Configuration de RADIUS avec un serveur Livingston

Contenu

Introduction

Ce document est destiné pour aider la première fois l'utilisateur RADIUS dans l'établissement et l'élimination des imperfections une configuration RADIUS à un serveur Livingston RADIUS. Ce n'est pas une description exhaustive des capacités de RAYON de Cisco IOS®. La documentation de Livingston est fournie par le site Web de Lucent Technologies.

La configuration de routeur est identique n'importe ce que le serveur est utilisé. Cisco offre le code disponible dans le commerce de RAYON dans le NA de couscous, les couscous UNIX, ou le Cisco Access Registrar.

Cette configuration de routeur a été développée sur un routeur qui exécute la version du logiciel Cisco IOS 11.3.3 ; La version 12.0.5.T et ultérieures utilise le **rayon de groupe** au lieu du **rayon**, ainsi les déclarations telles que le **radius enable d'aaa authentication login default** apparaissent en tant que **radius enable de groupe d'aaa authentication login default**.

Référez-vous aux informations de RAYON dans la documentation Cisco IOS pour des détails sur des commandes de routeur de RAYON.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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 le code de RAYON sur le serveur Unix. Les configurations du serveur supposent que vous utilisez le code de serveur Livingston RADIUS. Les configurations de routeur doivent fonctionner avec l'autre code de serveur mais les configurations du serveur diffèrent. Le code, radiusd, doit être exécuté comme racine.
2. Le code de Livingston RADIUS est livré avec trois fichiers témoin qui doivent être personnalisés pour votre système : clients.example, users.example, et dictionnaire. Ce sont tous habituellement trouvés dans le répertoire de raddb. Vous pouvez modifier ces fichiers ou les utilisateurs et les fichiers de clients à la fin de ce document. Chacun des trois fichiers doit être placé dans un répertoire de travail. Test à être sûr les débuts de serveur de RAYON avec les trois fichiers :`radiusd -x -d (directory_containing_3_files)`Erreurs dans le besoin de démarrage d'être imprimé à l'écran ou au directory_containing_3_files_logfile. Signez la commande pour être RAYON sûr commencé, d'une autre fenêtre de serveur :`ps -aux | grep radiusd`
   `(or ps -ef | grep radiusd)`Vous voyez deux processus de radiusd.
3. Détruisez le processus de rayon :`kill -9 highest_radiusd_pid`
4. Sur le port de console du routeur, début pour configurer le RAYON. Entrez dans le **mode enable** et tapez **configure terminal** avant de configurer la commande. Cette syntaxe s'assure que vous n'êtes pas verrouillé hors du routeur au commencement, étant donné que le RAYON ne fonctionne 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. Remain a ouvert une session au routeur par le port de console tandis que vous signez la commande pour être sûr que vous pouvez encore accéder au routeur par le telnet avant que vous continuiez. Puisque le radiusd ne s'exécute pas, le mot de passe d'enable doit être reçu avec n'importe quel ID utilisateur.**Attention :** Gardez la session de port de console active et restez dans le mode enable. Assurez-vous que cette session ne chronomètre pas. Ne vous verrouillez pas tandis que vous apportez des modifications de configuration.Émettez ces commandes afin de voir le serveur à l'interaction de routeur au routeur :`terminal monitor debug aaa authentication`
6. Comme racine, RAYON de début sur le serveur :`radiusd -x -d`

`(directory_containing_3_files)`Des erreurs dans le startup sont imprimées à l'écran ou au directory_containing_3_files_logfile. Vérifiez pour être RAYON sûr commencé d'une autre fenêtre de serveur :`Ps -aux | grep radiusd`
`(or Ps -ef | grep radiusd)`Vous devez voir deux processus de radiusd.

7. Les utilisateurs (vty) de telnet maintenant doivent authentifier par le RAYON. Avec mettez au point sur le routeur et le serveur, étapes 5 et 6, telnet dans le routeur d'une autre partie du réseau. Le routeur produit une demande de nom d'utilisateur et 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 de RAYON, par exemple, ce qui est envoyée où, des réponses, et des demandes, et ainsi de suite. Corrigez tous les problèmes avant que vous continuiez.
8. Si vous voulez également que vos utilisateurs authentifient par le RAYON pour entrer dans le mode enable, assurez-vous votre session de port de console est toujours en activité 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. Le besoin de l'utilisateur doit maintenant **activer** par le RAYON. Avec mettez au point aller sur le routeur et le serveur, étapes 5 et 6, telnet dans le routeur d'une autre partie du réseau. Le routeur doit produire une demande de nom d'utilisateur et mot de passe à laquelle vous répondez :`ciscousr (username from users file)`
`ciscopas (password from users file)`Quand vous écrivez le 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 de RAYON, par exemple, ce qui est envoyée où, des réponses, et des demandes, et ainsi de suite. Corrigez tous les problèmes avant que vous continuiez.
10. Vérifiez l'authentification de vos utilisateurs de port de console par le RAYON par l'établissement d'une session de telnet au routeur, qui les besoins d'authentifier par le RAYON. Restent Telnetted dans le routeur et dans le mode enable jusqu'à ce que vous soyez sûr que vous pouvez ouvrir une session au routeur par le port de console, déconnectez de-vous votre connexion d'origine au routeur par le port de console, et puis rebranchez au port de console. L'authentification de port de console à ouvrir une session et activer par l'utilisation des IDs utilisateurs et les mots de passe dans l'étape 9 doivent être maintenant par le RAYON.
11. Tandis que vous restez connecté par ou une session de telnet ou le port de console et avec mettent au point aller sur le routeur et le serveur, étapes 5 et 6, établissez une connexion modem pour rayer 1. ligne besoin de l'utilisateur doivent maintenant ouvrir une session et activer par le RAYON. Le routeur doit produire une demande de nom d'utilisateur et mot de passe à laquelle vous répondez :`ciscousr (username from users file)`
`ciscopas (password from users file)`Quand vous écrivez le 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 de RAYON, par exemple, ce qui est envoyée où, des réponses, et des demandes, et ainsi de suite. Corrigez tous les problèmes avant que vous continuiez.

Ajout de la comptabilité

L'ajout de la comptabilité est facultatif.

1. La comptabilité n'a pas lieu à moins que configuré 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. Commencez le RAYON sur le serveur avec l'option de comptabilité :`Start RADIUS on the server with the accounting option:`
3. Afin de voir le serveur à l'interaction de routeur au routeur :`terminal monitor`
   `debug aaa accounting`
4. Accédez au routeur tandis que vous observez le serveur et l'interaction de routeur par le débogage, et puis vérifiez le répertoire de comptabilité pour des fichiers journal.

Fichiers de test

C'est le fichier de test d'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
```

C'est le fichier de test de 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

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