Configurar mapeamento de atributos LDAP no ASA para VPN de cliente seguro

Contents

- Introdução
  - Requisitos
    - Requisitos do Cisco ASA
    - Requisitos de Rede
    - Requisitos do cliente
  - Componentes Utilizados
- Configuration Steps
  - Etapa 1. Definir Políticas de Grupo
  - Etapa 2. Configurar o mapa de atributos LDAP
  - Etapa 3. Configurar o servidor AAA LDAP
  - Etapa 4. Definir o grupo de túneis
- Verificar
  - Verificar atribuição de sessão VPN
- Troubleshooting
  - Habilitar depuração LDAP
  - Iniciar uma conexão VPN
  - Revisar saída de depuração
  - Desabilitar Depuração Após Verificação
  - Problemas comuns

Introdução

Este documento descreve a configuração do mapeamento de atributos LDAP no Cisco ASA para atribuir políticas de grupo VPN com base em grupos do Ative Diretory.

Requisitos

Requisitos do Cisco ASA

- Cisco ASA executando uma versão de software compatível.
- Acesso administrativo ao dispositivo ASA.

Requisitos de Rede

- Domínio do Ative Diretory (AD) acessível ao ASA.
- LDAP sobre SSL (LDAPS) configurado no servidor AD (porta padrão 636).

Requisitos do cliente

- Cliente seguro instalado nos dispositivos cliente.

Componentes Utilizados

As informações neste documento não estão restritas a versões específicas de software e hardware.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configuration Steps

Etapa 1. Definir Políticas de Grupo

As políticas de grupo determinam as permissões e restrições para usuários VPN. Crie as políticas de grupo necessárias alinhadas aos requisitos de acesso da sua organização.

Criar uma Política de Grupo para Usuários Autorizados

```
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
```

Crie uma Política de Grupo Padrão para Negar Acesso.

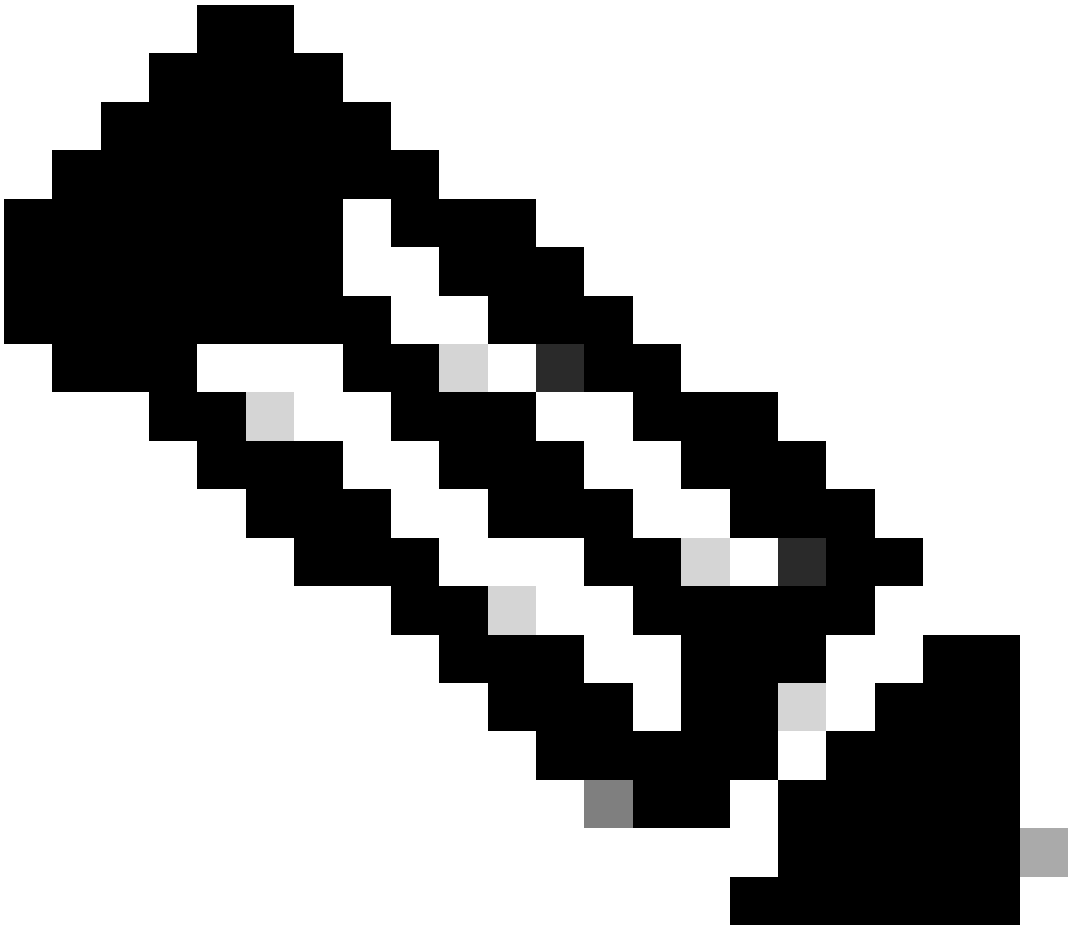
```
group-policy No_Access_Policy internal
group-policy No_Access_Policy attributes
  vpn-simultaneous-logins 0
```

Etapa 2. Configurar o mapa de atributos LDAP

O mapa de atributos converte atributos LDAP em atributos ASA, permitindo que o ASA atribua usuários à política de grupo correta com base em suas associações de grupo 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
```



Note: O nome distinto (DN) do grupo LDAP sempre deve estar entre aspas duplas (""). Isso garante que o ASA interprete corretamente os espaços e os caracteres especiais no DN.

Etapa 3. Configurar o servidor AAA LDAP

Configure o ASA para se comunicar com o servidor AD para autenticação e mapeamento de grupo.

```
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
```

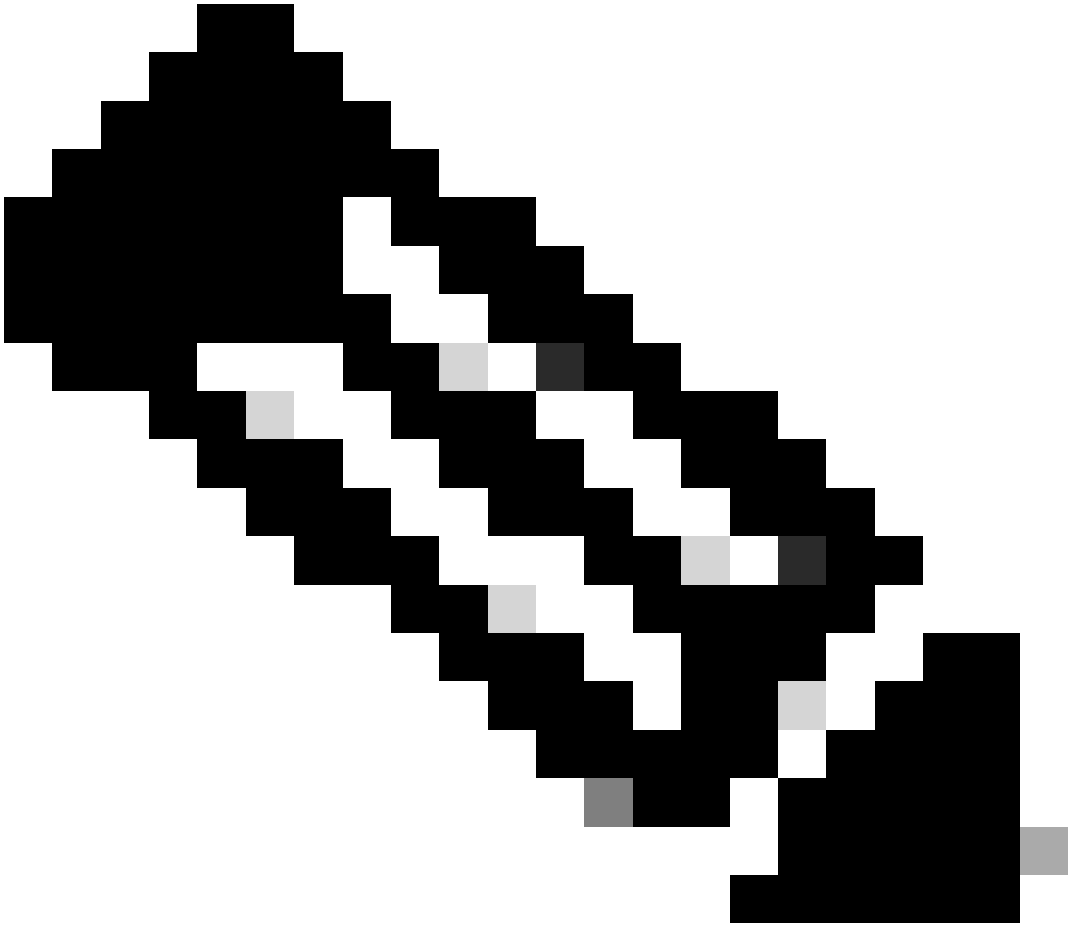
```
  ldap-login-password ********
  ldap-login-dn CN=ldap_bind_user,OU=Service Accounts,DC=example,DC=com
  ldap-over-ssl enable
  ldap-attribute-map VPN_Access_Map
```

Etapa 4. Definir o grupo de túneis

O grupo de túneis define os parâmetros de VPN e vincula a autenticação ao servidor 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
```



Note: A política de grupo padrão é definida como No_Access_Policy, negando o acesso a usuários que não correspondam a nenhum critério de mapa de atributos LDAP.

Verificar

Após concluir a configuração, verifique se os usuários foram autenticados corretamente e receberam as políticas de grupo apropriadas.

Verificar atribuição de sessão VPN

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

Substitua <username> pela conta de teste real.

Troubleshooting

Use esta seção para resolver problemas de configuração.

Habilitar depuração LDAP

Se os usuários não estiverem recebendo as políticas de grupo esperadas, habilite a depuração para identificar problemas.

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

Iniciar uma conexão VPN

Faça com que um usuário teste tente se conectar usando o Cisco Secure Client.

Revisar saída de depuração

Verifique os logs do Cisco ASA para garantir que o usuário esteja mapeado para a política de grupo correta com base na associação de grupo do Ative Diretory (AD).

Desabilitar Depuração Após Verificação

```
undebug all
```

Problemas comuns

Os mapeamentos de atributos LDAP diferenciam maiúsculas de minúsculas. Certifique-se de que os nomes do grupo AD nas instruções map-value correspondam exatamente, incluindo diferenciação de maiúsculas e minúsculas.

Verifique se os usuários são membros diretos dos grupos AD especificados. As associações a grupos aninhados nem sempre são reconhecidas, o que leva a problemas de autorização.

Os usuários que não corresponderem a nenhum critério de valor de mapa recebem a política de grupo padrão (No_Access_Policy neste caso), impedindo o acesso.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.