AAA ACS 5.x cachant dans l'exemple de configuration Cisco IOS

Contenu

Introduction

Ce document décrit les étapes nécessaires afin de configurer la mise en cache des identifiants utilisateurs d'admin TACACS+ pour l'accès de telnet et de ligne VTY. La mise en cache d'autorisation et d'authentification a été intégrée dans la version 15.0(1)M de Cisco IOS®. Cette caractéristique permet à un routeur d'enregistrer des qualifications d'Authentification, autorisation et comptabilité (AAA) dans son cache après qu'elle reçoive une réponse TACACS+ à une demande d'AAA. Le cache est utilisé afin d'amplifier la représentation et réduire la quantité de demandes envoyées au serveur d'AAA, ou comme méthode d'authentification de chute au cas où le serveur d'AAA serait inaccessible.

Conditions préalables

Conditions requises

Cisco recommande que vous :

- Confirmez la connectivité IP entre le routeur et la version 5.x du Cisco Secure Access Control Server (ACS).
- Définissez le routeur sur l'ACS en tant que client d'AAA (périphériques de réseau) avec la même chose secret partagé.

Composants utilisés

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

- Version 5 ACS
- Routeurs qui exécutent la version 15.1 de Cisco IOS

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.

Configurez

Configuration sur un routeur Cisco IOS

1. Sélectionnez ces commandes afin de définir le serveur TACACS et la clé pré-partagée :

```
Router(config)#tacacs-server host 192.168.159.41
Router(config)#tacacs-server timeout 4
Router(config)#tacacs-server key SECRET12345
```

2. Sélectionnez ces commandes afin de définir les groupes de profil de cache.
   Note: Chaque nom de profil doit apparier un aaa username.

```
Router(config)#aaa cache profile admin
Router(config-profile-map)# profile peteradmin
```

3. Sélectionnez ces commandes afin d'assigner les règles de mise en cache d'authentification et d'autorisation aux Groupes de serveurs AAA :

```
Router(config-profile-map)# aaa group server tacacs+ admin-tac
Router(config-sg-tacacs+)# server 192.168.159.41
Router(config-sg-tacacs+)# cache authentication profile admin
Router(config-sg-tacacs+)# cache authorization profile admin
```

4. Définissez les listes d'authentification et d'authorization method qui contiennent la méthode de cache. Dans cet exemple de configuration, le cache est seulement utilisé si les serveurs d'AAA ne répondent pas. Si la commande est commutée **pour cacher admin-TAC le groupe admin-TAC**, le cache est regardé- d'abord.
   Note: Le mot de passe d'enable de TACACS n'est pas caché.

```
aaa authentication login mtac group admin-tac cache admin-tac local
aaa authorization exec default group admin-tac cache admin-tac local
aaa accounting exec default start-stop group admin-tac
```

5. Sélectionnez ces commandes afin de configurer TACACS+ sur les lignes VTY :

```
Router(config)#line vty 0 4
Router(config-line)#login authentication mtac
```

Configuration sur l'ACS

1. Créez un utilisateur dans ACS. Naviguez vers des **utilisateurs et les mémoires d'identité > créent l'utilisateur**. Cet exemple utilise l'utilisateur **Peteradmin de** test.

2. Les utilisateurs d'admin TACACS+ ont besoin un profil de shell qui leur permet un niveau de privilège de **15** de sorte qu'ils puissent écrire le **mode enable**. Afin de configurer le profil de shell, naviguez des **profils** vers des **éléments de stratégie > l'autorisation et des autorisations > de périphérique gestion > shell**.

3. Créez une règle de sélection de service sous des **stratégies > des services d'accès d'Access** pour apparier TACACS :

4. Naviguez vers l'**admin de périphérique priv15 > des protocoles permis > des Protocoles d'authentification choisis**, et configurez les **protocoles permis**. Cet exemple utilise **PAP/ASCII**.

5. Naviguez **pour accéder à des stratégies > des services d'accès > l'admin de périphérique priv15 > identité**, et configurez la source d'identité pour des **utilisateurs internes**.

6. Configurez la stratégie d'autorisation sous des **stratégies d'Access > des services d'accès > l'admin de périphérique priv15 > autorisation**.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Telnet Access de test

Ceux-ci met au point sont utilisés afin de vérifier la mise en cache d'authentification et d'autorisation pour TACACS+ :

- événements de debug tacacs
- debug aaa cache group

Telnet au routeur avec le mot de passe d'utilisateur TACACS et d'enable TACACS :

```
username: peteradmin
password: peteradmin

R102>en
password: cpeter
R102#

R102#debug tacacs events
R102#debug aaa cache group
R102#
11:35:47.151: TPLUS: Queuing AAA Authentication request 16 for processing
11:35:47.159: TPLUS: processing authentication start request id 16
11:35:47.163: TPLUS: Authentication start packet created for 16()
11:35:47.167: TPLUS: Using server 192.168.159.41
11:35:47.187: TPLUS(00000010)/0/NB_WAIT/69540BEC: Started 4 sec timeout
11:35:47.223: TPLUS(00000010)/0/NB_WAIT: wrote entire 37 bytes request
11:35:47.227: TPLUS: Would block while reading pak header
11:35:47.251: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 16
bytes)
11:35:47.255: TPLUS(00000010)/0/READ: read entire 28 bytes response
11:35:47.255: TPLUS(00000010)/0/69540BEC: Processing the reply packet
11:35:47.259: TPLUS: Received authen response status GET_USER (7)
11:35:47.263: AAA/AUTHEN/CACHE: No username in response
11:35:56.703: TPLUS: Queuing AAA Authentication request 16 for processing
11:35:56.711: TPLUS: processing authentication continue request id 1611:35:56.715:
TPLUS: Authentication continue packet generated for 16
11:35:56.719: TPLUS(00000010)/0/WRITE/69540BEC: Started 4 sec timeout
11:35:56.727: TPLUS(00000010)/0/WRITE: wrote entire 27 bytes request
11:35:56.751: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 16
bytes)
11:35:56.751: TPLUS(00000010)/0/READ: read entire 28 bytes response
11:35:56.755: TPLUS(00000010)/0/69540BEC: Processing the reply packet
11:35:56.759: TPLUS: Received authen response status GET_PASSWORD (8)
11:35:56.763: AAA/AUTHEN/CACHE: Request status = 8, cannot add to cache
11:36:02.943: TPLUS: Queuing AAA Authentication request 16 for processing
11:36:02.955: TPLUS: processing authentication continue request id 16
11:36:02.959: TPLUS: Authentication continue packet generated for 16
11:36:02.963: TPLUS(00000010)/0/WRITE/69540BEC: Started 4 sec timeout
11:36:02.967: TPLUS(00000010)/0/WRITE: wrote entire 27 bytes request
11:36:03.971: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 6
bytes)
11:36:03.975: TPLUS(00000010)/0/READ: read entire 18 bytes response
11:36:03.975: TPLUS(00000010)/0/69540BEC: Processing the reply packet
11:36:03.979: TPLUS: Received authen response status PASS (2)
11:36:03.983: AAA/AUTHEN/CACHE: SG profile admin
11:36:03.987: AAA/AUTHEN/CACHE: SG block for admin found
11:36:03.987: AAA/AUTHEN/CACHE: matching profile found for peteradmin in admin
11:36:03.991: AAA/AUTHEN/CACHE: Dealing with authen_type = 1
11:36:03.995: TPLUS: Error occurs in reading packet header, shutdown the single
connection
11:36:04.047: TPLUS: Queuing AAA Authorization request 16 for processing
11:36:04.055: TPLUS: processing authorization request id 16
11:36:04.059: TPLUS: Protocol set to None .....Skipping
11:36:04.063: TPLUS: Sending AV service=shell
```

```
11:36:04.067: TPLUS: Sending AV cmd*
11:36:04.067: TPLUS: Authorization request created for 16(peteradmin)
11:36:04.071: TPLUS: using previously set server 192.168.159.41 from group
admin-tac
11:36:04.091: TPLUS(00000010)/0/NB_WAIT/689C0FDC: Started 4 sec timeout
11:36:04.127: TPLUS(00000010)/0/NB_WAIT: wrote entire 66 bytes request
11:36:04.131: TPLUS: Would block while reading pak header
11:36:05.319: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 6
bytes)
11:36:05.323: TPLUS(00000010)/0/READ: read entire 18 bytes response
11:36:05.327: TPLUS(00000010)/0/689C0FDC: Processing the reply packet
11:36:05.327: TPLUS: received authorization response for 16: PASS
11:36:05.335: AAA/AUTHEN/CACHE: SG profile admin
11:36:05.335: AAA/AUTHEN/CACHE: SG block for admin found
11:36:05.339: AAA/AUTHEN/CACHE: matching profile found for peteradmin in admin
11:36:05.339: AAA/AUTHOR/CACHE(00000010): Existing entry no set for authorization
11:36:05.347: TPLUS: Error occurs in reading packet header, shutdown the single
connection
11:36:05.419: TPLUS: Queuing AAA Accounting request 16 for processing
11:36:05.431: TPLUS: processing accounting request id 16
11:36:05.439: TPLUS: Sending AV task_id=6
11:36:05.439: TPLUS: Sending AV timezone=UTC
11:36:05.443: TPLUS: Sending AV service=shell
11:36:05.443: TPLUS: Accounting request created for 16(peteradmin)
11:36:05.447: TPLUS: using previously set server 192.168.159.41 from group
admin-tac
11:36:05.471: TPLUS(00000010)/0/NB_WAIT/689C0FDC: Started 4 sec timeout
11:36:05.523: TPLUS(00000010)/0/NB_WAIT: wrote entire 85 bytes request
11:36:05.523: TPLUS: Would block while reading pak header
11:36:05.587: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 5
bytes)
11:36:05.591: TPLUS(00000010)/0/READ: read entire 17 bytes response
11:36:05.591: TPLUS(00000010)/0/689C0FDC: Processing the reply packet
11:36:05.595: TPLUS: Received accounting response with status PASS
11:36:05.603: TPLUS: Error occurs in reading packet header, shutdown the single
connection
R102#
```

Vérifiez le cache

Sélectionnez ces commandes afin d'examiner et effacer les informations de cache :

- show aaa cache group [nom de groupe de cache] tout
- clear aaa cache group [nom de groupe de cache] tout

```
R102#show aaa cache group admin-tac all
----------------------------------------------------------
Entries in Profile dB admin-tac for exact match
----------------------------------------------------------
Profile: peteradmin
Updated: 00:00:42
Parse User: N
Authen User: Y
Query Count: 2
6731AF7C 0 00000009 username(422) 10 peteradmin, service shell, protocol none
6731AF8C 0 0000000A cmd(73) 0 , service shell, protocol none
----------------------------------------------------------
Entries in Profile dB admin-tac for regexp match
----------------------------------------------------------
No entries found for regexp match
```

Simulez une panne ACS

Démontez le serveur ACS du réseau afin de simuler une panne et appeler vérifier de cache.

Telnet au routeur avec l'utilisateur TACACS et le mot de passe local d'enable (le mot de passe d'enable de TACACS ne peut pas être caché) :

```
username: peteradmin
password: peteradmin

R102>en
password:
R102#
11:39:10.723: TPLUS: Queuing AAA Authentication request 17 for processing
11:39:10.735: TPLUS: processing authentication start request id 17
11:39:10.739: TPLUS: Authentication start packet created for 17()
11:39:10.743: TPLUS: Using server 192.168.159.41
11:39:10.759: TPLUS(00000011)/0/NB_WAIT/68A4A820: Started 4 sec timeout
11:39:14.759: TPLUS(00000011)/0/NB_WAIT/68A4A820: timed out
11:39:14.763: TPLUS(00000011)/0/NB_WAIT/68A4A820: timed out, clean up
11:39:14.767: TPLUS(00000011)/0/68A4A820: Processing the reply packet
11:39:14.771: AAA/AUTHEN/CACHE: Don't cache responses with errors
11:39:14.779: AAA/AUTHEN/CACHE(00000011): GET_USER for username NULL
11:39:23.315: AAA/AUTHEN/CACHE(00000011): GET_PASSWORD for username peteradmin
11:39:25.191: AAA/AUTHEN/CACHE(00000011): Found a match
11:39:25.195: AAA/AUTHEN/CACHE(00000011): PASS for username peteradmin
11:39:25.215: TPLUS: Queuing AAA Authorization request 17 for processing
11:39:25.223: TPLUS: processing authorization request id 17
11:39:25.227: TPLUS: Protocol set to None .....Skipping
11:39:25.231: TPLUS: Sending AV service=shell
11:39:25.235: TPLUS: Sending AV cmd*
11:39:25.239: TPLUS: Authorization request created for 17(peteradmin)
11:39:25.239: TPLUS: Using server 192.168.159.41
11:39:25.243: TPLUS(00000011)/0/IDLE/689C3A0C: got immediate connect on new 0
11:39:25.247: TPLUS(00000011)/0/WRITE/689C3A0C: Started 4 sec timeout
11:39:25.251: TPLUS(00000011)/0/WRITE: write to 192.168.159.41 failed with errno
257((ENOTCONN))
11:39:25.255: TPLUS: Protocol set to None .....Skipping
11:39:25.259: TPLUS: Sending AV service=shell
11:39:25.259: TPLUS: Sending AV cmd*
11:39:25.263: TPLUS: Authorization request created for 17(peteradmin)
11:39:25.263: TPLUS(00000011): Start write failed
11:39:29.247: TPLUS(00000011)/0/WRITE/689C3A0C: timed out
11:39:29.251: TPLUS: Protocol set to None .....Skipping
11:39:29.255: TPLUS: Sending AV service=shell
11:39:29.255: TPLUS: Sending AV cmd*
11:39:29.259: TPLUS: Authorization request created for 17(peteradmin)
11:39:29.263: TPLUS(00000011)/0/WRITE/689C3A0C: timed out, clean up
11:39:29.267: TPLUS: Error occured while writing, shutdown the single
connection
11:39:29.267: TPLUS(00000011)/0/689C3A0C: Processing the reply packet
11:39:29.271: AAA/AUTHEN/CACHE: Don't cache responses with errors
11:39:29.331: TPLUS: Queuing AAA Accounting request 17 for processing
11:39:29.343: TPLUS: processing accounting request id 17
11:39:29.351: TPLUS: Sending AV task_id=7
11:39:29.351: TPLUS: Sending AV timezone=UTC
11:39:29.355: TPLUS: Sending AV service=shell
11:39:29.359: TPLUS: Accounting request created for 17(peteradmin)
11:39:29.359: TPLUS: using previously set server 192.168.159.41 from group
admin-tac
11:39:29.379: TPLUS(00000011)/0/NB_WAIT/689C0FDC: Started 4 sec timeout
```

```
11:39:33.375: TPLUS(00000011)/0/NB_WAIT/689C0FDC: timed out
11:39:33.379: TPLUS: Choosing next server 192.168.159.41
11:39:33.383: TPLUS(00000011)/689C0FDC: releasing old socket 0
11:39:33.387: TPLUS(00000011)/0/NB_WAIT/689C0FDC: got immediate connect on
new 0
11:39:33.387: TPLUS(00000011)/0/WRITE/689C0FDC: Started 4 sec timeout
11:39:33.391: TPLUS(00000011)/0/WRITE: write to 192.168.159.41 failed with errno
257((ENOTCONN))
11:39:33.399: TPLUS: Sending AV task_id=7
11:39:33.399: TPLUS: Sending AV timezone=UTC
11:39:33.403: TPLUS: Sending AV service=shell
11:39:33.403: TPLUS: Accounting request created for 17(peteradmin)
11:39:33.407: TPLUS(00000011)/0/WRITE/689C0FDC: Write failed, this request
will be cleaned up after timeout
11:39:37.387: TPLUS(00000011)/0/WRITE/689C0FDC: timed out
11:39:37.395: TPLUS: Sending AV task_id=7
11:39:37.395: TPLUS: Sending AV timezone=UTC
11:39:37.399: TPLUS: Sending AV service=shell
11:39:37.403: TPLUS: Accounting request created for 17(peteradmin)
11:39:37.407: TPLUS: Choosing next server 192.168.159.41
11:39:37.407: TPLUS(00000011)/689C0FDC: releasing old socket 0
11:39:37.411: TPLUS(00000011)/0/WRITE/689C0FDC: got immediate connect on
new 0
11:39:37.415: TPLUS(00000011)/0/WRITE/689C0FDC: Started 4 sec timeout
11:39:37.415: TPLUS(00000011)/0/WRITE: write to 192.168.159.41 failed with errno
257((ENOTCONN))
11:39:37.423: TPLUS: Sending AV task_id=7
11:39:37.427: TPLUS: Sending AV timezone=UTC
11:39:37.427: TPLUS: Sending AV service=shell
11:39:37.431: TPLUS: Accounting request created for 17(peteradmin)
11:39:37.431: TPLUS(00000011)/0/WRITE/689C0FDC: Write failed, this request
will be cleaned up after timeout
11:39:41.411: TPLUS(00000011)/0/WRITE/689C0FDC: timed out
11:39:41.419: TPLUS: Sending AV task_id=7
11:39:41.423: TPLUS: Sending AV timezone=UTC
11:39:41.423: TPLUS: Sending AV service=shell
11:39:41.427: TPLUS: Accounting request created for 17(peteradmin)
11:39:41.431: TPLUS(00000011)/0/WRITE/689C0FDC: timed out, clean up
11:39:41.431: TPLUS: Error occured while writing, shutdown the single
connection
11:39:41.435: TPLUS(00000011)/0/689C0FDC: Processing the reply packet

Cached username and password works.

R102#clear aaa cache group admin-tac all
R102#show aaa cache group admin-tac all
-----------------------------------------------------------
Entries in Profile dB admin-tac for exact match
-----------------------------------------------------------
No entries found in Profile dB
```

Dépannez

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.