Use LDAP Attribute Maps Configuration Example

Contents

Introduction

This document describes how any Microsoft/AD attribute can be mapped to a Cisco attribute.

Procedure

1. On the Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) server:Choose **user1**.Right-click **> Properties**.Choose a tab to be used in order to set an attribute (for example, General tab).Choose a field/attribute, for example, the Office field, to be used in order to enforce time-range, and enter the banner text (for example, Welcome to LDAP !!!!). The Office configuration on the GUI is stored in the AD/LDAP attribute physicalDeliveryOfficeName.
2. On the Adaptive Security Appliance (ASA), in order to create an LDAP attribute mapping table, map the AD/LDAP attribute physicalDeliveryOfficeName to the ASA attribute Banner1:

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

3. Associate the LDAP attribute map to the aaa-server entry:

```
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. Establish the Remote Access session and verify that the Banner Welcome to LDAP !!!! is presented to the VPN user.

Place LDAP Users in a Specific Group-Policy (Generic Example)

This example demonstrates the authentication of user1 on the AD-LDAP server and retrieves the department field value so it can be mapped to an ASA/PIX group-policy from which policies can be enforced.

1. On the AD/LDAP server:Choose **user1**.Right-click **> Properties**.Choose a tab to be used in order to set an attribute (for example, Organization tab).Choose a field/attribute, for example, Department, to be used in order to enforce a group-policy, and enter the value of the group-policy (Group-Policy1) on the ASA/PIX. The Department configuration on the GUI is stored in the AD/LDAP attribute department.
2. Define an ldap-attribute-map table.

   ```
   5520-1(config)# show runn ldap
   ldap attribute-map Our-AD-Map
   map-name department Group-Policy
   5520-1(config)#
   ```
3. Define the group-policy, Group_policy1, on the appliance and the required policy attributes.
4. Establish the VPN remote access tunnel and verify that the session inherits the attributes from Group-Policy1 (and any other applicable attributes from the default group-policy). **Note**: Add more attributes to the map as required. This example shows only the minimum to control this specific function (place a user in a specific ASA/PIX 7.1.x group-policy). The third example shows this type of map.

Configure a NOACCESS Group-policy

You can create a NOACCESS group-policy in order to deny the VPN connection when the user is not part of any of the LDAP groups. This configuration snippet is shown for your reference:

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

You must apply this group policy as a default group policy to the tunnel-group. This allows users who get a mapping from the LDAP attribute map, for example, those who belong to a desired LDAP group, to get their desired group policies, and users who do not get any mapping, for example, those who do not belong to any of the desired LDAP groups, to get NOACCESS group-policy from the tunnel-group, which blocks the access for them.

> **Tip**: Since the vpn-simultaneous-logins attribute is set to 0 here, it must be explicitly defined in all the other group-policies as well; otherwise, it can be inherited from the default group-policy for that tunnel group, which in this case is the NOACCESS policy.

Group-Based Attributes Policy Enforcement (Example)

1. On the AD-LDAP server, Active Directory Users and Computers, set up a user record (VPNUserGroup) that represents a group where the VPN attributes are configured.
2. On the AD-LDAP server, Active Directory Users and Computers, define each user record's Department field to point to the group-record (VPNUserGroup) in Step 1. The user name in this example is web1. **Note**: The Department AD attribute was used only because logically department refers to the group-policy. In reality, any field could be used. The requirement is that this field has to map to the Cisco VPN attribute Group-Policy as shown in this example.
3. Define an ldap-attribute-map table:

   ```
   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)#
   ```

   The two AD-LDAP attributes, Description and Office, (represented by AD names description and PhysicalDeliveryOfficeName) are the group record attributes (for VPNUSerGroup) which maps to Cisco VPN attributes Banner1 and IETF-Radius-Session-Timeout.The department attribute is for the user record to map to the name of external group-policy on the ASA (VPNUSer), which then maps back to the VPNuserGroup record on the AD-LDAP server, where attributes are defined.**Note**: The Cisco attribute (Group-Policy) must be defined in the ldap-attribute-map. Its mapped AD-attribute can be any settable AD attribute. This example uses department because it is the most logical name that refers to group-policy.
4. Configure the aaa-server with the ldap-attribute-map name to be used for LDAP Authentication, Authorization, and Accounting (AAA) operations:

   ```
   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. Define a tunnel-group with with either LDAP Authentication or LDAP Authorization. Example with LDAP Authentication. Performs authentication + (authorization) attribute policy enforcement if attributes are defined.

   ```
   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)#
   ```

   Example with LDAP Authorization. Configuration used for Digital Certificates.

   ```
   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. Define an external group-policy. The name of the group-policy is the value of the AD-LDAP

user record that represents the group (VPNUserGroup).

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

7. Establish the tunnel and verify that attributes are enforced. In this case, the Banner and Session-Timeout is enforced from the VPNuserGroup record on the AD.

Active Directory Enforcement of “Assign a Static IP Address” for IPsec and SVC Tunnels

The AD attribute is msRADIUSFramedIPAddress. The attribute is configured in AD User Properties, Dial-in tab, Assign a Static IP Address.

Here are the steps:

1. On the AD server, under user Properties, Dial-in tab, Assign a Static IP Address, enter the value of the IP Address in order to assign to the IPsec/SVC session (10.20.30.6).
2. On the ASA create a an ldap-attribute-map with this mapping:

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

3. On the ASA, verify the vpn-address-assigment is configured to include 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. Establish the IPsec/SVC Remote Authority (RA) sessions and verify the show vpn-sessiondb remote|svc that the Assigned IP field is correct (10.20.30.6).

Active Directory Enforcement of “Remote Access Permission Dial-in, Allow/Deny Access ”

Supports all VPN Remote Acccess sessions: IPSec, WebVPN, and SVC. Allow Access has a value of TRUE. Deny Acccess has a value of FALSE. The AD attribute name is msNPAllowDialin.

This example demonstrates the creation of an ldap-attribute-map that uses the Cisco Tunneling-Protocols to create Allow Access (TRUE) and Deny (FALSE) conditions. For example, if you map the tunnel-protocol=L2TPover IPsec (8), you can create a FALSE condition if you try to enforce access for WebVPN and IPsec. The reverse logic applies too.

Here are the steps:

1. On the AD server user1 Properties, Dial-In, choose the appropriate allow Access or Deny access for each user. **Note**: If you choose the third option, Control access through the Remote Access Policy, no value is returned from the AD server, so the permissions that are enforced are based on the ASA/PIX’s internal group-policy’s setting.
2. On the ASA, create an ldap-attribute-map with this mapping:

   ```
   ldap attribute-map LDAP-MAP
   map-name msNPAllowDialin Tunneling-Protocols
   map-value msNPAllowDialin FALSE 8
   map-value msNPAllowDialin TRUE 20
   ```

```
5540-1#
```

Note: Add more attributes to the map as required. This example shows only the minimum to control this specific function (Allow or Deny Access based on Dial-In setting).What does the ldap-attribute-map mean or enforce?map-value msNPAllowDialin FALSE 8Deny Access for a user1. The FALSE value condition maps to tunnel-protocol L2TPoverIPsec, (value 8).Allow Access for user2 . The TRUE value condition maps to tunnel-protocol WebVPN + IPsec, (value 20).A WebVPN/IPsec user, authenticaticated as user1 on AD, would fail due to the tunnel-protocol mismatch.A L2TPoverIPsec, authenticaticated as user1 on AD, would fail due to the Deny rule.A WebVPN/IPsec user, authenticaticated as user2 on AD, would succeed (Allow rule + matched tunnel protocol).A L2TPoverIPsec, authenticaticated as user2 on AD, would fail due to the tunnel-protocol mismatch.

Support for Tunnel Protocol, as defined in RFCs 2867 and 2868.

Active Directory Enforcement of “Member Of ”/Group Membership to Allow or Deny Access

This case is closely related to Case 5, and provides for a more logical flow, and is the recommended method, since it establishes the group-membership check as a condition.

1. Configure the AD user to be Member Of a specific group. Use a name that places it at the top of the group-hierarchy (ASA-VPN-Consultants). In AD-LDAP, Group membership is defined by the AD attribute memberOf. It is important that the group be at the top of the list, since you can currently only apply the rules to the first group/memberOf string. In Release 7.3, you are able to perform multiple-group filtering and enforcement.
2. On the ASA, create an ldap-attribute-map with the the minimum mapping:
   ```
   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#
   ```
   Note: Add more attributes to the map as required. This examples shows only the minimum to control this specific function (Allow or Deny Access based on Group membership).What does the ldap-attribute-map mean or enforce?User=joe_consultant, part of AD, which is member of AD group ASA-VPN-Consultants can be allowed access only if the user uses IPsec (tunnel-protocol=4=IPSec).User=joe_consultant, part of AD, can fail VPN access during any other remote access client (PPTP/L2TP, L2TP/IPSec, WebVPN/SVC, and so on).User=bill_the_hacker can NOT be allowed in since the user has no AD membership.

Active Directory Enforcement of “Logon Hours/Time-of-Day Rules”

This use case describes how to set up and enforce the Time of Day rules on AD/LDAP.

Here is the procedure to do this:

1. On the AD/LDAP server:Choose the user.Right-click **> Properties**.Choose a tab to be used in order to set an attribute (Example. General tab).Choose a field/attribute, for example, the Office field, to be used in order to enforce time-range, and enter the name of the time-range (for example, Boston). The Office configuration on the GUI is stored in the AD/LDAP attribute physicalDeliveryOfficeName.
2. On the ASA Create an LDAP attribute mapping table.Map the AD/LDAP attribute

"physicalDeliveryOfficeName" to the ASA attribute "Access-Hours".Example:

```
B200-54(config-time-range)# show run ldap
ldap attribute-map TimeOfDay
map-name physicalDeliveryOfficeName Access-Hours
```

3. On the ASA, associate the LDAP attribute map to the aaa-server entry:

```
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. On the ASA, create a time-range object that has the name value that is assigned to the user (Office value in step 1):

```
B200-54(config-time-range)# show runn time-range
!
time-range Boston
periodic weekdays 8:00 to 17:00
!
```

5. Establish the VPN remote access session: The session can succeed if within the time-range.The session can fail if outside the time-range.

Use the ldap-map Configuration to Map a User into a Specific Group-policy and Use the authorization-server-group Command, in the Case of Double Authentication

1. In this scenario, double authentication is used. The first authentication server used is RADIUS, and the second authentication sever used is a LDAP server. Configure the LDAP server as well as the RADIUS server. Here is an example:

```
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 *****
```

   Definine the LDAP attribute-map. Here is an example:

```
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
```

   Define the tunnel-group and associate the RADIUS and LDAP server for authentication. Here is an example:

```
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
```

View the group-policy that is used in the tunnel-group configuration:

```
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
```

With this configuration, AnyConnect users who were mapped correctly with the use of LDAP attributes were not placed in the group-policy, Test-Policy-Safenet. Instead, they were still placed in the default group-policy, in this case NoAccess.See the snippet of the debugs (debug ldap 255) and syslogs at 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.
```

These syslogs show failure as the user was given the NoAccess group-policy which had simultaneous-login set to 0 even though syslogs say it retrieved a user specific group-policy.In order to have the user assigned in the group-policy, based on the LDAP-map, you must have this command: **authorization-server-group test-ldap** (in this case, **test-ldap** is the LDAP server name). Here is an example:

```
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. Now, if the first authentication server (RADIUS, in this example) did send the user-specific attributes, for example, the IEFT-class attribute, in that case, the user can be mapped to the group-policy sent by RADIUS. So even though the secondary server has a LDAP map configured and the user's LDAP attributes do map the user to a different group-policy, the group-policy sent by the first authentication server can be enforced. In order to have the user placed into a group-policy based on the LDAP map attribute, you must specify this command under the tunnel-group: **authorization-server-group test-ldap**.
3. If the first authentication server is SDI or OTP, which cannot pass the user-specific attribute, then the user would fall into the default group-policy of the tunnel-group. In this case, NoAccess even though the LDAP mapping is correct. In this case, you also would need the command, **authorization-server-group test-ldap**, under the tunnel-group for the user to be placed into the correct group-policy.
4. If both of the servers are the same RADIUS or LDAP servers, then you do not need the **authorization-server-group** command in order for the group-policy lock to work.

Verify

```
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 this section to troubleshoot your configuration.

Debug the LDAP Transaction

These debugs can be used in order to help isolate issues with the DAP configuraiton:

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

ASA is Not Able to Authenticate Users from LDAP Server

In case the ASA is not able to authenticate users from LDAP serve, here are some sample debugs:

```
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
```

From these debugs, either the LDAP Login DN format is incorrect or the password is incorrect so verify both in order to resolve the issue.