Configuration de la fonctionnalité de secours du serveur RADIUS sur les contrôleurs LAN sans fil

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Fonction de secours du serveur RADIUS
  - Modes de secours
    - Mode actif
    - Mode passif
    - Mode arrêt
- Configurer
  - Configuration de la fonction de secours du serveur RADIUS avec l'interface de ligne de commande
  - Configuration de la fonction de secours du serveur RADIUS avec l'interface utilisateur graphique
- Vérifier
- Dépannage
- Informations connexes

Introduction

Ce document décrit comment configurer la fonctionnalité de secours du serveur RADIUS avec des contrôleurs LAN sans fil (WLC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de la configuration des points d'accès légers (LAP) et des WLC Cisco
- Connaissances de base sur le contrôle et le provisionnement du protocole CAPWAP (Wireless Access Point Protocol)
- Connaissances de base des solutions de sécurité sans fil

Composants utilisés

Les informations contenues dans ce document sont basées sur un contrôleur Cisco 5508/5520.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Fonction de secours du serveur RADIUS

Les versions du logiciel WLC antérieures à la version 5.0 ne prennent pas en charge le mécanisme de secours du serveur RADIUS. Lorsque le serveur RADIUS principal devient indisponible, le WLC bascule vers le prochain serveur RADIUS de sauvegarde active. Le WLC continuera à utiliser le serveur RADIUS secondaire pour toujours, même si le serveur principal est disponible. En général, le serveur principal est hautes performances et le serveur préféré.

Dans WLC 5.0 et versions ultérieures, le WLC prend en charge la fonctionnalité de secours du serveur RADIUS. Avec cette fonctionnalité, le WLC peut être configuré pour vérifier si le serveur principal est disponible et rebascule vers le serveur RADIUS principal une fois qu'il est disponible. Pour ce faire, le WLC prend en charge deux nouveaux modes, passive et active, afin de vérifier l'état du serveur RADIUS. Le WLC revient au serveur le plus préférable après la valeur de délai d'attente spécifiée.

Modes de secours

Mode actif

En mode actif, lorsqu'un serveur ne répond pas à la demande d'authentification WLC, le WLC marque le serveur comme étant mort, puis déplace le serveur vers le pool de serveurs non actifs et commence à envoyer des messages d'analyse périodiquement jusqu'à ce que ce serveur réponde. Si le serveur répond, alors le WLC déplace le serveur mort vers le pool actif et arrête d'envoyer des messages de sonde. Dans ce mode, lorsqu'une demande d'authentification arrive, le WLC choisit toujours le serveur d'index le plus bas (priorité la plus élevée) dans le pool actif de serveurs RADIUS.

Le WLC envoie un paquet de sonde après le délai d'attente (la valeur par défaut est 300 secondes) afin de déterminer l'état du serveur au cas où le serveur ne répondrait pas plus tôt.

Mode passif

En mode passif, si un serveur ne répond pas à la demande d'authentification WLC, le WLC déplace le serveur vers la file d'attente inactive et définit un compteur. Lorsque le minuteur expire, le WLC déplace le serveur vers la file d'attente active indépendamment de l'état réel du serveur. Lorsqu'une demande d'authentification arrive, le WLC choisit le serveur d'index le plus bas (priorité la plus élevée) dans la file d'attente active (qui peut inclure le serveur non actif). Si le serveur ne répond pas, alors le WLC le marque comme inactif, définit le minuteur et passe au

serveur de priorité la plus élevée suivante. Ce processus continue jusqu'à ce que le WLC trouve un serveur RADIUS actif ou que le pool de serveurs actif soit épuisé.

Le WLC suppose que le serveur est actif après le délai d'attente (la valeur par défaut est 300 secondes) au cas où le serveur ne répondrait pas plus tôt. S'il ne répond toujours pas, le WLC attend un autre délai d'attente et réessaie lorsqu'une demande d'authentification arrive.

Mode arrêt

En mode arrêt, le WLC prend uniquement en charge le basculement. En d'autres termes, la reprise est désactivée. Lorsque le serveur RADIUS principal tombe en panne, le WLC bascule vers le prochain serveur RADIUS de sauvegarde active. Le WLC continue d'utiliser le serveur RADIUS secondaire pour toujours, même si le serveur principal est disponible.

Configurer

Configuration de la fonction de secours du serveur RADIUS avec l'interface de ligne de commande

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

Utilisez ces commandes de l'interface de ligne de commande du WLC afin d'activer la fonctionnalité de secours du serveur RADIUS sur le WLC.

La première étape consiste à sélectionner le mode de reprise du serveur RADIUS. Comme mentionné précédemment, le WLC prend en charge les modes actif et passif de secours.

Afin de sélectionner le mode de secours, entrez cette commande :

```
<#root>

WLC1 >

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

- active : envoie des sondes aux serveurs inactifs pour tester l'état.
- passive : définit l'état du serveur en fonction de la dernière transaction.
- off : désactive le test de secours du serveur (par défaut).

L'étape suivante consiste à sélectionner l'intervalle qui spécifie l'intervalle de sonde pour le mode actif ou le temps inactif pour les modes passifs de fonctionnement.

Afin de définir l'intervalle, entrez cette commande :

<#root>

```
WLC1 >
```

config radius fallback-test mode interval *{180 - 3600}*

<180 to 3600> - Entrez l'intervalle d'analyse ou la durée d'inactivité en secondes (la valeur par défaut est 300 secondes).

L'intervalle spécifie l'intervalle d'analyse dans le cas d'une reprise en mode actif ou le temps d'inactivité dans le cas d'une reprise en mode passif.

Pour le mode de fonctionnement actif, vous devez configurer un nom d'utilisateur qui sera utilisé dans la demande d'analyse envoyée au serveur RADIUS.

Afin de configurer le nom d'utilisateur, entrez cette commande :

<#root>

```
WLC1 >
```

config radius fallback-test username *{username}*

<username> : saisissez un nom comportant jusqu'à 16 caractères alphanumériques (la valeur par défaut est cisco-probe).

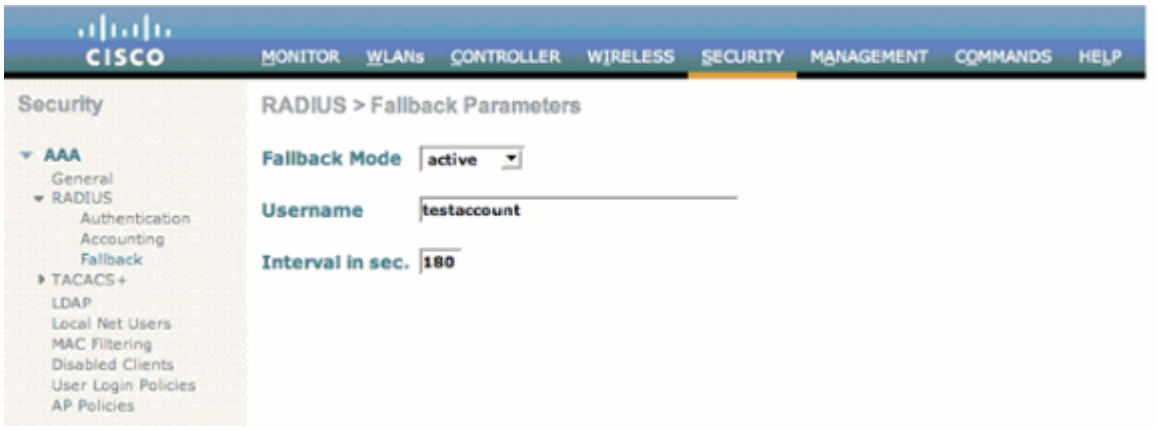
Remarque : Vous pouvez saisir votre propre nom d'utilisateur ou le conserver par défaut. Le nom d'utilisateur par défaut est « cisco-probe ». Étant donné que ce nom d'utilisateur est utilisé pour envoyer des messages d'analyse, vous n'avez pas besoin de configurer de mot de passe.

Configuration de la fonction de secours du serveur RADIUS avec l'interface utilisateur graphique

Complétez ces étapes afin de configurer le WLC avec l'interface graphique utilisateur :

1. Configurez le mode de reprise du serveur RADIUS. Pour ce faire, sélectionnez Security > RADIUS > Fallback dans l'interface graphique du WLC. La page RADIUS > Fallback Parameters s'affiche.
2. Dans la liste déroulante Fallback Mode, sélectionnez le mode de secours. Les options disponibles sont active, passive et off.

   Voici un exemple de capture d'écran pour la configuration du mode de secours actif comme illustré dans l'image.



3. Pour le mode de fonctionnement actif, saisissez le nom d'utilisateur dans le champ username.

4. Entrez la valeur de l'intervalle d'analyse dans le champ Interval in sec. champ.

5. Cliquez sur Apply.

Si la fonctionnalité de basculement agressif est activée dans le WLC, le WLC est trop agressif pour marquer le serveur AAA comme « ne répondant pas ». Cependant, cela ne devrait pas être fait parce que le serveur AAA ne répond peut-être pas seulement à ce client particulier si vous ne supprimez silencieusement. Il peut s'agir d'une réponse à d'autres clients valides avec des certificats valides. Le WLC peut toujours marquer le serveur AAA comme « ne répond pas » et « ne fonctionne pas ».

Pour remédier à ce problème, désactivez la fonctionnalité de basculement agressif. Entrez la commande config radius agressif-failover disable à partir de l'interface graphique du contrôleur afin d'effectuer ceci. Si cette option est désactivée, le contrôleur bascule vers le serveur AAA suivant uniquement si trois clients consécutifs ne reçoivent pas de réponse du serveur RADIUS.

Remarque : Changement de fonctionnalité introduit dans les versions 8.5.140,8.8.100,8.10.105 et ultérieures : Lorsque le basculement agressif RADIUS pour le contrôleur est désactivé : Le paquet est retenté six fois, sauf en cas d'abandon de la part des clients. Le serveur RADIUS (à la fois AUTH et ACCT) est marqué comme inaccessible après trois événements de délai d'attente (18 tentatives consécutives) de plusieurs clients (auparavant, de trois clients exactement). Lorsque le basculement agressif RADIUS pour le contrôleur est activé : Le paquet est retenté six fois, sauf en cas d'abandon de la part des clients. Le serveur RADIUS (à la fois AUTH et ACCT) est marqué comme inaccessible après un événement de délai d'attente (6 tentatives consécutives) provenant de plusieurs clients (auparavant, provenant exactement d'un client). Cela signifie que 18 tentatives consécutives par serveur RADIUS (AUTH ou ACCT) peuvent provenir de plusieurs clients. Par conséquent, il n'est pas toujours garanti que chaque paquet sera retenté six fois.

Vérifier

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

L'outil Output Interpreter Tool (Registered Customers only) (OIT) prend en charge certaines commandes show. Utilisez l'OIT afin d'afficher une analyse du résultat de la commande show.

Entrez la commande show radius summary afin de vérifier votre configuration de secours. Voici un exemple :

```
<#root>

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
```

Dépannage

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

Remarque : Référez-vous aux informations importantes sur les commandes de débogage

avant d'utiliser les commandes de débogage.

- debug dot1x events enable - Configure les débogages des événements 802.1X.
- debug aaa events enable - Configure les débogages de tous les événements AAA.

Informations connexes

- Exemple de configuration de l'authentification EAP avec des contrôleurs WLAN (WLC)
- Enregistrement d'un point d'accès léger (LAP) sur un contrôleur LAN sans fil (WLC)
- Configuration des solutions de sécurité
- Exemple de configuration de l'affectation dynamique de VLAN avec le serveur RADIUS et le contrôleur LAN sans fil
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.