RADIUS configureren met Livingston Server

Inhoud

Inleiding

Dit document is bedoeld om de eerste RADIUS-gebruiker bij te staan bij het opzetten en afluisteren van een RADIUS-configuratie naar een Livingston RADIUS-server. Het is geen volledige beschrijving van de mogelijkheden van Cisco IOS® RADIUS. De documentatie van Livingston is beschikbaar op de website van Lucent Technologies.

De routerconfiguratie is hetzelfde, ongeacht welke server wordt gebruikt. Cisco biedt commercieel beschikbare RADIUS-code in Couscouses NA, Couscouses UNIX of Cisco Access Registrar.

Deze routerconfiguratie is ontwikkeld op een router waarop Cisco IOS-softwarerelease 11.3.3 wordt uitgevoerd; Release 12.0.5.T en gebruikt later **groepsstraal** in plaats van **straal**, zodat de verklaringen zoals **aaa standaardopdradisering van de authenticatie** kunnen verschijnen zoals **aaa standaardinstellingen van de authenticatie**.

Raadpleeg de RADIUS-informatie in Cisco IOS-documentatie voor meer informatie over RADIUS-routeropdrachten.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Verificatie

Voer de volgende stappen uit:

1. Zorg ervoor dat u de RADIUS-code op de UNIX-server hebt gecompileerd. De serverconfiguraties gaan ervan uit dat u de Livingston RADIUS-servercode gebruikt. De routerconfiguraties moeten werken met andere servercode maar de serverconfiguraties verschillen. De code, radiusd, moet als wortel worden gebruikt.
2. De Livingston RADIUS-code wordt geleverd met drie voorbeeldbestanden die voor uw systeem moeten worden aangepast: klanten.voorbeeld, gebruikers.voorbeeld, en woordenboek. Deze zijn allemaal te vinden in de raddb folder. U kunt deze bestanden of de gebruikers- en clientbestanden aan het einde van dit document wijzigen. Alle drie bestanden moeten in een werkmap worden geplaatst. Test om zeker te zijn dat de RADIUS-server met de drie bestanden begint:
   ```
   radiusd -x -d (directory_containing_3_files)
   ```
   Fouten in opstarten moeten worden afgedrukt op het scherm of in het directory_bevattende_3_files_logfile. Controleer om er zeker van te zijn dat RADIUS is gestart vanuit een ander servervenster:
   ```
   ps -aux | grep radiusd
   (or ps -ef | grep radiusd)
   ```
   Je ziet twee radiusprocessen.
3. Vermoord het Straalproces:
   ```
   kill -9 highest_radiusd_pid
   ```
4. Op de poort van de routerconsole, begin om RADIUS te configureren. Geef de modus op en typ **de configureerbare terminal** voordat de opdracht wordt ingesteld. Deze syntaxis garandeert dat u niet eerst vanuit de router bent vergrendeld, aangezien RADIUS niet op de server actief is:

   ```
   !--- 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. Inloggen op de router door de console poort terwijl u controleert om zeker te zijn dat u nog toegang hebt tot de router door telnet voordat u verdergaat. Omdat radiusd niet actief is, moet het machtigingswachtwoord bij elke gebruiker worden geaccepteerd.**Waarschuwing:** houd de console poortsessie actief en blijf in de Enable modus. Zorg ervoor dat deze sessie niet wordt uitgesteld. Sluit jezelf niet af als u de configuratie verandert.Geef deze opdrachten uit om de interactie tussen server en router op de router te zien:
   ```
   terminal monitor
   ```

```
debug aaa authentication
```

6. Als wortel, start RADIUS op de server:
   ```
   radiusd -x -d (directory_containing_3_files)
   ```
   Fouten in het opstartbeeld worden afgedrukt op het scherm of folder_bevattende_3_files_logfile. Controleer of RADIUS vanuit een ander servervenster is gestart:
   ```
   Ps -aux | grep radiusd
   (or Ps -ef | grep radiusd)
   ```
   Je moet twee radiusprocessen zien.
7. Telnet (vty) gebruikers moeten nu authentiek door RADIUS. Met debug op de router en de server, stappen 5 en 6, telnet in de router van een ander deel van het netwerk. De router produceert een gebruikersnaam en een wachtwoord herinnering waarop u antwoordt:
   ```
   ciscousr (username from users file)
   ciscopas (password from users file)
   ```
   Kijk naar de server en de router waar je de RADIUS-interactie moet zien, bijvoorbeeld wat er wordt verzonden waar, reacties en verzoeken, enzovoort. Corrigeer alle problemen voordat u verdergaat.
8. Als u ook wilt dat uw gebruikers door RADIUS voor authentiek verklaren om in machtigingsmodus te geraken, zorg er dan voor dat uw console poortsessie nog actief is en voeg deze opdracht aan de router toe.

   ```
   !--- For enable mode, list "default" looks to RADIUS !--- then enable password if RADIUS
   not running. aaa authentication enable default radius enable
   ```
9. Gebruikers moeten nu via RADIUS in **staat stellen**. Met debug op de router en de server, stappen 5 en 6, telnet in de router van een ander deel van het netwerk. De router moet een gebruikersnaam en een wachtwoord opgeven waarop u antwoordt:
   ```
   ciscousr (username from users file)
   ciscopas (password from users file)
   ```
   Wanneer u Enable Mode invoert, verstuurt de router gebruikersnaam $Enable15$ en vraagt u om een wachtwoord, waarop u antwoordt:
   ```
   shared
   ```
   Kijk naar de server en de router waar je de RADIUS-interactie moet zien, bijvoorbeeld wat er wordt verzonden waar, reacties en verzoeken, enzovoort. Corrigeer alle problemen voordat u verdergaat.
10. Controleer voor authenticatie van uw console poortgebruikers door RADIUS door het instellen van een Telnet-sessie aan de router, die door RADIUS moet worden geauthentiseerd. Blijft Telnetted in de router en in plaats zet wijze toe tot u zeker bent u aan de router door de console haven kunt inloggen, uit uw originele verbinding aan de router door de console haven, en dan opnieuw aan de console haven kunt verbinden. Console poortverificatie om in te loggen en door het gebruik van gebruikers en wachtwoorden in stap 9 mogelijk te maken, moet nu via RADIUS worden uitgevoerd.
11. Terwijl u aangesloten blijft door een Telnet-sessie of de console poort en met debug in de router en de server, dienen stappen 5 en 6 een modemverbinding naar regel 1 te maken. De gebruikers van de lijn moeten nu inloggen en door RADIUS mogelijk maken. De router moet een gebruikersnaam en een wachtwoord opgeven waarop u antwoordt:
    ```
    ciscousr (username from users file)
    ciscopas (password from users file)
    ```
    Wanneer u Enable Mode invoert, verstuurt de router gebruikersnaam $Enable15$ en vraagt u om een wachtwoord, waarop u antwoordt:
    ```
    shared
    ```
    Kijk naar de server en de router waar je de RADIUS-interactie moet zien, bijvoorbeeld wat

er wordt verzonden waar, reacties en verzoeken, enzovoort. Corrigeer alle problemen voordat u verdergaat.

Boekhouding toevoegen

Boekhouding toevoegen is niet verplicht.

1. Boekhouding vindt niet plaats tenzij dit in de router is ingesteld. Laat accounting in de router zoals in dit voorbeeld toe:
   ```
   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. Start RADIUS op de server met de accounting optie:
   ```
   Start RADIUS on the server with the accounting option:
   ```
3. Zo ziet u een interactie tussen server en router op de router:
   ```
   terminal monitor
   debug aaa accounting
   ```
4. Toegang tot de router terwijl u de server en de routerinteractie door het debug observeert en controleer vervolgens de accounting directory voor logbestanden.

Bestanden testen

Dit is het testbestand van gebruikers:

```
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
```

Dit is het testbestand van cliënten:

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

Gerelateerde informatie

- Inbelservice voor externe verificatie (RADIUS)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems