

# La VPN de acceso remoto no funciona cuando se configura la autenticación y autorización RADIUS

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema](#)

[Solución](#)

[Autorización local frente a autorización RADIUS](#)

[Configuración en funcionamiento](#)

[Configuración del router](#)

[Configuración del servidor de RADIUS](#)

[Troubleshoot](#)

[Depuraciones de protocolo de administración de claves \(ISAKMP\) y Asociación de seguridad de Internet](#)

[debugs AAA](#)

## Introducción

Este documento describe el comportamiento para la autenticación extendida (XAUTH) para los usuarios de VPN cuando se configuran la autenticación y la autorización.

## Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Autenticación, autorización y administración (AAA)
- VPN de acceso remoto

## Componentes Utilizados

La información de este documento se basa en un router de servicios de agregación (ASR) de

Cisco serie 1000 que ejecuta el software Cisco IOS® XE.

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.

## Problema

Los usuarios de VPN se configuran para ser autenticados y autorizados por un servidor RADIUS. La configuración en el ASR se muestra aquí:

```
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
```

Sin embargo, cuando intente autenticar, nunca se le solicitarán las credenciales. En el cliente, este mensaje de error se ve en los mensajes de registro:

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

Los debugs en el ASR indican que el nombre del grupo VPN se utiliza como **User-Name** para el intento de autorización.

```
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.
```

**Nota:** Sin embargo, todo funciona bien cuando se configura la autorización local.

## Solución

Se espera el comportamiento informado y no un error. La VPN de acceso remoto tiene dos procesos de autenticación independientes:

1. Autenticación de clave previamente compartida para el túnel al que se conecta el usuario.
2. XAUTH que autentica al usuario individual.

XAUTH es la Fase 1.5 y se produce sólo después de que la autenticación de clave previamente compartida tenga éxito en la Fase 1. La razón por la que no puede ver una solicitud de contraseña de usuario es porque la Fase 1 todavía no ha finalizado. El nombre de usuario que se envía en las depuraciones es en realidad para la autenticación de clave precompartida Fase 1.

## Autorización local frente a autorización RADIUS

Cuando se configura la autorización local, el centro distribuidor VPN recoge el valor de clave configurado bajo la configuración de grupo para completar la Fase 1. Esto permite que se complete la fase 1, para que el router pueda continuar con 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\_MSG\_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\_MSG\_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\_MSG\_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:
vpncient.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

```

Cuando el router se configura para autorizar con el servidor RADIUS, no funciona porque para obtener la **clave** (para la autenticación previamente compartida), debe realizar una consulta de solicitud de acceso al servidor RADIUS. Sin embargo, la consulta de solicitud de acceso requiere un **nombre de usuario** para ser enviado a RADIUS y dado que XAUTH aún no se ha hecho, no puede utilizar el **nombre de usuario** del cliente. En esta situación, utiliza el **nombre de grupo** como **nombre de usuario** en su lugar. Sin embargo, dado que el servidor RADIUS no se ha configurado para verificar ningún usuario por ese ID, rechaza la solicitud. Debido a esto, la Fase 1 nunca se completa y al usuario nunca se le solicita las credenciales.

## Configuración en funcionamiento

### Configuración del router

Esta es la configuración para el router.

```

aaa group server radius Radius-Server
server-private X.X.X.X auth-port 1812 acct-port 1813 key 7 <removed>

aaa authentication login VPN_Client group Radius-Server
aaa authorization network VPN_Client Radius-Server
aaa accounting network VPN_Client start-stop group Radius-Server

```

```
crypto isakmp policy 10
encr 3des
authentication pre-share
group 2
```

```
crypto isakmp client configuration group vpnclient
key <removed>
dns x.x.x.x
wins x.x.x.x
domain cisco.com
pool VPN_Pool
acl 101
group-lock
```

```
crypto isakmp profile vpnclient.cisco.com
match identity group vpnclient
client authentication list VPN_Client
isakmp authorization list VPN_Client
client configuration address respond
accounting VPN_Client
```

```
crypto ipsec transform-set TRANS-DES esp-des esp-md5-hmac
mode tunnel
```

```
crypto dynamic-map DYN-MAP 10
set transform-set TRANS-DES
set isakmp-profile vpnclient.cisco.com
reverse-route
```

```
crypto map VPN local-address TenGigabitEthernet 0/0/0
crypto map VPN 10 ipsec-isakmp dynamic DYN-MAP
```

```
interface TenGigabitEthernet0/0/0
ip address X.X.X.X 255.255.255.0
crypto map VPN
```

## Configuración del servidor de RADIUS

Complete estos pasos para configurar el servidor RADIUS.

1. Configure el usuario **Groupname**:



**General**

Name:  Status:

Description:

Identity Group:

**Password Information**

Password must:

- Contain 4 - 32 characters

Change password on next login

**Enable Password Information**

**User Information**

ACS-RESERVED-Never-Expired:

= Required fields

2. Configure un perfil de autorización para asignar todos los pares de valor de atributo (AV):

**General** | Common Tasks | **RADIUS Attributes**

Name:

Description:

= Required fields

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Create

**\*General** | Common Tasks | **RADIUS Attributes**

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value
CVPN3000/ASA/PIX7.x-IPSec-Authentication	Enumeration	Internal
CVPN3000/ASA/PIX7.x-Group-Based-Address	String	VPN_Pool
CVPN3000/ASA/PIX7.x-Access-List-Inbound	String	101
CVPN3000/ASA/PIX7.x-IPSec-Group-Name	String	vpncient.cisco.com
CVPN3000/ASA/PIX7.x-IPSec-Split-DNS-Nan	String	X.X.X.X

Dictionary Type:

RADIUS Attribute:

Attribute Type:

Attribute Value:

= Required fields

3. Configure una política de acceso para permitir la conexión y utilizar ese perfil:

**General**  
 Name:  Status:

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

**Conditions**

NDG:Location:

Time And Date:

Device IP Address:

**Results**  
 Authorization Profiles:

vpncient.cisco.com

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

## Troubleshoot

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver un análisis de información de salida del comando show.

**Nota:** Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

Estas depuraciones están habilitadas en la cabecera VPN:

## Depuraciones de protocolo de administración de claves (ISAKMP) y Asociación de seguridad de Internet

```
debug crypto isakmp
```

### debugs AAA

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