Exemple de configuration des fonctionnalités de verrouillage de groupe ASA et Cisco IOS et des attributs AAA et WebVPN

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Configurations](#)
[ASA Local Group-lock](#)
[ASA avec attribut AAA VPN3000/ASA/PIX7.x-Tunnel-Group-Lock](#)
[ASA avec attribut AAA VPN3000/ASA/PIX7.x-IPSec-User-Group-Lock](#)
[Cisco IOS Local Group-lock pour Easy VPN](#)
[Cisco IOS AAA ipsec:user-vpn-group pour Easy VPN](#)
[Cisco IOS AAA ipsec:user-vpn-group and Group lock pour Easy VPN](#)
[IOS Webvpn Group Lock](#)
[Vérification](#)
[Dépannage](#)
[Informations connexes](#)

Introduction

Cet article décrit les fonctionnalités de verrouillage de groupe sur l'appliance de sécurité adaptative (ASA) de Cisco et dans Cisco IOS® et présente le comportement des différents attributs AAA (Authentication, Authorization, and Accounting). Pour Cisco IOS, la différence entre le verrouillage de groupe et les groupes vpn utilisateur est expliquée, ainsi qu'un exemple qui utilise les deux fonctions complémentaires en même temps. Il existe également un exemple Cisco IOS WebVPN avec des domaines d'authentification.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez une connaissance de base de ces sujets :

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

- Configuration VPN d'accès à distance sur l'ASA et Cisco IOS

Components Used

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

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurations

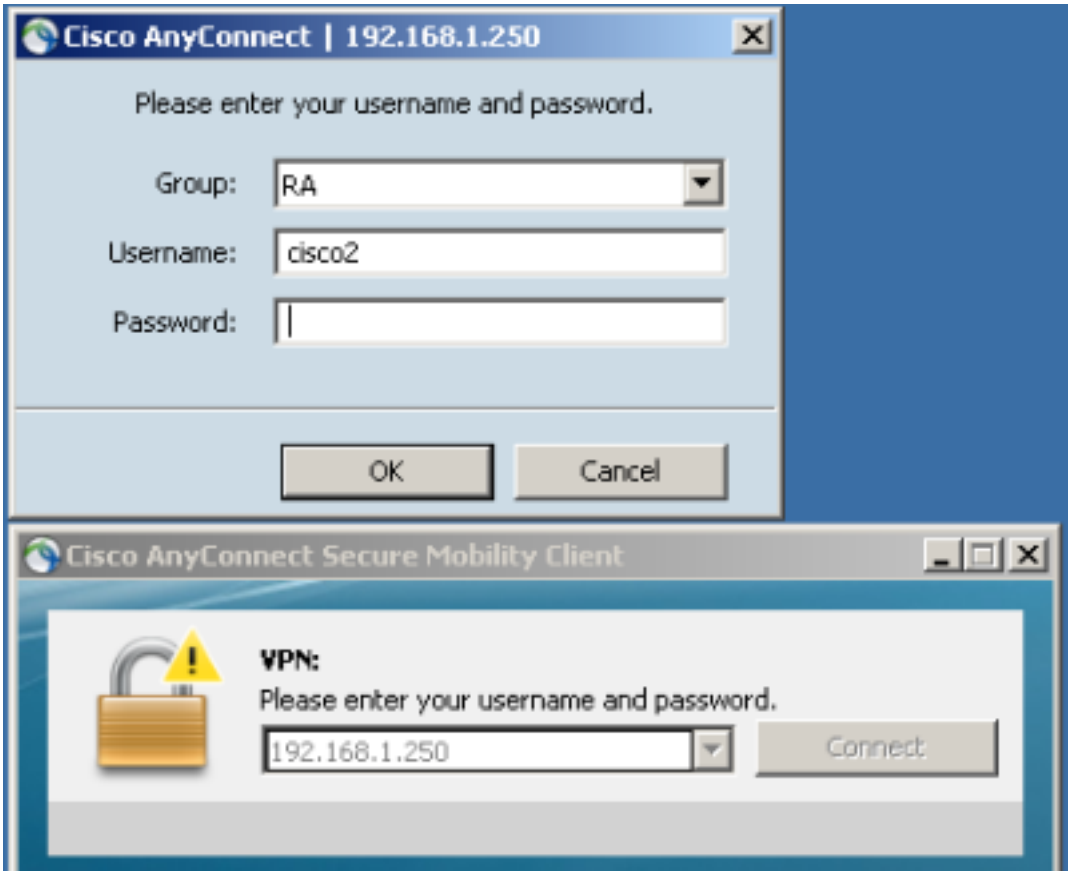
ASA Local Group-lock

Vous pouvez définir cet attribut sous l'utilisateur ou la stratégie de groupe. Voici un exemple pour l'attribut 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 cisco ne peut utiliser que le groupe de tunnels RA et l'utilisateur cisco2 ne peut utiliser que le groupe de tunnels RA2.

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

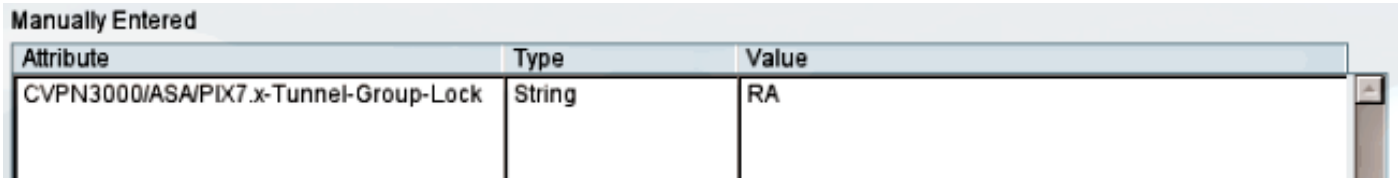



```
May 17 2013 17:24:54: %ASA-4-113040: Group <MY> User <cisco2> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA>. Reason: This connection is
group locked to .
```

ASA avec attribut AAA VPN3000/ASA/PIX7.x-Tunnel-Group-Lock

L'attribut 3076/85 (Tunnel-Group-Lock) retourné par le serveur AAA fait exactement la même chose. Il peut être transmis avec l'authentification de l'utilisateur ou du groupe de politiques (ou de l'attribut 25 de l'IETF (Internet Engineering Task Force) et verrouille l'utilisateur dans un groupe de tunnels spécifique.

Voici un exemple de profil d'autorisation sur Cisco Access Control Server (ACS) :



Lorsque l'attribut est retourné par AAA, les débogages RADIUS 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 le même lorsque vous essayez d'accéder au groupe de tunnels RA2 alors que le groupe est verrouillé dans le groupe de tunnels RA :

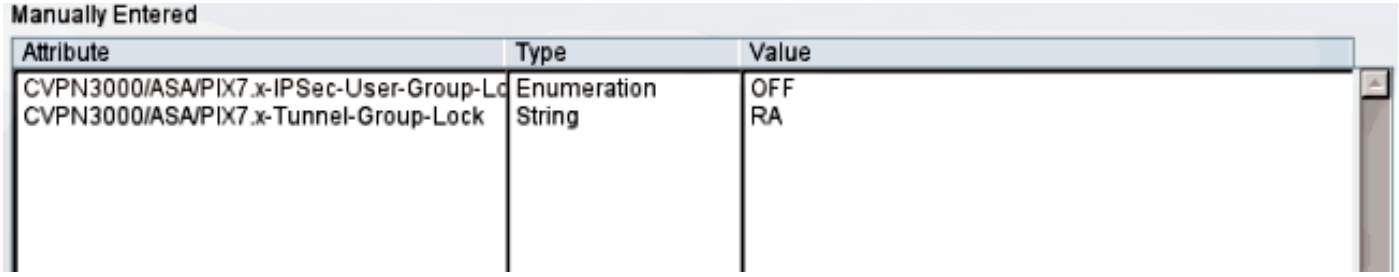
```
May 17 2013 17:41:33: %ASA-4-113040: Group <MY> User <cisco> IP <192.168.1.88>
Terminating the VPN connection attempt from <RA2>. Reason: This connection is
group locked to
```

ASA avec attribut AAA VPN3000/ASA/PIX7.x-IPSec-User-Group-Lock

Cet attribut provient également du répertoire VPN3000 hérité par l'ASA. Il est toujours présent dans le guide de configuration 8.4 (bien qu'il soit supprimé dans une version plus récente du guide de configuration) et décrit comme suit :

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

Il semble que l'attribut puisse être utilisé afin de désactiver le verrouillage de groupe, même si l'attribut Tunnel-Group-Lock est présent. Si vous essayez de renvoyer l'attribut défini sur 0 avec Tunnel-Group-Lock (il ne s'agit que de l'authentification de l'utilisateur), voici ce qui se passe. Cela semble étrange lorsque vous essayez de désactiver le verrouillage de groupe lors du retour d'un nom de groupe de tunnels spécifique :



Les débogages montrent :

```
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
```

Cela donne le même résultat (le verrouillage de groupe a été appliqué et le verrouillage de groupe d'utilisateurs IPSec 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
```

La stratégie de groupe externe a retourné IPSec-User-Group-Lock=0 et a également obtenu Tunnel-Group-Lock=RA pour l'authentification de l'utilisateur. Néanmoins, l'utilisateur a été verrouillé, ce qui signifie que le verrouillage de groupe a été effectué.

Pour la configuration opposée, la stratégie de groupe externe retourne un nom de groupe de tunnels spécifique (Tunnel-Group-Lock) alors qu'elle tente de désactiver le verrouillage de groupe pour un utilisateur spécifique (IPSec-User-Group-Lock=0), et le verrouillage de groupe a toujours été appliqué pour cet utilisateur.

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

Cisco IOS Local Group-lock pour Easy VPN

L'option de verrouillage de groupe local sous la configuration de groupe dans Cisco IOS fonctionne différemment que sur l'ASA. Sur l'ASA, vous spécifiez le nom du groupe de tunnels auquel l'utilisateur est verrouillé. L'option de verrouillage de groupe Cisco IOS (il n'y a aucun argument) permet une vérification supplémentaire et compare le groupe fourni avec le nom d'utilisateur (format user@group) avec IKEID (nom de groupe).

Pour plus d'informations, reportez-vous au Guide de configuration Easy VPN, Cisco IOS version 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 montre que la vérification du verrouillage de groupe est activée pour GROUP1. Pour GROUP1, le seul utilisateur autorisé est cisco1@GROUP1. Pour GROUP2 (pas de verrouillage de groupe), les deux utilisateurs peuvent se connecter.

Pour une authentification réussie, utilisez 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, utilisez cisco2@GROUP2 avec GROUP1 :

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

Cisco IOS AAA ipsec:user-vpn-group pour Easy VPN

L'attribut **ipsec : user-vpn-group** est l'attribut RADIUS retourné par le serveur AAA, et il peut être appliqué uniquement pour l'authentification des utilisateurs (le verrouillage de groupe a été utilisé pour le groupe). Ces deux fonctions sont complémentaires et appliquées à différentes étapes.

Pour plus d'informations, reportez-vous au Guide de configuration Easy VPN, Cisco IOS version 15M&T.

Il fonctionne différemment du groupe-lock et vous permet toujours d'obtenir le même résultat. La différence est que l'attribut doit avoir une valeur spécifique (comme pour l'ASA) et que cette valeur spécifique est comparée au nom de groupe IKEID (Internet Security Association and Key Management Protocol) ; si elle ne correspond pas, la connexion échoue. Voici ce qui se passe si vous modifiez l'exemple précédent afin d'avoir l'authentification AAA du client et désactiver le verrouillage de groupe pour le moment :

```
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'attribut ipsec : user-vpn-group est défini pour l'utilisateur et le verrouillage de groupe est défini pour le groupe.

Sur 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**.

Lorsque l'utilisateur cisco2 tente de se connecter avec GROUP1, cette erreur est signalée :

```
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
```

En effet, l'ACS de l'utilisateur cisco2 renvoie **ipsec : user-vpn-group=GROUP2**, qui est comparé par Cisco IOS à GROUP1.

De cette façon, le même objectif a été atteint que pour le blocage de groupe. Vous pouvez voir que l'utilisateur final n'a pas besoin de fournir user@group comme nom d'utilisateur, mais peut utiliser l'utilisateur (sans le groupe @group).

Pour le verrouillage de groupe, cisco1@GROUP1 doit être utilisé, car Cisco IOS a retiré la dernière partie (après @) et l'a comparée à IKEID (nom de groupe).

Pour le groupe ipsec:user-vpn, il suffit d'utiliser uniquement cisco1 dans le client VPN Cisco, car cet utilisateur est défini sur l'ACS et le groupe ipsec:user-vpn spécifique est renvoyé (dans ce cas, il s'agit de =GROUP1) et cet attribut est comparé à IKEID.

Cisco IOS AAA ipsec:user-vpn-group and Group lock pour Easy VPN

Pourquoi ne pas utiliser les deux fonctionnalités en même temps ?

Vous pouvez ajouter à nouveau le verrouillage de groupe :

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

Voici le flux :

1. L'utilisateur VPN Cisco configure la connexion GROUP1 et se connecte.
2. La phase du mode agressif a réussi et Cisco IOS envoie une requête xAuth pour le nom d'utilisateur et le mot de passe.
3. L'utilisateur VPN Cisco reçoit une fenêtre contextuelle et entre le nom d'utilisateur cisco1@GROUP1 avec le mot de passe correct défini sur l'ACS.
4. Cisco IOS vérifie le verrouillage de groupe : il supprime le nom de groupe fourni dans le nom d'utilisateur et le compare à IKEID. Il a réussi.
5. Cisco IOS envoie une requête AAA au serveur ACS (pour l'utilisateur cisco1@GROUP1).
6. ACS renvoie un objet RADIUS-Accept avec **ipsec : user-vpn-group=GROUP1**.
7. Cisco IOS effectue une deuxième vérification ; cette fois, il compare le groupe fourni par l'attribut RADIUS avec IKEID.

   Lorsqu'elle échoue à l'étape 4 (verrouillage de groupe), l'erreur est consignée immédiatement après avoir fourni des informations d'identification :

```
*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
```

Lorsqu'elle échoue à l'étape 7 (ipsec : user-vpn-group), l'erreur est renvoyée après réception de l'attribut RADIUS pour l'authentification AAA :

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

IOS Webvpn Group Lock

Sur l'ASA, le tunnel-Group-Lock peut être utilisé pour tous les services VPN d'accès à distance (IPSec, SSL, WebVPN). Pour le verrouillage de groupe Cisco IOS et le groupe ipsec:user-vpn, il fonctionne uniquement pour IPSec (Easy VPN Server). Afin de verrouiller des utilisateurs spécifiques dans des contextes WebVPN spécifiques (et des stratégies de groupe associées), les domaines d'authentification doivent 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 existe deux contextes : C1 et C2. Chaque contexte a sa propre stratégie de groupe avec des paramètres spécifiques. C1 permet l'accès AnyConnect. La passerelle est configurée pour écouter les deux contextes : C1 et C2.

Lorsque l'utilisateur cisco1 accède au contexte C1 avec https://10.48.67.137/C1, le domaine d'authentification ajoute **C1** et s'authentifie par rapport au nom d'utilisateur cisco1@C1 défini localement (liste LIST) :


```
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"
```

Lorsque vous essayez de vous connecter avec cisco2 en tant que nom d'utilisateur pendant que vous accédez au contexte C1 (https://10.48.67.137/C1), cet échec 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
```

En effet, aucun utilisateur cisco2@C1 n'est défini. l'utilisateur cisco ne peut se connecter à aucun contexte.

Vérification

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

Dépannage

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

Informations connexes

- Guide de configuration Easy VPN, Cisco IOS version 15M&T
- Guide de configuration du CLI VPN de la série Cisco ASA, 9.1
- Support et documentation techniques - Cisco Systems