Configurez pour sécuriser un switchport de Flexconnect AP avec le dot1x

Contenu

Introduction

Ce document décrit la configuration pour sécuriser des switchports où les Points d'accès de FlexConnect (AP) authentifient avec le dot1x utilisant le VSA de rayon de device-traffic-class=switch pour permettre le trafic des réseaux locaux Sans fil localement commutés (WLAN).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- FlexConnect sur le contrôleur Sans fil de réseau local (WLC)
- 802.1x sur des Commutateurs de Cisco
- Topologie d'authentification de frontière du réseau (ORDONNÉE)

Composants utilisés

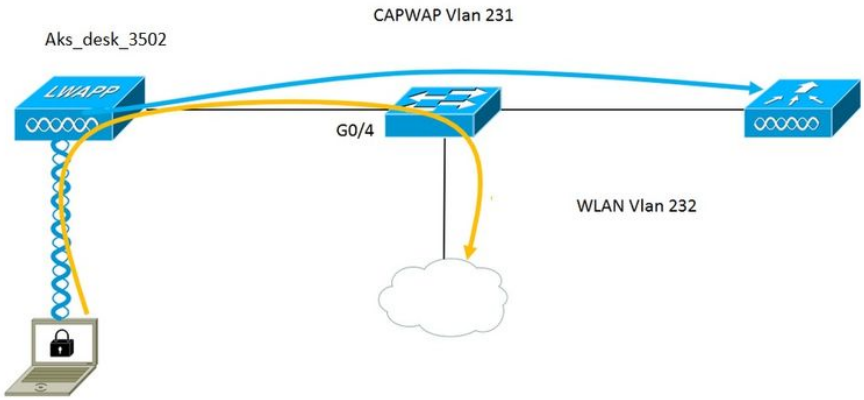
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0
- Engine de gestion d'identité (ISE) 2.0

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Diagramme du réseau



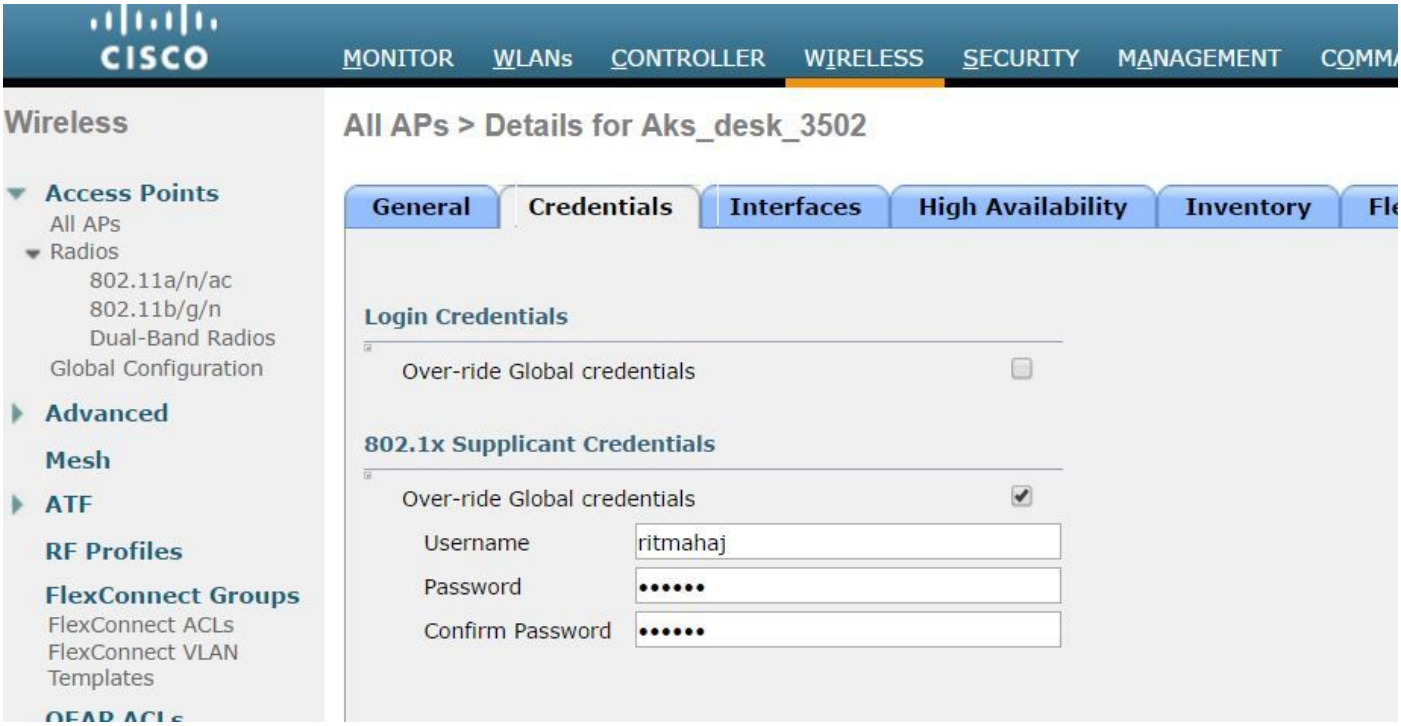
En cela installé le Point d'accès agit en tant que suppliant de 802.1x et est authentifié par le commutateur contre ISE utilisant l'EAP-FAST. Une fois le port est configuré pour l'authentification de 802.1x, le commutateur ne permet pas à n'importe quel trafic autre que le trafic de 802.1x pour traverser le port jusqu'à ce que le périphérique connecté au port authentifie avec succès.

Une fois que le Point d'accès authentifie avec succès contre ISE, le commutateur device-traffic-class=switch reçoit de Cisco VSA attribut « et il déplace automatiquement le port au joncteur réseau.

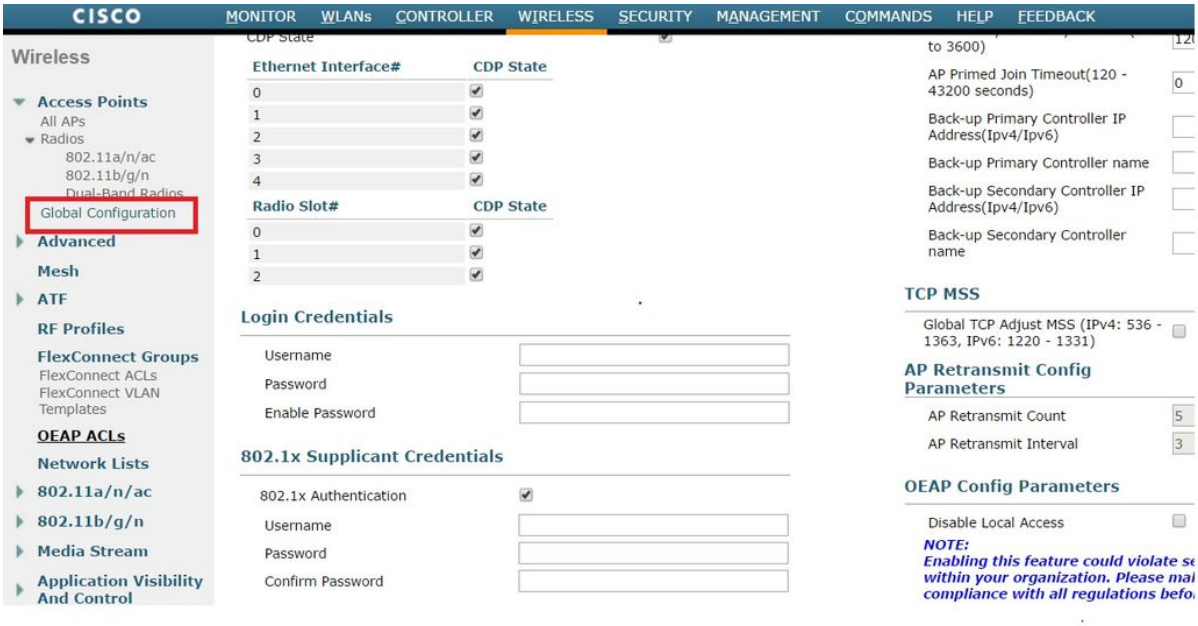
Ce des moyens, si AP prend en charge le mode de FlexConnect et a localement commuté le SSID configuré, il pourra envoyer le trafic étiqueté. Assurez-vous que le support de VLAN est activé sur AP et le VLAN indigène correct est configuré.

Configuration AP : -

1. Si AP est déjà joint au WLC, allez l'onglet sans fil et cliquez sur en fonction le Point d'accès. Allez le champ de Credetials et le nder les qualifications de suppliant de 802.1x se dirigeant, cochent la case **globale de qualifications de priorité** pour placer le nom d'utilisateur et mot de passe de 802.1x pour ce Point d'accès.



Vous pouvez également placer un nom d'utilisateur et mot de passe de comman pour tous les Points d'accès qui sont joints au WLC avec le menu de configuration globale.



2. Si le Point d'accès n'a pas joint un WLC encore, vous devez consoler dans le RECOUVREMENT pour placer les qualifications et pour utiliser cette commande CLI :

Console cli de capwap de LAP#debug
<password> de mot de passe de <username> de nom d'utilisateur de dot1x de LAP#capwap AP

Configuration de commutateur : -

1. Activez le dot1x sur le commutateur globalement et ajoutez le serveur ISE pour commuter

aaa new-model

!
rayon d'aaa authentication dot1x default group

!
rayon de groupe par défaut d'aaa authorization network

!

dot1x system-auth-control

!

serveur ISE de rayon
acct-port 1646 du l'authentique-port 1645 de 10.48.39.161 d'address ipv4
 clé 7 123A0C0411045D5679

2. Configurez maintenant le port de commutateur AP

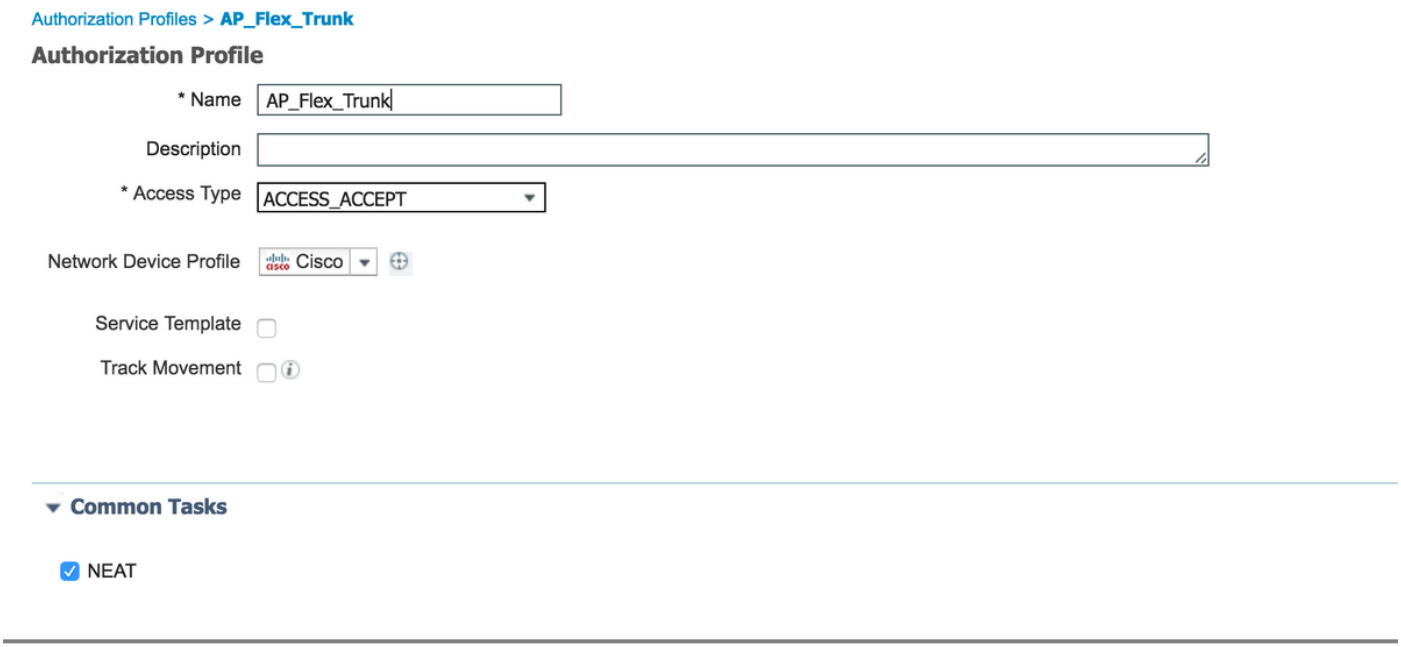
interface GigabitEthernet0/4
switchport access vlan 231
switchport trunk allowed vlan 231,232
switchport mode access
arrêt
multi-hôte d'authentication host-mode
dot1x d'authentication order
automatique d'authentication port-control
authentificateur de dot1x pae
périphérie de spanning-tree portfast

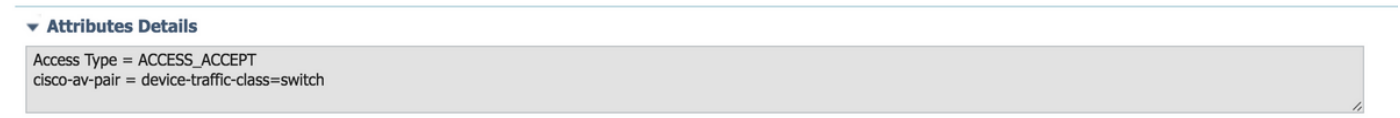
Si on veut configurer le MAB au lieu du dot1x puis le config de port ressemble à : -

interface GigabitEthernet0/4
switchport access vlan 231
switchport trunk allowed vlan 231,232
switchport mode access
arrêt
multi-hôte d'authentication host-mode
mab d'authentication order
automatique d'authentication port-control
mab
périphérie de spanning-tree portfast

Configuration ISE : -

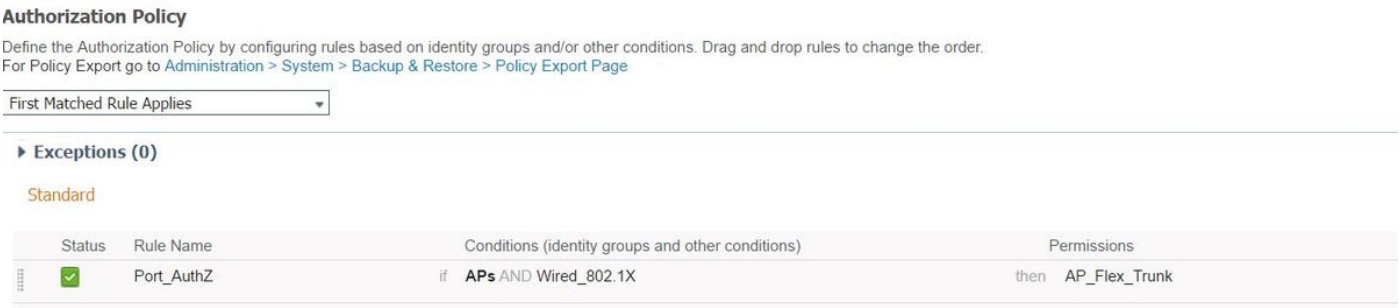
1. Sur ISE, on peut simplement activer ORDONNÉ pour le profil d'autorisation AP afin de placer l'attribut correct, cependant, sur d'autres serveurs de RAYON, vous pouvez configurer manuellement.





2. Sur ISE, on doit également configurer la stratégie de stratégie d'authentification et d'autorisation. Dans ce cas nous frappons la règle d'authentification par défaut qui est MAB de câble dot.1x(wired en cas de MAB) mais on peut le personnaliser selon la condition requise.

Quant à la stratégie d'autorisation (Port_AuthZ), dans ce cas nous avons ajouté les qualifications AP à un groupe d'utilisateurs (aps) et avons poussé le profil d'autorisation (AP_Flex_Trunk) basé sur ceci.



Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

1. Sur le commutateur, une fois peut utiliser la commande « autocfg tout de caractéristique de debug authentication » de vérifier si le port est déplacé au port de joncteur réseau ou pas.

20 février 12:34:18.119 : %LINK-3-UPDOWN : Interface GigabitEthernet0/4, état modifié à
20 février 12:34:19.122 : %LINEPROTO-5-UPDOWN : Line protocol on Interface GigabitEthernet0/4, état modifié à
akshat_sw#
akshat_sw#
20 février 12:38:11.113 : AUTHENTIC-FEAT-AUTOCFG-EVENT : Dans le start_fn d'AutoCfg de

dot1x, epm_handle : 3372220456
20 février 12:38:11.113 : AUTHENTIC-FEAT-AUTOCFG-EVENT : [588d.0997.061d, type de périphérique Gi0/4] = commutateur
20 février 12:38:11.113 : AUTHENTIC-FEAT-AUTOCFG-EVENT : [588d.0997.061d, nouveau client Gi0/4]
20 février 12:38:11.113 : AUTHENTIC-FEAT-AUTOCFG-EVENT : État interne d'application [Gi0/4] Autocfg macro : 1
20 février 12:38:11.113 : AUTHENTIC-FEAT-AUTOCFG-EVENT : Type de périphérique [Gi0/4] : 2
20 février 12:38:11.113 : AUTHENTIC-FEAT-AUTOCFG-EVENT : Auto-config [Gi0/4] : le stp a le port_config 0x85777D8
20 février 12:38:11.113 : AUTHENTIC-FEAT-AUTOCFG-EVENT : Auto-config [Gi0/4] : le port_config de stp a le guard_config 2 de bpdu
20 février 12:38:11.116 : AUTHENTIC-FEAT-AUTOCFG-EVENT : [Gi0/4] appliquant l'automatique-cfg sur le port.
20 février 12:38:11.116 : AUTHENTIC-FEAT-AUTOCFG-EVENT : VLAN [Gi0/4] : VLAN-streptocoque 231 : 231
20 février 12:38:11.116 : AUTHENTIC-FEAT-AUTOCFG-EVENT : [Gi0/4] appliquant la macro-instruction dot1x_autocfg_supp
20 février 12:38:11.116 : Appliquant la commande… 'aucun switchport access vlan 231' à Gi0/4
20 février 12:38:11.127 : Appliquant la commande… « aucun switchport nonegotiate » à Gi0/4
20 février 12:38:11.127 : Appliquant la commande… « switchport mode trunk » à Gi0/4
20 février 12:38:11.134 : Appliquant la commande… 'switchport trunk native vlan 231' à Gi0/4
20 février 12:38:11.134 : Appliquant la commande… « joncteur réseau de spanning-tree portfast » à Gi0/4
20 février 12:38:12.120 : %LINEPROTO-5-UPDOWN : Line protocol on Interface GigabitEthernet0/4, état modifié à vers le bas
20 février 12:38:15.139 : %LINEPROTO-5-UPDOWN : Line protocol on Interface GigabitEthernet0/4, état modifié à

2. La sortie du « passage international g0/4" d'exposition prouvera que le port a changé à un port de joncteur réseau.

Configuration en cours : 295 octets
!
interface GigabitEthernet0/4
switchport trunk allowed vlan 231,232,239
switchport trunk native vlan 231
switchport mode trunk
multi-hôte d'authentication host-mode
dot1x d'authentication order
automatique d'authentication port-control
authentificateur de dot1x pae
joncteur réseau de périphérie de spanning-tree portfast
extrémité

3. Sur ISE, sous Operations>>Radius Livelogs un pouvons nous l'authentification étant réussie et le profil correct d'autorisation étant poussé.

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. Si nous connectons un client après que ceci alors son MAC address soit appris sur le port de commutateur AP dans le VLAN 232 de client.

adresse-table international g0/4 de MAC d'akshat_sw#sh
Tableau de MAC address

Ports de type de MAC address de VLAN
---- ----------- -------- -----
231 588d.0997.061d Gi0/4 STATIQUES - AP
232 c0ee.fbd7.8824 Gi0/4 DYNAMIQUES - Client

Sur le WLC, dans le petit groupe de client il peut voir que ce client appartient le VLAN 232 et le SSID est localement commuté. Voici un extrait.

Petit groupe c0:ee:fb:d7:88:24 de client de >show (de contrôleur de Cisco)
Adresse MAC ..... c0:ee:fb:d7:88:24 de client
NON APPLICABLE de nom d'utilisateur de client .....
Adresse MAC ..... b4:14:89:82:cb:90 AP
Nom AP ..... Aks_desk_3502
Id d'emplacement de radio AP 1
État de client ..... Associé
Groupe d'utilisateurs de client .....
État du client NAC OOB ..... Access
Id Sans fil de RÉSEAU LOCAL 2
Nom de réseau LAN sans fil (SSID) ..... Port-Auth
Nom Sans fil de profil LAN ..... Port-auth
Point névralgique (802.11u) ..... Non pris en charge
BSSID b4:14:89:82:cb:9f
Connecté pendant ..... 42 sec
La Manche 44
Adresse IP 192.168.232.90
Adresse de passerelle 192.168.232.1
Netmask 255.255.255.0
Id d'association 1
Algorithme d'authentification ..... Système ouvert
Code de raison 1
Code d'état 0

Commutateur de données de FlexConnect ..... Gens du pays
État DHCP de FlexConnect ..... Gens du pays
Le VLAN de FlexConnect a basé la commutation centrale ..... Non
Authentification de FlexConnect ..... Central
Association centrale de FlexConnect ..... Non
VLAN 232 de NOM de FlexConnect VLAN .....
Quarantaine VLAN 0
Access VLAN 232
VLAN traversier local 232

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

- Si l'authentification échoue, le **debug dot1x d'**utilisation, **debug authentication** commande.
- Si le port n'est pas déplacé au joncteur réseau, écrivez l'**autocfg de caractéristique de debug authentication toute la** commande.
- Assurez que vous faites configurer le mode de multi-hôte (multi-hôte d'authentication host-mode). Le Multi-hôte doit être activé afin de permettre des adresses de MAC sans fil de client.
- la commande de « aaa authorization network » devrait être configurée pour que le commutateur reçoive et pour applique les attributs envoyés par ISE.