LDAP属性マップの使用の設定例

内容

概要

このドキュメントでは、任意のMicrosoft/AD属性をCisco属性にマッピングする方法について説明します。

手順

1. Active Directory(AD)/Lightweight Directory Access Protocol(LDAP)サーバで、次の手順を実行します。**user1**を選択します。[>Properties] を右クリックします。属性を設定するために使用するタブを選択します（たとえば、[General]タブ）。[Office]フィールドなどのフィールド/属性を選択して時間範囲を適用し、バナーテキストを入力します(たとえば、[Welcome to LDAP !!!!])。GUIのOffice設定は、AD/LDAP属性physicalDeliveryOfficeNameに保存されます。
2. 適応型セキュリティアプライアンス(ASA)で、LDAP属性マッピングテーブルを作成するために、AD/LDAP属性physicalDeliveryOfficeNameをASA属性Banner1にマッピングします。

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

3. LDAP 属性マップを aaa-server エントリに関連付けます。

```
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. リモートアクセスセッションを確立し、[Welcome to LDAP !!!!]というバナーがVPNユーザに表示されることを確認します。

特定のグループポリシーへのLDAPユーザの配置（一般的な例）

この例では、AD-LDAPサーバでのuser1の認証を示し、departmentフィールドの値を取得して、ポリシーを適用できるASA/PIXグループポリシーにマッピングできるようにします。

1. AD/LDAP サーバで次を実行します。**user1**を選択します。[>Properties] を右クリックします。属性を設定するために使用するタブを選択します(たとえば、[組織(Organization)]タブ)。グループポリシーを適用するために使用するフィールド/属性（たとえば、Department）を選択し、ASA/PIXのグループポリシー(Group-Policy1)の値を入力します。GUIのDepartment設定は、AD/LDAP属性departmentに保存されます。
2. LDAP 属性マップ テーブルを定義します。

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

3. アプライアンスでグループポリシーGroup_policy1を定義し、必要なポリシー属性を定義します。
4. このユーザとして VPN によるリモート アクセストンネルを確立し、Group-Policy1 からの属性（およびその他に適用可能な、デフォルトのグループ ポリシーからの属性）がセッションに継承されていることを確認します。 **注**：必要に応じて、マップに属性を追加します。この例では、この特別な機能（ユーザに特定の ASA/PIX 7.1.x グループ ポリシーを割り当てる機能）の最低限の操作を示したものです。3 番目の例は、このタイプのマップを示します。

NOACCESS グループ ポリシーの設定

ユーザが LDAP グループのいずれにも所属しない場合に VPN 接続を拒否するよう、NOACCESS グループ ポリシーを作成できます。参考として、この設定のスニペットを示します。

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

トンネル グループには、このグループ ポリシーをデフォルト グループ ポリシーとして適用する必要があります。これにより、LDAP属性マップからマッピングを取得するユーザ（たとえば、目的のLDAPグループに属するユーザ）は目的のグループポリシーを取得でき、マッピングを取得しないユーザ（たとえば、目的のLDAPグループに属さないユーザ）はトンネルグループからNOACCESSグループポリシーを取得して、それらのアクセスをブロックできます。

ヒント：ここではvpn-simultaneous-logins属性が0に設定されているため、他のすべてのグループポリシーでもこの属性を明示的に定義する必要があります。そうでない場合は、そのトンネルグループのデフォルトのグループポリシー（この場合はNOACCESSポリシー）から属性を継承できます。

グループベース属性ポリシーの適用（例）

1. AD-LDAP サーバの [Active Directory Users and Computers] で、VPN 属性を設定するグループを示すユーザレコード（VPNUserGroup）を設定します。
2. AD-LDAP サーバの [Active Directory Users and Computers] で、各ユーザ レコードの [Department] フィールドが手順 1 のグループレコード（VPNUserGroup）を指すように定義します。この例でのユーザ名は web1 です。 **注**:Department AD属性は、論理的にdepartmentがグループポリシーを参照するため、使用されました。実際には、どのフィールドでも使用できます。以下の例のように、このフィールドが Cisco VPN 属性 Group-Policy に関連付けられることが要件となっています。
3. LDAP 属性マップテーブルを定義します。

```
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)#
```

2つのAD-LDAP属性であるDescriptionおよびOffice（AD names descriptionおよびPhysicalDeliveryOfficeNameで表される）は、Cisco VPN属性Banner1およびIETF-Radius-Session-Timeoutにマッピングされるグループレコード属性（VPNUSerGroup用）です。department 属性は、ASA の外部グループ ポリシーへマッピングするユーザ レコードのためのもので（VPNUSer）、これは属性が定義されるとき再度 AD-LDAP サーバの VPNuserGroup レコードにマッピングされます。**注**:Cisco属性(Group-Policy)は、ldap属性マップで定義する必要があります。マッピングされた AD 属性は、設定可能な AD 属性であれば任意です。この例では、グループ ポリシーを表すのに最も論理的な名前である department を使用しています。

4. aaa-server に、認証、認可、およびアカウンティング（AAA）処理で使用する LDAP 属性マップ名を設定します。

```
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. LDAP 認証または LDAP 認可のいずれかで、トンネルグループを定義します。 LDAP 認証の例：属性が定義されている場合、認証 +（認可）属性へポリシーを適用します。

```
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)#
```

LDAP 認可の例：デジタル証明書に使用される設定。

```
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. 外部グループ ポリシーを定義します。グループ ポリシーの名前は、グループ（VPNUserGroup）を示す AD-LDAP ユーザ レコードの値です。
```
5520-1(config)# show runn group-policy VPNUserGroup
group-policy VPNUserGroup external server-group LDAP-AD11
5520-1(config)#
```
7. トンネルを確立し、属性が適用されていることを確認します。このケースでは、AD 上の VPNuserGroup レコードから Banner と Session-Timeout が適用されます。

Active DirectoryでのIPsecおよびSVCトンネルの「静的IPアドレスの割り当て」の適用

AD 属性は msRADIUSFramedIPAddress です。この属性は、[AD User Properties]の[Dial-in]タブの[Assign a Static IP Address]で設定します。

内容は次のとおりです。

1. ADサーバの[User Properties]の[Dial-in]タブで、[Assign a Static IP Address]に、IPsec/SVCセッション(10.20.30.6)に割り当てるIPアドレスの値を入力します。
2. ASA で、以下のマッピングをした LDAP 属性マップを作成します。
```
5540-1# show running-config ldap
ldap attribute-map Assign-IP
map-name msRADIUSFramedIPAddress IETF-Radius-Framed-IP-Address
5540-1#
```
3. ASAで、vpn-address-assigmentがvpn-addr-assign-aaaを含むように設定されていることを確認します。
```
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. IPsec/SVC Remote Authority(RA)セッションを確立し、show vpn-sessiondb remote|svcを実行して、[Assigned IP]フィールド(10.20.30.6)が正しいことを確認します。

Active Directoryでの「リモートアクセス許可ダイヤルイン、アクセスの許可/拒否」の適用

すべてのVPNリモートアクセスセッション（IPSec、WebVPN、およびSVC）をサポートします。Allow Access の値は TRUE です。Deny Acccess の値は FALSE です。AD 属性名は msNPAllowDialin です。

この例では、Cisco Tunneling-Protocols を使用し、Allow Access（TRUE）と Deny（FALSE）条件を指定する LDAP 属性マップの作成を示します。たとえば、tunnel-protocol=L2TPover IPsec（8）をマッピングすると、WebVPN、IPsec のアクセスを強制しようとした場合に FALSE となる条件を作成できます。逆の口ジックも適用されます。

内容は次のとおりです。

1. ADサーバの[user1 Properties]、[Dial-In]で、各ユーザに対して適切な[allow Access]または[Deny access]を選択します。 **注：**3番目のオプションである[Control access through the Remote Access Policy]を選択すると、ADサーバから値が返されないため、適用される権限

はASA/PIXの内部グループポリシーの設定に基づきます。

2. ASA で、以下のマッピングをした LDAP 属性マップを作成します。

```
ldap attribute-map LDAP-MAP
map-name msNPAllowDialin Tunneling-Protocols
map-value msNPAllowDialin FALSE 8
map-value msNPAllowDialin TRUE 20
5540-1#
```

注：必要に応じて、マップに属性を追加します。この例では、この特別な機能の最低限の操作（Dial-In の設定に基づいて [Allow] または [Deny Access] を指定）を示したものです。LDAP 属性マップ何を意味し、強制しますか。map-value msNPAllowDialin FALSE 8user1 のアクセスの拒否。FALSE 値の条件は、トンネル プロトコル L2TPoverIPsec（値 8）にマッピングされます。user2 のアクセスの許可。TRUE 値の条件は、トンネル プロトコル WebVPN + IPsec（値 20）にマッピングされます。AD で user1 として認証された WebVPN/IPsec ユーザはトンネル プロトコル不一致が原因で失敗します。AD で user1 として認証された L2TPoverIPsec は Deny ルールが原因で失敗します。AD で user2 として認証された WebVPN/IPsec ユーザは成功します（Allow ルール + トンネル プロトコルの一致）。AD で user2 として認証された L2TPoverIPsec はトンネル プロトコル不一致が原因で失敗します。
トンネル プロトコルのサポート。RFC 2867 および 2868 で定義されています。

アクセスを許可または拒否するためのActive Directoryの「Member Of 」/Groupメンバーシップの適用

このケースはケース5と密接に関連しており、より論理的なフローを提供し、グループメンバーシップのチェックを条件として確立するため、推奨される方法です。

1. ADユーザを特定のグループのメンバとして設定します。グループ階層のトップ（ASA-VPN-Consultants）となる名前を使用します。AD-LDAPでは、グループメンバーシップはAD属性memberOfによって定義されます。現在、ルールを適用できるのは最初のgroup/memberOf文字列だけなので、グループがリストの先頭にあることが重要です。リリース7.3では、複数グループのフィルタリングと適用を実行できます。
2. ASA で、最低限のマッピングのみの LDAP 属性マップを作成します。

```
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#
```

注：必要に応じて、マップに属性を追加します。この例では、この特別な機能の最低限の操作（グループ メンバーシップに基づいて [Allow] または [Deny Access] を指定）を示したものです。LDAP 属性マップ何を意味し、強制しますか。ADグループASA-VPN-ConsultantsのメンバーであるADの一部であるuser=joe_consultantは、ユーザがIPsec(tunnel-protocol=4=IPSec)を使用している場合にのみアクセスを許可できます。ADの一部であるUser=joe_consultantは、他のリモートアクセスクライアント（PPTP/L2TP、L2TP/IPSec、WebVPN/SVCなど）の実行中にVPNアクセスに失敗する可能性があります。User=bill_the_hackerは、ユーザーにADメンバーシップがないため許可されません。

Active Directoryでの「ログオン時間/Time-of-Dayルール」の適用

このケースでは AD/LDAP で Time of Day 規則を設定し、適用する方法について説明します。

その手順は次のとおりです。

1. AD/LDAP サーバで次を実行します。ユーザを選択します。[>Properties] を右クリックします。属性を設定するために使用するタブを選択します（例：一般タブ）。[Office]フィールドなどのフィールド/属性を選択して時間範囲を適用し、時間範囲の名前（Bostonなど）を入力します。GUIのOffice設定は、AD/LDAP属性physicalDeliveryOfficeNameに保存されます。
2. ASA LDAP 属性マッピング テーブルを作成します。AD/LDAP 属性「physicalDeliveryOfficeName」を ASA 属性「Access-Hours」にマッピングします。例：
```
B200-54(config-time-range)# show run ldap
ldap attribute-map TimeOfDay
map-name physicalDeliveryOfficeName Access-Hours
```
3. ASA で、LDAP 属性マップを aaa-server エントリに関連付けます。
```
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. ASA で、ユーザに割り当てられている名前を値とする時間範囲オブジェクトを作成します（手順 1 の Office の値）。
```
B200-54(config-time-range)# show runn time-range
!
time-range Boston
periodic weekdays 8:00 to 17:00
!
```
5. VPN リモート アクセス セッションを確立します。 時間範囲内であれば、セッションは成功する可能性があります。時間範囲外の場合、セッションが失敗する可能性があります。

ユーザを特定のグループ ポリシーにマッピングするための LDAP マップ設定の使用と、二重認証時における authorization-server-group コマンドの使用

1. このシナリオでは、二重認証が使用されます。最初に使用する認証サーバはRADIUSで、2番目に使用する認証サーバはLDAPサーバです。 LDAP サーバ、RADIUS サーバを設定します。以下が一例です。
```
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 *****
```
LDAP 属性マップを定義します。以下が一例です。
```
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
```
トンネル グループを定義し、認証のために RADIUS および LDAP サーバを関連付けます。以下が一例です。
```
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
```

トンネル グループ設定で使用するグループ ポリシーを確認します。

```
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
```

この設定では、LDAP 属性を使用して正しくマッピングされた AnyConnect ユーザには Test-Policy-Safenet グループ ポリシーは適用されていません。代わりに、デフォルトのグループ ポリシー（この場合 NoAccess）が設定されたままになっていました。デバッグのスニペット（debug ldap 255）と、情報レベルの syslog を確認します。

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

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.
```

これらのsyslogには、ユーザにNoAccessグループポリシーが割り当てられ、同時ログインが0に設定されているため、ユーザ固有のグループポリシーを取得したとsyslogに記録されていても、失敗が示されます。LDAPマップに基づいてユーザをグループポリシーに割り当てるには、**authorization-server-group test-ldap**コマンドが必要です(この場合、**test-ldap**はLDAPサーバ名です)。以下が一例です。

```
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. ここで、最初の認証サーバ（この例ではRADIUS）がユーザ固有の属性（この例ではIEFT-class属性など）を送信した場合、ユーザはRADIUSによって送信されたグループポリシーにマッピングできます。したがって、セカンダリサーバにLDAPマップが設定されており、ユーザのLDAP属性がユーザを異なるグループポリシーにマッピングする場合でも、最初の認証サーバによって送信されたグループポリシーを適用できます。 LDAPマップ属性に基づいてユーザをグループポリシーに割り当てるには、tunnel-groupで**authorization-server-group test-ldap**コマンドを指定する必要があります。
3. 最初の認証サーバがユーザ固有の属性を送信できない SDI または OTP である場合は、ユーザにはトンネルグループのデフォルトのグループポリシーが割り当てられます。この場合、LDAP のマッピングが正しくとも、NoAccess になってしまいます。 この場合、ユーザをグループポリシーに割り当てるため、トンネル グループで **authorization-server-group test-ldap** コマンドが必要になります。
4. 両方のサーバの両方が同じく RADIUS または LDAP サーバであれば、グループポリシーを合わせるための **authorization-server-group コマンドは不要です。**

確認

```
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
```

トラブルシュート

このセクションは、設定のトラブルシューティングを行う際に参照してください。

LDAP のトランザクションのデバッグ

DAP 設定の問題を特定するため、以下のデバッグを行います。

- debug ldap 255
- debug dap trace

- aaa 認証のデバッグ

ASA で LDAP サーバからユーザが認証できない問題

ASA が LDAP サーバでユーザを認証できない場合のためのデバッグの例を示します。:

```
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
```

これらのデバッグ以外では、LDAP ログイン DN の形式またはパスワードのいずれか、ないしは両方が正しくないことによるため、問題解決にはこの両方を確認します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。