Configurer l’AAA de base sur un serveur d’accès

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Conventions
  - Composants utilisés
- Informations générales
  - Diagramme du réseau
- Configuration générale de AAA
  - Activer le protocole AAA
  - Spécifier le serveur AAA externe
  - Configuration du serveur AAA
- Configuration de l’authentification
  - Authentification de connexion
    - Exemple 1 : Accès en exécution avec Radius puis Local
    - Exemple 2 : Accès à la console avec mot de passe de ligne
    - Exemple 3 : Activer le mode d’accès utilisé avec le serveur AAA externe
  - Authentification PPP
    - Exemple 1 : Méthode d’authentification PPP unique pour tous les utilisateurs
    - Exemple 2 : Authentification PPP utilisée avec une liste spécifique
    - Exemple 3 : Protocole PPP lancé à partir d’une session en mode caractère
- Configuration de l’autorisation
  - Autorisation exec
    - Exemple 1 : Mêmes méthodes d’authentification en exécution pour tous les utilisateurs
    - Exemple 2 : Attribution de niveaux de privilèges d’exécution à partir du serveur AAA
    - Exemple 3 : Attribution d’un délai d’inactivité à partir du serveur AAA
  - Autorisation de réseau
    - Exemple 1 : Mêmes méthodes d’autorisation de réseau pour tous les utilisateurs
    - Exemple 2 : Appliquer des attributs propres à l’utilisateur
    - Exemple 3 : Autorisation PPP avec une liste précise
- Configuration de la traçabilité
  - Exemples de configuration de la traçabilité
    - Exemple 1 : Générer des enregistrements de traçabilité de début et de fin
    - Exemple 2 : Générer uniquement des enregistrements de traçabilité de fin
    - Exemple 3 : Générer des enregistrements de ressources pour les échecs d'authentification et de négociation
    - Exemple 4 : Activer la traçabilité complète des ressources
- Informations connexes

Introduction

Ce document décrit comment configurer le protocole AAA (authentication, authorization and accounting) sur un routeur Cisco avec les protocoles Radius ou TACACS+.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Conventions

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

Composants utilisés

Les renseignements contenus dans ce document sont basés sur la branche principale de la version logicielle 12 de Cisco IOS®.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

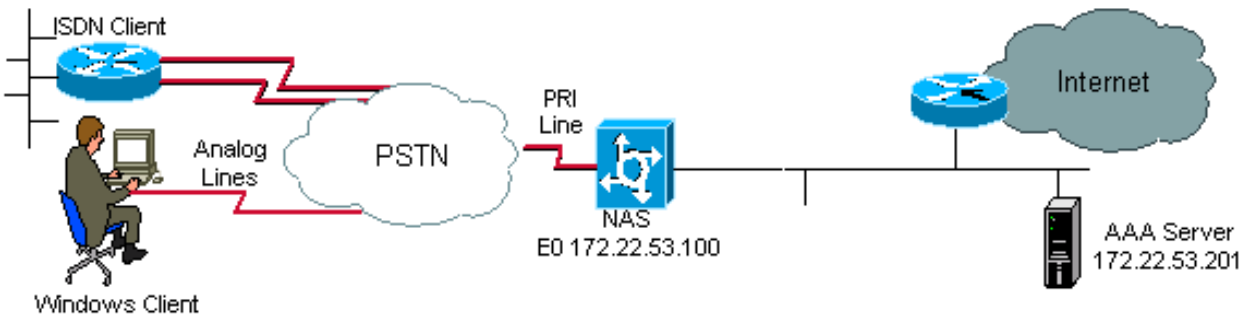
Informations générales

Ce document explique comment configurer le protocole AAA (authentication, authorization and accounting) sur un routeur Cisco avec les protocoles Radius ou TACACS+. Le but de ce document n'est pas de couvrir toutes les fonctionnalités d'AAA, mais d'expliquer les commandes principales et fournir quelques exemples et lignes directrices.

Remarque : Consultez la section sur la configuration générale du protocole AAA avant de procéder à la configuration de Cisco IOS. Le non-respect de cette consigne peut entraîner une mauvaise configuration et un verrouillage ultérieur.

Pour en savoir plus, consultez le Guide de configuration du protocole AAA (authentication, authorization and accounting).

Diagramme du réseau



Configuration générale de AAA

Activer le protocole AAA

Pour activer AAA, vous devez configurer la commande aaa new-model en configuration globale.

Remarque : Tant que cette commande n’est pas activée, toutes les autres commandes du protocole AAA sont masquées.

Avertissement : La commande aaa new-model applique immédiatement l’authentification locale à toutes les lignes et interfaces (à l’exception de la ligne de console ligne con 0). Si une session Telnet est ouverte vers le routeur après l’activation de cette commande (ou si une connexion expire et doit être reconnectée), l’utilisateur doit s’authentifier avec la base de données locale du routeur. Il est recommandé de définir un nom d’utilisateur et un mot de passe sur le serveur d’accès avant de commencer la configuration du protocole AAA afin de ne pas être bloqué du routeur. Voir l’exemple de code suivant.

<#root>

```
Router(config)#
```

username xxx password yyy

Conseil : avant de configurer vos commandes AAA, save votre configuration. Vous ne pouvez save réactiver la configuration qu'après avoir terminé votre configuration AAA (et être certain qu'elle fonctionne correctement). Cela vous permet de vous rétablir d’un verrouillage inattendu, car vous pouvez annuler toute modification en rechargeant le routeur.

Spécifier le serveur AAA externe

En configuration globale, définissez le protocole de sécurité utilisé avec AAA (Radius, TACACS+). Si vous ne voulez utiliser aucun de ces deux protocoles, vous pouvez utiliser la base de données locale sur le routeur.

Si vous utilisez TACACS+, saisissez la commande tacacs-server host<IP address of the AAA server> <key> .

Si vous utilisez Radius, saisissez la commande radius-server host<IP address of the AAA server> <key> .

Configuration du serveur AAA

Sur le serveur AAA, configurez les paramètres suivants :

- Le nom du serveur d'accès.
- L'adresse IP que le serveur d'accès l'utilise pour communiquer avec le serveur AAA.

> Remarque : Si les deux appareils se trouvent sur le même réseau Ethernet, par défaut, le serveur d’accès utilise l’adresse IP définie sur l’interface Ethernet lorsqu’il envoie le paquet AAA. Cette question est importante quand le routeur a plusieurs interfaces (et, par conséquent, plusieurs adresses).

- Exactement la même clé <key> configurée dans le serveur d'accès.

> Remarque : La valeur de la clé est sensible à la casse.

- Le protocole utilisé par le serveur d'accès (TACACS+ ou Radius).

Reportez-vous à la documentation de votre serveur AAA pour connaître la procédure exacte utilisée pour configurer les paramètres précédents. Si le serveur AAA n’est pas configuré correctement, les demandes AAA du serveur d’accès au réseau peuvent être ignorées par le serveur AAA et il est possible que la connexion échoue.

Le serveur AAA doit avoir un IP accessible depuis le serveur d'accès (effectuez un test ping pour vérifier la connectivité).

Configuration de l’authentification

L'authentification vérifie les utilisateurs avant qu'ils soient autorisés à l'accéder au réseau et aux services réseau (qui sont vérifiés avec l'autorisation).

Pour configurer l'authentification AAA :

1. Définissez d'abord une liste nommée de méthodes d'authentification (dans le mode de configuration globale).
2. Appliquez cette liste à une ou plusieurs interfaces (dans le mode de configuration de l'interface).

La seule exception est la liste de méthodes par défaut (nommée default). La liste de méthodes par défaut est automatiquement appliquée à toutes les interfaces excepté à celles qui ont une liste de méthodes explicitement définies. Une liste de méthodes définies remplace la liste de méthodes par défaut.

Ces exemples d’authentification utilisent l’authentification Radius, par connexion et PPP (Point-to-Point Protocol) pour expliquer des concepts tels que les méthodes et les listes nommées. Dans

tous les exemples, TACACS+ peut être substitué à Radius ou à l'authentification locale.

Le logiciel Cisco IOS utilise la première méthode listée pour authentifier des utilisateurs. Si cette méthode échoue à réagir (indiqué par une ERREUR), le logiciel Cisco IOS sélectionne la prochaine méthode d'authentification figurant dans la liste de méthodes. Ce processus continue jusqu'à ce qu'une transmission réussisse avec une méthode d'authentification listée ou que toutes les méthodes définies dans la liste de méthodes soient épuisées.

Il est important de noter que le logiciel Cisco IOS essaie d'authentifier avec la méthode d'authentification suivante listée seulement quand il n'y a aucune réponse à la méthode précédente. Si l'authentification échoue à un moment quelconque de ce cycle, c'est-à-dire si les réponses du serveur AAA ou de la base de données locale des noms d'utilisateur sont de refuser l'accès de l'utilisateur (indiqué par un ÉCHEC), le processus d'authentification s'arrête et aucune autre méthode d'authentification n'est tentée.

Pour permettre une vérification de l'utilisateur, vous devez configurer le nom d'utilisateur et le mot de passe sur le serveur AAA.

Authentification de connexion

Vous pouvez utiliser la commande aaa authentication login pour authentifier les utilisateurs qui veulent un accès exec dans le serveur d'accès (tty, vty, console et aux).

Exemple 1 : Accès en exécution avec Radius puis Local

<#root>

```
Router(config)#
```

```
aaa authentication login default group radius local
```

Dans la commande précédente :

- La liste nommée est la liste par défaut (défaut).
- il y a deux méthodes d'authentification (groupe Radius et Local).

Tous les utilisateurs sont authentifiés avec le serveur Radius (la première méthode). Si le serveur Radius ne répond pas, la base de données locale du routeur est utilisée (deuxième méthode). Pour l'authentification locale, définissez le nom d'utilisateur et le mot de passe :

<#root>

```
Router(config)#
```

```
username xxx password yyy
```

Comme la liste par défaut est utilisée dans la commande aaa authentication log, l'authentification par connexion est automatiquement appliquée à toutes les connexions (par exemple tty, vty, console et aux).

Remarque : Le serveur (Radius ou TACACS+) ne peut pas répondre à une demande aaa authentication envoyée par le serveur d'accès s'il n'y a pas de connectivité IP, si le serveur d'accès n'est pas correctement défini sur le serveur AAA ou si le serveur AAA n'est pas correctement défini sur le serveur d'accès.

Remarque : Si vous utilisez l'exemple précédent, sans le mot-clé local, le résultat est le suivant :

<#root>

```
Router(config)#
```

aaa authentication login default group radius

Remarque : Si le serveur AAA ne répond pas à la demande d'authentification, l'authentification échoue (car le routeur n'a pas d'autre méthode à essayer).

Remarque : Le mot-clé group permet de regrouper les hôtes du serveur actuel. La fonctionnalité permet à l'utilisateur de sélectionner un sous-ensemble d'hôtes du serveur configurés et de les utiliser pour un service particulier.

Exemple 2 : Accès à la console avec mot de passe de ligne

Étendez la configuration à partir de l'exemple 1 de sorte que la connexion à la console ne soit authentifiée que par le mot de passe défini sur la ligne con 0.

La liste de CONSOLE est définie, puis appliquée à la ligne de connexion 0.

Configuration:

<#root>

```
Router(config)#
```

aaa authentication login CONSOLE line

Dans la commande précédente :

- la liste nommée est CONSOLE.
- Il y a seulement une méthode d'authentification (ligne).

Lorsqu'une liste nommée (dans cet exemple, CONSOLE) est créée, elle doit être appliquée à une ligne ou à une interface avant son exécution. Pour ce faire, utilisez login authentication

la commande :

<#root>

```
Router(config)#
line con 0

Router(config-line)#
exec-timeout 0 0

Router(config-line)#
password cisco

Router(config-line)#
login authentication CONSOLE
```

La liste de CONSOLE écrase la liste de méthode par défaut sur la ligne de connexion 0. Après cette configuration à la connexion à la ligne con 0, vous devez saisir le mot de passe cisco pour obtenir l'accès à la console. La liste par défaut est toujours utilisée sur tty, vty et aux.

Remarque : Pour que l'accès à la console soit authentifié à l'aide d'un nom d'utilisateur et d'un mot de passe locaux, utilisez l'exemple de code suivant :

<#root>

```
Router(config)#
aaa authentication login CONSOLE local
```

Dans ce cas, un nom d'utilisateur et mot de passe doivent être configurés dans la base de données locale du routeur. La liste doit également être appliquée à la ligne ou à l'interface.

Remarque : Pour qu'il n'y ait pas d'authentification, utilisez l'exemple de code suivant :

<#root>

```
Router(config)#
```

aaa authentication login CONSOLE none

Dans ce cas, il n'y a aucune authentification pour obtenir l'accès à la console. La liste doit également être appliquée à la ligne ou à l'interface.

Exemple 3 : Activer le mode d’accès utilisé avec le serveur AAA externe

Vous pouvez émettre l'authentification pour accéder au mode activer (privilège 15).

Configuration:

<#root>

```
Router(config)#
```

aaa authentication enable default group radius enable

Seul le mot de passe peut être demandé, le nom d’utilisateur est $enab15$. Par conséquent, le nom d'utilisateur $enab15$ doit être défini sur le serveur AAA.

Si le serveur Radius ne répond pas, il se peut qu’il faille saisir le mot de passe d’activation configuré localement sur le routeur.

Authentification PPP

La commande aaa authentication ppp est utilisée pour authentifier une connexion PPP. Il est généralement utilisé pour authentifier les utilisateurs distants analogiques ou de réseau RNIS qui tentent d’accéder à Internet ou à un bureau central par l’intermédiaire d’un serveur d’accès.

Exemple 1 : Méthode d’authentification PPP unique pour tous les utilisateurs

Le serveur d’accès possède une interface de réseau RNIS configurée pour accepter les numéros de clients PPP. Nous utilisons dialer rotary-group 0, mais la configuration peut être effectuée sur l’interface principale ou sur l’interface de profil du composeur.

Configuration:

<#root>

```
Router(config)#
```

aaa authentication ppp default group radius local

Cette commande authentifie tous les utilisateurs PPP avec Radius. Si le serveur Radius ne répond pas, la base de données locale est utilisée.

Exemple 2 : Authentification PPP utilisée avec une liste spécifique

Pour utiliser une liste nommée plutôt que la liste par défaut, configurez les commandes suivantes :

```
<#root>
Router(config)#
aaa authentication ppp ISDN_USER group radius


Router(config)#
interface dialer 0

Router(config-if)#
ppp authentication chap ISDN_USER
```

Dans cet exemple, la liste est ISDN_USER et la méthode est Radius.

Exemple 3 : Protocole PPP lancé à partir d'une session en mode caractère

Le serveur d'accès a une carte de modem interne (Mica, Microcom ou port suivant). Supposons que les commandes aaa authentication log et aaa authentication ppp soient configurées.

Si un utilisateur de modem accède pour la première fois au routeur par une session d'exécution en mode caractère (par exemple, avec une fenêtre de terminal après la numérotation), l'utilisateur est authentifié sur une ligne tty. Pour lancer une session en mode paquet, les utilisateurs doivent saisir ppp default ou ppp. Puisque l'authentification PPP est explicitement configurée (avec aaa authentication ppp), l'utilisateur est authentifié de nouveau au niveau PPP.

Pour éviter cette deuxième authentification, utilisez le mot clé if-needed :

```
<#root>
Router(config)#
aaa authentication login default group radius local
Router(config)#
aaa authentication ppp default group radius local if-needed
```

 Remarque : Si le client démarre directement une session PPP, l'authentification PPP est

effectuée directement, car il n’y a pas d’accès par connexion au serveur d’accès.

Configuration de l’autorisation

L’autorisation permet de pouvez contrôler ce qu’un utilisateur peut faire ou non.

L'autorisation AAA a les mêmes règles que l'authentification :

1. Définissez d'abord une liste nommée de méthodes d'autorisation.
2. Appliquez alors cette liste à une ou plusieurs interfaces (excepté pour la liste de méthodes par défaut).
3. La première méthode énumérée est utilisée. Si elle échoue à répondre, la deuxième est utilisée et ainsi de suite.

Les listes de méthodes sont spécifiques au type d'autorisation demandé. Le présent document porte sur les types d’autorisations Exécution et Réseau.

Pour en savoir plus sur les autres types d’autorisations, consultez le Guide de configuration de la sécurité de Cisco IOS.

Autorisation exec

La commande aaa authorization exec détermine si l'utilisateur est autorisé à exécuter un interpréteur de commandes EXEC. Cette fonction peut renvoyer les renseignements de profil de l’utilisateur tels que les informations de commande automatique, le délai d’inactivité, le délai d’expiration de session, la liste d’accès, les privilèges et d’autres facteurs par utilisateur.

L'autorisation Exec est seulement effectuée sur les lignes vty et tty.

L’exemple suivant utilise Radius.

Exemple 1 : Mêmes méthodes d’authentification en exécution pour tous les utilisateurs

Lorsqu’il est authentifié avec :

<#root>

```
Router(config)#
aaa authentication login default group radius local
```

Tous les utilisateurs qui souhaitent se connecter au serveur d’accès doivent être autorisés avec Radius (première méthode) ou avec une base de données locale (deuxième méthode).

Configuration:

<#root>

```
Router(config)#
```

aaa authorization exec default group radius local

Remarque : Sur le serveur AAA, Service-Type =1 (connexion) doit être sélectionné.

Remarque : Dans cet exemple, si le mot-clé local n'est pas inclus et que le serveur AAA ne répond pas, l'autorisation ne peut être obtenue et il se peut que la connexion échoue.

Remarque : Dans les exemples 2 et 3 suivants, vous n'avez à ajouter aucune commande sur le routeur. Il vous suffit de configurer le profil sur le serveur d'accès.

Exemple 2 : Attribution de niveaux de privilèges d'exécution à partir du serveur AAA

En vous basant sur l'exemple 1, configurez la prochaine paire attribut/valeur de Cisco sur le serveur AAA afin qu'un utilisateur puisse se connecter au serveur d'accès et passer directement en mode d'activation :

```
shell:priv-lvl=15
```

L'utilisateur peut maintenant passer directement au mode d'activation.

Remarque : Si la première méthode ne fonctionne pas, la base de données locale est utilisée. Cependant, l'utilisateur ne peut pas passer directement au mode d'activation, mais doit saisir la commande d'activation et fournir le mot de passe enable.

Exemple 3 : Attribution d'un délai d'inactivité à partir du serveur AAA

Pour configurer un délai d'inactivité (afin que la session soit fermée en cas d'absence de trafic après le délai d'inactivité), utilisez l'attribut IETF Radius 28 : Idle-Timeout sous le profil de l'utilisateur.

Autorisation de réseau

La commande`aaa authorization network`exécute l'autorisation pour toutes les demandes de service liées au réseau telles que PPP, SLIP et ARAP. Cette section porte sur le protocole PPP, le protocole le plus couramment utilisé.

Le serveur AAA vérifie si une session PPP du client est autorisée. De plus, les options du protocole PPP peuvent être demandées par le client : rappel, compression, adresse IP, etc. Ces options doivent être configurées sur le profil de l'utilisateur sur le serveur AAA. De plus, le profil AAA peut contenir des attributs idle-timeout, access-list et d'autres attributs par utilisateur pour un client en particulier qui peuvent être téléchargés par le logiciel Cisco IOS et appliqués à ce client.

Les exemples suivants montrent une autorisation avec Radius.

Exemple 1 : Mêmes méthodes d'autorisation de réseau pour tous les utilisateurs

On utilise le serveur d'accès pour accepter les connexions PPP à distance.

Les utilisateurs sont authentifiés (comme configuré précédemment) avec :

<#root>

```
Router(config)#
aaa authentication ppp default group radius local
```

Utilisez la commande suivante pour attribuer des autorisations aux utilisateurs :

<#root>

```
Router(config)#
aaa authorization network default group radius local
```

Remarque : Sur le serveur AAA, configurez : Service-Type=7 (avec trame) et Framed-Protocol=PPP.

Exemple 2 : Appliquer des attributs propres à l'utilisateur

Vous pouvez utiliser le serveur AAA pour affecter des attributs par utilisateur tels que l'adresse IP, le numéro de rappel, la valeur de délai d'inactivité du composeur ou la liste d'accès, etc. Dans une telle implémentation, NAS télécharge les attributs appropriés du profil d'utilisateur du serveur AAA.

Exemple 3 : Autorisation PPP avec une liste précise

Comme pour l'authentification, configurez un nom de liste plutôt qu'une valeur par défaut :

<#root>

```
Router(config)#
```

```
aaa authorization network ISDN_USER group radius local
```

Ensuite, appliquez cette liste à l’interface :

```
<#root>

  Router(config)#

interface dialer 0


  Router(config-if)#

ppp authorization ISDN_USER
```

Configuration de la traçabilité

La fonctionnalité de traçabilité du protocole AAA vous permet de faire le suivi des services auxquels les utilisateurs accèdent et la quantité de ressources réseau qu’ils consomment.

La comptabilité AAA a les mêmes règles que l'authentification et l'autorisation :

1. Vous devez d'abord définir une liste nommée de méthodes de comptabilité.
2. Appliquez alors cette liste à une ou plusieurs interfaces (excepté pour la liste de méthodes par défaut).
3. La première méthode énumérée est utilisée, si elle ne répond pas, c'est la deuxième méthode qui est utilisée et ainsi de suite.

- La traçabilité de réseau fournit des renseignements pour toutes les sessions PPP, SLIP et Arap (AppleTalk Remote Access Protocol) : nombre de paquets, nombre d’octets, durée de la session, heures de début et de fin.
- La traçabilité d’exécution fournit des renseignements sur les sessions de terminal EXEC de l’utilisateur (une session Telnet, par exemple) du serveur d’accès réseau : durée de la session, heures de début et de fin.

Les exemples suivants portent sur la manière dont les renseignements peuvent être envoyés au serveur AAA.

Exemples de configuration de la traçabilité

Exemple 1 : Générer des enregistrements de traçabilité de début et de fin

Pour chaque session PPP entrante, les renseignements de traçabilité sont envoyés au serveur AAA une fois le client authentifié et après la déconnexion avec le mot-clé start-stop.

<#root>

```
Router(config)#
aaa accounting network default start-stop group radius local
```

Exemple 2 : Générer uniquement des enregistrements de traçabilité de fin

Si les renseignements de traçabilité ne doivent être envoyés qu’après la déconnexion d’un client, utilisez le mot clé stop et configurez la ligne suivante :

<#root>

```
Router(config)#
aaa accounting network default stop group radius local
```

Exemple 3 : Générer des enregistrements de ressources pour les échecs d’authentification et de négociation

Jusqu'à ce stade, la comptabilité AAA fournit le support d'enregistrement de début et de fin pour les appels qui ont été soumis à l'authentification de l'utilisateur.

Si l'authentification ou la négociation PPP échoue, il n'y a aucun enregistrement d'authentification.

La solution est d'utiliser la comptabilité d'arrêt des pannes de ressources AAA :

<#root>

```
Router(config)#
aaa accounting send stop-record authentication failure
```

Un enregistrement d'arrêt est envoyé au serveur AAA.

Exemple 4 : Activer la traçabilité complète des ressources

Pour activer la comptabilité de pleine ressource, qui génère un enregistrement de début à l'établissement de l'appel et un enregistrement d'arrêt à la fin de l'appel, configurez :

<#root>

```
Router(config)#
aaa accounting resource start-stop
```

Cette commande a été introduite dans la version 12.1(3)T du logiciel Cisco IOS.

Avec cette commande, l'enregistrement comptable de début et de fin d'établissement d'un appel et de déconnexion d'un appel suit la progression de la connexion de la ressource au périphérique. Un enregistrement comptable de début-fin de l'authentification de l'utilisateur distinct suit la progression de gestion des utilisateurs. Ces deux ensembles d’enregistrements de traçabilité sont liés par un identifiant de session unique pour l’appel.

Informations connexes

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.