透過RADIUS伺服器驗證無線區域網路控制器的公用入口管理員

目錄

簡介

本檔案介紹使用RADIUS伺服器驗證無線LAN控制器(WLC)的接待管理員時涉及的組態步驟。

必要條件

需求

嘗試此組態設定之前，請確保您符合以下需求：

- 瞭解如何在WLC上配置基本引數
- 瞭解如何配置RADIUS伺服器，如Cisco Secure ACS
- WLC中訪客使用者的知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行版本7.0.216.0的Cisco 4400無線LAN控制器
- 運行軟體版本4.1的Cisco Secure ACS，在此配置中用作RADIUS伺服器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

接待管理員（也稱為WLC的接待大使）可以在無線LAN控制器(WLC)上建立和管理訪客使用者帳戶。接待大使具有有限的配置許可權，只能訪問用於管理訪客帳戶的網頁。接待大使可以指定訪客使用者帳戶保持活動狀態的時間。經過指定時間後，訪客使用者帳戶將自動過期。

有關訪客使用者的詳細資訊，請參閱部署指南：使用Cisco無線區域網控制器的Cisco訪客接入。

若要在WLC上建立訪客使用者帳戶，您需要以接待管理員身分登入控制器。本檔案將說明使用者如何根據RADIUS伺服器傳回的屬性以接待管理員身分透過WLC驗證。

注意：也可以根據WLC上本地配置的大廳管理員帳戶執行大廳管理員身份驗證。請參閱建立接待大使帳戶獲取有關如何在控制器上本地建立接待管理員帳戶的資訊。

設定

本節提供如何根據本文檔所述目的配置WLC和Cisco Secure ACS的資訊。

組態

本文件使用以下組態：

- WLC的管理介面IP地址為10.77.244.212/27。
- RADIUS伺服器的IP地址是10.77.244.197/27。
- 存取點(AP)和RADIUS伺服器上使用的共用金鑰是cisco123。
- 在RADIUS伺服器中配置的大廳管理員的使用者名稱和密碼都是lobbyadmin。

在本文檔的配置示例中，使用使用者名稱和密碼作為lobbyadmin登入到控制器的所有使用者都被分配了接待管理員的角色。

WLC配置

開始必要的WLC組態之前，請確認控制器執行的是4.0.206.0版或更新版本。這是因為Cisco錯誤ID CSCsg89868(僅供註冊客戶使用)，其中控制器的Web介面在RADIUS資料庫中儲存使用者名稱時，為LobbyAdmin使用者顯示錯誤的網頁。LobbyAdmin具有ReadOnly介面而非LobbyAdmin介面。

此錯誤已在WLC 4.0.206.0版中解決。因此，請確保您的控制器版本是4.0.206.0或更高版本。有關如何將控制器升級到適當版本的說明，請參閱無線LAN控制器(WLC)軟體升級。

要使用RADIUS伺服器執行控制器管理身份驗證，請確保在控制器上啟用Admin-auth-via-RADIUS標誌。可以從show radius summary命令的輸出中進行驗證。

第一步是在控制器上配置RADIUS伺服器資訊，並在控制器和RADIUS伺服器之間建立第3層可接通性。

在控制器上配置RADIUS伺服器資訊

完成以下步驟，以便使用ACS詳細資訊配置WLC：

1. 從WLC GUI中，選擇Security頁籤並配置ACS伺服器的IP地址和共用金鑰。

   要在WLC與ACS通訊，ACS上的共用金鑰必須相同。

   注意： ACS共用金鑰區分大小寫。因此，請確保正確輸入共用金鑰資訊。

   下圖顯示了一個示例：

2. 選中Management覈取方塊以允許ACS管理WLC使用者，如步驟1中的圖所示。然後，按一下Apply。

3. 使用ping命令驗證控制器與已配置RADIUS伺服器之間的第3層可接通性。此ping選項在WLC GUI的Security>RADIUS Authentication頁籤中的「configured RADIUS server」頁上也可用。

   此圖顯示來自RADIUS伺服器的ping成功應答。因此，控制器和RADIUS伺服器之間可以使用第3層可接通性。

RADIUS伺服器配置

要配置RADIUS伺服器，請完成以下部分中的步驟：

1. 將WLC作為AAA客戶端增加到RADIUS伺服器
2. 為接待管理員配置適當的RADIUS IETF服務型別屬性

將WLC作為AAA客戶端增加到RADIUS伺服器

完成以下步驟，以便將WLC增加為RADIUS伺服器中的AAA客戶端。如前所述，本文檔使用ACS作為RADIUS伺服器。此配置可以使用任何RADIUS伺服器。

要在ACS中將WLC增加為AAA客戶端，請完成以下步驟：

1. 從ACS GUI中，選擇Network Configuration頁籤。
2. 在AAA Clients下，按一下Add Entry。
3. 在Add AAA Client窗口中，輸入WLC主機名、WLC的IP地址和共用金鑰。請參閱步驟5下的範例圖表。

4. 從Authenticate Using下拉選單中，選擇RADIUS (Cisco Aironet)。

5. 按一下Submit + Restart以儲存配置。

為接待管理員配置適當的RADIUS IETF服務型別屬性

要透過RADIUS伺服器將控制器的管理使用者驗證為接待管理員，必須將該使用者增加到RADIUS資料庫，其中IETF RADIUS Service-Type屬性設定為Callback Administrative。此屬性為特定使用者分配控制器上接待管理員的角色。

本文檔顯示作為接待管理員的使用者lobbyadmin示例。要配置此使用者，請在ACS上完成以下步驟：

1. 從ACS GUI中，選擇User Setup頁籤。

2. 輸入要增加到ACS的使用者名稱，如以下示例窗口所示：

3. 按一下Add/Edit轉到「User Edit」頁。

4. 在「使用者編輯」頁面上，提供此使用者的實際名稱、說明和密碼詳細資訊。

   在本示例中，使用的使用者名稱和密碼均為lobbyadmin。

5. 向下滾動到IETF RADIUS Attributes設定並選中Service-Type Attribute覈取方塊。

6. 從Service-Type下拉選單中選擇Callback Administrative，然後按一下Submit。

   此屬性會指定此使用者為接待管理員的角色。

   有時，使用者設定下看不到此Service-Type屬性。在這種情況下，請完成以下步驟使其可見：

   a. 從ACS GUI中，選擇Interface Configuration > RADIUS (IETF)以在使用者配置窗口中啟用IETF屬性。

      這會顯示RADIUS (IETF)設定頁面。

   b. 在「RADIUS (IETF)設定」(RADIUS (IETF)設定頁面，您可以啟用需要顯示在使用者或組設定下的IETF屬性。對於此配置，請檢查User列的Service-Type，然後按一下Submit。

      此視窗顯示範例：

      注意：此示例指定基於每個使用者的身份驗證。您也可以根據特定使用者所屬的組執行身份驗證。在這種情況下，請選中Group覈取方塊，以便在Group settings下看到此屬性。

      注意：此外，如果身份驗證基於組，則需要將使用者分配到特定組，並配置組設定IETF屬性以提供對該組使用者的訪問許可權。有關如何配置和管理組的詳細資訊，請參閱使用者組管理。

驗證

使用本節內容，確認您的組態是否正常運作。

若要驗證組態是否正常運作，請透過GUI (HTTP/HTTPS)模式存取WLC。

注意：接待大使無法訪問控制器CLI介面，因此只能從控制器GUI中建立訪客使用者帳戶。

出現登入提示時，輸入在ACS上配置的使用者名稱和密碼。如果配置正確，則表明您作為接待管理員已成功透過WLC的身份驗證。此範例顯示大廳管理員的GUI在成功驗證後如何尋找：

注意：您可以看到除訪客使用者管理外，接待管理員沒有其他選項。

為了從CLI模式進行驗證，請以Read-Write管理員身分Telnet至控制器。在控制器CLI中發出debug aaa all enable命令。

```
<#root>

(Cisco Controller) >

debug aaa all enable


(Cisco Controller) >
*aaaQueueReader: Aug 26 18:07:35.072: ReProcessAuthentication previous proto 28,
 next proto 20001
*aaaQueueReader: Aug 26 18:07:35.072: AuthenticationRequest: 0x3081f7dc
*aaaQueueReader: Aug 26 18:07:35.072:   Callback.....................................0x10756dd0
*aaaQueueReader: Aug 26 18:07:35.072:   protocolType.................................0x00020001
*aaaQueueReader: Aug 26 18:07:35.072:   proxyState....................................00:00:00:40:
00:00-00:00
*aaaQueueReader: Aug 26 18:07:35.072:   Packet contains 5 AVPs (not shown)
*aaaQueueReader: Aug 26 18:07:35.072: apfVapRadiusInfoGet: WLAN(0) dynamic int attributes srcAddr:
0x0, gw:0x0, mask:0x0, vlan:0, dpPort:0, srcPort:0
*aaaQueueReader: Aug 26 18:07:35.073: 00:00:00:40:00:00 Successful transmission of Authentication
Packet (id 39) to 10.77.244.212:1812, proxy state 00:00:00:40:00:00-00:01
*aaaQueueReader: Aug 26 18:07:35.073: 00000000: 01 27 00 47 00 00 00 00  00 00 00 00 00 00 00 00
.'.G............
*aaaQueueReader: Aug 26 18:07:35.073: 00000010: 00 00 00 00 01 0c 6c 6f  62 62 79 61 64 6d 69 6e
......lobbyadmin
*aaaQueueReader: Aug 26 18:07:35.073: 00000020: 02 12 5f 5b 5c 12 c5 c8  52 d3 3f 4f 4f 8e 9d 38
 .._[\...R.?OO..8
*aaaQueueReader: Aug 26 18:07:35.073: 00000030: 42 91 06 06 00 00 00 07  04 06 0a 4e b1 1a 20 09
B..........N....
*aaaQueueReader: Aug 26 18:07:35.073: 00000040: 57 4c 43 34 34 30 30 WLC4400
*radiusTransportThread: Aug 26 18:07:35.080: 00000000: 02 27 00 40 7e 04 6d 533d ed 79 9c b6 99 d1
f8  .'.@~.mS=.y.....
*radiusTransportThread: Aug 26 18:07:35.080: 00000010: d0 5a 8f 4f 08 06 ff ffff ff 06 06 00 00 00
0b  .Z.O............
*radiusTransportThread: Aug 26 18:07:35.080: 00000020: 19 20 43 41 43 53 3a 302f 61 65 32 36 2f 61
34  ..CACS:0/ae26/a4
*radiusTransportThread: Aug 26 18:07:35.080: 00000030: 65 62 31 31 61 2f 6c 6f62 62 79 61 64 6d 69
6e  eb11a/lobbyadmin
*radiusTransportThread: Aug 26 18:07:35.080: ****Enter processIncomingMessages: response code=2
*radiusTransportThread: Aug 26 18:07:35.080: ****Enter processRadiusResponse: response code=2
*radiusTransportThread: Aug 26 18:07:35.080: 00:00:00:40:00:00 Access-Accept received from RADIUS
server 10.77.244.212 for mobile 00:00:00:40:00:00 receiveId = 0
```

```
*radiusTransportThread: Aug 26 18:07:35.080: AuthorizationResponse: 0x13c73d50
*radiusTransportThread: Aug 26 18:07:35.080:    structureSize.............................118
*radiusTransportThread: Aug 26 18:07:35.080:    resultCode................................0
*radiusTransportThread: Aug 26 18:07:35.080:    protocolUsed..............................0x00000001
*radiusTransportThread: Aug 26 18:07:35.080:    proxyState................................00:00:00:4
*radiusTransportThread: Aug 26 18:07:35.080:    Packet contains 3 AVPs:
*radiusTransportThread: Aug 26 18:07:35.080:        AVP[01] Framed-IP-Address.....................0x
*radiusTransportThread: Aug 26 18:07:35.080:
```

AVP[02] Service-Type.....0x0000000b (11) (4 bytes

)
*radiusTransportThread: Aug 26 18:07:35.080:

AVP[03] Class.....
CACS:0/ae26/a4eb11a/lobbyadmin (30 bytes)

***emWeb: Aug 26 18:07:35.084: Authentication succeeded for lobbyadmin**

在此輸出中突出顯示的資訊中，您可以看到service-type attribute 11（回撥管理）從ACS伺服器傳遞到控制器，並且使用者以接待管理員的身份登入。

這些指令可能會有額外的說明：

- debug aaa details enable
- debug aaa events enable
- debug aaa packets enable

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

疑難排解

當您使用接待大使許可權登入到控制器時，您無法使用「0」生命週期值（永不過期的帳戶）建立訪客使用者帳戶。在這些情況下，您會收到`Lifetime value cannot be 0`錯誤消息。

這是由思科錯誤ID CSCsf32392(僅供註冊客戶使用)所致，該錯誤主要與WLC版本4.0相關。此錯誤已在WLC版本4.1中解決。

相關資訊

- 控制器上管理使用者的RADIUS伺服器身份驗證配置示例
- Cisco Unified Wireless Network TACACS+配置
- Cisco無線LAN控制器組態設定指南4.0版-管理使用者帳戶
- 無線區域網控制器上的ACL配置示例
- 無線 LAN 控制器 (WLC) 常見問題
- 無線區域網控制器上的ACL：規則、限制和示例
- 使用無線 LAN 控制器的外部 Web 驗證組態範例
- 無線 LAN 控制器 Web 驗證組態範例
- 使用WLC的訪客WLAN和內部WLAN的配置示例

- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。