在ASA上为安全客户端VPN配置LDAP属性映射

目录

简介

本文档介绍如何在Cisco ASA上配置LDAP属性映射，以根据Active Directory组分配VPN组策略。

要求

Cisco ASA要求

- 运行受支持的软件版本的Cisco ASA。
- 对ASA设备的管理访问。

网络要求

- ASA可访问的Active Directory(AD)域。
- AD服务器（默认端口636）上配置的LDAP over SSL(LDAPS)。

客户端要求

- 客户端设备上安装的安全客户端。

使用的组件

本文档中的信息并不限于特定的软件和硬件版本。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置步骤

步骤1.定义组策略

组策略确定VPN用户的权限和限制。创建必要的组策略，使其符合组织的访问要求。

为授权用户创建组策略

```
 group-policy VPN_User_Policy internal
 group-policy VPN_User_Policy attributes
   vpn-simultaneous-logins 3
   split-tunnel-policy tunnelspecified
   split-tunnel-network-list value SPLIT_TUNNEL_ACL
```

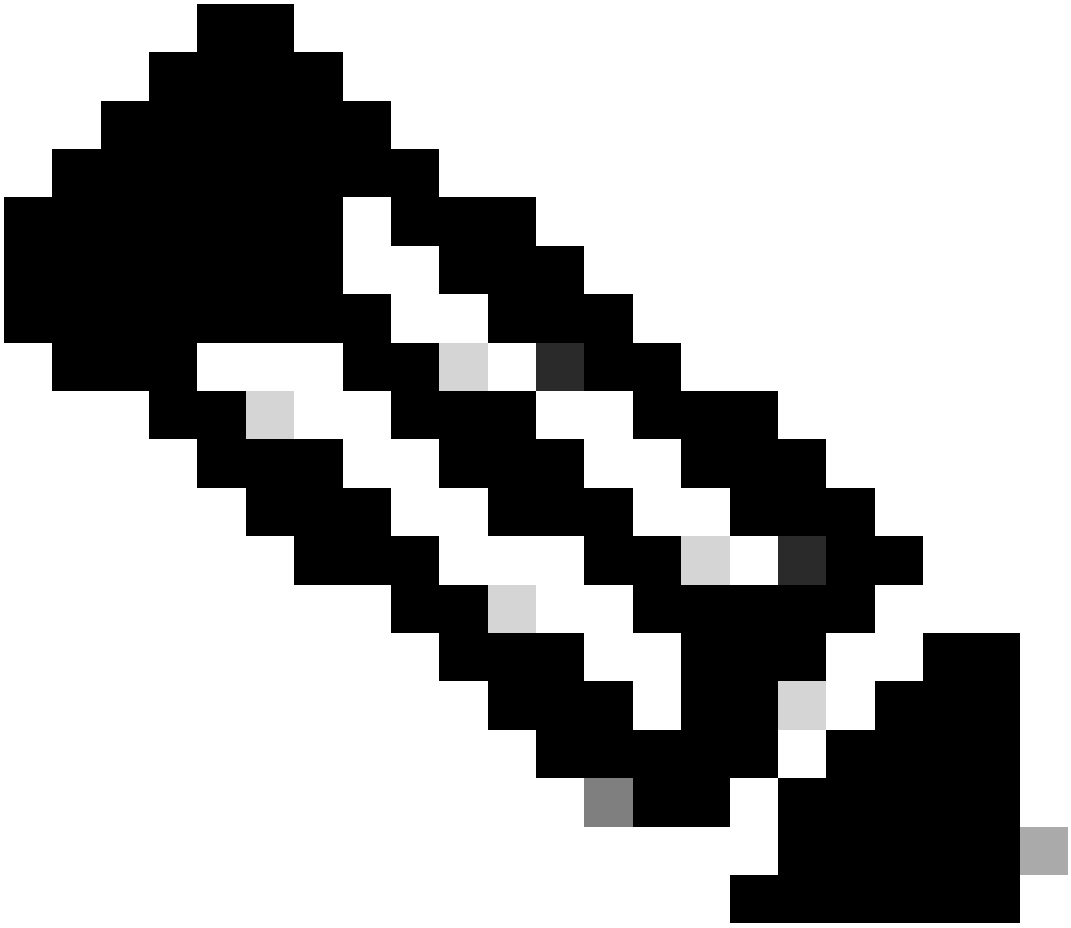
创建默认组策略以拒绝访问。

```
group-policy No_Access_Policy internal
 group-policy No_Access_Policy attributes
   vpn-simultaneous-logins 0
```

步骤2.配置LDAP属性映射

属性映射将LDAP属性转换为ASA属性，使ASA能够根据用户的LDAP组成员身份将用户分配到正确的组策略。

```
ldap attribute-map VPN_Access_Map
   map-name  memberOf Group-Policy
   map-value memberOf "CN=VPN_Users,OU=Groups,DC=example,DC=com" VPN_User_Policy
```



注意：LDAP组的可分辨名称(DN)必须始终用双引号("")括起来。 这可确保ASA正确解释DN中的空格和特殊字符。

步骤3.配置LDAP AAA服务器

设置ASA以与AD服务器进行通信，以进行身份验证和组映射。

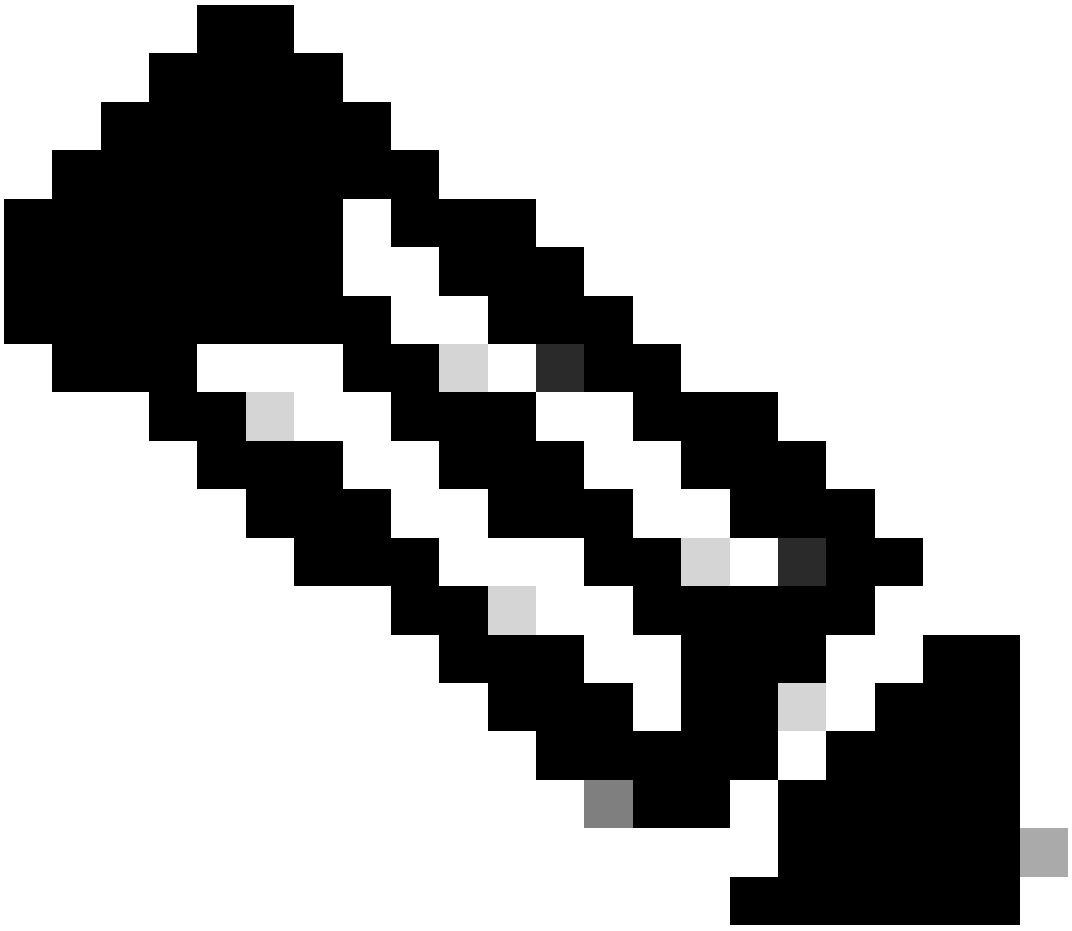
```
aaa-server AD_LDAP_Server protocol ldap
aaa-server AD_LDAP_Server (inside) host 192.168.1.10
  ldap-base-dn dc=example,dc=com
  ldap-scope subtree
  ldap-naming-attribute sAMAccountName
  ldap-login-password ********
  ldap-login-dn CN=ldap_bind_user,OU=Service Accounts,DC=example,DC=com
  ldap-over-ssl enable
  ldap-attribute-map VPN_Access_Map
```

步骤4.定义隧道组

隧道组定义VPN参数并将身份验证与LDAP服务器关联。

```
tunnel-group VPN_Tunnel type remote-access
tunnel-group VPN_Tunnel general-attributes
  address-pool VPN_Pool
  authentication-server-group AD_LDAP_Server
  default-group-policy No_Access_Policy

tunnel-group VPN_Tunnel webvpn-attributes
  group-alias VPN_Tunnel enable
```



注意：default-group-policy设置为No_Access_Policy，拒绝对不匹配任何LDAP属性映射条件的用户的访问。

验证

完成设置后，验证用户是否已正确通过身份验证并分配了相应的组策略。

验证VPN会话分配

```
show vpn-sessiondb anyconnect filter name
```

将<username>替换为实际测试帐户。

故障排除

使用本部分可排除配置故障。

启用LDAP调试

如果用户未收到预期的组策略，请启用调试以识别问题。

```
debug ldap 255
debug aaa common 255
debug aaa shim 255
```

启动VPN连接

让测试用户尝试使用Cisco Secure Client进行连接。

查看调试输出

检查Cisco ASA日志，确保用户根据其Active Directory(AD)组成员身份映射到正确的组策略。

验证后禁用调试

```
undebug all
```

常见问题

LDAP属性映射区分大小写。确保map-value语句中的AD组名称完全匹配，包括区分大小写。

验证用户是指定AD组的直接成员。嵌套组成员身份并非总是可识别的，从而导致授权问题。

不匹配任何映射值条件的用户会收到default-group-policy（本例中为No_Access_Policy），阻止访问。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。