Configurer le VPN d'accès à distance avec l'authentification RADIUS sur ISE et le mappage de stratégie de groupe

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

- Configuration
- ASA
- ISE

Vérifier

- Scénario de travail

Dépannage

- Scénario 1 non opérationnel
- Scénario 2 non opérationnel
- Scénario 3 non opérationnel

Vidéo

Introduction

Ce document décrit la configuration du VPN d'accès à distance pour le mappage de stratégie de groupe avec Cisco Identity Services Engine (ISE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Client sécurisé Cisco (AnyConnect)
- Cisco ISE

- VPN d'accès à distance sur Cisco Adaptive Security Appliance (ASA)

Composants utilisés

Le contenu de ce document est basé sur ces versions logicielles et matérielles.

- ASA 5506 doté de la version 9.8.1 du logiciel
- AnyConnect version 4.8
- ISE Version 2.4.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

Dans cet exemple de configuration, les utilisateurs distants se connectant à l'ASA via VPN à l'aide de Cisco Secure Client (AnyConnect) ne sont pas autorisés à sélectionner un profil de connexion (groupe de tunnels) dans le menu déroulant, car Cisco ISE les mappe à une stratégie de groupe spécifique basée sur les stratégies configurées.

Avec cette configuration, vous pouvez attribuer une stratégie de groupe à chaque utilisateur AnyConnect via ISE. Comme les utilisateurs n'ont pas la possibilité de sélectionner le groupe de tunnels, ils sont initialement connectés au groupe de tunnels DefaultWEBVPNGroup et à la stratégie de groupe DfltGrpPolicy. Après l'authentification, si l'attribut de classe RADIUS (Group-policy) est envoyé par ISE dans la réponse d'authentification, l'utilisateur est affecté à la stratégie de groupe correspondante, recevant ainsi les autorisations appropriées. Si ISE ne renvoie aucun attribut Class ou un libellé de stratégie de groupe qui n'est pas configuré sur l'ASA, l'utilisateur reste affecté à DfltGrpPolicy. Pour empêcher les utilisateurs sans stratégie de groupe assignée de se connecter via le VPN, vous pouvez configurer la commande vpn-simultanément-logins 0 sous la stratégie de groupe DfltGrpPolicy.

Configuration

ASA

Serveur AAA

```
aaa-server ISE_AAA protocol radius
aaa-server ISE_AAA (Outside) host 10.31.124.82
 key cisco123
```

Configuration VPN d'accès à distance

```
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-4.7.01076-webdeploy-k9.pkg 1
 anyconnect enable

tunnel-group DefaultWEBVPNGroup general-attributes
 address-pool Remote_users
 authentication-server-group ISE_AAA

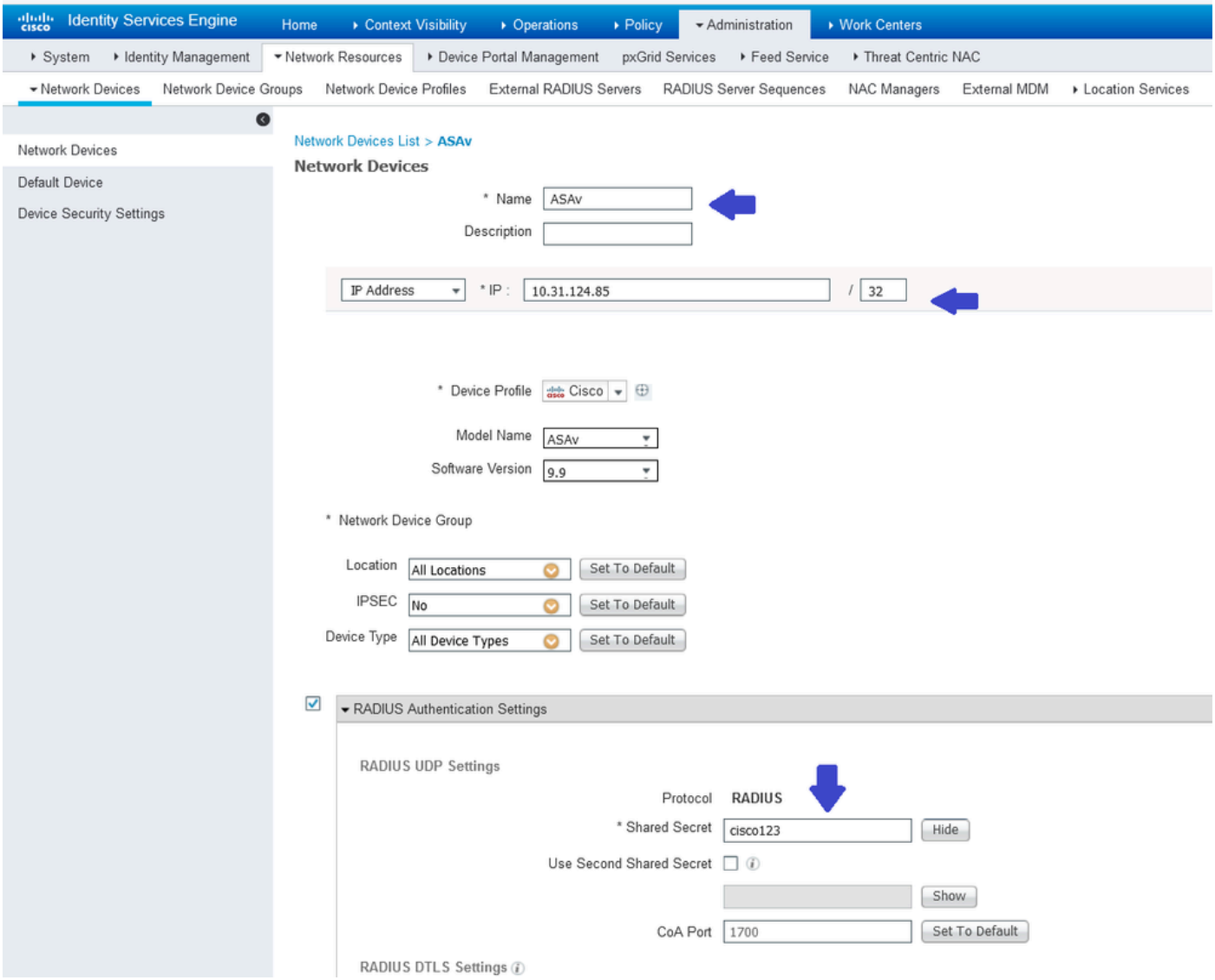
group-policy DfltGrpPolicy attributes
 banner value ###YOU DON'T HAVE AUTHORIZATION TO ACCESS ANY INTERNAL RESOURCES###
 vpn-simultaneous-logins 0
 vpn-tunnel-protocol ssl-client

group-policy RADIUS-USERS internal
group-policy RADIUS-USERS attributes
 banner value YOU ARE CONNECTED TO ### RADIUS USER AUTHENTICATION###
 vpn-simultaneous-logins 3
 vpn-tunnel-protocol ssl-client
 split-tunnel-network-list value SPLIT_ACL

group-policy RADIUS-ADMIN internal
group-policy RADIUS-ADMIN attributes
 banner value YOU ARE CONNECTED TO ###RADIUS ADMIN AUTHENTICATION ###
 vpn-simultaneous-logins 3
 vpn-tunnel-protocol ssl-client
 split-tunnel-network-list none
```

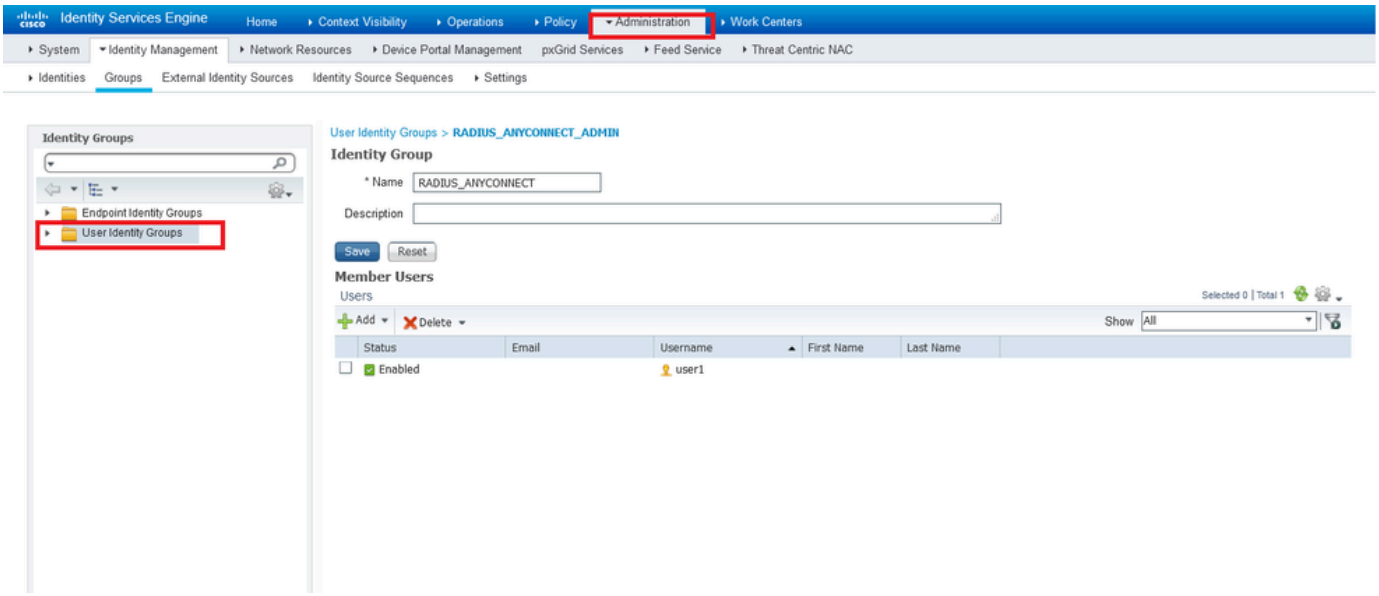
ISE

Étape 1 : enregistrement de l’ASA comme périphérique réseau valide sur ISE et configuration de la clé secrète partagée pour RADIUS Pour cela, accédez à Administration > Network Resources > Network Devices.



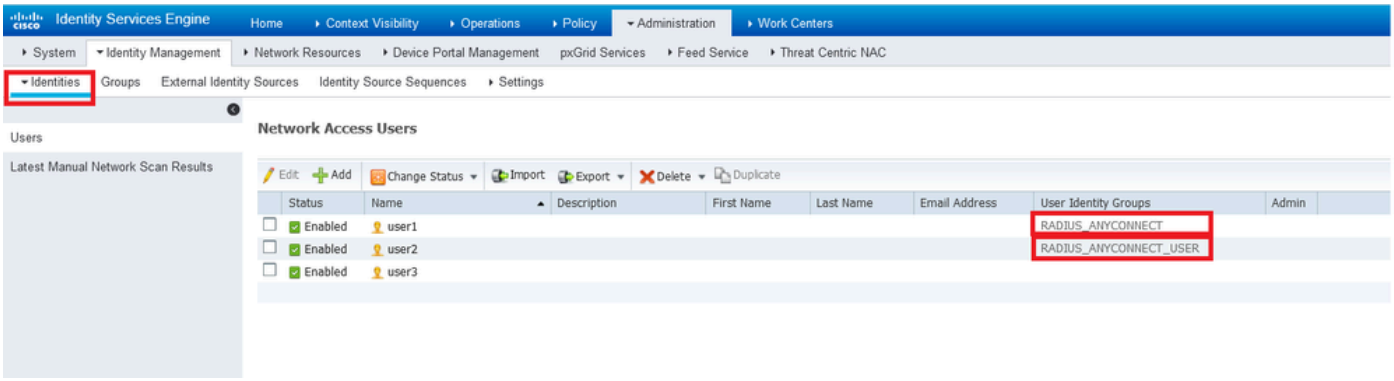
Étape 2 : création de groupes d’identités

Définissez des groupes d'identité pour associer des utilisateurs ayant des caractéristiques similaires et qui partagent des autorisations similaires. Elles sont utilisées dans les étapes suivantes. Accédez à Administration > Groups > User Identity Groups.



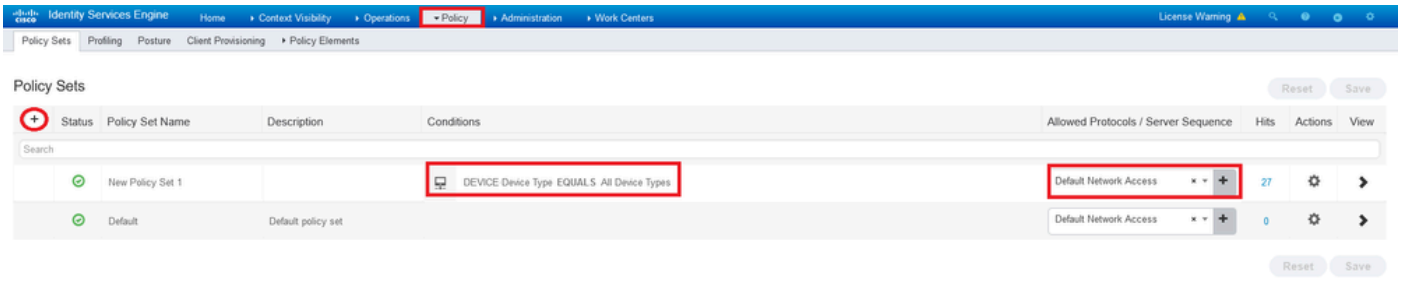
Étape 3. Associer des utilisateurs à des groupes d'identité

Associez les utilisateurs au groupe d'identité approprié. Accédez à Administration > Identities > Users.



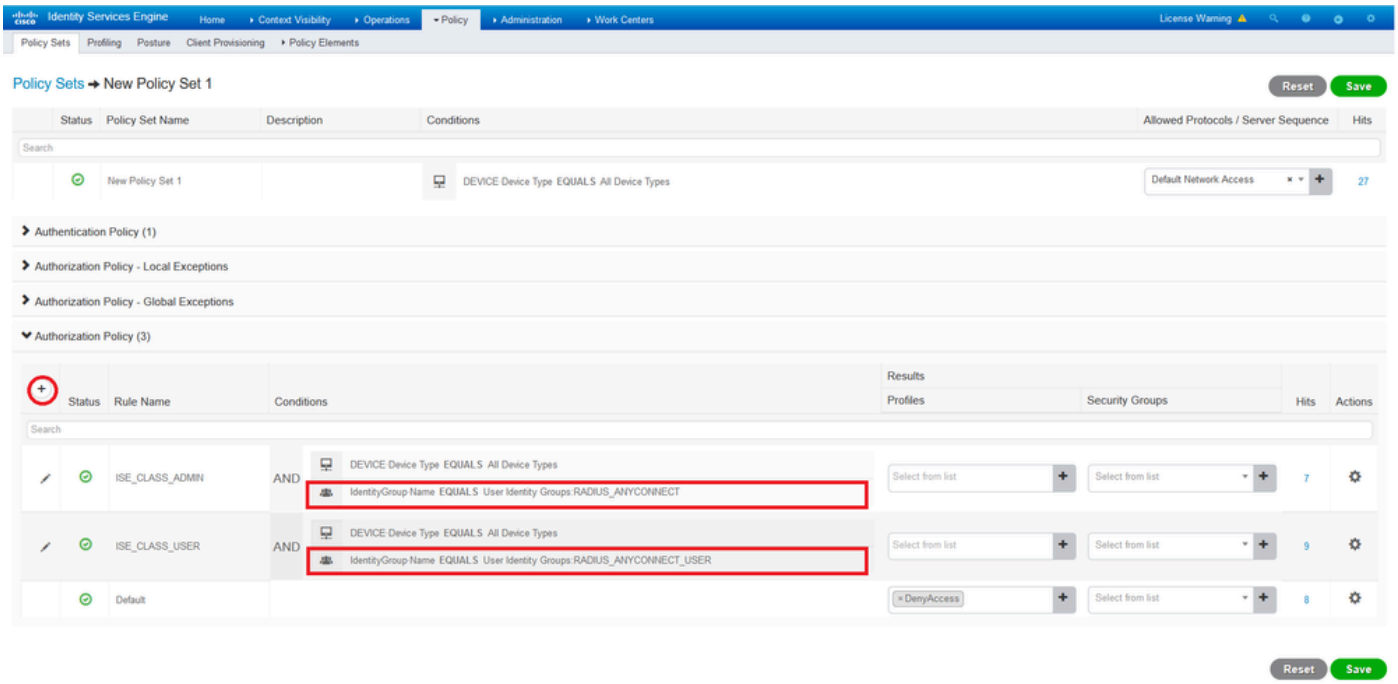
Étape 4 : création d'un ensemble de stratégies

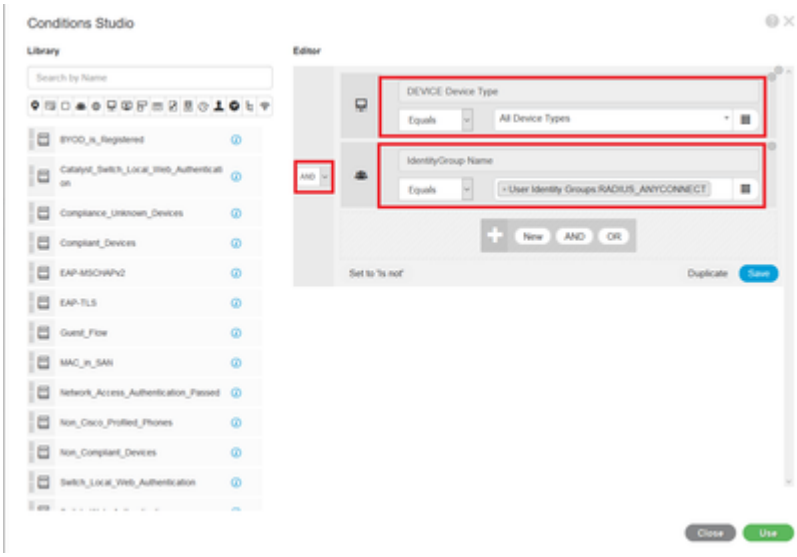
Définissez un nouvel ensemble de stratégies et définissez les conditions qui correspondent à la stratégie. Dans cet exemple, tous les types de périphériques sont autorisés dans ces conditions. Pour cela, accédez à Policy > Policy sets.



Étape 5. Créer une stratégie d’autorisation

Définissez une nouvelle stratégie d'autorisation avec les conditions requises pour correspondre à la stratégie. Veillez à inclure comme condition les groupes d'identité créés à l'étape 2.





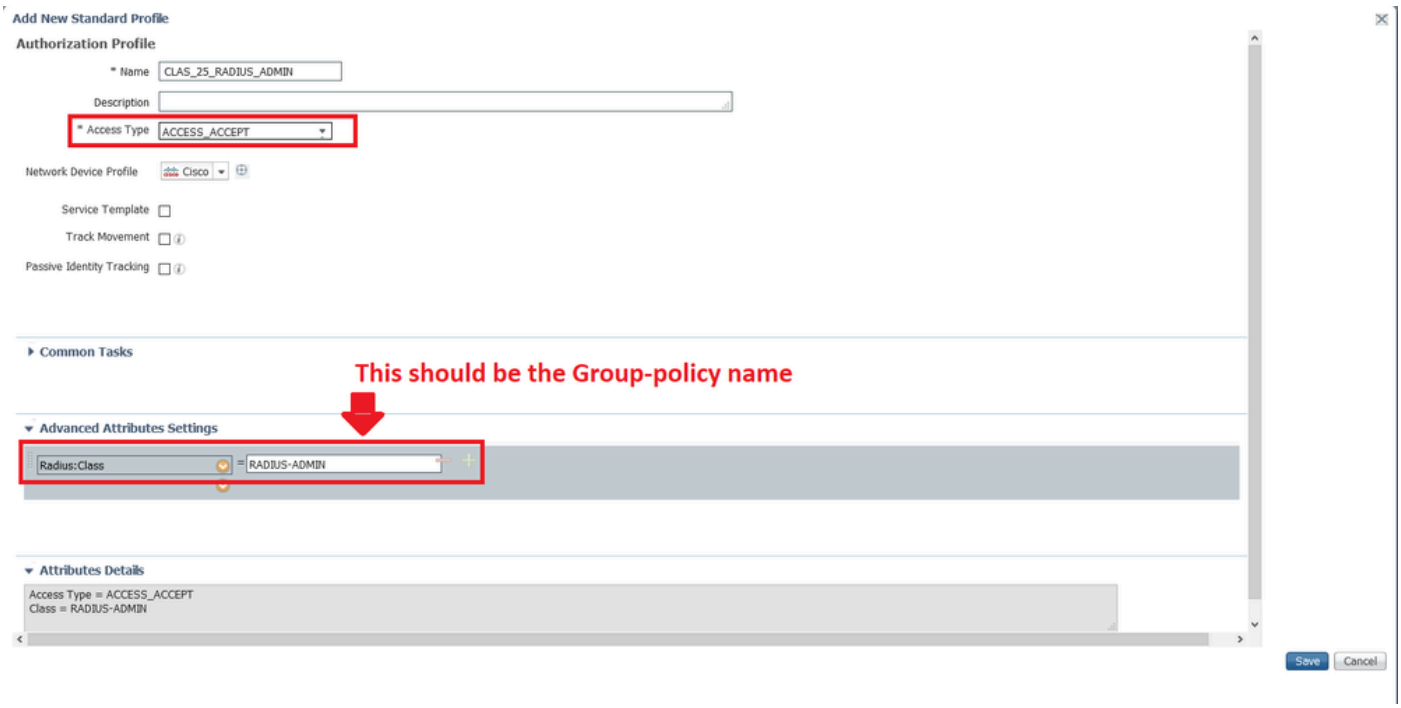
Étape 6. Créer un profil d’autorisation

Le profil d'autorisation inclut les actions qui sont entreprises lorsque la stratégie d'autorisation est mise en correspondance. Créez un nouveau profil d'autorisation qui inclut les attributs suivants :

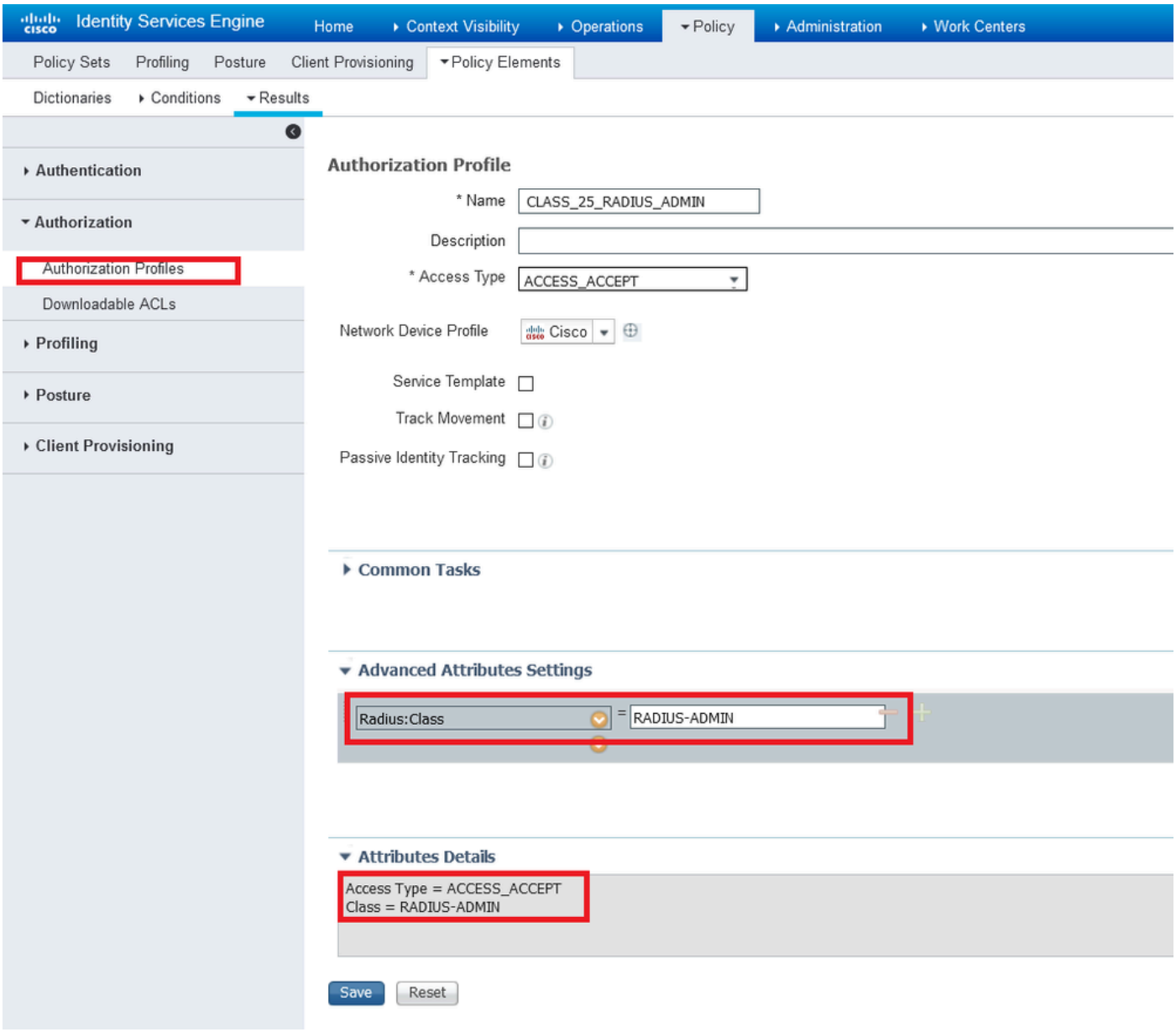
- Classe RADIUS = <Group-policy-ASA>
- Type d'accès : ACCESS_ACCEPT.

Remarque : Vous devez modifier la configuration affichée dans les images précédentes pour qu'elle corresponde au nom des stratégies de groupe que vous avez définies dans votre configuration ASA.

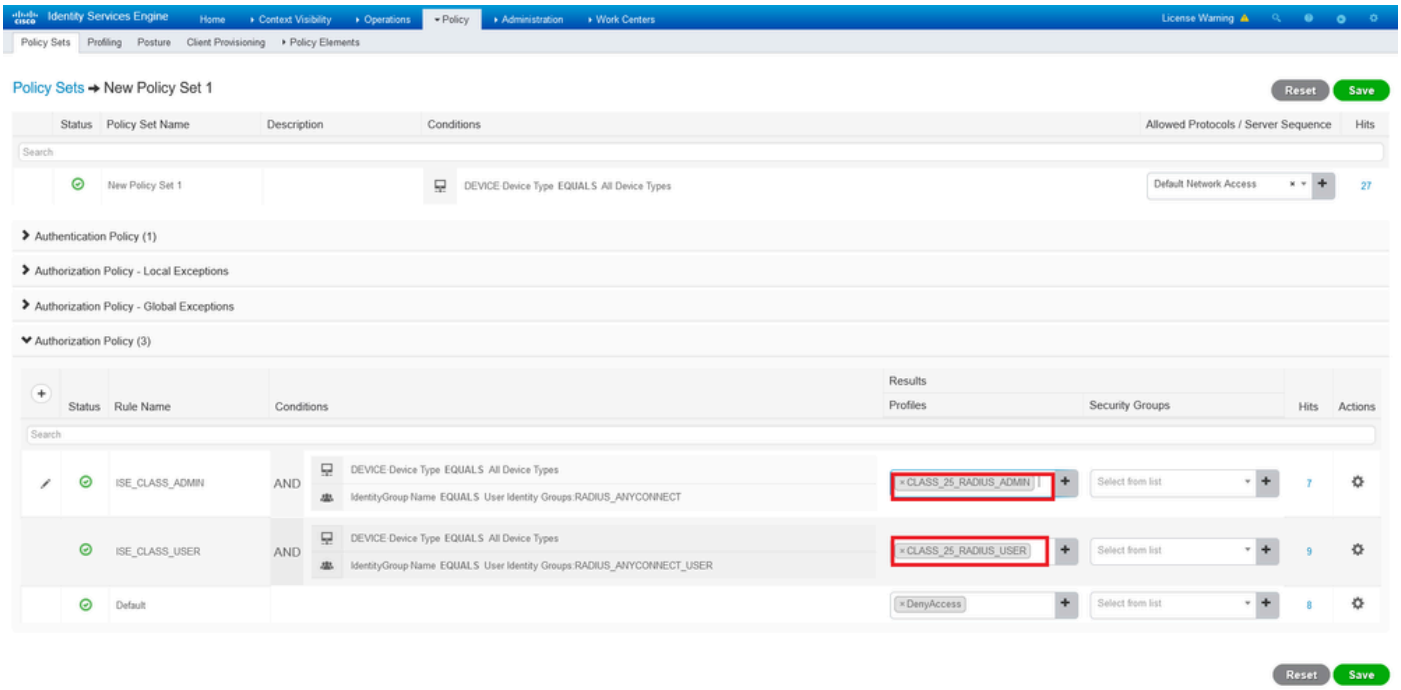




Étape 7 : vérification de la configuration du profil d’autorisation



Remarque : Dans le même jeu de stratégies, vous pouvez avoir aucune stratégie d'autorisation, pour mapper chaque groupe d'identité à une stratégie de groupe spécifique définie sur l'ASA.



Avec cet exemple de configuration, vous pouvez affecter la stratégie de groupe de manière dynamique à chaque utilisateur du client sécurisé via la configuration ISE en fonction du groupe d'identité auquel l'utilisateur appartient.

Vérifier

L'un des débogages les plus utiles est debug radius. Il affiche les détails de la demande d'authentification RADIUS et de la réponse d'authentification entre le serveur AAA (ISE) et l'ASA.

```
debug radius
```

La commande test aaa-server est un autre outil utile. Vous voyez maintenant si l'authentification est ACCEPTÉE ou REFUSÉE et les attributs (attribut de classe dans cet exemple) qui ont été échangés dans le processus d'authentification.

```
test aaa-server authentication <aaa_server_group> [host <name>|<host_ip>] username <user> password <pas
```

Scénario de travail

Dans l'exemple de configuration mentionné précédemment, user1 appartient à la stratégie de groupe RADIUS-ADMIN selon la configuration ISE. Il peut être vérifié si vous exécutez le test aaa-server et activez les débogages radius sur l'ASA. Les lignes correspondantes des débogages sont indiquées en gras.

<#root>

```
ASAv# debug radius
ASAv#test aaa-server authentication ISE_AAA host 10.31.124.82 username user1 password *****
INFO: Attempting Authentication test to IP address (10.31.124.82) (timeout: 12 seconds)


RADIUS packet decode (authentication request)


--------------------------------------
Raw packet data (length = 84).....
01 1e 00 54 ac b6 7c e5 58 22 35 5e 8e 7c 48 73    |  ...T..|.X"5^.|Hs
04 9f 8c 74 01 07 75 73 65 72 31 02 12 ad 19 1c    |  ...t..user1.....
40 da 43 e2 ba 95 46 a7 35 85 52 bb 6f 04 06 0a    |  @.C...F.5.R.o...
1f 7c 55 05 06 00 00 00 06 3d 06 00 00 00 05 1a    |  .|U......=......
15 00 00 00 09 01 0f 63 6f 61 2d 70 75 73 68 3d    |  .......coa-push=
74 72 75 65                                        |  true

Parsed packet data.....
Radius: Code = 1 (0x01)
Radius: Identifier = 30 (0x1E)
Radius: Length = 84 (0x0054)
Radius: Vector: ACB67CE55822355E8E7C4873049F8C74
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
75 73 65 72 31                                     |

user1


Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
ad 19 1c 40 da 43 e2 ba 95 46 a7 35 85 52 bb 6f    |  ...@.C...F.5.R.o
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.31.124.85 (0x0A1F7C55)
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x6
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 21 (0x15)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 15 (0x0F)
Radius: Value (String) =
63 6f 61 2d 70 75 73 68 3d 74 72 75 65             |  coa-push=true
send pkt 10.31.124.82/1645
rip 0x00007f03b419fb08 state 7 id 30
```

```
rad_vrfy() : response message verified
rip 0x00007f03b419fb08
 : chall_state ''
 : state 0x7
 : reqauth:
     ac b6 7c e5 58 22 35 5e 8e 7c 48 73 04 9f 8c 74
 : info 0x00007f03b419fc48
     session_id 0x80000007
     request_id 0x1e
     user 'user1'
     response '***'
     app 0
     reason 0
     skey 'cisco123'
     sip 10.31.124.82
     type 1
```

RADIUS packet decode (response)

```
--------------------------------------
Raw packet data (length = 188).....
02 1e 00 bc 9e 5f 7c db ad 63 87 d8 c1 bb 03 41    |  ....._|..c.....A
37 3d 7a 35 01 07 75 73 65 72 31 18 43 52 65 61    |  7=z5..user1.CRea
75 74 68 53 65 73 73 69 6f 6e 3a 30 61 31 66 37    |  uthSession:0a1f7
63 35 32 52 71 51 47 52 72 70 36 5a 35 66 4e 4a    |  c52RqQGRrp6Z5fNJ
65 4a 39 76 4c 54 6a 73 58 75 65 59 35 4a 70 75    |  eJ9vLTjsXueY5Jpu
70 44 45 61 35 36 34 66 52 4f 44 57 78 34 19 0e    |  pDEa564fRODWx4..
52 41 44 49 55 53 2d 41 44 4d 49 4e 19 50 43 41    |  RADIUS-ADMIN.PCA
43 53 3a 30 61 31 66 37 63 35 32 52 71 51 47 52    |  CS:0a1f7c52RqQGR
72 70 36 5a 35 66 4e 4a 65 4a 39 76 4c 54 6a 73    |  rp6Z5fNJeJ9vLTjs
58 75 65 59 35 4a 70 75 70 44 45 61 35 36 34 66    |  XueY5JpupDEa564f
52 4f 44 57 78 34 3a 69 73 65 61 6d 79 32 34 2f    |  RODWx4:iseamy24/
33 37 39 35 35 36 37 34 35 2f 33 31                |  379556745/31

Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 30 (0x1E)
Radius: Length = 188 (0x00BC)
Radius: Vector: 9E5F7CDBAD6387D8C1BB0341373D7A35
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
75 73 65 72 31                                     |
```

user1

```
Radius: Type = 24 (0x18) State
Radius: Length = 67 (0x43)
Radius: Value (String) =
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61    |  ReauthSession:0a
31 66 37 63 35 32 52 71 51 47 52 72 70 36 5a 35    |  1f7c52RqQGRrp6Z5
66 4e 4a 65 4a 39 76 4c 54 6a 73 58 75 65 59 35    |  fNJeJ9vLTjsXueY5
4a 70 75 70 44 45 61 35 36 34 66 52 4f 44 57 78    |  JpupDEa564fRODWx
34                                                 |  4
```

Radius: Type = 25 (0x19) Class

```
Radius: Length = 14 (0x0E)
Radius: Value (String) =
52 41 44 49 55 53 2d 41 44 4d 49 4e                |
```

RADIUS-ADMIN

```
Radius: Type = 25 (0x19) Class
Radius: Length = 80 (0x50)
Radius: Value (String) =
43 41 43 53 3a 30 61 31 66 37 63 35 32 52 71 51    |  CACS:0a1f7c52RqQ
47 52 72 70 36 5a 35 66 4e 4a 65 4a 39 76 4c 54    |  GRrp6Z5fNJeJ9vLT
6a 73 58 75 65 59 35 4a 70 75 70 44 45 61 35 36    |  jsXueY5JpupDEa56
34 66 52 4f 44 57 78 34 3a 69 73 65 61 6d 79 32    |  4fRODWx4:iseamy2
34 2f 33 37 39 35 35 36 37 34 35 2f 33 31          |  4/379556745/31
rad_procpkt: ACCEPT
```

RADIUS_ACCESS_ACCEPT

```
: normal termination
RADIUS_DELETE
remove_req 0x00007f03b419fb08 session 0x80000007 id 30
free_rip 0x00007f03b419fb08
radius: send queue empty
```

INFO: Authentication Successful

Une autre façon de vérifier si la stratégie de groupe correcte a été attribuée à l'utilisateur user1 par ISE lorsqu'il est connecté via le client sécurisé est avec la commande show vpn-sessiondb anyconnect.

<#root>

ASAv#

show vpn-sessiondb anyconnect

```
Session Type: AnyConnect
```

Username   : user1

```
                Index        : 28
Assigned IP  : 10.100.2.1            Public IP    : 10.100.1.3
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15604                 Bytes Rx     : 28706
```

Group Policy : RADIUS-ADMIN

```
Tunnel Group : DefaultWEBVPNGroup

Login Time   : 04:14:45 UTC Wed Jun 3 2020
Duration     : 0h:01m:29s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6401010001c0005ed723b5
Security Grp : none
```

Dépannage

Vous pouvez également utiliser les commandes debug radius et test aaa-server pour dépanner quand des problèmes se produisent. Les problèmes les plus courants sont décrits ci-après.

Scénario 1 non opérationnel

Si l'authentification échoue sur Anyconnect et que l'ISE répond par un REJECT, vous devez vérifier si l'utilisateur est associé à un groupe d'identité d'utilisateur ou si le mot de passe est incorrect. Accédez à Operations > Live logs > Details.

<#root>

```
RADIUS packet decode (response)

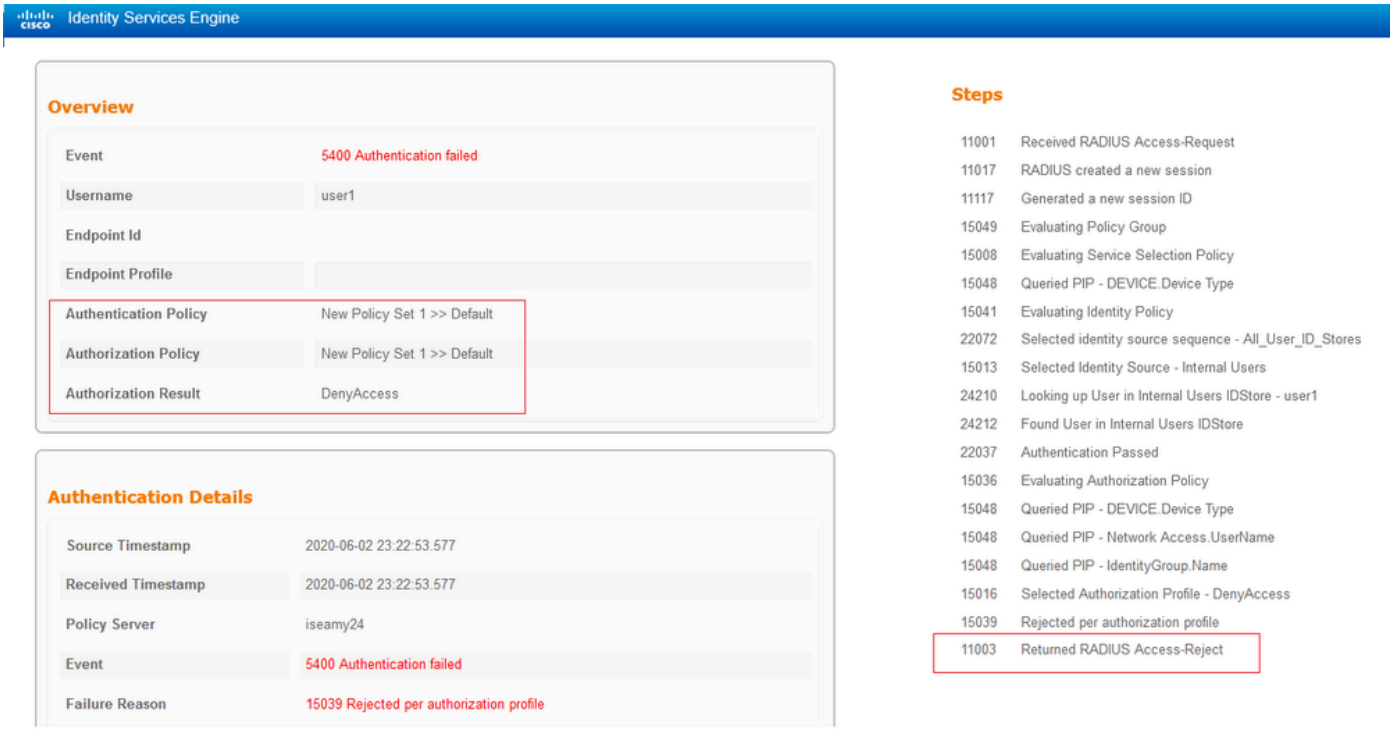
--------------------------------------
Raw packet data (length = 20).....
03 21 00 14 dd 74 bb 43 8f 0a 40 fe d8 92 de 7a    |  .!...t.C..@....z
27 66 15 be                                        |  'f..

Parsed packet data.....
Radius: Code = 3 (0x03)
Radius: Identifier = 33 (0x21)
Radius: Length = 20 (0x0014)
Radius: Vector: DD74BB438F0A40FED892DE7A276615BE
rad_procpkt:

REJECT

RADIUS_DELETE
remove_req 0x00007f03b419fb08 session 0x80000009 id 33
free_rip 0x00007f03b419fb08
radius: send queue empty

ERROR: Authentication Rejected: AAA failure
```



Remarque : Dans cet exemple, l'utilisateur user1 n'est associé à aucun groupe d'identité d'utilisateur. Par conséquent, il atteint les stratégies d'authentification et d'autorisation par défaut sous le nouvel ensemble de stratégies 1 avec l'action Refuser l'accès. Vous pouvez modifier cette action en PermitAccess dans la stratégie d'autorisation par défaut pour autoriser les utilisateurs sans le groupe d'identité d'utilisateur associé à s'authentifier.

Scénario 2 non opérationnel

Si l'authentification échoue sur Anyconnect et que la stratégie d'autorisation par défaut est PermitAccess, l'authentification est acceptée. Cependant, l'attribut class n'est pas présenté dans la réponse Radius, par conséquent l'utilisateur est situé dans DfltGrpPolicy et il ne se connecte pas en raison de la commande configurée : vpn-simultanément-logins 0.

<#root>

RADIUS packet decode (response)

```
--------------------------------------
Raw packet data (length = 174).....
02 24 00 ae 5f 0f bc b1 65 53 64 71 1a a3 bd 88    |  .$.._...eSdq....
7c fe 44 eb 01 07 75 73 65 72 31 18 43 52 65 61    |  |.D...user1.CRea
75 74 68 53 65 73 73 69 6f 6e 3a 30 61 31 66 37    |  uthSession:0a1f7
63 35 32 32 39 54 68 33 47 68 6d 44 54 49 35 71    |  c5229Th3GhmDTI5q
37 48 46 45 30 7a 6f 74 65 34 6a 37 50 76 69 4b    |  7HFE0zote4j7PviK
5a 35 77 71 6b 78 6c 50 39 33 42 6c 4a 6f 19 50    |  Z5wqkxlP93BlJo.P
```

```
43 41 43 53 3a 30 61 31 66 37 63 35 32 32 39 54    |  CACS:0a1f7c5229T
68 33 47 68 6d 44 54 49 35 71 37 48 46 45 30 7a    |  h3GhmDTI5q7HFE0z
6f 74 65 34 6a 37 50 76 69 4b 5a 35 77 71 6b 78    |  ote4j7PviKZ5wqkx
6c 50 39 33 42 6c 4a 6f 3a 69 73 65 61 6d 79 32    |  lP93BlJo:iseamy2
34 2f 33 37 39 35 35 36 37 34 35 2f 33 37          |  4/379556745/37

Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 36 (0x24)
Radius: Length = 174 (0x00AE)
Radius: Vector: 5F0FBCB1655364711AA3BD887CFE44EB
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
75 73 65 72 31                                     |
```

user1

```
Radius: Type = 24 (0x18) State
Radius: Length = 67 (0x43)
Radius: Value (String) =
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61    |  ReauthSession:0a
31 66 37 63 35 32 32 39 54 68 33 47 68 6d 44 54    |  1f7c5229Th3GhmDT
49 35 71 37 48 46 45 30 7a 6f 74 65 34 6a 37 50    |  I5q7HFE0zote4j7P
76 69 4b 5a 35 77 71 6b 78 6c 50 39 33 42 6c 4a    |  viKZ5wqkxlP93BlJ
6f                                                 |  o
Radius: Type = 25 (0x19) Class
Radius: Length = 80 (0x50)
Radius: Value (String) =
43 41 43 53 3a 30 61 31 66 37 63 35 32 32 39 54    |  CACS:0a1f7c5229T
68 33 47 68 6d 44 54 49 35 71 37 48 46 45 30 7a    |  h3GhmDTI5q7HFE0z
6f 74 65 34 6a 37 50 76 69 4b 5a 35 77 71 6b 78    |  ote4j7PviKZ5wqkx
6c 50 39 33 42 6c 4a 6f 3a 69 73 65 61 6d 79 32    |  lP93BlJo:iseamy2
34 2f 33 37 39 35 35 36 37 34 35 2f 33 37          |  4/379556745/37
rad_procpkt: ACCEPT
```

RADIUS_ACCESS_ACCEPT

```
: normal termination
RADIUS_DELETE
remove_req 0x00007f03b419fb08 session 0x8000000b id 36
free_rip 0x00007f03b419fb08
radius: send queue empty
```

INFO: Authentication Successful

```
ASAv#
```

Si la valeur vpn-simultanément-logins 0 est remplacée par 1, l'utilisateur se connecte comme indiqué dans le résultat :

<#root>

```
ASAv# show vpn-sessiondb anyconnect
```

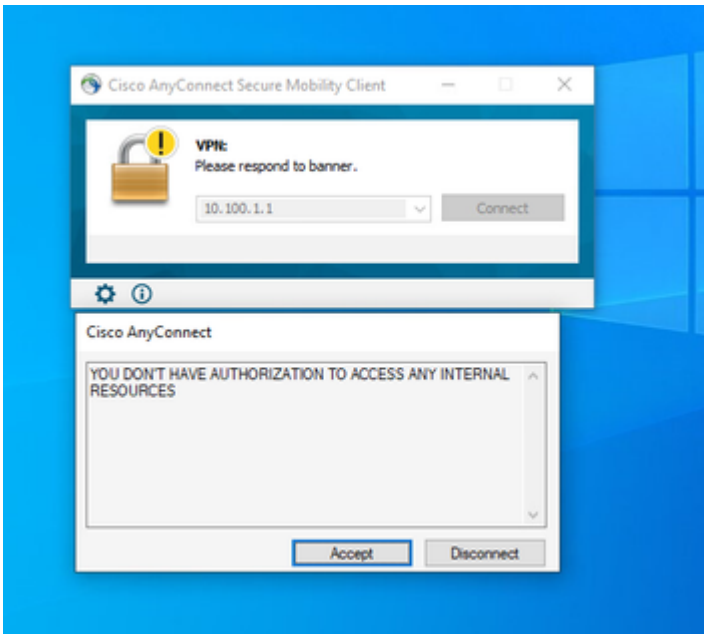
```
Session Type: AnyConnect


Username     : user1

                Index        : 41
Assigned IP  : 10.100.2.1             Public IP    : 10.100.1.3
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15448                  Bytes Rx     : 15528

Group Policy : DfltGrpPolicy          Tunnel Group : DefaultWEBVPNGroup

Login Time   : 18:43:39 UTC Wed Jun 3 2020
Duration     : 0h:01m:40s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a640101000290005ed7ef5b
Security Grp : none
```



Scénario 3 non opérationnel

Si l'authentification réussit mais que l'utilisateur n'a pas les bonnes stratégies appliquées, par exemple, si la stratégie de groupe connectée a le tunnel partagé au lieu du tunnel complet comme il doit l'être. L'utilisateur peut se trouver dans un groupe d'identité utilisateur incorrect.

<#root>

```
ASAv# sh vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect

Username     : user1

                 Index        : 29
Assigned IP  : 10.100.2.1             Public IP    : 10.100.1.3
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384
Bytes Tx     : 15592                  Bytes Rx     : 0

Group Policy : RADIUS-USERS

          Tunnel Group : DefaultWEBVPNGroup
Login Time   : 04:36:50 UTC Wed Jun 3 2020
Duration     : 0h:00m:20s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6401010001d0005ed728e2
Security Grp : none
```

Vidéo

Cette vidéo présente les étapes à suivre pour configurer SSL Anyconnect avec l'authentification ISE et l'attribut de classe pour le mappage de stratégie de groupe.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.