ACS 5.x: Autenticação TACACS+ e comando authorization baseados no exemplo de configuração da membrasia do clube AD

Índice

Introdução

Este documento fornece um exemplo de configurar a autenticação TACACS+ e o comando authorization baseados na membrasia do clube AD de um usuário o Cisco Secure Access Control System (ACS) 5.x e mais tarde. O ACS usa o Microsoft Active Directory (AD) como um armazenamento de identidade externa para armazenar recursos, como usuários, máquinas, grupos e atributos.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- O ACS 5.x é integrado inteiramente ao domínio desejado AD. Se o ACS não é integrado com o domínio desejado AD, refira ACS 5.x e mais tarde: Integração com exemplo de configuração do microsoft ative directory para mais informação a fim executar a tarefa da integração.

Componentes Utilizados

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

- Cisco Secure ACS 5.3

- Liberação 12.2(44)SE6 do Cisco IOS ® Software.**Nota:** Esta configuração pode ser feita em todos os dispositivos IOS Cisco.
- Domínio 2003 do Microsoft Windows server

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.

Configuração

Configurar ACS 5.x para a authentication e autorização

Antes que você comece a configuração do ACS 5.x para a authentication e autorização, o ACS deve ter sido integrado com sucesso com Microsoft AD. Se o ACS não é integrado com o domínio desejado AD, refira ACS 5.x e mais tarde: Integração com exemplo de configuração do microsoft ative directory para mais informação a fim executar a tarefa da integração.

Nesta seção, você traça dois grupos AD a dois conjuntos de comandos diferentes e dois perfis do shell, um com acesso direto e o outro com limitado-acesso nos dispositivos IOS Cisco.

1. Log no ACS GUI usando credenciais Admin.
2. Escolha **usuários e a identidade armazena > identidade externo armazena > diretório ativo** e verifica que o ACS se juntou ao domínio desejado e também que o **estado da Conectividade** está mostrado como **conectado**.Clique sobre a aba dos **grupos do diretório**.
3. Clique **seleto**.
4. Escolha os grupos que precisam de ser traçados parte de aos perfis e aos conjuntos de comandos do shell no mais atrasado a configuração. Clique em **OK**.
5. Clique **mudanças da salvaguarda**.
6. Escolha **políticas de acesso > acesso presta serviços de manutenção > regras de seleção do serviço** e identificam o serviço do acesso, que processa a autenticação TACACS+. Neste exemplo, é o **dispositivo Admin do padrão**.
7. Escolha o **dispositivo das políticas de acesso > dos serviços > do padrão do acesso Admin > identidade** e clique **seleto** ao lado da **fonte da identidade**.
8. Escolha **AD1** e clique a **APROVAÇÃO**.
9. Clique **mudanças da salvaguarda**.
10. Escolha o **dispositivo das políticas de acesso > dos serviços > do padrão do acesso Admin > autorização** e clique sobre **Customize**.
11. Copie **AD1:ExternalGroups de disponível à seção selecionada de condições Customize** e mova então o **perfil** e os **conjuntos de comandos do shell de disponível** para a **seção selecionada de resultados Customize**. Clique agora a **APROVAÇÃO**.
12. O clique **cria** a fim criar uma regra nova.
13. Clique **seleto na** condição **AD1:ExternalGroups**.
14. Escolha o grupo que você quer fornecer o acesso direto no dispositivo IOS Cisco. Clique

em **OK**.
15. Clique **seleto no** campo do perfil do shell.
16. O clique **cria** a fim criar um **perfil** novo do **shell** para usuários do acesso direto.
17. Forneça um **nome** e um **Description(optional) no tab geral** e clique sobre a aba **comum das tarefas**.
18. Mude o **privilégio padrão** e o **privilégio máximo à estática** com **valor 15**. Clique em Submit.
19. Agora escolha o **perfil** recém-criado do **shell do** acesso direto (FULL-privilégio neste exemplo) e clique a **APROVAÇÃO**.
20. Clique **seleto no** campo dos conjuntos de comandos.
21. O clique **cria** a fim criar um comando new **ajustado** para usuários do **acesso direto**.
22. Forneça um **nome** e assegure-se de que a caixa de verificação ao lado do **comando permit any que não está na tabela abaixo** esteja verificada. Clique em Submit.**Nota:** Refira a criação, a duplicação, e os grupos do comando editing para a administração do dispositivo para obter mais informações sobre dos conjuntos de comandos.
23. Clique em **OK**.
24. Clique em **OK**. Isto termina a configuração de **Rule-1**.
25. O clique **cria** a fim criar uma regra nova para usuários **limitados do acesso**.
26. Escolha **AD1:ExternalGroups** e clique **seleto**.
27. Escolha os grupos do grupo (ou) que você quer fornecer acesso limitado a e clicar a **APROVAÇÃO**.
28. Clique **seleto no** campo do perfil do shell.
29. O clique **cria** a fim criar um **perfil** novo do **shell** para acesso limitado.
30. Forneça um **nome** e um **Description(optional) no tab geral** e clique sobre a aba **comum das tarefas**.
31. Mude o **privilégio padrão** e o **privilégio máximo à estática** com valores **1** e **15** respectivamente. Clique em Submit.
32. Clique em **OK**.
33. Clique **seleto no** campo dos conjuntos de comandos.
34. O clique **cria** para criar um comando new **ajustado** para o grupo de acesso limitado.
35. Forneça um **nome** e assegure-se de que a caixa de seleção ao lado do **comando permit any que não está na tabela abaixo** não esteja selecionada. O clique **adiciona** após a **mostra de** datilografia no espaço fornecido no **comando section** e escolhe a **licença na** seção de **Grant** de modo que somente os comandos show sejam permitidos para os usuários no grupo de acesso limitado.
36. Adicionar similarmente todos os outros comandos ser permitido para os usuários em grupo de acesso limitado com o uso **Add**. Clique em Submit.**Nota:** Refira a criação, a duplicação, e os grupos do comando editing para a administração do dispositivo para obter mais informações sobre dos conjuntos de comandos.
37. Clique em **OK**.
38. Clique em **OK**.
39. Clique **mudanças da salvaguarda**.
40. O clique **cria** a fim adicionar o **dispositivo IOS Cisco** como um **cliente de AAA no** ACS.
41. Forneça um **nome, um endereço IP de Um ou Mais Servidores Cisco ICM NT, um segredo compartilhado** para o **TACACS+** e um clique **submetem-se**.

Configurar o dispositivo IOS Cisco para a authentication e autorização

Termine estas etapas a fim configurar o dispositivo IOS Cisco e o ACS para a authentication e

autorização.

1. Crie um usuário local com o privilégio completo para a reserva com o **comando username** como mostrado aqui:`username admin privilege 15 password 0 cisco123!`
2. Forneça o endereço IP de Um ou Mais Servidores Cisco ICM NT do ACS a fim permitir o AAA e adicionar ACS 5.x como o servidor de TACACS.`aaa new-model`
   `tacacs-server host 192.168.26.51 key cisco123`**Nota:** A chave deve combinar com o Compartilhar-segredo fornecido no ACS para este dispositivo IOS Cisco.
3. Teste a alcançabilidade do servidor de TACACS com o [comando aaa do teste](#) como mostrado.`test aaa group tacacs+ user1 xxxxx legacy`
   `Attempting authentication test to server-group tacacs+ using tacacs+`
   `User was successfully authenticated.`A saída do comando precedente mostra que o servidor de TACACS é alcançável e o usuário esteve autenticado com sucesso.**Nota:** O usuário1 e a senha xxx pertencem ao AD. Se o teste falha por favor assegure-se de que o Compartilhar-segredo fornecido na etapa precedente esteja correto.
4. Configurar o início de uma sessão e permita autenticações e use então o executivo e as autorizações de comando como mostrado aqui:
```
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 0 default group tacacs+ local
aaa authorization commands 1 default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa authorization config-commands
```
   Nota: O Local e permite palavras-chaves está usado para a reserva ao usuário local do Cisco IOS e permite o segredo respectivamente se o servidor de TACACS é inacessível.

Verificar

A fim verificar a authentication e autorização entre ao dispositivo IOS Cisco com o telnet.

1. Telnet ao dispositivo IOS Cisco como o usuário1 que pertence ao grupo do acesso direto no AD. O grupo de Admins da rede é o grupo no AD que é comando set traçado do perfil e do acesso direto do shell do FULL-privilégio no ACS. Tente executar o comando any assegurar-se de que você tenha o acesso direto.
2. Telnet ao dispositivo IOS Cisco como user2 que pertence ao grupo do limitado-acesso no AD. (O grupo da **equipe da manutenção de rede** é o grupo no AD que é **comando set** traçado do **perfil** e do Mostra-**acesso do shell do Limitado-privilégio no** ACS). Se você tenta executar o comando any a não ser esses mencionados no comando set do Mostra-acesso, você deve obter um erro `falhado comando authorization`, que mostre que o user2 limitou o acesso.
3. Entre ao ACS GUI e lance a **monitoração e relate o visor**. Escolha o **protocolo de AAA > o TACACS+Authorization** a fim verificar as atividades executadas pelo usuário1 e pelo user2.

Informações Relacionadas

- [Cisco Secure Access Control System]
- [Suporte Técnico e Documentação - Cisco Systems]