Dépannez les questions d'authentification TACACS

Contenu

Introduction

Ce document décrit les étapes pour dépanner des questions de l'authentification de système de contrôle d'accès de Terminal Access Controller (TACACS) sur des Routeurs et des Commutateurs de Cisco IOS/IOS-XE.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration d'authentification, d'autorisation et de comptabilité (AAA) sur des périphériques de Cisco
- Configuration TACACS

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Comment TACACS fonctionne

Le protocole TACACS+ utilise le Protocole TCP (Transmission Control Protocol) comme protocole de transport avec la destination port le numéro 49. Quand le routeur reçoit une demande de procédure de connexion, elle établit une connexion TCP avec le serveur TACACS, signalent qu'une invite de nom d'utilisateur est affiché à l'utilisateur. Quand l'utilisateur écrit le nom d'utilisateur, le routeur communique de nouveau avec le serveur TACACS pour l'invite du mot de

passe. Une fois que l'utilisateur entre le mot de passe, le routeur envoient ces informations au serveur TACACS de nouveau. Le serveur TACACS vérifie les identifiants utilisateurs et envoie une réponse de nouveau au routeur. Le résultat d'une session d'AAA peut être l'un de ces :

PASSAGE : Quand vous êtes authentifié le service commence seulement si l'autorisation d'AAA est configurée sur le routeur. La phase d'autorisation commence à ce moment.

ÉCHOUER : Quand vous avez manqué l'authentification. Vous pourriez être refusé davantage d'accès ou être incité à relancer la séquence d'ouverture de connexion, selon le démon TACACS+. En cela, vous pouvez devoir vérifier les stratégies configurées pour l'utilisateur dans le serveur TACACS, si vous recevez une ÉCHOUER du serveur

ERREUR : Il indique qu'une erreur s'est produite pendant l'authentification. Ceci peut être au démon ou dans la connexion réseau entre le démon et le routeur. Si une réponse d'ERREUR est reçue, de routeur les essais typiquement pour employer une approche alternative pour authentifier l'utilisateur.

Ce sont la configuration de base de l'AAA et TACACS sur un routeur de Cisco

```
aaa new-model

aaa authentication login default group tacacs+ local

aaa authorization exec default group tacacs+ local

!

tacacs server prod

address ipv4 10.106.60.182

key cisco123

!

ip tacacs source-interface Gig 0/0
```

Dépannez les questions TACACS

Étape 1. Vérifiez la Connectivité au serveur TACACS avec un **telnet** sur le port 49 du routeur avec l'interface appropriée de source. Au cas où le routeur ne pourrait pas se connecter au serveur TACACS sur le port 49, il pourrait y avoir un certain Pare-feu ou liste d'accès bloquant le trafic.

```
Router#telnet 10.106.60.182 49
Trying 10.106.60.182, 49 ... Open
```

Étape 2. Vérifiez que le client d'AAA est correctement configuré sur le serveur TACACS avec l'adresse IP correcte et la clé secrète partagée. Si le routeur a de plusieurs interfaces sortantes, on lui suggère de configurer l'interface de source TACACS à l'aide de la commande suivante. Vous pouvez devoir configurer l'interface, dont l'adresse IP est configurée comme adresse IP de client sur le serveur TACACS, comme l'interface de source TACACS sur le routeur

```
Router(config)#ip tacacs source-interface Gig 0/0
```

Étape 3. Vérifiez si l'interface de source TACACS est sur un Virtual Routing and Forwarding

(VRF). Au cas où l'interface serait sur un VRF, vous pouvez devoir configurer les informations de VRF sous le Groupe de serveurs AAA. Référez-vous le lien pour la configuration du VRF TACACS averti.

Étape 4. Exécutez l'**AAA de test** et le vérifiez que nous recevons la réponse correcte du serveur

```
Router#test aaa group tacacs+ cisco cisco legacy
Sending password
User successfully authenticated
```

Étape 5. Si l'**AAA de test** échoue, activez ces derniers met au point ensemble pour analyser les transactions entre le routeur et le serveur TACACS pour identifier la cause principale.

```
debug aaa authentication

debug aaa authorization

debug tacacs

debug ip tcp transaction
```

C'est un exemple de sortie de débogage dans un scénario fonctionnant :

```
*Apr  6 13:32:50.462: AAA/BIND(00000054): Bind i/f
*Apr  6 13:32:50.462: AAA/AUTHEN/LOGIN (00000054): Pick method list 'default'
*Apr  6 13:32:50.462: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr  6 13:32:50.462: TPLUS(00000054) login timer started 1020 sec timeout
*Apr  6 13:32:50.462: TPLUS: processing authentication start request id 84
*Apr  6 13:32:50.462: TPLUS: Authentication start packet created for 84()
*Apr  6 13:32:50.462: TPLUS: Using server 10.106.60.182
*Apr  6 13:32:50.462: TPLUS(00000054)/0/NB_WAIT/2432818: Started 5 sec timeout
*Apr  6 13:32:50.466: TPLUS(00000054)/0/NB_WAIT: socket event 2
*Apr  6 13:32:50.466: TPLUS(00000054)/0/NB_WAIT: wrote entire 38 bytes request
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: Would block while reading
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 43 bytes data)
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: read entire 55 bytes response
*Apr  6 13:32:50.466: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr  6 13:32:50.466: TPLUS: Received authen response status GET_USER (7)
*Apr  6 13:32:53.242: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr  6 13:32:53.242: TPLUS(00000054) login timer started 1020 sec timeout
*Apr  6 13:32:53.242: TPLUS: processing authentication continue request id 84
*Apr  6 13:32:53.242: TPLUS: Authentication continue packet generated for 84
*Apr  6 13:32:53.242: TPLUS(00000054)/0/WRITE/10882BBC: Started 5 sec timeout
*Apr  6 13:32:53.242: TPLUS(00000054)/0/WRITE: wrote entire 22 bytes request
*Apr  6 13:32:53.246: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:53.246: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 16 bytes data)
*Apr  6 13:32:53.246: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:53.246: TPLUS(00000054)/0/READ: read entire 28 bytes response
*Apr  6 13:32:53.246: TPLUS(00000054)/0/10882BBC: Processing the reply packet
*Apr  6 13:32:53.246: TPLUS: Received authen response status GET_PASSWORD (8)
*Apr  6 13:32:54.454: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr  6 13:32:54.454: TPLUS(00000054) login timer started 1020 sec timeout
*Apr  6 13:32:54.454: TPLUS: processing authentication continue request id 84
*Apr  6 13:32:54.454: TPLUS: Authentication continue packet generated for 84
*Apr  6 13:32:54.454: TPLUS(00000054)/0/WRITE/2432818: Started 5 sec timeout
*Apr  6 13:32:54.454: TPLUS(00000054)/0/WRITE: wrote entire 22 bytes request
*Apr  6 13:32:54.458: TPLUS(00000054)/0/READ: socket event 1
```

```
*Apr  6 13:32:54.458: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Apr  6 13:32:54.458: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:54.458: TPLUS(00000054)/0/READ: read entire 18 bytes response
*Apr  6 13:32:54.458: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr  6 13:32:54.458: TPLUS: Received authen response status PASS (2)
*Apr  6 13:32:54.462: AAA/AUTHOR (0x54): Pick method list 'default'
*Apr  6 13:32:54.462: TPLUS: Queuing AAA Authorization request 84 for processing
*Apr  6 13:32:54.462: TPLUS(00000054) login timer started 1020 sec timeout
*Apr  6 13:32:54.462: TPLUS: processing authorization request id 84
*Apr  6 13:32:54.462: TPLUS: Protocol set to None .....Skipping
*Apr  6 13:32:54.462: TPLUS: Sending AV service=shell
*Apr  6 13:32:54.462: TPLUS: Sending AV cmd*
*Apr  6 13:32:54.462: TPLUS: Authorization request created for 84(cisco)
*Apr  6 13:32:54.462: TPLUS: using previously set server 10.106.60.182 from group tacacs+
*Apr  6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT/2432818: Started 5 sec timeout
*Apr  6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT: socket event 2
*Apr  6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT: wrote entire 62 bytes request
*Apr  6 13:32:54.462: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:54.462: TPLUS(00000054)/0/READ: Would block while reading
*Apr  6 13:32:54.470: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:54.470: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 18 bytes data)
*Apr  6 13:32:54.470: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:54.470: TPLUS(00000054)/0/READ: read entire 30 bytes response
*Apr  6 13:32:54.470: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr  6 13:32:54.470: TPLUS: Processed AV priv-lvl=15
*Apr  6 13:32:54.470: TPLUS: received authorization response for 84: PASS
*Apr  6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): processing AV cmd=
*Apr  6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): processing AV priv-lvl=15
*Apr  6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): Authorization successful
```

C'est un exemple de sortie de débogage du routeur, quand le serveur TACACS est configuré avec une clé pré partagée fausse

```
*Apr  6 13:35:07.826: AAA/BIND(00000055): Bind i/f
*Apr  6 13:35:07.826: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*Apr  6 13:35:07.826: TPLUS: Queuing AAA Authentication request 85 for processing
*Apr  6 13:35:07.826: TPLUS(00000055) login timer started 1020 sec timeout
*Apr  6 13:35:07.826: TPLUS: processing authentication start request id 85
*Apr  6 13:35:07.826: TPLUS: Authentication start packet created for 85()
*Apr  6 13:35:07.826: TPLUS: Using server 10.106.60.182
*Apr  6 13:35:07.826: TPLUS(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*Apr  6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: socket event 2
*Apr  6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*Apr  6 13:35:07.830: TPLUS(00000055)/0/READ: socket event 1
*Apr  6 13:35:07.830: TPLUS(00000055)/0/READ: Would block while reading
*Apr  6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr  6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Apr  6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr  6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 18 bytes response
*Apr  6 13:35:07.886: TPLUS(00000055)/0/225FE2DC: Processing the reply packet
*Apr  6 13:35:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*Apr  6 13:35:07.886: TPLUS: Invalid AUTHEN packet (check keys).
```

Informations connexes

- Configuration TACACS sur le Cisco IOS
- Support et documentation techniques - Cisco Systems