配置集成的ISE用LDAP服务器

目录

简介

本文描述如何配置一思科身份服务引擎(ISE)集成的用思科轻量级目录访问协议(LDAP)服务器。

> **注意**：本文为使用LDAP作为外部标识来源ISE认证和授权的设置是有效。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

信息本文根据这些软件和硬件版本：

- Cisco与补丁程序2的ISE版本1.3
- 与安装的OpenLDAP的Microsoft Windows版本7 x64

- Cisco无线LAN控制器(WLC)版本8.0.100.0
- Microsoft Windows的Cisco AnyConnect版本3.1
- Cisco网络接入管理器配置文件编辑器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

这些认证方法支持与LDAP ：

- 可扩展的认证协议âÂ Â 通用的令牌卡(EAP-GTC)
- 可扩展的认证协议âÂ Â 传输层安全(EAP-TLS)
- 已保护可扩展的认证协议âÂ Â 传输层安全(PEAP-TLS)

配置

此部分描述如何配置网络设备和集成ISE用LDAP服务器。

网络图

在本例中配置示例，终端使用一个无线适配器为了与无线网络产生关联。在WLC的无线局域网(WLAN)配置为了通过ISE验证用户。在ISE， LDAP配置作为外部标识存储。

此镜像说明使用的网络拓扑：

配置OpenLDAP

OpenLDAP的安装Microsoft Windows的通过GUI完成，并且是直接的。默认位置是**C ：> OpenLDAP**。在安装以后，您应该看到此目录：

特别是注意到两个目录：

- **ClientTools** âÂ Â 此目录包括使用为了编辑LDAP数据库的一套二进制。
- **ldifdata** âÂ Â 这是您应该存储有LDAP对象的文件的位置。

添加此结构到LDAP数据库：

在*根目录下*，您必须配置两个组织单位(OU)。*OU=groups* OU应该有一个子组(在本例中的**cn=domainusers**)。*OU=people* OU定义了属于*cn=domainusers*组的两个用户帐户。

为了填充数据库，您必须首先创建*ldif*文件。以前被提及的结构从此文件创建：

```
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
```

为了添加对LDAP数据库的对象，您能使用**ldapmodify**二进制：

```
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"
```

集成与ISE的OpenLDAP

请使用在此部分中的镜像被提供为了配置LDAP作为ISE的外部标识存储的信息。

您能配置从*常规选项卡的*这些属性：

- **附属的Objectclass** âÂ Â 此字段对应于用户帐户的对象类在*ldif*文件的。根据IDAP配置，您能使用四类之一这里：

  顶部

  人

  OrganizationalPerson

  InetOrgPerson

- **主题名称属性**âÂ Â 这是由LDAP获取的属性，当ISE询问时一个特定用户名是否在数据库包括。在此方案中，您必须使用**john.doe或**jan.kowalskias在终端的用户名。

- **组Objectclass** âÂ Â 此字段对应于一组的对象类*ldif*文件的。在此方案中， *cn=domainusers*组的对象类是**posixGroup**。

- **组地图属性**âÂ Â 此属性定义了用户如何被映射给组。在*ldif*文件的*cn=domainusers*组下，您能看到对应于用户的两个*memberUid*属性。

ISE也提供一些预先配置的模式(Microsoft Active Directory， Sun， Novell) ：

在您设置正确IP地址和管理域名称后，您能*测试捆绑*到服务器。这时，因为搜索基础没有配置，您不应该检索任何主题或组。

在Next选项，您能配置附属/组搜索库。这是ISE的*加入*点对LDAP。您能检索是您加入的点的孩子仅的主题和组。在此方案中，从*OU=people的*主题和从*OU=groups的*组被检索：

从*组*选项卡，您能导入从LDAP的组在ISE ：

配置 WLC

请使用在这些镜像被提供为了配置802.1x验证的WLC的信息：

配置EAP-GTC

其中一LDAP的支持的认证方法是EAP-GTC。它在思科AnyConnect中是可用的，但是您必须安装网

络访问管理器配置文件编辑器为了正确地配置配置文件。您必须也编辑网络访问管理器配置，默认情况下查找此处：

C ：> ProgramData > Cisco> Cisco AnyConnect安全移动客户端>网络访问Manager>系统> configuration.xml文件

请使用在这些镜像被提供为了配置在终端的EAP-GTC的信息：

请使用在这些镜像被提供为了更改在ISE的认证和授权策略的信息：

在您运用配置后，您应该能连接到网络：

验证

为了验证LDAP和ISE配置，您应该能检索主题和组有测试连接的对服务器：

这些镜像说明从ISE的一示例报告：

故障排除

此部分描述遇到与此配置和如何排除故障他们的一些常见错误：

- 在OpenLDAP的安装以后，您也许遇到错误表明**gssapi.dll**未命中。为了排除错误，您必须重新启动Microsoft Windows.
- 直接地编辑思科的AnyConnect *configuration.xml文件*也许是不可能的。在另一个位置保存您新的配置然后请使用它替换旧有文件。
- 在验证报告，您也许发现此错误消息：
  `Authentication method is not supported by any applicable identity store`此错误消息表明您选择LDAP不支持的方法。保证在同一报告的*认证协*议显示其中一支持的方法(EAP-GTC、EAP-TLS或者PEAP-TLS)。
- 在验证报告，您也许注意主题未在标识存储被找到。这意味着从报告的用户名不匹配任何用户的*主题名称属性*LDAP数据库的。在此方案中，值设置为此属性的**uid**，因此意味着ISE查找对*uid*值为LDAP用户，当尝试查找匹配时。
- 主题和组也许不正确地被检索在*捆绑期间服务器测试的*。此问题的多数可能原因是搜索基础的一个不正确的配置。切记必须从分支对根和*dc*指定LDAP层级(能包括多个词)。

  提示：为了排除故障在WLC侧的EAP验证，参考与WLAN控制器(WLC)配置示例Cisco文档的EAP验证。