Configurazione di un router Cisco con autenticazione TACACS+

Sommario

Introduzione

In questo documento viene descritto come configurare un router Cisco per l'autenticazione con TACACS+ in esecuzione su UNIX. TACACS+ non offre tante funzionalità quante ne offre Cisco Secure ACS per Windows o Cisco Secure ACS UNIX in commercio.

Il software TACACS+ precedentemente fornito da Cisco Systems è stato discontinuo e non è più supportato da Cisco Systems.

Oggi, è possibile trovare molte versioni freeware TACACS+ disponibili quando si cerca "TACACS+ freeware" sul proprio motore di ricerca Internet preferito. Cisco non consiglia specificamente un'implementazione specifica del freeware TACACS+.

Cisco Secure Access Control Server (ACS) è disponibile per l'acquisto tramite i normali canali di vendita e distribuzione Cisco in tutto il mondo. Cisco Secure ACS for Windows include tutti i componenti necessari per un'installazione indipendente su una workstation Microsoft Windows. Cisco Secure ACS Solution Engine è fornito con una licenza software Cisco Secure ACS preinstallata. Per inoltrare un ordine, visitare la home page Ordini Cisco (solo utenti registrati).

Nota: per ottenere la versione di valutazione di 90 giorni di Cisco Secure ACS per Windows, è necessario avere un account CCO con un contratto di assistenza associato.

La configurazione del router descritta in questo documento è stata sviluppata su un router con software Cisco IOS® versione 11.3.3. Il software Cisco IOS versione 12.0.5.T e successive usano **group tacacs+** anziché **tacacs+**, quindi le istruzioni come **aaa authentication login default tacacs+ enable** appaiono come **aaa authentication login default group tacacs+ enable**.

Per informazioni più complete sui comandi del router, consultare la documentazione del software

Cisco IOS.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per questo documento, sono stati usati i software Cisco IOS versione 11.3.3 e Cisco IOS versione 12.0.5.T e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

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 TACACS+ (TAC+) sul server UNIX.Le configurazioni server qui descritte presuppongono l'utilizzo del codice server Cisco TAC+. Le configurazioni dei router dovrebbero funzionare indipendentemente dal fatto che il codice del server sia o meno codice server Cisco. TAC+ deve essere utilizzato come radice; su a radice se necessario.
2. Copiare il test_file alla fine del documento, inserirlo nel server TAC+ e denominarlo **test_file**.Verificare che il daemon **tac_plus_executable** inizi con **test_file**. In questo comando, l'opzione **-P** verifica la presenza di errori di compilazione ma non avvia il daemon:
   `tac_plus_executable -P -C test_file`
   Èpossibile che il contenuto di test_file scorra verso il basso nella finestra, ma è consigliabile non visualizzare messaggi quali `impossibile trovare il file`, `previsto testo non crittografato`, `trovato testo non crittografato` o `imprevisto }`. In caso di errori, controllare i percorsi di test_file, verificare nuovamente la digitazione e ripetere il test prima di continuare.
3. Avviare la configurazione di TAC+ sul router.Immettere la modalità **enable** e digitare **configure terminal** prima del set di comandi. Questa sintassi del comando assicura che non si sia inizialmente bloccati fuori dal router, a condizione che **tac_plus_executable** non sia in esecuzione:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of
authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !---
```

tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list.

```
!
aaa authentication login linmethod tacacs+ enable
aaa authentication login vtymethod tacacs+ enable
aaa authentication login conmethod tacacs+ enable
!
!--- Point the router to the server, where #.#.#.# !--- is the server IP address. !
tacacs-server host #.#.#.# 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
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
```

4. Prima di continuare, verificare che sia ancora possibile accedere al router con Telnet e tramite la porta della console. Poiché **tac_plus_executable** non è in esecuzione, la password di **abilitazione** deve essere accettata.**Nota:** mantenere attiva la sessione della porta della console e rimanere in modalità abilitazione. Questa sessione non deve scadere. A questo punto, l'accesso al router è limitato e l'utente deve essere in grado di apportare modifiche alla configurazione senza doversi bloccare.Utilizzare questi comandi per verificare l'interazione tra server e router sul router:
   ```
   terminal monitor
     debug aaa authentication
   ```
5. Come root, avviare TAC+ sul server:
   ```
   tac_plus_executable -C test_file -d 16
   ```
6. Verificare che TAC+ sia stato avviato:
   ```
   ps -aux | grep tac_plus_executable
   ```
   o
   ```
   ps -ef | grep tac_plus_executable
   ```
   Se TAC+ non viene avviato, in genere si tratta di un problema di sintassi nel file_test. Tornare al punto 1 per correggere l'errore.
7. Digitare **tail -f /var/tmp/tac_plus.log** per verificare l'interazione tra router e server sul server.**Nota:** l'opzione `-d 16` al passo 5 invia l'output di tutte le transazioni alla cartella /var/tmp/tac_plus.log.
8. Gli utenti Telnet (VTY) devono ora autenticarsi tramite TAC+.Con il debug in corso sul router e sul server (passaggi 4 e 7), eseguire Telnet nel router da un'altra parte della rete.Il router genera un prompt con nome utente e password, al quale l'utente risponde:
   ```
   'authenuser'   (username from test_file)
   'admin'   (password from test_file)
   ```
   L'utente `authenuser` si trova in group `admin`, che dispone della password `admin`.Osservare il server e il router da cui è possibile visualizzare l'interazione TAC+, ad esempio la destinazione dell'invio, le risposte, le richieste e così via. Correggere eventuali problemi prima di continuare.
9. Se si desidera inoltre che gli utenti eseguano l'autenticazione tramite TAC+ per accedere alla modalità di abilitazione, verificare che la sessione della porta console sia ancora attiva e aggiungere questo comando al router:

   ```
   !--- For enable mode, list 'default' looks to TAC+ !--- then enable password if TAC+ does
   not run. aaa authentication enable default tacacs+ enable
   ```
   Gli utenti devono ora abilitare la funzione tramite TAC+.
10. Con il debug in corso sul router e sul server (passaggi 4 e 7), eseguire Telnet nel router da un'altra parte della rete. Il router genera un prompt con nome utente e password, al quale l'utente risponde:
    ```
    'authenuser'   (username from test_file)
    ```

`'admin'  (password from test_file)`

Quando si entra in modalità abilitazione, il router richiede una password, a cui si risponde: `'cisco'  (*$enable$ password from test_file*)`

Osservare il server e il router da cui dovrebbe essere visualizzata l'interazione TAC+, ad esempio la destinazione dell'invio, le risposte, le richieste e così via. Correggere eventuali problemi prima di continuare.

11. Disattivare il processo TAC+ sul server mentre è ancora connesso alla porta della console per essere certi che gli utenti possano ancora accedere al router se TAC+ non è attivo:
```
ps -aux | grep tac_plus_executable
```
o
```
ps -ef | grep tac_plus_executable)
  kill -9 pid_of_tac_plus_executable
```
Ripetere la procedura Telnet e abilitare la procedura precedente. Il router si rende quindi conto che il processo TAC+ non risponde e consente agli utenti di accedere e abilitare il sistema con le password predefinite.
12. Verificare l'autenticazione degli utenti della porta della console tramite TAC+. A tale scopo, avviare nuovamente il server TAC+ (passaggi 5 e 6) e stabilire una sessione Telnet con il router (da autenticare tramite TAC+).Rimanere connessi tramite Telnet al router in modalità abilitazione finché non si è certi di poter accedere al router tramite la porta della console.Uscire dalla connessione originale al router tramite la porta della console, quindi riconnettersi alla porta della console. L'autenticazione della porta console per eseguire il login e abilitare l'utilizzo di ID utente e password (mostrati nel passaggio 10) deve essere ora eseguita tramite TAC+.
13. Mentre si rimane connessi tramite una sessione Telnet o la porta console e il debug è in corso sul router e sul server (passaggi 4 e 7), stabilire una connessione modem alla linea 1.Gli utenti della linea devono ora effettuare il login e abilitarlo tramite TAC+.Il router genera un prompt con nome utente e password, al quale l'utente risponde:
```
'authenuser'   (username from test_file)
'admin'   (password from test_file)
```
Quando si accede alla modalità abilitazione, il router richiede una password.Reply: `'cisco'  (*$enable$ password from test_file*)`

Guarda il server e il router dove vedi l'interazione TAC+: dove viene inviato, risposte, richieste e così via. Correggere eventuali problemi prima di continuare.Gli utenti devono ora abilitare la funzione tramite TAC+.

Aggiungi autorizzazione

L'aggiunta dell'autorizzazione è facoltativa.

Per impostazione predefinita, sul router sono disponibili tre livelli di comando:

- livello di privilegio 0 che include disable, enable, exit, help e logout
- livello di privilegio 1 - livello normale su Telnet - il prompt dice `router>`
- livello di privilegio 15 - livello di abilitazione - il prompt dice `router#`

Poiché i comandi disponibili dipendono dal set di funzionalità IOS, dalla versione di Cisco IOS, dal modello di router e così via, non esiste un elenco completo di tutti i comandi ai livelli 1 e 15. Ad esempio, **show ipx route** non è presente in un set di funzionalità solo IP, **show ip nat trans** non è presente nel software Cisco IOS versione 10.2.x perché NAT non è stato introdotto in quel momento e **show environment** non è presente nei modelli di router senza alimentazione e monitoraggio della temperatura. I comandi disponibili in un particolare router a un particolare

livello sono disponibili quando si immette il comando **?** al prompt nel router quando si trova a quel livello di privilegio.

L'autorizzazione della porta console non è stata aggiunta come funzionalità finché non è stato implementato l'ID bug Cisco CSCdi82030 (solo utenti registrati). Per impostazione predefinita, l'autorizzazione della porta console è disattivata per ridurre la probabilità che il router venga accidentalmente bloccato. Se un utente ha accesso fisico al router tramite la console, l'autorizzazione della porta della console non è molto efficace. Tuttavia, l'autorizzazione della porta console può essere attivata alla riga `con 0` in un'immagine in cui l'ID bug Cisco CSCdi82030 (solo utenti registrati) è stato implementato con il comando:

```
authorization exec default|WORD
```

1. Il router può essere configurato per autorizzare i comandi tramite TAC+ a tutti i livelli o ad alcuni livelli.Questa configurazione del router consente a tutti gli utenti di impostare l'autorizzazione per comando sul server. Qui autorizziamo tutti i comandi tramite TAC+, ma se il server non funziona, non è necessaria alcuna autorizzazione.
   ```
   aaa authorization commands 1 default tacacs+ none
     aaa authorization commands 15 default tacacs+ none
   ```
2. Mentre il server TAC+ è in esecuzione, connettersi al router in modalità Telnet con l'ID utente **authenuser**.Poiché authenuser dispone di default service = permission in test_file, questo utente dovrebbe essere in grado di eseguire tutte le funzioni.Nel router, accedere alla modalità di **abilitazione** e attivare il debug delle autorizzazioni:
   ```
   terminal monitor
     debug aaa authorization
   ```
3. Accedere al router in modalità Telnet con l'**utente autore** e l'**operatore** password.Questo utente non è in grado di eseguire i due comandi show **traceroute** e **logout** (vedere il file_test).Osservare il server e il router dove dovrebbe essere visualizzata l'interazione TAC+ (dove, risposte, richieste e così via). Correggere eventuali problemi prima di continuare.
4. Se si desidera configurare un utente per un comando automatico, eliminare l'utente con commento temporaneo nel file_test e inserire una destinazione di indirizzo IP valida al posto di #.#.#.#.Arrestare e avviare il server TAC+.Sul router:
   ```
   aaa authorization exec default tacacs+
   ```
   Telnet su router con ID utente **temporaneo** e password **transitoria**. Il comando **telnet #.#.#.#** viene eseguito e l'utente temporaneo viene inviato all'altro percorso.

Aggiungi accounting

L'aggiunta dell'accounting è facoltativa.

Il riferimento al file di accounting è in file_di_test - file di accounting = /var/log/tac.log. Tuttavia, l'accounting non ha luogo a meno che non sia stato configurato nel router (a condizione che il router esegua una versione del software Cisco IOS successiva alla 11.0).

1. Abilitare l'accounting nel router:
   ```
   aaa accounting exec default start-stop tacacs+
     aaa accounting connection default start-stop tacacs+
     aaa accounting network default start-stop tacacs+
     aaa accounting system default start-stop tacacs+
   ```
   Nota: in alcune versioni l'accounting AAA non esegue l'accounting per comando. Per risolvere il problema, è possibile utilizzare l'autorizzazione per comando e registrare

l'occorrenza nel file di accounting. (fare riferimento all'ID bug Cisco CSCdi44140.) Se si utilizza un'immagine in cui è utilizzato questo fisso [software Cisco IOS versione 11.2(1.3)F, 11.2(1.2), 11.1(6.3), 11.1(6.3)AA01, 11.1(6.3)CA al 24 settembre 1997], è possibile abilitare anche la contabilità dei comandi.

2. Mentre TAC+ è in esecuzione sul server, immettere questo comando sul server per visualizzare le voci che vanno nel file di accounting:
   ```
   tail -f /var/log/tac.log
   ```
   Quindi, accedere al router e uscire dal router, usare Telnet e così via. Se necessario, sul router immettere:
   ```
   terminal monitor
     debug aaa accounting
   ```

File di test

```
- - - - - - - (cut here) - - - - - - -

# Set up accounting file if enabling accounting on NAS
accounting file = /var/log/tac.log

# Enable password setup for everyone:
user = $enable$ {
        login = cleartext "cisco"
        }

# Group listings must be first:
group = admin {
# Users in group 'admin' have cleartext password
        login = cleartext "admin"
        expires = "Dec 31 1999"
}

group = operators {
# Users in group 'operators' have cleartext password
        login = cleartext "operator"
        expires = "Dec 31 1999"
}

group = transients {
# Users in group 'transient' have cleartext password
        login = cleartext "transient"
        expires = "Dec 31 1999"
}

# This user is a member of group 'admin' & uses that group's password to log in.
#  The $enable$ password is used to enter enable mode.  The user can perform all commands.
 user = authenuser {
        default service = permit
        member = admin
        }

# This user is limitted in allowed commands when aaa authorization is enabled:
 user = telnet {
        login = cleartext "telnet"
        cmd = telnet {
        permit .*
        }
        cmd = logout {
        permit .*
        }
```

```
        }

# user = transient {
#       member = transients
#       service = exec {
        # When transient logs on to the NAS, he's immediately
        # zipped to another site
#       autocmd = "telnet #.#.#.#"
#       }
#       }

# This user is a member of group 'operators'
# & uses that group's password to log in
 user = authenuser {
        member = operators
# Since this user does not have 'default service = permit' when command
# authorization through TACACS+ is on at the router, this user's commands
# are limited to:
        cmd = show {
        permit ver
        permit ip
        }
        cmd = traceroute {
        permit .*
        }
        cmd = logout {
        permit .*
        }
}
- - - - (end cut here) - - - -
```

Nota: questo messaggio di errore viene generato se il server TACACS non è raggiungibile: `%AAAA-3-DROPACCTSNDFAIL: record di accounting eliminato, invio al server non riuscito: avvio del sistema`. Verificare che il server TACACS+ sia operativo.

Informazioni correlate

- Sicurezza accesso alla rete per utente singolo TACACS+
- TACACS+ (Terminal Access Controller Access Control System)
- Cisco Secure Access Control Server per Windows
- Documentazione e supporto tecnico – Cisco Systems