Empêchez les bas Sans fil de grande puissance de fonte de réseau de RADIUS

Contenu

Introduction

Ce document fournit à une brève présentation des instructions de configuration de base pour des déploiements Sans fil de grande puissance tels que le contrôleur LAN Sans fil d'AireOS (WLC) en RADIUS le Logiciel Cisco Identity Services Engine (ISE) ou le Cisco Secure Access Control Server (ACS). Ce document met en référence d'autres documents avec un plus grand détail technique.

Symptômes observés

Typiquement les environnements d'université rencontrent cet état de fusion d'Authentification, autorisation et comptabilité (AAA). Cette section décrit les symptômes/logs habituels étés témoin dans cet environnement.

1. Surveillez la représentation de RADIUS

Le client de Dotx éprouve un grand retard avec beaucoup de relances pour authentifier.

Utilisez le **show radius auth statistics de** commande (GUI : **Moniteur > statistiques > serveurs de RADIUS**) afin de rechercher des problèmes. Recherchez spécifiquement un grand nombre de relances, d'anomalies, 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 :

- Relance élevée : Premier rapport de demande (devrait être pas plus de 10%)
- Anomalie élevée : Recevez le rapport
- Délai d'attente élevé : Premier rapport de demande (devrait être pas plus de 5%)

S'il y a des problèmes, vérifiez :

- Clients Misconfigured
- Problèmes d'accessibilité de réseau entre le WLC et le serveur de RADIUS
- Problèmes entre le serveur de RADIUS et la base de données principale, si en service, comme avec le Répertoire actif (AD)

2. Le WLC voit la file d'attente de RADIUS complètement sur le Msglogs

Le WLC reçoit ce message au sujet de la file d'attente de 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'attente d'**erreur d'AAA **(-5)** pour des périphériques mobiles. Le serveur d'AAA est inaccessible et est suivi par déautorisation de client.

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

Voici le déroutement heure système de log :

```
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
```

Accord de pratique recommandée

Accord de WLC-Side

- Protocole EAP (Extensible Authentication Protocol) - Faites le travail d'exclusion de client de 802.1X.

  Exclusion de client d'enable globalement pour le 802.1X.
  Placez l'exclusion de client sur les réseaux locaux Sans fil de 802.1X (WLAN) au moins à 120 secondes.
  Placez les temporisateurs d'EAP comme décrit dans l'exclusion de client de 802.1X sur un article d'AireOS WLC.

- Placez les délais d'attente de retransmission de RADIUS au moins à cinq secondes.

- Placez la session-timeout au moins à huit heures.

- Désactivez le Basculement agressif, qui ne permet pas à un suppliant de mauvaise conduite simple pour faire échouer le WLC entre les serveurs de RADIUS.

- Configurez l'itinérance sécurisée rapide pour vos clients.

  Assurez-vous qu'accès protégé par Wi-Fi 2 d'utilisation de clients d'EAP de Microsoft Windows (la norme de chiffrement WPA2)/Advanced (AES) ainsi ils peuvent utiliser le Key Caching opportuniste (OKC).

  Si vous pouvez isoler des clients IOS d'Apple à leur propre WLAN, alors vous pouvez activer 802.11r sur ce WLAN.

  Activez le Cisco Centralized Key Management (CCKM) pour n'importe quel WLAN qui prend

en charge les téléphones 792x (mais n'activez pas CCKM sur aucun Identifiant SSID (Service Set Identifier) qui prend en charge des clients de Microsoft Windows ou d'Android, parce qu'ils tendent à avoir des réalisations problématiques CCKM).

Activez le Key Caching Rémanent (SKC) pour n'importe quel EAP WLAN qui prend en charge le système d'exploitation Mac (MAC OS) des clients X et/ou d'Android.

Référez-vous à l'itinérance du 802.11 WLAN et à l'itinérance Rapide-sécurisée sur le pour en savoir plus CUWN.

Note: Surveillez votre utilisation de cache du Pairwise Master Key WLC (PMK) aux heures de pointe avec le **show pmk-cache toute la** commande. Si vous atteignez votre taille maximum de PMK-cache, ou l'obtenez près de elle, alors vous devrez probablement désactiver SKC. Si vous utilisez ISE avec le profilage, alors utilisez le profilage du WLC-side DHCP/HTTP. Ceci enveloppe les données de profilage dans un paquet de comptabilité de RADIUS qui est facilement chargement-équilibré, qui s'assure que toutes les données pour le point final atteignent le même réseau de service public (le RPC).

Assurez-vous que la comptabilité intérimaire est éteinte à moins que vous ayez besoin de elle pour des services basés sur octet de facturation. Autrement la comptabilité intérimaire ajoute seulement le chargement sans l'allocation complémentaire.

Exécutez le meilleur code WLC.

Accord de côté serveur de RADIUSRéduisez le débit se connectant. La plupart des serveurs de RADIUS sont configurables au sujet de ce que se connectant ils enregistreront. Si l'ACS ou l'ISE est utilisé, un administrateur peut choisir ce que les catégories sont enregistré à la base de données de surveillance. Un exemple pourrait être si la donnée de comptabilité est envoyée du serveur de RADIUS et visualisée avec une autre application telle que le SYSLOG, alors n'écrivent pas les données à la base de données localement. Sur l'ISE, assurez-vous que les restes de suppression de log ont activé à tout moment. S'il doit être désactivé pour dépannage des buts, alors aller à la **gestion > au système > se connectant > la collecte filtre** et emploie l'option de suppression de contournement afin de désactiver la suppression sur un point final ou un utilisateur individuel. Dans la version 1.3 et ultérieures ISE, un point final peut être cliqué avec le bouton droit dans la commande vivante d'authentication login pour désactiver la suppression aussi bien.

Assurez que la latence principale d'authentification est basse (AD, Protocole LDAP (Lightweight Directory Access Protocol), Rivest, Shamir, Adleman (RSA)). Si vous utilisez l'ACS ou l'ISE, les comptes rendus succincts d'authentification peuvent être exécutés afin de surveiller la latence sur une base de par-serveur pour la moyenne et la latence de crête. Plus

il dure une demande d'être traité, plus le débit d'authentification est inférieur l'ACS ou l'ISE peut traiter. 95% du temps, latence élevée est dû à une réponse lente d'une base de données principale.

Relances de mot de passe du Protected Extensible Authentication Protocol de débronchement (PEAP). La plupart des périphériques ne prennent en charge pas des relances de mot de passe à l'intérieur du tunnel PEAP, ainsi une relance du serveur d'EAP fait cesser le périphérique de répondre et reprise avec une nouvelle session d'EAP. Ceci entraîne des délais d'attente d'EAP au lieu des anomalies, ainsi il signifie que des exclusions de client ne seront pas frappées.

Protocoles inutilisés d'EAP de débronchement. Ce n'est pas essentiel mais ajoute de l'efficacité à l'échange d'EAP et s'assure qu'un client ne peut pas utiliser une méthode faible ou fortuite d'EAP.

La reprise de session de l'enable PEAP et rapide rebranchent.

N'envoyez pas les authentifications MAC à l'AD sinon requis. C'est une mauvaise configuration commune qui augmente le chargement sur les contrôleurs de domaine contre lesquels ISE authentifie. Ceux-ci souvent mènent aux recherches négatives qui sont coûteuses en temps et augmentent la latence moyenne.

Utilisez le capteur de périphérique le cas échéant (particularité ISE).