Configuração da rede de Cisco Unified Wireless TACACS+

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Aplicação TACACS+ no controlador
Autenticação
Autorização
Relatório
Configuração TACACS+ no WLC
Adicionar um server da autenticação TACACS+
Adicionar um server da autorização TACACS+
Adicionar um servidor de contabilidade TACACS+
Configurar a ordem de autenticação
Verifique a configuração
Configurar o server do Cisco Secure ACS
Configuração de rede
Configuração da interface
Usuário/instalação de grupo
Registros de contabilidade no Cisco Secure ACS
Configuração TACACS+ no WCS
WCS usando Domínios Virtuais
Configurar o Cisco Secure ACS para usar o WCS
Configuração de rede
Configuração da interface
Usuário/instalação de grupo
Debugs
Debuga do WLC para role1=ALL
Debuga do WLC para papéis múltiplos
Debuga de um WLC para a falha na autorização
Informações Relacionadas

Introdução

Este documento fornece um exemplo de configuração do Terminal Access Controller Access Control System Plus (TACACS+) em um Controller de LAN Wireless (WLC) e de um Cisco

Wireless Control System (WLC) para uma Cisco Unified Wireless Network. Este documento também fornece dicas básicas de troubleshooting.

O TACACS+ é um protocolo cliente/servidor que forneça a Segurança centralizada para os usuários que tentam ganhar o acesso de gerenciamento a um roteador ou a um servidor do acesso de rede. O TACACS+ proporciona estes serviços AAA:

- Autenticação dos usuários que tentam entrar ao equipamento de rede
- Autorização determinar que nível de usuários do acesso deve ter
- Explicar para manter-se a par de todas as mudanças o usuário faz

Refira configurar o TACACS+ para obter mais informações sobre dos serviços AAA e da funcionalidade TACACS+.

Refira a comparação de TACACS+ e radius para uma comparação do TACACS+ e do RAIO.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento de como configurar WLC e Lightweight Access Points (regaços) para a operação básica
- Conhecimento de métodos de pouco peso do protocolo (LWAPP) e da segurança Wireless do Access point
- RAIO do conhecimento básico e TACACS+
- Conhecimento básico da configuração ACS de Cisco

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 4.0 do Cisco Secure ACS for Windows
- Controlador de LAN do Cisco Wireless que executa a versão 4.1.171.0. A funcionalidade TACACS+ em WLC é apoiada versão de software em 4.1.171.0 ou em mais tarde.
- Sistema de controle sem fio da Cisco que executa a versão 4.1.83.0. A funcionalidade TACACS+ no WCS é apoiada versão de software em 4.1.83.0 ou em 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.

Aplicação TACACS+ no controlador

Autenticação

A autenticação pode ser executada usando um base de dados local, um server do RAIO, ou TACACS+ que use um username e uma senha. A aplicação não é inteiramente modular. Os serviços de authentication e autorização são amarrados entre si. Por exemplo, se a autenticação é executada usando o base de dados RADIUS/local, a seguir a autorização não é executada com o TACACS+. Usaria as permissões associadas para o usuário no local ou base de dados RADIUS, tal como de leitura apenas ou de leitura/gravação, visto que quando a autenticação for executada com o TACACS+, a autorização é amarrada ao TACACS+.

Nos casos onde os bases de dados múltiplos são configurados, um CLI é fornecido para ditar a sequência em que o base de dados backend deve ser consultado.

Autorização

A autorização é tarefa baseada um pouco do que por-comando real uma autorização baseada. As tarefas são traçadas às várias abas que correspondem aos sete artigos da barra de menus que estão atualmente na Web GUI. Estes são os artigos da barra de menus:

- MONITOR
- WLAN
- CONTROLADOR
- TECNOLOGIA WIRELESS
- SEGURANÇA
- GERENCIAMENTO
- COMANDO

A razão para este mapeamento é baseada no fato de que a maioria de clientes usam a interface da WEB para configurar o controlador em vez do CLI.

Um papel adicional para o Gerenciamento admin da entrada (ENTRADA) está disponível para os usuários que precisam de ter privilégios admin da entrada somente.

A tarefa que um usuário está autorizado é configurada no server TACACS+ (ACS) usando os pares feitos sob encomenda do valor de atributo (AV). O usuário pode ser autorizado para um ou tarefas múltiplas. A autorização mínima é MONITOR somente e o máximo é TUDO (autorizado para executar todas as sete abas). Se um usuário não é autorizado para uma tarefa particular, está permitido ainda ao usuário alcançar essa tarefa no modo somente leitura. Se a autenticação é permitida e o Authentication Server se torna inacessível ou incapaz de autorizar, o usuário não pode entrar ao controlador.

Nota: Para que a autenticação do gerenciamento básico através do TACACS+ a suceder, você deve configurar server da authentication e autorização no WLC. A configuração explicando é opcional.

Relatório

A contabilidade ocorre sempre que uma ação USER-iniciada detalhe é executada com sucesso. Os atributos mudados são entrados o servidor de contabilidade TACACS+ junto com estes:

- O usuário - identificação do indivíduo que fez a mudança

- O host remoto de onde o usuário é entrado
- A data e hora em que o comando foi executado
- Autorização em nível do usuário
- Uma corda que forneça a informação a respeito de que ação foi executada e os valores fornecidos

Se o servidor de contabilidade se torna inacessível, o usuário pode ainda continuar a sessão.

Nota: Os registros de contabilidade não são gerados do WCS no Software Release 4.1 ou Anterior.

Configuração TACACS+ no WLC

A liberação de software WLC 4.1.171.0 e introduz mais tarde CLI novos e Web GUI muda a fim permitir a funcionalidade TACACS+ no WLC. Os CLI introduzidos são alistados nesta seção para a referência. As mudanças correspondentes para a Web GUI são adicionadas sob a ABA de segurança.

Este documento supõe que a configuração básica do WLC está terminada já.

A fim configurar o TACACS+ no controlador WLC, você precisa de terminar estas etapas:

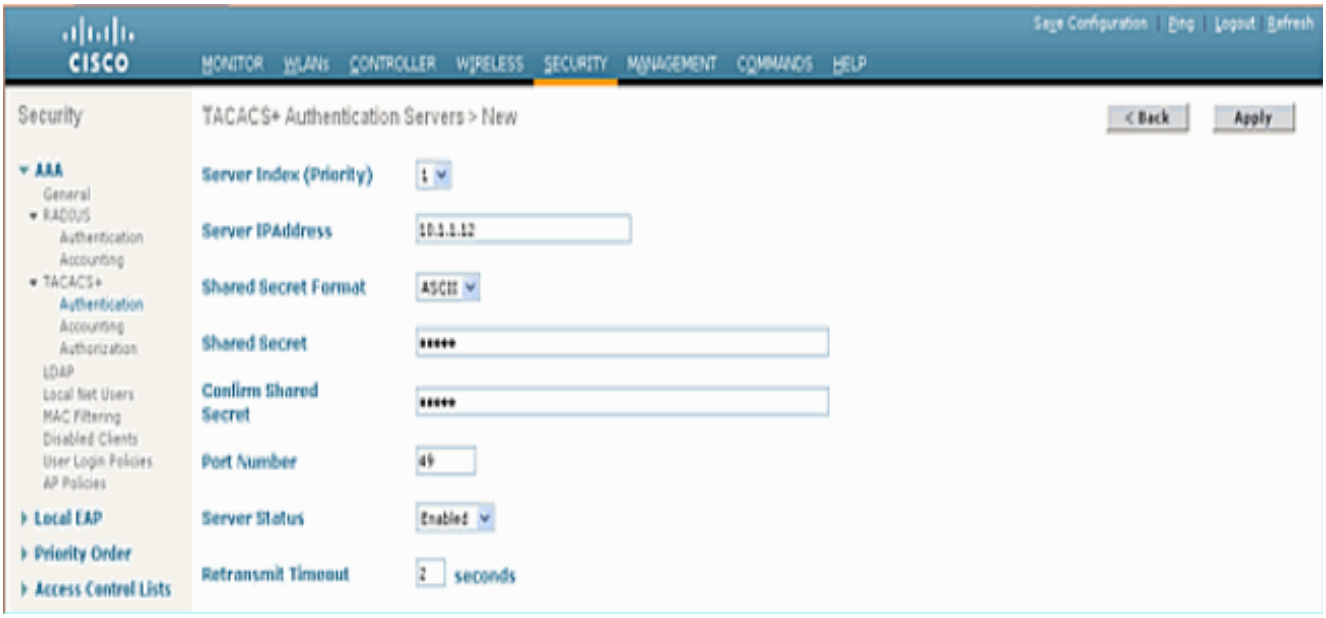
1. Adicionar um server da autenticação TACACS+
2. Adicionar um server da autorização TACACS+
3. Adicionar um servidor de contabilidade TACACS+
4. Configurar a ordem de autenticação

Adicionar um server da autenticação TACACS+

Termine estas etapas a fim adicionar um server da autenticação TACACS+:

1. Use o GUI, e vá à **Segurança > ao TACACS+ > à autenticação**.

2. Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT do server TACACS+ e incorpore a chave secreta compartilhada. Se for necessário, mude a porta padrão do TCP/49.

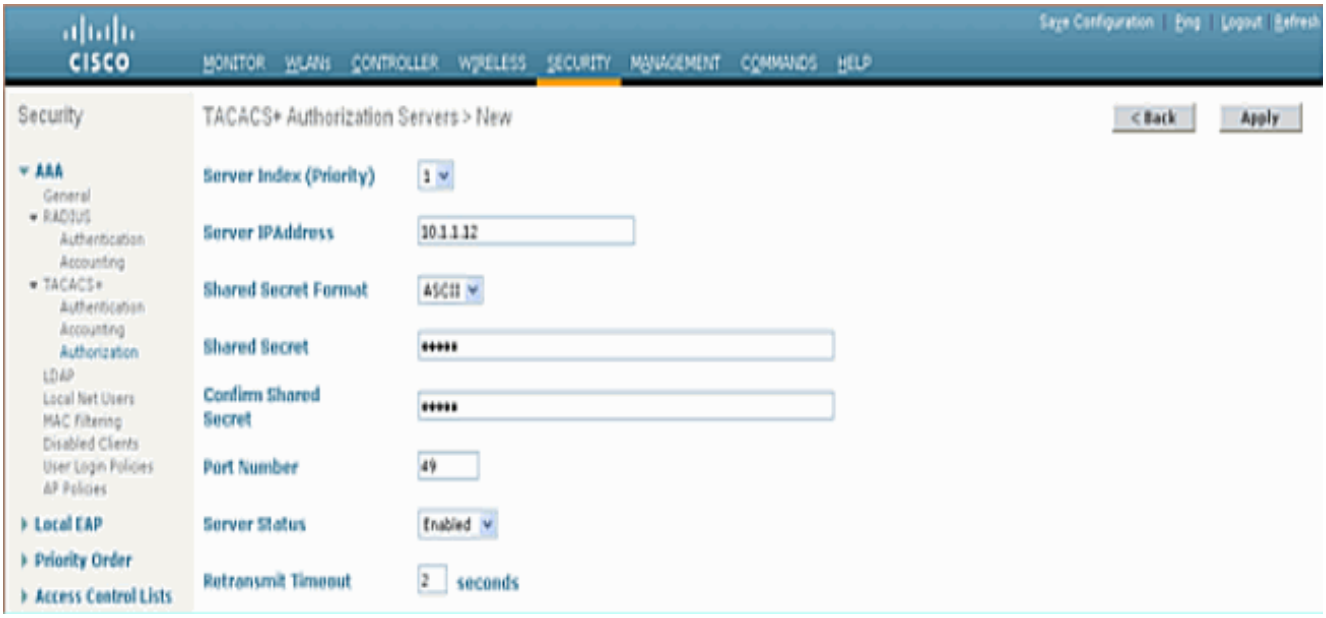


3. Clique em Apply.Você pode realizar este do CLI usando os **tacacs que da configuração o AUTH adiciona o** comando do **<secret> do** *[ascii/hex] do <port> do addr> de Index> <IP do <Server*:`(Cisco Controller) >config tacacs auth add 1 10.1.1.12 49 ascii cisco123`

Adicionar um server da autorização TACACS+

Termine estas etapas a fim adicionar um server da autorização TACACS+:

1. Do GUI, vá à **Segurança > ao TACACS+ > à autorização**.
2. Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT do server TACACS+ e incorpore a chave secreta compartilhada. Se for necessário, mude a porta padrão do TCP/49.



3. Clique em Apply.Você pode realizar este do CLI usando os **tacacs que da configuração o athr adiciona o** comando do **<secret> do** *[ascii/hex] do <port> do addr> de Index> <IP do <Server*:`(Cisco Controller) >config tacacs athr add 1 10.1.1.12 49 ascii cisco123`

Adicionar um servidor de contabilidade TACACS+

Termine estas etapas a fim adicionar um servidor de contabilidade TACACS+:

1. Use o GUI, e vá à **Segurança > ao TACACS+ > à contabilidade**.
2. Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT do server e incorpore a chave secreta compartilhada. Se for necessário, mude a porta padrão do TCP/49.

3. Clique em Apply.Você pode realizar este do CLI usando os **tacacs que da configuração o acct adiciona o** comando do **<secret> do** *[ascii/hex] do <port> do addr> de Index> <IP do <Server*:`(Cisco Controller) >config tacacs acct add 1 10.1.1.12 49 ascii cisco123`

Configurar a ordem de autenticação

Esta etapa explica como configurar a ordem AAA de autenticação quando há uns bases de dados múltiplos configurados. A ordem de autenticação pode ser **local e RAIO**, ou **local e TACACS**. A configuração de controle do padrão para a ordem de autenticação é *local e RAIO*.

Termine estas etapas a fim configurar a ordem de autenticação:

1. Do GUI, vá ao **usuário da Segurança > da ordem > do Gerenciamento da prioridade**.
2. Selecione a prioridade da autenticação.Neste exemplo, o TACACS+ foi selecionado.
3. O clique **aplica-se** para que a seleção ocorra.

Você pode realizar este do CLI usando o comando do **mgmt** *<server1> <server2> do* **AUTH aaa da configuração**:`(Cisco Controller) >config aaa auth mgmt tacacs local`

Verifique a configuração

Esta seção descreve os comandos usados para verificar a configuração TACACS+ no WLC. Estes são alguns comandos de exibição úteis que ajudam a determinar se a configuração está correta:

- **mostre o AUTH aaa** — Fornece informação na ordem da autenticação.
```
(Cisco Controller) >show aaa auth Management authentication server order:
1..... local
2..... Tacacs
```
- **mostre o sumário dos tacacs** — Indica um sumário de serviços e de estatísticas TACACS+.
```
(Cisco Controller) >show tacacs summary Authentication Servers Idx Server Address Port State Tout --- --------------- ------ -------- ---- 1 10.1.1.12 49 Enabled 2 Authorization Servers Idx Server Address Port State Tout --- --------------- ------ ------- ---- 1 10.1.1.12 49 Enabled 2 Accounting Servers Idx Server Address Port State Tout --- --------------- ------ ------- ---- 1 10.1.1.12 49 Enabled 2
```
- **mostre o stats do AUTH dos tacacs** — Estatísticas do servidor da autenticação TACACS+ dos indicadores.
```
(Cisco Controller) >show tacacs auth statistics Authentication Servers:
Server Index..... 1 Server
Address..... 10.1.1.12 Msg Round Trip
Time..... 0 (1/100 second) First
Requests..... 7 Retry
Requests..... 3 Accept
Responses..... 3 Reject
Responses..... 0 Error
Responses..... 0 Restart
Responses..... 0 Follow
Responses..... 0 GetData
Responses..... 0 Encrypt no secret
Responses..... 0 Challenge Responses..... 0
Malformed Msgs..... 0 Bad Authenticator
Msgs..... 0 Timeout Requests..... 12
Unknowntype Msgs..... 0 Other
Drops..... 0
```
- **mostre o stats do athr dos tacacs** — Estatísticas do servidor da autorização TACACS+ dos indicadores.
```
(Cisco Controller) >show tacacs athr statistics Authorization Servers: Server
Index..... 1 Server
Address..... 10.1.1.12 Msg Round Trip
Time..... 0 (1/100 second) First
Requests..... 3 Retry
Requests..... 3 Received
Responses..... 3 Authorization Success.....
3 Authorization Failure..... 0 Challenge
Responses..... 0 Malformed Msgs.....
0 Bad Athrenticator Msgs..... 0 Timeout
Requests..... 0 Unknowntype
Msgs..... 0 Other Drops..... 0
```
- **mostre o stats do acct dos tacacs** — Estatísticas do servidor de contabilidade dos indicadores TACACS+.
```
(Cisco Controller) >show tacacs acct statistics Accounting Servers: Server
Index..... 1 Server
Address..... 10.1.1.12 Msg Round Trip
Time..... 0 (1/100 second) First
Requests..... 133 Retry
Requests..... 0 Accounting
Response..... 0 Accounting Request Success..... 0
Accounting Request Failure..... 0 Malformed
Msgs..... 0 Bad Authenticator Msgs.....
0 Timeout Requests..... 399 Unknowntype
Msgs..... 0 Other Drops..... 0
```

Configurar o server do Cisco Secure ACS

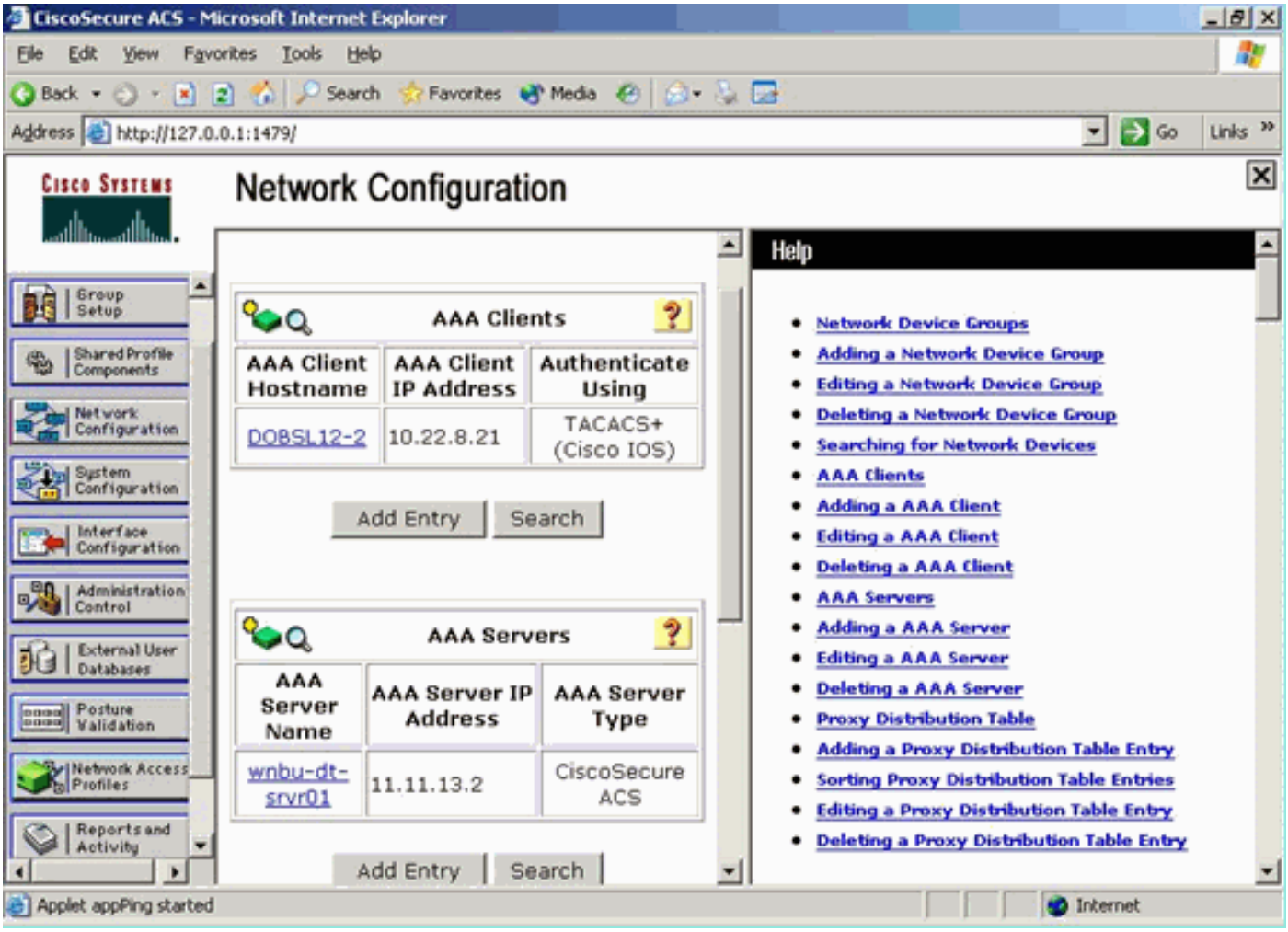
Esta seção fornece as etapas envolvidas no servidor ACS TACACS+ para criar serviços e atributos feitos sob encomenda, e atribui os papéis aos usuários ou aos grupos.

A criação dos usuários e do grupo não é explicada nesta seção. Supõe-se que os usuários e os grupos estão criados como necessários. Refira o Guia do Usuário para o server 4.0 do Cisco Secure ACS for Windows para obter informações sobre de como criar usuários e grupos de usuário.

Configuração de rede

Termine esta etapa:

Adicionar o endereço IP de gerenciamento do controlador como o cliente de AAA com o mecanismo da autenticação como TACACS+ (Cisco IOS).

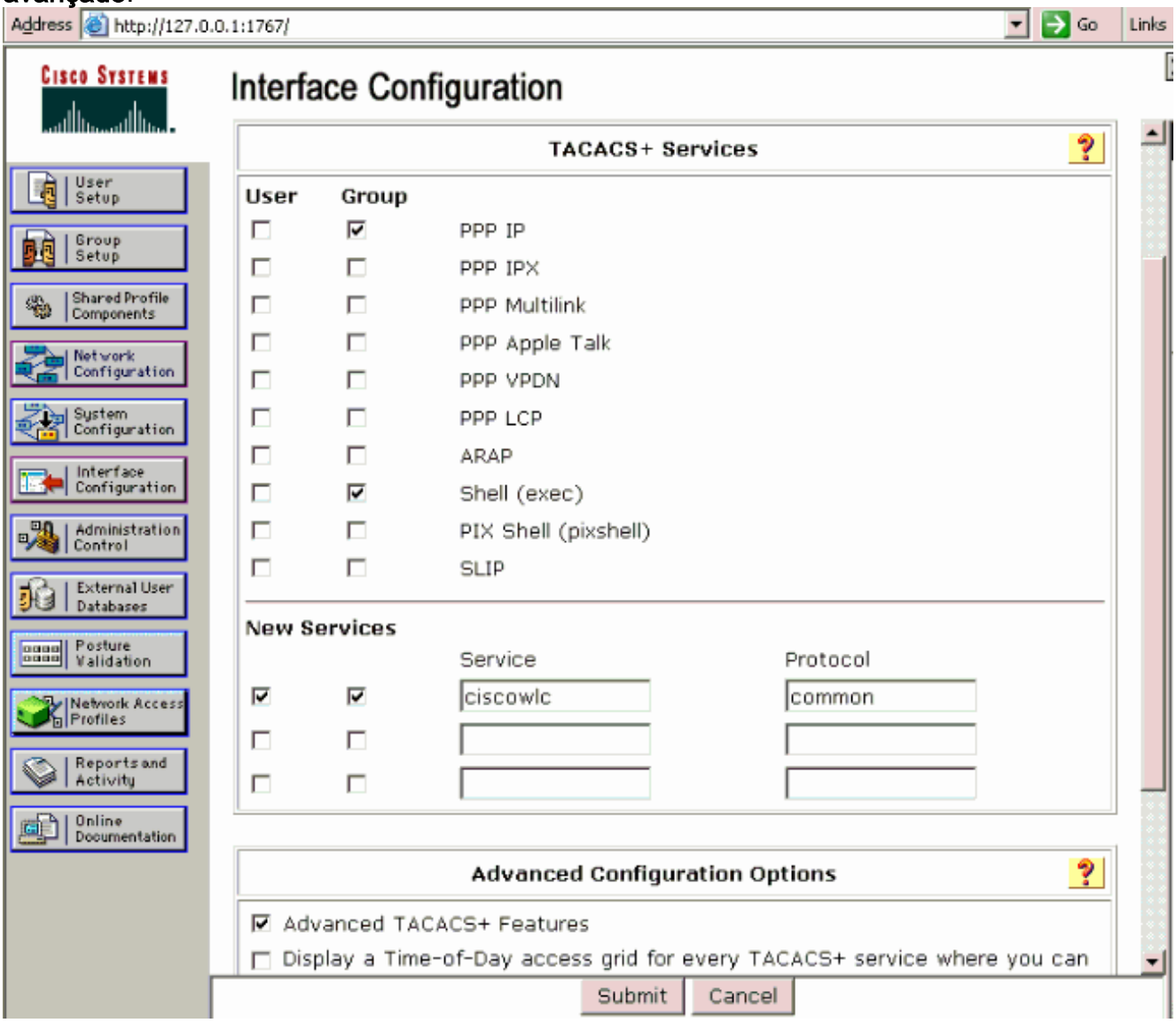


Configuração da interface

Conclua estes passos:

1. No menu da configuração da interface, selecione o link **TACACS+** (Cisco IOS).
2. Permita os **serviços novos**.
3. Verifique as caixas do **usuário** e de **verificação de atributo**.

4. Incorpore o **ciscowlc** para o serviço e a **terra comum** para o protocolo.
5. Permita as **características do TACACS+ avançado**.

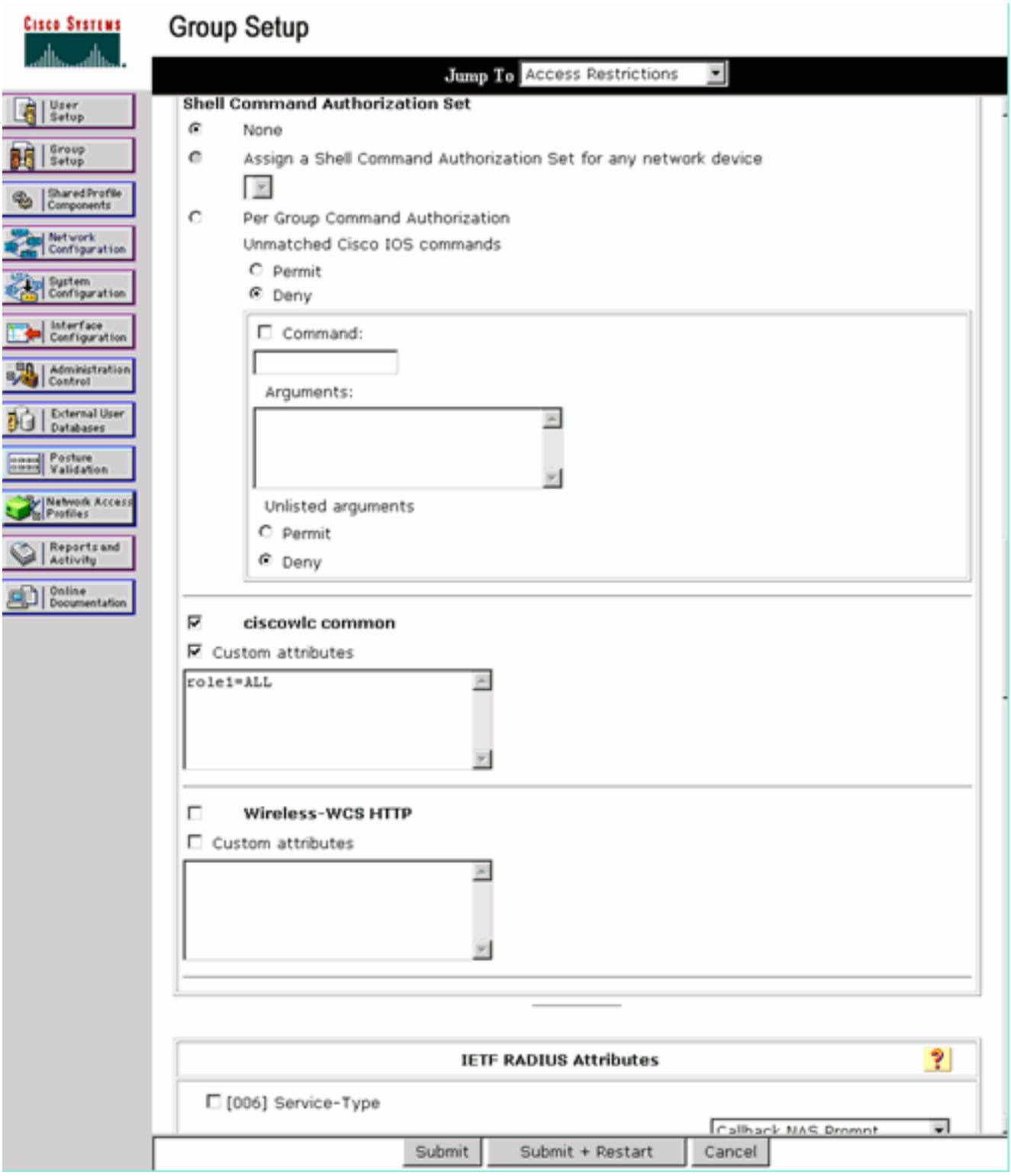


6. O clique **submete-se** a fim aplicar as mudanças.

Usuário/instalação de grupo

Conclua estes passos:

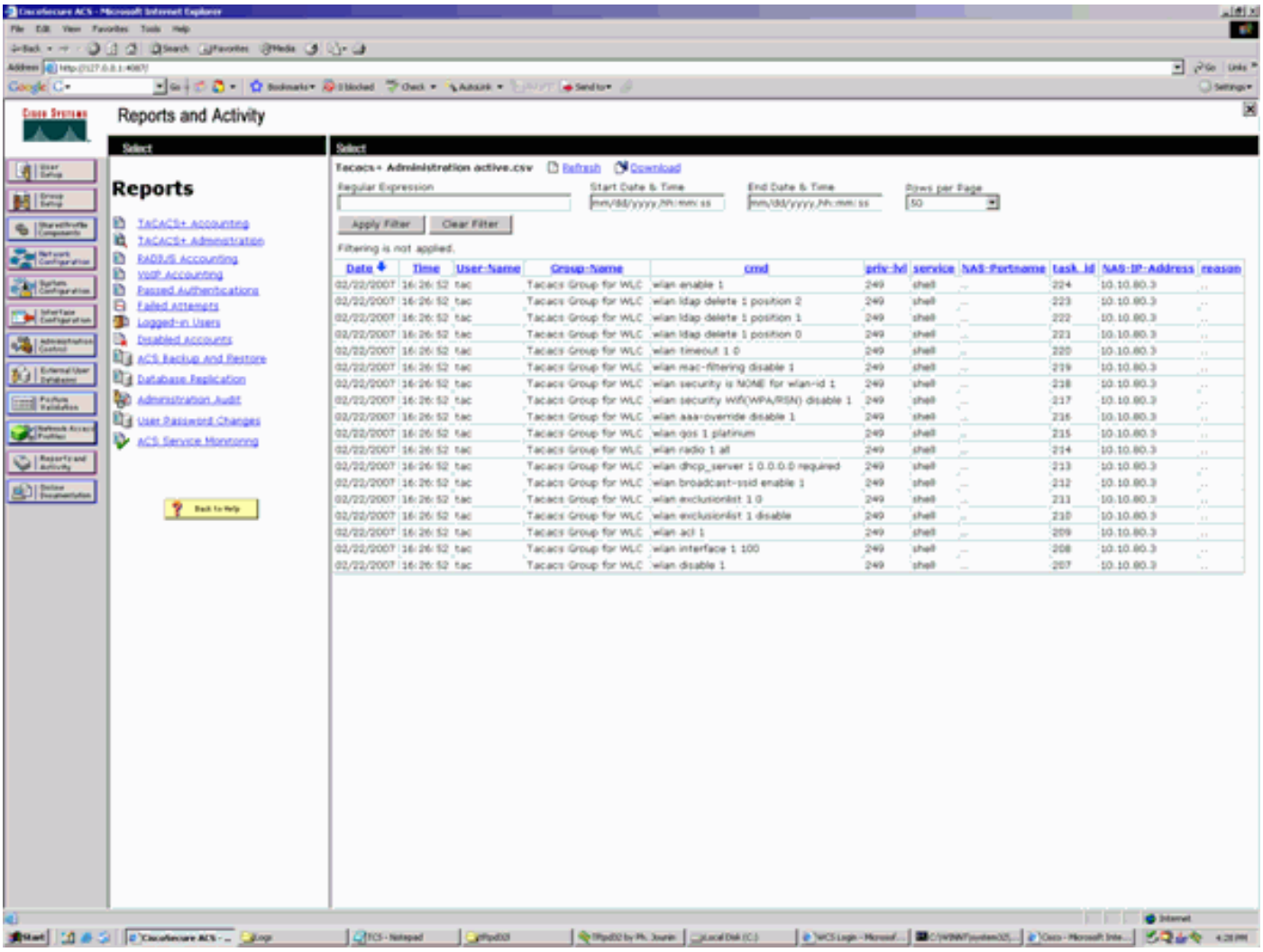
1. Selecione um usuário/grupo previamente criados.
2. Vá aos **ajustes TACACS+**.
3. Verifique a caixa de verificação que corresponde ao serviço do *ciscowlc* que foi criado na seção de configuração da interface.
4. Verifique a caixa de verificação dos **atributos feitos sob encomenda**.



5. Na caixa de texto abaixo dos atributos feitos sob encomenda, incorpore este texto se o usuário criado precisa o acesso somente ao WLAN, à SEGURANÇA e ao CONTROLADOR: **role1=WLAN role2=SECURITY role3=CONTROLLER**.Se o usuário precisa o acesso somente à ABA de segurança, incorpore este texto: **role1=SECURITY**.O papel corresponde aos sete artigos da barra de menus na Web GUI do controlador. Os artigos da barra de menus são MONITOR, WLAN, CONTROLADOR, SEM FIO, SEGURANÇA, GERENCIAMENTO e COMANDO.
6. Incorpore o papel que necessidades de usuário para role1, role2 e assim por diante. Se as necessidades de usuário todos os papéis, **TODA a** palavra-chave forem usadas então. Para o papel admin da entrada, a **ENTRADA da** palavra-chave deve ser usada.

Registros de contabilidade no Cisco Secure ACS

Os registros de contabilidade TACACS+ do WLC estão disponíveis no Cisco Secure ACS na administração TACACS+ dos relatórios e da atividade:



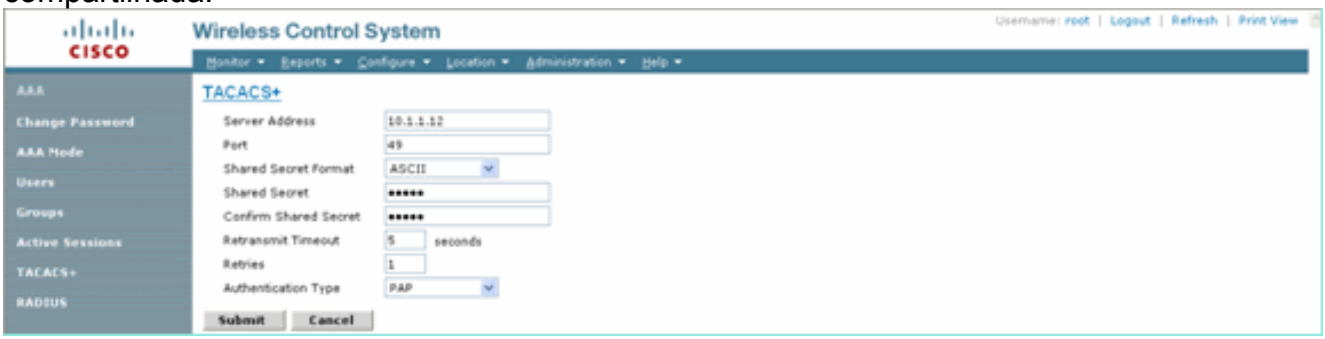
Configuração TACACS+ no WCS

Conclua estes passos:

1. Do GUI, entre ao WCS com a conta raiz.
2. Adicionar o server TACACS+. Vá à **administração > ao server do > Add TACACS+ AAA > TACACS+**.

3. Adicionar os detalhes do server TACACS+, tais como o endereço IP de Um ou Mais Servidores Cisco ICM NT, o número de porta (49 são padrão), e a chave secreta

compartilhada.



4. Permita a autenticação TACACS+ para a administração no WCS. Vai à **administração > ao modo AAA > AAA > o TACACS+ seleto**.

WCS usando Domínios Virtuais

O Domínio Virtual é uns novos recursos introduzidos com versão 5.1 WCS. Um domínio virtual WCS consiste em um conjunto de dispositivo e em mapas e restringe uma opinião de usuário à informação relevante a estes dispositivos e mapas. Através de um domínio virtual, um administrador pode assegurar-se de que os usuários possam somente ver os dispositivos e os mapas para que são responsáveis. Além, devido aos filtros do domínio virtual, os usuários podem configurar, ver alarmes, e gerar relatórios para somente o seu atribuído parte da rede. O administrador especifica um grupo de domínios virtuais permitidos para cada usuário. Somente um destes pode ser ativo para esse usuário no início de uma sessão. O usuário pode mudar o domínio virtual atual selecionando um domínio virtual permitido diferente do menu suspenso do Domínio Virtual na parte superior da tela. Todos os relatórios, os alarmes, e a outra funcionalidade são filtrados agora por esse domínio virtual.

Se há somente um domínio virtual definido (raiz) no sistema e o usuário não tem nenhuns domínios virtuais nos atributos feitos sob encomenda coloca no server TACACS+/RADIUS, o usuário está atribuído o domínio virtual da raiz à revelia.

Se há mais de um domínio virtual, e o usuário não tem nenhuns atributos especificada, a seguir o usuário está obstruído da abertura. A fim permitir que o usuário entre, os atributos feitos sob encomenda do Domínio Virtual devem ser exportados para o server Radius/TACACS+.

O indicador dos atributos feitos sob encomenda do Domínio Virtual permite que você indique os dados apropriados do específico de protocolo para cada domínio virtual. O botão da exportação atributos do RAIO e TACACS+ nos PRE-formatos do sidebar da hierarquia do Domínio Virtual do domínio virtual. Você pode copiar e colar estes atributos no servidor ACS. Isto permite que você copie somente os domínios virtuais aplicáveis à tela do servidor ACS e assegura-se de que os usuários tenham somente o acesso a estes domínios virtuais.

A fim aplicar os atributos PRE-formatados do RAIO e TACACS+ ao servidor ACS, termine as

etapas explicadas no RAIO do Domínio Virtual e o TACACS+ atribui a seção.

Configurar o Cisco Secure ACS para usar o WCS

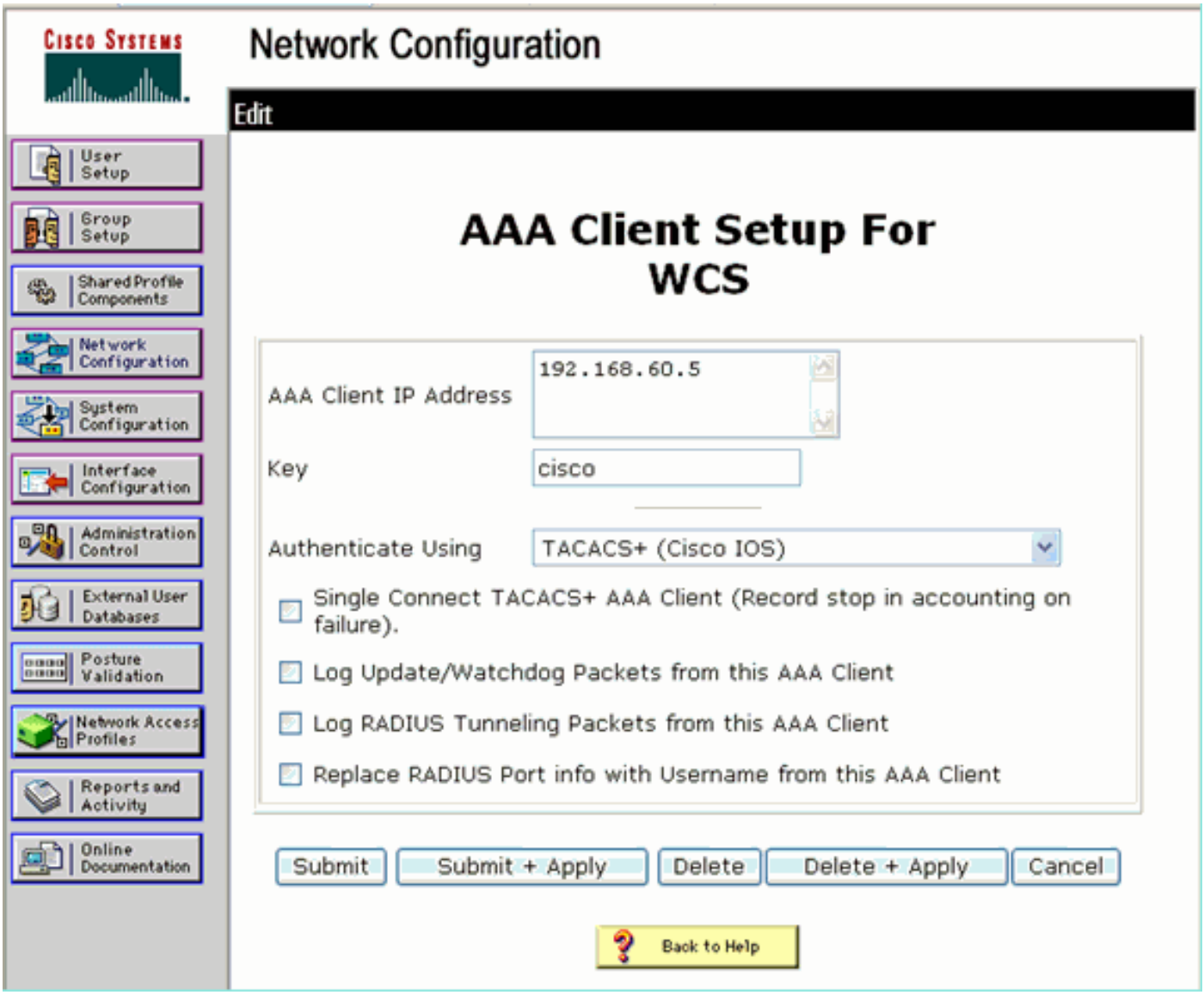
A seção fornece as etapas envolvidas no servidor ACS TACACS+ para criar serviços e atributos feitos sob encomenda, e atribui os papéis aos usuários ou aos grupos.

A criação dos usuários e do grupo não é explicada nesta seção. Supõe-se que os usuários e os grupos estão criados como necessários.

Configuração de rede

Termine esta etapa:

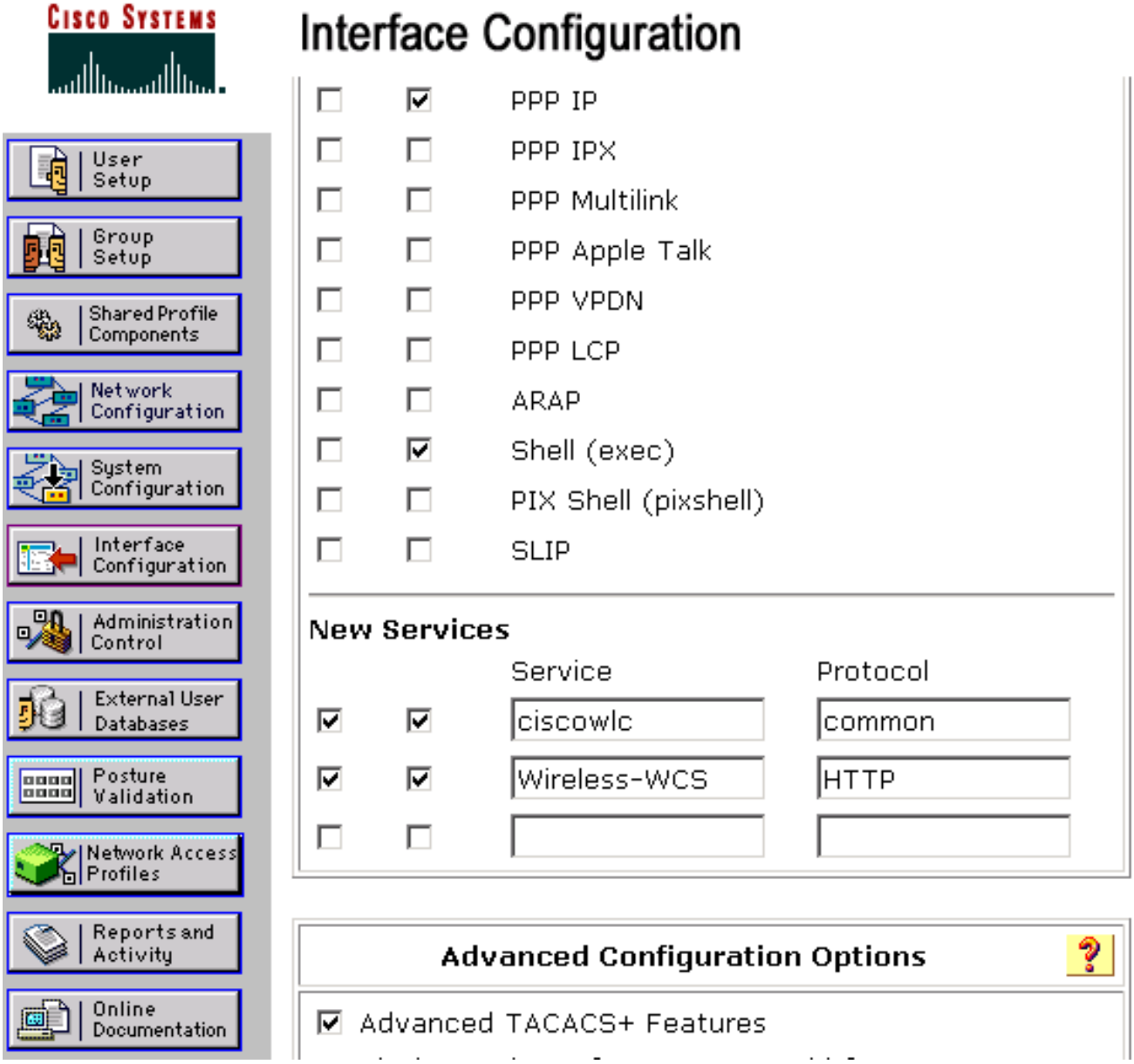
Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT WCS como o cliente de AAA com o mecanismo da autenticação como TACACS+ (Cisco IOS).



Configuração da interface

Conclua estes passos:

1. No menu da configuração da interface, selecione o link **TACACS+** (Cisco IOS).
2. Permita os **serviços novos**.
3. Verifique as caixas do **usuário** e de **verificação de atributo**.
4. Incorpore o Sem fio-**WCS** para o serviço e o **HTTP** para o protocolo.**Nota:** O HTTP deve estar nos TAMPÕES.
5. Permita as **características do TACACS+ avançado**.

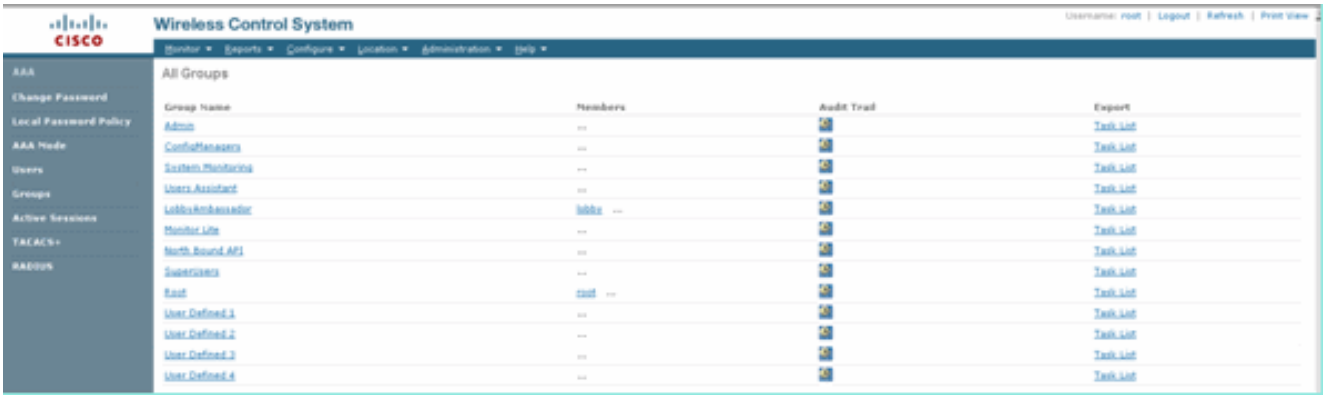


6. O clique **submete-se** a fim aplicar as mudanças.

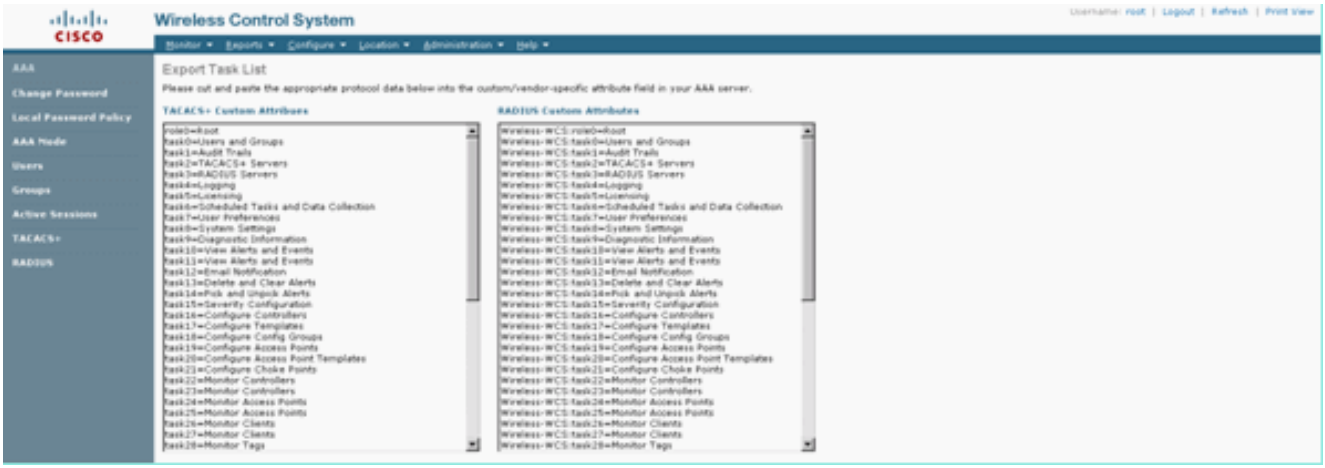
Usuário/instalação de grupo

Conclua estes passos:

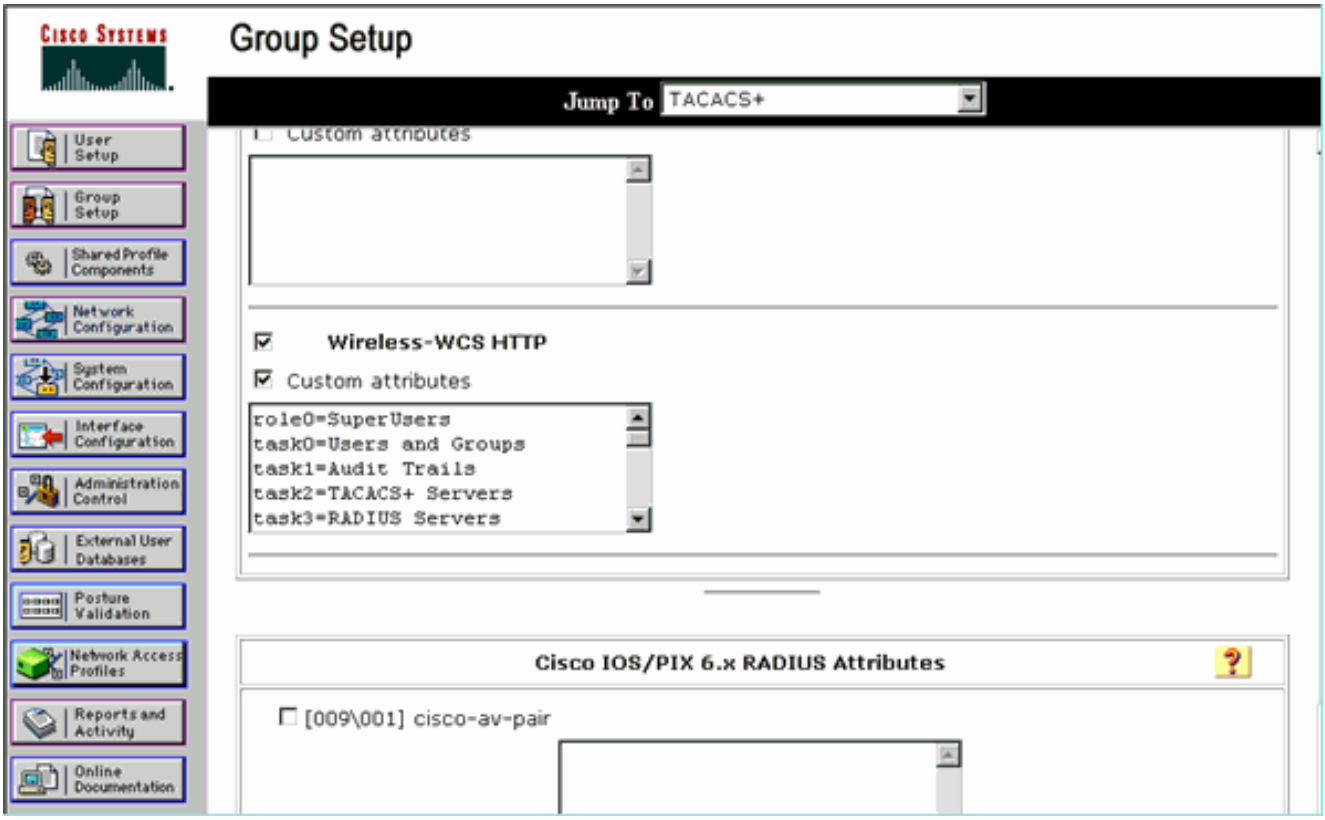
1. No WCS GUI, navegue à **administração > ao AAA > aos grupos** para selecionar alguns dos grupos de usuário PRE-configurados, tais como SuperUsers no WCS.



2. Selecione a lista de tarefas para os grupos de usuário e a pasta PRE-configurados da cópia ao
ACS.



3. Selecione um usuário/grupo previamente criados e vá aos **ajustes TACACS+**.
4. Em ACS GUI, selecione a caixa de verificação que corresponde ao serviço Sem fio-WCS que foi criado mais cedo.
5. Em ACS GUI, verifique a caixa dos **atributos feitos sob encomenda**.
6. Na caixa de texto abaixo dos atributos feitos sob encomenda, incorpore esta informação do papel e da tarefa copiada do WCS. Por exemplo, incorpore a lista de tarefas permitidas pelos
SuperUsers.



7. Então, início de uma sessão ao WCS com o username/senha recém-criados no ACS.

Debugs

Debuga do WLC para role1=ALL

```
(Cisco Controller) >debug aaa tacacs enable (Cisco Controller) >Wed Feb 28 17:36:37 2007:
Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:36:37 2007: tplus response: type=1
seq_no=2 session_id=5eaa857e length=16 encrypted=0 Wed Feb 28 17:36:37 2007:
TPLUS_AUTHEN_STATUS_GETPASS Wed Feb 28 17:36:37 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:36:37 2007: processTplusAuthResponse: Continue auth transaction Wed Feb 28
17:36:37 2007: tplus response: type=1 seq_no=4 session_id=5eaa857e length=6 encrypted=0 Wed Feb
28 17:36:37 2007: tplus_make_author_request() from tplus_authen_passed returns rc=0 Wed Feb 28
17:36:37 2007: Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:36:37 2007: author response
body: status=1 arg_cnt=1 msg_len=0 data_len=0 Wed Feb 28 17:36:37 2007: arg[0] = [9][role1=ALL]
Wed Feb 28 17:36:37 2007: User has the following mgmtRole fffffff8
```

Debuga do WLC para papéis múltiplos

```
(Cisco Controller) >debug aaa tacacs enable Wed Feb 28 17:59:33 2007: Forwarding request to
10.1.1.12 port=49 Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=2 session_id=b561ad88
length=16 encrypted=0 Wed Feb 28 17:59:34 2007: TPLUS_AUTHEN_STATUS_GETPASS Wed Feb 28 17:59:34
2007: auth_cont get_pass reply: pkt_length=22 Wed Feb 28 17:59:34 2007:
processTplusAuthResponse: Continue auth transaction Wed Feb 28 17:59:34 2007: tplus response:
type=1 seq_no=4 session_id=b561ad88 length=6 encrypted=0 Wed Feb 28 17:59:34 2007:
tplus_make_author_request() from tplus_authen_passed returns rc=0 Wed Feb 28 17:59:34 2007:
Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:59:34 2007: author response body: status=1
arg_cnt=4 msg_len=0 data_len=0 Wed Feb 28 17:59:34 2007: arg[0] = [11][role1=WLAN] Wed Feb 28
17:59:34 2007: arg[1] = [16][role2=CONTROLLER] Wed Feb 28 17:59:34 2007: arg[2] =
[14][role3=SECURITY] Wed Feb 28 17:59:34 2007: arg[3] = [14][role4=COMMANDS] Wed Feb 28 17:59:34
2007: User has the following mgmtRole 150
```

Debuga de um WLC para a falha na autorização

```
(Cisco Controller) >debug aaa tacacs enable Wed Feb 28 17:53:04 2007: Forwarding request to
```

```
10.1.1.12 port=49 Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=2 session_id=89c553a1
length=16 encrypted=0 Wed Feb 28 17:53:04 2007: TPLUS_AUTHEN_STATUS_GETPASS Wed Feb 28 17:53:04
2007: auth_cont get_pass reply: pkt_length=22 Wed Feb 28 17:53:04 2007:
processTplusAuthResponse: Continue auth transaction Wed Feb 28 17:53:04 2007: tplus response:
type=1 seq_no=4 session_id=89c553a1 length=6 encrypted=0 Wed Feb 28 17:53:04 2007:
tplus_make_author_request() from tplus_authen_passed returns rc=0 Wed Feb 28 17:53:04 2007:
Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:53:04 2007: author response body:
status=16 arg_cnt=0 msg_len=0 data_len=0 Wed Feb 28 17:53:04 2007:User has the following
mgmtRole 0 Wed Feb 28 17:53:04 2007: Tplus authorization for tac failed status=16
```

Informações Relacionadas

- Controlador de LAN do Cisco Wireless (WLC) e exemplo de configuração de Cisco ACS 5.x (TACACS+) para a autenticação da Web
- Configurando o TACACS+
- Como configurar a autenticação TACACS e a autorização para os usuários Admin e NON-Admin em ACS 5.1
- Comparação TACACS+ e RADIUS
- Suporte Técnico e Documentação - Cisco Systems