Configuratie van TACACS+, RADIUS en Kerberos op Catalyst Switches

Inhoud

Inleiding

De Cisco Catalyst reeks switches (Catalyst 4000, Catalyst 5000 en Catalyst 6000 die CatOS uitvoeren) heeft enige vorm van authenticatie ondersteund, die in de 2.2 code begint. Verbeteringen zijn toegevoegd met latere versies. De TACACS+ TCP poort 49, niet XTACACS User Datagram Protocol (UDP) poort 49), RADIUS of Kerberos Server user Setup voor verificatie, autorisatie en accounting (AAA) is hetzelfde als voor routergebruikers. Dit document bevat voorbeelden van de minimale opdrachten die voor deze functies nodig zijn. Er zijn aanvullende opties beschikbaar in de documentatie bij de switch voor de versie in kwestie.

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.

Achtergrondinformatie

Sinds latere versies van codeondersteuning voor extra opties, moet u de opdracht **show versie** uitgeven om de versie van code op de switch te bepalen. Nadat u de versie van de code hebt bepaald die op de switch wordt gebruikt, gebruikt u deze tabel om te bepalen welke opties op uw apparatuur beschikbaar zijn en welke opties u wilt configureren.

Blijf altijd in de switch wanneer u authenticatie en autorisatie toevoegt. Test de configuratie in een ander venster om te voorkomen dat deze per ongeluk wordt afgesloten.

Methode (minimum)	**CATALYST, versie 2.2 t/m 5.1**	**CATALYST, versie 5.1 t/m 5.4.1**	**CATALYST, versie 5.4.1 t/m 7.5.1**	**Katalyse, versie 7.5.1 en hoger**
TACACS+ verificatie OF	Stap A	Stap A	Stap A	Stap A
RADIUS-verificatie OF	N.v.t.	Stap B	Stap B	Stap B
Kerberos-verificatie OF	N.v.t.	N.v.t.	Stap K	Stap K
Verificatie/autorisatie van lokale gebruikers	N.v.t.	N.v.t.	N.v.t.	Stap C
Plus (opties)				
Verificatie voor TACACS+ opdracht	N.v.t.	N.v.t.	Stap D	Stap D
Toestemming voor TACACS+ EXec	N.v.t.	N.v.t.	Stap E	Stap E
RADIUS-EXEC autorisatie	N.v.t.	N.v.t.	Stap F	Stap F
Accounting -	N.v.t.	N.v.t.	Stap G	Stap G

TACACS+ of RADIUS				
Toestemming voor TACACS+ inschakelen	Stap H	Stap H	Stap H	Stap H
RADIUS-autorisatie inschakelen	N.v.t.	Stap I	Stap I	Stap I
Toestemming voor TACACS+ inschakelen	N.v.t.	N.v.t.	Stap J	Stap J

Configuratiestappen

Stap A - TACACS+ verificatie

Met eerdere versies van code zijn opdrachten niet zo complex als bij sommige latere versies. Aanvullende opties in latere versies kunnen op uw switch beschikbaar zijn.

1. Geef de **ingestelde lokale inlognaam voor verificatie uit** om opdracht te geven om er zeker van te zijn dat er een achterdeur in de switch is als de server uitvalt.
2. Geef de **ingestelde authenticatie-tac's uit om** opdracht te geven om TACACS+ verificatie mogelijk te maken.
3. Geef de **ingestelde tacacs server #.#.#** opdracht uit om de server te definiëren.
4. Geef de **set tacacs-toets** *your_key* **uit om de** servertoets te definiëren, die optioneel is voor TACACS+, omdat de switch-to-server gegevens versleuteld worden. Indien gebruikt, moet het overeenkomen met de server.**Opmerking:** Cisco Catalyst OS-software accepteert **niet** dat het vraagteken (**?**) deel uitmaakt van een willekeurige toets of wachtwoorden. Het vraagteken wordt expliciet gebruikt voor hulp bij de opdrachtsyntaxis.

Stap B - RADIUS-verificatie

Met eerdere versies van code zijn opdrachten niet zo complex als bij sommige latere versies. Aanvullende opties in latere versies kunnen op uw switch beschikbaar zijn.

1. Geef de **ingestelde lokale inlognaam voor verificatie uit** om opdracht te geven om er zeker van te zijn dat er een achterdeur in de switch is als de server uitvalt.
2. Geef de **ingestelde authenticatiegrens uit om** opdracht te geven om RADIUS-verificatie mogelijk te maken.
3. Defineert de server. Voor alle andere Cisco-apparatuur zijn de standaard RADIUS-poorten 1645/1646 (verificatie/accounting).Op de Catalyst is de standaardpoort 1812/1813. Als u Cisco Secure gebruikt of een server die communiceert met andere Cisco-apparatuur, gebruikt u de 1645/1646 poort. Geef de **ingestelde straal server #.#.#. Auto-poort 1645 ingang-poort 1646 primaire** opdracht uit om de server en de gelijkwaardige opdracht in Cisco IOS te definiëren als **straal-server bron-poorten 1645-1646**.
4. Defineert de servertoets.Dit is verplicht, omdat het ervoor zorgt dat het switch-naar-server

wachtwoord wordt versleuteld zoals in de RADIUS-verificatie/autorisatie RFC 2865 en RADIUS-accounting RFC 2866 . Indien gebruikt, moet het overeenkomen met de server. Geef de **ingestelde Straaltoets *uw_key* opdracht uit**.

Stap C - Verificatie/autorisatie van lokale gebruikers

Vanaf CatOS versie 7.5.1 is lokale gebruikersverificatie mogelijk. Bijvoorbeeld, kunt u authenticatie/vergunning bereiken met het gebruik van een gebruikersnaam en wachtwoord dat op de Catalyst opgeslagen is, in plaats van authenticatie met een lokaal wachtwoord.

Er zijn slechts twee voorkeursniveaus voor lokale gebruikersauthenticatie, 0 of 15. Niveau 0 is het niet-bevoorrechte exec-niveau. Niveau 15 is het geprivilegieerde haalbaarheidsniveau.

Als u deze opdrachten in dit voorbeeld toevoegt, arriveert de `gebruiker` Poweruser in Enable mode op een telnet of console aan de switch en komt de gebruiker non-allow exec mode op een telnet of console aan de switch aan.

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

N.B.: Als de gebruiker `niet` weet **hoe** wachtwoord **wordt** ingesteld, dan kan de gebruiker de modus blijven inschakelen.

Na het configureren worden de wachtwoorden opgeslagen versleuteld.

Lokale gebruikersnaam kan worden gebruikt in combinatie met een externe TACACS+-toets, een opdrachtaccounting of een externe RADIUS-exec-accounting. Het kan ook worden gebruikt in combinatie met een externe TACACS+-optie of een commando-machtiging, maar het is niet logisch om het op deze manier te gebruiken omdat de gebruikersnaam zowel op de TACACS+-server als lokaal op de switch moet worden opgeslagen.

Stap D - Goedkeuring TACACS+

In dit voorbeeld, wordt de switch verteld om vergunning voor slechts configuratieopdrachten met TACACS+ te vereisen. In het geval dat de TACACS+ server is gedeactiveerd, is de verificatie geen naam. Dit is van toepassing op zowel de console poort als de Telnet sessie. Deze opdracht geven:

set autorisatie opdrachten maken configuratie tacacs mogelijk

In dit voorbeeld kunt u de TACACS+ server configureren om toe te staan wanneer u deze parameters instelt:

```
command=set
arguments (permit)=port 2/12
```

De **ingestelde poort laat 2/12** opdracht toe wordt naar de TACACS+ server gestuurd ter controle.

Opmerking: Als opdrachtautorisatie is ingeschakeld, in tegenstelling tot in de router waar Enable niet als een opdracht wordt beschouwd, **verstuurt** de switch de machtigingsopdracht naar de

server wanneer er een poging is gedaan om de opdracht te activeren. Zorg ervoor dat de server ook is ingesteld zodat de opdracht **activeren** is.

Stap E - Toestemming voor TACACS+ EXE

In dit voorbeeld wordt de switch verteld om toestemming te eisen voor een buitengewone zitting met TACACS+. In het geval dat de TACACS+ server is gedeactiveerd, is de vergunning geen enkele. Dit is van toepassing op zowel de console poort als de Telnet sessie. Geef het **ingestelde autorisatie exec af en laat tacacs+ geen van beide** opdrachten toe

Naast de verificatieaanvraag stuurt dit een afzonderlijk vergunningsverzoek vanuit de switch naar de TACACS+-server. Als het gebruikersprofiel op de TACACS+ server voor shell/coup is ingesteld, kan die gebruiker de switch benaderen.

Dit voorkomt dat gebruikers zonder shell/exec service die op de server, zoals PPP gebruikers, is ingesteld, in de switch kunnen loggen. U ontvangt een bericht met de tekst `Exec Mode autorisatie mislukt`. Naast het toestaan/ontkennen van exec-modus voor gebruikers, kunt u gedwongen worden om modus in te schakelen wanneer u het voorkeursniveau 15 invoert dat op de server is toegewezen. Het moet een code uitvoeren waarin Cisco bug-ID CSCdr51314 (alleen geregistreerde klanten) is gerepareerd.

Stap F - RADIUS-uitvoervergunning

Er is geen opdracht om een RADIUS-exec-vergunning mogelijk te maken. Het alternatief is om de Service-Type (RADIUS-kenmerk 6) in te stellen op Administratief (een waarde van 6) in de RADIUS-server om de gebruiker te starten en de modus in de RADIUS-server in te schakelen. Als het service-type is ingesteld voor iets anders dan 6-poorts beheerprogramma, bijvoorbeeld 1-inloggen, 7-shell of 2-framed, dan arriveert de gebruiker bij de switch-prompt maar niet bij de wizard.

Voeg deze opdrachten toe in de switch voor verificatie en autorisatie:

```
aaa authorization exec TEST group radius
 line vty 0 4
 authorization exec TEST
 login authentication TEST
```

Stap G - accounting - TACACS+ of RADIUS

Om TACACS+-boekhouding mogelijk te maken voor:

1. Als u de switch prompt krijgt, geeft u de **ingestelde accounting optie uit om start-stop tacacs+** opdracht **in te schakelen**.
2. Gebruikers die tellen uit de switch geven de **ingestelde accounting verbinden maken start-stop tacacs+** opdracht **mogelijk**.
3. Als u de switch opnieuw start, geeft u het **ingestelde accounting systeem** uit **om start-stop tacacs+** opdracht **mogelijk te maken**.
4. Gebruikers die opdrachten uitvoeren, geven de **ingestelde accounting opdrachten uit om alle start-stop tacacs+** opdracht **uit te voeren**.
5. Herinnert aan de server bijvoorbeeld om records één keer per minuut te uploaden om aan te tonen dat de gebruiker nog inlogt, geeft de **set accounting update periodieke 1** opdracht uit.

Zo kan RADIUS-accounting voor:

1. Gebruikers die de switch prompt krijgen, geven de **ingestelde accounting exec** uit **om start-stop straal** opdracht **mogelijk te maken**.
2. Gebruikers die tellen uit de switch, geven de **ingestelde accounting** uit **maken maken verbinding met start-stop straal** opdracht.
3. Wanneer u de switch opnieuw start, geeft u het **ingestelde accounting systeem** uit **om start-stop straal** opdracht **mogelijk te maken**.
4. Herinnert aan de server bijvoorbeeld om records eenmaal per minuut te uploaden om aan te tonen dat de gebruiker nog inlogt, geeft de **ingestelde accounting update periodiek 1** opdracht uit.

Gegevens TACACS+ software

Deze uitvoer is een voorbeeld van hoe de records op de server kunnen verschijnen:

```
Fri Mar 24 13:22:41 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=5 start_time=953936729 timezone=UTC
service=shell disc-cause=2 elapsed_time=236
Fri Mar 24 13:22:50 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=15 start_time=953936975 timezone=UTC
service=shell priv-lvl=0 cmd=enable
Fri Mar 24 13:22:54 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=16 start_time=953936979 timezone=UTC
service=shell priv-lvl=15 cmd=write terminal
Fri Mar 24 13:22:59 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=17 start_time=953936984 timezone=UTC
service=shell priv-lvl=15 cmd=show version
Fri Mar 24 13:23:19 2000 10.31.1.151 pinecone telnet85
171.68.118.100 update task_id=14 start_time=953936974 timezone=UTC
service=shell
```

RADIUS op UNIX-record-uitvoer

Deze uitvoer is een voorbeeld van hoe de records op de server kunnen verschijnen:

```
Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Start
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
Login-Host = 171.68.118.100
Acct-Delay-Time = 0
```

```
Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Stop
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
Login-Host = 171.68.118.100
Acct-Session-Time = 9
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Received unknown attribute 49
Acct-Session-Time = 30
Acct-Delay-Time = 0
```

Stap H - verificatie met TACACS+ inschakelen

Voer de volgende stappen uit:

1. Geef de **ingestelde authenticatie uit zodat lokaal** opdracht wordt **ingeschakeld** om er zeker van te zijn dat er een achterdeur is als de server uitvalt.
2. Geef de **ingestelde authenticatie uit zodat tacacs** opdracht geven om de switch te vertellen om verzoeken naar de server te verzenden.

Stap I - RADIUS-verificatie

Voeg deze opdrachten toe om de switch te laten de gebruikersnaam `$enab15$`toe aan de RADIUS-server. Niet alle RADIUS-servers ondersteunen dit soort gebruikersnaam. Zie Stap E voor een ander alternatief, bijvoorbeeld, als u een service-type [RADIUS-kenmerk 6 - administratieve] instelt, dat individuele gebruikers start om modus mogelijk te maken.

1. Geef de **ingestelde authenticatie uit zodat lokaal** opdracht **mogelijk** wordt om er zeker van te zijn dat er een achterdeur is in als de server uitvalt.
2. Geef de **ingestelde authenticatie** uit**, waardoor** opdracht wordt **gegeven** om de switch te vertellen verzoeken naar de server te verzenden als uw RADIUS-server de gebruikersnaam voor $enab15$ ondersteunt.

Stap J - TACACS+ autorisatie inschakelen

De toevoeging van deze opdracht resulteert in het verzenden van de switch, waarmee de server kan worden ingeschakeld wanneer de gebruiker probeert de functie te activeren. De server moet de opdracht toegestaan hebben. In dit voorbeeld is er een failover aan geen in het geval de server is neergeslagen:

de ingestelde auteur zet tacacs+ geen van beiden in

Stap K - Kerberos-verificatie

Raadpleeg Toegang tot de Switch controleren en controleren met behulp van verificatie, autorisatie en accounting voor meer informatie over het instellen van Kerberos in de switch.

Wachtwoordherstel

Raadpleeg de wachtwoordherstelprocedures voor meer informatie over de wachtwoordherstelprocedures.

Deze pagina is de index voor wachtwoordherstelprocedures voor Cisco-producten.

IP-vergunningsopdrachten voor extra beveiliging

Voor extra veiligheid, kan Catalyst worden gevormd om de toegang van het telnet door de **ip vergunning** opdrachten te controleren:

ip - vergunning instellen

ip *spreidingsmasker* **|***host*

Dit staat alleen het bereik of de hosts toe die aan telnet in de switch zijn gespecificeerd.

Debug in de Catalyst

Voordat u het debuggen op Catalyst toelaat, controleer de server logboeken om redenen voor falen. Dit is gemakkelijker en minder storend voor de switch. Op eerdere versies van de switch werd het **debug** in de technische modus uitgevoerd. Het is niet nodig om toegang te krijgen tot de technische modus om **debug** opdrachten in latere versies van code uit te voeren:

reeks-tac's|Straal|kerberos 4

Opmerking: de **ingestelde tacacs|Straal|kerberos 0**-opdracht keert de Catalyst terug naar de niet-overtrekmodus.

Raadpleeg de pagina Productondersteuning voor Switches voor meer informatie over meerlaagse LAN-Switches.

Gerelateerde informatie

- Vergelijking van TACACS+ en RADIUS
- RADIUS, TACACS+ en Kerberos in Cisco IOS-documentatie
- RADIUS-ondersteuningspagina
- Ondersteuningspagina voor TACACS/TACACS+
- Categoriepagina voor Kerberos-ondersteuning
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems