Configure el ISE para la integración con un servidor LDAP

Contenido

Introducción

Este documento describe cómo configurar un Cisco Identity Services Engine (ISE) para la integración con un servidor del Directory Access Protocol de las livianas de Cisco (LDAP).

> Nota: Este documento es válido para las configuraciones que utilizan el LDAP como la fuente externa de la identidad para la autenticación y autorización ISE.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información este documento se basa en estas versiones de software y hardware:

- Versión 1.3 de Cisco ISE con la corrección 2
- La versión 7 x64 de Microsoft Windows con OpenLDAP instaló
- Versión 8.0.100.0 del controlador LAN de la tecnología inalámbrica de Cisco (WLC)
- Versión 3.1 de Cisco AnyConnect para Microsoft Windows
- Editor del perfil del Access Manager de la red de Cisco

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Estos métodos de autentificación se soportan con el LDAP:

- Placa Token genérica del del Â del âÂ del protocolo extensible authentication (EAP-GTC)
- Transport Layer Security (EAP-TLS) del Â del âÂ del protocolo extensible authentication
- protegido Transport Layer Security (PEAP-TLS) del Â del âÂ del protocolo extensible authentication

Configurar

Esta sección describe cómo configurar los dispositivos de red e integrar el ISE con un servidor LDAP.

Diagrama de la red

En este ejemplo de configuración, el punto final utiliza un adaptador de red inalámbrica para asociarse a la red inalámbrica. El Wireless LAN (red inalámbrica (WLAN)) en el WLC se configura para autenticar a los usuarios vía el ISE. En el ISE, el LDAP se configura como almacén externo de la identidad.

Esta imagen ilustra la topología de red se utiliza que:

Configuración OpenLDAP

La instalación del OpenLDAP para Microsoft Windows se completa vía el GUI, y es directa. La ubicación predeterminada es **C: > OpenLDAP**. Después de la instalación, usted debe ver este directorio:

Tome la nota de dos directorios particularmente:

- El del Â del âÂ de **ClientTools** este directorio incluye un conjunto de binaries que se utiliza para editar la base de datos de LDAP.

- el del Â del âÂ del **ldifdata** esto es la ubicación en la cual usted debe salvar los archivos con los objetos LDAP.

Agregue esta estructura a la base de datos de LDAP:

Conforme al *directorio raíz*, usted debe configurar dos unidades organizativas (OU). *El OU=groups* OU debe tener un grupo derivado (**cn=domainusers** en este ejemplo). *El OU=people* OU define las dos cuentas de usuario que pertenecen al grupo de los *cn=domainusers*.

Para poblar la base de datos, usted debe crear el archivo del *ldif* primero. La estructura previamente mencionada fue creada de este archivo:

```
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
```

Para agregar los objetos a la base de datos de LDAP, usted puede utilizar el binario del

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 con el ISE

Utilice la información que se proporciona en las imágenes en esta sección para configurar el LDAP como almacén externo de la identidad en el ISE.

Usted puede configurar estos atributos de la *ficha general*:

- El **sujeto del** Â del âÂ de **Objectclass** este campo corresponde a la clase de objeto de las cuentas de usuario en el archivo del *ldif*. Según la Configuración LDAP, usted puede utilizar una de cuatro clases aquí:

  Arriba

  Persona

  OrganizationalPerson

  InetOrgPerson

- El del Â del âÂ del **atributo de asunto** esto es el atributo que es extraído por el LDAP cuando el ISE investiga si un Nombre de usuario específico está incluido en una base de datos. En este escenario, usted debe utilizar **john.doe o** jan.kowalskias el Nombre de usuario en el punto final.

- El del Â del âÂ de **Objectclass del grupo** este campo corresponde a la clase de objeto para un grupo en el archivo del *ldif*. En este escenario, la clase de objeto para el grupo de los *cn=domainusers* es **posixGroup**.

- El del Â del âÂ del **atributo del mapa del grupo** este atributo define cómo asocian a los

usuarios a los grupos. Bajo grupo de los *cn=domainusers* en el archivo del *ldif*, usted puede ver dos atributos del *memberUid* que correspondan a los usuarios.

El ISE también ofrece algunos esquemas preconfigurados (Microsoft Active Directory, Sun, Novell):

Después de que usted fije la dirección IP y el nombre correctos del dominio administrativo, usted puede *probar el lazo al* servidor. En este momento, usted no debe extraer ningunos temas o grupos porque las bases de la búsqueda todavía no se configuran.

En la lengueta siguiente, usted puede configurar la base de la búsqueda del tema/del grupo. Ésta es la punta del *unido* para el ISE al LDAP. Usted puede extraer solamente los temas y a los grupos que son niños de su punta que se une a. En este escenario, extraen a los temas del *OU=people* y a los grupos del *OU=groups*:

De los grupos lengueta, usted puede importar a los grupos del LDAP en el ISE:

Configure el WLC

Utilice la información que se proporciona en estas imágenes para configurar el WLC para la autenticación del 802.1x:

Configure el EAP-GTC

Uno de los métodos de autentificación soportados para el LDAP es EAP-GTC. Está disponible en Cisco AnyConnect, pero usted debe instalar el editor del perfil del administrador del acceso a la red para configurar el perfil correctamente. Usted debe también editar la configuración de administrador del acceso a la red, que por abandono se localiza aquí:

C: > ProgramData > Cisco > Cliente de movilidad Cisco AnyConnect Secure > administrador del acceso a la red > sistema > archivo configuration.xml

Utilice la información que se proporciona en estas imágenes para configurar el EAP-GTC en el punto final:

Utilice la información que se proporciona en estas imágenes para cambiar las directivas de la autenticación y autorización en el ISE:

Después de que usted aplique la configuración, usted debe poder conectar con la red:

Verificación

Para verificar las configuraciones LDAP y ISE, usted debe poder extraer los temas y a los grupos con una conexión de prueba al servidor:

Estas imágenes ilustran un informe de la muestra del ISE:

Troubleshooting

Esta sección describe algunos errores comunes que se encuentren con esta configuración y cómo resolverlos problemas:

- Después de la instalación del OpenLDAP, usted puede ser que encuentre un error para indicar que un **gssapi.dll falta**. Para eliminar el error, usted debe recomenzar el Microsoft Windows.

- Puede ser que no sea posible editar el *archivo configuration.xml* para Cisco AnyConnect directamente. Salve su nueva configuración en otra ubicación y después utilícela para substituir el viejo archivo.

- En el informe de la autenticación, usted puede ser que vea este mensaje de error: `Authentication method is not supported by any applicable identity store`Este mensaje de error indica que el método que usted escogió no es soportado por el LDAP. Asegúrese de que el *protocolo de autenticación* en el mismo informe muestre uno de los métodos aceptados (EAP-GTC, EAP-TLS, o PEAP-TLS).

- En el informe de la autenticación, usted puede ser que note que el tema no fue encontrado en el almacén de la identidad. Esto significa que el Nombre de usuario del informe no hace juego el *atributo de asunto* para ningún usuario en la base de datos de LDAP. En este escenario, el valor fue fijado al **uid** para este atributo, así que significa que el ISE mira a los valores del *uid* para el usuario LDAP cuando intenta encontrar una coincidencia.

- Los temas y los grupos no pudieron ser extraídos correctamente durante un *lazo a la* prueba del *servidor*. La mayoría de la causa probable de este problema es una configuración incorrecta para las bases de la búsqueda. Recuerde que la jerarquía LDAP se debe especificar de la hoja-a-raíz y de la *C.C.* (puede consistir en las palabras múltiples).

  Consejo: Para resolver problemas la autenticación EAP en el lado del WLC, refiera a la autenticación EAP con el documento de Cisco del ejemplo de configuración de los controladores de WLAN (WLC).