在Cisco IOS头端上使用LDAP的AnyConnect客户端的策略组分配配置示例

目录

简介

本文档介绍如何配置轻量级目录访问协议(LDAP)属性映射，以便根据用户的凭证自动向用户分配正确的VPN策略。

> **注意**：Cisco Bug ID CSCuj20940将跟踪对连接到Cisco IOS®头端的安全套接字层VPN(SSL VPN)用户的LDAP身份验证的支持。在正式添加支持之前，LDAP支持是最大努力。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科IOS上的SSL VPN
- 思科IOS上的LDAP身份验证
- 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
- 思科IOS软件，C880软件(C880DATA-UNIVERSALK9-M)，版本15.1(4)M，版本软件(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是开放的、供应商中立的行业标准应用协议，用于通过Internet协议(IP)网络访问和维护分布式目录信息服务。目录服务在内部网和Internet应用程序的开发中发挥着重要作用，因为它们允许在整个网络中共享有关用户、系统、网络、服务和应用程序的信息。

管理员需要经常为 VPN 用户提供不同的访问权限或 WebVPN 内容。这可以通过在VPN服务器上配置不同的VPN策略和根据用户凭证将这些策略集分配给每个用户来完成。虽然这可以手动完成，但使用目录服务自动执行流程会更加高效。要使用LDAP向用户分配组策略，您需要配置映射，将LDAP属性(如Active Directory(AD)属性“memberOf”)映射到VPN头端所理解的属性。

在自适应安全设备(ASA)上，通过向不同用户分配不同的组策略，并使用LDAP属性映射，如ASA使用LDAP属性映射配置示例所示。

在Cisco IOS上，在WebVPN环境下配置不同策略组和使用LDAP属性映射可以实现相同的目标，以确定用户将分配的策略组。在Cisco IOS头端上，“memberOf” AD属性映射到身份验证、授权和记帐(AAA)属性supplicant客户端组。有关默认属性映射的详细信息，请参阅IOS设备上使用动态属性映射的LDAP配置示例。但是，对于SSL VPN，有两个相关的AAA属性映射：

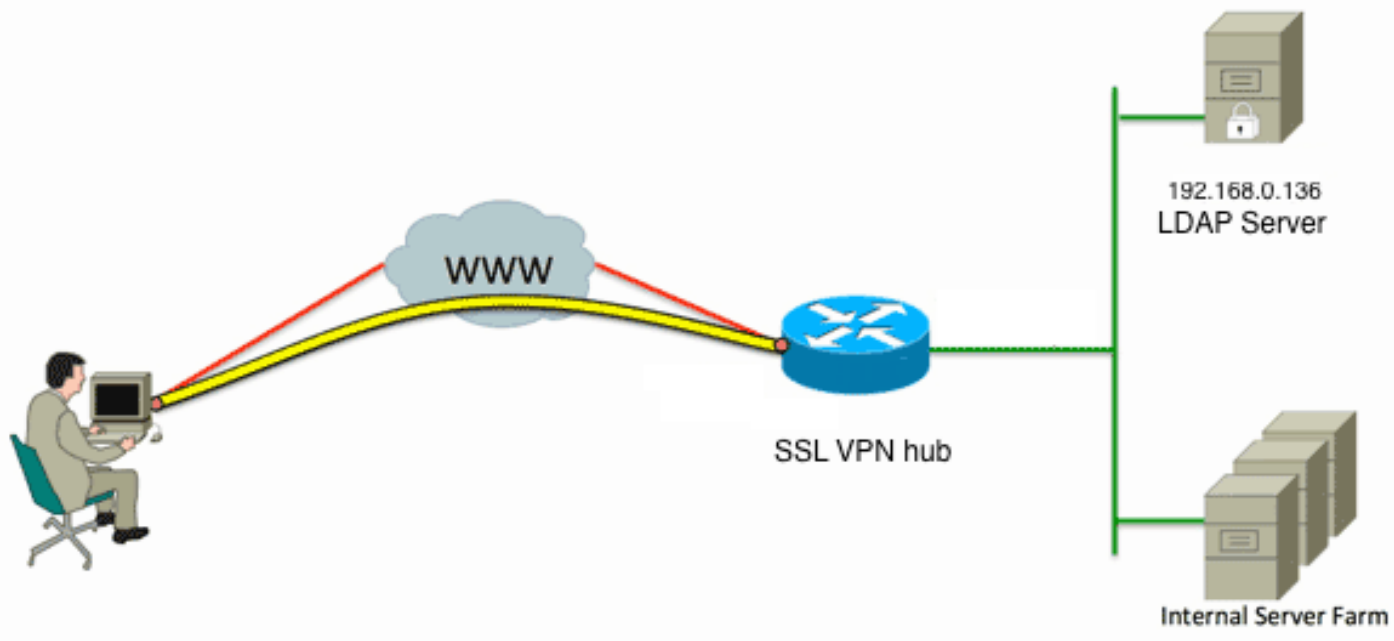
AAA属性名称	SSL VPN相关性
user-vpn-group	映射到在WebVPN上下文下定义的策略组
webvpn-context	映射到实际WebVPN环境本身

因此，LDAP属性映射需要将相关LDAP属性映射到这两个AAA属性中的任一属性。

配置

> **注意：**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LDAP属性映射将“memberOf” LDAP属性映射到AAA属性user-vpn-group。

1. 配置身份验证方法和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属性映射。

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

3. 配置引用先前LDAP属性映射的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. 将路由器配置为WebVPN服务器。在本示例中，由于“memberOf”属性将映射到“user-vpn-group”属性，因此单个WebVPN上下文配置了多个策略组，其中包括“NOACCESS”策略。此策略组适用于没有匹配“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
```

注意事项

1. 如果用户是“memberOf”多个组，则路由器使用第一个“memberOf”值。
2. 此配置中的奇怪之处在于，策略组的名称必须与LDAP服务器为“memberOf值”推送的完整字符串的**完全**匹配。 管理员通常为策略组使用更短且更相关的名称，例如VPNACCESS，但除了表面问题外，这还可能导致更大的问题。“memberOf”属性字符串比本示例中使用的字符串大很多，这种情况并不罕见。例如，请考虑以下调试消息：

   ```
   004090: Aug 23 08:26:57.235 PCTime: %SSLVPN-6-INVALID_RADIUS_CONFIGURATION:
   Radius configured group policy "CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,
   DC=chillsthrills,DC=local" does not exist
   ```

   它清楚地显示从AD接收的字符串是：

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

   但是，由于未定义此策略组，因此如果管理员尝试配置此组策略，则会导致错误，因为Cisco IOS对策略组名称中的字符数有限制：

   ```
   HOURTR1(config-webvpn-context)#webvpn context VPNACCESS
   HOURTR1(config-webvpn-context)# policy group "CN=VPNACCESS,OU=Security Groups,
   OU=MyBusiness,DC=chillsthrills,DC=local"
   Error: group policy name cannot exceed 63 characters
   ```

在这种情况下，有两种可能的解决方法：

1. 使用不同的LDAP属性，如“department”。考虑以下LDAP属性映射：

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

   在这种情况下，用户的部门属性值可以设置为VPNACCESS等值，而WebVPN配置更简单：

   ```
   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. 在LDAP属性映射中使用DN-to-string关键字。如果以前的解决方法不适合，则管理员可以在LDAP属性映射中使用dn-to-string关键字，以便仅从"memberOf"字符串中提取公用名(CN)值。在此方案中，LDAP属性映射为：

```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group format dn-to-string
```

WebVPN配置为：

```
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
```

注意：在ASA中，您可以在属性映射下使用**map value**命令，以便将从LDAP服务器接收的值

与某些其他本地有效值匹配，而Cisco IOS头端没有此选项，因此不灵活。为解决此问题，已提交思科漏洞ID CSCts31840。

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。使用输出解释器工具来查看 show 命令输出的分析。

- show ldap attributes
- show ldap server all

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。

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

要排除LDAP属性映射故障，请启用以下调试：

- debug ldap all
- debug ldap event
- debug aaa authentication
- debug aaa authorization