在ASA上為安全客戶端VPN配置LDAP屬性對映

目錄

簡介

本文檔介紹如何在Cisco ASA上配置LDAP屬性對映，以便根據Active Directory組分配VPN組策略。

需求

Cisco ASA要求

- 運行受支援的軟體版本的Cisco ASA。
- 對ASA裝置的管理訪問。

網路要求

- ASA可訪問的Active Directory(AD)域。
- AD伺服器（預設埠636）上配置的LDAP over SSL(LDAPS)。

客戶端要求

- 安裝在客戶端裝置上的安全客戶端。

採用元件

本檔案中的資訊不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定步驟

步驟1.定義組策略

組策略確定VPN使用者的許可權和限制。建立符合組織訪問要求的必要組策略。

為授權使用者建立組策略

```
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
```

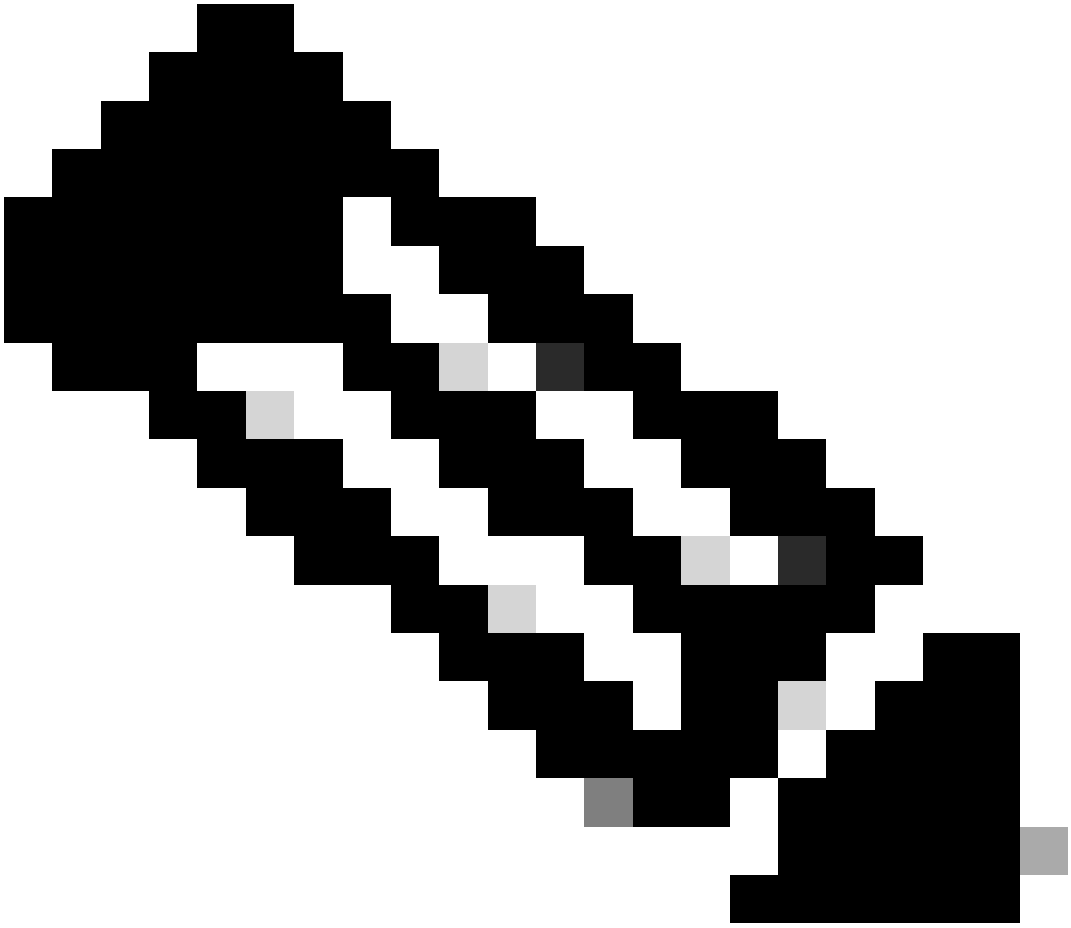
建立預設組策略以拒絕訪問。

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

步驟2.配置LDAP屬性對映

屬性對映將LDAP屬性轉換為ASA屬性，使ASA能夠根據使用者的LDAP組成員身份將使用者分配到正確的組策略。

```
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
```



附註：LDAP組的唯一判別名(DN)必須始終用雙引號("")括起來。 這可確保ASA正確解釋DN中的空格和特殊字元。

步驟3.配置LDAP AAA伺服器

將ASA設定為與AD伺服器進行通信以進行身份驗證和組對映。

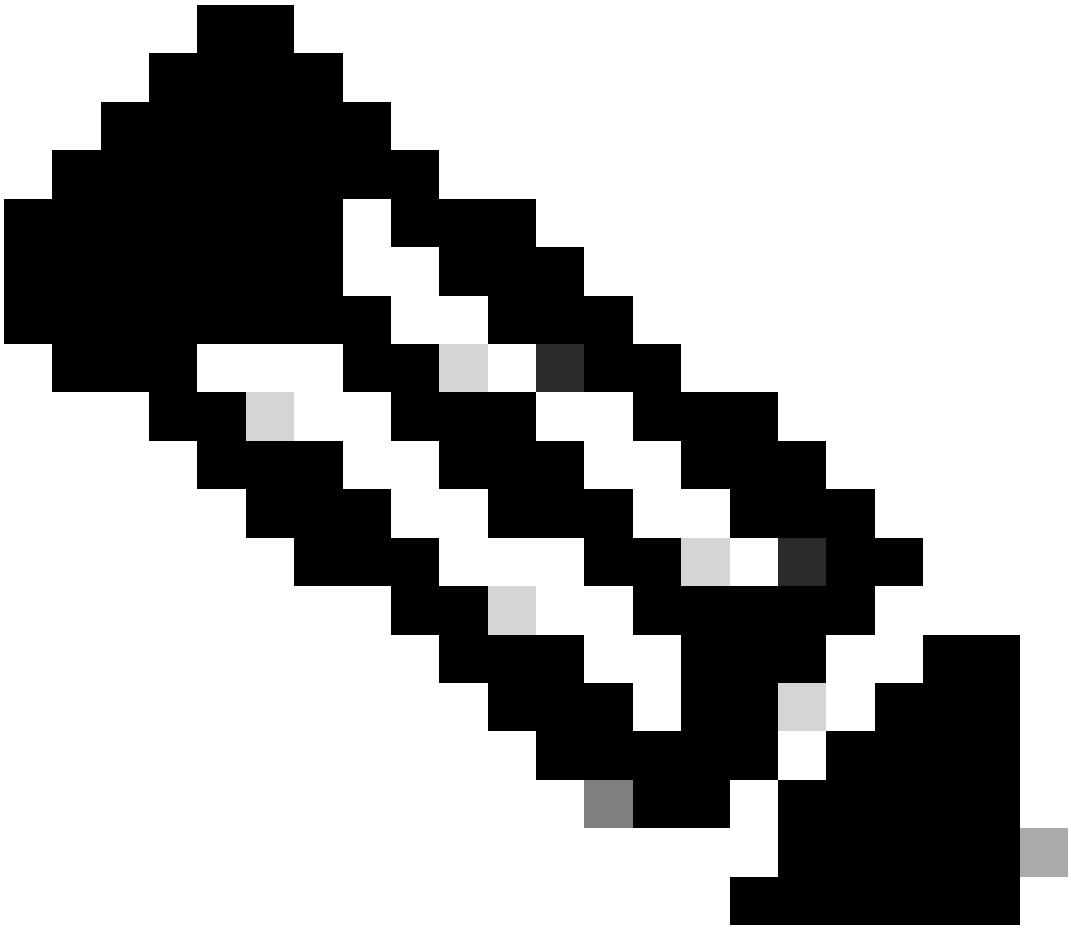
```
aaa-server AD_LDAP_Server protocol ldap
aaa-server AD_LDAP_Server (inside) host 192.168.1.10
  ldap-base-dn dc=example,dc=com
  ldap-scope subtree
  ldap-naming-attribute sAMAccountName
  ldap-login-password ********
  ldap-login-dn CN=ldap_bind_user,OU=Service Accounts,DC=example,DC=com
  ldap-over-ssl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

步驟4.定義通道組

隧道組定義VPN引數並將身份驗證繫結到LDAP伺服器。

```
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
```



附註：default-group-policy設定為No_Access_Policy，拒絕對不匹配任何LDAP屬性對映條件的使用者的訪問。

驗證

完成設定後，驗證使用者是否正確通過身份驗證並分配了相應的組策略。

驗證VPN會話分配

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

將<username> 替換為實際測試帳戶。

疑難排解

本節內容可協助您疑難排解組態問題。

啟用LDAP調試

如果使用者沒有收到預期的組策略，請啟用調試以發現問題。

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

啟動VPN連線

讓測試使用者嘗試使用Cisco Secure Client進行連線。

檢視調試輸出

檢查Cisco ASA日志，確保根據使用者的Active Directory(AD)組成員身份將使用者對映到正確的組策略。

驗證後禁用調試

```
undebug all
```

常見問題

LDAP屬性對映區分大小寫。確保map-value語句中的AD組名稱完全匹配，包括區分大小寫。

驗證使用者是指定AD組的直接成員。巢狀組成員身份並非始終可識別，這會導致授權問題。

不匹配任何對映值條件的使用者會收到預設組策略（本例中為No_Access_Policy），從而阻止訪問。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。