AAA et base de données locale

Ce chapitre décrit l'authentification, l'autorisation et la traçabilité (AAA, prononcé « trois A »). Le protocole AAA regroupe un ensemble de services destinés à contrôler l'accès aux ressources informatiques, à appliquer des politiques, à évaluer l'utilisation et à fournir les renseignements nécessaires pour facturer les services. Ces processus sont considérés comme importants pour une gestion et une sécurité efficaces du réseau.

Ce chapitre décrit également comment configurer la base de données locale pour la fonctionnalité AAA. Pour les serveurs AAA externes, consultez le chapitre correspondant à votre type de serveur.

À propos d'AAA et de la base de données locale

Cette section décrit AAA et la base de données locale.

Authentification

L'authentification fournit un moyen d'identifier un utilisateur, généralement en demandant à l'utilisateur de saisir un nom d'utilisateur et un mot de passe valides avant que l'accès ne soit accordé. Le serveur AAA compare les renseignements d'authentification d'un utilisateur à ceux d'autres utilisateurs stockés dans une base de données. Si les renseignements d'authentification correspondent, l'utilisateur est autorisé à accéder au réseau. Dans le cas contraire, l'authentification échoue et l'accès au réseau est refusé.

Vous pouvez configurer l'ASA pour authentifier les éléments suivants :

- Toutes les connexions administratives à l'ASA, y compris les sessions suivantes :
  - Telnet
  - SSH
  - Console de série
  - ASDM à l'aide de HTTPS
  - Accès à la gestion du VPN

- La commande **enable**
- Accès au réseau
- Accès VPN

Autorisation

L'autorisation est le processus d'application des politiques : qui détermine les types d'activités, de ressources ou de services auxquels un utilisateur est autorisé à accéder. Une fois qu'un utilisateur est authentifié, cet utilisateur peut être autorisé pour différents types d'accès ou d'activités.

Vous pouvez configurer l'ASA pour autoriser les éléments suivants :

- Commandes de gestion
- Accès au réseau
- Accès VPN

Comptabilité

La comptabilité mesure les ressources qu'un utilisateur consomme lors de l'accès, qui peuvent inclure la durée du système ou la quantité de données qu'un utilisateur a envoyées ou reçues au cours d'une session. La comptabilisation est effectuée au moyen de la journalisation des statistiques de session et des renseignements d'utilisation, qui sont utilisés pour les activités de contrôle des autorisations, de facturation, d'analyse des tendances, d'utilisation des ressources et de planification de la capacité.

Interaction entre authentification, autorisation et traçabilité

Vous pouvez utiliser l'authentification seule ou avec l'autorisation et la comptabilité. L'autorisation nécessite toujours qu'un utilisateur soit d'abord authentifié. Vous pouvez utiliser la comptabilité seule ou avec l'authentification et l'autorisation.

Serveurs et groupes de serveurs AAA

Le serveur AAA est un serveur de réseau utilisé pour le contrôle d'accès. L'authentification identifie l'utilisateur. L'autorisation met en œuvre des politiques qui déterminent les ressources et les services auxquels un utilisateur authentifié peut accéder. La comptabilité fait le suivi des ressources de temps et de données utilisées pour la facturation et l'analyse.

Si vous souhaitez utiliser un serveur AAA externe, vous devez d'abord créer un groupe de serveurs AAA pour le protocole utilisé par le serveur externe et ajouter le serveur au groupe. Vous pouvez créer plusieurs groupes par protocole et des groupes distincts pour tous les protocoles que vous souhaitez utiliser. Chaque groupe de serveurs est propre à un type de serveur ou de service.

Consultez les rubriques suivantes pour en savoir plus sur la création des groupes :

- Configurer les groupes de serveurs RADIUS
- Configurer les groupes de serveurs TACACS+
- Configurer les groupes de serveurs LDAP

- Configurer les groupes de serveurs AAA Kerberos
- Configurer les groupes de serveurs RSA SecurID pour AAA

Consultez le guide de configuration de VPN pour en savoir plus sur l'utilisation de la délégation sous contraintes de Kerberos et du formulaire HTTP.

Le tableau suivant résume les types de serveurs pris en charge et leurs utilisations, y compris la base de données locale.

Tableau 1 : Services pris en charge pour les serveurs AAA

Type de serveur et service	Authentification	Autorisation	Gestion de comptes
Base de données locale			
Administrateurs	Oui	Oui	Non
Utilisateurs VPN	Oui	Non	Non
Sessions de pare-feu (règles AAA)	Oui	Oui	Non
RADIUS			
Administrateurs	Oui	Oui	Oui
Utilisateurs VPN	Oui	Oui	Oui
Sessions de pare-feu (règles AAA)	Oui	Oui	Oui
TACACS+			
Administrateurs	Oui	Oui	Oui
Utilisateurs VPN	Oui	Non	Oui
Sessions de pare-feu (règles AAA)	Oui	Oui	Oui
LDAP			
Administrateurs	Oui	Non	Non
Utilisateurs VPN	Oui	Oui	Non
Sessions de pare-feu (règles AAA)	Oui	Non	Non
Kerberos			
Administrateurs	Oui	Non	Non
Utilisateurs VPN	Oui	Non	Non

Type de serveur et service	Authentification	Autorisation	Gestion de comptes
Sessions de pare-feu (règles AAA)	Oui	Non	Non
SDI (RSA SecurID)			
Administrateurs	Oui	Non	Non
Utilisateurs VPN	Oui	Non	Non
Sessions de pare-feu (règles AAA)	Oui	Non	Non
Formulaire HTTP			
Administrateurs	Non	Non	Non
Utilisateurs VPN	Oui	Non	Non
Sessions de pare-feu (règles AAA)	Non	Non	Non

Notes

- RADIUS : la comptabilisation des administrateurs n'inclut pas la comptabilisation des commandes.
- RADIUS : l'autorisation des sessions de pare-feu est prise en charge uniquement avec les listes d'accès spécifiques à l'utilisateur, qui sont reçues ou spécifiées dans une réponse à la demande d'authentification RADIUS.
- TACACS+ : la comptabilisation des administrateurs comprend la comptabilisation des commandes.
- Formulaire HTTP : opérations d'authentification et SSO pour les sessions utilisateur du SSL VPN sans client uniquement.

À propos de la base de données locale

L'ASA gère une base de données locale que vous pouvez remplir avec les profils d'utilisateurs. Vous pouvez utiliser une base de données locale au lieu de serveurs AAA pour assurer l'authentification, l'autorisation et la traçabilité des utilisateurs.

Vous pouvez utiliser la base de données locale pour les fonctions suivantes :

- Accès à ASDM par utilisateur
- Authentification de la console
- Authentification Telnet et SSH
- Authentification de la commande **enable**

  Ce paramètre est réservé à l'accès à l'interface de ligne de commande et n'influe pas sur la connexion à Cisco ASDM.
- Autorisation de commande

Si vous activez l'autorisation de commande à l'aide de la base de données locale, l'ASA fait référence au niveau de privilège de l'utilisateur pour déterminer quelles commandes sont disponibles. Sinon, le niveau de privilège n'est généralement pas utilisé. Par défaut, toutes les commandes sont de niveau de privilège 0 ou de niveau 15.

- Authentification d'accès au réseau
- Authentification du client VPN

Pour le mode de contexte multiple, vous pouvez configurer les noms d'utilisateur dans l'espace d'exécution du système pour fournir des connexions individuelles au niveau de l'interface de ligne de commande à l'aide de la commande **login**; cependant, vous ne pouvez pas configurer de règles AAA qui utilisent la base de données locale dans l'espace d'exécution du système.

Remarque Vous ne pouvez pas utiliser la base de données locale pour l'autorisation d'accès au réseau.

Prise en charge du basculement

La base de données locale peut servir de méthode de secours pour plusieurs fonctions. Ce comportement est conçu pour vous aider à éviter le verrouillage accidentel de l'ASA.

Lorsqu'un utilisateur se connecte, les serveurs du groupe sont accessibles un par un en commençant par le premier serveur que vous spécifiez dans la configuration, jusqu'à ce qu'un serveur réponde. Si tous les serveurs du groupe sont indisponibles, l'ASA essaie la base de données locale si vous l'avez configurée comme méthode de secours (pour l'authentification et l'autorisation de gestion uniquement). Si vous n'avez pas de méthode de secours, l'ASA continue d'essayer les serveurs AAA.

Pour les utilisateurs qui ont besoin d'une prise en charge de secours, nous recommandons que leurs noms d'utilisateur et mots de passe dans la base de données locale correspondent à leurs noms d'utilisateur et mots de passe sur les serveurs AAA. Cette pratique offre une prise en charge de secours transparente. Étant donné que l'utilisateur ne peut pas déterminer si un serveur AAA ou la base de données locale fournit le service, l'utilisation de noms d'utilisateur et de mots de passe sur des serveurs AAA qui sont différents de ceux de la base de données locale signifie que l'utilisateur ne peut pas être certain du nom d'utilisateur et du mot de passe à fournir.

La base de données locale prend en charge les fonctions de secours suivantes :

- Console et activation de l'authentification par mot de passe : si les serveurs du groupe sont tous indisponibles, l'ASA utilise la base de données locale pour authentifier l'accès administratif, qui peut également inclure l'activation de l'authentification par mot de passe.
- Autorisation de commande : si les serveurs TACACS+ du groupe sont tous indisponibles, la base de données locale est utilisée pour autoriser les commandes en fonction des niveaux de privilège.
- Authentification et autorisation VPN : l'authentification et l'autorisation VPN sont prises en charge pour permettre l'accès à distance à l'ASA si les serveurs AAA qui prennent normalement en charge ces services VPN ne sont pas disponibles. Lorsqu'un client VPN d'un administrateur spécifie un groupe de tunnels configuré pour un basculement vers la base de données locale, le tunnel VPN peut être établi même si le groupe de serveurs AAA n'est pas disponible, à condition que la base de données locale soit configurée avec les attributs nécessaires.

Fonctionnement du basculement avec plusieurs serveurs dans un groupe

Si vous configurez plusieurs serveurs dans un groupe de serveurs et que vous activez le basculement vers la base de données locale pour le groupe de serveurs, le basculement se produit lorsqu'aucun serveur du groupe ne répond à la demande d'authentification de l'ASA. Par exemple, envisagez le scénario suivant :

Vous configurez un groupe de serveurs LDAP avec deux serveurs Active Directory, le serveur 1 et le serveur 2, dans cet ordre. Lorsque l'utilisateur distant se connecte, l'ASA tente de s'authentifier auprès du serveur 1.

Si le serveur 1 répond par un échec d'authentification (par exemple, un utilisateur introuvable), l'ASA ne tente pas de s'authentifier auprès du serveur 2.

Si le serveur 1 ne répond pas dans le délai d'expiration (ou si le nombre de tentatives d'authentification dépasse le maximum configuré), l'ASA essaie le serveur 2.

Si les deux serveurs du groupe ne répondent pas et que l'ASA est configuré pour revenir à la base de données locale, l'ASA tente de s'authentifier auprès de la base de données locale.

Remarque Par défaut, un client RADIUS envoie trois demandes avant d'expirer. Lorsque le client tente d'établir une connexion SSH, la demande est envoyée à un serveur à la fois. À l'expiration des demandes, le serveur est marqué comme ayant ÉCHOUÉ. La prochaine demande RADIUS est envoyée au serveur ACTIF suivant, marquant par la suite tous les serveurs comme ayant ÉCHOUÉ et revenant finalement à l'authentification LOCALE (si elle est configurée). Les serveurs marqués comme ayant ÉCHOUÉ finissent par se rétablir et sont rendus ACTIFS. Dans ce cas, si vous avez 3 ou 4 serveurs dans le groupe, vous pourriez observer des problèmes de connexion intermittents.

Lignes directrices relatives à la base de données locale

Assurez-vous d'empêcher un verrouillage de l'ASA lorsque vous utilisez la base de données locale pour l'authentification ou l'autorisation.

Ajouter un compte d'utilisateur à la base de données locale

Pour ajouter un utilisateur à la base de données locale, procédez comme suit :

Procédure

Étape 1 Créez un compte utilisateur.

username *username* [**password** *password*] [**privilege** *priv_level*]

Exemple :

```
ciscoasa(config)# username exampleuser1 password madmaxfuryroadrules privilege 1
```

Le mot clé**username** *username* est une chaîne de 3 à 64 caractères, utilisant n'importe quelle combinaison de caractères imprimables ASCII (codes 32 à 126), à l'exception des espaces et du point d'interrogation. Le

mot clé **password** *password* est une chaîne de 8 à 127 caractères. Il peut s'agir de n'importe quelle combinaison de caractères imprimables ASCII (codes 32 à 126), avec les exceptions suivantes :

- Aucun espace
- Aucun point d'interrogation
- Il est interdit d'utiliser trois caractères ASCII (ou plus) qui se suivent ou qui se répètent. Par exemple, les mots de passe suivants seront refusés :
  - **abc**utilisateur1
  - utilisateur**543**
  - utilisateur**aaaa**
  - utilisateur2**666**

Par exemple, vous souhaiterez peut-être créer un nom d'utilisateur sans mot de passe si vous utilisez l'authentification par clé publique SSH. Le mot clé **privilege** *priv_level* définit le niveau de privilège, qui varie de 0 à 15. La valeur par défaut est 2. Ce niveau de privilège est utilisé avec l'autorisation de commande.

Mise en garde
Si vous n'utilisez pas l'autorisation de commande (la commande **aaa authorization console LOCAL**), le niveau par défaut 2 permet l'accès de gestion au mode d'exécution privilégié. Si vous souhaitez limiter l'accès au mode d'exécution privilégié, définissez le niveau de privilège à 0 ou 1, ou utilisez la commande **service-type**.

Ces options moins utilisées ne s'affichent pas dans la syntaxe ci-dessus : le mot clé **nopassword** crée un compte d'utilisateur qui accepte n'importe quel mot de passe; cette option n'est pas sécurisée et n'est pas conseillée.

Le mot clé **encrypted** (pour les mots de passe de 32 caractères ou moins dans les versions 9.6 et antérieures) ou le mot clé **pbkdf2** (pour les mots de passe de plus de 32 caractères dans les versions 9.6 et ultérieures, et les mots de passe de toutes les longueurs dans les versions 9.7 et ultérieures) indique que le mot de passe est chiffré (à l'aide d'un hachage basé sur MD5 ou d'un hachage PBCDF2 (Password-Based Key Derivation Function 2)). Notez que les mots de passe existants continuent d'utiliser le hachage basé sur MD5, sauf si vous entrez un nouveau mot de passe. Lorsque vous définissez un mot de passe dans la commande **username**, l'ASA le chiffre avant de l'enregistrer dans la configuration à des fins de sécurité. Lorsque vous entrez la commande **show running-config**, la commande **username** n'affiche pas le mot de passe réel. Elle affiche le mot de passe chiffré suivi du mot clé **encrypted** ou **pbkdf2**. Par exemple, si vous entrez le mot de passe « test », la sortie de la commande **show running-config** se présentera comme suit :

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

Vous ne saisirez le mot clé **encrypted** ou **pbkdf2** dans l'interface de ligne de commande que si vous coupez-collez un fichier de configuration pour l'utiliser dans un autre ASA et que vous utilisez le même mot de passe.

Étape 2 (Facultatif) Configurez les attributs de nom d'utilisateur.

username *nom d'utilisateur* **attributes**

Exemple :

```
ciscoasa(config)# username exampleuser1 attributes
```

L'argument *username* est le nom d'utilisateur que vous avez créé à la première étape.

Par défaut, les utilisateurs VPN que vous ajoutez avec cette commande n'ont aucun attribut ni association de stratégie de groupe. Vous devez configurer toutes les valeurs explicitement à l'aide de la commande **username attributes**. Consultez le guide de configuration de VPN pour en savoir plus.

Étape 3 (Facultatif) Configurez le niveau d'utilisateur si vous avez configuré l'autorisation de gestion à l'aide de la commande **aaa authorization exec**.

service-type {**admin** | **nas-prompt** | **remote-access**}

Exemple :

```
ciscoasa(config-username)# service-type admin
```

Le mot clé **admin** permet un accès complet à tous les services spécifiés par les commandes **aaa authentication console LOCAL**. Le mot clé **admin** est la valeur par défaut.

Le mot clé **nas-prompt** permet l'accès à l'interface de ligne de commande lorsque vous configurez la commande **aaa authentication** {**telnet** | **ssh** | **serial**} **console**, mais refuse l'accès à la configuration ASDM si vous configurez la commande **aaa authentication http console**. L'accès à la surveillance ASDM est autorisé. Si vous activez l'authentification avec la commande **aaa authentication enable console**, l'utilisateur ne peut pas accéder au mode d'exécution privilégié à l'aide de la commande **enable** (ou de la commande **login**).

Le mot clé **remote-access** refuse l'accès de gestion. Vous ne pouvez pas utiliser les services spécifiés par les commandes **aaa authentication console** (à l'exception du mot clé **serial**, l'accès série est autorisé).

Étape 4 (Facultatif) Pour l'authentification par clé publique des connexions SSH à l'ASA par utilisateur, consultez Configurer SSH pour l'accès par clé publique.

Étape 5 (Facultatif) Si vous utilisez ce nom d'utilisateur pour l'authentification VPN, vous pouvez configurer de nombreux attributs VPN pour l'utilisateur. Consultez le guide de configuration de VPN pour en savoir plus.

Exemples

L'exemple suivant attribue un niveau de privilège de 15 au compte d'utilisateur admin :

```
ciscoasa(config)# username admin password farscape1 privilege 15
```

L'exemple suivant active l'autorisation de gestion, crée un compte d'utilisateur avec un mot de passe, passe en mode de configuration du nom d'utilisateur et spécifie un **service-type** de **nas-prompt** :

```
ciscoasa(config)# aaa authorization exec authentication-server
ciscoasa(config)# username user1 password gOrgeOus
ciscoasa(config)# username user1 attributes
ciscoasa(config-username)# service-type nas-prompt
```

Supervision de la base de données locale

Consultez les commandes suivantes pour superviser la base de données locale :

- **show aaa-server**

  Cette commande affiche les statistiques de la base de données configurée. Pour effacer les statistiques du serveur AAA, saisissez la commande **clear aaa-server statistics**.

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

  Cette commande montre la configuration en cours d'exécution du serveur AAA. Pour effacer la configuration du serveur AAA, saisissez la commande **clear configure aaa-server**.

Historique de la base de données locale

Tableau 2 : Historique de la base de données locale

Nom de la caractéristique	Versions de plateforme	Description
Configuration de la base de données locale pour AAA	7.0(1)	Décrit comment configurer la base de données locale pour une utilisation AAA. Nous avons introduit les commandes suivantes : **username**, **aaa authorization exec authentication-server**, **aaa authentication console LOCAL**, **aaa authorization exec LOCAL**, **service-type, aaa authentication** {**telnet | ssh | serial**} **console LOCAL**, **aaa authentication http console LOCAL**, **aaa authentication enable console LOCAL**, **show running-config aaa-server**, **show aaa-server**, **clear configure aaa-server**, **clear aaa-server statistics**.
Prise en charge de l'authentification par clé publique SSH	9.1(2)	Vous pouvez désormais activer l'authentification par clé publique pour les connexions SSH à l'ASA par utilisateur. Vous pouvez spécifier une clé formatée de fichier de clé publique (PKF) ou une clé Base64. La clé PKF peut comporter jusqu'à 4 096 bits. Utilisez le format PKF pour les clés qui sont trop grandes pour la prise en charge ASA du format Base64 (jusqu'à 2 048 bits). Nous avons introduit les commandes suivantes : **ssh authentication**. *Également disponible dans 8.4(4.1); la prise en charge du format de clé PKF uniquement dans 9.1(2).*

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de mots de passe plus longs pour les mots de passe locaux **username** et **enable** (jusqu'à 127 caractères)	9.6(1)	Vous pouvez désormais créer des mots de passe **username** et **enable** locaux jusqu'à 127 caractères (l'ancienne limite était de 32). Lorsque vous créez un mot de passe de plus de 32 caractères, il est stocké dans la configuration à l'aide d'un hachage PBCDF2 (Password-Based Key Derivation Function 2). Les mots de passe plus courts continuent d'utiliser la méthode de hachage basée sur MD5. Nous avons modifié les commandes suivantes : **enable, username**
Améliorations de l'authentification par clé publique SSH	9.6(2)	Dans les versions antérieures, vous pouviez activer l'authentification par clé publique SSH (**ssh authentication**) sans activer également l'authentification SSH AAA avec la base de données d'utilisateurs locale (**aaa authentication ssh console LOCAL**). La configuration est désormais modifiée de manière à ce que vous deviez explicitement activer l'authentification SSH AAA. Pour empêcher les utilisateurs d'utiliser un mot de passe au lieu de la clé privée, vous pouvez désormais créer un nom d'utilisateur sans mot de passe défini. Nous avons modifié les commandes suivantes : **ssh authentication, username**
Hachage PBKDF2 pour tous les mots de passe locaux **username** et **enable**	9.7(1)	Les mots de passe locaux **username** et **enable** de toutes les longueurs sont stockés dans la configuration à l'aide du hachage PBKDF2 (Password-Based Key Derivation Function 2). Auparavant, les mots de passe de 32 caractères et moins utilisaient la méthode de hachage basée sur MD5. Les mots de passe existants continuent d'utiliser le hachage basé sur MD5, sauf si vous entrez un nouveau mot de passe. Consultez le chapitre « Logiciels et configurations » du Guide de configuration des opérations générales pour connaître les lignes directrices relatives à la rétrogradation. Nous avons modifié les commandes suivantes : **enable, username**

Nom de la caractéristique	Versions de plateforme	Description
Authentification distincte pour les utilisateurs disposant d'une authentification par clé publique SSH et les utilisateurs disposant de mots de passe	9.6(3)/9.8(1)	Dans les versions antérieures à 9.6(2), vous pouviez activer l'authentification par clé publique SSH (**ssh authentication**) sans activer explicitement l'authentification SSH AAA avec la base de données des utilisateurs locale (**aaa authentication ssh console LOCAL**). Dans 9.6(2), l'ASA vous a demandé d'activer explicitement l'authentification SSH AAA. Dans cette version, vous n'avez plus à activer explicitement l'authentification SSH AAA; lorsque vous configurez la commande **ssh authentication** pour un utilisateur, l'authentification locale est activée par défaut pour les utilisateurs avec ce type d'authentification. De plus, lorsque vous configurez explicitement l'authentification SSH AAA, cette configuration s'applique uniquement aux noms d'utilisateur avec *mots de passe*, et vous pouvez utiliser n'importe quel type de serveur AAA (**aaa authentication ssh console radius_1**, par exemple). Par exemple, certains utilisateurs peuvent utiliser l'authentification par clé publique à l'aide de la base de données locale et d'autres utilisateurs peuvent utiliser des mots de passe avec RADIUS. Nous n'avons pas modifié de commandes.
Exigences relatives à l'utilisateur local et au mot de passe d'activation	9.17(1)	Pour les utilisateurs locaux et le mot de passe d'activation, les exigences de mot de passe suivantes ont été ajoutées : • Longueur du mot de passe : au moins 8 caractères. Auparavant, le minimum était de 3 caractères. • Caractères répétitifs et séquentiels : trois caractères ASCII ou plus consécutifs ne sont pas autorisés. Par exemple, les mots de passe suivants seront refusés : • **abc**utilisateur1 • utilisateur**543** • utilisateur**aaaa** • utilisateur2**666** Commandes nouvelles/modifiées : **enable password**, **username**

Nom de la caractéristique	Versions de plateforme	Description
Modifications du verrouillage de l'utilisateur local	9.17(1)	L'ASA peut verrouiller les utilisateurs locaux après un nombre configurable de tentatives de connexion échouées. Cette fonctionnalité ne s'applique pas aux utilisateurs ayant le niveau de privilège 15. De plus, un utilisateur serait verrouillé indéfiniment jusqu'à ce qu'un administrateur déverrouille son compte. Désormais, les utilisateurs seront déverrouillés après 10 minutes, à moins qu'un administrateur n'utilise la commande **clear aaa local user lockout** avant. Les utilisateurs ayant le niveau de privilège 15 sont également concernés par le paramètre de verrouillage. Commandes nouvelles ou modifiées : **aaa local authentication attempts max-fail** , **show aaa local user**
Invite de modification du mot de passe SSH et Telnet	9.17(1)	La première fois qu'un utilisateur local se connecte à l'ASA à l'aide de SSH ou de Telnet, il est invité à changer de mot de passe. Il sera également invité à se connecter pour la première fois après qu'un administrateur aura modifié son mot de passe. Si l'ASA se recharge, les utilisateurs ne seront pas invités, même s'il s'agit de leur première connexion. Commandes nouvelles ou modifiées : **show aaa local user**

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.