# Exemple de configuration des mots de passe Telnet, console et ports auxiliaires sur les routeurs Cisco

## Contenu



# Introduction

Ce document fournit des exemples de configuration pour configurer la protection par mot de passe des connexions d'arrivée EXEC au routeur.

# Conditions préalables

## Conditions requises

Afin d'effectuer les tâches décrites dans ce document, vous devez avoir un accès EXEC privilégié à l'interface de ligne de commande (CLI) du routeur. Pour des informations sur l'utilisation de la

ligne de commande et pour comprendre les modes de commande, référez-vous à Utilisation du logiciel Cisco IOS.

Pour des instructions sur la façon de connecter une console à votre routeur, référez-vous à la documentation fournie avec votre routeur ou à la documentation en ligne pour votre matériel.

### Composants utilisés

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

- Routeur Cisco 2509
- Logiciel Cisco IOS® Version 12.2(19)

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 de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

## Informations générales

L'utilisation de la protection par mot de passe pour contrôler ou restreindre l'accès à l'interface de ligne de commande (CLI) de votre routeur est l'un des éléments fondamentaux d'un plan global de sécurité.

La protection du routeur contre l'accès à distance non autorisé, en général Telnet, est la sécurité la plus courante qui a besoin d'être configurée, mais la protection du routeur de l'accès local non autorisé ne peut pas être négligée.

**Remarque:** La protection par mot de passe est juste une des nombreuses étapes que vous devriez utiliser dans un système approfondi et efficace de sécurité du réseau. Les pare-feux, les listes d'accès et le contrôle de l'accès physique au matériel sont d'autres éléments qui doivent être considérés lors de la mise en œuvre de votre plan de sécurité.

L'accès à la ligne de commande, ou EXEC, à un routeur peut être fait de façons diverses, mais dans tous les cas la connexion en entrée au routeur est établie sur une ligne TTY. Il y a quatre grands types de ligne TTY, comme vu dans cet exemple de sortie **show line** :

```
2509#show line Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int * 0 CTY - - - - - 0
0 0/0 - 1 TTY 9600/9600 - - - - - 0 0 0/0 - 2 TTY 9600/9600 - - - - - 0 0 0/0 - 3 TTY 9600/9600
- - - - - 0 0 0/0 - 4 TTY 9600/9600 - - - - - 0 0 0/0 - 5 TTY 9600/9600 - - - - - 0 0 0/0 - 6
TTY 9600/9600 - - - - - 0 0 0/0 - 7 TTY 9600/9600 - - - - - 0 0 0/0 - 8 TTY 9600/9600 - - - - -
0 0 0/0 - 9 AUX 9600/9600 - - - - - 0 0 0/0 - 10 VTY - - - - - 0 0 0/0 - 11 VTY - - - - - 0 0
0/0 - 12 VTY - - - - - 0 0 0/0 - 13 VTY - - - - - 0 0 0/0 - 14 VTY - - - - - 0 0 0/0 - 2509#
```

Le type de ligne **CTY** est le port de console. Sur n'importe quel routeur, il apparaît dans la configuration du routeur comme **line con 0** et dans la sortie de la commande **show line** comme **cty**. Le port de console est principalement utilisé pour un l'accès système local à l'aide d'un terminal de

console.

Les **lignes TTY** sont les lignes asynchrones utilisées pour les connexions entrantes ou sortantes du modem et du terminal et peuvent être vues dans une configuration de routeur ou de serveur d'accès en tant que **line x.** Les numéros de ligne spécifiques sont une fonction du matériel intégré ou installé sur le routeur ou le serveur d'accès.

La ligne **AUX** est le port auxiliaire, vu dans configuration en tant que **line aux 0**.

Les lignes **VTY** sont les lignes du terminal virtuel du routeur, utilisées seulement pour contrôler les connexions d'arrivée de Telnet. Elles sont virtuelles dans le sens où qu'elles sont une fonction du logiciel - aucun matériel ne leur est associé. Elles apparaissent dans la configuration en tant que **line vty 0 4.**

Chacun de ces types de ligne peut être configuré avec la protection par mot de passe. Des lignes peuvent être configurées pour utiliser un mot de passe pour tous les utilisateurs ou pour des mots de passe spécifiques au utilisateur. Des mots de passe spécifiques à des utilisateurs peuvent être configurés localement sur le routeur, ou vous pouvez utiliser un serveur d'authentification pour fournir l'authentification.

Il n'y a aucune interdiction de configurer différentes lignes avec des types différents de protection par mot de passe. Il est, en fait, courant de voir des routeurs avec un mot de passe unique pour la console et des mots de passe spécifiques aux utilisateurs pour d'autres connexions entrantes.

Voici ci-dessous un exemple de sortie du routeur de la commande **show running-config**:

```
2509#show running-config Building configuration... Current configuration : 655 bytes ! version 12.2 . . . !--- Configuration edited for brevity line con 0 line 1 8 line aux 0 line vty 0 4 ! end
```

# Configurer les mots de passe sur la ligne

Pour spécifier un mot de passe sur une ligne, utilisez la commande **password** dans le mode de configuration de la ligne. Pour activer la vérification du mot de passe à la connexion, utilisez la commande **login** dans le mode de configuration de la ligne.

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

## Procédure de configuration

Dans cet exemple, un mot de passe est configuré pour tous les utilisateurs essayant d'utiliser la console.

1. Àpartir de l'invite EXEC privilégié (ou « enable »), entrez le mode de configuration, puis passez au mode de configuration de la ligne à l'aide des commandes suivantes. Notez que l'invite change pour refléter le mode en cours.`router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. router(config)#line con 0 router(config-line)#`
2. Configurez le mot de passe et activez la vérification des mots de passe à la connexion.`router(config-line)#password letmein router(config-line)#login`
3. Quittez le mode de configuration.`router(config-line)#end router# %SYS-5-CONFIG_I: Configured from console by console` **Remarque:** Ne sauvegardez pas les changements de configuration à

**line con 0** jusqu'à ce que votre capacité à vous connecter ait été vérifiée.

**Remarque:** Dans la configuration de la console de ligne, **login** est une commande de configuration requise pour activer la vérification des mots de passe à la connexion. L'authentification de la console exige le fonctionnement à la fois des commandes **password** et **login**.

## Vérifier la configuration

Examinez configuration du routeur pour vérifier que les commandes ont été correctement saisies :

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show running-config** - affiche la configuration en cours du routeur.`router#show running-config Building configuration... ... !--- Lines omitted for brevity ! line con 0 password letmein login line 1 8 line aux 0 line vty 0 4 ! end` Pour tester la configuration, fermez la session de la console et connectez-vous de nouveau à l'aide du mot de passe configuré pour accéder au routeur :`router#exit router con0 is now available Press RETURN to get started. User Access Verification Password: !--- Password entered here is not displayed by the router router>`
  **Remarque:** Avant d'exécuter ce test, assurez-vous que vous avez une autre connexion dans le routeur, telle que Telnet ou Dial-In, au cas où il y aurait un problème de connexion de nouveau dans le routeur.

## Échec du dépannage de la connexion

Si vous ne pouvez pas vous reconnecter au routeur et que vous n'avez pas sauvegardé la configuration, recharger le routeur éliminera tout changement de configuration que vous avez fait.

Si les modifications de configuration ont été sauvegardées et que vous ne pouvez pas vous connecter au routeur, vous devrez exécuter une récupération du mot de passe. Référez-vous à Procédures de récupération des mots de passe pour obtenir les instructions pour votre plate-forme particulière.

# Configurer les mots de passe spécifiques aux utilisateurs locaux

Pour établir un système d'authentification basée sur les noms d'utilisateur, utilisez la commande **username** dans le mode de configuration globale. Pour activer la vérification du mot de passe à la connexion, utilisez la commande **login local** dans le mode de configuration de la ligne.

## Procédure de configuration

Dans cet exemple, des mots de passe sont configurés pour des utilisateurs essayant de se connecter au routeur sur les lignes VTY à l'aide de Telnet.

1. À l'invite EXEC privilégié (ou « enable »), entrez le mode de configuration et entrez les combinaisons nom d'utilisateur/mot de passe, une pour chaque utilisateur auquel vous voulez permettre l'accès au routeur :`router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. router(config)#username russ password montecito router(config)#username cindy password belgium router(config)#username mike password rottweiler`
2. Passez au mode de configuration de la ligne à l'aide des commandes suivantes. Notez que

l'invite change pour refléter le mode en cours.`router(config)#`**`line vty 0 4`** `router(config-line)#`

3. Configurez la vérification des mots de passe à la connexion.`router(config-line)#`**`login local`**
4. Quittez le mode de configuration.`router(config-line)#`**`end`** `router# %SYS-5-CONFIG_I: Configured from console by console` **Remarque:** Afin de désactiver le Telnet automatique quand vous entrez un nom sur la CLI, configurez **no logging preferred** sur la ligne utilisée. Tandis que **transport preferred none** fournit la même sortie, il désactive également le Telnet automatique pour le hôte défini qui est configuré avec la commande **ip host**. Ceci est différent de la commande **no logging preferred**, qui l'arrête pour les hôtes non définis et le laisse fonctionner pour les hôtes définis.

## Vérifier la configuration

Examinez configuration du routeur pour vérifier que les commandes ont été correctement saisies :

- **show running-config** - affiche la configuration en cours du routeur.`router#`**`show running-config`** `Building configuration... ! !--- Lines omitted for brevity !` **`username russ password 0 montecito username cindy password 0 belgium username mike password 0 rottweiler`** `! !--- Lines omitted for brevity ! line con 0 line 1 8 line aux 0 line vty 0 4` **`login local`** `! end` Pour tester cette configuration, une connexion Telnet doit être faite au routeur. Ceci peut être fait en se connectant depuis un hôte différent sur le réseau, mais vous pouvez également tester depuis le routeur lui-même en effectuant une connexion Telnet à l'adresse IP d'interface sur le routeur qui est dans un état up/up, comme vu dans la sortie de la commande **show interfaces**.Voici un exemple de sortie si l'adresse d'**interface ethernet 0** était 10.1.1.1 :`router#`**`telnet 10.1.1.1`** `Trying 10.1.1.1 ... Open User Access Verification Username: mike Password: !--- Password entered here is not displayed by the router router`

## Dépanner l'échec du mot de passe spécifique à l'utilisateur

Les noms d'utilisateur et mots de passe distinguent les majuscules et minuscules. Des utilisateurs essayant de se connecter avec un nom d'utilisateur ou un mot de passe avec une mauvaise casse seront rejetés.

Si les utilisateurs ne peuvent pas se connecter au routeur avec leur mot de passe spécifique, reconfigurez le nom d'utilisateur et le mot de passe sur le routeur.

# Configurez la ligne AUX. mot de passe

Afin de spécifier un mot de passe sur la ligne AUX., émettez la commande de **mot de passe** dans la ligne mode de configuration. Afin d'activer le mot de passe vérifiant à la procédure de connexion, émettez la **commande login** dans la ligne mode de configuration.

## Procédure de configuration

Dans cet exemple, un mot de passe est configuré pour tous les utilisateurs tentant d'utiliser le port auxiliaire.

1. Émettez la commande de **show line** afin de vérifier la ligne utilisée par le port auxiliaire.`R1#`**`show line`** `Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int * 0 CTY`

```
- - - - - 0 0 0/0 - 65 AUX 9600/9600 - - - - - 0 1 0/0 - 66 VTY - - - - - 0 0 0/0 - 67 VTY
- - - - - 0 0 0/0 -
```

2. Dans cet exemple, le port auxiliaire est sur la ligne 65. Émettez ces commandes afin de configurer la ligne AUX du routeur :`R1# conf t R1(config)# line 65 R1(config-line)#modem inout R1(config-line)#speed 115200 R1(config-line)#transport input all R1(config-line)#flowcontrol hardware R1(config-line)#login R1(config-line)#password cisco R1(config-line)#end R1#`

## Vérifiez la configuration

Examinez la configuration du routeur afin de vérifier que les commandes ont été correctement sélectionnées :

- **La commande show running-config** affiche la configuration en cours du routeur :`R1#show running-config Building configuration... ! !--- Lines omitted for brevity. line aux 0 password cisco login modem InOut transport input all speed 115200 flowcontrol hardware !--- Lines omitted for brevity. ! end`

# Configurer l'authentification AAA pour la connexion

Pour activer l'authentification, l'autorisation et l'authentification de la comptabilité (AAA, pour authentication, authorization, and accounting) des procédures de connexion, utilisez la commande **login authentication** dans le mode de configuration de la ligne. Les services AAA doivent également être configurés.

## Procédure de configuration

Dans cet exemple, le routeur est configuré pour récupérer les mots de passe d'utilisateurs depuis un serveur TACACS+ quand les utilisateurs essayent de se connecter au routeur.

**Remarque:** La configuration du routeur pour utiliser d'autres types de serveurs AAA (RADIUS, par exemple) est semblable. Référez-vous à Configuration de l'authentification pour des informations supplémentaires.

**Remarque:** Ce document ne traite pas de la configuration du serveur AAA lui-même. Référez-vous à Protocoles de serveur de sécurité pour des informations sur la configuration du serveur AAA.

1. À l'invite EXEC privilégié (ou « enable »), entrez le mode de configuration et sélectionnez les commandes pour configurer le routeur pour qu'il utilise les services AAA pour l'authentification :`router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. router(config)#aaa new-model router(config)#aaa authentication login my-auth-list tacacs+ router(config)#tacacs-server host 192.168.1.101 router(config)#tacacs-server key letmein`
2. Passez au mode de configuration de la ligne à l'aide des commandes suivantes. Notez que l'invite change pour refléter le mode en cours.`router(config)#line 1 8 router(config-line)#`
3. Configurez la vérification des mots de passe à la connexion.`router(config-line)#login authentication my-auth-list`
4. Quittez le mode de configuration.`router(config-line)#end router# %SYS-5-CONFIG_I: Configured from console by console`

## Vérifier la configuration

Examinez configuration du routeur pour vérifier que les commandes ont été correctement saisies :

- **show running-config** - affiche la configuration en cours du routeur.`router#write terminal Building configuration... Current configuration: ! version 12.0 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname router ! aaa new-model aaa authentication login my-auth-list tacacs+ ! !--- Lines omitted for brevity ... ! tacacs-server host 192.168.1.101 tacacs-server key letmein ! line con 0 line 1 8 login authentication my-auth-list line aux 0 line vty 0 4 ! end`

Pour tester cette configuration particulière, une connexion entrante ou sortante doit être établie sur la ligne. Référez-vous à Guide de connexion du modem-routeur pour des informations spécifiques sur la configuration des lignes asynchrones pour des connexions par modem.

Alternativement, vous pouvez configurer une ou plusieurs lignes VTY pour qu'elles exécutent authentification AAA et pour réaliser votre test à partir de là.

## Échec du dépannage de la connexion AAA

Avant d'émettre des commandes **Debug**, référez-vous à Informations importantes sur les commandes Debug.

Pour dépanner un échec de tentative de connexion, utilisez la commande **debug** qui correspond à votre configuration :

- debug aaa authentication
- debug radius
- debug kerberos

# Informations connexes

- Configuration de l'authentification
- Référence des commandes de débogage Cisco IOS
- Support technique - Cisco Systems