

NAC (CCA): Configurar a autenticação no Access Manager limpo (CAM) com ACS

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Etapas para configurar a autenticação no CCA com ACS](#)

[Configuração ACS](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento descreve como configurar a autenticação no Access Manager limpo (CAM) com Serviço de controle de acesso Cisco Secure (ACS). Para uma configuração similar usando ACS 5.x e mais tarde, refira [NAC \(CCA\): Configurar a autenticação no Access Manager limpo com ACS 5.x e mais tarde](#).

[Pré-requisitos](#)

[Requisitos](#)

Esta configuração é aplicável à versão 3.5 e mais recente CAM.

[Componentes Utilizados](#)

A informação neste documento é baseada na versão 4.1 CAM.

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.

[Configurar](#)

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a [Command Lookup Tool \(somente clientes registrados\)](#) para obter mais informações sobre os comandos usados nesta seção.

[Diagrama de Rede](#)

Este documento utiliza a seguinte configuração de rede:

[Etapas para configurar a autenticação no CCA com ACS](#)

Conclua estes passos:

1. **Adicionar papéis novos** Crie um papel AdminNo CAM, escolha o **gerenciamento de usuário > os papéis de usuário > papel novo**. Dê entrada com um nome exclusivo, **admin**, para o papel no campo de nome do papel. Incorpore o **papel de usuário admin** como uma descrição opcional do papel. Escolha o **papel normal do início de uma sessão** como o tipo do papel. Configurar **(OOB) o papel de usuário fora da banda** VLAN com o VLAN apropriado. Por exemplo, escolha o ID de VLAN e especifique o ID como o 10. Quando terminado, o clique **cria o papel**. A fim restaurar propriedades padrão no formulário, **restauração do clique**. O papel aparece agora na lista de aba dos papéis segundo as indicações da [etiqueta VLAN para a seção Papel-baseada OOB dos mapeamentos](#). Crie um papel de usuárioNo CAM, escolha o **gerenciamento de usuário > os papéis de usuário > papel novo**. Dê entrada com um nome exclusivo, **usuários**, para o papel no campo de nome do papel. Incorpore o **papel de usuário normal** como uma descrição opcional do papel. Configurar **(OOB) o papel de usuário fora da banda** VLAN com o VLAN apropriado. Por exemplo, escolha o ID de VLAN e especifique o ID como 20. Quando terminado, o clique **cria o papel**. A fim restaurar propriedades padrão no formulário, **restauração do clique**. O papel aparece agora na lista de aba dos papéis segundo as indicações da [etiqueta VLAN para a seção Papel-baseada OOB dos mapeamentos](#).
2. **A etiqueta VLAN para OOB Papel-baseou mapeamentos**No CAM, escolha o **gerenciamento de usuário > os papéis de usuário > a lista de papéis** a fim ver até agora a lista de papéis.
3. **Adicionar o servidor de autenticação do RAIIO (o ACS)** Escolha o **gerenciamento de usuário > os servidores de autenticação > novo**. Do menu suspenso do tipo de autenticação, escolha o **raio**. Dê entrada com o nome do fornecedor como o **ACS**. Dê entrada com o nome do servidor como **auth.cisco.com**. **Porta de servidor** — O número de porta **1812 em** que o servidor Radius está escutando. **Tipo do raio** — O método de autenticação RADIUS. Os métodos suportados incluem EAPMD5, PAP, RACHADURA, MSCHAP e MSCHAP2. **O papel do padrão** está usado se traçando ao ACS não está definido nem está ajustado corretamente, ou se o atributo RADIUS não está definido nem está ajustado corretamente no ACS. **Segredo compartilhado** — O RAIIO compartilhou do limite do segredo ao endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente especificado. **Nas-ip-address** — Este valor a ser enviado

com todos os pacotes da autenticação RADIUS. O clique **adiciona o server**.

4. **Usuários do mapa ACS aos papéis de usuário CCA** Escolha o **gerenciamento de usuário > os servidores de autenticação > traçando o > Add das regras que traça o link** a fim traçar o usuário admin no ACS ao papel de usuário admin CCA. Escolha o **gerenciamento de usuário > os servidores de autenticação > traçando o > Add das regras que traça o link** a fim traçar o usuário normal no ACS ao papel de usuário CCA. Está aqui o papel de usuário do sumário do mapeamento:
5. **Permita fornecedores alternativos na página de usuário** Escolha a **administração > páginas de usuário > > Add > índice da página de login** a fim permitir fornecedores alternativos na página do login de usuário.

Configuração ACS

1. Escolha a **configuração da interface** a fim certificar-se de que o atributo de classe [025] do RAIO (IETF) está permitido.
2. **Adicionar o cliente RADIUS ao servidor ACS** Escolha a **configuração de rede** a fim adicionar como mostrado o cliente de AAA CAM: Clique **Submit + Restart**. **Nota:** Certifique-se de que a chave do RAIO combina com o cliente de AAA e usa o RAIO (IETF). Escolha a **configuração de rede** a fim adicionar como mostrado o cliente de AAA CAS: Clique **Submit + Restart**. **Nota:** Para a contabilidade do RAIO do gateway de VPN, a política CCA deve permitir que os pacotes da contabilidade do RAIO (UDP 1646/1813) do endereço IP de Um ou Mais Servidores Cisco ICM NT de CAS passem não-autenticado ao endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor ACS. Escolha a **configuração de rede** a fim adicionar como mostrado o cliente de AAA ASA: Endereço da relação do próximo-lado PIX/ASA do usuário (tipicamente interface interna) Ajuste o tipo ao RAIO (Cisco IOS/PIX).
3. **Adicionar grupos de /Configure no servidor ACS** Crie o **admin group** Ajuste o atributo de classe [025] do RADIUS IETF para apropriar o valor de grupo. O valor deve combinar aquele configurado no traço de CAS. **Crie o grupo de usuário** Adicionar/configurar o grupo para que cada papel de usuário limpo do acesso seja traçado. **Adicionar/configurar usuários no servidor ACS** Adicionar/configurar o usuário ACS para que cada usuário limpo do acesso seja autenticado pelo ACS. Ajuste a membrasia do clube ACS. O ACS igualmente apoia a autenticação de proxy a outros servidores internos.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Na seção da monitoração ACS, você pode ver a informação nas autenticações passadas como mostrado:

Similarmente, você pode ver o tiro de tela para a contabilidade do RAIO:

Troubleshooting

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

Informações Relacionadas

- [Página de suporte da ferramenta NAC de Cisco](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)