NAC(CCA) 4.x: Usuários do mapa a determinados papéis usando o exemplo da configuração ldap

Índice

Introdução

Este documento descreve o Lightweight Directory Access Protocol (LDAP) que traça a característica a fim traçar os usuários a determinados papéis no dispositivo do Network Admission Control (NAC) ou no acesso limpo de Cisco (CCA).

A ferramenta NAC de Cisco (anteriormente acesso limpo de Cisco) é um produto facilmente distribuído NAC que use a infraestrutura de rede para reforçar a conformidade da política de segurança em todos os dispositivos que procuram aos recursos de computação da rede de acesso. Com ferramenta NAC, os administradores de rede podem autenticar, autorizam, avaliam, e remediate prendido, Sem fio, e usuários remotos e suas máquinas antes do acesso de rede. Identifica se os dispositivos em rede tais como portáteis, Telefones IP, ou consoles do jogo são complacentes com políticas de segurança da sua rede e repara todas as vulnerabilidades antes de permitir o acesso à rede.

Pré-requisitos

Requisitos

Este documento supõe que o gerente CCA, o server CCA e o servidor ldap estão instalados e trabalham corretamente.

Componentes Utilizados

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

- 3300 Series da ferramenta NAC de Cisco - Limpe o Access Manager 4.0
- 3300 Series da ferramenta NAC de Cisco - Limpe o servidor de acesso 4.0

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.

Autenticação contra o diretório ativo backend

Diversos tipos de fornecedores da autenticação no Access Manager limpo podem ser usados para autenticar usuários contra um server do diretório ativo (AD), o serviço de diretório proprietário de Microsoft. Estes incluem Windows NT(NTLM), Kerberos e LDAP (preferidos).

Se você usa o LDAP para conectar ao AD, o nome destacado (DN) completo de Search(Admin) tipicamente tem que ser ajustado ao DN de uma conta com privilégios administrativos ou privilégios básicos do usuário. A primeira entrada do Common Name (CN) deve ser um administrador do AD, ou um usuário com privilégios lidos. Note que o filtro da busca, SAMAccountName, é o nome de login de usuário no esquema do padrão AD.

Exemplo de configuração AD/LDAP

Isto ilustra uma configuração de exemplo usando o LDAP para comunicar-se com o diretório ativo backend:

1. Crie um usuário admin do domínio dentro dos usuários e dos computadores de diretório ativo. Coloque este usuário na pasta de usuários.
2. Dentro dos usuários e dos computadores de diretório ativo, selecione o **achado do** menu de ações.Certifique-se de que seus resultados mostram a coluna da membrasia do clube para o usuário criado. Seus resultados da busca devem mostrar o **usuário** e a **membrasia do clube** associada dentro do diretório ativo. Esta é a informação que você precisará de transferir no Access Manager limpo.
3. Do console de web limpo do Access Manager, vai ao **gerenciamento de usuário > aos servidores de autenticação > o** formulário **novo do server**.
4. Escolha o **LDAP** como o tipo de servidor.
5. Para o **Search(Admin) os campos baixos completos do contexto DN** e de **busca**, entraram os resultados do achado dentro dos usuários e dos computadores de diretório ativo.
6. Estes campos são tudo que é necessário para estabelecer corretamente este servidor de autenticação dentro do CAM:**ServerURL**: ldap://192.168.137.10:389 - Esta é a porta de escuta do endereço IP de Um ou Mais Servidores Cisco ICM NT e LDAP do controlador de

domínio.**Search(Admin) DN completo**: Muir de CN=sheldon, cn=Users, DC=domainname, dc=com**Contexto baixo da busca**: DC=domainname, dc=com**Papel do padrão**: Selecione o papel que do padrão um usuário será posto no autenticado uma vez.Descrição: Usado apenas para a referência.**Nome do fornecedor**: Este é o nome do servidor ldap usado para a instalação de página de usuário no CAM.**Senha da busca**: a senha de domínio dos muir do sheldon**Filtro da busca**: SAMAccountName=$user$

7. O clique **adiciona o server**.Neste momento, seu teste do AUTH deve trabalhar.
8. Autenticação de teste:**Do gerenciamento de usuário > dos servidores de autenticação > da aba do teste do AUTH**, selecione o fornecedor contra que você quer testar credenciais na lista do **fornecedor**. Se o fornecedor não aparece, certifique-se que está configurado corretamente na **lista de** aba dos **server**.Incorpore o nome de usuário e senha para o usuário e se necessário um valor do ID de VLAN.O clique **autentica**.Os resultados de teste aparecem na parte inferior do indicador.**Autenticação bem sucedida:**Para algum tipo do fornecedor, resultado: A autenticação bem sucedida e o papel do usuário são indicados quando o teste do AUTH sucede.Para server LDAP/RADIUS, quando a autenticação é bem sucedida e regras do mapeamento está configurado, os atributos/valores especificados na regra do mapeamento estão indicados igualmente se o servidor de autenticação (LDAP/RADIUS) retorna aqueles valores. Por exemplo:`Result: Authentication successful`
`Role: <role name>`
`Attributes for Mapping:`
`<Attribute Name>=<Attribute value>` **Autenticação falhada:**Quando a autenticação falha, as exibições de mensagem junto com a autenticação falharam o resultado como mostrado.

Usuários do mapa aos papéis usando os atributos ou o VLAN ID

Os formulários das regras do **mapeamento** podem ser usados para traçar usuários no papel de usuário baseado nestes parâmetros:

- O ID de VLAN do tráfego de usuário que origina do lado não confiável de CAS (todos os tipos de servidor de autenticação)
- Atributos da autenticação passados dos servidores de autenticação LDAP e de RAIO (e atributos RADIUS passados dos Cisco VPN concentratores)

Por exemplo, se você tem dois grupos de usuários na mesma sub-rede IP mas com privilégios de acesso de rede diferentes, tais como empregados wireless e estudantes, você pode usar um atributo de um servidor ldap para traçar um grupo de usuários em um papel de usuário particular. Você pode então criar políticas de tráfego para permitir o acesso de rede a um papel e para negar o acesso de rede a outros papéis.

A ferramenta NAC de Cisco executa a sequência do mapeamento como mostrado:

A ferramenta NAC de Cisco permite que o administrador especifique expressões booleanas complexas ao definir o mapeamento ordena para o Kerberos, LDAP e servidores de autenticação RADIUS. Traçando as regras são divididas em circunstâncias e você pode usar expressões booleanas para combinar os atributos do usuário múltiplo e o vlan múltiplo ID a fim traçar usuários em papéis de usuário. Traçar regras pode ser criado para uma escala de VLAN ID, e os fósforos do atributo podem ser feitos não diferenciando maiúsculas e minúsculas. Isto permite que as circunstâncias múltiplas sejam configuradas flexivelmente para uma regra do mapeamento.

Uma regra do mapeamento compreende um tipo do fornecedor do AUTH, uma expressão da

regra, e o papel de usuário em que para traçar o usuário. A expressão da regra compreende um ou uma combinação de circunstâncias que os parâmetros do usuário devem combinar para ser traçado no papel de usuário especificado. Uma circunstância é compreendida de um tipo da circunstância, de um nome do atributo da fonte, de um operador, e do valor de atributo contra que o atributo particular é combinado.

A fim criar uma regra do mapeamento, você adiciona primeiramente condições (da salvaguarda) para configurar uma expressão da regra. Então, uma vez que uma expressão da regra é criada, você pode adicionar a regra do mapeamento ao servidor de autenticação para o papel de usuário especificado.

Traçar regras pode conectar. Se uma fonte tem mais de uma regra de traço, as regras estão avaliadas na ordem em que aparecem na lista das regras do mapeamento. O papel para a primeira regra positiva do mapeamento é usado. Uma vez que uma regra é encontrada, outras regras não estão testadas. Se nenhuma regra é verdadeira, o papel do padrão para essa fonte da autenticação está usado.

Configurar a regra do mapeamento

Conclua estes passos:

1. Vá ao **gerenciamento de usuário > aos servidores de autenticação > às regras do mapeamento** e clique o link da **regra do mapeamento adicionar** para o Authentication Server.O formulário da **regra do mapeamento adicionar** aparece.
2. Configurar condições para traçar a regra (a):**Nome do fornecedor** — O nome do fornecedor ajusta os campos do formulário das regras do mapeamento para esse tipo de Authentication Server. Por exemplo, o formulário permite somente a configuração da regra do mapeamento do ID de VLAN para tipos de servidor de autenticação do Kerberos, do Windows NT, do Windows NetBIOS SSO, e S/Ident. O formulário permite a configuração da regra do mapeamento do ID de VLAN ou do atributo para o RAIO, o LDAP, e os tipos do AUTH de Cisco VPN SSO.**Tipo da circunstância** — Configurar e adicionar circunstâncias primeiramente (pisa **A na** figura) antes de adicionar a regra do mapeamento. Escolha um destes do menu dropdown a fim ajustar os campos do formulário da circunstância:**Atributo** — Para o LDAP, RAIO, fornecedores do AUTH de Cisco VPN SSO somente.**ID de VLAN** — Todos os tipos de servidor de autenticação.Para um tipo da circunstância de ID de VLAN (veja a figura), este campo é chamado **nome apropriado**. À revelia, isto é povoado com “ID de VLAN” (e desabilitado para editar).**Nome do atributo** — Para servidores ldap (veja a figura), o **nome do atributo** é um campo de texto em que você incorpora o atributo que da fonte você quer testar. O nome deve ser idêntico (diferencia maiúscula e minúscula) ao nome do atributo passado pela fonte da autenticação, a menos que você escolher os **iguais ignorar o** operador do **caso** para criar a circunstância.**Valor de atributo** — Incorpore o valor a ser testado contra o **nome do atributo da** fonte.**Operador (atributo)** — Escolha o operador que define o teste da corda do atributo da fonte:**iguais** — Retifique se o valor do **nome do atributo** combina o **valor de atributo**.**não iguais** — Retifique se o valor do **nome do atributo** não combina o **valor de atributo**.**contém** — Retifique se o valor do **nome do atributo** contém o **valor de atributo**.**começa com** — Retifique se o valor do **nome do atributo** começa com o **valor de atributo**.**extremidades com** — Retifique se o valor do **nome do atributo** termina com o **valor de atributo**.**os semelhantes ignoram o caso** — Retifique se o valor do **nome do atributo** combina a corda do **valor de atributo**. Não importa se a corda seja caixa ou

lowercase.**Operador (ID de VLAN)** — Se você escolhe o ID de VLAN como o **tipo da circunstância**, escolha um destes operadores definir uma circunstância essa testes contra inteiros do ID de VLAN:**iguais** — Retifique se o ID de VLAN combina o ID de VLAN no campo de **valor do proprietário**.**não iguais** — Retifique se o ID de VLAN não combina o ID de VLAN no campo de **valor do proprietário**.**pertence a** — Retifique se o ID de VLAN cai dentro da escala dos valores configurados para o campo de **valor do proprietário**. O valor deve ser um ou vário VLAN separado vírgula ID. As escalas de VLAN ID podem ser especificadas pelo hífen (-), por exemplo, [2,5,7,100-128,556-520]. Somente os inteiros podem ser incorporados, não cordas. Note que os suportes são opcionais.**Exemplo:Adicionar a circunstância (a condição da salvaguarda)** — Certifique-se configurar a circunstância, a seguir clique-se **adicionam a circunstância** a fim adicionar a circunstância à expressão da regra (se não sua configuração não salvar).

3. Adicionar a regra do mapeamento ao papel (b): Adicionar a regra do mapeamento (etapa **B na** figura) depois que você configurou e adicionou as circunstâncias.**Nome do papel** — Depois que você adicionou pelo menos uma circunstância, escolha o papel de usuário a que você aplicará o mapeamento do menu dropdown.**Prioridade** — Selecione uma prioridade do dropdown para determinar a ordem em que as regras do mapeamento são testadas. A primeira regra que avalia para retificar é usada para atribuir ao usuário um papel.**Expressão da regra** — A fim ajudar em configurar indicações condicionais para a regra do mapeamento, este campo indica os índices da última circunstância a ser adicionada. Após ter adicionado as circunstâncias, você deve clicar **adiciona a regra do mapeamento** a fim salvar todas as circunstâncias à regra.**Descrição** — Uma descrição opcional da regra do mapeamento.**Adicionar o mapeamento (o mapeamento da salvaguarda)** — Clique este botão quando adicionar feito condiciona para criar a regra do mapeamento para o papel. Você tem que adicionar ou salvar o mapeamento para um papel especificado, ou sua configuração e suas circunstâncias não salvar.

Edite regras do mapeamento

- **Prioridade** — A fim mudar mais tarde a prioridade de uma regra do mapeamento, clique a seta up/down ao lado da entrada no **gerenciamento de usuário > nos servidores de autenticação > na lista de server**. A prioridade determina a ordem em que as regras são testadas. A primeira regra que avalia para retificar é usada para atribuir o usuário a um papel.
- **Edite** — Clique o botão Edit ao lado da regra para alterar a regra do mapeamento, ou suprima de circunstâncias da regra. Note que ao editar uma condição composta, as condições (criado mais tarde) não estão indicadas embaixo. Esta é evitar laços.
- **Supressão** — Clique o botão Delete Button ao lado da entrada da regra do mapeamento para que um servidor de autenticação suprima dessa regra individual do mapeamento. Clique o botão Delete Button ao lado de uma circunstância no formulário da regra do mapeamento da edição para remover essa circunstância da regra do mapeamento. Note que você não pode remover uma circunstância que seja dependente de uma outra regra em uma indicação composta. A fim suprimir de uma condição individual, você tem que suprimir da condição composta primeiramente.

Troubleshooting

Se o traço do usuário AD ao papel de usuário CCA não está trabalhando, a seguir certifique-se de

que você traça usuários a um papel baseado em atributos com memberof, Operator=contains, e atributo Value= de Names= do atributo (nome do grupo).

Informações Relacionadas

- Página de suporte da ferramenta NAC de Cisco
- Suporte Técnico e Documentação - Cisco Systems