

Exemplo de configuração da autenticação LDAP para a central UCS

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informação do recolhimento](#)

[Detalhes do usuário do ligamento](#)

[Detalhes baixos DN](#)

[Detalhes do fornecedor](#)

[Propriedade do filtro](#)

[Adicionar e configurar atributos](#)

[Adicionar o atributo de CiscoAVPair](#)

[Atualize o atributo de CiscoAVPair](#)

[Atualize o atributo predefinido](#)

[Configurar a autenticação LDAP na central UCS](#)

[Configurar o fornecedor LDAP](#)

[Configurar o grupo do fornecedor LDAP](#)

[Mude a regra nativa da autenticação](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento fornece uma configuração de exemplo para a autenticação do Lightweight Directory Access Protocol (LDAP) para a central do Cisco Unified Computing System (UCS). Os procedimentos usam a interface gráfica de usuário (GUI) central UCS, um domínio do exemplo de bgluks.com, e um nome de usuário de exemplo do usuário de teste.

Na versão 1.0 do software central UCS, o LDAP é o único protocolo de autenticação remota apoiado. A versão 1.0 tem apoio muito limitado para a autenticação remota e a configuração ldap para a central UCS própria. Contudo, você pode usar a central UCS a fim configurar todas as opções para os domínios do gerente UCS controlados pela central UCS.

As limitações da autenticação remota central UCS incluem:

- O RADIUS e o TACACS não são apoiados.

- Os grupos do mapeamento da membrasia do clube LDAP para a atribuição do papel e do fornecedor LDAP para controladores do domínio múltiplo não são apoiados.
- O LDAP usa somente o atributo de CiscoAVPair ou todo o atributo não utilizado a fim passar o papel. O papel passado é um dos papéis predefinidos no base de dados local da central UCS.
- Os domínios/protocolos da autenticação múltipla não são apoiados.

Pré-requisitos

Requisitos

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

- A central UCS é distribuída.
- O microsoft active directory é distribuído.

Componentes Utilizados

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

- Versão 1.0 da central UCS
- Microsoft active directory

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.

Recolha a informação

Esta seção resume a informação que você precisa de recolher antes que você comece a configuração.

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

Ligue detalhes do usuário

O usuário do ligamento pode ser todo o usuário LDAP no domínio que tem o acesso de leitura ao domínio; um usuário do ligamento é exigido para a configuração ldap. A central UCS usa o nome de usuário e senha do usuário do ligamento a fim conectar e assim por diante e perguntar o diretório ativo (AD) para a autenticação de usuário. Este exemplo usa a conta de administrador como o usuário do ligamento.

Este procedimento descreve como um administrador LDAP pode usar o editor das relações do serviço de diretório ativo (ADSI) a fim encontrar o DN.

1. Abra o editor ADSI.
2. Encontre o usuário do ligamento. O usuário está no mesmo trajeto que no AD.
3. Clicar com o botão direito o usuário, e escolha **propriedades**.
4. Na caixa de diálogo das propriedades, fazer duplo clique o **distinguishedName**.
5. Copie o DN do campo de valor.
6. Clique o **cancelamento** a fim fechar todos os indicadores.

Para obter a senha para o usuário do ligamento, contacte o administrador AD.

Baseie detalhes DN

A base DN é o DN da unidade organizacional (OU) ou do recipiente onde a busca para o usuário e os detalhes do usuário começa. Você pode usar o DN de um OU criado no AD para a central UCS ou UCS. Contudo, você pode encontrá-la mais simples usar o DN para a raiz do domínio próprio.

Este procedimento descreve como um administrador LDAP pode usar o editor ADSI a fim encontrar a base DN.

1. Abra o editor ADSI.
2. Encontre o OU ou o recipiente a ser usados como a base DN.
3. Clicar com o botão direito o OU ou o recipiente, e escolha **propriedades**.
4. Na caixa de diálogo das propriedades, fazer duplo clique o **distinguishedName**.
5. Copie o DN do campo de valor, e note todos os outros detalhes que você precisar.
6. Clique o **cancelamento** a fim fechar todos os indicadores.

Detalhes do fornecedor

O fornecedor joga um papel chave na autenticação LDAP e a autorização na central UCS. O fornecedor é um dos server AD que perguntas centrais UCS a fim procurar e autenticar o usuário e a fim obter detalhes do usuário tais como a informação do papel. Seja certo recolher o hostname ou o endereço IP de Um ou Mais Servidores Cisco ICM NT do server do fornecedor AD.

Filtre a propriedade

O campo ou a propriedade do filtro são usados a fim procurar o base de dados AD. O usuário - a identificação incorporada no início de uma sessão é passada de volta ao AD e comparada contra o filtro.

Você pode usar sAMAccountName=\$userid como o valor do filtro. o sAMAccountName é um atributo no AD e tem o mesmo valor como o usuário AD - a identificação, que é usada a fim entrar ao UCS GUI central.

Adicionar e configurar atributos

Esta seção resume a informação que você precisa a fim adicionar o atributo de CiscoAVPair (se

for necessário) e atualizar o atributo ou outro de CiscoAVPair, atributo predefinido antes que você comece a configuração ldap.

O campo do atributo especifica o atributo AD (sob a propriedade de usuário), que passa para trás o papel a ser atribuído ao usuário. Na liberação 1.0a do software central UCS, o atributo feito sob encomenda CiscoAVPair ou todo o outro atributo não utilizado no AD podem ser transformados a fim passar este papel.

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

[Adicionar o atributo de CiscoAVPair](#)

A fim adicionar um atributo novo ao domínio, expandir o esquema do domínio, e adicionar o atributo à classe (que, neste exemplo, é usuário).

Este procedimento descreve como expandir o esquema em um server de Windows AD e adicionar o atributo de CiscoAVPair.

1. Início de uma sessão a um server AD.
2. Clique o **Iniciar > Executar**, datilografe o **mmc**, e pressione-o **entram** a fim abrir um console vazio do Microsoft Management Console (MMC).
3. No MMC, o **> Add do arquivo do** clique/**remove Pressão-no > Add**.
4. Adicionar autônomo Pressão-na caixa de diálogo, selecione o **esquema de diretório ativo**, e o clique **adiciona**.
5. No MMC, expanda o **esquema de diretório ativo**, clicar com o botão direito **atributos**, e escolha-os **criam o atributo**.A caixa de diálogo nova do atributo da criação aparece
6. Crie um atributo nomeado CiscoAVPair no serviço de autenticação remota.Nos campos de nome do Common Name e do indicador LDAP, entre em **CiscoAVPair**.No campo original da identificação de objeto 500, incorpore **1.3.6.1.4.1.9.287247.1**.No campo de descrição, entre no **papel e no lugar UCS**.No campo da sintaxe, selecione a **corda de Unicode da** lista de drop-down.Clique a **APROVAÇÃO** a fim salvar o atributo e fechar a caixa de diálogo.O atributo é adicionado uma vez ao esquema, deve ser traçado ou incluído na classe de usuário. Isto permite que você edite a propriedade de usuário e especifique o valor o papel a ser passado.
7. No mesmo MMC usado para a expansão do esquema AD, expanda **classes**, clicar com o botão direito o **usuário**, e escolha **propriedades**.
8. Na caixa de diálogo das propriedades de usuário, clique a aba dos **atributos**, e o clique **adiciona**.
9. Na caixa de diálogo seleta do objeto do esquema, clique **CiscoAVPair**, e clique a **APROVAÇÃO**.
10. Na caixa de diálogo das propriedades de usuário, o clique **aplica-se**.
11. Clicar com o botão direito o **esquema de diretório ativo**, e escolha o **Reload o esquema** a fim incluir as mudanças novas.
12. Caso necessário, use o editor ADSI para atualizar o esquema. Clicar com o botão direito o **host local**, e escolha o **esquema da atualização agora**.

[Atualize o atributo de CiscoAVPair](#)

Este procedimento descreve como atualizar o atributo de CiscoAVPair. A sintaxe é `shell: roles= " <role>".`

1. No ADSI edite a caixa de diálogo, encontram o usuário que precisa o acesso à central UCS.
2. Clicar com o botão direito o usuário, e escolha **propriedades**.
3. Na caixa de diálogo das propriedades, clique a aba do **editor do atributo**, clicam **CiscoAVPair**, e o clique **edita**.
4. Na caixa de diálogo Multi-avaliada do editor da corda, incorpore o **shell do valor: roles= " admin" na APROVAÇÃO** do campo e do clique de valores.
5. Clique a **APROVAÇÃO** a fim salvar as mudanças e fechar a caixa de diálogo das propriedades.

Atualize o atributo predefinido

Este procedimento descreve como atualizar um atributo predefinido, onde o papel seja um dos papéis de usuário predefinidos na central UCS. Este exemplo usa a *empresa do* atributo a fim passar o papel. A sintaxe é `shell: roles= " <role>".`

1. No ADSI edite a caixa de diálogo, encontram o usuário que precisa o acesso à central UCS.
2. Clicar com o botão direito o usuário, e escolha **propriedades**.
3. Na caixa de diálogo das propriedades, clique a aba do **editor do atributo**, clicam a **empresa**, e o clique **edita**.
4. Na caixa de diálogo do editor do atributo da corda, incorpore o **shell do valor: roles= " admin" no** campo de valor, e **APROVAÇÃO do** clique.
5. Clique a **APROVAÇÃO** a fim salvar as mudanças e fechar a caixa de diálogo das propriedades.

Configurar a autenticação LDAP na central UCS

A configuração ldap na central UCS é terminada sob o Gerenciamento de operações.

1. Início de uma sessão à central UCS sob uma conta local.
2. Clique o **Gerenciamento de operações**, expanda **grupos de domínio**, e clique o **> segurança operacional das políticas**.
3. A fim configurar a autenticação LDAP, tome estas etapas: [Configurar o fornecedor LDAP](#). [Configurar o grupo do fornecedor LDAP](#) (não disponível na liberação 1.0a). [Mude a regra nativa da autenticação](#).

Configurar o fornecedor LDAP

1. Clique o **LDAP**, clicar com o botão direito **fornecedores**, e escolha-os **criam o fornecedor LDAP**.
2. Na caixa de diálogo do fornecedor da criação LDAP, adicionar estes detalhes, que foram recolhidos mais cedo. Hostname ou IP do fornecedor Ligamento DNBase DN Filtro Atributo (CiscoAVPair ou um atributo predefinido tal como a empresa Senha (senha do usuário usado no ligamento DN)
3. Clicam a **APROVAÇÃO** a fim salvar a configuração e fechar a caixa de diálogo.

Nota: Nenhum outro valor precisa de ser alterado nesta tela. As regras do grupo LDAP não são

apoiadas para a autenticação central UCS nesta liberação.

Configurar o grupo do fornecedor LDAP

Nota: Na liberação 1.0a, os grupos do fornecedor não são apoiados. Este procedimento descreve como configurar um grupo do fornecedor do manequim para usar-se mais tarde na configuração.

1. Clique o **LDAP**, clicar com o botão direito o **grupo do fornecedor**, e escolha-o **criam o grupo do fornecedor LDAP**.
2. Na caixa de diálogo do grupo do fornecedor da criação LDAP, dê entrada com o nome para o grupo no campo de nome.
3. Da lista de fornecedores disponíveis à esquerda, selecione o fornecedor, e clique o maior do que o símbolo (>) a fim mover esse fornecedor para fornecedores atribuídos à direita.
4. Clique a **APROVAÇÃO** a fim salvar as mudanças e fechar a tela.

Mude a regra nativa da autenticação

A liberação 1.0a não apoia domínios da autenticação múltipla como no gerente UCS. A fim trabalhar em torno disto, você precisa de alterar a regra nativa da autenticação.

A autenticação nativa tem a opção para alterar a autenticação para inícios de uma sessão ou consoles de login do padrão. Desde que os domínios múltiplos não são apoiados, você pode usar a conta local ou uma conta LDAP, mas não ambos. Mude o valor do reino a fim usar o local ou o LDAP como a fonte de autenticação.

1. Clique a **autenticação**, clicar com o botão direito a **autenticação nativa**, e escolha **propriedades**.
2. Determine se você quer a autenticação padrão, a autenticação do console, ou ambos. Use a autenticação padrão para o GUI e o comando line interface(cli). Use a autenticação do console para a opinião núcleo-baseada virtual de máquina virtual de máquina (VM) (KVM).
3. Escolha o **ldap da** lista de drop-down do reino. O valor do reino determina se o local ou o LDAP são a fonte de autenticação.
4. **APROVAÇÃO** do clique a fim fechar a página.
5. Nas políticas pagine, clique a **salv guarda** se for necessário a fim salvar as mudanças.

Nota: Não faz a saída de sua sessão atual ou para alterar a autenticação do console até que você verifique que a autenticação LDAP trabalha corretamente. A autenticação do console fornece uma maneira de reverter à configuração precedente. Refira a seção da [verificação](#).

Verificar

Este procedimento descreve como testar a autenticação LDAP.

1. Abra uma sessão nova na central UCS, e incorpore o nome de usuário e senha. Você não precisa de incluir um domínio ou um caráter antes do username. Este exemplo usa testucs como o usuário do domínio.
2. A autenticação LDAP é bem sucedida se você vê o painel da central UCS. O usuário é indicado na parte inferior da página.

Troubleshooting

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

Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)