تأمين محول نقطة وصول FlexConnect باستخدام DOT1x

المحتويات

المقدمة

يصف هذا وثيقة التشكيل أن يؤمن switchports حيث FlexConnect منفذ نقطة (AP) يصدق مع dot1x يستعمل أداة-traffic-class=switch radius VSA أن يسمح حركة مرور من يحول محليا LANs السلكي (WLANs).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية (WLC) طراز FlexConnect
- 802.1x على محولات Cisco
- مخطط مصادقة حافة الشبكة (NEAT)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

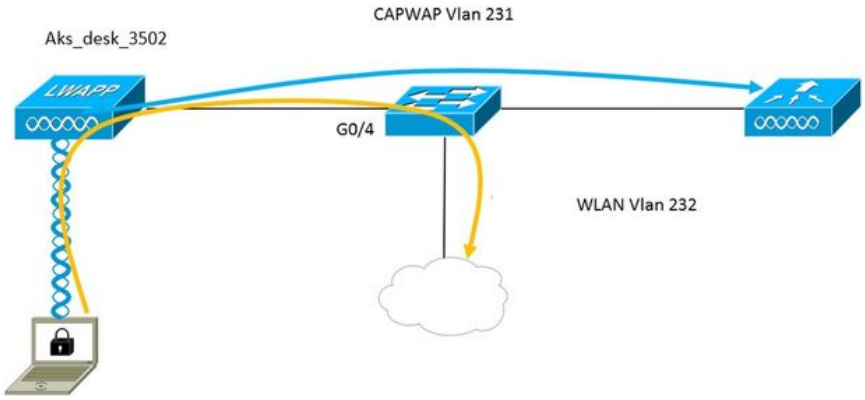
- WS-C3560CX-8PC-S، 15.2(4)E1
- AIR-CT-2504-K9، 8.2.141.0
- Identity Service Engine (ISE) 2.0
- نقاط الوصول المستندة إلى IOS (سلسلة x500،x600،x700).

لا تدعم نقاط الوصول من السلسلة Wave 2 المستندة إلى نظام تشغيل AP خط اتصال FlexConnect dot1x اعتبارا من وقت هذه الكتابة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الرسم التخطيطي للشبكة



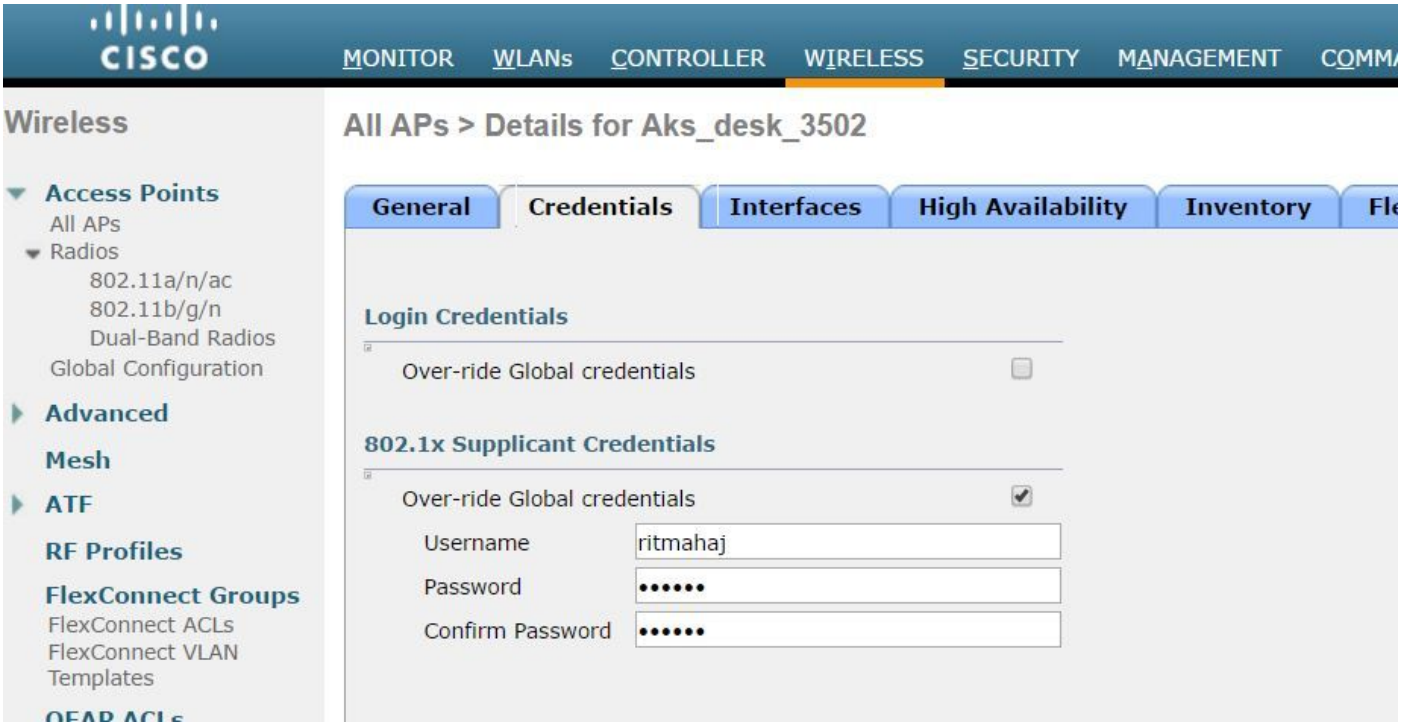
في هذا الإعداد، تعمل نقطة الوصول كمقوم 802.1x وتمت مصادقتها بواسطة المحول مقابل ISE باستخدام EAP-FAST. ما إن اكتملت المصادقة 802.1x، المفتاح الذي يسمح أي حركة مرور غير 802.1x حركة مرور أن يمر عبر الميناء إلى أن الأداة يربط إلى الميناء يصادق بنجاح.

وبمجرد أن تتم مصادقة نقطة الوصول بنجاح ضد ISE، يستقبل المحول سمة Cisco VSA "device-traffic-class=switch ويقل المنفذ تلقائيا إلى خط الاتصال.

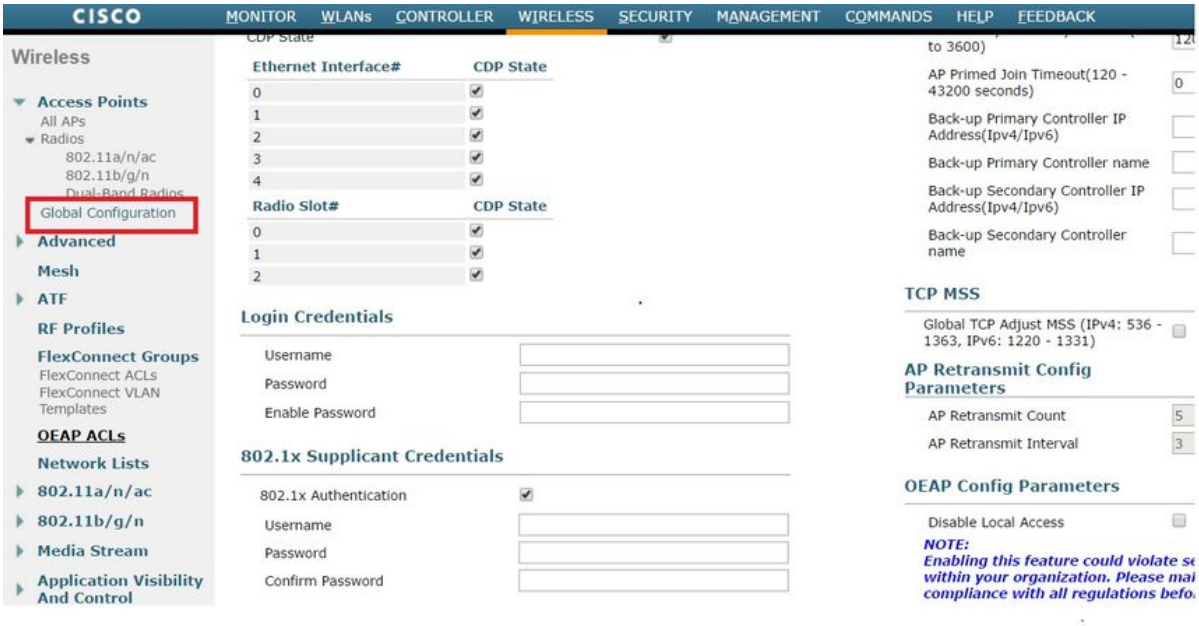
وهذا يعني، إذا كانت نقطة الوصول تدعم وضع FlexConnect وكانت تحتوي على عناوين SSID محولة محليا تم تكوينها، فإنها ستكون قادرة على إرسال حركة مرور ذات علامات تمييز. ضمنت أن مكنت دعم VLAN على ال ap وال يصح VLAN أهلي طبيعي شكلت.

تكوين نقطة الوصول:-

1. إذا كانت نقطة الوصول متصلة بالفعل مع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، فانتقل إلى علامة التبويب اللاسلكية وانقر على نقطة الوصول. انتقل إلى حقل Credetials وأدخل عنوان بيانات اعتماد متبرع 802.1x، وحدد مربع **بيانات الاعتماد العالمية** لإعادة **التشغيل** لتعيين اسم المستخدم وكلمة المرور الخاصين بنقطة الوصول هذه وفقا لمعيار 802.1x.



أنت يستطيع أيضا ثبتت فاصلة username وكلمة ل all the منفذ نقطة أن يكون اقترنت إلى ال WLC مع الشامل تشكيل قائمة.



2. إذا لم تكن نقطة الوصول قد انضمت إلى عنصر تحكم في الشبكة المحلية اللاسلكية (WLC) بعد، فيجب عليك وحدة تحكم في نقطة الوصول لتعيين بيانات الاعتماد واستخدام أمر واجهة سطر الأوامر (CLI) هذا:

LAP#debug Capwap Console CLI
LAP#capwap ap dot1x username <username> كلمة <password>

تكوين المحول:-

1. قم بتمكين dot1x على المحول بشكل عام وإضافة خادم ISE إلى المحول

نموذج AAA جديد

!
نقطة مصادقة AAA1x نصف قطر المجموعة الافتراضية

!
نصف قطر المجموعة الافتراضية لشبكة تفويض AAA

!

dot1x system-auth-control

!

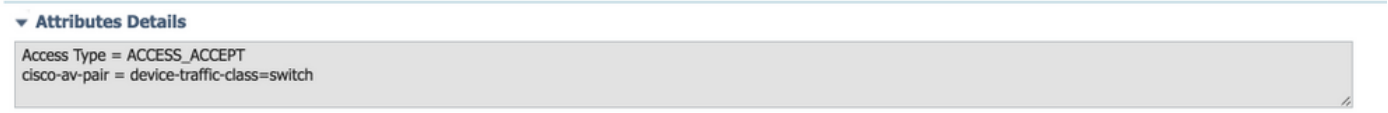
ISE لخادم RADIUS
عنوان IPv4 10.48.39.161 auth-port 1645 acct-port 1646
key 7 123a0c0411045d5679

2. قم الآن بتكوين منفذ محول AP

interface GigabitEthernet0/4
switchport access vlan 231
switchport trunk allowed vlan 231،232
الوصول إلى وضع Switchport
مضيف متعدد الوضع للمصادقة
أمر المصادقة dot1x
التحكم التلقائي في منفذ المصادقة
dot1x Pae Authenticator
حافة PortFast للشجرة الممتدة

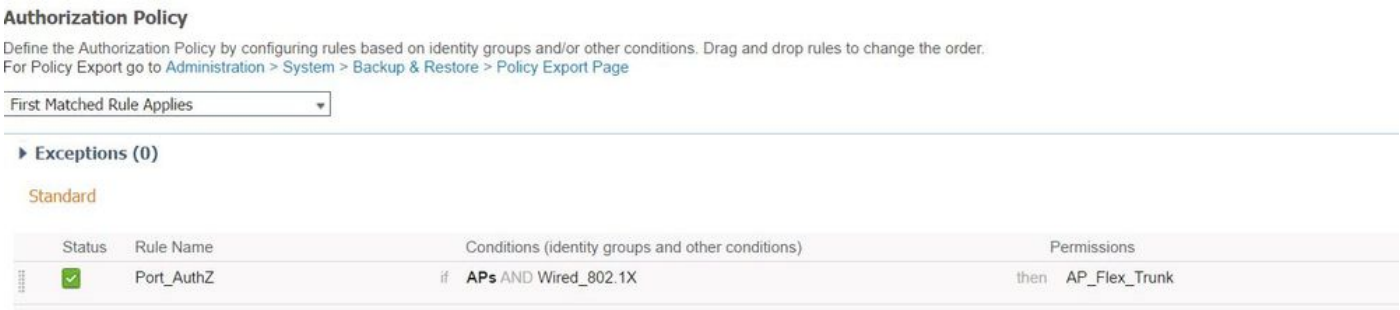
تكوين ISE:-

1. في ISE، يستطيع واحد ببساطة مكنت neat لملف تعريف توخيل نقطة الوصول in order to ثبتت السمة صحيح، على أي حال، على آخر RADIUS دان، أنت يستطيع شكلت يدويا.



2. في ISE، يحتاج المرء أيضا إلى تكوين سياسة المصادقة وسياسة التخويل. في هذه الحالة، نطبق قاعدة المصادقة الافتراضية التي تكون سلكية dot1x ولكن يمكن للمرء تخصيصها وفقا للمتطلبات.

بالنسبة لنهج التفويض (Port_AuthZ)، في هذه الحالة أضفنا بيانات اعتماد AP إلى مجموعة مستخدمين (APs) ودفعنا ملف تعريف التفويض (AP_Flex_Trunk) استنادا إلى هذا.



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

1. على المحول، يمكن مرة واحدة إستخدام الأمر "debug authentication feature autocfg all" للتحقق من نقل المنفذ إلى منفذ خط الاتصال أو ال.

20 فبراير 12:34:18.119: %LINK-3-UPDOWN: الواجهة GigabitEthernet0/4، تم تغيير الحالة إلى أعلى
20 فبراير 12:34:19.122: %LINEPROTO-5-UPDOWN: برتوكول الخط على الواجهة GigabitEthernet0/4، تم تغيير الحالة إلى أعلى
akshat_sw#
akshat_sw#
20 فبراير 12:38:11.113: auth-feat-autocfg-event: in dot1x AutoCfg start_fn، epm_handle: 3372220456
20 فبراير 12:38:11.113: auth-feat-autocfg-event: [588d.0997.061d، gi0/4] نوع الجهاز = المحول
20 فبراير 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d، Gi0/4] عميل جديد
20 فبراير 12:38:11.113: auth-feat-autoCFG-event: [Gi0/4] حالة تطبيق الماكرو الداخلي ل AutoCFG : 1
20 فبراير 12:38:11.113: auth-feat-autocfg-event: [Gi0/4] نوع الجهاز : 2
20 فبراير:12:38:11.113: auth-feat-autocfg-event: [Gi0/4] Auto-config: يحتوي برتوكول الشجرة المتفرعة (STP) على port_config 0x85777D8
20 فبراير 12:38:11.113: auth-feat-autocfg-event: [Gi0/4] Auto-config: stp port_config لديه BPDU guard_config 2
20 فبراير 12:38:11.116: auth-feat-autocfg-event: [Gi0/4] تطبيق auto-cfg على المنفذ.
20 فبراير 12:38:11.116: auth-feat-autocfg-event: [Gi0/4] VLAN: 231 VLAN-STR: 231
20 فبراير 12:38:11.116: auth-feat-autocfg-event: [Gi0/4] تطبيق dot1x_autocfg_supp macro
20 فبراير 12:38:11.116: تطبيق الأمر.. 'no switchport access vlan 231' على gi0/4
20 فبراير 12:38:11.127: تطبيق الأمر... 'ال منفذ وجود switchport nonegotiate' في Gi0/4
20 فبراير 12:38:11.127: تطبيق الأمر.. 'switchport mode trunk' في Gi0/4
20 فبراير 12:38:11.134: تطبيق الأمر.. 'switchport trunk native vlan 231' على gi0/4
20 فبراير 12:38:11.134: تطبيق الأمر 'arbre-portfast trunk' على Gi0/4

فبراير 20 12:38:12.120: %LINEPROTO-5-UPDOWN: برتوكول الخط على الواجهة GigabitEthernet0/4، تم تغيير الحالة إلى أسفل
فبراير 20 12:38:15.139: %LINEPROTO-5-UPDOWN: برتوكول الخط على الواجهة GigabitEthernet0/4، تم تغيير الحالة إلى أعلى

2. سيظهر إخراج "show run int g0/4" أن المنفذ قد تغير إلى منفذ خط اتصال.

التكوين الحالي : 295 بايت
!
interface GigabitEthernet0/4
switchport trunk allowed vlan 231،232،239
switchport trunk أهلي طبيعي vlan 231
خط اتصال وضع switchport
مضيف متعدد الوضع للمصادقة
أمر المصادقة dot1x
التحكم التلقائي في منفذ المصادقة
dot1x Pae Authenticator
خط اتصال PortFast Edge لشجرة المتمتدة
نهاية

3. على محرك خدمات الهوية (ISE)، وتحت بند "العمليات">يمكن لمصادقة Radius Livelogs أن تكون المصادقة ناجحة وملف تعريف التفويض الصحيح الذي يتم دفعه.

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. إذا قمنا بتوصيل عميل بعد ذلك، فسيتم تعلم عنوان MAC الخاص به على منفذ محول AP في شبكة VLAN الخاصة بالعميل 232.

akshat_sw#sh mac address-table int g0/4
جدول عناوين MAC
—

منافذ نوع عنوان MAC لشبكة VLAN
— — — —
231 588d.0997.061d ساكن إستاتيكي gi0/4 - AP
232 c0ee.fbd7.8824 Dynamic Gi0/4 - العميل

على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، في تفاصيل العميل، يمكن ملاحظة أن هذا العميل ينتمي إلى شبكة VLAN رقم 232 ويتم توجيه SSID محليا. هنا قصاصة.

(وحدة التحكم من Cisco) >إظهار تفاصيل العميل c0:ee:fb:d7:88:24
عنوان MAC للعميل..... c0:ee:fb:d7:88:24
اسم مستخدم العميل ..... غير متوفر
عنوان MAC لنقطة الوصول..... b4:14:89:82:cb:90
اسم نقطة الوصول..... aks_desk_3502
معرف فتحة راديو AP.....1
حالة العميل..... تعاشرتن
مجموعة مستخدمي العميل.....
حالة NAC OOB للعميل..... وصول

معرف شبكة LAN اللاسلكية.................................2
اسم شبكة LAN اللاسلكية (SSID)................ Port-Auth
اسم ملف تعريف شبكة LAN اللاسلكية....................... Port-auth
نقطة فعالة (802.11u)................................ غير مدعومة
بي إس دي... b4:14:89:82:cb:9f
متصل ل .... 42 ثانية
القناة...44
عنوان IP...................................... 192.168.232.90
عنوان البوابة................................. 192.168.232.1
قناع الشبكة....................................... 255.255.255.0
معرف الاقتران.................................. 1
خوارزمية المصادقة........................ نظام مفتوح
رمز السبب..................................... 1
رمز الحالة..................................... 0

تحويل بيانات FlexConnect...................... محلي
حالة FlexConnect DHCP....................... محلي
تحويل مركزي قائم على شبكة VLAN بتقنية FlexConnect......... لا
مصادقة FlexConnect...................... سنترال
الارتباط المركزي عبر تقنية FlexConnect................. لا
اسم شبكة VLAN الخاصة بتقنية FlexConnect........................... VLAN 232
عزل شبكة VLAN.................................0
الوصول إلى شبكة VLAN.................................... 232
راج التوصيل المحلي لشبكة VLAN.............................232

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- إذا فشلت المصادقة، فاستخدم أوامر **debug dot1x**، **debug authentication**.
- إذا لم يتم نقل المنفذ إلى خط الاتصال، فأدخل الأمر **debug authentication feature autocfg all**.
- تأكد من تكوين وضع مضيف متعدد (وضع هوية صحة) (وضع مضيف متعدد). وضع المضيف المتعدد ينبغي تكون تمكنت in order to سمحت زبون اللاسلكي كامل عنوان.
- يجب تكوين الأمر "AAA authorization network" من أجل أن يقبل المحول السمات التي تم إرسالها بواسطة ISE وتطبيقها.

تدعم نقاط الوصول المستندة إلى IOS من Cisco TLS 1.0 فقط. قد يتسبب ذلك في حدوث مشكلة إذا تم تكوين خادم RADIUS للسماح فقط بمصادقة TLS 1.2 802.1X

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).