Configuration de RADIUS avec un serveur Livingston

Contenu

Introduction

Ce document est destiné à aider le premier utilisateur RADIUS à configurer et déboguer une configuration RADIUS sur un serveur RADIUS de Livingston. Il ne s'agit pas d'une description exhaustive des fonctionnalités de Cisco IOS® RADIUS. La documentation de Livingston est disponible sur le site Web de Lucent Technologies.

La configuration du routeur est identique quel que soit le serveur utilisé. Cisco propose un code RADIUS disponible sur le marché dans Couscouses NA, Couscouses UNIX ou Cisco Access Registrar.

Cette configuration de routeur a été développée sur un routeur qui exécute le logiciel Cisco IOS Version 11.3.3 ; La version 12.0.5.T et ultérieure utilise **le groupe radius** au lieu de **radius**, de sorte que les instructions telles que **aaa authentication login default radius enable** apparaissent comme **aaa authentication login default group radius enable**.

Reportez-vous aux informations RADIUS de la documentation Cisco IOS pour plus de détails sur les commandes de routeur RADIUS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Assurez-vous que vous avez compilé du code RADIUS sur le serveur UNIX. Les configurations du serveur supposent que vous utilisez le code du serveur RADIUS de Livingston. Les configurations des routeurs doivent fonctionner avec d'autres codes serveur, mais les configurations des serveurs diffèrent. Le code, rayé, doit être exécuté en tant que racine.
2. Le code RADIUS de Livingston est fourni avec trois exemples de fichiers qui doivent être personnalisés pour votre système : clients.exemple, users.exemple et dictionnaire. Elles se trouvent généralement dans le répertoire raddb. Vous pouvez modifier ces fichiers ou les fichiers utilisateurs et clients à la fin de ce document. Les trois fichiers doivent être placés dans un répertoire de travail. Testez pour vous assurer que le serveur RADIUS commence par les trois fichiers suivants :
   ```
   radiusd -x -d (directory_containing_3_files)
   ```
   Les erreurs de démarrage doivent être imprimées à l'écran ou dans le répertoire contenant_3_files_logfile. Vérifiez que RADIUS a démarré à partir d'une autre fenêtre de serveur :
   ```
   ps -aux | grep radiusd
   (or ps -ef | grep radiusd)
   ```
   Vous voyez deux processus rayés.
3. Tuer le processus de rayon :
   ```
   kill -9 highest_radiusd_pid
   ```
4. Sur le port de console du routeur, commencez à configurer RADIUS. Entrez dans le mode enable et tapez **configure terminal** avant de configurer la commande. Cette syntaxe garantit que vous n'êtes pas verrouillé du routeur initialement, étant donné que RADIUS ne s'exécute pas sur le serveur :

   ```
   !--- Turn on RADIUS aaa new-model enable password whatever !--- These are lists of
   authentication methods, !--- that is, "linmethod", "vtymethod", "conmethod" 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 radiusd !--- not being
   started, the enable password will be !--- accepted because it is in each list. aaa
   authentication login default radius enable aaa authentication login linmethod radius enable
   aaa authentication login vtymethod radius enable aaa authentication login conmethod radius
   enable !--- Point the router to the server, that is, !--- #.#.#.# is the server IP address.
   radius-server host #.#.#.# !--- Enter a key for handshaking !--- with the RADIUS server:
   radius-server key cisco 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
   password whatever 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. Restez connecté au routeur via le port de console pendant votre vérification afin de vous assurer que vous pouvez toujours accéder au routeur via Telnet avant de continuer. Comme radiusd n'est pas en cours d'exécution, le mot de passe enable doit être accepté avec

n'importe quel ID utilisateur.**Attention :** Maintenez la session du port de console active et restez en mode enable. Assurez-vous que cette session n'expire pas. Ne vous verrouillez pas lorsque vous modifiez la configuration.Émettez ces commandes afin de voir l'interaction serveur-routeur au niveau du routeur :

```
terminal monitor
debug aaa authentication
```

6. En tant que racine, démarrez RADIUS sur le serveur :

   ```
   radiusd -x -d (directory_containing_3_files)
   ```

   Les erreurs de démarrage sont imprimées à l'écran ou dans le répertoire contenant_3_files_logfile. Vérifiez que RADIUS a démarré à partir d'une autre fenêtre de serveur :

   ```
   Ps -aux | grep radiusd
   (or Ps -ef | grep radiusd)
   ```

   Vous devez voir deux processus rayés.
7. Les utilisateurs de Telnet (vty) doivent désormais s'authentifier via RADIUS. Avec le débogage sur le routeur et le serveur, étapes 5 et 6, établissez une connexion Telnet avec le routeur à partir d'une autre partie du réseau. Le routeur génère une invite de nom d'utilisateur et de mot de passe à laquelle vous répondez :

   ```
   ciscousr (username from users file)
   ciscopas (password from users file)
   ```

   Observez le serveur et le routeur où vous devez voir l'interaction RADIUS, par exemple, ce qui est envoyé, où, les réponses, les requêtes, etc. Corrigez tous les problèmes avant que vous continuiez.
8. Si vous souhaitez également que vos utilisateurs s'authentifient via RADIUS pour passer en mode enable, assurez-vous que votre session de port de console est toujours active et ajoutez cette commande au routeur.

   ```
   !--- For enable mode, list "default" looks to RADIUS !--- then enable password if RADIUS not running. aaa authentication enable default radius enable
   ```

9. Les utilisateurs doivent désormais **activer** via RADIUS. Une fois le débogage exécuté sur le routeur et le serveur, les étapes 5 et 6, établissez une connexion Telnet avec le routeur à partir d'une autre partie du réseau. Le routeur doit produire une invite de nom d'utilisateur et de mot de passe à laquelle vous répondez :

   ```
   ciscousr (username from users file)
   ciscopas (password from users file)
   ```

   Lorsque vous passez en mode enable, le routeur envoie le nom d'utilisateur $enable15$$ et demande un mot de passe auquel vous répondez :

   ```
   shared
   ```

   Observez le serveur et le routeur où vous devez voir l'interaction RADIUS, par exemple, ce qui est envoyé, où, les réponses, les requêtes, etc. Corrigez tous les problèmes avant que vous continuiez.
10. Vérifiez l'authentification des utilisateurs de votre port de console via RADIUS en établissant une session Telnet vers le routeur, qui doit s'authentifier via RADIUS. Restez connecté via Telnet au routeur et en mode enable jusqu'à ce que vous soyez sûr de pouvoir vous connecter au routeur via le port de console, déconnectez-vous de votre connexion d'origine au routeur via le port de console, puis reconnectez-vous au port de console. L'authentification du port de console pour se connecter et s'activer via l'utilisation d'ID utilisateur et de mots de passe à l'étape 9 doit maintenant passer par RADIUS.
11. Pendant que vous restez connecté via une session Telnet ou le port de console et que le débogage est exécuté sur le routeur et le serveur, étapes 5 et 6, établissez une connexion par modem à la ligne 1. Les utilisateurs de ligne doivent maintenant se connecter et

s'activer via RADIUS. Le routeur doit produire une invite de nom d'utilisateur et de mot de passe à laquelle vous répondez :

```
ciscousr (username from users file)
ciscopas (password from users file)
```

Lorsque vous passez en mode enable, le routeur envoie le nom d'utilisateur $enable15$$ et demande un mot de passe auquel vous répondez :

```
shared
```

Observez le serveur et le routeur où vous devez voir l'interaction RADIUS, par exemple, ce qui est envoyé, où, les réponses, les requêtes, etc. Corrigez tous les problèmes avant que vous continuiez.

Ajout de comptabilité

L'ajout de la comptabilité est facultatif.

1. La comptabilité n'a pas lieu à moins d'être configurée dans le routeur. Activez la comptabilité dans le routeur comme dans cet exemple :
   ```
   aaa accounting exec default start-stop radius
   aaa accounting connection default start-stop radius
   aaa accounting network default start-stop radius
   aaa accounting system default start-stop radius
   ```
2. Démarrez RADIUS sur le serveur avec l'option de comptabilité :
   ```
   Start RADIUS on the server with the accounting option:
   ```
3. Afin de voir l'interaction serveur-routeur au niveau du routeur :
   ```
   terminal monitor
   debug aaa accounting
   ```
4. Accédez au routeur pendant que vous observez le serveur et l'interaction du routeur via le débogage, puis vérifiez le répertoire de comptabilité pour les fichiers journaux.

Fichiers de test

Il s'agit du fichier de test des utilisateurs :

```
ciscousr        Password = "ciscopas"
                User-Service-Type = Login-User,
                Login-Host = 1.2.3.4,
                Login-Service = Telnet

$enable15$      Password = "shared"
                User-Service-Type = Shell-User
```

Il s'agit du fichier de test des clients :

```
# 1.2.3.4 is the ip address of the client router and cisco is the key
1.2.3.4         cisco
```

Informations connexes

- RADIUS (Remote Authentication Dial-In User Service)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems