在無線LAN控制器上設定RADIUS伺服器回退功能

目錄

簡介

本檔案介紹如何使用無線LAN控制器(WLC)設定RADIUS伺服器回退功能。

必要條件

需求

思科建議您瞭解以下主題：

- 輕量型存取點(LAP)和Cisco WLC組態的基本知識
- 無線存取點通訊協定(CAPWAP)的控制和布建基礎知識
- 無線安全解決方案基礎知識

採用元件

本檔案中的資訊是根據Cisco 5508/5520控制器。

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。

背景資訊

RADIUS伺服器回退功能

低於5.0的WLC軟體版本不支援RADIUS伺服器回退機制。當主RADIUS伺服器不可用時，WLC將故障切換到下一個主備份RADIUS伺服器。即使主伺服器可用，WLC也會一直使用輔助RADIUS伺服器。通常，主伺服器是高效能和首選伺服器。

在WLC 5.0和更新版本中，WLC支援RADIUS伺服器回退功能。使用此功能，可以將WLC配置為檢查主伺服器是否可用，並在主伺服器可用後切換回主RADIUS伺服器。為此，WLC支援兩種新模式（被動和主動），以檢查RADIUS伺服器的狀態。在指定的逾時值後，WLC會回復到最理想的伺服器。

回退模式

主動模式

在主動模式下，當伺服器沒有響應WLC身份驗證請求時，WLC會將伺服器標籤為停機，然後將伺服器移動到非主動伺服器池並開始定期傳送探測消息，直到該伺服器作出響應。如果伺服器回應，WLC會將失效伺服器移動到作用中池，並停止傳送探測訊息。在此模式下，當收到驗證要求時，WLC一律從RADIUS伺服器的作用中池中選擇最低索引（最高優先順序）伺服器。

WLC在逾時後傳送探查封包（預設值為300秒），以確定伺服器狀態，以防伺服器之前沒有回應。

被動模式

在被動模式下，如果伺服器沒有響應WLC身份驗證請求，WLC會將伺服器移動到非活動隊列並設定計時器。計時器到期時，WLC會將伺服器移動到作用中佇列，與伺服器的實際狀態無關。收到驗證要求時，WLC會從作用中佇列（可能包括非作用中伺服器）中選取最低索引（最高優先順序）伺服器。 如果伺服器沒有回應，則WLC會將其標示為不活動，設定計時器，並移動到下一個最高優先順序的伺服器。此程式會一直持續，直到WLC找到作用中RADIUS伺服器或作用中伺服器池耗盡。

WLC會假設伺服器逾時後處於作用中狀態（預設值為300秒），以防伺服器之前沒有回應。如果仍然沒有回應，WLC會等待另一個逾時，並在驗證要求傳入時再次嘗試。

關閉模式

在關閉模式下，WLC僅支援故障切換。換句話說，回退是禁用的。當主RADIUS伺服器關閉時，WLC將故障切換到下一個主備份RADIUS伺服器。WLC會一直使用輔助RADIUS伺服器，即使主伺服器可用。

設定

使用CLI設定RADIUS伺服器回退功能

> **附註**：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

在WLC CLI上使用這些命令，以便在WLC上啟用RADIUS伺服器回退功能。

第一步是選擇RADIUS伺服器回退模式。如前所述，WLC支援主動和被動回退模式。

若要選擇回退模式，請輸入以下命令：

```
WLC1 > config radius fallback-test mode {active/passive/off}
```

- active — 將探測器傳送到失效伺服器以測試狀態。
- passive — 根據上一個事務設定伺服器狀態。
- off — 禁用伺服器回退測試（預設）。

下一步是選擇指定主動模式的探測間隔或被動操作模式的非活動時間的間隔。

若要設定時間間隔，請輸入以下命令：

```
WLC1 > config radius fallback-test mode interval {180 - 3600}
```

<180到3600> - 輸入探測間隔或非活動時間（秒）（預設值為300秒）。

間隔指定在主動模式回退情況下的探測間隔或在被動模式回退情況下的非活動時間。

對於活動操作模式，您需要配置一個使用者名稱，該使用者名稱將用於傳送到RADIUS伺服器的探測請求。

若要設定使用者名稱，請輸入以下命令：

```
WLC1 >config radius fallback-test username {username}
```

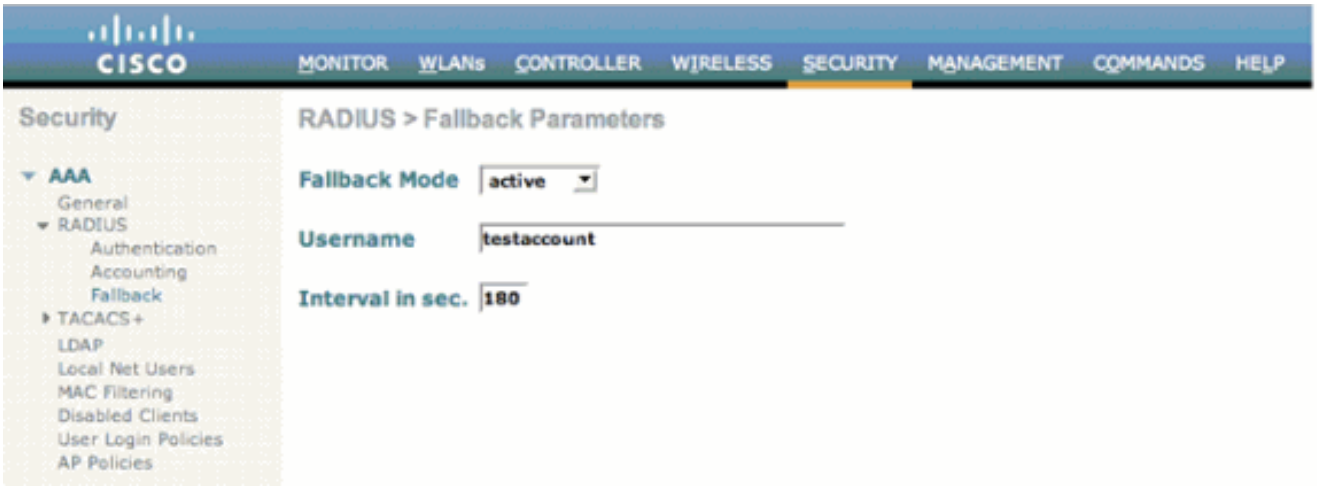
<username> — 輸入最多16個字母數字字元的名稱（預設值為cisco-probe）。

> **附註**：您可以輸入自己的使用者名稱，也可以保留為預設值。預設使用者名稱為「cisco-probe」。 由於此使用者名稱用於傳送探測消息，因此不需要配置密碼。

使用GUI配置RADIUS伺服器回退功能

完成以下步驟，以便使用GUI設定WLC:

1. 配置RADIUS伺服器回退的模式。若要執行此操作，請從WLC GUI中選擇**Security > RADIUS > Fallback**。此時會顯示「**RADIUS > Fallback Parameters**」頁。
2. 在「**Fallback Mode**」下拉選單中，選擇回退模式。可用選項包括主動、被動和關閉。以下是活動回退模式配置的螢幕截圖，如下圖所示。



3. 對於活動操作模式，請在使用者名稱欄位中輸入使用者名稱。
4. 在Interval（以秒為單位）中輸入探測間隔值。欄位.
5. 按一下「**Apply**」。

如果在WLC中啟用了主動故障切換功能，則WLC過於主動，無法將AAA伺服器標籤為「無響應」。但是，不應執行此操作，因為，如果您執行靜默丟棄，則AAA伺服器可能只響應該特定客戶端。它可能是對具有有效證書的其他有效客戶端的響應。WLC仍可將AAA伺服器標籤為「not responding」和「not functional」。

為了克服此問題，請禁用主動故障切換功能。從控制器GUI輸入**config radius aggressive-failover disable**命令以執行此操作。如果此選項處於禁用狀態，則只有在連續三個客戶端無法從RADIUS伺服器接收響應時，控制器才會故障切換到下一個AAA伺服器。

> **附註**：8.5.140、8.8.100、8.10.105及更新版本中引入的功能變更：當控制器的RADIUS主動故障切換被禁用時：除非從使用者端進行中止，否則封包將重試六次。來自多個使用者端（之前僅來自三個使用者端）的三個逾時事件（18次連續重試）後，RADIUS伺服器（身份驗證和acct）會標籤為無法連線。 啟用控制器的RADIUS主動故障切換時：除非從使用者端進行中止，否則封包將重試六次。RADIUS伺服器（AUTH和ACCT）在從多個使用者端（之前僅從一個使用者端）發生一次逾時事件（連續重試6次）後標示為無法連線。 這表示每個RADIUS伺服器（AUTH或ACCT）可從多個使用者端連續重試18次。因此，不能保證每個資料包都會重試六次。

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**指令輸出的分析。

輸入**show radius summary**命令以驗證回退配置。以下是範例：

```
WLC1 >show radius summary

Vendor Id Backward Compatibility..... Disabled
Call Station Id Type..................... IP Address
Aggressive Failover..................... Enabled
Keywrap.................................. Disabled
```

```
Fallback Test:
Test Mode..................................... Active
Probe User Name............................... testaccount
Interval (in seconds)......................... 180

Authentication Servers

Idx Type Server Address Port State Tout RFC3576 IPSec-AuthMode/Phase1/Group/Lifetime/Auth/Encr
--- ---- -------------- ---- ------- ---- ------- ----------------------------------------------
1 NM 10.1.1.12 1812 Enabled 2 Disabled Disabled-none/unknown/group-0/0 none/none

Accounting Servers

Idx Type Server Address Port State Tout RFC3576 IPSec-AuthMode/Phase1/Group/Lifetime/Auth/E
--- ---- -------------- ---- ------- ---- ------- ----------------------------------------
1 N 10.1.1.12 1813 Enabled 2 N/A Disabled-none/unknown/group-0/0 none/nonen
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

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

- **debug dot1x events enable** -配置802.1X事件的調試。
- **debug aaa events enable** - 配置所有AAA事件的調試。

相關資訊

- 使用WLAN控制器(WLC)的EAP驗證組態範例
- 輕量AP(LAP)註冊到無線LAN控制器(WLC)
- 配置安全解決方案
- 使用RADIUS伺服器和無線LAN控制器進行動態VLAN分配配置示例
- 技術支援與文件 - Cisco Systems