

Serveurs TACACS+ pour AAA

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

- À propos des serveurs TACACS+ pour AAA, à la page 1
- Lignes directrices relatives aux serveurs TACACS+ pour AAA, à la page 3
- Configurer les serveurs TACACS+, à la page 3
- Tester l'authentification et l'autorisation des serveurs TACACS+, à la page 6
- Supervision des serveurs TACACS+ pour AAA, à la page 7
- Historique des serveurs TACACS+ pour AAA, à la page 8

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 4.

Étape 3 (Facultatif) Ajouter une invite d'authentification, 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 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 **TACACS+** :

Étape 5 Cliquez sur **Simultaneous** ou **Single (Single)** dans le champ **Accounting Mode (Mode de comptabilité)**.

En mode unique, l'ASA envoie des données comptables à un seul serveur.

En mode simultané, l'ASA envoie des données comptables à tous les serveurs du groupe.

Étape 6 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 7 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 8 Ajoutez le nombre maximum de transactions AAA échouées avec un serveur à autoriser.

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

Étape 9 Cliquez sur **OK**.

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) se ferme et le nouveau groupe de serveurs est ajouté au tableau **AAA Server Groups** (Groupes de serveurs AAA).

Étape 10 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Ajouter un serveur TACACS+ à un groupe

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

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 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 le nom de l'interface sur laquelle se trouve le serveur d'authentification.

Étape 5 Ajoutez un nom de serveur ou une adresse IP pour le 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 Spécifiez le Server Port (Port du serveur). Le port du serveur est le numéro de port 139 ou le numéro de port TCP utilisé par l'ASA pour communiquer avec le serveur TACACS+.

Étape 8 Spécifiez la clé secrète du serveur. La clé secrète partagée utilisée pour authentifier le serveur TACACS+ auprès de l'ASA. La clé secrète du serveur que vous configurez ici doit correspondre à celle configurée sur le serveur TACACS+. Si vous ne connaissez pas la clé secrète du serveur, demandez à l'administrateur du serveur TACACS+. La longueur maximale du champ est de 64 caractères.

Étape 9 Cliquez sur **OK**.

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) se ferme et le serveur AAA est ajouté au groupe de serveurs AAA.

Étape 10 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Ajouter une invite d'authentification

Vous pouvez spécifier le texte à afficher à l'utilisateur pendant le processus de défi d'authentification AAA. Vous pouvez spécifier le texte de défi AAA pour l'accès HTTP, FTP et Telnet par l'intermédiaire de l'ASA lors de la demande d'authentification de l'utilisateur sur les serveurs TACACS+. Ce texte est principalement cosmétique et apparaît au-dessus des invites de nom d'utilisateur et de mot de passe que les utilisateurs voient lorsqu'ils se connectent.

Si vous ne spécifiez pas d'invite d'authentification, les utilisateurs voient les éléments suivants lorsqu'ils s'authentifient auprès d'un serveur TACACS+ :

Type de connexion	Invite par défaut
FTP	Authentification FTP

Type de connexion	Invite par défaut
HTTP	Authentification HTTP
Telnet	Aucune

Pour ajouter une invite d'authentification, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **Authentication Prompt (Invite d'authentification)**.

Étape 2 Ajoutez du texte pour qu'il s'affiche au-dessus des invites de nom d'utilisateur et de mot de passe que les utilisateurs voient lorsqu'ils se connectent.

Le tableau suivant affiche les limites de caractères autorisées pour les invites d'authentification :

Application	Limite de caractères pour l'invite d'authentification
Microsoft Internet Explorer	37
Telnet	235.
FTP	235.

Étape 3 Ajoutez des messages dans les champs **User accepted message** (Message accepté par l'utilisateur) et **User rejected message** (Message refusé par l'utilisateur).

Si l'authentification de l'utilisateur a lieu à partir de Telnet, vous pouvez utiliser les options **User accepted message** (Message accepté par l'utilisateur) et **User rejected message** (Message refusé par l'utilisateur) pour afficher différents états afin d'indiquer que la tentative d'authentification est acceptée ou refusée par le serveur AAA.

Si le serveur AAA authentifie l'utilisateur, l'ASA affiche le texte **User accepted message** (Message accepté par l'utilisateur), si spécifié, à l'utilisateur; sinon, l'ASA affiche le texte **User rejected message** (Message refusé par l'utilisateur), si cela est spécifié. L'authentification des sessions HTTP et FTP affiche uniquement le texte de défi à l'invite. Le texte des messages acceptés ou refusés par l'utilisateur ne s'affiche pas.

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Tester l'authentification et l'autorisation des serveurs TACACS+

Pour déterminer si l'ASA peut communiquer avec un serveur TACACS+ et authentifier ou autoriser un utilisateur, procédez comme suit :

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 le groupe de serveurs dans lequel se trouve le serveur.

Étape 3 Cliquez sur le serveur que vous souhaitez tester.

Étape 4 Cliquez sur **Test**.

La boîte de dialogue **Test AAA Server** (Tester un serveur AAA) s'affiche pour le groupe de serveurs sélectionné.

Étape 5 Cliquez sur le type de test que vous souhaitez effectuer : **Authentication** (Authentification) ou **Authorization** (Autorisation).

Étape 6 Saisissez un nom d'utilisateur.

Étape 7 Si vous testez l'authentification, saisissez le mot de passe correspondant au nom d'utilisateur.

Étape 8 Cliquez sur **OK**.

L'ASA envoie un message de test d'authentification ou d'autorisation au serveur. Si le test échoue, un message d'erreur s'affiche.

Supervision des serveurs TACACS+ pour AAA

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

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

  Ce volet affiche les statistiques du serveur TACACS+ configuré.

- **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**

  Ce volet vous permet d'exécuter diverses commandes non interactives et d'afficher les résultats.

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 écrans suivants : Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Server Groups (Groupes de serveurs AAA) Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > Authentication Prompt (Invite d'authentification)
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 écrans AAA pour accepter ces nouvelles limites.

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.

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.