Configurar o ISE para a integração com um servidor ldap

Índice

Introdução

Este documento descreve como configurar um Cisco Identity Services Engine (ISE) para a integração com um server do Directory Access Protocol da leve Cisco (LDAP).

> **Note**: Este documento é válido para as instalações que usam o LDAP como a fonte externo da identidade para a authentication e autorização ISE.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação este documento é baseada nestes versão de software e hardware:

- Versão 1.3 de Cisco ISE com correção de programa 2
- A versão 7 x64 de Microsoft Windows com OpenLDAP instalou
- Versão 8.0.100.0 do controlador de LAN do Cisco Wireless (WLC)
- Versão 3.1 de Cisco AnyConnect para Microsoft Windows
- Editor do perfil do Access Manager da rede Cisco

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.

Informações de Apoio

Estes métodos de autenticação são apoiados com LDAP:

- Placa de token genérica do do Â do âÂ do protocolo extensible authentication (EAP-GTC)
- Transport Layer Security do do Â do âÂ do protocolo extensible authentication (EAP-TLS)
- Transport Layer Security protegido do do Â do âÂ do protocolo extensible authentication (PEAP-TLS)

Configurar

Esta seção descreve como configurar os dispositivos de rede e integrar o ISE com um servidor ldap.

Diagrama de Rede

Neste exemplo de configuração, o valor-limite usa um adaptador Wireless a fim associar com a rede Wireless. O Wireless LAN (WLAN) no WLC é configurado a fim autenticar os usuários através do ISE. No ISE, o LDAP é configurado como uma loja externo da identidade.

Esta imagem ilustra a topologia de rede que é usada:

Configurar OpenLDAP

A instalação do OpenLDAP para Microsoft Windows é terminada através do GUI, e é direta. O local padrão é **C: > OpenLDAP**. Após a instalação, você deve ver este diretório:

Tome uma nota de dois diretórios em particular:

- O do Â do âÂ de **ClientTools** este diretório inclui um grupo de binários que são usados a fim editar o base de dados LDAP.

- o do Â do âÂ do **ldifdata** isto é o lugar em que você deve armazenar os arquivos com objetos LDAP.

Adicionar esta estrutura ao base de dados LDAP:

Sob o *diretório raiz*, você deve configurar duas unidades organizacionais (OU). *O OU=groups* OU deve ter um grupo filho (**cn=domainusers n**este exemplo). *O OU=people* OU define as duas contas de usuário que pertencem ao grupo dos *cn=domainusers*.

A fim povoar o base de dados, você deve criar o arquivo do *ldif* primeiramente. A estrutura previamente mencionada foi criada deste arquivo:

```
dn: ou=groups,dc=maxcrc,dc=com
changetype: add
ou: groups
description: All groups in organisation
objectclass: organizationalunit

dn: ou=people,dc=maxcrc,dc=com
changetype: add
ou: people
description: All people in organisation
objectclass: organizationalunit

dn: uid=john.doe,ou=people,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: john.doe
givenName: John
sn: Doe
cn: John Doe
mail: john.doe@example.com
userPassword: password

dn: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: jan.kowalski
givenName: Jan
sn: Kowalski
cn: Jan Kowalski
mail: jan.kowalski@example.com
userPassword: password

dn: cn=domainusers,ou=groups,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: posixGroup
gidNumber: 678
memberUid: uid=john.doe,ou=people,dc=maxcrc,dc=com
memberUid: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com
```

A fim adicionar os objetos ao base de dados LDAP, você pode usar o binário do **ldapmodify**:

```
C:\OpenLDAP\ClientTools>ldapmodify.exe -a -x -h localhost -p 389 -D "cn=Manager,
dc=maxcrc,dc=com" -w secret -f C:\OpenLDAP\ldifdata\test.ldif
ldap_connect_to_host: TCP localhost:389
ldap_new_socket: 496
ldap_prepare_socket: 496
ldap_connect_to_host: Trying ::1 389
ldap_pvt_connect: fd: 496 tm: -1 async: 0
attempting to connect:
connect success
adding new entry "ou=groups,dc=maxcrc,dc=com"

adding new entry "ou=people,dc=maxcrc,dc=com"

adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com"

adding new entry "uid=jan.kowalski,ou=people,dc=maxcrc,dc=com"

adding new entry "cn=domainusers,ou=groups,dc=maxcrc,dc=com"
```

Integre OpenLDAP com o ISE

Use a informação que é fornecida nas imagens durante todo esta seção a fim configurar o LDAP como uma loja externo da identidade no ISE.

Você pode configurar estes atributos do *tab geral*:

- O **sujeito do** Â do âÂ de **Objectclass** este campo corresponde à classe de objeto das contas de usuário no arquivo do *ldif*. Conforme a configuração ldap, você pode usar uma de quatro classes aqui:

  Superior

  Pessoa

  OrganizationalPerson

  InetOrgPerson

- O do Â do âÂ do **atributo de nome do sujeito** isto é o atributo que está recuperado pelo LDAP quando o ISE inquire se um nome de usuário específico está incluído em um base de dados. Nesta encenação, você deve usar **john.doe ou** jan.kowalskias o nome de usuário no valor-limite.

- O do Â do âÂ de **Objectclass do grupo** este campo corresponde à classe de objeto para um grupo no arquivo do *ldif*. Nesta encenação, a classe de objeto para o grupo dos *cn=domainusers* é **posixGroup**.

- O do Â do âÂ do **atributo do mapa do grupo** este atributo define como os usuários são

traçados aos grupos. Sob o grupo dos *cn=domainusers no* arquivo do *ldif*, você pode ver dois atributos do *memberUid* que correspondem aos usuários.

O ISE igualmente oferece alguns esquemas PRE-configurados (microsoft ative directory, Sun, Novell):

Depois que você ajusta o endereço IP de Um ou Mais Servidores Cisco ICM NT e o nome corretos do campo administrativo, você pode *testar o ligamento ao* server. Neste momento, você não deve recuperar nenhuns assuntos ou grupos porque as bases da busca não são configuradas ainda.

Na aba seguinte, você pode configurar a base da busca do assunto/grupo. Este é o ponto da *junta* para o ISE ao LDAP. Você pode recuperar somente os assuntos e os grupos que são crianças de seu ponto de junta. Nesta encenação, os assuntos do *OU=people* e os grupos do *OU=groups* são recuperados:

Dos grupos aba, você pode importar os grupos do LDAP no ISE:

Configurar o WLC

Use a informação que é fornecida nestas imagens a fim configurar o WLC para a autenticação do 802.1x:

Configurar o EAP-GTC

Um dos métodos de autenticação apoiados para o LDAP é EAP-GTC. Está disponível em Cisco AnyConnect, mas você deve instalar o editor do perfil do gerente do acesso de rede a fim configurar corretamente o perfil. Você deve igualmente editar a configuração de gerenciador do acesso de rede, que é encontrada à revelia aqui:

C : > ProgramData > Cisco > Cliente de mobilidade Cisco AnyConnect Secure > gerente do acesso de rede > sistema > arquivo configuration.xml

Use a informação que é fornecida nestas imagens a fim configurar o EAP-GTC no valor-limite:

Use a informação que é fornecida nestas imagens a fim mudar as políticas da authentication e autorização no ISE:

Depois que você aplica a configuração, você deve poder conectar à rede:

Verificar

A fim verificar as configurações LDAP e ISE, você deve poder recuperar os assuntos e os grupos com uma conexão de teste ao server:

Estas imagens ilustram um relatório da amostra do ISE:

Troubleshooting

Esta seção descreve alguns erros comuns que são encontrados com esta configuração e como os pesquisar defeitos:

- Após a instalação do OpenLDAP, você pôde encontrar um erro para indicar que um **gssapi.dll falta**. A fim eliminar o erro, você deve reiniciar o Microsoft windows.

- Não pôde ser possível editar diretamente o *arquivo configuration.xml* para Cisco AnyConnect. Salvar sua configuração nova em um outro lugar e use-a então para substituir o arquivo velho.

- No relatório da autenticação, você pôde ver este Mensagem de Erro:

  `Authentication method is not supported by any applicable identity store`
  Este Mensagem de Erro indica que o método que você escolheu não está apoiado pelo LDAP. Assegure-se de que o *protocolo de autenticação no* mesmo relatório mostre um dos métodos suportados (EAP-GTC, EAP-TLS, ou PEAP-TLS).

- No relatório da autenticação, você pôde observar que o assunto não esteve encontrado na loja da identidade. Isto significa que o nome de usuário do relatório não combina o *atributo de nome do sujeito* para nenhum usuário no base de dados LDAP. Nesta encenação, o valor foi ajustado ao **uid** para este atributo, assim que significa que o ISE olha aos valores do *uid* para o usuário LDAP quando tenta encontrar um fósforo.

- Os assuntos e os grupos não puderam ser recuperados corretamente durante um *ligamento ao* teste do *server*. A maioria de causa provável desta edição é uma configuração incorreta para as bases da busca. Recorde que a hierarquia LDAP deve ser especificada da folha-à-raiz e da *C.C.* (pode consistir em palavras múltiplas).

  Tip: A fim pesquisar defeitos a autenticação de EAP no lado WLC, refira a autenticação de EAP com documento Cisco do exemplo de configuração dos controladores de WLAN (WLC).