在ISE和组策略映射上配置具有RADIUS身份验证的远程访问VPN

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 配置
- ASA
- ISE

验证

- 工作场景

故障排除

- 非工作场景1
- 非工作场景2
- 非工作场景3

视频

简介

本文档介绍使用思科身份服务引擎(ISE)为组策略映射配置远程访问VPN。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全客户端(AnyConnect)
- 思科ISE
- 思科自适应安全设备(ASA)上的远程访问VPN

使用的组件

本文档的内容基于这些软件和硬件版本。

- 软件版本为 9.8.1 的 ASA 5506
- AnyConnect 版本 4.8
- ISE版本2.4。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

在此配置示例中，使用Cisco Secure Client(AnyConnect)通过VPN连接到ASA的远程用户不允许从下拉菜单中选择连接配置文件（隧道组），因为Cisco ISE会根据配置的策略将其映射到特定组策略。

通过此设置，您可以通过ISE为每个AnyConnect用户分配组策略。由于用户没有选择隧道组的选项，因此它们最初连接到DefaultWEBVPNGroup隧道组和DfltGrpPolicy组策略。身份验证后，如果ISE在身份验证响应中发送RADIUS类属性（组策略），则用户被分配到相应的组策略，从而接收适当的权限。如果ISE不返回任何Class属性或返回未在ASA上配置的组策略标签，则用户保持分配给DfltGrpPolicy。要防止没有分配组策略的用户通过VPN连接，您可以在DfltGrpPolicy group-policy下配置vpn-simultaneous-logins 0命令。

配置

ASA

aaa-server

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

远程访问VPN配置

```
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

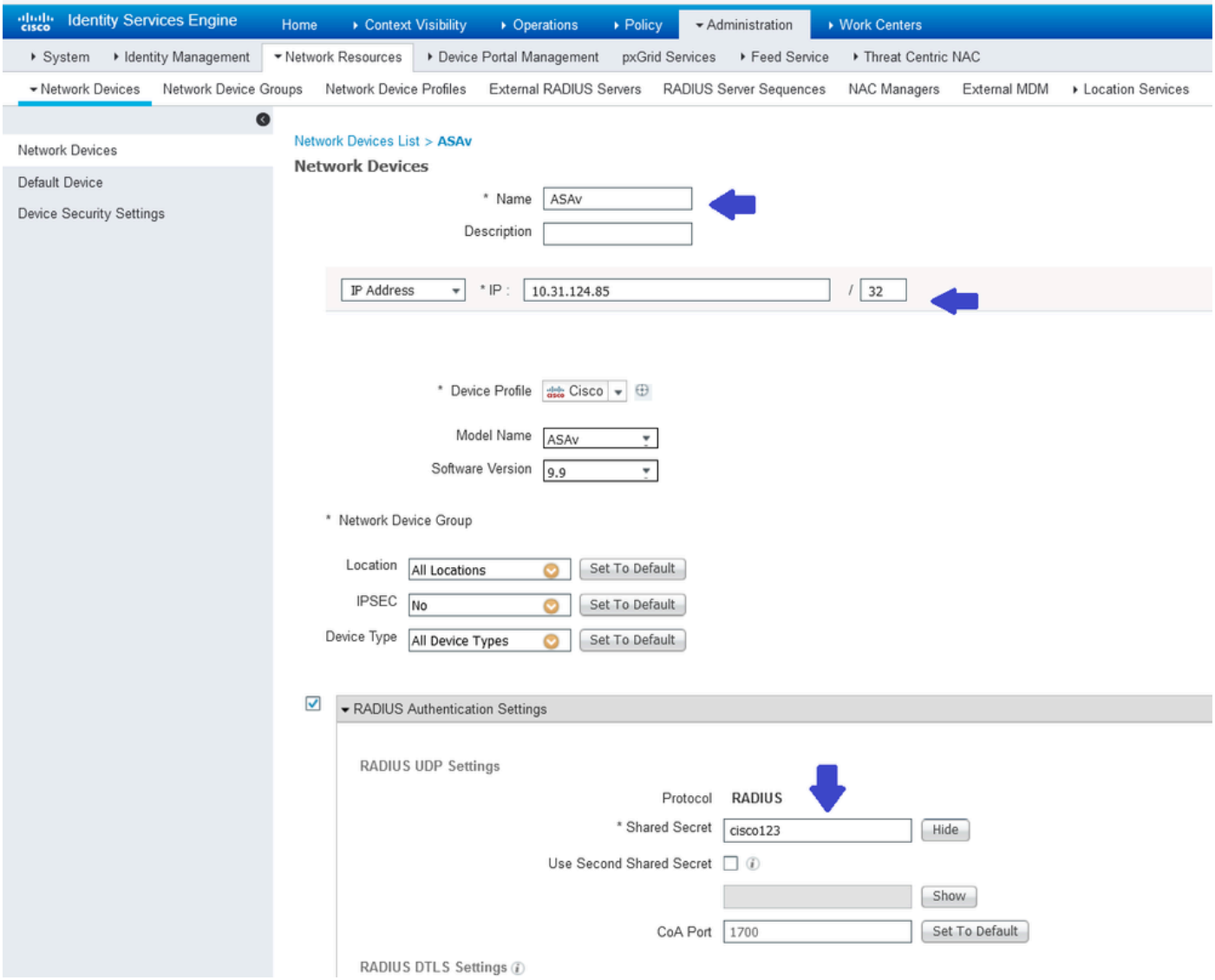
group-policy DfltGrpPolicy attributes
 banner value ###YOU DON'T HAVE AUTHORIZATION TO ACCESS ANY INTERNAL RESOURCES###
 vpn-simultaneous-logins 0
 vpn-tunnel-protocol ssl-client

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
```

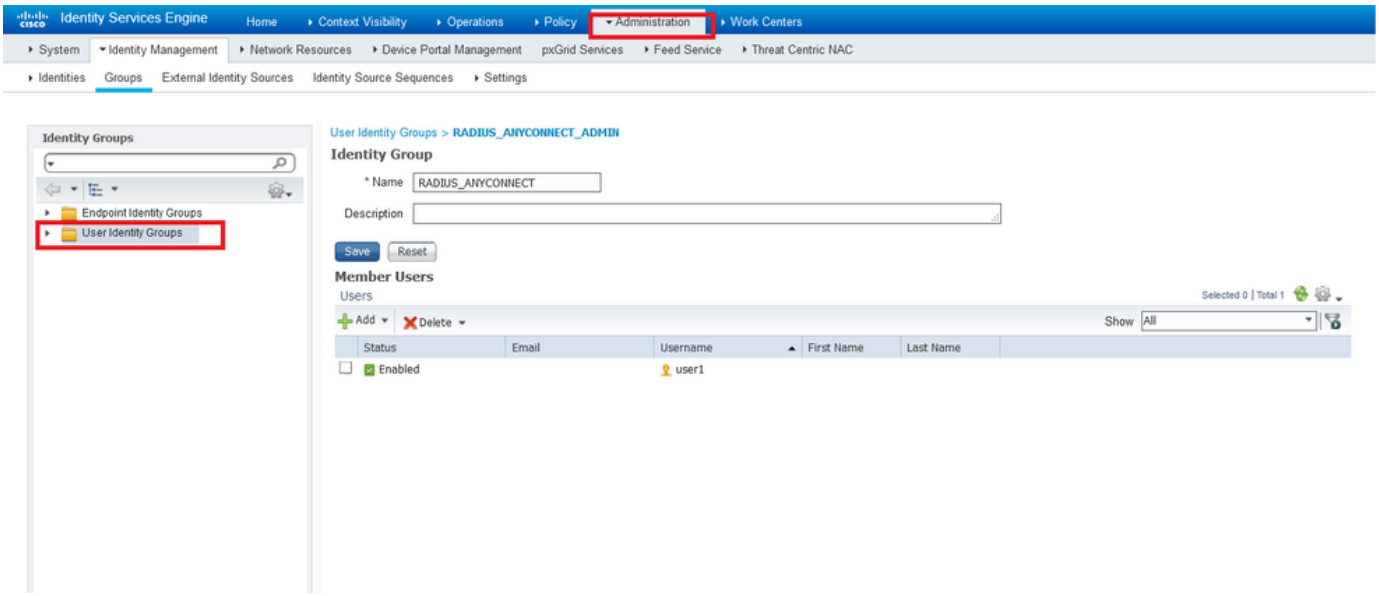
ISE

步骤1.将ASA注册为ISE上的有效网络设备并配置RADIUS的共享密钥。为此，请导航到管理>网络资源>网络设备。



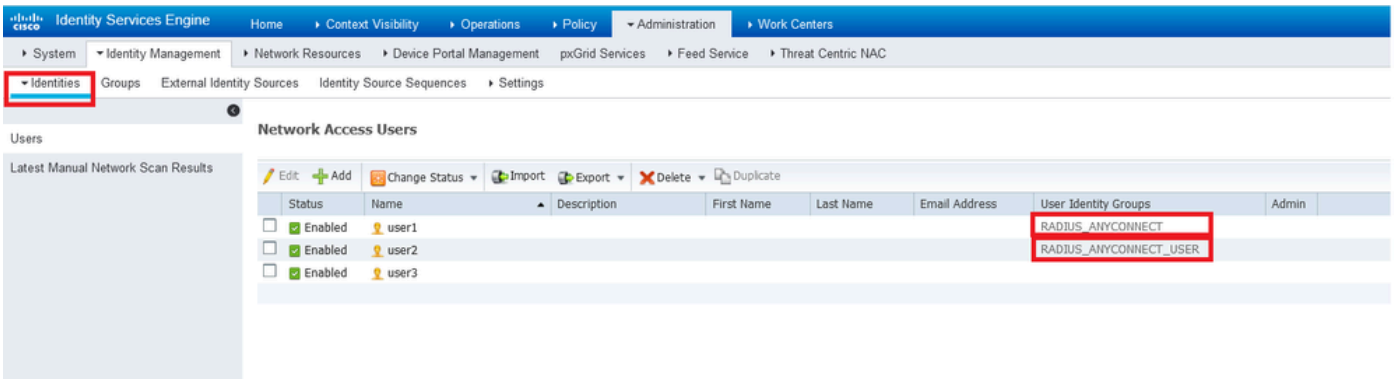
步骤2.创建身份组。

定义身份组，以关联具有相似特征以及共享相似权限的用户。这些将在后续步骤中使用。导航到 Administration > Groups > User Identity Groups。



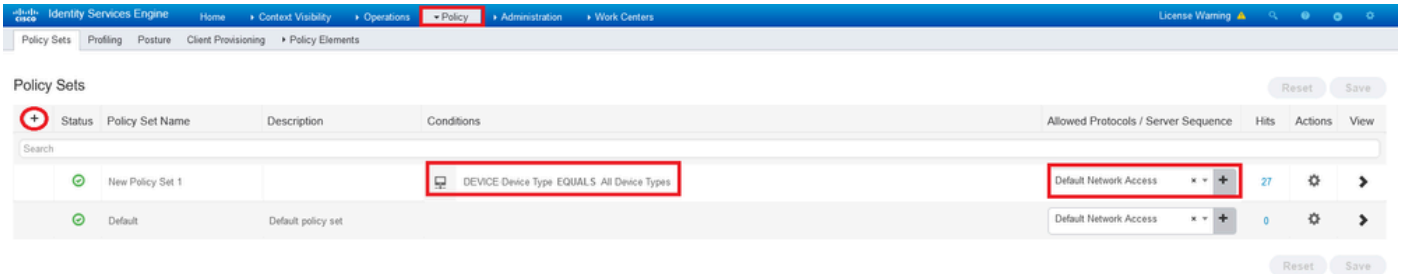
步骤3.将用户与身份组关联。

将用户关联到正确的身份组。导航到管理>身份>用户。



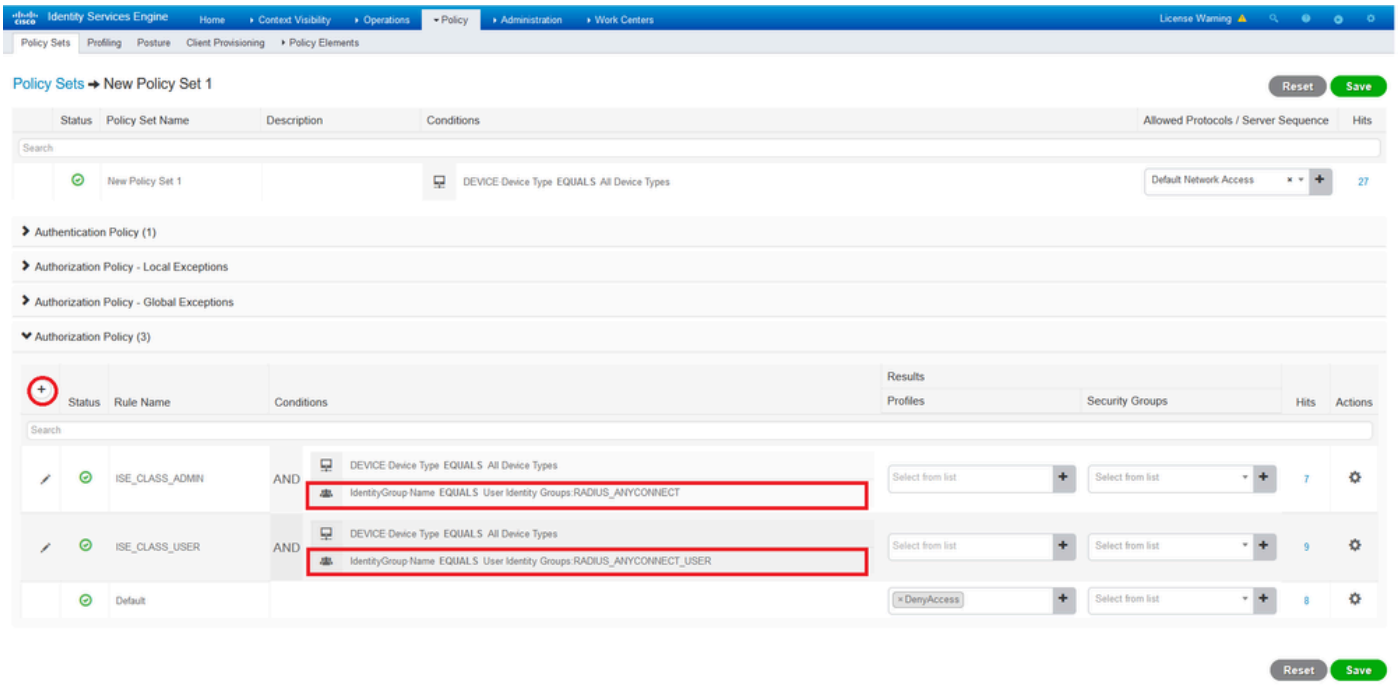
步骤4.创建策略集。

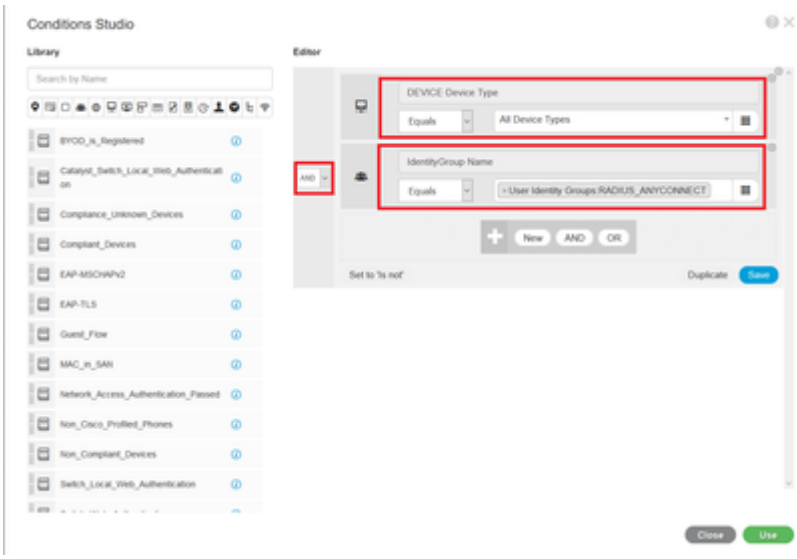
定义新的策略集并定义与策略匹配的条件。在本例中，在这些条件下允许所有设备类型。为此，请导航到Policy > Policy sets。



步骤5.创建授权策略。

定义新的授权策略以及匹配策略的所需条件。确保将步骤2中创建的身份组作为条件包含在内。





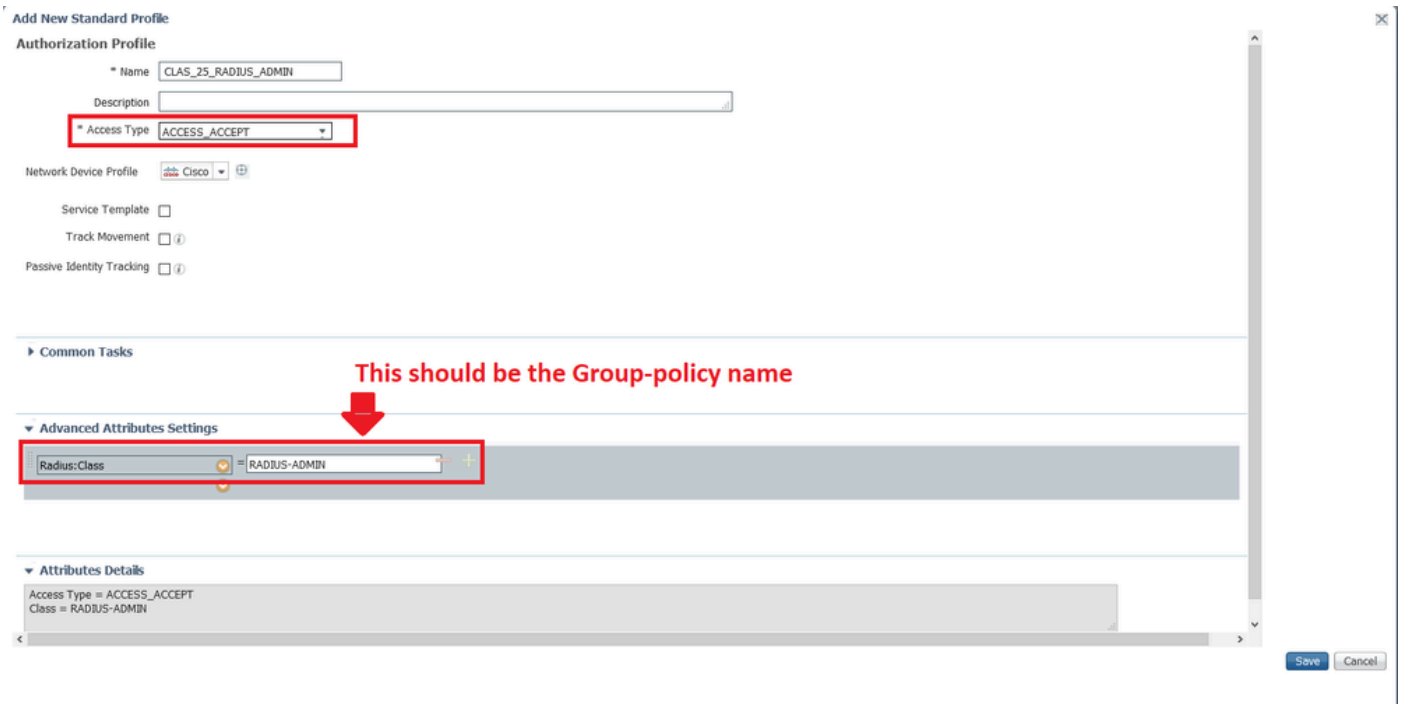
步骤6.创建授权配置文件。

授权配置文件包括匹配授权策略时执行的操作。创建包含下列属性的新授权配置文件:

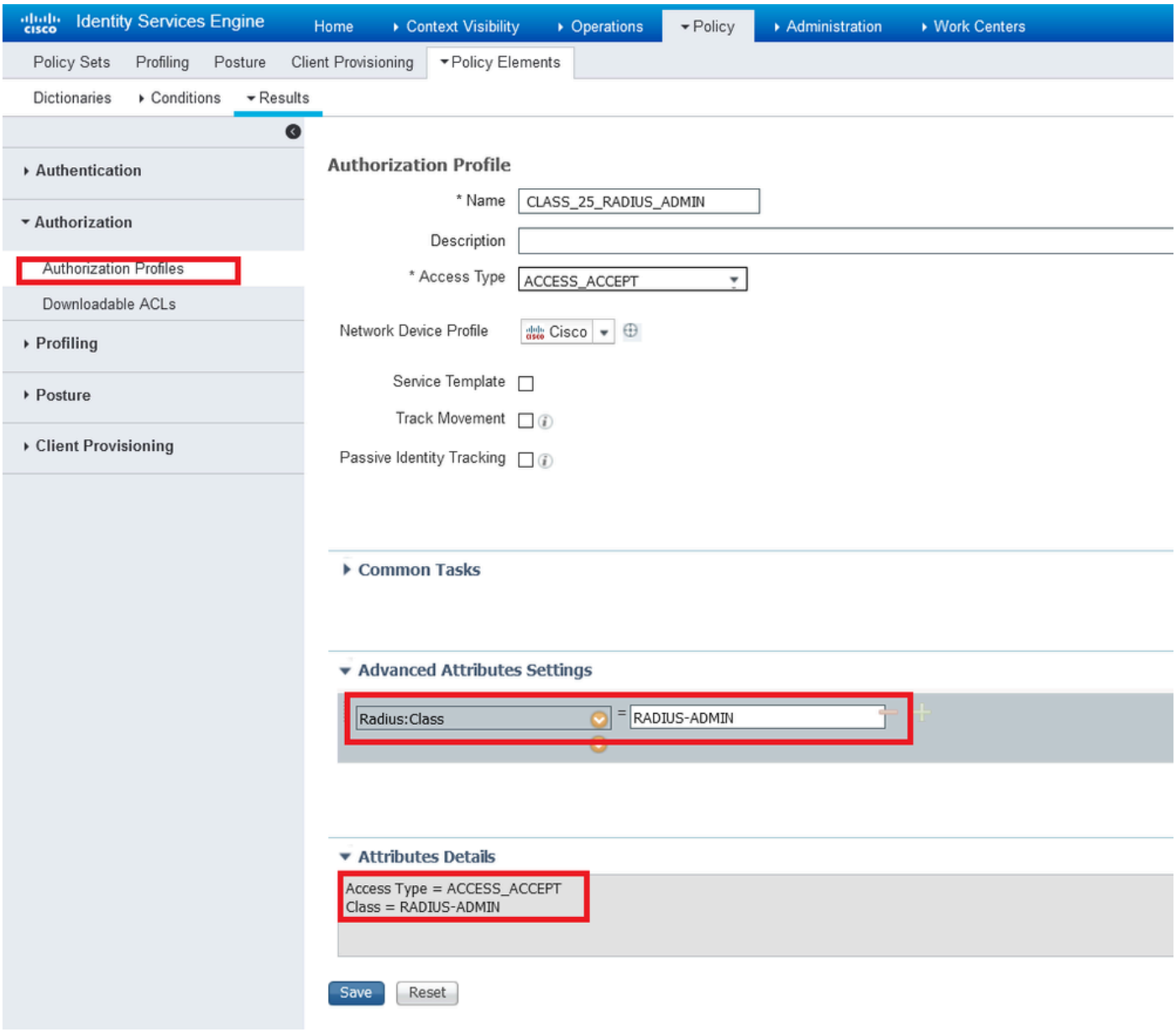
- RADIUS类= <Group-policy-ASA>
- 访问类型：ACCESS_ACCEPT。

注意：您必须编辑先前映像中显示的配置，以匹配在ASA配置中定义的组策略的名称。

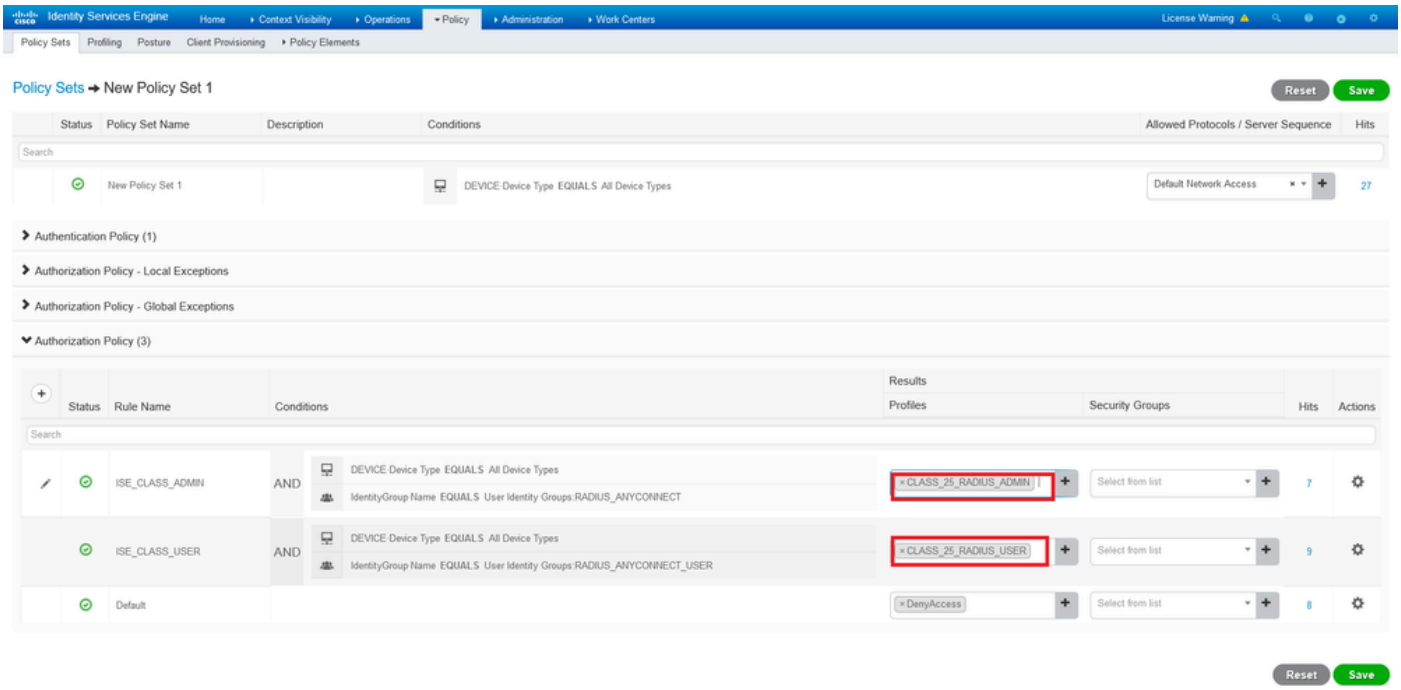




步骤7.检查授权配置文件配置。



注意：在同一策略集中，您可以拥有授权策略，以将每个身份组映射到ASA上定义的特定组策略。



在此配置示例中，您可以根据用户所属的身份组通过ISE配置将组策略动态分配到每个安全客户端用户。

验证

最有用的调试功能之一是debug radius。它显示了AAA服务器(ISE)和ASA之间的RADIUS身份验证请求和身份验证响应的详细信息。

```
debug radius
```

另一个有用的工具是test aaa-server命令。您现在可以看到身份验证是ACCEPTED还是REFUSED，以及身份验证过程中交换的属性（本示例中的类属性）。

```
test aaa-server authentication

      [host

      |
```

```
      ] username


        password
```

工作场景

在前面提到的配置示例中，根据ISE配置，user1属于RADIUS-ADMIN组策略。如果运行测试aaa-server并在ASA上启用radius调试，则可以验证该配置。调试中的相关行以粗体标记。

<#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

另一种验证通过安全客户端连接时ISE是否为user1分配了正确的组策略的方法是使用show vpn-sessiondb anyconnect命令。

```
<#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
```

故障排除

您还可以使用debug radius和test aaa-server命令对出现的问题进行故障排除。下面将介绍最常见的问题。

非工作场景1

如果Anyconnect上的身份验证失败，并且ISE回复REJECT，您需要验证用户是否与用户身份组关联，或者密码不正确。 导航到操作>实时日志>详细信息。

<#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
```

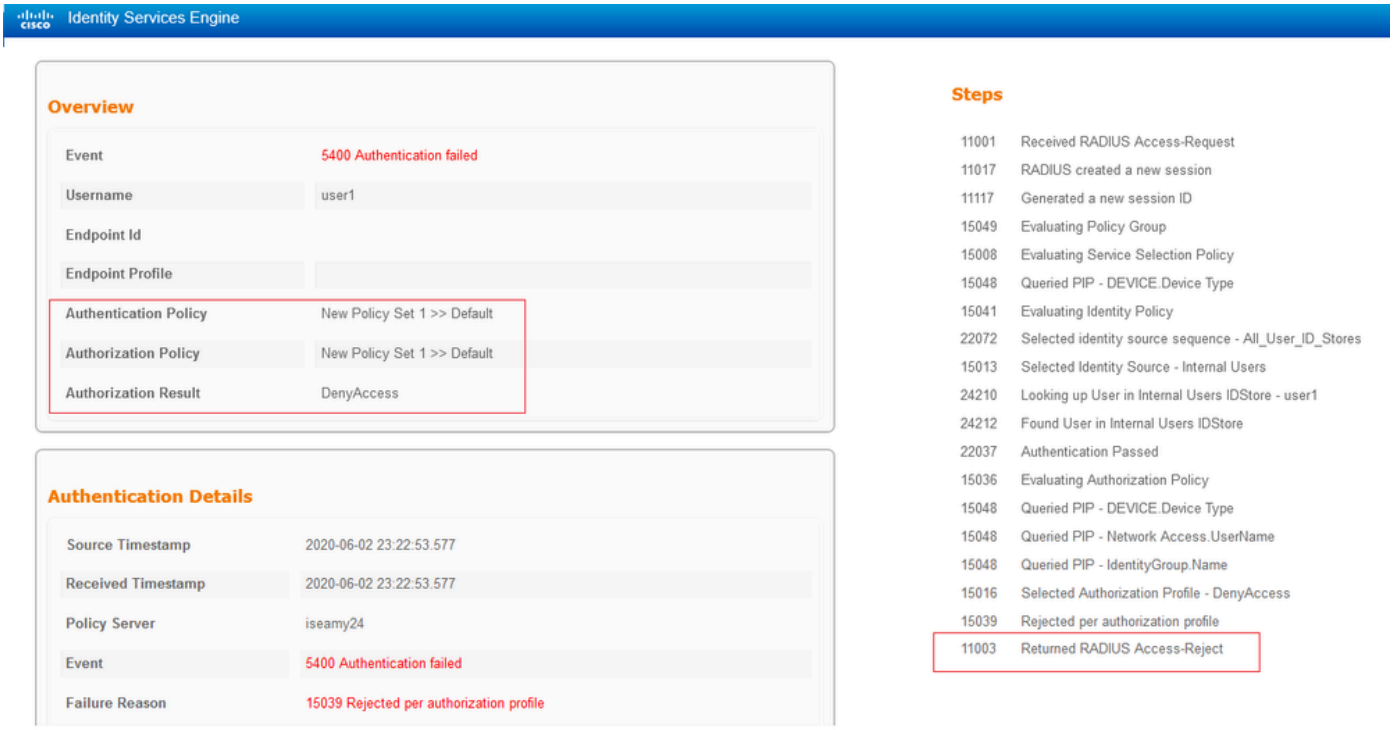
```
27 66 15 be                                          |  'f..

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



注意：在本示例中，user1未与任何用户身份组关联。因此，它通过DenyAccess操作命中新策略集1下的默认身份验证和授权策略。您可以将此操作修改为Default Authorization Policy中的PermitAccess，以允许没有关联用户身份组的用户进行身份验证。

非工作场景2

如果Anyconnect上的身份验证失败且默认授权策略为PermitAccess，则接受身份验证。但是，类属性未显示在Radius响应中，因此用户位于DfltGrpPolicy中，并且由于配置的命令vpn-simultaneous-

logins 0未连接。

<#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#
```

如果vpn-simultaneous-logins 0更改为1，则用户进行连接，如输出所示：

```
<#root>
ASAv# show vpn-sessiondb anyconnect

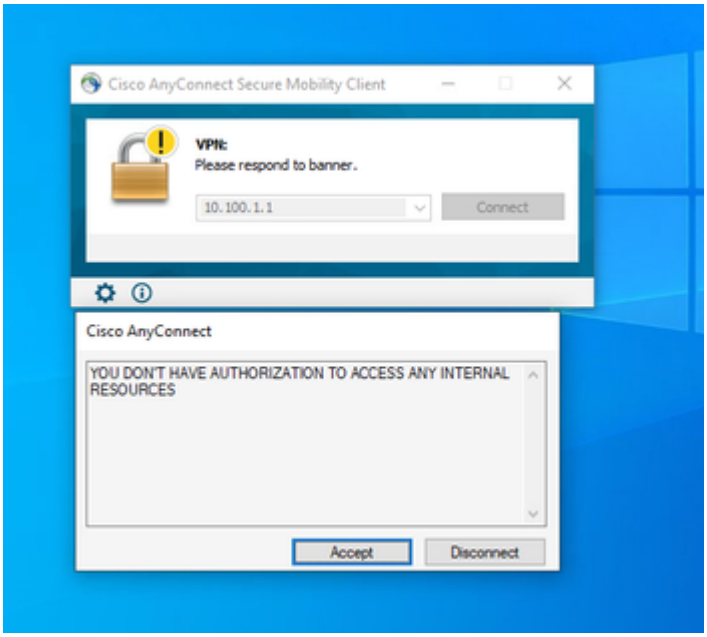
Session Type: AnyConnect


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
```



非工作场景3

如果身份验证通过，但用户没有应用正确的策略，例如，如果连接的组策略具有拆分隧道，而不是必须的全隧道。用户可能位于错误的用户身份组中。

<#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
```

视频

此视频提供了使用ISE身份验证和组策略映射的类属性配置SSL Anyconnect的步骤。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。