

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, à la page 1
- Lignes directrices relatives à la base de données locale, à la page 6
- Ajouter un compte d'utilisateur à la base de données locale, à la page 6
- Tester l'authentification et l'autorisation de la base de données locale, à la page 8
- Supervision de la base de données locale, à la page 9
- Historique de la base de données locale, à la page 9

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

Type de serveur et service	Authentification	Autorisation	Gestion de comptes
Utilisateurs VPN	Oui	Non	Non
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. ASDM vous permet d'activer trois niveaux de privilèges prédéfinis, avec des commandes attribuées au niveau 15 (Admin), au niveau 5 (Lecture seule) et au niveau 3 (Superviser uniquement). Si vous utilisez les niveaux prédéfinis, affectez des utilisateurs à l'un de ces trois niveaux de privilège.

- 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 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)**, puis cliquez sur **Add** (Ajouter).

La boîte de dialogue **Add User Account-Identity** (Ajouter une identité de compte d'utilisateur) apparaît.

Étape 2 Saisissez un nom d'utilisateur de 4 à 64 caractères.

Étape 3 (Facultatif) Saisissez un mot de passe compris entre 8 et 127 caractères.

Les valeurs des mots de passe respectent la casse. 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**

Le champ affiche uniquement des astérisques. Par exemple, vous souhaiterez peut-être créer un nom d'utilisateur sans mot de passe si vous utilisez l'authentification par clé publique SSH.

Remarque Pour configurer le mot de passe d'activation à partir du volet **User Accounts** (Comptes d'utilisateurs), modifiez le mot de passe de l'utilisateur enable_15. L'utilisateur enable_15 est toujours présent dans le volet **User Accounts** (Comptes d'utilisateurs) et représente le nom d'utilisateur par défaut. Cette méthode de configuration du mot de passe d'activation est la seule méthode disponible dans ASDM pour la configuration système. Si vous avez configuré d'autres mots de passe de niveau d'activation au niveau de l'interface de ligne de commande (par exemple, le mot de passe enable 10), ces utilisateurs sont répertoriés comme enable_10, et ainsi de suite.

Étape 4 Entrez le mot de passe de nouveau.

Pour des raisons de sécurité, seuls les astérisques apparaissent dans les champs du mot de passe.

Étape 5 Cochez la case **User authenticated using MSCHAP** (Utilisateur authentifié à l'aide de MSCHAP) si vous utilisez MSCHAP pour l'authentification.

Étape 6 Définissez le niveau d'accès de gestion d'un utilisateur dans la zone **Access Restriction** (Restriction d'accès). Vous devez d'abord activer l'autorisation de gestion en cliquant sur l'option **Perform authorization for exec shell access** (Effectuer l'autorisation pour l'accès au shell d'exécution) sous l'onglet **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Access (Accès AAA)** > **Authorization (Authorisation)**.

Choisissez une des options suivantes :

- **Full Access (ASDM, Telnet, SSH and console)** (Accès complet (ASDM, Telnet, SSH et console)) : si vous configurez l'authentification pour l'accès de gestion à l'aide de la base de données locale, cette option permet à l'utilisateur d'utiliser ASDM, SSH, Telnet et le port de console. Si vous activez également l'authentification, l'utilisateur peut accéder au mode de configuration globale.
  - **Privilege Level** (Niveau de privilège) : définit le niveau de privilège pour ASDM et l'autorisation de commande locale. La plage va de 0 (le plus bas) à 15 (le plus élevé). Spécifiez 15 pour accorder un accès administrateur sans restriction. Les rôles ASDM prédéfinis utilisent 15 pour l'administration,

5 pour la lecture seule et 3 pour la surveillance uniquement (ce qui limite l'utilisateur aux volets Home (Accueil) et Monitoring (Supervision)).

- **CLI login prompt for SSH, Telnet and console (no ASDM access)** (Invite de connexion à l'interface de ligne de commande pour SSH, Telnet et la console (sans accès ASDM)) : si vous configurez l'authentification pour l'accès de gestion à l'aide de la base de données locale, cette option permet à l'utilisateur d'utiliser SSH, Telnet et le port de console. L'utilisateur ne peut pas utiliser ASDM pour la configuration (si vous configurez l'authentification HTTP). La surveillance ASDM est autorisée. Si vous configurez également l'authentification de l'activation, l'utilisateur ne peut pas accéder au mode de configuration globale.
- **No ASDM, SSH, Telnet, or console access** (Aucun accès ASDM, SSH, Telnet ou à la console) : si vous configurez l'authentification pour l'accès de gestion à l'aide de la base de données locale, cette option empêche l'utilisateur d'accéder à toute méthode d'accès de gestion pour laquelle vous avez configuré l'authentification (à l'exception de l'option de série; l'accès en série est autorisé).

Étape 7 (Facultatif) Pour activer l'authentification par clé publique pour les connexions SSH à l'ASA par utilisateur, consultez Configurer l'accès HTTPS pour ASDM, autres clients.

Étape 8 Cliquez sur **VPN Policy** (Politique VPN) pour configurer les attributs de la politique VPN pour cet utilisateur. Consultez le guide de configuration du VPN.

Étape 9 Cliquez sur **Apply** (Appliquer).

L'utilisateur est ajouté à la base de données locale et les modifications sont enregistrées dans la configuration en cours d'exécution.

Astuces Vous pouvez rechercher du texte spécifique dans chaque colonne du volet **Configuration** > **Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (Comptes d'utilisateurs)**. Saisissez le texte que vous souhaitez localiser dans la zone **Find** (Rechercher), puis cliquez sur la flèche **vers le haut** ou **vers le bas**. Vous pouvez également utiliser l'astérisque (« * ») et le point d'interrogation (« ? ») comme caractères génériques dans la recherche de texte.

Tester l'authentification et l'autorisation de la base de données locale

Pour déterminer si l'ASA peut communiquer avec une base de données locale et authentifier ou autoriser un utilisateur, procédez comme suit :

Procédure

Étape 1 Dans le tableau **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs AAA)** > **AAA Server Groups (Groupes de serveurs AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**, cliquez sur le groupe de serveurs dans lequel se trouve le serveur.

Étape 2 Cliquez sur le serveur que vous souhaitez tester dans le tableau **Servers in the Selected Group** (Serveurs du groupe sélectionné).

Étape 3 Cliquez sur **Test**.

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

Étape 4 Cliquez sur le type de test que vous souhaitez effectuer : **Authentication** (Authentification) ou **Authorization** (Autorisation).

Étape 5 Saisissez un nom d'utilisateur.

Étape 6 Si vous testez l'authentification, saisissez le mot de passe correspondant au nom d'utilisateur.

Étape 7 Cliquez sur **OK**.

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

Supervision de la base de données locale

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

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

  Ce volet affiche les statistiques du serveur AAA.

- **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 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 écrans suivants : Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Server Groups Configuration (Configuration des groupes de serveurs AAA) > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (Comptes d'utilisateurs).

Nom de la caractéristique	Versions de plateforme	Description
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 écrans suivants : Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (Comptes d'utilisateurs) > Edit User Account (Modifier le compte d'utilisateur) > Public Key Authentication (Authentification par clé publique) Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (Comptes d'utilisateurs) > Edit User Account (Modifier le compte d'utilisateur) > Public Key Using PKF (Clé publique utilisant PKF) *Également disponible dans 8.4(4.1); la prise en charge du format de clé PKF uniquement dans 9.1(2).*
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 écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)** > **Enable Password (Mot de passe d'activation)** **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)** > **Add/Edit User Account (Ajouter/Modifier un compte d'utilisateur)** > **Identity (Identité)**

Nom de la caractéristique	Versions de plateforme	Description
Améliorations de l'authentification par clé publique SSH	9.6(2)	Dans les versions antérieures, vous pouviez activer l'authentification par clé publique SSH sans activer également l'authentification SSH AAA avec la base de données d'utilisateurs locale . 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 écrans suivants : **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ASDM/HTTPS/Telnet/SSH** **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)** > **Add/Edit User Account (Ajouter/Modifier un compte d'utilisateur)**
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 écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)** > **Enable Password (Mot de passe d'activation)** **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)** > **Add/Edit User Account (Ajouter/Modifier un compte d'utilisateur)** > **Identity (Identité)**

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 d'écrans.
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** Écrans Nouveaux ou modifiés : • **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)** • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)**

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.