# Serveurs Kerberos pour AAA

Les rubriques suivantes expliquent comment configurer les serveurs Kerberos utilisés dans l'AAA. Vous pouvez utiliser des serveurs Kerberos pour l'authentification des connexions de gestion, l'accès réseau et l'accès utilisateur VPN.



# Lignes directrices relatives aux serveurs Kerberos pour AAA

- Vous pouvez avoir jusqu'à 200 groupes de serveurs en mode unique ou 8 groupes de serveurs par contexte en mode multiple.
- Chaque groupe peut avoir jusqu'à 16 serveurs en mode unique ou 8 serveurs en mode multiple. Lorsqu'un utilisateur se connecte, les serveurs sont accessibles un par un en commençant par le premier serveur que vous spécifiez dans la configuration, jusqu'à ce qu'un serveur réponde.

# Configurer les serveurs Kerberos pour AAA

Les rubriques suivantes expliquent comment configurer les groupes de serveurs Kerberos. Vous pouvez ensuite utiliser ces groupes lors de la configuration de l'accès de gestion ou des VPN.

## Configurer les groupes de serveurs AAA Kerberos

Si vous souhaitez utiliser un serveur Kerberos pour l'authentification, vous devez d'abord créer au moins un groupe de serveurs Kerberos et ajouter un ou plusieurs serveurs à chaque groupe.

### Procédure

**Étape 1** Créez le groupe de serveurs AAA Kerberos et passez en mode de configuration aaa-server-group.

**aaa-server** *server_group_name* **protocol kerberos**

**Exemple :**

```
ciscoasa(config)# aaa-server watchdog protocol kerberos
```

**Étape 2** (Facultatif) Précisez le nombre maximum de transactions AAA échouées avec un serveur AAA du groupe avant d'essayer le serveur suivant.

**max-failed-attempts** *number*

**Exemple :**

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

L'argument *number* peut aller de 1 à 5. La valeur par défaut est de 3.

Si vous avez configuré une méthode de secours à l'aide de la base de données locale (pour l'accès de gestion uniquement), et que tous les serveurs du groupe ne répondent pas ou que leurs réponses ne sont pas valides, le groupe est considéré comme ne répondant pas et la méthode de secours est essayée. Le groupe de serveurs reste marqué comme ne répondant pas pendant une période de 10 minutes (par défaut), de sorte que les demandes AAA supplémentaires effectuées dans cette période ne résultent pas en une tentative d'entrer en contact avec le groupe de serveurs et que la méthode de secours est utilisée immédiatement. Pour modifier la période de non-réponse par défaut, consultez la commande **reactivation-mode** à l'étape suivante.

Si vous n'avez pas de méthode de secours, l'ASA continue de réessayer les serveurs du groupe.

**Étape 3** (Facultatif) Précisez la méthode (politique de réactivation) par laquelle les serveurs défaillants d'un groupe sont réactivés.

**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**}

**Exemple :**

```
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
```

Le mot clé **depletion** réactive les serveurs défaillants uniquement après que tous les serveurs du groupe sont inactifs. Il s'agit du mode par défaut.

La paire mot clé-argument **deadtime** *minutes* spécifie le temps en minutes, entre 0 et 1 440, qui s'écoule entre la désactivation du dernier serveur du groupe et la réactivation ultérieure de tous les serveurs. Le temps mort s'applique uniquement si vous configurez le secours pour la base de données locale; l'authentification est tentée localement jusqu'à l'expiration du temps mort. La valeur par défaut est 10 minutes.

Le mot clé **timed** réactive les serveurs défaillants après 30 secondes d'arrêt.

**Étape 4** (Facultatif) Activer la validation du centre de distribution des clés Kerberos (KDC)

**validate-kdc**

**Exemple :**

```
ciscoasa(config-aaa-server-group)# validate-kdc
```

Pour réaliser l'authentification, vous devez également importer un fichier keytab que vous avez exporté du centre de distribution des clés Kerberos (KDC). En validant le KDC, vous pouvez empêcher une attaque où l'agresseur usurpe le KDC de sorte que les informations d'authentification de l'utilisateur soient authentifiées sur le serveur Kerberos de l'agresseur.

Pour savoir comment charger le fichier keytab, consultez Configurer la validation du centre de distribution des clés Kerberos, à la page 5.

### Exemple

L'exemple suivant crée un groupe de serveurs Kerberos nommé watchdogs, ajoute un serveur et définit le domaine sur EXEMPLE.COM.

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
hostname(config-aaa-server-host)# exit
hostname(config)#
```

# Ajouter des serveurs Kerberos à un groupe de serveurs Kerberos

Avant de pouvoir utiliser un groupe de serveurs Kerberos, vous devez ajouter au moins un serveur Kerberos au groupe.

### Procédure

**Étape 1** Ajoutez le serveur Kerberos au groupe de serveurs Kerberos.

**aaa-server** *server_group* [**(***interface_name***)**] **host** *server_ip*

**Exemple :**

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

Si vous ne spécifiez pas d'interface, l'ASA utilise par défaut la de l'interface **interne**.

Vous pouvez utiliser une adresse IPv4 ou IPv6.

**Étape 2** Spécifiez la valeur du délai d'expiration pour les tentatives de connexion au serveur.

**timeout** *seconds*

Spécifiez l'intervalle du délai d'expiration (1 à 300 secondes) du serveur; la valeur par défaut est de 10 secondes. Pour chaque transaction AAA, l'ASA relance les tentatives de connexion (en fonction de l'intervalle défini dans la commande **retry-interval**) jusqu'à ce que le délai d'expiration soit atteint. Si le nombre de transactions consécutives ayant échoué atteint la limite spécifiée dans la commande max-failed-attempts dans le groupe de serveurs AAA, le serveur AAA est désactivé et l'ASA commence à envoyer des demandes à un autre serveur AAA s'il est configuré.

**Exemple :**

```
ciscoasa(config-aaa-server-host)# timeout 15
```

**Étape 3** Spécifiez l'intervalle entre les tentatives, qui correspond au temps d'attente du système avant de réessayer une demande de connexion.

**retry-interval** *seconds*

Vous pouvez spécifier une valeur comprise entre 1 et 10 secondes. La valeur par défaut est 10.

**Exemple :**

```
ciscoasa(config-aaa-server-host)# retry-interval 6
```

**Étape 4** Spécifiez le port du serveur s'il diffère du port Kerberos par défaut, qui est TCP/88. L'ASA communique avec le serveur Kerberos sur ce port.

**server-port** *port_number*

**Exemple :**

```
ciscoasa(config-aaa-server-host)# server-port 8888
```

**Étape 5** Configurez le domaine Kerberos.

**kerberos-realm** *name*

Les noms de domaine Kerberos utilisent uniquement des chiffres et des lettres majuscules et peuvent comporter jusqu'à 64 caractères. Le nom doit correspondre à la sortie de la commande Microsoft Windows **set USERDNSDOMAIN** lorsqu'elle est exécutée sur le serveur Active Directory pour le domaine Kerberos. Dans l'exemple suivant, EXEMPLE.COM est le nom de domaine Kerberos :

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

Bien que l'ASA accepte les lettres minuscules dans le nom, il ne convertit pas les lettres minuscules en majuscules. Assurez-vous d'utiliser uniquement des lettres majuscules.

**Exemple :**

```
ciscoasa(config-asa-server-group)# kerberos-realm EXAMPLE.COM
```

---

**Exemple**

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

# Configurer la validation du centre de distribution des clés Kerberos

Vous pouvez configurer un groupe de serveurs AAA Kerberos pour authentifier les serveurs du groupe. Pour réaliser l'authentification, vous devez importer un fichier keytab que vous avez exporté du centre de distribution des clés Kerberos (KDC). En validant le KDC, vous pouvez empêcher une attaque où l'agresseur usurpe le KDC de sorte que les informations d'authentification de l'utilisateur soient authentifiées sur le serveur Kerberos de l'agresseur.

Lorsque vous activez la validation KDC, après avoir obtenu le billet d'octroi de billets (TGT) et validé l'utilisateur, le système demande également un billet de service au nom de l'utilisateur pour host/ASA_hostname. Le système valide ensuite le billet de service renvoyé par rapport à la clé secrète du KDC, qui est stockée dans un fichier keytab que vous avez généré à partir du KDC, puis téléchargé sur l'ASA. En cas d'échec de l'authentification KDC, le serveur est considéré comme non fiable et l'utilisateur n'est pas authentifié.

La procédure suivante explique comment réaliser l'authentification KDC.

### Avant de commencer

Vous ne pouvez pas utiliser la validation KDC conjointement avec la délégation Kerberos contrainte (KCD). La commande **validate-kdc** sera ignorée si le groupe de serveurs est utilisé pour le KCD.

### Procédure

**Étape 1** (Sur le KDC.) Créez un compte d'utilisateur dans Microsoft Active Directory pour l'ASA (accédez à **Start (Démarrage)** > **Programs (Programmes)** > **Administrative Tools (Outils administratifs)** > **Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory)**). Par exemple, si le nom de domaine complet (FQDN) de l'ASA est asahost.example.com, créez un utilisateur nommé asahost.

**Étape 2** (Sur le KDC.) Créez un nom principal de service d'hôte (SPN) pour l'ASA à l'aide du FQDN et du compte d'utilisateur :

```
C:> setspn -A HOST/asahost.example.com asahost
```

**Étape 3** (Sur le KDC.) Créez un fichier keytab pour l'ASA (des sauts de ligne ont été ajoutés pour plus de clarté) :

```
C:\Users\Administrator> ktpass /out new.keytab +rndPass
/princ host/asahost@EXAMPLE.COM
/mapuser asahost@example.com
/ptype KRB5_NT_SRV_HST
/mapop set
```

**Étape 4** (Sur l'ASA.) Importez le fichier keytab (dans cet exemple, new.keytab) dans l'ASA à l'aide de la commande **aaa kerberos import-keytab**.

```
ciscoasa(config)# aaa kerberos import-keytab ftp://ftpserver.example.com/new.keytab
ftp://ftpserver.example.com/new.keytab imported successfully
```

**Étape 5** (Sur l'ASA.) Ajoutez la commande **validate-kdc** à la configuration du groupe de serveurs AAA Kerberos. Le fichier keytab est utilisé uniquement par les groupes de serveurs qui contiennent cette commande.

```
ciscoasa(config)# aaa-server svrgrp1 protocol kerberos
ciscoasa(config-aaa-server-group)# validate-kdc
```

# Superviser les serveurs Kerberos pour AAA

Vous pouvez utiliser les commandes suivantes pour superviser et effacer les renseignements relatifs à Kerberos.

- **show aaa-server**

  Affiche les statistiques du serveur AAA. Utilisez la commande **clear aaa-server statistics** pour effacer les statistiques du serveur.

- **show running-config aaa-server**

  Affiche les serveurs AAA configurés pour le système. Utilisez la commande **clear configure aaa-server** pour supprimer la configuration du serveur AAA.

- **show aaa kerberos** [**username** *utilisateur*]

  Affiche tous les billets Kerberos ou les billets pour un nom d'utilisateur donné.

- **clear aaa kerberos tickets** [**username** *utilisateur*]

  Efface tous les billets Kerberos ou les billets pour un nom d'utilisateur donné.

- **show aaa kerberos keytab**

  Affiche des renseignements sur le fichier keytab Kerberos.

- **clear aaa kerberos keytab**

  Efface le fichier keytab Kerberos.

# Historique des serveurs Kerberos pour AAA

| Nom de la caractéristique | Versions de plateforme | Description |
|---|---|---|
| Serveurs Kerberos | 7.0(1) | Prise en charge des serveurs Kerberos pour AAA.<br>Nous avons introduit les commandes suivantes :<br>**aaa-server protocol**, **max-failed-attempts**, **reactivation-mode**, **aaa-server host**, **kerberos-realm**, **server-port**, **clear aaa-server statistics**, **clear configure aaa-server**, **show aaa-server**, **show running-config aaa-server**, **timeout**. |
| Adresses IPv6 pour AAA | 9.7(1) | Vous pouvez maintenant utiliser une adresse IPv4 ou IPv6 pour le serveur AAA. |

| Nom de la caractéristique | Versions de plateforme | Description |
|---|---|---|
| Augmentation des limites pour les groupes de serveurs AAA et le nombre de serveurs par groupe. | 9.13(1) | Vous pouvez configurer d'autres groupes de serveurs AAA. En mode de contexte unique, vous pouvez configurer 200 groupes de serveurs AAA (l'ancienne limite était de 100). En mode de contexte multiple, vous pouvez en configurer 8 (l'ancienne limite était de 4).<br><br>En outre, en mode de contexte multiple, vous pouvez configurer 8 serveurs par groupe (l'ancienne limite était de 4 serveurs par groupe). La limite de 16 par groupe en mode de contexte unique reste inchangée.<br><br>Nous avons modifié les commandes suivantes pour accepter ces nouvelles limites : **aaa-server**, **aaa-server host**. |
| Authentification du centre de distribution des clés Kerberos (KDC). | 9.8(4) et versions provisoires ultérieures jusqu'à 9.14(1) | Vous pouvez importer un fichier keytab à partir d'un centre de distribution de clés (KDC) Kerberos, et le système peut authentifier que le serveur Kerberos n'est pas falsifié avant de l'utiliser pour authentifier les utilisateurs. Pour réaliser l'authentification par KDC, vous devez configurer un nom de principal de service (SPN) **hôte**/*ASA_hostname* sur le KDC Kerberos, puis exporter un fichier keytab pour ce SPN. Vous devez ensuite charger le fichier keytab sur l'ASA et configurer le groupe de serveurs AAA Kerberos pour valider le KDC.<br><br>Nous avons ajouté les commandes suivantes : **aaa kerberos import-keytab**, **clear aaa kerberos keytab**, **show aaa kerberos keytab**, **validate-kdc**. |

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.