使用Dot1x保護Flexconnect AP交換機埠

目錄

簡介

本檔案介紹用於保護Switchport的組態，其中FlexConnect存取點(AP)使用device-traffic-class=switch Radius VSA與Dot1x進行驗證，以允許來自本地交換無線LAN(WLAN)的流量。

必要條件

需求

思科建議您瞭解以下主題：

- 無線Lan控制器(WLC)上的FlexConnect
- 思科交換機上的802.1x
- 網路邊緣驗證拓撲(NEAT)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

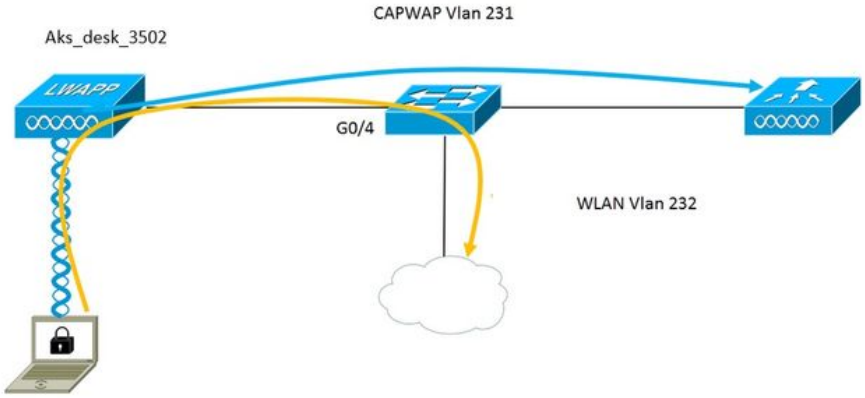
- WS-C3560CX-8PC-S，15.2(4)E1
- AIR-CT-2504-K9,8.2.141.0
- 身分識別服務引擎(ISE)2.0
- 基於IOS的接入點（x500、x600、x700系列）。

截至本文編寫時，基於AP作業系統的Wave 2 AP不支援flexconnect中繼dot1x。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表



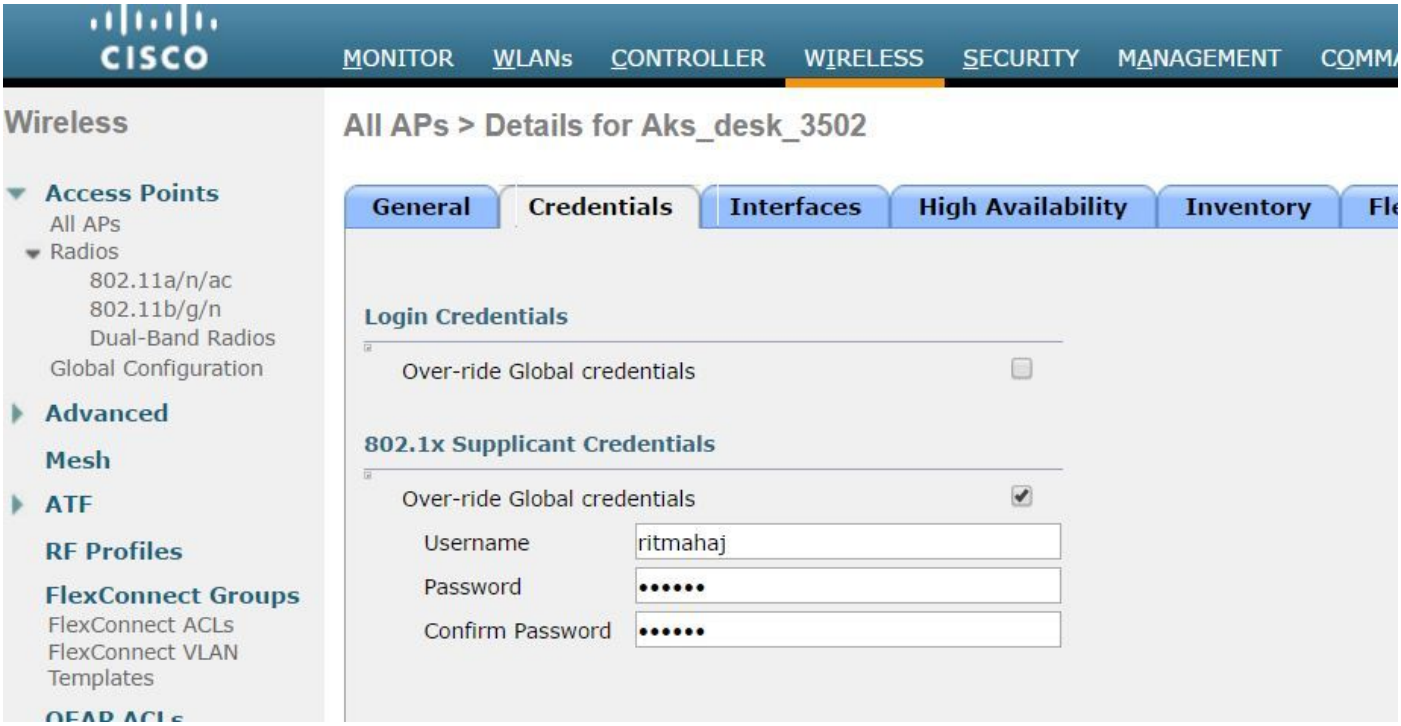
在此設定中，接入點充當802.1x請求方，並由交換機使用EAP-FAST針對ISE進行身份驗證。在連線埠設定為802.1x驗證後，在連線到連線埠的裝置成功進行驗證之前，交換器不會允許802.1x流量以外的任何流量通過該連線埠。

接入點成功通過ISE進行身份驗證後，交換機將收到Cisco VSA屬性「device-traffic-class=switch，並自動將埠移至中繼。

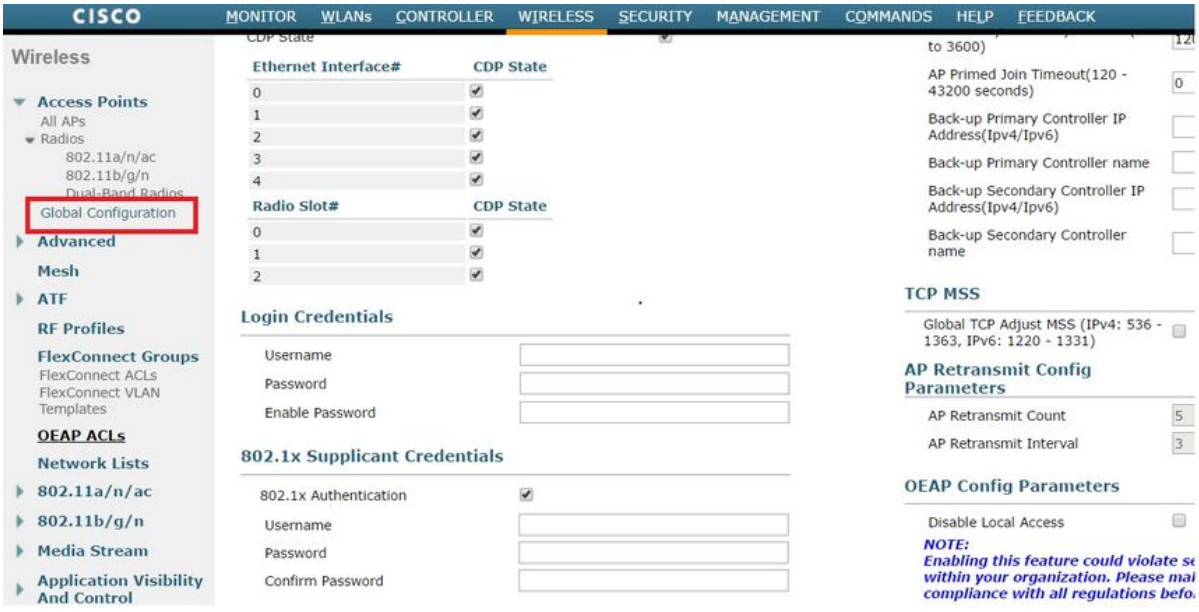
這意味著，如果AP支援FlexConnect模式並且配置了本地交換SSID，它將能夠傳送已標籤的流量。確保AP上啟用了VLAN支援，並且配置了正確的本地VLAN。

AP配置：-

1.如果AP已加入WLC，請轉到Wireless（無線）頁籤並按一下接入點。轉到Credentials欄位，在802.1x Supplicant Credentials標題下，選中**Over-ride Global credentials**框，為此接入點設定802.1x使用者名稱和密碼。



您還可以使用「全域組態」功能表，為加入WLC的所有存取點設定命令使用者名稱和密碼。



2.如果接入點尚未加入WLC，則必須通過控制檯連線到LAP以設定憑據並使用以下CLI命令：

LAP#debug capwap console cli
LAP#capwap ap dot1x username <username> password <password>

交換機配置：-

1.在交換機上全域性啟用dot1x並將ISE伺服器新增到交換機

aaa new-model

!
aaa authentication dot1x default group radius

!
aaa authorization network default group radius

!

dot1x system-auth-control

!

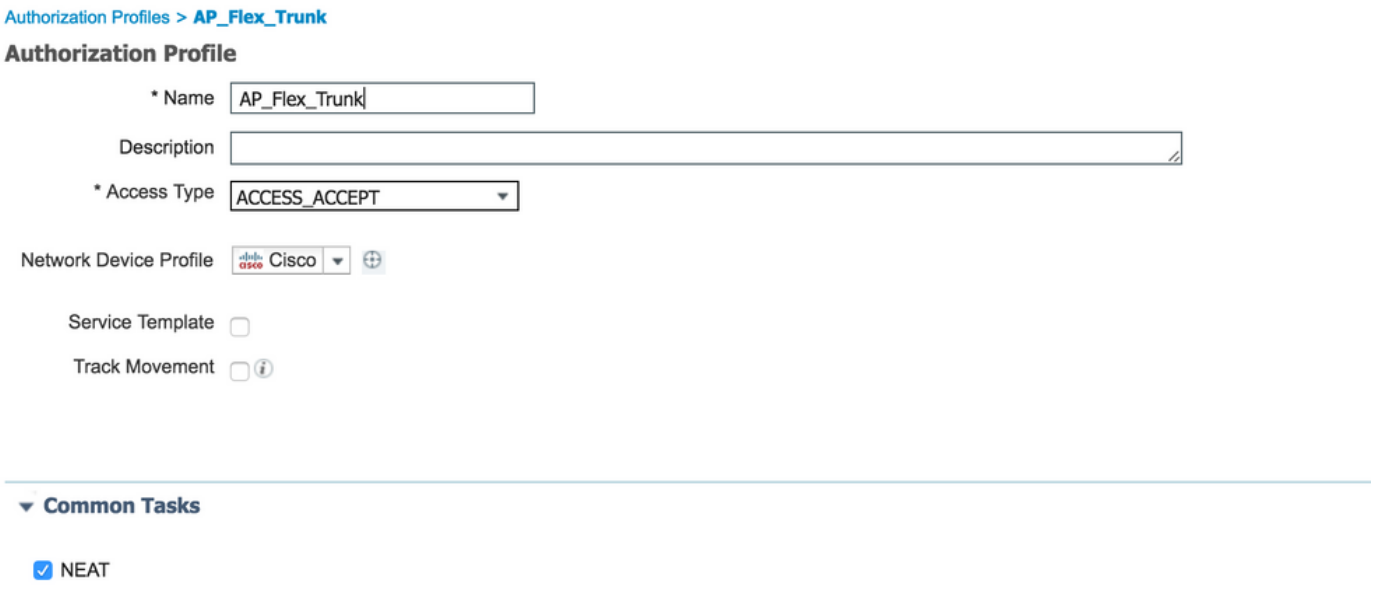
radius伺服器ISE
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
 金鑰7 123A0C0411045D5679

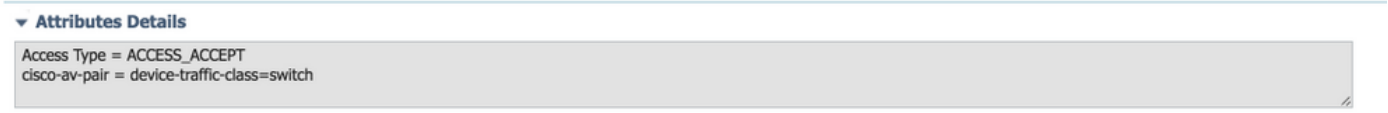
2.現在配置AP交換機埠

interface GigabitEthernet0/4
switchport access vlan 231
switchport trunk allowed vlan 231,232
switchport mode access
authentication host-mode multi-host
驗證順序dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge

ISE配置：-

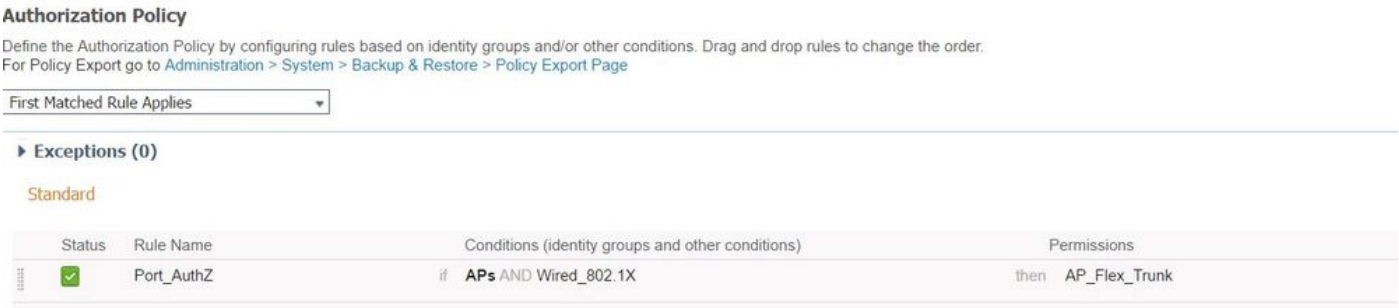
1.在ISE上，只需為AP授權配置檔案啟用NEAT即可設定正確的屬性，但是，在其他RADIUS伺服器上，您可以手動配置。





2.在ISE上，還需要配置身份驗證策略和授權策略。在這種情況下，我們點選了預設身份驗證規則，即有線dot1x，但可以根據要求自定義該規則。

對於授權策略(Port_AuthZ)，在這種情況下，我們將AP憑證新增至使用者群組(AP)，並據此推送授權設定檔(AP_Flex_Trunk)。



驗證

使用本節內容，確認您的組態是否正常運作。

1.在交換機上，一次可以使用「debug authentication feature autocfg all」命令檢查是否將埠移至中繼埠。

2月20日12:34:18.119:%LINK-3-UP:Interface GigabitEthernet0/4, changed state to up
2月20日12:34:19.122:%LINEPROTO-5-UPDOWN:介面GigabitEthernet0/4上的線路協定，狀態更改為up
akshat_sw#
akshat_sw#
2月20日12:38:11.113:AUTH-FEAT-AUTOCFG-EVENT:在dot1x AutoCfg start_fn中，epm_handle:3372220456
2月20日12:38:11.113:AUTH-FEAT-AUTOCFG-EVENT:[588d.0997.061d， Gi0/4]裝置型別=交換機
2月20日12:38:11.113:AUTH-FEAT-AUTOCFG-EVENT:[588d.0997.061d， Gi0/4]新客戶端
2月20日12:38:11.113:AUTH-FEAT-AUTOCFG-EVENT:[Gi0/4]內部Autocfg宏應用程式狀態：1
2月20日12:38:11.113:AUTH-FEAT-AUTOCFG-EVENT:[Gi0/4]裝置型別：2
2月20日12:38:11.113:AUTH-FEAT-AUTOCFG-EVENT:[Gi0/4]自動配置：stp具有port_config 0x85777D8
2月20日12:38:11.113:AUTH-FEAT-AUTOCFG-EVENT:[Gi0/4]自動配置：stp port_config具有bpdu guard_config 2
2月20日12:38:11.116:AUTH-FEAT-AUTOCFG-EVENT:[Gi0/4]在埠上應用auto-cfg。
2月20日12:38:11.116:AUTH-FEAT-AUTOCFG-EVENT:[Gi0/4] Vlan:231 Vlan-Str:231
2月20日12:38:11.116:AUTH-FEAT-AUTOCFG-EVENT:[Gi0/4]應用dot1x_autocfg_supp宏
2月20日12:38:11.116:正在應用命令…… 'no switchport access vlan 231' at Gi0/4
2月20日12:38:11.127:正在應用命令…… 'no switchport nonegotiate' at Gi0/4
2月20日12:38:11.127:正在應用命令……位於Gi0/4的「switchport mode trunk」
2月20日12:38:11.134:正在應用命令……位於Gi0/4的「switchport trunk native vlan 231」
2月20日12:38:11.134:正在應用命令……位於Gi0/4的「spanning-tree portfast trunk」
2月20日12:38:12.120:%LINEPROTO-5-UPDOWN:介面GigabitEthernet0/4上的線路協定，狀態更改為關閉
2月20日12:38:15.139:%LINEPROTO-5-UPDOWN:介面GigabitEthernet0/4上的線路協定，狀態更

改為up

2. 「show run int g0/4」的輸出將顯示該埠已更改為中繼埠。

當前配置：295 位元組
!
interface GigabitEthernet0/4
switchport trunk allowed vlan 231,232,239
switchport trunk native vlan 231
switchport mode trunk
authentication host-mode multi-host
驗證順序dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge trunk
end

3.在ISE上，在Operations>>Radius Livelogs下，我們可以成功進行身份驗證並推送正確的授權配置檔案。

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2017-02-20 15:05:48.991			0	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:05:48.991				ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:04:49.272				ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	

4.如果在此之後連線客戶端，則會在客戶端vlan 232的AP交換機埠上獲取其mac地址。

akshat_sw#sh mac address-table int g0/4
Mac地址表

Vlan Mac地址型別埠
---- ----------- -------- -----
231 588d.0997.061d靜態Gi0/4 - AP
232 c0ee.fbd7.8824 DYNAMIC Gi0/4 — 客戶端

在WLC上，在客戶端詳細資訊中可以看到此客戶端屬於VLAN 232並且SSID在本地交換。這裡有一個片段。

（思科控制器）>show client detail c0:ee:fb:d7:88:24
客戶端MAC地址…….....c0:ee:fb:d7:88:24
客戶端使用者名稱…….....不適用
AP MAC地址…….....b4:14:89:82:cb:90
AP名稱…….....Aks_desk_3502
AP無線電插槽ID.....1
客戶端狀態…….....關聯
客戶端使用者組…….....
客戶端NAC OOB狀態…….....存取
無線LAN ID.....2
無線LAN網路名稱(SSID)。.....Port-Auth
無線LAN設定檔名稱…….....Port-auth
熱點(802.11u)。.....不支援
BSSID.....b4:14:89:82:cb:9f

已連線……..... 42秒
頻道……..... 44
IP 位址.....192.168.232.90
網關地址……..... 192.168.232.1
網路掩碼……..... 255.255.255.0
關聯ID..... 1
身份驗證演算法……..... 開放系統
原因代碼……..... 1
狀態代碼……..... 0

FlexConnect資料交換……..... 本地
FlexConnect Dhcp狀態……..... 本地
基於FlexConnect Vlan的集中交換……..... 否
FlexConnect身份驗證……..... 中央
FlexConnect中心關聯……..... 否
FlexConnect VLAN名稱……..... VLAN 232
隔離VLAN.....0
訪問VLAN..... 232
本地橋接VLAN..... 232

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

- 如果驗證失敗，請使用**debug dot1x**、**debug authentication**命令。
- 如果埠未移動到TRUNK，請輸入**debug authentication feature autocfg all**命令。
- 確保配置了多主機模式（身份驗證主機模式多主機）。必須啟用多主機才能允許客戶端無線MAC地址。
- 必須配置「aaa authorization network」命令，交換機才能接受並應用ISE傳送的屬性。

基於Cisco IOS的接入點僅支援TLS 1.0。如果您的RADIUS伺服器配置為僅允許TLS 1.2 802.1X身份驗證，則可能導致問題