ASA 8.0:為WebVPN使用者配置RADIUS身份驗證

目錄

簡介

本文檔演示如何配置思科自適應安全裝置(ASA)以使用遠端身份驗證撥入使用者服務(RADIUS)伺服器進行WebVPN使用者身份驗證。在此範例中，RADIUS伺服器是Cisco存取控制伺服器(ACS)版本4.1此組態是透過執行軟體版本8.0(2)的ASA上的調適型安全裝置管理員(ASDM)6.0(2)來執行。

注意：在此示例中，為WebVPN使用者配置了RADIUS身份驗證，但此配置也可用於其他型別的遠端訪問VPN。只需將AAA伺服器組分配到所需的連線配置檔案（隧道組），如下所示。

必要條件

- 需要基本WebVPN配置。
- Cisco ACS必須配置使用者以進行使用者身份驗證。有關詳細資訊，請參閱使用者管理的新增基本使用者帳戶部分。

配置ACS伺服器

本節提供在ACS和ASA上配置RADIUS身份驗證的資訊。

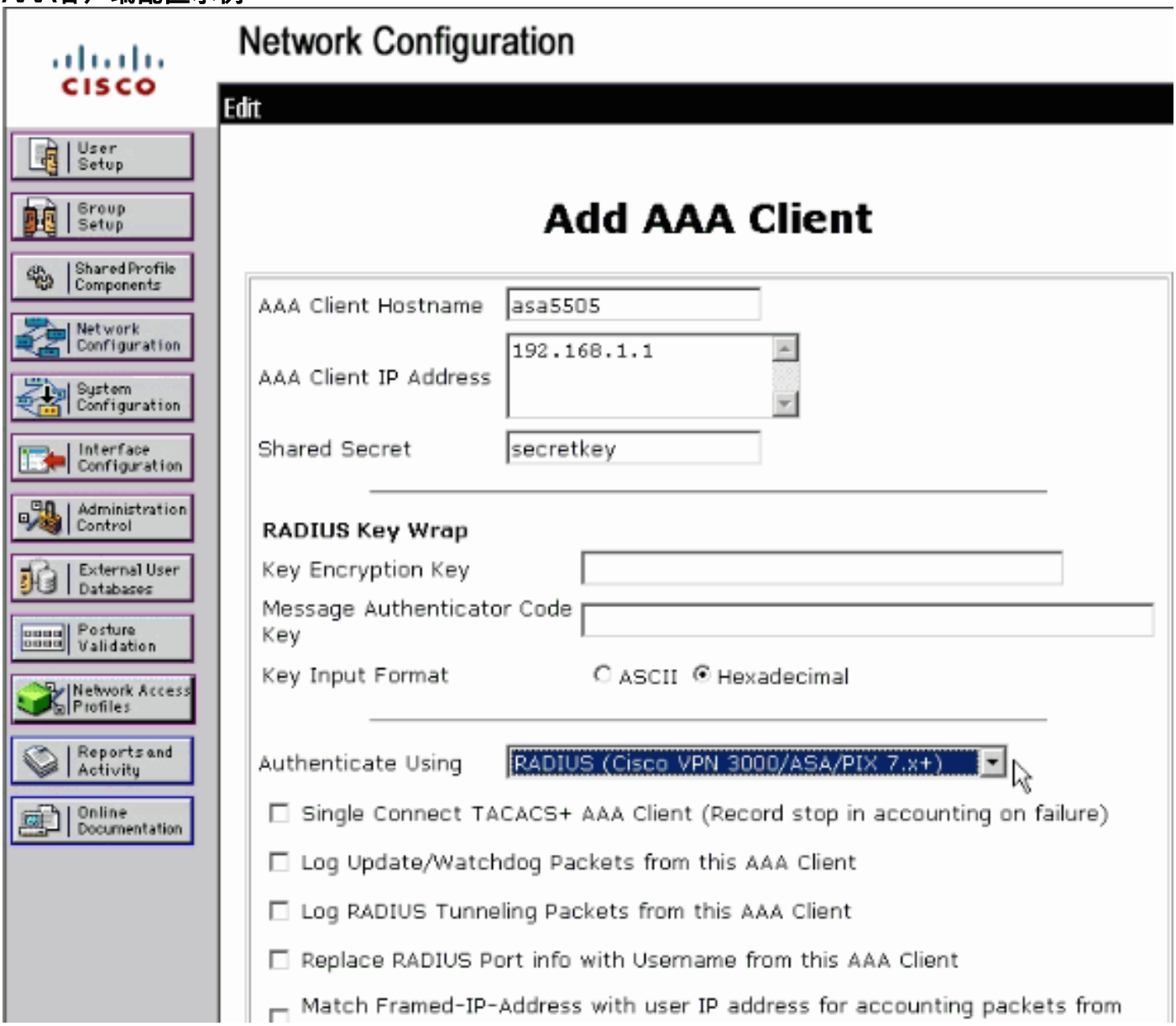
完成以下步驟，配置ACS伺服器與ASA通訊。

1. 從ACS螢幕的左側選單中選擇**Network Configuration**。
2. 在**AAA Clients**下選擇**Add Entry**。
3. 提供客戶端資訊：**AAA客戶端主**機名稱 — 您選擇的名稱**AAA Client IP Address** — 安全裝置與

ACS聯絡的地址**共用密碼** — 在ACS和安全裝置上配置的金鑰

4. 在「**Authenticate Using**」下拉選單中選擇**RADIUS(Cisco VPN 3000/ASA/PIX 7.x+)**。
5. 按一下「**Submit+Apply**」。

AAA客戶端配置示例

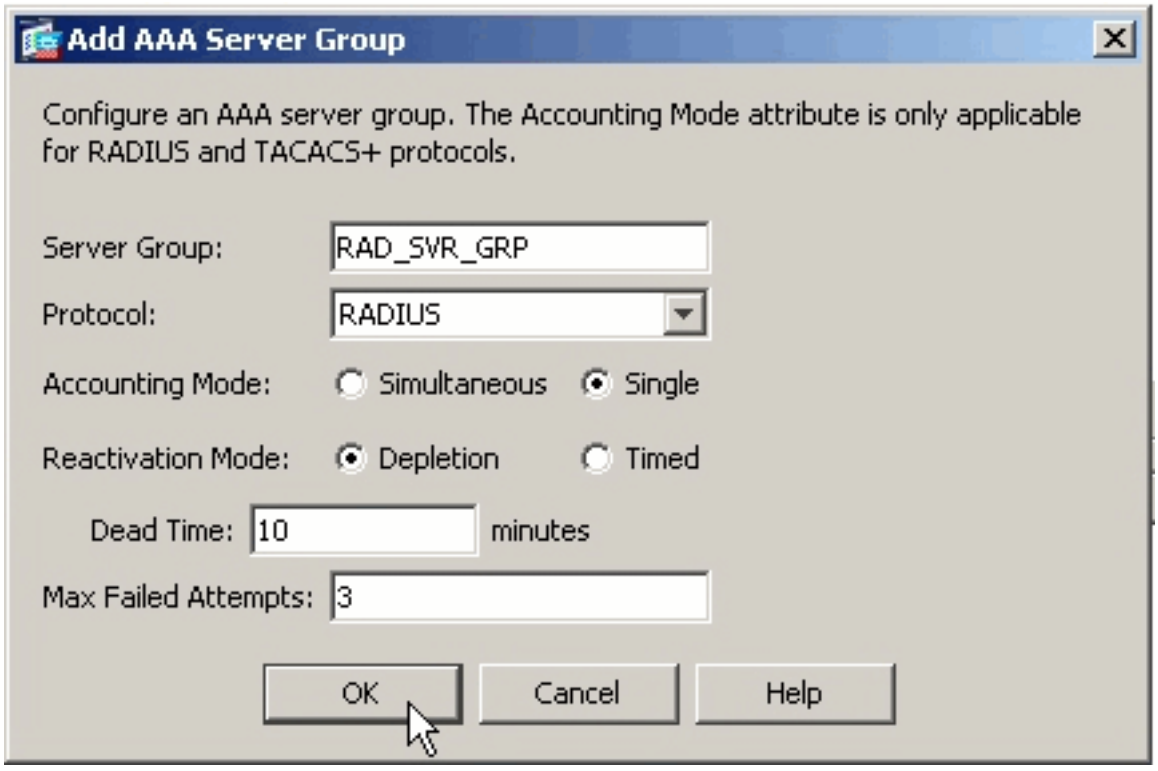


配置安全裝置

ASDM

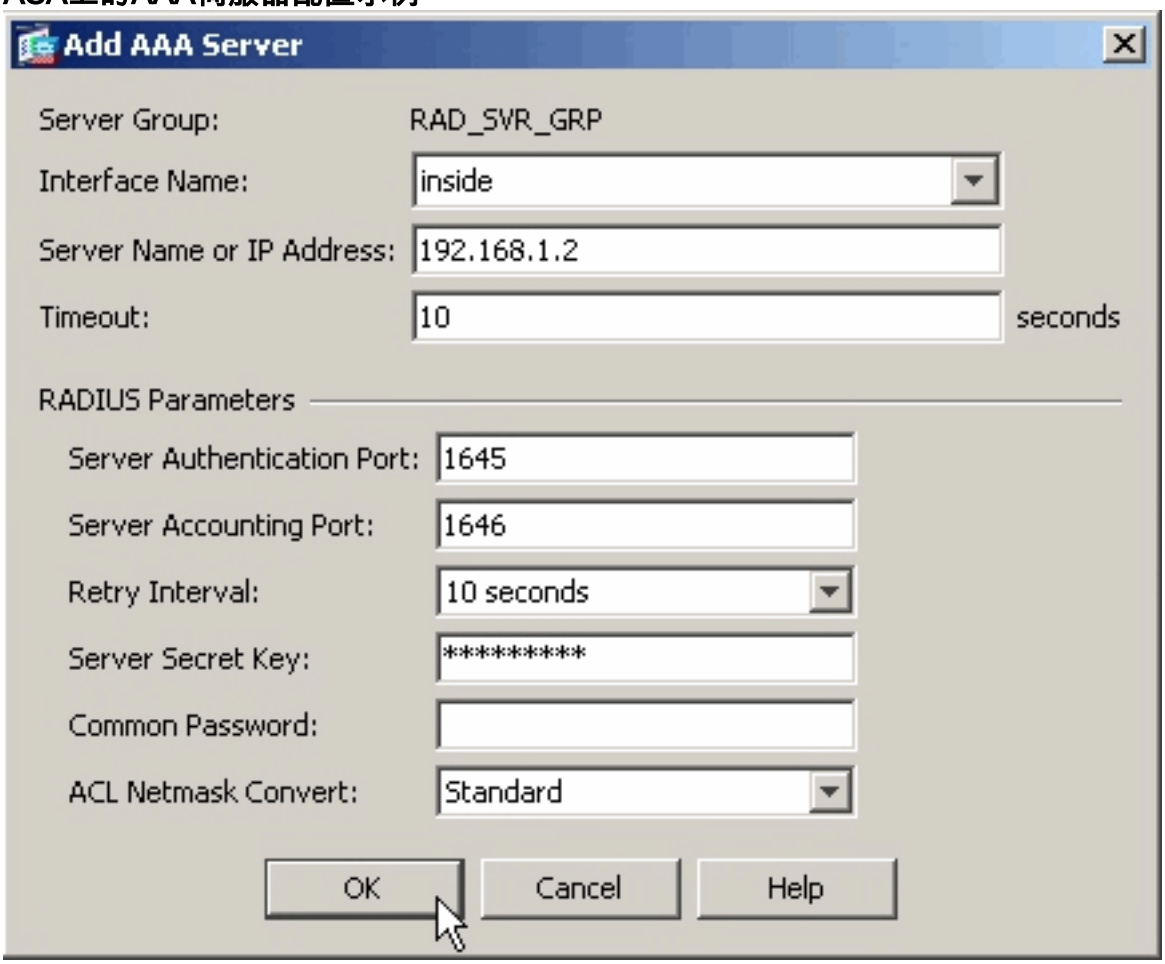
在ASDM中完成以下步驟，以配置ASA與ACS伺服器通訊並驗證WebVPN客戶端。

1. 選擇**Configuration > Remote Access VPN > AAA Setup > AAA Server Groups**。
2. 點選AAA Server Groups旁邊的**Add**。
3. 在顯示的視窗中，指定新AAA伺服器組的名稱，然後選擇**RADIUS**作為協定。完成後按一下



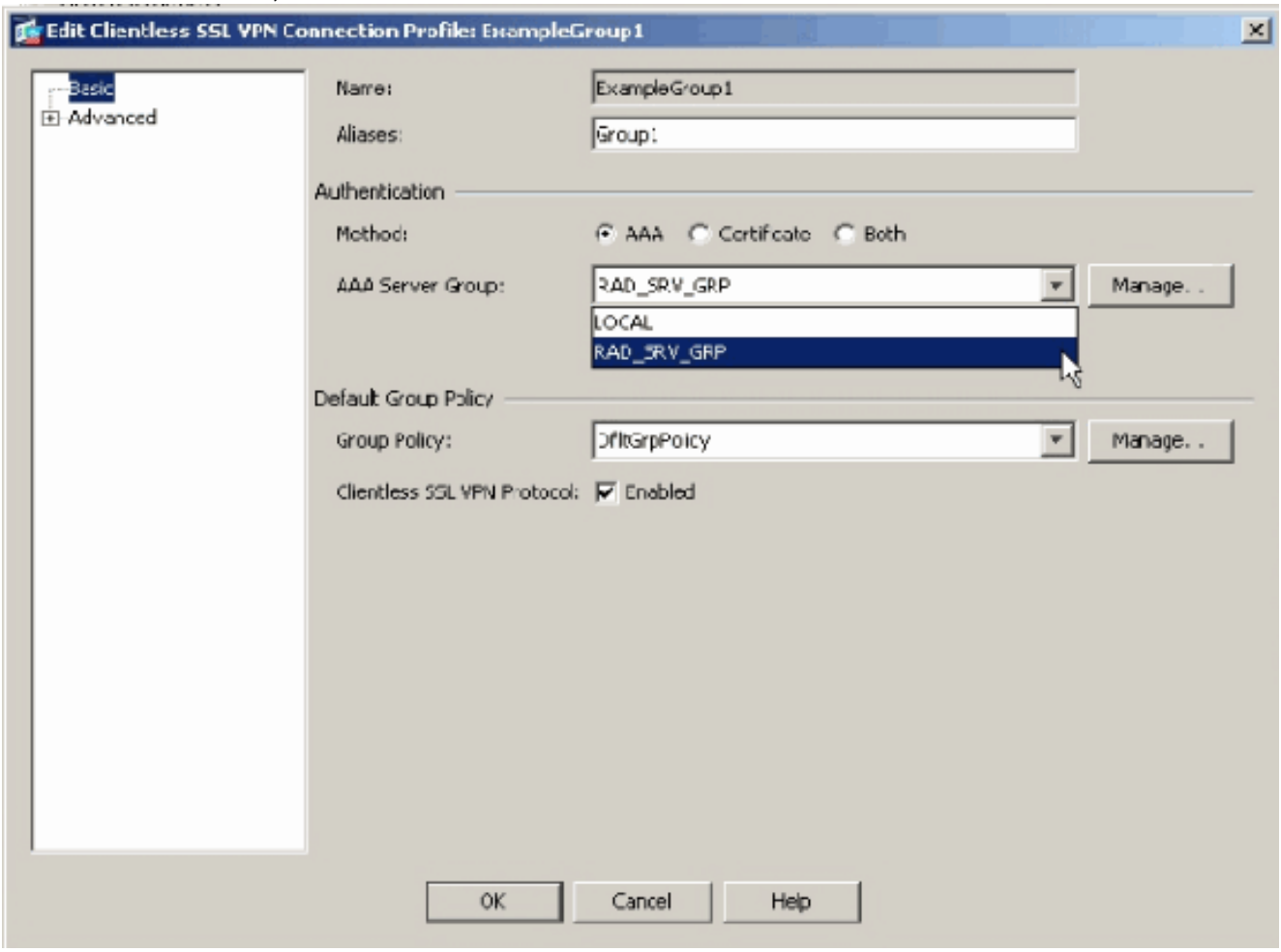
OK。

4. 確保在頂部窗格中選擇了新組，然後按一下下方窗格右側的**Add**。
5. 提供伺服器資訊：**Interface Name** - ASA必須用於訪問ACS伺服器的介面**伺服器名稱或IP**地址 — ASA必須用來訪問ACS伺服器的地址**伺服器密鑰** — 為ACS伺服器上的ASA配置的共用金鑰**ASA上的AAA伺服器配置示例**



6. 配置AAA伺服器組和伺服器後，導航到Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles以配置WebVPN以使用新的AAA配置。**注意**：即使此示例使用WebVPN，您也可以將任何遠端訪問連線配置檔案（隧道組）設定為使用此AAA設定。

7. 選擇要為其配置AAA的配置檔案，然後按一下**Edit**。
8. 在**Authentication**下，選擇之前建立的RADIUS伺服器組。完成後按一下**OK**。



命令列介面

在命令列介面(CLI)中完成以下步驟，以配置ASA與ACS伺服器通訊並驗證WebVPN客戶端。

```
ciscoasa#configure terminal

!--- Configure the AAA Server group. ciscoasa(config)# aaa-server RAD_SRV_GRP protocol RADIUS
ciscoasa(config-aaa-server-group)# exit !--- Configure the AAA Server. ciscoasa(config)# aaa-
server RAD_SRV_GRP (inside) host 192.168.1.2 ciscoasa(config-aaa-server-host)# key secretkey
ciscoasa(config-aaa-server-host)# exit !--- Configure the tunnel group to use the new AAA setup.
ciscoasa(config)# tunnel-group ExampleGroup1 general-attributes ciscoasa(config-tunnel-general)#
authentication-server-group RAD_SRV_GRP
```

驗證

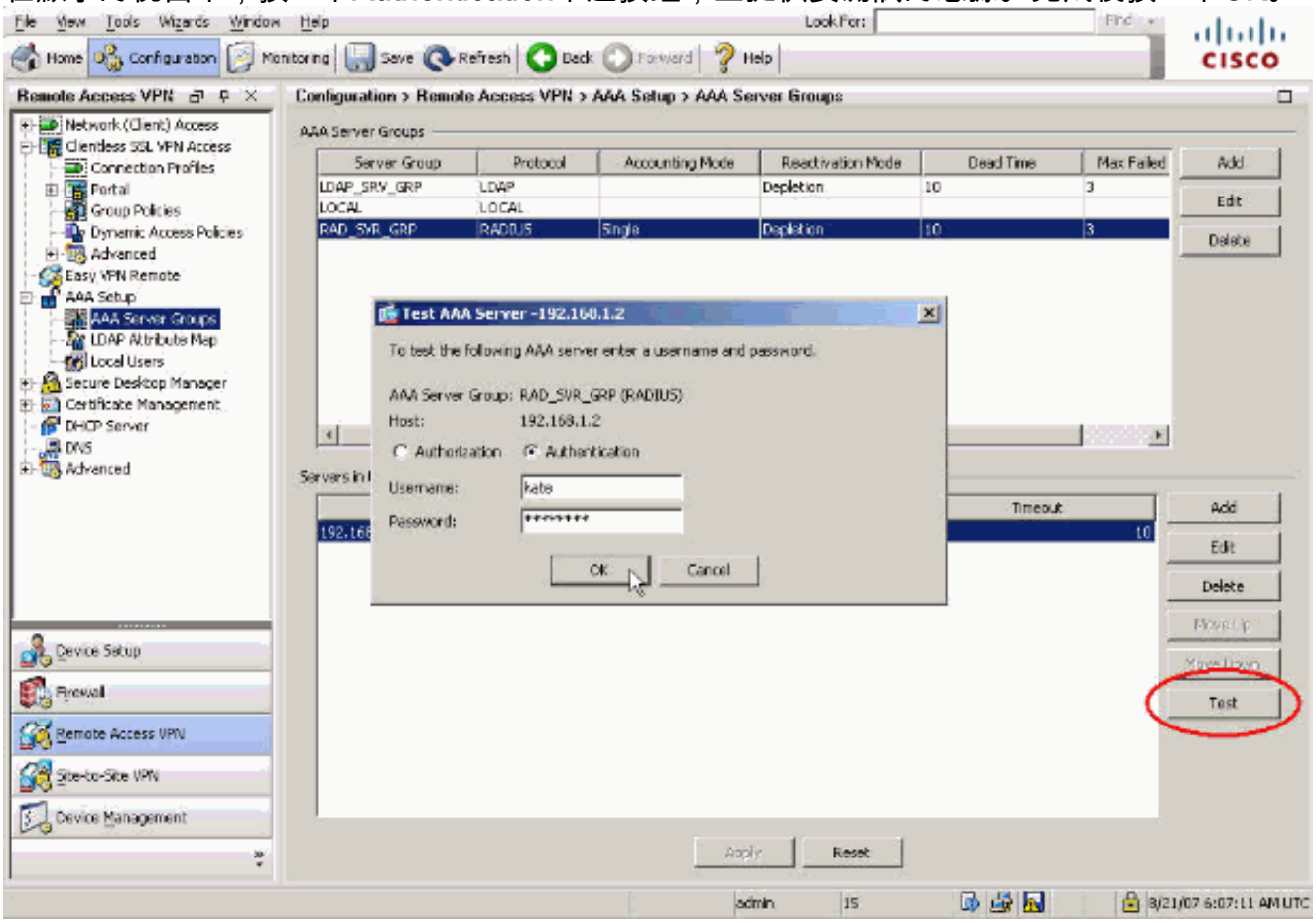
使用本節內容，確認您的組態是否正常運作。

使用ASDM測試

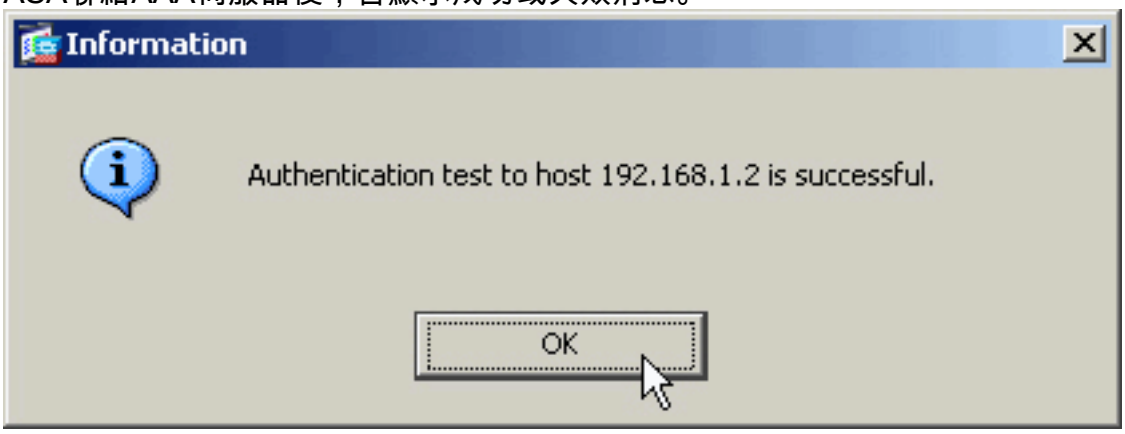
使用AAA Server Groups configuration螢幕上的**Test**按鈕驗證RADIUS配置。提供使用者名稱和密碼後，此按鈕允許您向ACS伺服器傳送測試身份驗證請求。

1. 選擇**Configuration > Remote Access VPN > AAA Setup > AAA Server Groups**。

2. 在頂部窗格中選擇所需的AAA伺服器組。
3. 在下窗格中選擇要測試的AAA伺服器。
4. 按一下下方窗格右側的**Test**按鈕。
5. 在顯示的視窗中，按一下**Authentication**單選按鈕，並提供要測試的憑據。完成後按一下**OK**。



6. ASA聯絡AAA伺服器後，會顯示成功或失敗消息。



使用CLI測試

您可以在命令列中使用**test**命令來測試AAA設定。向AAA伺服器傳送測試請求，並在命令列中顯示結果。

```
ciscoasa#test aaa-server authentication RAD_SVR_GRP host 192.168.1.2 username kate password
cisco123
INFO: Attempting Authentication test to IP address <192.168.1.2> (timeout: 12 seconds)
INFO: Authentication Successful
```

疑難排解

debug radius命令可協助您解決此案例中的驗證問題。此命令啟用RADIUS會話調試以及RADIUS資料包解碼。在顯示的每個調試輸出中，解碼的第一個資料包是從ASA傳送到ACS伺服器的資料包。第二個資料包是來自ACS伺服器的響應。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

驗證成功時，RADIUS伺服器會傳送**access-accept**訊息。

```
ciscoasa#debug radius

!--- First Packet. Authentication Request. ciscoassa#radius mkreq: 0x88 alloc_rip 0xd5627ae4 new
request 0x88 --> 52 (0xd5627ae4) got user '' got password add_req 0xd5627ae4 session 0x88 id 52
RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode (authentication request) ---------------
---------------------- Raw packet data (length = 62)..... 01 34 00 3e 18 71 56 d7 c4 ad e2 73
30 a9 2e cf | .4.>.qV....s0... 5c 65 3a eb 01 06 6b 61 74 65 02 12 0e c1 28 b7 |
\e:...kate....(. 87 26 ed be 7b 2c 7a 06 7c a3 73 19 04 06 c0 a8 | .&..{,z.|.s..... 01 01 05 06
00 00 00 34 3d 06 00 00 00 05 | .......4=..... Parsed packet data..... Radius: Code = 1 (0x01)
Radius: Identifier = 52 (0x34) Radius: Length = 62 (0x003E) Radius: Vector:
187156D7C4ADE27330A92ECF5C653AEB Radius: Type = 1 (0x01) User-Name Radius: Length = 6 (0x06)
Radius: Value (String) = 6b 61 74 65 | kate Radius: Type = 2 (0x02) User-Password Radius: Length
= 18 (0x12) Radius: Value (String) = 0e c1 28 b7 87 26 ed be 7b 2c 7a 06 7c a3 73 19 |
..(..&..{,z.|.s. Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06) Radius: Value
(IP Address) = 192.168.1.1 (0xC0A80101) Radius: Type = 5 (0x05) NAS-Port Radius: Length = 6
(0x06) Radius: Value (Hex) = 0x34 Radius: Type = 61 (0x3D) NAS-Port-Type Radius: Length = 6
(0x06) Radius: Value (Hex) = 0x5 send pkt 192.168.1.2/1645 rip 0xd5627ae4 state 7 id 52
rad_vrfy() : response message verified rip 0xd544d2e8 : chall_state '' : state 0x7 : timer 0x0 :
reqauth: 18 71 56 d7 c4 ad e2 73 30 a9 2e cf 5c 65 3a eb : info 0x88 session_id 0x88 request_id
0x34 user 'kate' response '***' app 0 reason 0 skey 'secretkey' sip 192.168.1.2 type 1 !---
Second Packet. Authentication Response. RADIUS packet decode (response) ------------------------
-------------- Raw packet data (length = 50)..... 02 34 00 32 35 a1 88 2f 8a bf 2a 14 c5 31 78
59 | .4.25../..*..1xY 60 31 35 89 08 06 ff ff ff ff 19 18 43 41 43 53 | `15.........CACS 3a 30
2f 32 61 36 2f 63 30 61 38 30 31 30 31 2f | :0/2a6/c0a80101/ 35 32 | 52 Parsed packet data.....
Radius: Code = 2 (0x02) Radius: Identifier = 52 (0x34) Radius: Length = 50 (0x0032) Radius:
Vector: 35A1882F8ABF2A14C531785960313589 Radius: Type = 8 (0x08) Framed-IP-Address Radius:
Length = 6 (0x06) Radius: Value (IP Address) = 255.255.255.255 (0xFFFFFFFF) Radius: Type = 25
(0x19) Class Radius: Length = 24 (0x18) Radius: Value (String) = 43 41 43 53 3a 30 2f 32 61 36
2f 63 30 61 38 30 | CACS:0/2a6/c0a80 31 30 31 2f 35 32 | 101/52 rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0xd5627ae4 session 0x88 id 52
free_rip 0xd5627ae4
radius: send queue empty
```

身份驗證失敗時，ACS伺服器會傳送**access-reject** 消息。

```
ciscoasa#debug radius

!--- First Packet. Authentication Request. ciscoasa# radius mkreq: 0x85 alloc_rip 0xd5627ae4 new
request 0x85 --> 49 (0xd5627ae4) got user '' got password add_req 0xd5627ae4 session 0x85 id 49
RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode (authentication request) ---------------
---------------------- Raw packet data (length = 62)..... 01 31 00 3e 88 21 46 07 34 5d d2 a3
a0 59 1e ff | .1.>.!F.4]...Y.. cc 15 2a 1b 01 06 6b 61 74 65 02 12 60 eb 05 32 |
..*...kate..`..2 87 69 78 a3 ce d3 80 d8 4b 0d c3 37 04 06 c0 a8 | .ix.....K..7.... 01 01 05 06
00 00 00 31 3d 06 00 00 00 05 | .......1=..... Parsed packet data..... Radius: Code = 1 (0x01)
Radius: Identifier = 49 (0x31) Radius: Length = 62 (0x003E) Radius: Vector:
```

```
88214607345DD2A3A0591EFFCC152A1B Radius: Type = 1 (0x01) User-Name Radius: Length = 6 (0x06)
Radius: Value (String) = 6b 61 74 65 | kate Radius: Type = 2 (0x02) User-Password Radius: Length
= 18 (0x12) Radius: Value (String) = 60 eb 05 32 87 69 78 a3 ce d3 80 d8 4b 0d c3 37 |
`..2.ix.....K..7 Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06) Radius: Value
(IP Address) = 192.168.1.1 (0xC0A80101) Radius: Type = 5 (0x05) NAS-Port Radius: Length = 6
(0x06) Radius: Value (Hex) = 0x31 Radius: Type = 61 (0x3D) NAS-Port-Type Radius: Length = 6
(0x06) Radius: Value (Hex) = 0x5 send pkt 192.168.1.2/1645 rip 0xd5627ae4 state 7 id 49
rad_vrfy() : response message verified rip 0xd544d2e8 : chall_state '' : state 0x7 : timer 0x0 :
reqauth: 88 21 46 07 34 5d d2 a3 a0 59 1e ff cc 15 2a 1b : info 0x85 session_id 0x85 request_id
0x31 user 'kate' response '***' app 0 reason 0 skey 'secretkey' sip 192.168.1.2 type 1 !---
Second packet. Authentication Response. RADIUS packet decode (response) ----------------------
-------------- Raw packet data (length = 32)..... 03 31 00 20 70 98 50 af 39 cc b9 ba df a7 bd
ff | .1. p.P.9....... 06 af fb 02 12 0c 52 65 6a 65 63 74 65 64 0a 0d | ......Rejected.. Parsed
packet data..... Radius: Code = 3 (0x03) Radius: Identifier = 49 (0x31) Radius: Length = 32
(0x0020) Radius: Vector: 709850AF39CCB9BADFA7BDFF06AFFB02 Radius: Type = 18 (0x12) Reply-Message
Radius: Length = 12 (0x0C) Radius: Value (String) =
52 65 6a 65 63 74 65 64 0a 0d                    |  Rejected..
rad_procpkt: REJECT
RADIUS_DELETE
remove_req 0xd5627ae4 session 0x85 id 49
free_rip 0xd5627ae4
radius: send queue empty
```

相關資訊

- 遠端驗證撥入使用者服務(RADIUS)
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems