ASA 8.0: LDAP-verificatie voor WebVPN-gebruikers configureren

Inhoud

Inleiding

Dit document toont aan hoe u de Cisco adaptieve security applicatie (ASA) moet configureren om een LDAP server te gebruiken voor verificatie van WebVPN-gebruikers. De LDAP server in dit voorbeeld is Microsoft Active Directory. Deze configuratie wordt uitgevoerd met Adaptieve Security Devices Manager (ASDM) 6.0(2) op een ASA die softwareversie 8.0(2) uitvoert.

Opmerking: In dit voorbeeld wordt de lichtgewicht Directory Access Protocol (LDAP) verificatie ingesteld voor WebVPN gebruikers, maar deze configuratie kan ook worden gebruikt voor alle andere soorten externe toegangsclients. U kunt de AAA-servergroep gewoon toewijzen aan het gewenste verbindingsprofiel (tunnelgroep) zoals wordt weergegeven.

Voorwaarden

Er is een basisconfiguratie voor VPN vereist. In dit voorbeeld wordt WebexVPN gebruikt.

Achtergrondinformatie

In dit voorbeeld controleert de ASA met een LDAP-server om de identiteit van de gebruikers te verifiëren die het echt authentiek maakt. Dit proces werkt niet als een traditionele inbel-gebruikersservice (RADIUS) of terminale toegangscontrollersysteem plus (TACACS+)-uitwisseling. Deze stappen verklaren, op hoog niveau, hoe de ASA een LDAP server gebruikt om gebruikersreferenties te controleren.

1. De gebruiker initieert een verbinding met de ASA.
2. De ASA is ingesteld om deze gebruiker te authenticeren met de Microsoft Active Directory (AD)/LDAP server.
3. De ASA bindt aan de LDAP-server met de aanmeldingsgegevens die op de ASA zijn ingesteld (in dit geval admin) en zoekt de opgegeven gebruikersnaam op. De **admin**-gebruiker krijgt ook de juiste aanmeldingsgegevens om de inhoud in de actieve map op te geven. Raadpleeg http://support.microsoft.com/?id=320528 voor meer informatie over het verlenen van LDP-zoekrechten.Opmerking: De website van Microsoft op http://support.microsoft.com/?id=320528 wordt beheerd door een derde partij provider. Cisco is niet verantwoordelijk voor de inhoud.
4. Als de gebruikersnaam wordt gevonden, probeert de ASA zich te binden aan de LDAP server met de referenties die de gebruiker bij inloggen heeft opgegeven.
5. Als de tweede bind succesvol is, slaagt de authenticatie en de ASA de eigenschappen van de gebruiker.**Toelichting:** In dit voorbeeld worden de eigenschappen voor niets gebruikt. Raadpleeg ASA/PIX: VPN-clients aan VPN-groepsbeleid toewijzen door middel van LDAP-configuratievoorbeeld om een voorbeeld te zien van hoe de ASA LDAP-eigenschappen kan verwerken.

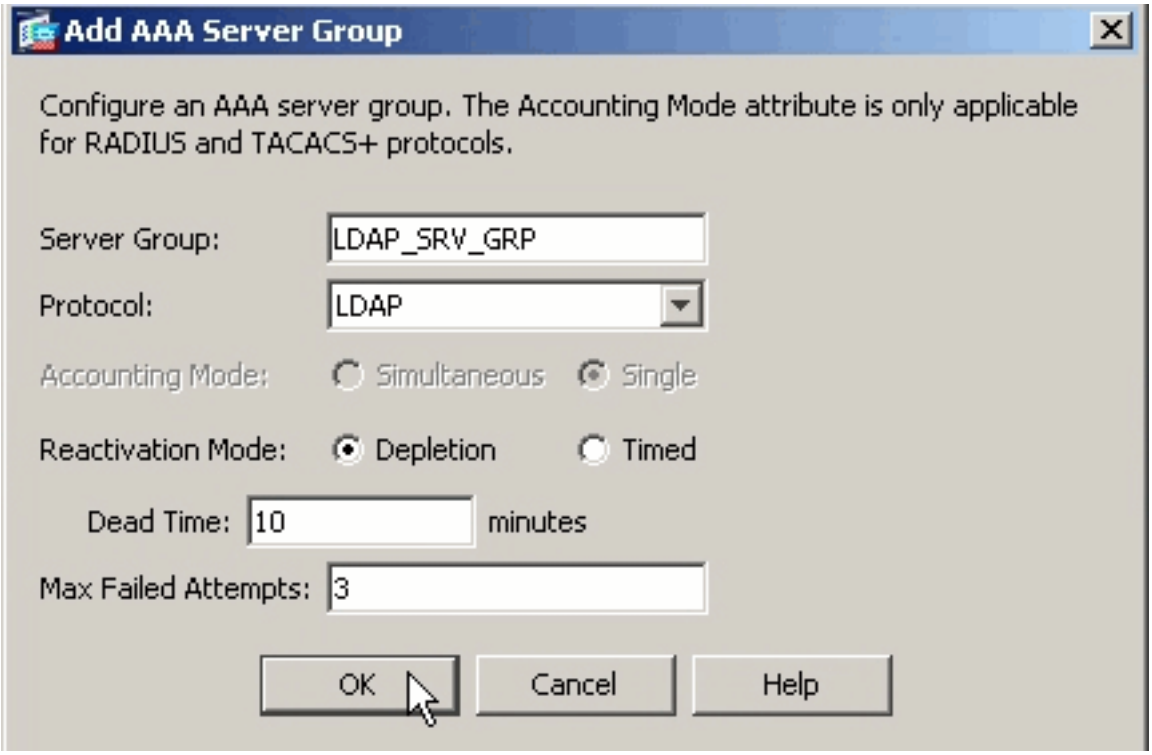
LDAP-verificatie configureren

In deze sectie, wordt u voorgesteld met de informatie om de ASA te vormen om een server te gebruiken LBP voor de authenticatie van WebVPN cliënten.

ASDM

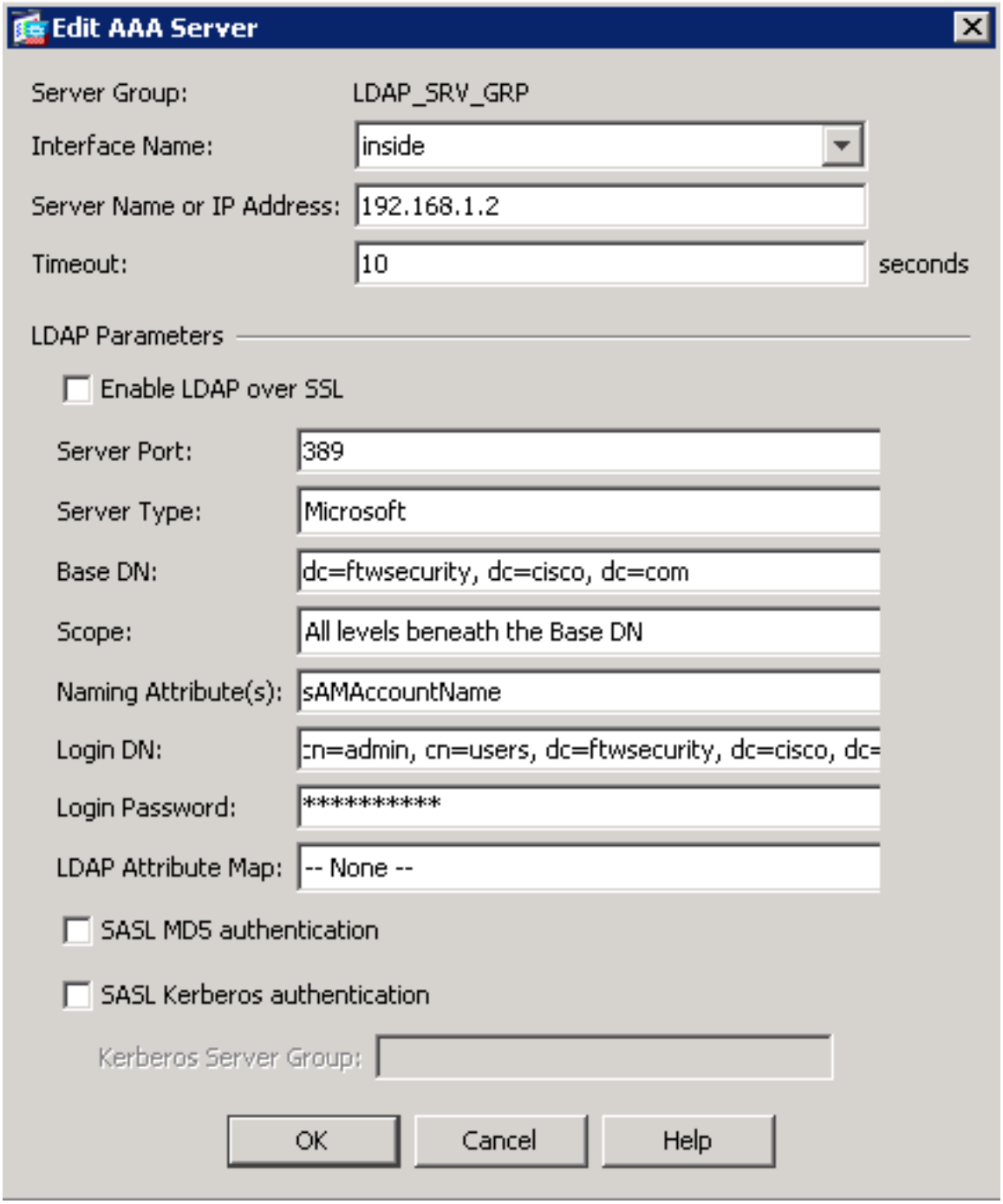
Voltooi deze stappen in de ASDM om de ASA te vormen om met de LDAP server te communiceren en om WebVPN clients te echt te maken.

1. Navigatie in naar Configuration > Remote Access VPN > AAA-instelling > AAA-servergroepen.
2. Klik op **Add** naast AAA-servergroepen
3. Specificeer een naam voor de nieuwe AAA-servergroep en kies **LDAP** als

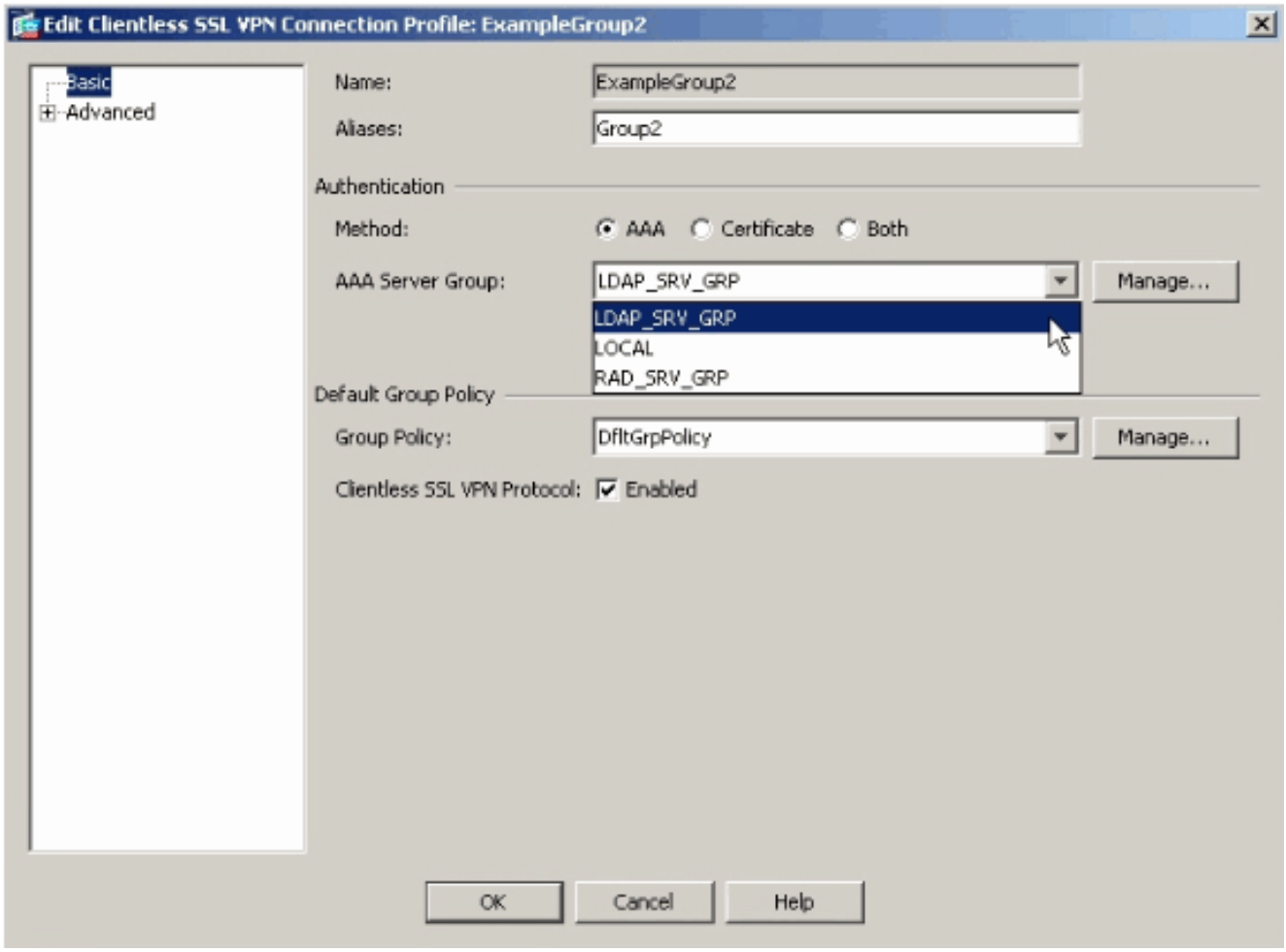


protocol.

4. Zorg dat uw nieuwe groep in het bovenvenster is geselecteerd en klik op **Toevoegen** naast de **servers in het** deelvenster **Geselecteerde groep**.
5. Geef de configuratieinformatie voor uw LDAP-server op. Het volgende screenshot illustreert een voorbeeldconfiguratie. Dit is een verklaring voor veel van de configuratieopties:**Interfacenaam** - de interface die de ASA gebruikt om de LDAP server te bereiken**servernaam of IP-adres**: het adres dat de ASA gebruikt om de LDAP-server te bereiken**Type server**: het type LDAP-server, zoals Microsoft**Base DN**-de locatie in de LDAP-hiërarchie waar de server moet beginnen met zoeken**Toepassingsgebied**: de reikwijdte van de zoekopdracht in de LDAP-hiërarchie die de server moet maken**Namingkenmerk** — de Relatieve eigenschap Naam (of eigenschappen) die een vermelding op de LDAP-server uniek identificeert. **sAMAcountName** is de standaardeigenschap in de Microsoft Active Directory. Andere veelgebruikte eigenschappen zijn CN, UID en userPrincipalName.**Login DN** - de DNA met voldoende bevoegdheden om gebruikers in de LDAP server te kunnen zoeken/lezen/raadplegen**Wachtwoord voor aanmelding**—het wachtwoord voor de DNS-account**Kaart van de LPDP-kenmerken** — een LBP-attributenkaart die moet worden gebruikt met reacties van deze server. Raadpleeg ASA/PIX: VPN-clients in kaart brengen met VPN-groepsbeleid door middel van LDAP Configuration Voorbeeld voor meer informatie over het configureren van LBP-attributiekaarten.



6. Nadat u de AAA-servergroep hebt ingesteld en er een server aan hebt toegevoegd, dient u uw verbindingsprofiel (tunnelgroep) te configureren om de nieuwe AAA-configuratie te gebruiken. Navigatie in naar Configuration > Remote Access VPN > Clientloze SSL VPN-toegang > Connection profielen.
7. Kies het verbindingsprofiel (tunnelgroep) waarvoor u AAA wilt configureren en klik op **Bewerken**
8. Kies onder **Verificatie** de LDAP servergroep die u eerder hebt gemaakt.



Opdrachtlijn-interface

Voltooi deze stappen in de opdrachtregel interface (CLI) om de ASA te configureren om te communiceren met de LDAP server en WebeVPN-clients te authenticeren.

```
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
```

Optioneel: meerdere domeinen zoeken

Optioneel. De ASA steunt momenteel niet het LDAP-verwijzingsmechanisme voor zoeken op meerdere domeinen (Cisco bug ID CSCsj32153). Doorzoekingen op meerdere domeinen worden ondersteund met de AD in de modus Global Catalog Server. Stel de AD-server in voor de modus Global Catalog Server, meestal met de belangrijkste parameters voor de LDAP-server in de ASA, om meerdere domeinen te kunnen doorzoeken. De sleutel is om een ldap-name-attribuut te gebruiken dat uniek moet zijn over de folder boom.

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

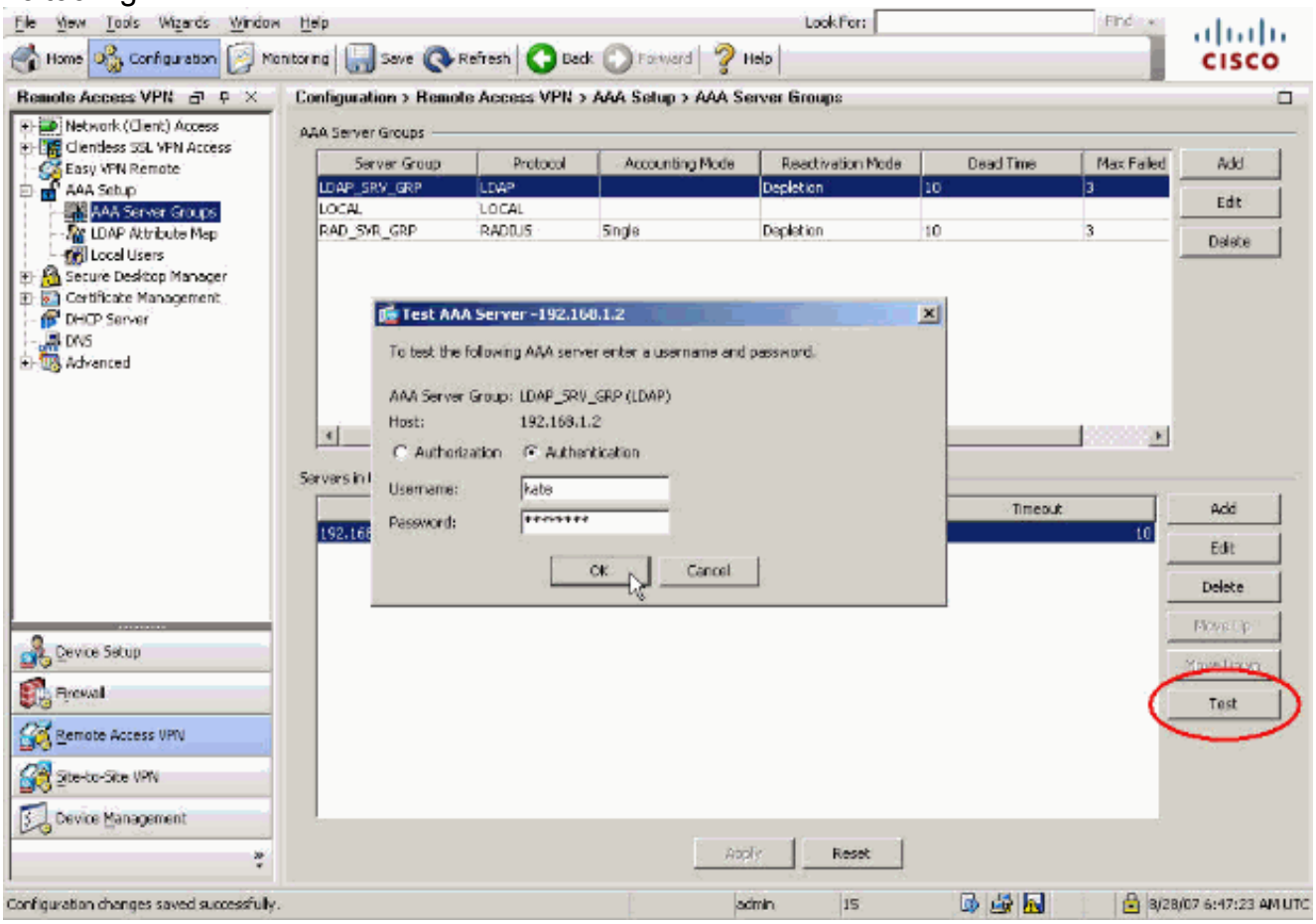
Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

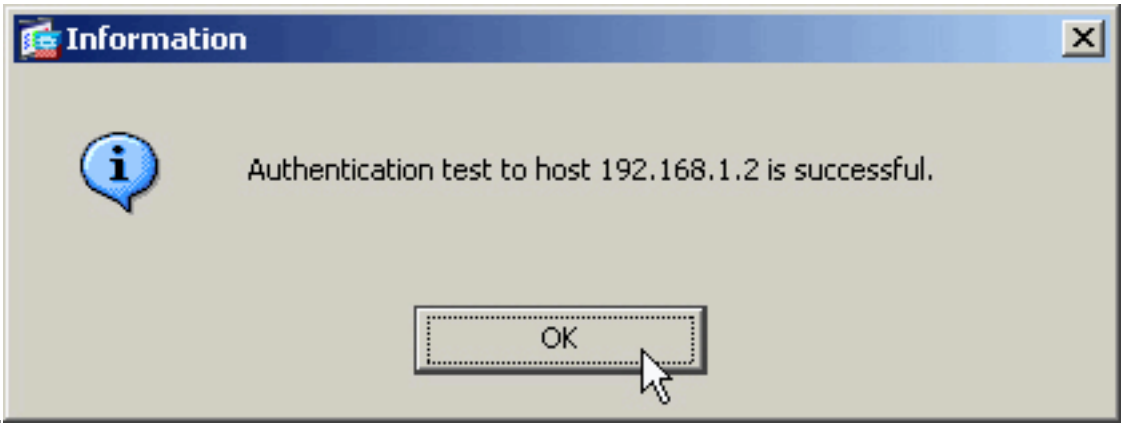
Test met ASDM

Controleer de configuratie van de LDAP met de **Test**-knop op het configuratiescherm van AAA-servergroepen. Zodra u een gebruikersnaam en wachtwoord hebt opgegeven, kunt u met deze knop een verzoek om verificatie naar de LDAP-server sturen.

1. Navigatie in naar Configuration > Remote Access VPN > AAA-instelling > AAA-servergroepen.
2. Selecteer uw gewenste AAA-servergroep in het bovenste venster.
3. Selecteer de AAA-server die u in het onderste venster wilt testen.
4. Klik op de knop **Test** rechts in het ondervenster.
5. Klik in het venster dat verschijnt op het radioknop **Verificatie** en specificeer de referenties waarmee u wilt testen. Klik op **OK** na voltooiing.



6. Nadat de ASA de LDAP server contacteert, verschijnt een succes of mislukking

bericht. 

Test met CLI

U kunt de testopdracht in de opdrachtregel gebruiken om de AAA-instelling te testen. Een testverzoek wordt naar de AAA server verzonden, en het resultaat verschijnt op de opdrachtregel.

```
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
```

Problemen oplossen

Als u niet zeker weet van het huidige DNS-string, kunt u de kledingopdracht uitgeven op een Windows Active Driectory-server vanaf een opdrachtmelding om het juiste DNA-string van een gebruikersobject te controleren.

```
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"
```

De opdracht **Debug Ldap 255** kan in dit scenario problemen met de verificatie van probleemoplossing helpen oplossen. Met deze opdracht kunt u de functie voor het fouilleren van LDAP uitvoeren en kunt u het proces volgen dat de ASA gebruikt om verbinding te maken met de LDAP server. Deze output laat zien dat de ASA verbinding heeft gemaakt met de LDAP server zoals beschreven in het gedeelte Achtergrondinformatie van dit document.

Dit debug toont een succesvolle authenticatie:

```
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
```

Dit debug toont een authenticatie die mislukt vanwege een incorrect wachtwoord:

```
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
```

Dit debug toont een authenticatie die mislukt omdat de gebruiker niet op de LDAP server kan worden gevonden:

```
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
```

Deze foutmelding wordt getoond wanneer de verbinding tussen de ASA en de LDAP-verificatieserver niet werkt:

```
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.
```

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems