CSU configureren voor UNIX (Solaris)

Inhoud

Inleiding

Cisco Secure ACS voor UNIX (CSU)-software helpt de beveiliging van het netwerk te garanderen en houdt de activiteit bij van mensen die met succes verbinding maken met het netwerk. CSU fungeert als een TACACS+ of RADIUS-server en gebruikt verificatie, autorisatie en accounting (AAA) om netwerkbeveiliging te bieden.

CSU ondersteunt deze databaseopties voor het opslaan van groep- en gebruikersprofielen en boekhoudingsinformatie:

- SQLAnywhere (meegeleverd met CSU).

  Deze versie van Sybase SQLAnywhere heeft geen client/server ondersteuning. Het is echter geoptimaliseerd om essentiële AAA-services uit te voeren met CSU.

  Waarschuwing: de SQLnywhere-databaseoptie ondersteunt geen profieldatabases die meer dan 5.000 gebruikers tellen, replicatie van profielinformatie tussen databaselocaties of de functie Cisco Secure Distribute Session Manager (DSM).

- Oracle of Sybase Relational Database Management System (RDBMS).

  Om Cisco Secure Profile databases van 5000 of meer gebruikers, databasereplicatie of de

functie Cisco Secure DSM te ondersteunen, moet u een Oracle (versie 7.3.2, 7.3.3 of 8.0.3) of Sybase SQL Server (versie 11) RDBMS vooraf installeren om uw Cisco Secure Profile-informatie te bevatten. De replicatie van een database vereist een verdere RDBMS-configuratie nadat de Cisco Secure-installatie is voltooid.

- De upgrade van een bestaande database van een vorige (2.x) versie van CSU.

  Als u een upgrade uitvoert van een eerdere versie van Cisco Secure 2.x, wordt de profieldatabase automatisch door het Cisco Secure-installatieprogramma bijgewerkt om compatibel te zijn met CSU 2.3 voor UNIX.

- Een bestaande profieldatabase importeren.

  U kunt bestaande freeware TACACS+ of RADIUS-profieldatabases of platte bestanden converteren voor gebruik met deze versie van de CSU.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Secure ACS 2.3 voor UNIX.

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.

CSU-configuratie

Gebruik deze procedures om CSU te configureren.

Start de Cisco Secure Administrator-interface

Gebruik deze procedure om in te loggen op de Cisco Secure Administrator.

1. Van elk werkstation met een webverbinding naar de ACS, start uw webbrowser.
2. Voer een van deze URL's in voor de Cisco Secure Administrator-website:

- Als de functie voor de beveiligingssocket op uw browser niet is ingeschakeld, voert u het volgende in:

  ```
  http://your_server/cs
  ```

  waar your_server de hostnaam is (of de volledig gekwalificeerde domeinnaam (FQDN), als hostnaam en FQDN verschillen) van het SPARCstation waar u CSU hebt geïnstalleerd. U kunt ook het IP-adres van SPARCstation vervangen door uw_server.

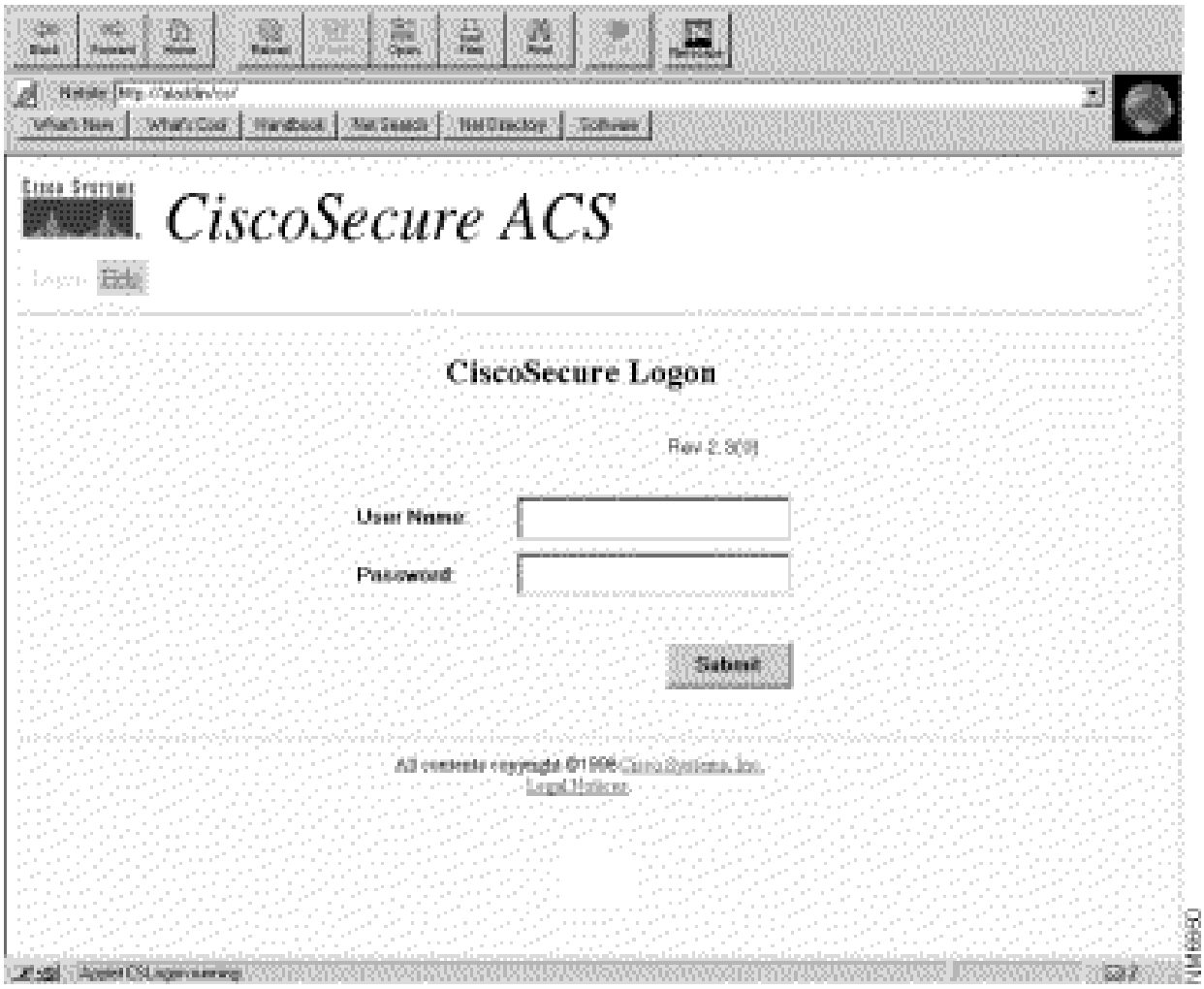
- Als de functie voor de beveiligingssocket in uw browser is ingeschakeld, specificeert u "https" in plaats van "http" als het hypertext-transmissieprotocol. Voer in:

  ```
  https://your_server/cs
  ```

  waar your_server de hostnaam is (of de FQDN, als hostnaam en FQDN verschillen) van het SPARCstation waar u CSU hebt geïnstalleerd. U kunt ook het IP-adres van SPARCstation vervangen door uw_server.

  Opmerking: URL's en servernamen zijn hoofdlettergevoelig. Ze moeten worden getypt met hoofdletters en kleine letters precies zoals aangegeven op de afbeelding.

  De CSU-aanmeldpagina wordt weergegeven.



3. Voer uw gebruikersnaam en wachtwoord in. Klik op Verzenden.

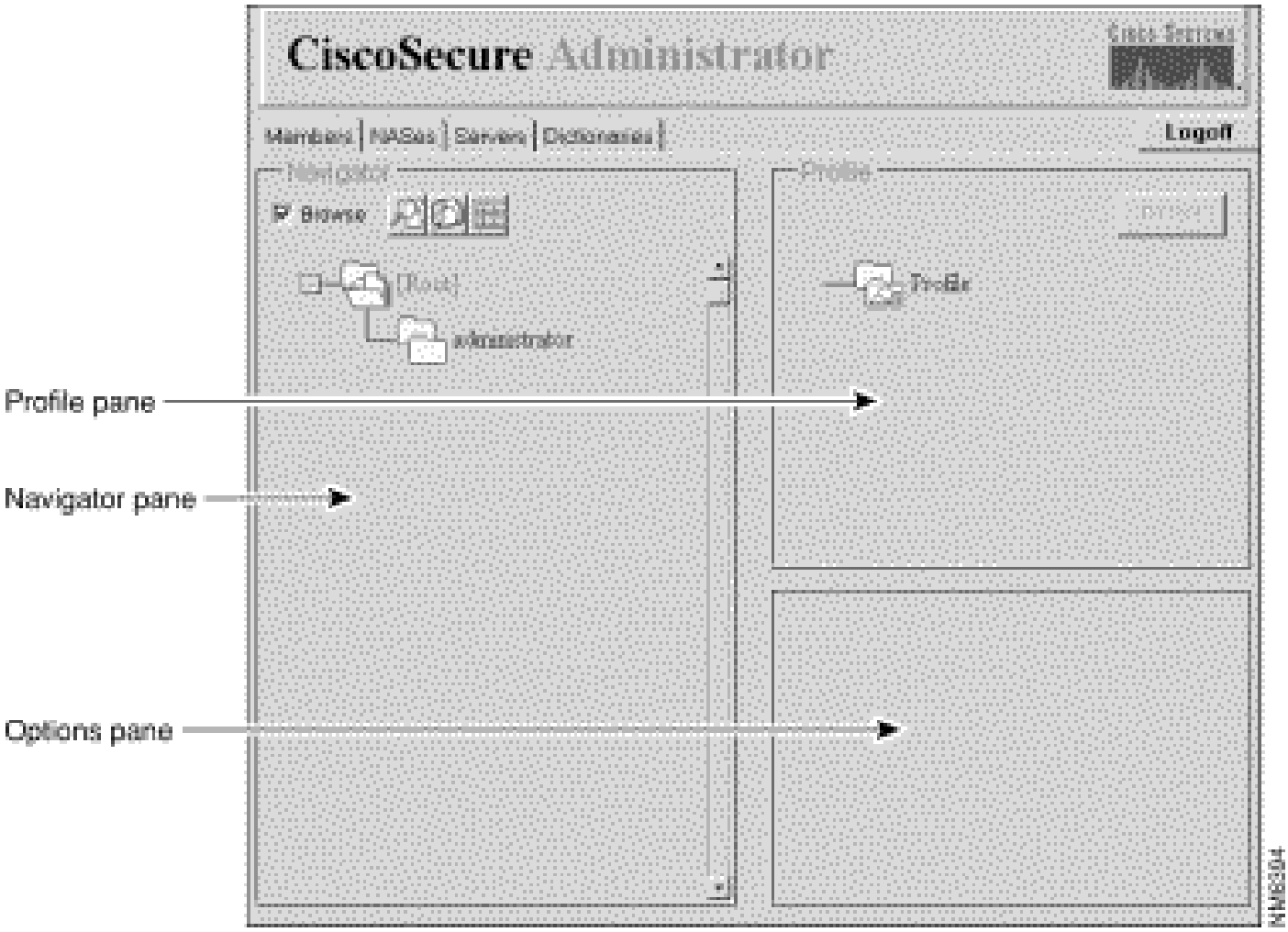
   Opmerking: de oorspronkelijke standaardgebruikersnaam is "superuser". Het defaultwachtwoord is "wijzigen". Na uw eerste aanmelding moet u de gebruikersnaam en het wachtwoord onmiddellijk wijzigen voor maximale beveiliging.

   Na u aanmelding wordt de CSU-hoofdpagina weergegeven met de hoofdmenubalk bovenaan. De CSU Main-menupagina wordt alleen weergegeven als de gebruiker een naam en wachtwoord invoert met rechten op beheerdersniveau. Als de gebruiker een naam en wachtwoord opgeeft die alleen rechten op gebruikersniveau hebben, wordt er een ander scherm weergegeven.

Start het programma voor geavanceerde configuratie

Start het op Java gebaseerde Cisco Secure Administrator Advanced Configuration-programma vanaf een van de CSU Administrator-webpagina's. Klik vanuit de menubalk van de CSU-webinterface op Geavanceerd en klik vervolgens nogmaals op Geavanceerd.

Het programma Cisco Secure Administrator Advanced Configuration verschijnt. Het kan een paar minuten duren om te laden.



Een groepsprofiel maken

Gebruik het programma Cisco Secure Administrator Advanced Configuration om groepsprofielen te maken en te configureren. Cisco raadt u aan groepsprofielen te maken om gedetailleerde AAA-vereisten te configureren voor grote aantallen soortgelijke gebruikers. Nadat het groepsprofiel is gedefinieerd, gebruikt u de CSU Webpagina Gebruikersprofielen toevoegen om snel gebruikersprofielen aan het groepsprofiel toe te voegen. De geavanceerde vereisten die voor de groep zijn geconfigureerd, zijn van toepassing op elke gebruiker.

Gebruik deze procedure om een groepsprofiel te maken.

1. Selecteer in het programma Cisco Secure Administrator Advanced Configuration het tabblad Leden. In het Navigator-venster deselecteert u het aankruisvakje Bladeren. Het pictogram Nieuw profiel maken wordt weergegeven.

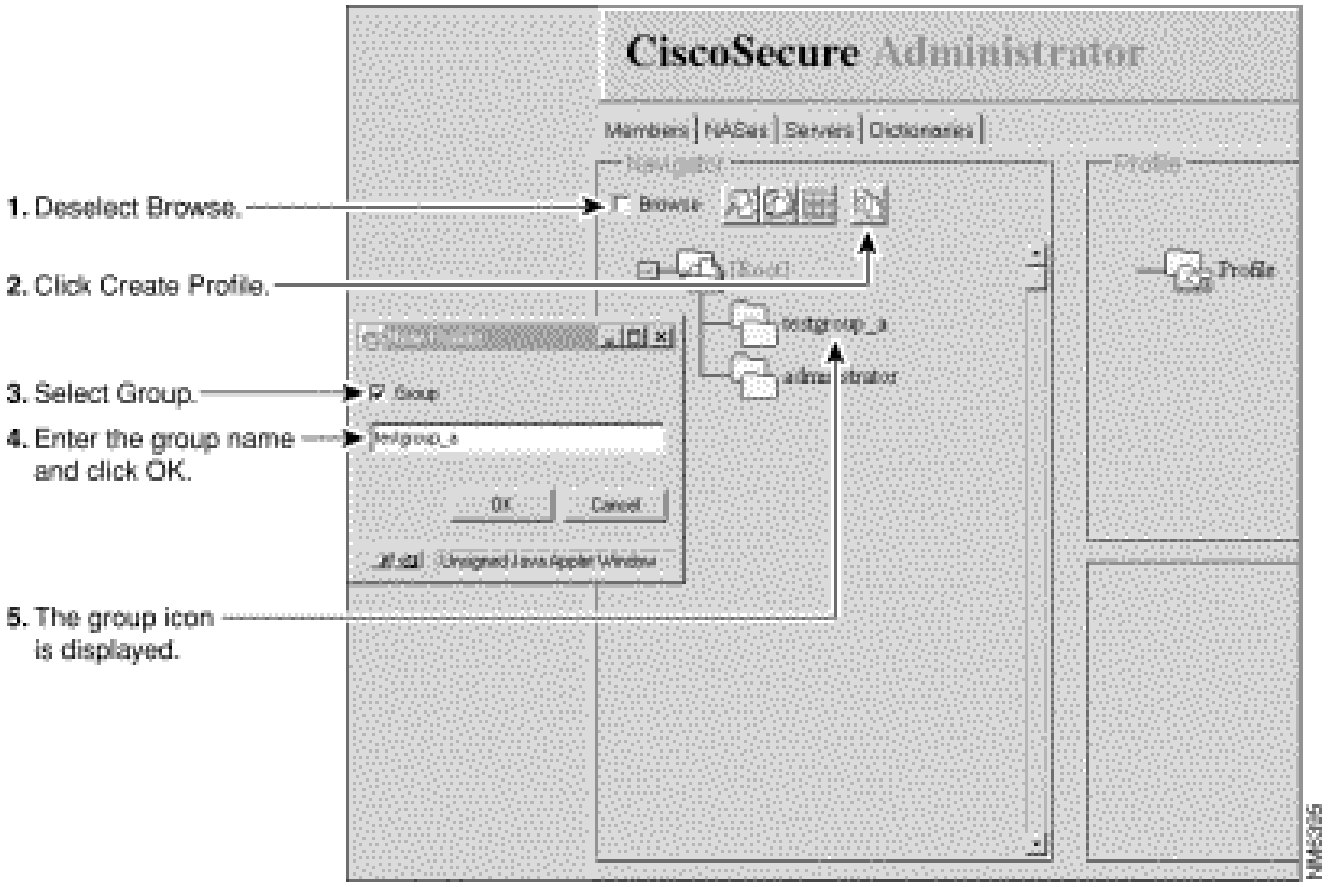
2. In het Navigator-venster voert u een van de volgende handelingen uit:

    - Als u een groepsprofiel zonder parent wilt maken, zoekt u het pictogram voor de [Root]-map en klikt u erop.

    - Als u uw groepsprofiel wilt aanmaken als het onderliggend element van een ander groepsprofiel, zoekt u de gewenste groep als het bovenliggend profiel en klikt u erop.

- Als de groep die u wilt zijn de ouder is een kindgroep, klik dan op de map van de oudergroep om deze weer te geven.

3. Klik op Nieuw profiel maken. Het dialoogvenster Nieuw profiel verschijnt.
4. Selecteer het aanvinkvakje Groep, typ de naam van de groep die u wilt maken en klik op OK. De nieuwe groep wordt in de boom weergegeven.
5. Nadat u het groepsprofiel hebt gemaakt, wijst u TACACS+- of RADIUS-kenmerken toe om specifieke AAA-eigenschappen te configureren.



Een gebruikersprofiel maken in de modus Geavanceerde configuratie

Gebruik de modus Geavanceerde configuratie voor Cisco Secure Administrator om een gebruikersprofiel te maken en te configureren. U kunt dit doen om de machtigings- en boekhoudingseigenschappen van het gebruikersprofiel meer in detail aan te passen dan mogelijk is met de pagina Een gebruiker toevoegen.

Gebruik deze procedure om een gebruikersprofiel te maken:

1. Selecteer in het programma Cisco Secure Administrator Advanced Configuration het tabblad Leden. Zoek in het navigator-venster en deselecteer de optie Bladeren. Het pictogram Nieuw profiel maken wordt weergegeven.
2. In het Navigator-venster voert u een van de volgende handelingen uit:

- Lokaliseer en klik op de groep waartoe de gebruiker behoort.
- Als u niet wilt dat de gebruiker tot een groep behoort, klikt u op het pictogram voor de map [Root].

3. Klik op Profiel maken. Het dialoogvenster Nieuw profiel verschijnt.
4. Zorg dat het selectievakje Groep is uitgeschakeld.
5. Voer de naam in van de gebruiker die u wilt maken en klik op OK. De nieuwe gebruiker verschijnt in de structuur.
6. Nadat u het gebruikersprofiel hebt gemaakt, kunt u specifieke TACACS+- of RADIUS-kenmerken toewijzen om specifieke AAA-eigenschappen te configureren:
   - Zie Tacacs+-kenmerken aan een groep- of gebruikersprofiel toewijzen om Tacacs+-profielen aan het gebruikersprofiel toe te wijzen.
   - Zie RADIUS-kenmerken aan een groep- of gebruikersprofiel toewijzen om RADIUS-profielen aan het gebruikersprofiel toe te wijzen.

Strategieën om kenmerken toe te passen

Gebruik de functies CSU-groepsprofiel en TACACS+ en RADIUS-kenmerken om verificatie en autorisatie van netwerkgebruikers via CSU te implementeren.

Kenmerken plan voor groepen en gebruikers

Met behulp van de groepsprofielfunctie van CSU kunt u een gemeenschappelijke reeks AAA-vereisten definiëren voor een groot aantal gebruikers.

U kunt een reeks TACACS+ of RADIUS-kenmerkwaarden toewijzen aan een groepsprofiel. Deze attribuutwaarden die aan de groep zijn toegewezen, gelden voor elke gebruiker die lid is of die als lid van die groep wordt toegevoegd.

Effectief gebruik maken van de groepsprofielfunctie

Om CSU te configureren voor het beheer van grote aantallen en verschillende typen gebruikers met complexe AAA-vereisten, raadt Cisco u aan de functies van het programma Cisco Secure Administrator Advanced Configuration te gebruiken om groepsprofielen te maken en te configureren.

Het groepsprofiel moet alle eigenschappen bevatten die niet specifiek zijn voor de gebruiker. Dit betekent gewoonlijk alle eigenschappen behalve het wachtwoord. U kunt vervolgens de pagina Een gebruiker toevoegen van de beveiligde Cisco-beheerder gebruiken om eenvoudige gebruikersprofielen met wachtwoordkenmerken te maken en deze gebruikersprofielen toe te wijzen aan het juiste groepsprofiel. De eigenschappen en de attributenwaarden die voor een bepaalde groep worden bepaald zijn dan op zijn ledengebruikers van toepassing.

Oudergroepen en kindergroepen

U kunt een hiërarchie van groepen maken. U kunt binnen een groepsprofiel kindergroepprofielen maken. De waarden van kenmerken die aan het profiel van de oudergroep zijn toegewezen, zijn de standaardwaarden voor de kindergroepprofielen.

Beheer op groepsniveau

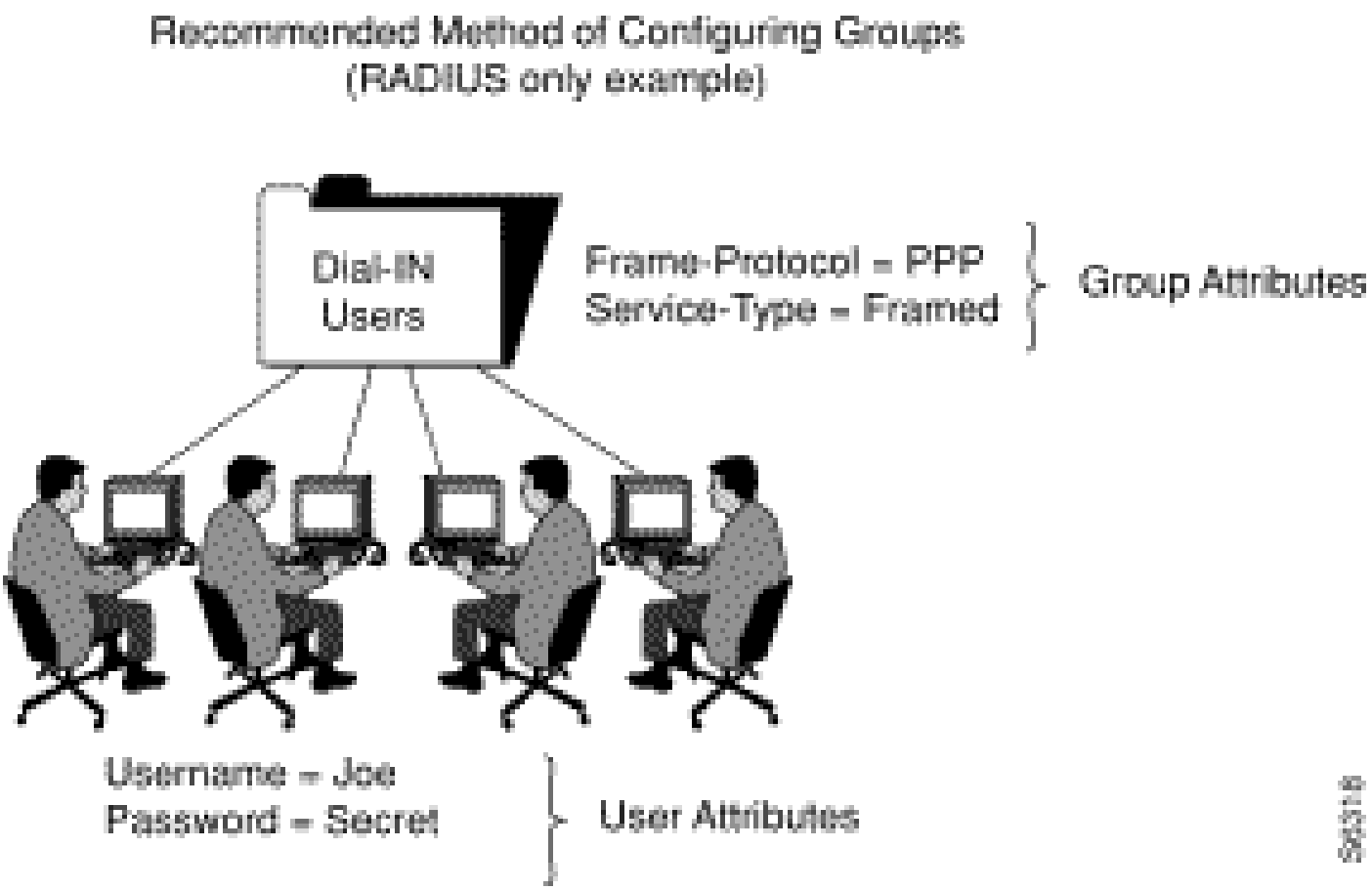
Een Cisco Secure-systeembeheerder kan de individuele beheerderstatus van Cisco Secure-gebruikersgroep toewijzen. Met de beheerderstatus van een groep kunnen individuele gebruikers alle kindergroepprofielen en gebruikersprofielen beheren die ondergeschikt zijn aan hun groep. Ze mogen echter geen groepen of gebruikers beheren die buiten de hiërarchie van hun groep vallen. Zo parcelt de systeembeheerder de taak van het beheren van een groot netwerk uit aan andere individuen zonder elk van hen gelijke autoriteit te verlenen.

Welke kenmerken definieer ik voor individuele gebruikers?

Cisco raadt aan individuele gebruikers fundamentele verificatiekenmerken toe te wijzen die uniek zijn voor de gebruiker, zoals kenmerken die de gebruikersnaam, het wachtwoord, het wachtwoordtype en de webrechten definiëren. Wijs de basiswaarden van verificatiekenmerken toe aan uw gebruikers via CSU's Een gebruiker bewerken of pagina's toevoegen.

Welke kenmerken definieer ik voor groepsprofielen?

Cisco raadt u aan kwalificatie-, autorisatie- en accounting-gerelateerde kenmerken op groepsniveau te definiëren.



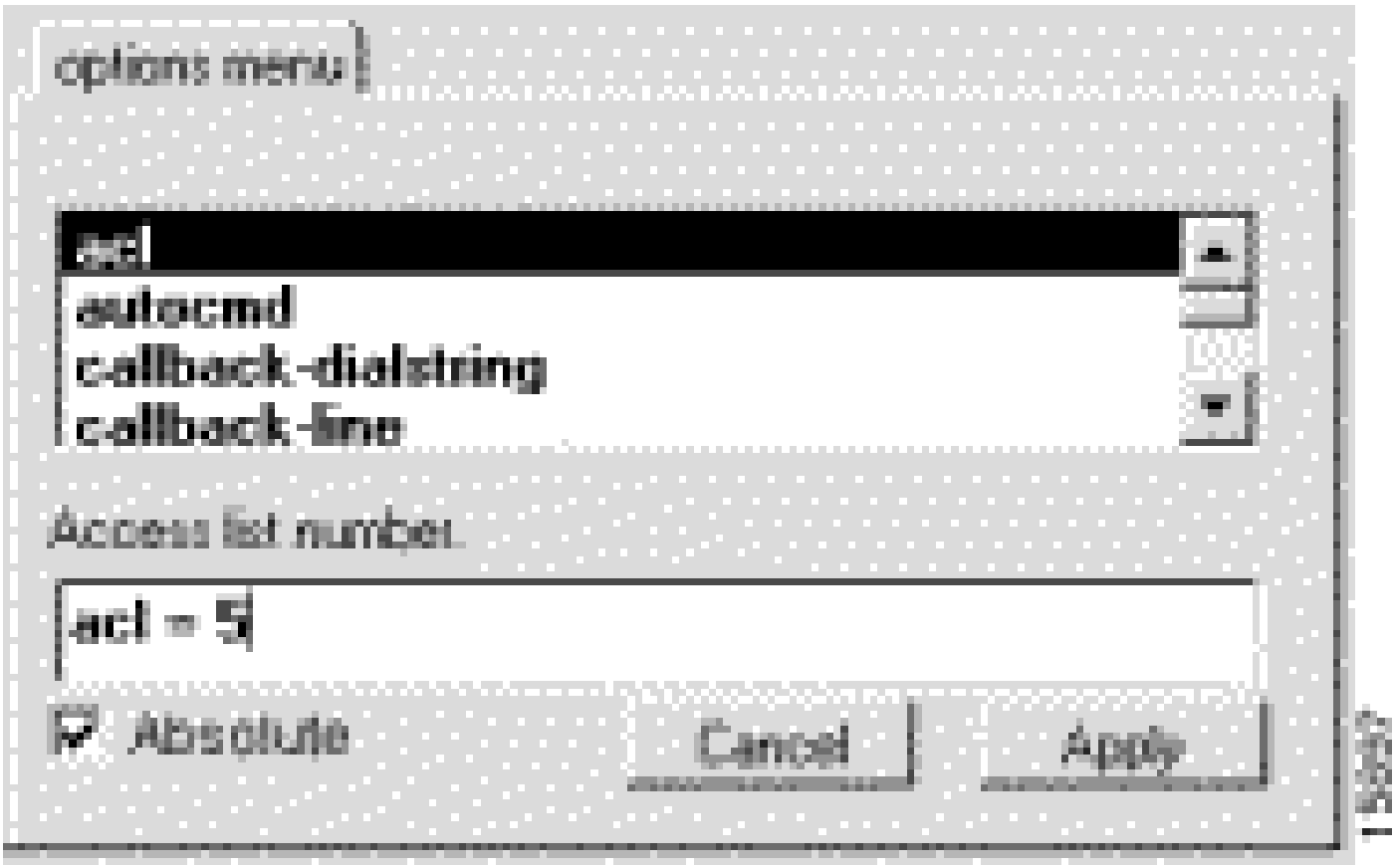
In dit voorbeeld wordt aan het groepsprofiel "Inbel-gebruikers" de attribuut-waarde paren Frame-Protocol=PPP en Service-Type=Framed toegewezen.

Wat zijn absolute kenmerken?

Een subset van de eigenschappen TACACS+ en RADIUS in CSU kan absolute status op het niveau van het groepsprofiel worden toegewezen. Een attributenwaarde die voor absolute status op het niveau van het groepsprofiel wordt toegelaten treedt om het even welke tegengestelde attributenwaarden op een profiel van de kindgroep of het niveau van het gebruikersprofiel van het lid met voeten.

Binnen netwerken op meerdere niveaus met meerdere niveaus van groepsbeheerders, maken absolute attributen een systeembeheerder in staat om geselecteerde groepsattributen waarden in te stellen die groepsbeheerders op lagere niveaus niet kunnen negeren.

Attributen die absolute status kunnen worden toegewezen, geven een selectievakje Absolute aan in het vakje Attributen van het programma Cisco Secure Administrator Advanced Configuration. Selecteer het aankruisvakje om de absolute status in te schakelen.



Kunnen de waarden van groepsattributen en de Waarden van Gebruikersattributen strijdig zijn?

Conflictresolutie tussen attributenwaarden die zijn toegewezen aan oudergroepprofielen, kindergroepprofielen en gebruikersprofielen van leden, is afhankelijk van de absolute waarde van de attributen en of deze TACACS+- of RADIUS-kenmerken zijn:

- De TACACS+- of RADIUS-kenmerkwaarden die aan een groepsprofiel zijn toegewezen met absolute status, negeren alle tegenovergestelde kenmerkwaarden die op het niveau van een kindgroep of gebruikersprofiel zijn ingesteld.
- Als de absolute status van een TACACS+ attributenwaarde niet is ingeschakeld op het niveau van het groepsprofiel, wordt deze waarde overschreven door een tegenovergestelde attribuutwaarde die is ingesteld op het niveau van de kindergroep of het gebruikersprofiel.
- Als de absolute status van een RADIUS-attribuut niet is ingeschakeld op het niveau van de oudergroep, dan resulteren alle tegenstrijdige attribuutwaarden die zijn ingesteld op een onderliggend groepresultaat in een onvoorspelbaar resultaat. Wanneer u RADIUS-kenmerkwaarden voor een groep en de gebruikers ervan definieert, moet u vermijden dat dezelfde eigenschap wordt toegewezen aan zowel de gebruikers- als de groepsprofielen.

Gebruik de opties Verbod en vergunning

Voor TACACS+, treed de beschikbaarheid van geërfde de dienstwaarden met voeten door het sleutelwoord voor te fixeren verbieden of vergunning aan de de dienstspecificatie. Het trefwoord vergunning staat de gespecificeerde diensten toe. Het verboden trefwoord verbiedt de opgegeven

services. Met het gebruik van deze trefwoorden samen, kunt u "alles behalve" configuraties. Deze configuratie biedt bijvoorbeeld toegang vanaf alle services behalve X.25:

```
default service = permit
prohibit service = x25
```

Toewijzen van TACACS+ kenmerken aan een groep- of gebruikersprofiel

Om specifieke TACACS+ diensten en attributen aan een groep of een gebruikersprofiel toe te wijzen, volg deze stappen:

1. Selecteer in het programma Cisco Secure Administrator Advanced Configuration het tabblad Leden. Klik in het navigatiedeelvenster op het pictogram voor het groep- of gebruikersprofiel waaraan TACACS+-kenmerken zijn toegewezen.

2. Indien nodig klikt u in het Profielvenster op het pictogram Profielen om dit uit te vouwen.

   Een lijst of dialoogvenster met eigenschappen die van toepassing zijn op het geselecteerde profiel of de geselecteerde service wordt weergegeven in het venster rechtsonder op het scherm. De informatie in dit venster verandert op basis van welk profiel of welke service u in het Profielvenster selecteert.

3. Klik op de service of het protocol dat u wilt toevoegen en klik op Toepassen. De service wordt toegevoegd aan het profiel.

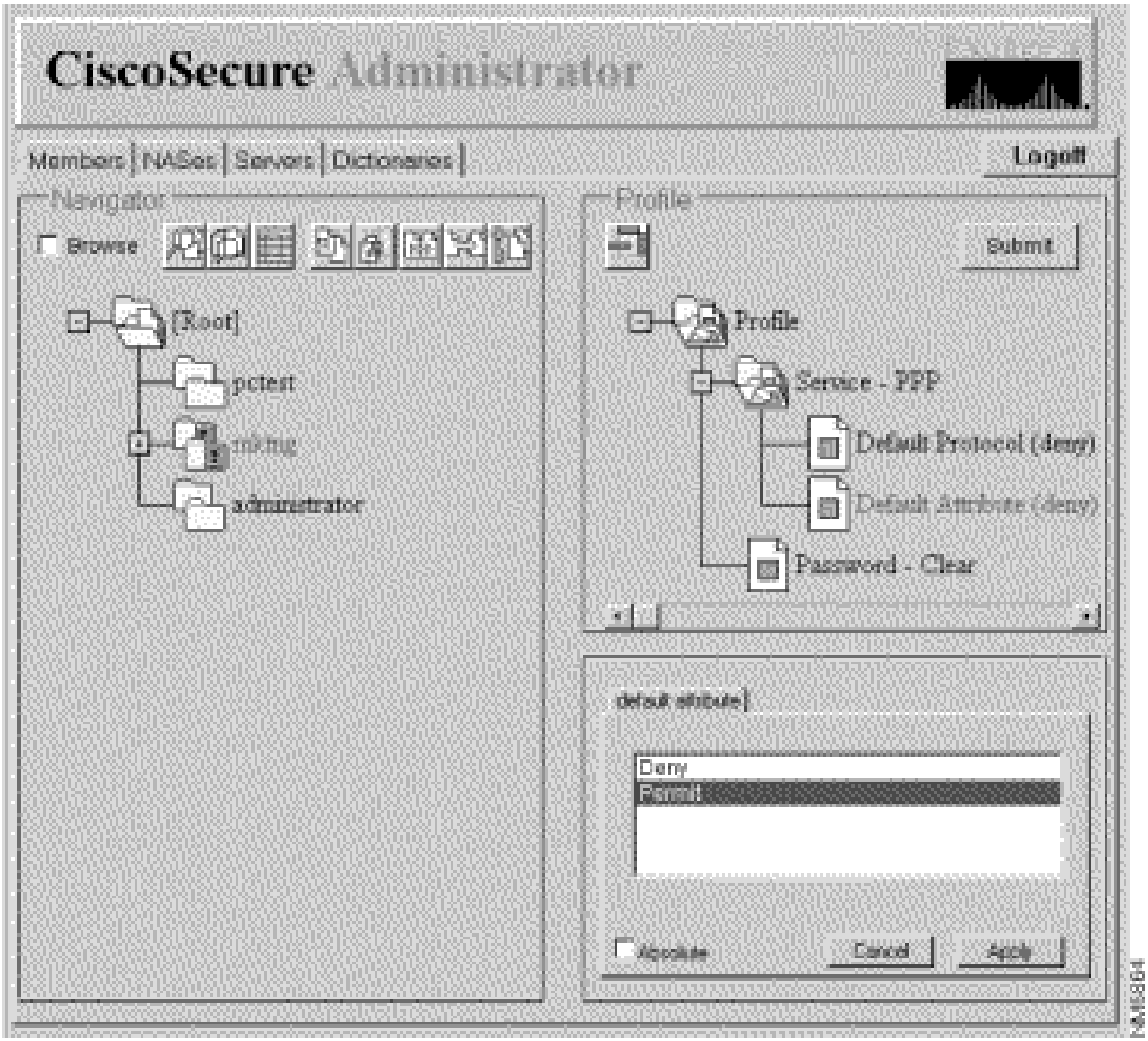
4. Voer de gewenste tekst in of selecteer deze in het venster Kenmerken.

   Geldige items worden uitgelegd in de sectie Strategieën voor het toepassen van eigenschappen van de CSU 2.3 voor UNIX Reference Guide.

   Opmerking: Als u een attribuut waarde toewijst op het niveau van het groepsprofiel en het attribuut dat u opgeeft een absoluut selectievakje weergeeft, selecteert u dat selectievakje om de waarde absolute status toe te kennen. Een aan een waarde toegewezen absolute status kan niet worden overschreven door tegenstrijdige waarden die zijn toegewezen op het niveau van het ondergeschikte groepsprofiel of het gebruikersprofiel.

5. Herhaal stap 1 tot en met voor elke extra service of protocol dat u moet toevoegen.

6. Wanneer alle wijzigingen zijn aangebracht, klikt u op Indienen.



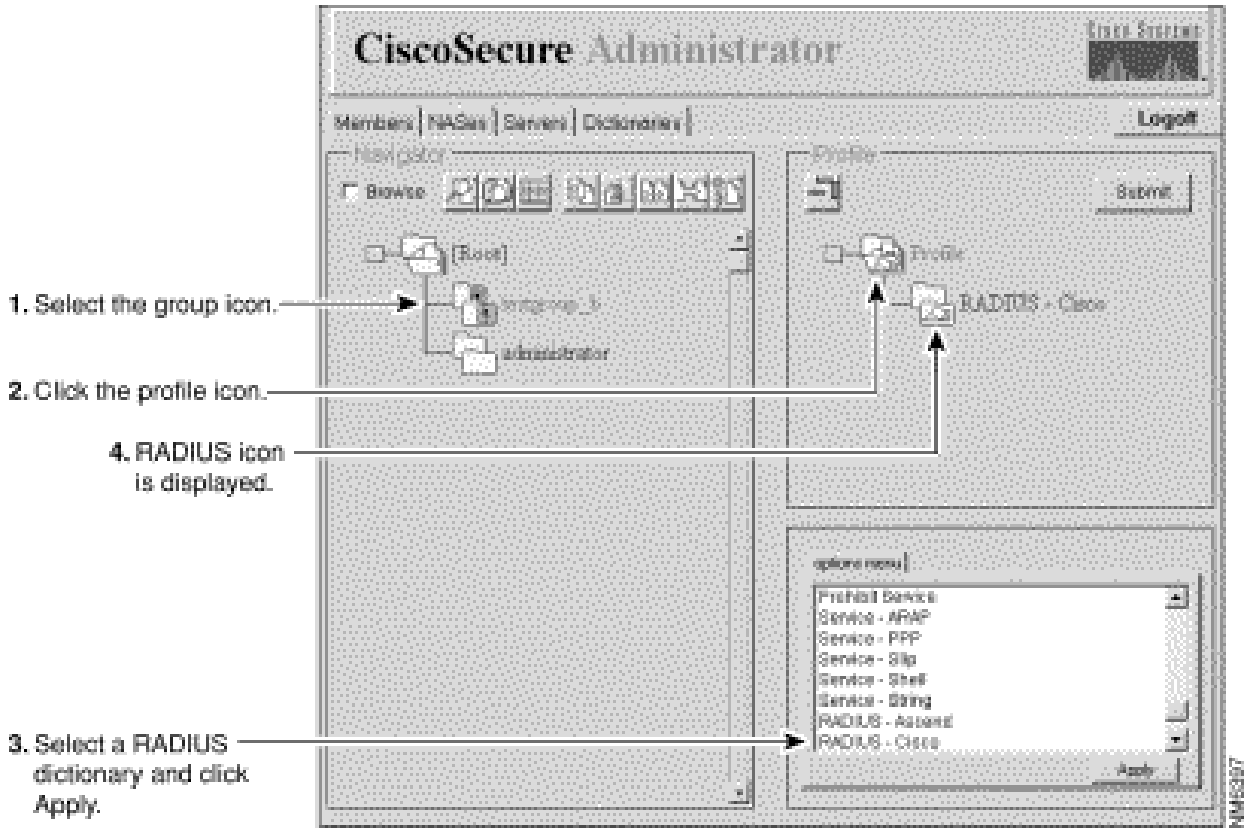
RADIUS-kenmerken toewijzen aan een groep- of gebruikersprofiel

U kunt als volgt specifieke RADIUS-kenmerken toewijzen aan een groep- of gebruikersprofiel:

1. Wijs een RADIUS-woordenboek toe aan het groepsprofiel:

    a. Klik op de pagina Leden van het programma Geavanceerde configuratie voor Cisco Secure Administrator op het pictogram Groep of Gebruiker en klik vervolgens op het pictogram Profiel in het deelvenster Profielen. In het deelvenster Kenmerken verschijnt het menu Opties.

    b. Klik in het menu Opties op de naam van het RADIUS-woordenboek dat de groep of gebruiker moet gebruiken. (Bijvoorbeeld RADIUS - Cisco.) Klik op Apply (Toepassen).



2. Voeg de vereiste controle-items en antwoord-kenmerken toe aan het RADIUS-profiel:

   N.B.: Controleer items zijn vereiste kenmerken voor verificatie, zoals gebruikers-id en wachtwoord. Antwoordkenmerken zijn kenmerken die naar de Network Access Server (NAS) worden verzonden nadat het profiel de verificatieprocedure heeft doorlopen, zoals Framed-Protocol. Raadpleeg voor lijsten en toelichtingen bij Eigenschappen controleren en Antwoordkenmerken de RADIUS Attribute-Value-paren en Woordenboekbeheer in CSU 2.3 voor UNIX Reference Guide.

   a. Klik in het profielvenster op het pictogram van de map RADIUS - woordenboek. (U moet waarschijnlijk op het +-symbool van het profiel klikken om de RADIUS-map uit te vouwen.) De opties Items controleren en Kenmerken antwoorden weergeven in het venster Attributengroep.

   b. Als u een of meer van deze kenmerken wilt gebruiken, klikt u op het attribuut of de attributen die u wilt gebruiken en vervolgens klikt u op Toepassen. U kunt meer dan één kenmerk tegelijk toevoegen.

   c. Klik op het symbool + voor de RADIUS - woordenboeknaam om de map uit te vouwen.

      Opmerking: Als u de optie RADIUS-Cisco11.3 selecteert, zorg er dan voor dat Cisco IOS®-softwarerelease 11.3.3(T) of hoger op uw aangesloten NAS's is geïnstalleerd en voeg nieuwe opdrachtregels toe aan uw NAS-configuraties. Raadpleeg het woordenboek RADIUS-Cisco11.3 volledig inschakelen in CSU 2.3 voor UNIX Reference Guide.

3. Specificeer waarden voor de toegevoegde punten van de Controle en attributen van het

Antwoord:

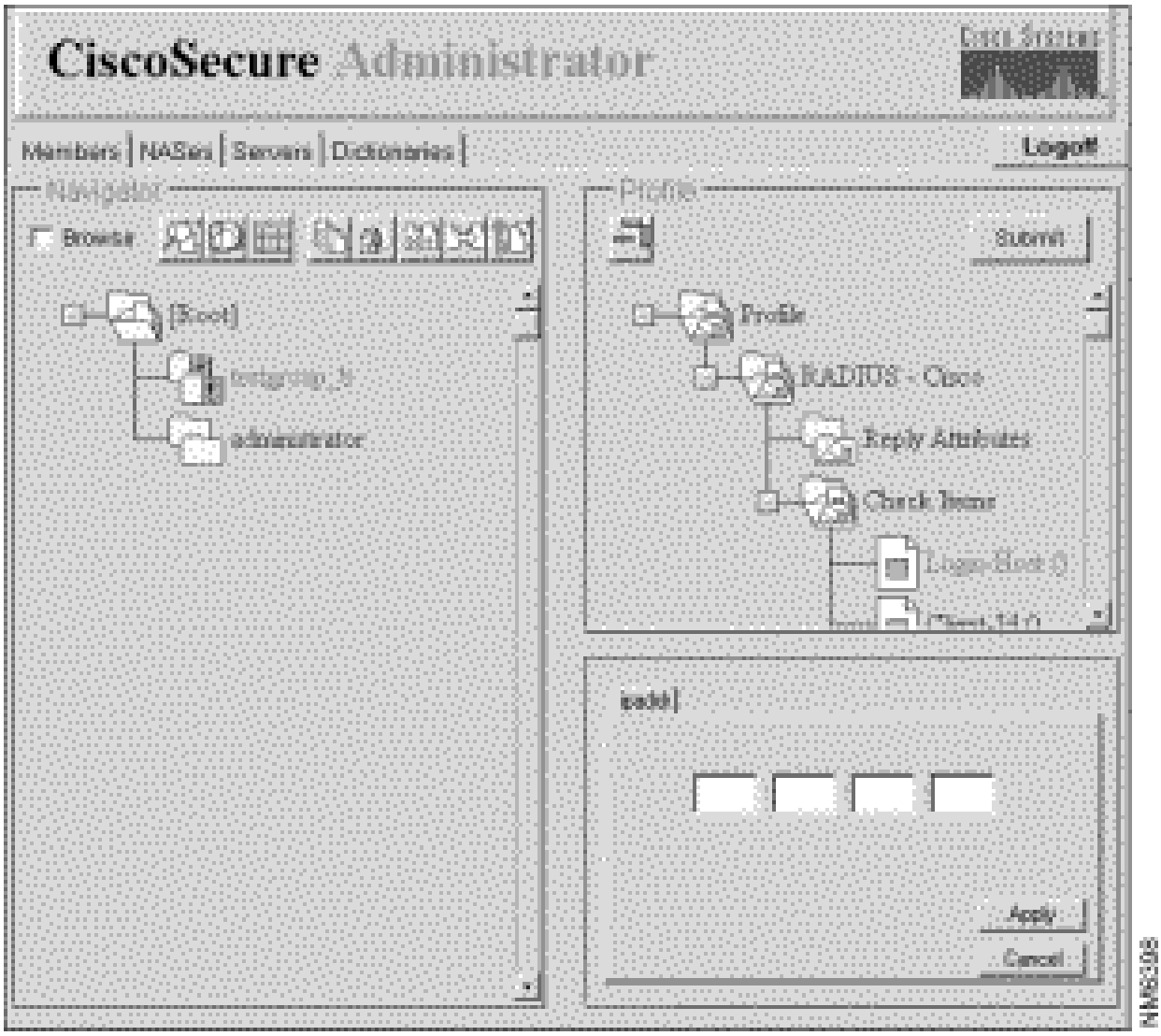
Waarschuwing: voor het RADIUS-protocol is overerving additief in plaats van hiërarchisch. (Het TACACS+ protocol maakt gebruik van hiërarchische overerving). Als u bijvoorbeeld dezelfde antwoordkenmerken toekent aan zowel de gebruikers- als de groepsprofielen, mislukt de autorisatie omdat de NAS twee keer het aantal attributen ontvangt. Het is niet logisch wat de antwoordattributen zijn. Wijs niet hetzelfde item voor controle toe of ken niet hetzelfde antwoord toe aan zowel de groep- als de gebruikersprofielen.

a. Klik op Items controleren of Kenmerken antwoorden of klik op beide. In het rechter benedenvenster verschijnt een lijst met de toepasselijke waarden voor controleitems en kenmerken van antwoord. Klik op het +-symbool om de map uit te vouwen.

b. Klik op de waarden die u wilt toewijzen en klik vervolgens op Toepassen. Raadpleeg voor meer informatie over de waarden RADIUS-kenmerken/waardeparen en woordenboekbeheer in CSU 2.3 voor de UNIX-referentiegids.

   Opmerking: Als u een attribuut waarde toewijst op het niveau van het groepsprofiel en het attribuut dat u opgeeft een absoluut selectievakje weergeeft, selecteert u dat selectievakje om de waarde absolute status toe te wijzen. Een absolute status van een waarde kan niet worden overschreven door tegenstrijdige waarden die zijn toegewezen op het niveau van het ondergeschikte groepsprofiel of het gebruikersprofiel.

c. Klik op Indienen als u klaar bent met het maken van wijzigingen.



4. Als u een of meer van deze kenmerken wilt gebruiken, klikt u op het attribuut of de attributen die u wilt gebruiken en vervolgens klikt u op Toepassen. U kunt meer dan één eigenschap tegelijkertijd toepassen.

Toegangscontroleniveaus toewijzen

De superuser beheerder gebruikt het web privilege attribuut om een niveau van toegangscontrole privilege toe te wijzen aan Cisco Secure-gebruikers.

1. Klik in het programma Geavanceerde configuratie van Cisco Secure Administrator op de gebruiker aan wie u de toegangsrechten wilt toewijzen en klik vervolgens op het pictogram Profielen in het deelvenster Profielen.

2. Klik in het menu Opties op Web Privilege en selecteer een van deze waarden.

    - 0 - Ontkent de gebruiker alle toegangscontrolerechten die de mogelijkheid bieden om het Cisco Secure-wachtwoord van de gebruiker te wijzigen.

    - 1 - Geeft de gebruiker toegang tot de CSU-webpagina. Hiermee kunnen Cisco Secure-gebruikers hun Cisco Secure-wachtwoorden wijzigen. Voor meer informatie over het

wijzigen van wachtwoorden, raadpleegt u Functies op gebruikersniveau (Wachtwoord wijzigen) in Eenvoudig gebruikers- en ACS-beheer.

- 12 - Verleent de gebruikersgroepbeheerdersrechten.
- 15 - Verleent de gebruikerssysteembeheerderrechten.

Opmerking: als u een andere web privilege optie dan 0 selecteert, moet u ook een wachtwoord opgeven. Om te voldoen aan de web privilege wachtwoordvereiste, is één lege ruimte minimaal acceptabel.

CSU starten en stoppen

Gewoonlijk start CSU automatisch wanneer u het SPARCstation start of opnieuw start waar het is geïnstalleerd. U kunt CSU echter handmatig starten of afsluiten zonder het gehele SPARCS-station te sluiten.

Log in als [Root] op het SPARCS-station waar u CSU hebt geïnstalleerd.

Als u CSU handmatig wilt starten, typt u:

```
# /etc/rc2.d/S80CiscoSecure
```

Als u CSU handmatig wilt stoppen, typt u:

```
# /etc/rc0.d/K80CiscoSecure
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Cisco Secure ACS voor UNIX-ondersteuningspagina
- Pagina met TACACS+ ondersteuning
- Pagina voor RADIUS-ondersteuning
- Requests for Comments (RFC's)

- 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.