter les enregistrements de ce fichier à votre système DNS :
/tmp/ipa.system.records.6zdjqxh3.db
```

Voici un exemple du contenu du fichier :

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



NOTE

Après avoir ajouté les enregistrements de ressources DNS LDAP et Kerberos pour le serveur IdM à votre système DNS, assurez-vous que les outils de gestion DNS n'ont pas ajouté d'enregistrements PTR pour **ipa-ca**. La présence d'enregistrements PTR pour **ipa-ca** dans votre système DNS pourrait faire échouer les installations ultérieures de répliques IdM.

CHAPITRE 7. INSTALLATION D'UN SERVEUR IDM OU D'UN RÉPLICA AVEC DES PARAMÈTRES DE BASE DE DONNÉES PERSONNALISÉS À PARTIR D'UN FICHIER LDIF

Vous pouvez installer un serveur IdM et des répliques IdM avec des paramètres personnalisés pour la base de données du serveur Directory. La procédure suivante vous montre comment créer un fichier LDAP Data Interchange Format (LDIF) avec les paramètres de la base de données et comment transmettre ces paramètres aux commandes d'installation du serveur IdM et des réplicas.

Conditions préalables

- Vous avez déterminé des paramètres personnalisés pour le serveur d'annuaire qui améliorent les performances de votre environnement IdM. Voir Ajustement des performances du serveur d'annuaire IdM.

Procédure

1. Créez un fichier texte au format LDIF avec vos paramètres de base de données personnalisés. Séparez les modifications d'attributs LDAP par un tiret (-). Cet exemple définit des valeurs par défaut pour le délai d'inactivité et le nombre maximum de descripteurs de fichiers.

```
dn: cn=config
changetype: modify
replace: nsslapd-idletimeout
nsslapd-idletimeout=1800
-
replace: nsslapd-maxdescriptors
nsslapd-maxdescriptors=8192
```

2. Utilisez le paramètre **--dirsrv-config-file** pour transmettre le fichier LDIF au script d'installation.

   a. Pour installer un serveur IdM :

   ```
   # ipa-server-install --dirsrv-config-file filename.ldif
   ```

   b. Pour installer une réplique IdM :

   ```
   # ipa-replica-install --dirsrv-config-file filename.ldif
   ```

Ressources supplémentaires

- Options pour les commandes **ipa-server-install** et **ipa-replica-install**

CHAPITRE 8. DÉPANNAGE DE L'INSTALLATION DU SERVEUR IDM

Les sections suivantes décrivent comment recueillir des informations sur l'échec de l'installation d'un serveur IdM et comment résoudre les problèmes d'installation les plus courants.

8.1. EXAMEN DES JOURNAUX D'ERREUR DE L'INSTALLATION DU SERVEUR IDM

Lorsque vous installez un serveur Identity Management (IdM), les informations de débogage sont ajoutées aux fichiers journaux suivants :

- **/var/log/ipaserver-install.log**
- **/var/log/httpd/error_log**
- **/var/log/dirsrv/slapd-*INSTANCE-NAME*/access**
- **/var/log/dirsrv/slapd-*INSTANCE-NAME*/errors**

Les dernières lignes des fichiers journaux indiquent le succès ou l'échec, et les entrées **ERROR** et **DEBUG** fournissent un contexte supplémentaire.

Pour dépanner une installation de serveur IdM défaillante, examinez les erreurs à la fin des fichiers journaux et utilisez ces informations pour résoudre les problèmes correspondants.

Conditions préalables

- Vous devez avoir les privilèges **root** pour afficher le contenu des fichiers journaux IdM.

Procédure

1. La commande **tail** permet d'afficher les dernières lignes d'un fichier journal. L'exemple suivant affiche les 10 dernières lignes de **/var/log/ipaserver-install.log**.

```
[user@server ~]$ sudo tail -n 10 /var/log/ipaserver-install.log
[sudo] password for user:
value = gen.send(prev_value)
File "/usr/lib/python3.6/site-packages/ipapython/install/common.py", line 65, in _install
for unused in self._installer(self.parent):
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/init.py", line 564, in main
master_install(self)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/install.py", line 291, in decorated
raise ScriptError()

2020-05-27T22:59:41Z DEBUG The ipa-server-install command failed, exception:
ScriptError:
2020-05-27T22:59:41Z ERROR The ipa-server-install command failed. See
/var/log/ipaserver-install.log for more information
```

2. Pour consulter un fichier journal de manière interactive, ouvrez la fin du fichier journal à l'aide de l'utilitaire **less** et utilisez les touches fléchées ↑ et ↓ pour naviguer. L'exemple suivant ouvre le fichier **/var/log/ipaserver-install.log** de manière interactive.

```
[user@server ~]$ sudo less -N G /var/log/ipaserver-install.log
```

3. Recueillez des informations de dépannage supplémentaires en répétant ce processus d'examen avec les fichiers journaux restants.

```
[user@server ~]$ sudo less -N +G /var/log/httpd/error_log

[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/access

[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/errors
```

Ressources supplémentaires

- Si vous ne parvenez pas à résoudre l'échec de l'installation d'un serveur IdM et que vous disposez d'un abonnement au support technique de Red Hat, ouvrez un dossier de support technique sur le portail client de Red Hat et fournissez une adresse **sosreport** du serveur.
- L'utilitaire **sosreport** collecte des détails de configuration, des journaux et des informations système à partir d'un système RHEL. Pour plus d'informations sur l'utilitaire **sosreport**, voir Qu'est-ce qu'un rapport sos et comment en créer un dans Red Hat Enterprise Linux ?

8.2. EXAMEN DES ERREURS D'INSTALLATION DE L'AUTORITÉ DE CERTIFICATION IDM

Lorsque vous installez le service d'autorité de certification (CA) sur un serveur de gestion des identités (IdM), les informations de débogage sont ajoutées aux emplacements suivants (par ordre de priorité recommandé) :

Location	Description
/var/log/pki/pki-ca-spawn.*$TIME_OF_INSTALLATION*.log	Problèmes de haut niveau et traces Python pour le processus d'installation de **pkispawn**
journalctl -u pki-tomcatd@pki-tomcat sortie	Erreurs provenant du service **pki-tomcatd@pki-tomcat**
/var/log/pki/pki-tomcat/ca/debug.*$DATE*.log	Grandes traces d'activité JAVA au cœur du produit d'infrastructure à clé publique (PKI)
/var/log/pki/pki-tomcat/ca/signedAudit/ca_audit fichier journal	Journal d'audit du produit PKI
• **/var/log/pki/pki-tomcat/ca/system** • **/var/log/pki/pki-tomcat/ca/transactions** • **/var/log/pki/pki-tomcat/catalina.*$DATE*.log**	Données de débogage de bas niveau des opérations de certificat pour les mandants de service, les hôtes et les autres entités qui utilisent des certificats

NOTE

Si une installation complète du serveur IdM échoue lors de l'installation du composant CA optionnel, aucun détail concernant le CA n'est consigné ; un message est consigné dans le fichier **/var/log/ipaserver-install.log** indiquant que le processus d'installation global a échoué. Red Hat recommande d'examiner les fichiers journaux énumérés ci-dessus pour obtenir des détails spécifiques à l'échec de l'installation de l'AC.

La seule exception à ce comportement est lorsque vous installez le service d'autorité de certification et que l'autorité de certification racine est une autorité de certification externe. En cas de problème avec le certificat de l'autorité de certification externe, les erreurs sont consignées dans **/var/log/ipaserver-install.log**.

Pour dépanner une installation défaillante de l'autorité de certification IdM, examinez les erreurs à la fin de ces fichiers journaux et utilisez ces informations pour résoudre les problèmes correspondants.

Conditions préalables

- Vous devez avoir les privilèges **root** pour afficher le contenu des fichiers journaux IdM.

Procédure

1. Pour examiner un fichier journal de manière interactive, ouvrez la fin du fichier journal à l'aide de l'utilitaire **less** et utilisez les touches fléchées ↑ et ↓ pour naviguer, tout en recherchant les entrées **ScriptError**. L'exemple suivant ouvre **/var/log/pki/pki-ca-spawn.*$TIME_OF_INSTALLATION*.log**.

```
[user@server ~]$ sudo less -N G /var/log/pki/pki-ca-spawn.20200527185902.log
```

2. Recueillez des informations de dépannage supplémentaires en répétant ce processus d'examen avec tous les fichiers journaux énumérés ci-dessus.

Ressources supplémentaires

- Si vous ne parvenez pas à résoudre l'échec de l'installation d'un serveur IdM et que vous disposez d'un abonnement au support technique de Red Hat, ouvrez un dossier de support technique sur le portail client de Red Hat et fournissez une adresse **sosreport** du serveur.
- L'utilitaire **sosreport** collecte des détails de configuration, des journaux et des informations système à partir d'un système RHEL. Pour plus d'informations sur l'utilitaire **sosreport**, voir Qu'est-ce qu'un rapport sos et comment en créer un dans Red Hat Enterprise Linux ?

8.3. SUPPRESSION D'UNE INSTALLATION PARTIELLE DU SERVEUR IDM

Si l'installation d'un serveur IdM échoue, certains fichiers de configuration peuvent être laissés sur place. D'autres tentatives d'installation du serveur IdM échouent et le script d'installation signale que l'IPA est déjà configuré.

Exemple de système avec une configuration IdM partielle existante

```
[root@server ~]# ipa-server-install

The log file for this installation can be found in /var/log/ipaserver-install.log
```

```
IPA server is already configured on this system.
If you want to reinstall the IPA server, please uninstall it first using 'ipa-server-install --uninstall'.
The ipa-server-install command failed. See /var/log/ipaserver-install.log for more information
```

Pour résoudre ce problème, désinstallez la configuration partielle du serveur IdM et réessayez la procédure d'installation.

Conditions préalables

- Vous devez avoir les privilèges de **root**.

Procédure

1. Désinstallez le logiciel du serveur IdM de l'hôte que vous essayez de configurer comme serveur IdM.

```
[root@server ~]# ipa-server-install --uninstall
```

2. Si vous continuez à éprouver des difficultés à installer un serveur IdM en raison d'échecs répétés, réinstallez le système d'exploitation.
   L'une des conditions requises pour l'installation d'un serveur IdM est de disposer d'un système propre, sans aucune personnalisation. Les installations qui ont échoué peuvent avoir compromis l'intégrité de l'hôte en modifiant de manière inattendue les fichiers du système.

Ressources supplémentaires

- Pour plus de détails sur la désinstallation d'un serveur IdM, voir Désinstallation d'un serveur IdM .
- Si les tentatives d'installation échouent après des tentatives répétées de désinstallation, et que vous disposez d'un abonnement au support technique de Red Hat, ouvrez un dossier de support technique sur le portail client de Red Hat et fournissez une adresse **sosreport** du serveur.
- L'utilitaire **sosreport** collecte des détails de configuration, des journaux et des informations système à partir d'un système RHEL. Pour plus d'informations sur l'utilitaire **sosreport**, voir Qu'est-ce qu'un rapport sos et comment en créer un dans Red Hat Enterprise Linux ?

Ressources supplémentaires

- Pour plus de détails sur la désinstallation d'un serveur IdM, voir Désinstallation d'un serveur IdM .
- Si les tentatives d'installation échouent après des tentatives répétées de désinstallation, et que vous disposez d'un abonnement au support technique de Red Hat, ouvrez un dossier de support technique sur le portail client de Red Hat et fournissez une adresse **sosreport** du serveur.
- L'utilitaire **sosreport** collecte des détails de configuration, des journaux et des informations système à partir d'un système RHEL. Pour plus d'informations sur l'utilitaire **sosreport**, voir Qu'est-ce qu'un rapport sos et comment en créer un dans Red Hat Enterprise Linux ?

8.4. RESSOURCES SUPPLÉMENTAIRES

- Dépannage de l'installation des répliques IdM
- Dépannage de l'installation du client IdM

- Sauvegarde et restauration de l'IdM

CHAPITRE 9. DÉSINSTALLATION D'UN SERVEUR IDM

Cette procédure décrit comment désinstaller un serveur de gestion des identités (IdM) nommé **server123.idm.example.com** (server123).

Conditions préalables

- Vous avez un accès **root** au serveur123.
- Vous disposez des informations d'identification d'un administrateur IdM.

Procédure

1. Si votre environnement IdM utilise des DNS intégrés, assurez-vous que le serveur 123 n'est pas le seul serveur DNS **enabled**:

```
[root@server123 ~]# ipa server-role-find --role 'DNS server'
----------------------
2 server roles matched
----------------------
  Server name: server456.idm.example.com
  Role name: DNS server
  Role status: enabled
[...]
----------------------------
Number of entries returned 2
----------------------------
```

   Si server123 est le seul serveur DNS restant dans la topologie, ajoutez le rôle de serveur DNS à un autre serveur IdM. Pour plus d'informations, voir la page de manuel **ipa-dns-install(1)**.

2. Si votre environnement IdM utilise une autorité de certification (CA) intégrée :

   a. Assurez-vous que le serveur 123 n'est pas le seul serveur CA **enabled**:

```
[root@server123 ~]# ipa server-role-find --role 'CA server'
----------------------
2 server roles matched
----------------------
  Server name: server123.idm.example.com
  Role name: CA server
  Role status: enabled

  Server name: r8server.idm.example.com
  Role name: CA server
  Role status: enabled
----------------------------
Number of entries returned 2
----------------------------
```

   Si server123 est le seul serveur CA restant dans la topologie, ajoutez le rôle de serveur CA à un autre serveur IdM. Pour plus d'informations, voir la page de manuel **ipa-ca-install(1)**.

b. Si vous avez activé les chambres fortes dans votre environnement IdM, assurez-vous que server123.idm.example.com n'est pas le seul serveur **enabled** Key Recovery Authority (KRA) :

```
[root@server123 ~]# ipa server-role-find --role 'KRA server'
----------------------
2 server roles matched
----------------------
  Server name: server123.idm.example.com
  Role name: KRA server
  Role status: enabled

  Server name: r8server.idm.example.com
  Role name: KRA server
  Role status: enabled
----------------------------
Number of entries returned 2
----------------------------
```

Si server123 est le seul serveur KRA restant dans la topologie, ajoutez le rôle de serveur KRA à un autre serveur IdM. Pour plus d'informations, voir **man ipa-kra-install(1)**.

c. Assurez-vous que server123.idm.example.com n'est pas le serveur de renouvellement de l'autorité de certification :

```
[root@server123 ~]# ipa config-show | grep 'CA renewal'
  IPA CA renewal master: r8server.idm.example.com
```

Si server123 est le serveur de renouvellement de l'autorité de certification, voir Modification et réinitialisation du serveur de renouvellement de l'autorité de certification IdM pour plus d'informations sur la manière de déplacer le rôle de serveur de renouvellement de l'autorité de certification vers un autre serveur.

d. Assurez-vous que server123.idm.example.com n'est pas l'éditeur actuel de la liste de révocation des certificats (CRL) :

```
[root@server123 ~]# ipa-crlgen-manage status
CRL generation: disabled
```

Si la sortie montre que la génération de CRL est activée sur server123, voir Generating CRL on an IdM CA server pour plus d'informations sur la façon de déplacer le rôle d'éditeur de CRL vers un autre serveur.

3. Se connecter à un autre serveur IdM dans la topologie :

```
$ ssh idm_user@server456
```

4. Sur le serveur, obtenez les informations d'identification de l'administrateur IdM :

```
[idm_user@server456 ~]$ kinit admin
```

5. Affichez les plages d'ID DNA attribuées aux serveurs dans la topologie :

```
[idm_user@server456 ~]$ ipa-replica-manage dnarange-show
server123.idm.example.com: 1001-1500
```

```
server456.idm.example.com: 1501-2000
[...]
```

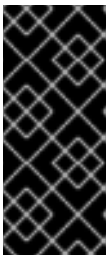
La sortie montre qu'une plage d'ID ADN est attribuée à la fois au serveur123 et au serveur456.

6. Si le serveur 123 est le seul serveur IdM de la topologie auquel une plage d'ID ADN a été attribuée, créez un utilisateur IdM de test sur le serveur 456 pour vous assurer qu'une plage d'ID ADN a été attribuée au serveur :

```
[idm_user@server456 ~]$ ipa user-add test_idm_user
```

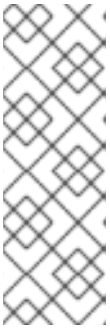
7. Supprimer server123.idm.example.com de la topologie :

```
[idm_user@server456 ~]$ ipa server-del server123.idm.example.com
```



IMPORTANT

Si la suppression de server123 entraîne une topologie déconnectée, le script vous en avertit. Pour plus d'informations sur la création d'un accord de réplication entre les répliques restantes afin que la suppression puisse avoir lieu, voir Configuration de la réplication entre deux serveurs à l'aide de l'interface de programmation.



NOTE

L'exécution de la commande **ipa server-del** supprime toutes les données de réplication et tous les accords liés au serveur123 pour les suffixes **domain** et **ca**. Contrairement aux topologies IdM de niveau 0 du domaine, où vous devez d'abord supprimer ces données à l'aide de la commande **ipa-replica-manage del *server123*** pour supprimer ces données. Les topologies IdM de niveau 0 sont celles qui fonctionnent sous RHEL 7.2 et les versions antérieures. Utilisez la commande **ipa domainlevel-get** pour afficher le niveau de domaine actuel.

8. Retournez sur server123.idm.example.com et désinstallez l'installation IdM existante :

```
[root@server123 ~]# ipa-server-install --uninstall
...
Are you sure you want to continue with the uninstall procedure? [no]: yes
```

9. Assurez-vous que tous les enregistrements DNS du serveur de noms (NS) pointant vers server123.idm.example.com sont supprimés de vos zones DNS. Cela s'applique indépendamment du fait que vous utilisiez un DNS intégré géré par IdM ou un DNS externe. Pour plus d'informations sur la manière de supprimer des enregistrements DNS de l'IdM, voir Suppression d'enregistrements DNS dans la CLI de l'IdM .

Ressources supplémentaires

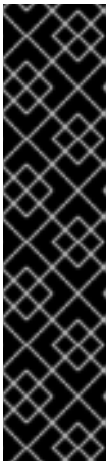
- Affichage et augmentation du niveau de domaine dans la documentation de RHEL 7
- Planification de la topologie du réplica
- Explication du serveur de renouvellement de l'autorité de certification IdM Génération de CRL sur un serveur de l'autorité de certification IdM

CHAPITRE 10. RENOMMER UN SERVEUR IDM

Vous ne pouvez pas modifier le nom d'hôte d'un serveur Identity Management (IdM) existant. Cependant, vous pouvez remplacer le serveur par une réplique portant un nom différent.

Procédure

1. Installez un nouveau réplica qui remplacera le serveur existant, en vous assurant que le réplica possède le nom d'hôte et l'adresse IP requis. Pour plus d'informations, voir Installation d'un réplica IdM.



IMPORTANT

Si le serveur que vous désinstallez est le serveur d'édition de la liste de révocation des certificats (CRL), faites d'un autre serveur le serveur d'édition de la CRL avant de continuer.

Pour plus de détails sur la manière de procéder dans le cadre d'une procédure de migration, voir les sections suivantes :

- Arrêt de la génération de CRL sur un serveur d'autorité de certification IdM RHEL 8
- Démarrage de la génération de CRL sur le nouveau serveur CA IdM RHEL 9

2. Arrêter l'instance existante du serveur IdM.

```
[root@old_server ~]# ipactl stop
```

3. Désinstallez le serveur existant comme décrit dans Désinstallation d'un serveur IdM .

CHAPITRE 11. MISE À JOUR ET RÉTROGRADATION DE L'IDM

11.1. MISE À JOUR DES PAQUETS IDM

Vous pouvez utiliser l'utilitaire **dnf** pour mettre à jour les paquets Identity Management (IdM) sur le système.

- Pour mettre à jour tous les paquets IdM qui sont pertinents pour votre profil et pour lesquels des mises à jour sont disponibles :

```
# dnf upgrade ipa-*
```

IMPORTANT

Avant d'installer une mise à jour, assurez-vous d'avoir appliqué tous les errata précédemment publiés concernant le système RHEL.

- Il est également possible d'installer ou de mettre à jour des paquets pour qu'ils correspondent à la dernière version disponible pour votre profil à partir de n'importe quel dépôt activé :

```
# dnf distro-sync ipa-*
```

Après avoir mis à jour les paquets IdM sur au moins un serveur, tous les autres serveurs de la topologie reçoivent le schéma mis à jour, même si vous ne mettez pas à jour leurs paquets. Cela garantit que toutes les nouvelles entrées qui utilisent le nouveau schéma peuvent être répliquées parmi les autres serveurs.

AVERTISSEMENT

Lorsque vous mettez à jour plusieurs serveurs IdM, attendez au moins 10 minutes après la mise à jour d'un serveur avant de mettre à jour un autre serveur. Toutefois, le temps réel nécessaire à la réussite de la mise à jour d'un serveur dépend de la topologie déployée, de la latence des connexions et du nombre de changements générés par la mise à jour.

Lorsque deux serveurs ou plus sont mis à jour simultanément ou avec de courts intervalles entre les mises à jour, il n'y a pas assez de temps pour répliquer les changements de données après la mise à jour dans toute la topologie, ce qui peut entraîner des événements de réplication conflictuels.

11.2. RÉTROGRADATION DES PAQUETS IDM

Red Hat ne prend pas en charge la rétrogradation de la gestion des identités.

11.3. RESSOURCES SUPPLÉMENTAIRES

- **dnf(8)** page de manuel

CHAPITRE 12. PRÉPARATION DU SYSTÈME POUR L'INSTALLATION DU CLIENT IDM

Ce chapitre décrit les conditions que doit remplir votre système pour installer un client de gestion d'identité (IdM).

12.1. EXIGENCES DNS POUR LES CLIENTS IDM

Par défaut, le programme d'installation du client tente de rechercher les enregistrements DNS SRV **_ldap._tcp.DOMAIN** pour tous les domaines qui sont parents de son nom d'hôte. Par exemple, si une machine cliente a un nom d'hôte **client1.idm.example.com**, le programme d'installation essaiera de récupérer le nom d'hôte d'un serveur IdM à partir des enregistrements DNS SRV **_ldap._tcp.idm.example.com**, **_ldap._tcp.example.com** et **_ldap._tcp.com**, respectivement. Le domaine découvert est ensuite utilisé pour configurer les composants du client (par exemple, SSSD et Kerberos 5) sur la machine.

Toutefois, les noms d'hôte des clients IdM ne doivent pas nécessairement faire partie du domaine DNS primaire. Si le nom d'hôte de la machine cliente ne se trouve pas dans un sous-domaine d'un serveur IdM, transmettez le domaine IdM en tant qu'option **--domain** de la commande **ipa-client-install**. Dans ce cas, après l'installation du client, les composants SSSD et Kerberos auront le domaine défini dans leurs fichiers de configuration et l'utiliseront pour découvrir automatiquement les serveurs IdM.

Ressources supplémentaires

- Pour plus d'informations sur les exigences en matière de DNS dans IdM, voir les exigences en matière de nom d'hôte et de DNS pour IdM.

12.2. EXIGENCES EN MATIÈRE DE PORT POUR LES CLIENTS IDM

Les clients de la gestion de l'identité (IdM) se connectent à un certain nombre de ports sur les serveurs IdM pour communiquer avec leurs services.

Sur le client IdM, ces ports doivent être ouverts *in the outgoing direction*. Si vous utilisez un pare-feu qui ne filtre pas les paquets sortants, tel que **firewalld**, les ports sont déjà disponibles dans la direction sortante.

Ressources supplémentaires

- Pour plus d'informations sur les ports spécifiques utilisés, voir Exigences en matière de ports pour IdM.

12.3. EXIGENCES IPV6 POUR LES CLIENTS IDM

La gestion des identités (IdM) n'exige pas que le protocole **IPv6** soit activé dans le noyau de l'hôte que vous souhaitez inscrire à IdM. Par exemple, si votre réseau interne n'utilise que le protocole **IPv4**, vous pouvez configurer le System Security Services Daemon (SSSD) pour qu'il n'utilise que **IPv4** pour communiquer avec le serveur IdM. Pour ce faire, insérez la ligne suivante dans la section **[domain/*NAME*]** du fichier **/etc/sssd/sssd.conf**:

```
lookup_family_order = ipv4_only
```

Ressources supplémentaires

- Pour plus d'informations sur l'option **lookup_family_order**, voir la page de manuel **sssd.conf(5)**.

12.4. INSTALLATION DES PAQUETS REQUIS POUR UN CLIENT IDM

L'installation du paquet **ipa-client** entraîne automatiquement l'installation d'autres paquets nécessaires en tant que dépendances, tels que les paquets System Security Services Daemon (SSSD).

Procédure

- Installez le paquetage **ipa-client**:

```
# dnf install ipa-client
```

CHAPITRE 13. INSTALLATION D'UN CLIENT IDM

Les sections suivantes décrivent comment configurer un système en tant que client IdM (Identity Management) à l'aide de l'utilitaire **ipa-client-install**. La configuration d'un système en tant que client IdM l'inscrit dans un domaine IdM et permet au système d'utiliser les services IdM sur les serveurs IdM du domaine.

Pour installer avec succès un client de gestion d'identité (IdM), vous devez fournir des informations d'identification qui peuvent être utilisées pour enrôler le client.

13.1. CONDITIONS PRÉALABLES

- Vous avez préparé le système pour l'installation du client IdM. Pour plus de détails, voir Préparation du système pour l'installation du client IdM .

13.2. INSTALLATION D'UN CLIENT À L'AIDE DES INFORMATIONS D'IDENTIFICATION DE L'UTILISATEUR : INSTALLATION INTERACTIVE

Cette procédure décrit l'installation d'un client de gestion d'identité (IdM) de manière interactive en utilisant les informations d'identification d'un utilisateur autorisé pour inscrire le système dans le domaine.

Conditions préalables

- Assurez-vous que vous disposez des informations d'identification d'un utilisateur autorisé à inscrire des clients dans le domaine IdM. Il peut s'agir, par exemple, d'un utilisateur de **hostadmin** ayant le rôle d'administrateur d'inscription.

Procédure

1. Exécutez l'utilitaire **ipa-client-install** sur le système que vous souhaitez configurer en tant que client IdM.

```
# ipa-client-install --mkhomedir
```

   Ajoutez l'option **--enable-dns-updates** pour mettre à jour les enregistrements DNS avec l'adresse IP du système client si l'une des conditions suivantes s'applique :

   - Le serveur IdM auprès duquel le client sera enrôlé a été installé avec un DNS intégré
   - Le serveur DNS sur le réseau accepte les mises à jour des entrées DNS avec le protocole GSS-TSIG

```
# ipa-client-install --enable-dns-updates --mkhomedir
```

   L'activation des mises à jour DNS est utile si votre client :

   - possède une adresse IP dynamique émise à l'aide du protocole de configuration dynamique de l'hôte (Dynamic Host Configuration Protocol)
   - possède une adresse IP statique mais celle-ci vient d'être attribuée et le serveur IdM n'en a pas connaissance

2. Le script d'installation tente d'obtenir automatiquement tous les paramètres requis, tels que les enregistrements DNS.

   - Si les enregistrements SRV sont correctement définis dans la zone DNS IdM, le script découvre automatiquement toutes les autres valeurs requises et les affiche. Saisissez **yes** pour confirmer.

     ```
     Client hostname: client.example.com
     Realm: EXAMPLE.COM
     DNS Domain: example.com
     IPA Server: server.example.com
     BaseDN: dc=example,dc=com

     Continue to configure the system with these values? [no]: yes
     ```

   - Pour installer le système avec des valeurs différentes, entrez **no**. Exécutez ensuite à nouveau **ipa-client-install** et spécifiez les valeurs requises en ajoutant des options de ligne de commande à **ipa-client-install**, par exemple :

     - **--hostname**
     - **--realm**
     - **--domain**
     - **--server**
     - **--mkhomedir**

     IMPORTANT

     Le nom de domaine pleinement qualifié doit être un nom DNS valide :

     - Seuls les chiffres, les caractères alphabétiques et les traits d'union (**-**) sont autorisés. Par exemple, les caractères de soulignement ne sont pas autorisés et peuvent entraîner des défaillances du système DNS.
     - Le nom d'hôte doit être en minuscules. Aucune majuscule n'est autorisée.

   - Si le script ne parvient pas à obtenir certains paramètres automatiquement, il vous demande de fournir les valeurs.

3. Le script demande un utilisateur dont l'identité sera utilisée pour inscrire le client. Il peut s'agir, par exemple, d'un utilisateur **hostadmin** ayant le rôle d'administrateur d'inscription :

   ```
   User authorized to enroll computers: hostadmin
   Password for hostadmin@EXAMPLE.COM:
   ```

4. Le script d'installation configure maintenant le client. Attendez la fin de l'opération.

   ```
   Client configuration complete.
   ```

Ressources supplémentaires

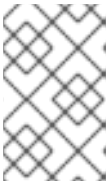
- Pour plus de détails sur la manière dont le script d'installation du client recherche les enregistrements DNS, voir la section **DNS Autodiscovery** dans la page de manuel **ipa-client-install**(1).

13.3. INSTALLATION D'UN CLIENT À L'AIDE D'UN MOT DE PASSE À USAGE UNIQUE : INSTALLATION INTERACTIVE

Cette procédure décrit l'installation d'un client Identity Management (IdM) de manière interactive en utilisant un mot de passe à usage unique pour inscrire le système dans le domaine.

Conditions préalables

- Sur un serveur du domaine, ajoutez le futur système client en tant qu'hôte IdM. Utilisez l'option **--random** avec la commande **ipa host-add** pour générer un mot de passe aléatoire à usage unique pour l'inscription.



NOTE

La commande **ipa host-add <client_fqdn>** exige que le FQDN du client puisse être résolu par le DNS. S'il n'est pas résoluble, fournissez l'adresse IP du système client IdM à l'aide de l'option **--ip address** ou utilisez l'option **--force**.

```
$ ipa host-add client.example.com --random
 ----------------------------------------------------
 Added host "client.example.com"
 ----------------------------------------------------
  Host name: client.example.com
  Random password: W5YpARl=7M.n
  Password: True
  Keytab: False
  Managed by: server.example.com
```

NOTE

Le mot de passe généré deviendra invalide lorsque vous l'utiliserez pour inscrire la machine dans le domaine IdM. Il sera remplacé par un keytab hôte approprié une fois l'enrôlement terminé.

Procédure

1. Exécutez l'utilitaire **ipa-client-install** sur le système que vous souhaitez configurer en tant que client IdM.
   Utilisez l'option **--password** pour fournir un mot de passe aléatoire à usage unique. Comme le mot de passe contient souvent des caractères spéciaux, mettez-le entre guillemets simples (').

```
# ipa-client-install --mkhomedir --password=password
```

   Ajoutez l'option **--enable-dns-updates** pour mettre à jour les enregistrements DNS avec l'adresse IP du système client si l'une des conditions suivantes s'applique :

   - Le serveur IdM auprès duquel le client sera enrôlé a été installé avec un DNS intégré

- Le serveur DNS sur le réseau accepte les mises à jour des entrées DNS avec le protocole GSS-TSIG

```
# ipa-client-install --password 'W5YpARl=7M.n' --enable-dns-updates --mkhomedir
```

L'activation des mises à jour DNS est utile si votre client :

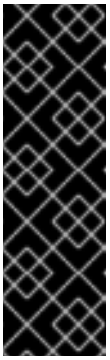
- possède une adresse IP dynamique émise à l'aide du protocole de configuration dynamique de l'hôte (Dynamic Host Configuration Protocol)
- possède une adresse IP statique mais celle-ci vient d'être attribuée et le serveur IdM n'en a pas connaissance

2. Le script d'installation tente d'obtenir automatiquement tous les paramètres requis, tels que les enregistrements DNS.
   - Si les enregistrements SRV sont correctement définis dans la zone DNS IdM, le script découvre automatiquement toutes les autres valeurs requises et les affiche. Saisissez **yes** pour confirmer.

```
Client hostname: client.example.com
Realm: EXAMPLE.COM
DNS Domain: example.com
IPA Server: server.example.com
BaseDN: dc=example,dc=com

Continue to configure the system with these values? [no]: yes
```

   - Pour installer le système avec des valeurs différentes, entrez **no**. Exécutez ensuite à nouveau **ipa-client-install** et spécifiez les valeurs requises en ajoutant des options de ligne de commande à **ipa-client-install**, par exemple :
     - **--hostname**
     - **--realm**
     - **--domain**
     - **--server**
     - **--mkhomedir**



IMPORTANT

Le nom de domaine pleinement qualifié doit être un nom DNS valide :

- Seuls les chiffres, les caractères alphabétiques et les traits d'union (**-**) sont autorisés. Par exemple, les caractères de soulignement ne sont pas autorisés et peuvent entraîner des défaillances du système DNS.
- Le nom d'hôte doit être en minuscules. Aucune majuscule n'est autorisée.

   - Si le script ne parvient pas à obtenir certains paramètres automatiquement, il vous demande de fournir les valeurs.

3. Le script d'installation configure maintenant le client. Attendez la fin de l'opération.

```
Client configuration complete.
```

Ressources supplémentaires

- Pour plus de détails sur la manière dont le script d'installation du client recherche les enregistrements DNS, voir la section **DNS Autodiscovery** dans la page de manuel **ipa-client-install**(1).

13.4. INSTALLATION D'UN CLIENT : INSTALLATION NON INTERACTIVE

Pour une installation non interactive, vous devez fournir toutes les informations nécessaires à l'utilitaire **ipa-client-install** à l'aide des options de la ligne de commande. Les sections suivantes décrivent les options minimales requises pour une installation non interactive.

Options pour la méthode d'authentification prévue pour l'inscription du client

Les options disponibles sont les suivantes :

- **--principal** et **--password** pour spécifier les informations d'identification d'un utilisateur autorisé à inscrire des clients
- **--random** pour spécifier un mot de passe aléatoire généré une seule fois pour le client
- **--keytab** pour spécifier le keytab d'une inscription précédente

La possibilité d'une installation sans surveillance

L'option **--unattended** permet d'exécuter l'installation sans demander la confirmation de l'utilisateur. Si les enregistrements SRV sont correctement définis dans la zone DNS IdM, le script découvre automatiquement toutes les autres valeurs requises. Si le script ne peut pas découvrir les valeurs automatiquement, fournissez-les à l'aide d'options de ligne de commande, telles que :

- **--hostname** pour spécifier un nom de domaine entièrement qualifié (FQDN) statique pour la machine cliente.

IMPORTANT

Le FQDN doit être un nom DNS valide :

  - Seuls les chiffres, les caractères alphabétiques et les traits d'union (-) sont autorisés. Par exemple, les caractères de soulignement ne sont pas autorisés et peuvent entraîner des défaillances du système DNS.
  - Le nom d'hôte doit être en minuscules. Aucune majuscule n'est autorisée.

- **--domain** pour spécifier le domaine DNS primaire d'un déploiement IdM existant, par exemple example.com. Le nom est une version minuscule du nom du domaine Kerberos de l'IdM.
- **--server** pour spécifier le FQDN du serveur IdM auquel se connecter. Lorsque cette option est utilisée, la recherche automatique de DNS pour Kerberos est désactivée et une liste fixe de serveurs KDC et Admin est configurée. Dans des circonstances normales, cette option n'est pas nécessaire car la liste des serveurs est récupérée à partir du domaine DNS IdM primaire.

- **--realm** pour spécifier le domaine Kerberos d'un déploiement IdM existant. Il s'agit généralement d'une version en majuscules du domaine DNS primaire utilisé par l'installation IdM. Dans des circonstances normales, cette option n'est pas nécessaire car le nom du domaine est récupéré à partir du serveur IdM.

Exemple de commande de base **ipa-client-install** pour une installation non interactive :

```
# ipa-client-install --password 'W5YpARl=7M.n' --mkhomedir --unattended
```

Exemple de commande **ipa-client-install** pour une installation non interactive avec plus d'options spécifiées :

```
# ipa-client-install --password 'W5YpARl=7M.n' --domain idm.example.com --server
server.idm.example.com --realm IDM.EXAMPLE.COM --mkhomedir --unattended
```

Ressources supplémentaires

- Pour une liste complète des options acceptées par **ipa-client-install**, voir la page de manuel **ipa-client-install** (1).

13.5. SUPPRESSION DE LA CONFIGURATION PRÉ-IDM APRÈS L'INSTALLATION D'UN CLIENT

Le script **ipa-client-install** ne supprime pas les configurations LDAP et System Security Services Daemon (SSSD) des fichiers **/etc/openldap/ldap.conf** et **/etc/sssd/sssd.conf**. Si vous avez modifié la configuration de ces fichiers avant d'installer le client, le script ajoute les nouvelles valeurs du client, mais les commente. Par exemple, le script ajoute les valeurs du nouveau client, mais les commente :

```
BASE   dc=example,dc=com
URI    ldap://ldap.example.com

#URI ldaps://server.example.com # modified by IPA
#BASE dc=ipa,dc=example,dc=com # modified by IPA
```

Pour appliquer les nouvelles valeurs de configuration Identity Management (IdM)} :

1. Ouvrez **/etc/openldap/ldap.conf** et **/etc/sssd/sssd.conf**.
2. Effacer la configuration précédente.
3. Décommenter la nouvelle configuration IdM.
4. Les processus de serveur qui reposent sur une configuration LDAP à l'échelle du système peuvent nécessiter un redémarrage pour appliquer les modifications. Les applications qui utilisent les bibliothèques **openldap** importent généralement la configuration lorsqu'elles sont lancées.

13.6. TEST D'UN CLIENT IDM

L'interface de ligne de commande vous informe que le site **ipa-client-install** a réussi, mais vous pouvez également effectuer votre propre test.

Pour vérifier que le client Identity Management (IdM) peut obtenir des informations sur les utilisateurs définis sur le serveur, vérifiez que vous êtes en mesure de résoudre un utilisateur défini sur le serveur. Par exemple, pour vérifier l'utilisateur par défaut **admin**:

```
[user@client ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

Pour tester le bon fonctionnement de l'authentification, **su** doit être utilisé par un utilisateur root à partir d'un utilisateur non-root :

```
[user@client ~]$ su -
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[root@client ~]#
```

13.7. CONNEXIONS EFFECTUÉES LORS DE L'INSTALLATION D'UN CLIENT IDM

Requêtes effectuées lors de l'installation d'un client IdM énumère les opérations effectuées par **ipa-client-install**, l'outil d'installation du client Identity Management (IdM).

Tableau 13.1. Demandes effectuées lors de l'installation d'un client IdM

Fonctionnement	Protocole utilisé	Objectif
Résolution DNS par rapport aux résolveurs DNS configurés sur le système client	DNS	Pour découvrir les adresses IP des serveurs IdM ; (optionnellement) pour ajouter des enregistrements A/AAAA et SSHFP
Demandes adressées aux ports 88 (TCP/TCP6 et UDP/UDP6) d'une réplique IdM	Kerberos	Pour obtenir un ticket Kerberos
Appels JSON-RPC au service web IdM Apache sur les serveurs IdM découverts ou configurés	HTTPS	Inscription du client IdM ; recherche de la chaîne de certificats de l'autorité de certification en cas d'échec de la méthode LDAP ; demande de délivrance d'un certificat si nécessaire
Requêtes via TCP/TCP6 vers les ports 389 des serveurs IdM, en utilisant l'authentification SASL GSSAPI, LDAP simple, ou les deux	LDAP	Inscription du client IdM ; récupération de l'identité par les processus SSSD ; récupération de la clé Kerberos pour le principal de l'hôte
Découverte et résolution du protocole de temps réseau (NTP) (en option)	NTP	Pour synchroniser l'heure entre le système client et un serveur NTP

13.8. LES COMMUNICATIONS DU CLIENT IDM AVEC LE SERVEUR PENDANT LE DÉPLOIEMENT POST-INSTALLATION

Le côté client du cadre de gestion de l'identité (IdM) est mis en œuvre avec deux applications différentes :

- l'interface de ligne de commande (CLI) **ipa**
- (*optional*) l'interface utilisateur Web basée sur un navigateur

Les opérations de post-installation CLI montrent les opérations effectuées par le CLI pendant le déploiement post-installation d'un client IdM. Les opérations de post-installation de l'interface Web montrent les opérations effectuées par l'interface Web pendant le déploiement post-installation d'un client IdM.

Tableau 13.2. Opérations post-installation CLI

Fonctionnement	Protocole utilisé	Objectif
Résolution DNS par rapport aux résolveurs DNS configurés sur le système client	DNS	Pour découvrir les adresses IP des serveurs IdM
Requêtes vers les ports 88 (TCP/TCP6 et UDP/UDP6) et 464 (TCP/TCP6 et UDP/UDP6) sur une réplique IdM	Kerberos	Pour obtenir un ticket Kerberos, modifier un mot de passe Kerberos, s'authentifier auprès de l'interface Web de l'IdM
Appels JSON-RPC au service web IdM Apache sur les serveurs IdM découverts ou configurés	HTTPS	toute utilisation de services publics **ipa**

Tableau 13.3. Opérations post-installation de l'interface Web

Fonctionnement	Protocole utilisé	Objectif
Appels JSON-RPC au service web IdM Apache sur les serveurs IdM découverts ou configurés	HTTPS	Pour récupérer les pages de l'interface Web IdM

Ressources supplémentaires

- SSSD communication patterns pour plus d'informations sur la façon dont le démon **SSSD** communique avec les services disponibles sur les serveurs IdM et Active Directory.
- Certmonger communication patterns pour plus d'informations sur la façon dont le démon **certmonger** communique avec les services disponibles sur les serveurs IdM et Active Directory.

13.9. MODÈLES DE COMMUNICATION SSSD

Le System Security Services Daemon (SSSD) est un service système qui permet d'accéder aux répertoires distants et aux mécanismes d'authentification. S'il est configuré sur un client IdM de gestion

d'identité, il se connecte au serveur IdM, qui fournit l'authentification, l'autorisation et d'autres informations relatives à l'identité et à la stratégie. Si le serveur IdM est en relation de confiance avec Active Directory (AD), SSSD se connecte également à AD pour effectuer l'authentification des utilisateurs AD à l'aide du protocole Kerberos. Par défaut, SSSD utilise Kerberos pour authentifier tout utilisateur non local. Dans des situations particulières, SSSD peut être configuré pour utiliser le protocole LDAP à la place.

Le SSSD peut être configuré pour communiquer avec plusieurs serveurs. Les tableaux ci-dessous présentent les schémas de communication courants pour le SSSD dans l'IdM.

Tableau 13.4. Modèles de communication de SSSD sur les clients IdM lorsqu'ils communiquent avec les serveurs IdM

Fonctionnement	Protocole utilisé	Objectif
Résolution DNS par rapport aux résolveurs DNS configurés sur le système client	DNS	Pour découvrir les adresses IP des serveurs IdM
Requêtes vers les ports 88 (TCP/TCP6 et UDP/UDP6), 464 (TCP/TCP6 et UDP/UDP6) et 749 (TCP/TCP6) sur une réplique de gestion des identités et des contrôleurs de domaine Active Directory	Kerberos	Pour obtenir un ticket Kerberos ; pour modifier un mot de passe Kerberos
Requêtes via TCP/TCP6 vers les ports 389 des serveurs IdM, en utilisant l'authentification SASL GSSAPI, LDAP simple, ou les deux	LDAP	Pour obtenir des informations sur les utilisateurs et les hôtes IdM, télécharger les règles HBAC et sudo, les cartes automount, le contexte utilisateur SELinux, les clés SSH publiques et d'autres informations stockées dans le LDAP IdM
(facultativement) En cas d'authentification par carte à puce, les demandes adressées au serveur OCSP (Online Certificate Status Protocol), s'il est configuré. Cela se fait souvent via le port 80, mais cela dépend de la valeur réelle de l'URL du répondeur OCSP dans le certificat du client.	HTTP	Pour obtenir des informations sur l'état du certificat installé dans la carte à puce

Tableau 13.5. Modèles de communication de SSSD sur les serveurs IdM agissant en tant qu'agents de confiance lorsqu'ils communiquent avec les contrôleurs de domaine Active Directory

Fonctionnement	Protocole utilisé	Objectif
Résolution DNS par rapport aux résolveurs DNS configurés sur le système client	DNS	Pour découvrir les adresses IP des serveurs IdM

Fonctionnement	Protocole utilisé	Objectif
Requêtes vers les ports 88 (TCP/TCP6 et UDP/UDP6), 464 (TCP/TCP6 et UDP/UDP6) et 749 (TCP/TCP6) sur une réplique de gestion des identités et des contrôleurs de domaine Active Directory	Kerberos	Obtenir un ticket Kerberos ; modifier un mot de passe Kerberos ; administrer Kerberos à distance
Requêtes vers les ports 389 (TCP/TCP6 et UDP/UDP6) et 3268 (TCP/TCP6)	LDAP	Pour interroger les informations sur les utilisateurs et les groupes d'Active Directory ; pour découvrir les contrôleurs de domaine d'Active Directory
(facultativement) En cas d'authentification par carte à puce, les demandes adressées au serveur OCSP (Online Certificate Status Protocol), s'il est configuré. Cela se fait souvent via le port 80, mais cela dépend de la valeur réelle de l'URL du répondeur OCSP dans le certificat du client.	HTTP	Pour obtenir des informations sur l'état du certificat installé dans la carte à puce

Ressources supplémentaires

- Les communications du client IdM avec le serveur pendant le déploiement post-installation

13.10. MODÈLES DE COMMUNICATION DE CERTMONGER

Certmonger est un démon qui s'exécute sur les serveurs et les clients de gestion d'identité (IdM) pour permettre le renouvellement en temps utile des certificats SSL associés aux services sur l'hôte. Le site Tableau 13.6, « Modèles de communication de Certmonger » montre les opérations effectuées par l'utilitaire **certmonger** sur les serveurs IdM.

Tableau 13.6. Modèles de communication de Certmonger

Fonctionnement	Protocole utilisé	Objectif
Résolution DNS par rapport aux résolveurs DNS configurés sur le système client	DNS	Pour découvrir les adresses IP des serveurs IdM
Requêtes vers les ports 88 (TCP/TCP6 et UDP/UDP6) et 464 (TCP/TCP6 et UDP/UDP6) sur une réplique IdM	Kerberos	Pour obtenir un ticket Kerberos
Appels JSON-RPC au service web IdM Apache sur les serveurs IdM découverts ou configurés	HTTPS	Pour demander de nouveaux certificats

Fonctionnement	Protocole utilisé	Objectif
Accès par le port 8080 (TCP/TCP6) sur le serveur IdM	HTTP	Pour obtenir un répondeur OCSP (Online Certificate Status Protocol) et l'état d'un certificat
(sur le premier serveur installé ou sur le serveur où le suivi des certificats a été transféré) Accès par le port 8443 (TCP/TCP6) sur le serveur IdM	HTTPS	Pour administrer l'autorité de certification sur le serveur IdM (uniquement lors de l'installation du serveur IdM et des répliques), **certmonger** sur le serveur ne contacte que son propre serveur local sur les ports 8080 et 8443 pour le renouvellement des certificats liés à l'autorité de certification.

Ressources supplémentaires

- Les communications du client IdM avec le serveur pendant le déploiement post-installation

CHAPITRE 14. INSTALLATION D'UN CLIENT IDM AVEC KICKSTART

Une inscription Kickstart ajoute automatiquement un nouveau système au domaine Identity Management (IdM) au moment de l'installation de Red Hat Enterprise Linux.

14.1. INSTALLATION D'UN CLIENT AVEC KICKSTART

Cette procédure décrit comment utiliser un fichier Kickstart pour installer un client Identity Management (IdM).

Conditions préalables

- Ne démarrez pas le service **sshd** avant l'inscription kickstart. Le démarrage de **sshd** avant l'inscription du client génère automatiquement les clés SSH, mais le fichier Kickstart de Section 14.2, « Fichier de démarrage pour l'installation du client » utilise un script dans le même but, ce qui est la solution préférée.

Procédure

1. Pré-créer l'entrée de l'hôte sur le serveur IdM et définir un mot de passe temporaire pour l'entrée :

   ```
   $ ipa host-add client.example.com --password=secret
   ```

   Le mot de passe est utilisé par Kickstart pour s'authentifier lors de l'installation du client et expire après la première tentative d'authentification. Une fois que le client est installé avec succès, il s'authentifie à l'aide de sa table de clés.

2. Créez un fichier Kickstart avec le contenu décrit dans Section 14.2, « Fichier de démarrage pour l'installation du client ». Assurez-vous que le réseau est correctement configuré dans le fichier Kickstart à l'aide de la commande **network**.

3. Utilisez le fichier Kickstart pour installer le client IdM.

14.2. FICHIER DE DÉMARRAGE POUR L'INSTALLATION DU CLIENT

Cette section décrit le contenu d'un fichier kickstart que vous pouvez utiliser pour installer un client Identity Management (IdM).

Le paquet **ipa-client** dans la liste des paquets à installer

Ajoutez le paquet **ipa-client** à la section %packages du fichier kickstart. Par exemple :

```
%packages
...
ipa-client
...
```

Instructions post-installation pour le client IdM

Les instructions postérieures à l'installation doivent comprendre

- Une instruction pour s'assurer que les clés SSH sont générées avant l'inscription

- Une instruction pour exécuter l'utilitaire **ipa-client-install**, tout en spécifiant :
  - Toutes les informations nécessaires pour accéder et configurer les services du domaine IdM
  - Le mot de passe que vous avez défini lors de la pré-création de l'hôte client sur le serveur IdM. dans Section 14.1, « Installation d'un client avec Kickstart » .

Par exemple, les instructions de post-installation pour une installation kickstart qui utilise un mot de passe à usage unique et récupère les options requises à partir de la ligne de commande plutôt que via le DNS peuvent ressembler à ceci :

```
%post --log=/root/ks-post.log

# Generate SSH keys; ipa-client-install uploads them to the IdM server by default
/usr/libexec/openssh/sshd-keygen rsa

# Run the client install script
/usr/sbin/ipa-client-install --hostname=client.example.com --domain=EXAMPLE.COM --enable-dns-updates --mkhomedir -w secret --realm=EXAMPLE.COM --server=server.example.com
```

En option, vous pouvez également inclure d'autres options dans le fichier Kickstart, telles que :

- Pour une installation non interactive, ajoutez l'option **--unattended** à **ipa-client-install**.
- Pour permettre au script d'installation du client de demander un certificat pour la machine :
  - Ajouter l'option **--request-cert** à **ipa-client-install**.
  - Définissez l'adresse du bus système sur **/dev/null** pour les utilitaires **getcert** et **ipa-client-install** dans l'environnement Kickstart **chroot**. Pour ce faire, ajoutez ces lignes aux instructions post-installation du fichier Kickstart avant l'instruction **ipa-client-install**:

    ```
    # env DBUS_SYSTEM_BUS_ADDRESS=unix:path=/dev/null getcert list
    # env DBUS_SYSTEM_BUS_ADDRESS=unix:path=/dev/null ipa-client-install
    ```

14.3. TEST D'UN CLIENT IDM

L'interface de ligne de commande vous informe que le site **ipa-client-install** a réussi, mais vous pouvez également effectuer votre propre test.

Pour vérifier que le client Identity Management (IdM) peut obtenir des informations sur les utilisateurs définis sur le serveur, vérifiez que vous êtes en mesure de résoudre un utilisateur défini sur le serveur. Par exemple, pour vérifier l'utilisateur par défaut **admin**:

```
[user@client ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

Pour tester le bon fonctionnement de l'authentification, **su** doit être utilisé par un utilisateur root à partir d'un utilisateur non-root :

```
[user@client ~]$ su -
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[root@client ~]#
```

CHAPITRE 15. DÉPANNAGE DE L'INSTALLATION DU CLIENT IDM

Les sections suivantes décrivent comment recueillir des informations sur l'échec de l'installation d'un client IdM et comment résoudre les problèmes d'installation les plus courants.

15.1. EXAMEN DES ERREURS D'INSTALLATION DU CLIENT IDM

Lorsque vous installez un client Identity Management (IdM), des informations de débogage sont ajoutées à **/var/log/ipaclient-install.log**. Si l'installation d'un client échoue, le programme d'installation consigne l'échec et annule les modifications apportées à l'hôte. La raison de l'échec de l'installation peut ne pas figurer à la fin du fichier journal, car le programme d'installation consigne également la procédure d'annulation.

Pour dépanner une installation défaillante du client IdM, examinez les lignes intitulées **ScriptError** dans le fichier **/var/log/ipaclient-install.log** et utilisez ces informations pour résoudre les problèmes correspondants.

Conditions préalables

- Vous devez avoir les privilèges **root** pour afficher le contenu des fichiers journaux IdM.

Procédure

1. Utilisez l'utilitaire **grep** pour récupérer toutes les occurrences du mot-clé **ScriptError** dans le fichier **/var/log/ipaserver-install.log**.

```
[user@server ~]$ sudo grep ScriptError /var/log/ipaclient-install.log
[sudo] password for user:
2020-05-28T18:24:50Z DEBUG The ipa-client-install command failed, exception:
ScriptError: One of password / principal / keytab is required.
```

2. Pour consulter un fichier journal de manière interactive, ouvrez la fin du fichier journal à l'aide de l'utilitaire **less** et utilisez les touches fléchées ↑ et ↓ pour naviguer.

```
[user@server ~]$ sudo less -N G /var/log/ipaclient-install.log
```

Ressources supplémentaires

- Si vous ne parvenez pas à résoudre une installation défaillante du client IdM et que vous disposez d'un abonnement au support technique de Red Hat, ouvrez un dossier de support technique sur le portail client de Red Hat et fournissez une copie du client à l'adresse **sosreport**.
- L'utilitaire **sosreport** collecte des détails de configuration, des journaux et des informations système à partir d'un système RHEL. Pour plus d'informations sur l'utilitaire **sosreport**, voir Qu'est-ce qu'un rapport sos et comment en créer un dans Red Hat Enterprise Linux ?

15.2. RÉSOLUTION DES PROBLÈMES SI L'INSTALLATION DU CLIENT NE PARVIENT PAS À METTRE À JOUR LES ENREGISTREMENTS DNS

Le programme d'installation du client IdM émet des commandes **nsupdate** pour créer des enregistrements PTR, SSHFP et d'autres enregistrements DNS. Cependant, le processus d'installation

échoue si le client n'est pas en mesure de mettre à jour les enregistrements DNS après l'installation et la configuration du logiciel client.

Pour résoudre ce problème, vérifiez la configuration et examinez les erreurs DNS sur **/var/log/client-install.log**.

Conditions préalables

- Vous utilisez IdM DNS comme solution DNS pour votre environnement IdM

Procédure

1. Assurez-vous que les mises à jour dynamiques de la zone DNS dans laquelle se trouve le client sont activées :

```
[user@server ~]$ ipa dnszone-mod idm.example.com. --dynamic-update=TRUE
```

2. Assurez-vous que le serveur IdM exécutant le service DNS a le port 53 ouvert pour les protocoles TCP et UDP.

```
[user@server ~]$ sudo firewall-cmd --permanent --add-port=53/tcp --add-port=53/udp
[sudo] password for user:
success
[user@server ~]$ firewall-cmd --runtime-to-permanent
success
```

3. Utilisez l'utilitaire **grep** pour récupérer le contenu des commandes **nsupdate** à partir de **/var/log/client-install.log** afin de voir quelles mises à jour d'enregistrements DNS échouent.

```
[user@server ~]$ sudo grep nsupdate /var/log/ipaclient-install.log
```

Ressources supplémentaires

- Si vous ne parvenez pas à résoudre une installation défaillante et que vous disposez d'un abonnement à l'assistance technique de Red Hat, ouvrez un dossier d'assistance technique sur le portail client de Red Hat et fournissez une adresse **sosreport** du client.
- L'utilitaire **sosreport** collecte des détails de configuration, des journaux et des informations système à partir d'un système RHEL. Pour plus d'informations sur l'utilitaire **sosreport**, voir Qu'est-ce qu'un rapport sos et comment en créer un dans Red Hat Enterprise Linux ?

15.3. RÉSOLUTION DES PROBLÈMES SI L'INSTALLATION DU CLIENT NE PARVIENT PAS À REJOINDRE LA ZONE KERBEROS IDM

Le processus d'installation du client IdM échoue si le client n'est pas en mesure de rejoindre le domaine Kerberos IdM.

```
Joining realm failed: Failed to add key to the keytab
child exited with 11

Installation failed. Rolling back changes.
```

Cet échec peut être causé par un keytab Kerberos vide.

Conditions préalables

- La suppression des fichiers système requiert les privilèges de **root**.

Procédure

1. Retirer **/etc/krb5.keytab**.

```
[user@client ~]$ sudo rm /etc/krb5.keytab
[sudo] password for user:
[user@client ~]$ ls /etc/krb5.keytab
ls: cannot access '/etc/krb5.keytab': No such file or directory
```

2. Réessayer l'installation du client IdM.

Ressources supplémentaires

- Si vous ne parvenez pas à résoudre une installation défaillante et que vous disposez d'un abonnement à l'assistance technique de Red Hat, ouvrez un dossier d'assistance technique sur le portail client de Red Hat et fournissez une adresse **sosreport** du client.
- L'utilitaire **sosreport** collecte des détails de configuration, des journaux et des informations système à partir d'un système RHEL. Pour plus d'informations sur l'utilitaire **sosreport**, voir Qu'est-ce qu'un rapport sos et comment en créer un dans Red Hat Enterprise Linux ?

15.4. RESSOURCES SUPPLÉMENTAIRES

- Pour résoudre les problèmes liés à l'installation du premier serveur IdM, voir Résolution des problèmes liés à l'installation du serveur IdM.
- Pour résoudre les problèmes liés à l'installation d'un réplica IdM, voir Résolution des problèmes liés à l'installation d'un réplica IdM.

CHAPITRE 16. RÉINSCRIPTION D'UN CLIENT IDM

16.1. RÉINSCRIPTION DU CLIENT À L'IDM

Cette section décrit comment réinscrire un client de gestion d'identité (IdM).

Si une machine cliente a été détruite et a perdu la connexion avec les serveurs IdM, par exemple en raison d'une défaillance matérielle du client, et que vous disposez toujours de son keytab, vous pouvez réinscrire le client. Dans ce scénario, vous souhaitez que le client soit réintégré dans l'environnement IdM avec le même nom d'hôte.

Pendant le réenrôlement, le client génère une nouvelle clé Kerberos et des clés SSH, mais l'identité du client dans la base de données LDAP reste inchangée. Après le réenrôlement, l'hôte a ses clés et d'autres informations dans le même objet LDAP avec le même **FQDN** que précédemment, avant la perte de connexion de la machine avec les serveurs IdM.

IMPORTANT

Vous ne pouvez réinscrire que les clients dont l'entrée de domaine est encore active. Si vous avez désinstallé un client (à l'aide de **ipa-client-install --uninstall**) ou désactivé son entrée d'hôte (à l'aide de **ipa host-disable**), vous ne pouvez pas le réinscrire.

Vous ne pouvez pas réinscrire un client après l'avoir renommé. En effet, dans IdM, l'attribut clé de l'entrée du client dans LDAP est le nom d'hôte du client, son **FQDN**. Contrairement au réenrôlement d'un client, au cours duquel l'objet LDAP du client reste inchangé, le résultat du renommage d'un client est que le client a ses clés et d'autres informations dans un objet LDAP différent avec un nouveau **FQDN**. La seule façon de renommer un client est donc de désinstaller l'hôte de l'IdM, de changer son nom d'hôte et de l'installer en tant que client IdM avec un nouveau nom. Pour plus de détails sur la manière de renommer un client, voir Renommer les systèmes clients IdM .

Que se passe-t-il lors de la réinscription d'un client ?

Lors de la réinscription, l'IdM :

- Révoque le certificat d'origine de l'hôte
- Création de nouvelles clés SSH
- Génère un nouveau keytab

16.2. RÉINSCRIPTION D'UN CLIENT À L'AIDE DES INFORMATIONS D'IDENTIFICATION DE L'UTILISATEUR : RÉINSCRIPTION INTERACTIVE

Cette procédure décrit le réenregistrement d'un client de gestion d'identité (IdM) de manière interactive en utilisant les informations d'identification d'un utilisateur autorisé.

1. Recréez la machine cliente avec le même nom d'hôte.
2. Exécutez la commande **ipa-client-install --force-join** sur la machine cliente :

```
# ipa-client-install --force-join
```

3. Le script demande un utilisateur dont l'identité sera utilisée pour réinscrire le client. Il peut s'agir, par exemple, d'un utilisateur **hostadmin** ayant le rôle d'administrateur d'inscription :

```
User authorized to enroll computers: hostadmin
Password for hostadmin@EXAMPLE.COM:
```

Ressources supplémentaires

- Pour une procédure plus détaillée sur l'inscription de clients à l'aide des informations d'identification d'un utilisateur autorisé, voir Installation d'un client à l'aide des informations d'identification de l'utilisateur : Installation interactive.

16.3. RÉINSCRIPTION D'UN CLIENT À L'AIDE DE LA BASE DE DONNÉES DU CLIENT : RÉINSCRIPTION NON INTERACTIVE

Conditions préalables

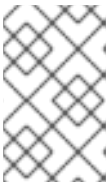
- Sauvegardez le fichier keytab original du client, par exemple dans le répertoire **/tmp** ou **/root**.

Procédure

Cette procédure décrit le réenrôlement d'un client Identity Management (IdM) de manière non interactive en utilisant le keytab du système client. Par exemple, le réenregistrement à l'aide du keytab du client est approprié pour une installation automatisée.

1. Recréez la machine cliente avec le même nom d'hôte.
2. Copiez le fichier keytab de l'emplacement de sauvegarde dans le répertoire **/etc/** sur l'ordinateur client recréé.
3. Utilisez l'utilitaire **ipa-client-install** pour réinscrire le client et spécifiez l'emplacement du fichier keytab à l'aide de l'option **--keytab**:

```
# ipa-client-install --keytab /etc/krb5.keytab
```



NOTE

Le keytab spécifié dans l'option **--keytab** n'est utilisé que lors de l'authentification pour initier l'inscription. Lors de la réinscription, l'IdM génère un nouveau keytab pour le client.

16.4. TEST D'UN CLIENT IDM

L'interface de ligne de commande vous informe que le site **ipa-client-install** a réussi, mais vous pouvez également effectuer votre propre test.

Pour vérifier que le client Identity Management (IdM) peut obtenir des informations sur les utilisateurs définis sur le serveur, vérifiez que vous êtes en mesure de résoudre un utilisateur défini sur le serveur. Par exemple, pour vérifier l'utilisateur par défaut **admin**:

```
[user@client ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

Pour tester le bon fonctionnement de l'authentification, **su** doit être utilisé par un utilisateur root à partir d'un utilisateur non-root :

```
[user@client ~]$ su -
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[root@client ~]#
```

CHAPITRE 17. DÉSINSTALLATION D'UN CLIENT IDM

En tant qu'administrateur, vous pouvez supprimer un client Identity Management (IdM) de l'environnement.

17.1. DÉSINSTALLATION D'UN CLIENT IDM

La désinstallation d'un client supprime ce dernier du domaine de gestion des identités (IdM), ainsi que toute la configuration IdM spécifique des services système, tels que System Security Services Daemon (SSSD). La configuration précédente du système client est ainsi rétablie.

Procédure

1. Entrez la commande **ipa-client-install --uninstall**:

```
[root@client ~]# ipa-client-install --uninstall
```

2. Facultatif : Vérifiez que vous ne pouvez pas obtenir de ticket Kerberos (TGT) pour un utilisateur IdM :

```
[root@client ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting initial credentials
[root@client ~]#
```

   Si un ticket TGT Kerberos a été renvoyé avec succès, suivez les étapes de désinstallation supplémentaires dans Désinstallation d'un client IdM : étapes supplémentaires après plusieurs installations antérieures.

3. Sur le client, supprimez les anciens mandants Kerberos de chaque keytab identifié autre que **/etc/krb5.keytab**:

```
[root@client ~]# ipa-rmkeytab -k /path/to/keytab -r EXAMPLE.COM
```

4. Sur un serveur IdM, supprimez toutes les entrées DNS pour l'hôte du client dans IdM :

```
[root@server ~]# ipa dnsrecord-del
Record name: old-client-name
Zone name: idm.example.com
No option to delete specific record provided.
Delete all? Yes/No (default No): yes
------------------------
Deleted record "old-client-name"
```

5. Sur le serveur IdM, supprimez l'entrée de l'hôte du client du serveur LDAP IdM. Cette opération supprime tous les services et révoque tous les certificats émis pour cet hôte :

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

IMPORTANT

La suppression de l'entrée de l'hôte du client du serveur LDAP IdM est cruciale si vous pensez réinscrire le client à l'avenir, avec une adresse IP ou un nom d'hôte différent.

17.2. DÉSINSTALLATION D'UN CLIENT IDM : ÉTAPES SUPPLÉMENTAIRES APRÈS PLUSIEURS INSTALLATIONS ANTÉRIEURES

Si vous installez et désinstallez plusieurs fois un hôte en tant que client Identity Management (IdM), la procédure de désinstallation risque de ne pas restaurer la configuration Kerberos antérieure à l'IdM.

Dans ce cas, vous devez supprimer manuellement la configuration IdM Kerberos. Dans les cas extrêmes, vous devez réinstaller le système d'exploitation.

Conditions préalables

- Vous avez utilisé la commande **ipa-client-install --uninstall** pour désinstaller la configuration du client IdM de l'hôte. Cependant, vous pouvez toujours obtenir un ticket Kerberos (TGT) pour un utilisateur IdM à partir du serveur IdM.
- Vous avez vérifié que le répertoire **/var/lib/ipa-client/sysrestore** est vide et que, par conséquent, vous ne pouvez pas restaurer la configuration du système antérieure au client IdM à l'aide des fichiers contenus dans ce répertoire.

Procédure

1. Vérifiez le fichier **/etc/krb5.conf.ipa**:
   - Si le contenu du fichier **/etc/krb5.conf.ipa** est identique au contenu du fichier **krb5.conf** avant l'installation du client IdM, vous pouvez :
     i. Supprimez le fichier **/etc/krb5.conf**:

     ```
     # rm /etc/krb5.conf
     ```

     ii. Renommez le fichier **/etc/krb5.conf.ipa** en **/etc/krb5.conf**:

     ```
     # mv /etc/krb5.conf.ipa /etc/krb5.conf
     ```

   - Si le contenu du fichier **/etc/krb5.conf.ipa** n'est pas le même que celui du fichier **krb5.conf** avant l'installation du client IdM, vous pouvez au moins restaurer la configuration Kerberos dans l'état où elle se trouvait juste après l'installation du système d'exploitation :

     i. Réinstallez le paquet **krb5-libs**:

     ```
     # dnf reinstall krb5-libs
     ```

     En tant que dépendance, cette commande réinstallera également le paquet **krb5-workstation** et la version originale du fichier **/etc/krb5.conf**.

2. Supprime le fichier **var/log/ipaclient-install.log** s'il est présent.

Verification steps

- Essayez d'obtenir les informations d'identification de l'utilisateur IdM. Cette tentative devrait échouer :

```
[root@r8server ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting initial credentials
[root@r8server ~]#
```

Le fichier **/etc/krb5.conf** est maintenant restauré dans son état d'origine. Par conséquent, vous ne pouvez pas obtenir de TGT Kerberos pour un utilisateur IdM sur l'hôte.

CHAPITRE 18. RENOMMER LES SYSTÈMES CLIENTS IDM

Les sections suivantes décrivent comment modifier le nom d'hôte d'un système client de gestion d'identité (IdM).

AVERTISSEMENT

Renommer un client est une procédure manuelle. Ne l'effectuez que si la modification du nom d'hôte est absolument nécessaire.

Renommer un client IdM implique :

1. Préparation de l'hôte. Pour plus de détails, voir Préparation d'un client IdM pour son renommage .
2. Désinstallation du client IdM de l'hôte. Pour plus de détails, voir Désinstallation d'un client.
3. Renommer l'hôte. Pour plus de détails, voir Renommer un client.
4. Installer le client IdM sur l'hôte avec le nouveau nom. Pour plus de détails, voir Réinstallation d'un client.
5. Configurer l'hôte après l'installation du client IdM. Pour plus d'informations, voir Réajout de services, re-génération de certificats et réajout de groupes d'hôtes.

18.1. PRÉPARATION D'UN CLIENT IDM POUR SON RENOMMAGE

Avant de désinstaller le client actuel, prenez note de certains paramètres du client. Vous appliquerez cette configuration après avoir réenrôlé la machine avec un nouveau nom d'hôte.

- Identifier les services en cours d'exécution sur la machine :
  - Utilisez la commande **ipa service-find** et identifiez les services avec des certificats dans le résultat :

    ```
    $ ipa service-find old-client-name.example.com
    ```

  - En outre, chaque hôte a un *host service* par défaut qui n'apparaît pas dans la sortie **ipa service-find**. Le principal du service de l'hôte, également appelé *host principal*, est le suivant **host/*old-client-name.example.com***.
- Pour tous les mandants de service affichés par **ipa service-find *old-client-name.example.com*** détermine l'emplacement des keytabs correspondants sur le système ***old-client-name.example.com*** système :

  ```
  # find / -name "*.keytab"
  ```

  Chaque service du système client possède un principal Kerberos sous la forme *service_name/host_name@REALM*, tel que **ldap/*old-client-name.example.com@EXAMPLE.COM***.

- Identifier tous les groupes d'hôtes auxquels la machine appartient.

```
# ipa hostgroup-find old-client-name.example.com
```

18.2. DÉSINSTALLATION D'UN CLIENT IDM

La désinstallation d'un client supprime ce dernier du domaine de gestion des identités (IdM), ainsi que toute la configuration IdM spécifique des services système, tels que System Security Services Daemon (SSSD). La configuration précédente du système client est ainsi rétablie.

Procédure

1. Entrez la commande **ipa-client-install --uninstall**:

```
[root@client ~]# ipa-client-install --uninstall
```

2. Facultatif : Vérifiez que vous ne pouvez pas obtenir de ticket Kerberos (TGT) pour un utilisateur IdM :

```
[root@client ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting initial credentials
[root@client ~]#
```

   Si un ticket TGT Kerberos a été renvoyé avec succès, suivez les étapes de désinstallation supplémentaires dans Désinstallation d'un client IdM : étapes supplémentaires après plusieurs installations antérieures.

3. Sur le client, supprimez les anciens mandants Kerberos de chaque keytab identifié autre que **/etc/krb5.keytab**:

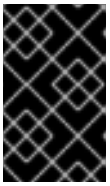
```
[root@client ~]# ipa-rmkeytab -k /path/to/keytab -r EXAMPLE.COM
```

4. Sur un serveur IdM, supprimez toutes les entrées DNS pour l'hôte du client dans IdM :

```
[root@server ~]# ipa dnsrecord-del
Record name: old-client-name
Zone name: idm.example.com
No option to delete specific record provided.
Delete all? Yes/No (default No): yes
----------------------
Deleted record "old-client-name"
```

5. Sur le serveur IdM, supprimez l'entrée de l'hôte du client du serveur LDAP IdM. Cette opération supprime tous les services et révoque tous les certificats émis pour cet hôte :

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



IMPORTANT

La suppression de l'entrée de l'hôte du client du serveur LDAP IdM est cruciale si vous pensez réinscrire le client à l'avenir, avec une adresse IP ou un nom d'hôte différent.

18.3. DÉSINSTALLATION D'UN CLIENT IDM : ÉTAPES SUPPLÉMENTAIRES APRÈS PLUSIEURS INSTALLATIONS ANTÉRIEURES

Si vous installez et désinstallez plusieurs fois un hôte en tant que client Identity Management (IdM), la procédure de désinstallation risque de ne pas restaurer la configuration Kerberos antérieure à l'IdM.

Dans ce cas, vous devez supprimer manuellement la configuration IdM Kerberos. Dans les cas extrêmes, vous devez réinstaller le système d'exploitation.

Conditions préalables

- Vous avez utilisé la commande **ipa-client-install --uninstall** pour désinstaller la configuration du client IdM de l'hôte. Cependant, vous pouvez toujours obtenir un ticket Kerberos (TGT) pour un utilisateur IdM à partir du serveur IdM.
- Vous avez vérifié que le répertoire **/var/lib/ipa-client/sysrestore** est vide et que, par conséquent, vous ne pouvez pas restaurer la configuration du système antérieure au client IdM à l'aide des fichiers contenus dans ce répertoire.

Procédure

1. Vérifiez le fichier **/etc/krb5.conf.ipa**:
   - Si le contenu du fichier **/etc/krb5.conf.ipa** est identique au contenu du fichier **krb5.conf** avant l'installation du client IdM, vous pouvez :
     i. Supprimez le fichier **/etc/krb5.conf**:

     ```
     # rm /etc/krb5.conf
     ```

     ii. Renommez le fichier **/etc/krb5.conf.ipa** en **/etc/krb5.conf**:

     ```
     # mv /etc/krb5.conf.ipa /etc/krb5.conf
     ```

   - Si le contenu du fichier **/etc/krb5.conf.ipa** n'est pas le même que celui du fichier **krb5.conf** avant l'installation du client IdM, vous pouvez au moins restaurer la configuration Kerberos dans l'état où elle se trouvait juste après l'installation du système d'exploitation :

     i. Réinstallez le paquet **krb5-libs**:

     ```
     # dnf reinstall krb5-libs
     ```

     En tant que dépendance, cette commande réinstallera également le paquet **krb5-workstation** et la version originale du fichier **/etc/krb5.conf**.
2. Supprime le fichier **var/log/ipaclient-install.log** s'il est présent.

Verification steps

- Essayez d'obtenir les informations d'identification de l'utilisateur IdM. Cette tentative devrait échouer :

```
[root@r8server ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting initial credentials
[root@r8server ~]#
```

Le fichier **/etc/krb5.conf** est maintenant restauré dans son état d'origine. Par conséquent, vous ne pouvez pas obtenir de TGT Kerberos pour un utilisateur IdM sur l'hôte.

18.4. RENOMMER LE SYSTÈME HÔTE

Renommez la machine comme vous le souhaitez. Par exemple :

```
# hostnamectl set-hostname new-client-name.example.com
```

Vous pouvez maintenant réinstaller le client Identity Management (IdM) sur le domaine IdM avec le nouveau nom d'hôte.

18.5. RÉINSTALLATION D'UN CLIENT IDM

Installez un client sur votre hôte renommé en suivant la procédure décrite dans Installation d'un client.

18.6. RÉAJUSTEMENT DES SERVICES, RE-GÉNÉRATION DES CERTIFICATS ET RÉAJUSTEMENT DES GROUPES D'HÔTES

Procédure

1. Sur le serveur de gestion des identités (IdM), ajouter un nouveau keytab pour chaque service identifié dans la préparation d'un client IdM pour son renommage .

```
[root@server ~]# ipa service-add service_name/new-client-name
```

2. Générer des certificats pour les services auxquels un certificat a été attribué dans le cadre de la préparation d'un client IdM à son renommage . Vous pouvez le faire :
   - Utilisation des outils d'administration de l'IdM
   - Utilisation de l'utilitaire **certmonger**
3. Réajoutez le client aux groupes d'hôtes identifiés dans la section Préparation d'un client IdM pour son renommage.

CHAPITRE 19. PRÉPARATION DU SYSTÈME POUR L'INSTALLATION D'UNE RÉPLIQUE IDM

Les liens suivants répertorient les conditions requises pour installer une réplique de gestion des identités (IdM). Avant l'installation, assurez-vous que votre système répond à ces exigences.

1. S'assurer que le système cible répond aux exigences générales pour l'installation du serveur IdM.
2. S'assurer que le système cible répond aux exigences supplémentaires en matière de version pour l'installation des répliques IdM.
3. [Facultatif] Si vous ajoutez une réplique Identity Management (IdM) RHEL 9 sur laquelle le mode FIPS est activé à un déploiement IdM RHEL 8 en mode FIPS, assurez-vous que les types de chiffrement corrects sont activés sur la réplique.
4. Autoriser le système cible à s'inscrire dans le domaine IdM. Pour plus d'informations, consultez l'une des sections suivantes qui correspond le mieux à vos besoins :
   - Autoriser l'installation d'une réplique sur un client IdM
   - Autoriser l'installation d'une réplique sur un système qui n'est pas enrôlé dans IdM

Ressources supplémentaires

- Planification de la topologie du réplica

19.1. EXIGENCES RELATIVES À LA VERSION RÉPLIQUÉE

Un réplica IdM doit exécuter la même version d'IdM que les autres serveurs ou une version plus récente. Par exemple :

- Vous avez un serveur IdM installé sur Red Hat Enterprise Linux 9 et il utilise les paquets IdM 4.x.
- Vous devez également installer le réplica sur Red Hat Enterprise Linux 9 et utiliser IdM version 4.x ou ultérieure.

Cela permet de s'assurer que la configuration peut être correctement copiée du serveur vers la réplique.

Pour plus de détails sur l'affichage de la version du logiciel IdM, voir Méthodes d'affichage de la version du logiciel IdM.

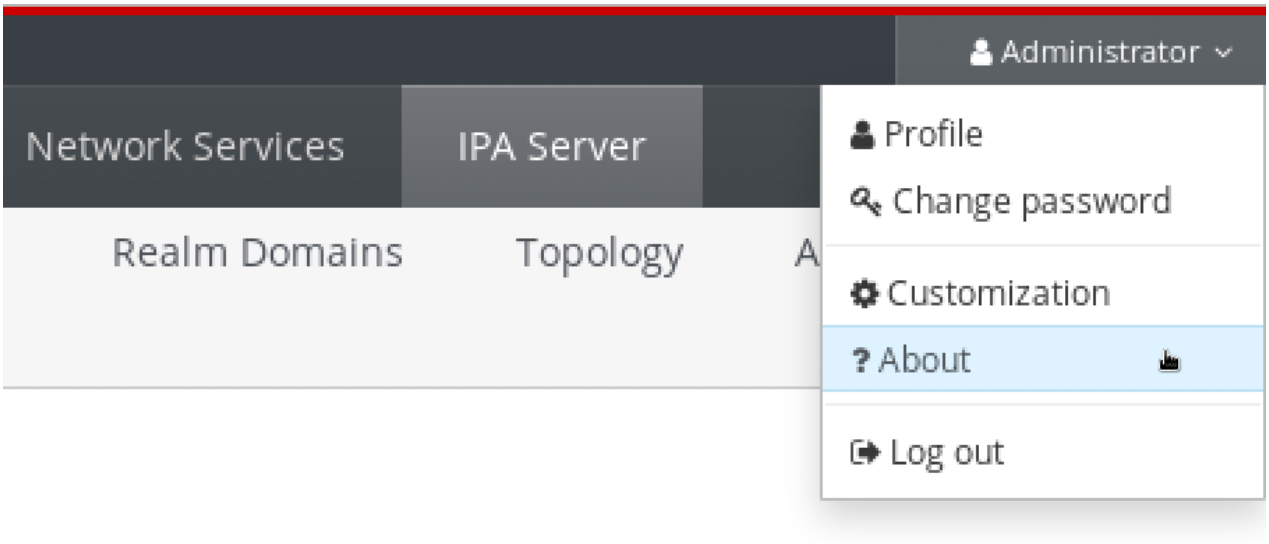
19.2. MÉTHODES D'AFFICHAGE DE LA VERSION DU LOGICIEL IDM

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

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

Affichage de la version via l'interface WebUI

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



Affichage de la version avec les commandes`ipa`

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

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

Affichage de la version avec les commandes`rpm`

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

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

19.3. ASSURER LA CONFORMITÉ FIPS D'UNE RÉPLIQUE RHEL 9 REJOIGNANT UN ENVIRONNEMENT IDM RHEL 8

Si RHEL Identity Management (IdM) a été installé à l'origine sur un système RHEL 8.6 ou antérieur, les types de chiffrement **AES HMAC-SHA1** qu'il utilise ne sont pas pris en charge par défaut par RHEL 9 en mode FIPS. Pour ajouter une réplique RHEL 9 en mode FIPS au déploiement, vous devez activer ces clés de chiffrement sur le système RHEL 9 en définissant la stratégie cryptographique sur **FIPS:AD-SUPPORT**.

En définissant la politique cryptographique sur **FIPS:AD-SUPPORT**, vous ajoutez la prise en charge des types de chiffrement suivants :

- **aes256-cts:normal**
- **aes256-cts:special**
- **aes128-cts:normal**
- **aes128-cts:special**

Conditions préalables

- Vous avez activé le mode FIPS sur votre système RHEL 9.

- Vous souhaitez configurer le système RHEL 9 en tant que réplique IdM pour votre environnement IdM RHEL 8 en mode FIPS.
- Le type de cryptage de votre clé principale IdM n'est pas **aes256-cts-hmac-sha384-192**. Pour plus d'informations, consultez le type de cryptage de votre clé principale IdM .

NOTE

L'implémentation Active Directory de Microsoft ne prend pas encore en charge les types de chiffrement Kerberos RFC8009 qui utilisent SHA-2 HMAC. Si une confiance IdM-AD est configurée, l'utilisation de la sous-politique cryptographique FIPS:AD-SUPPORT est donc requise même si le type de chiffrement de votre clé principale IdM est **aes256-cts-hmac-sha384-192**.

Procédure

- Sur le système RHEL 9, activez l'utilisation des types de chiffrement **AES HMAC-SHA1**:

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

19.4. AUTORISER L'INSTALLATION D'UNE RÉPLIQUE SUR UN CLIENT IDM

Lors de l'installation d'un réplica sur un client Identity Management (IdM) existant en exécutant l'utilitaire **ipa-replica-install**, choisissez **Method 1** ou **Method 2** ci-dessous pour autoriser l'installation du réplica. Choisissez **Method 1** si l'une des situations suivantes s'applique :

- Vous souhaitez qu'un administrateur système senior effectue la partie initiale de la procédure et qu'un administrateur junior effectue le reste.
- Vous souhaitez automatiser l'installation de votre réplique.

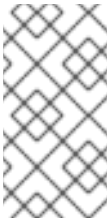
Méthode 1 : le groupe d'accueil ipaservers

1. Se connecter à n'importe quel hôte IdM en tant qu'administrateur IdM :

```
$ kinit admin
```

2. Ajoutez la machine cliente au groupe d'hôtes **ipaservers**:

```
$ ipa hostgroup-add-member ipaservers --hosts client.idm.example.com
  Host-group: ipaservers
  Description: IPA server hosts
  Member hosts: server.idm.example.com, client.idm.example.com
-------------------------
Number of members added 1
-------------------------
```



NOTE

L'appartenance au groupe **ipaservers** confère à la machine des privilèges élevés similaires à ceux de l'administrateur. Par conséquent, à l'étape suivante, l'utilitaire **ipa-replica-install** peut être exécuté avec succès sur l'hôte par un administrateur système débutant.

Méthode 2 : les informations d'identification d'un utilisateur privilégié

Choisissez l'une des méthodes suivantes pour autoriser l'installation du réplica en fournissant les informations d'identification d'un utilisateur privilégié :

- Laissez Identity Management (IdM) vous demander les informations d'identification de manière interactive après avoir lancé l'utilitaire **ipa-replica-install**. Il s'agit du comportement par défaut.
- Connectez-vous au client en tant qu'utilisateur privilégié juste avant d'exécuter l'utilitaire **ipa-replica-install**. L'utilisateur privilégié par défaut est **admin**:

```
$ kinit admin
```

Ressources supplémentaires

- Pour lancer la procédure d'installation, voir Installation d'un réplica IdM .
- Vous pouvez utiliser une séquence Ansible pour installer les répliques IdM. Pour plus d'informations, voir Installation d'une réplique Identity Management à l'aide d'un playbook Ansible.

19.5. AUTORISER L'INSTALLATION D'UNE RÉPLIQUE SUR UN SYSTÈME QUI N'EST PAS ENRÔLÉ DANS IDM

Lors de l'installation d'un réplica sur un système qui n'est pas inscrit dans le domaine Identity Management (IdM), l'utilitaire **ipa-replica-install** inscrit d'abord le système en tant que client, puis installe les composants du réplica. Pour ce scénario, choisissez **Method 1** ou **Method 2** ci-dessous pour autoriser l'installation du réplica. Choisissez **Method 1** si l'une des situations suivantes s'applique :

- Vous souhaitez qu'un administrateur système senior effectue la partie initiale de la procédure et qu'un administrateur junior effectue le reste.
- Vous souhaitez automatiser l'installation de votre réplique.

Méthode 1 : un mot de passe aléatoire généré sur un serveur IdM

Saisissez les commandes suivantes sur n'importe quel serveur du domaine :

1. Connectez-vous en tant qu'administrateur.

```
$ kinit admin
```

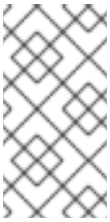
2. Ajoutez le système externe en tant qu'hôte IdM. Utilisez l'option **--random** avec la commande **ipa host-add** pour générer un mot de passe aléatoire à usage unique qui sera utilisé pour l'installation ultérieure du réplica.

```
$ ipa host-add replica.example.com --random
--------------------------------------------------
Added host "replica.example.com"
--------------------------------------------------
  Host name: replica.example.com
  Random password: W5YpARl=7M.n
  Password: True
  Keytab: False
  Managed by: server.example.com
```

Le mot de passe généré deviendra invalide lorsque vous l'utiliserez pour inscrire la machine dans le domaine IdM. Il sera remplacé par un keytab hôte approprié une fois l'enrôlement terminé.

3. Ajoutez le système au groupe d'hôtes **ipaservers**.

```
$ ipa hostgroup-add-member ipaservers --hosts replica.example.com
  Host-group: ipaservers
  Description: IPA server hosts
  Member hosts: server.example.com, replica.example.com
-------------------------
Number of members added 1
-------------------------
```



NOTE

L'appartenance au groupe **ipaservers** confère à la machine des privilèges élevés similaires à ceux de l'administrateur. Par conséquent, à l'étape suivante, l'utilitaire **ipa-replica-install** peut être exécuté avec succès sur l'hôte par un administrateur système junior qui fournit le mot de passe aléatoire généré.

Méthode 2 : les informations d'identification d'un utilisateur privilégié

Avec cette méthode, vous autorisez l'installation du réplica en fournissant les informations d'identification d'un utilisateur privilégié. L'utilisateur privilégié par défaut est **admin**.
Aucune action n'est requise avant l'exécution de l'utilitaire d'installation des répliques IdM. Ajoutez les options nom du principal et mot de passe (**--principal *admin* --admin-password *password***) à la commande **ipa-replica-install** directement pendant l'installation.

Ressources supplémentaires

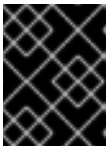
- Pour lancer la procédure d'installation, voir Installation d'un réplica IdM .
- Vous pouvez utiliser une séquence Ansible pour installer les répliques IdM. Pour plus d'informations, voir Installation d'une réplique Identity Management à l'aide d'un playbook Ansible.

CHAPITRE 20. INSTALLATION D'UNE RÉPLIQUE IDM

Les sections suivantes décrivent comment installer un réplica de gestion d'identité (IdM). Le processus d'installation du réplica copie la configuration du serveur existant et installe le réplica sur la base de cette configuration.

Conditions préalables

- Assurez-vous que votre système est prêt pour l'installation des répliques IdM.



IMPORTANT

Si cette préparation n'est pas effectuée, l'installation d'une réplique IdM échouera.

NOTE

Installez une réplique IdM à la fois. L'installation de plusieurs répliques en même temps n'est pas possible.

Procédure

Pour les différents types de procédures d'installation des répliques, voir :

- Section 20.1, « Installation d'une réplique IdM avec DNS intégré et une autorité de certification »
- Section 20.2, « Installation d'une réplique IdM avec DNS intégré et sans autorité de certification »
- Section 20.3, « Installation d'une réplique IdM sans DNS intégré et avec une AC »
- Section 20.4, « Installation d'une réplique IdM sans DNS intégré et sans autorité de certification »
- Section 20.5, « Installation d'une réplique cachée de l'IdM »

Pour résoudre les problèmes liés à la procédure d'installation de la réplique, voir :

- Chapitre 21, *Dépannage de l'installation des répliques IdM*

Après l'installation, voir :

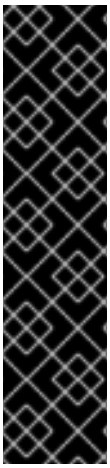
- Section 20.6, « Test d'une réplique IdM »
- Sauvegarde et restauration de l'IdM

20.1. INSTALLATION D'UNE RÉPLIQUE IDM AVEC DNS INTÉGRÉ ET UNE AUTORITÉ DE CERTIFICATION

Cette procédure décrit l'installation d'un réplica de gestion des identités (IdM) :

- Avec DNS intégré
- Avec une autorité de certification (AC)

Vous pouvez le faire, par exemple, pour répliquer le service d'autorité de certification à des fins de résilience après l'installation d'un serveur IdM avec une autorité de certification intégrée.



IMPORTANT

Lors de la configuration d'un réplica avec une autorité de certification, la configuration de l'autorité de certification du réplica doit refléter la configuration de l'autorité de certification de l'autre serveur.

Par exemple, si le serveur comprend une autorité de certification IdM intégrée en tant qu'autorité de certification racine, la nouvelle réplique doit également être installée avec une autorité de certification intégrée en tant qu'autorité de certification racine. Aucune autre configuration d'autorité de certification n'est disponible dans ce cas.

L'ajout de l'option **--setup-ca** à la commande **ipa-replica-install** permet de copier la configuration de l'autorité de certification du serveur initial.

Conditions préalables

- Assurez-vous que votre système est prêt pour l'installation d'une réplique IdM.

Procédure

1. Entrez dans **ipa-replica-install** avec ces options :
   - **--setup-dns** pour configurer le réplica en tant que serveur DNS
   - **--forwarder** pour spécifier un transitaire par serveur, ou **--no-forwarder** si vous ne voulez pas utiliser de transitaires par serveur. Pour spécifier plusieurs transitaires par serveur pour des raisons de basculement, utilisez plusieurs fois **--forwarder**.

NOTE

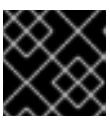
L'utilitaire **ipa-replica-install** accepte un certain nombre d'autres options liées aux paramètres DNS, telles que **--no-reverse** ou **--no-host-dns**. Pour plus d'informations à ce sujet, consultez la page de manuel **ipa-replica-install**(1).

   - **--setup-ca** pour inclure une autorité de certification sur la réplique

   Par exemple, pour configurer une réplique avec un serveur DNS intégré et une autorité de certification qui transmet toutes les demandes DNS non gérées par les serveurs IdM au serveur DNS fonctionnant sur l'adresse IP 192.0.2.1 :

```
# ipa-replica-install --setup-dns --forwarder 192.0.2.1 --setup-ca
```

2. Une fois l'installation terminée, ajoutez une délégation DNS du domaine parent au domaine DNS IdM. Par exemple, si le domaine DNS IdM est **idm.example.com**, ajoutez un enregistrement de serveur de noms (NS) au domaine parent **example.com**.



IMPORTANT

Répétez cette étape chaque fois que vous installez un serveur DNS IdM.

20.2. INSTALLATION D'UNE RÉPLIQUE IDM AVEC DNS INTÉGRÉ ET SANS AUTORITÉ DE CERTIFICATION

Cette procédure décrit l'installation d'un réplica de gestion des identités (IdM) :

- Avec DNS intégré
- Sans autorité de certification (AC) dans un environnement IdM où une AC est déjà installée. Le réplica transmet toutes les opérations de certificat au serveur IdM sur lequel une autorité de certification est installée.

Conditions préalables

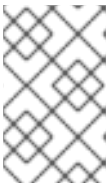
- Assurez-vous que votre système est prêt pour l'installation d'une réplique IdM.

Procédure

1. Entrez dans **ipa-replica-install** avec ces options :
   - **--setup-dns** pour configurer le réplica en tant que serveur DNS
   - **--forwarder** pour spécifier un transitaire par serveur, ou **--no-forwarder** si vous ne voulez pas utiliser de transitaires par serveur. Pour spécifier plusieurs transitaires par serveur pour des raisons de basculement, utilisez plusieurs fois **--forwarder**.

   Par exemple, pour configurer une réplique avec un serveur DNS intégré qui transmet toutes les demandes DNS non gérées par les serveurs IdM au serveur DNS fonctionnant sur l'adresse IP 192.0.2.1 :

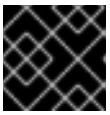
   ```
   # ipa-replica-install --setup-dns --forwarder 192.0.2.1
   ```

   NOTE

   L'utilitaire **ipa-replica-install** accepte un certain nombre d'autres options liées aux paramètres DNS, telles que **--no-reverse** ou **--no-host-dns**. Pour plus d'informations à ce sujet, consultez la page de manuel **ipa-replica-install**(1).

2. Une fois l'installation terminée, ajoutez une délégation DNS du domaine parent au domaine DNS IdM. Par exemple, si le domaine DNS IdM est **idm.example.com**, ajoutez un enregistrement de serveur de noms (NS) au domaine parent **example.com**.

   IMPORTANT

   Répétez cette étape chaque fois que vous installez un serveur DNS IdM.

20.3. INSTALLATION D'UNE RÉPLIQUE IDM SANS DNS INTÉGRÉ ET AVEC UNE AC

Cette procédure décrit l'installation d'un réplica de gestion des identités (IdM) :

- Sans DNS intégré
- Avec une autorité de certification (AC)

IMPORTANT

Lors de la configuration d'un réplica avec une autorité de certification, la configuration de l'autorité de certification du réplica doit refléter la configuration de l'autorité de certification de l'autre serveur.

Par exemple, si le serveur comprend une autorité de certification IdM intégrée en tant qu'autorité de certification racine, la nouvelle réplique doit également être installée avec une autorité de certification intégrée en tant qu'autorité de certification racine. Aucune autre configuration d'autorité de certification n'est disponible dans ce cas.

L'ajout de l'option **--setup-ca** à la commande **ipa-replica-install** permet de copier la configuration de l'autorité de certification du serveur initial.

Conditions préalables

- Assurez-vous que votre système est prêt pour l'installation d'une réplique IdM.

Procédure

1. Entrez **ipa-replica-install** avec l'option **--setup-ca**.

```
# ipa-replica-install --setup-ca
```

2. Ajoutez les enregistrements du service DNS IdM nouvellement créés à votre serveur DNS :
   a. Exporter les enregistrements du service DNS IdM dans un fichier au format **nsupdate**:

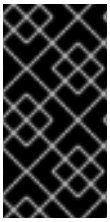
```
$ ipa dns-update-system-records --dry-run --out dns_records_file.nsupdate
```

   b. Soumettez une demande de mise à jour DNS à votre serveur DNS à l'aide de l'utilitaire **nsupdate** et du fichier **dns_records_file.nsupdate**. Pour plus d'informations, voir Mise à jour des enregistrements DNS externes à l'aide de nsupdate dans la documentation RHEL 7. Vous pouvez également vous référer à la documentation de votre serveur DNS pour l'ajout d'enregistrements DNS.

20.4. INSTALLATION D'UNE RÉPLIQUE IDM SANS DNS INTÉGRÉ ET SANS AUTORITÉ DE CERTIFICATION

Cette procédure décrit l'installation d'un réplica de gestion des identités (IdM) :

- Sans DNS intégré
- Sans autorité de certification (CA) en fournissant manuellement les certificats requis. On suppose ici que le premier serveur a été installé sans autorité de certification.



IMPORTANT

Vous ne pouvez pas installer un serveur ou un réplica à l'aide de certificats de serveur tiers auto-signés, car les fichiers de certificats importés doivent contenir la chaîne complète des certificats de l'autorité de certification qui a émis les certificats des serveurs LDAP et Apache.

Conditions préalables

- Assurez-vous que votre système est prêt pour l'installation d'une réplique IdM.

Procédure

- Saisissez **ipa-replica-install**, et fournissez les fichiers de certificat requis en ajoutant les options suivantes :
  - **--dirsrv-cert-file**
  - **--dirsrv-pin**
  - **--http-cert-file**
  - **--http-pin**

  Pour plus de détails sur les fichiers fournis à l'aide de ces options, voir Section 4.1, « Certificats requis pour l'installation d'un serveur IdM sans autorité de certification ».

  Par exemple :

```
# ipa-replica-install \
   --dirsrv-cert-file /tmp/server.crt \
   --dirsrv-cert-file /tmp/server.key \
   --dirsrv-pin secret \
   --http-cert-file /tmp/server.crt \
   --http-cert-file /tmp/server.key \
   --http-pin secret
```

NOTE

N'ajoutez pas l'option **--ca-cert-file**. L'utilitaire **ipa-replica-install** reprend automatiquement cette partie des informations du certificat du premier serveur que vous avez installé.

20.5. INSTALLATION D'UNE RÉPLIQUE CACHÉE DE L'IDM

Une réplique cachée (non annoncée) est un serveur de gestion d'identité (IdM) dont tous les services fonctionnent et sont 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.

Pour plus de détails sur les répliques cachées, voir Le mode réplique cachée.

Conditions préalables

- Assurez-vous que votre système est prêt pour l'installation d'une réplique IdM.

Procédure

- Pour installer une réplique cachée, utilisez la commande suivante :

```
ipa-replica-install --hidden-replica
```

Notez que la commande installe une réplique sans enregistrements DNS SRV et avec des rôles de serveur LDAP désactivés.

Vous pouvez également changer le mode d'un réplica existant en mode caché. Pour plus de détails, voir Rétrogradation et promotion des répliques cachées

20.6. TEST D'UNE RÉPLIQUE IDM

Après avoir créé un réplica, vérifiez si le réplica réplique les données comme prévu. Vous pouvez utiliser la procédure suivante.

Procédure

1. Créez un utilisateur sur la nouvelle réplique :

```
[admin@new_replica ~]$ ipa user-add test_user
```

2. Assurez-vous que l'utilisateur est visible sur une autre réplique :

```
[admin@another_replica ~]$ ipa user-show test_user
```

20.7. CONNEXIONS EFFECTUÉES LORS DE L'INSTALLATION D'UNE RÉPLIQUE IDM

Requêtes effectuées lors de l'installation d'un réplica IdM liste les opérations effectuées par **ipa-replica-install**, l'outil d'installation d'un réplica IdM (Identity Management).

Tableau 20.1. Demandes effectuées lors de l'installation d'une réplique IdM

Fonctionnement	Protocole utilisé	Objectif
Résolution DNS par rapport aux résolveurs DNS configurés sur le système client	DNS	Pour découvrir les adresses IP des serveurs IdM
Demandes adressées aux ports 88 (TCP/TCP6 et UDP/UDP6) des serveurs IdM découverts	Kerberos	Pour obtenir un ticket Kerberos
Appels JSON-RPC au service web IdM Apache sur les serveurs IdM découverts ou configurés	HTTPS	Enrôlement du client IdM ; récupération des clés de réplique et délivrance du certificat si nécessaire
Demandes via TCP/TCP6 au port 389 sur le serveur IdM, en utilisant l'authentification SASL GSSAPI, LDAP simple, ou les deux	LDAP	Enrôlement du client IdM ; récupération de la chaîne de certificats de l'autorité de certification ; réplication des données LDAP
Requêtes via TCP/TCP6 vers le port 22 du serveur IdM	SSH	Pour vérifier si la connexion fonctionne

Fonctionnement	Protocole utilisé	Objectif
(optionnellement) Accès par le port 8443 (TCP/TCP6) sur les serveurs IdM	HTTPS	Pour administrer l'autorité de certification sur le serveur IdM (uniquement lors de l'installation du serveur IdM et de la réplique)

CHAPITRE 21. DÉPANNAGE DE L'INSTALLATION DES RÉPLIQUES IDM

Les sections suivantes décrivent le processus de collecte d'informations sur l'échec de l'installation d'un réplica IdM et la manière de résoudre certains problèmes d'installation courants.

21.1. FICHIERS JOURNAUX DES ERREURS D'INSTALLATION DE LA RÉPLIQUE IDM

Lorsque vous installez une réplique Identity Management (IdM), les informations de débogage sont ajoutées aux fichiers journaux suivants sur le site **replica**:

- **/var/log/ipareplica-install.log**
- **/var/log/ipareplica-conncheck.log**
- **/var/log/ipaclient-install.log**
- **/var/log/httpd/error_log**
- **/var/log/dirsrv/slapd-*INSTANCE-NAME*/access**
- **/var/log/dirsrv/slapd-*INSTANCE-NAME*/errors**
- **/var/log/ipaserver-install.log**

Le processus d'installation du réplica ajoute également des informations de débogage aux fichiers journaux suivants sur l'IdM **server** que le réplica contacte :

- **/var/log/httpd/error_log**
- **/var/log/dirsrv/slapd-*INSTANCE-NAME*/access**
- **/var/log/dirsrv/slapd-*INSTANCE-NAME*/errors**

La dernière ligne de chaque fichier journal indique le succès ou l'échec, et les entrées **ERROR** et **DEBUG** fournissent un contexte supplémentaire.

Ressources supplémentaires

- Examen des erreurs d'installation des répliques IdM

21.2. EXAMEN DES ERREURS D'INSTALLATION DES RÉPLIQUES IDM

Pour dépanner une installation de réplique IdM défaillante, examinez les erreurs à la fin des fichiers journaux d'erreur d'installation sur la nouvelle réplique et sur le serveur, et utilisez ces informations pour résoudre les problèmes correspondants.

Conditions préalables

- Vous devez avoir les privilèges **root** pour afficher le contenu des fichiers journaux IdM.

Procédure

1. Utilisez la commande **tail** pour afficher les dernières erreurs du fichier journal primaire **/var/log/ipareplica-install.log**. L'exemple suivant affiche les 10 dernières lignes.

```
[user@replica ~]$ sudo tail -n 10 /var/log/ipareplica-install.log
[sudo] password for user:
  func(installer)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/replicainstall.py", line 424, in
decorated
  func(installer)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/replicainstall.py", line 785, in
promote_check
  ensure_enrolled(installer)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/replicainstall.py", line 740, in
ensure_enrolled
  raise ScriptError("Configuration of client side components failed!")

2020-05-28T18:24:51Z DEBUG The ipa-replica-install command failed, exception:
ScriptError: Configuration of client side components failed!
2020-05-28T18:24:51Z ERROR Configuration of client side components failed!
2020-05-28T18:24:51Z ERROR The ipa-replica-install command failed. See
/var/log/ipareplica-install.log for more information
```

2. Pour consulter le fichier journal de manière interactive, ouvrez la fin du fichier journal à l'aide de l'utilitaire **less** et utilisez les touches fléchées ↑ et ↓ pour naviguer.

```
[user@replica ~]$ sudo less -N G /var/log/ipareplica-install.log
```

3. (Facultatif) Bien que **/var/log/ipareplica-install.log** soit le fichier journal principal pour une installation de réplica, vous pouvez recueillir des informations de dépannage supplémentaires en répétant ce processus d'examen avec d'autres fichiers sur le réplica et le serveur.

   Sur la réplique :

```
[user@replica ~]$ sudo less -N +G /var/log/ipareplica-conncheck.log
[user@replica ~]$ sudo less -N +G /var/log/ipaclient-install.log
[user@replica ~]$ sudo less -N +G /var/log/httpd/error_log
[user@replica ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/access
[user@replica ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/errors
[user@replica ~]$ sudo less -N +G /var/log/ipaserver-install.log
```

   Sur le serveur :

```
[user@server ~]$ sudo less -N +G /var/log/httpd/error_log
[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/access
[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/errors
```

Ressources supplémentaires

- Fichiers journaux des erreurs d'installation de la réplique IdM
- Si vous ne parvenez pas à résoudre l'échec de l'installation d'un réplica et que vous disposez d'un abonnement à l'assistance technique de Red Hat, ouvrez un dossier d'assistance technique sur le portail client de Red Hat et fournissez une adresse **sosreport** du réplica et une adresse **sosreport** du serveur.

- L'utilitaire **sosreport** collecte des détails de configuration, des journaux et des informations système à partir d'un système RHEL. Pour plus d'informations sur l'utilitaire **sosreport**, voir Qu'est-ce qu'un rapport sos et comment en créer un dans Red Hat Enterprise Linux ?

21.3. FICHIERS JOURNAUX DES ERREURS D'INSTALLATION DE L'AUTORITÉ DE CERTIFICATION IDM

L'installation du service d'autorité de certification (CA) sur un réplica de gestion d'identité (IdM) ajoute des informations de débogage à plusieurs endroits sur le réplica et le serveur IdM avec lequel le réplica communique.

Tableau 21.1. Sur la réplique (par ordre de priorité recommandé) :

Location	Description
/var/log/pki/pki-ca-spawn.*$TIME_OF_INSTALLATION*.log	Problèmes de haut niveau et traces Python pour le processus d'installation de **pkispawn**
journalctl -u pki-tomcatd@pki-tomcat sortie	Erreurs provenant du service **pki-tomcatd@pki-tomcat**
/var/log/pki/pki-tomcat/ca/debug.*$DATE*.log	Grandes traces d'activité JAVA au cœur du produit d'infrastructure à clé publique (PKI)
/var/log/pki/pki-tomcat/ca/signedAudit/ca_audit	Journal d'audit du produit PKI
• **/var/log/pki/pki-tomcat/ca/system** • **/var/log/pki/pki-tomcat/ca/transactions** • **/var/log/pki/pki-tomcat/catalina.*$DATE*.log**	Données de débogage de bas niveau des opérations de certificat pour les mandants de service, les hôtes et les autres entités qui utilisent des certificats

Sur le serveur contacté par la réplique :

- **/var/log/httpd/error_log** fichier journal

L'installation du service CA sur une réplique IdM existante écrit également des informations de débogage dans le fichier journal suivant :

- **/var/log/ipareplica-ca-install.log** fichier journal

NOTE

Si une installation complète de réplique IdM échoue lors de l'installation du composant CA optionnel, aucun détail concernant le CA n'est consigné ; un message est consigné dans le fichier **/var/log/ipareplica-install.log** indiquant que le processus d'installation global a échoué. Red Hat recommande d'examiner les fichiers journaux énumérés ci-dessus pour obtenir des détails spécifiques à l'échec de l'installation de l'AC.

La seule exception à ce comportement est lorsque vous installez le service d'autorité de certification et que l'autorité de certification racine est une autorité de certification externe. En cas de problème avec le certificat de l'autorité de certification externe, les erreurs sont consignées dans **/var/log/ipareplica-install.log**.

Ressources supplémentaires

- Examen des erreurs d'installation de l'autorité de certification IdM

21.4. EXAMEN DES ERREURS D'INSTALLATION DE L'AUTORITÉ DE CERTIFICATION IDM

Pour dépanner une installation CA IdM défaillante, examinez les erreurs à la fin des fichiers journaux d'erreur de l'installation CA et utilisez ces informations pour résoudre les problèmes correspondants.

Conditions préalables

- Vous devez avoir les privilèges **root** pour afficher le contenu des fichiers journaux IdM.

Procédure

1. Pour examiner un fichier journal de manière interactive, ouvrez la fin du fichier journal à l'aide de l'utilitaire **less** et utilisez les touches fléchées ↑ et ↓ pour naviguer, tout en recherchant les entrées **ScriptError**. L'exemple suivant ouvre **/var/log/pki/pki-ca-spawn.*$TIME_OF_INSTALLATION*.log**.

```
[user@server ~]$ sudo less -N G /var/log/pki/pki-ca-spawn.20200527185902.log
```

2. Recueillez des informations de dépannage supplémentaires en répétant ce processus d'examen avec tous les fichiers journaux d'erreur de l'installation de CA.

Ressources supplémentaires

- Fichiers journaux des erreurs d'installation de l'autorité de certification IdM
- Si vous ne parvenez pas à résoudre l'échec de l'installation d'un serveur IdM et que vous disposez d'un abonnement au support technique de Red Hat, ouvrez un dossier de support technique sur le portail client de Red Hat et fournissez une adresse **sosreport** du serveur.
- L'utilitaire **sosreport** collecte des détails de configuration, des journaux et des informations système à partir d'un système RHEL. Pour plus d'informations sur l'utilitaire **sosreport**, voir Qu'est-ce qu'un rapport sos et comment en créer un dans Red Hat Enterprise Linux ?

21.5. SUPPRESSION D'UNE INSTALLATION PARTIELLE DE RÉPLIQUE IDM

Si l'installation d'un réplica IdM échoue, certains fichiers de configuration peuvent être laissés sur place. D'autres tentatives d'installation du réplica IdM peuvent échouer et le script d'installation signale que l'IPA est déjà configuré :

Exemple de système avec une configuration IdM partielle existante

```
[root@server ~]# ipa-replica-install
Your system may be partly configured.
Run /usr/sbin/ipa-server-install --uninstall to clean up.

IPA server is already configured on this system.
If you want to reinstall the IPA server, please uninstall it first using 'ipa-server-install --uninstall'.
The ipa-replica-install command failed. See /var/log/ipareplica-install.log for more information
```

Pour résoudre ce problème, désinstallez le logiciel IdM du réplica, supprimez le réplica de la topologie IdM et réessayez le processus d'installation.

Conditions préalables

- Vous devez avoir les privilèges de **root**.

Procédure

1. Désinstallez le logiciel du serveur IdM sur l'hôte que vous essayez de configurer comme réplique IdM.

   ```
   [root@replica ~]# ipa-server-install --uninstall
   ```

2. Sur tous les autres serveurs de la topologie, utilisez la commande **ipa server-del** pour supprimer toutes les références au réplica qui ne s'est pas installé correctement.

   ```
   [root@other-replica ~]# ipa server-del replica.idm.example.com
   ```

3. Tenter d'installer la réplique.

4. Si vous continuez à éprouver des difficultés à installer une réplique IdM en raison d'échecs répétés, réinstallez le système d'exploitation.
   L'une des conditions requises pour l'installation d'une réplique IdM est un système propre, sans aucune personnalisation. Les installations qui ont échoué peuvent avoir compromis l'intégrité de l'hôte en modifiant de manière inattendue les fichiers du système.

Ressources supplémentaires

- Pour plus de détails sur la désinstallation d'un réplica IdM, voir Désinstallation d'un réplica IdM .
- Si les tentatives d'installation échouent après des tentatives répétées de désinstallation et que vous disposez d'un abonnement au support technique de Red Hat, ouvrez un dossier de support technique sur le portail client de Red Hat et fournissez une adresse **sosreport** du réplica et une adresse **sosreport** du serveur.
- L'utilitaire **sosreport** collecte des détails de configuration, des journaux et des informations système à partir d'un système RHEL. Pour plus d'informations sur l'utilitaire **sosreport**, voir Qu'est-ce qu'un rapport sos et comment en créer un dans Red Hat Enterprise Linux ?

21.6. RÉSOUDRE LES ERREURS LIÉES AUX INFORMATIONS D'IDENTIFICATION NON VALIDES

Si l'installation d'un réplica IdM échoue avec une erreur **Invalid credentials**, les horloges système des hôtes peuvent être désynchronisées :

```
[27/40]: setting up initial replication
Starting replication, please wait until this has completed.
Update in progress, 15 seconds elapsed
[ldap://server.example.com:389] reports: Update failed! Status: [49 - LDAP error: Invalid credentials]

[error] RuntimeError: Failed to start replication
Your system may be partly configured.
Run /usr/sbin/ipa-server-install --uninstall to clean up.

ipa.ipapython.install.cli.install_tool(CompatServerReplicaInstall): ERROR    Failed to start replication
ipa.ipapython.install.cli.install_tool(CompatServerReplicaInstall): ERROR    The ipa-replica-install command failed. See /var/log/ipareplica-install.log for more information
```

Si vous utilisez les options **--no-ntp** ou **-N** pour tenter l'installation du réplica alors que les horloges sont désynchronisées, l'installation échoue car les services ne peuvent pas s'authentifier avec Kerberos.

Pour résoudre ce problème, synchronisez les horloges des deux hôtes et réessayez le processus d'installation.

Conditions préalables

- Vous devez disposer des privilèges **root** pour modifier l'heure du système.

Procédure

1. Synchroniser les horloges du système manuellement ou à l'aide de **chronyd**.

   Synchronisation manuelle

   Affichez l'heure du système sur le serveur et réglez l'heure de la réplique pour qu'elle corresponde.

   ```
   [user@server ~]$ date
   Thu May 28 21:03:57 EDT 2020

   [user@replica ~]$ sudo timedatectl set-time '2020-05-28 21:04:00'
   ```

   - **Synchronizing with chronyd**:
     Voir Utilisation de la suite Chrony pour configurer NTP pour configurer et régler l'heure du système avec les outils **chrony**.

2. Réessayez l'installation de la réplique IdM.

Ressources supplémentaires

- Si vous ne parvenez pas à résoudre l'échec de l'installation d'un réplica et que vous disposez d'un abonnement à l'assistance technique de Red Hat, ouvrez un dossier d'assistance technique sur

le portail client de Red Hat et fournissez une adresse **sosreport** du réplica et une adresse **sosreport** du serveur.

- L'utilitaire **sosreport** collecte des détails de configuration, des journaux et des informations système à partir d'un système RHEL. Pour plus d'informations sur l'utilitaire **sosreport**, voir Qu'est-ce qu'un rapport sos et comment en créer un dans Red Hat Enterprise Linux ?

21.7. RESSOURCES SUPPLÉMENTAIRES

- Dépannage de la première installation du serveur IdM
- Dépannage de l'installation du client IdM
- Sauvegarde et restauration de l'IdM

CHAPITRE 22. DÉSINSTALLATION D'UNE RÉPLIQUE IDM

En tant qu'administrateur IdM, vous pouvez supprimer un réplica Identity Management (IdM) de la topologie. Pour plus d'informations, voir Désinstallation d'un serveur IdM .

CHAPITRE 23. GESTION DE LA TOPOLOGIE DE RÉPLICATION

Ce chapitre décrit comment gérer la réplication entre les serveurs d'un domaine de gestion des identités (IdM).

Ressources supplémentaires

- Planification de la topologie du réplica

23.1. EXPLICATION DES ACCORDS DE RÉPLICATION, DES SUFFIXES DE TOPOLOGIE ET DES SEGMENTS DE TOPOLOGIE

Lorsque vous créez une réplique, Identity Management (IdM) crée un accord de réplication entre le serveur initial et la réplique. Les données répliquées sont ensuite stockées dans des suffixes de topologie et lorsque deux répliques ont un accord de réplication entre leurs suffixes, ces derniers forment un segment de topologie. Ces concepts sont expliqués plus en détail dans les sections suivantes :

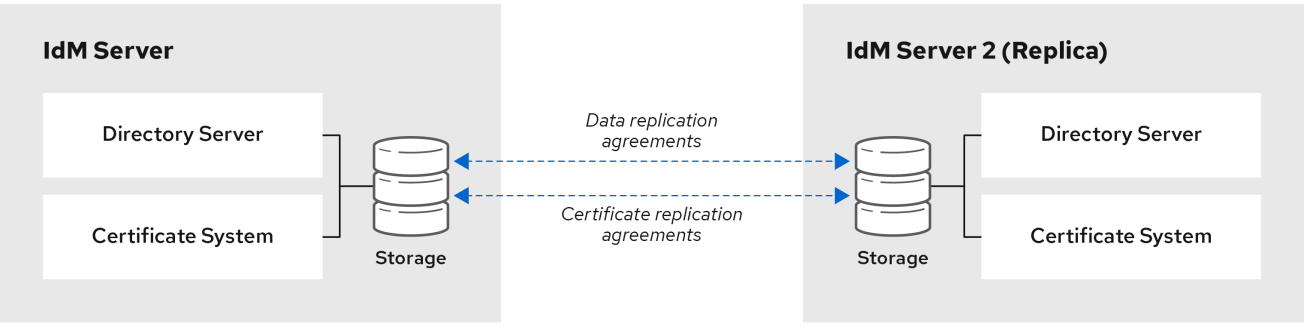
- Accords de réplication
- Suffixes de topologie
- Segments de topologie

23.1.1. 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 23.1. 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.

23.1.2. Suffixes de topologie

Topology suffixes stocker les données répliquées. IdM prend en charge deux types de suffixes de topologie : **domain** et **ca**. Chaque suffixe représente un serveur distinct, une topologie de réplication distincte.

Lorsqu'un accord de réplication est configuré, il joint deux suffixes de topologie du même type sur deux serveurs différents.

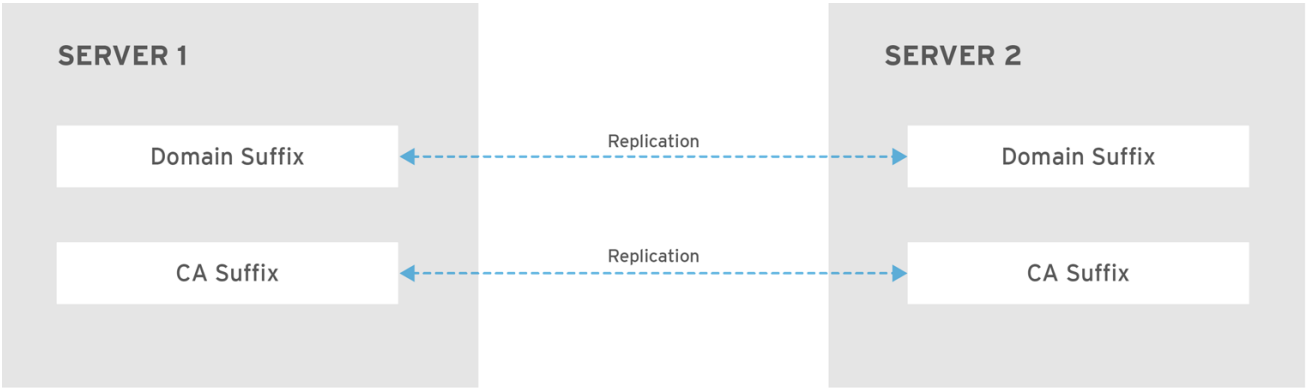
Le suffixe domain: dc=*example*,dc=*com*

Le suffixe **domain** contient toutes les données relatives au domaine.
Lorsque deux répliques ont un accord de réplication entre leurs suffixes **domain**, elles partagent les données de l'annuaire, telles que les utilisateurs, les groupes et les stratégies.

Le suffixe ca: o=ipaca

Le suffixe **ca** contient des données relatives au composant du système de certification. Il n'est présent que sur les serveurs sur lesquels une autorité de certification (CA) est installée.
Lorsque deux répliques ont un accord de réplication entre leurs suffixes **ca**, elles partagent les données du certificat.

Figure 23.2. Suffixes de topologie



Un accord initial de réplication de la topologie est établi entre deux serveurs par le script **ipa-replica-install** lors de l'installation d'une nouvelle réplique.

Exemple 23.1. Visualisation des suffixes de topologie

La commande **ipa topologysuffix-find** affiche une liste des suffixes de la topologie :

```
$ ipa topologysuffix-find
----------------------------
2 topology suffixes matched
----------------------------
  Suffix name: ca
  Managed LDAP suffix DN: o=ipaca
```

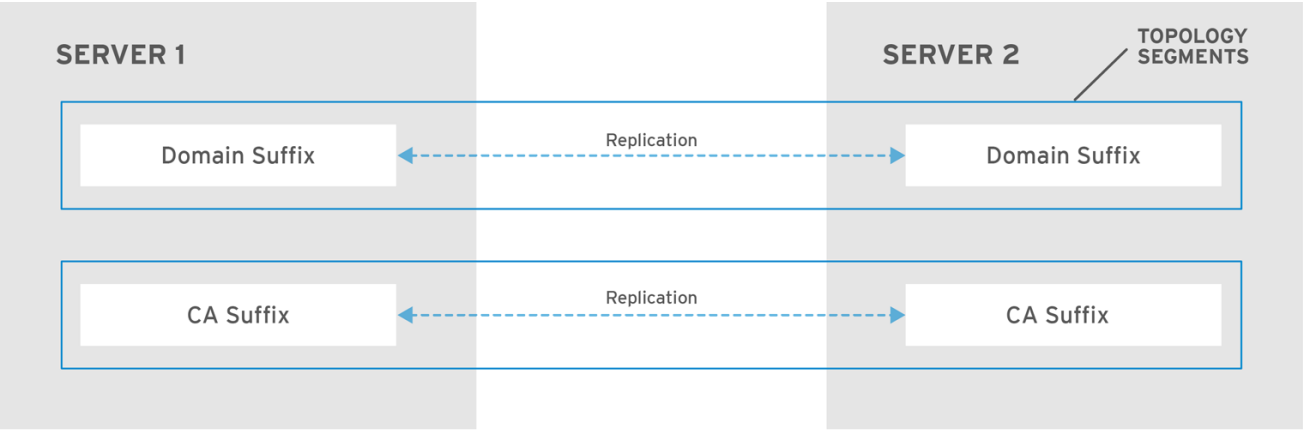
```
  Suffix name: domain
  Managed LDAP suffix DN: dc=example,dc=com
----------------------------
Number of entries returned 2
----------------------------
```

23.1.3. Segments de topologie

Lorsque deux répliques ont un accord de réplication entre leurs suffixes, les suffixes forment un *topology segment*. Chaque segment topologique est constitué d'un *left node* et d'un *right node*. Les nœuds représentent les serveurs liés par l'accord de réplication.

Les segments de topologie dans IdM sont toujours bidirectionnels. Chaque segment représente deux accords de réplication : du serveur A au serveur B, et du serveur B au serveur A. Les données sont donc répliquées dans les deux sens.

Figure 23.3. Segments de topologie



Exemple 23.2. Visualisation des segments de topologie

La commande **ipa topologysegment-find** montre les segments de topologie actuels configurés pour les suffixes de domaine ou de CA. Par exemple, pour le suffixe de domaine :

```
$ ipa topologysegment-find
Suffix name: domain
-----------------
1 segment matched
-----------------
  Segment name: server1.example.com-to-server2.example.com
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------
```

Dans cet exemple, les données relatives au domaine ne sont répliquées qu'entre deux serveurs : **server1.example.com** et **server2.example.com**.

Pour afficher les détails d'un segment particulier uniquement, utilisez la commande **ipa topologysegment-show**:

```
$ ipa topologysegment-show
Suffix name: domain
Segment name: server1.example.com-to-server2.example.com
  Segment name: server1.example.com-to-server2.example.com
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
```

23.2. UTILISATION DU GRAPHE TOPOLOGIQUE POUR GÉRER LA TOPOLOGIE DE RÉPLICATION

Le graphique de la topologie dans l'interface Web montre les relations entre les serveurs du domaine. L'interface Web permet de manipuler et de transformer la représentation de la topologie.

Accès au graphe topologique

Pour accéder au graphique de la topologie :

1. Sélectionner **Serveur IPA → Topologie → Graphique de la topologie**
2. Si vous apportez des modifications à la topologie qui ne sont pas immédiatement reflétées dans le graphique, cliquez sur **Actualiser**.

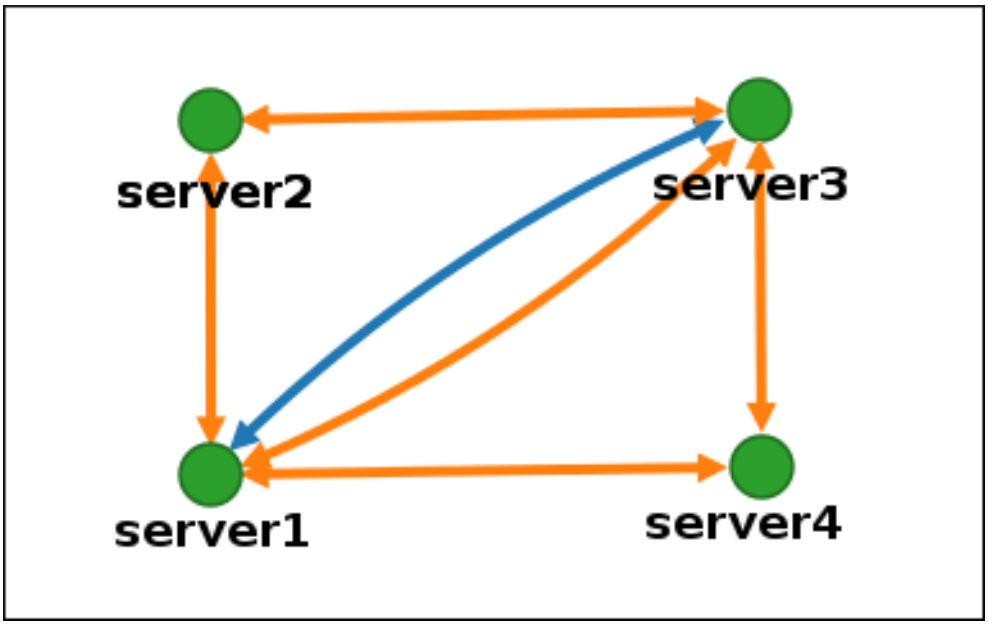
Interprétation du graphe topologique

Les serveurs liés par un accord de réplication de domaine sont reliés par une flèche orange. Les serveurs liés par un accord de réplication de CA sont reliés par une flèche bleue.

Exemple de graphique topologique : topologie recommandée

L'exemple de topologie recommandée ci-dessous montre l'une des topologies recommandées possibles pour quatre serveurs : chaque serveur est connecté à au moins deux autres serveurs, et plus d'un serveur est un serveur CA.

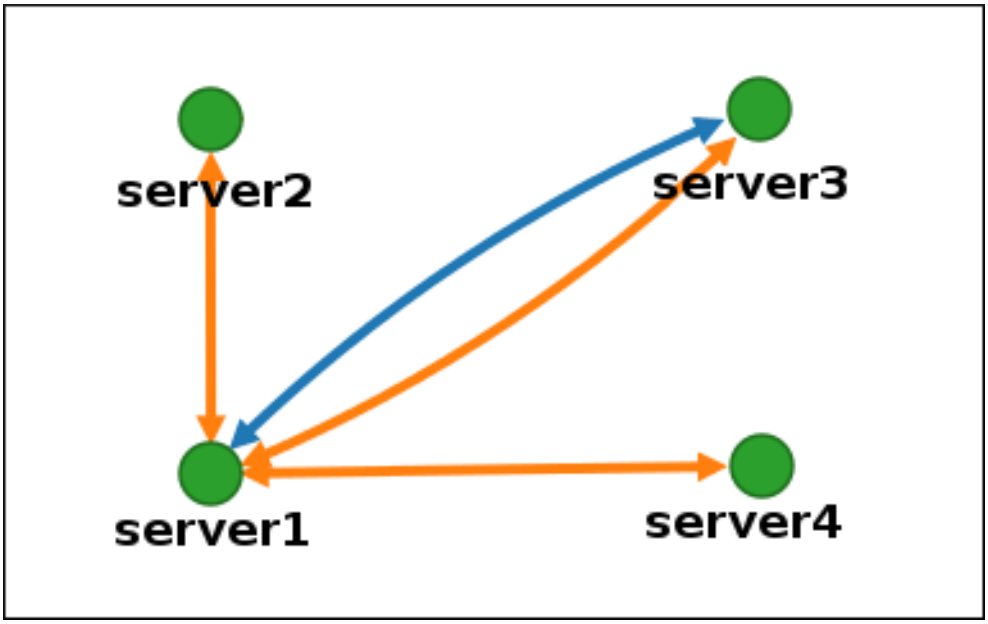
Figure 23.4. Exemple de topologie recommandée



Exemple de graphe topologique : topologie déconseillée

Dans l'exemple de topologie déconseillée ci-dessous, **server1** est un point de défaillance unique. Tous les autres serveurs ont des accords de réplication avec ce serveur, mais pas avec les autres serveurs. Par conséquent, si **server1** tombe en panne, tous les autres serveurs seront isolés. Évitez de créer des topologies de ce type.

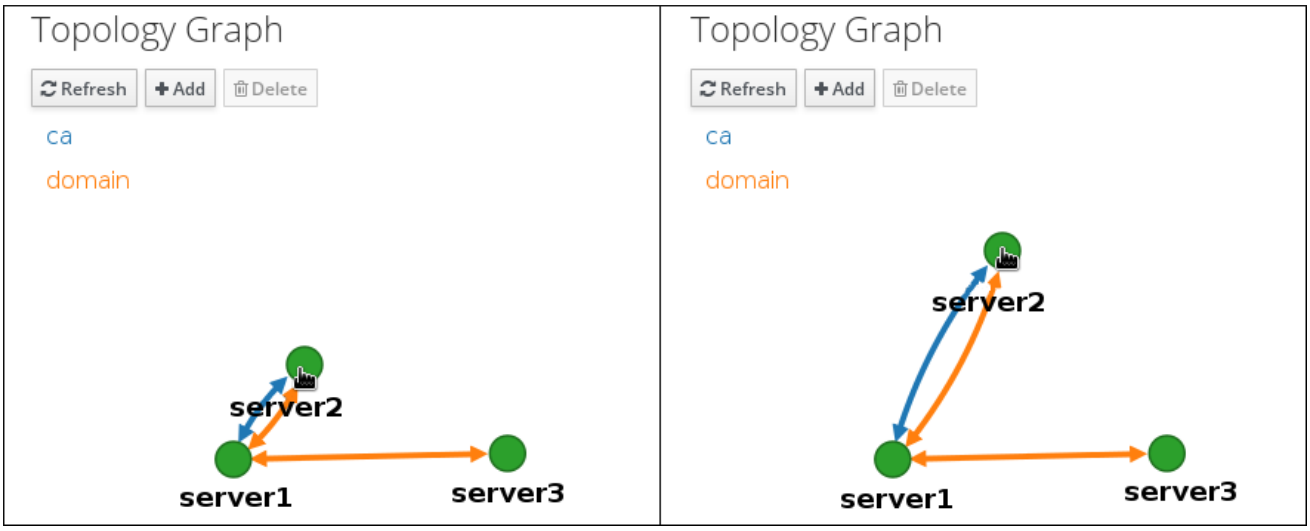
Figure 23.5. Exemple de topologie déconseillée : Point de défaillance unique



Personnaliser la vue topologique

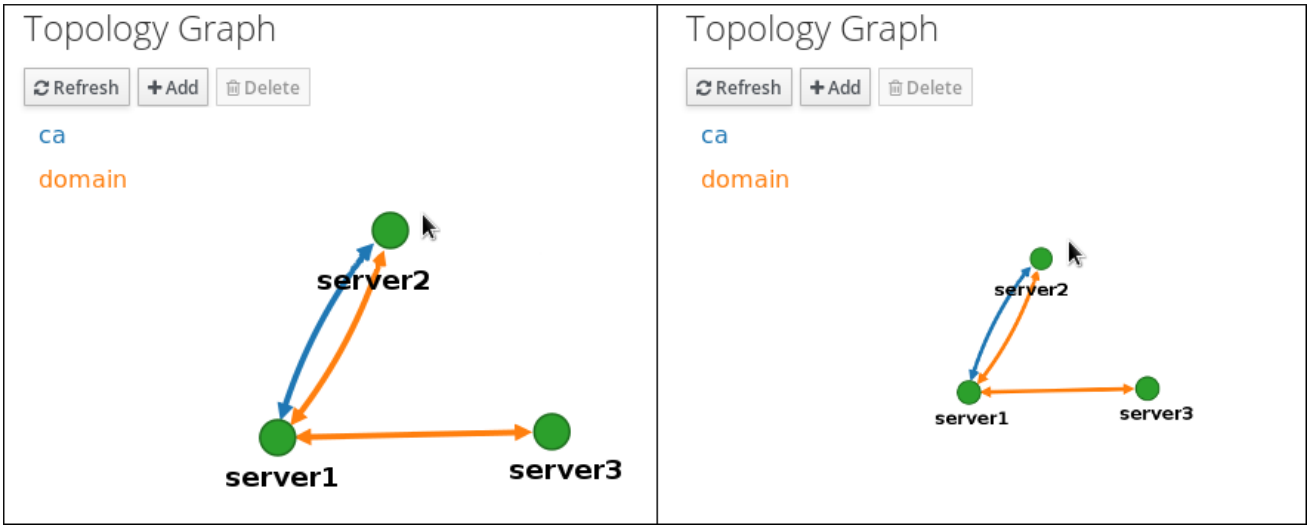
Vous pouvez déplacer des nœuds topologiques individuels en faisant glisser la souris :

Figure 23.6. Déplacement des nœuds du graphe topologique



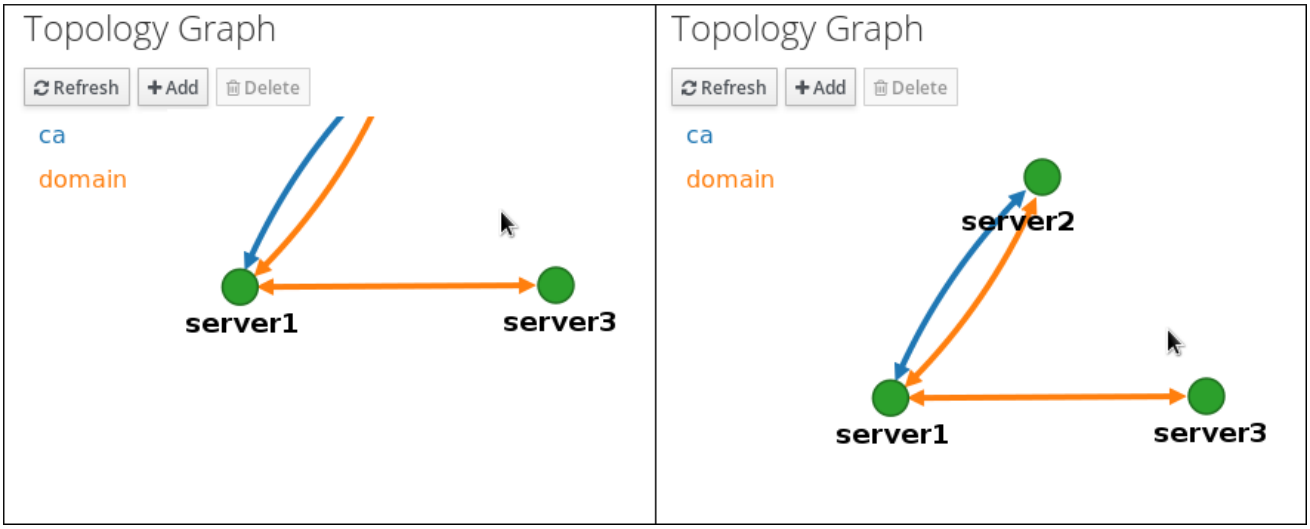
Vous pouvez agrandir ou réduire le graphique topologique à l'aide de la molette de la souris :

Figure 23.7. Zoom sur le graphe topologique



Vous pouvez déplacer le canevas du graphique topologique en maintenant le bouton gauche de la souris enfoncé :

Figure 23.8. Déplacement du canevas du graphe topologique



23.3. CONFIGURATION DE LA RÉPLICATION ENTRE DEUX SERVEURS À L'AIDE DE L'INTERFACE WEB

L'interface Web de la gestion des identités (IdM) vous permet de choisir deux serveurs et de créer un nouvel accord de réplication entre eux.

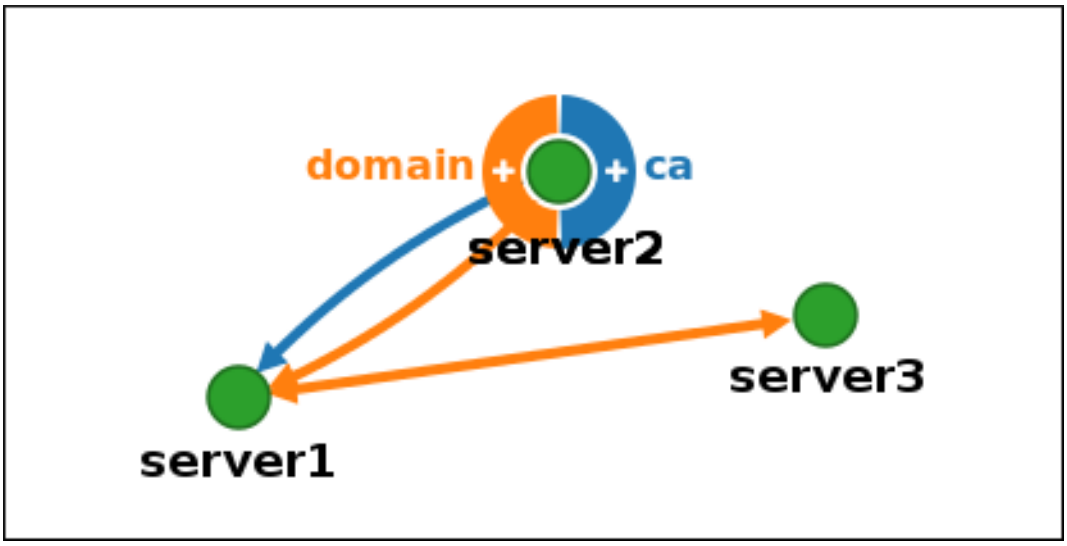
Conditions préalables

- Vous disposez des informations d'identification de l'administrateur IdM.

Procédure

1. Dans le graphique topologique, passez votre souris sur l'un des nœuds de serveur.

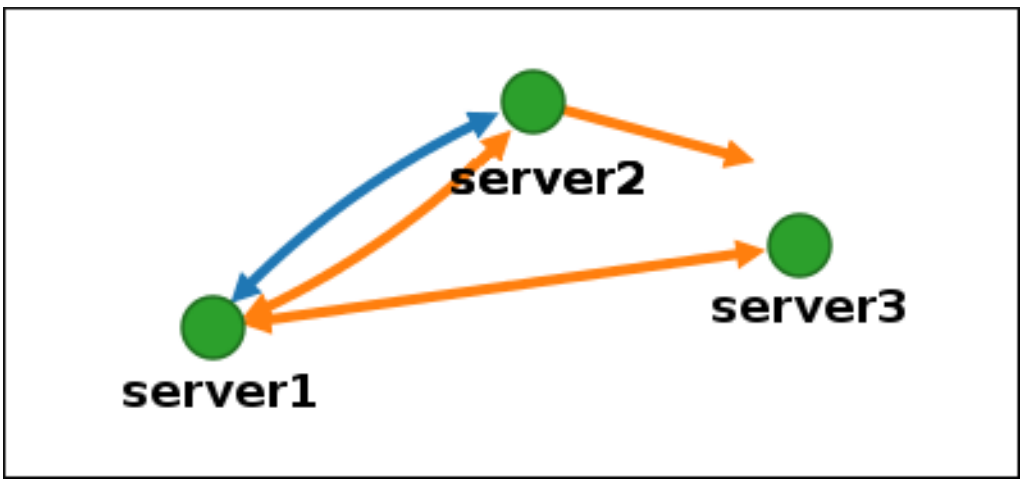
   Figure 23.9. Options de domaine ou d'autorité de certification

2. Cliquez sur la partie **domain** ou **ca** du cercle en fonction du type de segment topologique que vous souhaitez créer.

3. Une nouvelle flèche représentant le nouvel accord de réplication apparaît sous le pointeur de votre souris. Déplacez votre souris vers l'autre nœud de serveur et cliquez dessus.

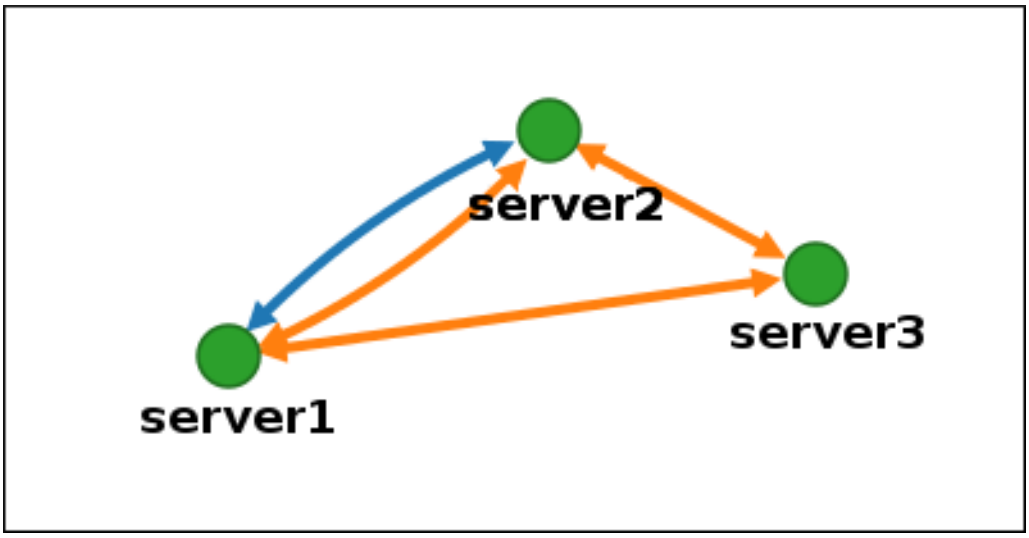
   Figure 23.10. Création d'un nouveau segment

4. Dans la fenêtre **Add topology segment**, cliquez sur **Ajouter** pour confirmer les propriétés du nouveau segment.

Le nouveau segment topologique entre les deux serveurs les associe à un accord de réplication. Le graphique de la topologie montre maintenant la topologie de réplication mise à jour :

Figure 23.11. Création d'un nouveau segment



23.4. ARRÊT DE LA RÉPLICATION ENTRE DEUX SERVEURS À L'AIDE DE L'INTERFACE WEB

L'interface web de la gestion des identités (IdM) permet de supprimer un accord de réplication des serveurs.

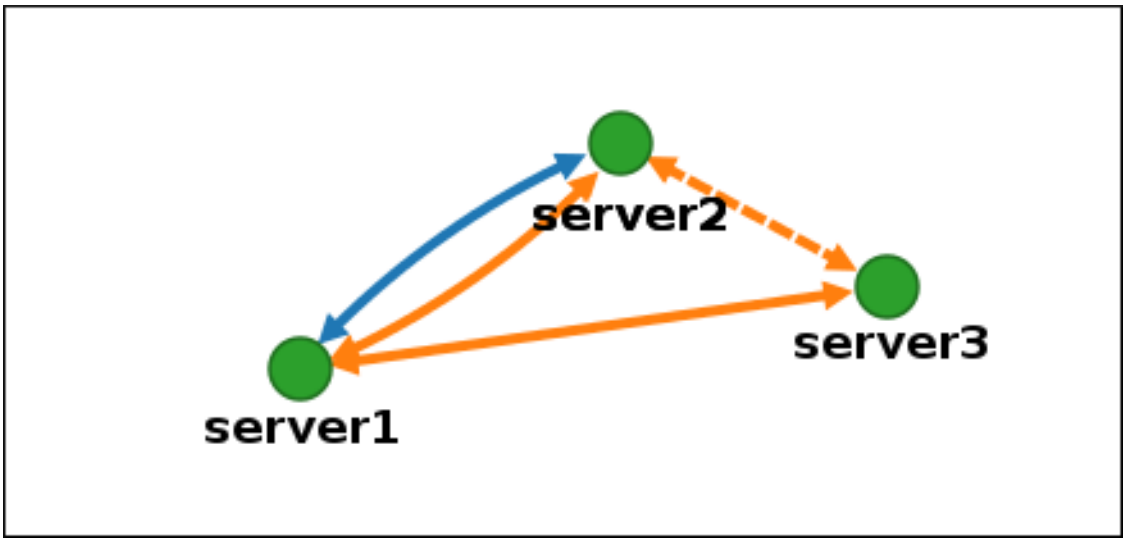
Conditions préalables

- Vous disposez des informations d'identification de l'administrateur IdM.

Procédure

1. Cliquez sur une flèche représentant l'accord de réplication que vous souhaitez supprimer. La flèche est mise en évidence.

   Figure 23.12. Segment de topologie mis en évidence

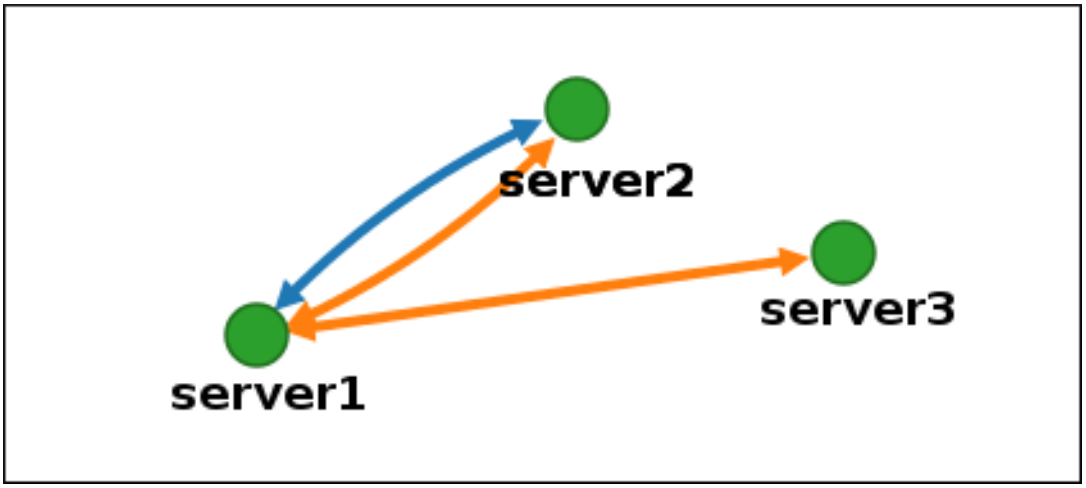
   

2. Click **Delete**.

3. Dans la fenêtre **Confirmation**, cliquez sur **OK**.

IdM supprime le segment de topologie entre les deux serveurs, ce qui supprime leur accord de réplication. Le graphique de la topologie montre maintenant la topologie de réplication mise à jour :

Figure 23.13. Segment de topologie supprimé



23.5. CONFIGURATION DE LA RÉPLICATION ENTRE DEUX SERVEURS À L'AIDE DU CLI

Vous pouvez configurer les accords de réplication entre deux serveurs à l'aide de la commande **ipa topologysegment-add**.

Conditions préalables

- Vous disposez des informations d'identification de l'administrateur IdM.

Procédure

1. Utilisez la commande **ipa topologysegment-add** pour créer un segment de topologie pour les deux serveurs. Lorsque vous y êtes invité, fournissez :
   - le suffixe topologique requis : **domain** ou **ca**
   - le nœud gauche et le nœud droit, représentant les deux serveurs
   - éventuellement, un nom personnalisé pour le segment
     Par exemple :

```
$ ipa topologysegment-add
Suffix name: domain
Left node: server1.example.com
Right node: server2.example.com
Segment name [server1.example.com-to-server2.example.com]: new_segment
----------------------------
Added segment "new_segment"
----------------------------
  Segment name: new_segment
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
```

L'ajout du nouveau segment joint les serveurs dans un accord de réplication.

2. *Optional.* Utilisez la commande **ipa topologysegment-show** pour vérifier que le nouveau segment est configuré.

```
$ ipa topologysegment-show
Suffix name: domain
Segment name: new_segment
  Segment name: new_segment
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
```

23.6. ARRÊT DE LA RÉPLICATION ENTRE DEUX SERVEURS À L'AIDE DE LA CLI

Vous pouvez mettre fin aux accords de réplication à partir de la ligne de commande en utilisant la commande **ipa topology_segment-del**.

Conditions préalables

- Vous disposez des informations d'identification de l'administrateur IdM.

Procédure

1. Pour arrêter la réplication, vous devez supprimer le segment de réplication correspondant entre les serveurs. Pour ce faire, vous devez connaître le nom du segment.
   Si vous ne connaissez pas le nom, utilisez la commande **ipa topologysegment-find** pour afficher tous les segments et localisez le segment requis dans la sortie. Lorsque vous y êtes invité, indiquez le suffixe de topologie requis : **domain** ou **ca**. Par exemple :

```
$ ipa topologysegment-find
Suffix name: domain
------------------
8 segments matched
------------------
  Segment name: new_segment
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both

...

----------------------------
Number of entries returned 8
----------------------------
```

2. Utilisez la commande **ipa topologysegment-del** pour supprimer le segment topologique reliant les deux serveurs.

```
$ ipa topologysegment-del
Suffix name: domain
Segment name: new_segment
```

```
----------------------------
Deleted segment "new_segment"
----------------------------
```

La suppression du segment supprime l'accord de réplication.

3. *Optional.* Utilisez la commande **ipa topologysegment-find** pour vérifier que le segment n'est plus répertorié.

```
$ ipa topologysegment-find
Suffix name: domain
------------------
7 segments matched
------------------
  Segment name: server2.example.com-to-server3.example.com
  Left node: server2.example.com
  Right node: server3.example.com
  Connectivity: both

...

----------------------------
Number of entries returned 7
----------------------------
```

23.7. SUPPRESSION D'UN SERVEUR DE LA TOPOLOGIE À L'AIDE DE L'INTERFACE WEB

Vous pouvez utiliser l'interface web de la gestion des identités (IdM) pour supprimer un serveur de la topologie.

Conditions préalables

- Vous disposez des informations d'identification de l'administrateur IdM.
- Le serveur que vous souhaitez supprimer est **not** le seul serveur qui relie les autres serveurs au reste de la topologie ; cela aurait pour effet d'isoler les autres serveurs, ce qui n'est pas autorisé.
- Le serveur que vous souhaitez supprimer est **not** votre dernier serveur CA ou DNS.

AVERTISSEMENT

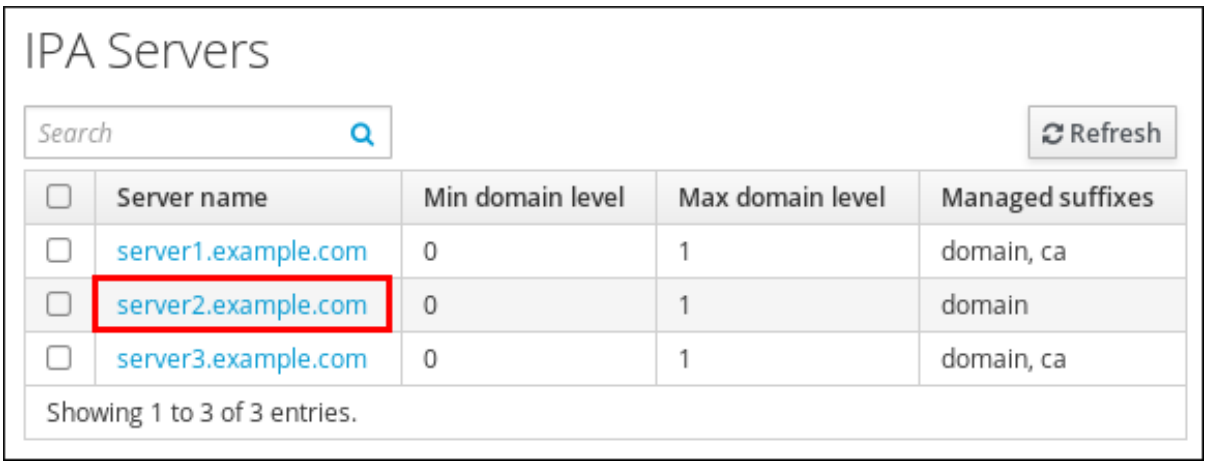
La suppression d'un serveur est une action irréversible. Si vous supprimez un serveur, la seule façon de le réintroduire dans la topologie est d'installer une nouvelle réplique sur la machine.

Procédure

Pour supprimer un serveur de la topologie sans désinstaller les composants du serveur de la machine :

1. Sélectionner **Serveur IPA → Topologie → Serveurs IPA**.
2. Cliquez sur le nom du serveur que vous souhaitez supprimer.

Figure 23.14. Sélection d'un serveur



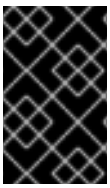
3. Cliquez sur **Supprimer le serveur**.

23.8. SUPPRESSION D'UN SERVEUR DE LA TOPOLOGIE À L'AIDE DE LA CLI

Vous pouvez utiliser l'interface de ligne de commande pour supprimer un serveur de la topologie.

Conditions préalables

- Vous disposez des informations d'identification de l'administrateur IdM.
- Le serveur que vous souhaitez supprimer est **not** le seul serveur qui relie les autres serveurs au reste de la topologie ; cela aurait pour effet d'isoler les autres serveurs, ce qui n'est pas autorisé
- Le serveur que vous souhaitez supprimer est **not** votre dernier serveur CA ou DNS.



IMPORTANT

La suppression d'un serveur est une action irréversible. Si vous supprimez un serveur, la seule façon de le réintroduire dans la topologie est d'installer une nouvelle réplique sur la machine.

Procédure

Pour supprimer **server1.example.com**:

1. Sur un autre serveur, exécutez la commande **ipa server-del** pour supprimer **server1.example.com**. La commande supprime tous les segments topologiques pointant vers le serveur :

```
[user@server2 ~]$ ipa server-del
Server name: server1.example.com
Removing server1.example.com from replication topology, please wait...
-----------------------------------------------------------
Deleted IPA server "server1.example.com"
-----------------------------------------------------------
```

2. *Optional*le programme de désinstallation du serveur se trouve à l'adresse suivante : **server1.example.com**, exécutez la commande **ipa server-install --uninstall** pour désinstaller les composants du serveur de l'ordinateur.

```
[root@server1 ~]# ipa server-install --uninstall
```

23.9. VISUALISATION DES RÔLES DE SERVEUR SUR UN SERVEUR IDM À L'AIDE DE L'INTERFACE WEB

En fonction des services installés sur un serveur IdM, celui-ci peut effectuer diverses opérations *server roles*. Par exemple :

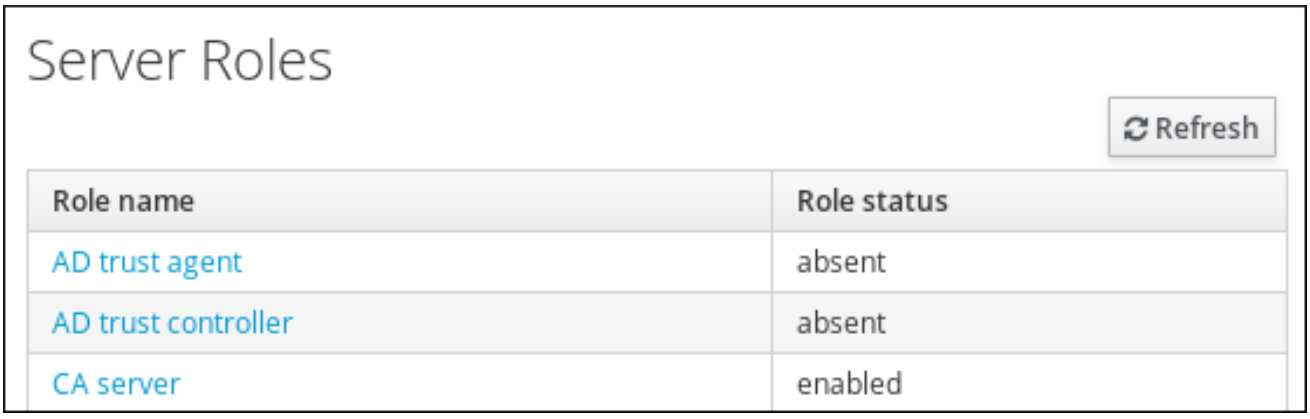
- Serveur CA
- Serveur DNS
- Serveur de l'autorité de recouvrement des clés (KRA).

Pour une liste complète des rôles de serveur pris en charge, voir **Serveur IPA → Topologie → Rôles du serveur**.

NOTE

- L'état du rôle **absent** signifie qu'aucun serveur de la topologie ne joue le rôle en question.
- Le statut du rôle **enabled** signifie qu'un ou plusieurs serveurs de la topologie jouent le rôle en question.

Figure 23.15. Rôles des serveurs dans l'interface web



23.10. VISUALISATION DES RÔLES DE SERVEUR SUR UN SERVEUR IDM À L'AIDE DE LA CLI

En fonction des services installés sur un serveur IdM, celui-ci peut effectuer diverses opérations *server roles*. Par exemple :

- Serveur CA
- Serveur DNS

- Serveur de l'autorité de recouvrement des clés (KRA).

Les commandes suivantes permettent de voir quels serveurs jouent quel rôle dans la topologie.

- La commande **ipa config-show** affiche tous les serveurs d'autorité de certification et le serveur de renouvellement d'autorité de certification actuel :

```
$ ipa config-show
  ...
  IPA masters: server1.example.com, server2.example.com, server3.example.com
  IPA CA servers: server1.example.com, server2.example.com
  IPA CA renewal master: server1.example.com
```

- La commande **ipa server-show** permet d'afficher la liste des rôles activés sur un serveur particulier. Par exemple, pour obtenir la liste des rôles activés sur *server.example.com*:

```
$ ipa server-show
Server name: server.example.com
  ...
  Enabled server roles: CA server, DNS server, KRA server
```

- Le site **ipa server-find --servrole** recherche tous les serveurs pour lesquels un rôle de serveur particulier est activé. Par exemple, pour rechercher tous les serveurs CA :

```
$ ipa server-find --servrole "CA server"
---------------------
2 IPA servers matched
---------------------
  Server name: server1.example.com
  ...

  Server name: server2.example.com
  ...
----------------------------
Number of entries returned 2
----------------------------
```

23.11. PROMOUVOIR UN RÉPLICA EN TANT QUE SERVEUR DE RENOUVELLEMENT DE L'AUTORITÉ DE CERTIFICATION ET SERVEUR D'ÉDITION DE CRL

Si votre déploiement IdM utilise une autorité de certification (CA) intégrée, l'un des serveurs CA IdM agit en tant que serveur de renouvellement CA, un serveur qui gère le renouvellement des certificats du sous-système CA. L'un des serveurs de l'autorité de certification IdM fait également office de serveur d'édition CRL IdM, un serveur qui génère des listes de révocation de certificats. Par défaut, les rôles de serveur de renouvellement de CA et de serveur d'édition de CRL sont installés sur le premier serveur sur lequel l'administrateur système a installé le rôle CA à l'aide de la commande **ipa-server-install** ou **ipa-ca-install**.

Conditions préalables

- Vous disposez des informations d'identification de l'administrateur IdM.

Procédure

Procedure

- Modifier le serveur de renouvellement de l'autorité de certification.
- Configurer le réplica pour qu'il génère des CRL.

23.12. RÉTROGRADER OU PROMOUVOIR DES RÉPLIQUES CACHÉES

Après l'installation d'un réplica, vous pouvez configurer si le réplica est caché ou visible.

Pour plus de détails sur les répliques cachées, voir Le mode réplique cachée.

Si le réplica est un serveur de renouvellement de l'AC, déplacez le service vers un autre réplica avant de rendre ce réplica masqué.

For details, see

Modification et réinitialisation du serveur de renouvellement de l'autorité de certification IdM

Procédure

- Pour masquer la réplique, entrez :

```
# ipa server-state replica.idm.example.com --state=hidden
```

Vous pouvez également rendre le réplica visible à l'aide de la commande suivante :

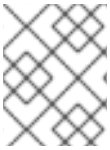
```
# ipa server-state replica.idm.example.com --state=enabled
```

CHAPITRE 24. INSTALLATION ET EXÉCUTION DE L'OUTIL IDM HEALTHCHECK

Ce chapitre décrit l'outil IdM Healthcheck et explique comment l'installer et l'exécuter.

24.1. CONTRÔLE DE SANTÉ DANS L'IDM

L'outil Healthcheck de la gestion des identités (IdM) permet de détecter les problèmes susceptibles d'affecter la santé de votre environnement IdM.



NOTE

L'outil Healthcheck est un outil de ligne de commande qui peut être utilisé sans authentification Kerberos.

Les modules sont indépendants

Le Healthcheck se compose de modules indépendants qui testent les éléments suivants

- Problèmes de réplication
- Validité du certificat
- Questions relatives à l'infrastructure de l'autorité de certification
- Questions relatives à la confiance dans IdM et Active Directory
- Autorisations d'accès aux fichiers et paramètres de propriété corrects

Deux formats de sortie

Healthcheck génère les sorties suivantes, que vous pouvez définir à l'aide de l'option **output-type**:

- **json**: Sortie lisible par la machine au format JSON (par défaut)
- **human**: Sortie lisible par l'homme

Vous pouvez spécifier une autre destination de fichier avec l'option **--output-file**.

Résultats

Chaque module de contrôle de santé renvoie l'un des résultats suivants :

SUCCÈS
: configuré comme prévu

AVERTISSEMENT
: il ne s'agit pas d'une erreur, mais cela vaut la peine de garder un œil ou d'évaluer la situation

ERREUR
: n'est pas configuré comme prévu

CRITIQUE
: n'est pas configuré comme prévu, avec un risque élevé d'impact

24.2. INSTALLATION DE IDM HEALTHCHECK

Cette section décrit comment installer l'outil IdM Healthcheck.

Procédure

- Installez le paquetage **ipa-healthcheck**:

```
[root@server ~]# dnf install ipa-healthcheck
```

Verification steps

- Utilisez l'option **--failures-only** pour que **ipa-healthcheck** ne signale que les erreurs. Une installation IdM fonctionnant parfaitement renvoie un résultat vide de **[]**.

```
[root@server ~]# ipa-healthcheck --failures-only
[]
```

Ressources supplémentaires

- Utilisez **ipa-healthcheck --help** pour voir tous les arguments soutenus.

24.3. EXÉCUTION DU CONTRÔLE DE SANTÉ DE L'IDM

Le bilan de santé peut être exécuté manuellement ou automatiquement à l'aide de la rotation des journaux

Conditions préalables

- L'outil Healthcheck doit être installé. Voir Installation de IdM Healthcheck.

Procédure

- Pour exécuter manuellement le contrôle de santé, entrez la commande **ipa-healthcheck**.

```
[root@server ~]# ipa-healthcheck
```

Ressources supplémentaires

Pour toutes les options, voir la page de manuel : **man ipa-healthcheck**.

24.4. RESSOURCES SUPPLÉMENTAIRES

- Voir les sections suivantes du guide Utilisation d'IdM Healthcheck pour surveiller votre environnement IdM pour des exemples d'utilisation d'IdM Healthcheck.
  - Services de contrôle
  - Vérification de la configuration de la confiance IdM et AD
  - Vérification des certificats

- Vérification des certificats du système
- Vérification de l'espace disque
- Vérification des autorisations des fichiers de configuration de l'IdM
- Vérification de la réplication

CHAPITRE 25. INSTALLATION D'UN SERVEUR DE GESTION DES IDENTITÉS À L'AIDE D'UN PLAYBOOK ANSIBLE

Les sections suivantes décrivent comment configurer un système en tant que serveur IdM à l'aide d'Ansible. La configuration d'un système en tant que serveur IdM établit un domaine IdM et permet au système d'offrir des services IdM aux clients IdM. Le déploiement est géré par le rôle Ansible **ipaserver**.

Conditions préalables

- Vous comprenez les concepts Ansible et IdM :
  - Rôles Ansible
  - Nœuds Ansible
  - Inventaire Ansible
  - Tâches Ansible
  - Modules Ansible
  - Jeux et carnets de jeu Ansible

25.1. ANSIBLE ET SES AVANTAGES POUR L'INSTALLATION D'IDM

Ansible est un outil d'automatisation utilisé pour configurer des systèmes, déployer des logiciels et effectuer des mises à jour continues. Ansible inclut la prise en charge de la gestion des identités (IdM) et vous pouvez utiliser des modules Ansible pour automatiser les tâches d'installation telles que la configuration d'un serveur IdM, d'un réplica, d'un client ou d'une topologie IdM complète.

Avantages de l'utilisation d'Ansible pour l'installation d'IdM

La liste suivante présente les avantages de l'installation de la gestion des identités à l'aide d'Ansible par rapport à une installation manuelle.

- Il n'est pas nécessaire de se connecter au nœud géré.
- Il n'est pas nécessaire de configurer les paramètres de chaque hôte à déployer individuellement. Au lieu de cela, vous pouvez avoir un seul fichier d'inventaire pour déployer un cluster complet.
- Vous pouvez réutiliser un fichier d'inventaire ultérieurement pour des tâches de gestion, par exemple pour ajouter des utilisateurs et des hôtes. Vous pouvez réutiliser un fichier d'inventaire même pour des tâches qui ne sont pas liées à l'IdM.

Ressources supplémentaires

- Automatiser l'installation de Red Hat Identity Management
- Planification de la gestion de l'identité
- Préparation du système pour l'installation du serveur IdM

25.2. INSTALLATION DU PAQUET ANSIBLE-FREEIPA

Cette section décrit comment installer les rôles **ansible-freeipa**.

Conditions préalables

- Sur le site **managed node**:
  - Assurez-vous que le nœud géré est un système Red Hat Enterprise Linux 9 avec une adresse IP statique et un gestionnaire de paquets fonctionnel.
- Sur le site **controller**:
  - Assurez-vous que le contrôleur est un système Red Hat Enterprise Linux avec un abonnement valide. Si ce n'est pas le cas, consultez la documentation officielle Ansible Guide d'installation pour obtenir d'autres instructions d'installation.
  - Assurez-vous que vous pouvez atteindre le nœud géré via le protocole **SSH** à partir du contrôleur. Vérifiez que le nœud géré est répertorié dans le fichier **/root/.ssh/known_hosts** du contrôleur.

Procédure

Exécutez la procédure suivante sur le contrôleur Ansible.

1. Activer le référentiel requis :

```
# subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
```

2. Installer les rôles Ansible IdM :

```
# dnf install ansible-freeipa
```

Les rôles sont installés dans le répertoire **/usr/share/ansible/roles/**.

25.3. EMPLACEMENT DES RÔLES ANSIBLE DANS LE SYSTÈME DE FICHIERS

Par défaut, les rôles **ansible-freeipa** sont installés dans le répertoire **/usr/share/ansible/roles/**. La structure du paquetage **ansible-freeipa** est la suivante :

- Le répertoire **/usr/share/ansible/roles/** stocke les rôles **ipaserver**, **ipareplica** et **ipaclient** sur le contrôleur Ansible. Chaque répertoire de rôle contient des exemples, une présentation de base, la licence et la documentation sur le rôle dans un fichier Markdown **README.md**.

```
[root@server]# ls -1 /usr/share/ansible/roles/
ipaclient
ipareplica
ipaserver
```

- Le répertoire **/usr/share/doc/ansible-freeipa/** contient la documentation sur les rôles individuels et la topologie dans des fichiers Markdown **README.md**. Il contient également le sous-répertoire **playbooks/**.

```
[root@server]# ls -1 /usr/share/doc/ansible-freeipa/
playbooks
README-client.md
README.md
```

```
README-replica.md
README-server.md
README-topology.md
```

- Le répertoire **/usr/share/doc/ansible-freeipa/playbooks/** contient les playbooks d'exemple :

```
[root@server]# ls -1 /usr/share/doc/ansible-freeipa/playbooks/
install-client.yml
install-cluster.yml
install-replica.yml
install-server.yml
uninstall-client.yml
uninstall-cluster.yml
uninstall-replica.yml
uninstall-server.yml
```

25.4. PARAMÉTRAGE D'UN DÉPLOIEMENT AVEC UN DNS INTÉGRÉ ET UNE AC INTÉGRÉE EN TANT QU'AC RACINE

Suivez cette procédure pour configurer le fichier d'inventaire en vue de l'installation d'un serveur IdM avec une autorité de certification intégrée en tant qu'autorité de certification racine dans un environnement qui utilise la solution DNS intégrée IdM.

NOTE

L'inventaire de cette procédure utilise le format **INI**. Vous pouvez également utiliser les formats **YAML** ou **JSON**.

Procédure

1. Ouvrez le fichier d'inventaire pour le modifier. Spécifiez les noms de domaine pleinement qualifiés (**FQDN**) de l'hôte que vous voulez utiliser comme serveur IdM. Assurez-vous que le site **FQDN** répond aux critères suivants :
   - Seuls les caractères alphanumériques et les tirets (-) sont autorisés. Les caractères de soulignement, par exemple, ne sont pas autorisés et peuvent entraîner des défaillances du système DNS.
   - Le nom d'hôte doit être en minuscules.
2. Spécifiez les informations relatives au domaine et à la sphère IdM.
3. Spécifiez que vous voulez utiliser le DNS intégré en ajoutant l'option suivante :

```
ipaserver_setup_dns=yes
```

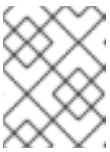
4. Spécifiez les paramètres de transfert DNS. Choisissez l'une des options suivantes :
   - Utilisez l'option **ipaserver_auto_forwarders=yes** si vous souhaitez que le programme d'installation utilise les redirections du fichier **/etc/resolv.conf**. N'utilisez pas cette option si le serveur de noms spécifié dans le fichier **/etc/resolv.conf** est l'adresse localhost 127.0.0.1 ou si vous êtes sur un réseau privé virtuel et que les serveurs DNS que vous utilisez sont normalement inaccessibles depuis l'internet public.

- Utilisez l'option **ipaserver_forwarders** pour spécifier manuellement vos transitaires. Le processus d'installation ajoute les adresses IP des transitaires au fichier **/etc/named.conf** du serveur IdM installé.
- L'option **ipaserver_no_forwarders=yes** permet de configurer les serveurs DNS racine à utiliser à la place.

NOTE

En l'absence de transitaires DNS, votre environnement est isolé et les noms des autres domaines DNS de votre infrastructure ne sont pas résolus.

5. Spécifiez les paramètres de l'enregistrement inverse et de la zone DNS. Choisissez parmi les options suivantes :
   - Utilisez l'option **ipaserver_allow_zone_overlap=yes** pour autoriser la création d'une zone (inverse) même si la zone est déjà résoluble.
   - Utilisez l'option **ipaserver_reverse_zones** pour spécifier manuellement vos zones inversées.
   - Utilisez l'option **ipaserver_no_reverse=yes** si vous ne souhaitez pas que le programme d'installation crée une zone DNS inversée.



NOTE

L'utilisation d'IdM pour gérer les zones inversées est facultative. Vous pouvez utiliser un service DNS externe à cette fin.

6. Spécifiez les mots de passe pour **admin** et pour **Directory Manager**. Utilisez Ansible Vault pour stocker le mot de passe, et faites référence au fichier Vault à partir du fichier playbook. Une autre solution, moins sûre, consiste à spécifier les mots de passe directement dans le fichier d'inventaire.
7. (Facultatif) Spécifiez une zone **firewalld** personnalisée à utiliser par le serveur IdM. Si vous ne définissez pas de zone personnalisée, IdM ajoutera ses services à la zone par défaut **firewalld**. La zone prédéfinie par défaut est **public**.

IMPORTANT

La zone **firewalld** spécifiée doit exister et être permanente.

Exemple de fichier d'inventaire contenant les informations requises sur le serveur (à l'exception des mots de passe)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=yes
ipaserver_auto_forwarders=yes
[...]
```

Exemple de fichier d'inventaire contenant les informations requises sur le serveur (y compris les mots de passe)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=yes
ipaserver_auto_forwarders=yes
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

Exemple de fichier d'inventaire avec une zone personnalisée `firewalld`

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=yes
ipaserver_auto_forwarders=yes
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
ipaserver_firewalld_zone=custom zone
```

Exemple de playbook pour configurer un serveur IdM en utilisant les mots de passe de l'administrateur et du gestionnaire d'annuaire stockés dans un fichier Ansible Vault

```
---
- name: Playbook to configure IPA server
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml

  roles:
  - role: ipaserver
    state: present
```

Exemple de playbook pour configurer un serveur IdM en utilisant les mots de passe de l'administrateur et du gestionnaire d'annuaire à partir d'un fichier d'inventaire

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

```
roles:
- role: ipaserver
  state: present
```

Ressources supplémentaires

- Pour les paramètres par défaut de la politique de transfert, voir la description de **--forward-policy** dans la page de manuel **ipa-dns-install(1)**.
- Pour plus d'informations sur les variables DNS utilisées par le rôle **ipaserver**, voir la section Variables DNS dans le fichier **README-server.md** du répertoire **/usr/share/doc/ansible-freeipa**.

25.5. PARAMÉTRAGE D'UN DÉPLOIEMENT AVEC DNS EXTERNE ET UNE AUTORITÉ DE CERTIFICATION INTÉGRÉE EN TANT QU'AUTORITÉ DE CERTIFICATION RACINE

Suivez cette procédure pour configurer le fichier d'inventaire en vue de l'installation d'un serveur IdM avec une autorité de certification intégrée en tant qu'autorité de certification racine dans un environnement qui utilise une solution DNS externe.

NOTE

Le fichier d'inventaire de cette procédure utilise le format **INI**. Vous pouvez également utiliser les formats **YAML** ou **JSON**.

Procédure

1. Ouvrez le fichier d'inventaire pour le modifier. Spécifiez les noms de domaine pleinement qualifiés (**FQDN**) de l'hôte que vous voulez utiliser comme serveur IdM. Assurez-vous que le site **FQDN** répond aux critères suivants :
   - Seuls les caractères alphanumériques et les tirets (-) sont autorisés. Les caractères de soulignement, par exemple, ne sont pas autorisés et peuvent entraîner des défaillances du système DNS.
   - Le nom d'hôte doit être en minuscules.
2. Spécifiez les informations relatives au domaine et à la sphère IdM.
3. Assurez-vous que l'option **ipaserver_setup_dns** est définie sur **no** ou qu'elle est absente.
4. Spécifiez les mots de passe pour **admin** et pour **Directory Manager**. Utilisez Ansible Vault pour stocker le mot de passe, et faites référence au fichier Vault à partir du fichier playbook. Une autre solution, moins sûre, consiste à spécifier les mots de passe directement dans le fichier d'inventaire.
5. (Facultatif) Spécifiez une zone **firewalld** personnalisée à utiliser par le serveur IdM. Si vous ne définissez pas de zone personnalisée, IdM ajoutera ses services à la zone par défaut **firewalld**. La zone prédéfinie par défaut est **public**.

IMPORTANT

La zone **firewalld** spécifiée doit exister et être permanente.

Exemple de fichier d'inventaire contenant les informations requises sur le serveur (à l'exception des mots de passe)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
[...]
```

Exemple de fichier d'inventaire contenant les informations requises sur le serveur (y compris les mots de passe)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

Exemple de fichier d'inventaire avec une zone personnalisée `firewalld`

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
ipaserver_firewalld_zone=custom zone
```

Exemple de playbook pour configurer un serveur IdM en utilisant les mots de passe de l'administrateur et du gestionnaire d'annuaire stockés dans un fichier Ansible Vault

```
---
- name: Playbook to configure IPA server
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
```

```
  roles:
  - role: ipaserver
    state: present
```

Exemple de playbook pour configurer un serveur IdM en utilisant les mots de passe de l'administrateur et du gestionnaire d'annuaire à partir d'un fichier d'inventaire

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

  roles:
  - role: ipaserver
    state: present
```

25.6. DÉPLOIEMENT D'UN SERVEUR IDM AVEC UNE AUTORITÉ DE CERTIFICATION INTÉGRÉE EN TANT QU'AUTORITÉ DE CERTIFICATION RACINE À L'AIDE D'UN PLAYBOOK ANSIBLE

Suivez cette procédure pour déployer un serveur IdM avec une autorité de certification (AC) intégrée en tant qu'AC racine à l'aide d'un playbook Ansible.

NOTE

L'inventaire de cette procédure utilise le format **INI**. Vous pouvez également utiliser les formats **YAML** ou **JSON**.

Conditions préalables

- Vous avez défini les paramètres correspondant à votre scénario en choisissant l'une des procédures suivantes :
  - Procédure avec DNS intégré
  - Procédure avec DNS externe

Procédure

1. Exécutez la commande **ansible-playbook** avec le nom du fichier playbook, par exemple **install-server.yml**. Spécifiez le fichier d'inventaire avec l'option **-i**:

```
$ ansible-playbook --vault-password-file=password_file -v -i
<path_to_inventory_directory>/hosts <path_to_playbooks_directory>/install-
server.yml
```

   Spécifiez le niveau de verbosité en utilisant l'option **-v**, **-vv**, ou **-vvv**.

   Vous pouvez visualiser la sortie du script Ansible playbook sur l'interface de ligne de commande (CLI). La sortie suivante montre que le script s'est exécuté avec succès puisque 0 tâche a échoué :

```
PLAY RECAP
server.idm.example.com : ok=18   changed=10   unreachable=0   failed=0   skipped=21
rescued=0   ignored=0
```

2. Choisissez l'une des options suivantes :

- Si votre déploiement IdM utilise un DNS externe : ajoutez les enregistrements de ressources DNS contenus dans le fichier **/tmp/ipa.system.records.UFRPto.db** aux serveurs DNS externes existants. Le processus de mise à jour des enregistrements DNS varie en fonction de la solution DNS utilisée.

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```

IMPORTANT

L'installation du serveur n'est pas terminée tant que vous n'avez pas ajouté les enregistrements DNS aux serveurs DNS existants.

- Si votre déploiement IdM utilise le DNS intégré :
  - Ajouter la délégation DNS du domaine parent au domaine DNS IdM. Par exemple, si le domaine DNS IdM est ***idm.example.com***ajoutez un enregistrement de serveur de noms (NS) au domaine parent **example.com**.

IMPORTANT

Répétez cette étape chaque fois qu'un serveur DNS IdM est installé.

  - Ajoutez un enregistrement de service **_ntp._udp** (SRV) pour votre serveur de temps à votre DNS IdM. La présence de l'enregistrement SRV pour le serveur de temps du serveur IdM nouvellement installé dans le DNS IdM garantit que les futures installations de répliques et de clients sont automatiquement configurées pour se synchroniser avec le serveur de temps utilisé par ce serveur IdM primaire.

Ressources supplémentaires

- Pour savoir comment déployer un serveur IdM avec une autorité de certification **external** en tant qu'autorité de certification racine, voir Déploiement d'un serveur IdM avec une autorité de certification externe en tant qu'autorité de certification racine à l'aide d'un playbook Ansible

25.7. PARAMÉTRAGE D'UN DÉPLOIEMENT AVEC UN DNS INTÉGRÉ ET UNE AUTORITÉ DE CERTIFICATION EXTERNE COMME AUTORITÉ DE CERTIFICATION RACINE

Suivez cette procédure pour configurer le fichier d'inventaire afin d'installer un serveur IdM avec une autorité de certification externe en tant qu'autorité de certification racine dans un environnement qui utilise la solution DNS intégrée IdM.

NOTE

Le fichier d'inventaire de cette procédure utilise le format **INI**. Vous pouvez également utiliser les formats **YAML** ou **JSON**.

Procédure

1. Ouvrez le fichier d'inventaire pour le modifier. Spécifiez les noms de domaine pleinement qualifiés (**FQDN**) de l'hôte que vous voulez utiliser comme serveur IdM. Assurez-vous que le site **FQDN** répond aux critères suivants :
   - Seuls les caractères alphanumériques et les tirets (-) sont autorisés. Les caractères de soulignement, par exemple, ne sont pas autorisés et peuvent entraîner des défaillances du système DNS.
   - Le nom d'hôte doit être en minuscules.
2. Spécifiez les informations relatives au domaine et à la sphère IdM.
3. Spécifiez que vous voulez utiliser le DNS intégré en ajoutant l'option suivante :

   ```
   ipaserver_setup_dns=yes
   ```

4. Spécifiez les paramètres de transfert DNS. Choisissez l'une des options suivantes :
   - Utilisez l'option **ipaserver_auto_forwarders=yes** si vous souhaitez que le processus d'installation utilise les redirections du fichier **/etc/resolv.conf**. Cette option n'est pas recommandée si le serveur de noms spécifié dans le fichier **/etc/resolv.conf** est l'adresse localhost 127.0.0.1 ou si vous êtes sur un réseau privé virtuel et que les serveurs DNS que vous utilisez sont normalement inaccessibles depuis l'internet public.
   - Utilisez l'option **ipaserver_forwarders** pour spécifier manuellement vos transitaires. Le processus d'installation ajoute les adresses IP des transitaires au fichier **/etc/named.conf** du serveur IdM installé.
   - L'option **ipaserver_no_forwarders=yes** permet de configurer les serveurs DNS racine à utiliser à la place.

     NOTE

     En l'absence de transitaires DNS, votre environnement est isolé et les noms des autres domaines DNS de votre infrastructure ne sont pas résolus.
5. Spécifiez les paramètres de l'enregistrement inverse et de la zone DNS. Choisissez parmi les options suivantes :
   - Utilisez l'option **ipaserver_allow_zone_overlap=yes** pour autoriser la création d'une zone (inverse) même si la zone est déjà résoluble.
   - Utilisez l'option **ipaserver_reverse_zones** pour spécifier manuellement vos zones inversées.
   - Utilisez l'option **ipaserver_no_reverse=yes** si vous ne souhaitez pas que le processus d'installation crée une zone DNS inversée.

NOTE

L'utilisation d'IdM pour gérer les zones inversées est facultative. Vous pouvez utiliser un service DNS externe à cette fin.

6. Spécifiez les mots de passe pour **admin** et pour **Directory Manager**. Utilisez Ansible Vault pour stocker le mot de passe, et faites référence au fichier Vault à partir du fichier playbook. Une autre solution, moins sûre, consiste à spécifier les mots de passe directement dans le fichier d'inventaire.

7. (Facultatif) Spécifiez une zone **firewalld** personnalisée à utiliser par le serveur IdM. Si vous ne définissez pas de zone personnalisée, IdM ajoute ses services à la zone par défaut **firewalld**. La zone prédéfinie par défaut est **public**.

IMPORTANT

La zone **firewalld** spécifiée doit exister et être permanente.

Exemple de fichier d'inventaire contenant les informations requises sur le serveur (à l'exception des mots de passe)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=yes
ipaserver_auto_forwarders=yes
[...]
```

Exemple de fichier d'inventaire contenant les informations requises sur le serveur (y compris les mots de passe)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=yes
ipaserver_auto_forwarders=yes
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

Exemple de fichier d'inventaire avec une zone personnalisée firewalld

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
```

```
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=yes
ipaserver_auto_forwarders=yes
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
ipaserver_firewalld_zone=custom zone

[...]
```

8. Créez un playbook pour la première étape de l'installation. Saisissez les instructions pour générer la demande de signature de certificat (CSR) et la copier du contrôleur vers le nœud géré.

```
---
- name: Playbook to configure IPA server Step 1
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
  vars:
    ipaserver_external_ca: yes

  roles:
  - role: ipaserver
    state: present

  post_tasks:
  - name: Copy CSR /root/ipa.csr from node to "{{ groups.ipaserver[0] + '-ipa.csr' }}"
    fetch:
      src: /root/ipa.csr
      dest: "{{ groups.ipaserver[0] + '-ipa.csr' }}"
      flat: yes
```

9. Créez un autre playbook pour la dernière étape de l'installation.

```
---
- name: Playbook to configure IPA server Step -1
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
  vars:
    ipaserver_external_cert_files: "/root/chain.crt"

  pre_tasks:
  - name: Copy "{{ groups.ipaserver[0] + '-chain.crt' }}" to /root/chain.crt on node
    copy:
      src: "{{ groups.ipaserver[0] + '-chain.crt' }}"
      dest: "/root/chain.crt"
      force: yes

  roles:
  - role: ipaserver
    state: present
```

Ressources supplémentaires

- Pour les paramètres par défaut de la politique de transfert, voir la description de **--forward-policy** dans la page de manuel **ipa-dns-install(1)**.
- Pour plus d'informations sur les variables DNS utilisées par le rôle **ipaserver**, voir la section Variables DNS dans le fichier **README-server.md** du répertoire **/usr/share/doc/ansible-freeipa**.

25.8. PARAMÉTRAGE D'UN DÉPLOIEMENT AVEC DNS EXTERNE ET UNE AUTORITÉ DE CERTIFICATION EXTERNE EN TANT QU'AUTORITÉ DE CERTIFICATION RACINE

Suivez cette procédure pour configurer le fichier d'inventaire en vue de l'installation d'un serveur IdM avec une autorité de certification externe en tant qu'autorité de certification racine dans un environnement qui utilise une solution DNS externe.

NOTE

Le fichier d'inventaire de cette procédure utilise le format **INI**. Vous pouvez également utiliser les formats **YAML** ou **JSON**.

Procédure

1. Ouvrez le fichier d'inventaire pour le modifier. Spécifiez les noms de domaine pleinement qualifiés (**FQDN**) de l'hôte que vous voulez utiliser comme serveur IdM. Assurez-vous que le site **FQDN** répond aux critères suivants :
   - Seuls les caractères alphanumériques et les tirets (-) sont autorisés. Les caractères de soulignement, par exemple, ne sont pas autorisés et peuvent entraîner des défaillances du système DNS.
   - Le nom d'hôte doit être en minuscules.
2. Spécifiez les informations relatives au domaine et à la sphère IdM.
3. Assurez-vous que l'option **ipaserver_setup_dns** est définie sur **no** ou qu'elle est absente.
4. Spécifiez les mots de passe pour **admin** et pour **Directory Manager**. Utilisez Ansible Vault pour stocker le mot de passe, et faites référence au fichier Vault à partir du fichier playbook. Une autre solution, moins sûre, consiste à spécifier les mots de passe directement dans le fichier d'inventaire.
5. (Facultatif) Spécifiez une zone **firewalld** personnalisée à utiliser par le serveur IdM. Si vous ne définissez pas de zone personnalisée, IdM ajoutera ses services à la zone par défaut **firewalld**. La zone prédéfinie par défaut est **public**.

IMPORTANT

La zone **firewalld** spécifiée doit exister et être permanente.

Exemple de fichier d'inventaire contenant les informations requises sur le serveur (à l'exception des mots de passe)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
[...]
```

Exemple de fichier d'inventaire contenant les informations requises sur le serveur (y compris les mots de passe)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

Exemple de fichier d'inventaire avec une zone personnalisée `firewalld`

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
ipaserver_firewalld_zone=custom zone

[...]
```

6. Créez un playbook pour la première étape de l'installation. Saisissez les instructions pour générer la demande de signature de certificat (CSR) et la copier du contrôleur vers le nœud géré.

```
---
- name: Playbook to configure IPA server Step 1
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
  vars:
    ipaserver_external_ca: yes

  roles:
  - role: ipaserver
```

```
    state: present

  post_tasks:
  - name: Copy CSR /root/ipa.csr from node to "{{ groups.ipaserver[0] + '-ipa.csr' }}"
    fetch:
      src: /root/ipa.csr
      dest: "{{ groups.ipaserver[0] + '-ipa.csr' }}"
      flat: yes
```

7. Créez un autre playbook pour la dernière étape de l'installation.

```
---
- name: Playbook to configure IPA server Step -1
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
  vars:
    ipaserver_external_cert_files: "/root/chain.crt"

  pre_tasks:
  - name: Copy "{{ groups.ipaserver[0] + '-chain.crt' }}" to /root/chain.crt on node
    copy:
      src: "{{ groups.ipaserver[0] + '-chain.crt' }}"
      dest: "/root/chain.crt"
      force: yes

  roles:
  - role: ipaserver
    state: present
```

Ressources supplémentaires

- Pour plus de détails sur les options disponibles lors de l'installation d'un serveur IdM avec DNS externe et une autorité de certification signée en externe, voir Installation d'un serveur IdM : Sans DNS intégré, avec une autorité de certification externe comme autorité de certification racine.

25.9. DÉPLOIEMENT D'UN SERVEUR IDM AVEC UNE AUTORITÉ DE CERTIFICATION EXTERNE EN TANT QU'AUTORITÉ DE CERTIFICATION RACINE À L'AIDE D'UN PLAYBOOK ANSIBLE

Suivez cette procédure pour déployer un serveur IdM avec une autorité de certification (AC) externe en tant qu'AC racine à l'aide d'un livre de jeu Ansible.

NOTE

Le fichier d'inventaire de cette procédure utilise le format **INI**. Vous pouvez également utiliser les formats **YAML** ou **JSON**.

Conditions préalables

- Vous avez défini les paramètres correspondant à votre scénario en choisissant l'une des procédures suivantes :
  - Procédure avec DNS intégré
  - Procédure avec DNS externe

Procédure

1. Exécutez la commande **ansible-playbook** avec le nom du fichier playbook qui contient les instructions pour la première étape de l'installation, par exemple **install-server-step1.yml**. Spécifiez le fichier d'inventaire avec l'option **-i**:

```
$ ansible-playbook --vault-password-file=password_file -v -i
<path_to_inventory_directory>/host.server <path_to_playbooks_directory>/install-
server-step1.yml
```

   Spécifiez le niveau de verbosité en utilisant l'option **-v**, **-vv** ou **-vvv**.

   Vous pouvez visualiser la sortie du script Ansible playbook sur l'interface de ligne de commande (CLI). La sortie suivante montre que le script s'est exécuté avec succès puisque 0 tâche a échoué :

```
PLAY RECAP
server.idm.example.com : ok=18   changed=10   unreachable=0   failed=0   skipped=21
rescued=0   ignored=0
```

2. Localisez le fichier de demande de signature de certificat **ipa.csr** sur le contrôleur et soumettez-le à l'autorité de certification externe.

3. Placez le certificat de l'autorité de certification IdM signé par l'autorité de certification externe dans le système de fichiers du contrôleur de manière à ce que le manuel de jeu de l'étape suivante puisse le trouver.

4. Exécutez la commande **ansible-playbook** avec le nom du fichier playbook qui contient les instructions pour la dernière étape de l'installation, par exemple **install-server-step2.yml**. Spécifiez le fichier d'inventaire avec l'option **-i**:

```
$ ansible-playbook -v -i <path_to_inventory_directory>/host.server
<path_to_playbooks_directory>/install-server-step2.yml
```

5. Choisissez l'une des options suivantes :

   - Si votre déploiement IdM utilise un DNS externe : ajoutez les enregistrements de ressources DNS contenus dans le fichier **/tmp/ipa.system.records.UFRPto.db** aux serveurs DNS externes existants. Le processus de mise à jour des enregistrements DNS varie en fonction de la solution DNS utilisée.

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```

IMPORTANT

L'installation du serveur n'est pas terminée tant que vous n'avez pas ajouté les enregistrements DNS aux serveurs DNS existants.

- Si votre déploiement IdM utilise le DNS intégré :
  - Ajouter la délégation DNS du domaine parent au domaine DNS IdM. Par exemple, si le domaine DNS IdM est ***idm.example.com***ajoutez un enregistrement de serveur de noms (NS) au domaine parent **example.com**.

    IMPORTANT

    Répétez cette étape chaque fois qu'un serveur DNS IdM est installé.

  - Ajoutez un enregistrement de service **_ntp._udp** (SRV) pour votre serveur de temps à votre DNS IdM. La présence de l'enregistrement SRV pour le serveur de temps du serveur IdM nouvellement installé dans le DNS IdM garantit que les futures installations de répliques et de clients sont automatiquement configurées pour se synchroniser avec le serveur de temps utilisé par ce serveur IdM primaire.

Ressources supplémentaires

Pour savoir comment déployer un serveur IdM avec une autorité de certification **integrated** en tant qu'autorité de certification racine, voir Déploiement d'un serveur IdM avec une autorité de certification intégrée en tant qu'autorité de certification racine à l'aide d'un livre de jeu Ansible

Ressources supplémentaires

- Notions d'inventaire : formats, hôtes et groupes
- Vous pouvez consulter des exemples de playbooks Ansible pour l'installation d'un serveur IdM et une liste de variables possibles dans la documentation en amont de **ansible-freeipa** .

CHAPITRE 26. INSTALLATION D'UNE RÉPLIQUE DE GESTION DES IDENTITÉS À L'AIDE D'UN PLAYBOOK ANSIBLE

La configuration d'un système en tant que réplique IdM à l'aide d'Ansible l'inscrit dans un domaine IdM et permet au système d'utiliser les services IdM sur les serveurs IdM du domaine.

Le déploiement est géré par le rôle Ansible **ipareplica**. Le rôle peut utiliser le mode de découverte automatique pour identifier les serveurs IdM, le domaine et d'autres paramètres. Cependant, si vous déployez plusieurs réplicas dans un modèle de type tiers, avec différents groupes de réplicas déployés à différents moments, vous devez définir des serveurs ou des réplicas spécifiques pour chaque groupe.

Conditions préalables

- Vous avez installé le paquet ansible-freeipa sur le nœud de contrôle Ansible.
- Vous comprenez les concepts Ansible et IdM :
  - Rôles Ansible
  - Nœuds Ansible
  - Inventaire Ansible
  - Tâches Ansible
  - Modules Ansible
  - Jeux et carnets de jeu Ansible

Ressources supplémentaires

- Planification de la topologie du réplica

26.1. SPÉCIFICATION DES VARIABLES DE BASE, DE SERVEUR ET DE CLIENT POUR L'INSTALLATION DE LA RÉPLIQUE IDM

Suivez cette procédure pour configurer le fichier d'inventaire en vue de l'installation d'une réplique 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**.

Procédure

1. Ouvrez le fichier d'inventaire pour le modifier. Spécifiez les noms de domaine pleinement qualifiés (FQDN) des hôtes qui deviendront des répliques IdM. Les FQDN doivent être des noms DNS valides :

   - Seuls les chiffres, les caractères alphabétiques et les traits d'union (**-**) sont autorisés. Par exemple, les caractères de soulignement ne sont pas autorisés et peuvent entraîner des défaillances du système DNS.

   - Le nom d'hôte doit être en minuscules.

   Exemple d'un fichier hosts d'inventaire simple avec seulement le FQDN des répliques défini

   ```
   [ipareplicas]
   replica1.idm.example.com
   replica2.idm.example.com
   replica3.idm.example.com
   [...]
   ```

   Si le serveur IdM est déjà déployé et que les enregistrements SRV sont correctement définis dans la zone DNS IdM, le script découvre automatiquement toutes les autres valeurs requises.

2. [Facultatif] Fournissez des informations supplémentaires dans le fichier d'inventaire en fonction de la façon dont vous avez conçu votre topologie :

   Scénario 1

   Si vous souhaitez éviter l'autodécouverte et que toutes les répliques répertoriées dans la section **[ipareplicas]** utilisent un serveur IdM spécifique, définissez le serveur dans la section **[ipaservers]** du fichier d'inventaire.

   Exemple de fichier hosts d'inventaire avec le FQDN du serveur IdM et les répliques définies

   ```
   [ipaservers]
   server.idm.example.com

   [ipareplicas]
   replica1.idm.example.com
   replica2.idm.example.com
   replica3.idm.example.com
   [...]
   ```

   Scénario 2

   Par ailleurs, si vous souhaitez éviter la découverte automatique mais déployer des répliques spécifiques avec des serveurs spécifiques, définissez les serveurs pour des répliques spécifiques individuellement dans la section **[ipareplicas]** du fichier d'inventaire.

   Exemple de fichier d'inventaire avec un serveur IdM spécifique défini pour une réplique spécifique

   ```
   [ipaservers]
   server.idm.example.com
   replica1.idm.example.com
   ```

```
[ipareplicas]
replica2.idm.example.com
replica3.idm.example.com ipareplica_servers=replica1.idm.example.com
```

Dans l'exemple ci-dessus, **replica3.idm.example.com** utilise le site **replica1.idm.example.com** déjà déployé comme source de réplication.

Scénario 3

Si vous déployez plusieurs répliques en un seul lot et que le temps vous est compté, le déploiement de répliques à plusieurs niveaux peut vous être utile. Définissez des groupes spécifiques de répliques dans le fichier d'inventaire, par exemple **[ipareplicas_tier1]** et **[ipareplicas_tier2]**, et concevez des séquences distinctes pour chaque groupe dans le livre de séquences **install-replica.yml**.

Exemple de fichier d'inventaire avec des niveaux de répliques définis

```
[ipaservers]
server.idm.example.com

[ipareplicas_tier1]
replica1.idm.example.com

[ipareplicas_tier2]
replica2.idm.example.com \
ipareplica_servers=replica1.idm.example.com,server.idm.example.com
```

La première entrée de **ipareplica_servers** sera utilisée. La deuxième entrée sera utilisée comme option de repli. Lorsque vous utilisez plusieurs niveaux pour déployer les répliques IdM, vous devez avoir des tâches séparées dans le playbook pour déployer d'abord les répliques du niveau 1 et ensuite les répliques du niveau 2 :

Exemple d'un fichier playbook avec des jeux différents pour des groupes de répliques différents

```
---
- name: Playbook to configure IPA replicas (tier1)
  hosts: ipareplicas_tier1
  become: true

  roles:
  - role: ipareplica
    state: present

- name: Playbook to configure IPA replicas (tier2)
  hosts: ipareplicas_tier2
  become: true

  roles:
  - role: ipareplica
    state: present
```

3. [Facultatif] Fournir des informations supplémentaires concernant **firewalld** et DNS :

Scénario 1

Si vous souhaitez que le réplica utilise une zone **firewalld** spécifique au lieu de la zone par défaut, vous pouvez la spécifier dans le fichier d'inventaire. Cela peut être utile, par exemple, lorsque vous souhaitez utiliser une zone **firewalld** interne pour votre installation IdM au lieu d'une zone publique définie par défaut.
Si vous ne définissez pas de zone personnalisée, IdM ajoutera ses services à la zone par défaut **firewalld**. La zone prédéfinie par défaut est **public**.

IMPORTANT

La zone **firewalld** spécifiée doit exister et être permanente.

Exemple d'un fichier hosts d'inventaire simple avec une zone firewalld personnalisée

```
[ipaservers]
server.idm.example.com

[ipareplicas]
replica1.idm.example.com
replica2.idm.example.com
replica3.idm.example.com
[...]

[ipareplicas:vars]
ipareplica_firewalld_zone=custom zone
```

Scénario 2

Si vous souhaitez que le réplica héberge le service DNS IdM, ajoutez la ligne **ipareplica_setup_dns=yes** à la section **[ipareplicas:vars]**. En outre, indiquez si vous souhaitez utiliser des redirections DNS par serveur :

- Pour configurer les transferts par serveur, ajoutez la variable **ipareplica_forwarders** et une liste de chaînes à la section **[ipareplicas:vars]**, par exemple : **ipareplica_forwarders=192.0.2.1,192.0.2.2**
- Pour ne pas configurer de forwarders par serveur, ajoutez la ligne suivante à la section **[ipareplicas:vars]**: **ipareplica_no_forwarders=yes**.
- Pour configurer les transitaires par serveur en fonction des transitaires répertoriés dans le fichier **/etc/resolv.conf** du réplica, ajoutez la variable **ipareplica_auto_forwarders** à la section **[ipareplicas:vars]**.

Exemple de fichier d'inventaire avec des instructions pour configurer le DNS et les forwarders par serveur sur les répliques

```
[ipaservers]
server.idm.example.com

[ipareplicas]
replica1.idm.example.com
replica2.idm.example.com
replica3.idm.example.com
```

```
[...]

[ipareplicas:vars]
ipareplica_setup_dns=yes
ipareplica_forwarders=192.0.2.1,192.0.2.2
```

Scénario 3

Spécifiez le résolveur DNS à l'aide des options **ipaclient_configure_dns_resolve** et **ipaclient_dns_servers** (le cas échéant) pour simplifier les déploiements de clusters. Ceci est particulièrement utile si votre déploiement IdM utilise un DNS intégré :

Un extrait de fichier d'inventaire spécifiant un résolveur DNS :

```
[...]
[ipaclient:vars]
ipaclient_configure_dns_resolver=true
ipaclient_dns_servers=192.168.100.1
```

NOTE

La liste **ipaclient_dns_servers** ne doit contenir que des adresses IP. Les noms d'hôtes ne sont pas autorisés.

Ressources supplémentaires

- Pour plus d'informations sur les variables **ipareplica**, voir le fichier Markdown **/usr/share/ansible/roles/ipareplica/README.md**.

26.2. SPÉCIFICATION DES INFORMATIONS D'IDENTIFICATION POUR L'INSTALLATION DE LA RÉPLIQUE IDM À L'AIDE D'UN PLAYBOOK ANSIBLE

Suivez cette procédure pour configurer l'autorisation d'installation du réplica 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**.

Procédure

1. Spécifiez le **password of a user authorized to deploy replicas**, par exemple l'IdM **admin**.

   - Red Hat recommande d'utiliser Ansible Vault pour stocker le mot de passe et de référencer le fichier Vault à partir du fichier playbook, par exemple **install-replica.yml**:

     Exemple de fichier playbook utilisant le principal d'un fichier d'inventaire et le mot de passe d'un fichier Ansible Vault

     ```
     - name: Playbook to configure IPA replicas
       hosts: ipareplicas
       become: true
       vars_files:
       - playbook_sensitive_data.yml

       roles:
       - role: ipareplica
         state: present
     ```

     Pour plus de détails sur l'utilisation d'Ansible Vault, voir la documentation officielle d'Ansible Vault.

   - De manière moins sûre, fournissez les informations d'identification de **admin** directement dans le fichier d'inventaire. Utilisez l'option **ipaadmin_password** dans la section **[ipareplicas:vars]** du fichier d'inventaire. Le fichier d'inventaire et le fichier playbook **install-replica.yml** peuvent alors se présenter comme suit :

     Exemple de fichier hosts.replica de l'inventaire

     ```
     [...]
     [ipareplicas:vars]
     ipaadmin_password=Secret123
     ```

     Exemple de playbook utilisant le principal et le mot de passe du fichier d'inventaire

     ```
     - name: Playbook to configure IPA replicas
       hosts: ipareplicas
       become: true

       roles:
       - role: ipareplica
         state: present
     ```

   - Une autre solution, moins sûre, consiste à fournir les informations d'identification d'un autre utilisateur autorisé à déployer une réplique directement dans le fichier d'inventaire. Pour spécifier un autre utilisateur autorisé, utilisez l'option **ipaadmin_principal** pour le nom d'utilisateur et l'option **ipaadmin_password** pour le mot de passe. Le fichier d'inventaire et le fichier playbook **install-replica.yml** peuvent alors se présenter comme suit :

     Exemple de fichier hosts.replica de l'inventaire

     ```
     [...]
     [ipareplicas:vars]
     ipaadmin_principal=my_admin
     ```

```
ipaadmin_password=my_admin_secret123
```

Exemple de playbook utilisant le principal et le mot de passe du fichier d'inventaire

```
- name: Playbook to configure IPA replicas
  hosts: ipareplicas
  become: true

  roles:
  - role: ipareplica
    state: present
```

Ressources supplémentaires

- Pour plus de détails sur les options acceptées par le rôle Ansible **ipareplica**, voir le fichier Markdown **/usr/share/ansible/roles/ipareplica/README.md**.

26.3. DÉPLOIEMENT D'UNE RÉPLIQUE IDM À L'AIDE D'UN PLAYBOOK ANSIBLE

Complétez cette procédure pour utiliser un playbook Ansible afin de déployer une réplique IdM.

Conditions préalables

- Vous avez configuré le fichier d'inventaire pour l'installation d'une réplique IdM .
- Vous avez configuré l'autorisation pour l'installation du réplica IdM .

Procédure

- Pour installer une réplique IdM à l'aide d'un playbook Ansible, utilisez la commande **ansible-playbook** avec le nom du fichier du playbook, par exemple **install-replica.yml**. Spécifiez le fichier d'inventaire avec l'option **-i**:

  ```
  $ ansible-playbook --vault-password-file=password_file -v -i
  <path_to_inventory_directory>/hosts.replica <path_to_playbooks_directory>/install-
  replica.yml
  ```

  Spécifiez le niveau de verbosité en utilisant l'option **-v**, **-vv** ou **-vvv**.

  Ansible vous informe de l'exécution du script du playbook Ansible. La sortie suivante montre que le script s'est exécuté avec succès puisque 0 tâche a échoué :

  ```
  PLAY RECAP
  replica.idm.example.com : ok=18   changed=10   unreachable=0   failed=0   skipped=21
  rescued=0   ignored=0
  ```

Vous avez maintenant installé une réplique IdM.

CHAPITRE 27. INSTALLATION D'UN CLIENT DE GESTION DES IDENTITÉS À L'AIDE D'UN PLAYBOOK ANSIBLE

Les sections suivantes décrivent comment configurer un système en tant que client de gestion d'identité (IdM) à l'aide d'Ansible. La configuration d'un système en tant que client IdM l'inscrit dans un domaine IdM et permet au système d'utiliser les services IdM sur les serveurs IdM du domaine.

Le déploiement est géré par le rôle Ansible **ipaclient**. Par défaut, le rôle utilise le mode de découverte automatique pour identifier les serveurs IdM, le domaine et d'autres paramètres. Le rôle peut être modifié pour que le playbook Ansible utilise les paramètres spécifiés, par exemple dans le fichier d'inventaire.

Conditions préalables

- Vous avez installé le paquet ansible-freeipa sur le nœud de contrôle Ansible.
- Vous comprenez les concepts Ansible et IdM :
  - Rôles Ansible
  - Nœuds Ansible
  - Inventaire Ansible
  - Tâches Ansible
  - Modules Ansible
  - Jeux et carnets de jeu Ansible

27.1. DÉFINITION DES PARAMÈTRES DU FICHIER D'INVENTAIRE POUR LE MODE D'INSTALLATION DU CLIENT D'AUTODÉCOUVERTE

Pour installer un client de gestion des identités à l'aide d'un playbook Ansible, configurez les paramètres de l'hôte cible dans un fichier d'inventaire, par exemple **inventory/hosts**:

- les informations sur l'hôte
- l'autorisation de la tâche

Le fichier d'inventaire peut être dans l'un des nombreux formats, en fonction des plugins d'inventaire que vous avez. Le format **INI-like** est l'un des formats par défaut d'Ansible et est utilisé dans les exemples ci-dessous.

NOTE

Pour utiliser les cartes à puce avec l'interface utilisateur graphique dans RHEL, assurez-vous d'inclure la variable **ipaclient_mkhomedir** dans votre playbook Ansible.

Conditions préalables

- Vous avez vérifié les instructions de déploiement sur le nœud de contrôle, voir Vérification des paramètres dans le fichier install-client.yml.

Procédure

Procédure

1. Indiquez le nom d'hôte entièrement qualifié (FQDN) de l'hôte qui doit devenir un client IdM. Le nom de domaine entièrement qualifié doit être un nom DNS valide :

   - Seuls les chiffres, les caractères alphabétiques et les traits d'union (**-**) sont autorisés. Par exemple, les caractères de soulignement ne sont pas autorisés et peuvent entraîner des défaillances du système DNS.
   - Le nom d'hôte doit être en minuscules. Aucune majuscule n'est autorisée.

   Si les enregistrements SRV sont correctement définis dans la zone DNS IdM, le script découvre automatiquement toutes les autres valeurs requises.

   Exemple d'un fichier d'inventaire simple avec seulement le FQDN du client défini

   ```
   [ipaclients]
   client.idm.example.com
   [...]
   ```

2. Spécifiez les informations d'identification pour l'inscription du client. Les méthodes d'authentification suivantes sont disponibles :

   - Le site **password of a user authorized to enroll clients**est l'option par défaut.
     - Red Hat recommande d'utiliser Ansible Vault pour stocker le mot de passe et de faire référence au fichier Vault à partir du fichier playbook, par exemple **install-client.yml**, directement :

       Exemple de fichier playbook utilisant le principal d'un fichier d'inventaire et le mot de passe d'un fichier Ansible Vault

       ```
       - name: Playbook to configure IPA clients with username/password
         hosts: ipaclients
         become: true
         vars_files:
         - playbook_sensitive_data.yml

         roles:
         - role: ipaclient
           state: present
       ```

     - De manière moins sûre, fournissez les informations d'identification de **admin** en utilisant l'option **ipaadmin_password** dans la section **[ipaclients:vars]** du fichier **inventory/hosts**. Pour spécifier un autre utilisateur autorisé, utilisez l'option **ipaadmin_principal** pour le nom d'utilisateur et l'option **ipaadmin_password** pour le mot de passe. Le fichier d'inventaire **inventory/hosts** et le fichier playbook **install-client.yml** peuvent alors se présenter comme suit :

       Exemple de fichier d'inventaire des hôtes

       ```
       [...]
       [ipaclients:vars]
       ipaadmin_principal=my_admin
       ipaadmin_password=Secret123
       ```

Exemple de Playbook utilisant le principal et le mot de passe du fichier d'inventaire

```
- name: Playbook to unconfigure IPA clients
  hosts: ipaclients
  become: true

  roles:
  - role: ipaclient
    state: true
```

- Le site **client keytab** de l'inscription précédente, s'il est encore disponible.
  Cette option est disponible si le système a été précédemment enregistré en tant que client de gestion d'identité. Pour utiliser cette méthode d'authentification, décommentez l'option **#ipaclient_keytab**, en spécifiant le chemin d'accès au fichier stockant le keytab, par exemple dans la section **[ipaclient:vars]** de **inventory/hosts**.

- Un **random, one-time password** (OTP) à générer lors de l'inscription. Pour utiliser cette méthode d'authentification, utilisez l'option **ipaclient_use_otp=yes** dans votre fichier d'inventaire. Par exemple, vous pouvez décommenter l'option **ipaclient_use_otp=yes** dans la section **[ipaclients:vars]** du fichier **inventory/hosts**. Notez qu'avec l'option OTP, vous devez également spécifier l'une des options suivantes :

  - L'adresse **password of a user authorized to enroll clients**, par exemple en fournissant une valeur pour **ipaadmin_password** dans la section **[ipaclients:vars]** du fichier **inventory/hosts**.

  - Le site **admin keytab**, par exemple en fournissant une valeur pour **ipaadmin_keytab** dans la section **[ipaclients:vars]** de **inventory/hosts**.

3. [Facultatif] Spécifiez le résolveur DNS à l'aide des options **ipaclient_configure_dns_resolve** et **ipaclient_dns_servers** (le cas échéant) pour simplifier les déploiements de clusters. Ceci est particulièrement utile si votre déploiement IdM utilise le DNS intégré :

   Un extrait de fichier d'inventaire spécifiant un résolveur DNS :

```
[...]
[ipaclients:vars]
ipaadmin_password: "{{ ipaadmin_password }}"
ipaclient_domain=idm.example.com
ipaclient_configure_dns_resolver=true
ipaclient_dns_servers=192.168.100.1
```

NOTE

La liste **ipaclient_dns_servers** ne doit contenir que des adresses IP. Les noms d'hôtes ne sont pas autorisés.

Ressources supplémentaires

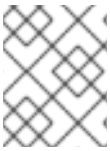
- **/usr/share/ansible/roles/ipaclient/README.md**

27.2. DÉFINITION DES PARAMÈTRES DU FICHIER D'INVENTAIRE LORSQUE L'AUTODÉCOUVERTE N'EST PAS POSSIBLE LORS DE L'INSTALLATION DU CLIENT

Pour installer un client de gestion des identités à l'aide d'un playbook Ansible, configurez les paramètres de l'hôte cible dans un fichier d'inventaire, par exemple **inventory/hosts**:

- les informations sur l'hôte, le serveur IdM et le domaine IdM ou le realm IdM
- l'autorisation de la tâche

Le fichier d'inventaire peut être dans l'un des nombreux formats, en fonction des plugins d'inventaire que vous avez. Le format **INI-like** est l'un des formats par défaut d'Ansible et est utilisé dans les exemples ci-dessous.



NOTE

Pour utiliser les cartes à puce avec l'interface utilisateur graphique dans RHEL, assurez-vous d'inclure la variable **ipaclient_mkhomedir** dans votre playbook Ansible.

Conditions préalables

- Vous avez vérifié les instructions de déploiement sur le nœud de contrôle, voir Vérification des paramètres dans le fichier install-client.yml.

Procédure

1. Indiquez le nom d'hôte entièrement qualifié (FQDN) de l'hôte qui doit devenir un client IdM. Le nom de domaine entièrement qualifié doit être un nom DNS valide :
   - Seuls les chiffres, les caractères alphabétiques et les traits d'union (**-**) sont autorisés. Par exemple, les caractères de soulignement ne sont pas autorisés et peuvent entraîner des défaillances du système DNS.
   - Le nom d'hôte doit être en minuscules. Aucune majuscule n'est autorisée.
2. Spécifiez d'autres options dans les sections correspondantes du fichier **inventory/hosts**:
   - le FQDN des serveurs dans la section **[ipaservers]** pour indiquer le serveur IdM auprès duquel le client sera enrôlé
   - l'une des deux options suivantes :
     - l'option **ipaclient_domain** dans la section **[ipaclients:vars]** pour indiquer le nom de domaine DNS du serveur IdM auprès duquel le client sera enrôlé
     - l'option **ipaclient_realm** dans la section **[ipaclients:vars]** pour indiquer le nom du domaine Kerberos contrôlé par le serveur IdM

     Exemple de fichier d'inventaire des hôtes avec le FQDN du client, le FQDN du serveur et le domaine défini

     ```
     [ipaclients]
     client.idm.example.com
     ```

```
[ipaservers]
server.idm.example.com

[ipaclients:vars]
ipaclient_domain=idm.example.com
[...]
```

3. Spécifiez les informations d'identification pour l'inscription du client. Les méthodes d'authentification suivantes sont disponibles :

   - Le site **password of a user authorized to enroll clients**est l'option par défaut.

     - Red Hat recommande d'utiliser Ansible Vault pour stocker le mot de passe et de référencer le fichier Vault à partir du fichier de script, par exemple **install-client.yml**, directement : .exemple de fichier de script utilisant le principal du fichier d'inventaire et le mot de passe d'un fichier Ansible Vault

```
- name: Playbook to configure IPA clients with username/password
  hosts: ipaclients
  become: true
  vars_files:
  - *playbook_sensitive_data.yml*

  roles:
  - role: ipaclient
    state: present
```

   - De manière moins sûre, fournissez les informations d'identification de **admin** en utilisant l'option **ipaadmin_password** dans la section **[ipaclients:vars]** du fichier **inventory/hosts**. Pour spécifier un autre utilisateur autorisé, utilisez l'option **ipaadmin_principal** pour le nom d'utilisateur et l'option **ipaadmin_password** pour le mot de passe. Le fichier du playbook **install-client.yml** peut alors se présenter comme suit :

     Exemple de fichier d'inventaire des hôtes

```
[...]
[ipaclients:vars]
ipaadmin_principal=my_admin
ipaadmin_password=Secret123
```

     Exemple de Playbook utilisant le principal et le mot de passe du fichier d'inventaire

```
- name: Playbook to unconfigure IPA clients
  hosts: ipaclients
  become: true

  roles:
  - role: ipaclient
    state: true
```

   - Le site **client keytab** de l'inscription précédente, s'il est encore disponible :
     Cette option est disponible si le système a été précédemment enregistré en tant que client de gestion d'identité. Pour utiliser cette méthode d'authentification, décommentez l'option **ipaclient_keytab**, en spécifiant le chemin d'accès au fichier stockant le keytab, par exemple dans la section **[ipaclient:vars]** de **inventory/hosts**.

- Un **random, one-time password** (OTP) à générer lors de l'inscription. Pour utiliser cette méthode d'authentification, utilisez l'option **ipaclient_use_otp=yes** dans votre fichier d'inventaire. Par exemple, vous pouvez décommenter l'option **#ipaclient_use_otp=yes** dans la section **[ipaclients:vars]** du fichier **inventory/hosts**. Notez qu'avec l'option OTP, vous devez également spécifier l'une des options suivantes :
  - L'adresse **password of a user authorized to enroll clients** par exemple en fournissant une valeur pour **ipaadmin_password** dans la section **[ipaclients:vars]** du fichier **inventory/hosts**.
  - Le site **admin keytab**, par exemple en fournissant une valeur pour **ipaadmin_keytab** dans la section **[ipaclients:vars]** de **inventory/hosts**.

Ressources supplémentaires

- Pour plus de détails sur les options acceptées par le rôle Ansible **ipaclient**, voir le fichier README de **/usr/share/ansible/roles/ipaclient/README.md**.

27.3. VÉRIFICATION DES PARAMÈTRES DANS LE FICHIER INSTALL-CLIENT.YML

Le fichier **install-client.yml** playbook contient des instructions pour le déploiement du client IdM.

Procédure

- Ouvrez le fichier et vérifiez si les instructions du playbook correspondent à ce que vous prévoyez pour votre déploiement. Le contenu ressemble généralement à ceci :

```
---
- name: Playbook to configure IPA clients with username/password
  hosts: ipaclients
  become: true

  roles:
  - role: ipaclient
    state: present
```

C'est ce que signifient les différentes entrées :

- L'entrée hosts spécifie la section du fichier **inventory/hosts** dans laquelle le script ansible recherche les **FQDNs** des hôtes sur lesquels le script **ipa-client-install** doit être exécuté.
- L'entrée **become: true** spécifie que les informations d'identification de root seront invoquées lors de l'exécution du script **ipa-client-install**.
- L'entrée **role: ipaclient** spécifie le rôle qui sera installé sur l'hôte : dans ce cas, il s'agit du rôle de client IPA.
- L'entrée **state: present** précise que le client doit être installé plutôt que désinstallé (**absent**).

27.4. OPTIONS D'AUTORISATION POUR L'INSCRIPTION D'UN CLIENT IDM À L'AIDE D'UN PLAYBOOK ANSIBLE

Cette section présente les options d'autorisation individuelle pour l'inscription du client IdM avec des exemples d'inventaire et de fichiers de jeu.

Tableau 27.1. Options d'autorisation pour l'enrôlement du client IdM à l'aide d'Ansible

Option d'autorisation	Note	Exemple de fichier d'inventaire	Exemple de fichier playbook **install-client.yml**

Mot de passe d'un utilisateur autorisé à inscrire un client : Option 1	Mot de passe stocké dans le coffre-fort d'Ansible	`[ipaclients:vars]`
		`[...]`
			`- name: Playbook to configure IPA clients with username/password`
			`  hosts: ipaclients`
			`  become: true`
			`  vars_files:`
			`  - playbook_sensitive_data.yml`
			
			`  roles:`
			`  - role: ipaclient`
			`  state: present`

Mot de passe d'un utilisateur autorisé à inscrire un client : Option 2	Mot de passe stocké dans le fichier d'inventaire	`[ipaclients:vars]`
		`ipaadmin_password=Secret123`
			`- name: Playbook to configure IPA clients`
			`  hosts: ipaclients`
			`  become: true`
			
			`  roles:`
			`  - role: ipaclient`
			`  state: true`

Un mot de passe aléatoire à usage unique (OTP) : Option 1	Mot de passe administrateur OTP	`[ipaclients:vars]`
		`ipaadmin_password=Secret123`
		`ipaclient_use_otp=true`
			`- name: Playbook to configure IPA clients`
			`  hosts: ipaclients`
			`  become: true`
			
			`  roles:`
			`  - role: ipaclient`
			`  state: true`

Un mot de passe aléatoire à usage unique (OTP) : Option 2	OTP un keytab administrateur	`[ipaclients:vars]`
		`ipaadmin_keytab=/root/admin.keytab`
		`ipaclient_use_otp=true`
			`- name: Playbook to configure IPA clients`
			`  hosts: ipaclients`
			`  become: true`
			
			`  roles:`
			`  - role: ipaclient`
			`  state: true`

Option d'autorisation	Note	Exemple de fichier d'inventaire	Exemple de fichier playbook **install-client.yml**
Le fichier clé du client de l'inscription précédente		[ipaclients:vars] ipaclient_keytab=/root/krb5.keytab	- name: Playbook to configure IPA clients hosts: ipaclients become: true roles: - role: ipaclient state: true

NOTE

Depuis RHEL 9.2, dans les deux scénarios d'autorisation OTP décrits ci-dessus, la demande du TGT de l'administrateur à l'aide de la commande **kinit** se produit sur le premier serveur IdM spécifié ou découvert. Par conséquent, aucune modification supplémentaire du nœud de contrôle Ansible n'est nécessaire. Avant RHEL 9.2, le paquetage **krb5-workstation** était requis sur le nœud de contrôle.

27.5. DÉPLOIEMENT D'UN CLIENT IDM À L'AIDE D'UN PLAYBOOK ANSIBLE

Complétez cette procédure pour utiliser un playbook Ansible afin de déployer un client IdM dans votre environnement IdM.

Conditions préalables

- Vous avez défini les paramètres du déploiement du client IdM en fonction de votre scénario de déploiement :
  - Définition des paramètres du fichier d'inventaire pour le mode d'installation du client d'autodécouverte
  - Définition des paramètres du fichier d'inventaire lorsque l'autodécouverte n'est pas possible lors de l'installation du client
- Vous avez vérifié les paramètres dans install-client.yml.

Procédure

- Pour installer un client IdM à l'aide d'un playbook Ansible, utilisez la commande **ansible-playbook** avec le nom du fichier du playbook, par exemple **install-client.yml**. Spécifiez le fichier d'inventaire avec l'option **-i**:

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory/hosts install-client.yml
```

Spécifiez le niveau de verbosité en utilisant l'option **-v**, **-vv** ou **-vvv**.

Ansible vous informe de l'exécution du script du playbook Ansible. La sortie suivante montre que le script s'est exécuté avec succès car aucune tâche n'a échoué :

```
PLAY RECAP
client1.idm.example.com : ok=18 changed=10 unreachable=0 failed=0 skipped=21
rescued=0 ignored=0
```

NOTE

Ansible utilise différentes couleurs pour fournir différents types d'informations sur le processus en cours. Vous pouvez modifier les couleurs par défaut dans la section **[colors]** du fichier **/etc/ansible/ansible.cfg**:

```
[colors]
[...]
#error = red
#debug = dark gray
#deprecate = purple
#skip = cyan
#unreachable = red
#ok = green
#changed = yellow
[...]
```

Vous avez maintenant installé un client IdM sur votre hôte à l'aide d'un playbook Ansible.

27.6. TEST D'UN CLIENT DE GESTION D'IDENTITÉ APRÈS L'INSTALLATION D'ANSIBLE

L'interface de ligne de commande (CLI) vous informe que la commande **ansible-playbook** a réussi, mais vous pouvez également effectuer votre propre test.

Pour vérifier que le client de gestion des identités peut obtenir des informations sur les utilisateurs définis sur le serveur, vérifiez que vous pouvez résoudre un utilisateur défini sur le serveur. Par exemple, pour vérifier l'utilisateur par défaut **admin**:

```
[user@client1 ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

Pour tester que l'authentification fonctionne correctement, **su -** en tant qu'autre utilisateur IdM déjà existant :

```
[user@client1 ~]$ su - idm_user
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[idm_user@client1 ~]$
```

27.7. DÉSINSTALLATION D'UN CLIENT IDM À L'AIDE D'UN PLAYBOOK ANSIBLE

Complétez cette procédure pour utiliser un playbook Ansible afin de désinstaller votre hôte en tant que client IdM.

Conditions préalables

- Informations d'identification de l'administrateur de l'IdM.

Procédure

- Pour désinstaller le client IdM, utilisez la commande **ansible-playbook** avec le nom du fichier playbook, par exemple **uninstall-client.yml**. Spécifiez le fichier d'inventaire avec l'option **-i** et, éventuellement, spécifiez le niveau de verbosité en utilisant les options **-v**, **-vv** ou **-vvv**:

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory/hosts uninstall-client.yml
```

IMPORTANT

La désinstallation du client supprime uniquement la configuration IdM de base de l'hôte, mais laisse les fichiers de configuration sur l'hôte au cas où vous décideriez de réinstaller le client. En outre, la désinstallation présente les limitations suivantes :

- Elle ne supprime pas l'entrée de l'hôte du client du serveur LDAP IdM. La désinstallation ne fait que désinscrire l'hôte.
- Il ne supprime pas les services résidant sur le client de l'IdM.
- Il ne supprime pas les entrées DNS du serveur IdM pour le client.
- Il ne supprime pas les anciens principes pour les keytabs autres que **/etc/krb5.keytab**.

Notez que la désinstallation supprime tous les certificats émis pour l'hôte par l'autorité de certification IdM.

Ressources supplémentaires

- Voir Désinstallation d'un client IdM.