Configurer les serveurs RSA SecurID pour AAA

Les rubriques suivantes expliquent comment configurer les serveurs RSA SecurID utilisés dans l'AAA. Les serveurs RSA SecureID sont également connus sous le nom de serveurs SDI, car SDI est le protocole utilisé pour communiquer avec eux. Vous pouvez utiliser des serveurs RSA SecurID pour l'authentification des connexions de gestion, l'accès réseau et l'accès utilisateur VPN.

À propos des serveurs RSA SecurID

Vous pouvez utiliser des serveurs RSA SecurID directement pour l'authentification, ou indirectement, comme deuxième facteur d'authentification. Dans ce dernier cas, vous devez configurer la relation avec le serveur SecurID entre le serveur SecurID et votre serveur RADIUS, et configurer l'ASA pour utiliser le serveur RADIUS.

Mais, si vous souhaitez vous authentifier directement auprès du serveur SecurID, vous devez créer un groupe de serveurs AAA pour le protocole SDI, qui est le protocole utilisé pour communiquer avec ces serveurs.

Lorsque vous utilisez SDI, vous n'avez qu'à préciser le serveur SecurID principal lorsque vous créez le groupe de serveurs AAA. L'ASA récupérera le fichier sdiconf.rec, qui répertorie toutes les répliques de serveur SecurID, lors de sa première connexion au serveur. L'ASA peut ensuite utiliser ces répliques pour l'authentification si le serveur principal ne répond pas.

En outre, vous devez enregistrer l'ASA en tant qu'agent d'authentification dans le gestionnaire d'authentification RSA. Les tentatives d'authentification échoueront jusqu'à ce que vous enregistriez l'ASA.

Lignes directrices relatives aux serveurs RSA SecurID 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 RSA SecurID pour AAA

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

Configurer les groupes de serveurs RSA SecurID pour AAA

Si vous souhaitez utiliser la communication directe avec un serveur RSA SecurID pour l'authentification, vous devez d'abord créer au moins un groupe de serveurs SDI et ajouter un ou plusieurs serveurs à chaque groupe. Si vous utilisez le serveur SecurID dans une relation mandataire avec un serveur RADIUS, il n'est pas nécessaire de configurer un groupe de serveurs AAA SDI sur l'ASA.

Procédure

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

aaa-server *server_group_name* **protocol sdi**

Exemple :

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

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.

Ajouter des serveurs RSA SecurID à un groupe de serveurs SDI

Avant de pouvoir utiliser un groupe de serveurs SDI, vous devez ajouter au moins un serveur RSA SecurID au groupe.

Les serveurs d'un groupe de serveurs SDI utilisent le protocole d'authentification et de gestion de serveur (ACE) pour communiquer avec l'ASA.

Procédure

Étape 1 Ajoutez le serveur RSA SecurID au groupe de serveurs SDI.

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 RSA SecurID par défaut, qui est TCP/5500. L'ASA communique avec le serveur RSA SecurID sur ce port.

server-port *port_number*

Exemple :

```
ciscoasa(config-aaa-server-host)# server-port 5555
```

Importer le fichier secret de nœud SDI

Vous pouvez importer manuellement le fichier secret du nœud généré par le serveur RSA Authentication Manager (SecurID).

Procédure

Étape 1 Exportez le fichier secret du nœud à partir du serveur RSA Authentication Manager. Pour en savoir plus, consultez la documentation de RSA Authentication Manager.

Étape 2 Placez une version décompressée du fichier secret du nœud sur un serveur auquel vous pouvez accéder à partir de l'ASA ou copiez-la sur l'ASA lui-même.

Le serveur doit prendre en charge l'un des protocoles de transfert suivants : FTP, HTTP, HTTPS, SCP, SMB, TFTP.

Étape 3 Importez le fichier secret du nœud.

aaa sdi import-node-secret *filepath rsa_server_address password*

où :

- *filepath* est le chemin complet vers le fichier secret du nœud décompressé qui a été exporté depuis le RSA Authentication Manager. Les fichiers sur le système local peuvent être désignés par disk0:, disk1: ou flash:. Pour les fichiers sur un serveur distant, utilisez la notation d'URL standard, comme ftp://.
- *rsa_server_address* est l'adresse IP ou le nom d'hôte complet du serveur RSA Authentication Manager auquel appartient le secret du nœud.

• *password* est le mot de passe utilisé pour protéger le fichier lorsque vous l'avez exporté.

Exemple :

```
ciscoasa# aaa sdi import-node-secret nodesecret.rec rsaam.example.com mysecret
nodesecret.rec imported successfully
ciscoasa#
```

Superviser les serveurs RSA SecurID pour AAA

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

- **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 sdi node-secrets**

  Affiche les serveurs RSA SecurID qui ont un fichier secret de nœud importé. Utilisez la commande **clear aaa sdi node-secret** pour supprimer un fichier secret de nœud.

Historique des serveurs RSA SecurID pour AAA

Nom de la caractéristique	Versions de plateforme	Description
Serveurs SecurID	7.2(1)	Prise en charge des serveurs SecureID pour AAA pour l'authentification de gestion. SecureID était pris en charge dans les versions précédentes pour l'authentification VPN.
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 commandes suivantes pour accepter ces nouvelles limites : **aaa-server**, **aaa-server host**.
Importation manuelle du fichier secret du nœud à partir du gestionnaire d'authentification RSA pour les groupes de serveurs AAA SDI.	9.15(1)	Vous pouvez importer le fichier secret du nœud que vous exportez à partir du gestionnaire d'authentification RSA pour l'utiliser avec les groupes de serveurs AAA SDI. Nous avons ajouté les commandes suivantes : **aaa sdi import-node-secret**, **clear aaa sdi node-secret**, **show aaa sdi node-secrets**.

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.