# Contenu



## Introduction

Ce document décrit comment configurer un routeur Cisco pour l'authentification avec le TACACS+ qui fonctionne sur l'UNIX. TACACS+ n'offre pas autant de fonctionnalités en tant que le Cisco Secure ACS pour des Windows ou Cisco Secure ACS UNIX disponible dans le commerce .

Le logiciel TACACS+ précédemment fourni par Cisco Systems a été discontinué et n'est plus pris en charge par Cisco Systems.

Aujourd'hui, vous pouvez trouver beaucoup de versions gratuites de TACACS+ quand vous recherchez « logiciel gratuit TACACS+ » sur votre moteur de recherche préféré sur Internet. Cisco ne recommande spécifiquement aucune implémentation particulière de logiciel gratuit TACACS+.

Le Cisco Secure Access Control Server (ACS) est disponible pour l'achat par des ventes de Cisco et des canaux réguliers de distribution dans le monde entier. Le Cisco Secure ACS pour des Windows inclut tous les composants nécessaires requis pour une installation indépendante sur une station de travail de Microsoft Windows. Le moteur de solution de Cisco Secure ACS est expédié avec une licence logicielle préinstallée de Cisco Secure ACS. Visitez la page d'accueil de commande Cisco (clients enregistrés seulement) pour passer une commande.

**Remarque:** Vous avez besoin d'un compte CCO avec un contrat de service associé pour obtenir la version d'essai valable 90 jours pour le Cisco Secure ACS pour Windows.

La configuration du routeur dans ce document a été développée sur un routeur qui exécute la version software 11.3.3 de Cisco IOS®. La version du logiciel Cisco IOS 12.0.5.T et les utilisations postérieures **groupent tacacs+** au lieu de **tacacs+**, ainsi les instructions telles que l'**enable de l'aaa authentication login default tacacs+** apparaissent pendant qu'**enable du groupe tacacs+ d'aaa authentication login default**.

Consultez la documentation de Logiciel Cisco IOS pour plus d'informations complètes sur des commandes du routeur.

## Conditions préalables

## Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

## Composants utilisés

Les informations de ce document sont basées sur la version du logiciel Cisco IOS 11.3.3 et la version du logiciel Cisco IOS 12.0.5.T et plus tard.

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.

## Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

# Authentification

Procédez comme suit :

1. Veillez à avoir compilé le code TACACS+ (TAC+) sur le serveur unix.Les configurations du serveur ici sont basées sur le code de serveur Cisco TAC+. Les configurations du routeur devraient fonctionner si le code de serveur est code de serveur Cisco. TAC+ doit être exécuté comme racine ; le su à enraciner s'il y a lieu.
2. Copiez le test_file à la fin de ce document, placez-le sur le serveur TAC+, et nommez-le **test_file**.Vérifiez si **tac_plus_executable de** démon débute avec **test_file**. Dans cette commande, l'option **-P** vérifie les erreurs de compilation mais ne commencent pas le démon :Vous pourriez consulter le contenu de test_file faire descendre l'écran la fenêtre, mais vous ne devriez pas consulter des messages tels que ne pouvez pas rechercher le fichier, texte clair prévu--texte clair, ou inattendu recherché}. S'il y a des erreurs, vérifiez les chemins de au test_file, revérifiez votre saisie et essayez à nouveau avant que vous continuiez.
3. Début pour configurer TAC+ sur le routeur.Entrez dans le **mode enable** et tapez **configure terminal** avant de configurer la commande. Cette syntaxe de commande assure que vous n'êtes pas verrouillé hors du routeur au début, fournissant le **tac_plus_executable** n'exécute pas :

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of
authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are
names of lists, and the methods !--- listed on the same lines are the methods !--- in the
order to be tried. As used here, if !--- authentication fails due to the !---
tac_plus_executable not being started, the !--- enable password is accepted because !--- it
is in each list.         !        aaa authentication login linmethod tacacs+ enable   aaa
authentication login vtymethod tacacs+ enable   aaa authentication login conmethod tacacs+
enable   !   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to
prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed
38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to
prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
vtymethod
```

4. Essayer pour être sûr que vous pouvez encore accéder au routeur avec le telnet et par le port de console avant que vous continuiez. Puisque le **tac_plus_executable** n'exécute pas, l'**activer mot de passe** devrait être accepté.**Remarque:** Gardez la session de port de console active et restez dans le mode enable. Cette session ne devrait pas expirer. L'access au routeur est limité en ce moment, et vous devez pouvoir apporter des modifications de configuration sans se verrouiller.Émettez ces commandes de consulter l'interaction de serveur-à-routeur au routeur :*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication vtymethod
5. Comme racine, lancez TAC+ sur le serveur :*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication vtymethod
6. Vérifiez pour être TAC+ sûr commencé :*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication vtymethod**OU***!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-

```
timeout 0 0 login authentication vtymethod
```
Si TAC+ ne démarre pas, c'est normalement un problème de syntaxe dans le test_file. Revenez à l'étape 1 pour corriger ceci.

7. Tapez **tail -f /var/tmp/tac_plus.log** pour consulter l'interaction du routeur au serveur.**Remarque:** L'option -d 16 dans l'étape 5 permet d'envoyer une sortie de toutes les transactions à /var/tmp/tac_plus.log.
8. Les utilisateurs du telnet (VTY) doivent maintenant s'authentifier par TAC+.Avec le débogage allant sur le routeur et le serveur (étapes 4 et 7), telnet entre dans le routeur d'une autre partie du réseau.Le routeur produit une invitation de nom d'utilisateur et mot de passe, pour vous :
```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list.         !         aaa authentication login linmethod tacacs+ enable   aaa authentication login vtymethod tacacs+ enable   aaa authentication login conmethod tacacs+ enable   !   !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod
```
L'authenuser d'utilisateur appartient au groupe admin avec le mot de passe admin.Observez le serveur et le routeur où vous pouvez voir l'interaction TAC+ ? ce qui est envoyé où, des réponses, des demandes, et ainsi de suite. Corrigez tous les problèmes avant que vous continuiez.
9. Si vous voulez également que vos utilisateurs s'authentifient par TAC+ afin d'entrer dans le mode enable, assurez-vous que votre session de port de console est toujours en activité et ajoutez cette commande au routeur :
```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list.         !         aaa authentication login linmethod tacacs+ enable   aaa authentication login vtymethod tacacs+ enable   aaa authentication login conmethod tacacs+ enable   !   !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod
```
Les utilisateurs doivent maintenant s'activer par TAC+.
10. Avec le débogage allant sur le routeur et le serveur (étapes 4 et 7), telnet entre dans le routeur d'une autre partie du réseau. Le routeur produit une invitation de nom d'utilisateur et mot de passe, pour vous :
```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list.         !         aaa authentication login linmethod tacacs+ enable   aaa authentication login vtymethod tacacs+ enable   aaa authentication login conmethod tacacs+ enable   !   !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login
```

```
authentication vtymethod
```
Quand vous écrivez le mode enable, le routeur demande un mot de passe, auquel vous répondez :
```
!--- Turn on TAC+. aaa new-model enable password whatever
!--- These are lists of authentication methods. !--- "linmethod", "vtymethod",
"conmethod", and !--- so on are names of lists, and the methods !--- listed on the same
lines are the methods !--- in the order to be tried. As used here, if !--- authentication
fails due to the !--- tac_plus_executable not being started, the !--- enable password is
accepted because !--- it is in each list.         !         aaa authentication login
linmethod tacacs+ enable    aaa authentication login vtymethod tacacs+ enable    aaa
authentication login conmethod tacacs+ enable    !    !--- Point the router to the server,
where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0
password whatever !--- No time-out to prevent being locked out !--- during debugging.
exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod
modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty
0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging.
exec-timeout 0 0 login authentication vtymethod
```
Observez le serveur et le routeur où vous devriez voir l'interaction TAC+ ? ce qui est envoyé où, des réponses, des demandes, et ainsi de suite. Corrigez tous les problèmes avant que vous continuiez.

11. Réduisez le processus TAC+ sur le serveur en étant connecté toujours au port de console pour être sûr que vos utilisateurs puissent encore accéder au routeur si TAC+ est en panne :
```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of
authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are
names of lists, and the methods !--- listed on the same lines are the methods !--- in the
order to be tried. As used here, if !--- authentication fails due to the !---
tac_plus_executable not being started, the !--- enable password is accepted because !---
it is in each list.         !         aaa authentication login linmethod tacacs+ enable
aaa authentication login vtymethod tacacs+ enable    aaa authentication login conmethod
tacacs+ enable    !    !--- Point the router to the server, where #.#.#.# !--- is the server
IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to
prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed
38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out
to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
vtymethod
```
**ou**
```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are
names of lists, and the methods !--- listed on the same lines are the methods !--- in the
order to be tried. As used here, if !--- authentication fails due to the !---
tac_plus_executable not being started, the !--- enable password is accepted because !---
it is in each list.         !         aaa authentication login linmethod tacacs+ enable
aaa authentication login vtymethod tacacs+ enable    aaa authentication login conmethod
tacacs+ enable    !    !--- Point the router to the server, where #.#.#.# !--- is the server
IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to
prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed
38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out
to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
vtymethod
```
Répétez le telnet et l'activation de l'étape précédente. Le routeur se rend alors compte que le processus TAC+ ne réagit pas et permet aux utilisateurs de se connecter et s'activer avec le mot de passe par défaut.
12. Recherchez l'authentification de vos utilisateurs de port de console par TAC+. Afin de faire ceci, amenez le lancez le serveur TAC+ de nouveau (étapes 5 et 6), et démarrez une session Telnet au routeur (qui devrait authentifier par TAC+).Restez connecté par le telnet au routeur dans le mode enable jusqu'à ce que vous soyez sûr que vous pouvez vous connecter au routeur par le port de console.Déconnectez-vous de votre connexion initiale au routeur par le port de console, puis reconnectez-vous au port de console. L'authentification de port de console à se connecter et activer utilisant des identifiants et mots de passe (montrés dans l'étape 10) se passera maintenant par TAC+.
13. Tandis que vous restez connecté par une session Telnet ou le port de console, et avec le

débogage exécuté sur routeur et serveur (étapes 4 et 7), établissez une connexion par modem à la ligne 1.Les utilisateurs de la ligne doivent se connecter et s'activer maintenant par TAC+.Le routeur produit une invitation de nom d'utilisateur et mot de passe, pour vous :

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of
authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are
names of lists, and the methods !--- listed on the same lines are the methods !--- in the
order to be tried. As used here, if !--- authentication fails due to the !---
tac_plus_executable not being started, the !--- enable password is accepted because !---
it is in each list.         !         aaa authentication login linmethod tacacs+ enable
aaa authentication login vtymethod tacacs+ enable    aaa authentication login conmethod
tacacs+ enable    !    !--- Point the router to the server, where #.#.#.# !--- is the server
IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to
prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed
38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out
to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
vtymethod
```

Quand vous entrez en mode enable, le routeur demande un mot de passe.Réponse :

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are
lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so
on are names of lists, and the methods !--- listed on the same lines are the methods !---
in the order to be tried. As used here, if !--- authentication fails due to the !---
tac_plus_executable not being started, the !--- enable password is accepted because !---
it is in each list.         !         aaa authentication login linmethod tacacs+ enable
aaa authentication login vtymethod tacacs+ enable    aaa authentication login conmethod
tacacs+ enable    !    !--- Point the router to the server, where #.#.#.# !--- is the server
IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to
prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed
38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out
to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
vtymethod
```

Observez le serveur et le routeur où vous voyez l'interaction TAC+ ? ce qui est envoyé où, des réponses, des demandes, et ainsi de suite. Corrigez tous les problèmes avant que vous continuiez.Les utilisateurs doivent maintenant s'activer par TAC+.

## Ajoutez l'autorisation

Ajouter l'autorisation est facultatif.

Par défaut, il y a trois niveaux de commande sur le routeur :

- niveau de privilège 0 incluant désactivation, activation, sortie, aide et déconnexion
- niveau de privilège 1 - niveau normal sur un telnet - l'invitation indique router>
- niveau de privilège 15 - niveau d'activation - l'invite indique router#

Puisque les commandes disponibles dépendent de l'ensemble de fonctionnalités d'IOS, de la version Cisco IOS, du modèle de routeur, etc., il n'y a pas une liste complète de toutes les commandes aux niveaux 1 et 15. Par exemple, le **show ipx route** n'est pas présent dans un jeu de fonctionnalités d'IP seulement, le **transport nat de show ip** n'est pas présent dans la version du logiciel Cisco IOS 10.2.x parce que NAT n'a pas été introduit, et le **show environment** n'est pas présent dans les modèles du routeur sans alimentation électrique et contrôle de température. Les commandes disponibles dans un routeur particulier à un niveau particulier peuvent être recherchées quand vous écrivez a **?** à l'invite du routeur correspondant à ce niveau de privilège.

L'autorisation de port de console n'a pas été ajoutée comme fonctionnalité jusqu'à ce que le Cisco bug ID CSCdi82030 (clients enregistrés seulement) ait été mis en application. L'autorisation de

port de console est désactivée par défaut pour diminuer le risque que vous soyez accidentellement verrouillé hors du routeur. Si un utilisateur a un accès physique au routeur par la console, l'autorisation de port de console n'est pas extrêmement pertinente. Cependant, l'autorisation de port de console peut être activée sous la ligne l'escroquerie 0 dans une image que le Cisco bug ID CSCdi82030 (clients enregistrés seulement) a été mis en application avec la commande :

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication
methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the
methods !--- listed on the same lines are the methods !--- in the order to be tried. As used
here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !-
-- enable password is accepted because !--- it is in each list.          !         aaa
authentication login linmethod tacacs+ enable    aaa authentication login vtymethod tacacs+
enable    aaa authentication login conmethod tacacs+ enable    !    !--- Point the router to the
server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0
password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-
timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut
transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password
whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0
login authentication vtymethod
```

1. Le routeur peut être configuré pour autoriser des commandes par TAC+ à tous les niveau ou certains niveaux.Cette configuration du routeur permet à tous les utilisateurs d'avoir l'autorisation par-commande installée sur le serveur. Ici nous autorisons toutes les commandes par TAC+, mais si le serveur est en panne, aucune autorisation n'est nécessaire.
```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are
names of lists, and the methods !--- listed on the same lines are the methods !--- in the
order to be tried. As used here, if !--- authentication fails due to the !---
tac_plus_executable not being started, the !--- enable password is accepted because !--- it
is in each list.          !         aaa authentication login linmethod tacacs+ enable    aaa
authentication login vtymethod tacacs+ enable    aaa authentication login conmethod tacacs+
enable    !    !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to
prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed
38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to
prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
vtymethod
```
2. Tandis que le serveur TAC+ fonctionne, Telnet dans le routeur avec l'identifiant **authenuser**.Puisque l'authenuser a le service par défaut = autorisation de test_file, cet utilisateur devrait pouvoir remplir toutes les fonctions.Dans le routeur, entrez le **mode enable**, et activez le débogage d'autorisation :
```
!--- Turn on TAC+. aaa new-model enable password
whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod",
"conmethod", and !--- so on are names of lists, and the methods !--- listed on the same
lines are the methods !--- in the order to be tried. As used here, if !--- authentication
fails due to the !--- tac_plus_executable not being started, the !--- enable password is
accepted because !--- it is in each list.          !         aaa authentication login
linmethod tacacs+ enable    aaa authentication login vtymethod tacacs+ enable    aaa
authentication login conmethod tacacs+ enable    !    !--- Point the router to the server,
where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0
password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-
timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem
InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4
password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-
timeout 0 0 login authentication vtymethod
```
3. Telnet dans le routeur avec l'identifiant **authoruser** et l'**opérateur de** mot de passe.Cet utilisateur ne peut pas faire afficher la **traceroute de** deux commandes et **se déconnecter** (consultez le test_file).Observez le serveur et le routeur où vous pouvez consulter

l'interaction TAC+ - ce qui est envoyé où, des réponses, des requêtes et ainsi de suite. Corrigez tous les problèmes avant que vous continuiez.

4. Si vous voulez configurer un utilisateur pour une autocommande, éliminez la position transitoire de l'utilisateur - dans le test_file, et saisissez une destination valide d'adresse IP au lieu du #.#.#.#.Arrêtez et mettez en marche le serveur TAC+.Sur le routeur :`!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod`Telnet au routeur avec l'identifiant **transitoire** et le mot de passe **transitoire**. **Le telnet #.#.#.#** exécute et la position transitoire d'utilisateur est envoyée à l'autre emplacement.

## Ajoutez la gestion des comptes

L'ajout de la comptabilité est facultatif.

La référence au fichier comptable est dans test_file ? fichier comptable = /var/log/tac.log. Mais la gestion des comptes n'a pas lieu à moins d'être configuré dans le routeur (à condition que le routeur exécute une version du logiciel Cisco IOS plus récente que 11,0).

1. Activer la gestion des comptes dans le routeur :`!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod`**Remarque:** La comptabilité AAA ne prend pas en charge la comptabilité par commande dans certaines versions. Une solution serait d'utiliser l'autorisation par commande et de rapporter l'occurrence dans le fichier de la comptabilité. (Consultez Cisco bug ID CSCdi44140.) Si vous utilisez une image où cette réparation est utilisée [versions du logiciel Cisco IOS 11.2(1.3)F, 11.2(1.2), 11.1(6.3), 11.1(6.3)AA01, 11.1(6.3)CA à partir du 24 septembre 1997] vous pouvez également activer command-accounting.
2. Tandis que TAC+ fonctionne sur le serveur, sélectionnez cette commande sur le serveur afin de consulter les entrées qui sont incluses dans le fichier comptable :`!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--`

```
- enable password is accepted because !--- it is in each list.          !         aaa
authentication login linmethod tacacs+ enable    aaa authentication login vtymethod tacacs+
enable    aaa authentication login conmethod tacacs+ enable    !    !--- Point the router to
the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line
con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging.
exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod
modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0
4 password whatever !--- No time-out to prevent being locked out !--- during debugging.
exec-timeout 0 0 login authentication vtymethod
```

Connectez et déconnectez-vous alors du routeur, telnet hors du routeur, et ainsi de suite. S'il y a lieu, entrez sur le routeur :

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication
methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and
the methods !--- listed on the same lines are the methods !--- in the order to be tried. As
used here, if !--- authentication fails due to the !--- tac_plus_executable not being
started, the !--- enable password is accepted because !--- it is in each list.          !
aaa authentication login linmethod tacacs+ enable    aaa authentication login vtymethod
tacacs+ enable    aaa authentication login conmethod tacacs+ enable    !    !--- Point the
router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host
#.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !---
during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login
authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400
flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being
locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod
```

## Fichier de test

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication
methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the
methods !--- listed on the same lines are the methods !--- in the order to be tried. As used
here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !-
-- enable password is accepted because !--- it is in each list.          !         aaa
authentication login linmethod tacacs+ enable    aaa authentication login vtymethod tacacs+
enable    aaa authentication login conmethod tacacs+ enable    !    !--- Point the router to the
server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0
password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-
timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut
transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password
whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0
login authentication vtymethod
```

**Remarque:** Ce message d'erreur est généré si votre serveur TACACS n'est pas accessible :

```
%AAAA-3-DROPACCTSNDFAIL : l'enregistrement des comptes déposé, envoi au serveur a manqué :
```

démarrage du système. Vérifiez que le serveur TACACS+ est bien opérationnel.

# Informations connexes

- Sécurité d'accès d'utilisateur unique au réseau TACACS+
- Terminal Access Controller Access Control System
- Cisco Secure Access Control Server pour Windows
- Support et documentation techniques - Cisco Systems