当RADIUS验证和授权配置时，远程访问VPN不工作

目录

简介

当两认证和授权配置时，本文描述扩展认证的行为VPN用户的。

先决条件

要求

Cisco 建议您了解以下主题：

- 验证、授权和记帐 (AAA)
- 远程访问 VPN

使用的组件

本文档中的信息根据思科聚合服务路由器(ASR)1000运行Cisco IOS XE软件的系列。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题

VPN用户配置为了由RADIUS服务器验证和授权。在ASR的配置显示此处：

```
aaa group server radius ACS-Rad
server-private 10.88.171.27 key cisco123
ip vrf forwarding Mgmt-intf
aaa group server tacacs+ ACS-Tac
server-private 10.88.171.27 key cisco123
ip vrf forwarding Mgmt-intf
aaa authentication login VPN_Client group ACS-Rad
aaa authentication login login_local local
aaa authorization network VPN_Client group ACS-Rad
aaa authorization network login_local local
aaa accounting network VPN_Client start-stop group ACS-Rad
aaa accounting network login_local start-stop group ACS-Rad
aaa session-id common
```

然而，每当您设法验证，您为您的凭证从未得到提示。 在客户端，此错误消息在日志消息被看到：

```
Unable to establish Phase 1 SA with server "X.X.X.X" because of
"DEL_REASON_PEER_NOT_RESPONDING"
```

在ASR的调试表明VPN组名称使用作为**用户名**授权尝试。

```
Sep 26 20:01:49.298: RADIUS(000025EA): Sending a IPv4 Radius Packet
Sep 26 20:01:49.298: RADIUS(000025EA): Send Access-Request to X.X.X.X id
1645/88,len 123
Sep 26 20:01:49.298: RADIUS:  authenticator 0B 18 41 30 23 35 91 D5 - C3 DE 78
4E BB AC 30 4C
Sep 26 20:01:49.298: RADIUS:  User-Name           [1]   19  "vpnclient.cisco.com"
Sep 26 20:01:49.298: RADIUS:  User-Password       [2]   18  *
Sep 26 20:01:49.298: RADIUS:  Calling-Station-Id  [31]  16  "X.X.X.X"
Sep 26 20:01:49.298: RADIUS:  NAS-Port-Type       [61]  6   Virtual             [5]
Sep 26 20:01:49.298: RADIUS:  NAS-Port            [5]   6   0
Sep 26 20:01:49.299: RADIUS:  NAS-Port-Id         [87]  16  "X.X.X.X"
Sep 26 20:01:49.299: RADIUS:  Service-Type        [6]   6   Outbound             [5]
Sep 26 20:01:49.299: RADIUS:  NAS-IP-Address      [4]   6   192.168.0.55
Sep 26 20:01:49.299: RADIUS:  Acct-Session-Id     [44]  10  "00002CD6"
Sep 26 20:01:49.299: RADIUS(000025EA): Started 5 sec timeout
Sep 26 20:01:49.326: RADIUS: Received from id 1645/88 X.X.X.X:1812, Access-Accept,
len 26
Sep 26 20:01:49.326: RADIUS:  authenticator D3 9D 20 7E 09 89 68 BD - 1A DF A3
B6 6E 25 8D 77
Sep 26 20:01:49.326: RADIUS:  Service-Type        [6]   6   Framed              [2]
Sep 26 20:01:49.326: RADIUS(000025EA): Received from id 1645/88
Sep 26
iacc02.crt#20:01:49.326: ISAKMP:(0):ISAKMP/tunnel: received callback from AAA
Sep 26 20:01:49.326: ISAKMP/tunnel: received tunnel atts
Sep 26 20:01:49.326: ISAKMP:Error - skey id.
```

注意：然而，当本地授权配置时，一切良好工作。

解决方案

报告的行为预计而不是bug。远程访问VPN有两独立的验证processess ：

1. 用户连接的通道的预共享密匙验证。

2. 验证个人用户的XAUTH。

在预共享密匙验证在阶段1之后，成功XAUTH是相位1.5并且发生。原因您不能发现用户提示输入密码是，因为阶段1未完成。在调试发送的用户名实际上是为阶段1预共享密匙验证。

本地授权与RADIUS授权

当本地authoriation配置时， VPN头端拾起关键值配置在组配置下为了完成阶段1。这允许相位1完成，因此路由器能继续到XAUTH ：

```
*Dec 26 12:42:13.926: ISAKMP:(0):ISAKMP/tunnel: setting up tunnel vpnclient
pw request
*Dec 26 12:42:13.926: AAA/AUTHOR (0x12): Pick method list 'login_local'
*Dec 26 12:42:13.926: ISAKMP:(0):ISAKMP/tunnel: Tunnel vpnclient PW Request
successfully sent to AAA
*Dec 26 12:42:13.926: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
*Dec 26 12:42:13.926: ISAKMP:(0):Old State = IKE_READY New State =
IKE_R_AM_AAA_AWAIT

*Dec 26 12:42:13.927: ISAKMP:(0):ISAKMP/tunnel: received callback from AAA
AAA/AUTHOR/IKE: Processing AV tunnel-password
AAA/AUTHOR/IKE: Processing AV default-domain
AAA/AUTHOR/IKE: Processing AV addr-pool
AAA/AUTHOR/IKE: Processing AV dns-servers
AAA/AUTHOR/IKE: Processing AV wins-servers
AAA/AUTHOR/IKE: Processing AV route-metric
AAA/AUTHOR/IKE: Processing AV max-users
AAA/AUTHOR/IKE: Processing AV max-logins
AAA/AUTHOR/IKE: Processing AV netmask
*Dec 26 12:42:13.927: ISAKMP/tunnel: received tunnel atts
*Dec 26 12:42:13.927: ISAKMP:(35002): constructed NAT-T vendor-02 ID
*Dec 26 12:42:13.927: ISAKMP:(35002):SA is doing pre-shared key authentication
plus XAUTH using id type ID_IPV4_ADDR
*Dec 26 12:42:13.927: ISAKMP (35002): ID payload
next-payload : 10
type : 1
address : 172.16.161.24
protocol : 0
port : 0
length : 12
*Dec 26 12:42:13.927: ISAKMP:(35002):Total payload length: 12
*Dec 26 12:42:13.927: ISAKMP:(35002): sending packet to X.X.X.X my_port 500
peer_port 65328 (R) AG_INIT_EXCH
*Dec 26 12:42:13.927: ISAKMP:(35002):Sending an IKE IPv4 Packet.
*Dec 26 12:42:13.927: ISAKMP:(35002):Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY
*Dec 26 12:42:13.927: ISAKMP:(35002):Old State = IKE_R_AM_AAA_AWAIT New State =
IKE_R_AM2

*Dec 26 12:42:14.017: ISAKMP (35002): received packet from X.X.X.X dport 4500 sport
59464 Mgmt-intf (R) AG_INIT_EXCH
*Dec 26 12:42:14.017: ISAKMP:(35002): processing HASH payload. message ID = 0
*Dec 26 12:42:14.017: ISAKMP:(35002): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 0x7F7796C1DDC0
*Dec 26 12:42:14.018: ISAKMP:received payload type 20
*Dec 26 12:42:14.018: ISAKMP (35002): His hash no match - this node outside NAT
*Dec 26 12:42:14.018: ISAKMP:received payload type 20
*Dec 26 12:42:14.018: ISAKMP (35002): His hash no match - this node outside NAT
*Dec 26 12:42:14.018: ISAKMP:(35002):SA authentication status:
authenticated
*Dec 26 12:42:14.018: ISAKMP:(35002):SA has been authenticated with X.X.X.X
*Dec 26 12:42:14.018: ISAKMP:(35002):Detected port,floating to port = 59464
```

```
*Dec 26 12:42:14.018: ISAKMP: Trying to find existing peer
X.X.X.X/X.X.X.X/59464/Outside
*Dec 26 12:42:14.018: ISAKMP:(35002):SA authentication status:
authenticated

*Dec 26 12:42:14.018: ISAKMP AAA: Profile vpnclient.cisco.com in use with AAA list
VPN_Client for peer X.X.X.X
*Dec 26 12:42:14.018: ISAKMP AAA: No peer record for address X.X.X.X, port 59464.
Create Accounting Record
*Dec 26 12:42:14.018: ISAKMP: Attempting to insert peer index node : 0x2
*Dec 26 12:42:14.018: ISAKMP AAA: Create Accounting Record 0x7F779645B5E0 for peer
X.X.X.X/59464 - peer-index 0x2
*Dec 26 12:42:14.018: ISAKMP AAA: NAS Port Id is already set to X.X.X.X
*Dec 26 12:42:14.018: ISAKMP AAA: crypto_ikmp_aaa_acct_rec_create: pki_sd 0

*Dec 26 12:42:14.018: ISAKMP:(35002):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
*Dec 26 12:42:14.018: ISAKMP:(35002):Old State = IKE_R_AM2 New State =
IKE_P1_COMPLETE

*Dec 26 12:42:14.018: ISAKMP:(35002):Need XAUTH
*Dec 26 12:42:14.018: ISAKMP: set new node 2793554424 to CONF_XAUTH
*Dec 26 12:42:14.018: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
*Dec 26 12:42:14.018: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
*Dec 26 12:42:14.018: ISAKMP:(35002): initiating peer config to X.X.X.X.
ID = 2793554424
*Dec 26 12:42:14.018: ISAKMP:(35002): sending packet to X.X.X.X my_port 4500
peer_port 59464 (R) CONF_XAUTH
*Dec 26 12:42:14.018: ISAKMP:(35002):Sending an IKE IPv4 Packet.
*Dec 26 12:42:14.018: ISAKMP:(35002):Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
*Dec 26 12:42:14.018: ISAKMP:(35002):Old State = IKE_P1_COMPLETE New State =
IKE_XAUTH_REQ_SENT

*Dec 26 12:42:21.572: ISAKMP (35002): received packet from X.X.X.X dport 4500
sport 59464 Mgmt-intf (R) CONF_XAUTH
*Dec 26 12:42:21.572: ISAKMP:(35002):processing transaction payload from
X.X.X.X. message ID = 2793554424
*Dec 26 12:42:21.572: ISAKMP: Config payload REPLY
*Dec 26 12:42:21.572: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
*Dec 26 12:42:21.572: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
*Dec 26 12:42:21.572: ISAKMP AAA: NAS Port Id is already set to X.X.X.X
*Dec 26 12:42:21.572: ISAKMP/Authen: unique id = 19
*Dec 26 12:42:21.572: ISAKMP:(35002):AAA Authen: setting up authen_request
*Dec 26 12:42:21.572: AAA/AUTHEN/LOGIN (00000013): Pick method list 'VPN_Client'
*Dec 26 12:42:21.572: ISAKMP:(35002):AAA Authen: Successfully sent authen
info to AAA

*Dec 26 12:42:21.572: ISAKMP:(35002):deleting node 2793554424 error FALSE
reason "Done with xauth request/reply exchange"
*Dec 26 12:42:21.572: ISAKMP:(35002):Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY
*Dec 26 12:42:21.572: ISAKMP:(35002):Old State = IKE_XAUTH_REQ_SENT New
State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT

*Dec 26 12:42:21.573: RADIUS/ENCODE(00000013):Orig. component type = VPN IPSEC
*Dec 26 12:42:21.573: RADIUS: AAA Unsupported Attr: interface [221]
13 32631
*Dec 26 12:42:21.573: RADIUS/ENCODE(00000013): dropping service type,
"radius-server attribute 6 on-for-login-auth" is off
*Dec 26 12:42:21.573: RADIUS(00000013): Config NAS IP: 0.0.0.0
*Dec 26 12:42:21.573: RADIUS(00000013): Config NAS IPv6: ::
*Dec 26 12:42:21.573: Getting session id for EXEC(00000013) : db=7F7792DEEAB8
*Dec 26 12:42:21.573: RADIUS/ENCODE(00000013): acct_session_id: 8
*Dec 26 12:42:21.573: RADIUS(00000013): sending
*Dec 26 12:42:21.573: RADIUS/ENCODE: Best Local IP-Address X.X.X.X for
```

```
Radius-Server X.X.X.X
*Dec 26 12:42:21.573: RADIUS(00000013): Sending a IPv4 Radius Packet
*Dec 26 12:42:21.573: RADIUS(00000013): Send Access-Request to 10.88.171.27:1645
id 1645/1,len 95
*Dec 26 12:42:21.573: RADIUS: authenticator B6 8C 79 D9 91 0C 79 50 - CB B0
2A 87 2A 61 03 E8
*Dec 26 12:42:21.573: RADIUS: User-Name [1] 10 "vpnclient-user"
*Dec 26 12:42:21.573: RADIUS: User-Password [2] 18 *
*Dec 26 12:42:21.573: RADIUS: Calling-Station-Id [31] 14 "X.X.X.X"
*Dec 26 12:42:21.573: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
*Dec 26 12:42:21.573: RADIUS: NAS-Port [5] 6 0
*Dec 26 12:42:21.573: RADIUS: NAS-Port-Id [87] 15 "X.X.X.X"
*Dec 26 12:42:21.573: RADIUS: NAS-IP-Address [4] 6 X.X.X.X
*Dec 26 12:42:21.573: RADIUS(00000013): Started 5 sec timeout
*Dec 26 12:42:21.671: RADIUS: Received from id 1645/1 X.X.X.X:1645, Access-Accept,
len 56
*Dec 26 12:42:21.671: RADIUS: authenticator E7 C1 B1 3D 04 59 48 22 - 4B 80 9D
1A 5E CA 0A A6
*Dec 26 12:42:21.671: RADIUS: User-Name [1] 10 "vpnclient-user"
*Dec 26 12:42:21.671: RADIUS: Class [25] 26
*Dec 26 12:42:21.671: RADIUS: 43 41 43 53 3A 41 43 53 2D 35 78 2F 31 37 33 32
[CACS:ACS-5x/1732]
*Dec 26 12:42:21.671: RADIUS: 37 32 35 30 33 2F 31 34 [ 72503/14]
*Dec 26 12:42:21.671: RADIUS(00000013): Received from id 1645/1
*Dec 26 12:42:21.672: ISAKMP:(35002):ISAKMP/author: Class attribute (len=24)
'CACS:ACS-5x/173272503/14'
*Dec 26 12:42:21.672: ISAKMP:(35002):AAA Authen: No group atts added
*Dec 26 12:42:21.672: ISAKMP: set new node 1771945814 to CONF_XAUTH
*Dec 26 12:42:21.672: ISAKMP:(35002): initiating peer config to X.X.X.X. ID =
1771945814
*Dec 26 12:42:21.672: ISAKMP:(35002): sending packet to X.X.X.X my_port 4500
peer_port 59464 (R) CONF_XAUTH
*Dec 26 12:42:21.672: ISAKMP:(35002):Sending an IKE IPv4 Packet.
*Dec 26 12:42:21.672: ISAKMP:(35002):Input = IKE_MESG_FROM_AAA,
IKE_AAA_CONT_LOGIN
*Dec 26 12:42:21.672: ISAKMP:(35002):Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT
New State = IKE_XAUTH_SET_SENT

*Dec 26 12:42:21.759: ISAKMP (35002): received packet from X.X.X.X dport 4500 sport
59464 Mgmt-intf (R) CONF_XAUTH
*Dec 26 12:42:21.759: ISAKMP:(35002):processing transaction payload from X.X.X.X.
message ID = 1771945814
*Dec 26 12:42:21.759: ISAKMP: Config payload ACK
*Dec 26 12:42:21.759: ISAKMP:(35002): (blank) XAUTH ACK Processed
*Dec 26 12:42:21.759: ISAKMP:(35002):deleting node 1771945814 error FALSE reason
"Transaction mode done"
*Dec 26 12:42:21.759: ISAKMP:(35002):Talking to a Unity Client
*Dec 26 12:42:21.759: ISAKMP:(35002):Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK
*Dec 26 12:42:21.759: ISAKMP:(35002):Old State = IKE_XAUTH_SET_SENT New State =
IKE_P1_COMPLETE

*Dec 26 12:42:21.759: ISAKMP:(35002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
*Dec 26 12:42:21.759: ISAKMP:(35002):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Dec 26 12:42:21.763: ISAKMP (35002): received packet from X.X.X.X dport 4500 sport
59464 Mgmt-intf (R) QM_IDLE
*Dec 26 12:42:21.763: ISAKMP: set new node 3504137478 to QM_IDLE
*Dec 26 12:42:21.763: ISAKMP:(35002):processing transaction payload from X.X.X.X.
message ID = 3504137478
*Dec 26 12:42:21.763: ISAKMP: Config payload REQUEST
*Dec 26 12:42:21.763: ISAKMP:(35002):checking request:
*Dec 26 12:42:21.763: ISAKMP: IP4_ADDRESS
*Dec 26 12:42:21.763: ISAKMP: IP4_NETMASK
```

```
*Dec 26 12:42:21.763: ISAKMP: IP4_DNS
*Dec 26 12:42:21.763: ISAKMP: IP4_NBNS
*Dec 26 12:42:21.763: ISAKMP: ADDRESS_EXPIRY
*Dec 26 12:42:21.763: ISAKMP: MODECFG_BANNER
*Dec 26 12:42:21.763: ISAKMP: MODECFG_SAVEPWD
*Dec 26 12:42:21.763: ISAKMP: DEFAULT_DOMAIN
*Dec 26 12:42:21.763: ISAKMP: SPLIT_INCLUDE
*Dec 26 12:42:21.763: ISAKMP: SPLIT_DNS
*Dec 26 12:42:21.763: ISAKMP: PFS
*Dec 26 12:42:21.763: ISAKMP: MODECFG_BROWSER_PROXY
*Dec 26 12:42:21.763: ISAKMP: BACKUP_SERVER
*Dec 26 12:42:21.763: ISAKMP: MODECFG_SMARTCARD_REMOVAL_DISCONNECT
*Dec 26 12:42:21.763: ISAKMP: APPLICATION_VERSION
*Dec 26 12:42:21.763: ISAKMP: Client Version is : Cisco Systems VPN Client
5.0.07.0440:WinNTp
*Dec 26 12:42:21.763: ISAKMP: FW_RECORD
*Dec 26 12:42:21.763: ISAKMP: MODECFG_HOSTNAME
*Dec 26 12:42:21.763: ISAKMP:(35002):ISAKMP/author: setting up the authorization
request for vpnclient
*Dec 26 12:42:21.763: AAA/AUTHOR (0x13): Pick method list 'login_local'
*Dec 26 12:42:21.763: ISAKMP/author: Author request for group vpnclientsuccessfully
sent to AAA
*Dec 26 12:42:21.763: ISAKMP:(35002):Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST
*Dec 26 12:42:21.763: ISAKMP:(35002):Old State = IKE_P1_COMPLETE New State =
IKE_CONFIG_AUTHOR_AAA_AWAIT

*Dec 26 12:42:21.764: ISAKMP:(0):ISAKMP/author: received callback from AAA
AAA/AUTHOR/IKE: Processing AV tunnel-password
AAA/AUTHOR/IKE: Processing AV default-domain
AAA/AUTHOR/IKE: Processing AV addr-pool
AAA/AUTHOR/IKE: Processing AV dns-servers
AAA/AUTHOR/IKE: Processing AV wins-servers
*Dec 26 12:42:21.764:
AAA/AUTHOR/IKE: no WINS addresses
AAA/AUTHOR/IKE: Processing AV route-metric
AAA/AUTHOR/IKE: Processing AV max-users
AAA/AUTHOR/IKE: Processing AV max-logins
AAA/AUTHOR/IKE: Processing AV netmask
*Dec 26 12:42:21.764: ISAKMP:(35002):ISAKMP/author: No Class attributes
*Dec 26 12:42:21.764: ISAKMP:(35002):attributes sent in message:
*Dec 26 12:42:21.764: Address: 0.2.0.0
*Dec 26 12:42:21.766: ISAKMP:(35002):allocating address X.X.X.X
*Dec 26 12:42:21.766: ISAKMP: Sending private address: X.X.X.X
*Dec 26 12:42:21.766: ISAKMP: Sending subnet mask: 255.255.255.0
*Dec 26 12:42:21.766: ISAKMP: Sending IP4_DNS server address: X.X.X.X
*Dec 26 12:42:21.766: ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the
address: 86392
*Dec 26 12:42:21.766: ISAKMP: Sending save password reply value 0
*Dec 26 12:42:21.766: ISAKMP: Sending DEFAULT_DOMAIN default domain name:
vpnclient.cisco.com
*Dec 26 12:42:21.766: ISAKMP: Sending smartcard_removal_disconnect reply
value 0
*Dec 26 12:42:21.766: ISAKMP: Sending APPLICATION_VERSION string: Cisco IOS Software,
IOS-XE Software (X86_64_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.2(4)S,
RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Mon 23-Jul-12 20:02 by mcpre
*Dec 26 12:42:21.766: ISAKMP (35002): Unknown Attr: MODECFG_HOSTNAME (0x700A)
*Dec 26 12:42:21.766: ISAKMP:(35002): responding to peer config from 72.163.84.76.
ID = 3504137478
*Dec 26 12:42:21.766: ISAKMP: Marking node 3504137478 for late deletion
*Dec 26 12:42:21.766: ISAKMP:(35002): sending packet to X.X.X.X my_port 4500 peer_port
59464 (R) CONF_ADDR
```

```
*Dec 26 12:42:21.766: ISAKMP:(35002):Sending an IKE IPv4 Packet.
*Dec 26 12:42:21.766: ISAKMP:(35002):Talking to a Unity Client
*Dec 26 12:42:21.766: ISAKMP:(35002):Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR
*Dec 26 12:42:21.766: ISAKMP:(35002):Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New
State = IKE_P1_COMPLETE

*Dec 26 12:42:21.766: ISAKMP:FSM error - Message from AAA grp/user.

*Dec 26 12:42:21.766: ISAKMP:(35002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
*Dec 26 12:42:21.766: ISAKMP:(35002):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
```

当路由器配置授权RADIUS服务器时，不工作，因为为了获得**密钥**(预共享验证)，必须执行访问请求查询到RADIUS服务器。然而，访问请求查询要求将发送的**用户名**对RADIUSA，并且，因为XAUTH没有执行，不能使用客户端用户**用户名**。在这种情况下，它使用**组名**作为**用户名**。然而，因为RADIUS服务器未由该ID设置验证任何用户，它拒绝请求。因此，阶段1从未完成，并且从未提示用户输入凭证。

工作配置

路由器配置

这是路由器的配置。

```
*Dec 26 12:42:13.926: ISAKMP:(0):ISAKMP/tunnel: setting up tunnel vpnclient
pw request
*Dec 26 12:42:13.926: AAA/AUTHOR (0x12): Pick method list 'login_local'
*Dec 26 12:42:13.926: ISAKMP:(0):ISAKMP/tunnel: Tunnel vpnclient PW Request
successfully sent to AAA
*Dec 26 12:42:13.926: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
*Dec 26 12:42:13.926: ISAKMP:(0):Old State = IKE_READY New State =
IKE_R_AM_AAA_AWAIT

*Dec 26 12:42:13.927: ISAKMP:(0):ISAKMP/tunnel: received callback from AAA
AAA/AUTHOR/IKE: Processing AV tunnel-password
AAA/AUTHOR/IKE: Processing AV default-domain
AAA/AUTHOR/IKE: Processing AV addr-pool
AAA/AUTHOR/IKE: Processing AV dns-servers
AAA/AUTHOR/IKE: Processing AV wins-servers
AAA/AUTHOR/IKE: Processing AV route-metric
AAA/AUTHOR/IKE: Processing AV max-users
AAA/AUTHOR/IKE: Processing AV max-logins
AAA/AUTHOR/IKE: Processing AV netmask
*Dec 26 12:42:13.927: ISAKMP/tunnel: received tunnel atts
*Dec 26 12:42:13.927: ISAKMP:(35002): constructed NAT-T vendor-02 ID
*Dec 26 12:42:13.927: ISAKMP:(35002):SA is doing pre-shared key authentication
plus XAUTH using id type ID_IPV4_ADDR
*Dec 26 12:42:13.927: ISAKMP (35002): ID payload
next-payload : 10
type : 1
address : 172.16.161.24
protocol : 0
port : 0
length : 12
*Dec 26 12:42:13.927: ISAKMP:(35002):Total payload length: 12
*Dec 26 12:42:13.927: ISAKMP:(35002): sending packet to X.X.X.X my_port 500
peer_port 65328 (R) AG_INIT_EXCH
*Dec 26 12:42:13.927: ISAKMP:(35002):Sending an IKE IPv4 Packet.
*Dec 26 12:42:13.927: ISAKMP:(35002):Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY
```

```
*Dec 26 12:42:13.927: ISAKMP:(35002):Old State = IKE_R_AM_AAA_AWAIT New State =
IKE_R_AM2

*Dec 26 12:42:14.017: ISAKMP (35002): received packet from X.X.X.X dport 4500 sport
59464 Mgmt-intf (R) AG_INIT_EXCH
*Dec 26 12:42:14.017: ISAKMP:(35002): processing HASH payload. message ID = 0
*Dec 26 12:42:14.017: ISAKMP:(35002): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 0x7F7796C1DDC0
*Dec 26 12:42:14.018: ISAKMP:received payload type 20
*Dec 26 12:42:14.018: ISAKMP (35002): His hash no match - this node outside NAT
*Dec 26 12:42:14.018: ISAKMP:received payload type 20
*Dec 26 12:42:14.018: ISAKMP (35002): His hash no match - this node outside NAT
*Dec 26 12:42:14.018: ISAKMP:(35002):SA authentication status:
authenticated
*Dec 26 12:42:14.018: ISAKMP:(35002):SA has been authenticated with X.X.X.X
*Dec 26 12:42:14.018: ISAKMP:(35002):Detected port,floating to port = 59464
*Dec 26 12:42:14.018: ISAKMP: Trying to find existing peer
X.X.X.X/X.X.X.X/59464/Outside
*Dec 26 12:42:14.018: ISAKMP:(35002):SA authentication status:
authenticated

*Dec 26 12:42:14.018: ISAKMP AAA: Profile vpnclient.cisco.com in use with AAA list
VPN_Client for peer X.X.X.X
*Dec 26 12:42:14.018: ISAKMP AAA: No peer record for address X.X.X.X, port 59464.
Create Accounting Record
*Dec 26 12:42:14.018: ISAKMP: Attempting to insert peer index node : 0x2
*Dec 26 12:42:14.018: ISAKMP AAA: Create Accounting Record 0x7F779645B5E0 for peer
X.X.X.X/59464 - peer-index 0x2
*Dec 26 12:42:14.018: ISAKMP AAA: NAS Port Id is already set to X.X.X.X
*Dec 26 12:42:14.018: ISAKMP AAA: crypto_ikmp_aaa_acct_rec_create: pki_sd 0

*Dec 26 12:42:14.018: ISAKMP:(35002):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
*Dec 26 12:42:14.018: ISAKMP:(35002):Old State = IKE_R_AM2 New State =
IKE_P1_COMPLETE

*Dec 26 12:42:14.018: ISAKMP:(35002):Need XAUTH
*Dec 26 12:42:14.018: ISAKMP: set new node 2793554424 to CONF_XAUTH
*Dec 26 12:42:14.018: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
*Dec 26 12:42:14.018: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
*Dec 26 12:42:14.018: ISAKMP:(35002): initiating peer config to X.X.X.X.
ID = 2793554424
*Dec 26 12:42:14.018: ISAKMP:(35002): sending packet to X.X.X.X my_port 4500
peer_port 59464 (R) CONF_XAUTH
*Dec 26 12:42:14.018: ISAKMP:(35002):Sending an IKE IPv4 Packet.
*Dec 26 12:42:14.018: ISAKMP:(35002):Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
*Dec 26 12:42:14.018: ISAKMP:(35002):Old State = IKE_P1_COMPLETE New State =
IKE_XAUTH_REQ_SENT

*Dec 26 12:42:21.572: ISAKMP (35002): received packet from X.X.X.X dport 4500
sport 59464 Mgmt-intf (R) CONF_XAUTH
*Dec 26 12:42:21.572: ISAKMP:(35002):processing transaction payload from
X.X.X.X. message ID = 2793554424
*Dec 26 12:42:21.572: ISAKMP: Config payload REPLY
*Dec 26 12:42:21.572: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
*Dec 26 12:42:21.572: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
*Dec 26 12:42:21.572: ISAKMP AAA: NAS Port Id is already set to X.X.X.X
*Dec 26 12:42:21.572: ISAKMP/Authen: unique id = 19
*Dec 26 12:42:21.572: ISAKMP:(35002):AAA Authen: setting up authen_request
*Dec 26 12:42:21.572: AAA/AUTHEN/LOGIN (00000013): Pick method list 'VPN_Client'
*Dec 26 12:42:21.572: ISAKMP:(35002):AAA Authen: Successfully sent authen
info to AAA

*Dec 26 12:42:21.572: ISAKMP:(35002):deleting node 2793554424 error FALSE
```

```
reason "Done with xauth request/reply exchange"
*Dec 26 12:42:21.572: ISAKMP:(35002):Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY
*Dec 26 12:42:21.572: ISAKMP:(35002):Old State = IKE_XAUTH_REQ_SENT New
State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT

*Dec 26 12:42:21.573: RADIUS/ENCODE(00000013):Orig. component type = VPN IPSEC
*Dec 26 12:42:21.573: RADIUS: AAA Unsupported Attr: interface [221]
13 32631
*Dec 26 12:42:21.573: RADIUS/ENCODE(00000013): dropping service type,
"radius-server attribute 6 on-for-login-auth" is off
*Dec 26 12:42:21.573: RADIUS(00000013): Config NAS IP: 0.0.0.0
*Dec 26 12:42:21.573: RADIUS(00000013): Config NAS IPv6: ::
*Dec 26 12:42:21.573: Getting session id for EXEC(00000013) : db=7F7792DEEAB8
*Dec 26 12:42:21.573: RADIUS/ENCODE(00000013): acct_session_id: 8
*Dec 26 12:42:21.573: RADIUS(00000013): sending
*Dec 26 12:42:21.573: RADIUS/ENCODE: Best Local IP-Address X.X.X.X for
Radius-Server X.X.X.X
*Dec 26 12:42:21.573: RADIUS(00000013): Sending a IPv4 Radius Packet
*Dec 26 12:42:21.573: RADIUS(00000013): Send Access-Request to 10.88.171.27:1645
id 1645/1,len 95
*Dec 26 12:42:21.573: RADIUS: authenticator B6 8C 79 D9 91 0C 79 50 - CB B0
2A 87 2A 61 03 E8
*Dec 26 12:42:21.573: RADIUS: User-Name [1] 10 "vpnclient-user"
*Dec 26 12:42:21.573: RADIUS: User-Password [2] 18 *
*Dec 26 12:42:21.573: RADIUS: Calling-Station-Id [31] 14 "X.X.X.X"
*Dec 26 12:42:21.573: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
*Dec 26 12:42:21.573: RADIUS: NAS-Port [5] 6 0
*Dec 26 12:42:21.573: RADIUS: NAS-Port-Id [87] 15 "X.X.X.X"
*Dec 26 12:42:21.573: RADIUS: NAS-IP-Address [4] 6 X.X.X.X
*Dec 26 12:42:21.573: RADIUS(00000013): Started 5 sec timeout
*Dec 26 12:42:21.671: RADIUS: Received from id 1645/1 X.X.X.X:1645, Access-Accept,
len 56
*Dec 26 12:42:21.671: RADIUS: authenticator E7 C1 B1 3D 04 59 48 22 - 4B 80 9D
1A 5E CA 0A A6
*Dec 26 12:42:21.671: RADIUS: User-Name [1] 10 "vpnclient-user"
*Dec 26 12:42:21.671: RADIUS: Class [25] 26
*Dec 26 12:42:21.671: RADIUS: 43 41 43 53 3A 41 43 53 2D 35 78 2F 31 37 33 32
[CACS:ACS-5x/1732]
*Dec 26 12:42:21.671: RADIUS: 37 32 35 30 33 2F 31 34 [ 72503/14]
*Dec 26 12:42:21.671: RADIUS(00000013): Received from id 1645/1
*Dec 26 12:42:21.672: ISAKMP:(35002):ISAKMP/author: Class attribute (len=24)
'CACS:ACS-5x/173272503/14'
*Dec 26 12:42:21.672: ISAKMP:(35002):AAA Authen: No group atts added
*Dec 26 12:42:21.672: ISAKMP: set new node 1771945814 to CONF_XAUTH
*Dec 26 12:42:21.672: ISAKMP:(35002): initiating peer config to X.X.X.X. ID =
1771945814
*Dec 26 12:42:21.672: ISAKMP:(35002): sending packet to X.X.X.X my_port 4500
peer_port 59464 (R) CONF_XAUTH
*Dec 26 12:42:21.672: ISAKMP:(35002):Sending an IKE IPv4 Packet.
*Dec 26 12:42:21.672: ISAKMP:(35002):Input = IKE_MESG_FROM_AAA,
IKE_AAA_CONT_LOGIN
*Dec 26 12:42:21.672: ISAKMP:(35002):Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT
New State = IKE_XAUTH_SET_SENT

*Dec 26 12:42:21.759: ISAKMP (35002): received packet from X.X.X.X dport 4500 sport
59464 Mgmt-intf (R) CONF_XAUTH
*Dec 26 12:42:21.759: ISAKMP:(35002):processing transaction payload from X.X.X.X.
message ID = 1771945814
*Dec 26 12:42:21.759: ISAKMP: Config payload ACK
*Dec 26 12:42:21.759: ISAKMP:(35002): (blank) XAUTH ACK Processed
*Dec 26 12:42:21.759: ISAKMP:(35002):deleting node 1771945814 error FALSE reason
"Transaction mode done"
*Dec 26 12:42:21.759: ISAKMP:(35002):Talking to a Unity Client
*Dec 26 12:42:21.759: ISAKMP:(35002):Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK
```

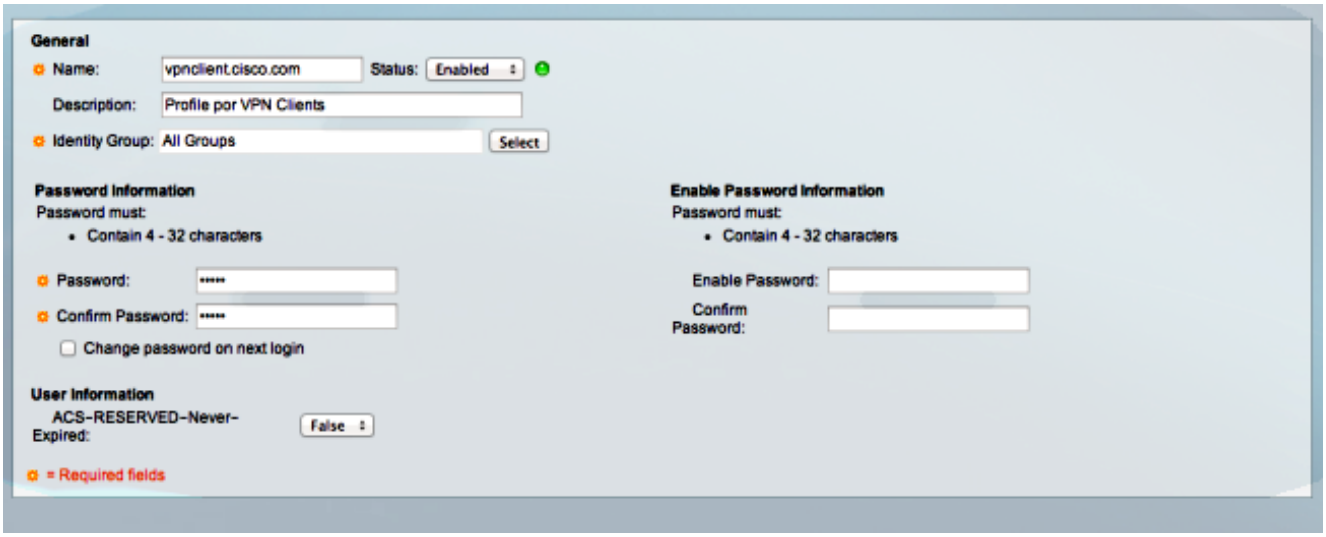
```
*Dec 26 12:42:21.759: ISAKMP:(35002):Old State = IKE_XAUTH_SET_SENT New State =
IKE_P1_COMPLETE

*Dec 26 12:42:21.759: ISAKMP:(35002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
*Dec 26 12:42:21.759: ISAKMP:(35002):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Dec 26 12:42:21.763: ISAKMP (35002): received packet from X.X.X.X dport 4500 sport
59464 Mgmt-intf (R) QM_IDLE
*Dec 26 12:42:21.763: ISAKMP: set new node 3504137478 to QM_IDLE
*Dec 26 12:42:21.763: ISAKMP:(35002):processing transaction payload from X.X.X.X.
message ID = 3504137478
*Dec 26 12:42:21.763: ISAKMP: Config payload REQUEST
*Dec 26 12:42:21.763: ISAKMP:(35002):checking request:
*Dec 26 12:42:21.763: ISAKMP: IP4_ADDRESS
*Dec 26 12:42:21.763: ISAKMP: IP4_NETMASK
*Dec 26 12:42:21.763: ISAKMP: IP4_DNS
*Dec 26 12:42:21.763: ISAKMP: IP4_NBNS
*Dec 26 12:42:21.763: ISAKMP: ADDRESS_EXPIRY
*Dec 26 12:42:21.763: ISAKMP: MODECFG_BANNER
*Dec 26 12:42:21.763: ISAKMP: MODECFG_SAVEPWD
*Dec 26 12:42:21.763: ISAKMP: DEFAULT_DOMAIN
*Dec 26 12:42:21.763: ISAKMP: SPLIT_INCLUDE
*Dec 26 12:42:21.763: ISAKMP: SPLIT_DNS
*Dec 26 12:42:21.763: ISAKMP: PFS
*Dec 26 12:42:21.763: ISAKMP: MODECFG_BROWSER_PROXY
*Dec 26 12:42:21.763: ISAKMP: BACKUP_SERVER
*Dec 26 12:42:21.763: ISAKMP: MODECFG_SMARTCARD_REMOVAL_DISCONNECT
*Dec 26 12:42:21.763: ISAKMP: APPLICATION_VERSION
*Dec 26 12:42:21.763: ISAKMP: Client Version is : Cisco Systems VPN Client
5.0.07.0440:WinNTp
*Dec 26 12:42:21.763: ISAKMP: FW_RECORD
*Dec 26 12:42:21.763: ISAKMP: MODECFG_HOSTNAME
*Dec 26 12:42:21.763: ISAKMP:(35002):ISAKMP/author: setting up the authorization
request for vpnclient
*Dec 26 12:42:21.763: AAA/AUTHOR (0x13): Pick method list 'login_local'
*Dec 26 12:42:21.763: ISAKMP/author: Author request for group vpnclientsuccessfully
sent to AAA
*Dec 26 12:42:21.763: ISAKMP:(35002):Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST
*Dec 26 12:42:21.763: ISAKMP:(35002):Old State = IKE_P1_COMPLETE New State =
IKE_CONFIG_AUTHOR_AAA_AWAIT

*Dec 26 12:42:21.764: ISAKMP:(0):ISAKMP/author: received callback from AAA
AAA/AUTHOR/IKE: Processing AV tunnel-password
AAA/AUTHOR/IKE: Processing AV default-domain
AAA/AUTHOR/IKE: Processing AV addr-pool
AAA/AUTHOR/IKE: Processing AV dns-servers
AAA/AUTHOR/IKE: Processing AV wins-servers
*Dec 26 12:42:21.764:
AAA/AUTHOR/IKE: no WINS addresses
AAA/AUTHOR/IKE: Processing AV route-metric
AAA/AUTHOR/IKE: Processing AV max-users
AAA/AUTHOR/IKE: Processing AV max-logins
AAA/AUTHOR/IKE: Processing AV netmask
*Dec 26 12:42:21.764: ISAKMP:(35002):ISAKMP/author: No Class attributes
*Dec 26 12:42:21.764: ISAKMP:(35002):attributes sent in message:
*Dec 26 12:42:21.764: Address: 0.2.0.0
*Dec 26 12:42:21.766: ISAKMP:(35002):allocating address X.X.X.X
*Dec 26 12:42:21.766: ISAKMP: Sending private address: X.X.X.X
*Dec 26 12:42:21.766: ISAKMP: Sending subnet mask: 255.255.255.0
*Dec 26 12:42:21.766: ISAKMP: Sending IP4_DNS server address: X.X.X.X
*Dec 26 12:42:21.766: ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the
address: 86392
*Dec 26 12:42:21.766: ISAKMP: Sending save password reply value 0
```

```
*Dec 26 12:42:21.766: ISAKMP: Sending DEFAULT_DOMAIN default domain name:
vpnclient.cisco.com
*Dec 26 12:42:21.766: ISAKMP: Sending smartcard_removal_disconnect reply
value 0
*Dec 26 12:42:21.766: ISAKMP: Sending APPLICATION_VERSION string: Cisco IOS Software,
IOS-XE Software (X86_64_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.2(4)S,
RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Mon 23-Jul-12 20:02 by mcpre
*Dec 26 12:42:21.766: ISAKMP (35002): Unknown Attr: MODECFG_HOSTNAME (0x700A)
*Dec 26 12:42:21.766: ISAKMP:(35002): responding to peer config from 72.163.84.76.
ID = 3504137478
*Dec 26 12:42:21.766: ISAKMP: Marking node 3504137478 for late deletion
*Dec 26 12:42:21.766: ISAKMP:(35002): sending packet to X.X.X.X my_port 4500 peer_port
59464 (R) CONF_ADDR
*Dec 26 12:42:21.766: ISAKMP:(35002):Sending an IKE IPv4 Packet.
*Dec 26 12:42:21.766: ISAKMP:(35002):Talking to a Unity Client
*Dec 26 12:42:21.766: ISAKMP:(35002):Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR
*Dec 26 12:42:21.766: ISAKMP:(35002):Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New
State = IKE_P1_COMPLETE

*Dec 26 12:42:21.766: ISAKMP:FSM error - Message from AAA grp/user.

*Dec 26 12:42:21.766: ISAKMP:(35002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
*Dec 26 12:42:21.766: ISAKMP:(35002):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
```

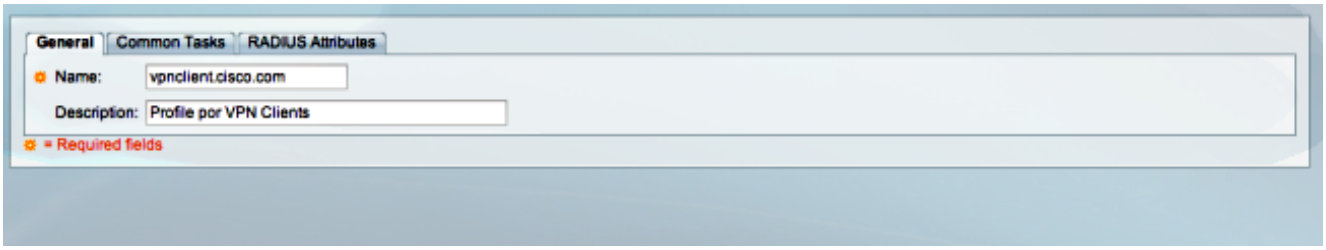
RADIUS 服务器配置

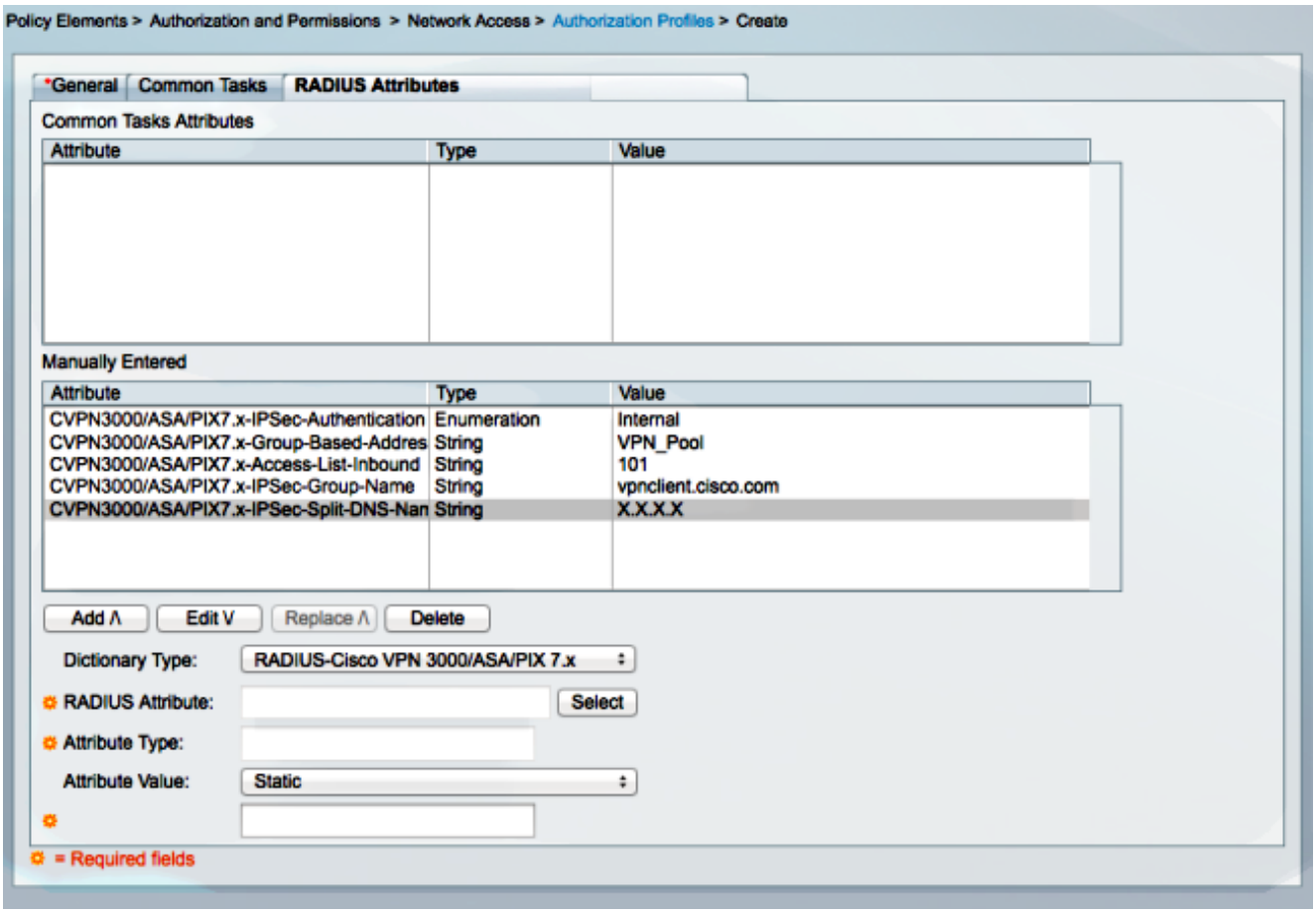
完成这些步骤为了配置RADIUS服务器。

1. 配置**组名**用户：

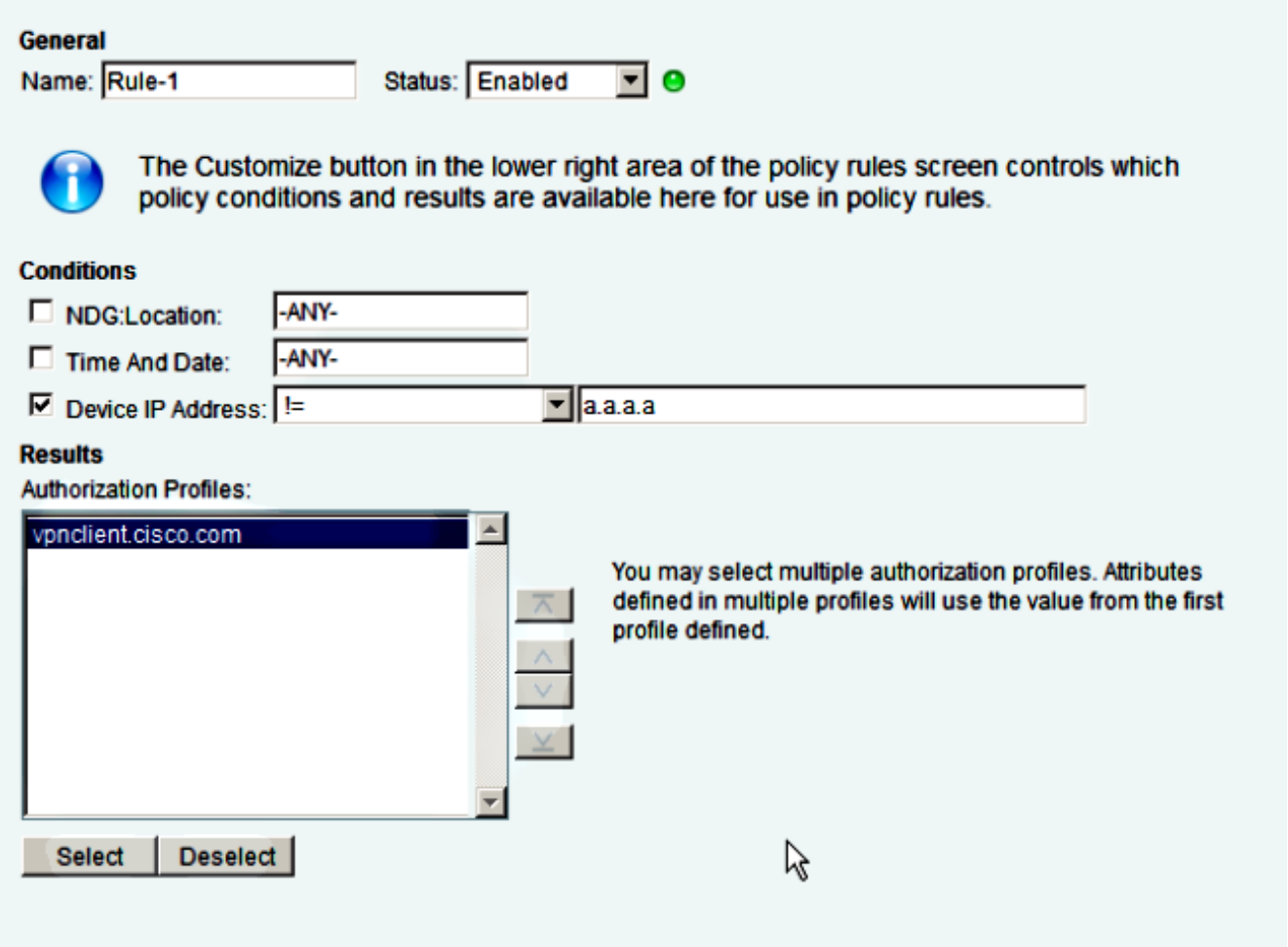


2. 配置授权配置文件为了给所有属性值(AV)对：





3. 配置访问策略为了允许描出的连接和使用：



故障排除

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

> **注意**：使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

这些调试在VPN头端启用：

互联网安全协会和密钥管理协议(ISAKMP)调试

```
debug crypto isakmp
```

AAA调试

```
debug aaa authentication
debug aaa authorization
debug aaa accounting
debug radius authentication
```