Atribuição do grupo de política para os clientes de AnyConnect que usam o LDAP no exemplo de configuração dos finais do cabeçalho do Cisco IOS

Índice

Introdução

Este documento descreve como configurar mapas do atributo do Lightweight Directory Access Protocol (LDAP) para atribuir automaticamente a política de VPN correta a um usuário baseado em suas credenciais.

> **Note**: O apoio para a autenticação LDAP para os usuários do secure sockets layer VPN (SSL VPN) que conectam a um final do cabeçalho do ® do Cisco IOS é seguido pela identificação de bug Cisco CSCuj20940. Até que o apoio esteja adicionado oficialmente, o suporte ldap é o melhor esforço.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- SSL VPN no Cisco IOS
- Autenticação LDAP no Cisco IOS

- Serviços de diretório

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CISCO881-SEC-K9
- Cisco IOS Software, software C880 (C880DATA-UNIVERSALK9-M), versão 15.1(4)M, SOFTWARE DE VERSÃO (fc1)

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O LDAP é um protocolo do aplicativo aberto, vendedor-neutro, do padrão para indústria para alcançar e manter serviços de informação de diretório distribuídos sobre uma rede do Protocolo IP. Os serviços de diretório jogam um papel importante no desenvolvimento do intranet e dos aplicativos de Internet enquanto permitem a partilha da informação sobre usuários, sistemas, redes, serviços, e aplicativos durante todo a rede.

Frequentemente, os administradores querem fornecer aos usuários VPN diferentes permissões de acesso ou conteúdo WebVPN. Isto pode ser terminado com a configuração de políticas de VPN diferentes no servidor de VPN e de atribuição destes política-grupos a cada dependente do usuário em cima de suas credenciais. Quando isto puder ser terminado manualmente, é mais eficiente para automatizar o processo com serviços de diretório. A fim usar o LDAP para atribuir uma política do grupo a um usuário, você precisa de configurar um mapa que trace um atributo LDAP tal como o atributo “memberOf” do diretório ativo (AD) a um atributo que seja compreendido pelo fim de cabeçalho de VPN.

Na ferramenta de segurança adaptável (ASA) isto é conseguido regularmente com a atribuição de políticas diferentes do grupo aos usuários diferentes com um mapa do atributo LDAP segundo as indicações do uso ASA do exemplo de configuração dos mapas do atributo LDAP.

No Cisco IOS a mesma coisa pode ser conseguida com a configuração de grupos de política diferentes sob o contexto WebVPN e o uso de mapas do atributo LDAP a fim determinar que grupo de política o usuário será atribuído. Em finais do cabeçalho do Cisco IOS, o atributo AD do “memberOf” é traçado ao suplicante-grupo do atributo do Authentication, Authorization, and Accounting (AAA). Para mais detalhes nos mapeamentos do atributo de padrão, veja o LDAP em dispositivos de IOS usando o exemplo de configuração dinâmico dos mapas do atributo. Contudo para SSL VPN, há dois mapeamentos relevantes do atributo AAA:

Nome do atributo AAA	Importância SSL VPN
USER-VPN-grupo	mapas ao grupo de política definido sob o contexto WebVPN
WebVPN-contexto	mapas ao contexto real WebVPN próprios

Consequentemente o mapa do atributo LDAP precisa de traçar o atributo relevante LDAP a qualquer um um destes dois atributos AAA.

Configurar

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Esta configuração usa um mapa do atributo LDAP a fim traçar o atributo LDAP do “memberOf” ao USER-VPN-grupo do atributo AAA.

1. Configurar o método de autenticação e o Grupo de servidores AAA.
```
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. Configurar um mapa do atributo LDAP.
```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group
```
3. Configurar o servidor ldap que provê o mapa precedente do atributo LDAP.
```
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. Configurar o roteador para atuar como um servidor VPN da Web. Neste exemplo, desde que o atributo do “memberOf” será traçado ao atributo do “USER-VPN-grupo”, um único contexto WebVPN é configurado com grupos de política múltipla que incluem uma política “NOACCESS”. Este grupo de política é para os usuários que não têm um valor de harmonização do “memberOf”.
```
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
```

Caveats

1. Se o usuário é grupos múltiplos de um “memberOf”, o primeiro valor do “memberOf” está usado pelo roteador.
2. O que é impar nesta configuração é que o nome do grupo de política tem que ser um exato - fósforo para a corda completa empurrada pelo servidor ldap para do “o valor memberOf”. Geralmente os administradores usam uns nomes mais curtos e mais relevantes para o grupo de política, tal como VPNACCESS, mas independentemente do problema cosmético este pode conduzir a um problema mais grande. Não é raro para a corda do atributo do “memberOf” ser consideravelmente maior do que o que foi usado neste exemplo. Por exemplo, considere isto debugam a mensagem:

```
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
```

Mostra claramente que a corda recebida do AD é:

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

Contudo, desde que não há nenhum tal grupo de política definido, se o administrador tenta configurar tal política do grupo conduz a um erro porque o Cisco IOS tem um limite no número de caráteres no nome de grupo de política:

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

Em tais situações há duas alternativas possíveis:

1. Use um atributo diferente LDAP, tal como o “departamento”.Considere este mapa do atributo LDAP:

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

   Neste caso o valor do atributo do departamento para um usuário pode ser ajustado a um valor tal como VPNACCESS e a configuração WebVPN é um bit mais simples:

   ```
   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. Use a palavra-chave da DN-à-corda no mapa do atributo LDAP.Se a ação alternativa precedente não é apropriada então o administrador pode usar a palavra-chave da dn-à-corda no mapa do atributo LDAP a fim extrair apenas o valor do Common Name (CN) da corda do “memberOf”. Nesta encenação o mapa do atributo LDAP seria:

```
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
```

E a configuração WebVPN seria:

```
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
```

Note: Ao contrário nos ASA onde você pode usar o **comando value do mapa** sob um mapa do atributo a fim combinar o valor recebido do servidor ldap a algum outro localmente - o valor significativo, finais do cabeçalho do Cisco IOS não tem esta opção e é consequentemente não como flexível. A identificação de bug Cisco CSCts31840 foi arquivada a fim endereçar esta.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

- **mostre atributos do ldap**
- **mostre o servidor ldap todo**

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Note: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

A fim pesquisar defeitos o mapeamento do atributo LDAP, permita estes debuga:

- **debugar o ldap todo**
- **debugar o evento do ldap**
- **debug aaa authentication**
- **debug aaa authorization**