

RADIUS-configuratie met Cisco 2000/3000 Series beheerde Switches en Windows-server 2008

Doel

Remote Authorisation Dial-in User Service (RADIUS) biedt een robuuste manier van authenticatie van gebruikers om toegang tot een netwerkdienst mogelijk te maken. Daarom bieden RADIUS-servers een gecentraliseerd toegangsbeheer, waarbij de serverbeheerder beslist of een specifiek segment al dan niet met RADIUS wordt geverifieerd. In dit artikel worden de algemene stappen beschreven om RADIUS in een client/server-omgeving op te zetten, waarbij de client wordt vertegenwoordigd door de Cisco 200/300 Series beheerde Switch en de server een Windows Server 2008 met RADIUS ingeschakeld uitvoert.

Toepasselijke apparaten

- Cisco 2600/3600 Series beheerde Switches

Stapsgewijze procedure

De configuratie vindt plaats in twee delen. Eerst moeten we de switch instellen als een RADIUS-client, dan moeten we de server correct instellen voor RADIUS.

RADIUS-instelling op de switch

Stap 1. Kies in het configuratiehulpprogramma SG200/300 Series **Security > RADIUS**. De pagina *RADIUS* wordt geopend:

RADIUS

Use Default Parameters

IP Version: Version 6 Version 4

Retries: 3 (Range: 1 - 10, Default: 3)

Timeout for Reply: 3 sec. (Range: 1 - 30, Default: 3)

Dead Time: 0 min. (Range: 0 - 2000, Default: 0)

Key String: (0/128 ASCII Alphanumeric Characters Used)

Apply Cancel

RADIUS Table

<input type="checkbox"/>	Server	Priority	Key String	Timeout for Reply	Authentication Port	Retries	Dead Time	Usage Type
0 results found.								

Add... Edit... Delete

Stap 2. Voer de standaardinstellingen voor RADIUS in.

- IP Versie - Hier wordt de ondersteunde IP-versie weergegeven.
- Pogingen — Voer in dit veld het aantal verzonden aanvragen in dat naar de RADIUS-server wordt verzonden voordat een fout optreedt.
- Time-out voor antwoord — Voer in dit veld de tijd in (in seconden) dat de switch wacht op een antwoord van de RADIUS-server voordat hij een query opnieuw probeert.
- Dode tijd — Voer in dit veld de tijd in minuten in die de switch wacht voordat hij de RADIUS-server omzeilt.
- Key String — Voer in dit veld de standaardstring in die wordt gebruikt voor verificatie en codering tussen de switch en de RADIUS-server. De toets moet overeenkomen met de toets die op de RADIUS-server is ingesteld.

Stap 3. Klik op **Toepassen** om de actieve configuratie van de switch met de RADIUS-instellingen bij te werken.



Stap 4. U moet de RADIUS-server aan de switch toevoegen. Klik op **Add** (Toevoegen). De pagina *RADIUS-server toevoegen* wordt geopend in een nieuw venster:

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Global

* Server IP Address/Name:

* Priority: (Range: 0 - 65535)

Key String: Use Default
 User Defined (0/128 ASCII Alphanumeric Characters Used)

* Timeout for Reply: Use Default
 User Defined sec. (Range: 1 - 30, Default: 3)

* Authentication Port: (Range: 0 - 65535, Default: 1812)

* Retries: Use Default
 User Defined (Range: 1 - 10, Default: 3)

* Dead Time: Use Default
 User Defined min. (Range: 0 - 2000, Default: 0)

Usage Type: Login
 802.1x
 All

Stap 5. Voer in de velden de waarden in voor de server. Als u de standaardwaarden wilt gebruiken, selecteert u **Standaard gebruiken** in het gewenste veld.

- Serverdefinitie — In dit veld geeft u aan hoe u verbinding kunt maken met de server, op IP-adres of op naam van de server.
- IP-versie — Als de server wordt geïdentificeerd aan de hand van IP-adres, selecteert u IPv4- of IPv6-adres.
- IPv6-adrestype — In dit veld wordt het algemene type van het IPv6-adres weergegeven.
- IP-adres/naam server — Voer in dit veld het IP-adres of de domeinnaam van de RADIUS-server in.
- Prioriteit — Voer in dit veld de prioriteit van de server in. Als er meer dan één server is geconfigureerd, zal de switch proberen verbinding te maken met elke server volgens deze prioriteitswaarde.
- Key String — Voer in dit veld de standaardstring in die wordt gebruikt voor verificatie en codering tussen de switch en de RADIUS-server. De toets moet overeenkomen met de toets die op de RADIUS-server is ingesteld.
- Time-out voor antwoord — Voer in dit veld de tijd in (in seconden) dat de switch wacht op een antwoord van de RADIUS-server voordat hij een query opnieuw probeert.
- Verificatiepoort — Voer in dit veld het UDP-poortnummer in dat voor de RADIUS-server is ingesteld voor verificatieverzoeken.
- Pogingen — Voer in dit veld het aantal verzonden aanvragen in dat naar de RADIUS-server wordt verzonden voordat een fout optreedt.
- Dode tijd — Voer in dit veld de tijd in minuten in die de switch wacht voordat hij de RADIUS-server omzeilt.
- Gebruikstype — Voer in dit veld het verificatietype van de RADIUS-server in. Er zijn drie

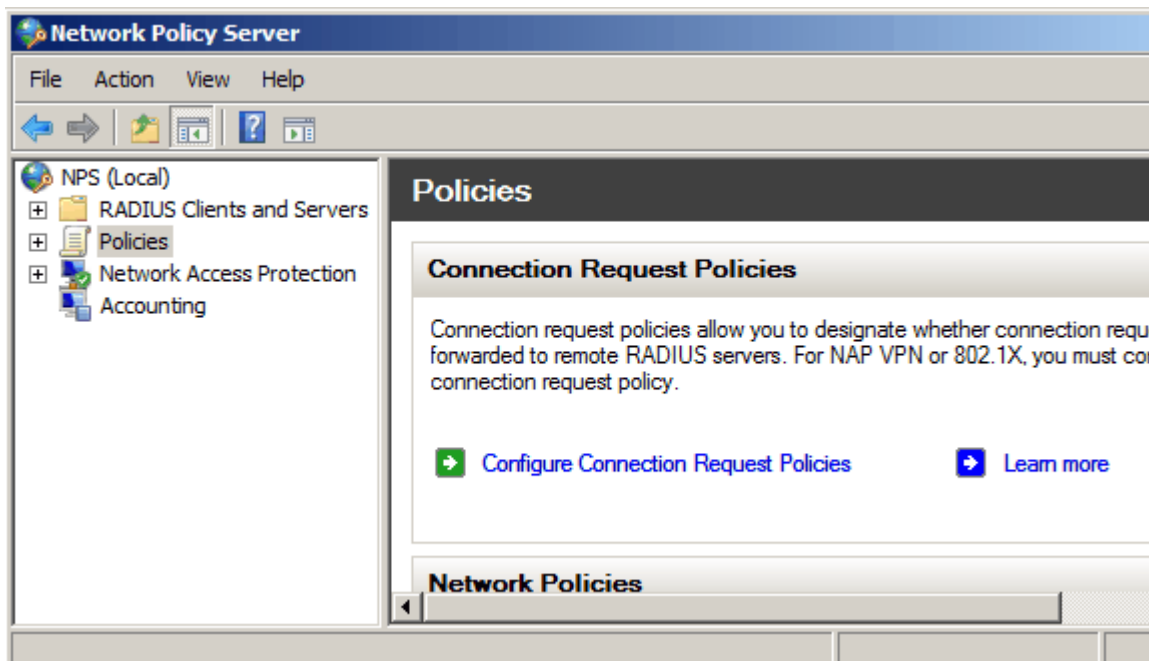
opties:

- Aanmelden — RADIUS-server verifieert gebruikers die de switch willen beheren.
- 802.1X — RADIUS-server wordt gebruikt voor 802.1X-verificatie.
- Alle — RADIUS-servers worden gebruikt voor login en 802.1X-verificaties.

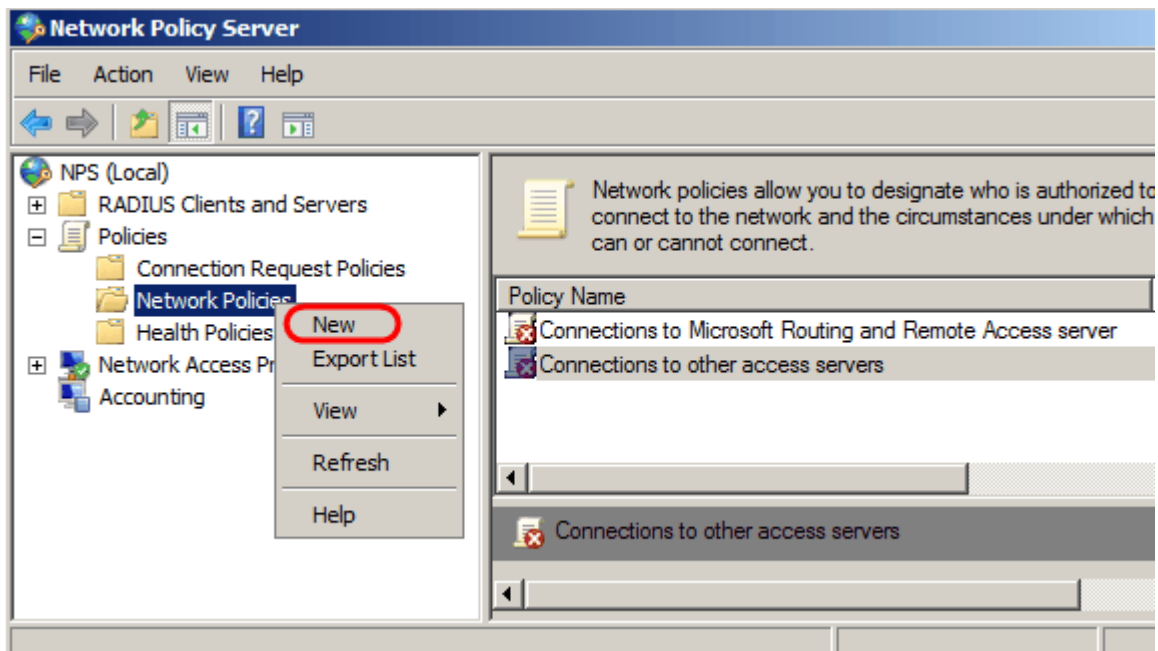
Stap 6. Klik op **Toepassen** om de serverdefinitie toe te voegen aan de actieve configuratie van de switch.

Windows Server 2008 configureren voor RADIUS

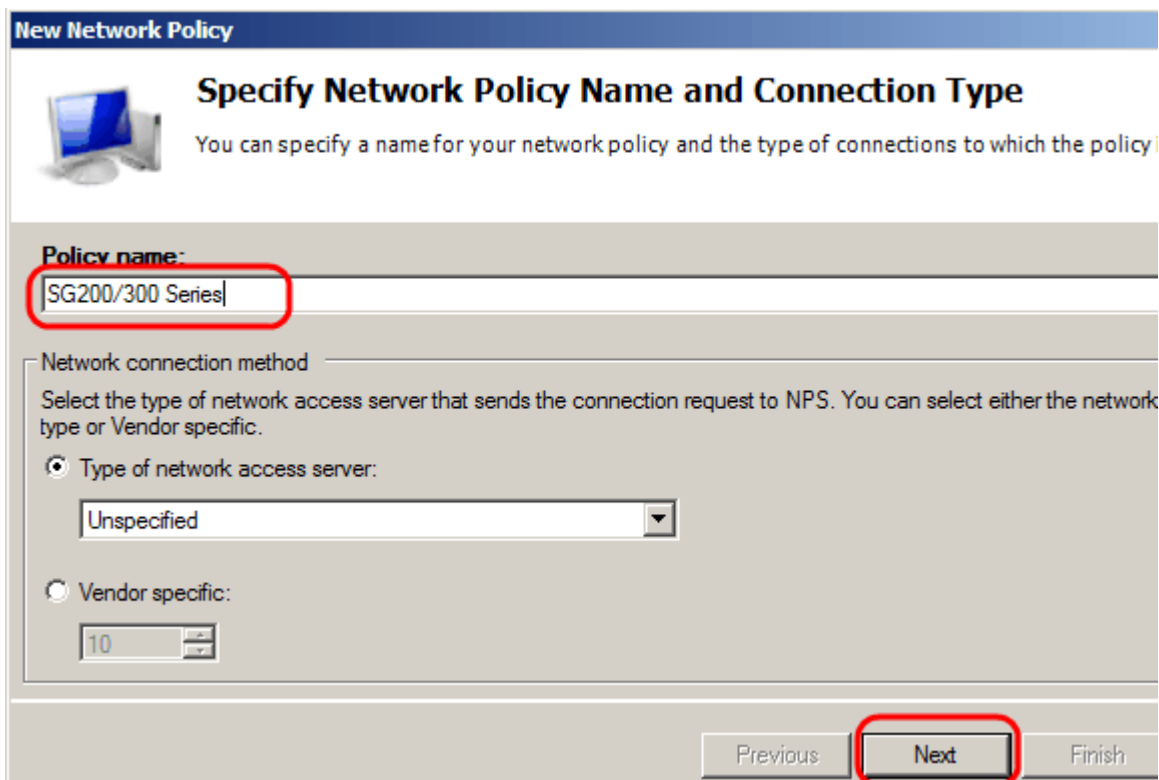
Stap 1. Kies op de Windows Server 2008-machine **Start > Administratieve tools > Network Policy Server**. Het venster *Network Policy Server* opent:



Stap 2. Om de RADIUS-server in te schakelen voor een specifiek segment van het netwerk, moet u een nieuw netwerkbeleid maken. Als u een nieuw netwerkbeleid wilt maken, kiest u **Beleid > Netwerkbeleid**, klikt u met de rechtermuisknop en vervolgens selecteert u **Nieuw**. Het *nieuwe* venster *Netwerkbeleid* wordt geopend:



Stap 3. Voer in het veld Beleidsnaam de naam voor het nieuwe beleid in. Klik op **Next** (Volgende).



Stap 4. U moet de voorwaarden van dit beleid specificeren. Er zijn twee voorwaarden nodig: aan welk segment van gebruikers de RADIUS-server wordt geïmplementeerd en welke methode wordt gebruikt om verbinding met dit segment te maken. Klik op **Add** om deze voorwaarden toe te voegen.



Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection of one condition is required.

Conditions:

Condition	Value

Condition description:

Stap 5. Onder Groepen zijn er drie opties: Windows-groepen, Machinegroepen en Gebruikersgroepen. Kies de groep volgens de instelling van het netwerk en klik op **Toevoegen**. Er wordt een nieuw venster geopend naar gelang de geselecteerde groep. Klik op **Groepen toevoegen**.

Select condition

Select a condition, and then click Add.

Groups

Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the s

Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected :

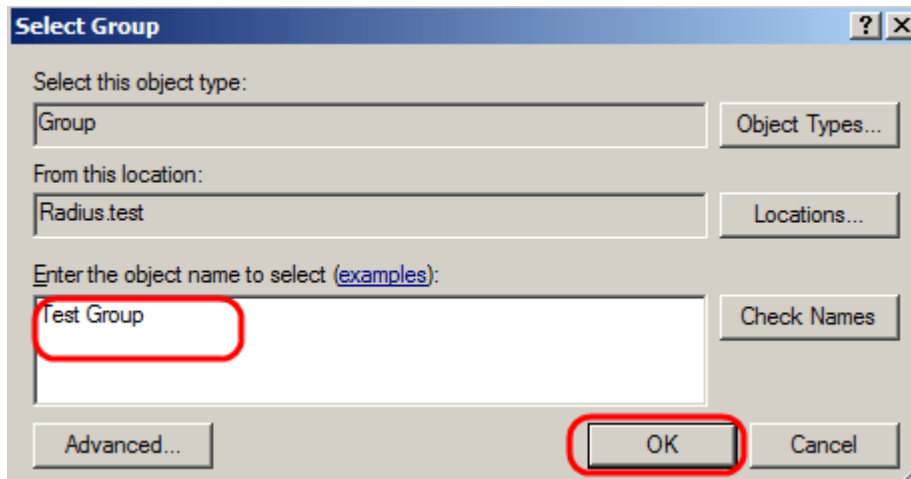
User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

HCAP

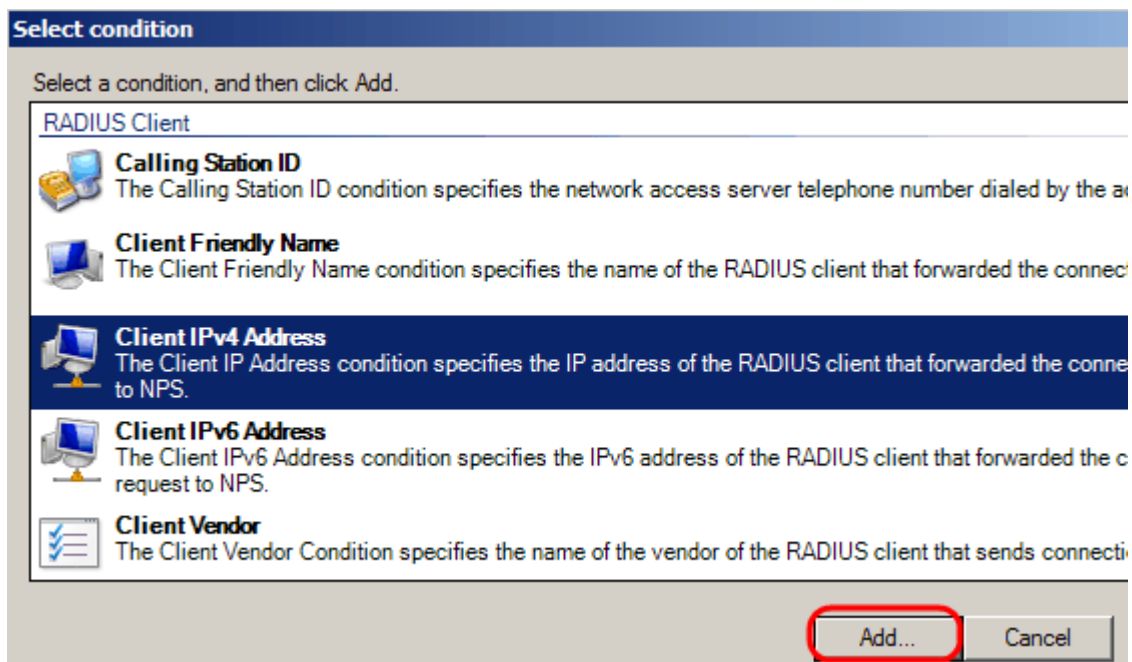
Location Groups
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) locatio required to match this policy. The HCAP protocol is used for communication between NPS and some third network access servers (NASs). See your NAS documentation before using this condition.

HCAP User Groups

Stap 6. Selecteer het objecttype, de locatie en voer de naam van het object in. Klik op **OK** en vervolgens op **OK**. Klik op **Add** om de volgende voorwaarde toe te voegen.



Stap 7. Selecteer onder RADIUS-client de optie IPv4-adres als de methode om de server aan te sluiten op de RADIUS-clients. Dit is in dit geval het IP-adres van de switch. Klik op **Add** (Toevoegen).



Stap 8. Voer het bijbehorende IP-adres in en klik op **OK**. Er wordt een lijst met toegevoegde voorwaarden weergegeven. Klik op **Volgende**.

Stap 9. Selecteer op de pagina Toegangsrechten opgeven de optie **Toegekende toegang opgeven**. Klik op **Next** (Volgende).

New Network Policy

Specify Access Permission

Configure whether you want to grant network access or deny network access if the policy.

Access granted
Grant access if client connection attempts match the conditions of this policy.

Access denied
Deny access if client connection attempts match the conditions of this policy.

Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous **Next**

Stap 10. Stel op de verificatiepagina de verificatiemethode in die het best op uw netwerk past. Klik op **Next** (Volgende).

New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request authentication, you must configure an EAP type. If you deploy NAP with 802.1X or Protected EAP in connection request policy, which overrides network policy authentication.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Move Up
Move Down

Add... Edit... Remove

Less secure authentication methods:

Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 User can change password after it has expired

Microsoft Encrypted Authentication (MS-CHAP)
 User can change password after it has expired

Encrypted authentication (CHAP)

Unencrypted authentication (PAP, SPAP)

Allow clients to connect without negotiating an authentication method.

Perform machine health check only

Previous **Next**

Stap 11. Gebruik in het venster Constricties configureren de standaardwaarden. Klik op **Next** (Volgende).

Stap 12. Klik op de pagina Instellingen configureren onder RADIUS-kenmerken op **Verkoopspecifiek** en klik vervolgens op **Toevoegen**.

N.B.: De overige instellingen op deze pagina zijn ingesteld op hun standaardwaarden. U hoeft alleen maar te zorgen voor de specifieke instellingen van de leverancier.

New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions are matched.

Settings:

- RADIUS Attributes**
 - Standard
 - Vendor Specific
- Network Access Protection**
 - NAP Enforcement
 - Extended State
- Routing and Remote Access**
 - Multilink and Bandwidth Allocation Protocol (BAP)
 - IP Filters
 - Encryption
 - IP Settings

To send additional attributes to RADIUS clients, select a Vendor then click Edit. If you do not configure an attribute, it is not sent to your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
------	--------	-------

Selecteer onder Verkoper **Cisco**. Klik op **Add** (Toevoegen). Het venster met de informatie over kenmerken wordt geopend.

Add Vendor Specific Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor:

Klik in het venster Kenmerkinformatie op **Add** en voer de waarde shell:priv-lvl:15 in. Klik op **OK**.

Attribute name:
Cisco-AV-Pair

Attribute number:
5000

Attribute format:
String

Attribute values:

Vendor	Value
Cisco	shell:priv-lvl:15

Buttons: Add..., Edit..., Remove, Move Up, Move Down, OK, Cancel

Opmerking:dit is de waarde die door Cisco is toegewezen zodat de RADIUS-server toegang kan verlenen tot het web-based switch Configuration utility.

Klik op **OK** om het venster met de kenmerken te sluiten en klik vervolgens op **Sluiten** om het venster met de specifieke kenmerken van de leverancier toe te voegen. Klik op **Next** (Volgende).

Stap 13. Er wordt een samenvatting van de instellingen voor dit beleid weergegeven. Klik op **Voltooien**. Het netwerkbeleid wordt gemaakt.



Completing New Network Policy

You have successfully created the following network policy:

SG200/300 Series

Policy conditions:

Condition	Value
Windows Groups	RADIUS\Test Group
Client IPv4 Address	192.168.1.10

Policy settings:

Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OF
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

Previous

Next

Finish

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.