LDAP 특성 맵 컨피그레이션 예 사용

목차

소개

이 문서에서는 Microsoft/AD 특성을 Cisco 특성에 매핑하는 방법에 대해 설명합니다.

절차

1. AD(Active Directory)/LDAP(Lightweight Directory Access Protocol) 서버에서**user1**을 **선택합니다**.마우스 오른쪽 버튼으로 **> 등록 정보**를 **클릭합니다**.속성을 설정하기 위해 사용할 탭을 선택합니다(예: 일반 탭).시간 범위를 적용하는 데 사용할 필드/특성(예: Office 필드)을 선택하고 배너 텍스트(예: LDAP !!!! 시작)를 입력합니다. GUI의 Office 컨피그레이션은 AD/LDAP 특성 physicalDeliveryOfficeName에 저장됩니다.
2. ASA(Adaptive Security Appliance)에서 LDAP 특성 매핑 테이블을 생성하려면 AD/LDAP 특성 physicalDeliveryOfficeName을 ASA 특성 Banner1에 매핑합니다.

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

3. LDAP 특성 맵을 aaa-server 항목에 연결합니다.

```
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. 원격 액세스 세션을 설정하고 VPN 사용자에게 배너 LDAP 시작 !!!!이 표시되는지 확인합니다.

특정 그룹 정책에 LDAP 사용자 배치(일반 예)

이 예에서는 AD-LDAP 서버에서 user1의 인증을 보여 주고 정책을 시행할 수 있는 ASA/PIX 그룹 정책에 매핑할 수 있도록 부서 필드 값을 검색합니다.

1. AD/LDAP 서버에서**user1**을 **선택합니다**.마우스 오른쪽 버튼으로 **> 등록 정보**를 **클릭합니다**.속성을 설정하기 위해 사용할 탭을 선택합니다(예: 조직 탭).그룹 정책을 시행하기 위해 사용할 필드/속성(예: Department)을 선택하고 ASA/PIX에서 그룹 정책(Group-Policy1)의 값을 입력합니다. GUI의 부서 컨피그레이션은 AD/LDAP 특성 부서에 저장됩니다.
2. ldap-attribute-map 테이블을 정의합니다.

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

3. 어플라이언스에서 group-policy, Group_policy1을 정의하고 필수 정책 특성을 정의합니다.
4. VPN 원격 액세스 터널을 설정하고 세션이 Group-Policy1의 특성(및 기본 그룹 정책의 다른 적용 가능한 특성)을 상속하는지 확인합니다. **참고**: 필요에 따라 맵에 특성을 더 추가합니다. 이 예에서는 이 특정 기능을 제어하기 위한 최소값만 보여줍니다(사용자를 특정 ASA/PIX 7.1.x 그룹 정책에 배치). 세 번째 예에서는 이 유형의 맵을 보여 줍니다.

NOACCESS 그룹 정책 구성

사용자가 LDAP 그룹의 일부가 아닐 때 VPN 연결을 거부하기 위해 NOACCESS 그룹 정책을 생성할 수 있습니다. 이 구성 코드 조각은 참조용으로 표시됩니다.

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

터널 그룹에 기본 그룹 정책으로 이 그룹 정책을 적용해야 합니다. 이렇게 하면 LDAP 특성 맵에서 매핑을 가져오는 사용자(예: 원하는 LDAP 그룹에 속한 사용자)는 원하는 그룹 정책을 가져오고, 매핑을 가져오지 않는 사용자(예: 원하는 LDAP 그룹에 속하지 않은 사용자)는 터널 그룹에서 NOACCESS 그룹 정책을 가져오므로 액세스가 차단됩니다.

> **팁**: vpn-simultaneous-logins 특성은 여기서 0으로 설정되므로 다른 모든 그룹 정책에서도 명시적으로 정의해야 합니다. 그렇지 않으면 터널 그룹에 대한 기본 그룹 정책에서 상속될 수 있습니다. 이 경우 NOACCESS 정책입니다.

그룹 기반 특성 정책 적용(예)

1. AD-LDAP 서버, Active Directory Users and Computers에서 VPN 특성이 구성된 그룹을 나타내는 사용자 레코드(VPNUserGroup)를 설정합니다.
2. AD-LDAP 서버인 Active Directory Users and Computers에서 1단계에서 그룹 레코드(VPNUserGroup)를 가리키도록 각 사용자 레코드의 Department 필드를 정의합니다. 이 예에서 사용자 이름은 web1입니다. **참고**: Department AD 특성은 논리적으로 department가 그룹 정책을 참조하기 때문에 사용되었습니다. 현실적으로 어떤 분야든 활용할 수 있다. 이 필드에는 이 예에 표시된 대로 Cisco VPN 특성 Group-Policy에 매핑해야 합니다.
3. ldap-attribute-map 테이블을 정의합니다.

```
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)#
```

AD 이름 설명 및 PhysicalDeliveryOfficeName으로 표시되는 두 가지 AD-LDAP 특성 Description 및 Office는 Cisco VPN 특성 Banner1 및 IETF-Radius-Session-Timeout에 매핑되는 그룹 레코드 특성(VPNUSerGroup용)입니다.부서 특성은 사용자 레코드가 ASA(VPNUSer)의 외부 그룹 정책 이름에 매핑되도록 하기 위한 것이며, 그런 다음 특성이 정의되는 AD-LDAP 서버의 VPNuserGroup 레코드에 다시 매핑됩니다.**참고**: Cisco 특성(Group-Policy)은 ldap-attribute-map에 정의되어야 합니다. 매핑된 AD 특성은 설정 가능한 AD 특성일 수 있습니다. 이 예에서는 department가 그룹 정책을 참조하는 가장 논리적인 이름이므로 department를 사용합니다.

4. LDAP AAA(Authentication, Authorization, and Accounting) 작업에 사용할 ldap-attribute-map 이름으로 aaa-server를 구성합니다.

```
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 인증 또는 LDAP 권한 부여를 사용하여 터널 그룹을 정의합니다. LDAP 인증의 예 특성이 정의된 경우 인증 + (권한 부여) 특성 정책 시행을 수행합니다.

```
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 권한 부여의 예 디지털 인증서에 사용되는 구성입니다.

```
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. 외부 그룹 정책을 정의합니다. 그룹 정책의 이름은 그룹(VPNUserGroup)을 나타내는 AD-LDAP 사용자 레코드의 값입니다.

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

7. 터널을 설정하고 특성이 적용되는지 확인합니다. 이 경우 배너 및 세션 시간 초과는 AD의 VPNuserGroup 레코드에서 적용됩니다.

IPsec 및 SVC 터널에 대한 "고정 IP 주소 할당"의 Active Directory 시행

AD 특성은 msRADIUSFramedIPAddress입니다. 이 특성은 AD User Properties(AD 사용자 속성),

Dial-in(전화 접속) 탭, Assign a Static IP Address(고정 IP 주소 할당)에서 구성됩니다.

단계는 다음과 같습니다.

1. AD 서버의 User Properties(사용자 속성), Dial-in(다이얼인) 탭의 Assign a Static IP Address(고정 IP 주소 할당)에서 IPsec/SVC 세션(10.20.30.6)에 할당할 IP 주소의 값을 입력합니다.
2. ASA에서 다음 매핑으로 ldap-attribute-map을 생성합니다.
```
5540-1# show running-config ldap
ldap attribute-map Assign-IP
map-name msRADIUSFramedIPAddress IETF-Radius-Framed-IP-Address
5540-1#
```
3. ASA에서 vpn-addr-assign-aaa를 포함하도록 vpn-address-assignment가 구성되었는지 확인합니다.
```
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 RA(원격 기관) 세션을 설정하고 show vpn-sessiondb remote|svc에서 Assigned IP(할당된 IP) 필드가 올바른지 확인합니다(10.20.30.6).

"원격 액세스 권한 다이얼인, 액세스 허용/거부"의 Active Directory 시행

모든 VPN 원격 액세스 세션(IPSec, WebVPN, SVC)을 지원합니다. Allow Access(액세스 허용)의 값은 TRUE(참)입니다. Deny Access(액세스 거부)의 값은 FALSE입니다. AD 특성 이름은 msNPAllowDialin입니다.

이 예에서는 Cisco Tunneling-Protocols를 사용하여 Allow Access(TRUE) 및 Deny(FALSE) 조건을 생성하는 ldap-attribute-map을 생성하는 방법을 보여 줍니다. 예를 들어 tunnel-protocol=L2TPover IPsec (8)을 매핑하는 경우 WebVPN 및 IPsec에 대한 액세스를 적용하려고 하면 FALSE 조건을 만들 수 있습니다. 역논리도 마찬가지다.

단계는 다음과 같습니다.

1. AD 서버 user1 Properties(사용자1 속성)에서 Dial-In(다이얼인)에서 각 사용자에 대해 적절한 Allow Access(액세스 허용) 또는 Deny access(액세스 거부)를 선택합니다. **참고**: 세 번째 옵션인 Control access through the Remote Access Policy(원격 액세스 정책을 통한 액세스 제어)를 선택하면 AD 서버에서 값이 반환되지 않으므로, 적용되는 권한은 ASA/PIX의 내부 그룹 정책 설정을 기반으로 합니다.
2. ASA에서 다음 매핑으로 ldap-attribute-map을 생성합니다.
```
ldap attribute-map LDAP-MAP
map-name msNPAllowDialin Tunneling-Protocols
map-value msNPAllowDialin FALSE 8
map-value msNPAllowDialin TRUE 20
5540-1#
```
참고: 필요에 따라 맵에 특성을 더 추가합니다. 이 예에서는 이 특정 기능(전화 접속 설정에 따라 액세스 허용 또는 거부)을 제어할 수 있는 최소값만 보여 줍니다.ldap-attribute-map은 무엇을 의미하거나 적용합니까?map-value msNPAllowDialin FALSE 8사용자1에 대한 액세스 거부 FALSE 값 조건은 터널 프로토콜 L2TPoverIPsec(값 8)에 매핑됩니다.user2에 대한 액세스 허용 TRUE 값 조건은 터널 프로토콜 WebVPN + IPsec(값 20)에 매핑됩니다.AD에서 user1로 인증된 WebVPN/IPsec 사용자는 터널 프로토콜 불일치로 인해 실패합니다.AD에서 user1로

인증된 L2TPoverIPsec은 거부 규칙 때문에 실패합니다.AD에서 user2로 인증된 WebVPN/IPsec 사용자가 성공합니다(허용 규칙 + 일치하는 터널 프로토콜).AD에서 user2로 인증된 L2TPoverIPsec은 터널 프로토콜 불일치로 인해 실패합니다.
RFC 2867 및 2868에 정의된 터널 프로토콜 지원

액세스를 허용하거나 거부하기 위한 "구성원"/그룹 멤버십의 Active Directory 시행

이 경우는 Case 5와 밀접한 관련이 있으며, 보다 논리적인 흐름을 제공하며, 그룹 멤버십 확인을 조건으로 설정하므로 권장되는 방법이다.

1. AD 사용자를 특정 그룹의 구성원으로 구성합니다. 그룹 계층 구조의 맨 위에 있는 이름을 사용합니다(ASA-VPN-Consultants). AD-LDAP에서 그룹 멤버십은 AD 특성 memberOf에 의해 정의됩니다. 현재 첫 번째 그룹/memberOf 문자열에만 규칙을 적용할 수 있으므로 그룹이 목록의 맨 위에 있어야 합니다. Release 7.3에서는 다중 그룹 필터링 및 시행을 수행할 수 있습니다.
2. ASA에서 최소 매핑으로 ldap-attribute-map을 생성합니다.
```
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#
```
참고: 필요에 따라 맵에 특성을 더 추가합니다. 이 예에서는 이 특정 기능(그룹 멤버십에 따라 액세스 허용 또는 거부)을 제어할 수 있는 최소값만 보여 줍니다.ldap-attribute-map은 무엇을 의미하거나 적용합니까?AD 그룹 ASA-VPN-Consultants의 멤버인 User=joe_consultant는 사용자가 IPsec(tunnel-protocol=4=IPSec)을 사용하는 경우에만 액세스가 허용됩니다 .User=joe_consultant(AD의 일부)는 다른 원격 액세스 클라이언트(PPTP/L2TP, L2TP/IPSec, WebVPN/SVC 등) 중에 VPN 액세스에 실패할 수 있습니다.사용자에게 AD 멤버십이 없으므로 User=bill_the_hacker를 허용할 수 없습니다.

Active Directory의 "로그온 시간/시간 규칙" 시행

이 활용 사례에서는 AD/LDAP에서 Time of Day 규칙을 설정하고 적용하는 방법에 대해 설명합니다 .

이 작업을 수행하는 절차는 다음과 같습니다.

1. AD/LDAP 서버에서사용자를 선택합니다.마우스 오른쪽 버튼으로 **> 등록 정보**를 **클릭합니다** .속성을 설정하기 위해 사용할 탭을 선택합니다(예: 일반 탭).시간 범위를 적용하는 데 사용할 필드/속성(예: Office 필드)을 선택하고 시간 범위의 이름(예: Boston)을 입력합니다. GUI의 Office 컨피그레이션은 AD/LDAP 특성 physicalDeliveryOfficeName에 저장됩니다.
2. ASA에서 LDAP 특성 매핑 테이블을 생성합니다.AD/LDAP 특성 "physicalDeliveryOfficeName"을 ASA 특성 "Access-Hours"에 매핑합니다.예:
```
B200-54(config-time-range)# show run ldap
ldap attribute-map TimeOfDay
map-name physicalDeliveryOfficeName Access-Hours
```
3. ASA에서 LDAP 특성 맵을 aaa-server 항목에 연결합니다.
```
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. ASA에서 사용자에게 할당된 이름 값을 갖는 시간 범위 객체를 만듭니다(1단계의 Office 값).

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

5. VPN 원격 액세스 세션을 설정합니다. 시간 범위 내에 있는 경우 세션이 성공할 수 있습니다.시간 범위를 벗어나는 경우 세션이 실패할 수 있습니다.

ldap-map 컨피그레이션을 사용하여 사용자를 특정 그룹 정책에 매핑하고 이중 인증의 경우 authorization-server-group 명령을 사용합니다

1. 이 시나리오에서는 이중 인증이 사용됩니다. 사용되는 첫 번째 인증 서버는 RADIUS이고, 사용되는 두 번째 인증 서버는 LDAP 서버입니다. LDAP 서버와 RADIUS 서버를 구성합니다. 예를 들면 다음과 같습니다.

```
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 attribute-map을 정의합니다. 예를 들면 다음과 같습니다.

```
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
```

터널 그룹을 정의하고 인증을 위해 RADIUS 및 LDAP 서버를 연결합니다. 예를 들면 다음과 같습니다.

```
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
```

tunnel-group 컨피그레이션에 사용되는 group-policy를 확인합니다.

```
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
```

이 컨피그레이션에서는 LDAP 특성을 사용하여 올바르게 매핑된 AnyConnect 사용자가 그룹 정책인 Test-Policy-Safenet에 배치되지 않았습니다. 대신, 기본 그룹 정책(이 경우에는 NoAccess)에 배치되었습니다.자세한 내용은 디버그(debug ldap 255) 및 syslogs의 코드 조각을 참조하십시오.

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

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.
```

이러한 syslog는 syslog가 사용자 특정 그룹 정책을 검색했다고 말하더라도 동시 로그인이 0으로 설정된 NoAccess 그룹 정책을 사용자에게 제공했을 때 오류를 표시합니다.LDAP-map을 기반으로 그룹 정책에서 사용자를 할당하려면 다음 명령을 사용해야 합니다. authorization-**server-group test-ldap**(이 경우 **test-ldap**는 LDAP 서버 이름). 예를 들면 다음과 같습니다.

```
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. 이제 첫 번째 인증 서버(이 예에서는 RADIUS)가 사용자별 특성(예: IEFT-class 특성)을 보낸 경우 사용자는 RADIUS에서 보낸 그룹 정책에 매핑될 수 있습니다. 따라서 보조 서버에 LDAP 맵이 구성되어 있고 사용자의 LDAP 특성이 사용자를 다른 그룹 정책에 매핑하더라도 첫 번째 인증 서버에서 보낸 그룹 정책을 적용할 수 있습니다. 사용자가 LDAP 맵 특성을 기반으로 그룹 정책에 배치되게 하려면 tunnel-group: authorization-server-group test-**ldap 아래**에 이 명령**을** 지정해야 합니다.
3. 첫 번째 인증 서버가 사용자별 특성을 전달할 수 없는 SDI 또는 OTP인 경우 사용자는 tunnel-group의 기본 그룹 정책에 속하게 됩니다. 이 경우 LDAP 매핑이 올바르더라도 NoAccess가 수행됩니다. 이 경우 사용자를 올바른 그룹 정책에 배치하려면 터널 그룹 아래에

authorization-server-group test-ldap 명령이 필요합니다.
4. 두 서버가 모두 동일한 RADIUS 또는 LDAP 서버인 경우 그룹 정책 잠금을 작동하기 위해 authorization-server-group 명령이 필요하지 않습니다.

다음을 확인합니다.

```
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
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결합니다.

LDAP 트랜잭션 디버그

이러한 디버그는 DAP 컨피그레이션의 문제를 격리하는 데 사용할 수 있습니다.

- ldap 255 디버그
- debug dap trace
- aaa 인증 디버그

ASA가 LDAP 서버에서 사용자를 인증할 수 없음

ASA에서 LDAP 서버의 사용자를 인증할 수 없는 경우, 몇 가지 샘플 디버깅이 있습니다.

```
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
```

이러한 디버그에서 LDAP 로그인 DN 형식이 잘못되었거나 비밀번호가 잘못되었으므로 문제를 해

결하기 위해 두 가지를 모두 확인하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.