Cisco IOS 헤드엔드에서 LDAP를 사용하는 AnyConnect 클라이언트에 대한 정책 그룹 할당 컨피그레이션 예

목차

소개

이 문서에서는 자격 증명을 기반으로 사용자에게 올바른 VPN 정책을 자동으로 할당하도록 LDAP(Lightweight Directory Access Protocol) 특성 맵을 구성하는 방법에 대해 설명합니다.

> **참고:** Cisco IOS® 헤드엔드에 연결하는 SSL VPN(Secure Sockets Layer VPN) 사용자에 대한 LDAP 인증 지원은 Cisco 버그 ID CSCuj20940을 통해 추적됩니다. 지원이 공식적으로 추가될 때까지 LDAP 지원이 최선의 방법입니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco IOS의 SSL VPN
- Cisco IOS의 LDAP 인증
- 디렉터리 서비스

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CISCO881-SEC-K9
- Cisco IOS 소프트웨어, C880 소프트웨어(C880DATA-UNIVERSALK9-M), 버전 15.1(4)M, 릴리스 소프트웨어(fc1)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

LDAP는 IP(Internet Protocol) 네트워크를 통해 분산된 디렉토리 정보 서비스에 액세스하고 이를 유지 관리하는 개방적이고 벤더에 중립적인 업계 표준 애플리케이션 프로토콜입니다. 디렉토리 서비스는 네트워크 전체에서 사용자, 시스템, 네트워크, 서비스 및 애플리케이션에 대한 정보를 공유할 수 있도록 하기 때문에 인트라넷 및 인터넷 애플리케이션 개발에 중요한 역할을 합니다.

관리자는 자주 VPN 사용자에게 서로 다른 액세스 권한 또는 WebVPN 콘텐츠를 제공하려고 합니다. 이 작업은 VPN 서버에서 서로 다른 VPN 정책을 구성하고 자격 증명에 따라 각 사용자에게 이러한 정책 집합을 할당하여 완료할 수 있습니다. 수동으로 완료할 수 있지만 디렉터리 서비스로 프로세스를 자동화하는 것이 더 효율적입니다. LDAP를 사용하여 사용자에게 그룹 정책을 할당하려면 VPN 헤드엔드에서 인식하는 특성에 AD(Active Directory) 특성 "memberOf"와 같은 LDAP 특성을 매핑하는 맵을 구성해야 합니다.

ASA(Adaptive Security Appliance)에서는 LDAP 특성 맵이 있는 다른 사용자에게 서로 다른 그룹 정책을 할당하여 정기적으로 이를 달성할 수 있습니다(ASA Use of LDAP Attribute Maps Configuration Example 참조).

Cisco IOS에서는 WebVPN 컨텍스트에서 서로 다른 정책 그룹의 컨피그레이션 및 LDAP 특성 맵을 사용하여 사용자가 어떤 정책 그룹을 할당할지 결정할 수 있습니다. Cisco IOS 헤드엔드에서 "memberOf" AD 특성은 AAA(Authentication, Authorization, and Accounting) 특성 신청자 그룹에 매핑됩니다. 기본 특성 매핑에 대한 자세한 내용은 Dynamic Attribute Maps Configuration Example을 사용하여 IOS 디바이스의 LDAP를 참조하십시오. 그러나 SSL VPN에는 두 가지 관련 AAA 특성 매핑이 있습니다.

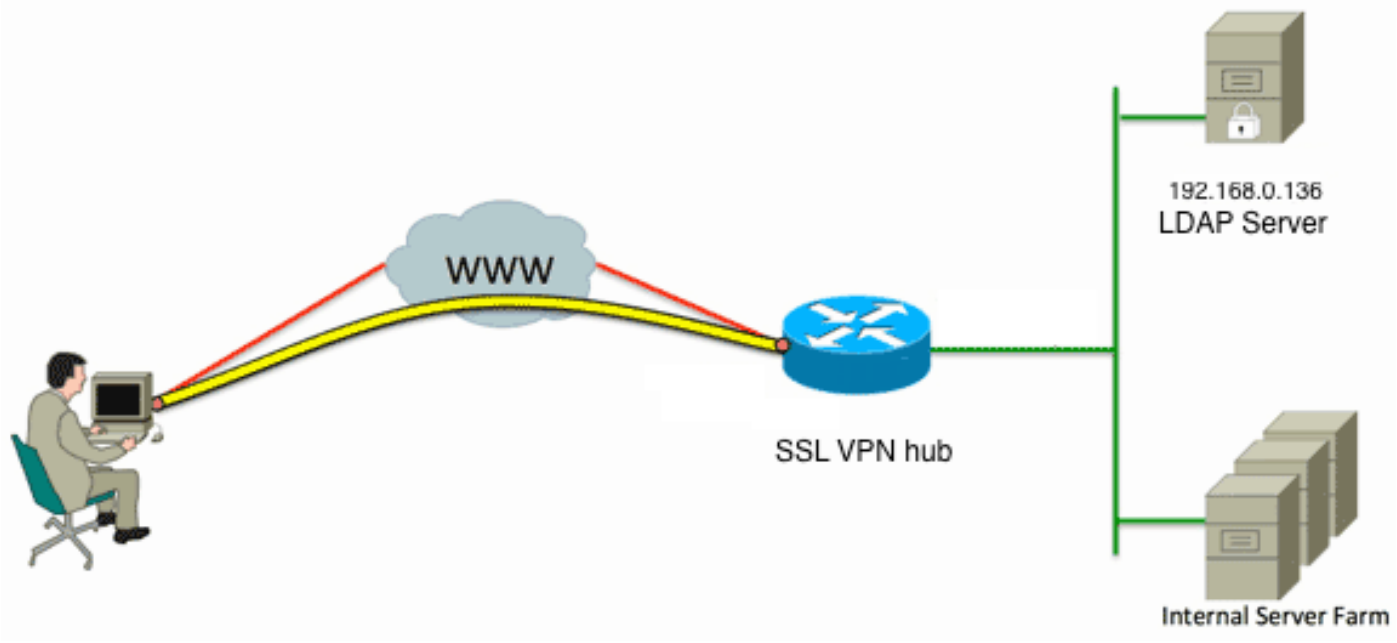
AAA 특성 이름	SSL VPN 관련성
user-vpn-group	WebVPN 컨텍스트에 정의된 정책 그룹에 매핑
webvpn 컨텍스트	실제 WebVPN 컨텍스트 자체에 매핑

따라서 LDAP 특성 맵은 관련 LDAP 특성을 이 두 AAA 특성 중 하나에 매핑해야 합니다.

구성

> **참고:** 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램



이 컨피그레이션에서는 LDAP 특성 맵을 사용하여 AAA 특성 user-vpn-group에 "memberOf" LDAP 특성을 매핑합니다.

1. 인증 방법 및 AAA 서버 그룹을 구성합니다.

```
aaa new-model
!
!
aaa group server ldap AD
 server DC1
!
aaa authentication login default local
aaa authentication login vpn local
aaa authentication login AD group ldap local
aaa authorization exec default local
```

2. LDAP 특성 맵을 구성합니다.

```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group
```

3. 이전 LDAP 특성 맵을 참조하는 LDAP 서버를 구성합니다.

```
ldap server DC1
 ipv4 192.168.0.136
 attribute map ADMAP
 bind authenticate root-dn CN=Cisco Systems,OU=Service Accounts,DC=chillsthrills,
DC=local password 7 <removed>
 base-dn DC=chillsthrills,DC=local
```

4. WebVPN 서버 역할을 하도록 라우터를 구성합니다. 이 예에서는 "memberOf" 특성이 "user-vpn-group" 특성에 매핑되므로 단일 WebVPN 컨텍스트가 "NOACCESS" 정책을 포함하는 여러 정책 그룹으로 구성됩니다. 이 정책 그룹은 일치하는 "memberOf" 값이 없는 사용자를 위한 것입니다.

```
ip local pool vpnpool 192.168.200.200 192.168.200.250
!
webvpn gateway gateway_1
 hostname vpn
 ip address 173.11.196.220 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-2564112419
 logging enable
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-2.5.2019-k9.pkg sequence 1
 !
```

```
webvpn install csd flash:/webvpn/sdesktop.pkg
 !
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
  hide-url-bar
  timeout idle 60
  timeout session 1
 !
 !
 policy group CN=T,OU=MyBusiness,DC=chillsthrills,DC=local
  functions svc-enabled
  banner "special access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
   svc split include 192.168.0.0 255.255.255.0
   svc split include 10.10.10.0 255.255.255.0
   svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

주의 사항

1. 사용자가 "memberOf" 여러 그룹인 경우 라우터에서 첫 번째 "memberOf" 값을 사용합니다.
2. 이 컨피그레이션에서는 "memberOf 값"에 대해 LDAP 서버가 푸시한 **전체** 문자열에 대해 정책 그룹 이름이 정확히 일치해야 합니다. 일반적으로 관리자는 VPNACCESS와 같은 정책 그룹에 대해 더 짧고 더 적절한 이름을 사용하지만, 코스메틱 문제와는 별도로 이 이름은 더 큰 문제로 이어질 수 있습니다. "memberOf" 특성 문자열이 이 예제에서 사용된 것보다 훨씬 큰 경우가 많습니다. 예를 들어 다음 디버그 메시지를 고려하십시오.

   ```
   004090: Aug 23 08:26:57.235 PCTime: %SSLVPN-6-INVALID_RADIUS_CONFIGURATION:
   Radius configured group policy "CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,
   DC=chillsthrills,DC=local" does not exist
   ```

   AD에서 받은 문자열은 다음과 같습니다.

   ```
   "CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,DC=chillsthrills,DC=local"
   ```

   그러나 정의된 정책 그룹이 없으므로 관리자가 그룹 정책을 구성하려고 하면 Cisco IOS는 정책 그룹 이름의 문자 수에 제한이 있으므로 오류가 발생합니다.

   ```
   HOURTR1(config-webvpn-context)#webvpn context VPNACCESS
   HOURTR1(config-webvpn-context)# policy group "CN=VPNACCESS,OU=Security Groups,
   OU=MyBusiness,DC=chillsthrills,DC=local"
   Error: group policy name cannot exceed 63 characters
   ```

이러한 경우 두 가지 해결 방법이 있습니다.

1. "department"와 같은 다른 LDAP 특성을 사용합니다.다음 LDAP 특성 맵을 고려하십시오.

   ```
   ldap attribute-map ADMAP
    map type department user-vpn-group
   ```

이 경우 사용자에 대한 부서 특성 값을 VPNACCESS와 같은 값으로 설정할 수 있으며 WebVPN 컨피그레이션이 약간 더 간단합니다.

```
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
 !
 policy group VPNACCESS
  functions svc-enabled
  banner "access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
  svc split include 192.168.0.0 255.255.255.0
  svc split include 10.10.10.0 255.255.255.0
  svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

2. LDAP 특성 맵에서 DN-to-string 키워드를 사용합니다.이전 해결 방법이 적합하지 않을 경우 관리자는 LDAP 특성 맵에서 dn-to-string 키워드를 사용하여 "memberOf" 문자열에서 CN(Common Name) 값만 추출할 수 있습니다. 이 시나리오에서 LDAP 특성 맵은 다음과 같습니다.

```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group format dn-to-string
```

WebVPN 구성은 다음과 같습니다.

```
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
 !
 policy group VPNACCESS
  functions svc-enabled
  banner "access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
  svc split include 192.168.0.0 255.255.255.0
  svc split include 10.10.10.0 255.255.255.0
  svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
```

```
 gateway gateway_1
 inservice
!
end
```

참고: LDAP 서버에서 수신한 값을 다른 로컬 중요 값으로 매칭하기 위해 특성 맵 아래의 **map value** 명령을 사용할 수 있는 ASA와 달리 Cisco IOS 헤드엔드는 이 옵션이 없으므로 유연하지 않습니다. Cisco 버그 ID CSCts31840이 해결되었습니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

- **ldap 특성 표시**
- **ldap 서버 모두 표시**

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

참고: debug 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

LDAP 특성 매핑을 트러블슈팅하려면 다음 디버그를 활성화합니다.

- **ldap 모두 디버그**
- **ldap 이벤트 디버그**
- **디버그 aaa 인증**
- **디버그 aaa 권한 부여**