Configurar a administração de WCS e NCS com ACS 5.x

Contents

Introduction

Este documento descreve como usar o Cisco Secure Access Control Server (ACS) 5.x para configurar a administração do Cisco Wireless Control System (WCS) e do Cisco Prime Network Control System (NCS).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Wireless Control System
- Sistema de controle de rede Cisco Prime
- Cisco Secure Access Control Server

Componentes Utilizados

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

- Cisco Wireless Control System 7.0.172.0
- Cisco Secure ACS 5.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

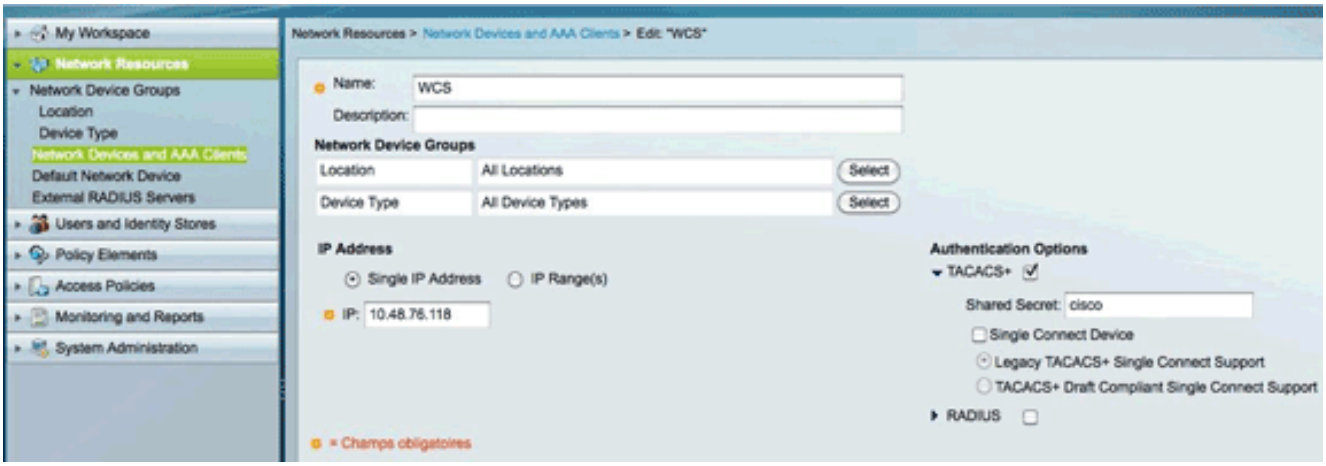
Configurar

Esta configuração de exemplo descreve como autenticar um usuário com TACACS+.

Observação: embora várias opções e possibilidades existam quando você autentica usuários do WCS/NCS com Cisco Secure ACS 5.x, nem todas as combinações são descritas neste documento. No entanto, este exemplo fornece as informações necessárias para entender como modificar o exemplo para a configuração precisa que você deseja obter.

Etapa 1. Adicione o WCS aos clientes ACS AAA.

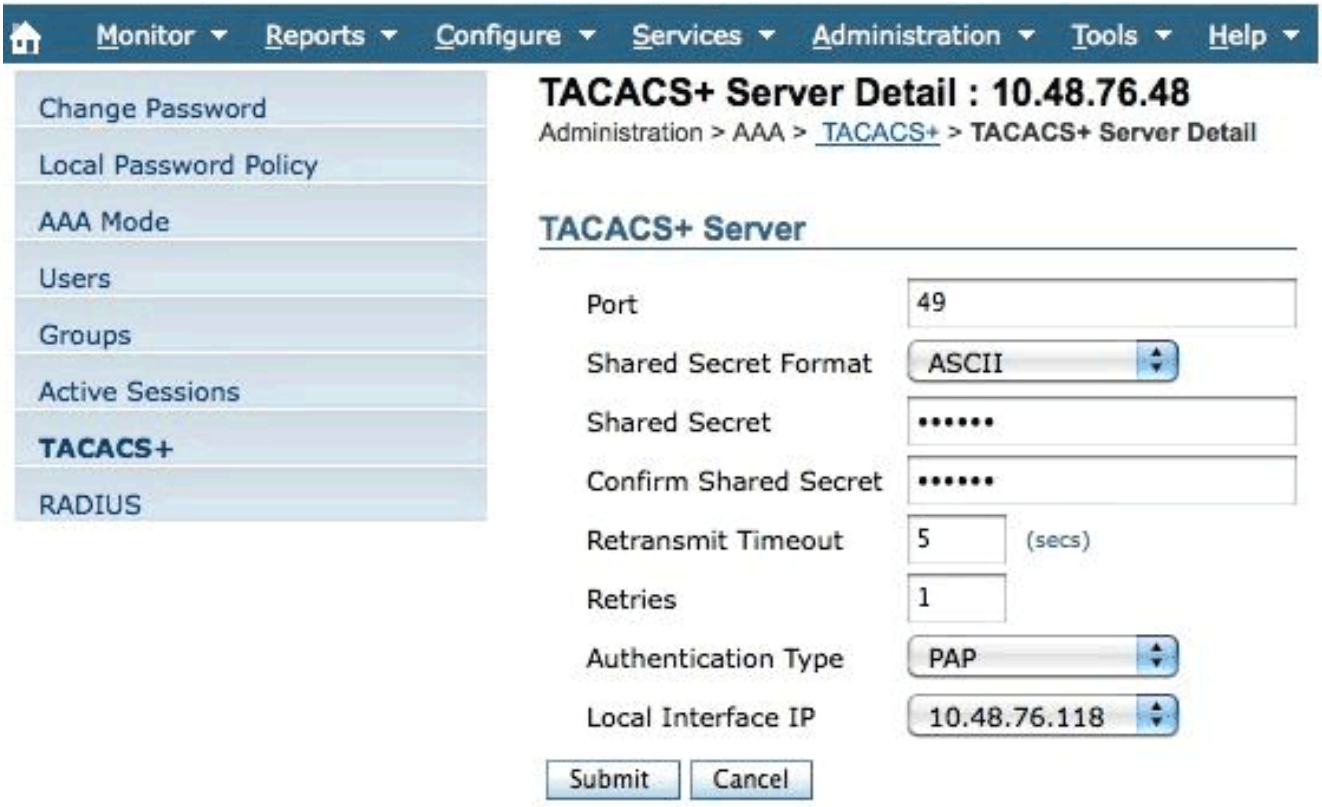
1. No Cisco Secure ACS, escolha **Network Resources > Network Devices and AAA Clients**.



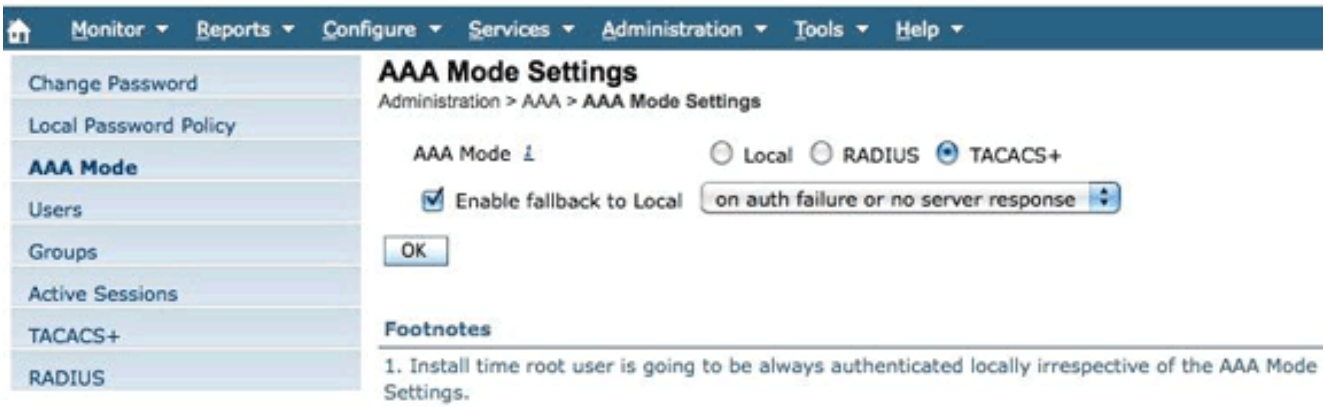
2. Digite um nome no campo Nome.
3. Insira o endereço IP do WCS no campo IP address (Endereço IP).
4. Na área Opções de autenticação, clique na caixa de seleção **TACACS+** para ativar TACACS+ e insira um termo a ser usado como um segredo compartilhado.**Observação:** este exemplo usa *cisco* como o segredo compartilhado; no entanto, por motivos de segurança, você deve usar um termo menos óbvio.

Etapa 2. Adicione o Cisco Secure ACS como um servidor TACACS+ no WCS.

1. Faça login no WCS e escolha **Administration > AAA**.
2. Clique em **TACACS+**.



3. Insira seu termo de segredo compartilhado nos campos Shared Secret e Confirm Shared Secret.
4. Escolha o endereço IP do Cisco ACS no campo Local Interface IP.
5. Na área de navegação à esquerda, clique em **AAA Mode (Modo AAA)**.



6. Clique no botão de opção **TACACS+**.**Observação:** por motivos de segurança, a Cisco recomenda que você escolha **uma falha de autenticação ou nenhuma resposta do servidor** na lista suspensa Ativar fallback para local. A escolha dessa opção impede que você seja bloqueado em caso de problemas. Você pode alterar a opção quando tudo funcionar corretamente.

Etapa 3. Configure o perfil de shell correto no ACS.

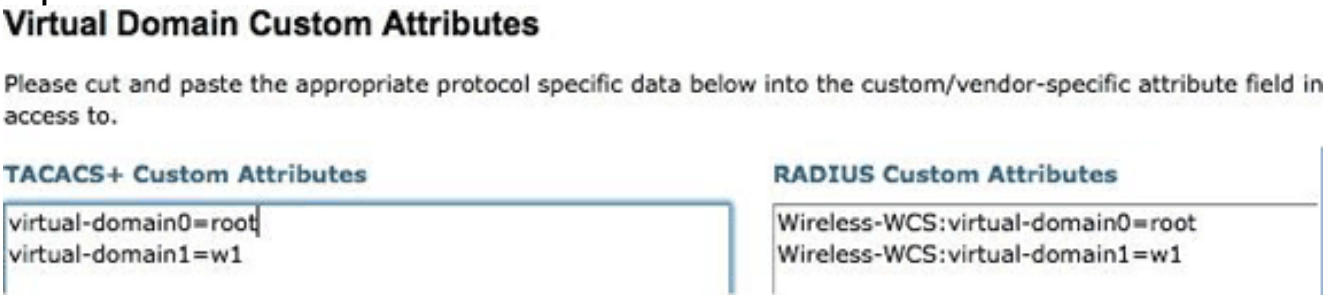
Esta etapa descreve como configurar o Cisco Secure ACS para retornar os atributos corretos para determinar os privilégios de usuário no WCS.

1. Na área de navegação à esquerda, clique em **Grupos**.Uma lista de tipos de usuário é exibida. Este exemplo autentica um usuário do tipo de usuário Lobby Embaixador.

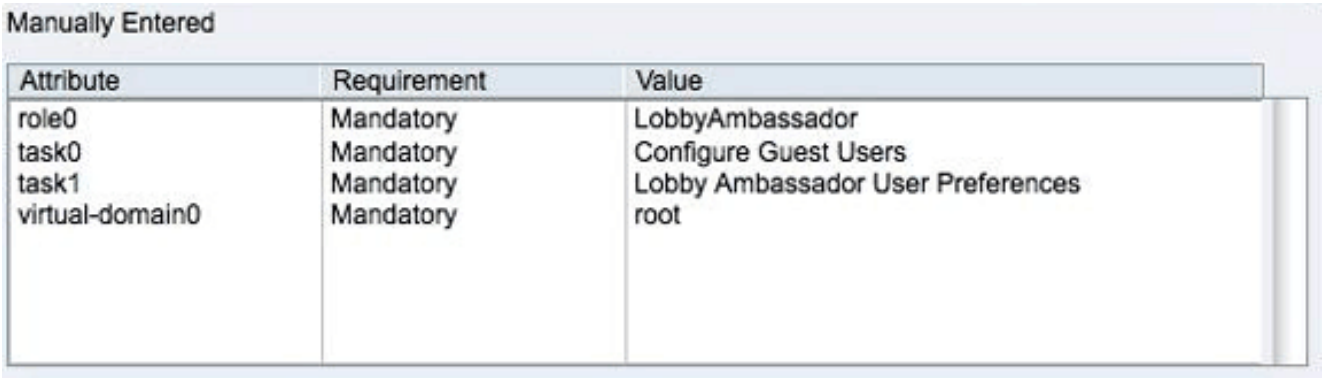
2. Clique no link **Lista de Tarefas** ao lado do grupo **Embaixador** de **Lobby**.

Observação: você deve configurar a função de usuário (Embaixador de Lobby neste exemplo) e uma lista de tarefas que eles podem executar e itens de menu que eles podem acessar. Se você usar uma versão recente do WCS, também deverá configurar o domínio virtual ao qual o usuário pertencerá.

3. Escolha **Administração > Domínios virtuais**.
4. Clique em **Exportar**.



5. Escolha **Elementos de política > Autorização e permissões > Administração de dispositivo > Perfis de shell** para criar um novo perfil de shell.
6. Insira um nome significativo (como *WCS*) e clique na guia **Custom Attributes**.
7. Configure os atributos como eles existem no WCS.



Observação: em versões do ACS anteriores à versão 5.2 patch 7, você pode enfrentar problemas ao inserir uma tarefa que contém a palavra "alerta". Isso é corrigido em versões posteriores do ACS. O mesmo problema existe em versões do Identity Services Engine (ISE) anteriores à 1.2.Aqui está um exemplo de como inserir manualmente os atributos:

```
-type "role0" in the "Attribute" field
-type "LobbyAmbassador" in the Value field
-click the "add" button.
Etc… for the other attributes.
```

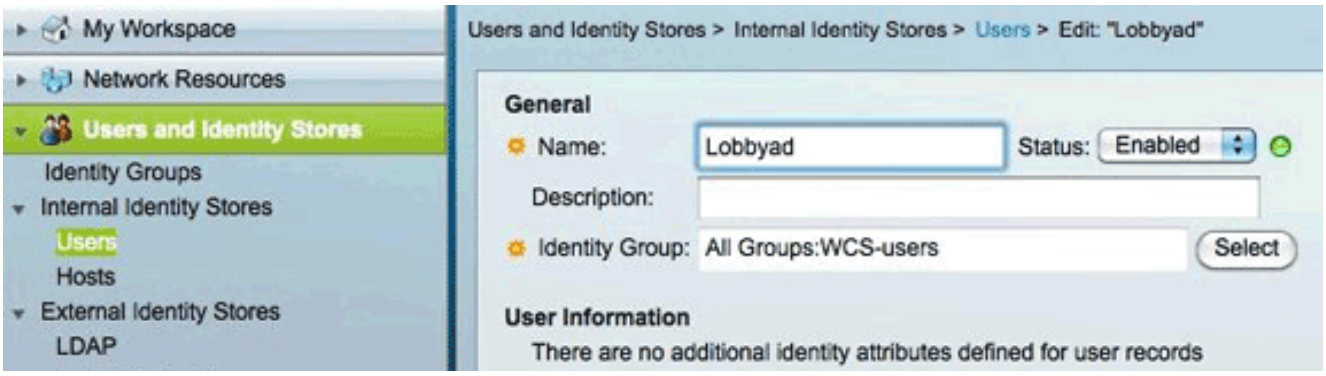
Observação: no ACS 4, foi possível copiar/colar a lista de atributos da GUI do WCS para a GUI do ACS 4. No ACS 5, eles devem ser inseridos um por um.No NCS e na Prime Infrastructure, o atributo deve ser inserido em uma ordem muito específica. O pedido é domínio virtual, função e lista de tarefas. Se inserido na ordem errada, o NCS/Prime recusa

a autenticação.

```
NCS:virtual-domain0=ROOT-DOMAIN
NCS:role0=Super Users
NCS:task0=View Alerts and Events
```

Etapa 4. Configure o Cisco Secure ACS para retornar os atributos.

1. Configure um usuário (este exemplo usa *Lobbyad*) como um usuário no ACS.



Observação: para facilitar a configuração, este exemplo adiciona o usuário Lobbyad ao grupo *WCS-users*. (Essa etapa é opcional.)

2. Nas políticas de Acesso, em **Default Device Admin > Authorization**, configure uma regra para corresponder à autenticação WCS.

3. Se o nome de usuário pertencer ao grupo *WCS-users*, retorne o perfil do shell *wcs* (que contém os atributos do grupo).
4. Para configurar outros tipos de usuários (como administradores), você deve configurar outro perfil do shell para retornar atributos diferentes. A partir daí, você deve agrupar administradores em um grupo diferente para diferenciar e saber qual perfil do shell retornar.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Guia de configuração do Cisco Wireless Control System, versão 7.0.172.0
- Guia do usuário do Cisco Secure Access Control System 5.2
- Suporte Técnico e Documentação - Cisco Systems