Red Hat Enterprise Linux 9

Travailler avec le DNS dans la gestion des identités

Gestion du service DNS intégré à l'IdM

Last Updated: 2024-01-18

Red Hat Enterprise Linux 9 Travailler avec le DNS dans la gestion des identités

Gestion du service DNS intégré à l'IdM

Notice légale

Résumé

Le DNS est un composant important dans un domaine Red Hat Identity Management (IdM). Par exemple, les clients utilisent le DNS pour localiser les services et identifier les serveurs sur le même site. Vous pouvez gérer les enregistrements, les zones, les emplacements et les transferts dans le serveur DNS intégré à IdM en utilisant la ligne de commande, l'interface Web IdM et les Playbooks Ansible.

Table des matières

RENDRE L'OPEN SOURCE PLUS INCLUSIF

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

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

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

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

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

Soumettre des commentaires sur des passages spécifiques

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

Soumettre des commentaires via Bugzilla (compte requis)

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

CHAPITRE 1. GÉRER LA CONFIGURATION DNS GLOBALE DANS IDM À L'AIDE DE PLAYBOOKS ANSIBLE

En utilisant le module Red Hat Ansible Engine **dnsconfig**, vous pouvez configurer la configuration globale pour le DNS de la gestion des identités (IdM). Les paramètres définis dans la configuration DNS globale sont appliqués à tous les serveurs DNS IdM. Cependant, la configuration globale a une priorité inférieure à la configuration d'une zone DNS IdM spécifique.

Le module **dnsconfig** prend en charge les variables suivantes :

- Les transitaires globaux, en particulier leurs adresses IP et le port utilisé pour la communication.
- La politique de transfert globale : seulement, d'abord ou aucune. Pour plus de détails sur ces types de politiques de transfert DNS, voir les politiques de transfert DNS dans IdM .
- La synchronisation des zones de recherche avancée et de recherche inversée.

Conditions préalables

- Le service DNS est installé sur le serveur IdM. Pour plus d'informations sur l'installation d'un serveur IdM avec DNS intégré, voir l'un des liens suivants :
  - Installation d'un serveur IdM : Avec DNS intégré, avec une autorité de certification intégrée comme autorité de certification racine
  - Installation d'un serveur IdM : Avec DNS intégré, avec une autorité de certification externe comme autorité de certification racine
  - Installation d'un serveur IdM : Avec DNS intégré, sans CA

Ce chapitre comprend les sections suivantes :

- Comment IdM s'assure que les forwarders globaux du fichier /etc/resolv.conf ne sont pas supprimés par NetworkManager
- Assurer la présence d'un DNS global forwarder dans IdM en utilisant Ansible
- S'assurer de l'absence d'un DNS global forwarder dans l'IdM en utilisant Ansible
- L'option **action: member** dans les modules ipadnsconfig ansible-freeipa
- Introduction aux politiques de transfert DNS dans l'IdM
- Utilisation d'un playbook Ansible pour s'assurer que la politique "forward first" est définie dans la configuration globale du DNS IdM
- Utilisation d'un playbook Ansible pour s'assurer que les redirections globales sont désactivées dans le DNS IdM
- Utilisation d'un playbook Ansible pour s'assurer que la synchronisation des zones de recherche directe et inversée est désactivée dans IdM DNS

1.1. COMMENT IDM S'ASSURE QUE LES FORWARDERS GLOBAUX DU FICHIER /ETC/RESOLV.CONF NE SONT PAS SUPPRIMÉS PAR NETWORKMANAGER

L'installation de la gestion des identités (IdM) avec DNS intégré configure le fichier **/etc/resolv.conf** pour qu'il pointe vers l'adresse **127.0.0.1** localhost :

```
# Generated by NetworkManager
search idm.example.com
nameserver 127.0.0.1
```

Dans certains environnements, tels que les réseaux qui utilisent **Dynamic Host Configuration Protocol** (DHCP), le service **NetworkManager** peut annuler les modifications apportées au fichier **/etc/resolv.conf**. Pour rendre la configuration DNS persistante, le processus d'installation de IdM DNS configure également le service **NetworkManager** de la manière suivante :

1. Le script d'installation DNS crée un fichier de configuration **/etc/NetworkManager/conf.d/zzz-ipa.conf NetworkManager** pour contrôler l'ordre de recherche et la liste des serveurs DNS :

```
# auto-generated by IPA installer
[main]
dns=default

[global-dns]
searches=$DOMAIN

[global-dns-domain-*]
servers=127.0.0.1
```

2. Le service **NetworkManager** est rechargé, ce qui crée toujours le fichier **/etc/resolv.conf** avec les paramètres du dernier fichier du répertoire **/etc/NetworkManager/conf.d/**. Dans le cas présent, il s'agit du fichier **zzz-ipa.conf**.

IMPORTANT

Ne modifiez pas manuellement le fichier **/etc/resolv.conf**.

1.2. ASSURER LA PRÉSENCE D'UN DNS GLOBAL FORWARDER DANS IDM EN UTILISANT ANSIBLE

Cette section décrit comment un administrateur Identity Management (IdM) peut utiliser un playbook Ansible pour assurer la présence d'un transitaire global DNS dans IdM. Dans l'exemple de procédure ci-dessous, l'administrateur IdM assure la présence d'un transitaire global DNS vers un serveur DNS avec une adresse Internet Protocol (IP) v4 de **7.7.9.9** et une adresse IP v6 de **2001:db8::1:0** sur le port **53**.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.

- L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
- L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.

- Vous connaissez le mot de passe de l'administrateur IdM.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsconfig
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **forwarders-absent.yml** Ansible playbook. Par exemple :

```
$ cp forwarders-absent.yml ensure-presence-of-a-global-forwarder.yml
```

4. Ouvrez le fichier **ensure-presence-of-a-global-forwarder.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes :
   a. Modifiez la variable **name** du playbook en **Playbook to ensure the presence of a global forwarder in IdM DNS**.
   b. Dans la section **tasks**, changez le **name** de la tâche en **Ensure the presence of a DNS global forwarder to 7.7.9.9 and 2001:db8::1:0 on port 53**.
   c. Dans la section **forwarders** de la partie **ipadnsconfig**:
      i. Remplacez la première valeur de **ip_address** par l'adresse IPv4 du transitaire global : **7.7.9.9**.
      ii. Remplacer la deuxième valeur **ip_address** par l'adresse IPv6 du transitaire global : **2001:db8::1:0**.
      iii. Vérifiez que la valeur **port** est définie sur **53**.
   d. Modifier le **state** en **present**.
   Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Playbook to ensure the presence of a global forwarder in IdM DNS
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
```

```
  - name: Ensure the presence of a DNS global forwarder to 7.7.9.9 and 2001:db8::1:0 on port
53
    ipadnsconfig:
      forwarders:
        - ip_address: 7.7.9.9
        - ip_address: 2001:db8::1:0
          port: 53
      state: present
```

6. Enregistrer le fichier.

7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file ensure-presence-
of-a-global-forwarder.yml
```

Ressources supplémentaires

- Voir le fichier **README-dnsconfig.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.

1.3. S'ASSURER DE L'ABSENCE D'UN DNS GLOBAL FORWARDER DANS L'IDM EN UTILISANT ANSIBLE

Cette section décrit comment un administrateur Identity Management (IdM) peut utiliser un playbook Ansible pour garantir l'absence d'un transitaire global DNS dans IdM. Dans l'exemple de procédure ci-dessous, l'administrateur IdM s'assure de l'absence d'un transitaire global DNS avec une adresse Internet Protocol (IP) v4 de **8.8.6.6** et une adresse IP v6 de **2001:4860:4860::8800** sur le port **53**.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous connaissez le mot de passe de l'administrateur IdM.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsconfig
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **forwarders-absent.yml** Ansible playbook. Par exemple :

```
$ cp forwarders-absent.yml ensure-absence-of-a-global-forwarder.yml
```

4. Ouvrez le fichier **ensure-absence-of-a-global-forwarder.yml** pour le modifier.

5. Adaptez le fichier en définissant les variables suivantes :

   a. Modifiez la variable **name** du playbook en **Playbook to ensure the absence of a global forwarder in IdM DNS**.

   b. Dans la section **tasks**, changez le **name** de la tâche en **Ensure the absence of a DNS global forwarder to 8.8.6.6 and 2001:4860:4860::8800 on port 53**.

   c. Dans la section **forwarders** de la partie **ipadnsconfig**:

      i. Remplacez la première valeur de **ip_address** par l'adresse IPv4 du transitaire global : **8.8.6.6**.

      ii. Remplacer la deuxième valeur **ip_address** par l'adresse IPv6 du transitaire global : **2001:4860:4860::8800**.

      iii. Vérifiez que la valeur **port** est définie sur **53**.

   d. Fixer la variable **action** à **member**.

   e. Vérifiez que **state** est défini sur **absent**.

Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Playbook to ensure the absence of a global forwarder in IdM DNS
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Ensure the absence of a DNS global forwarder to 8.8.6.6 and
2001:4860:4860::8800 on port 53
    ipadnsconfig:
      forwarders:
        - ip_address: 8.8.6.6
        - ip_address: 2001:4860:4860::8800
          port: 53
      action: member
      state: absent
```

IMPORTANT

Si vous n'utilisez que l'option **state: absent** dans votre séquence sans utiliser également **action: member**, la séquence échoue.

6. Enregistrer le fichier.
7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file ensure-absence-of-a-global-forwarder.yml
```

Ressources supplémentaires

- Le fichier **README-dnsconfig.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**
- L'option **action: member** dans les modules ipadnsconfig ansible-freeipa

1.4. L'OPTION ACTION: MEMBER DANS LES MODULES IPADNSCONFIG ANSIBLE-FREEIPA

L'exclusion des expéditeurs globaux dans la gestion de l'identité (IdM) à l'aide du module **ansible-freeipa ipadnsconfig** nécessite l'utilisation de l'option **action: member** en plus de l'option **state: absent**. Si vous utilisez uniquement **state: absent** dans votre manuel sans utiliser également **action: member**, le manuel échoue. Par conséquent, pour supprimer tous les transitaires globaux, vous devez tous les spécifier individuellement dans le cahier d'exécution. En revanche, l'option **state: present** ne nécessite pas **action: member**.

Le tableau suivant fournit des exemples de configuration pour l'ajout et la suppression de transitaires globaux DNS qui démontrent l'utilisation correcte de l'option action : member. Le tableau indique, dans chaque ligne :

- Les transitaires globaux configurés avant l'exécution d'un playbook
- Un extrait du manuel de jeu
- Les transitaires globaux configurés après l'exécution du playbook

Tableau 1.1. ipadnsconfig gestion des transitaires globaux

Transporteurs avant	Extrait du Playbook	Transporteurs après
8.8.6.6	[...] tasks: - name: Ensure the presence of DNS global forwarder 8.8.6.7 ipadnsconfig: forwarders: - ip_address: 8.8.6.7 state: present	8.8.6.7

Transporteurs avant	Extrait du Playbook	Transporteurs après
8.8.6.6	[...] tasks: - name: Ensure the presence of DNS global forwarder 8.8.6.7 ipadnsconfig: forwarders: - ip_address: 8.8.6.7 action: member state: present	8.8.6.6, 8.8.6.7
8.8.6.6, 8.8.6.7	[...] tasks: - name: Ensure the absence of DNS global forwarder 8.8.6.7 ipadnsconfig: forwarders: - ip_address: 8.8.6.7 state: absent	La tentative d'exécution du playbook aboutit à une erreur. La configuration originale - 8.8.6.6, 8.8.6.7 - reste inchangée.
8.8.6.6, 8.8.6.7	[...] tasks: - name: Ensure the absence of DNS global forwarder 8.8.6.7 ipadnsconfig: forwarders: - ip_address: 8.8.6.7 action: member state: absent	8.8.6.6

1.5. POLITIQUES DE TRANSFERT DNS DANS L'IDM

IdM prend en charge les politiques d'acheminement standard de BIND **first** et **only**, ainsi que la politique d'acheminement spécifique à IdM **none**.

En avant, d'abord *(default)*

Le service BIND de l'IdM transmet les requêtes DNS au transitaire configuré. Si une requête échoue en raison d'une erreur de serveur ou d'un dépassement de délai, BIND se rabat sur la résolution récursive en utilisant des serveurs sur l'internet. La politique **forward first** est la politique par défaut et convient pour optimiser le trafic DNS.

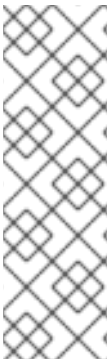
En avant seulement

Le service IdM BIND transmet les requêtes DNS au transitaire configuré. Si une requête échoue en raison d'une erreur du serveur ou d'un dépassement de délai, BIND renvoie une erreur au client. La stratégie **forward only** est recommandée pour les environnements avec une configuration DNS

divisée.

Aucun *(forwarding disabled)*

Les requêtes DNS ne sont pas transférées avec la politique de transfert **none**. La désactivation de la redirection n'est utile que pour remplacer la configuration globale de la redirection dans une zone spécifique. Cette option est l'équivalent pour IdM de la spécification d'une liste vide de transitaires dans la configuration de BIND.



NOTE

Vous ne pouvez pas utiliser le transfert pour combiner des données dans IdM avec des données provenant d'autres serveurs DNS. Vous ne pouvez transférer des requêtes que pour des sous-zones spécifiques de la zone primaire dans le DNS IdM.

Par défaut, le service BIND ne transmet pas les requêtes à un autre serveur si le nom DNS demandé appartient à une zone pour laquelle le serveur IdM fait autorité. Dans une telle situation, si le nom DNS demandé ne peut être trouvé dans la base de données IdM, la réponse **NXDOMAIN** est renvoyée. Le transfert n'est pas utilisé.

Exemple 1.1. Exemple de scénario

Le serveur IdM fait autorité pour la zone DNS **test.example.**. BIND est configuré pour transmettre les requêtes au serveur DNS avec l'adresse IP **192.0.2.254**.

Lorsqu'un client envoie une requête pour le nom DNS **nonexistent.test.example.**, BIND détecte que le serveur IdM fait autorité pour la zone **test.example.** et ne transmet pas la requête au serveur **192.0.2.254.**. En conséquence, le client DNS reçoit le message d'erreur **NXDomain**, informant l'utilisateur que le domaine interrogé n'existe pas.

1.6. UTILISATION D'UN PLAYBOOK ANSIBLE POUR S'ASSURER QUE LA POLITIQUE "FORWARD FIRST" EST DÉFINIE DANS LA CONFIGURATION GLOBALE DU DNS IDM

Cette section décrit comment un administrateur Identity Management (IdM) peut utiliser un playbook Ansible pour s'assurer que la politique de transfert global dans IdM DNS est définie sur **forward first**.

Si vous utilisez la stratégie **forward first** DNS forwarding, les requêtes DNS sont transmises au forwarder configuré. Si une requête échoue en raison d'une erreur de serveur ou d'un dépassement de délai, BIND revient à la résolution récursive en utilisant des serveurs sur Internet. La stratégie "forward first" est la stratégie par défaut. Elle convient à l'optimisation du trafic.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.

    - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.

- Vous connaissez le mot de passe de l'administrateur IdM.
- Votre environnement IdM contient un serveur DNS intégré.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsconfig
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **set-configuration.yml** Ansible playbook. Par exemple :

```
$ cp set-configuration.yml set-forward-policy-to-first.yml
```

4. Ouvrez le fichier **set-forward-policy-to-first.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes dans la section **ipadnsconfig** task :
    - Définissez la variable **ipaadmin_password** avec votre mot de passe d'administrateur IdM.
    - Fixer la variable **forward_policy** à **first**.
      Supprimez toutes les autres lignes du playbook original qui ne sont pas pertinentes. Voici le fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Playbook to set global forwarding policy to first
  hosts: ipaserver
  become: true

  tasks:
  - name: Set global forwarding policy to first.
    ipadnsconfig:
      ipaadmin_password: "{{ ipaadmin_password }}"
      forward_policy: first
```

6. Enregistrer le fichier.
7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file set-forward-policy-to-first.yml
```

Ressources supplémentaires

- Voir les politiques de transfert de DNS dans IdM .
- Voir le fichier **README-dnsconfig.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Pour obtenir d'autres exemples de playbooks, consultez le répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**.

1.7. UTILISATION D'UN PLAYBOOK ANSIBLE POUR S'ASSURER QUE LES REDIRECTIONS GLOBALES SONT DÉSACTIVÉES DANS LE DNS IDM

Cette section décrit comment un administrateur Identity Management (IdM) peut utiliser un playbook Ansible pour s'assurer que les redirections globales sont désactivées dans le DNS IdM. La désactivation s'effectue en définissant la variable **forward_policy** sur **none**.

La désactivation des transferts globaux a pour effet de ne pas transférer les requêtes DNS. La désactivation de la redirection n'est utile que pour remplacer la configuration de la redirection globale dans une zone spécifique. Cette option est l'équivalent pour IdM de la spécification d'une liste vide de transitaires dans la configuration de BIND.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous connaissez le mot de passe de l'administrateur IdM.
- Votre environnement IdM contient un serveur DNS intégré.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsconfig
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **disable-global-forwarders.yml** Ansible playbook. Par exemple :

```
$ cp disable-global-forwarders.yml disable-global-forwarders-copy.yml
```

4. Ouvrez le fichier **disable-global-forwarders-copy.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes dans la section **ipadnsconfig** task :
   - Définissez la variable **ipaadmin_password** avec votre mot de passe d'administrateur IdM.
   - Fixer la variable **forward_policy** à **none**.
     Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Playbook to disable global DNS forwarders
  hosts: ipaserver
  become: true

  tasks:
  - name: Disable global forwarders.
    ipadnsconfig:
      ipaadmin_password: "{{ ipaadmin_password }}"
      forward_policy: none
```

6. Enregistrer le fichier.
7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file disable-global-forwarders-copy.yml
```

Ressources supplémentaires

- Voir les politiques de transfert de DNS dans IdM .
- Voir le fichier **README-dnsconfig.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir d'autres exemples de playbooks dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**.

1.8. UTILISATION D'UN PLAYBOOK ANSIBLE POUR S'ASSURER QUE LA SYNCHRONISATION DES ZONES DE RECHERCHE DIRECTE ET INVERSÉE EST DÉSACTIVÉE DANS IDM DNS

Cette section décrit comment un administrateur de gestion des identités (IdM) peut utiliser un manuel de jeu Ansible pour s'assurer que les zones de recherche directe et inversée ne sont pas synchronisées dans le DNS IdM.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.

- L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
- L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.

- Vous connaissez le mot de passe de l'administrateur IdM.
- Votre environnement IdM contient un serveur DNS intégré.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsconfig
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **disallow-reverse-sync.yml** Ansible playbook. Par exemple :

```
$ cp disallow-reverse-sync.yml disallow-reverse-sync-copy.yml
```

4. Ouvrez le fichier **disallow-reverse-sync-copy.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes dans la section **ipadnsconfig** task :
   - Définissez la variable **ipaadmin_password** avec votre mot de passe d'administrateur IdM.
   - Fixer la variable **allow_sync_ptr** à **no**.
     Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Playbook to disallow reverse record synchronization
  hosts: ipaserver
  become: true

  tasks:
  - name: Disallow reverse record synchronization.
    ipadnsconfig:
      ipaadmin_password: "{{ ipaadmin_password }}"
      allow_sync_ptr: no
```

6. Enregistrer le fichier.
7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file disallow-reverse-sync-copy.yml
```

Ressources supplémentaires

- Voir le fichier **README-dnsconfig.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Pour obtenir d'autres exemples de playbooks, consultez le répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**.

CHAPITRE 2. GESTION DES ZONES DNS DANS L'IDM

En tant qu'administrateur Identity Management (IdM), vous pouvez gérer le fonctionnement des zones DNS IdM. Ce chapitre décrit les sujets et procédures suivants :

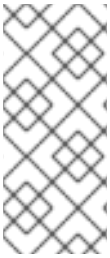
- Quels sont les types de zones DNS pris en charge par IdM ?
  - Comment ajouter des zones DNS primaires IdM à l'aide de l'interface Web IdM ?
  - Comment ajouter des zones DNS primaires IdM à l'aide de la CLI IdM
  - Comment supprimer les zones DNS primaires de l'IdM à l'aide de l'interface Web de l'IdM ?
  - Comment supprimer les zones DNS primaires de l'IdM à l'aide de la CLI de l'IdM
- Quels sont les attributs DNS que vous pouvez configurer dans IdM ?
  - Comment configurer ces attributs dans l'interface Web IdM
  - Comment configurer ces attributs dans la CLI IdM
- Comment fonctionnent les transferts de zone dans l'IdM
  - Comment autoriser les transferts de zone dans l'interface Web IdM
  - Comment autoriser les transferts de zone dans le CLI IdM

Conditions préalables

- Le service DNS est installé sur le serveur IdM. Pour plus d'informations sur l'installation d'un serveur IdM avec DNS intégré, voir l'un des liens suivants :
  - Installation d'un serveur IdM : Avec DNS intégré, avec une autorité de certification intégrée comme autorité de certification racine
  - Installation d'un serveur IdM : Avec DNS intégré, avec une autorité de certification externe comme autorité de certification racine
  - Installation d'un serveur IdM : Avec DNS intégré, sans CA

2.1. TYPES DE ZONES DNS PRISES EN CHARGE

Identity Management (IdM) prend en charge deux types de zones DNS : les zones *primary* et *forward*. Cette section décrit ces deux types de zones et inclut un exemple de scénario de transfert DNS.



NOTE

Ce guide utilise la terminologie BIND pour les types de zones, qui est différente de la terminologie utilisée pour le DNS de Microsoft Windows. Les zones primaires dans BIND ont la même fonction que *forward lookup zones* et *reverse lookup zones* dans le DNS de Microsoft Windows. Les zones de transfert dans BIND ont la même fonction que *conditional forwarders* dans le DNS de Microsoft Windows.

Zones DNS primaires

Les zones DNS primaires contiennent des données DNS faisant autorité et peuvent accepter des

mises à jour DNS dynamiques. Ce comportement est équivalent au paramètre **type master** dans la configuration standard de BIND. Vous pouvez gérer les zones primaires à l'aide des commandes **ipa dnszone-***.
Conformément aux règles DNS standard, chaque zone primaire doit contenir des enregistrements **start of authority** (SOA) et **nameserver** (NS). L'IdM génère automatiquement ces enregistrements lors de la création de la zone DNS, mais vous devez copier manuellement les enregistrements NS dans la zone mère pour créer une délégation correcte.

Conformément au comportement standard de BIND, les requêtes portant sur des noms pour lesquels le serveur ne fait pas autorité sont transmises à d'autres serveurs DNS. Ces serveurs DNS, appelés "forwarders", peuvent ou non faire autorité pour la requête.

> **Exemple 2.1. Exemple de scénario pour le transfert DNS**
>
> Le serveur IdM contient la zone primaire **test.example.**. Cette zone contient un enregistrement de délégation NS pour le nom **sub.test.example.**. En outre, la zone **test.example.** est configurée avec l'adresse IP du transitaire **192.0.2.254** pour la sous-zone **sub.text.example**.
>
> Un client interrogeant le nom **nonexistent.test.example.** reçoit la réponse **NXDomain** et aucun transfert n'a lieu car le serveur IdM fait autorité pour ce nom.
>
> D'autre part, les requêtes portant sur le nom **host1.sub.test.example.** sont transmises au transitaire configuré **192.0.2.254**, car le serveur IdM ne fait pas autorité pour ce nom.

Transférer des zones DNS

Du point de vue de l'IdM, les zones DNS avancées ne contiennent aucune donnée faisant autorité. En fait, une "zone" avancée ne contient généralement que deux éléments d'information :

- Un nom de domaine
- L'adresse IP d'un serveur DNS associé au domaine

Toutes les requêtes portant sur des noms appartenant au domaine défini sont transmises à l'adresse IP spécifiée. Ce comportement est équivalent au paramètre **type forward** dans la configuration standard de BIND. Vous pouvez gérer les zones de transfert à l'aide des commandes **ipa dnsforwardzone-***.

Les zones DNS à suivre sont particulièrement utiles dans le contexte des trusts IdM-Active Directory (AD). Si le serveur DNS IdM fait autorité pour la zone **idm.example.com** et que le serveur DNS AD fait autorité pour la zone **ad.example.com**, alors **ad.example.com** est une zone DNS de renvoi pour la zone primaire **idm.example.com**. Cela signifie que lorsqu'un client IdM demande l'adresse IP de **somehost.ad.example.com**, la requête est transmise à un contrôleur de domaine AD spécifié dans la zone de transfert DNS IdM **ad.example.com**.

2.2. AJOUT D'UNE ZONE DNS PRIMAIRE DANS L'INTERFACE WEB IDM

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

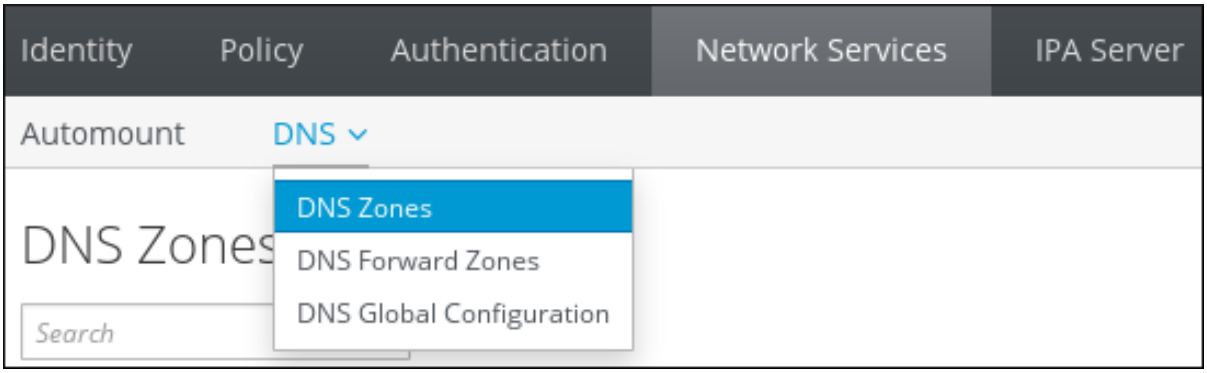
Conditions préalables

- Vous êtes connecté en tant qu'administrateur IdM.

Procédure

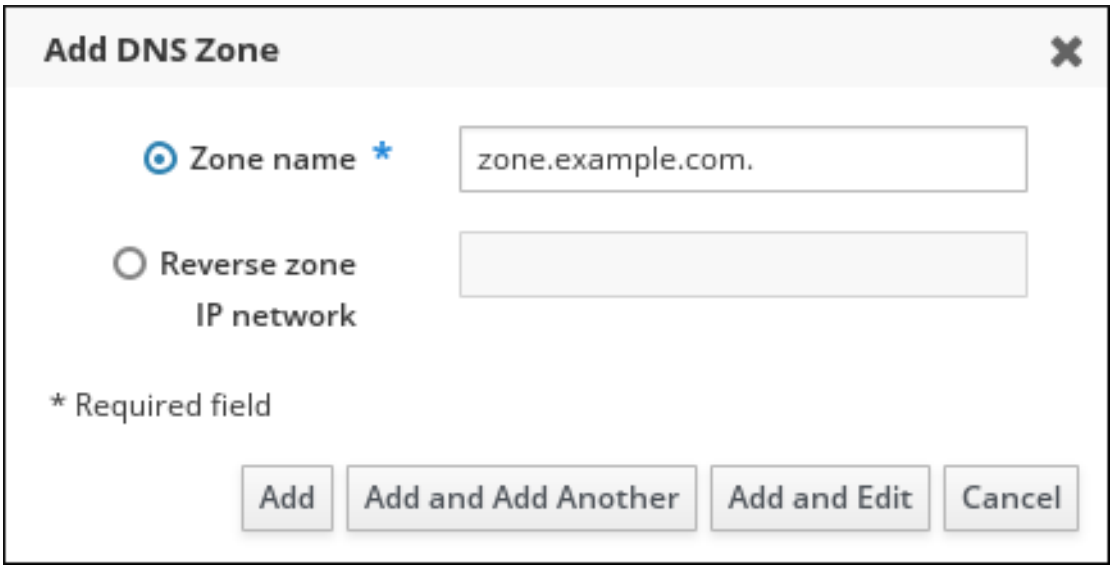
1. Dans l'interface Web IdM, cliquez sur **Network Services → DNS → DNS Zones**.

Figure 2.1. Gestion des zones primaires DNS de l'IdM



2. Cliquez sur **Ajouter** en haut de la liste de toutes les zones.
3. Indiquez le nom de la zone.

Figure 2.2. Entrer dans une nouvelle zone primaire IdM



4. Click **Add**.

2.3. AJOUT D'UNE ZONE DNS PRIMAIRE DANS LA CLI IDM

Cette section décrit comment ajouter une zone DNS primaire dans l'interface de ligne de commande (CLI) de la gestion des identités (IdM).

Conditions préalables

- Vous êtes connecté en tant qu'administrateur IdM.

Procédure

- La commande **ipa dnszone-add** ajoute une nouvelle zone au domaine DNS. L'ajout d'une nouvelle zone nécessite de spécifier le nom du nouveau sous-domaine. Vous pouvez transmettre le nom du sous-domaine directement avec la commande :

```
$ ipa dnszone-add newzone.idm.example.com
```

Si vous n'indiquez pas le nom à **ipa dnszone-add**, le script vous le demande automatiquement.

Ressources supplémentaires

- Voir **ipa dnszone-add --help**.

2.4. SUPPRESSION D'UNE ZONE DNS PRIMAIRE DANS L'INTERFACE WEB IDM

Cette section décrit comment supprimer une zone DNS primaire de la gestion des identités (IdM) à l'aide de l'interface Web IdM.

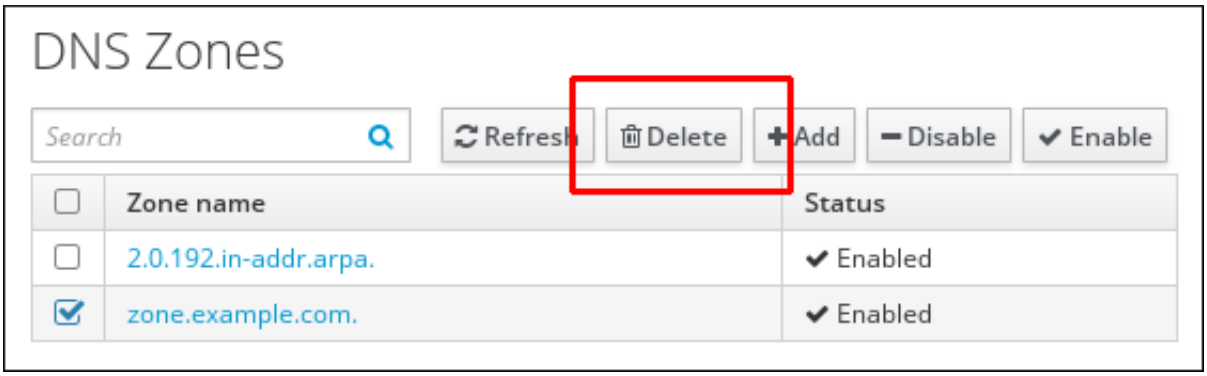
Conditions préalables

- Vous êtes connecté en tant qu'administrateur IdM.

Procédure

1. Dans l'interface Web IdM, cliquez sur **Network Services → DNS → DNS Zones**.
2. Cochez la case correspondant au nom de la zone et cliquez sur **Supprimer**.

Figure 2.3. Suppression d'une zone DNS primaire



3. Dans la fenêtre de dialogue **Remove DNS zones**, confirmez que vous souhaitez supprimer la zone sélectionnée.

2.5. SUPPRESSION D'UNE ZONE DNS PRIMAIRE DANS IDM CLI

Cette section décrit comment supprimer une zone DNS primaire de la gestion des identités (IdM) à l'aide de l'interface de ligne de commande (CLI) de l'IdM.

Conditions préalables

- Vous êtes connecté en tant qu'administrateur IdM.

Procédure

- Pour supprimer une zone DNS primaire, entrez la commande **ipa dnszone-del**, suivie du nom de la zone que vous souhaitez supprimer. Par exemple :

```
$ ipa dnszone-del idm.example.com
```

2.6. PRIORITÉS DE LA CONFIGURATION DNS

Vous pouvez configurer de nombreuses options de configuration DNS aux niveaux suivants. Chaque niveau a une priorité différente.

Configuration spécifique à la zone

Le niveau de configuration spécifique à une zone particulière définie dans IdM a la priorité la plus élevée. Vous pouvez gérer la configuration spécifique à une zone en utilisant les commandes **ipa dnszone-*** et **ipa dnsforwardzone-***.

Configuration par serveur

Lors de l'installation d'un serveur IdM, il vous est demandé de définir des transitaires par serveur. Vous pouvez gérer les forwarders par serveur en utilisant les commandes **ipa dnsserver-***. Si vous ne souhaitez pas définir de forwarder par serveur lors de l'installation d'un réplica, vous pouvez utiliser l'option **--no-forwarder**.

Configuration globale du DNS

Si aucune configuration spécifique à une zone n'est définie, IdM utilise la configuration DNS globale stockée dans LDAP. Vous pouvez gérer la configuration DNS globale à l'aide des commandes **ipa dnsconfig-***. Les paramètres définis dans la configuration DNS globale sont appliqués à tous les serveurs DNS de l'IdM.

Configuration en /etc/named.conf

La configuration définie dans le fichier **/etc/named.conf** sur chaque serveur IdM DNS a la priorité la plus basse. Elle est spécifique à chaque serveur et doit être modifiée manuellement.
Le fichier **/etc/named.conf** n'est généralement utilisé que pour spécifier la redirection DNS vers un cache DNS local. Les autres options sont gérées à l'aide des commandes de configuration DNS globale et spécifique à la zone mentionnées ci-dessus.

Vous pouvez configurer les options DNS à plusieurs niveaux en même temps. Dans ce cas, la configuration ayant la priorité la plus élevée est prioritaire sur la configuration définie aux niveaux inférieurs.

Ressources supplémentaires

- La section **Priority order of configuration** dans Per Server Config dans LDAP

2.7. ATTRIBUTS DE CONFIGURATION DES ZONES DNS PRIMAIRES DE L'IDM

Identity Management (IdM) crée une nouvelle zone avec certaines configurations par défaut, telles que les périodes de rafraîchissement, les paramètres de transfert ou les paramètres de cache. Dans les attributs de la zone DNS IdM , vous trouverez les attributs de la configuration de la zone par défaut que vous pouvez modifier à l'aide de l'une des options suivantes :

- La commande **dnszone-mod** dans l'interface de ligne de commande (CLI). Pour plus d'informations, voir Modifier la configuration d'une zone DNS primaire dans l'interface CLI de l'IdM.
- L'interface Web IdM. Pour plus d'informations, voir Modifier la configuration d'une zone DNS primaire dans l'interface Web IdM.
- Un playbook Ansible qui utilise le module **ipadnszone**. Pour plus d'informations, voir Gestion des zones DNS dans IdM.

Outre les informations relatives à la zone, les paramètres définissent la manière dont le serveur DNS traite les entrées de l'enregistrement *start of authority* (SOA) et la manière dont il met à jour ses enregistrements à partir du serveur de noms DNS.

Tableau 2.1. Attributs de la zone DNS de l'IdM

Attribut	Option de la ligne de commande	Description
Serveur de noms faisant autorité	**--name-server**	Définit le nom de domaine du serveur de noms DNS primaire, également connu sous le nom de SOA MNAME. Par défaut, chaque serveur IdM s'annonce lui-même dans le champ SOA MNAME. Par conséquent, la valeur stockée dans LDAP à l'aide de **--name-server** est ignorée.
Adresse électronique de l'administrateur	**--admin-email**	Définit l'adresse électronique à utiliser pour l'administrateur de zone. Par défaut, il s'agit du compte root de l'hôte.
Série SOA	**--serial**	Définit un numéro de série dans l'enregistrement SOA. Notez que l'IdM définit automatiquement le numéro de version et que les utilisateurs ne sont pas censés le modifier.
Actualisation de l'AOS	**--refresh**	Définit l'intervalle, en secondes, pendant lequel un serveur DNS secondaire doit attendre avant de demander des mises à jour au serveur DNS primaire.
Réessai SOA	**--retry**	Définit le délai, en secondes, à attendre avant de réessayer une opération de rafraîchissement qui a échoué.
SOA expirer	**--expire**	Définit la durée, en secondes, pendant laquelle un serveur DNS secondaire tentera d'effectuer une mise à jour avant de mettre fin à la tentative d'opération.
Minimum SOA	**--minimum**	Définit la valeur TTL (time to live) en secondes pour la mise en cache négative conformément à la RFC 2308.
Délai de mise en œuvre de la SOA	**--ttl**	Définit le TTL en secondes pour les enregistrements à l'apex de la zone. Dans la zone **example.com**, par exemple, tous les enregistrements (A, NS ou SOA) sous le nom **example.com** sont configurés, mais aucun autre nom de domaine, comme **test.example.com**, n'est affecté.
Durée de vie par défaut	**--default-ttl**	Définit la valeur par défaut du TTL (Time to Live) en secondes pour la mise en cache négative de toutes les valeurs d'une zone qui n'ont jamais eu de valeur TTL individuelle définie auparavant. Nécessite un redémarrage du service **named-pkcs11** sur tous les serveurs DNS IdM pour que les modifications soient prises en compte.

Attribut	Option de la ligne de commande	Description
Politique de mise à jour de BIND	**--update-policy**	Définit les autorisations accordées aux clients dans la zone DNS.
Mise à jour dynamique	**--dynamic-update**=VRAI|FAUX	Active les mises à jour dynamiques des enregistrements DNS pour les clients. Notez que si cette valeur est fixée à false, les machines clientes IdM ne pourront pas ajouter ou mettre à jour leur adresse IP.
Autoriser le transfert	**--allow-transfer**=*string*	Donne une liste d'adresses IP ou de noms de réseau autorisés à transférer la zone donnée, séparés par des points-virgules (;). Les transferts de zone sont désactivés par défaut. La valeur par défaut de **--allow-transfer** est **none**.
Autoriser l'interrogation	**--allow-query**	Donne une liste d'adresses IP ou de noms de réseau autorisés à émettre des requêtes DNS, séparés par des points-virgules (;).
Autoriser la synchronisation PTR	**--allow-sync-ptr**=1|0	Définit si les enregistrements A ou AAAA (enregistrements directs) de la zone seront automatiquement synchronisés avec les enregistrements PTR (enregistrements inversés).
Transitaires de zone	**--forwarder**=*IP_address*	Spécifie un transitaire spécifiquement configuré pour la zone DNS. Ce transitaire est distinct des transitaires globaux utilisés dans le domaine IdM. Pour spécifier plusieurs transitaires, utilisez l'option plusieurs fois.
Politique prévisionnelle	**--forward-policy**=unique|uniquement|premier	Spécifie la politique de transfert. Pour plus d'informations sur les politiques prises en charge, voir Politiques de transfert DNS dans IdM.

2.8. MODIFICATION DE LA CONFIGURATION D'UNE ZONE DNS PRIMAIRE DANS L'INTERFACE WEB IDM

Cette section décrit comment modifier les attributs de configuration d'un DNS primaire de gestion d'identité (IdM) à l'aide de l'interface Web IdM.

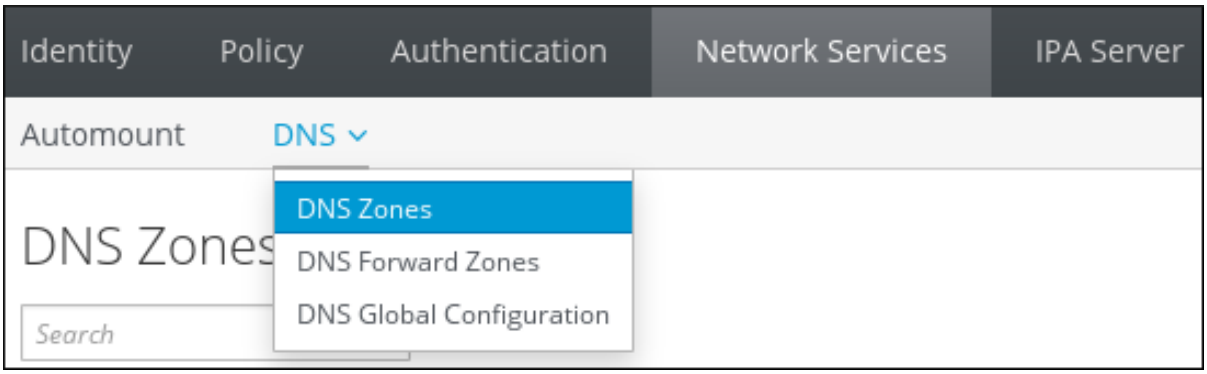
Conditions préalables

- Vous êtes connecté en tant qu'administrateur IdM.

Procédure

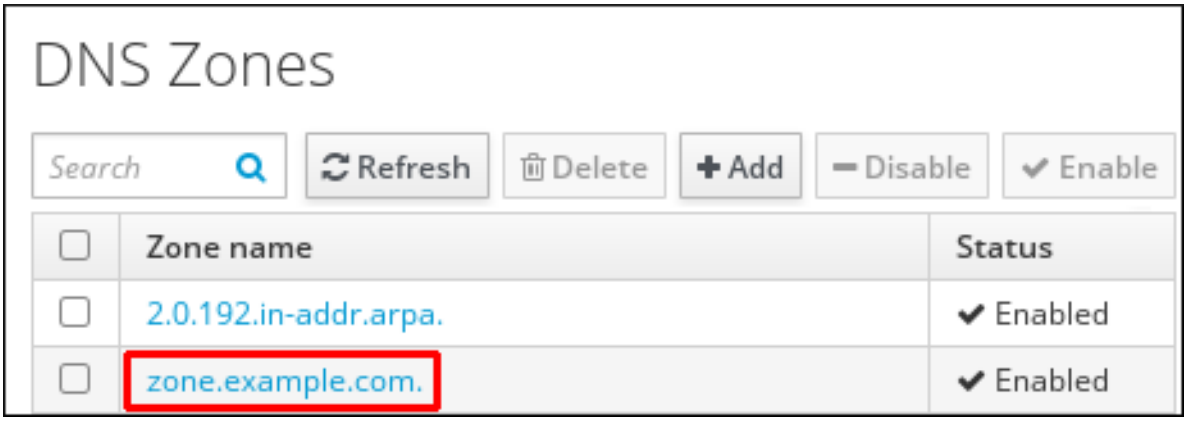
1. Dans l'interface Web IdM, cliquez sur **Network Services → DNS → DNS Zones**.

Figure 2.4. Gestion des zones primaires DNS



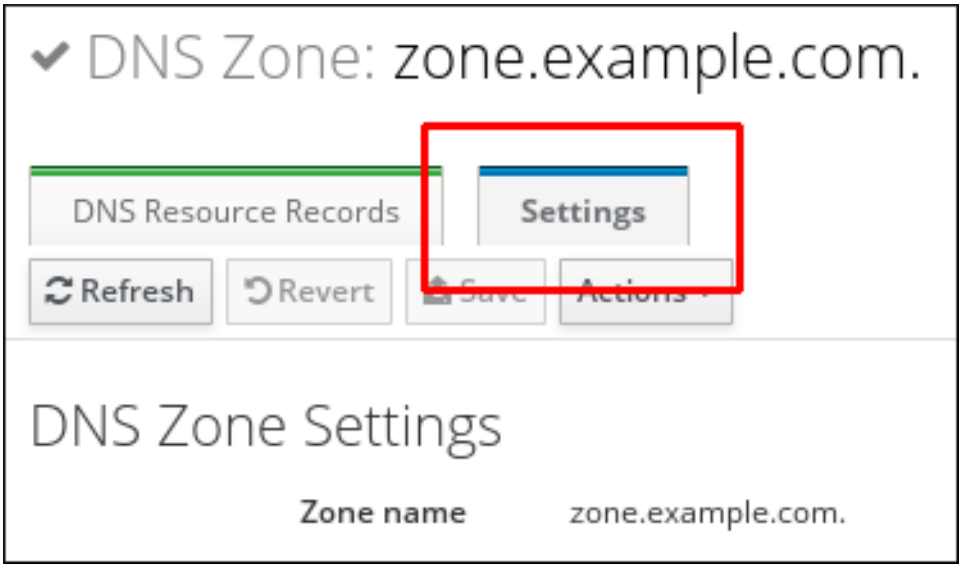
2. Dans la section **DNS Zones**, cliquez sur le nom de la zone dans la liste de toutes les zones pour ouvrir la page de la zone DNS.

Figure 2.5. Modification d'une zone primaire



3. Cliquez sur **Settings**.

Figure 2.6. L'onglet Paramètres de la page d'édition de la zone primaire



4. Modifiez la configuration de la zone si nécessaire.
Pour plus d'informations sur les paramètres disponibles, voir Attributs de la zone DNS IdM.

5. Cliquez sur **Enregistrer** pour confirmer la nouvelle configuration.

NOTE

Si vous modifiez la durée de vie (TTL) par défaut d'une zone, redémarrez le service **named-pkcs11** sur tous les serveurs DNS IdM pour que les modifications soient prises en compte. Tous les autres paramètres sont automatiquement activés immédiatement.

2.9. MODIFICATION DE LA CONFIGURATION D'UNE ZONE DNS PRIMAIRE DANS LA CLI IDM

Cette section décrit comment modifier la configuration d'une zone DNS primaire à l'aide de l'interface de ligne de commande (CLI) de la gestion des identités (IdM).

Conditions préalables

- Vous êtes connecté en tant qu'administrateur IdM.

Procédure

- Pour modifier une zone DNS primaire existante, utilisez la commande **ipa dnszone-mod**. Par exemple, pour fixer à 1800 secondes le délai d'attente avant de réessayer une opération de rafraîchissement qui a échoué :

```
$ ipa dnszone-mod --retry 1800
```

Pour plus d'informations sur les paramètres disponibles et les options CLI correspondantes, voir Attributs de la zone DNS IdM.

Si un paramètre spécifique n'a pas de valeur dans l'entrée de la zone DNS que vous modifiez, la commande **ipa dnszone-mod** ajoute la valeur. Si le paramètre n'a pas de valeur, la commande remplace la valeur actuelle par la valeur spécifiée.

NOTE

Si vous modifiez la durée de vie (TTL) par défaut d'une zone, redémarrez le service **named-pkcs11** sur tous les serveurs DNS IdM pour que les modifications soient prises en compte. Tous les autres paramètres sont automatiquement activés immédiatement.

Ressources supplémentaires

- Voir **ipa dnszone-mod --help**.

2.10. TRANSFERTS DE ZONES DANS L'IDM

Cette section décrit le fonctionnement des transferts de zone dans un déploiement de gestion des identités (IdM) qui a intégré le DNS.

Les serveurs de noms conservent les données faisant autorité pour leurs zones. Si vous apportez des modifications à la zone sur un serveur DNS qui fait autorité pour la zone DNS *zone A*, vous devez distribuer les modifications aux autres serveurs de noms du domaine DNS IdM qui se trouvent en dehors de *zone A*. Un site *zone transfer* copie tous les enregistrements de ressources d'un serveur de noms à un autre.

IMPORTANT

Le DNS intégré à l'IdM peut être écrit simultanément par différents serveurs. Les numéros de série Start of Authority (SOA) dans les zones IdM ne sont pas synchronisés entre les différents serveurs DNS IdM. Pour cette raison, configurez vos serveurs DNS en dehors de la zone à transférer pour qu'ils n'utilisent qu'un serveur DNS spécifique à l'intérieur de la zone à transférer. Cela permet d'éviter les échecs de transfert de zone causés par des numéros de série SOA non synchronisés.

L'IdM prend en charge les transferts de zone conformément aux normes RFC 5936 (AXFR) et RFC 1995 (IXFR).

Ressources supplémentaires

- Voir Activation des transferts de zone dans l'interface Web IdM .
- Voir Activation des transferts de zone dans l'interface CLI de l'IdM .

2.11. ACTIVATION DES TRANSFERTS DE ZONE DANS L'INTERFACE WEB IDM

Cette section décrit comment activer les transferts de zone dans la gestion des identités (IdM) à l'aide de l'interface Web IdM.

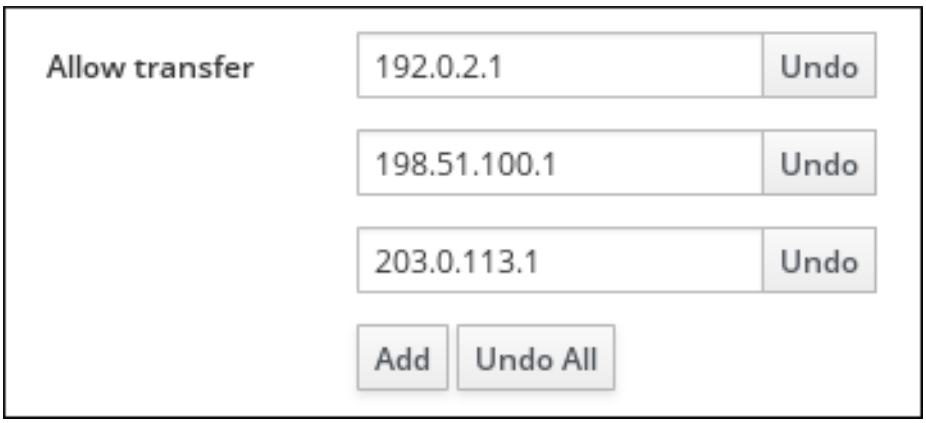
Conditions préalables

- Vous êtes connecté en tant qu'administrateur IdM.

Procédure

1. Dans l'interface Web IdM, cliquez sur **Network Services → DNS → DNS Zones**.
2. Cliquez sur **Settings**.
3. Sous **Allow transfer**, indiquez les serveurs de noms vers lesquels vous souhaitez transférer les enregistrements de zone.

   Figure 2.7. Permettre les transferts de zones

4. Cliquez sur **Enregistrer** en haut de la page de la zone DNS pour confirmer la nouvelle configuration.

2.12. ACTIVATION DES TRANSFERTS DE ZONE DANS L'INTERFACE DE GESTION DE L'IDM

Cette section explique comment activer les transferts de zone dans la gestion des identités (IdM) à l'aide de l'interface de ligne de commande (CLI) de l'IdM.

Conditions préalables

- Vous êtes connecté en tant qu'administrateur IdM.
- Vous disposez d'un accès root aux serveurs DNS secondaires.

Procédure

- Pour activer les transferts de zone dans le service **BIND**, entrez la commande **ipa dnszone-mod** et indiquez la liste des serveurs de noms situés en dehors de la zone à transférer vers lesquels les enregistrements de zone seront transférés à l'aide de l'option **--allow-transfer**. Par exemple :

```
$ ipa dnszone-mod --allow-transfer=192.0.2.1;198.51.100.1;203.0.113.1
idm.example.com
```

Verification steps

1. SSH à l'un des serveurs DNS pour lesquels le transfert de zone a été activé :

```
$ ssh 192.0.2.1
```

2. Transférer la zone DNS IdM à l'aide d'un outil tel que l'utilitaire **dig**:

```
# dig @ipa-server zone_name AXFR
```

Si la commande ne renvoie aucune erreur, vous avez activé avec succès le transfert de zone pour *zone_name*.

2.13. RESSOURCES SUPPLÉMENTAIRES

- Voir Utilisation des playbooks Ansible pour gérer les zones DNS de l'IdM .

CHAPITRE 3. UTILISER LES PLAYBOOKS ANSIBLE POUR GÉRER LES ZONES DNS DE L'IDM

En tant qu'administrateur Identity Management (IdM), vous pouvez gérer le fonctionnement des zones DNS IdM à l'aide du module **dnszone** disponible dans le package **ansible-freeipa**. Ce chapitre décrit les sujets et procédures suivants :

- Quels sont les types de zones DNS pris en charge par IdM ?
- Quels sont les attributs DNS que vous pouvez configurer dans IdM ?
- Comment utiliser un playbook Ansible pour créer une zone primaire dans IdM DNS
- Comment utiliser un playbook Ansible pour s'assurer de la présence d'une zone DNS IdM primaire avec plusieurs variables
- Comment utiliser un playbook Ansible pour s'assurer de la présence d'une zone pour la recherche DNS inversée lorsqu'une adresse IP est donnée ?

Conditions préalables

- Le service DNS est installé sur le serveur IdM. Pour plus d'informations sur l'utilisation de Red Hat Ansible Engine pour installer un serveur IdM avec DNS intégré, voir Installation d'un serveur de gestion d'identité à l'aide d'un playbook Ansible.

3.1. TYPES DE ZONES DNS PRISES EN CHARGE

Identity Management (IdM) prend en charge deux types de zones DNS : les zones *primary* et *forward*. Cette section décrit ces deux types de zones et inclut un exemple de scénario de transfert DNS.

NOTE

Ce guide utilise la terminologie BIND pour les types de zones, qui est différente de la terminologie utilisée pour le DNS de Microsoft Windows. Les zones primaires dans BIND ont la même fonction que *forward lookup zones* et *reverse lookup zones* dans le DNS de Microsoft Windows. Les zones de transfert dans BIND ont la même fonction que *conditional forwarders* dans le DNS de Microsoft Windows.

Zones DNS primaires

Les zones DNS primaires contiennent des données DNS faisant autorité et peuvent accepter des mises à jour DNS dynamiques. Ce comportement est équivalent au paramètre **type master** dans la configuration standard de BIND. Vous pouvez gérer les zones primaires à l'aide des commandes **ipa dnszone-***.
Conformément aux règles DNS standard, chaque zone primaire doit contenir des enregistrements **start of authority** (SOA) et **nameserver** (NS). L'IdM génère automatiquement ces enregistrements lors de la création de la zone DNS, mais vous devez copier manuellement les enregistrements NS dans la zone mère pour créer une délégation correcte.

Conformément au comportement standard de BIND, les requêtes portant sur des noms pour lesquels le serveur ne fait pas autorité sont transmises à d'autres serveurs DNS. Ces serveurs DNS, appelés "forwarders", peuvent ou non faire autorité pour la requête.

Exemple 3.1. Exemple de scénario pour le transfert DNS

> Le serveur IdM contient la zone primaire **test.example.**. Cette zone contient un enregistrement de délégation NS pour le nom **sub.test.example.**. En outre, la zone **test.example.** est configurée avec l'adresse IP du transitaire **192.0.2.254** pour la sous-zone **sub.text.example**.
>
> Un client interrogeant le nom **nonexistent.test.example.** reçoit la réponse **NXDomain** et aucun transfert n'a lieu car le serveur IdM fait autorité pour ce nom.
>
> D'autre part, les requêtes portant sur le nom **host1.sub.test.example.** sont transmises au transitaire configuré **192.0.2.254**, car le serveur IdM ne fait pas autorité pour ce nom.

Transférer des zones DNS

Du point de vue de l'IdM, les zones DNS avancées ne contiennent aucune donnée faisant autorité. En fait, une "zone" avancée ne contient généralement que deux éléments d'information :

- Un nom de domaine
- L'adresse IP d'un serveur DNS associé au domaine

Toutes les requêtes portant sur des noms appartenant au domaine défini sont transmises à l'adresse IP spécifiée. Ce comportement est équivalent au paramètre **type forward** dans la configuration standard de BIND. Vous pouvez gérer les zones de transfert à l'aide des commandes **ipa dnsforwardzone-***.

Les zones DNS à suivre sont particulièrement utiles dans le contexte des trusts IdM-Active Directory (AD). Si le serveur DNS IdM fait autorité pour la zone **idm.example.com** et que le serveur DNS AD fait autorité pour la zone **ad.example.com**, alors **ad.example.com** est une zone DNS de renvoi pour la zone primaire **idm.example.com**. Cela signifie que lorsqu'un client IdM demande l'adresse IP de **somehost.ad.example.com**, la requête est transmise à un contrôleur de domaine AD spécifié dans la zone de transfert DNS IdM **ad.example.com**.

3.2. ATTRIBUTS DE CONFIGURATION DES ZONES DNS PRIMAIRES DE L'IDM

Identity Management (IdM) crée une nouvelle zone avec certaines configurations par défaut, telles que les périodes de rafraîchissement, les paramètres de transfert ou les paramètres de cache. Dans les attributs de la zone DNS IdM , vous trouverez les attributs de la configuration de la zone par défaut que vous pouvez modifier à l'aide de l'une des options suivantes :

- La commande **dnszone-mod** dans l'interface de ligne de commande (CLI). Pour plus d'informations, voir Modifier la configuration d'une zone DNS primaire dans l'interface CLI de l'IdM.
- L'interface Web IdM. Pour plus d'informations, voir Modifier la configuration d'une zone DNS primaire dans l'interface Web IdM.
- Un playbook Ansible qui utilise le module **ipadnszone**. Pour plus d'informations, voir Gestion des zones DNS dans IdM.

Outre les informations relatives à la zone, les paramètres définissent la manière dont le serveur DNS traite les entrées de l'enregistrement *start of authority* (SOA) et la manière dont il met à jour ses enregistrements à partir du serveur de noms DNS.

Tableau 3.1. Attributs de la zone DNS de l'IdM

Attribut	variable ansible-freeipa	Description
Serveur de noms faisant autorité	**name_server**	Définit le nom de domaine du serveur de noms DNS primaire, également connu sous le nom de SOA MNAME. Par défaut, chaque serveur IdM s'annonce lui-même dans le champ SOA MNAME. Par conséquent, la valeur stockée dans LDAP à l'aide de **--name-server** est ignorée.
Adresse électronique de l'administrateur	**admin_email**	Définit l'adresse électronique à utiliser pour l'administrateur de zone. Par défaut, il s'agit du compte root de l'hôte.
Série SOA	**serial**	Définit un numéro de série dans l'enregistrement SOA. Notez que l'IdM définit automatiquement le numéro de version et que les utilisateurs ne sont pas censés le modifier.
Actualisation de l'AOS	**refresh**	Définit l'intervalle, en secondes, pendant lequel un serveur DNS secondaire doit attendre avant de demander des mises à jour au serveur DNS primaire.
Réessai SOA	**retry**	Définit le délai, en secondes, à attendre avant de réessayer une opération de rafraîchissement qui a échoué.
SOA expirer	**expire**	Définit la durée, en secondes, pendant laquelle un serveur DNS secondaire tentera d'effectuer une mise à jour avant de mettre fin à la tentative d'opération.
Minimum SOA	**minimum**	Définit la valeur TTL (time to live) en secondes pour la mise en cache négative conformément à la RFC 2308.
Délai de mise en œuvre de la SOA	**ttl**	Définit le TTL en secondes pour les enregistrements à l'apex de la zone. Dans la zone **example.com**, par exemple, tous les enregistrements (A, NS ou SOA) sous le nom **example.com** sont configurés, mais aucun autre nom de domaine, comme **test.example.com**, n'est affecté.
Durée de vie par défaut	**default_ttl**	Définit la valeur par défaut du TTL (Time to Live) en secondes pour la mise en cache négative de toutes les valeurs d'une zone qui n'ont jamais eu de valeur TTL individuelle définie auparavant. Nécessite un redémarrage du service **named-pkcs11** sur tous les serveurs DNS IdM pour que les modifications soient prises en compte.
Politique de mise à jour de BIND	**update_policy**	Définit les autorisations accordées aux clients dans la zone DNS.

Attribut	variable ansible-freeipa	Description
Mise à jour dynamique	**dynamic_update**=VRAI|FAUX	Active les mises à jour dynamiques des enregistrements DNS pour les clients. Notez que si cette valeur est fixée à false, les machines clientes IdM ne pourront pas ajouter ou mettre à jour leur adresse IP.
Autoriser le transfert	**allow_transfer**=*string*	Donne une liste d'adresses IP ou de noms de réseau autorisés à transférer la zone donnée, séparés par des points-virgules (;). Les transferts de zone sont désactivés par défaut. La valeur par défaut de **allow_transfer** est **none**.
Autoriser l'interrogation	**allow_query**	Donne une liste d'adresses IP ou de noms de réseau autorisés à émettre des requêtes DNS, séparés par des points-virgules (;).
Autoriser la synchronisation PTR	**allow_sync_ptr**=1|0	Définit si les enregistrements A ou AAAA (enregistrements directs) de la zone seront automatiquement synchronisés avec les enregistrements PTR (enregistrements inversés).
Transitaires de zone	**forwarder**=*IP_address*	Spécifie un transitaire spécifiquement configuré pour la zone DNS. Ce transitaire est distinct des transitaires globaux utilisés dans le domaine IdM. Pour spécifier plusieurs transitaires, utilisez l'option plusieurs fois.
Politique prévisionnelle	**forward_policy**=unique|uniquement|premier	Spécifie la politique de transfert. Pour plus d'informations sur les politiques prises en charge, voir Politiques de transfert DNS dans IdM.

Ressources supplémentaires

- Voir le fichier **README-dnszone.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.

3.3. UTILISER ANSIBLE POUR CRÉER UNE ZONE PRIMAIRE DANS IDM DNS

Cette section montre comment un administrateur Identity Management (IdM) peut utiliser un playbook Ansible pour s'assurer de l'existence d'une zone DNS primaire. Dans l'exemple utilisé dans la procédure ci-dessous, un administrateur IdM s'assure de la présence de la zone DNS **zone.idm.example.com**.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.

  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.

- Vous connaissez le mot de passe de l'administrateur IdM.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnszone**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnszone
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **dnszone-present.yml** Ansible playbook. Par exemple :

```
$ cp dnszone-present.yml dnszone-present-copy.yml
```

4. Ouvrez le fichier **dnszone-present-copy.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes dans la section **ipadnszone** task :
   - Définissez la variable **ipaadmin_password** avec votre mot de passe d'administrateur IdM.
   - Fixer la variable **zone_name** à **zone.idm.example.com**.
     Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Ensure dnszone present
  hosts: ipaserver
  become: true

  tasks:
  - name: Ensure zone is present.
    ipadnszone:
      ipaadmin_password: "{{ ipaadmin_password }}"
      zone_name: zone.idm.example.com
      state: present
```

6. Enregistrer le fichier.
7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file dnszone-present-copy.yml
```

Ressources supplémentaires

- Voir Types de zones DNS pris en charge .
- Voir le fichier **README-dnszone.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir les exemples de playbooks Ansible dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnszone**.

3.4. UTILISATION D'UN PLAYBOOK ANSIBLE POUR ASSURER LA PRÉSENCE D'UNE ZONE DNS PRIMAIRE DANS L'IDM AVEC PLUSIEURS VARIABLES

Cette section montre comment un administrateur Identity Management (IdM) peut utiliser un playbook Ansible pour s'assurer de l'existence d'une zone DNS primaire. Dans l'exemple utilisé dans la procédure ci-dessous, un administrateur IdM s'assure de la présence de la zone DNS **zone.idm.example.com**. Le playbook Ansible configure plusieurs paramètres de la zone.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous connaissez le mot de passe de l'administrateur IdM.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnszone**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnszone
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **dnszone-all-params.yml** Ansible playbook. Par exemple :

```
$ cp dnszone-all-params.yml dnszone-all-params-copy.yml
```

4. Ouvrez le fichier **dnszone-all-params-copy.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes dans la section **ipadnszone** task :

- Définissez la variable **ipaadmin_password** avec votre mot de passe d'administrateur IdM.
- Fixer la variable **zone_name** à **zone.idm.example.com**.
- Attribuez la valeur true à la variable **allow_sync_ptr** si vous souhaitez autoriser la synchronisation des enregistrements en aval et en amont, c'est-à-dire la synchronisation des enregistrements A et AAAA avec les enregistrements PTR.
- Définissez la variable **dynamic_update** sur true pour permettre aux machines clientes IdM d'ajouter ou de mettre à jour leurs adresses IP.
- Attribuez la valeur true à la variable **dnssec** pour permettre la signature DNSSEC en ligne des enregistrements dans la zone.
- Définissez la variable **allow_transfer** avec les adresses IP des serveurs de noms secondaires de la zone.
- Définissez la variable **allow_query** en fonction des adresses IP ou des réseaux autorisés à émettre des requêtes.
- Définissez la variable **forwarders** avec les adresses IP des transitaires globaux.
- Attribuer à la variable **serial** le numéro de série de l'enregistrement SOA.
- Définissez les valeurs **refresh**, **retry**, **expire**, **minimum**, **ttl**, et **default_ttl** pour les enregistrements DNS de la zone.
- Définir l'enregistrement NSEC3PARAM pour la zone en utilisant la variable **nsec3param_rec**.
- Définissez la variable **skip_overlap_check** sur true pour forcer la création d'un DNS même s'il chevauche une zone existante.
- Attribuez la valeur true à **skip_nameserver_check** pour forcer la création d'une zone DNS même si le serveur de noms n'est pas résolvable.
  Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Ensure dnszone present
 hosts: ipaserver
 become: true

 tasks:
 - name: Ensure zone is present.
   ipadnszone:
     ipaadmin_password: "{{ ipaadmin_password }}"
     zone_name: zone.idm.example.com
     allow_sync_ptr: true
     dynamic_update: true
     dnssec: true
     allow_transfer:
       - 1.1.1.1
       - 2.2.2.2
     allow_query:
       - 1.1.1.1
       - 2.2.2.2
     forwarders:
```

```
    - ip_address: 8.8.8.8
    - ip_address: 8.8.4.4
      port: 52
  serial: 1234
  refresh: 3600
  retry: 900
  expire: 1209600
  minimum: 3600
  ttl: 60
  default_ttl: 90
  name_server: server.idm.example.com.
  admin_email: admin.admin@idm.example.com
  nsec3param_rec: "1 7 100 0123456789abcdef"
  skip_overlap_check: true
  skip_nameserver_check: true
  state: present
```

6. Enregistrer le fichier.

7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file dnszone-all-params-copy.yml
```

Ressources supplémentaires

- Voir Types de zones DNS pris en charge .
- Voir Attributs de configuration des zones DNS primaires de l'IdM .
- Voir le fichier **README-dnszone.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir les exemples de playbooks Ansible dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnszone**.

3.5. UTILISATION D'UN PLAYBOOK ANSIBLE POUR S'ASSURER DE LA PRÉSENCE D'UNE ZONE POUR LA RECHERCHE DNS INVERSÉE LORSQU'UNE ADRESSE IP EST DONNÉE

Cette section montre comment un administrateur Identity Management (IdM) peut utiliser un playbook Ansible pour s'assurer de l'existence d'une zone DNS inversée. Dans l'exemple utilisé dans la procédure ci-dessous, un administrateur IdM s'assure de la présence d'une zone de recherche DNS inverse en utilisant l'adresse IP et la longueur du préfixe d'un hôte IdM.

En indiquant la longueur du préfixe de l'adresse IP de votre serveur DNS à l'aide de la variable **name_from_ip**, vous pouvez contrôler le nom de la zone. Si vous n'indiquez pas la longueur du préfixe, le système interroge les serveurs DNS sur les zones et, en fonction de la valeur **name_from_ip** de **192.168.1.2**, la requête peut renvoyer n'importe laquelle des zones DNS suivantes :

- **1.168.192.in-addr.arpa.**
- **168.192.in-addr.arpa.**
- **192.in-addr.arpa.**

Étant donné que la zone renvoyée par la requête peut ne pas correspondre à ce que vous attendez, **name_from_ip** ne peut être utilisé qu'avec l'option **state** réglée sur **present** afin d'éviter les suppressions accidentelles de zones.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous connaissez le mot de passe de l'administrateur IdM.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnszone**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnszone
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **dnszone-reverse-from-ip.yml** Ansible playbook. Par exemple :

```
$ cp dnszone-reverse-from-ip.yml dnszone-reverse-from-ip-copy.yml
```

4. Ouvrez le fichier **dnszone-reverse-from-ip-copy.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes dans la section **ipadnszone** task :
   - Définissez la variable **ipaadmin_password** avec votre mot de passe d'administrateur IdM.
   - Définissez la variable **name_from_ip** avec l'IP de votre serveur de noms IdM et indiquez la longueur de son préfixe.
     Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Ensure dnszone present
  hosts: ipaserver
  become: true

  tasks:
  - name: Ensure zone for reverse DNS lookup is present.
```

```
  ipadnszone:
    ipaadmin_password: "{{ ipaadmin_password }}"
    name_from_ip: 192.168.1.2/24
    state: present
  register: result
- name: Display inferred zone name.
  debug:
    msg: "Zone name: {{ result.dnszone.name }}"
```

Le playbook crée une zone pour la recherche DNS inversée à partir de l'adresse IP **192.168.1.2** et de sa longueur de préfixe de 24. Ensuite, le playbook affiche le nom de la zone résultante.

6. Enregistrer le fichier.
7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file dnszone-reverse-from-ip-copy.yml
```

Ressources supplémentaires

- Voir Types de zones DNS pris en charge .
- Voir le fichier **README-dnszone.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir les exemples de playbooks Ansible dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnszone**.

CHAPITRE 4. GESTION DES EMPLACEMENTS DNS DANS L'IDM

En tant qu'administrateur de la gestion des identités (IdM), vous pouvez gérer les emplacements DNS de la gestion des identités (IdM) à l'aide de l'interface Web IdM et de l'interface de ligne de commande IdM (CLI). Ce chapitre décrit les sujets et procédures suivants :

- Découverte de services basée sur le DNS
- Considérations relatives au déploiement des sites DNS
- Durée de vie du DNS (TTL)
- Création d'emplacements DNS à l'aide de l'interface Web IdM
- Création d'emplacements DNS à l'aide de la CLI IdM
- Attribution d'un serveur IdM à un emplacement DNS à l'aide de l'interface Web IdM
- Attribution d'un serveur IdM à un emplacement DNS à l'aide de l'interface Web IdM
- Configuration d'un client IdM pour utiliser des serveurs IdM situés au même endroit

4.1. DÉCOUVERTE DE SERVICES BASÉE SUR LE DNS

La découverte de services basée sur le DNS est un processus dans lequel un client utilise le protocole DNS pour localiser les serveurs d'un réseau qui offrent un service spécifique, tel que **LDAP** ou **Kerberos**. Un type d'opération typique consiste à permettre aux clients de localiser les serveurs d'authentification dans l'infrastructure réseau la plus proche, parce qu'ils offrent un débit plus élevé et une latence de réseau plus faible, ce qui réduit les coûts globaux.

Les principaux avantages de la découverte de services sont les suivants

- Il n'est pas nécessaire de configurer explicitement les clients avec les noms des serveurs proches.
- Les serveurs DNS sont utilisés comme fournisseurs centraux de politiques. Les clients qui utilisent le même serveur DNS ont accès à la même politique concernant les fournisseurs de services et leur ordre préférentiel.

Dans un domaine de gestion d'identité (IdM), il existe des enregistrements de service DNS (enregistrements SRV) pour **LDAP**, **Kerberos** et d'autres services. Par exemple, la commande suivante interroge le serveur DNS sur les hôtes fournissant un service **Kerberos** basé sur TCP dans un domaine DNS IdM :

Exemple 4.1. Résultats indépendants de l'emplacement du DNS

```
$ dig -t SRV +short _kerberos._tcp.idm.example.com
0 100 88 idmserver-01.idm.example.com.
0 100 88 idmserver-02.idm.example.com.
```

La sortie contient les informations suivantes :

- **0** (priorité) : Priorité de l'hôte cible. Une valeur inférieure est préférable.

- **100** (poids). Spécifie un poids relatif pour les entrées ayant la même priorité. Pour plus d'informations, voir RFC 2782, section 3.
- **88** (numéro de port) : Numéro de port du service.
- Nom canonique de l'hôte fournissant le service.

Dans l'exemple, les deux noms d'hôte renvoyés ont la même priorité et le même poids. Dans ce cas, le client utilise une entrée aléatoire de la liste des résultats.

Lorsque le client est configuré pour interroger un serveur DNS configuré dans un emplacement DNS, le résultat est différent. Pour les serveurs IdM qui sont affectés à un emplacement, des valeurs adaptées sont renvoyées. Dans l'exemple ci-dessous, le client est configuré pour interroger un serveur DNS dans l'emplacement **germany**:

Exemple 4.2. Résultats basés sur la localisation DNS

```
$ dig -t SRV +short _kerberos._tcp.idm.example.com
_kerberos._tcp.germany._locations.idm.example.com.
0 100 88 idmserver-01.idm.example.com.
50 100 88 idmserver-02.idm.example.com.
```

Le serveur DNS IdM renvoie automatiquement un alias DNS (CNAME) pointant vers un enregistrement SRV spécifique à l'emplacement DNS qui privilégie les serveurs locaux. Cet enregistrement CNAME est indiqué sur la première ligne de la sortie. Dans l'exemple, l'hôte **idmserver-01.idm.example.com** a la valeur de priorité la plus basse et est donc préféré. L'hôte **idmserver-02.idm.example.com** a une priorité plus élevée et n'est donc utilisé qu'en cas de sauvegarde, lorsque l'hôte préféré n'est pas disponible.

4.2. CONSIDÉRATIONS RELATIVES AU DÉPLOIEMENT DES SITES DNS

Identity Management (IdM) peut générer des enregistrements de service spécifiques à un emplacement (SRV) lors de l'utilisation du DNS intégré. Comme chaque serveur DNS IdM génère des enregistrements SRV spécifiques à l'emplacement, vous devez installer au moins un serveur DNS IdM dans chaque emplacement DNS.

L'affinité du client avec un emplacement DNS n'est définie que par les enregistrements DNS reçus par le client. C'est pourquoi vous pouvez combiner des serveurs DNS IdM avec des serveurs consommateurs et des récursoires DNS non IdM si les clients qui découvrent le service DNS résolvent les enregistrements spécifiques à l'emplacement à partir des serveurs DNS IdM.

Dans la majorité des déploiements avec des services DNS IdM et non IdM mixtes, les récursoires DNS sélectionnent automatiquement le serveur DNS IdM le plus proche en utilisant des mesures de temps d'aller-retour. En règle générale, cela garantit que les clients utilisant des serveurs DNS non IdM obtiennent des enregistrements pour l'emplacement DNS le plus proche et utilisent donc l'ensemble optimal de serveurs IdM.

4.3. DURÉE DE VIE DU DNS (TTL)

Les clients peuvent mettre en cache les enregistrements de ressources DNS pendant une durée définie dans la configuration de la zone. En raison de cette mise en cache, un client peut ne pas être en mesure de recevoir les modifications avant l'expiration de la valeur TTL (time to live). La valeur TTL par défaut

dans Identity Management (IdM) est **1 day**.

Si les ordinateurs de vos clients se déplacent d'un site à l'autre, vous devez adapter la valeur TTL de votre zone DNS IdM. Définissez une valeur inférieure au temps nécessaire aux clients pour se déplacer d'un site à l'autre. Cela garantit que les entrées DNS mises en cache sur le client expirent avant qu'il ne se reconnecte à un autre site et n'interroge le serveur DNS pour actualiser les enregistrements SRV spécifiques à l'emplacement.

Ressources supplémentaires

- Voir Attributs de configuration des zones DNS primaires de l'IdM .

4.4. CRÉATION D'EMPLACEMENTS DNS À L'AIDE DE L'INTERFACE WEB IDM

Vous pouvez utiliser les emplacements DNS pour augmenter la vitesse de communication entre les clients et les serveurs de gestion d'identité (IdM). Cette section décrit comment créer un emplacement DNS à l'aide de l'interface Web IdM.

Conditions préalables

- Votre déploiement IdM dispose d'un DNS intégré.
- Vous avez la permission de créer des emplacements DNS dans IdM. Par exemple, vous êtes connecté en tant qu'administrateur IdM.

Procédure

1. Ouvrez l'onglet **IPA Server**.
2. Sélectionnez le sous-onglet **Topology**.
3. Cliquez sur **IPA Locations** dans la barre de navigation.
4. Cliquez sur **Ajouter** en haut de la liste des lieux.
5. Complétez le nom de l'emplacement.
6. Cliquez sur le bouton **Ajouter** pour enregistrer l'emplacement.
7. Facultatif : Répétez les étapes pour ajouter d'autres lieux.

Ressources supplémentaires

- Voir Affectation d'un serveur IdM à un emplacement DNS à l'aide de l'interface Web IdM .
- Voir Utiliser Ansible pour s'assurer qu'un emplacement IdM est présent .

4.5. CRÉATION D'EMPLACEMENTS DNS À L'AIDE DE LA CLI IDM

Vous pouvez utiliser les emplacements DNS pour augmenter la vitesse de communication entre les clients et les serveurs de gestion d'identité (IdM). Cette section explique comment créer des emplacements DNS à l'aide de la commande **ipa location-add** dans l'interface de ligne de commande (CLI) de l'IdM.

Conditions préalables

- Votre déploiement IdM dispose d'un DNS intégré.
- Vous avez la permission de créer des emplacements DNS dans IdM. Par exemple, vous êtes connecté en tant qu'administrateur IdM.

Procédure

1. Par exemple, pour créer un nouvel emplacement **germany**, entrez :

```
$ ipa location-add germany
----------------------------
Added IPA location "germany"
----------------------------
  Location name: germany
```

2. Facultatif : Répétez l'étape pour ajouter d'autres lieux.

Ressources supplémentaires

- Voir Affectation d'un serveur IdM à un emplacement DNS à l'aide de la CLI IdM .
- Voir Utiliser Ansible pour s'assurer qu'un emplacement IdM est présent .

4.6. ATTRIBUTION D'UN SERVEUR IDM À UN EMPLACEMENT DNS À L'AIDE DE L'INTERFACE WEB IDM

Vous pouvez utiliser les emplacements DNS de la gestion d'identité (IdM) pour augmenter la vitesse de communication entre les clients et les serveurs IdM. Cette section explique comment affecter des serveurs IdM à des emplacements DNS à l'aide de l'interface Web IdM.

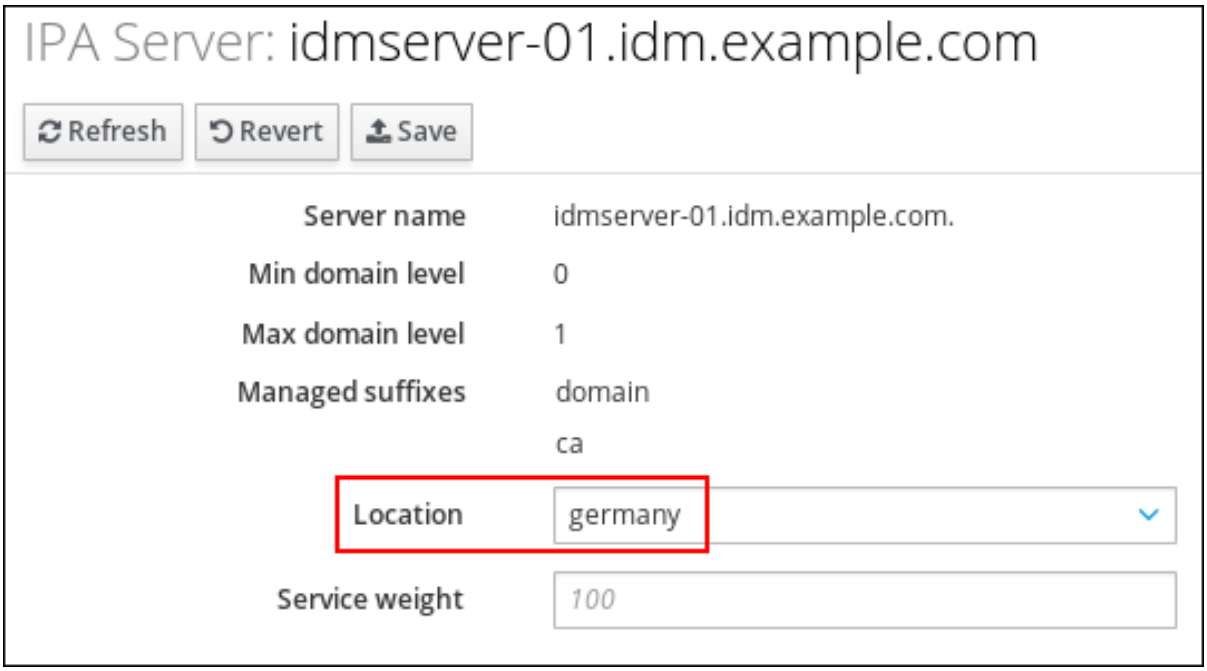
Conditions préalables

- Votre déploiement IdM dispose d'un DNS intégré.
- Vous êtes connecté en tant qu'utilisateur ayant le droit d'assigner un serveur à un emplacement DNS, par exemple l'utilisateur IdM admin.
- Vous disposez d'un accès **root** à l'hôte auquel vous souhaitez attribuer un emplacement DNS.
- Vous avez créé les emplacements DNS IdM auxquels vous voulez assigner des serveurs.

Procédure

1. Ouvrez l'onglet **IPA Server**.
2. Sélectionnez le sous-onglet **Topology**.
3. Cliquez sur **IPA Servers** dans la navigation.
4. Cliquez sur le nom du serveur IdM.
5. Sélectionnez un emplacement DNS et définissez éventuellement un poids de service :

Figure 4.1. Attribution d'un serveur à un emplacement DNS



6. Cliquez sur **Enregistrer**.

7. Dans l'interface de ligne de commande (CLI) de l'hôte auquel vous avez attribué l'emplacement DNS dans les étapes précédentes, redémarrez le service **named-pkcs11**:

```
[root@idmserver-01 ~]# systemctl restart named-pkcs11
```

8. Facultatif : Répétez les étapes pour attribuer des emplacements DNS à d'autres serveurs IdM.

Ressources supplémentaires

- Voir Configuration d'un client IdM pour utiliser des serveurs IdM situés au même endroit .

4.7. ATTRIBUTION D'UN SERVEUR IDM À UN EMPLACEMENT DNS À L'AIDE DE LA CLI IDM

Vous pouvez utiliser les emplacements DNS de la gestion d'identité (IdM) pour augmenter la vitesse de communication entre les clients et les serveurs IdM. Cette section explique comment affecter des serveurs IdM à des emplacements DNS à l'aide de l'interface de ligne de commande (CLI) IdM.

Conditions préalables

- Votre déploiement IdM dispose d'un DNS intégré.
- Vous êtes connecté en tant qu'utilisateur ayant le droit d'assigner un serveur à un emplacement DNS, par exemple l'utilisateur IdM admin.
- Vous disposez d'un accès **root** à l'hôte auquel vous souhaitez attribuer un emplacement DNS.
- Vous avez créé les emplacements DNS IdM auxquels vous voulez assigner des serveurs.

Procédure

1. Optionnel : Liste de tous les emplacements DNS configurés :

```
[root@server ~]# ipa location-find
-----------------------
2 IPA locations matched
-----------------------
Location name: australia
Location name: germany
----------------------------
Number of entries returned: 2
----------------------------
```

2. Attribuez le serveur à l'emplacement DNS. Par exemple, pour attribuer l'emplacement **germany** au serveur **idmserver-01.idm.example.com**, exécutez :

```
# ipa server-mod idmserver-01.idm.example.com --location=germany
ipa: WARNING: Service named-pkcs11.service requires restart on IPA server
idmserver-01.idm.example.com to apply configuration changes.
-----------------------------------------------
Modified IPA server "idmserver-01.idm.example.com"
-----------------------------------------------
Servername: idmserver-01.idm.example.com
Min domain level: 0
Max domain level: 1
Location: germany
Enabled server roles: DNS server, NTP server
```

3. Redémarrez le service **named-pkcs11** sur l'hôte auquel vous avez attribué l'emplacement DNS dans les étapes précédentes :

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

4. Facultatif : Répétez les étapes pour attribuer des emplacements DNS à d'autres serveurs IdM.

Ressources supplémentaires

- Voir Configuration d'un client IdM pour utiliser des serveurs IdM situés au même endroit .

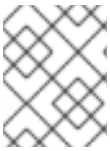
4.8. CONFIGURATION D'UN CLIENT IDM POUR UTILISER DES SERVEURS IDM SITUÉS AU MÊME ENDROIT

Les serveurs de gestion des identités (IdM) sont affectés à des emplacements DNS comme décrit dans la section Affectation d'un serveur IdM à un emplacement DNS à l'aide de l'interface Web IdM . Vous pouvez maintenant configurer les clients pour qu'ils utilisent un serveur DNS situé au même endroit que les serveurs IdM :

- Si un serveur **DHCP** attribue les adresses IP du serveur DNS aux clients, configurez le service **DHCP**. Pour plus de détails sur l'attribution d'un serveur DNS dans votre service **DHCP**, voir la documentation du service **DHCP**.

- Si vos clients ne reçoivent pas les adresses IP des serveurs DNS d'un serveur **DHCP**, définissez manuellement les adresses IP dans la configuration du réseau du client. Pour plus de détails sur la configuration du réseau sous Red Hat Enterprise Linux, reportez-vous à la section

Configuration des paramètres de connexion au réseau dans le Guide d'installation de Red Hat Enterprise Linux *Red Hat Enterprise Linux Networking Guide* .



NOTE

Si vous configurez le client pour qu'il utilise un serveur DNS assigné à un autre emplacement, le client contacte les serveurs IdM des deux emplacements.

Exemple 4.3. Différentes entrées du serveur de noms en fonction de l'emplacement du client

L'exemple suivant montre différentes entrées de serveur de noms dans le fichier **/etc/resolv.conf** pour des clients situés à différents endroits :

Clients à Prague :

```
nameserver 10.10.0.1
nameserver 10.10.0.2
```

Clients à Paris :

```
nameserver 10.50.0.1
nameserver 10.50.0.3
```

Clients à Oslo :

```
serveur de noms 10.30.0.1
```

Clients à Berlin :

```
serveur de noms 10.30.0.1
```

Si chacun des serveurs DNS est affecté à un emplacement dans IdM, les clients utilisent les serveurs IdM de leur emplacement.

4.9. RESSOURCES SUPPLÉMENTAIRES

- Voir Utiliser Ansible pour gérer les emplacements DNS dans IdM .

CHAPITRE 5. UTILISER ANSIBLE POUR GÉRER LES EMPLACEMENTS DNS DANS IDM

En tant qu'administrateur Identity Management (IdM), vous pouvez gérer les emplacements DNS IdM à l'aide du module **location** disponible dans le package **ansible-freeipa**. Ce chapitre décrit les sujets et procédures suivants :

- Découverte de services basée sur le DNS
- Considérations relatives au déploiement des sites DNS
- Durée de vie du DNS (TTL)
- Utiliser Ansible pour s'assurer qu'un emplacement IdM est présent
- Utiliser Ansible pour s'assurer qu'un emplacement IdM est absent

5.1. DÉCOUVERTE DE SERVICES BASÉE SUR LE DNS

La découverte de services basée sur le DNS est un processus dans lequel un client utilise le protocole DNS pour localiser les serveurs d'un réseau qui offrent un service spécifique, tel que **LDAP** ou **Kerberos**. Un type d'opération typique consiste à permettre aux clients de localiser les serveurs d'authentification dans l'infrastructure réseau la plus proche, parce qu'ils offrent un débit plus élevé et une latence de réseau plus faible, ce qui réduit les coûts globaux.

Les principaux avantages de la découverte de services sont les suivants

- Il n'est pas nécessaire de configurer explicitement les clients avec les noms des serveurs proches.
- Les serveurs DNS sont utilisés comme fournisseurs centraux de politiques. Les clients qui utilisent le même serveur DNS ont accès à la même politique concernant les fournisseurs de services et leur ordre préférentiel.

Dans un domaine de gestion d'identité (IdM), il existe des enregistrements de service DNS (enregistrements SRV) pour **LDAP**, **Kerberos** et d'autres services. Par exemple, la commande suivante interroge le serveur DNS sur les hôtes fournissant un service **Kerberos** basé sur TCP dans un domaine DNS IdM :

Exemple 5.1. Résultats indépendants de l'emplacement du DNS

```
$ dig -t SRV +short _kerberos._tcp.idm.example.com
0 100 88 idmserver-01.idm.example.com.
0 100 88 idmserver-02.idm.example.com.
```

La sortie contient les informations suivantes :

- **0** (priorité) : Priorité de l'hôte cible. Une valeur inférieure est préférable.
- **100** (poids). Spécifie un poids relatif pour les entrées ayant la même priorité. Pour plus d'informations, voir RFC 2782, section 3.
- **88** (numéro de port) : Numéro de port du service.
- Nom canonique de l'hôte fournissant le service.

Dans l'exemple, les deux noms d'hôte renvoyés ont la même priorité et le même poids. Dans ce cas, le client utilise une entrée aléatoire de la liste des résultats.

Lorsque le client est configuré pour interroger un serveur DNS configuré dans un emplacement DNS, le résultat est différent. Pour les serveurs IdM qui sont affectés à un emplacement, des valeurs adaptées sont renvoyées. Dans l'exemple ci-dessous, le client est configuré pour interroger un serveur DNS dans l'emplacement **germany**:

Exemple 5.2. Résultats basés sur la localisation DNS

```
$ dig -t SRV +short _kerberos._tcp.idm.example.com
_kerberos._tcp.germany._locations.idm.example.com.
0 100 88 idmserver-01.idm.example.com.
50 100 88 idmserver-02.idm.example.com.
```

Le serveur DNS IdM renvoie automatiquement un alias DNS (CNAME) pointant vers un enregistrement SRV spécifique à l'emplacement DNS qui privilégie les serveurs locaux. Cet enregistrement CNAME est indiqué sur la première ligne de la sortie. Dans l'exemple, l'hôte **idmserver-01.idm.example.com** a la valeur de priorité la plus basse et est donc préféré. L'hôte **idmserver-02.idm.example.com** a une priorité plus élevée et n'est donc utilisé qu'en cas de sauvegarde, lorsque l'hôte préféré n'est pas disponible.

5.2. CONSIDÉRATIONS RELATIVES AU DÉPLOIEMENT DES SITES DNS

Identity Management (IdM) peut générer des enregistrements de service spécifiques à un emplacement (SRV) lors de l'utilisation du DNS intégré. Comme chaque serveur DNS IdM génère des enregistrements SRV spécifiques à l'emplacement, vous devez installer au moins un serveur DNS IdM dans chaque emplacement DNS.

L'affinité du client avec un emplacement DNS n'est définie que par les enregistrements DNS reçus par le client. C'est pourquoi vous pouvez combiner des serveurs DNS IdM avec des serveurs consommateurs et des récursoires DNS non IdM si les clients qui découvrent le service DNS résolvent les enregistrements spécifiques à l'emplacement à partir des serveurs DNS IdM.

Dans la majorité des déploiements avec des services DNS IdM et non IdM mixtes, les récursoires DNS sélectionnent automatiquement le serveur DNS IdM le plus proche en utilisant des mesures de temps d'aller-retour. En règle générale, cela garantit que les clients utilisant des serveurs DNS non IdM obtiennent des enregistrements pour l'emplacement DNS le plus proche et utilisent donc l'ensemble optimal de serveurs IdM.

5.3. DURÉE DE VIE DU DNS (TTL)

Les clients peuvent mettre en cache les enregistrements de ressources DNS pendant une durée définie dans la configuration de la zone. En raison de cette mise en cache, un client peut ne pas être en mesure de recevoir les modifications avant l'expiration de la valeur TTL (time to live). La valeur TTL par défaut dans Identity Management (IdM) est **1 day**.

Si les ordinateurs de vos clients se déplacent d'un site à l'autre, vous devez adapter la valeur TTL de votre zone DNS IdM. Définissez une valeur inférieure au temps nécessaire aux clients pour se déplacer d'un site à l'autre. Cela garantit que les entrées DNS mises en cache sur le client expirent avant qu'il ne se reconnecte à un autre site et n'interroge le serveur DNS pour actualiser les enregistrements SRV spécifiques à l'emplacement.

Ressources supplémentaires

- Voir Attributs de configuration des zones DNS primaires de l'IdM .

5.4. UTILISER ANSIBLE POUR S'ASSURER QU'UN EMPLACEMENT IDM EST PRÉSENT

En tant qu'administrateur système de la gestion des identités (IdM), vous pouvez configurer les emplacements DNS IdM pour permettre aux clients de localiser les serveurs d'authentification dans l'infrastructure réseau la plus proche.

La procédure suivante décrit comment utiliser un playbook Ansible pour s'assurer qu'un emplacement DNS est présent dans IdM. L'exemple décrit comment s'assurer que l'emplacement DNS **germany** est présent dans IdM. En conséquence, vous pouvez assigner des serveurs IdM particuliers à cet emplacement afin que les clients IdM locaux puissent les utiliser pour réduire le temps de réponse du serveur.

Conditions préalables

- Vous connaissez le mot de passe de l'administrateur IdM.
- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous comprenez les considérations relatives au déploiement des sites DNS .

Procédure

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

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

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

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/location/location-present.yml location-present-copy.yml
```

3. Ouvrez le fichier **location-present-copy.yml** Ansible playbook pour l'éditer.
4. Adaptez le fichier en définissant les variables suivantes dans la section **ipalocation** task :
   - Adaptez le site **name** de la tâche pour qu'il corresponde à votre cas d'utilisation.
   - Définissez la variable **ipaadmin_password** avec le mot de passe de l'administrateur IdM.

- Définissez la variable **name** avec le nom de l'emplacement.

Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: location present example
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Ensure that the "germany" location is present
    ipalocation:
      ipaadmin_password: "{{ ipaadmin_password }}"
      name: germany
```

5. Enregistrer le fichier.

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

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory location-present-copy.yml
```

Ressources supplémentaires

- Voir Affectation d'un serveur IdM à un emplacement DNS à l'aide de l'interface Web Id M ou Affectation d'un serveur IdM à un emplacement DNS à l'aide de l'interface CLI IdM .

5.5. UTILISER ANSIBLE POUR S'ASSURER QU'UN EMPLACEMENT IDM EST ABSENT

En tant qu'administrateur système de la gestion des identités (IdM), vous pouvez configurer les emplacements DNS IdM pour permettre aux clients de localiser les serveurs d'authentification dans l'infrastructure réseau la plus proche.

La procédure suivante décrit comment utiliser un playbook Ansible pour s'assurer qu'un emplacement DNS est absent de l'IdM. L'exemple décrit comment s'assurer que l'emplacement DNS **germany** est absent de l'IdM. Par conséquent, vous ne pouvez pas attribuer de serveurs IdM particuliers à cet emplacement et les clients IdM locaux ne peuvent pas les utiliser.

Conditions préalables

- Vous connaissez le mot de passe de l'administrateur IdM.
- Aucun serveur IdM n'est assigné à l'emplacement DNS **germany**.
- 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**.

- L'exemple suppose que vous avez créé et configuré le répertoire ***~/MyPlaybooks/*** en tant qu'emplacement central pour stocker les copies des exemples de playbooks.

Procédure

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

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

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

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/location/location-absent.yml location-absent-copy.yml
```

3. Ouvrez le fichier **location-absent-copy.yml** Ansible playbook pour l'éditer.
4. Adaptez le fichier en définissant les variables suivantes dans la section **ipalocation** task :
   - Adaptez le site **name** de la tâche pour qu'il corresponde à votre cas d'utilisation.
   - Définissez la variable **ipaadmin_password** avec le mot de passe de l'administrateur IdM.
   - Définissez la variable **name** avec le nom de l'emplacement DNS.
   - Assurez-vous que la variable **state** est fixée à **absent**.

   Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: location absent example
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Ensure that the "germany" location is absent
    ipalocation:
      ipaadmin_password: "{{ ipaadmin_password }}"
      name: germany
      state: absent
```

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

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory location-absent-copy.yml
```

5.6. RESSOURCES SUPPLÉMENTAIRES

- Voir le fichier **README-location.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir les exemples de playbooks Ansible dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/location**.

CHAPITRE 6. GESTION DE LA REDIRECTION DNS DANS L'IDM

Les procédures suivantes décrivent comment configurer les forwarders globaux DNS et les zones de forward DNS dans l'interface Web de gestion des identités (IdM), dans la CLI IdM et à l'aide d'Ansible :

- Les deux rôles d'un serveur DNS IdM
- Politiques de transfert DNS dans l'IdM
- Ajout d'un transitaire global dans l'interface Web IdM
- Ajout d'un transitaire global dans l'interface de gestion
- Ajout d'une zone de transfert DNS dans l'interface Web IdM
- Ajout d'une zone de transfert DNS dans l'interface de programmation
- Mise en place d'un DNS Global Forwarder dans IdM à l'aide d'Ansible
- Assurer la présence d'un DNS global forwarder dans IdM en utilisant Ansible
- S'assurer de l'absence d'un DNS global forwarder dans l'IdM en utilisant Ansible
- S'assurer que les DNS Global Forwarders sont désactivés dans IdM à l'aide d'Ansible
- Assurer la présence d'une zone de transfert DNS dans IdM en utilisant Ansible
- S'assurer qu'une zone de transfert DNS a plusieurs transitaires dans IdM à l'aide d'Ansible
- S'assurer qu'une zone de transfert DNS est désactivée dans l'IdM à l'aide d'Ansible
- Garantir l'absence d'une zone de transfert DNS dans l'IdM à l'aide d'Ansible

6.1. LES DEUX RÔLES D'UN SERVEUR DNS IDM

La redirection DNS affecte la manière dont un service DNS répond aux requêtes DNS. Par défaut, le service Berkeley Internet Name Domain (BIND) intégré à l'IdM fait office de serveur DNS *authoritative* et *recursive*:

Serveur DNS autoritaire

Lorsqu'un client DNS interroge un nom appartenant à une zone DNS pour laquelle le serveur IdM fait autorité, BIND répond avec les données contenues dans la zone configurée. Les données faisant autorité ont toujours la priorité sur les autres données.

Serveur DNS récursif

Lorsqu'un client DNS interroge un nom pour lequel le serveur IdM ne fait pas autorité, BIND tente de résoudre la requête en utilisant d'autres serveurs DNS. Si les forwarders ne sont pas définis, BIND interroge les serveurs racine sur Internet et utilise un algorithme de résolution récursif pour répondre à la requête DNS.

Dans certains cas, il n'est pas souhaitable de laisser BIND contacter directement d'autres serveurs DNS et d'effectuer la récursivité sur la base des données disponibles sur Internet. Vous pouvez configurer BIND pour qu'il utilise un autre serveur DNS, *forwarder*, pour résoudre la requête.

Lorsque vous configurez BIND pour utiliser un transitaire, les requêtes et les réponses sont transmises entre le serveur IdM et le transitaire, et le serveur IdM fait office de cache DNS pour les données ne faisant pas autorité.

6.2. POLITIQUES DE TRANSFERT DNS DANS L'IDM

IdM prend en charge les politiques d'acheminement standard de BIND **first** et **only**, ainsi que la politique d'acheminement spécifique à IdM **none**.

En avant, d'abord *(default)*

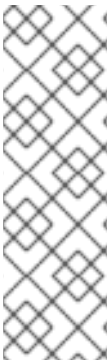
Le service BIND de l'IdM transmet les requêtes DNS au transitaire configuré. Si une requête échoue en raison d'une erreur de serveur ou d'un dépassement de délai, BIND se rabat sur la résolution récursive en utilisant des serveurs sur l'internet. La politique **forward first** est la politique par défaut et convient pour optimiser le trafic DNS.

En avant seulement

Le service IdM BIND transmet les requêtes DNS au transitaire configuré. Si une requête échoue en raison d'une erreur du serveur ou d'un dépassement de délai, BIND renvoie une erreur au client. La stratégie **forward only** est recommandée pour les environnements avec une configuration DNS divisée.

Aucun *(forwarding disabled)*

Les requêtes DNS ne sont pas transférées avec la politique de transfert **none**. La désactivation de la redirection n'est utile que pour remplacer la configuration globale de la redirection dans une zone spécifique. Cette option est l'équivalent pour IdM de la spécification d'une liste vide de transitaires dans la configuration de BIND.



NOTE

Vous ne pouvez pas utiliser le transfert pour combiner des données dans IdM avec des données provenant d'autres serveurs DNS. Vous ne pouvez transférer des requêtes que pour des sous-zones spécifiques de la zone primaire dans le DNS IdM.

Par défaut, le service BIND ne transmet pas les requêtes à un autre serveur si le nom DNS demandé appartient à une zone pour laquelle le serveur IdM fait autorité. Dans une telle situation, si le nom DNS demandé ne peut être trouvé dans la base de données IdM, la réponse **NXDOMAIN** est renvoyée. Le transfert n'est pas utilisé.

Exemple 6.1. Exemple de scénario

Le serveur IdM fait autorité pour la zone DNS **test.example.**. BIND est configuré pour transmettre les requêtes au serveur DNS avec l'adresse IP **192.0.2.254**.

Lorsqu'un client envoie une requête pour le nom DNS **nonexistent.test.example.**, BIND détecte que le serveur IdM fait autorité pour la zone **test.example.** et ne transmet pas la requête au serveur **192.0.2.254.**. En conséquence, le client DNS reçoit le message d'erreur **NXDomain**, informant l'utilisateur que le domaine interrogé n'existe pas.

6.3. AJOUT D'UN TRANSITAIRE GLOBAL DANS L'INTERFACE WEB IDM

Cette section décrit comment ajouter un transitaire DNS global dans l'interface utilisateur Web de la gestion des identités (IdM).

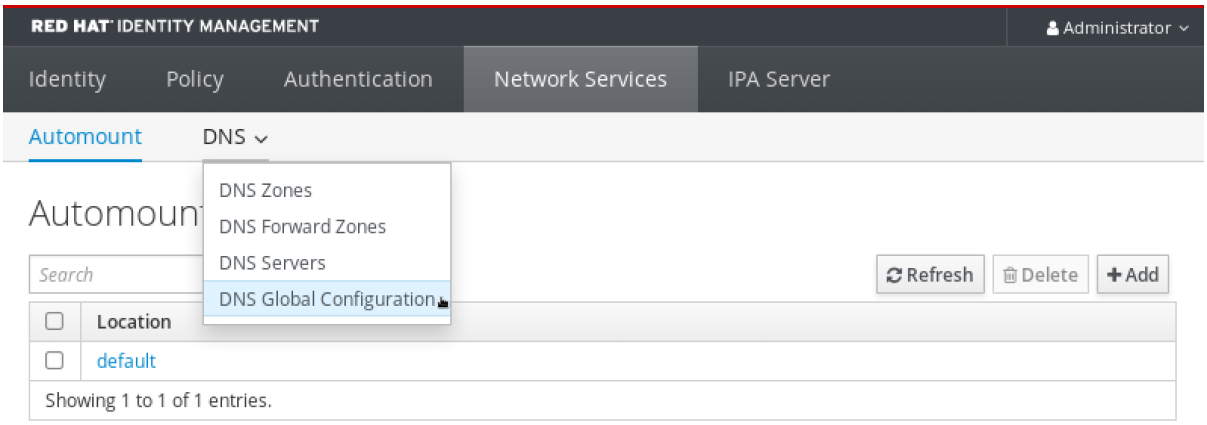
Conditions préalables

Conditions préalables

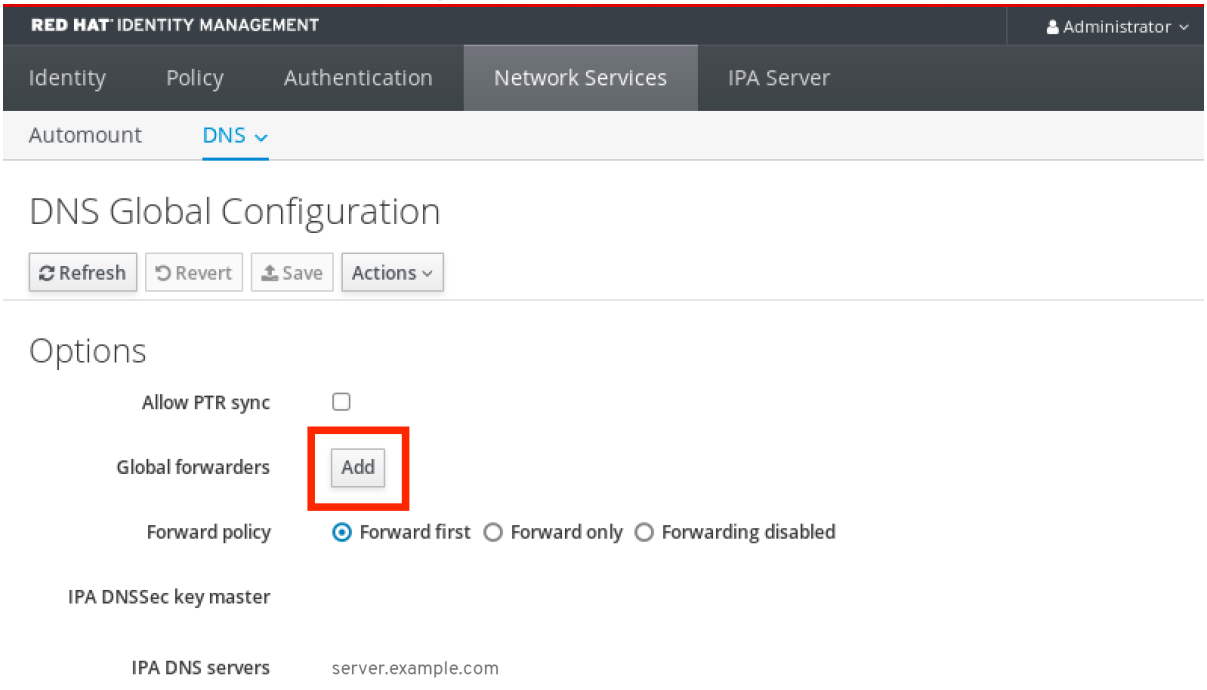
- Vous êtes connecté à l'interface Web de l'IdM en tant qu'administrateur de l'IdM.
- Vous connaissez l'adresse IP (Internet Protocol) du serveur DNS vers lequel transférer les requêtes.

Procédure

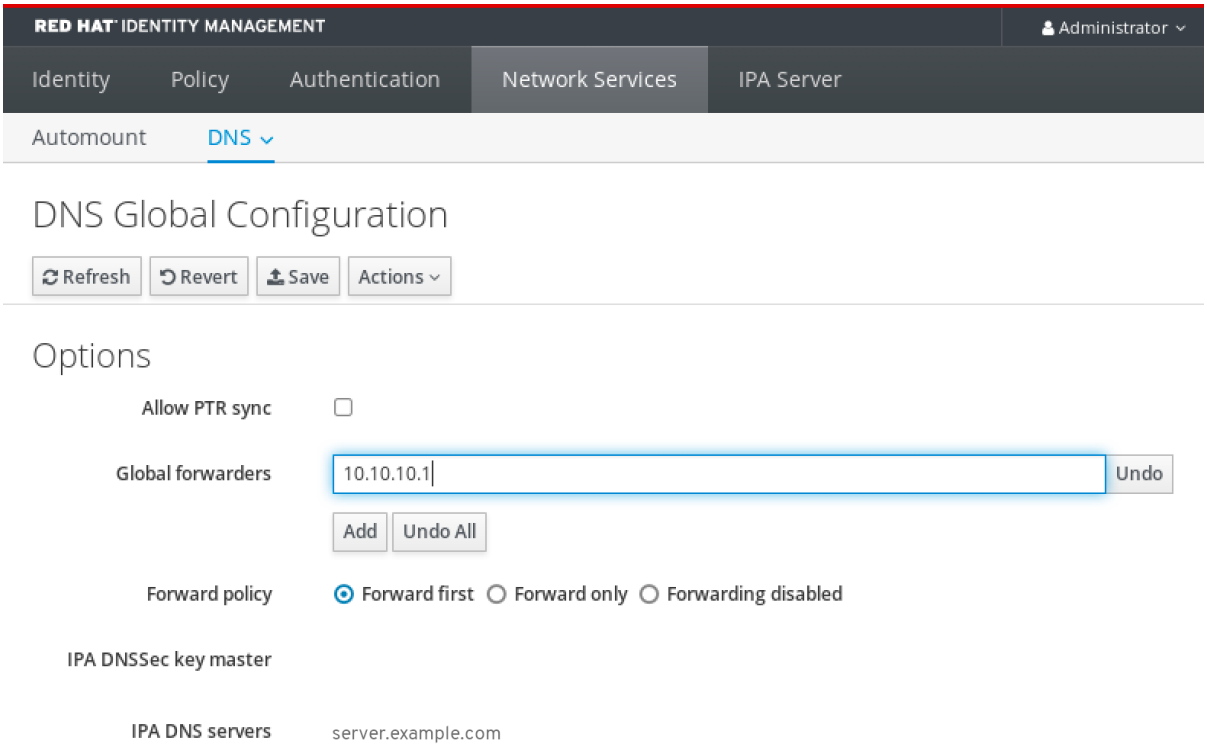
1. Dans l'interface Web IdM, sélectionnez **Network Services → DNS Global Configuration → DNS**.



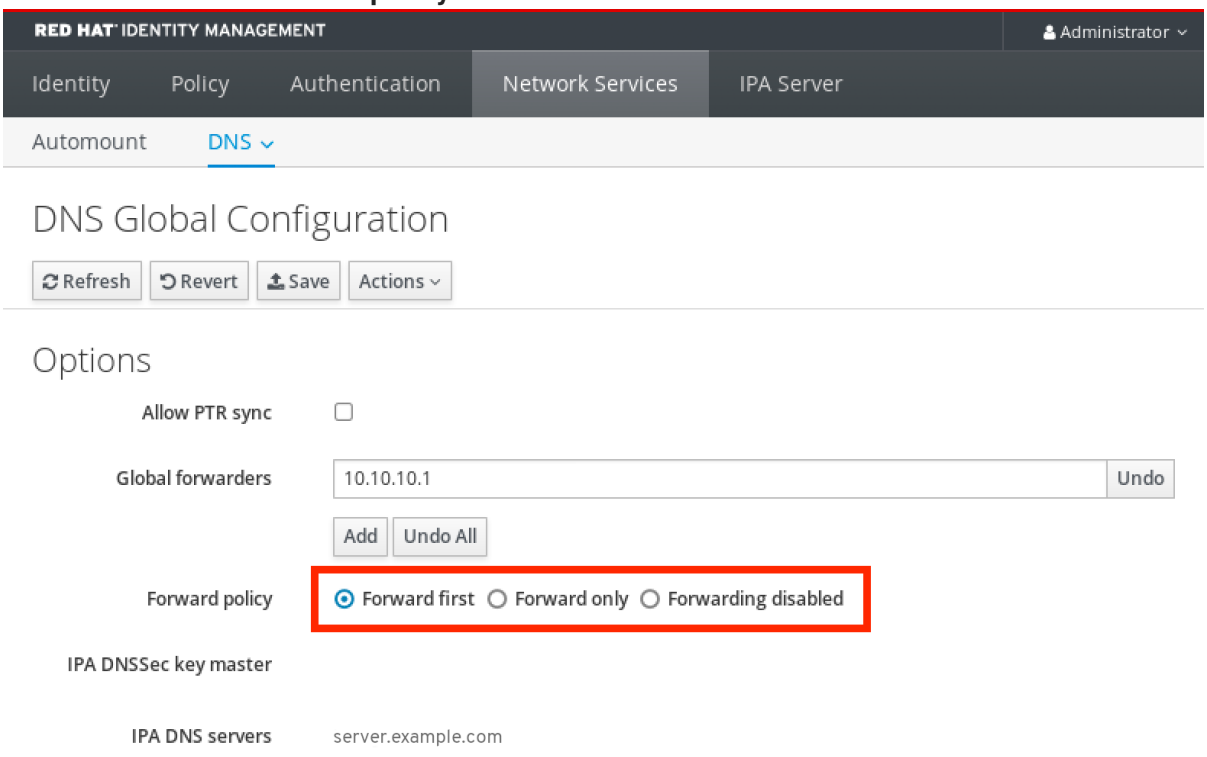
2. Dans la section **DNS Global Configuration**, cliquez sur **Add**.



3. Spécifiez l'adresse IP du serveur DNS qui recevra les requêtes DNS transférées.



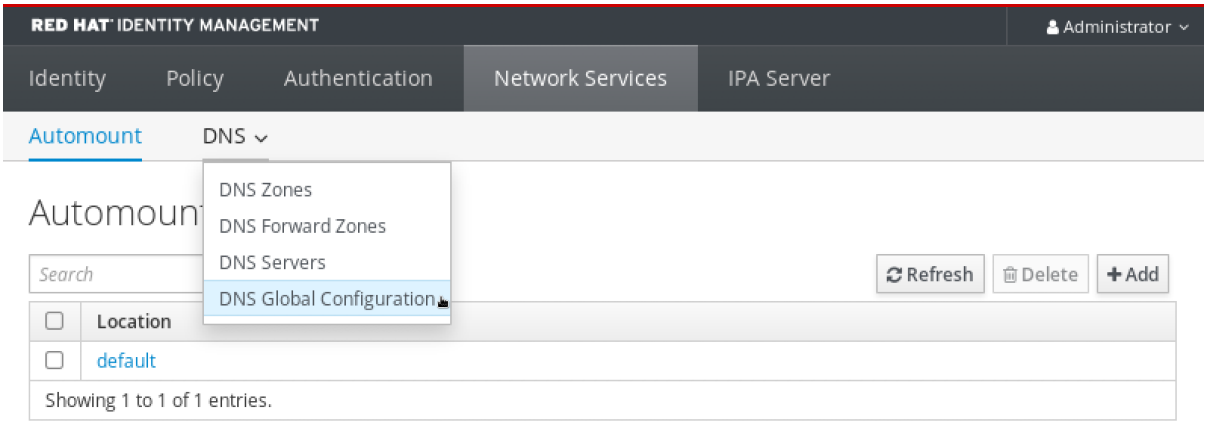
4. Sélectionnez le site **Forward policy**.



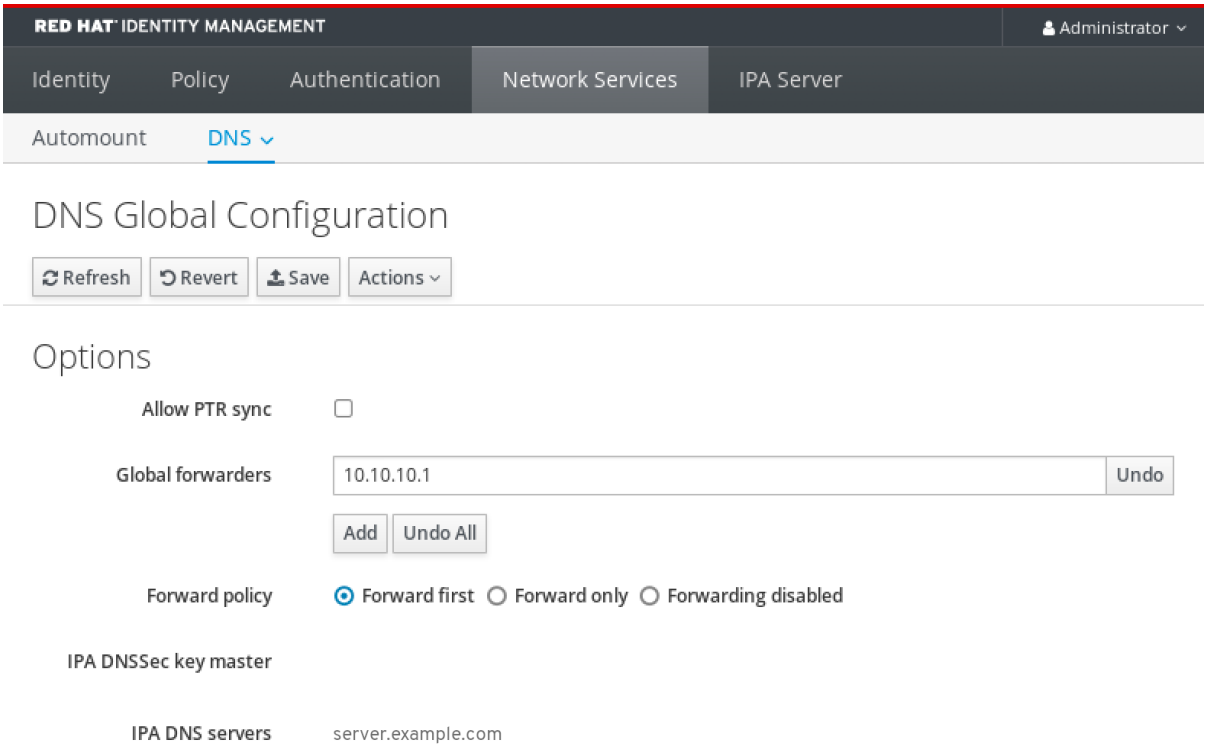
5. Cliquez sur **Save** en haut de la fenêtre.

Verification steps

1. Sélectionnez **Network Services → DNS Global Configuration → DNS**.



2. Vérifiez que le transitaire global, avec la politique de transfert que vous avez spécifiée, est présent et activé dans l'interface utilisateur Web IdM.



6.4. AJOUT D'UN TRANSITAIRE GLOBAL DANS L'INTERFACE DE GESTION

Cette section décrit comment ajouter un transitaire DNS global à partir de l'interface de ligne de commande (CLI).

Conditions préalables

- Vous êtes connecté en tant qu'administrateur IdM.
- Vous connaissez l'adresse IP (Internet Protocol) du serveur DNS vers lequel transférer les requêtes.

Procédure

- Utilisez la commande **ipa dnsconfig-mod** pour ajouter un nouveau transitaire global. Spécifiez l'adresse IP du transitaire DNS avec l'option **--forwarder**.

```
[user@server ~]$ ipa dnsconfig-mod --forwarder=10.10.0.1
Server will check DNS forwarder(s).
This may take some time, please wait ...
  Global forwarders: 10.10.0.1
  IPA DNS servers: server.example.com
```

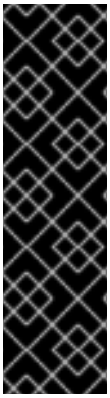
Verification steps

- Utilisez la commande **dnsconfig-show** pour afficher les transitaires globaux.

```
[user@server ~]$ ipa dnsconfig-show
  Global forwarders: 10.10.0.1
  IPA DNS servers: server.example.com
```

6.5. AJOUT D'UNE ZONE DE TRANSFERT DNS DANS L'INTERFACE WEB IDM

Cette section décrit comment ajouter une zone de transfert DNS dans l'interface utilisateur Web de la gestion des identités (IdM).



IMPORTANT

N'utilisez pas de zones de transmission, sauf en cas d'absolue nécessité. Les zones de transfert ne constituent pas une solution standard et leur utilisation peut entraîner un comportement inattendu et problématique. Si vous devez utiliser des zones de transfert, limitez leur utilisation à l'annulation d'une configuration de transfert globale.

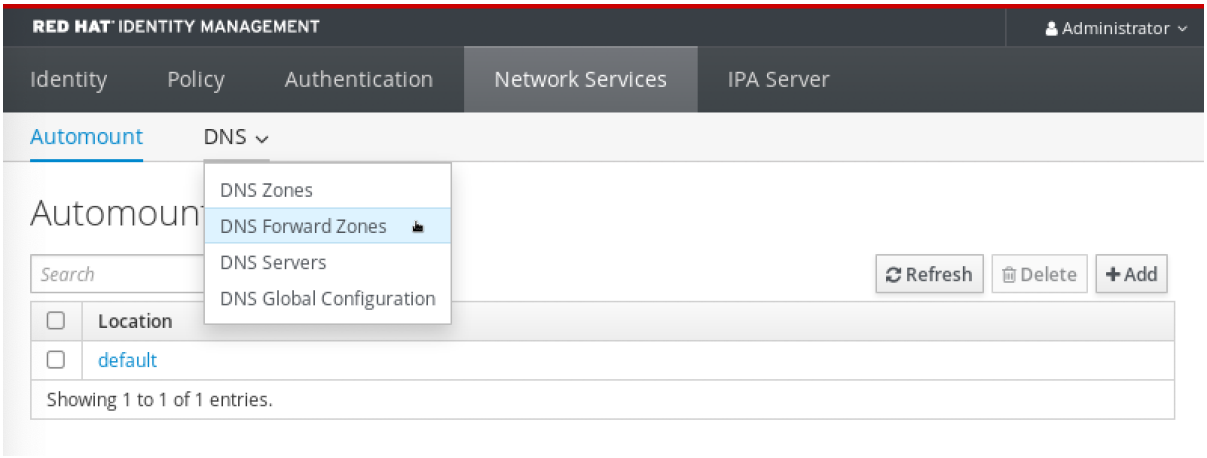
Lors de la création d'une nouvelle zone DNS, Red Hat recommande de toujours utiliser la délégation DNS standard à l'aide d'enregistrements de serveurs de noms (NS) et d'éviter les zones de transfert. Dans la plupart des cas, l'utilisation d'un transitaire global est suffisante et les zones de transfert ne sont pas nécessaires.

Conditions préalables

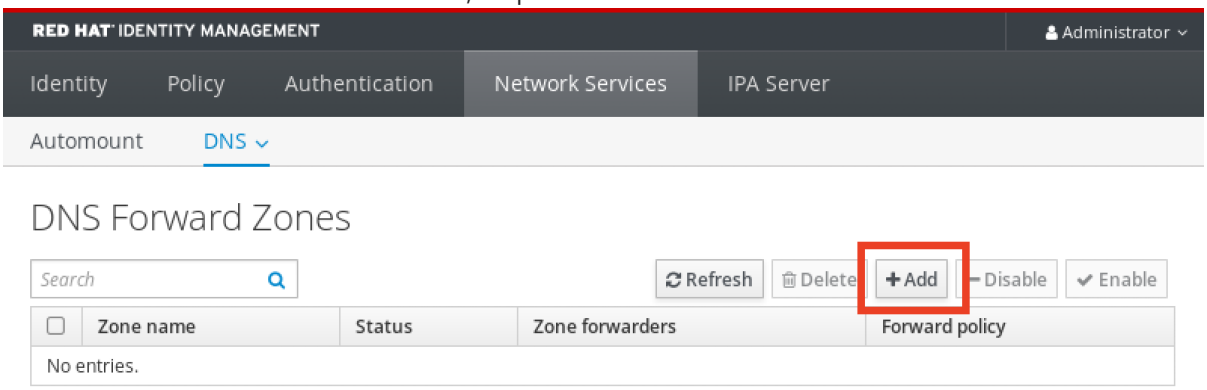
- Vous êtes connecté à l'interface Web de l'IdM en tant qu'administrateur de l'IdM.
- Vous connaissez l'adresse IP (Internet Protocol) du serveur DNS vers lequel transférer les requêtes.

Procédure

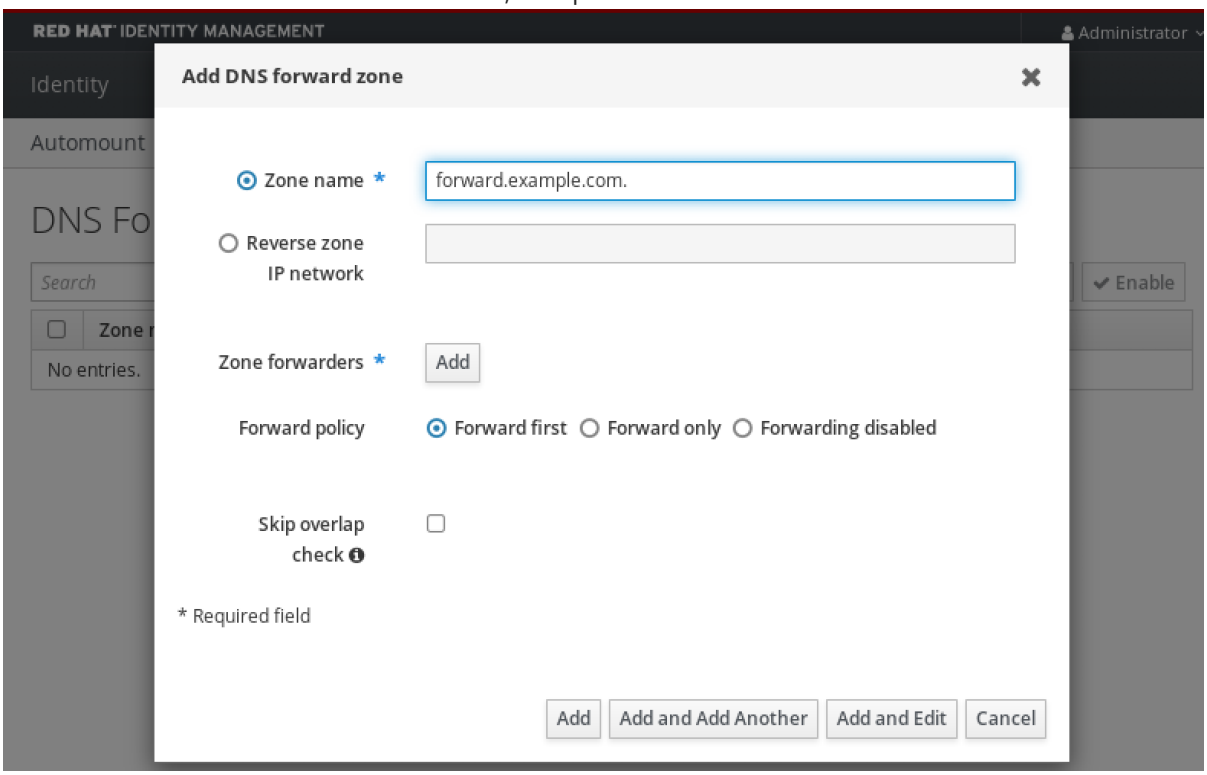
1. Dans l'interface Web IdM, sélectionnez **Network Services → DNS Forward Zones → DNS**.



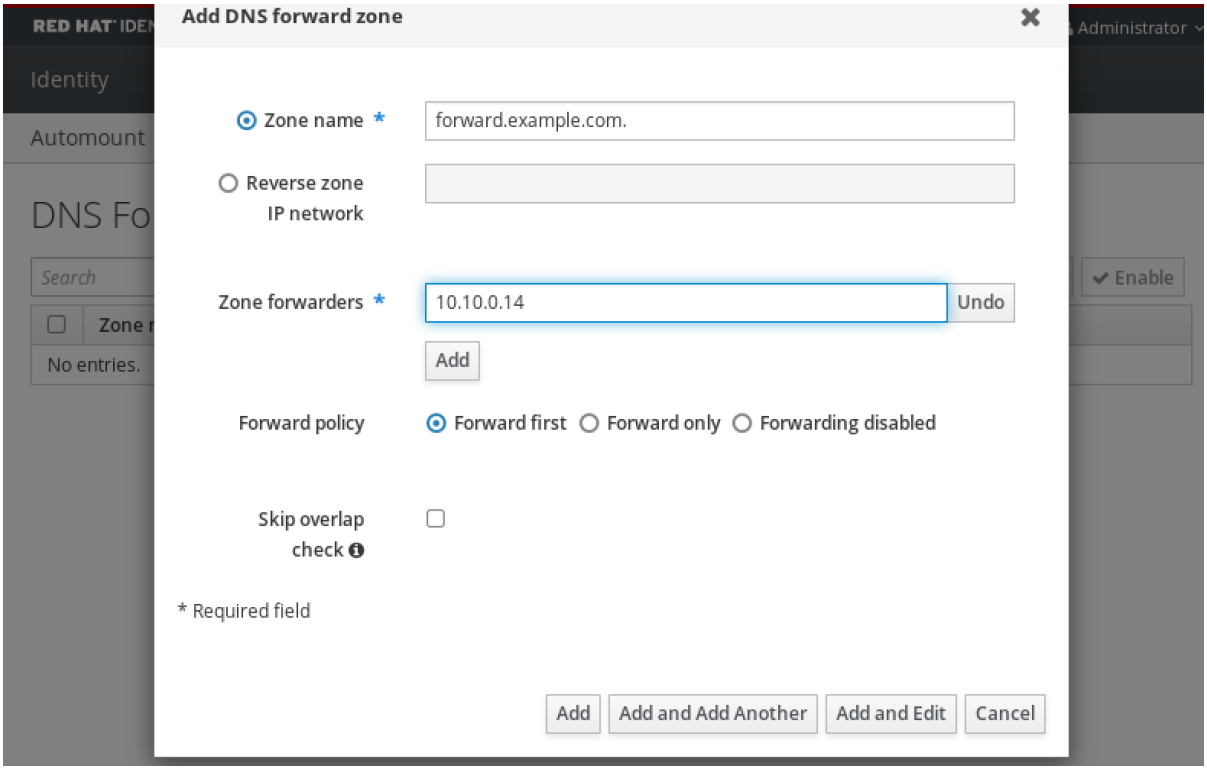
2. Dans la section **DNS Forward Zones**, cliquez sur **Add**.



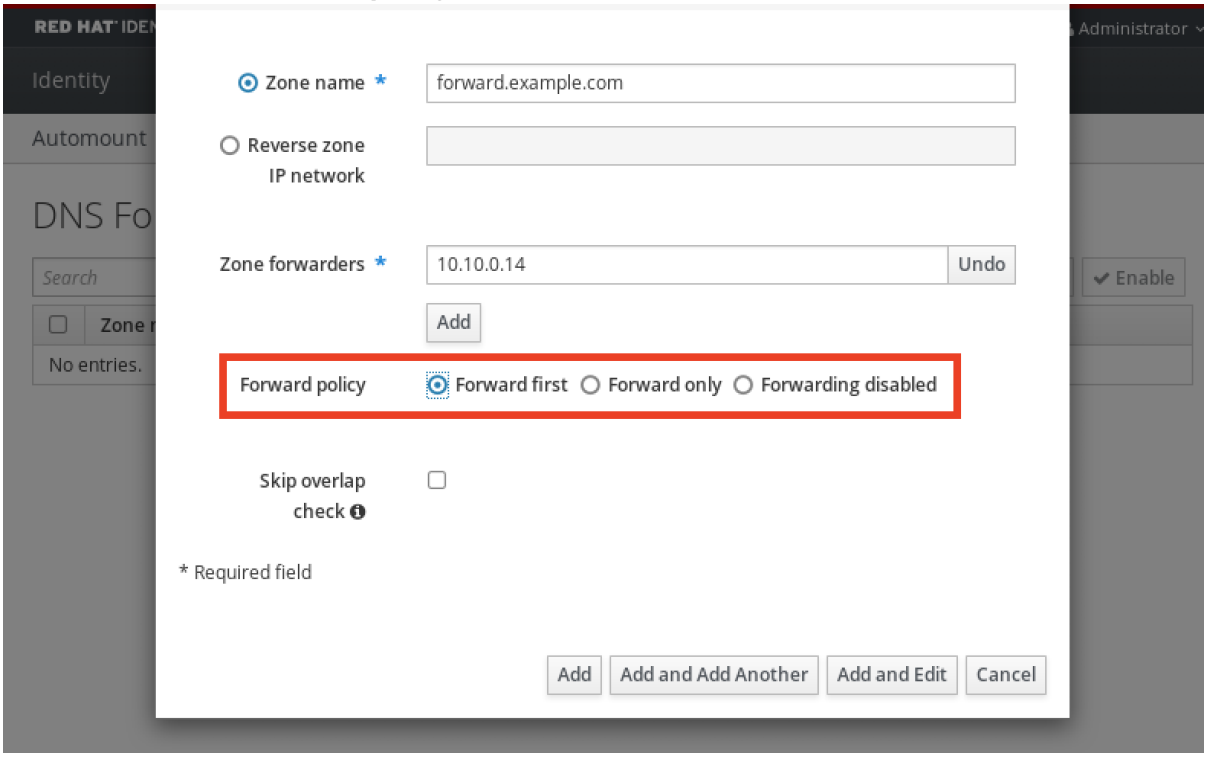
3. Dans la fenêtre **Add DNS forward zone**, indiquez le nom de la zone de transfert.



4. Cliquez sur le bouton **Add** et indiquez l'adresse IP d'un serveur DNS qui recevra la demande de transfert. Vous pouvez spécifier plusieurs serveurs de transfert par zone de transfert.



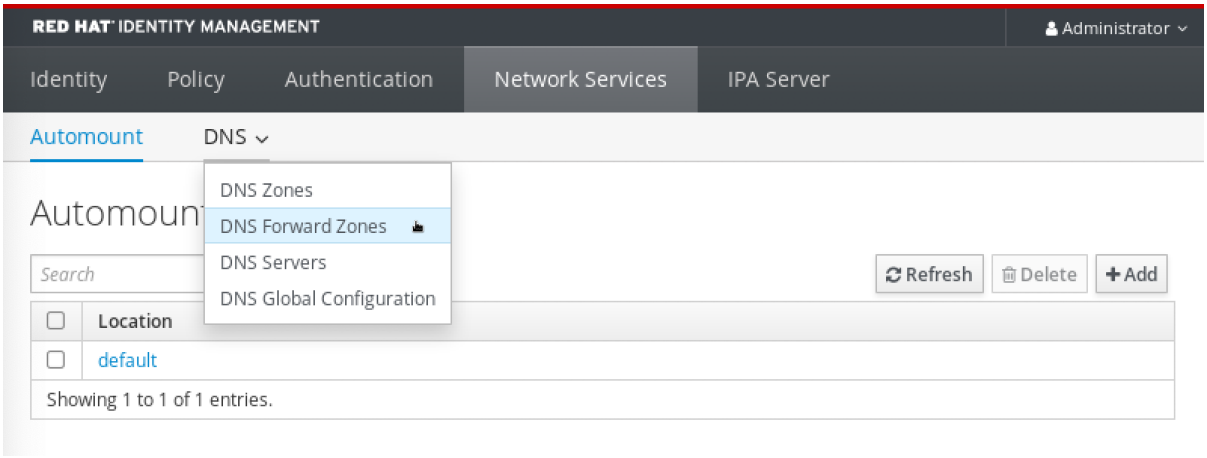
5. Sélectionnez le site **Forward policy**.



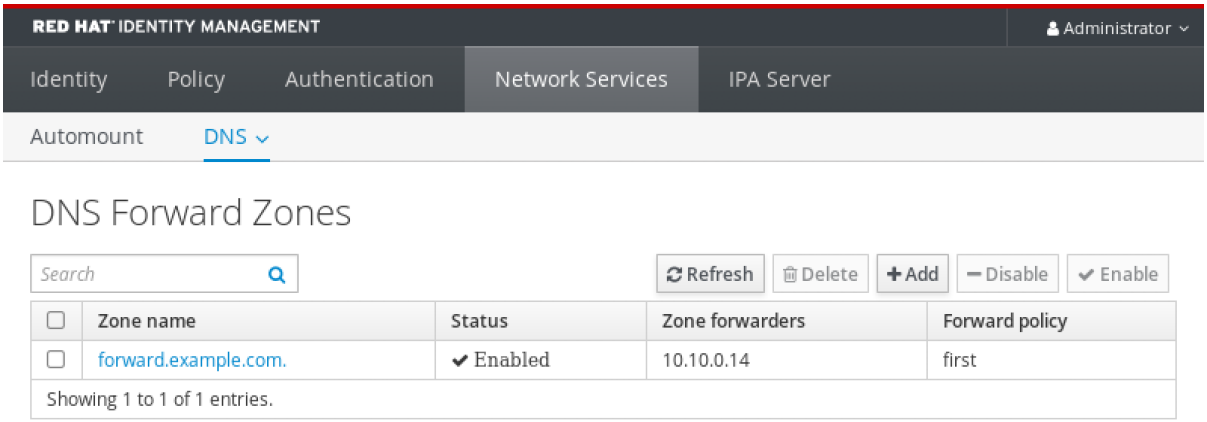
6. Cliquez sur **Add** en bas de la fenêtre pour ajouter la nouvelle zone de transmission.

Verification steps

1. Dans l'interface Web IdM, sélectionnez **Network Services → DNS Forward Zones → DNS**.

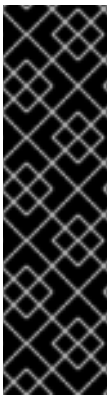


2. Vérifiez que la zone de transfert que vous avez créée, avec les transitaires et la politique de transfert que vous avez spécifiés, est présente et activée dans l'interface utilisateur Web d'IdM.



6.6. AJOUT D'UNE ZONE DE TRANSFERT DNS DANS L'INTERFACE DE PROGRAMMATION

Cette section décrit comment ajouter une zone de transfert DNS à partir de l'interface de ligne de commande (CLI).



IMPORTANT

N'utilisez pas de zones de transmission, sauf en cas d'absolue nécessité. Les zones de transfert ne constituent pas une solution standard et leur utilisation peut entraîner un comportement inattendu et problématique. Si vous devez utiliser des zones de transfert, limitez leur utilisation à l'annulation d'une configuration de transfert globale.

Lors de la création d'une nouvelle zone DNS, Red Hat recommande de toujours utiliser la délégation DNS standard à l'aide d'enregistrements de serveurs de noms (NS) et d'éviter les zones de transfert. Dans la plupart des cas, l'utilisation d'un transitaire global est suffisante et les zones de transfert ne sont pas nécessaires.

Conditions préalables

- Vous êtes connecté en tant qu'administrateur IdM.
- Vous connaissez l'adresse IP (Internet Protocol) du serveur DNS vers lequel transférer les requêtes.

Procédure

- Utilisez la commande **dnsforwardzone-add** pour ajouter une nouvelle zone de transfert. Spécifiez au moins un transitaire avec l'option **--forwarder** si la politique de transfert n'est pas **none**, et spécifiez la politique de transfert avec l'option **--forward-policy**.

```
[user@server ~]$ ipa dnsforwardzone-add forward.example.com. --
forwarder=10.10.0.14 --forwarder=10.10.1.15 --forward-policy=first

Zone name: forward.example.com.
Zone forwarders: 10.10.0.14, 10.10.1.15
Forward policy: first
```

Verification steps

- Utilisez la commande **dnsforwardzone-show** pour afficher la zone de transfert DNS que vous venez de créer.

```
[user@server ~]$ ipa dnsforwardzone-show forward.example.com.

Zone name: forward.example.com.
Zone forwarders: 10.10.0.14, 10.10.1.15
Forward policy: first
```

6.7. MISE EN PLACE D'UN DNS GLOBAL FORWARDER DANS IDM À L'AIDE D'ANSIBLE

Cette section décrit comment un administrateur de gestion des identités (IdM) peut utiliser un playbook Ansible pour établir un DNS Global Forwarder dans IdM.

Dans l'exemple de procédure ci-dessous, l'administrateur IdM crée une redirection globale DNS vers un serveur DNS avec une adresse Internet Protocol (IP) v4 de **8.8.6.6** et une adresse IPv6 de **2001:4860:4860::8800** sur le port **53**.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous connaissez le mot de passe de l'administrateur IdM.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsconfig
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **set-configuration.yml** Ansible playbook. Par exemple :

```
cp set-configuration.yml establish-global-forwarder.yml
```

4. Ouvrez le fichier **establish-global-forwarder.yml** pour le modifier.

5. Adaptez le fichier en définissant les variables suivantes :

   a. Modifiez la variable **name** du playbook en **Playbook to establish a global forwarder in IdM DNS**.

   b. Dans la section **tasks**, changez le **name** de la tâche en **Create a DNS global forwarder to 8.8.6.6 and 2001:4860:4860::8800**.

   c. Dans la section **forwarders** de la partie **ipadnsconfig**:

      i. Remplacez la première valeur de **ip_address** par l'adresse IPv4 du transitaire global : **8.8.6.6**.

      ii. Remplacer la deuxième valeur **ip_address** par l'adresse IPv6 du transitaire global : **2001:4860:4860::8800**.

      iii. Vérifiez que la valeur **port** est définie sur **53**.

   d. Modifier le **forward_policy** en **first**.
   Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Playbook to establish a global forwarder in IdM DNS
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Create a DNS global forwarder to 8.8.6.6 and 2001:4860:4860::8800
    ipadnsconfig:
      forwarders:
        - ip_address: 8.8.6.6
        - ip_address: 2001:4860:4860::8800
          port: 53
      forward_policy: first
      allow_sync_ptr: yes
```

6. Enregistrer le fichier.

7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file establish-global-forwarder.yml
```

Ressources supplémentaires

- Voir le fichier **README-dnsconfig.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.

6.8. ASSURER LA PRÉSENCE D'UN DNS GLOBAL FORWARDER DANS IDM EN UTILISANT ANSIBLE

Cette section décrit comment un administrateur Identity Management (IdM) peut utiliser un playbook Ansible pour assurer la présence d'un transitaire global DNS dans IdM. Dans l'exemple de procédure ci-dessous, l'administrateur IdM assure la présence d'un transitaire global DNS vers un serveur DNS avec une adresse Internet Protocol (IP) v4 de **7.7.9.9** et une adresse IP v6 de **2001:db8::1:0** sur le port **53**.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous connaissez le mot de passe de l'administrateur IdM.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsconfig
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **forwarders-absent.yml** Ansible playbook. Par exemple :

```
$ cp forwarders-absent.yml ensure-presence-of-a-global-forwarder.yml
```

4. Ouvrez le fichier **ensure-presence-of-a-global-forwarder.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes :
   a. Modifiez la variable **name** du playbook en **Playbook to ensure the presence of a global**

forwarder in IdM DNS.

b. Dans la section **tasks**, changez le **name** de la tâche en **Ensure the presence of a DNS global forwarder to 7.7.9.9 and 2001:db8::1:0 on port 53**.

c. Dans la section **forwarders** de la partie **ipadnsconfig**:

i. Remplacez la première valeur de **ip_address** par l'adresse IPv4 du transitaire global : **7.7.9.9**.

ii. Remplacer la deuxième valeur **ip_address** par l'adresse IPv6 du transitaire global : **2001:db8::1:0**.

iii. Vérifiez que la valeur **port** est définie sur **53**.

d. Modifier le **state** en **present**.
Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Playbook to ensure the presence of a global forwarder in IdM DNS
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Ensure the presence of a DNS global forwarder to 7.7.9.9 and 2001:db8::1:0 on port
53
    ipadnsconfig:
      forwarders:
        - ip_address: 7.7.9.9
        - ip_address: 2001:db8::1:0
          port: 53
      state: present
```

6. Enregistrer le fichier.

7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file ensure-presence-
of-a-global-forwarder.yml
```

Ressources supplémentaires

- Voir le fichier **README-dnsconfig.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.

6.9. S'ASSURER DE L'ABSENCE D'UN DNS GLOBAL FORWARDER DANS L'IDM EN UTILISANT ANSIBLE

Cette section décrit comment un administrateur Identity Management (IdM) peut utiliser un playbook Ansible pour garantir l'absence d'un transitaire global DNS dans IdM. Dans l'exemple de procédure ci-dessous, l'administrateur IdM s'assure de l'absence d'un transitaire global DNS avec une adresse Internet Protocol (IP) v4 de **8.8.6.6** et une adresse IP v6 de **2001:4860:4860::8800** sur le port **53**.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous connaissez le mot de passe de l'administrateur IdM.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsconfig
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **forwarders-absent.yml** Ansible playbook. Par exemple :

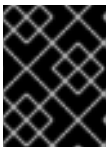
```
$ cp forwarders-absent.yml ensure-absence-of-a-global-forwarder.yml
```

4. Ouvrez le fichier **ensure-absence-of-a-global-forwarder.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes :
   a. Modifiez la variable **name** du playbook en **Playbook to ensure the absence of a global forwarder in IdM DNS**.
   b. Dans la section **tasks**, changez le **name** de la tâche en **Ensure the absence of a DNS global forwarder to 8.8.6.6 and 2001:4860:4860::8800 on port 53**.
   c. Dans la section **forwarders** de la partie **ipadnsconfig**:
      i. Remplacez la première valeur de **ip_address** par l'adresse IPv4 du transitaire global : **8.8.6.6**.
      ii. Remplacer la deuxième valeur **ip_address** par l'adresse IPv6 du transitaire global : **2001:4860:4860::8800**.
      iii. Vérifiez que la valeur **port** est définie sur **53**.
   d. Fixer la variable **action** à **member**.
   e. Vérifiez que **state** est défini sur **absent**.

Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Playbook to ensure the absence of a global forwarder in IdM DNS
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Ensure the absence of a DNS global forwarder to 8.8.6.6 and
2001:4860:4860::8800 on port 53
    ipadnsconfig:
      forwarders:
        - ip_address: 8.8.6.6
        - ip_address: 2001:4860:4860::8800
          port: 53
      action: member
      state: absent
```



IMPORTANT

Si vous n'utilisez que l'option **state: absent** dans votre séquence sans utiliser également **action: member**, la séquence échoue.

6. Enregistrer le fichier.
7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file ensure-absence-of-
a-global-forwarder.yml
```

Ressources supplémentaires

- Le fichier **README-dnsconfig.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**
- L'option **action: member** dans les modules ipadnsconfig ansible-freeipa

6.10. S'ASSURER QUE LES DNS GLOBAL FORWARDERS SONT DÉSACTIVÉS DANS IDM À L'AIDE D'ANSIBLE

Cette section décrit comment un administrateur Identity Management (IdM) peut utiliser un playbook Ansible pour s'assurer que les transitaires globaux DNS sont désactivés dans IdM. Dans l'exemple de procédure ci-dessous, l'administrateur IdM s'assure que la politique de transfert du transitaire global est définie sur **none**, ce qui désactive effectivement le transitaire global.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.

- L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
- L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.

- Vous connaissez le mot de passe de l'administrateur IdM.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsconfig
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Vérifiez le contenu du fichier **disable-global-forwarders.yml** Ansible playbook qui est déjà configuré pour désactiver toutes les redirections globales DNS. Par exemple :

```
$ cat disable-global-forwarders.yml
---
- name: Playbook to disable global DNS forwarders
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Disable global forwarders.
    ipadnsconfig:
      forward_policy: none
```

4. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file disable-global-forwarders.yml
```

Ressources supplémentaires

- Voir le fichier **README-dnsconfig.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.

6.11. ASSURER LA PRÉSENCE D'UNE ZONE DE TRANSFERT DNS DANS IDM EN UTILISANT ANSIBLE

Cette section décrit comment un administrateur de gestion des identités (IdM) peut utiliser un playbook Ansible pour assurer la présence d'une zone de transfert DNS dans IdM. Dans l'exemple de procédure ci-dessous, l'administrateur IdM assure la présence d'une zone de transfert DNS pour **example.com** vers un serveur DNS avec une adresse IP (Internet Protocol) de **8.8.8.8**.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous connaissez le mot de passe de l'administrateur IdM.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsconfig
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **forwarders-absent.yml** Ansible playbook. Par exemple :

```
cp forwarders-absent.yml ensure-presence-forwardzone.yml
```

4. Ouvrez le fichier **ensure-presence-forwardzone.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes :
   a. Modifiez la variable **name** du playbook en **Playbook to ensure the presence of a dnsforwardzone in IdM DNS**.
   b. Dans la section **tasks**, changez le **name** de la tâche en **Ensure presence of a dnsforwardzone for example.com to 8.8.8.8**.
   c. Dans la section **tasks**, remplacez le titre **ipadnsconfig** par **ipadnsforwardzone**.
   d. Dans la section **ipadnsforwardzone**:
      i. Ajoutez la variable **ipaadmin_password** et définissez-la comme votre mot de passe d'administrateur IdM.
      ii. Ajoutez la variable **name** et fixez-la à **example.com**.
      iii. Dans la section **forwarders**:
         A. Supprimer les lignes **ip_address** et **port**.

B. Ajoutez l'adresse IP du serveur DNS qui doit recevoir les requêtes transférées en la spécifiant après un tiret :

```
- 8.8.8.8
```

iv. Ajoutez la variable **forwardpolicy** et fixez-la à **first**.

v. Ajoutez la variable **skip_overlap_check** et fixez-la à **true**.

vi. Remplacez la variable **state** par **present**.

Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Playbook to ensure the presence of a dnsforwardzone in IdM DNS
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Ensure the presence of a dnsforwardzone for example.com to 8.8.8.8
  ipadnsforwardzone:
      ipaadmin_password: "{{ ipaadmin_password }}"
      name: example.com
      forwarders:
          - 8.8.8.8
      forwardpolicy: first
      skip_overlap_check: true
      state: present
```

6. Enregistrer le fichier.

7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file ensure-presence-forwardzone.yml
```

Ressources supplémentaires

- Voir le fichier **README-dnsforwardzone.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.

6.12. S'ASSURER QU'UNE ZONE DE TRANSFERT DNS A PLUSIEURS TRANSITAIRES DANS IDM À L'AIDE D'ANSIBLE

Cette section décrit comment un administrateur de gestion des identités (IdM) peut utiliser un playbook Ansible pour s'assurer qu'une zone de transfert DNS dans IdM a plusieurs transitaires. Dans l'exemple de procédure ci-dessous, l'administrateur IdM s'assure que la zone de transfert DNS pour **example.com** est transférée vers **8.8.8.8** et **4.4.4.4**.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :

- Vous utilisez la version 2.8 ou ultérieure d'Ansible.
- Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
- L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
- L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.

- Vous connaissez le mot de passe de l'administrateur IdM.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsconfig
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **forwarders-absent.yml** Ansible playbook. Par exemple :

```
cp forwarders-absent.yml ensure-presence-multiple-forwarders.yml
```

4. Ouvrez le fichier **ensure-presence-multiple-forwarders.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes :
   a. Modifiez la variable **name** du playbook en **Playbook to ensure the presence of multiple forwarders in a dnsforwardzone in IdM DNS**.
   b. Dans la section **tasks**, changez le **name** de la tâche en **Ensure presence of 8.8.8.8 and 4.4.4.4 forwarders in dnsforwardzone for example.com**.
   c. Dans la section **tasks**, remplacez le titre **ipadnsconfig** par **ipadnsforwardzone**.
   d. Dans la section **ipadnsforwardzone**:
      i. Ajoutez la variable **ipaadmin_password** et définissez-la comme votre mot de passe d'administrateur IdM.
      ii. Ajoutez la variable **name** et fixez-la à **example.com**.
      iii. Dans la section **forwarders**:
         A. Supprimer les lignes **ip_address** et **port**.
         B. Ajoutez l'adresse IP des serveurs DNS dont vous voulez vous assurer de la présence, précédée d'un tiret :

```
    - 8.8.8.8
    - 4.4.4.4
```

iv. Modifier la variable d'état pour qu'elle devienne présente.

Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: name: Playbook to ensure the presence of multiple forwarders in a dnsforwardzone
in IdM DNS
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Ensure presence of 8.8.8.8 and 4.4.4.4 forwarders in dnsforwardzone for
example.com
  ipadnsforwardzone:
      ipaadmin_password: "{{ ipaadmin_password }}"
     name: example.com
      forwarders:
          - 8.8.8.8
          - 4.4.4.4
      state: present
```

6. Enregistrer le fichier.

7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file ensure-presence-
multiple-forwarders.yml
```

Ressources supplémentaires

- Voir le fichier **README-dnsforwardzone.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.

6.13. S'ASSURER QU'UNE ZONE DE TRANSFERT DNS EST DÉSACTIVÉE DANS L'IDM À L'AIDE D'ANSIBLE

Cette section décrit comment un administrateur de gestion des identités (IdM) peut utiliser un playbook Ansible pour s'assurer qu'une zone de transfert DNS est désactivée dans IdM. Dans l'exemple de procédure ci-dessous, l'administrateur IdM s'assure que la zone de transfert DNS pour **example.com** est désactivée.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.

- L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
- L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.

- Vous connaissez le mot de passe de l'administrateur IdM.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsconfig
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **forwarders-absent.yml** Ansible playbook. Par exemple :

```
$ cp forwarders-absent.yml ensure-disabled-forwardzone.yml
```

4. Ouvrez le fichier **ensure-disabled-forwardzone.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes :
   a. Modifiez la variable **name** du playbook en **Playbook to ensure a dnsforwardzone is disabled in IdM DNS**.
   b. Dans la section **tasks**, changez le **name** de la tâche en **Ensure a dnsforwardzone for example.com is disabled**.
   c. Dans la section **tasks**, remplacez le titre **ipadnsconfig** par **ipadnsforwardzone**.
   d. Dans la section **ipadnsforwardzone**:
      i. Ajoutez la variable **ipaadmin_password** et définissez-la comme votre mot de passe d'administrateur IdM.
      ii. Ajoutez la variable **name** et fixez-la à **example.com**.
      iii. Retirer toute la section **forwarders**.
      iv. Remplacez la variable **state** par **disabled**.

   Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Playbook to ensure a dnsforwardzone is disabled in IdM DNS
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
```

```
tasks:
- name: Ensure a dnsforwardzone for example.com is disabled
ipadnsforwardzone:
    ipaadmin_password: "{{ ipaadmin_password }}"
    name: example.com
    state: disabled
```

6. Enregistrer le fichier.

7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file ensure-disabled-forwardzone.yml
```

Ressources supplémentaires

- Voir le fichier **README-dnsforwardzone.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.

6.14. GARANTIR L'ABSENCE D'UNE ZONE DE TRANSFERT DNS DANS L'IDM À L'AIDE D'ANSIBLE

Cette section décrit comment un administrateur de gestion des identités (IdM) peut utiliser un playbook Ansible pour garantir l'absence d'une zone de transfert DNS dans IdM. Dans l'exemple de procédure ci-dessous, l'administrateur IdM s'assure de l'absence d'une zone de transfert DNS pour **example.com**.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous connaissez le mot de passe de l'administrateur IdM.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsconfig**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsconfig
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **forwarders-absent.yml** Ansible playbook. Par exemple :

```
$ cp forwarders-absent.yml ensure-absence-forwardzone.yml
```

4. Ouvrez le fichier **ensure-absence-forwardzone.yml** pour le modifier.

5. Adaptez le fichier en définissant les variables suivantes :

   a. Modifiez la variable **name** du playbook en **Playbook to ensure the absence of a dnsforwardzone in IdM DNS**.

   b. Dans la section **tasks**, changez le **name** de la tâche en **Ensure the absence of a dnsforwardzone for example.com**.

   c. Dans la section **tasks**, remplacez le titre **ipadnsconfig** par **ipadnsforwardzone**.

   d. Dans la section **ipadnsforwardzone**:

      i. Ajoutez la variable **ipaadmin_password** et définissez-la comme votre mot de passe d'administrateur IdM.

      ii. Ajoutez la variable **name** et fixez-la à **example.com**.

      iii. Retirer toute la section **forwarders**.

      iv. Laissez la variable **state** comme **absent**.

   Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Playbook to ensure the absence of a dnsforwardzone in IdM DNS
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Ensure the absence of a dnsforwardzone for example.com
    ipadnsforwardzone:
      ipaadmin_password: "{{ ipaadmin_password }}"
      name: example.com
      state: absent
```

6. Enregistrer le fichier.

7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file ensure-absence-
forwardzone.yml
```

Ressources supplémentaires

- Voir le fichier **README-dnsforwardzone.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.

6.15. RESSOURCES SUPPLÉMENTAIRES

- Transfert DNS

CHAPITRE 7. GESTION DES ENREGISTREMENTS DNS DANS L'IDM

Ce chapitre décrit comment gérer les enregistrements DNS dans la gestion des identités (IdM). En tant qu'administrateur IdM, vous pouvez ajouter, modifier et supprimer des enregistrements DNS dans IdM. Ce chapitre contient les sections suivantes :

- Enregistrements DNS dans l'IdM
- Ajout d'enregistrements de ressources DNS à partir de l'interface Web IdM
- Ajout d'enregistrements de ressources DNS à partir de la CLI IdM
- Options courantes d'ipa dnsrecord-add
- Suppression d'enregistrements DNS dans l'interface Web IdM
- Suppression d'un enregistrement DNS entier dans l'interface Web IdM
- Suppression d'enregistrements DNS dans la CLI IdM

Conditions préalables

- Votre déploiement IdM contient un serveur DNS intégré. Pour plus d'informations sur l'installation d'IdM avec DNS intégré, voir l'un des liens suivants :
  - Installation d'un serveur IdM : Avec DNS intégré, avec une autorité de certification intégrée comme autorité de certification racine.
  - Installation d'un serveur IdM : Avec DNS intégré, avec une autorité de certification externe comme autorité de certification racine.

7.1. ENREGISTREMENTS DNS DANS L'IDM

La gestion des identités (IdM) prend en charge de nombreux types d'enregistrements DNS. Les quatre types suivants sont les plus fréquemment utilisés :

A

Il s'agit d'une correspondance de base entre un nom d'hôte et une adresse IPv4. Le nom d'un enregistrement A est un nom d'hôte, tel que **www**. La valeur **IP Address** d'un enregistrement A est une adresse IPv4, telle que **192.0.2.1**.
Pour plus d'informations sur les enregistrements A, voir RFC 1035.

AAAA

Il s'agit d'une correspondance de base entre un nom d'hôte et une adresse IPv6. Le nom d'un enregistrement AAAA est un nom d'hôte, tel que **www**. La valeur **IP Address** est une adresse IPv6, telle que **2001:DB8::1111**.
Pour plus d'informations sur les enregistrements AAAA, voir RFC 3596.

SRV

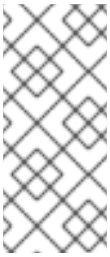
Service (SRV) resource records font correspondre les noms de service au nom DNS du serveur qui fournit ce service particulier. Par exemple, ce type d'enregistrement peut associer un service tel qu'un annuaire LDAP au serveur qui le gère.

Le nom d'un enregistrement SRV a le format suivant ***_service._protocol***, tel que **_ldap._tcp**. Les options de configuration des enregistrements SRV comprennent la priorité, le poids, le numéro de port et le nom d'hôte du service cible.

Pour plus d'informations sur les enregistrements SRV, voir RFC 2782.

PTR

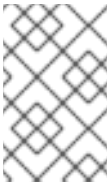
Un enregistrement de pointeur (PTR) ajoute un enregistrement DNS inverse, qui fait correspondre une adresse IP à un nom de domaine.



NOTE

Toutes les recherches DNS inversées pour les adresses IPv4 utilisent des entrées inversées définies dans le domaine **in-addr.arpa.**. L'adresse inversée, sous une forme lisible par l'homme, est l'inverse exact de l'adresse IP normale, à laquelle est ajouté le domaine **in-addr.arpa.**. Par exemple, pour l'adresse réseau **192.0.2.0/24**, la zone inversée est **2.0.192.in-addr.arpa**.

Le nom d'enregistrement d'un PTR doit être au format standard spécifié dans le RFC 1035, étendu dans le RFC 2317 et le RFC 3596. La valeur du nom d'hôte doit être un nom d'hôte canonique de l'hôte pour lequel vous souhaitez créer l'enregistrement.



NOTE

Les zones inversées peuvent également être configurées pour les adresses IPv6, avec des zones dans le domaine **.ip6.arpa.**. Pour plus d'informations sur les zones inversées IPv6, voir la RFC 3596.

Lors de l'ajout d'enregistrements de ressources DNS, il convient de noter que de nombreux enregistrements nécessitent des données différentes. Par exemple, un enregistrement CNAME nécessite un nom d'hôte, tandis qu'un enregistrement A nécessite une adresse IP. Dans l'interface Web de l'IdM, les champs du formulaire d'ajout d'un nouvel enregistrement sont mis à jour automatiquement pour refléter les données requises pour le type d'enregistrement sélectionné.

7.2. AJOUT D'ENREGISTREMENTS DE RESSOURCES DNS DANS L'INTERFACE WEB IDM

Cette section décrit comment ajouter des enregistrements de ressources DNS dans l'interface Web de gestion des identités (IdM).

Conditions préalables

- La zone DNS à laquelle vous voulez ajouter un enregistrement DNS existe et est gérée par IdM. Pour plus d'informations sur la création d'une zone DNS dans IdM DNS, voir Gestion des zones DNS dans IdM.
- Vous êtes connecté en tant qu'administrateur IdM.

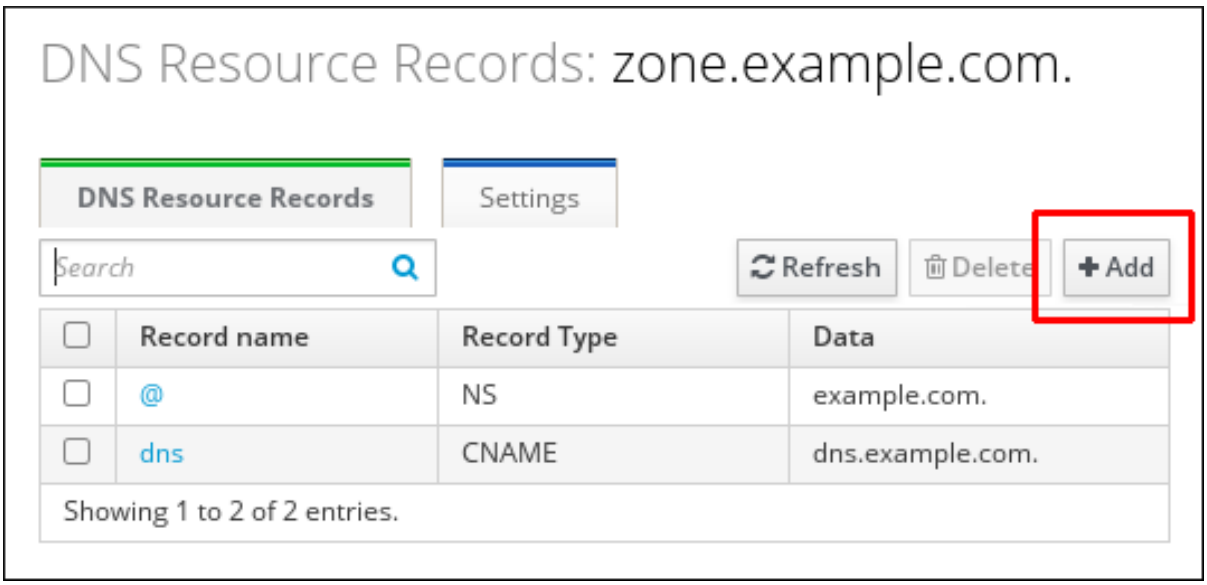
Procédure

1. Dans l'interface Web IdM, cliquez sur **Network Services → DNS → DNS Zones**.

2. Cliquez sur la zone DNS à laquelle vous souhaitez ajouter un enregistrement DNS.

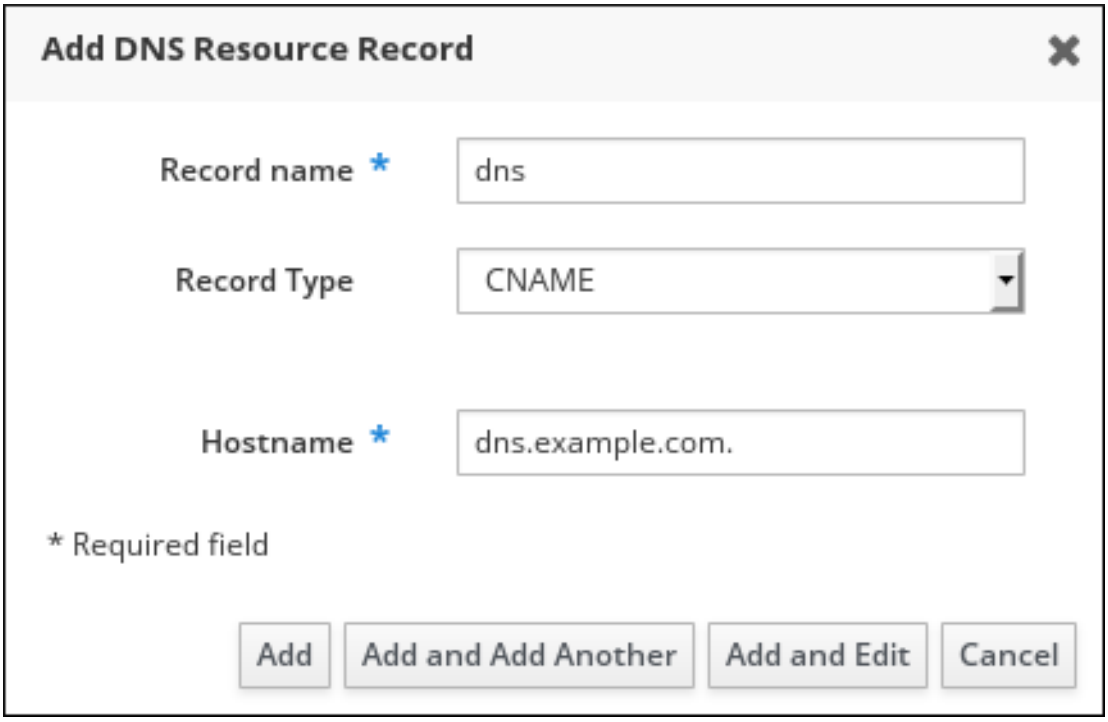
3. Dans la section **DNS Resource Records**, cliquez sur **Ajouter** pour ajouter un nouvel enregistrement.

Figure 7.1. Ajout d'un nouvel enregistrement de ressources DNS



4. Sélectionnez le type d'enregistrement à créer et remplissez les autres champs si nécessaire.

Figure 7.2. Définition d'un nouvel enregistrement de ressource DNS



5. Cliquez sur **Ajouter** pour confirmer le nouvel enregistrement.

7.3. AJOUT D'ENREGISTREMENTS DE RESSOURCES DNS À PARTIR DE LA CLI IDM

Cette section décrit comment ajouter un enregistrement de ressource DNS de n'importe quel type à partir de l'interface de ligne de commande (CLI).

Conditions préalables

- La zone DNS à laquelle vous voulez ajouter un enregistrement DNS existe. Pour plus d'informations sur la création d'une zone DNS dans IdM DNS, voir Gestion des zones DNS dans IdM.
- Vous êtes connecté en tant qu'administrateur IdM.

Procédure

1. Pour ajouter un enregistrement de ressource DNS, utilisez la commande **ipa dnsrecord-add**. La commande suit la syntaxe suivante :

```
$ ipa dnsrecord-add zone_name record_name --record_type_option=data
```

Dans la commande ci-dessus :

- Le *zone_name* est le nom de la zone DNS à laquelle l'enregistrement est ajouté.
- Le *record_name* est un identifiant pour le nouvel enregistrement de ressource DNS.

Par exemple, pour ajouter un enregistrement DNS de type A de **host1** à la zone **idm.example.com**, entrez :

```
$ ipa dnsrecord-add idm.example.com host1 --a-rec=192.168.122.123
```

7.4. OPTIONS COURANTES D'IPA DNSRECORD-*

Cette section décrit les options que vous pouvez utiliser pour ajouter, modifier et supprimer les types d'enregistrements de ressources DNS les plus courants dans la gestion des identités (IdM) :

- A (IPv4)
- AAAA (IPv6)
- SRV
- PTR

Dans **Bash**, vous pouvez définir plusieurs entrées en énumérant les valeurs dans une liste séparée par des virgules à l'intérieur d'accolades, comme **--option={val1,val2,val3}**.

Tableau 7.1. Options générales d'enregistrement

Option	*Description*
--ttl=*number*	Définit la durée de vie de l'enregistrement.
--structured	Analyse les enregistrements DNS bruts et les renvoie dans un format structuré.

Tableau 7.2. \Options d'enregistrement

Option	*Description*	*Examples*
--a-rec=*ARECORD*	Transmet un seul enregistrement A ou une liste d'enregistrements A.	**ipa dnsrecord-add idm.example.com host1 --a-rec=192.168.122.123**
	Peut créer un enregistrement A de type "wildcard" avec une adresse IP donnée.	**ipa dnsrecord-add idm.example.com "*" --a-rec=192.168.122.123** [a]
--a-ip-address=*string*	Indique l'adresse IP de l'enregistrement. Lors de la création d'un enregistrement, l'option permettant de spécifier la valeur de l'enregistrement **A** est **--a-rec**. Toutefois, lors de la modification d'un enregistrement **A**, l'option **--a-rec** est utilisée pour spécifier la valeur actuelle de l'enregistrement **A**. La nouvelle valeur est définie à l'aide de l'option **--a-ip-address**.	**ipa dnsrecord-mod idm.example.com --a-rec 192.168.122.123 --a-ip-address 192.168.122.124**

[a] L'exemple crée un enregistrement **A** avec l'adresse IP 192.0.2.123.

Tableau 7.3. \Options d'enregistrement "AAAA"

Option	*Description*	*Example*
--aaaa-rec=*AAAARECORD*	Transmet un seul enregistrement AAAA (IPv6) ou une liste d'enregistrements AAAA.	**ipa dnsrecord-add idm.example.com www --aaaa-rec 2001:db8::1231:5675**
--aaaa-ip-address=*string*	Indique l'adresse IPv6 de l'enregistrement. Lors de la création d'un enregistrement, l'option permettant de spécifier la valeur de l'enregistrement **A** est **--aaaa-rec**. Toutefois, lors de la modification d'un enregistrement **A**, l'option **--aaaa-rec** est utilisée pour spécifier la valeur actuelle de l'enregistrement **A**. La nouvelle valeur est définie à l'aide de l'option **--a-ip-address**.	**ipa dnsrecord-mod idm.example.com --aaaa-rec 2001:db8::1231:5675 --aaaa-ip-address 2001:db8::1231:5676**

Tableau 7.4. \Options d'enregistrement "PTR

Option	*Description*	*Example*

Option	*Description*	*Example*
--ptr-rec=*PTRRECORD*	Transmet un seul enregistrement PTR ou une liste d'enregistrements PTR. Lors de l'ajout d'un enregistrement DNS inversé, le nom de la zone utilisé avec la commande **ipa dnsrecord-add** est inversé par rapport à l'utilisation pour l'ajout d'autres enregistrements DNS. Généralement, l'adresse IP de l'hôte est le dernier octet de l'adresse IP dans un réseau donné. Le premier exemple à droite ajoute un enregistrement PTR pour **server4.idm.example.com** avec l'adresse IPv4 **192.168.122.4.**. Le deuxième exemple ajoute une entrée DNS inverse à la zone inverse **0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.** IPv6 pour l'hôte **server2.example.com** avec l'adresse IP **2001:DB8::1111**.	**ipa dnsrecord-add 122.168.192.in-addr.arpa 4 --ptr-rec server4.idm.example.com.** **$ ipa dnsrecord-add 0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa. 1.1.1.0.0.0.0.0.0.0.0.0.0.0.0.0 --ptr-rec server2.idm.example.com.**
--ptr-hostname=*string*	Indique le nom d'hôte de l'enregistrement.	

Tableau 7.5. \SRV Options d'enregistrement

Option	*Description*	*Example*
--srv-rec=*SRVRECORD*	Transmet un seul enregistrement SRV ou une liste d'enregistrements SRV. Dans les exemples ci-contre, **_ldap._tcp** définit le type de service et le protocole de connexion pour l'enregistrement SRV. L'option **--srv-rec** définit les valeurs de priorité, de poids, de port et de cible. Les valeurs de poids de 51 et 49 dans les exemples totalisent 100 et représentent la probabilité, en pourcentage, qu'un enregistrement particulier soit utilisé.	**# ipa dnsrecord-add idm.example.com _ldap._tcp --srv-rec="0 51 389 server1.idm.example.com."** **# ipa dnsrecord-add server.idm.example.com _ldap._tcp --srv-rec="1 49 389 server2.idm.example.com."**
--srv-priority=*number*	Définit la priorité de l'enregistrement. Il peut y avoir plusieurs enregistrements SRV pour un type de service. La priorité (0 - 65535) définit le rang de l'enregistrement ; plus le chiffre est bas, plus la priorité est élevée. Un service doit utiliser en premier l'enregistrement ayant la priorité la plus élevée.	**# ipa dnsrecord-mod server.idm.example.com _ldap._tcp --srv-rec="1 49 389 server2.idm.example.com." --srv-priority=0**

Option	*Description*	*Example*
--srv-weight=*number*	Définit le poids de l'enregistrement. Cela permet de déterminer l'ordre des enregistrements SRV ayant la même priorité. La somme des poids définis doit être égale à 100, ce qui représente la probabilité (en pourcentage) qu'un enregistrement particulier soit utilisé.	**# ipa dnsrecord-mod server.idm.example.com _ldap._tcp --srv-rec="0 49 389 server2.idm.example.com." --srv-weight=60**
--srv-port=*number*	Indique le port du service sur l'hôte cible.	**# ipa dnsrecord-mod server.idm.example.com _ldap._tcp --srv-rec="0 60 389 server2.idm.example.com." --srv-port=636**
--srv-target=*string*	Indique le nom de domaine de l'hôte cible. Il peut s'agir d'un seul point (.) si le service n'est pas disponible dans le domaine.	

Ressources supplémentaires

- Exécuter **ipa dnsrecord-add --help**.

7.5. SUPPRESSION D'ENREGISTREMENTS DNS DANS L'INTERFACE WEB IDM

Cette section décrit comment supprimer des enregistrements DNS dans la gestion des identités (IdM) à l'aide de l'interface Web IdM.

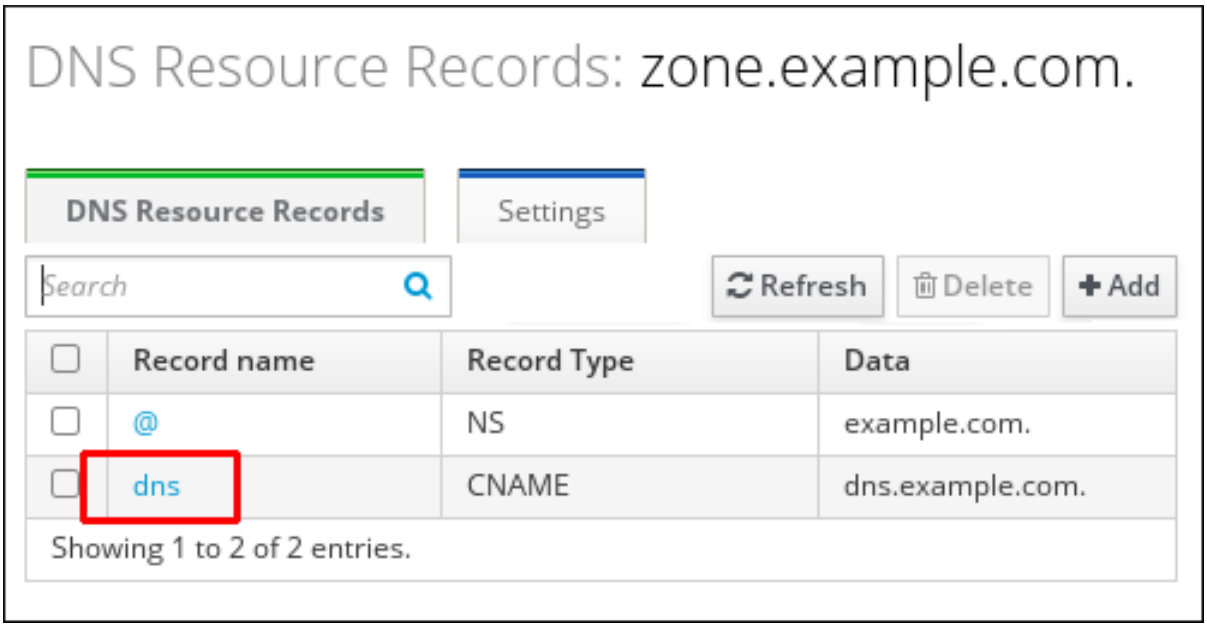
Conditions préalables

- Vous êtes connecté en tant qu'administrateur IdM.

Procédure

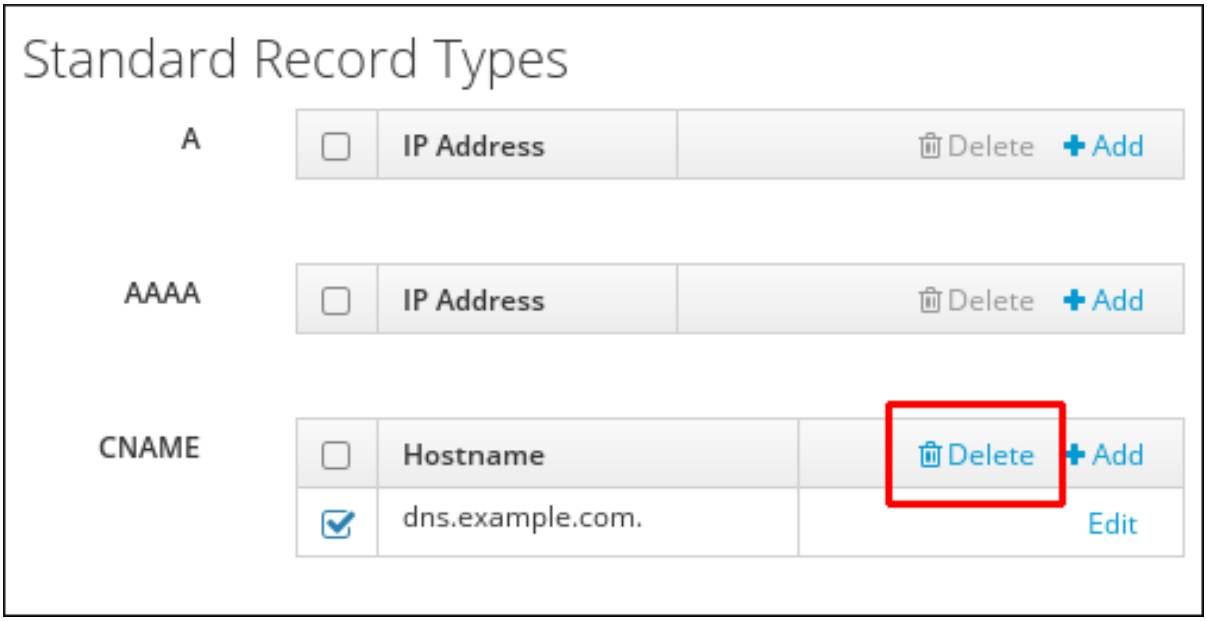
1. Dans l'interface Web IdM, cliquez sur **Network Services → DNS → DNS Zones**.
2. Cliquez sur la zone dont vous souhaitez supprimer un enregistrement DNS, par exemple **example.com.**.
3. Dans la section **DNS Resource Records**, cliquez sur le nom de l'enregistrement de ressource.

Figure 7.3. Sélection d'un enregistrement de ressource DNS



4. Cochez la case correspondant au nom du type d'enregistrement à supprimer.
5. Cliquez sur **Delete**.

Figure 7.4. Suppression d'un enregistrement de ressource DNS



Le type d'enregistrement sélectionné est maintenant supprimé. Le reste de la configuration de l'enregistrement de ressource est laissé intact.

Ressources supplémentaires

- Voir Suppression d'un enregistrement DNS entier dans l'interface Web IdM .

7.6. SUPPRESSION D'UN ENREGISTREMENT DNS ENTIER DANS L'INTERFACE WEB IDM

Cette section décrit comment supprimer tous les enregistrements d'une ressource particulière dans une zone à l'aide de l'interface Web de gestion des identités (IdM).

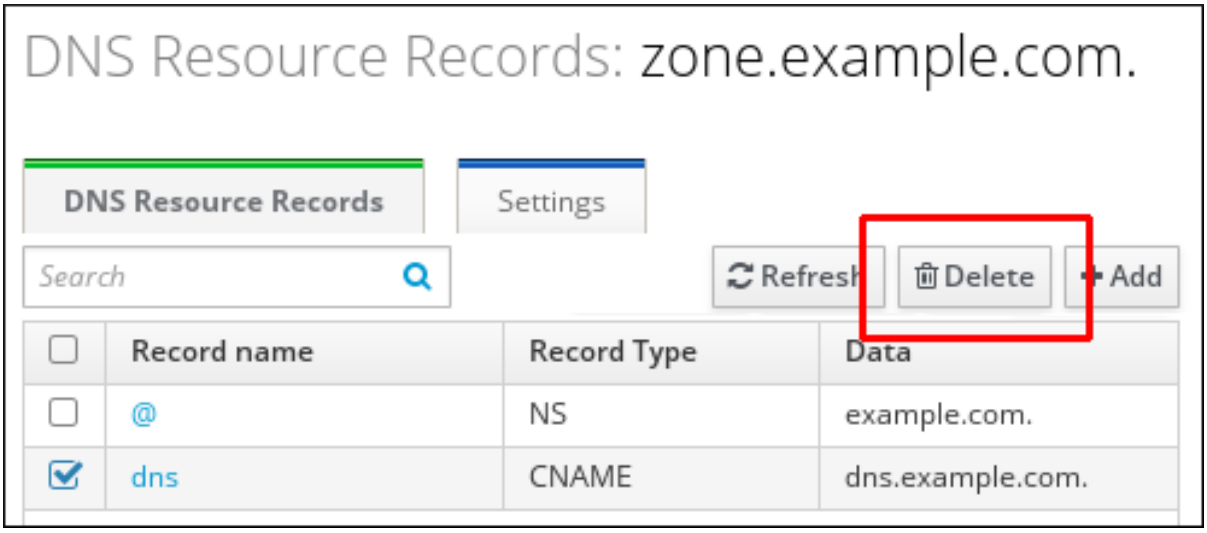
Conditions préalables

- Vous êtes connecté en tant qu'administrateur IdM.

Procédure

1. Dans l'interface Web IdM, cliquez sur **Network Services → DNS → DNS Zones**.
2. Cliquez sur la zone dont vous souhaitez supprimer un enregistrement DNS, par exemple **zone.example.com.**.
3. Dans la section **DNS Resource Records**, cochez la case de l'enregistrement de ressource à supprimer.
4. Click **Delete**.

Figure 7.5. Suppression d'un enregistrement de ressource entier



L'ensemble de l'enregistrement de ressource est maintenant supprimé.

7.7. SUPPRESSION D'ENREGISTREMENTS DNS DANS LA CLI IDM

Cette section décrit comment supprimer des enregistrements DNS d'une zone gérée par le DNS de gestion des identités (IdM).

Conditions préalables

- Vous êtes connecté en tant qu'administrateur IdM.

Procédure

- Pour supprimer des enregistrements d'une zone, utilisez la commande **ipa dnsrecord-del** et ajoutez l'option ***--recordType*-rec** à la valeur de l'enregistrement. Par exemple, pour supprimer un enregistrement de type A :

```
$ ipa dnsrecord-del example.com www --a-rec 192.0.2.1
```

Si vous exécutez **ipa dnsrecord-del** sans aucune option, la commande demande des informations sur l'enregistrement à supprimer. Notez que l'ajout de l'option **--del-all** à la commande supprime tous les enregistrements associés à la zone.

Ressources supplémentaires

- Exécutez la commande **ipa dnsrecord-del --help**.

7.8. RESSOURCES SUPPLÉMENTAIRES

- Voir Utiliser Ansible pour gérer les enregistrements DNS dans IdM .

CHAPITRE 8. UTILISER ANSIBLE POUR GÉRER LES ENREGISTREMENTS DNS DANS IDM

Ce chapitre décrit comment gérer les enregistrements DNS dans Identity Management (IdM) à l'aide d'un playbook Ansible. En tant qu'administrateur IdM, vous pouvez ajouter, modifier et supprimer des enregistrements DNS dans IdM. Ce chapitre contient les sections suivantes :

- Assurer la présence des enregistrements DNS A et AAAA dans l'IdM en utilisant Ansible
- Assurer la présence des enregistrements DNS A et PTR dans IdM en utilisant Ansible
- Assurer la présence de plusieurs enregistrements DNS dans IdM en utilisant Ansible
- Assurer la présence de plusieurs enregistrements CNAME dans IdM en utilisant Ansible
- Assurer la présence d'un enregistrement SRV dans IdM en utilisant Ansible

8.1. ENREGISTREMENTS DNS DANS L'IDM

La gestion des identités (IdM) prend en charge de nombreux types d'enregistrements DNS. Les quatre types suivants sont les plus fréquemment utilisés :

A

Il s'agit d'une correspondance de base entre un nom d'hôte et une adresse IPv4. Le nom d'un enregistrement A est un nom d'hôte, tel que **www**. La valeur **IP Address** d'un enregistrement A est une adresse IPv4, telle que **192.0.2.1**.
Pour plus d'informations sur les enregistrements A, voir RFC 1035.

AAAA

Il s'agit d'une correspondance de base entre un nom d'hôte et une adresse IPv6. Le nom d'un enregistrement AAAA est un nom d'hôte, tel que **www**. La valeur **IP Address** est une adresse IPv6, telle que **2001:DB8::1111**.
Pour plus d'informations sur les enregistrements AAAA, voir RFC 3596.

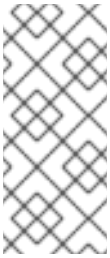
SRV

Service (SRV) resource records font correspondre les noms de service au nom DNS du serveur qui fournit ce service particulier. Par exemple, ce type d'enregistrement peut associer un service tel qu'un annuaire LDAP au serveur qui le gère.
Le nom d'un enregistrement SRV a le format suivant ***_service._protocol***, tel que **_ldap._tcp**. Les options de configuration des enregistrements SRV comprennent la priorité, le poids, le numéro de port et le nom d'hôte du service cible.

Pour plus d'informations sur les enregistrements SRV, voir RFC 2782.

PTR

Un enregistrement de pointeur (PTR) ajoute un enregistrement DNS inverse, qui fait correspondre une adresse IP à un nom de domaine.



NOTE

Toutes les recherches DNS inversées pour les adresses IPv4 utilisent des entrées inversées définies dans le domaine **in-addr.arpa.**. L'adresse inversée, sous une forme lisible par l'homme, est l'inverse exact de l'adresse IP normale, à laquelle est ajouté le domaine **in-addr.arpa.**. Par exemple, pour l'adresse réseau **192.0.2.0/24**, la zone inversée est **2.0.192.in-addr.arpa**.

Le nom d'enregistrement d'un PTR doit être au format standard spécifié dans le RFC 1035, étendu dans le RFC 2317 et le RFC 3596. La valeur du nom d'hôte doit être un nom d'hôte canonique de l'hôte pour lequel vous souhaitez créer l'enregistrement.

NOTE

Les zones inversées peuvent également être configurées pour les adresses IPv6, avec des zones dans le domaine **.ip6.arpa.**. Pour plus d'informations sur les zones inversées IPv6, voir la RFC 3596.

Lors de l'ajout d'enregistrements de ressources DNS, il convient de noter que de nombreux enregistrements nécessitent des données différentes. Par exemple, un enregistrement CNAME nécessite un nom d'hôte, tandis qu'un enregistrement A nécessite une adresse IP. Dans l'interface Web de l'IdM, les champs du formulaire d'ajout d'un nouvel enregistrement sont mis à jour automatiquement pour refléter les données requises pour le type d'enregistrement sélectionné.

8.2. OPTIONS COURANTES D'IPA DNSRECORD-*

Cette section décrit les options que vous pouvez utiliser pour ajouter, modifier et supprimer les types d'enregistrements de ressources DNS les plus courants dans la gestion des identités (IdM) :

- A (IPv4)
- AAAA (IPv6)
- SRV
- PTR

Dans **Bash**, vous pouvez définir plusieurs entrées en énumérant les valeurs dans une liste séparée par des virgules à l'intérieur d'accolades, comme **--option={val1,val2,val3}**.

Tableau 8.1. Options générales d'enregistrement

Option	*Description*
--ttl=*number*	Définit la durée de vie de l'enregistrement.
--structured	Analyse les enregistrements DNS bruts et les renvoie dans un format structuré.

Tableau 8.2. \Options d'enregistrement

Option	*Description*	*Examples*
--a-rec=*ARECORD*	Transmet un seul enregistrement A ou une liste d'enregistrements A.	**ipa dnsrecord-add idm.example.com host1 --a-rec=192.168.122.123**
	Peut créer un enregistrement A de type "wildcard" avec une adresse IP donnée.	**ipa dnsrecord-add idm.example.com "*" --a-rec=192.168.122.123** [a]
--a-ip-address=*string*	Indique l'adresse IP de l'enregistrement. Lors de la création d'un enregistrement, l'option permettant de spécifier la valeur de l'enregistrement **A** est **--a-rec**. Toutefois, lors de la modification d'un enregistrement **A**, l'option **--a-rec** est utilisée pour spécifier la valeur actuelle de l'enregistrement **A**. La nouvelle valeur est définie à l'aide de l'option **--a-ip-address**.	**ipa dnsrecord-mod idm.example.com --a-rec 192.168.122.123 --a-ip-address 192.168.122.124**

[a] L'exemple crée un enregistrement **A** avec l'adresse IP 192.0.2.123.

Tableau 8.3. \Options d'enregistrement "AAAA"

Option	*Description*	*Example*
--aaaa-rec=*AAAARECORD*	Transmet un seul enregistrement AAAA (IPv6) ou une liste d'enregistrements AAAA.	**ipa dnsrecord-add idm.example.com www --aaaa-rec 2001:db8::1231:5675**
--aaaa-ip-address=*string*	Indique l'adresse IPv6 de l'enregistrement. Lors de la création d'un enregistrement, l'option permettant de spécifier la valeur de l'enregistrement **A** est **--aaaa-rec**. Toutefois, lors de la modification d'un enregistrement **A**, l'option **--aaaa-rec** est utilisée pour spécifier la valeur actuelle de l'enregistrement **A**. La nouvelle valeur est définie à l'aide de l'option **--a-ip-address**.	**ipa dnsrecord-mod idm.example.com --aaaa-rec 2001:db8::1231:5675 --aaaa-ip-address 2001:db8::1231:5676**

Tableau 8.4. \Options d'enregistrement "PTR

Option	*Description*	*Example*

Option	*Description*	*Example*
--ptr-rec=*PTRRECORD*	Transmet un seul enregistrement PTR ou une liste d'enregistrements PTR. Lors de l'ajout d'un enregistrement DNS inversé, le nom de la zone utilisé avec la commande **ipa dnsrecord-add** est inversé par rapport à l'utilisation pour l'ajout d'autres enregistrements DNS. Généralement, l'adresse IP de l'hôte est le dernier octet de l'adresse IP dans un réseau donné. Le premier exemple à droite ajoute un enregistrement PTR pour **server4.idm.example.com** avec l'adresse IPv4 **192.168.122.4.**. Le deuxième exemple ajoute une entrée DNS inverse à la zone inverse **0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.** IPv6 pour l'hôte **server2.example.com** avec l'adresse IP **2001:DB8::1111**.	**ipa dnsrecord-add 122.168.192.in-addr.arpa 4 --ptr-rec server4.idm.example.com.** **$ ipa dnsrecord-add 0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa. 1.1.1.0.0.0.0.0.0.0.0.0.0.0.0.0 --ptr-rec server2.idm.example.com.**
--ptr-hostname=*string*	Indique le nom d'hôte de l'enregistrement.	

Tableau 8.5. \SRV Options d'enregistrement

Option	*Description*	*Example*
--srv-rec=*SRVRECORD*	Transmet un seul enregistrement SRV ou une liste d'enregistrements SRV. Dans les exemples ci-contre, **_ldap._tcp** définit le type de service et le protocole de connexion pour l'enregistrement SRV. L'option **--srv-rec** définit les valeurs de priorité, de poids, de port et de cible. Les valeurs de poids de 51 et 49 dans les exemples totalisent 100 et représentent la probabilité, en pourcentage, qu'un enregistrement particulier soit utilisé.	**# ipa dnsrecord-add idm.example.com _ldap._tcp --srv-rec="0 51 389 server1.idm.example.com."** **# ipa dnsrecord-add server.idm.example.com _ldap._tcp --srv-rec="1 49 389 server2.idm.example.com."**
--srv-priority=*number*	Définit la priorité de l'enregistrement. Il peut y avoir plusieurs enregistrements SRV pour un type de service. La priorité (0 - 65535) définit le rang de l'enregistrement ; plus le chiffre est bas, plus la priorité est élevée. Un service doit utiliser en premier l'enregistrement ayant la priorité la plus élevée.	**# ipa dnsrecord-mod server.idm.example.com _ldap._tcp --srv-rec="1 49 389 server2.idm.example.com." --srv-priority=0**

Option	*Description*	*Example*
--srv-weight=*number*	Définit le poids de l'enregistrement. Cela permet de déterminer l'ordre des enregistrements SRV ayant la même priorité. La somme des poids définis doit être égale à 100, ce qui représente la probabilité (en pourcentage) qu'un enregistrement particulier soit utilisé.	**# ipa dnsrecord-mod server.idm.example.com _ldap._tcp --srv-rec="0 49 389 server2.idm.example.com." --srv-weight=60**
--srv-port=*number*	Indique le port du service sur l'hôte cible.	**# ipa dnsrecord-mod server.idm.example.com _ldap._tcp --srv-rec="0 60 389 server2.idm.example.com." --srv-port=636**
--srv-target=*string*	Indique le nom de domaine de l'hôte cible. Il peut s'agir d'un seul point (.) si le service n'est pas disponible dans le domaine.	

Ressources supplémentaires

- Exécuter **ipa dnsrecord-add --help**.

8.3. ASSURER LA PRÉSENCE DES ENREGISTREMENTS DNS A ET AAAA DANS L'IDM EN UTILISANT ANSIBLE

Cette section montre comment un administrateur de gestion des identités (IdM) peut utiliser un playbook Ansible pour s'assurer que les enregistrements A et AAAA d'un hôte IdM particulier sont présents. Dans l'exemple utilisé dans la procédure ci-dessous, un administrateur IdM s'assure de la présence d'enregistrements A et AAAA pour **host1** dans la zone DNS **idm.example.com**.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous connaissez le mot de passe de l'administrateur IdM.

- La zone **idm.example.com** existe et est gérée par IdM DNS. Pour plus d'informations sur l'ajout d'une zone DNS primaire dans IdM DNS, voir Utilisation des playbooks Ansible pour gérer les zones IdM DNS.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsrecord**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsrecord
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **ensure-A-and-AAAA-records-are-present.yml** Ansible playbook. Par exemple :

```
$ cp ensure-A-and-AAAA-records-are-present.yml ensure-A-and-AAAA-records-are-present-copy.yml
```

4. Ouvrez le fichier **ensure-A-and-AAAA-records-are-present-copy.yml** pour le modifier.

5. Adaptez le fichier en définissant les variables suivantes dans la section **ipadnsrecord** task :

   - Définissez la variable **ipaadmin_password** avec votre mot de passe d'administrateur IdM.
   - Fixer la variable **zone_name** à **idm.example.com**.
   - Dans la variable **records**, fixez la variable **name** à **host1**, et la variable **a_ip_address** à **192.168.122.123**.
   - Dans la variable **records**, fixez la variable **name** à **host1**, et la variable **aaaa_ip_address** à **::1**.
     Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Ensure A and AAAA records are present
  hosts: ipaserver
  become: true
  gather_facts: false

  tasks:
  # Ensure A and AAAA records are present
  - name: Ensure that 'host1' has A and AAAA records.
    ipadnsrecord:
      ipaadmin_password: "{{ ipaadmin_password }}"
      zone_name: idm.example.com
      records:
      - name: host1
        a_ip_address: 192.168.122.123
      - name: host1
        aaaa_ip_address: ::1
```

6. Enregistrer le fichier.

7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file ensure-A-and-AAAA-records-are-present-copy.yml
```

Ressources supplémentaires

- Voir les enregistrements DNS dans IdM.
- Voir le fichier **README-dnsrecord.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir les exemples de playbooks Ansible dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsrecord**.

8.4. ASSURER LA PRÉSENCE DES ENREGISTREMENTS DNS A ET PTR DANS IDM EN UTILISANT ANSIBLE

Cette section montre comment un administrateur de gestion des identités (IdM) peut utiliser un playbook Ansible pour s'assurer qu'un enregistrement A pour un hôte IdM particulier est présent, avec un enregistrement PTR correspondant. Dans l'exemple utilisé dans la procédure ci-dessous, un administrateur IdM s'assure de la présence d'enregistrements A et PTR pour **host1** avec une adresse IP de **192.168.122.45** dans la zone **idm.example.com**.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous connaissez le mot de passe de l'administrateur IdM.
- La zone **idm.example.com** DNS existe et est gérée par IdM DNS. Pour plus d'informations sur l'ajout d'une zone DNS primaire dans IdM DNS, voir Utilisation des playbooks Ansible pour gérer les zones IdM DNS.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsrecord**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsrecord
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **ensure-dnsrecord-with-reverse-is-present.yml** Ansible playbook. Par exemple :

```
$ cp ensure-dnsrecord-with-reverse-is-present.yml ensure-dnsrecord-with-reverse-is-present-copy.yml
```

4. Ouvrez le fichier **ensure-dnsrecord-with-reverse-is-present-copy.yml** pour le modifier.

5. Adaptez le fichier en définissant les variables suivantes dans la section **ipadnsrecord** task :

   - Définissez la variable **ipaadmin_password** avec votre mot de passe d'administrateur IdM.
   - Fixer la variable **name** à **host1**.
   - Fixer la variable **zone_name** à **idm.example.com**.
   - Fixer la variable **ip_address** à 192.168.122.45.
   - Fixer la variable **create_reverse** à **yes**.
     Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Ensure DNS Record is present.
  hosts: ipaserver
  become: true
  gather_facts: false

  tasks:
  # Ensure that dns record is present
  - ipadnsrecord:
      ipaadmin_password: "{{ ipaadmin_password }}"
      name: host1
      zone_name: idm.example.com
      ip_address: 192.168.122.45
      create_reverse: yes
      state: present
```

6. Enregistrer le fichier.

7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file ensure-dnsrecord-with-reverse-is-present-copy.yml
```

Ressources supplémentaires

- Voir les enregistrements DNS dans IdM.

- Voir le fichier **README-dnsrecord.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir les exemples de playbooks Ansible dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsrecord**.

8.5. ASSURER LA PRÉSENCE DE PLUSIEURS ENREGISTREMENTS DNS DANS IDM EN UTILISANT ANSIBLE

Cette section montre comment un administrateur de gestion des identités (IdM) peut utiliser un playbook Ansible pour s'assurer que plusieurs valeurs sont associées à un enregistrement DNS IdM particulier. Dans l'exemple utilisé dans la procédure ci-dessous, un administrateur IdM s'assure de la présence de plusieurs enregistrements A pour **host1** dans la zone DNS **idm.example.com**.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous connaissez le mot de passe de l'administrateur IdM.
- La zone **idm.example.com** existe et est gérée par IdM DNS. Pour plus d'informations sur l'ajout d'une zone DNS primaire dans IdM DNS, voir Utilisation des playbooks Ansible pour gérer les zones IdM DNS.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsrecord**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsrecord
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **ensure-presence-multiple-records.yml** Ansible playbook. Par exemple :

```
$ cp ensure-presence-multiple-records.yml ensure-presence-multiple-records-copy.yml
```

4. Ouvrez le fichier **ensure-presence-multiple-records-copy.yml** pour le modifier.

5. Adaptez le fichier en définissant les variables suivantes dans la section **ipadnsrecord** task :
   - Définissez la variable **ipaadmin_password** avec votre mot de passe d'administrateur IdM.
   - Dans la section **records**, fixez la variable **name** à **host1**.
   - Dans la section **records**, la variable **zone_name** est remplacée par **idm.example.com**.
   - Dans la section **records**, la variable **a_rec** doit être remplacée par **192.168.122.112** et **192.168.122.122**.
   - Définir un deuxième enregistrement dans la section **records**:
     - Fixer la variable **name** à **host1**.
     - Fixer la variable **zone_name** à **idm.example.com**.
     - Fixer la variable **aaaa_rec** à **::1**.

   Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Test multiple DNS Records are present.
  hosts: ipaserver
  become: true
  gather_facts: false

  tasks:
  # Ensure that multiple dns records are present
  - ipadnsrecord:
      ipaadmin_password: "{{ ipaadmin_password }}"
      records:
        - name: host1
          zone_name: idm.example.com
          a_rec: 192.168.122.112
          a_rec: 192.168.122.122
        - name: host1
          zone_name: idm.example.com
          aaaa_rec: ::1
```

6. Enregistrer le fichier.
7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file ensure-presence-multiple-records-copy.yml
```

Ressources supplémentaires

- Voir les enregistrements DNS dans IdM.
- Voir le fichier **README-dnsrecord.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir les exemples de playbooks Ansible dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsrecord**.

8.6. ASSURER LA PRÉSENCE DE PLUSIEURS ENREGISTREMENTS CNAME DANS IDM EN UTILISANT ANSIBLE

Un enregistrement de nom canonique (enregistrement CNAME) est un type d'enregistrement de ressources dans le système de noms de domaine (DNS) qui fait correspondre un nom de domaine, un alias, à un autre nom, le nom canonique.

Les enregistrements CNAME peuvent s'avérer utiles lorsque plusieurs services sont exécutés à partir d'une même adresse IP : par exemple, un service FTP et un service web, chacun fonctionnant sur un port différent.

Cette section montre comment un administrateur de gestion des identités (IdM) peut utiliser un playbook Ansible pour s'assurer que plusieurs enregistrements CNAME sont présents dans le DNS IdM. Dans l'exemple utilisé dans la procédure ci-dessous, **host03** est à la fois un serveur HTTP et un serveur FTP. L'administrateur IdM s'assure de la présence des enregistrements CNAME **www** et **ftp** pour l'enregistrement A **host03** dans la zone **idm.example.com**.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous connaissez le mot de passe de l'administrateur IdM.
- La zone **idm.example.com** existe et est gérée par IdM DNS. Pour plus d'informations sur l'ajout d'une zone DNS primaire dans IdM DNS, voir Utilisation des playbooks Ansible pour gérer les zones IdM DNS.
- L'enregistrement A de **host03** existe dans la zone **idm.example.com**.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsrecord**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsrecord
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **ensure-CNAME-record-is-present.yml** Ansible playbook. Par exemple :

```
$ cp ensure-CNAME-record-is-present.yml ensure-CNAME-record-is-present-copy.yml
```

4. Ouvrez le fichier **ensure-CNAME-record-is-present-copy.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes dans la section **ipadnsrecord** task :
   - (Facultatif) Adaptez la description de la pièce fournie par le site **name**.
   - Définissez la variable **ipaadmin_password** avec votre mot de passe d'administrateur IdM.
   - Fixer la variable **zone_name** à **idm.example.com**.
   - Dans la section des variables de **records**, définissez les variables et valeurs suivantes :
     - Fixer la variable **name** à **www**.
     - Fixer la variable **cname_hostname** à **host03**.
     - Fixer la variable **name** à **ftp**.
     - Fixer la variable **cname_hostname** à **host03**.

   Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Ensure that 'www.idm.example.com' and 'ftp.idm.example.com' CNAME records
point to 'host03.idm.example.com'.
  hosts: ipaserver
  become: true
  gather_facts: false

  tasks:
  - ipadnsrecord:
      ipaadmin_password: "{{ ipaadmin_password }}"
      zone_name: idm.example.com
      records:
      - name: www
        cname_hostname: host03
      - name: ftp
        cname_hostname: host03
```

6. Enregistrer le fichier.
7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file ensure-
CNAME-record-is-present.yml
```

Ressources supplémentaires

- Voir le fichier **README-dnsrecord.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir les exemples de playbooks Ansible dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsrecord**.

8.7. ASSURER LA PRÉSENCE D'UN ENREGISTREMENT SRV DANS IDM EN UTILISANT ANSIBLE

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

Cette section montre comment un administrateur Identity Management (IdM) peut utiliser un playbook Ansible pour s'assurer qu'un enregistrement SRV est présent dans le DNS IdM. Dans l'exemple utilisé dans la procédure ci-dessous, un administrateur IdM s'assure de la présence de l'enregistrement SRV **_kerberos._udp.idm.example.com** avec la valeur **10 50 88 idm.example.com**. Cela définit les valeurs suivantes :

- Il fixe la priorité du service à 10.
- Il fixe le poids du service à 50.
- Il fixe le port à utiliser par le service à 88.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous connaissez le mot de passe de l'administrateur IdM.
- La zone **idm.example.com** existe et est gérée par IdM DNS. Pour plus d'informations sur l'ajout d'une zone DNS primaire dans IdM DNS, voir Utilisation des playbooks Ansible pour gérer les zones IdM DNS.

Procédure

1. Naviguez jusqu'au répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsrecord**:

```
$ cd /usr/share/doc/ansible-freeipa/playbooks/dnsrecord
```

2. Ouvrez votre fichier d'inventaire et assurez-vous que le serveur IdM que vous souhaitez configurer est répertorié dans la section **[ipaserver]**. Par exemple, pour demander à Ansible de configurer **server.idm.example.com**, entrez :

```
[ipaserver]
server.idm.example.com
```

3. Faites une copie du fichier **ensure-SRV-record-is-present.yml** Ansible playbook. Par exemple :

```
$ cp ensure-SRV-record-is-present.yml ensure-SRV-record-is-present-copy.yml
```

4. Ouvrez le fichier **ensure-SRV-record-is-present-copy.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes dans la section **ipadnsrecord** task :
   - Définissez la variable **ipaadmin_password** avec votre mot de passe d'administrateur IdM.
   - Fixer la variable **name** à **_kerberos._udp.idm.example.com**.
   - Fixer la variable **srv_rec** à **'10 50 88 idm.example.com'**.
   - Fixer la variable **zone_name** à **idm.example.com**.
     Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Test multiple DNS Records are present.
  hosts: ipaserver
  become: true
  gather_facts: false

  tasks:
  # Ensure a SRV record is present
  - ipadnsrecord:
      ipaadmin_password: "{{ ipaadmin_password }}"
      name: _kerberos._udp.idm.example.com
      srv_rec: '10 50 88 idm.example.com'
      zone_name: idm.example.com
      state: present
```

6. Enregistrer le fichier.
7. Exécutez le manuel de jeu :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory.file ensure-SRV-record-is-present.yml
```

Ressources supplémentaires

- Voir les enregistrements DNS dans IdM.
- Voir le fichier **README-dnsrecord.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir les exemples de playbooks Ansible dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/dnsrecord**.

CHAPITRE 9. UTILISATION DE NOMS D'HÔTES DNS CANONISÉS DANS L'IDM

La canonisation du DNS est désactivée par défaut sur les clients de gestion d'identité (IdM) afin d'éviter les risques de sécurité potentiels. Par exemple, si un pirate contrôle le serveur DNS et un hôte du domaine, il peut faire en sorte que le nom d'hôte court, tel que **demo**, soit résolu par un hôte compromis, tel que **malicious.example.com**. Dans ce cas, l'utilisateur se connecte à un serveur différent de celui auquel il s'attendait.

Cette section décrit comment utiliser les noms d'hôtes canonisés sur les clients IdM.

9.1. AJOUTER UN ALIAS À UN PRINCIPAL D'HÔTE

Par défaut, les clients de gestion d'identité (IdM) inscrits à l'aide de la commande **ipa-client-install** n'autorisent pas l'utilisation de noms d'hôtes courts dans les principaux services. Par exemple, les utilisateurs ne peuvent utiliser que **host/demo.example.com@EXAMPLE.COM** au lieu de **host/demo@EXAMPLE.COM** pour accéder à un service.

Cette section explique comment ajouter un alias à un principal Kerberos. Notez que vous pouvez également activer la canonisation des noms d'hôtes dans le fichier **/etc/krb5.conf**. Pour plus de détails, voir Activation de la canonisation des noms d'hôtes dans les principaux de service sur les clients .

Conditions préalables

- Le client IdM est installé.
- Le nom d'hôte est unique dans le réseau.

Procédure

1. S'authentifier auprès de l'IdM en tant qu'utilisateur de **admin**:

```
kinit admin
```

2. Ajoutez l'alias au principal de l'hôte. Par exemple, pour ajouter l'alias **demo** au principal de l'hôte **demo.examle.com**:

```
$ ipa host-add-principal demo.example.com --principal=demo
```

9.2. ACTIVATION DE LA CANONISATION DES NOMS D'HÔTES DANS LES SERVICES PRINCIPAUX SUR LES CLIENTS

Cette section explique comment activer la canonisation des noms d'hôtes dans les services principaux sur les clients.

Notez que si vous utilisez des alias de principal d'hôte, comme décrit dans Ajouter un alias à un principal d'hôte, vous n'avez pas besoin d'activer la canonisation.

Conditions préalables

- Le client Identity Management (IdM) est installé.

- Vous êtes connecté au client IdM en tant qu'utilisateur **root**.
- Le nom d'hôte est unique dans le réseau.

Procédure

1. Dans la section **[libdefaults]** du fichier **/etc/krb5.conf**, le paramètre **dns_canonicalize_hostname** doit être réglé sur **false**:

```
[libdefaults]
...
dns_canonicalize_hostname = true
```

9.3. OPTIONS POUR L'UTILISATION DES NOMS D'HÔTES LORSQUE LA CANONISATION DES NOMS D'HÔTES DNS EST ACTIVÉE

Si vous avez défini **dns_canonicalize_hostname = true** dans le fichier **/etc/krb5.conf** comme expliqué dans Activation de la canonisation des noms d'hôtes dans les mandants de service sur les clients , vous disposez des options suivantes lorsque vous utilisez un nom d'hôte dans un mandant de service :

- Dans les environnements de gestion des identités (IdM), vous pouvez utiliser le nom d'hôte complet dans un principal de service, tel que **host/demo.example.com@EXAMPLE.COM**.
- Dans les environnements sans IdM, mais si l'hôte RHEL est membre d'un domaine Active Directory (AD), aucune autre considération n'est nécessaire, car les contrôleurs de domaine AD (DC) créent automatiquement des mandants de service pour les noms NetBIOS des machines inscrites dans AD.