Routeur Cisco IOS : Exemple de configuration de l'authentification locale, TACACS+ et RADIUS de la connexion HTTP

Contenu

Introduction

Ce document affiche comment configurer des gens du pays, l'authentification TACACS+, et de RAYON de la connexion HTTP. Quelques commandes de débogage appropriées sont également fournies.

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur les versions de logiciel et de matériel ci-dessous.

- Versions de logiciel 11.2 ou ultérieures de Cisco IOS®
- Matériel qui prend en charge ces révisions de logiciel

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Théorie générale

Dans la version de logiciel 11.2 de Cisco IOS®, une caractéristique pour gérer le routeur par le HTTP a été ajoutée. La section « d'ordres de navigateur Web de Cisco IOS » de la référence de commandes de bases de configuration de Cisco IOS inclut les informations suivantes sur cette caractéristique.

« Les commandes enables d'**ip http authentication** vous pour spécifier une méthode d'authentification particulière pour des utilisateurs de serveur HTTP. Le serveur HTTP emploie la méthode de mot de passe d'enable pour authentifier un utilisateur au niveau de privilège 15. La commande d'**ip http authentication** vous permet maintenant de spécifier l'enable, les gens du pays, le TACACS, ou l'authentification d'utilisateur de serveur HTTP d'Authentification, autorisation et comptabilité (AAA). »

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Ce document utilise les configurations présentées ci-dessous.

- Configurer l'authentification locale pour des utilisateurs de serveur HTTP
- Configurer l'authentification TACACS+ pour des utilisateurs de serveur HTTP
- Configurer l'authentification de RAYON pour des utilisateurs de serveur HTTP

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Configurer l'authentification locale pour des utilisateurs de serveur HTTP

- Configurations de routeur
- Résultats d'utilisateur

Configurations de routeur

Authentification locale avec le Logiciel Cisco IOS version 11.2
`!--- This is the part of the configuration related to`

```
local authentication. ! aaa new-model aaa authentication
login default local aaa authorization exec local
username one privilege 15 password one username three
password three username four privilege 7 password four
ip http server ip http authentication aaa ! !--- Example
of command moved from level 15 (enable) to level 7 !
privilege exec level 7 clear line
```

Authentification locale avec versions du logiciel Cisco IOS 11.3.3.T ou plus tard

```
!--- This is the part of the configuration !--- related
to local authentication. ! aaa new-model aaa
authentication login default local aaa authorization
exec default local username one privilege 15 password
one username three password three username four
privilege 7 password four ip http server ip http
authentication local ! !--- Example of command moved
from level 15 (enable) to level 7 ! privilege exec level
7 clear line
```

Résultats d'utilisateur

Ces résultats s'appliquent aux utilisateurs en configurations de routeur précédentes.

- **Utilisateur un**L'utilisateur passera l'autorisation Web si l'URL est écrit comme http://#.#.#.#.Après Telnet au routeur, l'utilisateur peut exécuter toutes les commandes après l'authentification de connexion.L'utilisateur sera dans le mode enable après procédure de connexion (le **show privilege** sera 15).Si l'autorisation de commande est ajoutée au routeur, l'utilisateur réussira toujours à toutes les commandes.
- **Utilisateur trois**L'utilisateur échouera autorisation Web due à ne pas avoir un niveau de privilège.Après Telnet au routeur, l'utilisateur peut exécuter toutes les commandes après l'authentification de connexion.L'utilisateur sera dans le mode non activé après procédure de connexion (le **show privilege** sera 1).Si l'autorisation de commande est ajoutée au routeur, l'utilisateur réussira toujours à toutes les commandes.
- **Utilisateur quatre**L'utilisateur passera l'autorisation Web si l'URL est écrit comme http://#.#.#.#/level/7/exec.Les commandes du niveau 1 plus la commande de **clear line du** niveau 7 apparaîtront.Après Telnet au routeur, l'utilisateur peut exécuter toutes les commandes après l'authentification de connexion.L'utilisateur sera au niveau de privilège 7 après procédure de connexion (le **show privilege** sera 7)Si l'autorisation de commande est ajoutée au routeur, l'utilisateur réussira toujours à toutes les commandes.

Configurer l'authentification TACACS+ pour des utilisateurs de serveur HTTP

Configurations de routeur

Authentification avec le Logiciel Cisco IOS version 11.2

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Authentification avec les versions du logiciel Cisco IOS 11.3.3.T à 12.0.5.T

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec default tacacs
ip http server
ip http authentication aaa|tacacs
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Authentification avec les versions du logiciel Cisco IOS 12.0.5.T et plus tard

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Résultats d'utilisateur

Les résultats suivants s'appliquent aux utilisateurs en configurations du serveur ci-dessous.

- **Utilisateur un**L'utilisateur passera l'autorisation Web si l'URL est écrit comme http://#.#.#.#.Après Telnet au routeur, l'utilisateur peut exécuter toutes les commandes après l'authentification de connexion.L'utilisateur sera dans le mode enable après procédure de connexion (le **show privilege** sera 15).Si l'autorisation de commande est ajoutée au routeur, l'utilisateur réussira toujours à toutes les commandes.
- **Utilisateur deux**L'utilisateur passera l'autorisation Web si l'URL est écrit comme http://#.#.#.#.Après Telnet au routeur, l'utilisateur peut exécuter toutes les commandes après l'authentification de connexion.L'utilisateur sera dans le mode enable après procédure de connexion (le **show privilege** sera 15).Si l'autorisation de commande est ajoutée au routeur, l'utilisateur échouera toutes les commandes car la configuration du serveur ne les autorise pas.
- **Utilisateur trois**L'utilisateur échouera autorisation Web due à ne pas avoir un niveau de privilège.Après Telnet au routeur, l'utilisateur peut exécuter toutes les commandes après l'authentification de connexion.L'utilisateur sera dans le mode non activé après procédure de connexion (le **show privilege** sera 1).Si l'autorisation de commande est ajoutée au routeur, l'utilisateur réussira toujours à toutes les commandes.

- **Utilisateur quatre**L'utilisateur passera l'autorisation Web si l'URL est écrit comme http://#.#.#.#/level/7/exec.Les commandes du niveau 1 plus la commande de **clear line du** niveau 7 apparaîtront.Après Telnet au routeur, l'utilisateur peut exécuter toutes les commandes après l'authentification de connexion.L'utilisateur sera au niveau de privilège 7 après procédure de connexion (le **show privilege** sera 7)Si l'autorisation de commande est ajoutée au routeur, l'utilisateur réussira toujours à toutes les commandes.

Configuration du serveur de Freeware Daemon

```
user = one {
default service = permit
login = cleartext "one"
service = exec {
priv-lvl = 15
}
}

user = two {
login = cleartext "two"
service = exec {
priv-lvl = 15
}
}

user = three {
default service = permit
login = cleartext "three"
}

user = four {
default service = permit
login = cleartext "four"
service = exec {
priv-lvl = 7
}
}
```

Cisco Secure ACS pour la configuration de serveur Unix

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 27
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u two
User Profile Information
user = two{
profile_id = 28
profile_cycle = 1
password = clear "********"
service=shell {
set priv-lvl=15
}
}
```

```
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 29
profile_cycle = 1
password = clear "********"
default service=permit
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 30
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=7
}
}
```

[Cisco Secure ACS pour la configuration de Windows Server]

Utilisateur un dans le groupe un

- Configurations de groupe**Shell de** contrôle **(exécutif)**.**Privilège level=15 de** contrôle.**Services (non définis) de par défaut de** contrôle.**Remarque:** Si cette option n'apparaît pas, allez à la **configuration d'interface** et sélectionnez **TACACS+** et puis **options de configuration avancée**. Choisissez la configuration **(non définie) de service de par défaut d'enable d'affichage**.
- Paramètres utilisateursMot de passe de n'importe quelle base de données ; entrez le mot de passe et le confirmez dans la zone supérieure.

Utilisateur deux dans le groupe deux

- Configurations de groupe**Shell de** contrôle **(exécutif)**.**Privilège level=15 de** contrôle.Ne vérifiez pas les **services (non définis) de par défaut**.
- Paramètres utilisateursMot de passe de n'importe quelle base de données ; entrez le mot de passe et le confirmez dans la zone supérieure.

Utilisateur trois dans le groupe trois

- Configurations de groupe**Shell de** contrôle **(exécutif)**.Blanc de **niveau de privilège de** congé.**Services (non définis) de par défaut de** contrôle.**Remarque:** Si cette option n'apparaît pas, allez à la **configuration d'interface** et sélectionnez **TACACS+** et puis **options de configuration avancée**. Choisissez la configuration **(non définie) de service de par défaut d'enable d'affichage**.
- Paramètres utilisateursMot de passe de n'importe quelle base de données ; entrez le mot de passe et le confirmez dans la zone supérieure.

Utilisateur quatre dans le groupe quatre

- Configurations de groupe**Shell de** contrôle **(exécutif)**.**Privilège level=7 de** contrôle.**Services (non définis) de par défaut de** contrôle.**Remarque:** Si cette option n'apparaît pas, allez à la **configuration d'interface** et sélectionnez **TACACS+** et puis **options de configuration avancée**. Choisissez la configuration **(non définie) de service de par défaut d'enable d'affichage**.
- Paramètres utilisateursMot de passe de n'importe quelle base de données ; entrez le mot de passe et le confirmez dans la zone supérieure.

Configurer l'authentification de RAYON pour des utilisateurs de serveur HTTP

Configurations de routeur

Authentification avec le Logiciel Cisco IOS version 11.2

```
aaa new-model
aaa authentication login default radius
aaa authorization exec radius
ip http server
ip http authentication aaa
!
!--- Example of command moved from level 15 (enable) to
level 7 ! privilege exec level 7 clear line radius-
server host 171.68.118.101 radius-server key cisco
```

Authentification avec les versions du logiciel Cisco IOS 11.3.3.T à 12.0.5.T

```
aaa new-model
aaa authentication login default radius
aaa authorization exec default radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

Authentification avec les versions du logiciel Cisco IOS 12.0.5.T et plus tard

```
aaa new-model
aaa authentication login default group radius
aaa authorization exec default group radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

Résultats d'utilisateur

Les résultats suivants s'appliquent aux utilisateurs en configurations du serveur ci-dessous.

- **Utilisateur un**L'utilisateur passera l'autorisation Web si l'URL est écrit comme http://#.#.#.#.Après Telnet au routeur, l'utilisateur peut exécuter toutes les commandes après l'authentification de connexion.L'utilisateur sera dans le mode enable après procédure de connexion (le **show privilege** sera 15).
- **Utilisateur trois**L'utilisateur échouera autorisation Web due à ne pas avoir un niveau de privilège.Après Telnet au routeur, l'utilisateur peut exécuter toutes les commandes après

l'authentification de connexion.L'utilisateur sera dans le mode non activé après procédure de connexion (le **show privilege** sera 1).

- **Utilisateur quatre**L'utilisateur passera l'autorisation Web si l'URL est écrit comme http://#.#.#.#/level/7/exec.Les commandes du niveau 1 plus la commande de **clear line du** niveau 7 apparaîtront.Après Telnet au routeur, l'utilisateur peut exécuter toutes les commandes après l'authentification de connexion.L'utilisateur sera au niveau de privilège 7 après procédure de connexion (le **show privilege** sera 7)

Configuration RADIUS sur le serveur qui prend en charge des paires AV de Cisco

```
one Password= "one"
Service-Type = Shell-User
cisco-avpair = "shell:priv-lvl=15"

three Password = "three"
Service-Type = Login-User

four Password= "four"
Service-Type = Login-User
cisco-avpair = "shell:priv-lvl=7"
```

Cisco Secure ACS pour la configuration de serveur Unix

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 31
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="one"
}
reply_attributes= {
6=6
}
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 32
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="three"
}
reply_attributes= {
6=1
}
}
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 33
profile_cycle = 1
radius=Cisco {
check_items= {
```

```
2="four"
}
reply_attributes= {
6=1
9,1="shell:priv-lvl=7"
}
}
}
```

Cisco Secure ACS pour la configuration de Windows Server

- Utilisateur = un, type de service (attribut 6) = administratif
- Utilisateur = trois, type de service (attribut 6) = procédure de connexion
- Utilisateur = quatre, type de service (l'attribut 6) = procédure de connexion, cochent la case de paires AV de Cisco et écrivent shell:priv-lvl=7

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

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

Dépannage des commandes

Les commandes suivantes sont utiles pour mettre au point l'authentification HTTP. Ils sont émis sur le routeur.

Remarque: Avant d'exécuter les commandes **debug**, référez-vous à la section **Informations importantes sur les commandes Debug**.

- **terminal monitor** - Les affichages **mettent au point des** messages d'erreur de sortie de commande et de système pour le terminal et la session en cours.
- **debug aaa authentication** - Affiche des informations sur l'authentification AAA/TACACS+.
- **autorisation de debug aaa** - Affiche des informations sur l'autorisation AAA/TACACS+.
- **debug radius** - Affiche les informations de débogage détaillées associées avec le RAYON.
- **debug tacacs** - Affiche des informations associée avec TACACS.
- **debug ip http authentication** - Utilisez cette commande de dépanner des problèmes d'authentification HTTP. Affiche la méthode d'authentification le routeur tenté et des messages d'état d'authentification-particularité.

Informations connexes

- Page de support de Logiciel d'accès Cisco TACACS+
- Page d'assistance RADIUS
- Cisco Secure ACS pour la page d'assistance de Windows
- Cisco Secure ACS pour la page de support UNIX
- Demandes de commentaires (RFC)

- Support et documentation techniques - Cisco Systems