Empêcher les pales de fusion de réseau RADIUS sans fil à grande échelle

Contenu

Introduction

Ce document fournit un bref aperçu des directives de configuration de base pour les déploiements sans fil à grande échelle tels que le contrôleur LAN sans fil AireOS (WLC) avec RADIUS avec Cisco Identity Services Engine (ISE) ou Cisco Secure Access Control Server (ACS). Ce document fait référence à d'autres documents avec plus de détails techniques.

Symptômes observés

En général, les environnements universitaires sont confrontés à cet état de fusion AAA (Authentication, Authorization, and Accounting). Cette section décrit les symptômes/journaux habituels observés dans cet environnement.

1. Surveillance des performances RADIUS

Le client Dotx connaît un retard important avec de nombreuses tentatives d'authentification.

Utilisez la commande **show radius auth statistics** (GUI : **Monitor > Statistics > RADIUS Servers**) afin de rechercher des problèmes. Recherchez un grand nombre de tentatives, de rejets et de délais d'attente. Voici un exemple :

```
Server Index..................................... 2
Server Address................................... 192.168.88.1
Msg Round Trip Time.............................. 3 (msec)
First Requests................................... 1256
Retry Requests................................... 5688
Accept Responses................................. 22
Reject Responses................................. 1
```

```
Challenge Responses.............................. 96
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 1
Timeout Requests................................. 6824
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

Cherchez :

- Tentative élevée : Taux de première demande (ne doit pas dépasser 10 %)
- Refus élevé : Taux d'acceptation
- Délai d'attente élevé : Taux de première demande (ne doit pas dépasser 5 %)

En cas de problème, recherchez :

- Clients mal configurés
- Problèmes d'accessibilité du réseau entre le WLC et le serveur RADIUS
- Problèmes entre le serveur RADIUS et la base de données principale, s'ils sont utilisés, par exemple avec Active Directory (AD)

2. Le WLC voit la file d'attente RADIUS pleine sur les msglogs

Le WLC reçoit ce message à propos de la file d'attente RADIUS :

```
Univ-WISM2-02: *aaa QueueReader: Dec 02 14:25:31.565: #AAA-3-3TXQUEUE_ADD_FAILED:
radius_db.c:889 Transmission queue full. Que name: Radius queue. Dropping
sessionpackets.
host = x.x.x.x.
```

3. Debug AAA

Un débogage d'AAA affiche ce message :

```
*aaaQueueReader: Dec 02 21 09:19:52.198: xx:xx:xx:xx:xx:xx Returning AAA Error
'Out of Memory' (-2) for mobile xx:xx:xx:xx:xx:xx
```

Un débogage d'AAA renvoie le **délai d'**erreur AAA **(-5)** pour les périphériques mobiles. Le serveur AAA est inaccessible et est suivi de la désautorisation du client.

4. Le serveur RADIUS est trop occupé et ne répond pas

Voici le déroutement temporel du système de journalisation :

```
0 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 available
1 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 available
2 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 activated on WLAN 6
3 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 deactivated on WLAN 6
4 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 unavailable
5 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 22) for client 68:96:7b:0e:46:7f / user 'user1@univ1.edu'
6 Wed Aug 20 15:29:57 2014 User Larry_Dull_231730 logged Out. Client MAC:84:a6:c8:
87:13:9c, Client IP:198.21.137.22, AP MAC:c0:7b:bc:cf:af:40, AP Name:Dot1x-AP
```

```
7 Wed Aug 20 15:28:42 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 183) for client 48:d7:05:7d:93:a5 / user ' user2@univ2.edu '
8 Wed Aug 20 15:28:42 2014 RADIUS auth-server x.x.x.x:1812 unavailable
9 Wed Aug 20 15:28:42 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 154) for client 40:0e:85:76:00:68 / user ' user1@univ1.edu '
10 Wed Aug 20 15:28:41 2014 RADIUS auth-server x.x.x.x:1812 available
11 Wed Aug 20 15:28:41 2014 RADIUS auth-server x.x.x.x:1812 unavailable
12 Wed Aug 20 15:28:41 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 99) for client 50:2e:5c:ea:e4:ba / user ' user3@univ3.edu '
13 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 available
14 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 unavailable
15 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 30) for client b4:18:d1:60:6b:51 / user ' user1@univ1.edu '
16 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 available
17 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 activated on WLAN 6
18 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 deactivated on WLAN 6
19 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 unavailable
```

Réglage des meilleures pratiques

Réglage côté WLC

- EAP (Extensible Authentication Protocol) : permet de faire fonctionner l'exclusion de client 802.1X.

  Activez l'exclusion globale du client pour 802.1X.
  Définissez l'exclusion du client sur les LAN sans fil 802.1X (WLAN) sur au moins 120 secondes.
  Définissez les compteurs EAP comme décrit dans l'article 802.1X Exclusion du client sur un WLC AireOS.

- Définissez les délais d'attente de retransmission RADIUS sur au moins cinq secondes.

- Définissez le délai d'attente de session sur au moins huit heures.

- Désactivez le basculement agressif, qui ne permet pas à un seul demandeur de comportement incorrect de provoquer l'échec du WLC entre les serveurs RADIUS.

- Configurez l'itinérance sécurisée rapide pour vos clients.

  Assurez-vous que les clients EAP Microsoft Windows utilisent la norme WPA2 (Wi-Fi Protected Access 2)/AES (Advanced Encryption Standard) pour pouvoir utiliser la mise en cache de clés opportunistes (OKC).

  Si vous pouvez séparer les clients Apple iOS de leur propre WLAN, vous pouvez activer 802.11r sur ce WLAN.

  Activez Cisco Centralized Key Management (CCKM) pour tout WLAN prenant en charge les

téléphones 792x (mais n'activez **pas** CCKM sur un SSID (Service Set Identifier) prenant en charge les clients Microsoft Windows ou Android, car ils ont tendance à avoir des implémentations CCKM problématiques).

Activez la mise en cache des clés rémanentes (SKC) pour tout WLAN EAP prenant en charge les clients X et/ou Android du système d'exploitation Macintosh (MAC OS).

Référez-vous à Itinérance WLAN 802.11 et Itinérance Fast-Secure sur CUWN pour plus d'informations.

Note : Surveillez l'utilisation du cache de votre clé maître par paire WLC (PMK) aux heures de pointe avec la commande **show pmk-cache all**. Si vous atteignez la taille maximale de votre cache PMK ou que vous vous en approchez, vous devrez probablement désactiver SKC.
Si vous utilisez ISE avec profilage, utilisez le profilage DHCP/HTTP côté WLC. Cela encapsule les données de profilage dans un paquet de comptabilité RADIUS facilement équilibré en charge, ce qui garantit que toutes les données du point de terminaison atteignent le même réseau de services publics (PSN).

Assurez-vous que la comptabilité intermédiaire est désactivée, sauf si vous en avez besoin pour les services de facturation basés sur les octets. Dans le cas contraire, la comptabilité intermédiaire ajoute uniquement de la charge sans avantage supplémentaire.

Exécutez le meilleur code WLC.

Réglage côté serveur RADIUSRéduire le taux de journalisation. La plupart des serveurs RADIUS sont configurables sur la journalisation qu'ils stockeront. Si ACS ou ISE est utilisé, un administrateur peut choisir les catégories enregistrées dans la base de données de surveillance. Par exemple, si les données de comptabilité sont envoyées hors du serveur RADIUS et affichées avec une autre application telle que SYSLOG, alors n'écrivez pas les données dans la base de données localement. Sur ISE, assurez-vous que la suppression des journaux reste activée à tout moment. S'il doit être désactivé à des fins de dépannage, accédez à **Administration > System > Logging > Collection Filters** et utilisez l'option Bypass Suppression afin de désactiver la suppression sur un terminal ou un utilisateur individuel. Dans ISE version 1.3 et ultérieure, un point de terminaison peut être cliqué avec le bouton droit dans le journal d'authentification en direct afin de désactiver également la suppression.

Assurez-vous que la latence de l'authentification principale est faible (AD, LDAP (Lightweight Directory Access Protocol), Rivest, Shamir, Adleman (RSA)). Si vous utilisez ACS ou ISE, les rapports récapitulatifs d'authentification peuvent être exécutés afin de surveiller la latence par serveur pour la latence moyenne et la latence maximale. Plus le traitement d'une demande est long, plus le débit d'authentification qu'ACS ou ISE peut traiter est faible. 95 % du temps,

une latence élevée est due à une réponse lente d'une base de données principale.

Désactivez les tentatives de mot de passe PEAP (Protected Extensible Authentication Protocol). La plupart des périphériques ne prennent pas en charge les tentatives de mot de passe à l'intérieur du tunnel PEAP. Par conséquent, une nouvelle tentative à partir du serveur EAP entraîne l'arrêt de la réponse et le redémarrage du périphérique avec une nouvelle session EAP. Cela entraîne des délais d'attente EAP au lieu de rejets, ce qui signifie que les exclusions de client ne seront pas touchées.

Désactivez les protocoles EAP inutilisés. Cela n'est pas essentiel, mais cela ajoute une certaine efficacité à l'échange EAP et garantit qu'un client ne peut pas utiliser une méthode EAP faible ou non intentionnelle.

Activez la reprise de session PEAP et la reconnexion rapide.

N'envoyez pas d'authentifications MAC à l'AD si ce n'est pas nécessaire. Il s'agit d'une erreur de configuration courante qui augmente la charge sur les contrôleurs de domaine sur lesquels ISE s'authentifie. Ces résultats conduisent souvent à des recherches négatives qui prennent du temps et augmentent la latence moyenne.

Utilisez le détecteur de périphériques, le cas échéant (spécifique à ISE).