Basis AAA op een toegangsserver configureren

Inhoud

Inleiding

Dit document beschrijft hoe u verificatie, autorisatie en accounting (AAA) kunt configureren op een

Cisco-router met RADIUS- of TACACS+-protocollen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Conventies

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de hoofdregel van Cisco IOS®-softwarerelease 12.

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

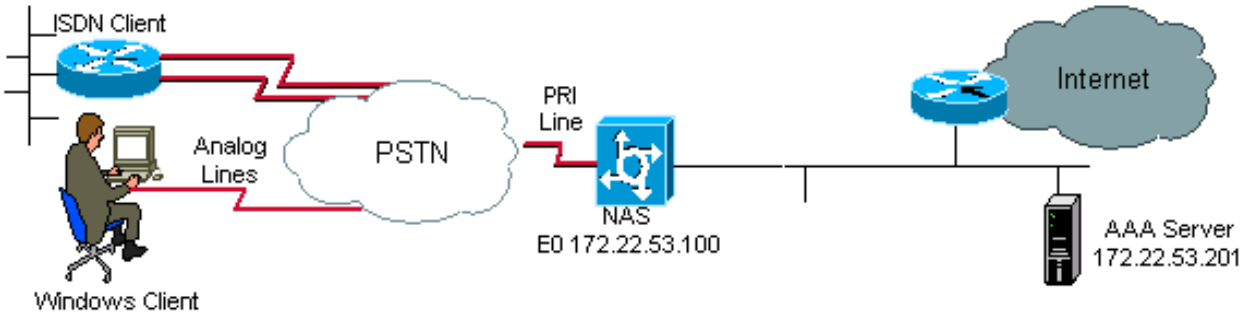
Achtergrondinformatie

Dit document legt uit hoe u verificatie, autorisatie en accounting (AAA) kunt configureren op een Cisco-router met RADIUS- of TACACS+-protocollen. Het doel van dit document is niet om alle AAA-functies te beschrijven, maar om alleen de belangrijkste opdrachten te bespreken en enkele voorbeelden en richtlijnen te geven.

> **Opmerking:** Lees de sectie over de algemene AAA-configuratie voordat u doorgaat met de Cisco IOS-configuratie. Wanneer u dit niet doet, kan dit leiden tot verkeerde configuratie en daaropvolgende uitsluiting.

Zie Configuratiehandleiding voor verificatie, autorisatie en accounting voor meer informatie.

Netwerkdiagram



Netwerkdiagram

Algemene AAA-configuratie

AAA inschakelen

Om AAA in te schakelen moet u de opdracht **aaa new-model configureren in de algemene configuratie.**

> **Opmerking:** Totdat deze opdracht is ingeschakeld, zijn alle andere AAA-opdrachten verborgen.

> **Waarschuwing**: De **aaa new-model** opdracht past onmiddellijk lokale verificatie toe op alle lijnen en interfaces (behalve de console lijn **con 0**). Als een Telnet-sessie wordt geopend naar de router nadat deze opdracht is ingeschakeld (of als een verbinding wordt uitgezet en opnieuw moet worden verbonden), dan moet de gebruiker worden geverifieerd met de lokale database van de router. Het wordt aanbevolen om een gebruikersnaam en wachtwoord op de toegangsserver te definiëren voordat u de AAA-configuratie start, zodat u niet uitgesloten bent van de router. Zie het volgende codevoorbeeld.

```
Router(config)#username xxx password yyy
```

> **Tip**: Voordat u uw AAA-opdrachten configureert, `save` uw configuratie. U kunt `save` de configuratie pas opnieuw nadat u de AAA-configuratie hebt voltooid (en ervan overtuigd bent dat deze correct werkt). Dit staat u toe om van onverwachte lockouts te herstellen aangezien u om het even welke verandering met een herladen van de router kunt terugrollen.

De externe AAA-server opgeven

Definieer het security protocol dat wordt gebruikt met AAA (RADIUS, TACACS+) in de algemene configuratie. Als u geen van deze twee protocollen wilt gebruiken, kunt u de lokale database op de router gebruiken.

Als u TACACS+ gebruikt, gebruikt u de opdracht **<IP-adres van de AAA-server> <key> voor de Tacacs-server**.

Als u RADIUS gebruikt, gebruikt u de opdracht **RADIUS-server host <IP-adres van de AAA-server> <key>**.

Configuratie van de AAA-server

Configureer op de AAA-server de volgende parameters:

- De naam van de toegangsserver.
- Het IP-adres dat de toegangsserver gebruikt om met de AAA-server te communiceren.**Opmerking:** Als beide apparaten zich in hetzelfde Ethernet-netwerk bevinden, gebruikt de toegangsserver standaard het IP-adres dat op de Ethernet-interface is gedefinieerd wanneer het AAA-pakket wordt verzonden. Dit is belangrijk om te weten wanneer de router meerdere interfaces (en dus meerdere adressen) heeft.

- Precies dezelfde sleutel **<key>** die is geconfigureerd op de toegangsserver.**Opmerking:** De sleutel is hoofdlettergevoelig.
- Het protocol dat door de toegangsserver (TACACS+ of RADIUS) wordt gebruikt.

Raadpleeg de documentatie bij de AAA-server voor de exacte procedure die is gebruikt om de vorige parameters te configureren. Als de AAA-server niet correct is geconfigureerd, kunnen AAA-aanvragen van de NAS worden genegeerd door de AAA-server en kan de verbinding mislukken.

De AAA-server moet via IP bereikbaar zijn vanaf de toegangsserver (gebruik **ping om de connectiviteit te verifiëren).**

Verificatieconfiguratie

Verificatie controleert gebruikers voordat ze toegang krijgen tot het netwerk en netwerkservices (die worden geverifieerd met autorisatie).

AAA-verificatie configureren:

1. Definieer eerst een benoemde lijst met verificatiemethoden (in modus Global Configuration).
2. Pas die lijst op een of meer interfaces toe (in de configuratiemodus van de interface).

De enige uitzondering is de standaardmethodelijst (die **standaard** wordt genoemd). De standaardmethodelijst wordt automatisch toegepast op alle interfaces, behalve die waarvoor expliciet een benoemde methodelijst is gedefinieerd. Een gedefinieerde methodelijst heeft voorrang op de standaardmethodelijst.

Deze verificatievoorbeelden maken gebruik van RADIUS, login en Point-to-Point Protocol (PPP)-verificatie om concepten zoals methoden en benoemde lijsten te verklaren. In alle voorbeelden kan TACACS+ worden vervangen door RADIUS of lokale verificatie.

De Cisco IOS-software gebruikt de eerste methode in de lijst om gebruikers te verifiëren. Als die methode niet reageert (aangegeven met ERROR), dan selecteert de Cisco IOS-software de volgende verificatiemethode die in de methodelijst wordt vermeld. Dit proces gaat door totdat er succesvolle communicatie is via een verificatiemethode in de lijst, of tot alle methoden in de methodelijst zijn uitgeput.

Het is belangrijk om op te merken dat de Cisco IOS-software alleen verificatie probeert met de volgende verificatiemethode in de lijst als er geen reactie is via de huidige methode. Als de authenticatie op een punt in dit programma mislukt, dat wil zeggen als de AAA-server of de lokale gebruikersnaamdatabase antwoorden de toegang van de gebruiker moeten weigeren (aangegeven door een FAIL), stopt het verificatieproces en worden er geen andere verificatiemethoden geprobeerd.

Om gebruikersverificatie toe te staan, moet u de gebruikersnaam en het wachtwoord op de AAA-server configureren.

Login-verificatie

U kunt de opdracht **aaa authentication login gebruiken om gebruikers te verifiëren die Exec-toegang willen tot de toegangsserver (tty, vty, console en aux).**

Voorbeeld 1: Exec-toegang met straal en vervolgens lokaal

```
Router(config)#aaa authentication login default group radius local
```

In de vorige opdracht:

- Is de benoemde lijst de standaardlijst (default).
- Zijn er twee verificatiemethoden (group radius en local).

Alle gebruikers worden geverifieerd met de Radius-server (de eerste methode). Als de Radius-server niet reageert, wordt de lokale database van de router gebruikt (de tweede methode). Definieer de gebruikersnaam en het wachtwoord voor lokale verificatie:

```
Router(config)#username xxx password yyy
```

Omdat de lijst standaard in de **aaa authenticatie login** opdracht wordt gebruikt, login authenticatie automatisch toegepast op alle login verbindingen (zoals tty, vty, console en aux).

> **Opmerking:** De server (RADIUS of TACACS+) kan niet reageren op een **aaa-verificatieaanvraag** die door de toegangsserver is verzonden als er geen IP-verbinding is, als de toegangsserver niet correct is gedefinieerd op de AAA-server of als de AAA-server niet juist is gedefinieerd op de toegangsserver.

> **Opmerking:** Als u het vorige voorbeeld zonder **lokaal** trefwoord gebruikt, is het resultaat:

```
Router(config)#aaa authentication login default group radius
```

> **Opmerking:** Als de AAA-server niet reageert op het verificatieverzoek, mislukt de verificatie (omdat de router geen alternatieve methode heeft om te proberen).

> **Opmerking:** Het **groepssleutelwoord** biedt een manier om huidige serverhosts te groeperen. Met deze functie kan de gebruiker een subset van de geconfigureerde serverhosts selecteren en voor een bepaalde service gebruiken.

Voorbeeld 2: Toegang tot console gebruikt met lijnwachtwoord

Breid de configuratie uit van Voorbeeld 1 zodat consolelogin alleen wordt geverifieerd door het wachtwoord dat online is ingesteld op pictogram 0.

De lijst CONSOLE wordt gedefinieerd en dan toegepast op line con 0.

Configuratie:

```
Router(config)#aaa authentication login CONSOLE line
```

In de vorige opdracht:

- is de benoemde lijst CONSOLE.
- Is er slechts één verificatiemethode (line).

Wanneer een benoemde lijst (in dit voorbeeld, CONSOLE) wordt gemaakt, moet deze worden toegepast op een regel of interface voordat deze wordt uitgevoerd. Dit gebeurt met de login authentication opdracht:

```
Router(config)#line con 0
Router(config-line)#exec-timeout 0 0
Router(config-line)#password cisco
Router(config-line)#login authentication CONSOLE
```

De CONSOLE-lijst heeft voorrang op de standaardmethodelijst **standaard** on line con 0. Na deze configuratie on line con 0, moet u het wachtwoord invoeren in **Cisco** om toegang tot de console te krijgen. De standaardlijst wordt nog steeds gebruikt op tty, vty en aux.

> **Opmerking:** Om consoletoegang te hebben die door een lokaal gebruikersbenaming en een wachtwoord voor authentiek wordt verklaard, gebruik het volgende codevoorbeeld:

```
Router(config)#aaa authentication login CONSOLE local
```

In dit geval, moeten een gebruikersbenaming en een wachtwoord in het lokale gegevensbestand van de router worden gevormd. De lijst moet ook op de lijn of interface worden toegepast.

> **Opmerking:** Als u geen verificatie wilt uitvoeren, gebruikt u het volgende codevoorbeeld:

```
Router(config)#aaa authentication login CONSOLE none
```

In dit geval is er geen authenticatie te krijgen op de console toegang. De lijst moet ook op de lijn of interface worden toegepast.

Voorbeeld 3: Toegang in modus inschakelen voor gebruik met externe AAA-server

U kunt verificatie opgeven om de enable-modus (bevoegdheid 15) in te schakelen.

Configuratie:

```
Router(config)#aaa authentication enable default group radius enable
```

Alleen het wachtwoord kan worden aangevraagd, de gebruikersnaam is $enab15$. Daarom moet de gebruikersnaam $enab15$ op de AAA-server worden gedefinieerd.

Als de Radius-server niet antwoordt, kan het wachtwoord voor het inschakelen dat lokaal op de router is geconfigureerd, moeten worden ingevoerd.

PPP-verificatie

De opdracht **aaa authentication ppp wordt gebruikt om een PPP-verbinding te verifiëren.** Het wordt

meestal gebruikt voor het verifiëren van ISDN of analoge externe gebruikers die toegang willen tot het internet of een centraal kantoor via een toegangsserver.

Voorbeeld 1: Eén PPP-verificatiemethode voor alle gebruikers

De toegangsserver heeft een ISDN-interface die is geconfigureerd om PPP-inbelclients te accepteren. We gebruiken een **dialer rotary-groep 0**, maar de configuratie kan worden uitgevoerd op de hoofdinterface of dialer profielinterface.

Configuratie:

```
Router(config)#aaa authentication ppp default group radius local
```

Deze opdracht verifieert alle PPP-gebruikers met Radius. Als de Radius-server niet reageert, wordt de lokale database gebruikt.

Voorbeeld 2: PPP-verificatie gebruikt met een specifieke lijst

U kunt als volgt een benoemde lijst gebruiken in plaats van de standaardlijst:

```
Router(config)#aaa authentication ppp ISDN_USER group radius

Router(config)#interface dialer 0
Router(config-if)#ppp authentication chap ISDN_USER
```

In dit voorbeeld is de lijst ISDN_USER en is de methode RADIUS.

Voorbeeld 3: PPP gestart vanuit een sessie in tekstmodus

De toegangsserver heeft een interne modemkaart (MICA, Microcom of NextPort). Veronderstel dat zowel **aaa-verificatielogin** als **aaa-verificatie ppp-**opdrachten zijn geconfigureerd.

Als een modemgebruiker eerst de router met een execsessie van de tekenmodus benadert (bijvoorbeeld met Terminal Window na Dial), wordt de gebruiker op een tekstregel geverifieerd. Om een sessie in pakketmodus te starten moeten gebruikers **ppp default of ppp invoeren.** Aangezien PPP-verificatie expliciet is geconfigureerd (met **aaa authentication ppp), wordt de gebruiker opnieuw op PPP-niveau geverifieerd.**

Om deze tweede verificatie te voorkomen, gebruikt u het **indien nodig** sleutelwoord:

```
Router(config)#aaa authentication login default group radius local
Router(config)#aaa authentication ppp default group radius local if-needed
```

> **Opmerking:** Als de client een PPP-sessie direct start, wordt PPP-verificatie direct uitgevoerd omdat er geen inlogtoegang tot de toegangsserver is.

Vergunning configureren

Autorisatie is het proces waarmee u kunt bepalen wat een gebruiker kan doen.

Voor AAA-autorisatie gelden dezelfde regels als voor verificatie:

1. Definieer allereerst een benoemde lijst met autorisatiemethoden.
2. Pas die lijst vervolgens toe op een of meer interfaces (behalve de standaardmethodelijst).
3. De eerste methode in de lijst wordt gebruikt. Als deze niet reageert, wordt de tweede gebruikt, enzovoort.

Methodelijsten zijn specifiek voor het soort autorisatie dat wordt gevraagd. Dit document concentreert zich op de autorisatietypen Exec en Network.

Raadpleeg de Cisco IOS security configuratiegids voor meer informatie over de andere soorten autorisatie.

Exec-autorisatie

De opdracht **aaa authorization exec bepaalt of de gebruiker een EXEC-shell mag starten.** Deze faciliteit kan informatie over gebruikersprofielen, zoals automatische opdrachtinformatie, tijdelijke onderbreking, sessieonderbreking, toegangslijst en voorrechten en andere factoren per gebruiker teruggeven.

Exec-autorisatie wordt alleen verleend via vty- en tty-lijnen.

Het volgende voorbeeld gebruikt Straal.

Voorbeeld 1: Dezelfde Exec-verificatiemethoden voor alle gebruikers

Wanneer het is geverifieerd met:

```
Router(config)#aaa authentication login default group radius local
```

Alle gebruikers die willen inloggen op de toegangsserver moeten geautoriseerd zijn met Radius (eerste methode) of lokale database (tweede methode).

Configuratie:

```
Router(config)#aaa authorization exec default group radius local
```

> **Opmerking:** Op de AAA-server moet Service-Type=1 (aanmelding) worden geselecteerd.

> **Opmerking:** Als in dit voorbeeld het **lokale** trefwoord niet wordt opgenomen en de AAA-server niet reageert, is de autorisatie daarom niet mogelijk en kan de verbinding mislukken.

> **Opmerking:** In volgende Voorbeelden 2 en 3, moet u geen bevel op de router toevoegen. U hoeft alleen het profiel op de toegangsserver te configureren.

Voorbeeld 2: Exec-prioriteitsniveaus toewijzen vanaf de AAA-server

Gebaseerd op voorbeeld 1, configureer het volgende Cisco AV-paar op de AAA-server zodat een gebruiker zich bij de toegangsserver kan aanmelden en de inschakelmodus rechtstreeks kan invoeren:

```
shell:priv-lvl=15
```

De gebruiker kan nu rechtstreeks naar de inschakelmodus gaan.

> **Opmerking:** Als de eerste methode niet reageert, wordt de lokale database gebruikt. De gebruiker kan echter niet rechtstreeks naar de inschakelt-modus gaan, maar moet de opdracht Inschakelen invoeren en het wachtwoord **inschakelen** leveren.

Voorbeeld 3: Wijs de inactiviteitstimer uit de AAA-server toe

Gebruik IETF Radius-kenmerk 28 om een time-out bij inactief gebruik te configureren (zodat de sessie wordt losgekoppeld als er geen verkeer is na de tijdelijke onderbreking): Inactiviteitstimer onder het gebruikersprofiel.

Netwerkautorisatie

Het **aaa authorization network** opdracht voert autorisatie uit voor alle netwerkgerelateerde serviceaanvragen zoals PPP, SLIP en ARAP. Deze sectie concentreert zich op PPP, die het meest meestal wordt gebruikt.

De AAA-server controleert of een PPP-sessie door de klant wordt toegestaan. Bovendien kan de klant om PPP-opties vragen: callback, compression, IP-adres, enzovoort. Deze opties moeten in het gebruikersprofiel op de AAA-server worden geconfigureerd. Bovendien kan het AAA-profiel voor een specifieke client kenmerken voor inactiviteitstimer, toegangslijst en andere kenmerken per gebruiker bevatten die door de Cisco IOS-software kunnen worden gedownload en voor deze client kunnen worden toegepast.

De volgende voorbeelden tonen vergunning met Radius.

Voorbeeld 1: Dezelfde methoden voor netwerkautorisatie voor alle gebruikers

De toegangsserver wordt gebruikt om PPP inbelverbindingen te accepteren.

Gebruikers worden geverifieerd (zoals eerder geconfigureerd) met:

```
Router(config)#aaa authentication ppp default group radius local
```

Gebruik de volgende opdracht om de gebruikers te autoriseren:

```
Router(config)#aaa authorization network default group radius local
```

Opmerking: Configureer op de AAA-server: **Service-Type=7** (framed) en **Framed-Protocol=PPP**.

Voorbeeld 2: Gebruikersspecifieke kenmerken toepassen

U kunt de AAA-server gebruiken om per gebruiker kenmerken toe te wijzen zoals IP-adres, callback-nummer, dialer idle timeout-waarde of toegangslijst, enzovoort. Bij een dergelijke implementatie downloadt de NAS de juiste kenmerken uit het gebruikersprofiel van de AAA-server.

Voorbeeld 3: PPP-autorisatie met een specifieke lijst

Gelijkaardig aan authentificatie, vorm een lijstnaam eerder dan standaard:

```
Router(config)#aaa authorization network ISDN_USER group radius local
```

Pas de lijst vervolgens op de interface toe:

```
Router(config)#interface dialer 0
Router(config-if)#ppp authorization ISDN_USER
```

Accountconfiguratie

Met de AAA-boekhoudingsfunctie kunt u de services volgen waartoe gebruikers toegang hebben en de hoeveelheid netwerkbronnen die ze verbruiken.

AAA-accounting volgt dezelfde regels als verificatie en autorisatie:

1. U moet eerst een benoemde lijst van accountingmethoden definiëren.
2. Pas die lijst vervolgens toe op een of meer interfaces (behalve de standaardmethodelijst).
3. De eerste methode in de lijst wordt gebruikt en als deze geen respons oplevert, wordt de tweede wordt gebruikt, enzovoort.

- Netwerkaccounting bevat informatie voor alle sessies met PPP, SLIP en ARAP (AppleTalk Remote Access Protocol): telling van pakketten, telling van octecten, sessietijd, begin- en eindtijd.
- Exec-accounting biedt informatie over EXEC-terminalsessies (bijvoorbeeld een telnetsessie) door gebruikers van de netwerktoegangsserver: sessietijd, begin- en eindtijd.

De volgende voorbeelden concentreren zich op hoe de informatie naar de server van de AAA kan worden verzonden.

Configuratievoorbeelden voor accounting

Voorbeeld 1: Accounting records starten en stoppen

Voor elke inbel-PPP-sessie wordt de boekhoudingsinformatie naar de AAA-server verzonden zodra de client is geverifieerd en na het verbreken met het sleutelwoord **start-stop**.

```
Router(config)#aaa accounting network default start-stop group radius local
```

Voorbeeld 2: Alleen stop-accounting records genereren

Als de boekhoudingsinformatie moet worden verzonden slechts nadat een cliënt heeft losgemaakt, gebruik het **sleutelwoordeinde** en vorm de volgende lijn:

```
Router(config)#aaa accounting network default stop group radius local
```

Voorbeeld 3: Resourcegids genereren voor verificatie- en onderhandelingsfouten

Op dit punt biedt AAA-accounting ondersteuning voor begin- en eindrecords voor oproepen die de gebruikersverificatie met succes hebben doorlopen.

Als de verificatie of de PPP-onderhandeling mislukt, is er geen record van de verificatiepoging.

De oplossing is om eindaccounting voor mislukken van AAA-bronnen te gebruiken:

```
Router(config)#aaa accounting send stop-record authentication failure
```

Een eindrecord wordt naar de AAA-server verzonden.

Voorbeeld 4: Volledige resourceaccounting inschakelen

Om volledige bron-accounting in te schakelen die zowel een beginrecord bij het opbouwen van de oproep als een eindrecord bij het verbreken ervan genereert, moet u het volgende configureren:

```
Router(config)#aaa accounting resource start-stop
```

Deze opdracht is geïntroduceerd in Cisco IOS-softwarerelease 12.1(3)T.

Met deze opdracht wordt de voortgang van de bronverbinding met het apparaat bijgehouden via begin- en eind-accountingrecords bij het opbouwen van de oproep en het verbreken ervan. Afzonderlijke begin- en eind-accountingrecords voor gebruikersverificatie houdt de voortgang van het gebruikersbeheer bij. Deze twee reeksen van boekhoudingsverslagen zijn met een unieke zitting-ID voor de vraag verbonden.

Gerelateerde informatie

- Technische ondersteuning – 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.