

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, à la page 1
- Lignes directrices relatives aux serveurs RSA SecurID pour AAA, à la page 1
- Configurer les serveurs RSA SecurID pour AAA, à la page 2
- Superviser les serveurs RSA SecurID pour AAA, à la page 4
- Historique des serveurs RSA SecurID pour AAA, à la page 5

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 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 **SDI** :

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 Cliquez sur **OK**.

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 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 5500 par défaut ou le numéro de port TCP utilisé par l'ASA pour communiquer avec le serveur RSA SecurID.

Étape 9 Cliquez sur **OK**.

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 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA SDI**.

Étape 3 Cliquez sur **Upload** (Charger), sélectionnez le fichier secret du nœud décompressé qui a été exporté depuis le RSA Authentication Manager, puis chargez-le sur le système.

Étape 4 Sous **Import Node Secret for SDI** (Importer le secret du nœud pour SDI), saisissez les renseignements suivants :

- **Server IP** (Adresse IP du serveur) : l'adresse IP ou le nom d'hôte complet du serveur RSA Authentication Manager auquel appartient le secret du nœud.
- **Password** (Mot de passe) : le mot de passe utilisé pour protéger le fichier lorsque vous l'avez exporté.
- **File Name** (Nom de fichier) : cliquez sur **Browse** (Parcourir) et sélectionnez le fichier secret du nœud décompressé que vous avez chargé.

Superviser les serveurs RSA SecurID pour AAA

Vous pouvez utiliser les commandes suivantes pour superviser et effacer les renseignements relatifs à RSA SecurID. 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 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.
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.
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 l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA SDI**.

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.

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.