Cisco Secure ACS: Limitações do acesso de rede com os clientes de AAA para usuários e grupos de usuário

Índice

Introdução

Este documento descreve como configurar as Restrições de Acesso de Rede (NAR) na versão 4.x do Cisco Secure Access Control Server (ACS) com clientes de AAA (inclui roteadores, PIX, ASA e controladores wireless) para Usuários e Grupos de usuários.

Pré-requisitos

Requisitos

Este documento é criado com a suposição que o Cisco Secure ACS e os clientes de AAA estão configurados e trabalham corretamente.

Componentes Utilizados

A informação neste documento é baseada no 3.0 do Cisco Secure ACS e mais tarde.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Restrições de acesso à rede

Esta seção descreve NAR, e fornece instruções detalhadas para configurar e controlar NAR compartilhados.

Esta seção contém estes assuntos:

- Sobre limitações do acesso de rede
- Adicionar um NAR compartilhado
- Edite um NAR compartilhado
- Suprima de um NAR compartilhado

Sobre limitações do acesso de rede

Um NAR é uma definição, que você faça no ACS, das circunstâncias adicionais que você deve estar conformes antes que um usuário possa alcançar a rede. O ACS aplica estas circunstâncias usando a informação dos atributos que seus clientes de AAA enviam. Embora você possa estabelecer NAR em diversas maneiras, todos são baseados na informação de atributos de harmonização que um cliente de AAA envia. Consequentemente, você deve compreender o formato e o índice dos atributos que seus clientes de AAA enviam se você quer empregar NAR eficazes.

Quando você estabelece um NAR, você pode escolher se o filtro se opera positivamente ou negativamente. Isto é, no NAR você especifica se ao acesso de rede do permit or deny, com base na informação enviada dos clientes de AAA quando comparado à informação armazenada no NAR. Contudo, se um NAR não encontra a informação suficiente para se operar, opta o acesso negado. Esta tabela mostra estas circunstâncias:

	Com base em IP	Não-IP baseado	Informação insuficiente
Licença	Acesso concedido	Acesso negado	Acesso negado
Negue	Acesso negado	Acesso concedido	Acesso negado

O ACS apoia dois tipos de filtros NAR:

- **Filtros com base em IP** — O NAR com base em IP filtra o acesso do limite baseado nos endereços IP de Um ou Mais Servidores Cisco ICM NT do cliente do utilizador final e do cliente de AAA. Veja a seção aproximadamente com base em IP dos filtros NAR para mais informação.
- **filtros NON-IP-baseados** — o NAR NON-IP-baseado filtra o acesso do limite baseado na comparação de série simples de um valor enviado do cliente de AAA. O valor pode ser o número do Calling Line Identification (CLI), o número do Dialed Number Identification Service

(DNIS), o MAC address, ou um outro valor que origine do cliente. Para este tipo de NAR a operar-se, o valor na descrição NAR deve exatamente combinar o que está sendo enviado do cliente, que inclui o que formato é usado. Por exemplo, o (217) 555-4534 do número de telefone não combina 217-555-4534. Veja a seção aproximadamente NON-IP-baseada dos filtros NAR para mais informação.

Você pode definir um NAR para, e aplica ao, a um usuário ou um grupo de usuário específico. Veja as limitações do acesso de rede do grupo para um usuário ou ajuste limitações do acesso de rede para seções de um grupo de usuário para mais informação. Contudo, na seção dos componentes de perfil compartilhado do ACS você pode criar e nomear um NAR compartilhado sem diretamente mencionar qualquer usuário ou grupo de usuário. Você dá ao NAR compartilhado um nome que possa ser provido em outras partes da interface da WEB ACS. Então, quando você estabelece usuários ou grupos de usuário, você pode não selecionar nenhuns, um, ou limitações compartilhadas múltiplo ser aplicado. Quando você especifica o aplicativo de NAR compartilhados múltiplo a um usuário ou a um grupo de usuário, você escolhe um de dois critérios do acesso:

- Todos os filtros selecionados devem permitir.
- Todo o um filtro selecionado deve permitir.

Você deve compreender o ordem de precedência que é relacionado aos tipos diferentes de NAR. Esta é a ordem de filtração NAR:

1. NAR compartilhado no nível de usuário
2. NAR compartilhado a nível do grupo
3. NAR NON-compartilhado no nível de usuário
4. NAR NON-compartilhado a nível do grupo

Você deve igualmente compreender que a **recusa do acesso a todo o nível toma a precedência sobre os ajustes a outro nível que não negam o acesso**. Esta é a uma exceção no ACS à regra que os ajustes do nível de usuário cancelam ajustes do grupo-nível. Por exemplo, um usuário particular pôde não ter nenhuma limitação NAR no nível de usuário que se aplica. Contudo, se esse usuário pertence a um grupo que esteja restringido por um NAR compartilhado ou NON-compartilhado, o usuário é negado o acesso.

Os NAR compartilhados são mantidos no base de dados interno ACS. Você pode usar as características alternativas ACS e da restauração para suportar, e restaura-as. Você pode igualmente replicate os NAR compartilhados, junto com outras configurações, aos ACS secundários.

Sobre filtros com base em IP NAR

Para filtros com base em IP NAR, o ACS usa os atributos como mostrado, que depende do protocolo de AAA do pedido de autenticação:

- **Se você está usando o TACACS+** — O campo do `rem_addr do` corpo do pacote do começo TACACS+ é usado.**Note**: Quando um pedido de autenticação é enviado pelo proxy a um ACS, todos os NAR para pedidos TACACS+ estão aplicados ao endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor AAA da transmissão, não ao endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente de AAA da origem.
- **Se você está usando o RAIO IETF** — `A chamar-estação-identificação` (atributo 31) deve ser usada.**Note**: Os filtros com base em IP NAR funcionam somente se o ACS recebe atributos Chamar-Estação-identificação do raio os 31) (. A Chamar-Estação-identificação (31) deve

conter um endereço IP válido. Se não faz, cairá sobre às regras DNIS.

Os clientes de AAA que não fornecem a suficiente informação do endereço IP de Um ou Mais Servidores Cisco ICM NT (por exemplo, alguns tipos de Firewall) não apoiam a funcionalidade completa NAR.

Outros atributos para limitações **com base em IP**, pelo protocolo, incluem os campos NAR como mostrado:

- **Se você está usando o TACACS+** — Os campos NAR no ACS usam estes valores:**Cliente de AAA** — O Nas-ip-address é tomado do endereço de origem no soquete entre o ACS e o cliente TACACS+.**Porta** — O campo de porta é tomado do corpo do pacote do começo TACACS+.

Sobre filtros NON-IP-baseados NAR

Um filtro NON-IP-baseado NAR (isto é, um filtro DNIS/CLI-based NAR) é uma lista de chamada ou de ponto permitido ou negado dos lugar do acesso que você pode usar para restringir um cliente de AAA quando você não tem uma conexão com base em IP estabelecida. A característica NON-IP-baseada NAR usa geralmente o número CLI e o número DNIS.

Contudo, quando você incorpora um endereço IP de Um ou Mais Servidores Cisco ICM NT no lugar do CLI, você pode usar o filtro NON-IP-baseado; mesmo quando o cliente de AAA não usa um software release de Cisco IOS® que apoie o CLI ou o DNIS. Em uma outra exceção a incorporar um CLI, você pode incorporar um MAC address ao acesso do permit or deny. Por exemplo, quando você usar um cliente de AAA do Cisco Aironet. Igualmente, você poderia incorporar o MAC address do Cisco Aironet AP no lugar do DNIS. O formato do que você especifica na caixa CLI — CLI, endereço IP de Um ou Mais Servidores Cisco ICM NT, ou MAC address — deve combinar o formato do que você recebe de seu cliente de AAA. Você pode determinar este formato de seu log de contabilidade do RAIO.

Os atributos para limitações DNIS/CLI-based, pelo protocolo, incluem os campos NAR como mostrado:

- **Se você está usando o TACACS+** — Os campos NAR alistados empregam estes valores:**Cliente de AAA** — `O Nas-ip-address` é tomado do endereço de origem no soquete entre o ACS e o cliente TACACS+.**Porta** — O campo de `porta no` corpo do pacote do começo TACACS+ é usado.**CLI** — O campo do REM-`ADDR no` corpo do pacote do começo TACACS+ é usado.**DNIS** — O campo do REM-`ADDR` tomado do corpo do pacote do começo TACACS+ é usado. Nos casos em que os dados do REM-ADDR começam com o corte (/), o campo DNIS contém os dados do REM-ADDR sem o corte (/).**Note**: Quando um pedido de autenticação é enviado pelo proxy a um ACS, todos os NAR para pedidos TACACS+ estão aplicados ao endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor AAA da transmissão, não ao endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente de AAA da origem.
- **Se você está usando o RAIO** — Os campos NAR alistados usam estes valores:**Cliente de AAA** — `O Nas-ip-address` (atributo 4) ou, se o Nas-ip-address não existe, o NAS-`identificador` (atributo RADIUS 32) são usados.**Porta** — `A NAS-porta` (atributo 5) ou, se a NAS-porta não existe, o `nas-port-id` (atributo 87) são usados.**CLI** — `O chamar-estação-ID` (atributo 31) é usado.**DNIS** — `O chamar-estação-ID` (atributo 30) é usado.

Quando você especifica um NAR, você pode usar um asterisco (*) como um convite para todo o valor, ou como parte de qualquer valor para estabelecer uma escala. Todos os valores ou

condições em uma descrição NAR devem ser estados conformes para que o NAR restrinja o acesso. Isto significa que os valores contêm um booleano E.

Adicionar um NAR compartilhado

Você pode criar um NAR compartilhado que contenha muitas restrições de acesso. Embora a interface da WEB ACS não reforce limites ao número de restrições de acesso em um NAR compartilhado ou ao comprimento de cada restrição de acesso, você deve aderir a estes limites:

- A combinação de campos para cada item de linha não pode exceder 1024 caráteres.
- O NAR compartilhado não pode ter mais de 16 KB dos caráteres. Os artigos do número de linha apoiados dependem do comprimento de cada item de linha. Por exemplo, se você cria um CLI/DNIS-based NAR onde os nomes do cliente de AAA sejam os caráteres 10, os números de porta são os caráteres 5, as entradas CLI são 15 caráteres, e as entradas DNIS são 20 caráteres, você podem adicionar 450 itens de linha antes que você alcance o limite 16 KB.

Note: Antes que você defina um NAR, assegure que você estabeleça os elementos que você pretende se usar nesse NAR. Consequentemente, você deve ter especificado todo o NAFs e NDGs, e ter definido todos os clientes de AAA relevantes, antes que você lhes faça parte da definição NAR. Veja aproximadamente a seção das limitações do acesso de rede para mais informação.

Termine estas etapas a fim adicionar um NAR compartilhado:

1. Na barra de navegação, clique **componentes de perfil compartilhado**.O indicador dos componentes de perfil compartilhado aparece.
2. **Limitações do acesso de rede do** clique.
3. Clique em Add.O indicador da limitação do acesso de rede aparece.
4. Na caixa de nome, dê entrada com um nome para o NAR compartilhado novo.**Note**: O nome pode conter até 31 caráteres. A condução e os espaços de trailing não são permitidos. Os nomes não podem conter estes caráteres: suporte esquerdo ([), right bracket (]), vírgula (,), ou corte (/).
5. Na caixa da descrição, incorpore uma descrição do NAR compartilhado novo. A descrição pode ser até 30,000 caráteres.
6. Se você quer ao permit or deny o acesso baseado no endereçamento de IP:Verifique a caixa de verificação **com base em IP das descrições do acesso da definição**.A fim especificar se você está alistando os endereços que são permitidos ou negados, da tabela define a lista, selecionam o valor aplicável.Selecione ou incorpore a informação aplicável a cada um destas caixas:**Cliente de AAA** — Selecione **todos os clientes de AAA**, ou o nome do NDG, ou do cliente de AAA NAF, ou individual, a que o acesso é permitido ou negado.**Porta** — Incorpore o número da porta a que você quer ao permit or deny o acesso. Você pode usar o asterisco (*) como um convite ao acesso do permit or deny a todas as portas no cliente de AAA selecionado.**Endereço IP de Um ou Mais Servidores Cisco ICM NT de Src** — Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT para filtrar em ao executar restrições de acesso. Você pode usar o asterisco (*) como um convite para especificar todos os endereços IP de Um ou Mais Servidores Cisco ICM NT.**Note**: O número total de caráteres na lista do cliente de AAA, e a porta e as caixas de endereço IP de Src, não devem exceder 1024. Embora o ACS aceite mais de 1024 caráteres quando você adiciona um NAR, você não pode editar o NAR e o ACS não pode exatamente aplicá-lo aos usuários.O clique

entra.O cliente de AAA, a porta, e a informação de endereço aparecem como um item de linha na tabela.Repita as etapas c e d a fim incorporar itens de linha com base em IP adicionais.

7. Se você quer ao permit or deny o acesso baseado em chamar o lugar ou os valores diferentes dos endereços IP de Um ou Mais Servidores Cisco ICM NT:Verifique a caixa de verificação **baseada CLI/DNIS das restrições de acesso da definição**.A fim especificar se você está alistando os lugar que são permitidos ou negado da tabela define a lista, selecione o valor aplicável.A fim especificar os clientes a que este NAR se aplica, selecione um destes valores da lista do cliente de AAA:O nome do NDGO nome do cliente de AAA particularTodos os clientes de AAA**Tip**: Somente NDGs que você tem configurado já está listado.A fim especificar a informação em que este NAR deve filtrar, incorpore valores a estas caixas, como aplicável:**Tip**: Você pode incorporar um asterisco (*) como um convite para especificar **tudo** como um valor.**Porta** — Incorpore o número da porta em que para filtrar.**CLI** — Incorpore o número CLI em que para filtrar. Você pode igualmente usar esta caixa para restringir o acesso baseado em valores diferentes dos CLI, tais como um endereço IP de Um ou Mais Servidores Cisco ICM NT ou um MAC address. Veja aproximadamente a seção das limitações do acesso de rede para mais informação.**DNIS** — Incorpore o número que está sendo discado dentro a qual para filtrar.**Note**: O número total de caráteres na lista do cliente de AAA e nas caixas da porta, CLI, e DNIS não deve exceder 1024. Embora o ACS aceite mais de 1024 caráteres quando você adiciona um NAR, você não pode editar o NAR e o ACS não pode exatamente aplicá-lo aos usuários.O clique **entra**.A informação que especifica o item de linha NAR aparece na tabela.Repita as etapas c a e a fim incorporar itens de linha NON-IP-baseados adicionais NAR.O clique **submete-se** a fim salvar a definição compartilhada NAR.O ACS salvar o NAR compartilhado e alista-o na tabela das **limitações do acesso de rede**.

Edite um NAR compartilhado

Termine estas etapas a fim editar um NAR compartilhado:

1. Na barra de navegação, clique **componentes de perfil compartilhado**.O indicador dos componentes de perfil compartilhado aparece.
2. **Limitações do acesso de rede do** clique.A tabela das limitações do acesso de rede aparece.
3. Na coluna do nome, clique o NAR compartilhado que você quer editar.O indicador da limitação do acesso de rede aparece e indica a informação para o NAR selecionado.
4. Edite o nome ou a descrição do NAR, como aplicável. A descrição pode ser até 30,000 caráteres.
5. A fim editar um item de linha na tabela com base em IP das restrições de acesso:Fazer duplo clique o item de linha que você quer editar.A informação para o item de linha é removida da tabela e redigida às caixas sob a tabela.Edite a informação, como necessário.**Note**: O número total de caráteres na lista do cliente de AAA e na porta e nas caixas de endereço IP de Src não deve exceder 1024. Embora o ACS possa aceitar mais de 1024 caráteres quando você adiciona um NAR, você não pode editar tais NAR e ACS não pode exatamente aplicá-lo aos usuários.O clique **entra**.A informação editada para este item de linha é redigida à tabela com base em IP das restrições de acesso.
6. A fim remover um item de linha da tabela com base em IP das restrições de acesso:Selecione o item de linha.Sob a tabela, o clique **remove**.O item de linha é removido da tabela com base em IP das restrições de acesso.

7. A fim editar um item de linha na tabela das restrições de acesso CLI/DNIS:Fazer duplo clique o item de linha que você quer editar.A informação para o item de linha é removida da tabela e redigida às caixas sob a tabela.Edite a informação, como necessário.**Note**: O número total de caráteres na lista do cliente de AAA e nas caixas da porta, CLI, e DNIS não deve exceder 1024. Embora o ACS possa aceitar mais de 1024 caráteres quando você adiciona um NAR, você não pode editar tais NAR e ACS não pode exatamente aplicá-lo aos usuários.O clique **entra**A informação editada para este item de linha é redigida à tabela das restrições de acesso CLI/DNIS.
8. A fim remover um item de linha da tabela das restrições de acesso CLI/DNIS:Selecione o item de linha.Sob a tabela, o clique **remove**.O item de linha é removido da tabela das restrições de acesso CLI/DNIS.
9. O clique **submete-se** a fim salvar as mudanças que você fez.O ACS reenters o filtro com a informação nova, que toma o efeito imediatamente.

Suprima de um NAR compartilhado

Note: Assegure-se de que você remova a associação de um NAR compartilhado a todo o usuário ou agrupe-se antes que você suprima desse NAR.

Termine estas etapas a fim suprimir de um NAR compartilhado:

1. Na barra de navegação, clique **componentes de perfil compartilhado**.O indicador dos componentes de perfil compartilhado aparece.
2. **Limitações do acesso de rede do** clique.
3. Clique o nome do NAR compartilhado de que você quer suprimir.O indicador da limitação do acesso de rede aparece e indica a informação para o NAR selecionado.
4. Na parte inferior do indicador, **supressão do** clique.Uma caixa de diálogo adverte-o que você está a ponto de suprimir de um NAR compartilhado.
5. Clique a **APROVAÇÃO** a fim confirmar que você quer suprimir do NAR compartilhado.O NAR compartilhado selecionado é suprimido.

Ajuste limitações do acesso de rede para um usuário

Você usa a tabela das limitações do acesso de rede na área avançada dos ajustes da instalação de usuário para ajustar NAR em três maneiras:

- Aplique NAR compartilhados existentes por nome.
- Defina restrições de acesso com base em IP ao acesso de usuário do permit or deny a um cliente de AAA especificado ou às portas especificadas em um cliente de AAA quando uma conexão IP foi estabelecida.
- Defina restrições de acesso CLI/DNIS-based ao acesso de usuário do permit or deny baseado no CLI/DNIS que é usado.**Note**: Você pode igualmente usar a área das restrições de acesso CLI/DNIS-based para especificar outros valores. Veja a seção das limitações do acesso de rede para mais informação.

Tipicamente, você define NAR (compartilhados) de dentro da seção compartilhada dos componentes de modo que você possa aplicar estas limitações a mais de um grupo ou usuário. Veja adicionar uma seção compartilhada NAR para mais informação. Você deve ter selecionado a caixa de verificação das **limitações do acesso de rede do nível de usuário na** página avançada

das opções da seção de configuração da interface para que este conjunto de opções apareça na interface da WEB.

Contudo, você pode igualmente usar o ACS para definir e aplicar um NAR para um usuário único de dentro da seção de instalação de usuário. Você deve ter permitido as **limitações do acesso de rede do nível de usuário que** ajustam-se na página avançada das opções da seção de configuração da interface para que opções de filtro com base em IP do usuário único e as opções de filtro do usuário único CLI/DNIS-based apareçam na interface da WEB.

Note: Quando um pedido de autenticação é enviado pelo proxy a um ACS, todos os NAR para pedidos do Terminal Access Controller Access Control System (TACACS+) estão aplicados ao endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor AAA da transmissão, não ao endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente de AAA da origem.

Quando você cria restrições de acesso em uma base do usuário per., o ACS não reforça limites ao número de restrições de acesso e não reforça um limite ao comprimento de cada restrição de acesso. Contudo, há uns limites restritos:

- A combinação de campos para cada item de linha não pode exceder 1024 caráteres de comprimento.
- O NAR compartilhado não pode ter mais de 16 KB dos caráteres. Os artigos do número de linha apoiados dependem do comprimento de cada item de linha. Por exemplo, se você cria um CLI/DNIS-based NAR onde os nomes do cliente de AAA sejam os caráteres 10, os números de porta são os caráteres 5, as entradas CLI são 15 caráteres, e as entradas DNIS são 20 caráteres, você podem adicionar 450 itens de linha antes que você alcance o limite 16 KB.

Termine estas etapas a fim ajustar NAR para um usuário:

1. Execute etapas 1 a 3 de adicionar uma conta de usuário básica.A instalação de usuário edita o indicador abre. O username que você adiciona ou edita aparece na parte superior do indicador.
2. A fim aplicar um NAR compartilhado previamente configurado a este usuário:**Note**: A fim aplicar um NAR compartilhado, você deve tê-lo configurado sob limitações do acesso de rede na seção dos componentes de perfil compartilhado. Veja adicionar uma seção compartilhada NAR para mais informação.Verifique o **único permitem o acesso de rede quando** caixa de verificação.A fim especificar se um ou todo o NAR compartilhado deve se aplicar para que o usuário seja acesso permitido, selecione um, como aplicável:Todos os NAR selecionados conduzem à licença.Alguns resultados selecionados um NAR na licença.Selecione um nome compartilhado NAR na lista NAR, e clique-o então --> (botão da seta direita) para mover o nome nos NAR selecionados aliste.**Tip**: A fim ver os detalhes do server dos NAR que compartilhados você selecionou para se aplicar, você pode clicar **IP NAR** ou **vista CLID/DNIS NAR da vista**, como aplicável.
3. A fim definir e aplicar um NAR, para este usuário particular, que permite ou nega este acesso de usuário baseado no endereço IP de Um ou Mais Servidores Cisco ICM NT, ou endereço IP de Um ou Mais Servidores Cisco ICM NT e porta:**Note**: Você deve definir a maioria de NAR de dentro da seção compartilhada dos componentes de modo que você possa os aplicar a mais de um grupo ou usuário. Veja adicionar uma seção compartilhada NAR para mais informação.Na tabela das limitações do acesso de rede, abaixo por limitações definidas pelo utilizador do acesso de rede, verifique a caixa de verificação **com**

base em IP das restrições de acesso da definição.A fim especificar se a lista subsequente especifica endereços IP de Um ou Mais Servidores Cisco ICM NT permitidos ou negados, da tabela define a lista, escolhem um:**Permitted Calling/Point of Access LocationsDenied Calling/Point of Access Locations**Selecione ou incorpore a informação a estas caixas:**Cliente de AAA** — Selecione **todos os clientes de AAA**, ou o nome de um grupo de dispositivo de rede (NDG), ou o nome do cliente de AAA individual, a que ao acesso do permit or deny.**Porta** — Incorpore o número da porta a que ao acesso do permit or deny. Você pode usar o asterisco (*) como um convite ao acesso do permit or deny a todas as portas no cliente de AAA selecionado.**Endereço** — Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT ou os endereços para usar-se ao executar restrições de acesso. Você pode usar o asterisco (*) como um convite.**Note**: O número total de caráteres na lista do cliente de AAA, e a porta e as caixas de endereço IP de Src não devem exceder 1024. Embora o ACS aceite mais de 1024 caráteres quando você adiciona um NAR, você não pode editar o NAR e o ACS não pode exatamente aplicá-lo aos usuários.O clique **entra**.O cliente de AAA, a porta, e a informação de endereço especificados aparecem na tabela acima da lista do cliente de AAA.

4. Permit or deny este acesso de usuário baseado em chamar o lugar ou os valores diferentes de um endereço IP de Um ou Mais Servidores Cisco ICM NT estabelecido:Verifique a caixa de verificação **baseada CLI/DNIS das restrições de acesso da definição**.A fim especificar se a lista subsequente especifica valores permitidos ou negados, da tabela define a lista, escolhem um:**Permitted Calling/Point of Access LocationsDenied Calling/Point of Access Locations**Termine as caixas como mostrado:**Note**: Você deve fazer uma entrada em cada caixa. Você pode usar o asterisco (*) como um convite para o todo ou uma parte de um valor. O formato que você usa deve combinar o formato da corda que você recebe de seu cliente de AAA. Você pode determinar este formato de seu log de contabilidade do RAIO.**Cliente de AAA** — Selecione **todos os clientes de AAA**, ou o nome do NDG, ou o nome do cliente de AAA individual, a que ao acesso do permit or deny.**PORTA** — Incorpore o número da porta a que ao acesso do permit or deny. Você pode usar o asterisco (*) como um convite ao acesso do permit or deny a todas as portas.**CLI** — Incorpore o número CLI a que ao acesso do permit or deny. Você pode usar o asterisco (*) como um convite ao acesso do permit or deny baseado parte de no número.**Tip**: Use a entrada CLI se você quer restringir o acesso baseado em outros valores tais como um endereço MAC de cliente do Cisco Aironet. Veja aproximadamente a seção das limitações do acesso de rede para mais informação.**DNIS** — Entre no número DNIS a que ao acesso do permit or deny. Use esta entrada para restringir o acesso baseado no número em que o usuário discará. Você pode usar o asterisco (*) como um convite ao acesso do permit or deny baseado parte de no número.**Tip**: Use a seleção DNIS se você quer restringir o acesso baseado em outros valores tais como um MAC address do Cisco Aironet AP. Veja aproximadamente a seção das limitações do acesso de rede para mais informação.**Note**: O número total de caráteres na lista do cliente de AAA e nas caixas da **porta**, **CLI** e **DNIS** não deve exceder 1024. Embora o ACS aceite mais de 1024 caráteres quando você adiciona um NAR, você não pode editar o NAR e o ACS não pode exatamente aplicá-lo aos usuários.O clique **entra**.A informação que especifica o cliente de AAA, a porta, o CLI, e o DNIS aparecem na tabela acima da lista do cliente de AAA.
5. Se você é terminado que configura as opções da conta de usuário, o clique **submete-se** a fim gravar as opções.

Ajuste limitações do acesso de rede para um grupo de usuário

Você usa a tabela das limitações do acesso de rede na instalação de grupo para aplicar NAR em três maneiras distintas:

- Aplique NAR compartilhados existentes por nome.
- Defina restrições de acesso com base em IP do grupo ao acesso do permit or deny a um cliente de AAA especificado ou às portas especificadas em um cliente de AAA quando uma conexão IP foi estabelecida.
- Defina o grupo NAR CLI/DNIS-based ao acesso do permit or deny a, ou ambos, o número CLI ou o número DNIS usado.**Note**: Você pode igualmente usar a área das restrições de acesso CLI/DNIS-based para especificar outros valores. Veja aproximadamente a seção das limitações do acesso de rede para mais informação.

Tipicamente, você define NAR (compartilhados) de dentro da seção compartilhada dos componentes de modo que estas limitações possam se aplicar a mais de um grupo ou usuário. Veja adicionar uma seção compartilhada NAR para mais informação. Você deve verificar a caixa de verificação da **restrição de acesso da rede compartilhada do Grupo-nível na** página **avançada das opções da** seção de configuração da interface para ver se há estas opções para aparecer na interface da WEB ACS.

Contudo, você pode igualmente usar o ACS para definir e aplicar um NAR para um único grupo de dentro da **seção de instalação do grupo**. Você deve verificar o ajuste da **limitação do acesso de rede do Grupo-nível** sob a página avançada das opções da seção de configuração da interface para ver se há opções de filtro com base em IP do único grupo e únicas opções de filtro de grupo CLI/DNIS-based aparecer na interface da WEB ACS.

Note: Quando um pedido de autenticação é enviado pelo proxy a um servidor ACS, todos os NAR para requisições RADIUS estão aplicados ao endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor AAA da transmissão, não ao endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente de AAA da origem.

Termine estas etapas a fim ajustar NAR para um grupo de usuário:

1. Na barra de navegação, clique a **instalação de grupo**.O indicador seleto da instalação de grupo abre.
2. Da lista do grupo, selecione um grupo, e clique-o então **editam ajustes**.O nome do grupo aparece na parte superior do indicador das configurações de grupo.
3. A fim aplicar um NAR compartilhado previamente configurado a este grupo:**Note**: A fim aplicar um NAR compartilhado, você deve tê-lo configurado sob limitações do acesso de rede na seção dos componentes de perfil compartilhado. Veja adicionar uma seção compartilhada NAR para mais informação.Verifique o **único permitem o acesso de rede quando** caixa de verificação.A fim especificar se um ou todo o NAR compartilhado deve se aplicar para um membro do grupo para ser acesso permitido, verifique uma destas opções:Todos selecionados compartilharam do resultado NAR na licença.Todo o um NAR compartilhado selecionado conduz à licença.Selecione um nome compartilhado NAR na lista compartilhada NAR, e clique-o então --> (botão da seta direita) para mover o nome nos NAR compartilhados selecionados aliste.**Tip**: A fim ver os detalhes do server dos NAR compartilhados que você aplicou, você pode clicar **IP NAR** ou **vista CLID/DNIS NAR da vista**, como aplicável.

4. A fim definir e aplicar um NAR para este grupo de usuário particular, esse permitem ou negam o acesso a este grupo baseado no endereço IP de Um ou Mais Servidores Cisco ICM NT, ou o endereço IP de Um ou Mais Servidores Cisco ICM NT e a porta:**Note**: Você deve definir a maioria de NAR de dentro da seção compartilhada dos componentes de modo que as limitações possam se aplicar a mais de um grupo ou usuário. Veja adicionar uma seção compartilhada NAR para mais informação.No pela rede definida do grupo as restrições de acesso que a seção das limitações do acesso de rede apresenta, verifica a caixa de verificação **com base em IP das restrições de acesso da definição**.A fim especificar se a lista subsequente especifica endereços IP de Um ou Mais Servidores Cisco ICM NT permitidos ou negados, da tabela define a lista, escolhem o **Permitted Calling/Point of Access Locations** ou o **Denied Calling/Point of Access Locations**.Selecione ou incorpore a informação a estas caixas:**Cliente de AAA** — Selecione todos os clientes de AAA ou o nome do NDG ou o nome do cliente de AAA individual a que você quer ao permit or deny o acesso.**Porta** — Incorpore o número da porta a que ao acesso do permit or deny. Você pode usar o asterisco (*) como um convite ao acesso do permit or deny a todas as portas no cliente de AAA selecionado.**Endereço** — Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT ou os endereços para filtrar em ao executar restrições de acesso. Você pode usar o asterisco (*) como um convite.**Note**: O número total de caráteres na lista do cliente de AAA e na porta e nas caixas de endereço IP de Src não deve exceder 1024. Embora o ACS aceite mais de 1024 caráteres quando você adiciona um NAR, você não pode editar o NAR e o ACS não pode exatamente aplicá-lo aos usuários.O clique **entra**.Especificado o cliente de AAA, a porta, e a informação de endereço aparece no **Access Control List NAR**.
5. O permit or deny alcança a este grupo de usuário baseado em chamar o lugar ou os valores diferentes de um endereço IP de Um ou Mais Servidores Cisco ICM NT estabelecido:Verifique a caixa de verificação das **restrições de acesso da definição CLI/DNIS-based**.A fim especificar se a lista subsequente especifica valores permitidos ou negados, da tabela define a lista, escolhem um:**Permitted Calling/Point of Access LocationsDenied Calling/Point of Access Locations**Da lista do cliente de AAA, escolha **todos os clientes de AAA**, ou o nome do NDG ou o nome do cliente de AAA particular a que ao acesso do permit or deny.Termine estas caixas:**Note**: Você deve incorporar uma entrada a cada caixa. Você pode usar o asterisco (*) como um convite para o todo ou uma parte de um valor. O formato que você usa deve combinar o formato da corda que você recebe de seu cliente de AAA. Você pode determinar este formato de seu log de contabilidade do RAIO.**PORTA** — Incorpore o número da porta a que ao acesso do permit or deny. Você pode usar o asterisco (*) como um convite ao acesso do permit or deny a todas as portas.**CLI** — Incorpore o número CLI a que ao acesso do permit or deny. Você pode usar o asterisco (*) como um convite ao acesso do permit or deny baseado parte de em número ou em todos os números.**Tip**: O CLI é igualmente a seleção a usar-se se você quer restringir o acesso baseado em outros valores, tais como um endereço MAC de cliente do Cisco Aironet. Veja aproximadamente a seção das limitações do acesso de rede para mais informação.**DNIS** — Entre no número DNIS para restringir o acesso baseado no número em que o usuário estará discando. Você pode usar o asterisco (*) como um convite ao acesso do permit or deny baseado parte de em número ou em todos os números.**Tip**: O DNIS é igualmente a seleção se você quer restringir o acesso baseado em outros valores, tais como um MAC address do Cisco Aironet AP. Veja aproximadamente a seção das limitações do acesso de rede para mais informação.**Note**: O número total de caráteres na lista do cliente de AAA, e as caixas da porta, CLI, e DNIS não devem exceder 1024. Embora o ACS aceite mais de 1024 caráteres quando você adiciona um NAR, você não pode editar o NAR e o

ACS não pode exatamente aplicá-lo aos usuários.O clique **entra**.A informação que especifica o cliente de AAA, a porta, o CLI, e o DNIS aparecem na lista.

6. O clique **submete-se** a fim salvar as configurações de grupo que você apenas fez.Refira mudanças de salvamento aos ajustes do grupo de usuário para mais informação.

Informações Relacionadas

- Página de suporte do Serviço de controle de acesso Cisco Secure
- Suporte Técnico e Documentação - Cisco Systems