Configurazione del mapping degli attributi LDAP sull'appliance ASA per la VPN client sicura

Sommario

- Introduzione
  - Requisiti
    - Requisiti per Cisco ASA
    - Requisiti di rete
    - Requisiti del client
  - Componenti usati
- Procedura di configurazione
  - Passaggio 1. Definizione dei criteri di gruppo
  - Passaggio 2. Configurare la mappa degli attributi LDAP
  - Passaggio 3. Configurare il server LDAP AAA
  - Passaggio 4. Definizione del gruppo di tunnel
- Verifica
  - Verifica assegnazione sessione VPN
- Risoluzione dei problemi
  - Abilita debug LDAP
  - Avvio di una connessione VPN
  - Verifica output di debug
  - Disabilita debug dopo verifica
  - Problemi comuni

Introduzione

In questo documento viene descritta la configurazione della mappatura degli attributi LDAP su Cisco ASA per assegnare i criteri di gruppo VPN basati sui gruppi di Active Directory.

Requisiti

Requisiti per Cisco ASA

- Cisco ASA con una versione software supportata.
- Accesso amministrativo al dispositivo ASA.

Requisiti di rete

- Dominio di Active Directory (AD) accessibile all'appliance ASA.
- LDAP over SSL (LDAPS) configurato sul server AD (porta predefinita 636).

Requisiti del client

- Secure Client installato sui dispositivi client.

Componenti usati

Le informazioni di questo documento non si limitano a versioni software e hardware specifiche.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Procedura di configurazione

Passaggio 1. Definizione dei criteri di gruppo

I criteri di gruppo determinano le autorizzazioni e le restrizioni per gli utenti VPN. Creare i criteri di gruppo necessari in linea con i requisiti di accesso dell'organizzazione.

Creazione di Criteri di gruppo per gli utenti autorizzati

```
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
```

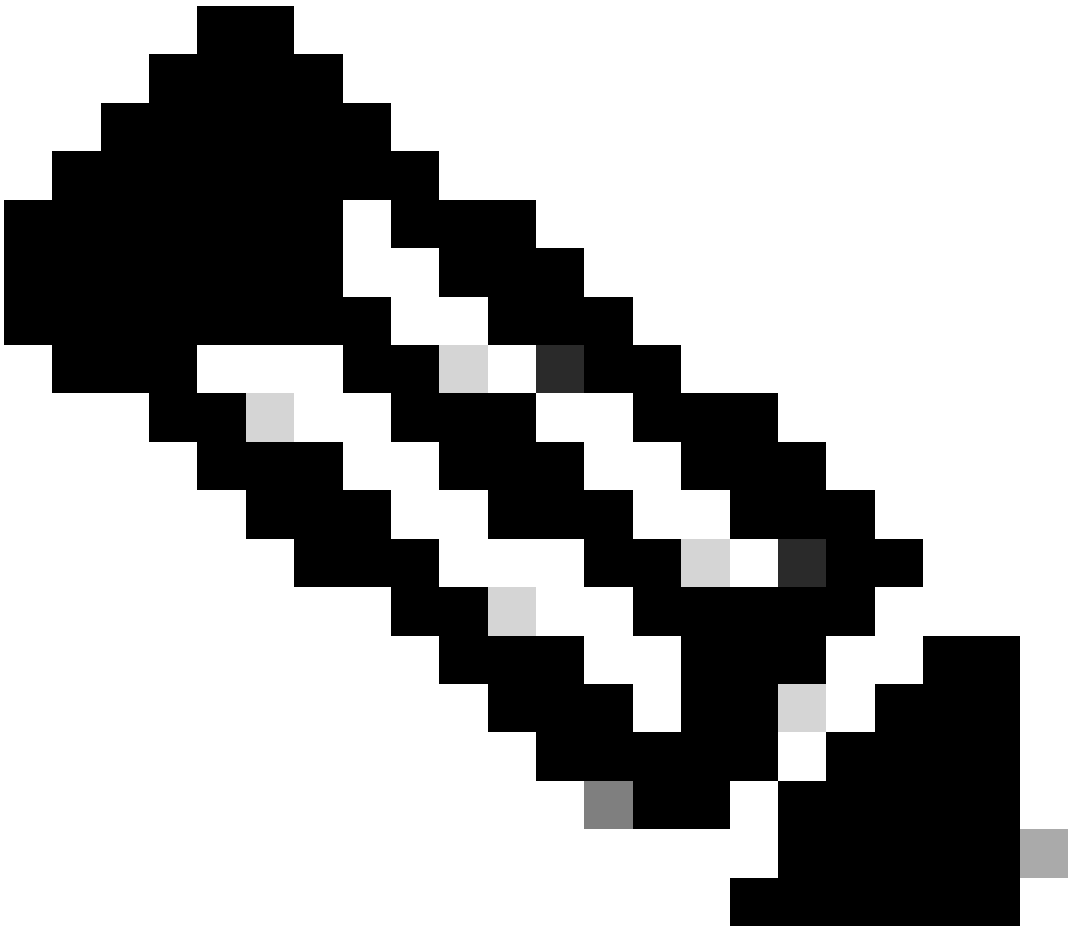
Creare un criterio di gruppo predefinito per negare l'accesso.

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

Passaggio 2. Configurare la mappa degli attributi LDAP

La mappa degli attributi converte gli attributi LDAP in attributi ASA, consentendo all'ASA di assegnare gli utenti ai criteri di gruppo corretti in base all'appartenenza ai gruppi LDAP.

```
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
```



Nota: Il nome distinto (DN) del gruppo LDAP deve essere sempre racchiuso tra virgolette doppie (""). In questo modo, l'ASA interpreta correttamente gli spazi e i caratteri speciali nel DN.

Passaggio 3. Configurare il server LDAP AAA

Configurare l'appliance ASA per comunicare con il server AD per l'autenticazione e il mapping dei gruppi.

```
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
```

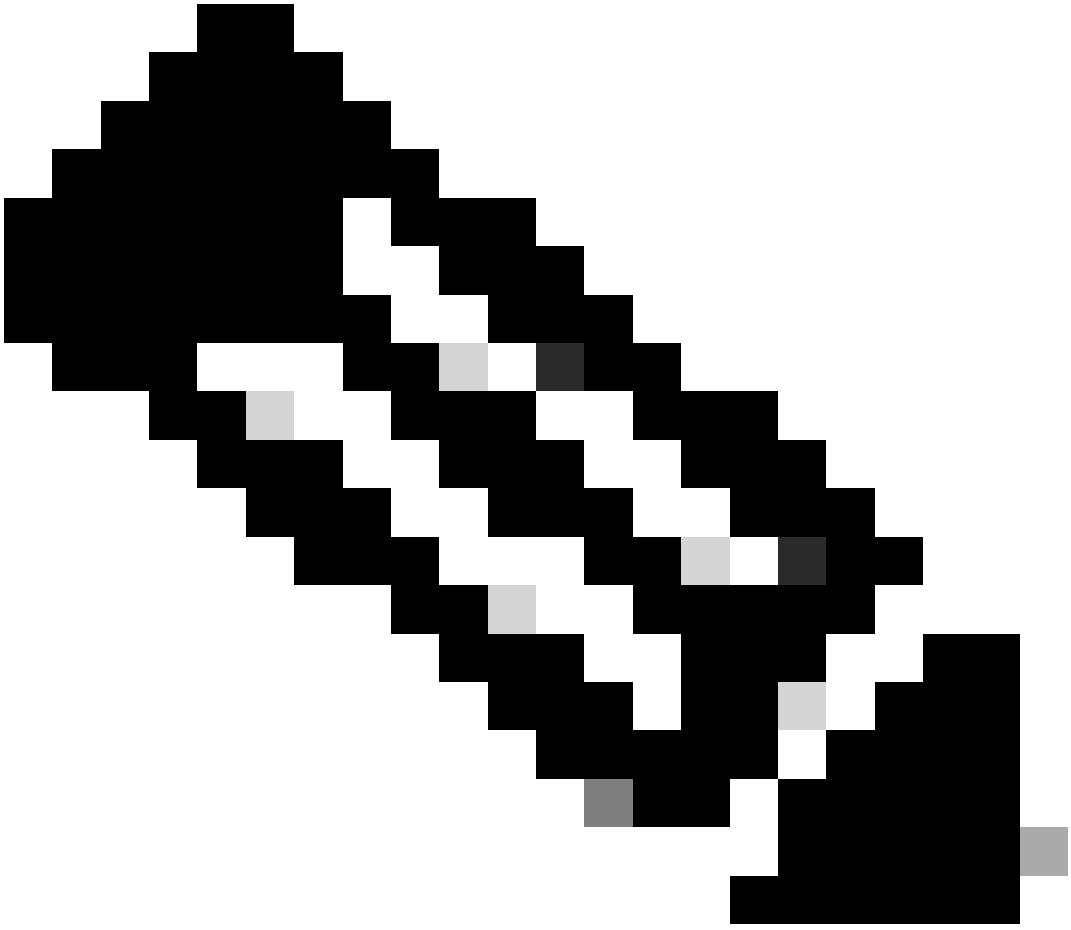
```
  ldap-attribute-map VPN_Access_Map
```

Passaggio 4. Definizione del gruppo di tunnel

Il gruppo di tunnel definisce i parametri VPN e collega l'autenticazione al server LDAP.

```
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
```



Nota: L'impostazione predefinita di Criteri di gruppo è No_Access_Policy, che nega

l'accesso agli utenti che non soddisfano i criteri di mapping degli attributi LDAP.

Verifica

Al termine dell'installazione, verificare che gli utenti siano autenticati correttamente e che dispongano dei criteri di gruppo appropriati.

Verifica assegnazione sessione VPN

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

Sostituire <username> con l'account di test effettivo.

Risoluzione dei problemi

Consultare questa sezione per risolvere i problemi di configurazione.

Abilita debug LDAP

Se gli utenti non ricevono i criteri di gruppo previsti, abilitare il debug per identificare i problemi.

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

Avvio di una connessione VPN

Fare in modo che un utente di prova tenti di connettersi utilizzando Cisco Secure Client.

Verifica output di debug

Controllare i log di Cisco ASA per verificare che l'utente sia mappato ai Criteri di gruppo corretti in base all'appartenenza al gruppo Active Directory (AD).

Disabilita debug dopo verifica

```
undebug all
```

Problemi comuni

Per i mapping di attributi LDAP viene fatta distinzione tra maiuscole e minuscole. Verificare che i nomi dei gruppi AD nelle istruzioni map-value corrispondano esattamente, compresa la distinzione tra maiuscole e minuscole.

Verificare che gli utenti siano membri diretti dei gruppi AD specificati. Le appartenenze ai gruppi nidificati non vengono sempre riconosciute e ciò comporta problemi di autorizzazione.

Gli utenti che non soddisfano alcun criterio relativo al valore della mappa ricevono il criterio di gruppo predefinito (No_Access_Policy in questo caso), che impedisce l'accesso.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).