

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, à la page 1
- Configurer les serveurs Kerberos pour AAA, à la page 1
- Superviser les serveurs Kerberos pour AAA, à la page 5
- Historique des serveurs Kerberos pour AAA, à la page 5

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 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**.

Étape 2 Cliquez sur **Add** (Ajouter) dans le champ **AAA Server Groups** (Groupes de serveurs AAA).

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) apparaît.

Étape 3 Saisissez un nom pour le groupe dans le champ **Server Group** (Groupe de serveurs).

Étape 4 Dans la liste déroulante **Protocol** (Protocole), choisissez le type de serveur **Kerberos** :

Étape 5 Cliquez sur **Depletion** (Épuisement) ou **Timed** (Temporisé) dans le champ **Reactivation Mode** (Mode de réactivation).

En mode Depletion (Épuisement), les serveurs défaillants ne sont réactivés qu'une fois que tous les serveurs du groupe sont inactifs. En mode d'épuisement, lorsqu'un serveur est désactivé, il reste inactif jusqu'à ce que tous les autres serveurs du groupe soient inactifs. Lorsque et si cela se produit, tous les serveurs du groupe sont réactivés. Cette approche réduit le nombre de retards de connexion en raison de serveurs défaillants.

En mode Timed (Temporisé), les serveurs défaillants sont réactivés après 30 secondes de temps d'arrêt.

Étape 6 Si vous avez choisi le mode de réactivation Depletion (Épuisement), saisissez un intervalle de temps dans le champ **Dead Time** (Temps mort).

Le temps mort est la durée, en minutes, qui s'écoule entre la désactivation du dernier serveur d'un 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.

Étape 7 Précisez le nombre maximum de transactions AAA échouées avec un serveur AAA du groupe avant d'essayer le serveur suivant.

Cette option définit le nombre de transactions AAA ayant échoué avant de déclarer inactif un serveur qui ne répond pas.

Étape 8 (Facultatif) Sélectionnez **Validate KDC** (Valider le KDC) pour activer la validation du centre de distribution des clés de Kerberos (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 3.

Étape 9 Cliquez sur **OK**.

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 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**.

Étape 2 Sélectionnez le groupe de serveurs auquel vous souhaitez ajouter un serveur.

Étape 3 Cliquez sur **Add** (Ajouter) dans la zone **Servers in the Selected Group** (Serveurs du groupe sélectionné).

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) s'affiche pour le groupe de serveurs.

Étape 4 Choisissez l'**Interface Name** (Nom de l'interface) dans lequel se trouve le serveur d'authentification.

Étape 5 Saisissez le nom ou l'adresse IP du serveur que vous ajoutez au groupe.

Étape 6 Spécifiez la valeur du délai d'expiration pour les tentatives de connexion au serveur.

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 de nouvelle tentative) jusqu'à ce que le délai d'expiration soit atteint. Si le nombre de transactions consécutives ayant échoué atteint la limite maximum-failed-attempts spécifiée 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.

Étape 7 Sélectionnez l'intervalle entre les tentatives, qui correspond au temps d'attente du système avant de réessayer une demande de connexion. Vous pouvez sélectionner de 1 à 10 secondes. La valeur par défaut est de 10 secondes.

Étape 8 Spécifiez le Server Port (Port du serveur). Le port du serveur est le numéro de port 88 ou le numéro de port TCP utilisé par l'ASA pour communiquer avec le serveur Kerberos.

Étape 9 Configurez le domaine Kerberos.

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.

Étape 10 Cliquez sur **OK**.

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 option de validation 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.) Choisissez **Tools (Outils)** > **File Management (Gestion des fichiers)**, puis dans le menu **File Transfer (Transfert de fichiers)**, sélectionnez l'option appropriée pour charger le fichier keytab dans la mémoire flash, selon s'il se trouve sur votre ordinateur ou sur un serveur distant.

Étape 5 (Sur l'ASA.) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Kerberos**, puis cliquez sur **Browse Flash** (Parcourir la mémoire flash) et sélectionnez le fichier keytab chargé.

Étape 6 (Sur l'ASA.) Ajoutez l'option **Validate KDC** (Valider le KDC) à la configuration du groupe de serveurs AAA Kerberos. Le fichier keytab est utilisé uniquement par les groupes de serveurs configurés avec cette option.

a) Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**.

b) Sélectionnez le groupe de serveurs Kerberos et cliquez sur **Edit** (Modifier). Vous pouvez également créer un nouveau groupe à ce stade.

c) Sélectionnez l'option **Validate KDC** (Valider le KDC).
d) Cliquez sur **OK**.

Superviser les serveurs Kerberos pour AAA

Vous pouvez utiliser les commandes suivantes pour superviser et effacer les renseignements relatifs à Kerberos. Saisissez les commandes dans la fenêtre **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

- **Monitoring (Supervision)** > **Properties (Propriétés)** > **AAA Servers (Serveurs AAA)**

  Cette fenêtre affiche les statistiques du serveur AAA.

- **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. Nous avons introduit les écrans suivants : **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**
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). 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. Nous avons modifié les écrans AAA pour accepter ces nouvelles limites.
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. Nous avons ajouté ou modifié les écrans suivants : **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Kerberos**, **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)** Add/Edit dialog box for Kerberos server groups (Boîte de dialogue Ajouter/Modifier pour les groupes de serveurs Kerberos).

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.

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.

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.

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.

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.

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.

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.

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.