使用LDAP屬性對映配置示例

目錄

[簡介](#)
[程式](#)
[將LDAP使用者置於特定組策略（通用示例）](#)
[配置NOACCESS組策略](#)
[基於組的屬性策略實施（示例）](#)
[Active Directory為IPsec和SVC通道實施「分配靜態IP地址」](#)
[Active Directory實施「遠端訪問許可權撥入，允許/拒絕訪問」](#)
[Active Directory強制「/組成員」以允許或拒絕訪問](#)
[Active Directory實施「登入時間/時間規則」](#)
[使用ldap-map配置將使用者對映到特定組策略，並在雙重身份驗證的情況下使用authorization-server-group命令](#)
[驗證](#)
[疑難排解](#)
[調試LDAP事務](#)
[ASA無法從LDAP伺服器驗證使用者](#)

簡介

本檔案介紹如何將任何Microsoft/AD屬性對映到Cisco屬性。

程式

1. 在Active Directory(AD)/輕量型目錄訪問協定(LDAP)伺服器上：選擇**user1**。按一下右鍵**> Properties**。選擇要用於設定屬性的頁籤（例如，常規頁籤）。選擇要用於強制實施時間範圍的欄位/屬性，例如Office欄位，然後輸入標語文本(例如，歡迎使用LDAP服!!!!)。GUI上的Office配置儲存在AD/LDAP屬性physicalDeliveryOfficeName中。
2. 在自適應安全裝置(ASA)上，為了建立LDAP屬性對映表，請將AD/LDAP屬性physicalDeliveryOfficeName對映到ASA屬性Banner1:

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

3. 將LDAP屬性對映關聯到aaa-server條目：

```
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. 建立遠端訪問會話並驗證是否向VPN使用者!!!!示Banner Welcome to LDAP Session。

將LDAP使用者置於特定組策略（通用示例）

此示例演示AD-LDAP伺服器上的user1身份驗證，並檢索department欄位值，以便可以將其對映至可從其實施策略的ASA/PIX組策略。

1. 在AD/LDAP伺服器上：選擇**user1**。按一下右鍵**> Properties**。選擇要用於設定屬性的頁籤（例如，「組織」頁籤）。選擇要用於實施組策略的欄位/屬性（例如Department），並在ASA/PIX上輸入組策略(Group-Policy1)的值。GUI上的Department配置儲存在AD/LDAP屬性部門。
2. 定義ldap-attribute-map表。

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

3. 定義裝置上的組策略Group_policy1和所需的策略屬性。
4. 建立VPN遠端訪問隧道並驗證會話是否繼承來自Group-Policy1的屬性（以及來自預設組策略的任何其他適用屬性）。 **注意**：根據需要向對映中新增更多屬性。此示例僅顯示控制此特定功能（將使用者置於特定ASA/PIX 7.1.x組策略中）的最小值。第三個示例顯示這種型別的地圖。

配置NOACCESS組策略

您可以建立NOACCESS組策略，以便在使用者不屬於任何LDAP組時拒絕VPN連線。系統會顯示此組態片段以供參考：

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

您必須將此組策略作為預設組策略應用到隧道組。這樣，從LDAP屬性對映獲取對映的使用者（例如，屬於所需LDAP組的使用者）可以獲取所需的組策略，而未獲取任何對映的使用者（例如，不屬於任何所需LDAP組的使用者）可以從隧道組獲取NOACCESS組策略，該策略會阻止對它們的訪問。

提示：因為vpn-simultaneous-logins屬性在此設定為0，所以也必須在所有其他組策略中顯式定義該屬性；否則，它可以從該隧道組的預設組策略繼承，在本例中為NOACCESS策略。

基於組的屬性策略實施（示例）

1. 在AD-LDAP伺服器（Active Directory使用者和電腦）上，設定代表配置VPN屬性的組的使用者記錄(VPNUserGroup)。
2. 在AD-LDAP伺服器、Active Directory使用者和電腦上，定義每個使用者記錄的Department欄位，以指向步驟1中的組記錄(VPNUserGroup)。本示例中的使用者名稱是web1。 **註**：之所以使用「部門AD」屬性，只是因為邏輯上部門引用組策略。實際上，任何領域都可以使用。要求此欄位必須對映到Cisco VPN屬性Group-Policy，如本例所示。
3. 定義ldap-attribute-map表：

```
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)#
```

兩個AD-LDAP屬性Description和Office（由AD名稱描述和PhysicalDeliveryOfficeName表示）是對映到Cisco VPN屬性Banner1和IETF-Radius-Session-Timeout的組記錄屬性（對於VPNUSerGroup）。department屬性用於使用者記錄對映到ASA(VPNUSer)上的外部組策略名稱，然後該名稱對映回AD-LDAP伺服器上的VPNuserGroup記錄，其中定義了屬性。**註**：必須在ldap-attribute-map中定義Cisco屬性(Group-Policy)。其對映的AD屬性可以是任何可設定的AD屬性。此示例使用department，因為它是引用組策略的最邏輯名稱。

4. 使用ldap-attribute-map name配置aaa-server以用於LDAP身份驗證、授權和記帳(AAA)操作：

```
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. 使用LDAP身份驗證或LDAP授權定義隧道組。 LDAP身份驗證示例。如果定義了屬性，則執行身份驗證+（授權）屬性策略實施。

```
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授權示例。用於數位證書的配置。

```
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. 定義外部組策略。group-policy的名稱是代表該組(VPNUserGroup)的AD-LDAP使用者記錄的值。

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

7. 建立通道並驗證屬性是否已實施。在這種情況下，將從AD上的VPNuserGroup記錄中強制執行Banner和Session-Timeout。

Active Directory為IPsec和SVC通道實施「分配靜態IP地址」

AD屬性為msRADIUSFramedIPAddress。該屬性在AD使用者屬性、撥入頁籤和分配靜態IP地址中配置。

以下是步驟：

1. 在AD伺服器上的user Properties， Dial-in（使用者屬性，撥入）頁籤Assign a Static IP

Address（分配靜態IP地址）下，輸入IP地址的值以分配給IPsec/SVC會話(10.20.30.6)。

2. 在ASA上，使用以下對映建立ldap屬性對映：
```
5540-1# show running-config ldap
ldap attribute-map Assign-IP
map-name msRADIUSFramedIPAddress IETF-Radius-Framed-IP-Address
5540-1#
```
3. 在ASA上，驗證vpn-address-assigment是否配置為包括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. 建立IPsec/SVC遠端授權(RA)會話並驗證show vpn-sessiondb remote|svc中「分配的IP」欄位是否正確(10.20.30.6)。

Active Directory實施「遠端訪問許可權撥入，允許/拒絕訪問」

支援所有VPN遠端訪問會話：IPSec、WebVPN和SVC。Allow Access的值為TRUE。Deny Access的值為FALSE。AD屬性名稱為msNPAllowDialin。

此示例演示如何建立使用Cisco Tunneling-Protocols建立Allow Access(TRUE)和Deny(FALSE)條件的ldap-attribute-map。例如，如果對映tunnel-protocol=L2TPover IPsec(8)，則如果嘗試為WebVPN和IPsec實施訪問，則可以建立FALSE條件。相反的邏輯也適用。

以下是步驟：

1. 在AD伺服器user1的Properties（屬性）中，為每個使用者選擇適當的allow Access（允許訪問）或Deny access（拒絕訪問）。 **註**：如果選擇第三個選項「通過遠端訪問策略控制訪問」，則不會從AD伺服器返回任何值，因此實施的許可權基於ASA/PIX的內部組策略設定。
2. 在ASA上，使用以下對映建立ldap-attribute-map:
```
ldap attribute-map LDAP-MAP
map-name msNPAllowDialin Tunneling-Protocols
map-value msNPAllowDialin FALSE 8
map-value msNPAllowDialin TRUE 20
5540-1#
```
注意：根據需要向對映中新增更多屬性。此示例只顯示控制此特定功能的最小值（允許或拒絕基於撥入設定的訪問）。ldap-attribute-map表示或強制實施什麼？map-value msNPAllowDialin FALSE 8拒絕使用者1的訪問。FALSE值條件對映到隧道協定L2TPoverIPsec（值8）。允許使用者2訪問。TRUE值條件對映到隧道協定WebVPN + IPsec（值20）。由於tunnel-protocol不匹配，在AD上驗證為user1的WebVPN/IPsec使用者將失敗。由於「拒絕」規則，在AD上驗證為user1的L2TPoverIPsec將失敗。在AD上驗證為user2的WebVPN/IPsec使用者將成功（允許規則+匹配的隧道協定）。由於tunnel-protocol不匹配，在AD上驗證為user2的L2TPoverIPsec將失敗。
支援RFC 2867和2868中定義的隧道協定。

Active Directory強制「/組成員」以允許或拒絕訪問

此案例與案例5密切相關，並提供了更邏輯的流程，並且是推薦方法，因為它將組成員身份檢查建立為一種條件。

1. 將AD使用者配置為特定組的成員。使用將其置於組層次結構(ASA-VPN-Consultants)頂部的名稱。在AD-LDAP中，組成員資格由AD屬性memberOf定義。組位於清單頂部非常重要，因為

您當前只能將規則應用於第一個組/memberOf字串。在7.3版中，您可以執行多組過濾和實施。

2. 在ASA上，建立具有最小對映的ldap-attribute-map:

```
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#
```

注意：根據需要向對映中新增更多屬性。此示例只顯示控制此特定功能的最小值（根據組成員身份允許或拒絕訪問）。ldap-attribute-map表示或強制實施什麼？User=joe_consultant，AD的一部分，是AD組ASA-VPN-Consultants的成員，僅當使用者使用IPsec(tunnel-protocol=4=IPSec)時，才允許訪問。AD的user=joe_consultant可能會在任何其他遠端訪問客戶端（PPTP/L2TP、L2TP/IPSec、WebVPN/SVC等）期間無法進行VPN訪問。不能允許User=bill_the_hacker，因為使用者沒有AD成員資格。

Active Directory實施「登入時間/時間規則」

本使用案例介紹如何在AD/LDAP上設定和實施時間規則。

以下是執行此操作的程式：

1. 在AD/LDAP伺服器上：選擇使用者。按一下右鍵**> Properties**。選擇要用於設定屬性的頁籤（「示例」、「常規」頁籤）。選擇要用於強制實施時間範圍的欄位/屬性，例如「辦公室」欄位，然後輸入時間範圍的名稱（例如，波士頓）。GUI上的Office配置儲存在AD/LDAP屬性physicalDeliveryOfficeName中。
2. 在ASA上 建立LDAP屬性對映表。將AD/LDAP屬性「physicalDeliveryOfficeName」對映到ASA屬性「Access-Hours」。範例：

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

3. 在ASA上，將LDAP屬性對映關聯到aaa伺服器條目：

```
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. 在ASA上，建立具有分配給使用者的名稱值的時間範圍對象（步驟1中的Office值）：

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

5. 建立VPN遠端訪問會話： 如果在時間範圍內，會話可以成功。如果超出時間範圍，會話可能會失敗。

使用ldap-map配置將使用者對映到特定組策略，並在雙重身份驗證的情況下使用authorization-server-group命令

1. 在此案例中，使用雙重驗證。使用的第一個身份驗證伺服器是RADIUS，使用的第二個身份驗證伺服器是LDAP伺服器。 配置LDAP伺服器以及RADIUS伺服器。以下是範例：

```
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 *****
```

定義LDAP屬性對映。以下是範例：

```
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
```

定義隧道組並關聯RADIUS和LDAP伺服器以進行身份驗證。以下是範例：

```
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
```

檢視隧道組配置中使用的組策略：

```
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
```

在此配置下，使用LDAP屬性正確對映的AnyConnect使用者未置於組策略Test-Policy-Safenet中。相反，它們仍位於預設組策略中，在本例中為NoAccess。請參閱調試代碼段(debug ldap 255)和syslogs（級別資訊）：

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

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.
```

這些系統日誌顯示失敗，因為向使用者提供了NoAccess組策略，該策略將同時登入設定為0，即使系統日誌聲稱它檢索了使用者特定的組策略。要根據LDAP對映在組策略中分配使用者，您必須使用以下命令：**authorization-server-group test-ldap**(在本例中，**test-ldap**是LDAP伺服器名稱)。以下是範例：

```
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. 現在，如果第一個驗證伺服器（在本範例中為RADIUS）確實傳送了使用者特定的屬性，例如IEFT-class屬性，在這種情況下，使用者可以對映到由RADIUS傳送的群組原則。因此，即使輔助伺服器配置了LDAP對映，並且使用者的LDAP屬性確實將使用者對映到其他組策略，也可以實施由第一身份驗證伺服器傳送的組策略。 若要根據LDAP對映屬性將使用者置於組策略中，必須在tunnel-group: **authorization-server-group test-ldap**下指定此命令。
3. 如果第一個身份驗證伺服器是SDI或OTP（無法傳遞使用者特定屬性），則使用者將進入隧道組的預設組策略。在這種情況下，即使LDAP對映正確，也使用NoAccess。 在這種情況下，還需要在tunnel-group下使用**authorization-server-group test-ldap**命令，以便將該使用者置於正確的組策略中。
4. 如果兩個伺服器都是相同的RADIUS或LDAP伺服器，則無需使用**authorization-server-group**命令即可使組策略鎖定生效。

驗證

```
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
```

疑難排解

使用本節內容，對組態進行疑難排解。

調試LDAP事務

可以使用這些調試幫助隔離DAP配置的問題：

- debug ldap 255
- debug dap trace
- 調試aaa身份驗證

ASA無法從LDAP伺服器驗證使用者

如果ASA無法通過LDAP伺服器對使用者進行身份驗證，下面是一些調試示例：

```
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
```

在這些調試中，LDAP登入DN格式不正確或密碼不正確，因此請檢驗這兩種格式以解決問題。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。