ASA 8.0:WebVPN 사용자를 위한 LDAP 인증 구성

목차

소개

이 문서에서는 WebVPN 사용자 인증에 LDAP 서버를 사용하도록 Cisco ASA(Adaptive Security Appliance)를 구성하는 방법을 보여 줍니다.이 예에서 LDAP 서버는 Microsoft Active Directory입니다.이 컨피그레이션은 소프트웨어 버전 8.0(2)을 실행하는 ASA에서 ASDM(Adaptive Security Device Manager) 6.0(2)을 사용하여 수행됩니다.

참고: 이 예에서는 WebVPN 사용자에 대해 LDAP(Lightweight Directory Access Protocol) 인증이 구성되지만 이 컨피그레이션은 다른 모든 유형의 원격 액세스 클라이언트에도 사용할 수 있습니다.표시된 대로 원하는 연결 프로파일(터널 그룹)에 AAA 서버 그룹을 할당하기만 하면 됩니다.

사전 요구 사항

기본 VPN 컨피그레이션이 필요합니다.이 예에서는 WebVPN이 사용됩니다.

배경 정보

이 예에서는 ASA가 인증하는 사용자의 ID를 확인하기 위해 LDAP 서버를 확인합니다.이 프로세스는 기존의 RADIUS(Remote Authentication Dial-In User Service) 또는 TACACS+(Terminal Access Controller Access-Control System Plus) 교환과는 다르게 작동합니다.이 단계는 ASA에서 사용자 자격 증명을 확인하기 위해 LDAP 서버를 사용하는 방법에 대해 개괄적으로 설명합니다.

1. 사용자가 ASA에 대한 연결을 시작합니다.
2. ASA는 해당 사용자를 Microsoft AD(Active Directory)/LDAP 서버로 인증하도록 구성됩니다.

3. ASA는 ASA에 구성된 자격 증명(이 경우 admin)을 사용하여 LDAP 서버에 바인딩하고 제공된 사용자 이름을 조회합니다.또한 **관리자** 사용자는 Active Directory 내에서 내용을 나열하는 데 적합한 자격 증명을 얻습니다.LDAP 쿼리 권한을 부여하는 방법에 대한 자세한 내용은 http://support.microsoft.com/?id=320528 를 참조하십시오.**참고:**Microsoft 웹 사이트 (http://support.microsoft.com/?id=320528) 는 타사 공급자가 관리합니다.Cisco는 해당 콘텐츠에 대해 책임을 지지 않습니다.
4. 사용자 이름이 발견되면 ASA는 로그인 시 사용자가 제공한 자격 증명을 사용하여 LDAP 서버에 바인딩하려고 시도합니다.
5. 두 번째 바인딩이 성공하면 인증이 성공하고 ASA가 사용자의 특성을 처리합니다.**참고:** 이 예에서는 속성이 어떤 것에도 사용되지 않습니다.ASA/PIX 참조:LDAP 컨피그레이션을 통해 VPN 클라이언트를 VPN 그룹 정책에 매핑하여 ASA가 LDAP 특성을 처리하는 방법의 예를 확인합니다.

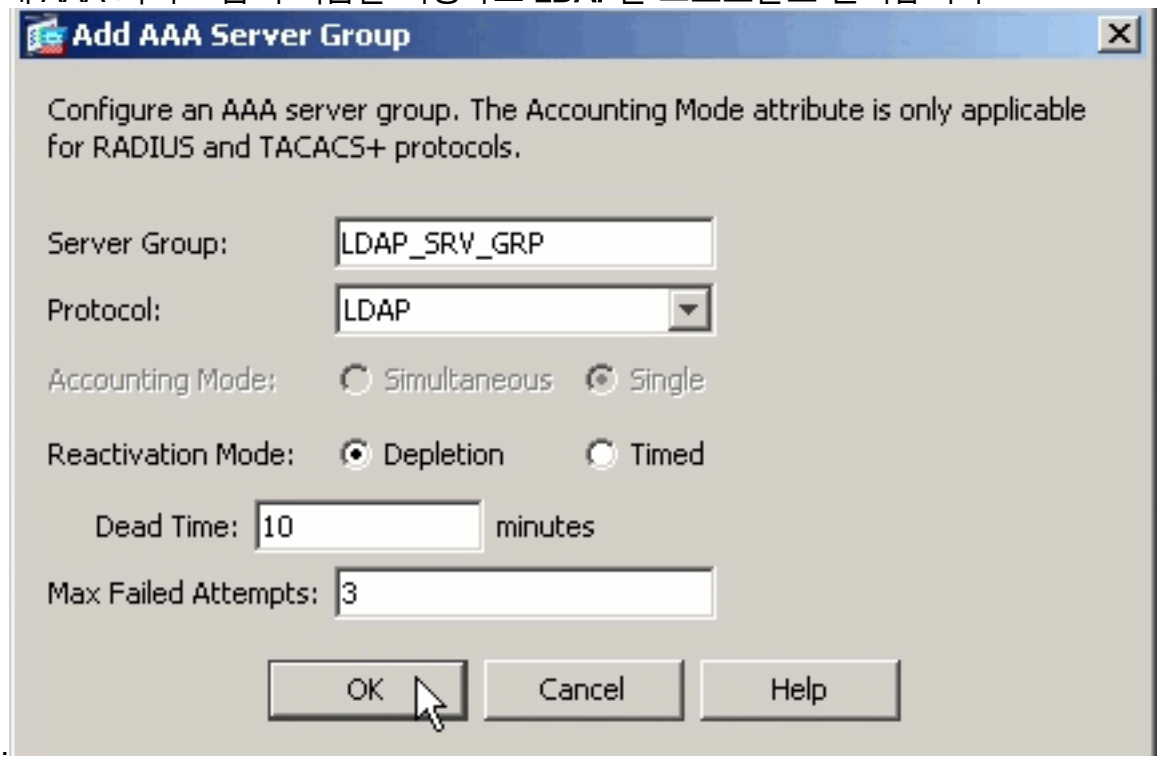
LDAP 인증 구성

이 섹션에서는 WebVPN 클라이언트 인증을 위해 LDAP 서버를 사용하도록 ASA를 구성하는 정보를 제공합니다.

ASDM

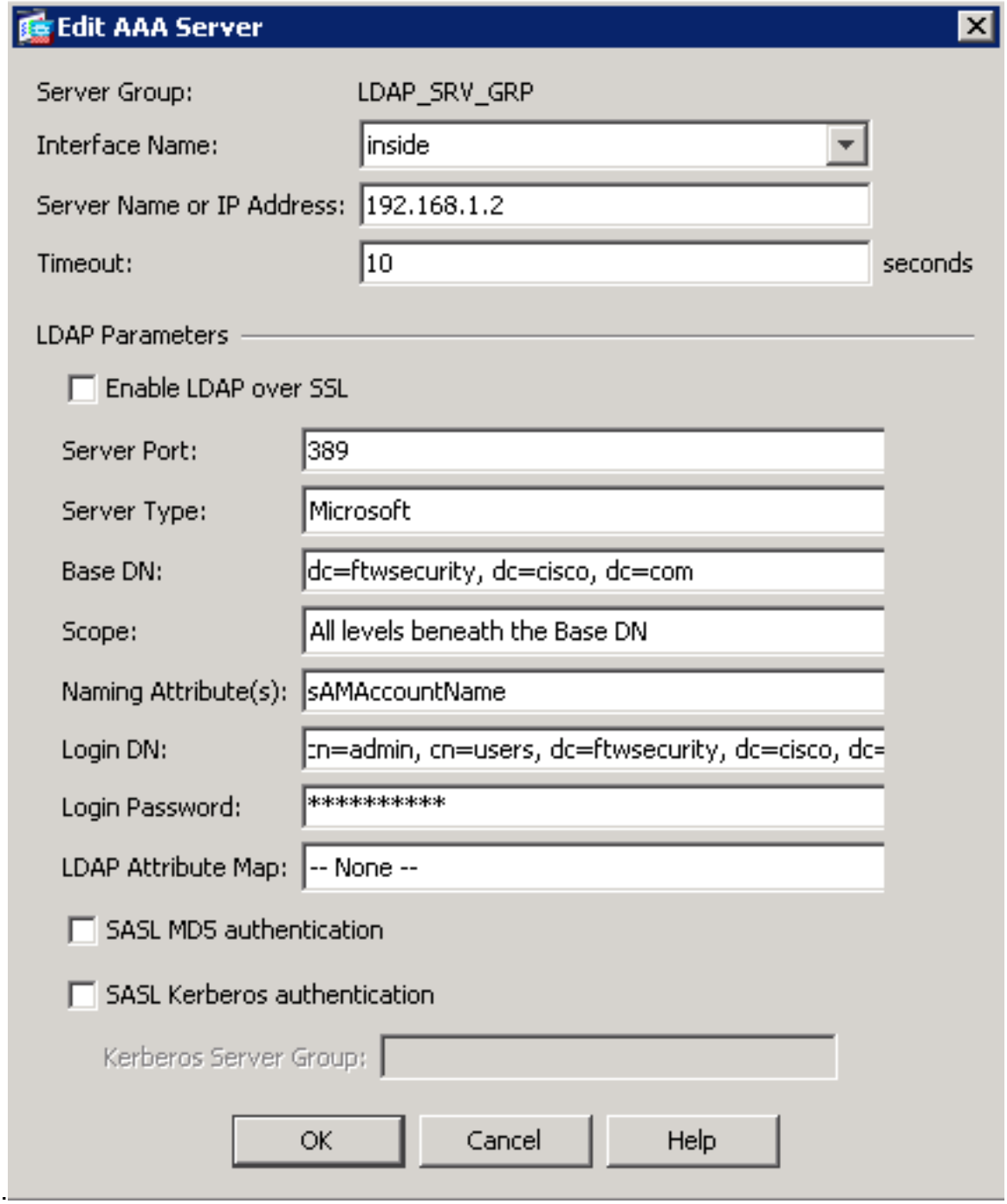
ASA가 LDAP 서버와 통신하고 WebVPN 클라이언트를 인증하도록 구성하려면 ASDM에서 다음 단계를 완료합니다.

1. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > AAA Setup(AAA 설정) > AAA Server Groups(AAA 서버 그룹)로 이동합니다.
2. AAA Server Groups(AAA 서버 그룹) 옆의 Add(추가)를 클릭합니다.
3. 새 AAA 서버 그룹의 이름을 지정하고 **LDAP**를 프로토콜로 선택합니다



4. 맨 위 창에서 새 그룹이 선택되었는지 확인하고 Selected Group(선택한 그룹) 창의 Servers(**서버**) 옆**에 Add(추가)를** 클릭합니다.
5. LDAP 서버에 대한 컨피그레이션 정보를 제공합니다.다음 스크린샷은 컨피그레이션의 예를

보여줍니다.다음은 여러 컨피그레이션 옵션에 대한 설명입니다.**Interface Name**—ASA가 LDAP 서버에 연결하기 위해 사용하는 인터페이스**Server Name or IP address(서버 이름 또는 IP 주소)** - LDAP 서버에 연결하기 위해 ASA에서 사용하는 주소입니다.**Server Type**(서버 유형) - LDAP 서버의 유형(예: Microsoft)**Base DN**—서버가 검색을 시작해야 하는 LDAP 계층 구조의 위치**범위** - 서버가 생성해야 하는 LDAP 계층 구조에서 검색의 범위**Naming Attribute**—LDAP 서버의 항목을 고유하게 식별하는 Relative Distinguished Name 특성(또는 특성).**sAMAccountName**은 Microsoft Active Directory의 기본 속성입니다.다른 일반적으로 사용되는 특성은 CN, UID 및 userPrincipalName입니다.**Login DN**—LDAP 서버에서 사용자를 검색/읽기/조회할 수 있는 충분한 권한이 있는 DN**Login Password**(로그인 비밀번호) - DN 계정의 비밀번호**LDAP Attribute Map** - 이 서버의 응답과 함께 사용할 LDAP 특성 맵입니다 .ASA/PIX 참조:LDAP 특성 맵을 구성하는 방법에 대한 자세한 내용은 LDAP 컨피그레이션을 통해 VPN 클라이언트를 VPN 그룹 정책에 매핑합니다

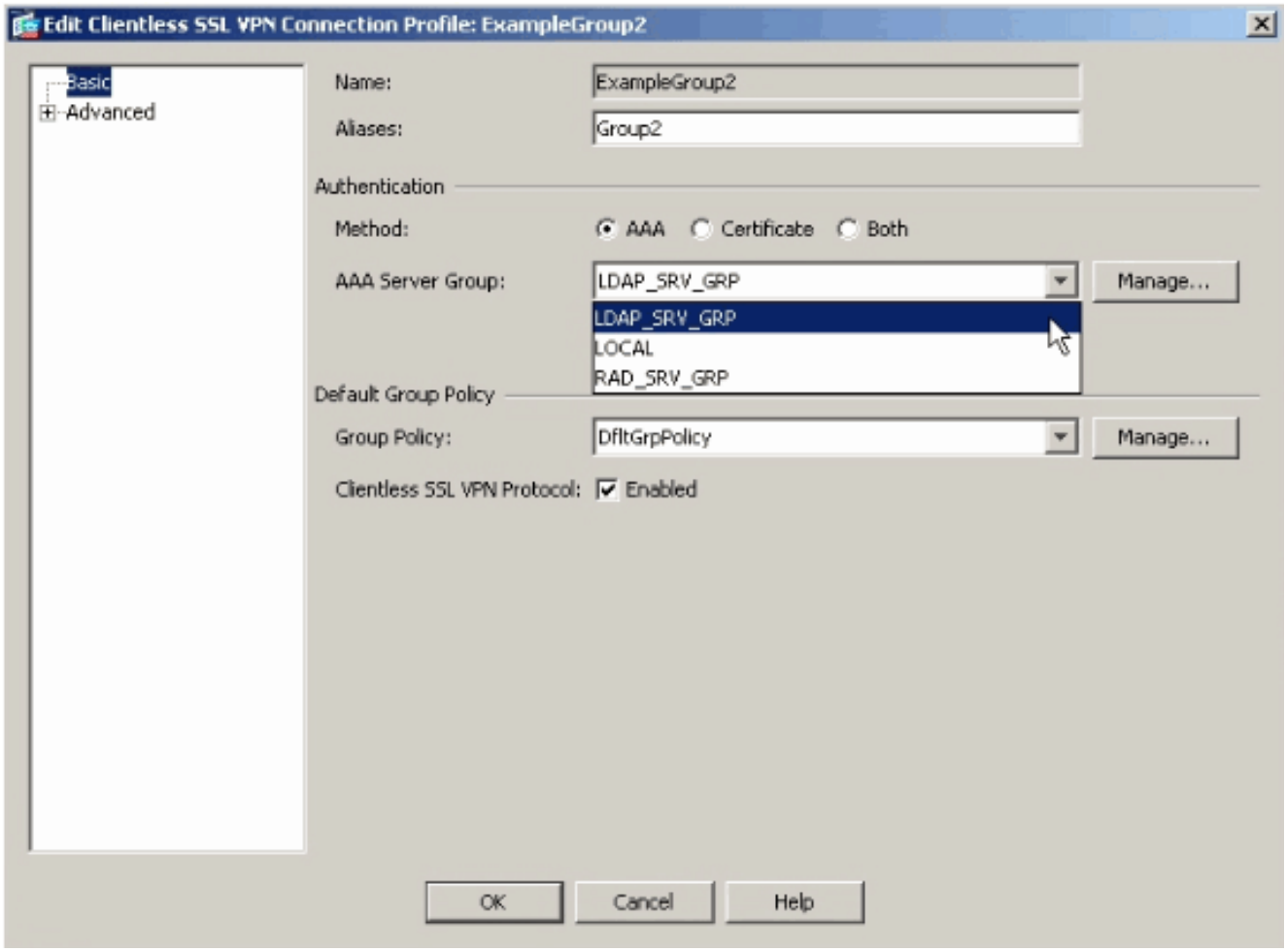


6. AAA 서버 그룹을 구성하고 서버에 서버를 추가한 후에는 새 AAA 컨피그레이션을 사용하도록 연결 프로파일(터널 그룹)을 구성해야 합니다.Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) >

Connection Profiles(연결 프로파일)로 이동합니다.

7. AAA를 구성할 연결 프로파일(터널 그룹)을 선택하고 Edit(수정)를 클릭합니다.
8. Authentication(**인증**)에서 이전에 생성한 LDAP 서버 그룹을 선택합니다

.



명령줄 인터페이스

LDAP 서버와 통신하고 WebVPN 클라이언트를 인증하도록 ASA를 구성하려면 CLI(Command Line Interface)에서 다음 단계를 완료합니다.

```
ciscoasa#configure terminal

!--- Configure the AAA Server group. ciscoasa(config)#aaa-server LDAP_SRV_GRP protocol ldap !---
Configure the AAA Server. ciscoasa(config-aaa-server-group)#aaa-server LDAP_SRV_GRP (inside)
host 192.168.1.2 ciscoasa(config-aaa-server-host)#ldap-base-dn dc=ftwsecurity, dc=cisco, dc=com
ciscoasa(config-aaa-server-host)#ldap-login-dn cn=admin, cn=users, dc=ftwsecurity, dc=cisco,
dc=com ciscoasa(config-aaa-server-host)#ldap-login-password ********** ciscoasa(config-aaa-
server-host)#ldap-naming-attribute sAMAccountName ciscoasa(config-aaa-server-host)#ldap-scope
subtree ciscoasa(config-aaa-server-host)#server-type microsoft ciscoasa(config-aaa-server-
host)#exit !--- Configure the tunnel group to use the new AAA setup. ciscoasa(config)#tunnel-
group ExampleGroup2 general-att ciscoasa(config-tunnel-general)#authentication-server-group
LDAP_SRV_GRP
```

다중 도메인 검색 수행(선택 사항)

선택 사항입니다.ASA는 현재 다중 도메인 검색을 위한 LDAP 참조 메커니즘을 지원하지 않습니다(Cisco 버그 ID CSCsj32153). 다중 도메인 검색은 글로벌 카탈로그 서버 모드의 AD에서 지원됩니다.다중 도메인 검색을 수행하려면 ASA의 LDAP 서버 항목에 대한 이러한 키 매개 변수와 함께 글

로벌 카탈로그 서버 모드에 대한 AD 서버를 설정합니다.키는 디렉토리 트리에서 고유해야 하는 ldap-name-attribute를 사용하는 것입니다.

```
server-port 3268
ldap-scope subtree
ldap-naming-attribute userPrincipalName
```

다음을 확인합니다.

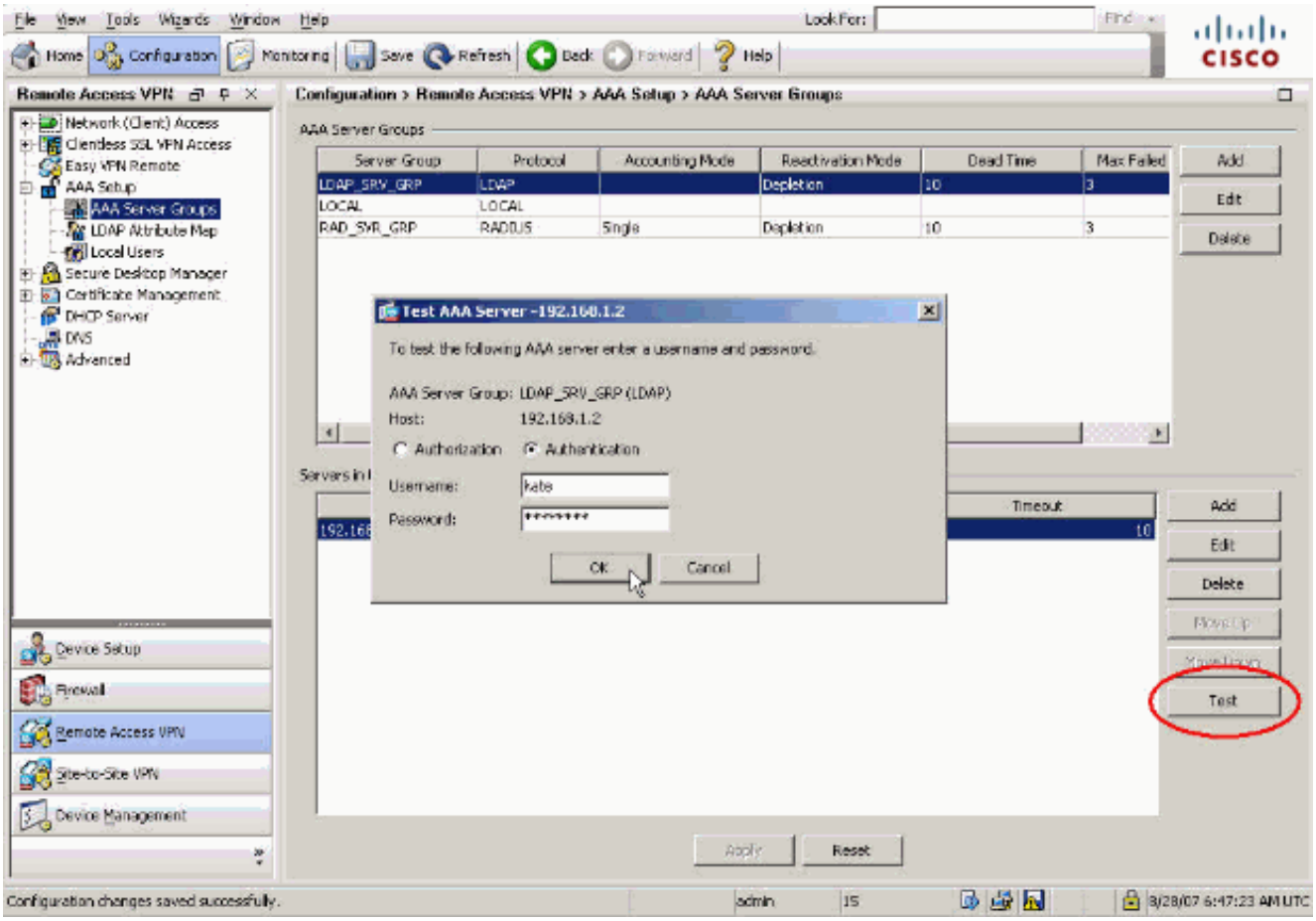
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

ASDM을 사용한 테스트

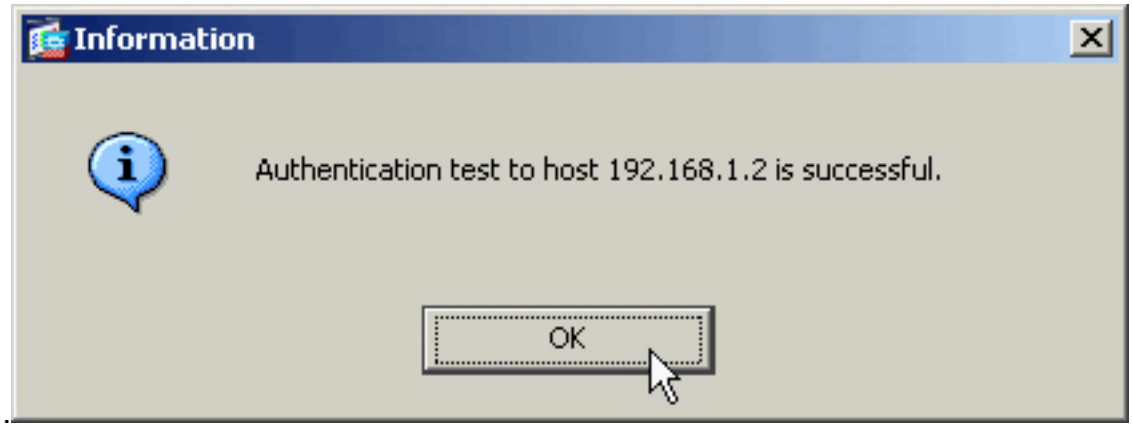
AAA Server Groups 컨피그레이션 화면의 **Test** 버튼을 사용하여 LDAP 컨피그레이션을 확인합니다.사용자 이름과 비밀번호를 입력하면 이 버튼을 사용하여 LDAP 서버에 테스트 인증 요청을 보낼 수 있습니다.

1. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > AAA Setup(AAA 설정) > AAA Server Groups(AAA 서버 그룹)로 이동합니다.
2. 상단 창에서 원하는 AAA 서버 그룹을 선택합니다.
3. 하단 창에서 테스트할 AAA 서버를 선택합니다.
4. 아래쪽 창 오른쪽의 **Test** 버튼을 클릭합니다.
5. 표시되는 창에서 **Authentication** 라디오 버튼을 클릭하고 테스트할 자격 증명을 입력합니다.완료되면 **OK(확인)**를 클릭합니다

.



6. ASA가 LDAP 서버에 접속하면 성공 또는 실패 메시지가 나타납니다



CLI로 테스트

명령행에서 **test** 명령을 사용하여 AAA 설정을 테스트할 수 있습니다.테스트 요청이 AAA 서버로 전송되고 그 결과가 명령줄에 나타납니다.

```
ciscoasa#test aaa-server authentication LDAP_SRV_GRP host 192.168.1.2
   username kate password cisco123
INFO: Attempting Authentication test to IP address <192.168.1.2>
   (timeout: 12 seconds)
INFO: Authentication Successful
```

문제 해결

사용할 현재 DN 문자열을 잘 모르는 경우 명령 프롬프트에서 **dsquery** 명령을 실행하여 사용자 객체의 적절한 DN 문자열을 확인할 수 있습니다.

```
C:\Documents and Settings\Administrator>dsquery user -samid kate

!--- Queries Active Directory for samid id "kate" "CN=Kate
Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com"
```

debug ldap 255 명령은 이 시나리오의 인증 문제를 해결하는 데 도움이 될 수 있습니다.이 명령은 LDAP 디버깅을 활성화하고 ASA가 LDAP 서버에 연결하는 데 사용하는 프로세스를 감시할 수 있도록 합니다.이 출력은 이 문서의 Background Information(배경 정보) 섹션에 설명된 대로 LDAP 서버에 ASA 연결을 보여줍니다.

이 디버그는 성공적인 인증을 보여줍니다.

```
ciscoasa#debug ldap 255
[7] Session Start
[7] New request Session, context 0xd4b11730, reqType = 1
[7] Fiber started
[7] Creating LDAP context with uri=ldap://192.168.1.2:389
[7] Connect to LDAP server: ldap://192.168.1.2:389, status = Successful
[7] defaultNamingContext: value = DC=ftwsecurity,DC=cisco,DC=com
[7] supportedLDAPVersion: value = 3
[7] supportedLDAPVersion: value = 2
[7] supportedSASLMechanisms: value = GSSAPI
[7] supportedSASLMechanisms: value = GSS-SPNEGO
[7] supportedSASLMechanisms: value = EXTERNAL
[7] supportedSASLMechanisms: value = DIGEST-MD5
```

```
!--- The ASA connects to the LDAP server as admin to search for kate. [7] Binding as
administrator
[7] Performing Simple authentication for admin to 192.168.1.2
[7] LDAP Search:
        Base DN = [dc=ftwsecurity, dc=cisco, dc=com]
        Filter  = [sAMAccountName=kate]
        Scope   = [SUBTREE]
[7] User DN = [CN=Kate Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com]
[7] Talking to Active Directory server 192.168.1.2
[7] Reading password policy for kate, dn:CN=Kate Austen,CN=Users,
      DC=ftwsecurity,DC=cisco,DC=com
[7] Read bad password count 1

!--- The ASA binds to the LDAP server as kate to test the password. [7] Binding as user
[7] Performing Simple authentication for kate to 192.168.1.2
[7] Checking password policy for user kate
[7] Binding as administrator
[7] Performing Simple authentication for admin to 192.168.1.2
[7] Authentication successful for kate to 192.168.1.2
[7] Retrieving user attributes from server 192.168.1.2
[7] Retrieved Attributes:
[7]     objectClass: value = top
[7]     objectClass: value = person
[7]     objectClass: value = organizationalPerson
[7]     objectClass: value = user
[7]     cn: value = Kate Austen
[7]     sn: value = Austen
[7]     givenName: value = Kate
[7]     distinguishedName: value = CN=Kate Austen,CN=Users,DC=ftwsecurity,
          DC=cisco,DC=com
[7]     instanceType: value = 4
[7]     whenCreated: value = 20070815155224.0Z
[7]     whenChanged: value = 20070815195813.0Z
[7]     displayName: value = Kate Austen
[7]     uSNCreated: value = 16430
[7]     memberOf: value = CN=Castaways,CN=Users,DC=ftwsecurity,DC=cisco,DC=com
[7]     memberOf: value = CN=Employees,CN=Users,DC=ftwsecurity,DC=cisco,DC=com
[7]     uSNChanged: value = 20500
[7]     name: value = Kate Austen
[7]     objectGUID: value = ..z...yC.q0.....
[7]     userAccountControl: value = 66048
[7]     badPwdCount: value = 1
[7]     codePage: value = 0
[7]     countryCode: value = 0
[7]     badPasswordTime: value = 128321799570937500
[7]     lastLogoff: value = 0
[7]     lastLogon: value = 128321798130468750
[7]     pwdLastSet: value = 128316667442656250
[7]     primaryGroupID: value = 513
[7]     objectSid: value = ............Q..p..*.p?E.Z...
[7]     accountExpires: value = 9223372036854775807
[7]     logonCount: value = 0
[7]     sAMAccountName: value = kate
[7]     sAMAccountType: value = 805306368
[7]     userPrincipalName: value = kate@ftwsecurity.cisco.com
[7]     objectCategory: value = CN=Person,CN=Schema,CN=Configuration,
          DC=ftwsecurity,DC=cisco,DC=com
[7]     dSCorePropagationData: value = 20070815195237.0Z
[7]     dSCorePropagationData: value = 20070815195237.0Z
[7]     dSCorePropagationData: value = 20070815195237.0Z
[7]     dSCorePropagationData: value = 16010108151056.0Z
[7] Fiber exit Tx=685 bytes Rx=2690 bytes, status=1
[7] Session End
```

이 디버그는 잘못된 암호로 인해 실패한 인증을 표시합니다.

```
ciscoasa#debug ldap 255
[8] Session Start
[8] New request Session, context 0xd4b11730, reqType = 1
[8] Fiber started
[8] Creating LDAP context with uri=ldap://192.168.1.2:389
[8] Connect to LDAP server: ldap://192.168.1.2:389, status = Successful
[8] defaultNamingContext: value = DC=ftwsecurity,DC=cisco,DC=com
[8] supportedLDAPVersion: value = 3
[8] supportedLDAPVersion: value = 2
[8] supportedSASLMechanisms: value = GSSAPI
[8] supportedSASLMechanisms: value = GSS-SPNEGO
[8] supportedSASLMechanisms: value = EXTERNAL
[8] supportedSASLMechanisms: value = DIGEST-MD5

!--- The ASA connects to the LDAP server as admin to search for kate. [8] Binding as
administrator
[8] Performing Simple authentication for admin to 192.168.1.2
[8] LDAP Search:
        Base DN = [dc=ftwsecurity, dc=cisco, dc=com]
        Filter  = [sAMAccountName=kate]
        Scope   = [SUBTREE]
[8] User DN = [CN=Kate Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com]
[8] Talking to Active Directory server 192.168.1.2
[8] Reading password policy for kate, dn:CN=Kate Austen,CN=Users,
      DC=ftwsecurity,DC=cisco,DC=com
[8] Read bad password count 1

!--- The ASA attempts to bind as kate, but the password is incorrect. [8] Binding as user
[8] Performing Simple authentication for kate to 192.168.1.2
[8] Simple authentication for kate returned code (49) Invalid credentials
[8] Binding as administrator
[8] Performing Simple authentication for admin to 192.168.1.2
[8] Reading bad password count for kate, dn: CN=Kate Austen,CN=Users,
      DC=ftwsecurity,DC=cisco,DC=com
[8] Received badPwdCount=1 for user kate
[8] badPwdCount=1 before, badPwdCount=1 after for kate
[8] now: Tue, 28 Aug 2007 15:33:05 GMT, lastset: Wed, 15 Aug 2007 15:52:24 GMT,
      delta=1122041, maxage=3710851 secs
[8] Invalid password for kate
[8] Fiber exit Tx=788 bytes Rx=2904 bytes, status=-1
[8] Session End
```

이 디버그는 LDAP 서버에서 사용자를 찾을 수 없으므로 실패한 인증을 표시합니다.

```
ciscoasa#debug ldap 255
[9] Session Start
[9] New request Session, context 0xd4b11730, reqType = 1
[9] Fiber started
[9] Creating LDAP context with uri=ldap://192.168.1.2:389
[9] Connect to LDAP server: ldap://192.168.1.2:389, status = Successful
[9] defaultNamingContext: value = DC=ftwsecurity,DC=cisco,DC=com
[9] supportedLDAPVersion: value = 3
[9] supportedLDAPVersion: value = 2
[9] supportedSASLMechanisms: value = GSSAPI
[9] supportedSASLMechanisms: value = GSS-SPNEGO
[9] supportedSASLMechanisms: value = EXTERNAL
[9] supportedSASLMechanisms: value = DIGEST-MD5

!--- The user mikhail is not found. [9] Binding as administrator
```

```
[9] Performing Simple authentication for admin to 192.168.1.2
[9] LDAP Search:
        Base DN = [dc=ftwsecurity, dc=cisco, dc=com]
        Filter  = [sAMAccountName=mikhail]
        Scope   = [SUBTREE]
[9] Requested attributes not found
[9] Fiber exit Tx=256 bytes Rx=607 bytes, status=-1
[9] Session End
```

ASA와 LDAP 인증 서버 간의 연결이 작동하지 않을 경우 디버그에서 이 오류 메시지를 표시합니다.

```
ciscoasa# debug webvpn 255
INFO: debug webvpn  enabled at level 255.
ciscoasa# webvpn_portal.c:ewaFormSubmit_webvpn_login[2162]
ewaFormSubmit_webvpn_login: tgCookie = NULL
ewaFormSubmit_webvpn_login: cookie = 1
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
....not resuming [2587]
webvpn_portal.c:http_webvpn_kill_cookie[787]
webvpn_auth.c:http_webvpn_pre_authentication[2327]
WebVPN: calling AAA with ewsContext (-847917520) and nh (-851696992)!
webvpn_auth.c:webvpn_add_auth_handle[5118]
WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[5158]
WebVPN: AAA status = (ERROR)
webvpn_portal.c:ewaFormSubmit_webvpn_login[2162]
ewaFormSubmit_webvpn_login: tgCookie = NULL
ewaFormSubmit_webvpn_login: cookie = 1
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
....resuming [2564]
webvpn_auth.c:http_webvpn_post_authentication[1506]
WebVPN: user: (utrcd01) auth error.
```

관련 정보

- 기술 지원 및 문서 – Cisco Systems