Ejemplo de Configuración de Uso de Mapas de Atributo LDAP

Contenido

Introducción

Este documento describe cómo cualquier atributo de Microsoft/AD se puede asignar a un atributo de Cisco.

Procedimiento

1. En el servidor de Active Directory (AD)/protocolo ligero de acceso a directorios (LDAP):Elija **user1**.Haga clic con el botón derecho **> Propiedades**.Elija una pestaña que se utilizará para establecer un atributo (por ejemplo, la pestaña General).Elija un campo/atributo, por ejemplo, el campo Office, que se utilizará para aplicar el rango de tiempo, e ingrese el texto del banner (por ejemplo, Bienvenido a LDAP !!!!). La configuración de Office en la GUI se almacena en el atributo físicoDeliveryOfficeName de AD/LDAP.
2. En el dispositivo de seguridad adaptable (ASA), para crear una tabla de asignación de atributos LDAP, asigne el atributo AD/LDAP physicalDeliveryOfficeName al atributo ASA Banner1:

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

3. Asocie el mapa de atributo LDAP a la 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. Establezca la sesión de acceso remoto y verifique que el Banner Welcome to LDAP !!!! se presente al usuario de VPN.

Colocar usuarios de LDAP en una política de grupo específica (ejemplo genérico)

En este ejemplo se muestra la autenticación del usuario 1 en el servidor AD-LDAP y se recupera el valor del campo del departamento para que se pueda asignar a una política de grupo ASA/PIX desde la cual se pueden aplicar las políticas.

1. En el servidor AD/LDAP:Elija **user1**.Haga clic con el botón derecho del ratón **>** **Propiedades**.Elija una pestaña que se utilizará para establecer un atributo (por ejemplo, la pestaña Organización).Elija un campo/atributo, por ejemplo, Department, que se utilizará para aplicar una política de grupo, e ingrese el valor de la política de grupo (Group-Policy1) en ASA/PIX. La configuración del departamento en la GUI se almacena en el departamento de atributos de AD/LDAP.
2. Defina una tabla 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 la política de grupo, Group_policy1, en el dispositivo y los atributos de política requeridos.
4. Establezca el túnel de acceso remoto VPN y verifique que la sesión hereda los atributos de Group-Policy1 (y cualquier otro atributo aplicable de la política de grupo predeterminada). **Nota**: Añada más atributos al mapa según sea necesario. Este ejemplo muestra solamente el mínimo para controlar esta función específica (colocar un usuario en una política de grupo específica de ASA/PIX 7.1.x). El tercer ejemplo muestra este tipo de mapa.

Configurar una política de grupo de NOACCESS

Puede crear una política de grupo NOACCESS para denegar la conexión VPN cuando el usuario no forma parte de ninguno de los grupos LDAP. Este fragmento de configuración se muestra como referencia:

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

Debe aplicar esta política de grupo como política de grupo predeterminada al grupo de túnel. Esto permite a los usuarios que obtienen una asignación del mapa de atributos LDAP, por ejemplo, aquellos que pertenecen a un grupo LDAP deseado, obtener sus políticas de grupo deseadas, y a los usuarios que no obtienen ninguna asignación, por ejemplo, aquellos que no pertenecen a ninguno de los grupos LDAP deseados, obtener la política de grupo NOACCESS del grupo de

túnel, que bloquea el acceso para ellos.

> **Sugerencia**: Dado que el atributo vpn-simultanealinicios de sesión se establece en 0 aquí, también debe definirse explícitamente en todas las demás políticas de grupo; de lo contrario, se puede heredar de la política de grupo predeterminada para ese grupo de túnel, que en este caso es la política NOACCESS.

Atributos basados en grupo Aplicación de políticas (ejemplo)

1. En el servidor AD-LDAP, Usuarios y equipos de Active Directory, configure un registro de usuario (VPNUserGroup) que represente un grupo en el que se configuren los atributos VPN.
2. En el servidor AD-LDAP, Usuarios y equipos de Active Directory, defina el campo Departamento de cada registro de usuario para que señale al registro de grupo (VPNUserGroup) en el paso 1. El nombre de usuario de este ejemplo es web1. **Nota**: El atributo AD del departamento se ha utilizado sólo porque, lógicamente, el departamento hace referencia a la política de grupo. En realidad, cualquier campo podría ser utilizado. El requisito es que este campo tenga que asignarse al atributo de Cisco VPN Group-Policy, como se muestra en este ejemplo.
3. Defina una tabla 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)#
   ```

   Los dos atributos de AD-LDAP, Description y Office (representados por la descripción de los nombres de AD y PhysicalDeliveryOfficeName) son los atributos de registro de grupo (para VPNUSerGroup) que se asignan a los atributos de Cisco VPN Banner1 e IETF-Radius-Session-Timeout.El atributo del departamento es para que el registro de usuario se asigne al nombre de la política de grupo externa en el ASA (VPNUSer), que luego se asigna nuevamente al registro VPNuserGroup en el servidor AD-LDAP, donde se definen los atributos.**Nota**: El atributo de Cisco (Group-Policy) debe definirse en ldap-attribute-map. Su atributo AD asignado puede ser cualquier atributo AD configurable. En este ejemplo se utiliza el nombre de departamento porque es el nombre más lógico que hace referencia a la directiva de grupo.
4. Configure el servidor aaa con el nombre ldap-attribute-map que se utilizará para las operaciones de autenticación LDAP, autorización y contabilidad (AAA):

   ```
   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 un grupo de túnel con autenticación LDAP o autorización LDAP. Ejemplo con autenticación LDAP. Realiza la aplicación de políticas de atributos de autenticación +

(autorización) si se han definido atributos.

```
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)#
```

Ejemplo con autorización LDAP. Configuración utilizada para certificados digitales.

```
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 una política de grupo externa. El nombre de la política de grupo es el valor del registro de usuario de AD-LDAP que representa el grupo (VPNUserGroup).

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

7. Establezca el túnel y compruebe que los atributos se aplican. En este caso, Banner y Session-Timeout se aplican desde el registro VPNuserGroup en AD.

Aplicación de Active Directory de "Asignar una dirección IP estática" para túneles IPsec y SVC

El atributo AD es msRADIUSFramedIPAddress. El atributo se configura en Propiedades de usuario de AD, ficha Marcado de entrada, Asignar una dirección IP estática.

Éstos son los pasos:

1. En el servidor AD, en Propiedades del usuario, ficha Marcado de entrada, Asignar una dirección IP estática, introduzca el valor de la dirección IP para asignarla a la sesión IPsec/SVC (10.20.30.6).
2. En el ASA, cree un ldap-attribute-map con esta asignación:

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

3. En ASA, verifique que la asignación de dirección vpn esté configurada 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. Establezca las sesiones de Autoridad remota (RA) IPsec/SVC y verifique que el campo de IP asignada es correcto (10.20.30.6) en show vpn-sessiondb remote|svc.

Aplicación en Active Directory de "Acceso telefónico de permiso de acceso remoto, permitir/denegar acceso"

Admite todas las sesiones de acceso remoto a VPN: IPSec, WebVPN y SVC. Permitir acceso

tiene el valor TRUE. Denegar acceso tiene el valor FALSE. El nombre del atributo de AD es msNPAllowDialin.

En este ejemplo se muestra la creación de un mapa de atributos ldap que utiliza los protocolos de túnel de Cisco para crear condiciones Permitir acceso (TRUE) y Denegar (FALSE). Por ejemplo, si asigna tunnel-protocol=L2TPover IPsec (8), puede crear una condición FALSE si intenta forzar el acceso para WebVPN e IPsec. También se aplica la lógica inversa.

Éstos son los pasos:

1. En Propiedades de usuario1 del servidor AD, Marcado de entrada, elija las opciones Permitir acceso o Denegar acceso para cada usuario. **Nota**: si elige la tercera opción, Controlar el acceso a través de la política de acceso remoto, no se devuelve ningún valor desde el servidor AD, por lo que los permisos que se aplican se basan en la configuración de la política de grupo interna de ASA/PIX.
2. En ASA, cree un ldap-attribute-map con esta asignación:
   ```
   ldap attribute-map LDAP-MAP
   map-name msNPAllowDialin Tunneling-Protocols
   map-value msNPAllowDialin FALSE 8
   map-value msNPAllowDialin TRUE 20
   5540-1#
   ```
   Nota: Añada más atributos al mapa según sea necesario. En este ejemplo se muestra sólo el mínimo necesario para controlar esta función específica (Permitir o Denegar acceso según la configuración de marcado de entrada).¿Qué significa o impone ldap-attribute-map?map-value msNPAllowDialin FALSE 8Denegar acceso para un usuario1. La condición de valor FALSE se asigna al protocolo de túnel L2TPoverIPsec, (valor 8).Permitir acceso para el usuario 2 . La condición de valor TRUE se asigna al protocolo de túnel WebVPN + IPsec, (valor 20).Un usuario de WebVPN/IPsec, autenticado como usuario1 en AD, fallaría debido a la discordancia de protocolo de túnel.Un L2TPoverIPsec, autenticado como usuario1 en AD, fallaría debido a la regla Denegar.Un usuario de WebVPN/IPsec, autenticado como user2 en AD, se realizará correctamente (regla de permiso + protocolo de túnel coincidente).Un L2TPoverIPsec, autenticado como usuario2 en AD, fallaría debido a la discordancia de protocolo de túnel.
   Compatibilidad con el protocolo de túnel, como se define en los RFC 2867 y 2868.

Aplicación de Active Directory de "Miembro de"/pertenencia a grupo para permitir o denegar acceso

Este caso está estrechamente relacionado con el caso 5, y proporciona un flujo más lógico, y es el método recomendado, ya que establece la verificación de pertenencia a grupo como una condición.

1. Configure el usuario de AD para que sea miembro de un grupo específico. Utilice un nombre que lo sitúe en la parte superior de la jerarquía del grupo (ASA-VPN-Consultants). En AD-LDAP, la pertenencia a un grupo la define el atributo memberOf de AD. Es importante que el grupo esté al principio de la lista, ya que actualmente sólo puede aplicar las reglas a la primera cadena group/memberOf. En la versión 7.3, puede realizar el filtrado y la aplicación en varios grupos.
2. En ASA, cree un ldap-attribute-map con la asignación mínima:
   ```
   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#
```

Nota: Añada más atributos al mapa según sea necesario. En este ejemplo se muestra sólo el mínimo necesario para controlar esta función específica (Permitir o Denegar acceso según la pertenencia a un grupo).¿Qué significa o impone ldap-attribute-map?User=joe_consulting, parte de AD, que es miembro del grupo de AD ASA-VPN-Consultants puede tener acceso solo si el usuario utiliza IPsec (tunnel-protocol=4=IPSec).User=joe_consulting, parte de AD, puede fallar el acceso VPN durante cualquier otro cliente de acceso remoto (PPTP/L2TP, L2TP/IPSec, WebVPN/SVC, etc.).User=bill_the_hacker NO se puede permitir en puesto que el usuario no es miembro de AD.

Aplicación de Active Directory de "Horas de inicio de sesión/Normas de hora del día"

Este caso práctico describe cómo configurar y aplicar las reglas de hora del día en AD/LDAP.

Este es el procedimiento para hacer esto:

1. En el servidor AD/LDAP:Elija el usuario.Haga clic con el botón derecho **> Propiedades**.Elija una pestaña que se utilizará para establecer un atributo (Ejemplo: pestaña General).Elija un campo/atributo, por ejemplo, el campo Office, que se utilizará para aplicar el rango de tiempo, e introduzca el nombre del rango de tiempo (por ejemplo, Boston). La configuración de Office en la GUI se almacena en el atributo físicoDeliveryOfficeName de AD/LDAP.
2. En el ASA Cree una tabla de asignación de atributos LDAP.Asigne el atributo AD/LDAP "physicalDeliveryOfficeName" al atributo ASA "Access-Hours".Ejemplo:
```
B200-54(config-time-range)# show run ldap
ldap attribute-map TimeOfDay
map-name physicalDeliveryOfficeName Access-Hours
```
3. En ASA, asocie el mapa de atributo LDAP a la 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. En ASA, cree un objeto de intervalo de tiempo que tenga el valor name asignado al usuario (valor de Office en el paso 1):
```
B200-54(config-time-range)# show runn time-range
!
time-range Boston
periodic weekdays 8:00 to 17:00
!
```
5. Establezca la sesión de acceso remoto VPN: La sesión puede tener éxito si se encuentra dentro del rango de tiempo.La sesión puede fallar si está fuera del rango de tiempo.

Utilice la configuración ldap-map para asignar un usuario a una política de grupo específica y utilice el comando authorization-server-group, en caso de doble autenticación

1. En este escenario, se utiliza la doble autenticación. El primer servidor de autenticación utilizado es RADIUS y el segundo servidor de autenticación utilizado es un servidor LDAP. Configure el servidor LDAP así como el servidor RADIUS. Aquí tiene un ejemplo:

```
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 el mapa de atributos LDAP. Aquí tiene un ejemplo:

```
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 el grupo de túnel y asocie el servidor RADIUS y LDAP para la autenticación. Aquí tiene un ejemplo:

```
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
```

Vea la política de grupo que se utiliza en la configuración del grupo de túnel:

```
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
```

Con esta configuración, los usuarios de AnyConnect que se asignaron correctamente con el uso de atributos LDAP no se colocaron en la política de grupo Test-Policy-Safenet. En su lugar, seguían estando en la política de grupo predeterminada, en este caso NoAccess.Vea el fragmento de los debugs (debug ldap 255) y los syslogs en el nivel informativo:

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

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.
```

Estos syslogs muestran fallas ya que al usuario se le dio la política de grupo NoAccess que tenía el login simultáneo establecido en 0 aunque los syslogs digan que recuperó una política de grupo específica del usuario.Para tener al usuario asignado en la política de grupo, basada en el LDAP-map, debe tener este comando: **authorization-server-group test-ldap** (en este caso, **test-ldap** es el nombre del servidor LDAP). Aquí tiene un ejemplo:

```
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. Ahora, si el primer servidor de autenticación (RADIUS, en este ejemplo) envió los atributos específicos del usuario, por ejemplo, el atributo IEFT-class, en ese caso, el usuario se puede asignar a la política de grupo enviada por RADIUS. Por lo tanto, aunque el servidor secundario tiene un mapa LDAP configurado y los atributos LDAP del usuario asignan al usuario a una política de grupo diferente, la política de grupo enviada por el primer servidor de autenticación se puede aplicar. Para que el usuario se coloque en una política de grupo basada en el atributo de mapa LDAP, debe especificar este comando bajo tunnel-group: **authorization-server-group test-ldap**.
3. Si el primer servidor de autenticación es SDI u OTP, que no puede pasar el atributo específico del usuario, el usuario caería en la política de grupo predeterminada del grupo de túnel. En este caso, NoAccess aunque la asignación LDAP sea correcta. En este caso, también necesitaría el comando **authorization-server-group test-ldap**, bajo tunnel-group para que el usuario se coloque en la política de grupo correcta.
4. Si ambos servidores son los mismos servidores RADIUS o LDAP, no necesita el comando **authorization-server-group** para que funcione el bloqueo de política de grupo.

Verificación

```
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 sección para resolver problemas de configuración.

Depurar la transacción LDAP

Estas depuraciones se pueden utilizar para ayudar a aislar problemas con la configuración DAP:

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

ASA no puede autenticar usuarios del servidor LDAP

En caso de que ASA no pueda autenticar a los usuarios desde el servidor LDAP, aquí hay algunos ejemplos de depuración:

```
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
```

Desde estos debugs, el formato LDAP Login DN es incorrecto o la contraseña es incorrecta, así que verifique ambos para resolver el problema.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).