Caractéristiques de group-lock ASA et de Cisco IOS et attributs d'AAA et exemple de configuration de webvpn

Contenu

Introduction

Cet article décrit les caractéristiques de groupe-verrouillage sur l'appliance de sécurité adaptable Cisco (ASA) et dans le Cisco IOS® et présente le comportement pour différents attributs d'Authentification, autorisation et comptabilité (AAA). Pour le Cisco IOS, la différence entre le group-lock et les utilisateur-VPN-groupes est expliquée avec un exemple qui utilise les deux caractéristiques complémentaires en même temps. Il y a également un exemple de webvpn de Cisco IOS avec des domaines d'authentification.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de baisc de ces thèmes :

- Configuration ASA CLI et configuration du VPN de Secure Sockets Layer (SSL)

- Configuration du VPN d'Accès à distance sur l'ASA et le Cisco IOS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Logiciel ASA, version 8.4 et ultérieures
- Cisco IOS, version 15.1 et ultérieures

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurations

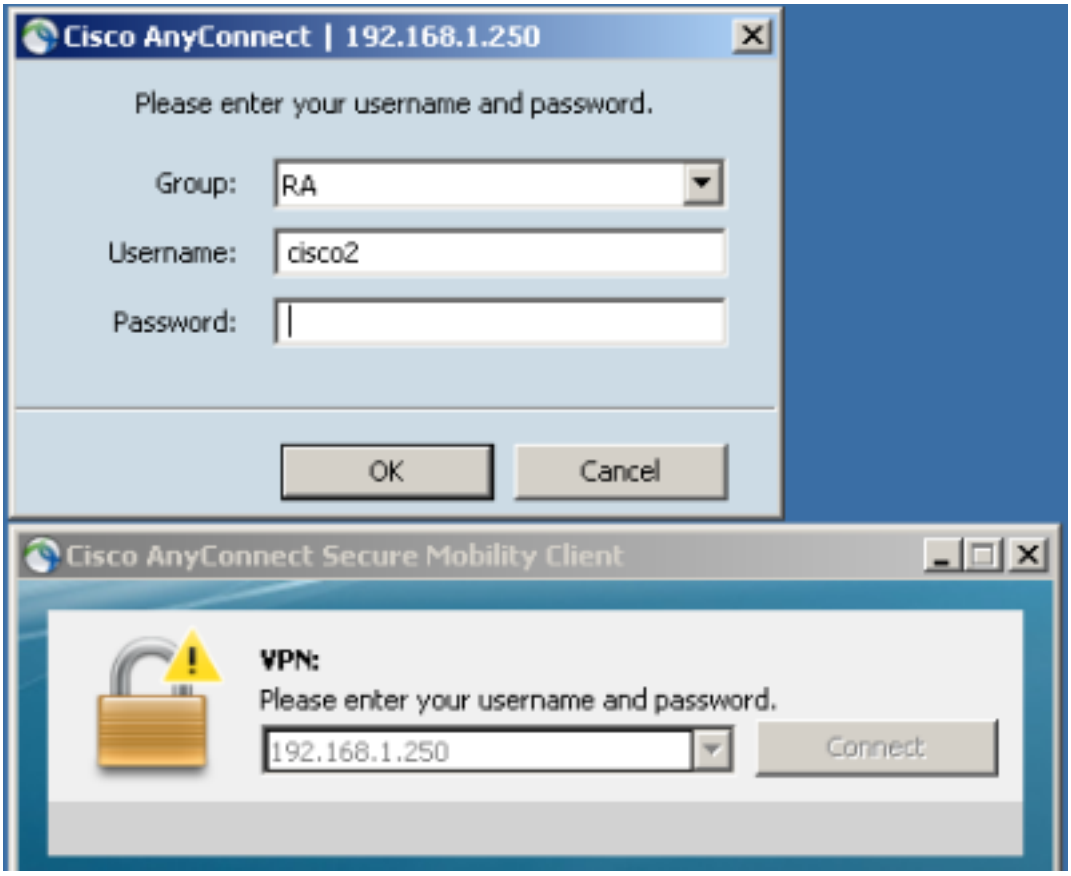
Group-lock de gens du pays ASA

Vous pouvez définir cet attribut dans le cadre de l'utilisateur ou de la stratégie de groupe. Voici un exemple pour l'attribut d'utilisateur local.

```
username cisco password 3USUcOPFUiMCO4Jk encrypted
username cisco attributes
 group-lock value RA
username cisco2 password BAtr3u1T7j1eEcYr encrypted
username cisco2 attributes
 group-lock value RA2

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 default-group-policy MY
tunnel-group RA webvpn-attributes
 group-alias RA enable

tunnel-group RA2 type remote-access
tunnel-group RA2 general-attributes
 default-group-policy MY
tunnel-group RA2 webvpn-attributes
 group-alias RA2 enable

group-policy MY attributes
 address-pools value POOL

webvpn
 enable inside
 anyconnect enable
 tunnel-group-list enable
```

L'utilisateur de Cisco peut utiliser seulement le groupe de tunnels de RA, et l'utilisateur cisco2 peut utiliser seulement le groupe de tunnels RA2.

Si l'utilisateur cisco2 choisit le groupe de tunnels de RA, alors la connexion est refusée :

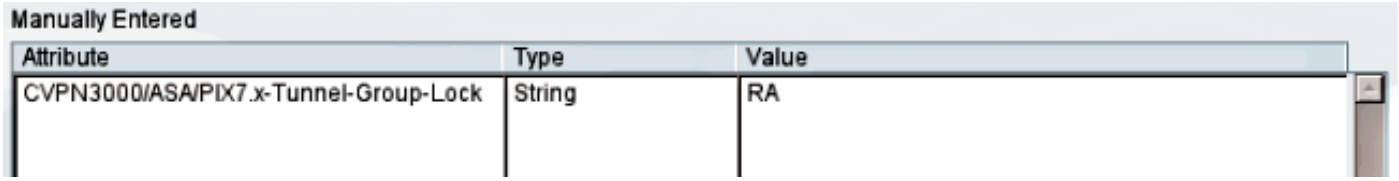



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to <RA2>.
```

ASA avec l'aaa attribute VPN3000/ASA/PIX7.x-Tunnel-Group-Lock

Attribuez 3076/85 (Tunnel-Groupe-verrouillage) qui est retourné par le serveur d'AAA fait exactement la même chose. Il peut être passé avec l'utilisateur ou l'authentification de policy group (ou attribut 25 d'Internet Engineering Task Force (IETF)) et verrouille l'utilisateur à un groupe de tunnels spécifique.

Voici un profil d'autorisation d'exemple sur le serveur de contrôle d'accès de Cisco (ACS) :



Quand l'attribut est retourné par AAA, le RAYON met au point l'indiquent :

```
tunnel-group RA2 general-attributes
 authentication-server-group ACS54 Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 2 (0x02)
Radius: Length = 61 (0x003D)
Radius: Vector: E55D5EBF1558CA455DA46F5BF3B67354
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
63 69 73 63 6f                                  |  cisco
Radius: Type = 25 (0x19) Class
```

```
Radius: Length = 24 (0x18)
Radius: Value (String) =
43 41 43 53 3a 61 63 73 35 34 2f 31 35 38 33 33    |  CACS:acs54/15833
34 34 38 34 2f 33                                  |  4484/3
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 10 (0x0A)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 85 (0x55) The tunnel group that tunnel must be associated with
Radius: Length = 4 (0x04)
Radius: Value (String) =
52 41                                              |  RA
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
```

Le résultat est identique quand vous essayez d'accéder au groupe de tunnels RA2 tandis que groupe-verrouillé au sein du groupe de tunnels de RA :

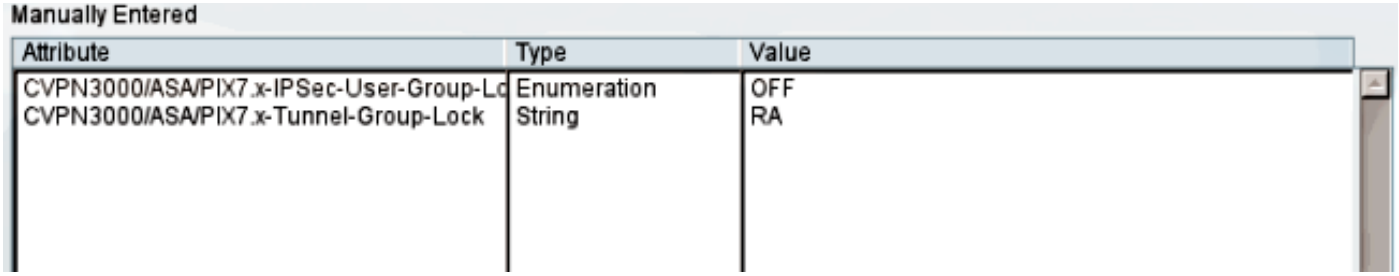
```
May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to <RA>
```

ASA avec l'aaa attribute VPN3000/ASA/PIX7.x-IPSec-User-Group-Lock

Cet attribut est également pris à partir du répertoire VPN3000 hérité par l'ASA. Il est encore présent dans le guide de configuration 8.4 (bien qu'il est retiré dans une plus nouvelle version de guide de configuration) et décrit en tant que :

```
IPsec-User-Group-Lock
0 = Disabled
1 = Enabled
```

Il s'avère que l'attribut pourrait être utilisé afin de désactiver le groupe-verrouillage, même si l'attribut de Tunnel-Groupe-verrouillage est présent. Si vous essayez de retourner qu'attribut réglé à 0 avec le Tunnel-Groupe-verrouillage (c'est toujours juste authentification de l'utilisateur), voici ce qui se produit. Il semble étrange quand vous essayez de désactiver le groupe-verrouillage tout en renvoyant un nom de groupe de tunnels spécifique :



Exposition de debugs :

```
Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 3 (0x03)
Radius: Length = 73 (0x0049)
Radius: Vector: 7C6260DDFC3E523CCC34AD8B828DD014
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
63 69 73 63 6f                                     |  cisco
Radius: Type = 25 (0x19) Class
Radius: Length = 24 (0x18)
Radius: Value (String) =
43 41 43 53 3a 61 63 73 35 34 2f 31 35 38 33 33    |  CACS:acs54/15833
```

```
34 34 38 34 2f 34                                    |  4484/4
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 33 (0x21) Group-Lock
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 0 (0x0000)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 10 (0x0A)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 85 (0x55) The tunnel group that tunnel must be associated with
Radius: Length = 4 (0x04)
Radius: Value (String) =
52 41                                                |  RA
rad_procpkt: ACCEPT
```

Ceci donne le même résultat (le verrouillage de groupe a été imposé, et l'IPSec-Utilisateur-Groupe-verrouillage n'a pas été pris en compte).

```
May 17 2013 17:42:34: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to <RA>
```

La stratégie de groupe externe a renvoyé IPSec-User-Group-Lock=0 et a également obtenu Tunnel-Group-Lock=RA pour l'authentification de l'utilisateur. Toujours, l'utilisateur a été verrouillé, ainsi il signifie que le verrouillage de groupe a été exécuté.

Pour la configuration opposée, la stratégie de groupe externe renvoie un nom de groupe de tunnels spécifique (Tunnel-Groupe-verrouillage) tandis qu'il essaye de désactiver le groupe-verrouillage pour un utilisateur spécifique (IPSec-User-Group-Lock=0), et groupe-verrouillant a été toujours imposé pour cet utilisateur.

Ceci confirme que l'attribut n'est plus utilisé. Cet attribut a été utilisé dans la vieille gamme VPN3000. L'ID de bogue Cisco CSCui34066 a été ouvert.

Group-lock local de Cisco IOS pour l'Easy VPN

L'option de group-lock locale sous la configuration de groupe dans des travaux de Cisco IOS différemment que sur l'ASA. Sur l'ASA, vous spécifiez le nom de groupe de tunnels auquel l'utilisateur est verrouillé. Les enables vérification supplémentaire d'option de group-lock de Cisco IOS (il n'y a aucun argument) et compare le groupe équipé de nom d'utilisateur (format user@group) à IKEID (nom de groupe).

Le pour en savoir plus, se rapportent au guide de configuration Easy VPN, la version de Cisco IOS 15M&T.

Voici un exemple :

```
aaa new-model
aaa authentication login LOGIN local
aaa authorization network LOGIN local

username cisco1@GROUP1 password 0 cisco1
username cisco2@GROUP2 password 0 cisco2

crypto isakmp client configuration group GROUP1
 key cisco
 pool POOL
```

```
 group-lock
 save-password
!
crypto isakmp client configuration group GROUP2
 key cisco
 pool POOL
 save-password

crypto isakmp profile prof1
   match identity group GROUP1
   client authentication list LOGIN
   isakmp authorization list LOGIN
   client configuration address respond
   client configuration group GROUP1
   virtual-template 1

crypto isakmp profile prof2
   match identity group GROUP2
   client authentication list LOGIN
   isakmp authorization list LOGIN
   client configuration address respond
   client configuration group GROUP2
   virtual-template 2

crypto ipsec transform-set aes esp-aes 256 esp-sha-hmac
 mode tunnel

crypto ipsec profile prof1
 set transform-set aes
 set isakmp-profile prof1

crypto ipsec profile prof2
 set transform-set aes
 set isakmp-profile prof2

interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile prof1

interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile prof2

ip local pool POOL 10.10.10.10 10.10.10.15
```

Ceci affiche que cela le groupe-verrouillage de la vérification est activé pour GROUP1. Pour GROUP1, le seul utilisateur permis est cisco1@GROUP1. Pour GROUP2 (aucun group-lock), les deux utilisateurs peuvent ouvrir une session.

Pour l'authentification réussie, utilisation cisco1@GROUP1 avec GROUP1 :

```
*May 19 18:21:37.983: ISAKMP:(0): Profile prof1 assigned peer the group named GROUP1
*May 19 18:21:40.595: ISAKMP/author: Author request for group GROUP1successfully
sent to AAA
```

Pour l'authentification, utilisation cisco2@GROUP2 avec GROUP1 :

```
*May 19 18:24:10.210: ISAKMP:(1011):User Authentication in this group failed
```

Ipsec d'AAA de Cisco IOS : utilisateur-VPN-groupe pour l'Easy VPN

L'ipsec : l'utilisateur-VPN-groupe est l'attribut RADIUS retourné par le serveur d'AAA, et il peut être appliqué seulement pour l'authentification de l'utilisateur (le group-lock a été utilisé pour le groupe). Les deux caractéristiques sont complémentaires, et elles sont appliquées à différentes étapes.

Le pour en savoir plus, se rapportent au guide de configuration Easy VPN, la version de Cisco IOS 15M&T.

Cela fonctionne différemment que le group-lock et te permet toujours pour réaliser le même résultat. La différence est que l'attribut doit avoir une valeur spécifique (comme pour l'ASA) et que la valeur spécifique est comparée au nom de groupe de Protocole ISAKMP (Internet Security Association and Key Management Protocol) (IKEID) ; s'il ne s'assortit pas, alors la connexion échoue. Voici ce qui se produit si vous changez l'exemple précédent afin d'avoir l'authentification d'AAA de client et désactiver le group-lock pour l'instant :

```
username cisco password 0 cisco        #for testing
aaa authentication login AAA group radius

crypto isakmp client configuration group GROUP1
no group-lock
crypto isakmp client configuration group GROUP2
no group-lock

crypto isakmp profile prof1
client authentication list AAA
crypto isakmp profile prof2
client authentication list AAA
```

Notez que l'ipsec : l'attribut d'utilisateur-VPN-groupe est défini pour l'utilisateur et le group-lock est défini pour le groupe.

Sur l'ACS, il y a deux utilisateurs, cisco1 et cisco2. Pour l'utilisateur cisco1, cet attribut est retourné : **ipsec:user-vpn-group=GROUP1**. Pour l'utilisateur cisco2, cet attribut est retourné : **ipsec:user-vpn-group=GROUP2**.

Quand les essais de l'utilisateur cisco2 à ouvrir une session avec GROUP1, cette erreur est signalés :

```
debug radius verbose
debug crypto isakmp
debug crypto isakmp aaa

*May 19 19:44:10.153: RADIUS:   Cisco AVpair       [1]   29
"ipsec:user-vpn-group=GROUP2"
*May 19 19:44:10.153: RADIUS(00000055): Received from id 1645/23
AAA/AUTHOR/IKE: Processing AV user-vpn-group
*May 19 19:44:10.154:
AAA/AUTHOR/IKE: User group GROUP2 does not match VPN group GROUP1 - access denied
```

C'est parce que l'ACS pour l'utilisateur cisco2 renvoie **ipsec:user-vpn-group=GROUP2**, qui est comparé par Cisco IOS à GROUP1.

De cette façon, le même but a été réalisée quant au group-lock. Vous pouvez voir qu'en ce moment, l'utilisateur final n'a pas besoin de fournir user@group comme nom d'utilisateur, mais pouvez utiliser l'utilisateur (sans @group).

Pour le group-lock, cisco1@GROUP1 devrait être utilisé, parce que le Cisco IOS a dénudé la dernière partie (après @) et l'a comparée à IKEID (nom de groupe).

Pour l'ipsec : utilisateur-VPN-groupe, il est suffisant d'utiliser seulement cisco1 dans le Client VPN Cisco, parce que cet utilisateur est défini sur l'ACS et l'ipsec spécifique : l'utilisateur-VPN-groupe est retourné (dans ce cas, c'est =GROUP1) et cet attribut est comparé contre IKEID.

Ipsec d'AAA de Cisco IOS : utilisateur-VPN-groupe et group-lock pour l'Easy VPN

Pourquoi ne devriez-vous pas utiliser les deux caractéristiques en même temps ?

Vous pouvez ajouter le group-lock de nouveau :

```
crypto isakmp client configuration group GROUP1
group-lock
crypto isakmp client configuration group GROUP2
group-lock
```

Voici l'écoulement :

1. L'utilisateur de Cisco VPN configure la connexion GROUP1 et se connecte.
2. La phase agressive de mode est réussie, et le Cisco IOS envoie une demande de Xauth du nom d'utilisateur et mot de passe.
3. L'utilisateur de Cisco VPN reçoit un instantané, et écrit le nom d'utilisateur de cisco1@GROUP1 avec le mot de passe correct défini sur l'ACS.
4. Le Cisco IOS exécute un vérifier le group-lock : il élimine le nom de groupe fourni dans le nom d'utilisateur et le compare à IKEID. Il est réussi.
5. Le Cisco IOS envoie une demande d'AAA au serveur ACS (pour utilisateur cisco1@GROUP1).

6. ACS renvoie un Rayon-recevoir avec **ipsec:user-vpn-group=GROUP1**.

7. Le Cisco IOS exécute une deuxième vérification ; cette fois, il compare le groupe fourni par l'attribut RADIUS à IKEID.

   Quand il échoue à l'étape 4 (verrouillage de groupe), l'erreur est enregistré juste après qu'elle fournit des qualifications :

   ```
   *May 19 20:14:31.678: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
   *May 19 20:14:31.678: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
   *May 19 20:14:31.678: ISAKMP:(1041):User Authentication in this group failed
   ```

   Quand il échoue à l'étape 7 (ipsec : l'utilisateur-VPN-groupe), l'erreur est retourné après qu'elle reçoive l'attribut RADIUS pour l'authentification d'AAA :

   ```
   AAA/AUTHOR/IKE: User group GROUP2 does not match VPN group GROUP1 - access denied
   ```

Verrouillage de groupe de webvpn IOS

Sur l'ASA, le Tunnel-Groupe-verrouillage peut être utilisé pour tous les services de l'Accès à distance VPN (IPSec, SSL, webvpn). Pour le group-lock de Cisco IOS et l'ipsec : utilisateur-VPN-groupe, cela fonctionne seulement pour IPSec (serveur VPN facile). Des utilisateurs spécifiques de group-lock dans des contextes spécifiques de webvpn (et des stratégies de groupe reliées), des domaines d'authentification devraient être utilisés.

Voici un exemple :

```
aaa new-model
aaa authentication login LIST local

username cisco password 0 cisco
username cisco1@C1 password 0 cisco
username cisco2@C2 password 0 cisco

webvpn gateway GW
 ip address 10.48.67.137 port 443
 http-redirect port 80
 logging enable
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-3.1.02040-k9.pkg sequence 1
 !
webvpn context C1
 ssl authenticate verify all
 !
 policy group C1
  functions file-access
  functions file-browse
  functions file-entry
  functions svc-enabled
  svc address-pool "POOL"
  svc default-domain "cisco.com"
  svc keep-client-installed
 default-group-policy C1
 aaa authentication list LIST
 aaa authentication domain @C1
 gateway GW domain C1 #accessed via https://IP/C1
 logging enable
 inservice
!
!
webvpn context C2
 ssl authenticate verify all

 url-list "L2"
  heading "Link2"
  url-text "Display2" url-value "http://2.2.2.2"

 policy group C2
  url-list "L2"
 default-group-policy C2
 aaa authentication list LIST
 aaa authentication domain @C2
 gateway GW domain C2 #accessed via https://IP/C2
 logging enable
 inservice

ip local pool POOL 7.7.7.10 7.7.7.20
```

Dans l'exemple suivant, il y a deux contextes : C1 et C2. Chaque contexte a sa propre stratégie de groupe avec les configurations spécifiques. C1 tient compte de l'accès d'AnyConnect. Le gataway est configuré afin d'écouter les deux contextes : C1 et C2.

Quand les accès client cisco1 le contexte C1 avec https://10.48.67.137/C1, le domaine d'authentification ajoute **C1** et l'authentifie contre (LISTE de liste) le nom d'utilisateur localement défini de cisco1@C1 :


```
debug webvpn aaa
debug webvpn

*May 20 16:30:07.518: WV: validated_tp :  cert_username :  matched_ctx :
*May 20 16:30:07.518: WV-AAA: AAA authentication request sent for user: "cisco1"
*May 20 16:30:07.518: WV: ASYNC req sent
*May 20 16:30:07.518: WV-AAA: AAA Authentication Passed!
*May 20 16:30:07.518: %SSLVPN-5-LOGIN_AUTH_PASSED: vw_ctx: C1 vw_gw: GW remote_ip:
10.61.218.146 user_name: cisco1, Authentication successful, user logged in
*May 20 16:30:07.518: WV-AAA: User "cisco1" has logged in from "10.61.218.146" to gateway "GW"
            context "C1"
```

Quand vous essayez d'ouvrir une session avec cisco2 comme nom d'utilisateur tandis que vous accédez au contexte C1 (https://10.48.67.137/C1), cette panne est signalé :

```
*May 20 16:33:56.930: WV: validated_tp :  cert_username :  matched_ctx :
*May 20 16:33:56.930: WV-AAA: AAA authentication request sent for user: "cisco2"
*May 20 16:33:56.930: WV: ASYNC req sent
*May 20 16:33:58.930: WV-AAA: AAA Authentication Failed!
*May 20 16:33:58.930: %SSLVPN-5-LOGIN_AUTH_REJECTED: vw_ctx: C1 vw_gw: GW
remote_ip: 10.61.218.146 user_name: cisco2, Failed to authenticate user credentials
```

C'est parce qu'il n'y a aucun cisco2@C1 défini par l'utilisateur. l'utilisateur de Cisco ne peut pas n'ouvrir une session à aucun contexte.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Guide de configuration Easy VPN, version de Cisco IOS 15M&T
- Guide de configuration de la gamme VPN CLI de Cisco ASA, 9.1

- Support et documentation techniques - Cisco Systems