Affectation dynamique VLAN avec l'exemple du serveur ACS 5.2 de RAYON et de la configuration WLC

Contenu

Introduction

Ce document présente le concept d'affectation de VLAN dynamique. Il décrit également comment configurer le Contrôleur de réseau local sans fil (WLC) et un serveur RADIUS - le Serveur de contrôle d'accès (ACS) qui exécute la version 5.2 - afin d'affecter des clients de Réseau local sans fil (WLAN) à un VLAN spécifique de manière dynamique.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant que vous tentiez cette configuration :

- Ayez une connaissance de base du WLC et du Point d'accès léger (les recouvrements)
- Ayez une connaissance fonctionnelle du serveur d'AAA
- Ayez une connaissance complète des réseaux Sans fil et des problèmes de sécurité Sans fil

Composants utilisés

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

- Cisco 5508 WLC qui exécute la version de microprogramme 7.0.220.0
- RECOUVREMENT de gamme Cisco 3502
- Supplicant d'indigène de Microsoft Windows 7 avec la version 14.3 de gestionnaire d'Intel 6300-N
- Cisco Secure ACS qui exécute la version 5.2
- Commutateur de gamme Cisco 3560

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Affectation dynamique VLAN avec un serveur de RAYON

Dans la plupart des systèmes WLAN, chaque WLAN a une stratégie statique qui s'applique à tous les clients associés à un SSID (Service Set Identifier), ou WLAN dans la terminologie du contrôleur. Bien que puissante, cette méthode a des limitations parce qu'elle exige que les clients soient associés à des SSID différents afin d'hériter de QoS et de stratégies de sécurité différentes.

Cependant, la solution WLAN de Cisco prend en charge la mise en réseau d'identités. Ceci permet au réseau pour annoncer un SSID simple, mais permet aux utilisateurs spécifiques pour hériter de QoS différent, d'attributs VLAN, et/ou de stratégies de sécurité basées sur les identifiants utilisateurs.

L'affectation de VLAN dynamique est une fonction qui place un utilisateur sans fil dans un VLAN spécifique en fonction des informations fournies par l'utilisateur. Cette tâche d'assigner des utilisateurs à une particularité VLAN est gérée par un serveur d'authentification RADIUS, tel que le Cisco Secure ACS. Elle peut être utilisée, par exemple, pour permettre à l'hôte sans fil de rester sur le même VLAN alors qu'il se déplace au sein d'un réseau de campus.

En conséquence, quand les tentatives d'un client de s'associer à un RECOUVREMENT enregistré avec un contrôleur, le RECOUVREMENT passe les qualifications de l'utilisateur au serveur de RAYON pour la validation. Une fois que l'authentification est réussie, le serveur RADIUS passe certains attributs de l'Internet Engineering Task Force (IETF) à l'utilisateur. Ces attributs RADIUS décident de l'ID de VLAN qui doit être affecté au client sans fil. Le SSID (WLAN, en termes de WLC) du client n'importe pas parce que l'utilisateur est toujours affecté à cet ID de VLAN prédéterminé.

Les attributs d'utilisateur RADIUS utilisés pour l'affectation de l'ID de VLAN sont :

- IETF 64 (type de tunnel) - Placez ceci au **VLAN**.
- IETF 65 (type de support de tunnel) - placez ceci à **802**.
- IETF 81 (identification groupe privée de tunnel) - placez ceci à l'ID DE VLAN.

L'ID du VLAN est de 12 bits et prend une valeur entre 1 et 4 094, inclus. Puisque Tunnel-Private-Group-ID est de type chaîne, comme défini dans RFC2868 pour une utilisation avec IEEE 802.1X, la valeur entière de l'ID de VLAN est codée en tant que chaîne. Quand ces attributs de tunnel sont envoyés, il est nécessaire de renseigner la zone Tag.

Comme observé dans RFC2868 , section 3.1 : **La zone Tag a une longueur d'un octet et sa fonction est de fournir un moyen de regrouper les attributs dans le même paquet qui fait référence au même tunnel.** Les valeurs valides pour cette zone sont comprises entre 0x01 et 0x1F, inclus. Si la zone Tag est inutilisée, elle doit avoir pour valeur zéro (0x00). Référez-vous à RFC 2868 pour plus d'informations sur tous les attributs RADIUS.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Note: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Voici les détails de configuration des composants utilisés dans ce diagramme :

- L'adresse IP du serveur ACS (RAYON) est 192.168.150.24.
- L'adresse d'interface de Gestion et d'AP-gestionnaire du WLC est 192.168.75.44.
- L'adresse 192.168.150.25 de serveurs DHCP.
- VLAN 253 et VLAN 257 sont utilisés dans toute cette configuration. Student-1 est configuré pour le placement dans VLAN 253 et Teacher-1 est configuré pour le placement dans VLAN 257 par le serveur de RAYON quand les deux utilisateurs se connectent au même SSID « goa ».VLAN 253 : 192.168.153.x/24. Passerelle : 192.168.153.1VLAN 257 : 192.168.157.x/24. Passerelle : 192.168.157.1VLAN 75 : 192.168.75.x/24. Passerelle : 192.168.75.1
- Ce document utilise le 802.1x avec le PEAP comme mécanisme de sécurité.**Note**: Cisco vous recommande d'utiliser des méthodes d'authentification avancées, telles que l'authentification EAP-FAST et EAP-TLS, afin de sécuriser le WLAN.

Suppositions

- Des Commutateurs sont configurés pour toute la couche 3 VLAN.
- Le serveur DHCP est assigné une portée de DHCP.
- La Connectivité de la couche 3 existe entre tous les périphériques dans le réseau.
- Le RECOUVREMENT est déjà joint au WLC.
- Chaque VLAN a le masque de /24.
- ACS 5.2 a un certificat Auto-signé installé.

Étapes de configuration

Cette configuration est séparée dans trois étapes de haut niveau :

1. Configurez le serveur de RAYON.
2. Configurez le WLC.
3. Configurez l'utilitaire de client sans fil.

Configurez le serveur de RAYON

La configuration du serveur de RAYON est divisée en quatre étapes :

1. Ressources en configure network.
2. Configurez les utilisateurs.
3. Définissez les éléments de stratégie.
4. Appliquez les stratégies d'accès.

ACS 5.x est un système basé sur la politique de contrôle d'accès. C'est-à-dire, ACS 5.x utilise un modèle basé sur les règles de stratégie au lieu du modèle basé sur groupe utilisé dans les versions 4.x.

Le modèle basé sur les règles de stratégie ACS 5.x fournit un contrôle d'accès plus puissant et plus flexible comparé à l'approche basée sur groupe plus ancienne.

Dans le modèle basé sur groupe plus ancien, un groupe définit la stratégie parce qu'elle contient et attache ensemble trois types d'informations :

- Les informations d'identité - Ces informations peuvent être basées sur l'adhésion dans des groupes d'AD ou de LDAP ou une affectation statique pour les utilisateurs internes ACS.
- D'autres restrictions ou conditions - Restrictions temporelles, restrictions de périphérique, et ainsi de suite.
- Autorisations - Niveaux de privilège VLAN ou de Cisco IOS®.

Le modèle de stratégie ACS 5.x est basé sur des règles de la forme :

- Si la condition résultent alors

Par exemple, nous utilisons les informations décrites pour le modèle basé sur groupe :

- S'identité-état, autorisation-profil de restriction-état puis.

En conséquence, ceci nous donne la flexibilité de limiter dans quelles conditions l'utilisateur est permis pour accéder au réseau aussi bien que quelles niveau d'autorisation est permis quand des

conditions spécifiques sont remplies.

Ressources en configure network

Cette procédure explique comment ajouter le WLC comme client AAA sur le serveur RADIUS de sorte que le WLC puisse passer les informations d'identification des utilisateurs au serveur RADIUS.

Procédez comme suit :

1. Du GUI ACS, allez aux **ressources de réseau >** aux **groupes de périphériques réseau >** à l'**emplacement**, et le clic **créent** (au bas).
2. Ajoutez les champs requis, et cliquez sur Submit.Vous verrez maintenant cet écran :
3. **Le type de périphérique de** clic **> créent**.
4. Cliquez sur **Submit**. Vous verrez maintenant cet écran :
5. Allez aux **ressources de réseau >** aux **périphériques de réseau et aux clients d'AAA**.
6. Le clic **créent**, et complètent les détails comme affiché ici :
7. Cliquez sur **Submit**. Vous verrez maintenant cet écran :

Configurer des utilisateurs

Dans cette section, vous créerez des utilisateurs locaux sur ACS (Student-1 et Teacher-1). Student-1 est assigné au groupe de « étudiants » et Teacher-1 est assigné au groupe de « professeurs ».

1. Allez aux **utilisateurs et l'identité enregistre >** des **groupes d'identité > créent**.
2. Une fois que vous cliquez sur Submit, la page ressemblera à ceci :
3. Créez et assignez à des utilisateurs Student-1 et Teacher-1 à leurs groupes respectifs.
4. **Les utilisateurs et l'identité de** clic **enregistre > identité groupe >** des **utilisateurs > créent**.
5. De même, créez Teacher-1.L'écran ressemblera à ceci :

Définissez les éléments de stratégie

Terminez-vous ces étapes afin de définir des attributs IETF pour les utilisateurs :

1. Allez aux **éléments >** à l'**autorisation de stratégie et les autorisations >** les **profils d'accès au réseau >** d'**autorisation > créent**.
2. De l'onglet de fonctionnalités usuelles :
3. Ajoutez ces attributs IETF :Tunnel-type = 64 = VLANTunnel-Support-type = 802Tunnel-Private-Group-ID = 253 (Student-1) et 257 (Teacher-1)Pour des étudiants de groupe :Pour des professeurs de groupe :
4. Une fois que les deux attributs sont ajoutés, l'écran ressemblera à ceci :

Appliquez les stratégies d'Access

Terminez-vous ces étapes afin de sélectionner que des méthodes d'authentification doivent être utilisé et comment les règles doivent être configurées (basé sur les étapes précédentes) :

1. Allez à **Access les stratégies >** les **services d'accès >** l'**accès au réseau de par défaut >**

éditent : « Accès au réseau par défaut ».
2. Sélectionnez que la méthode d'EAP vous comme les clients sans fil authentifierait. Dans cet exemple, nous utilisons **PEAP- MSCHAP-V2**.
3. Cliquez sur **Submit**.
4. Vérifiez le groupe d'identité que vous avez sélectionné. Dans cet exemple, nous utilisons les **utilisateurs internes**, que nous avons créés sur ACS. **Sauvegardez les** modifications.
5. Afin de vérifier le profil d'autorisation, allez à **Access les stratégies** > les **services d'accès** > l'**accès au réseau** > l'**autorisation de par défaut**.Vous pouvez personnaliser dans quelles conditions vous permettrez à accès client au réseau et quelles profil d'autorisation (attributs) vous passerez une fois authentifié. Cette finesse est seulement disponible dans ACS5.x. Dans cet exemple, nous site sélectionné, **type de périphérique**, **Protocol**, **groupe d'identité**, et **méthode d'authentification EAP**.
6. Cliquez sur OK, et **sauvegardez les modifications**.
7. L'étape suivante est de créer une règle. Si aucune règle n'est définie, on ne permet au client l'accès sans aucune condition.Le clic **créent** > **Rule-1**. Cette règle est pour Student-1.
8. De même, créez une règle pour Teacher-1. **Modifications de sauvegarde de** clic.L'écran ressemblera à ceci :
9. Nous définirons maintenant des règles de sélection de service. Employez cette page afin de configurer une stratégie simple ou basée sur les règles pour déterminer quel service à s'appliquer aux demandes en entrée. Dans cet exemple, une stratégie basée sur les règles est utilisée.

Configurez le WLC

Cette configuration requiert les étapes suivantes :

1. Configurez le WLC avec les coordonnées du serveur d'authentification.
2. Configurez les interfaces dynamiques (VLAN).
3. Configurez les WLAN (SSID).

Configurer le WLC avec les détails du serveur d'authentification

Il est nécessaire de configurer le WLC ainsi il peut communiquer avec le serveur de RAYON afin d'authentifier les clients, et également pour toutes les autres transactions.

Procédez comme suit :

1. Dans l'interface graphique du contrôleur, cliquez sur **Security**.
2. Entrez l'adresse IP du serveur RADIUS et la clé Shared Secret utilisée entre le serveur RADIUS et le WLC.Cette clé secrète partagée devrait être identique que celle configurée dans le serveur de RAYON.

Configurer les interfaces dynamiques (VLAN)

Cette procédure décrit comment configurer des interfaces dynamiques sur le WLC. Comme expliqué plus tôt dans ce document, l'ID de VLAN spécifié sous l'attribut Tunnel-Private-Group ID du serveur RADIUS doit également exister dans le WLC.

Dans l'exemple, Student-1 est spécifié avec l'**ID de Tunnel-Privé-groupe de 253 (VLAN =253)** sur le serveur de RAYON. De même, Teacher-1 est spécifié avec l'**ID de Tunnel-Privé-groupe de 257 (VLAN =257)** sur le serveur de RAYON. Voyez la section d'IETF RADIUS Attributes de la fenêtre d'installation utilisateur.

Procédez comme suit :

1. L'interface dynamique est configurée du GUI de contrôleur, dans la fenêtre de **Controller > Interfaces**.
2. Cliquez sur **Apply**.Ceci vous porte à la fenêtre d'éditer de cette interface dynamique (VLAN 253 ici).
3. Entrez l'adresse IP et la passerelle par défaut de cette interface dynamique.
4. Cliquez sur **Apply**.
5. De même, nous créerons une interface dynamique pour VLAN 257 pour Teacher-1.
6. Les interfaces configurées configurées ressembleront à ceci :

Configurer les WLAN (SSID)

Terminez-vous ces étapes afin de configurer les WLAN dans le WLC :

1. Du GUI de contrôleur, allez à des **WLAN > créent nouveau** afin de créer un nouveau WLAN. La fenêtre New WLANs est affichée.
2. Entrez l'ID de WLAN et le SSID du WLAN.Vous pouvez écrire n'importe quel nom comme WLAN SSID. Cet exemple utilise le **goa** comme WLAN SSID.
3. Cliquez sur Apply afin d'aller à la fenêtre d'éditer du goa WLAN.
4. Activez l'option d'**Allow AAA Override** dans le contrôleur pour chaque WLAN (SSID) configuré. L'option d'Allow AAA Override d'un WLAN te permet pour configurer le WLAN pour le réseau d'identité. Il te permet pour s'appliquer l'étiquetage, le QoS, et l'ACLs VLAN à différents clients basés sur les attributs RADIUS retournés à partir du serveur d'AAA. Dans cet exemple, il est utilisé afin d'assigner un VLAN aux clients.La majeure partie de la configuration pour permettre le dépassement d'AAA est faite au serveur de RAYON. L'activation de ce paramètre permet au contrôleur pour recevoir les attributs retournés par le serveur de RAYON. Le contrôleur s'applique alors ces attributs à ses clients.**Note**: Quand le groupe d'interface est tracé à un WLAN et aux clients se connectent au WLAN, le client n'obtient pas l'adresse IP d'une mode de recherche séquentielle. Le dépassement d'AAA avec le groupe d'interface n'est pas pris en charge.

Configurez l'utilitaire de client sans fil

Dans notre client de test, nous utilisons le suppliant indigène de Windows 7 avec une carte d'Intel 6300-N exécutant la version de 14.3 gestionnaires. Il est recommandé pour tester utilisant les derniers gestionnaires des constructeurs.

Terminez-vous ces étapes afin de créer un profil dans le config de Windows Zero (WZC) :

1. Allez au **panneau de configuration** > au **réseau et l'Internet > gèrent des réseaux sans fil**.
2. Cliquez sur l'onglet d'**ajouter**.
3. Le clic **créent manuellement un profil réseau**.

4. Ajoutez les détails comme configurés sur le WLC.**Note**: Le SSID distingue les majuscules et minuscules.
5. Cliquez sur **Next** (Suivant).
6. **Paramètres de connexion de modification de** clic afin de revérifier les configurations.
7. Dans cet exemple, nous ne validons pas le certificat de serveur. Si vous cochez cette case et ne pouvez pas connecter, essayer désactiver la caractéristique et le test de nouveau.
8. Alternativement, vous pouvez employer vos qualifications de Windows afin d'ouvrir une session. Cependant, dans cet exemple nous n'allons pas utiliser cela. Cliquez sur **OK**.
9. **Paramètres avancés de** clic afin de configurer le nom d'utilisateur et mot de passe.
10. Une fois que vous avez fini de tester Student-1, testez Teacher-1. Cliquez sur **OK**.

Votre utilitaire client est maintenant prêt à se connecter.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Vérifiez Student-1

Du GUI WLC, allez au **Monitor > Clients**, et sélectionnez l'adresse MAC.

Stats de RAYON WLC :

```
(Cisco Controller) >show radius auth statistics
Authentication Servers:
Server Index..................................... 1
Server Address................................... 192.168.150.24
Msg Round Trip Time.............................. 1 (msec)
First Requests................................... 8
Retry Requests................................... 0
Accept Responses................................. 1
Reject Responses................................. 0
Challenge Responses.............................. 7
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

Logs ACS :

1. Terminez-vous ces étapes afin de visualiser les nombres de hits :Si vous vérifiez les logs dans un délai de 15 minutes d'authentification, veillez-vous pour régénérer le nombre de hits.Vous avez un onglet pour le **nombre de hits** en bas de la même page.
2. **La surveillance de** clic **et les états** et une nouvelle fenêtre externe apparaît. Allez aux **authentifications – Rayon – Aujourd'hui**. Vous pouvez également cliquer sur les **détails** afin de vérifier qui entretiennent la règle de sélection étaient appliqués.

Vérifiez Teacher-1

Du GUI WLC, allez au **Monitor > Clients**, et sélectionnez l'adresse MAC.

Logs ACS :

1. Terminez-vous ces étapes afin de visualiser les nombres de hits :Si vous vérifiez les logs dans un délai de 15 minutes d'authentification, veillez-vous pour régénérer le nombre de hits.Vous avez un onglet pour le **nombre de hits** en bas de la même page.
2. **La surveillance de** clic **et les états** et une nouvelle fenêtre externe apparaît. Allez aux **authentifications – Rayon – Aujourd'hui**. Vous pouvez également cliquer sur les **détails** afin de vérifier qui entretiennent la règle de sélection étaient appliqués.

Dépannez

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

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Note: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

1. Si vous rencontrez n'importe quels problèmes, émettez ces commandes sur le WLC :**mettez au point le client que le** *<mac ajoutent du client>***debug aaa all enable***addr> de <mac de* ***show client detail*** - Vérifiez l'état de gestionnaire de stratégie.**show radius auth statistics** - Vérifiez la raison de panne.**debug disable-all** - Arrêtez met au point.statistiques **authentiques de** rayon de **fin d'alerte de clear stats radius** sur le WLC.
2. Vérifiez les logins l'ACS et notez la raison de panne.

Informations connexes

- Affectation dynamique VLAN avec le serveur ACS 4.1 de RAYON et l'exemple Sans fil de configuration de contrôleur LAN
- Support et documentation techniques - Cisco Systems