Configuration de la fonction AAA de base sur un serveur d'accès

Contenu

Introduction

Ce document explique comment configurer AAA (authentification, autorisation et comptabilité) sur un routeur Cisco utilisant les protocoles Radius et 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: Veuillez lire la section sur la configuration générale AAA avant de procéder à la configuration de Cisco IOS®. L'échec à procéder de la sorte peut résulter en une erreur de configuration et un verrouillage consécutif.

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

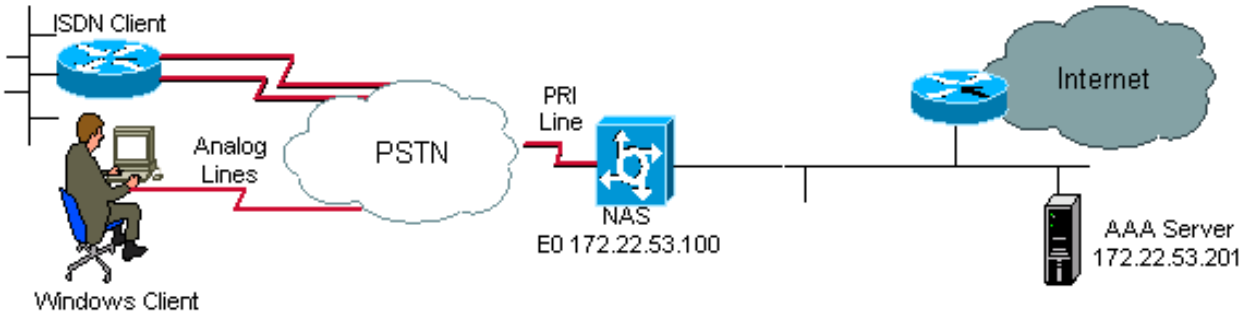
Pour obtenir une présentation de AAA et pour des détails complets au sujet des commandes et des options AAA, veuillez vous reporter au Guide de configuration de la sécurité IOS 12.2 : Utilisation de l'authentification, l'autorisation et la comptabilité

Composants utilisés

Les informations de ce document sont basées sur la ligne principale de la version 12.1 du logiciel Cisco IOS.

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.

Diagramme du réseau



Configuration générale de AAA

Activer AAA

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

Remarque: Jusqu'à ce que cette commande soit activée, toutes les autres commandes AAA sont masquées.

Avertissement : La commande **aaa new-model** applique immédiatement l'authentification locale à toutes les lignes et interfaces (excepté la ligne de console **line con 0**). Si une session telnet est ouverte sur le routeur après avoir activé cette commande (ou si une connexion expire et doit être réétablie), alors l'utilisateur doit être authentifié à l'aide de la base de données locale du routeur. Pour éviter d'être verrouillé hors du routeur, nous recommandons que vous définissiez un nom d'utilisateur et un mot de passe sur le serveur d'accès avant de commencer la configuration AAA. Procédez comme suit :

```
Router(config)# username xxx password yyy
```

Conseil : Sauvegardez votre configuration avant de configurer vos commandes AAA. Sauvegardez la configuration de nouveau une fois que vous avez terminé toutes vos configurations AAA (et que vous êtes satisfait de son fonctionnement). Ceci vous permet de récupérer de verrouillages imprévus (avant d'enregistrer la configuration) 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+, utilisez la commande **tacacs-server host <IP address of the AAA server> <key>** .

Si vous utilisez Radius, utilisez 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 périphériques sont sur le même réseau Ethernet alors, par défaut, le serveur d'accès utilise l'adresse IP définie sur l'interface Ethernet en envoyant 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 clé est sensible à la casse.
- Le protocole utilisé par le serveur d'accès (TACACS+ ou Radius).

Consultez votre documentation de serveur AAA pour la procédure exacte utilisée pour configurer les paramètres ci-dessus. Si le serveur AAA n'est pas correctement configuré, alors des requêtes AAA du NAS seront ignorées par le serveur AAA et la connexion peut échouer.

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 réside en la liste de méthodes par défaut (qui est nommée « par défaut »). 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.

Les exemples d'authentification ci-dessous utilisent Radius, la connexion et l'authentification de Protocole point à point (PPP) (le plus couramment utilisé) pour expliquer des concepts tels que des 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 point quelconque de ce cycle, ce qui signifie que le serveur AAA ou la base de données de noms d'utilisateur local répond en refusant l'accès de l'utilisateur (indiqué par un FAIL), le processus d'authentification s'interrompt et aucune autre méthode d'authentification n'est essayée.

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 Exec en utilisant Radius, puis Local

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

Dans la commande ci-dessus :

- 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 en utilisant le serveur RADIUS (première méthode). Si le serveur RADIUS ne répond pas, alors 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 :

```
Router(config)# username xxx password yyy
```

Puisque nous utilisons la liste par défaut dans la commande **aaa authentication login**, l'authentification de connexion est automatiquement appliquée pour toutes les connexions (telles que le tty, vty, la console et aux).

Remarque: Le serveur (Radius ou TACACS+) ne répondra pas à une requête **aaa authentication** envoyée par le serveur d'accès s'il n'y a aucune 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: Avec l'exemple ci-dessus, si nous n'incluons pas le mot clé local, nous avons :

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

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

Remarque: Le mot clé **group** fournit une façon de grouper les hôtes serveurs existants. La fonctionnalité permet à l'utilisateur de sélectionner un sous-ensemble d'hôtes du serveur configurés et de les utiliser pour un service particulier. Pour plus d'informations sur cette fonctionnalité avancée, reportez-vous au document AAA Server-Group.

Exemple 2 : Accès par console en utilisant le mot de passe de ligne

Développons la configuration de l'exemple 1 de sorte que l'ouverture de session sur la console soit seulement authentifiée par le mot de passe défini sur la ligne de connexion 0.

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

Nous configurons :

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

Dans la commande ci-dessus :

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

Une fois qu'une liste nommée (dans cet exemple, CONSOLE) est créée, elle doit être appliquée à une ligne ou à une interface pour prendre effet. Ceci est fait à l'aide de la commande d'authentification de connexion **list_name** :

```
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. Vous devez entrer le mot de passe « cisco » (configuré sur ligne de connexion 0) pour obtenir l'accès à la console. La liste par défaut est encore utilisée tty, vty et aux.

Remarque: Pour avoir un accès à la console authentifié par un nom d'utilisateur local et un mot de passe, utilisez :

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

Remarque: 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 n'avoir aucune authentification, utilisez

```
Router(config)# aaa authentication login CONSOLE none
```

Remarque: 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 en utilisant le serveur AAA externe

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

Nous configurons :

```
Router(config)# aaa authentication enable default group radius enable
```

Seul le mot de passe sera 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, le mot de passe activé configuré localement sur le routeur devra être entré.

Authentification PPP

La commande **aaa authentication ppp** est utilisée pour authentifier une connexion PPP. Elle est généralement utilisée pour authentifier l'ISDN ou les utilisateurs distants analogiques qui veulent accéder à Internet ou un site central à travers un serveur d'accès.

Exemple 1 : Méthode d'authentification PPP simple pour tous les utilisateurs

Le serveur d'accès a une interface ISDN qui est configurée pour accepter des clients PPP entrants. Nous utilisons un **dialer rotary-group 0**, mais la configuration peut être faite sur l'interface principale ou l'interface du profil numéroteur.

Nous configurons

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

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

Exemple 2 : Authentication PPP en utilisant une liste spécifique

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

```
Router(config)# aaa authentication ppp ISDN_USER group radius Router(config)# int dialer 0
Router(config-if)# pp authentication chap ISDN_USER
```

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

Exemple 3 : PPP lancé de la session de mode caractère

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

Si l'utilisateur d'un modem accède d'abord au routeur en utilisant une session exec en mode

caractère (par exemple, en utilisant Terminal Window after Dial), 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, nous pouvons utiliser le mot clé **if-needed**.

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

Remarque: Si le client commence une session PPP directement, l'authentification PPP est directement exécutée puisqu'il n'y a aucun accès de connexion au serveur d'accès.

Pour plus d'informations sur l'authentification AAA, reportez-vous au Guide de configuration de la sécurité IOS 12.2 : Configuration de l'authentification et Étude de cas d'implémentation AAA de Cisco.

Configurer l'autorisation

L'autorisation est le processus par lequel vous pouvez contrôler ce qu'un utilisateur peut ou ne peut pas faire.

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. Ce document se concentre sur les types d'autorisation Exec et Réseau.

Pour plus d'informations sur les autres types d'autorisation, veuillez vous reporter au Guide de configuration de sécurité Cisco IOS, version 12.2.

Autorisation exec

La commande **aaa authorization exec** détermine si l'utilisateur est autorisé à exécuter un interpréteur de commandes EXEC. Cette installation pourrait retourner les informations sur le profil de l'utilisateur telles que les informations d'autocommande, le délai d'inactivité, l'expiration de la session, la liste d'accès et privilège ainsi que 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 pour tous les utilisateurs

Une fois authentifié avec :

```
Router(config)# aaa authentication login default group radius local
```
Tous les utilisateurs qui veulent se connecter au serveur d'accès doivent être autorisés à l'aide de Radius (première méthode) ou de la base de données locale (deuxième méthode).

Nous configurons :

```
Router(config)# aaa authorization exec default group radius local
```
Remarque: Sur le serveur AAA, Service-Type=1 (connexion) doit être sélectionné.

Remarque: Avec cet exemple, si le mot clé **local** n'est pas inclus et que le serveur AAA ne répond pas, alors l'autorisation ne sera jamais possible et la connexion échouera.

Remarque: Dans les exemples 2 et 3 ci-dessous, nous n'avons besoin d'ajouter aucune commande sur le routeur, mais seulement de configurer le profil sur le serveur d'accès.

Exemple 2 : Attribuer les niveaux de privilège Exec au serveur AAA

Àpartir de l'exemple 1, si un utilisateur qui se connecte au serveur d'accès doit être autorisé à entrer directement le mode « activer », configurez le couple attribut-valeur suivant de Cisco sur le serveur AAA :

```
shell:priv-lvl=15
```
Ceci signifie que l'utilisateur passera directement au mode enable.

Remarque: Si la première méthode échoue à répondre, alors la base de données locale est utilisée. Cependant, l'utilisateur ne passera pas directement au mode d'activation, mais devra lancer la commande d'activation et fournir le **mot de passe d'activation**.

Exemple 3 : Attribuer Idle-Timeout du serveur AAA

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

Autorisation de réseau

La commande de réseau d'autorisation AAA exécute l'autorisation pour toutes les demandes de service liées à l'ensemble du réseau, telles que PPP, SLIP et ARAP. Cette section se concentre sur PPP, qui est le plus couramment utilisé.

Le serveur AAA vérifie si une session PPP du client est autorisée. De plus, des options PPP peuvent être demandées par le client : rappel, compression, adresse IP et ainsi de suite. Ces options doivent être configurées sur le profil de l'utilisateur sur le serveur AAA. De plus, pour un client déterminé, le profil AAA peut contenir le délai d'inactivité, la liste d'accès et d'autres attributs par utilisateur qui seront téléchargés par le logiciel Cisco IOS et appliqués pour ce client.

L'exemple qui suit montre l'autorisation utilisant Radius :

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

Le serveur d'accès est utilisé pour accepter des connexions entrantes PPP.

Premièrement, les utilisateurs sont authentifiés (comme cela a été précédemment configuré), à l'aide de :

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

puis ils doivent être autorisés en utilisant :

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

Remarque: Sur le serveur AAA, configurez :

- Service-Type=7 (encadré)
- Protocole encadré = PPP

Exemple 2 : Appliquer des attributs spécifiques à l'utilisateur

Vous pouvez utiliser le serveur AAA pour allouer des attributs par utilisateur, tels que l'adresse IP, le numéro de rappel, la valeur de la durée d'inactivité du numéroteur, 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 spécifique

Comme pour l'authentification, nous pouvons configurer un nom de liste plutôt qu'utiliser celui par défaut :

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

Puis, cette liste est appliquée à l'interface :

```
Router(config)# int dialer 0
Router(config-if)# ppp authorization ISDN_USER
```

Pour plus d'informations sur l'authentification AAA, reportez-vous au Guide de configuration de la sécurité IOS 12.2 : Configuration de l'authentification et Étude de cas d'implémentation AAA de Cisco.

Configurer la comptabilité

La fonctionnalité de comptabilité AAA vous permet de suivre les services auxquels les utilisateurs accèdent et la quantité des 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 première méthode énumérée est utilisée, si elle ne répond pas, c'est la deuxième méthode qui

est utilisée et ainsi de suite.

- La comptabilité de réseau fournit des informations pour toutes les sessions PPP, Slip et Protocole d'accès à distance AppleTalk (ARAP) : le comptage de paquets, le comptage des octets, le temps de session et l'heure de début et de fin.
- La comptabilité Exec fournit des informations au sujet des sessions terminales Exec de l'utilisateur (session telnet par exemple) du serveur d'accès au réseau : temps de session, heure de début et de fin.

Pour plus d'informations sur les autres types d'autorisation, veuillez vous reporter au Guide de configuration de sécurité Cisco IOS, version 12.2.

Les exemples ci-dessous se concentrent sur la façon dont les informations peuvent être envoyées au serveur AAA.

Configurer des exemples de comptabilité

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

Pour chaque session entrante PPP, l'information de comptabilité est envoyée au serveur AAA une fois que le client est authentifié et après la déconnexion en utilisant le mot clé **start-stop**.

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

Exemple 2 : Générer seulement des enregistrements comptables d'arrêt

Si l'information de comptabilité doit être envoyée seulement après la déconnexion d'un client, utilisez le mot clé **arrêt** et configurez la ligne suivante :

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

Exemple 3 : Générer des enregistrements de ressources pour des problèmes 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 :

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

Un enregistrement d'arrêt est envoyé au serveur AAA.

Exemple 4 : Activer la comptabilité de pleine ressource

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 :

```
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 comptables sont liés en utilisant une seule session ID pour l'appel.

Pour plus d'informations sur l'authentification AAA, reportez-vous au Guide de configuration de la sécurité IOS 12.2 : Configuration de l'authentification et Étude de cas d'implémentation AAA de Cisco.

Informations connexes

- Support technique - Cisco Systems