Exemplo de configuração de mapas de atributos LDAP do usuário

Contents

[Introduction](#)
[Procedimento](#)
[Colocar Usuários LDAP em uma Política de Grupo Específica (Exemplo Genérico)](#)
[Configurar uma política de grupo NOACCESS](#)
[Aplicação de política de atributos com base em grupo (Exemplo)](#)
[Aplicação do Ative Diretory de "Atribuir um endereço IP estático" para túneis IPsec e SVC](#)
[Aplicação do Ative Diretory de "Discagem de permissão de acesso remoto, permitir/negar acesso"](#)
[Aplicação do Ative Diretory de "Membro de"/Associação de grupo para permitir ou negar acesso](#)
[Aplicação de "horas de logon/regras de hora do dia" no Ative Diretory](#)
[Use a configuração ldap-map para mapear um usuário em uma política de grupo específica e use o comando authorization-server-group, no caso de autenticação dupla](#)
[Verificar](#)
[Troubleshoot](#)
[Depurar a transação LDAP](#)
[O ASA não pode autenticar usuários do servidor LDAP](#)

Introduction

Este documento descreve como qualquer atributo do Microsoft/AD pode ser mapeado para um atributo da Cisco.

Procedimento

1. No servidor Ative Diretory (AD)/Lightweight Diretory Access Protocol (LDAP):Escolha **user1**.Clique com o botão direito do mouse em **> Propriedades**.Escolha uma guia a ser usada para definir um atributo (por exemplo, guia Geral).Escolha um campo/atributo, por exemplo, o campo Escritório, a ser usado para aplicar o intervalo de tempo, e insira o texto do banner (por exemplo, Bem-vindo ao !!!! LDAP). A configuração do Office na GUI é armazenada no atributo AD/LDAP physicalDeliveryOfficeName.
2. No Adaptive Security Appliance (ASA), para criar uma tabela de mapeamento de atributos LDAP, mapeie o atributo AD/LDAP physicalDeliveryOfficeName para o atributo ASA Banner1:

```
B200-54(config)# show run ldap
ldap attribute-map Banner
map-name physicalDeliveryOfficeName Banner1
```

3. Associe o mapa de atributos LDAP à entrada aaa-server:

```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
```

```
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map Banner
```

4. Estabeleça a sessão de Acesso Remoto e verifique se a !!!! Banner Welcome to LDAP é apresentada ao usuário da VPN.

Colocar Usuários LDAP em uma Política de Grupo Específica (Exemplo Genérico)

Este exemplo demonstra a autenticação de user1 no servidor AD-LDAP e recupera o valor do campo de departamento para que ele possa ser mapeado para uma política de grupo do ASA/PIX a partir da qual as políticas podem ser aplicadas.

1. No servidor AD/LDAP:Escolha **user1**.Clique com o botão direito do mouse em **> Propriedades**.Escolha uma guia a ser usada para definir um atributo (por exemplo, guia Organização).Escolha um campo/atributo, por exemplo, Departamento, a ser usado para impor uma política de grupo e insira o valor da política de grupo (Group-Policy1) no ASA/PIX. A configuração de Departamento na GUI é armazenada no departamento de atributos do AD/LDAP.
2. Defina uma tabela ldap-attribute-map.

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department Group-Policy
5520-1(config)#
```

3. Defina a política de grupo, Group_policy1, no dispositivo e os atributos de política necessários.
4. Estabeleça o túnel de acesso remoto VPN e verifique se a sessão herda os atributos de Group-Policy1 (e quaisquer outros atributos aplicáveis da política de grupo padrão). **Observação**: adicione mais atributos ao mapa conforme necessário. Este exemplo mostra apenas o mínimo para controlar essa função específica (colocar um usuário em uma política de grupo específica do ASA/PIX 7.1.x). O terceiro exemplo mostra esse tipo de mapa.

Configurar uma política de grupo NOACCESS

Você pode criar uma política de grupo NOACCESS para negar a conexão VPN quando o usuário não fizer parte de nenhum dos grupos LDAP. Este snippet de configuração é mostrado para sua referência:

```
group-policy NOACCESS internal
group-policy NOACCESS attributes
vpn-simultaneous-logins 0
vpn-tunnel-protocol IPSec webvpn
```

Você deve aplicar essa política de grupo como uma política de grupo padrão ao grupo de túneis. Isso permite que os usuários que obtêm um mapeamento do mapa de atributos LDAP, por exemplo, aqueles que pertencem a um grupo LDAP desejado, obtenham suas políticas de grupo desejadas e os usuários que não obtêm nenhum mapeamento, por exemplo, aqueles que não pertencem a nenhum dos grupos LDAP desejados, obtenham a política de grupo NOACCESS do grupo de túneis, que bloqueia o acesso para eles.

Dica: como o atributo vpn-simultaneous-logins está definido como 0 aqui, ele também deve ser explicitamente definido em todas as outras políticas de grupo; caso contrário, ele pode ser herdado da política de grupo padrão para esse grupo de túneis, que nesse caso é a política NOACCESS.

Aplicação de política de atributos com base em grupo (Exemplo)

1. No servidor AD-LDAP, Usuários e Computadores do Ative Diretory, configure um registro de usuário (VPNUserGroup) que represente um grupo onde os atributos de VPN estão configurados.
2. No servidor AD-LDAP, Ative Diretory Users and Computers, defina o campo Department de cada registro de usuário para apontar para o registro de grupo (VPNUserGroup) na Etapa 1. O nome de usuário neste exemplo é web1. **Observação**: o atributo AD de departamento foi usado somente porque logicamente o departamento se refere à política de grupo. Na realidade, qualquer campo poderia ser usado. O requisito é que esse campo tenha que mapear para o atributo Cisco VPN Group-Policy, como mostrado neste exemplo.
3. Defina uma tabela ldap-attribute-map:

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department IETF-Radius-Class
map-name description\Banner1
map-name physicalDeliveryOfficeName IETF-Radius-Session-Timeout
5520-1(config)#
```

   Os dois atributos AD-LDAP, Description e Office, (representados por nomes AD description e PhysicalDeliveryOfficeName) são os atributos de registro de grupo (para VPNUSerGroup) que são mapeados para os atributos Cisco VPN Banner1 e IETF-Radius-Session-Timeout.O atributo department serve para que o registro do usuário seja mapeado para o nome da política de grupo externa no ASA (VPNUSer), que é mapeado de volta para o registro VPNuserGroup no servidor AD-LDAP, onde os atributos são definidos.**Observação**: o atributo Cisco (Group-Policy) deve ser definido no ldap-attribute-map. Seu atributo AD mapeado pode ser qualquer atributo AD definível. Este exemplo usa departamento porque é o nome mais lógico que se refere à política de grupo.
4. Configure o aaa-server com o nome ldap-attribute-map a ser usado para operações de Autenticação, Autorização e Contabilização (AAA) LDAP:

```
5520-1(config)# show runn aaa-server LDAP-AD11
aaa-server LDAP-AD11 protocol ldap
aaa-server LDAP-AD11 host 10.148.1.11
ldap-base-dn cn=Users,dc=nelson,dc=cisco,dc=com
ldap-scope onelevel
ldap-naming-attribute sAMAccountName
ldap-login-password altiga
ldap-login-dn cn=Administrator,cn=Users,dc=nelson,dc=cisco,dc=com
ldap-attribute-map Our-AD-Map
5520-1(config)#
```

5. Defina um grupo de túneis com Autenticação LDAP ou Autorização LDAP. Exemplo com autenticação LDAP. Executa autenticação + (autorização) aplicação da política de atributo se os atributos forem definidos.

```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group LDAP-AD11
accounting-server-group RadiusACS28
```

```
5520-1(config)#
```

Exemplo com Autorização LDAP. Configuração usada para certificados digitais.

```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group none
authorization-server-group LDAP-AD11
accounting-server-group RadiusACS28
authorization-required
authorization-dn-attributes ea
5520-1(config)#
```

6. Defina uma política de grupo externa. O nome da política de grupo é o valor do registro de usuário AD-LDAP que representa o grupo (VPNUserGroup).

```
5520-1(config)# show runn group-policy VPNUserGroup
group-policy VPNUserGroup external server-group LDAP-AD11
5520-1(config)#
```

7. Estabeleça o túnel e verifique se os atributos estão sendo aplicados. Nesse caso, o Banner e o Session-Timeout são aplicados a partir do registro VPNuserGroup no AD.

Aplicação do Ative Diretory de "Atribuir um endereço IP estático" para túneis IPsec e SVC

O atributo do AD é msRADIUSFramedIPAddress. O atributo é configurado em Propriedades do usuário do AD, guia Discagem, Atribuir um endereço IP estático.

Aqui estão as etapas:

1. No servidor AD, em Propriedades do usuário, guia Discagem, Atribuir um endereço IP estático, insira o valor do endereço IP para atribuir à sessão IPsec/SVC (10.20.30.6).
2. No ASA, crie um ldap-attribute-map com este mapeamento:

```
5540-1# show running-config ldap
ldap attribute-map Assign-IP
map-name msRADIUSFramedIPAddress IETF-Radius-Framed-IP-Address
5540-1#
```

3. No ASA, verifique se vpn-address-assigment está configurado para incluir vpn-addr-assign-aaa:

```
5520-1(config)# show runn all vpn-addr-assign
vpn-addr-assign aaa
no vpn-addr-assign dhcp
vpn-addr-assign local
5520-1(config)#
```

4. Estabeleça as sessões da Autoridade Remota (RA) IPsec/SVC e verifique o comando show vpn-sessiondb remote|svc se o campo IP atribuído está correto (10.20.30.6).

Aplicação do Ative Diretory de "Discagem de permissão de acesso remoto, permitir/negar acesso"

Suporta todas as sessões de VPN Remote Access: IPSec, WebVPN e SVC. Permitir Acesso tem um valor TRUE. Negar Acesso tem um valor de FALSO. O nome do atributo do AD é msNPAllowDialin.

Este exemplo demonstra a criação de um ldap-attribute-map que usa os Cisco Tunneling-Protocols para criar condições de Permitir Acesso (TRUE) e Negar (FALSE). Por exemplo, se você mapear tunnel-protocol=L2TPover IPsec (8), poderá criar uma condição FALSE se tentar

impor o acesso para WebVPN e IPsec. A lógica inversa também se aplica.

Aqui estão as etapas:

1. Em AD server user1 Properties, Dial-In, escolha o acesso de permissão ou negação apropriado para cada usuário. **Observação**: se você escolher a terceira opção, Controlar o acesso por meio da Política de acesso remoto, nenhum valor será retornado do servidor AD, portanto, as permissões que são aplicadas são baseadas na configuração da política de grupo interna do ASA/PIX.
2. No ASA, crie um ldap-attribute-map com este mapeamento:
   ```
   ldap attribute-map LDAP-MAP
   map-name msNPAllowDialin Tunneling-Protocols
   map-value msNPAllowDialin FALSE 8
   map-value msNPAllowDialin TRUE 20
   5540-1#
   ```
   Observação: adicione mais atributos ao mapa conforme necessário. Este exemplo mostra apenas o mínimo para controlar essa função específica (Permitir ou Negar Acesso com base na configuração de Discagem).O que significa ou impõe o ldap-attribute-map?msNPAllowDialin de valor de mapa FALSE 8Negar acesso a um usuário1. A condição de valor FALSE é mapeada para L2TPoverIPsec de protocolo de túnel, (valor 8).Permitir Acesso para usuário2. A condição de valor TRUE mapeia para WebVPN de protocolo de túnel + IPsec, (valor 20).Um usuário WebVPN/IPsec, autenticado como user1 no AD, falharia devido à incompatibilidade de protocolo de túnel.Um L2TPoverIPsec, autenticado como user1 no AD, falharia devido à regra Deny (Negar).Um usuário WebVPN/IPsec, autenticado como user2 no AD, teria êxito (Permitir regra + protocolo de túnel correspondente).Um L2TPoverIPsec, autenticado como user2 no AD, falharia devido à incompatibilidade de protocolo de túnel.
   Suporte para protocolo de túnel, conforme definido nas RFCs 2867 e 2868.

Aplicação do Ative Diretory de "Membro de"/Associação de grupo para permitir ou negar acesso

Esse caso está intimamente relacionado ao Caso 5 e fornece um fluxo mais lógico, além de ser o método recomendado, já que estabelece a verificação de associação de grupo como uma condição.

1. Configure o usuário do AD para ser Membro de um grupo específico. Use um nome que o coloque no topo da hierarquia de grupos (ASA-VPN-Consultants). No AD-LDAP, a associação de grupo é definida pelo atributo do AD memberOf. É importante que o grupo esteja no topo da lista, já que atualmente você só pode aplicar as regras à primeira string group/memberOf. Na versão 7.3, você pode executar a filtragem e a aplicação de vários grupos.
2. No ASA, crie um ldap-attribute-map com o mapeamento mínimo:
   ```
   ldap attribute-map LDAP-MAP
   map-name memberOf Tunneling-Protocols
   map-value memberOf cn=ASA-VPN-Consultants,cn=Users,dc=abcd,dc=com 4
   5540-1#
   ```
   Observação: adicione mais atributos ao mapa conforme necessário. Este exemplo mostra apenas o mínimo para controlar essa função específica (Permitir ou Negar Acesso com base na associação do Grupo).O que significa ou impõe o ldap-attribute-

map?User=joe_consultant, parte do AD, que é membro do grupo do AD ASA-VPN-Consultants pode ter acesso somente se o usuário usar IPsec (tunnel-protocol=4=IPSec).User=joe_consultant, parte do AD, pode falhar o acesso VPN durante qualquer outro cliente de acesso remoto (PPTP/L2TP, L2TP/IPSec, WebVPN/SVC, etc.).User=bill_the_hacker NÃO pode ser permitido em, pois o usuário não tem associação ao AD.

Aplicação de "horas de logon/regras de hora do dia" no Ative Diretory

Este caso de uso descreve como configurar e aplicar as regras de horário no AD/LDAP.

Este é o procedimento para fazer isso:

1. No servidor AD/LDAP:Escolha o usuário.Clique com o botão direito do mouse em **> Propriedades**.Escolha uma guia a ser usada para definir um atributo (Exemplo. guia Geral).Escolha um campo/atributo, por exemplo, o campo Escritório, a ser usado para impor um intervalo de tempo, e insira o nome do intervalo de tempo (por exemplo, Boston). A configuração do Office na GUI é armazenada no atributo AD/LDAP physicalDeliveryOfficeName.
2. No ASA Crie uma tabela de mapeamento de atributos LDAP.Mapeie o atributo AD/LDAP "physicalDeliveryOfficeName" para o atributo ASA "Access-Hours".Exemplo:
```
B200-54(config-time-range)# show run ldap
ldap attribute-map TimeOfDay
map-name physicalDeliveryOfficeName Access-Hours
```
3. No ASA, associe o mapa de atributos LDAP à entrada aaa-server:
```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map TimeOfDay
```
4. No ASA, crie um objeto de intervalo de tempo que tenha o valor de nome atribuído ao usuário (valor Office na etapa 1):
```
B200-54(config-time-range)# show runn time-range
!
time-range Boston
periodic weekdays 8:00 to 17:00
!
```
5. Estabeleça a sessão de acesso remoto VPN: A sessão poderá ser bem-sucedida se estiver dentro do intervalo de tempo.A sessão pode falhar se estiver fora do intervalo de tempo.

Use a configuração ldap-map para mapear um usuário em uma política de grupo específica e use o comando authorization-server-group, no caso de autenticação dupla

1. Neste cenário, a autenticação dupla é usada. O primeiro servidor de autenticação usado é o RADIUS e o segundo servidor de autenticação usado é um servidor LDAP. Configure o servidor LDAP e o servidor RADIUS. Aqui está um exemplo:
```
ASA5585-S10-K9# show runn aaa-server
```

```
aaa-server test-ldap protocol ldap
aaa-server test-ldap (out) host 10.201.246.130
 ldap-base-dn cn=users, dc=htts-sec, dc=com
 ldap-login-password *****
 ldap-login-dn cn=Administrator, cn=Users, dc=htts-sec, dc=com
 server-type microsoft
 ldap-attribute-map Test-Safenet-MAP
aaa-server test-rad protocol radius
aaa-server test-rad (out) host 10.201.249.102
 key *****
```

Defina o mapa de atributos LDAP. Aqui está um exemplo:

```
ASA5585-S10-K9# show runn ldap
ldap attribute-map Test-Safenet-MAP
map-name memberOf IETF-Radius-Class
map-value memberOf "CN=DHCP Users,CN=Users,DC=htts-sec,DC=com" Test-Policy-Safenet
```

Defina o grupo de túneis e associe os servidores RADIUS e LDAP para autenticação. Aqui está um exemplo:

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

Exiba a política de grupo usada na configuração do grupo de túneis:

```
ASA5585-S10-K9# show runn group-policy
group-policy NoAccess internal
group-policy NoAccess attributes
wins-server none
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 0
default-domain none
group-policy Test-Policy-Safenet internal
group-policy Test-Policy-Safenet attributes
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 15
vpn-idle-timeout 30
vpn-tunnel-protocol ikev1 ssl-client ssl-clientless
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Safenet-Group-Policy-SplitAcl
default-domain none
```

Com essa configuração, os usuários do AnyConnect que foram mapeados corretamente com o uso de atributos LDAP não foram colocados na política de grupo, Test-Policy-Safenet. Em vez disso, eles ainda foram colocados na política de grupo padrão, nesse caso NoAccess.Consulte o snippet das depurações (debug ldap 255) e syslogs no level informational:

```
----------------------------------------------------------------------------

memberOf: value = CN=DHCP Users,CN=Users,DC=htts-sec,DC=com

[47]                        mapped to IETF-Radius-Class: value = Test-Policy-Safenet

[47]                        mapped to LDAP-Class: value = Test-Policy-Safenet

----------------------------------------------------------------------------

Syslogs :

%ASA-6-113004: AAA user authentication Successful : server = 10.201.246.130 : user =
```

```
test123

%ASA-6-113003: AAA group policy for user test123 is set to Test-Policy-Safenet

%ASA-6-113011: AAA retrieved user specific group policy (Test-Policy-Safenet) for user =
test123

%ASA-6-113009: AAA retrieved default group policy (NoAccess) for user = test123

%ASA-6-113013: AAA unable to complete the request Error : reason = Simultaneous logins
exceeded for user : user = test123

%ASA-6-716039: Group <DfltGrpPolicy> User <test123> IP <10.116.122.154> Authentication:
rejected, Session Type: WebVPN.
```

Esses syslogs mostram falha, pois o usuário recebeu a política de grupo NoAccess, que tinha login simultâneo definido como 0, embora os syslogs digam que recuperaram uma política de grupo específica do usuário.Para que o usuário seja atribuído na política de grupo, com base no mapa LDAP, você deve ter este comando: **authorization-server-group test-ldap** (nesse caso, **test-ldap** é o nome do servidor LDAP). Aqui está um exemplo:

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
authorization-server-group test-ldap
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

2. Agora, se o primeiro servidor de autenticação (RADIUS, neste exemplo) tiver enviado os atributos específicos do usuário, por exemplo, o atributo classe IEFT, nesse caso, o usuário poderá ser mapeado para a política de grupo enviada pelo RADIUS. Assim, mesmo que o servidor secundário tenha um mapa LDAP configurado e os atributos LDAP do usuário mapeiem o usuário para uma política de grupo diferente, a política de grupo enviada pelo primeiro servidor de autenticação pode ser aplicada. Para que o usuário seja colocado em uma política de grupo com base no atributo de mapa LDAP, você deve especificar esse comando no comando tunnel-group: **authorization-server-group test-ldap**.
3. Se o primeiro servidor de autenticação for SDI ou OTP, que não pode passar o atributo específico do usuário, o usuário se enquadra na política de grupo padrão do grupo de túneis. Nesse caso, NoAccess mesmo que o mapeamento LDAP esteja correto. Nesse caso, você também precisaria do comando, **authorization-server-group test-ldap**, no grupo de túneis para que o usuário fosse colocado na política de grupo correta.
4. Se ambos os servidores forem os mesmos servidores RADIUS ou LDAP, você não precisará do comando **authorization-server-group** para que o bloqueio da política de grupo funcione.

Verificar

```
ASA5585-S10-K9# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : test123                  Index        : 2
Assigned IP  : 10.34.63.1             Public IP    : 10.116.122.154
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License      : AnyConnect Essentials
Encryption   : 3DES 3DES 3DES         Hashing      : SHA1 SHA1 SHA1
Bytes Tx     : 14042                  Bytes Rx     : 8872
Group Policy : Test-Policy-Safenet    Tunnel Group : Test_Safenet
Login Time   : 10:45:28 UTC Fri Sep 12 2014
Duration     : 0h:01m:12s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Troubleshoot

Use esta seção para resolver problemas de configuração.

Depurar a transação LDAP

Essas depurações podem ser usadas para ajudar a isolar problemas com a configuração do DAP:

- debug ldap 255
- debug dap trace
- debug aaa authentication

O ASA não pode autenticar usuários do servidor LDAP

Caso o ASA não possa autenticar usuários do servidor LDAP, aqui estão alguns exemplos de depurações:

```
ldap 255 output:[1555805] Session Start[1555805] New request Session, context
0xcd66c028, reqType = 1[1555805]
Fiber started[1555805] Creating LDAP context with uri=ldaps://172.30.74.70:636
[1555805] Connect to LDAP server:
ldaps://172.30.74.70:636, status = Successful[1555805] supportedLDAPVersion:
value = 3[1555805]
supportedLDAPVersion: value = 2[1555805] Binding as administrator[1555805]
Performing Simple
authentication for sysservices to 172.30.74.70[1555805] Simple authentication
for sysservices returned code (49)
Invalid credentials[1555805] Failed to bind as administrator returned code
(-1) Can't contact LDAP server[1555805]
Fiber exit Tx=222 bytes Rx=605 bytes, status=-2[1555805] Session End
```

A partir dessas depurações, o formato do DN de logon LDAP está incorreto ou a senha está incorreta; portanto, verifique ambos para resolver o problema.

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.