使用在Cisco IOS头端配置示例的LDAP的AnyConnect客户端的策略组分配

目录

简介

本文描述如何配置轻量级目录访问协议(LDAP)属性地图自动地分配正确VPN策略到根据他们的凭证的用户。

> **Note**:LDAP认证的支持连接对Cisco IOS头端的安全套接字协议层VPN (SSL VPN)用户的由Cisco Bug ID CSCuj20940跟踪。直到支持正式被添加， LDAP支持是尽力。

先决条件

要求

Cisco 建议您了解以下主题：

- 在Cisco IOS的SSL VPN
- 在Cisco IOS的LDAP认证
- 目录服务

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CISCO881-SEC-K9
- Cisco IOS软件， C880软件(C880DATA-UNIVERSALK9-M)，版本15.1(4)M，发行软件(fc1)

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

LDAP是访问和保养在网络协议(IP)网络的分布式目录信息服务的一个开放，供应商中立，工业标准应用协议。当他们允许共享关于用户、系统、网络、服务和应用程序的信息在网络中，目录服务播放在内联网和互联网应用程序的开发的一重要的角色。

管理员需要经常为 VPN 用户提供不同的访问权限或 WebVPN 内容。这可以完成与不同的VPN策略的这些策略集的配置在VPN服务器的和分配对每个用户的从属在他们的凭证。当这可以手工时完成，它是自动化与目录服务的进程的更有效的。为了使用LDAP分配组策略对用户，您需要配置映射一个LDAP属性例如激活目录(AD)属性“memberOf”对属性由VPN头端了解的地图。

在可适应安全工具(ASA)上如ASA使用LDAP属性地图配置示例所显示，这通过不同的组策略的分配对不同的用户的有规律地达到用LDAP属性地图。

在Cisco IOS同一件事可以用不同的策略组的配置在WebVPN上下文下的和使用LDAP属性地图完成为了确定哪个策略组用户将分配。在Cisco IOS头端，“memberOf” AD属性被映射给验证、授权和统计(AAA)属性请求方组。使用动态属性地图配置示例，欲了解更详细的信息在省缺属性映射，请参阅在IOS设备的LDAP。然而对于SSL VPN，有两相关AAA属性映射：

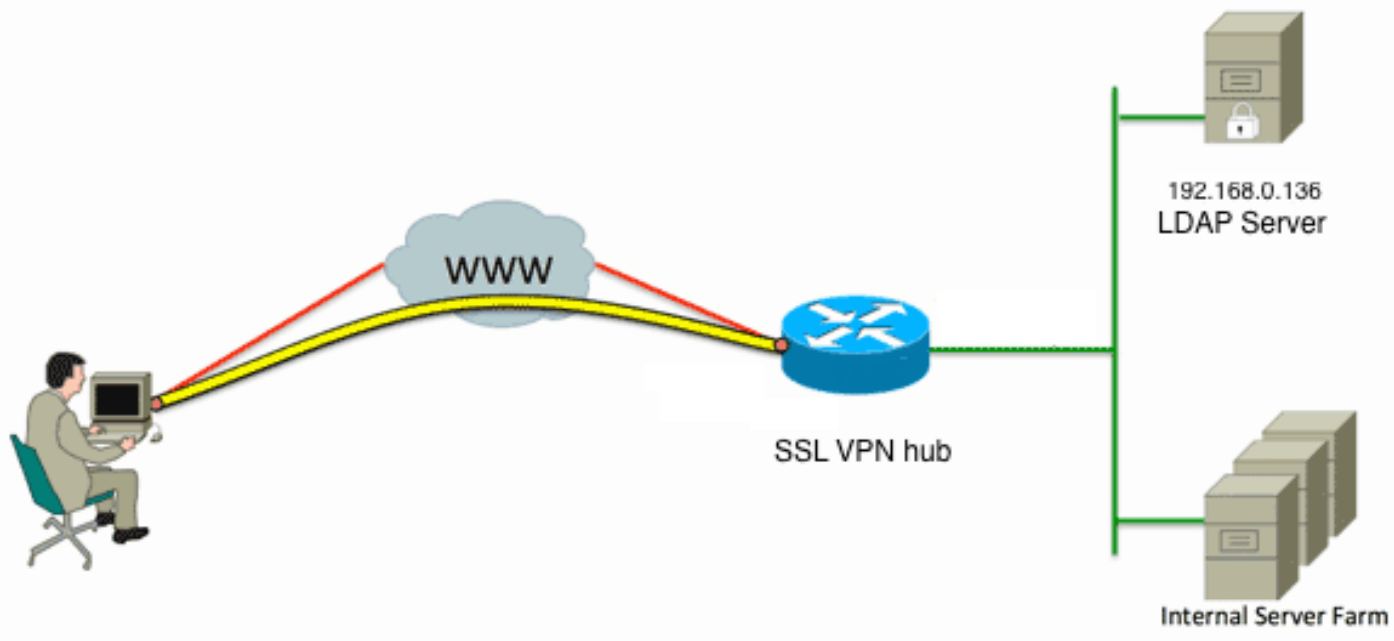
AAA属性名称	SSL VPN相关性
用户VPN组	对策略组的地图定义在WebVPN上下文下
WebVPN上下文	对实际WebVPN上下文的地图

所以LDAP属性地图需要映射相关LDAP属性到二者之一这两个AAA属性之一。

配置

> **Note**:使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图



此配置使用一张LDAP属性地图为了映射“memberOf” LDAP属性对AAA属性用户VPN组。

1. 配置认证方法和AAA服务器组。

```
aaa new-model
!
!
aaa group server ldap AD
 server DC1
!
aaa authentication login default local
aaa authentication login vpn local
aaa authentication login AD group ldap local
aaa authorization exec default local
```

2. 配置LDAP属性地图。

```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group
```

3. 配置参考上一个LDAP属性地图的LDAP服务器。

```
ldap server DC1
 ipv4 192.168.0.136
 attribute map ADMAP
 bind authenticate root-dn CN=Cisco Systems,OU=Service Accounts,DC=chillsthrills,
DC=local password 7 <removed>
 base-dn DC=chillsthrills,DC=local
```

4. 配置路由器作为WebVPN服务器。在本例中，因为“memberOf”属性将被映射对“用户VPN组”属性，单个WebVPN上下文配置与包括“NOACCESS”策略的多项策略组。此策略组是为没有一个匹配的“memberOf”值的用户。

```
ip local pool vpnpool 192.168.200.200 192.168.200.250
!
webvpn gateway gateway_1
 hostname vpn
 ip address 173.11.196.220 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-2564112419
 logging enable
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-2.5.2019-k9.pkg sequence 1
 !
webvpn install csd flash:/webvpn/sdesktop.pkg
 !
```

```
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
  hide-url-bar
  timeout idle 60
  timeout session 1
 !
 !
 policy group CN=T,OU=MyBusiness,DC=chillsthrills,DC=local
  functions svc-enabled
  banner "special access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
   svc split include 192.168.0.0 255.255.255.0
   svc split include 10.10.10.0 255.255.255.0
   svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

警告

1. 如果用户是“memberOf”多个组，路由器使用第一个“memberOf”值。
2. 什么是多的在此配置方面是策略组的名称必须是“memberOf值的” LDAP服务器推送的**完整**字符串的完全匹配。通常管理员使用更短和更加相关的名称策略组，例如VPNACCESS，但是除表面问题外这可能导致一更大的问题。显著地大于“memberOf”属性字符串是不不常见的什么用于此示例。例如，请考虑此调试消息：

```
ip local pool vpnpool 192.168.200.200 192.168.200.250
!
webvpn gateway gateway_1
 hostname vpn
 ip address 173.11.196.220 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-2564112419
 logging enable
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-2.5.2019-k9.pkg sequence 1
 !
webvpn install csd flash:/webvpn/sdesktop.pkg
 !
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
```

```
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
  hide-url-bar
  timeout idle 60
  timeout session 1
 !
 !
 policy group CN=T,OU=MyBusiness,DC=chillsthrills,DC=local
  functions svc-enabled
  banner "special access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
   svc split include 192.168.0.0 255.255.255.0
   svc split include 10.10.10.0 255.255.255.0
   svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

它清楚显示从AD接收的字符串是：

```
"CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,DC=chillsthrills,DC=local"
```

然而，因为没有定义的这样策略组，如果管理员设法配置这样组策略导致错误，因为Cisco IOS有在字符数量的一限制在策略组组名：

```
"CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,DC=chillsthrills,DC=local"
```

在这些情况下有两可能的应急方案：

1. 请使用一个不同的LDAP属性，例如“部门”。考虑此LDAP属性地图：

```
"CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,DC=chillsthrills,DC=local"
```

在这种情况下部门属性的值用户的可以设置为一个值例如VPNACCESS，并且WebVPN配置有点更加简单：

```
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
 !
 policy group VPNACCESS
  functions svc-enabled
  banner "access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
  svc split include 192.168.0.0 255.255.255.0
  svc split include 10.10.10.0 255.255.255.0
  svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
```

```
 inservice
!
end
```

2. 请使用DN对字符串关键字在LDAP属性地图。如果上一个应急方案不是适当的那么管理员在LDAP属性地图能使用DN对字符串关键字为了解压缩从“memberOf”字符串的共同名称(CN)值。在此方案中LDAP属性地图是：

```
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
 !
 policy group VPNACCESS
  functions svc-enabled
  banner "access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
  svc split include 192.168.0.0 255.255.255.0
  svc split include 10.10.10.0 255.255.255.0
  svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

并且WebVPN配置是：

```
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
 !
 policy group VPNACCESS
  functions svc-enabled
  banner "access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
  svc split include 192.168.0.0 255.255.255.0
  svc split include 10.10.10.0 255.255.255.0
  svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
```

```
end
```

Note:因此不同于在您能使用**Map值**命令在属性地图下为了匹配从LDAP服务器接收的值到若干其他局部重要的值的ASA， Cisco IOS头端没有此选项并且是没有如灵活。归档Cisco Bug ID CSCts31840为了寻址此。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

- **show ldap属性**
- **show ldap server全部**

故障排除

本部分提供了可用于对配置进行故障排除的信息。

Note:使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

为了排除故障LDAP属性映射，请启用这些调试：

- **调试ldap全部**
- **调试ldap事件**
- **debug aaa authentication**
- **debug aaa authorization**