Serveurs RADIUS pour AAA

Ce chapitre décrit comment configurer les serveurs RADIUS pour AAA.

À propos des serveurs RADIUS pour AAA

L'ASA prend en charge les serveurs RADIUS conformes à la norme RFC suivants pour AAA :

- Cisco Secure ACS 3.2, 4.0, 4.1, 4.2 et 5.x
- Cisco Identity Services Engine (ISE)
- RSA RADIUS dans RSA Authentication Manager 5.2, 6.1 et 7.x
- Microsoft

Méthodes d'authentification prises en charge

L'ASA prend en charge les méthodes d'authentification suivantes avec les serveurs RADIUS :

- PAP : pour tous les types de connexion.
- CHAP et MS-CHAPv1 : pour les connexions L2TP-over-IPsec.
- MS-CHAPv2 : pour les connexions L2TP sur IPsec et pour les connexions d'accès à distance IPsec normales lorsque la fonctionnalité de gestion des mots de passe est activée. Vous pouvez également utiliser MS-CHAPv2 avec des connexions sans client.
- Modes de mandataire pour l'authentification : pour les connexions RADIUS à Active-Directory, RADIUS à RSA/SDI, RADIUS à serveur de jeton et RSA/SDI à RADIUS.

Remarque Pour activer MS-CHAPv2 comme protocole utilisé entre l'ASA et le serveur RADIUS pour une connexion VPN, la gestion des mots de passe doit être activée dans les attributs généraux du groupe de tunnels. L'activation de la gestion des mots de passe génère une demande d'authentification MS-CHAPv2 de l'ASA au serveur RADIUS. Consultez la description de la commande **password-management** pour en savoir plus.

Si vous utilisez la double authentification et activez la gestion des mots de passe dans le groupe de tunnels, les demandes d'authentification principale et secondaire incluent les attributs de demande MS-CHAPv2. Si un serveur RADIUS ne prend pas en charge MS-CHAPv2, vous pouvez configurer ce serveur pour envoyer une demande d'authentification non MS-CHAPv2 à l'aide de la commande **no mschapv2-capable**.

Autorisation des utilisateurs pour les connexions VPN

L'ASA peut utiliser des serveurs RADIUS pour l'autorisation des utilisateurs d'accès à distance VPN et des sessions de mandataire direct de pare-feu à l'aide d'ACL dynamiques ou de noms d'ACL par utilisateur. Pour mettre en œuvre des ACL dynamiques, vous devez configurer le serveur RADIUS pour les prendre en charge. Lorsque l'utilisateur s'authentifie, le serveur RADIUS envoie une ACL téléchargeable ou un nom d'ACL à l'ASA. L'accès à un service donné est autorisé ou refusé par l'ACL. L'ASA supprime l'ACL lorsque la session d'authentification expire.

En plus des ACL, l'ASA prend en charge de nombreux autres attributs pour l'autorisation et la définition des autorisations pour l'accès à distance au VPN et les sessions de mandataire direct par le pare-feu.

Ensembles d'attributs RADIUS pris en charge

L'ASA prend en charge les ensembles d'attributs RADIUS suivants :

- Attributs d'authentification définis dans les RFC 2138 et 2865.
- Attributs de traçabilité définis dans les RFC 2139 et 2866.
- Attributs RADIUS pour la prise en charge du protocole tunnelé, définis dans les RFC 2868 et 6929.
- Attributs spécifiques au fournisseur (VSA) Cisco IOS, identifiés par l'ID de fournisseur RADIUS 9.
- VSA liés au VPN Cisco, identifiés par l'ID de fournisseur RADIUS 3076.
- VSA Microsoft, définis dans la RFC 2548.

Attributs d'autorisation RADIUS pris en charge

L'autorisation désigne le processus d'application d'autorisations ou d'attributs. Un serveur RADIUS défini comme serveur d'authentification applique des autorisations ou des attributs s'ils sont configurés. Ces attributs ont l'ID de prestataire 3076.

Le tableau suivant répertorie les attributs RADIUS pris en charge qui peuvent être utilisés pour l'autorisation de l'utilisateur.

Remarque Les noms d'attributs RADIUS ne contiennent pas le préfixe cVPN3000. Cisco Secure ACS 4.x prend en charge cette nouvelle nomenclature, mais les noms d'attributs dans les versions ACS antérieures à la version 4.0 incluent toujours le préfixe cVPN3000. Les ASA appliquent les attributs RADIUS en fonction de l'ID numérique de l'attribut, et non du nom de l'attribut.

Tous les attributs répertoriés dans le tableau suivant sont des attributs en aval envoyés du serveur RADIUS à l'ASA, à l'exception des numéros d'attribut suivants : 146, 150, 151 et 152. Ces numéros d'attribut sont des attributs en amont qui sont envoyés de l'ASA au serveur RADIUS. Les attributs RADIUS 146 et 150 sont envoyés de l'ASA au serveur RADIUS pour les demandes d'authentification et d'autorisation. Les quatre attributs précédemment répertoriés sont envoyés de l'ASA au serveur RADIUS pour les demandes de démarrage, de mise à jour provisoire et d'arrêt de gestion. Les attributs RADIUS en amont 146, 150, 151 et 152 ont été introduits dans la version 8.4(3).

Tableau 1 : Attributs d'autorisation RADIUS pris en charge

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Heures d'accès	O	1	Chaîne	Unique	Nom de la plage temporelle, par exemple, H ouvrables
Liste d'accès entrant	O	86	Chaîne	Unique	ID d'ACL
Liste d'accès sortante	O	87	Chaîne	Unique	ID d'ACL
Ensembles des adresses	O	217	Chaîne	Unique	Nom de l'ensemble d'adresses IP locales
Allow-Network-Extension-Mode	O	64	Booléen	Unique	0 = Désactivé 1 = Activé
Authenticated-User-Idle-Timeout	O	50	nombre entier	Unique	1 à 35791394 minutes
Authorization-DN-Field	O	67	Chaîne	Unique	Valeurs possibles : UID, OU, O, CN, L, SP, N, GN, SN, I, GENQ, DNQ, SER, use-entire
Authorization-Required		66	nombre entier	Unique	0 = non 1 = oui
Authorization-Type	O	65	nombre entier	Unique	0 = Aucun 1 = RADIUS 2 = LDAP
Banner1	O	15	Chaîne	Unique	Chaîne de caractères de bannière à afficher p sessions d'accès à distance VPN Cisco : IPse Secure Client (services client sécurisés) SSL-TLS/DTLS/IKEv2 et Clientless SSL

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Banner2	O	36	Chaîne	Unique	Chaîne de caractères de bannière à afficher pour sessions d'accès à distance VPN Cisco : IPsec IK Secure Client (services client sécurisés) SSL-TLS/DTLS/IKEv2 et Clientless SSL La ch Bannière2 est concaténée à la chaîne Bannière1, est configurée.
Cisco-IP-Phone-Bypass	O	51	nombre entier	Unique	0 = Désactivé 1 = Activé
Cisco-LEAP-Bypass	O	75	nombre entier	Unique	0 = Désactivé 1 = Activé
Type de client	O	150	nombre entier	Unique	1 = Cisco VPN Client (IKEv1) 2 = Secure Client (client sécurisés) SSL VPN 3 = Clientless SSL V Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN 6 = Client (services client sécurisés) IPsec VPN (IK
Client-Type-Version-Limiting	O	77	Chaîne	Unique	Chaîne du numéro de version de VPN IPSec
DHCP-Network-Scope	O	61	Chaîne	Unique	Adresse IP
Extended-Authentication-On-Rekey	O	122	nombre entier	Unique	0 = Désactivé 1 = Activé
Framed-Interface-Id	O	96	Chaîne	Unique	ID de l'interface IPv6 affectée. Se combine avec Framed-IPv6-Prefix pour créer une adresse IPv6 co Par exemple : Framed-Interface-ID=1:1:1:1 comb Framed-IPv6-Prefix= 2001:0db8::/64 donne l'ad attribuée 2001:0db8::1:1:1:1.
Framed-IPv6-Prefix	O	97	Chaîne	Unique	Préfixe et longueur IPv6 affectées. À combiner a Framed-Interface-Id pour créer une adresse IPv6 complète. Par exemple : prefix 2001:0db8::/64 c avec Framed-Interface-Id=1:1:1:1:1 donne l'adr 2001:0db8::1:1:1:1. Vous pouvez utiliser cet attri attribuer une adresse IP sans utiliser Framed-Inter en attribuant l'adresse IPv6 complète avec la lon de préfixe /128, par exemple, Framed-IPv6-Prefix=2001:0db8::1/128.
Politique de groupe	O	25	Chaîne	Unique	Définit la politique de groupe pour la session VPN à distance. Pour les versions 8.2.x et ultérieures, cet attribut au lieu de IETF-Radius-Class. Vous p utiliser l'un des formats suivants : • *nom de la politique de groupe* • OU=*nom de la politique de groupe* • OU=*nom de la politique de groupe*;
IE-Proxy-Bypass-Local		83	nombre entier	Unique	0 = aucun 1 = local

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
IE-Proxy-Exception-List		82	Chaîne	Unique	Nouvelle liste de domaines DNS séparés par (\n)
URL-PAC-IE-Proxy	O	133	Chaîne	Unique	Chaîne d'adresse PAC
IE-Proxy-Server		80	Chaîne	Unique	Adresse IP
IE-Proxy-Server-Policy		81	nombre entier	Unique	1 = Aucune modification 2 = Aucun mandat Détection automatique 4 = Utiliser le paramè concentrateur
IKE-KeepAlive-Confidence-Interval	O	68	nombre entier	Unique	10 à 300 secondes
IKE-Keepalive-Retry-Interval	O	84	nombre entier	Unique	2 à 10 secondes
IKE-Keep-Alives	O	41	Booléen	Unique	0 = Désactivé 1 = Activé
Intercept-DHCP-Configure-Msg	O	62	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Allow-Passwd-Store	O	16	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Authentication		13	nombre entier	Unique	0 = Aucun 1 = RADIUS 2 = LDAP (autorisa seulement) 3 = Domaine NT 4 = SDI 5 = Int RADIUS avec expiration 7 = Kerberos/Activ
IPsec-Auth-On-Rekey	O	42	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Backup-Server-List	O	60	Chaîne	Unique	Adresses du serveur (délimitées par un espac
IPsec-Backup-Servers	O	59	Chaîne	Unique	1 = Utiliser la liste configurée par le client 2 = et effacer la liste du client 3 = Utiliser la liste de sauvegarde
IPsec-Client-Firewall-Filter-Name		57	Chaîne	Unique	Spécifie le nom du filtre à envoyer au client politique de pare-feu
IPsec-Client-Firewall-Filter-Optional	O	58	nombre entier	Unique	0 = obligatoire 1 = facultatif
IPsec-Default-Domain	O	28	Chaîne	Unique	Spécifie le nom de domaine par défaut à envo (1 à 255 caractères).
IPsec-IKE-Peer-ID-Check	O	40	nombre entier	Unique	1 = Obligatoire 2 = Si pris en charge par le c homologue 3 = Ne pas vérifier
IPsec-IP-Compression	O	39	nombre entier	Unique	0 = Désactivé 1 = Activé
IPsec-Mode-Config	O	31	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Over-UDP	O	34	Booléen	Unique	0 = Désactivé 1 = Activé
IPsec-Over-UDP-Port	O	35	nombre entier	Unique	4001à 49151. La valeur par défaut est 10 000

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
IPsec-Required-Client-Firewall-Capability	O	56	nombre entier	Unique	0 = Aucune 1 = Politique définie par le micro-lo Are You There (Ayt) distant 2 = Politique transm CPP 4 = Politique du serveur
IPsec-Sec-association		12	Chaîne	Unique	Nom de l'association de sécurité
IPsec-Split-DNS-Names	O	29	Chaîne	Unique	Spécifie la liste des noms de domaines secondai envoyer au client (1 à 255 caractères).
IPsec-Split-Tunneling-Policy	O	55	nombre entier	Unique	0 = Aucun tunnellisation fractionnée 1 = Tunnel fractionnée 2 = LAN local autorisé
IPsec-Split-Tunnel-List	O	27	Chaîne	Unique	Spécifie le nom du réseau ou de la liste de contr d'accès qui décrit la liste d'inclusion du tunnel fra
IPsec-Tunnel-Type	O	30	nombre entier	Unique	1 = LAN à LAN 2 = Accès à distance
IPsec-User-Group-Lock		33	Booléen	Unique	0 = Désactivé 1 = Activé
IPv6-Address-Pools	O	218	Chaîne	Unique	Name of IP local pool-IPv6
IPv6-VPN-Filter	O	219	Chaîne	Unique	Valeur ACL
L2TP-Encryption		21	nombre entier	Unique	Bitmap : 1 = Chiffrement requis 2 = 40 bits 4 = 8 = Stateless-Req 15 = 40/128-Encr/Stateless-R
L2TP-MPPC-Compression		38	nombre entier	Unique	0 = Désactivé 1 = Activé
Member-Of	O	145	Chaîne	Unique	Chaîne délimitée par des virgules, par exemple `Engineering, Sales` Attribut administratif qui peut être utilisé dans l politiques d'accès dynamique. Elle ne définit pa politique de groupe.
MS-Client-Subnet-Mask	O	63	Booléen	Unique	Une adresse IP
NAC-Default-ACL		92	Chaîne		ACL
NAC-Enable		89	nombre entier	Unique	0 = non 1 = oui
NAC-Revalidation-Timer		91	nombre entier	Unique	300 à 86 400 secondes
NAC-Settings	O	141	Chaîne	Unique	Nom de la politique NAC
NAC-Status-Query-Timer		90	nombre entier	Unique	30 à 1800 secondes
Perfect-Forward-Secrecy-Enable	O	88	Booléen	Unique	0 = non 1 = oui
PPTP-Encryption		20	nombre entier	Unique	Bitmap : 1 = Chiffrement requis 2 = 40 bits 4 = 8 = Stateless-Requis 15= 40/128-Encr/Stateless-

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
PPTP-MPPC-Compression		37	nombre entier	Unique	0 = Désactivé 1 = Activé
Primary-DNS	O	5	Chaîne	Unique	Une adresse IP
Primary-WINS	O	7	Chaîne	Unique	Une adresse IP
Privilege-Level	O	220	nombre entier	Unique	Un nombre entier entre 0 et 15.
Required-Client- Firewall-Vendor-Code	O	45	nombre entier	Unique	1 = Cisco Systems (avec Cisco Integrated Cl Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cis (avecCisco Intrusion Prevention Security Ag
Required-Client-Firewall-Description	O	47	Chaîne	Unique	Chaîne
Required-Client-Firewall-Product Code	O	46	nombre entier	Unique	Produits Cisco Systems : 1 = Cisco Intrusion Prevention Security Age Integrated Client (CIC) Produits Zone Labs : 1 = Alarme de zone 2 = zone Pro 3 = Zone Labs Integrity Produit NetworkICE : 1 = NoirIce Defender/ Produits Sygate : 1 = Personal Firewall 2 = F Firewall Pro 3 = security Agent
Required-Individual-User-Auth	O	49	nombre entier	Unique	0 = Désactivé 1 = Activé
Require-HW-Client-Auth	O	48	Booléen	Unique	0 = Désactivé 1 = Activé
Secondary-DNS	O	6	Chaîne	Unique	Une adresse IP
Secondary-WINS	O	8	Chaîne	Unique	Une adresse IP
SEP-Card-Attribution		9	nombre entier	Unique	Non utilisé
Sous-type de session	O	152	nombre entier	Unique	0 = Aucun 1 = Sans client 2 = Client 3 = Clien Le sous-type de session s'applique uniqueme l'attribut de type de session (151) a les valeurs 1, 2, 3 et 4.
Type de séance	O	151	nombre entier	Unique	0 = Aucun 1 = Secure Client (services client VPN SSL 2 = Secure Client (services client VPN IPSec (IKEv2) 3 = VPN SSL sans client mandataire de messagerie sans client 5 = Cli VPN (IKEv1) 6 = IKEv1 LAN-LAN 7 = IKE LAN-LAN 8 = Équilibrage de charge VPN
Connexions simultanées	O	2	nombre entier	Unique	0 à 2147483647
Smart-Tunnel	O	136	Chaîne	Unique	Nom d'un tunnel intelligent

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
Smart-Tunnel-Auto	O	138	nombre entier	Unique	0 = Désactivé 1 = Activé 2 = Démarrage automa
Smart-Tunnel-Auto-Signon-Enable	O	139	Chaîne	Unique	Nom d'une liste de connexion automatique de tu Smart à côté du nom de domaine
Strip-Realm	O	135	Booléen	Unique	0 = Désactivé 1 = Activé
SVC-Ask	O	131	Chaîne	Unique	0 = Désactivé 1 = Activé 3 = Active le service pa 5 = Active l'absence de client par défaut (2 et 4 utilisés)
SVC-Ask-Timeout	O	132	nombre entier	Unique	5 à 120 secondes
Client-SVC-DPD-Interval	O	108	nombre entier	Unique	0 = Désactivé, 5 à 3 600 secondes
Passerelle-SVC-DPD-Interval	O	109	nombre entier	Unique	0 = Désactivé) 5 à 3 600 secondes
SVC-DTLS	O	123	nombre entier	Unique	0 = faux 1 = vrai
SVC-Keepalive	O	107	nombre entier	Unique	0 = Désactivé, 15–600 secondes
SVC-Modules	O	127	Chaîne	Unique	Chaîne de caractères (nom d'un module)
SVC-MTU	O	125	nombre entier	Unique	Valeur MTU 256 à 1406 en octets
SVC-Profiles	O	128	Chaîne	Unique	Chaîne de caractères (nom d'un profil)
SVC-Rekey-Time	O	110	nombre entier	Unique	0 = Désactivé 1 à 10 080 minutes
Tunnel Group Name	O	146	Chaîne	Unique	1 à 253 caractères
Tunnel-Group-Lock	O	85	Chaîne	Unique	Nom du groupe de tunnels ou « none » (aucun)
Tunneling-Protocoles	O	11	nombre entier	Unique	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2T 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8 s'excluent mutuellement. 0 à 11, 16 à 27, 32 à 4 59 sont des valeurs autorisées.
Use-Client-Address		17	Booléen	Unique	0 = Désactivé 1 = Activé
VLAN	O	140	nombre entier	Unique	0 à 4094
WebVPN-Access-List	O	73	Chaîne	Unique	Nom de la liste d'accès
WebVPN ACL	O	73	Chaîne	Unique	Nom d'une ACL WebVPN sur le périphérique
WebVPN-ActiveX-Relay	O	137	nombre entier	Unique	0 = Désactivé Sinon = Activé
WebVPN-Apply-ACL	O	102	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Auto-HTTP-Signon	O	124	Chaîne	Unique	Réservé

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
WebVPN-Citrix-Metaframe-Enable	O	101	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Content-Filter-Parameters	O	69	nombre entier	Unique	1 = Java ActiveX 2 = Java Script 4 = Image 8 dans les images
WebVPN-Customization	O	113	Chaîne	Unique	Nom de la personnalisation
WebVPN-Default-Homepage	O	76	Chaîne	Unique	Une URL telle que http://exemple-exemple.c
WebVPN-Deny-Message	O	116	Chaîne	Unique	Chaîne de caractères valide (jusqu'à 500 car
WebVPN-Download_Max-Size	O	157	nombre entier	Unique	0x7fffffff
WebVPN-File-Access-Enable	O	94	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-File-Server-Browsing-Enable	O	96	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-File-Server-Entry-Enable	O	95	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	O	78	Chaîne	Unique	DNS/IP séparés par des virgules avec un car générique facultatif (*) (par exemple *.cisco 192.168.1.*, wwwin.cisco.com)
WebVPN-Hidden-Shares	O	126	nombre entier	Unique	0 = aucun 1 = visible
WebVPN-Home-Page-Use-Smart-Tunnel	O	228	Booléen	Unique	Activé si la page d'accueil sans client doit êt par l'intermédiaire de Smart Tunnel.
WebVPN-HTML-Filter	O	69	Bitmap	Unique	1 = ActiveX Java 2 = Scripts 4 = Image 8 =
WebVPN-HTTP-Compression	O	120	nombre entier	Unique	0 = Désactivé 1 = Décompression
WebVPN-HTTP-Proxy-IP-Address	O	74	Chaîne	Unique	DNS/IP séparé par des virgules:port, avec le p ou https= (par exemple http=10.10.10:80, https=11.11.11.11:443)
WebVPN-Idle-Timeout-Alert-Interval	O	148	nombre entier	Unique	0 à 30. 0 = Désactivé.
WebVPN-Keepalive-Ignore	O	121	nombre entier	Unique	0 à 900
WebVPN-Macro-Substitution	O	223	Chaîne	Unique	Illimité.
WebVPN-Macro-Substitution	O	224	Chaîne	Unique	Illimité.
WebVPN-Port-Forwarding-Enable	O	97	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	O	98	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Port-Forwarding-HTTP-Proxy	O	99	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-Port-Forwarding-List	O	72	Chaîne	Unique	Nom de la liste de transferts de port

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
WebVPN-Port-Forwarding-Name	O	79	Chaîne	Unique	Nom de chaîne de caractères (par exemple, « Corporate-Apps »). Ce texte remplace la chaîne par défaut « Applica Access » dans la page d'accueil du portail sans c
WebVPN-post-maximum-taille	O	159	nombre entier	Unique	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	O	149	nombre entier	Unique	0 à 30. 0 = Désactivé.
WebVPN Smart-Card-Removal-Disconnect	O	225	Booléen	Unique	0 = Désactivé 1 = Activé
WebVPN-Smart-Tunnel	O	136	Chaîne	Unique	Nom d'un tunnel intelligent
WebVPN-Smart-Tunnel-Auto-Sign-On	O	139	Chaîne	Unique	Nom d'une liste de connexion automatique de S Tunnel ajouté par le nom de domaine
WebVPN-Smart-Tunnel-Auto-Start	O	138	nombre entier	Unique	0 = Désactivé 1 = Activé 2 = Démarrage automa
WebVPN-Smart-Tunnel-Tunnel-Policy	O	227	Chaîne	Unique	Un des choix « e networkname », « i networkna « a », où networkname est le nom d'une liste de Smart Tunnels, e indiquant le tunnel exclu, i le t spécifié et a indique tous les tunnels.
WebVPN-SSL-VPN-Client-Enable	O	103	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SSL-VPN-Client-Keep- Installation	O	105	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SSL-VPN-Client-Required	O	104	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SSO-Server-Name	O	114	Chaîne	Unique	Chaîne de caractères valide
WebVPN-Storage-Key	O	162	Chaîne	Unique	
WebVPN-Storage-Objects	O	161	Chaîne	Unique	
WebVPN-SVC-Keepalive-Frequency	O	107	nombre entier	Unique	15 à 600 secondes, 0 = désactivé
WebVPN-SVC-Client-DPD-Frequency	O	108	nombre entier	Unique	5 à 3 600 secondes, 0 = désactivé
WebVPN-SVC-DTLS-Enable	O	123	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-SVC-DTLS-MTU	O	125	nombre entier	Unique	La valeur MTU est comprise entre 256 et 1406 c
WebVPN-SVC-Gateway-DPD-Frequency	O	109	nombre entier	Unique	5 à 3 600 secondes, 0 = désactivé
WebVPN-SVC-Rekey-Time	O	110	nombre entier	Unique	4 à 10 080 minutes, 0 = Désactivé
WebVPN-SVC-Rekey-Method	O	111	nombre entier	Unique	0 (désactivé), 1 (SSL), 2 (nouveau tunnel)
WebVPN-SVC-Compression	O	112	nombre entier	Unique	0 (Désactivé), 1 (Décompression)

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
WebVPN-UNIX-Group-ID (GID)	O	222	nombre entier	Unique	ID de groupe UNIX valides
WebVPN-UNIX-User-ID (UIDs)	O	221	nombre entier	Unique	ID d'utilisateur UNIX valides
WebVPN-Upload-Max-Size	O	158	nombre entier	Unique	0x7fffffff
WebVPN-URL-Entry-Enable	O	93	nombre entier	Unique	0 = Désactivé 1 = Activé
WebVPN-URL-List	O	71	Chaîne	Unique	Nom de la liste d'URL
WebVPN-User-Storage	O	160	Chaîne	Unique	
WebVPN-VDI	O	163	Chaîne	Unique	Liste des paramètres

Attributs d'autorisation RADIUS IETF pris en charge

Le tableau suivant présente les attributs RADIUS IETF pris en charge.

Tableau 2 : Attributs RADIUS IETF pris en charge

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
IETF-Radius-Class	O	25		Unique	Pour les versions 8.2.x et ultérieures, nous vous recommandons d'utiliser l'attribut Group-Policy (VSA 3076, n° 25) : • *nom de la politique de groupe* • OU=*nom de la politique de groupe* • OU=*nom de la politique de groupe*
IETF-Radius-Filter-Id	O	11	Chaîne	Unique	Nom de l'ACL défini sur l'ASA, qui s'applique uniquement aux clients SSL VPN et IPsec du tunnel complet.
IETF-Radius-Framed-IP-Address	O	S.O.	Chaîne	Unique	Une adresse IP
IETF-Radius-Framed-IP-Netmask	O	S.O.	Chaîne	Unique	Un masque d'adresse IP
IETF-Radius-Idle-Timeout	O	28	nombre entier	Unique	Secondes

Nom de l'attribut	ASA	Attr. Non.	Syntaxe/Type	Valeur unique ou valeurs multiples	Description ou valeur
IETF-Radius-Service-Type	O	6	nombre entier	Unique	Secondes. Valeurs possibles pour le type de service : • .Administrative : l'utilisateur a accès à l'invite de configuration. • .NAS-Prompt : l'utilisateur a accès à l'invite d'exécution. • .remote-access : l'utilisateur a accès au réseau.
IETF-Radius-Session-Timeout	O	27	nombre entier	Unique	Secondes

Codes de motif de déconnexion comptable RADIUS

Ces codes sont renvoyés si l'ASA rencontre une déconnexion lors de l'envoi de paquets :

Code de motif de déconnexion
ACCT_DISC_USER_REQ = 1
ACCT_DISC_LOST_CARRIER = 2
ACCT_DISC_LOST_SERVICE = 3
ACCT_DISC_IDLE_TIMEOUT = 4
ACCT_DISC_SESS_TIMEOUT = 5
ACCT_DISC_ADMIN_RESET = 6
ACCT_DISC_ADMIN_REBOOT = 7
ACCT_DISC_PORT_ERROR = 8
ACCT_DISC_NAS_ERROR = 9
ACCT_DISC_NAS_REQUEST = 10
ACCT_DISC_NAS_REBOOT = 11
ACCT_DISC_PORT_UNNEEDED = 12
ACCT_DISC_PORT_PREEMPTED = 13
ACCT_DISC_PORT_SUSPENDED = 14
ACCT_DISC_SERV_UNAVAIL = 15
ACCT_DISC_CALLBACK = 16

Code de motif de déconnexion
ACCT_DISC_USER_ERROR = 17
ACCT_DISC_HOST_REQUEST = 18
ACCT_DISC_ADMIN_SHUTDOWN = 19
ACCT_DISC_SA_EXPIRED = 21
ACCT_DISC_MAX_REASONS = 22

Lignes directrices relatives aux serveurs RADIUS pour AAA

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

- 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.
- La longueur maximale de la charge utile RADIUS est de 4096 octets.

Configurer les serveurs RADIUS pour AAA

Cette section décrit comment configurer les serveurs RADIUS pour AAA.

Procédure

Étape 1 Chargez les attributs ASA dans le serveur RADIUS. La méthode que vous utilisez pour charger les attributs dépend du type de serveur RADIUS que vous utilisez :

- Si vous utilisez Cisco ACS : le serveur intègre déjà ces attributs. Vous pouvez ignorer cette étape.
- Pour les serveurs RADIUS d'autres fournisseurs (par exemple, le service d'authentification Internet Microsoft) : vous devez définir manuellement chaque attribut ASA. Pour définir un attribut, utilisez le nom ou le numéro d'attribut, le type, la valeur et le code du fournisseur (3076).

Étape 2 Configurer les groupes de serveurs RADIUS, à la page 14.

Étape 3 Ajouter un serveur RADIUS à un groupe, à la page 17.

Configurer les groupes de serveurs RADIUS

Si vous souhaitez utiliser un serveur RADIUS externe pour l'authentification, l'autorisation ou la gestion de comptes, vous devez d'abord créer au moins un groupe de serveurs RADIUS par protocole AAA et ajouter un ou plusieurs serveurs à chaque groupe.

Procédure

Étape 1 Créez le groupe de serveurs AAA RADIUS.

aaa-server *group_name* **protocol radius**

Exemple :

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)#
```

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

Étape 2 (Facultatif) Précisez le nombre maximum de transactions AAA échouées avec un serveur RADIUS du groupe avant d'essayer le serveur suivant.

max-failed-attempts *number*

La plage se situe entre 1 et 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.

Exemple :

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

Étape 3 (Facultatif) Précisez la méthode (politique de réactivation) par laquelle les serveurs défaillants d'un groupe sont réactivés.

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

Lieu :

- **depletion** [**deadtime** *minutes*] réactive les serveurs défaillants seulement après que tous les serveurs du groupe sont inactifs. Il s'agit du mode de réactivation par défaut. Vous pouvez préciser la durée, entre 0 et 1 440 minutes, 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.

- **timed** réactive les serveurs défaillants après 30 secondes de temps d'arrêt.

Exemple :

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

Étape 4 (Facultatif) Envoyez des messages de traçabilité à tous les serveurs du groupe.

accounting-mode simultaneous

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

Exemple :

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

Étape 5 (Facultatif) Activez la génération périodique de messages RADIUS interim-accounting-update.

interim-accounting-update [**periodic** [*hours*]]

ISE gère un répertoire des sessions actives en fonction des enregistrements de traçabilité qu'il reçoit des périphériques NAS comme l'ASA. Cependant, si ISE ne reçoit aucune indication que la session est toujours active (message de traçabilité ou transactions de posture) pendant une période de 5 jours, il supprimera l'enregistrement de session de sa base de données. Pour vous assurer que les connexions VPN de longue durée ne sont pas supprimées, configurez le groupe pour envoyer des messages interim-accounting-update périodiques à ISE pour toutes les sessions actives.

- **periodic** [*hours*] permet la génération et la transmission périodiques des enregistrements de comptabilité pour chaque session VPN configurée pour envoyer des enregistrements de comptabilité au groupe de serveurs en question. Vous pouvez éventuellement inclure l'intervalle, en heures, pour l'envoi de ces mises à jour. La valeur par défaut est de 24 heures, la plage est comprise entre 1 et 120.
- (Aucun paramètre.) Si vous utilisez cette commande sans le mot clé **periodic**, l'ASA envoie des messages interim-accounting-update uniquement lorsqu'une connexion de tunnel VPN est ajoutée à une session VPN sans client. Lorsque cela se produit, la mise à jour de comptabilité est générée afin d'informer le serveur RADIUS de la nouvelle adresse IP attribuée.

Exemple :

```
hostname(config-aaa-server-group)# interim-accounting-update periodic 12
```

Étape 6 (Facultatif) Activez les services d'autorisation dynamique RADIUS (changement d'autorisation, CoA, d'ISE) pour le groupe de serveurs AAA.

dynamic-authorization [**port** *number*]

La définition d'un port est facultative. La valeur par défaut est 1700, la plage est comprise entre 1024 et 65535.

Lorsque vous utilisez le groupe de serveurs dans un tunnel VPN, le groupe de serveurs RADIUS sera enregistré pour la notification CoA et l'ASA écoutera le port pour détecter les mises à jour de politique CoA d'ISE. Activez l'autorisation dynamique uniquement si vous utilisez ce groupe de serveurs dans un VPN d'accès à distance en conjonction avec l'ISE.

Exemple :

```
ciscoasa(config-aaa-server-group)# dynamic-authorization
```

Étape 7 (Facultatif) Si vous ne souhaitez pas utiliser ISE pour l'authentification, activez le mode d'autorisation seulement pour le groupe de serveurs RADIUS. (Activez le mode d'autorisation uniquement si vous utilisez ce groupe de serveurs dans un VPN d'accès à distance en conjonction avec l'ISE.)

authorize-only

Cela indique que lorsque ce groupe de serveurs est utilisé pour l'autorisation, le message de demande d'accès RADIUS sera généré en tant que demande « Autorize Only » (Autorisation uniquement), par opposition aux méthodes de mot de passe configurées pour le serveur AAA. Si vous configurez un mot de passe commun à l'aide de la commande **radius-common-pw** pour le serveur RADIUS, il sera ignoré.

Par exemple, vous utiliserez le mode d'autorisation seulement si vous souhaitez utiliser des certificats pour l'authentification plutôt que ce groupe de serveurs. Vous utiliserez toujours ce groupe de serveurs pour l'autorisation et la gestion de comptes dans le tunnel VPN.

Exemple :

```
ciscoasa(config-aaa-server-group)# authorize-only
```

Étape 8 (Facultatif) Fusionnez une ACL téléchargeable avec l'ACL reçue dans la paire AV de Cisco à partir d'un paquet RADIUS.

merge-dacl {**before-avpair** | **after-avpair**}

Exemple :

```
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

Cette option s'applique uniquement aux connexions VPN. Pour les utilisateurs de VPN, les ACL peuvent prendre la forme d'ACL de paire attribut/valeur de Cisco, d'ACL téléchargeables et d'une ACL configurée sur l'ASA. Cette option détermine si l'ACL téléchargeable et l'ACL de la paire attribut/valeur sont fusionnées, et ne s'applique à aucune ACL configurée sur l'ASA.

Le paramètre par défaut est **no merge dacl**, ce qui indique que les ACL téléchargeables ne seront pas fusionnées avec les ACL de paire attribut/valeur de Cisco. Si une paire AV et une ACL téléchargeable sont reçues, la paire AV a la priorité et est utilisée.

L'option **before-avpair** signifie que les entrées d'ACL téléchargeables doivent être placées avant les entrées de la paire d'AV de Cisco.

L'option **after-avpair** signifie que les entrées d'ACL téléchargeables doivent être placées après les entrées de la paire d'AV de Cisco.

Exemples

L'exemple suivant montre comment ajouter un groupe RADIUS avec un seul serveur :

```
ciscoasa(config)# aaa-server AuthOutbound protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
```

```
ciscoasa(config-aaa-server-host)# key RadUauthKey
ciscoasa(config-aaa-server-host)# exit
```

L'exemple suivant montre comment configurer un groupe de serveurs ISE pour les mises à jour d'autorisation dynamique (CoA) et la comptabilité périodique horaire. La configuration du groupe de tunnels qui configure l'authentification par mot de passe avec ISE est incluse.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

L'exemple suivant montre comment configurer un groupe de tunnels pour la validation et l'autorisation des certificats locaux avec ISE. Incluez la commande authorize-only dans la configuration du groupe de serveurs, car le groupe de serveurs ne sera pas utilisé pour l'authentification.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

Ajouter un serveur RADIUS à un groupe

Pour ajouter un serveur RADIUS à un groupe, procédez comme suit :

Procédure

Étape 1 Identifiez le serveur RADIUS et le groupe de serveurs AAA 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.

Étape 2 Spécifiez comment l'ASA traite les masques réseau reçus dans une ACL téléchargeable d'un serveur RADIUS.

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

Exemple :

```
ciscoasa(config-aaa-server-host)# acl-netmask-convert standard
```

Le mot clé **auto-detect** spécifie que l'ASA doit tenter de déterminer le type d'expression de masque réseau utilisé. Si l'ASA détecte une expression de masque réseau à caractère générique, il la convertit en une expression de masque réseau standard.

Le mot clé **standard** spécifie que l'ASA suppose que les ACL téléchargeables reçues du serveur RADIUS contiennent uniquement des expressions de masque réseau standard. Aucune conversion des expressions de masque réseau à caractère générique n'est effectuée.

Le mot clé **wildcard** spécifie que l'ASA suppose que les ACL téléchargeables reçues du serveur RADIUS contiennent uniquement des expressions de masque réseau à caractère générique et les convertit toutes en des expressions de masque réseau standard lorsque les ACL sont téléchargées.

Étape 3 Spécifiez un mot de passe commun à utiliser pour tous les utilisateurs qui accèdent à un serveur d'autorisation RADIUS par l'intermédiaire de l'ASA.

radius-common-pw *string*

Exemple :

```
ciscoasa(config-aaa-server-host)# radius-common-pw examplepassword123abc
```

L'argument *string* est un mot clé alphanumérique sensible à la casse d'un maximum de 127 caractères à utiliser comme mot de passe commun pour toutes les transactions d'autorisation avec le serveur RADIUS.

Étape 4 Activez les demandes d'authentification MS-CHAPv2 sur le serveur RADIUS.

mschapv2-capable

Exemple :

```
ciscoasa(config-aaa-server-host)# mschapv2-capable
```

Étape 5 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 6 Configurez le délai entre les tentatives de reconnexion pour un serveur AAA spécifique désigné dans une commande précédente.

retry-interval *seconds*

Exemple :

```
ciscoasa(config-aaa-server-host)# retry-interval 8
```

L'argument *seconds* spécifie l'intervalle de reconnexion (1 à 10 secondes) pour la requête. Il s'agit du temps que l'ASA attend avant de réessayer une demande de connexion.

Remarque
Pour le protocole RADIUS, si le serveur répond par un message de port ICMP inaccessible, le paramètre retry-interval est ignoré et le serveur AAA passe immédiatement à l'état d'échec. S'il s'agit du seul serveur du groupe AAA, il est réactivé et une autre requête lui est envoyée. Il s'agi du comportement prévu.

Étape 7 Envoyez des messages de traçabilité à tous les serveurs du groupe.

accounting-mode simultaneous

Exemple :

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

Saisissez la commande **accounting-mode single** pour rétablir le paramètre par défaut consistant à envoyer des messages uniquement au serveur actif.

Étape 8 Spécifiez le port d'authentification comme numéro de port 1645 ou le port du serveur à utiliser pour l'authentification des utilisateurs.

authentication-port *port*

Exemple :

```
ciscoasa(config-aaa-server-host)# authentication-port 1646
```

Étape 9 Spécifiez le port de traçabilité comme numéro de port 1646 ou le port de serveur à utiliser pour la traçabilité de cet hôte.

accounting-port *port*

Exemple :

```
ciscoasa(config-aaa-server-host)# accounting-port 1646
```

Étape 10 Spécifiez la valeur de clé secrète de serveur utilisée pour authentifier le serveur RADIUS auprès de l'ASA. La clé du serveur que vous configurez doit correspondre à celle configurée sur le serveur RADIUS. Si vous ne connaissez pas la valeur de la clé secrète du serveur, demandez à l'administrateur du serveur RADIUS. La longueur maximale est de 64caractères.

key

Exemple :

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

La clé du serveur que vous configurez doit correspondre à celle configurée sur le serveur RADIUS. Si vous ne connaissez pas la valeur de la clé secrète du serveur, demandez à l'administrateur du serveur RADIUS. La longueur maximale est de 64caractères.

Exemple

L'exemple suivant montre comment ajouter un serveur RADIUS à un groupe de serveurs RADIUS existant :

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# acl-netmask-convert wildcard
ciscoasa(config-aaa-server-host)# radius-common-pw myexaplepasswordabc123
ciscoasa(config-aaa-server-host)# mschapv2-capable
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# accounting-mode simultaneous
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# authorization-port 1645
ciscoasa(config-aaa-server-host)# key mysecretkeyexampleiceage2
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

Supervision des serveurs RADIUS pour AAA

Consultez les commandes suivantes pour superviser l'état des serveurs RADIUS pour AAA :

- **show aaa-server**

  Cette commande affiche les statistiques du serveur RADIUS configuré. Vous pouvez utiliser la commande **clear aaa-server statistics** pour réinitialiser les compteurs à zéro.

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

  Cette commande montre la configuration d'exécution du serveur RADIUS.

Historique des serveurs RADIUS pour AAA

Tableau 3 : Historique des serveurs RADIUS pour AAA

Nom de la caractéristique	Versions de plateforme	Description
Serveurs RADIUS pour AAA	7.0(1)	Décrit comment configurer les serveurs RADIUS pour AAA. Nous avons introduit les commandes suivantes : **aaa-server protocol**, **max-failed-attempts**, **reactivation-mode**, **accounting-mode simultaneous**, **aaa-server host**, **show aaa-server**, **show running-config aaa-server**, **clear aaa-server statistics**, **authentication-port**, **accounting-port**, **retry-interval**, **acl-netmask-convert**, **clear configure aaa-server**, **merge-dacl**, **radius-common-pw, key**.
Attributs propres au fournisseur de clé (VSA) envoyés dans les paquets de demande d'accès et de demande de comptabilité RADIUS à partir de l'ASA	8.4(3)	Quatre nouveaux VSA : le nom du groupe de tunnels (146) et le type de client (150) sont envoyés dans les paquets de demande d'accès RADIUS à partir de l'ASA. Le type de session (151) et le sous-type de session (152) sont envoyés dans les paquets de demande de comptabilité RADIUS à partir de l'ASA. Les quatre attributs sont envoyés pour tous les types de paquets de demande de comptabilité : Start, Interim-Update et Stop. Le serveur RADIUS (par exemple, ACS et ISE) peut alors appliquer des attributs d'autorisation et de politique ou les utiliser à des fins de comptabilité et de facturation.
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.