Configurazione di RADIUS con Livingston Server

Sommario

Introduzione

Questo documento aiuta il primo utente RADIUS a configurare e eseguire il debug di una configurazione RADIUS su un server RADIUS Livingston. Non è una descrizione completa delle funzionalità di Cisco IOS® RADIUS. La documentazione di Livingston è disponibile sul sito web di Lucent Technologies.

La configurazione del router è la stessa indipendentemente dal server in uso. Cisco offre in commercio codice RADIUS in Couscouses NA, Couscouses UNIX o Cisco Access Registrar.

La configurazione del router è stata sviluppata su un router con software Cisco IOS versione 11.3.3; La release 12.0.5.T e successive utilizzano il **raggio di gruppo** anziché il **raggio**, quindi istruzioni come **aaa authentication login default radius enable** appaiono come **aaa authentication login default group radius enable**.

Per i dettagli sui comandi dei router RADIUS, consultare le informazioni sul RADIUS nella documentazione di Cisco IOS.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Autenticazione

Attenersi alla seguente procedura:

1. Assicurarsi di aver compilato il codice RADIUS sul server UNIX. Le configurazioni server presuppongono l'utilizzo del codice server RADIUS Livingston. Le configurazioni del router devono funzionare con altro codice server, ma le configurazioni del server sono diverse. Il codice radiusd deve essere eseguito come root.
2. Il codice Livingston RADIUS viene fornito con tre file di esempio da personalizzare per il sistema: clients.example, users.example e dictionary. Questi si trovano generalmente nella directory raddb. È possibile modificare questi file oppure i file degli utenti e dei client alla fine di questo documento. Tutti e tre i file devono essere collocati in una directory di lavoro. Verificare che il server RADIUS venga avviato con i tre file seguenti:
   ```
   radiusd -x -d (directory_containing_3_files)
   ```
   Gli errori all'avvio devono essere stampati sullo schermo o nella directory_contains_3_files_logfile. Per verificare che RADIUS sia stato avviato da un'altra finestra del server, verificare quanto segue:
   ```
   ps -aux | grep radiusd
   (or ps -ef | grep radiusd)
   ```
   Vedete due processi radiusd.
3. Terminare il processo di raggio:
   ```
   kill -9 highest_radiusd_pid
   ```
4. Sulla porta della console del router, avviare la configurazione di RADIUS. Immettere la modalità di abilitazione e digitare **configure terminal** prima del set di comandi. Questa sintassi garantisce che inizialmente il router non sia bloccato, dal momento che RADIUS non viene eseguito sul server:

   ```
   !--- 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. Durante il controllo, rimanere collegati al router tramite la porta della console per essere certi di poter ancora accedere al router tramite Telnet prima di continuare. Poiché radiusd non è in esecuzione, la password enable deve essere accettata con qualsiasi ID utente.**Attenzione:** mantenere attiva la sessione della porta console e rimanere in modalità abilitazione. Assicurarsi che la sessione non scada. Non bloccare l'utente mentre si apportano modifiche alla configurazione.Per verificare l'interazione tra il server e il router, eseguire questi comandi:
   ```
   terminal monitor
   ```

```
debug aaa authentication
```

6. Come root, avviare RADIUS sul server:
   ```
   radiusd -x -d (directory_containing_3_files)
   ```
   Gli errori all'avvio vengono stampati sullo schermo o nella directory_contains_3_files_logfile. Verificare che RADIUS sia stato avviato da un'altra finestra del server:
   ```
   Ps -aux | grep radiusd
   (or Ps -ef | grep radiusd)
   ```
   Ènecessario visualizzare due processi radiusd.
7. Gli utenti Telnet (vty) devono ora autenticarsi tramite RADIUS. Con il debug sul router e sul server, seguire i passaggi 5 e 6, collegarsi in modalità Telnet al router da un'altra parte della rete. Il router genera un prompt con nome utente e password a cui l'utente risponde:
   ```
   ciscousr (username from users file)
   ciscopas (password from users file)
   ```
   Osservare il server e il router in cui è necessario verificare l'interazione RADIUS, ad esempio il tipo di invio, le risposte, le richieste e così via. Correggere eventuali problemi prima di continuare.
8. Se si desidera inoltre che gli utenti eseguano l'autenticazione tramite RADIUS per accedere alla modalità di abilitazione, verificare che la sessione della porta della console sia ancora attiva e aggiungere questo comando al router.

   ```
   !--- For enable mode, list "default" looks to RADIUS !--- then enable password if RADIUS
   not running. aaa authentication enable default radius enable
   ```
9. A questo punto, gli utenti devono essere **abilitati** tramite RADIUS. Con il debug sul router e sul server, seguire i passaggi 5 e 6, collegarsi in modalità Telnet al router da un'altra parte della rete. Il router deve generare un prompt con nome utente e password a cui rispondere:
   ```
   ciscousr (username from users file)
   ciscopas (password from users file)
   ```
   Quando si entra in modalità abilitazione, il router invia il nome utente $enable15$ e richiede una password, alla quale si risponde:
   ```
   shared
   ```
   Osservare il server e il router in cui è necessario verificare l'interazione RADIUS, ad esempio il tipo di invio, le risposte, le richieste e così via. Correggere eventuali problemi prima di continuare.
10. Verificare l'autenticazione degli utenti della porta della console tramite RADIUS stabilendo una sessione Telnet con il router, che deve eseguire l'autenticazione tramite RADIUS. Rimanere connessi in modalità Telnet sul router e in modalità abilitazione finché non si è certi di poter accedere al router tramite la porta della console, disconnettersi dalla connessione originale al router tramite la porta della console e quindi riconnettersi alla porta della console. L'autenticazione della porta console per l'accesso e l'abilitazione tramite l'utilizzo di ID utente e password nel passaggio 9 deve essere ora eseguita tramite RADIUS.
11. Mentre si rimane connessi tramite una sessione Telnet o la porta console e con il debug in corso sul router e sul server, i passaggi 5 e 6, stabilire una connessione modem alla linea 1. Gli utenti di linea devono ora effettuare il login e abilitare il protocollo RADIUS. Il router deve generare un prompt con nome utente e password a cui rispondere:
    ```
    ciscousr (username from users file)
    ciscopas (password from users file)
    ```
    Quando si entra in modalità abilitazione, il router invia il nome utente $enable15$ e richiede una password, alla quale si risponde:
    ```
    shared
    ```
    Osservare il server e il router in cui è necessario verificare l'interazione RADIUS, ad

esempio il tipo di invio, le risposte, le richieste e così via. Correggere eventuali problemi prima di continuare.

Aggiunta di accounting

L'aggiunta dell'accounting è facoltativa.

1. L'accounting non viene eseguito se non è configurato nel router. Abilitare l'accounting nel router come illustrato nell'esempio seguente:
   ```
   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. Avviare RADIUS sul server con l'opzione di accounting:
   ```
   Start RADIUS on the server with the accounting option:
   ```
3. Per verificare l'interazione tra server e router sul router:
   ```
   terminal monitor
   debug aaa accounting
   ```
4. Accedere al router mentre si osserva l'interazione tra il server e il router durante il debug, quindi verificare la presenza di file di registro nella directory di accounting.

File di test

File di test dell'utente:

```
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
```

File di test client:

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

Informazioni correlate

- RADIUS (Remote Authentication Dial-In User Service)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems