Een Cisco-router met TACACS+ verificatie configureren

Inhoud

Inleiding

Dit document beschrijft hoe u een Cisco-router voor verificatie kunt configureren met de TACACS+ die op UNIX wordt uitgevoerd. TACACS+ biedt niet zoveel functies als de commercieel beschikbare Cisco Secure ACS voor Windows of Cisco Secure ACS UNIX.

De software voor TACACS+ die voorheen door Cisco Systems werd geleverd, is stopgezet en wordt niet langer ondersteund door Cisco Systems.

Vandaag de dag vindt u veel beschikbare versies van TACACS+ freeware wanneer u zoekt naar "TACACS+ freeware" op uw favoriete internet zoekmachine. Cisco adviseert niet specifiek een bepaalde TACACS+ freeware implementatie.

Cisco Secure Access Control Server (ACS) is wereldwijd beschikbaar voor aankoop via reguliere verkoop- en distributiekanalen van Cisco. Cisco Secure ACS voor Windows bevat alle benodigde onderdelen voor een onafhankelijke installatie op een Microsoft Windows-werkstation. De Cisco Secure ACS Solution Engine wordt geleverd met een vooraf geïnstalleerde Cisco Secure ACS-softwarelicentie. Bezoek de Cisco Ordering Home Page (alleen geregistreerde klanten) om een bestelling te plaatsen.

Opmerking: u hebt een CCO-account met een gekoppeld servicecontract nodig om de proefversie van 90 dagen voor Cisco Secure ACS for Windows te hebben.

De routerconfiguratie in dit document is ontwikkeld op een router waarop Cisco IOS®-softwarerelease 11.3.3 wordt uitgevoerd. Cisco IOS-softwarerelease 12.0.5.T en maakt later gebruik van groep-tacacs+ in plaats van tacacs+, zodat verklaringen zoals aaa-verificatie, inloggen, standaard-tacacs+ verschijnen als aaa-verificatie, inlognaam, standaard-groep tacacs+

inschakelen.

Raadpleeg de Cisco IOS-softwaredocumentatie voor meer volledige informatie over routeropdrachten.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS-softwarerelease 11.3.3 en Cisco IOS-softwarerelease 12.0.5.T en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

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 TACACS+ (TAC+) code hebt gecompileerd op de UNIX server.

   Bij de serverconfiguraties hier wordt ervan uitgegaan dat u de Cisco TAC+ servercode gebruikt. De routerconfiguraties moeten werken, ongeacht of de servercode Cisco-servercode is. TAC+ moet als root worden uitgevoerd; We kunnen zo nodig wortelen.

2. Kopieer het test_file aan het einde van dit document, plaats het op de TAC+ server en noem het test_file.

   Controleer of de tac_plus_executable daemon start met test_file. In deze opdracht controleert de -P optie op compilatiefouten, maar wordt de daemon niet gestart:

   ```
   tac_plus_executable -P -C test_file
   ```

   Je zou de inhoud van test_file scroll door het venster kunnen zien, maar je zou geen

berichten moeten zien zoals `kan bestand`, `cleartext verwacht-found cleartext`, of `onverwacht`. Als er fouten zijn, controleer paden naar test_file, hercontroleer uw typen en hertest voordat u doorgaat.

3. Start TAC+ te configureren op de router.

   Typ de modus inschakelen en typ de terminal configureren voordat de opdrachtset wordt geopend. Deze opdrachtsyntaxis zorgt ervoor dat u niet in eerste instantie uit de router bent vergrendeld op voorwaarde dat de tac_plus_executable niet actief is:

   <#root>

```
!--- Turn on TAC+.

   aaa new-model
   enable password whatever

!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !-
```

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. Test zeker dat u nog steeds toegang hebt tot de router met Telnet en via de consolepoort voordat u doorgaat. Omdat tac_plus_executable niet actief is, dient het wachtwoord voor inschakelen te worden geaccepteerd.

   Opmerking: Houd de sessie van de consolepoort actief en blijf in de activeringsmodus. Deze sessie mag geen time-out veroorzaken. De toegang tot de router is op dit punt beperkt, en u moet configuratieveranderingen kunnen aanbrengen zonder uzelf te sluiten.

   Geef deze opdrachten uit om de server-to-router-interactie bij de router te zien:

```
terminal monitor
  debug aaa authentication
```

5. Als wortel, begin TAC+ op de server:

```
tac_plus_executable -C test_file -d 16
```

6. Controleer of TAC+ is gestart:

```
ps -aux | grep tac_plus_executable
```

   of

```
ps -ef | grep tac_plus_executable
```

   Als TAC+ niet start, is het meestal een probleem met syntaxis in het test_file. Ga terug naar stap 1 om dit te corrigeren.

7. Typ tail -f /var/tmp/tac_plus.log om router-to-server interactie op de server te zien.

   Opmerking: de optie `-d 16` in stap 5 verstuurt uitvoer van alle transacties naar de /var/tmp/tac_plus.log.

8. De gebruikers van Telnet (VTY) zouden nu door TAC+ moeten moeten voor authentiek verklaren.

   Met debug die op de router en de server (stappen 4 en 7) gaat, Telnet in de router van een ander deel van het netwerk.

De router produceert een gebruikersbenaming en wachtwoordherinnering, waarop u antwoordt:

```
'authenuser'   (username from test_file)
'admin'   (password from test_file)
```

De gebruiker `authenuser` is in groep `admin`, die het wachtwoord `admin` heeft.

Let op de server en de router waar u de TAC+ interactie kunt zien - wat wordt verzonden waar, reacties, verzoeken, etc. Corrigeer eventuele problemen voordat u doorgaat.

9. Als u ook wilt dat uw gebruikers via TAC+ authenticeren om in de inschakelmodus te komen, zorg er dan voor dat uw console-poortsessie nog actief is en voeg deze opdracht toe aan de router:

```
!--- For enable mode, list 'default' looks to TAC+ !--- then enable password if TAC+ does not run.

  aaa authentication enable default tacacs+ enable
```

Gebruikers moeten nu via TAC+ inschakelen.

10. Met debug die op de router en de server (stappen 4 en 7) gaat, Telnet in de router van een ander deel van het netwerk. De router produceert een gebruikersbenaming en wachtwoordherinnering, waarop u antwoordt:

```
'authenuser'   (username from test_file)
'admin'   (password from test_file)
```

Wanneer u de inschakelt-modus invoert, vraagt de router een wachtwoord aan, waarop u antwoordt:

```
'cisco'  ($enable$ password from test_file)
```

Let op de server en de router waar u de TAC+ interactie zou moeten zien - wat wordt verzonden waar, reacties, verzoeken, etc. Corrigeer eventuele problemen voordat u doorgaat.

11. Breng het TAC+ proces op de server terwijl nog verbonden met de consolepoort naar

beneden om er zeker van te zijn dat uw gebruikers nog steeds toegang tot de router kunnen hebben als TAC+ neer is:

```
ps -aux | grep tac_plus_executable
```

of

```
ps -ef | grep tac_plus_executable)
  kill -9 pid_of_tac_plus_executable
```

Herhaal het Telnet en schakel de vorige stap in. De router realiseert zich dan dat het TAC+ proces niet antwoordt en staat gebruikers toe om aan te melden en met de standaardwachtwoorden toe te laten.

12. Controleer de verificatie van uw consolepoortgebruikers via TAC+. Om dit te doen, breng de TAC+ server opnieuw ter sprake (stap 5 en 6) en maak een Telnet-sessie aan de router (die door TAC+ moet worden geverifieerd).

    Blijf verbonden via Telnet in de router in de inactiviteitmodus tot u er zeker van bent dat u via de consolepoort bij de router kunt inloggen.

    Log uit van uw oorspronkelijke verbinding met de router via de consolepoort en sluit vervolgens opnieuw aan op de consolepoort. De console-poortverificatie om in te loggen en het gebruik van gebruikers-id's en wachtwoorden (weergegeven in stap 10) in te schakelen, verloopt nu via TAC+.

13. Terwijl u verbonden blijft via een Telnet-sessie of de consolepoort en met debug op de router en de server (stappen 4 en 7), zet u een modemverbinding op lijn 1.

    Lijngebruikers moeten nu inloggen en via TAC+ inschakelen.

    De router produceert een gebruikersbenaming en wachtwoordherinnering, waarop u antwoordt:

```
'authenuser'   (username from test_file)
'admin'   (password from test_file)
```

    Wanneer u inschakelt modus, vraagt de router een wachtwoord aan.

    Antwoord:

```
'cisco'   ($enable$ password from test_file)
```

Let op de server en de router waar u de TAC+ interactie ziet - wat wordt verzonden waar, reacties, verzoeken, enzovoort. Corrigeer eventuele problemen voordat u doorgaat.

Gebruikers moeten nu via TAC+ inschakelen.

Toestemming toevoegen

Toevoeging van een vergunning is facultatief.

Door gebrek, zijn er drie bevel-niveaus op de router:

- voorrecht niveau 0 dat onbruikbaar maakt, toelaat, uitgang, hulp, en logout omvat
- voorrecht niveau 1 - normaal niveau op een Telnet - prompt zegt `router>`
- voorrecht niveau 15 - laat niveau toe - de herinnering zegt `router#`

Aangezien de beschikbare opdrachten afhankelijk zijn van de IOS-functieset, versie van Cisco IOS, model van router enzovoort, is er geen uitgebreide lijst van alle opdrachten op niveau 1 en 15. Toon bijvoorbeeld ipx-route niet aanwezig is in een functieset voor IP alleen, toon ip Nat-trans niet in Cisco IOS-softwarerelease 10.2.x omdat NAT niet op dat moment is geïntroduceerd, en toon dat de omgeving niet aanwezig is in routermodellen zonder bewaking van voeding en temperatuur. Opdrachten die op een bepaald niveau beschikbaar zijn in een bepaalde router, kunnen worden gevonden wanneer u een ? op de prompt in de router wanneer op dat voorrangsniveau.

De autorisatie van consolepoorten werd niet als een functie toegevoegd tot Cisco bug-id CSC82030 (alleen geregistreerde klanten) werd geïmplementeerd. De poortautorisatie van de console is standaard uitgeschakeld om de kans te verkleinen dat u per ongeluk wordt uitgesloten van de router. Als een gebruiker fysieke toegang tot de router via de console heeft, is de autorisatie van de consolepoort niet extreem effectief. De autorisatie van consolepoorten kan echter worden ingeschakeld onder de lijn `con 0` in een afbeelding waarin Cisco bug-id CSC82030 (alleen geregistreerde klanten) is geïmplementeerd in overeenstemming met de opdracht:

```
authorization exec default|WORD
```

1. De router kan worden geconfigureerd om opdrachten via TAC+ op alle of bepaalde niveaus te autoriseren.

   Deze routerconfiguratie staat alle gebruikers toe om per-bevel vergunningsopstelling op de server te hebben. Hier autoriseren we alle opdrachten via TAC+, maar als de server niet

actief is, is er geen autorisatie nodig.

```
aaa authorization commands 1 default tacacs+ none
  aaa authorization commands 15 default tacacs+ none
```

2. Terwijl de TAC+ server draait, wordt Telnet met de user-id authenuser in de router uitgevoerd.

   Omdat authenuser de standaarddienst = vergunning in test_file heeft, zou deze gebruiker alle functies moeten kunnen uitvoeren.

   Terwijl in de router, laat de wijze toe, en zet vergunning het zuiveren aan:

```
terminal monitor
  debug aaa authorization
```

3. Telnet in de router met user-id auteurgebruiker en wachtwoordexploitant.

   Deze gebruiker kan niet de twee show commando's traceroute en logout doen (zie de test_file).

   Let op de server en de router waar u de TAC+ interactie (wat wordt verzonden waar, reacties, verzoeken, etc.) zou moeten zien. Corrigeer eventuele problemen voordat u doorgaat.

4. Als u een gebruiker voor een autocommando wilt configureren, elimineert u de uitgezonden user transient in de test_file en zet u een geldige IP-adresbestemming in plaats van de #.#.#.#.

   Stop en start de TAC+ server.

   Op de router:

```
aaa authorization exec default tacacs+
```

   Telnet naar de router met user-id transient en wachtwoord transient. Telnet #.#.# wordt uitgevoerd en de gebruikerstransiënt wordt verzonden naar de andere plaats.

Accounting toevoegen

Het toevoegen van accounting is optioneel.

Verwijzing naar het boekhoudbestand is in test_file - accounting file = /var/log/tac.log. Maar de boekhouding vindt niet plaats tenzij geconfigureerd in de router (op voorwaarde dat de router een versie van Cisco IOS-software later dan 1.0 uitvoert).

1. Schakel accounting in de router in:

```
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+
```

   Opmerking: AAA-accounting doet in sommige versies niet per-opdracht accounting. Een tijdelijke oplossing is het gebruik van autorisatie per opdracht en het vastleggen van de gebeurtenis in het boekhoudbestand. (Raadpleeg Cisco-bug-id CSC4140.) Als u een afbeelding gebruikt waarin deze vaste schijf wordt gebruikt [Cisco IOS-softwarereleases 11.2(1.3)F, 11.2(1.2), 11.1(6.3), 11.1(6.3)AA01, 11.1(6.3)CA vanaf 24 september 1997], kunt u ook opdrachtaccounting inschakelen.

2. Terwijl TAC+ op de server wordt uitgevoerd, voert u deze opdracht in op de server om de vermeldingen te zien die in het boekhoudbestand worden ingevoerd:

```
tail -f /var/log/tac.log
```

   Dan log in en uit de router, Telnet uit de router, enzovoort. Indien nodig voert u op de router het volgende in:

```
terminal monitor
  debug aaa accounting
```

Testbestand

```
- - - - - - - (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) - - - -
```

Opmerking: deze foutmelding wordt gegenereerd als uw TACACS-server niet bereikbaar is: `%AAA-3 DROPACCTSNADFAIL: accounting record verbroken, verzenden naar server mislukt: systeemstart.` Controleer of de TACACS+ server operationeel is.

Gerelateerde informatie

- Beveiliging voor netwerktoegang met één gebruiker - TACACS+
- Terminal Access Controller-toegangscontrolesysteem (TACACS+)
- Cisco Secure Access Control Server voor Windows
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.