Configuratievoorbeeld van TACACS+ en RADIUS voor meerdere Cisco- en niet-Cisco-apparaten

Inhoud

Inleiding

Dit document biedt een verzameling eigenschappen die verschillende Cisco- en niet-Cisco-producten verwachten te ontvangen van een AAA-server (Verificatie, autorisatie en accounting); In dit geval is de AAA-server een Access Control Server (ACS). ACS kan deze eigenschappen samen met een access-Accept als deel van een shell-profiel (TACACS+) of autorisatieprofiel (RADIUS) teruggeven.

Dit document geeft stap voor stap instructies over het toevoegen van aangepaste eigenschappen aan shell profielen en autorisatieprofielen. Dit document bevat ook een lijst met apparaten en de eigenschappen TACACS+ en RADIUS die de apparaten verwachten te zien terugkeren vanaf de AAA-server. Alle onderwerpen omvatten voorbeelden.

De lijst met eigenschappen in dit document is niet volledig of gezaghebbend en kan te allen tijde zonder bijwerking van dit document worden gewijzigd.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op ACS versie 5.2/5.3.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Een Shell-profiel maken (TACACS+)

Een shell-profiel is een basis permissies container voor TACACS+ gebaseerde toegang. U kunt specificeren welke TACACS+ eigenschappen en attribuut waarden met de Access-Accept moeten worden teruggegeven, naast het niveau van Cisco® IOS privilege, de sessietijd en andere parameters.

Voltooi deze stappen om aangepaste eigenschappen aan een nieuw shell-profiel toe te voegen:

1. Meld u aan bij de ACS-interface.
2. Navigeer naar **elementen van het beleid > Vergunning en toegangsrechten > Apparaatbeheer > Shell profielen**.
3. Klik op de knop **Maken**.
4. Geef het shell profiel aan.
5. Klik op het tabblad **Aangepaste kenmerken**.
6. Voer de eigenschap naam in in het veld **Eigenschappen**.
7. Kies of het vereiste **verplicht** is of **optioneel** van de vervolgkeuzelijst Vereiste.
8. Laat de vervolgkeuzelijst voor de eigenschap waarde ingesteld op **Static**. Als de waarde statisch is, kunt u de waarde in het volgende veld invoeren. Als de waarde dynamisch is, kunt u de eigenschap niet handmatig invoeren; in plaats daarvan wordt de toegewezen waarde in kaart gebracht aan een eigenschap in een van de identiteitszaken.
9. Typ de waarde van de eigenschap in het laatste veld.
10. Klik op de knop **Toevoegen** om de ingang aan de tabel toe te voegen.
11. Herhaal om alle eigenschappen te configureren die u nodig hebt.
12. Klik op de knop **Indienen** onder in het scherm.

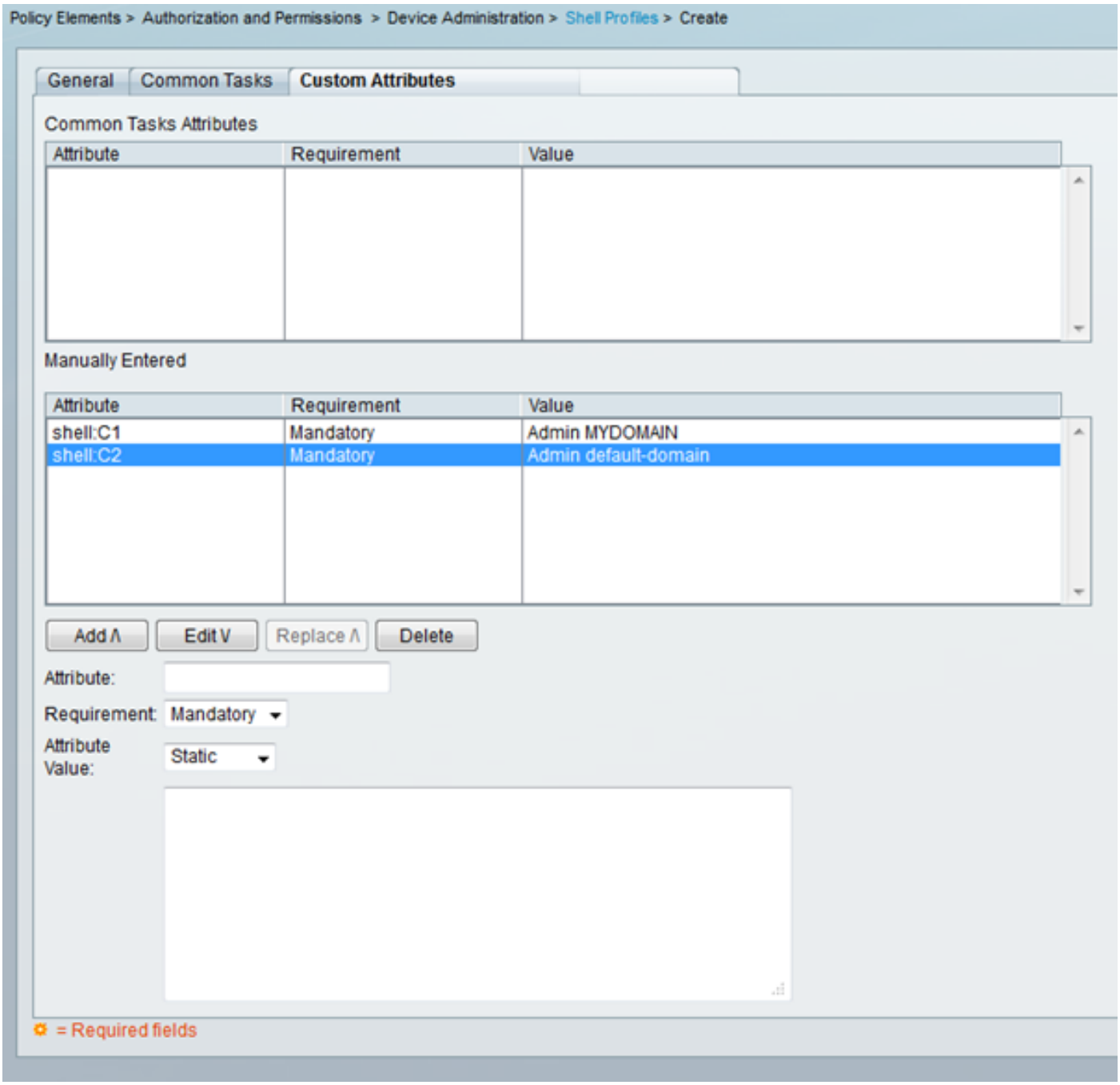
Configuratievoorbeeld

Apparaat: Application Control Engine

Kenmerken: `shell:<context-naam>`

Waarde(n): `<Rol-naam> <domeinnaam1>`

Gebruik: De rol en het domein worden van elkaar gescheiden door een spatieteken. U kunt een gebruiker (bijvoorbeeld USER1) configureren die een rol (bijvoorbeeld ADMIN) en een domein (bijvoorbeeld MYDOMAIN) krijgt toegewezen wanneer de gebruiker zich inlogt in een context (bijvoorbeeld C1).



Een autorisatieprofiel maken (RADIUS)

Een autorisatieprofiel is een elementaire permissies container voor RADIUS-gebaseerde toegang. U kunt specificeren welke RADIUS-eigenschappen en waaraan waarden moeten worden teruggegeven met de Access-Accept, naast de VLAN's, toegangscontrolelijsten (ACL's) en andere parameters.

Voltooi deze stappen om aangepaste eigenschappen aan een nieuw vergunningprofiel toe te voegen:

1. Meld u aan bij de ACS-interface.
2. Navigatie in naar **beleidselementen > autorisatie en toegangsrechten > Toegang tot netwerk > autorisatieprofielen**.
3. Klik op de knop **Maken**.
4. Naam van het vergunningprofiel.
5. Klik op het tabblad **RADIUS-kenmerken**.
6. Selecteer een woordenboek uit de vervolgkeuzelijst **Woordenboek type**.
7. Als u de eigenschap voor het veld RADIUS-kenmerken wilt instellen, klikt u op de knop **Selecteren**. Er verschijnt een nieuw venster.
8. Bekijk de beschikbare eigenschappen, maak uw selectie en klik op **OK**. De waarde **van** het **Type** van **Eigenschappen** wordt standaard ingesteld, op basis van de zojuist gemaakte selectie.
9. Laat de vervolgkeuzelijst voor de eigenschap waarde ingesteld op **Static**. Als de waarde statisch is, kunt u de waarde in het volgende veld invoeren. Als de waarde dynamisch is, kunt u de eigenschap niet handmatig invoeren; in plaats daarvan wordt de toegewezen waarde in kaart gebracht aan een eigenschap in een van de identiteitszaken.
10. Typ de waarde van de eigenschap in het laatste veld.
11. Klik op de knop **Toevoegen** om de ingang aan de tabel toe te voegen.
12. Herhaal om alle eigenschappen te configureren die u nodig hebt.
13. Klik op de knop **Indienen** onder in het scherm.

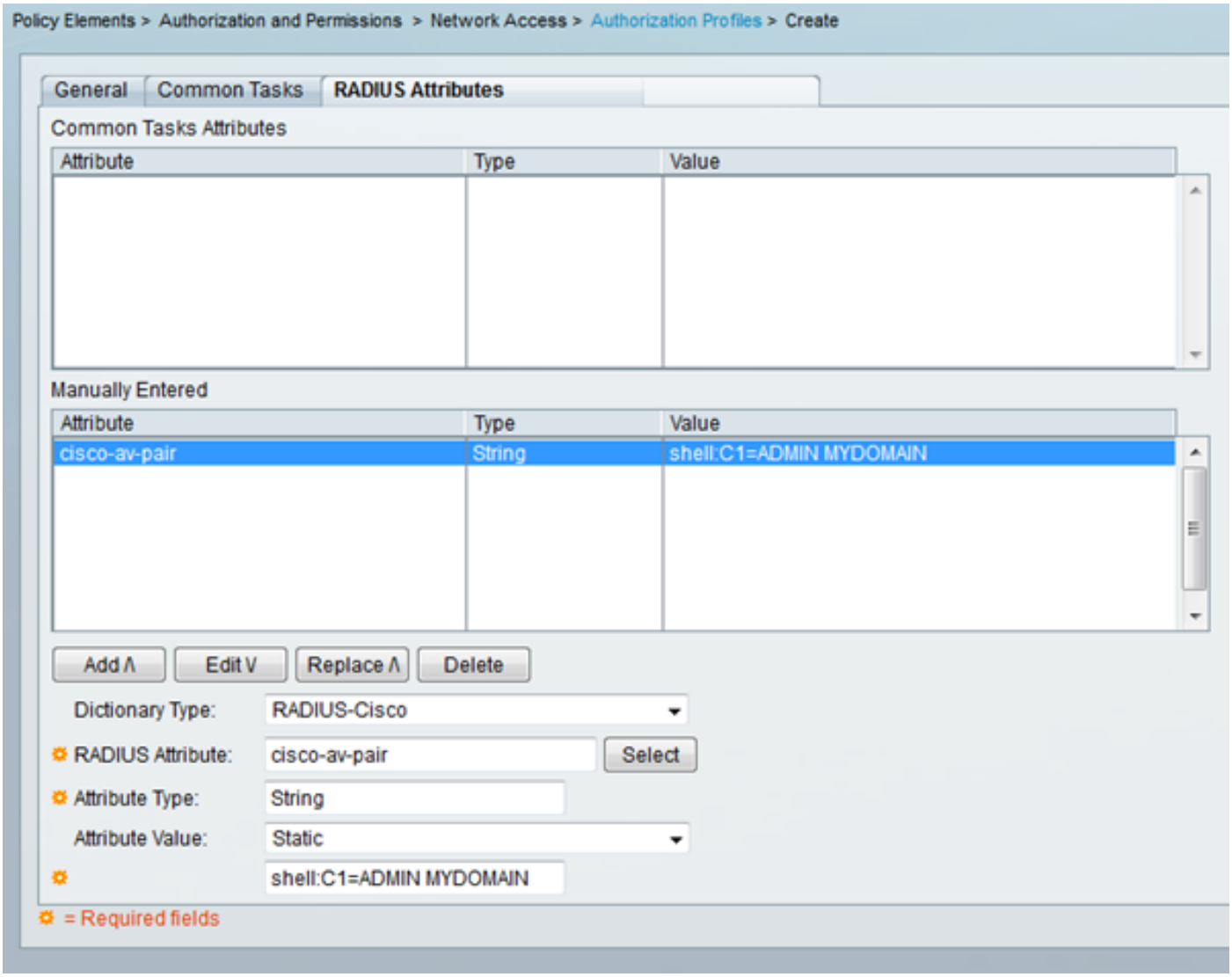
Configuratievoorbeeld

Apparaat: ACE

Kenmerken: `cisco-av-paar`

Waarde(n): `shell:<context-naam>=<role-naam> <domeinnaam1> <domeinnaam2>`

Gebruik: Elke waarde na het gelijk teken wordt gescheiden door een spatieteken. U kunt een gebruiker (bijvoorbeeld USER1) configureren die een rol (bijvoorbeeld ADMIN) en een domein (bijvoorbeeld MYDOMAIN) krijgt toegewezen wanneer de gebruiker zich inlogt in een context (bijvoorbeeld C1).



Apparaatlijst

Aggregation Services routers (ASR)

RADIUS (machtigingsprofiel)

Kenmerken: `cisco-av-paar`

Waarde(n): `shell:taken="#<rol-naam>,<toestemming><proces>"`

Gebruik: Stel de waarden van `<role-name>` in op de naam van een rol die lokaal is gedefinieerd op de router. De rolhiërarchie kan worden beschreven in termen van een boom, waarbij de rol `#root` boven in de boom staat en de rol `#leaf` extra opdrachten toevoegt. Deze twee rollen kunnen worden gecombineerd en teruggegeven indien: `shell:taken="#root,#leaf"`.

De toegangsrechten kunnen ook op een individuele procesbasis worden doorgegeven, zodat een gebruiker privileges kan worden verleend voor bepaalde processen die hij wil lezen, schrijven en uitvoeren. Stel de waarde in op: om een gebruiker lees- en schrijfrechten voor het bgp-proces te geven, `shell:taken="#root,rw:bgp"`. De volgorde van de eigenschappen doet er niet toe; het resultaat is hetzelfde ongeacht of de waarde is ingesteld op `shell:taken="#root,rw:bgp"` of `shell:taken="rw:bgp,#root"`.

Voorbeeld - *Voeg de eigenschap toe aan een vergunningsprofiel*

Type woordenboek	RADIUS-kenmerk	Type kenmerken	Waarde van kenmerken
RADIUS-Cisco	`cisco-av-pair`	String	`shell:tasks="#root,#leaf, rwx:bgp,r:ospf"`

Application Control Engine

TACACS+ (Shell-profiel)

Kenmerken: `shell:<context-naam>`

Waarde(n): `<Rol-naam> <domeinnaam1>`

Gebruik: De rol en het domein worden van elkaar gescheiden door een spatieteken. U kunt een gebruiker (bijvoorbeeld USER1) configureren die een rol (bijvoorbeeld ADMIN) en een domein (bijvoorbeeld MYDOMAIN) krijgt toegewezen wanneer de gebruiker zich inlogt in een context (bijvoorbeeld C1).

Voorbeeld - *Voeg de eigenschap toe aan een Shell-profiel*

Kenmerken	Vereisten	Waarde van kenmerken
`shell:C1`	Verplicht	`Admin MYDOMAIN`

Als USER1 zich in de C1-context inlogt, wordt die gebruiker automatisch de ADMIN-rol en het MYDOMAIN-domein toegewezen (op voorwaarde dat een autorisatieregel is ingesteld waarbij, zodra USER1 inlogt, zij dit autorisatieprofiel krijgen).

Als USER1 zich inlogt door een andere context, die niet wordt teruggegeven in de waarde van de eigenschap die ACS terugstuurt, wordt die gebruiker automatisch de standaardrol (Network-Monitor) en het standaarddomein (standaard-domein) toegewezen.

RADIUS (machtigingsprofiel)

Kenmerken: `cisco-av-paar`

Waarde(n): `shell:<context-naam>=<role-naam> <domeinnaam1> <domeinnaam2>`

Gebruik: Elke waarde na het gelijk teken wordt gescheiden door een spatieteken. U kunt een gebruiker (bijvoorbeeld USER1) configureren die een rol (bijvoorbeeld ADMIN) en een domein (bijvoorbeeld MYDOMAIN) krijgt toegewezen wanneer de gebruiker zich in een context inlogt (bijvoorbeeld C1).

Voorbeeld - *Voeg de eigenschap toe aan een vergunningsprofiel*

Type woordenboek	RADIUS-kenmerk	Type kenmerken	Waarde van kenmerken
RADIUS-		String	

Cisco	`cisco-av-pair`		`shell:C1=ADMIN MYDOMAIN`

Als USER1 zich in de C1-context inlogt, wordt die gebruiker automatisch de ADMIN-rol en het MYDOMAIN-domein toegewezen (op voorwaarde dat een autorisatieregel is ingesteld waarbij, zodra USER1 inlogt, zij dit autorisatieprofiel krijgen).

Als USER1 zich inlogt door een andere context, die niet wordt teruggegeven in de waarde van de eigenschap die ACS terugstuurt, wordt die gebruiker automatisch de standaardrol (Network-Monitor) en het standaarddomein (standaard-domein) toegewezen.

BlueCoat Packet Shaper

RADIUS (machtigingsprofiel)

Kenmerken: `Packet-AVPlucht`

Waarde(n): `toegang=<niveau>`

Gebruik: `<niveau>` is het toegangsniveau voor subsidies. Touch access is gelijk aan lezen-schrijven, terwijl blijkbaar toegang gelijk is aan alleen-lezen.

BlueCoat VSA bestaat standaard niet in de ACS-woordenboeken. Om de BlueCoat eigenschap in een autorisatieprofiel te gebruiken, moet u een BlueCoat woordenboek maken en de BlueCoat eigenschappen aan dat woordenboek toevoegen.

Het woordenboek maken:

1. Navigeer naar **systeembeheer > Configuratie > Woordenboeken > protocollen > RADIUS- > RADIUS VSA.**
2. Klik op **Maken**.
3. Voer de details van het woordenboek in:Name: Blauwe jasVerkopers-ID: 2334Voorvoegsel van kenmerken: Packet-over
4. Klik op **Inzenden**.

Een eigenschap in het nieuwe woordenboek maken:

1. navigeren naar **systeembeheer > Configuratie > Woordenboeken > protocollen > RADIU S > RADIUS VSA > BlueCoat.**
2. Klik op **Maken**.
3. Voer de details van de eigenschap in:Kenmerk: `Packet-AVPlucht`Beschrijving: Gebruikt om toegangsniveau te bepalenID van leverancierkenmerk: 1Richting: OUTBOUNDMeervoudig toegestaan: OnjuistEigenschappen in logbestand opnemen: gecontroleerdType kenmerk: String
4. Klik op **Inzenden**.

Voorbeeld - ***Voeg de eigenschap toe aan een machtigingsprofiel (voor alleen-lezen toegang)***

Type woordenboek	**RADIUS-kenmerk**	**Type kenmerken**	**Waarde van kenmerken**
RADIUS-		String	

Blauwe Coat	`Packeteer-AVPair`		`access=look`

Voorbeeld - *Voeg de eigenschap toe aan een machtigingsprofiel (voor toegang tot lezen)*

Type woordenboek	RADIUS-kenmerk	Type kenmerken	Waarde van kenmerken
RADIUS-Blauwe Coat	`Packeteer-AVPair`	String	`access=touch`

Bladeswitches

RADIUS (machtigingsprofiel)

Kenmerken: `Tunnel-Private-Group-ID`

Waarde(n): `U:<VLAN1>`; `T:<VLAN2>`

Gebruik: Stel `<VLAN1>`in op de waarde van het VLAN-gegevens. Stel `<VLAN2>`in op de waarde van het spraak-VLAN. In dit voorbeeld, is het data VLAN 10, en de stem VLAN is VLAN 21.

Voorbeeld - *Voeg de eigenschap toe aan een vergunningsprofiel*

Type woordenboek	RADIUS-kenmerk	Type kenmerken	Waarde van kenmerken
RADIUS-IETF	`Tunnel-Private-Group-ID`	Tagged string	`U:10;T:21`

Cisco Unity Express (CUE)

RADIUS (machtigingsprofiel)

Kenmerken: `cisco-av-paar`

Waarde(n): `fonds:groepen=<groep-naam>`

Gebruik: `<group-name>` is de naam van de groep met de privileges die u aan de gebruiker wilt verlenen. Deze groep moet worden ingesteld op Cisco Unity Express (CUE).

Voorbeeld - *Voeg de eigenschap toe aan een vergunningsprofiel*

Type woordenboek	RADIUS-kenmerk	Type kenmerken	Waarde van kenmerken
RADIUS-Cisco	`cisco-av-pair`	String	`fndn:groups=Administrators`

Infoblox

RADIUS (machtigingsprofiel)

Kenmerken: `Infoblox-groepsinformatie`

Waarde(n): `<naam van de groep>`

Gebruik: `<group-name>` is de naam van de groep met de privileges die u aan de gebruiker wilt verlenen. Deze groep moet worden ingesteld op het Infoblox-apparaat. In dit configuratievoorbeeld is de groepsnaam MyGroup.

De Infoblox VSA bestaat standaard niet in de ACS-woordenboeken. Om de Infoblox eigenschap in een vergunningprofiel te gebruiken, moet u een Infoblox-woordenboek maken en de Infoblox-eigenschappen aan dat woordenboek toevoegen.

Het woordenboek maken:

1. Navigeer naar **systeembeheer > Configuratie > Woordenboeken > protocollen > RADIU S > RADIUS VSA.**
2. Klik op **Maken**.
3. Klik op de kleine pijl naast **Gebruik** de **optie Geavanceerde leveranciers**.
4. Voer de details van het woordenboek in:Name: InfobloxVerkopers-ID: 7779Lengte verkoper: 1Veldgrootte verkoper: 1
5. Klik op **Inzenden**.

Een eigenschap in het nieuwe woordenboek maken:

1. navigeren naar **systeembeheer > Configuratie > Woordenboeken > protocollen > RADIU S > RADIUS VSA > Infoblox.**
2. Klik op **Maken**.
3. Voer de details van de eigenschap in:Kenmerk: `Infoblox-groepsinformatie`ID van leverancierkenmerk: 009Richting: OUTBOUNDMeervoudig toegestaan: OnjuistEigenschappen in logbestand opnemen: gecontroleerdType kenmerk: String
4. Klik op **Inzenden**.

Voorbeeld - *Voeg de eigenschap toe aan een vergunningsprofiel*

Type woordenboek	RADIUS-kenmerk	Type kenmerken	Waarde van kenmerken
RADIUS-Infoblox	`Infoblox-Group-Info`	String	`MyGroup`

Inbraakpreventiesysteem (IPS)

RADIUS (machtigingsprofiel)

Kenmerken: `IPS-rol`

Waarde(n): `<naam rol>`

Gebruik: De waarde `<role name>` kan een van de vier gebruikersrollen van het

Inbraakpreventiesysteem (IPS) zijn: kijker, exploitant, beheerder of dienst. Raadpleeg de configuratiehandleiding voor uw versie van IPS voor de details van de permissies die aan elk type gebruikersrol zijn toegekend.

- Cisco-configuratiegids voor inbraakpreventiesysteem voor IPS 7.0
- Cisco-configuratiegids voor inbraakpreventiesysteem voor IPS 7.1

Voorbeeld - *Voeg de eigenschap toe aan een vergunningsprofiel*

Type woordenboek	RADIUS-kenmerk	Type kenmerken	Waarde van kenmerken
RADIUS-Cisco	`cisco-av-pair`	String	`ips-role:administrator`

Juniper

TACACS+ (Shell-profiel)

Kenmerken: `oppervlakkige opdrachten` ; `opstelling van de begrenzing` ; `naam van de plaatselijke gebruiker` ; `ontkenningsopdrachten` ; `ontconfiguratie`; `gebruikersrechten`

Waarde(n): `<allow-opdrachten-regex>` ; `<allow-configuratie-regex>`; `<plaatselijke gebruikersnaam>`; `<ontkenningsopdrachten-regex>` ; `<ontkenning-configuratie-regex>`

Gebruik: Stel de waarde van `<local-user-name>` (d.w.z. de waarde van de locale-user-name eigenschap) in op een gebruikersnaam die lokaal op het Juniper-apparaat bestaat. U kunt bijvoorbeeld een gebruiker (bijvoorbeeld USER1) configureren die dezelfde gebruikerssjabloon krijgt toegewezen als een gebruiker (bijvoorbeeld JUSER) die lokaal op het Juniper-apparaat bestaat, wanneer u de waarde van de locale gebruiker-name-eigenschap instelt op JUSER. De waarden van de toestaat-opdrachten, de configuratie, de ontkenningsopdrachten, en de ontkenningsconfiguratieeigenschappen kunnen in regex formaat worden ingevoerd. De waarden waarop deze eigenschappen worden ingesteld, komen bovenop de opdrachten van de operationele/configuratiemodus die zijn toegestaan door de bits met de inlogklasse en de rechten van de gebruiker.

Voorbeeld - *Eigenschappen aan een Shell Profile 1 toevoegen*

Kenmerken	Vereisten	Waarde van kenmerken
`allow-commands`	Optioneel	`"(request system) | (show rip neighbor)"`
`allow-configuration`	Optioneel	
`local-user-name`	Optioneel	`sales`
`deny-commands`	Optioneel	`"<^clear"`
`deny-configuration`	Optioneel	

Voorbeeld - *Eigenschappen aan een Shell Profile 2 toevoegen*

Kenmerken	Vereisten	Waarde van kenmerken
`allow-commands`	Optioneel	`"monitor | help | show | ping | traceroute"`
`allow-configuration`	Optioneel	
`local-user-name`	Optioneel	`engineering`
`deny-commands`	Optioneel	`"configure"`
`deny-configuration`	Optioneel	

Nexus-switches

RADIUS (machtigingsprofiel)

Kenmerken: `cisco-av-paar`

Waarde(n): `shell:rollen="<rol1> <rol2>"`

Gebruik: Stel de waarden van `<role1>` en `<rol2>`in op de namen van rollen die lokaal op de schakelaar zijn gedefinieerd. Wanneer u meerdere rollen toevoegt, scheidt u deze met een spatie-teken. Wanneer meerdere rollen van de AAA server aan de Nexus schakelaar worden doorgegeven, is het resultaat dat de gebruiker toegang heeft tot opdrachten die door de unie van alle drie de rollen zijn gedefinieerd.

De ingebouwde rollen worden gedefinieerd in Gebruikersrekeningen en RBAC configureren.

Voorbeeld - *Voeg de eigenschap toe aan een vergunningsprofiel*

Type woordenboek	RADIUS-kenmerk	Type kenmerken	Waarde van kenmerken
RADIUS-Cisco	`cisco-av-pair`	String	`shell:roles="network-admin vdc-admin vdc-operator"`

rivierbedding

TACACS+ (Shell-profiel)

Kenmerken: `dienst` ; `naam van de plaatselijke gebruiker`

Waarde(n): `rbt-exec` ; `<gebruikersnaam>`

Gebruik: Om de gebruiker alleen-lezen toegang te geven, moet de `<gebruikersnaam>`waarde worden ingesteld op monitor. Om de gebruiker read-writer toegang te geven tot het lezen, moet de `<gebruikersnaam>`waarde worden ingesteld op de beheerder. Als u een andere account hebt die

naast het beheer en de monitor is gedefinieerd, moet u deze naam dan configureren.

Voorbeeld - *Add Attributes to a Shell Profile (voor alleen-lezen toegang)*

Kenmerken	Vereisten	Waarde van kenmerken
`service`	Verplicht	`rbt-exec`
`local-user-name`	Verplicht	`monitor`

Voorbeeld - *Add Attributes aan een Shell Profile (voor read-schrijf toegang)*

Kenmerken	Vereisten	Waarde van kenmerken
`service`	Verplicht	`rbt-exec`
`local-user-name`	Verplicht	`admin`

Draadloze LAN-controller (WLC)

RADIUS (machtigingsprofiel)

Kenmerken: `servicetype`

Waarde(n): `Administratief (6)` / `NAS-prompt (7)`

Gebruik: Om de gebruiker toegang tot de draadloze LAN-controller (WLC) te bieden, moet de waarde administratief zijn; voor alleen-lezen toegang moet de waarde NAS-Prompt zijn.

Zie RADIUS-serververificatie van beheergebruikers voor meer informatie over het configuratievoorbeeld van de draadloze LAN-controller (WLC)

Voorbeeld - *Voeg de eigenschap toe aan een machtigingsprofiel (voor alleen-lezen toegang)*

Type woordenboek	RADIUS-kenmerk	Type kenmerken	Waarde van kenmerken
RADIUS-IETF	`Service-Type`	Oplage	`NAS-Prompt`

Voorbeeld - *Voeg de eigenschap toe aan een machtigingsprofiel (voor toegang tot lezen)*

Type woordenboek	RADIUS-kenmerk	Type kenmerken	Waarde van kenmerken
RADIUS-IETF	`Service-Type`	Oplage	`Administratief`

Data Center Network Manager (DCNM)

DCNM moet opnieuw worden gestart nadat de authenticatiemethode is gewijzigd. Anders kan het de rechten van de netwerkbeheerder toewijzen in plaats van de beheerder van het netwerk.

DCNM-rol	RADIUS-Cisco-AV-paar	Tacacs-Cisco-AV-paar
Gebruiker	`shell:roles = "network-operator"`	`cisco-av-pair=shell:roles="network-operator"`
administrateur	`shell:roles = "network-admin"`	`cisco-av-pair=shell:roles="network-admin"`

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems
- Terminal Access Control-systeem (TACACS+)
- Inbelservice voor externe verificatie (RADIUS)
- Verzoeken om opmerkingen (RFC's)