Serveurs TACACS+ pour AAA

Ce chapitre décrit comment configurer les serveurs TACACS+ utilisés dans AAA.

À propos des serveurs TACACS+ pour AAA

L'ASA prend en charge l'authentification du serveur TACACS+ avec les protocoles suivants : ASCII, PAP, CHAP et MS-CHAPv1.

Attributs TACACS+

L'ASA prend en charge les attributs TACACS+. Les attributs TACACS+ séparent les fonctions d'authentification, d'autorisation et de gestion de comptes. Le protocole prend en charge deux types d'attributs : obligatoires et facultatifs. Le serveur et le client doivent comprendre un attribut obligatoire, et l'attribut obligatoire doit être appliqué à l'utilisateur. Un attribut facultatif peut ne pas être compris ou utilisé.

Remarque Pour utiliser les attributs TACACS+, assurez-vous d'avoir activé les services AAA sur le NAS.

Le tableau suivant répertorie les attributs de réponse d'autorisation TACACS+ pris en charge pour les connexions de mandataire direct.

Tableau 1 : Attributs de réponse d'autorisation TACACS+ pris en charge

Attribut	Description
acl	Identifie une ACL configurée localement à appliquer à la connexion.
idletime	Indique la durée d'inactivité en minutes qui est autorisée avant la fin de la session de l'utilisateur authentifié.

Attribut	Description
timeout	Spécifie la durée absolue en minutes pendant laquelle les informations d'authentification restent actives avant la fin de la session de l'utilisateur authentifié.

Le tableau suivant répertorie les attributs de comptabilité TACACS+ pris en charge.

.

Tableau 2 : Attributs de comptabilité TACACS+ pris en charge

Attribut	Description
bytes_in	Spécifie le nombre d'octets d'entrée transférés lors de cette connexion (enregistrements d'arrêt uniquement).
bytes_out	Spécifie le nombre d'octets de sortie transférés lors de cette connexion (enregistrements d'arrêt uniquement).
CMD	Définit la commande exécutée (comptabilisation des commandes uniquement).
disc-cause	Indique le code numérique qui identifie la raison de la déconnexion (enregistrements d'arrêt uniquement).
elapsed_time	Définit le temps écoulé en secondes pour la connexion (enregistrements d'arrêt uniquement).
foreign_ip	Indique l'adresse IP du client pour les connexions du tunnel. Définit l'adresse sur l'interface de sécurité la plus basse pour les connexions de mandataire direct.
local_ip	Spécifie l'adresse IP à laquelle le client s'est connecté pour les connexions du tunnel. Définit l'adresse sur l'interface de sécurité la plus élevée pour les connexions de mandataire direct.
Port NAS	Contient un ID de session pour la connexion.
packs_in	Indique le nombre de paquets d'entrée transférés lors de cette connexion.
packs_out	Indique le nombre de paquets de sortie transférés lors de cette connexion.
priv-level	Définit le niveau de privilège de l'utilisateur pour les demandes de comptabilité des commandes ou 1 dans le cas contraire.
rem_iddr	Indique l'adresse IP du client.
service	Spécifie le service utilisé. Toujours défini sur « shell » pour la comptabilisation des commandes uniquement.
task_id	Spécifie un ID de tâche unique pour la transaction de comptabilité.
nom d'utilisateur	Indique le nom de l'utilisateur.

Lignes directrices relatives aux serveurs TACACS+ pour AAA

Cette section décrit les lignes directrices et les limites que vous devez vérifier avant de configurer les serveurs TACACS+ pour l'AAA.

IPv6

Le serveur AAA peut utiliser une adresse IPv4 ou IPv6.

Directives supplémentaires

- Vous pouvez avoir jusqu'à 200 groupes de serveurs en mode unique ou 4 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.
- Si vous configurez l'authentification à plusieurs facteurs avec ISE TACACS+ et Duo, vous devrez peut-être saisir à nouveau votre mot de passe lorsque vous établirez des connexions SSH après avoir confirmé la connexion avec Duo.
- Pour la série FPR1000, FPR2100 ou FPR3100 qui s'exécute sur l'ASA en mode appareil, vous devez vous conformer à ces conventions de nom d'utilisateur :
  - Les noms d'utilisateur doivent être valides sous Linux.
  - Ils doivent être uniquement en minuscules.
  - Ils peuvent inclure des caractères alphanumériques, des points (.) ou des tirets (-).
  - Ils ne doivent pas inclure d'autres caractères spéciaux tels que l'arobase (@) et la barre oblique (/).

Configurer les serveurs TACACS+

Cette section décrit comment configurer les serveurs TACACS+.

Procédure

Étape 1 Configurer les groupes de serveurs TACACS+, à la page 3.

Étape 2 Ajouter un serveur TACACS+ à un groupe, à la page 5.

Configurer les groupes de serveurs TACACS+

Si vous souhaitez utiliser un serveur TACACS+ pour l'authentification, l'autorisation ou la gestion de comptes, vous devez d'abord créer au moins un groupe de serveurs TACACS+ et ajouter un ou plusieurs serveurs à chaque groupe. Vous identifiez les groupes de serveurs TACACS+ par leur nom.

Pour ajouter un groupe de serveurs TACACS+, procédez comme suit :

Procédure

Étape 1 Identifiez le nom du groupe de serveurs et le protocole.

aaa-server *server_tag* **protocol tacacs+**

Exemple :

```
ciscoasa(config)# aaa-server servergroup1 protocol tacacs+
```

Lorsque vous saisissez la commande **aaa-server protocol**, vous passez en mode de configuration du groupe aaa-server.

Étape 2 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 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.

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 Envoyez des messages de traçabilité à tous les serveurs du groupe.

accounting-mode simultaneous

Exemple :

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

Pour rétablir la valeur par défaut d'envoi de messages uniquement au serveur actif, saisissez la commande **accounting-mode single**.

Exemple

L'exemple suivant montre comment ajouter un groupe TACACS+ avec un serveur principal et un serveur de sauvegarde:

```
ciscoasa(config)# aaa-server AuthInbound protocol tacacs+
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.1
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.2
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey2
ciscoasa(config-aaa-server-host)# exit
```

Ajouter un serveur TACACS+ à un groupe

Pour ajouter un serveur TACACS+ à un groupe, procédez comme suit :

Procédure

Étape 1 Identifiez le serveur TACACS+ et le groupe de serveurs auquel il appartient.

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 de **(***nom d'interface***)**, l'ASA utilise la de l'interface **interne** par défaut.

Le serveur peut 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 le port du serveur comme numéro de port 49 ou le numéro de port TCP utilisé par l'ASA pour communiquer avec le serveur TACACS+.

server-port *port_number*

Exemple :

```
ciscoasa(config-aaa-server-host)# server-port 49
```

Étape 4 Spécifiez la valeur secrète du serveur utilisée pour authentifier le NAS auprès du serveur TACACS+.

key

Exemple :

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

Cette valeur est un mot clé alphanumérique sensible à la casse pouvant comporter jusqu'à 127 caractères, ce qui correspond à la même valeur que la clé sur le serveur TACACS+. Tout caractère au-delà de 127 est ignoré. La clé est utilisée entre le client et le serveur pour chiffrer les données entre eux et doit être identique sur les systèmes du client et du serveur. La clé ne peut pas contenir d'espaces, mais d'autres caractères spéciaux sont autorisés.

Supervision des serveurs TACACS+ pour AAA

Consultez les commandes suivantes pour superviser les serveurs TACACS+ pour AAA :

- **show aaa-server**

  Cette commande affiche les statistiques du serveur TACACS+ configuré. Saisissez la commande **clear aaa-server statistics** pour effacer les statistiques du serveur TACACS+.

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

  Cette commande montre la configuration en cours d'exécution du serveur TACACS+. Saisissez la commande **clear configure aaa-server** pour effacer la configuration du serveur TACACS+.

Historique des serveurs TACACS+ pour AAA

Tableau 3 : Historique des serveurs TACACS+ pour AAA

Nom de la caractéristique	Versions de plateforme	Description
Serveurs TACACS+	7.0(1)	Décrit comment configurer les serveurs TACACS+ pour AAA. Nous avons introduit les commandes suivantes : **aaa-server protocol**, **max-failed-attempts, reactivation-mode, accounting-mode simultaneous, aaa-server host, aaa authorization exec authentication-server**, **server-port, key**, **clear aaa-server statistics**, **clear configure aaa-server**, **show aaa-server**, **show running-config aaa-server**, **username**, **service-type**, **timeout**.
Serveurs TACACS+ avec 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 commandes suivantes pour accepter ces nouvelles limites : **aaa-server**, **aaa-server host**.

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.