ASA 8.0: Konfigurieren der LDAP-Authentifizierung für WebVPN-Benutzer

Inhalt

Einführung

Dieses Dokument veranschaulicht, wie die Cisco Adaptive Security Appliance (ASA) so konfiguriert wird, dass sie einen LDAP-Server für die Authentifizierung von WebVPN-Benutzern verwendet. Der LDAP-Server in diesem Beispiel ist Microsoft Active Directory. Diese Konfiguration wird mit dem Adaptive Security Device Manager (ASDM) 6.0(2) auf einer ASA ausgeführt, die die Softwareversion 8.0(2) ausführt.

Hinweis: In diesem Beispiel wird die LDAP-Authentifizierung (Lightweight Directory Access Protocol) für WebVPN-Benutzer konfiguriert. Diese Konfiguration kann jedoch auch für alle anderen Typen von Remote-Zugriffs-Clients verwendet werden. Weisen Sie einfach die AAA-Servergruppe dem gewünschten Verbindungsprofil (Tunnelgruppe) zu, wie dargestellt.

Voraussetzungen

Eine grundlegende VPN-Konfiguration ist erforderlich. In diesem Beispiel wird WebVPN verwendet.

Hintergrundinformationen

In diesem Beispiel überprüft die ASA mit einem LDAP-Server die Identität der Benutzer, die sie authentifiziert. Dieser Prozess funktioniert nicht wie bei einem herkömmlichen RADIUS-Austausch (Remote Authentication Dial-In User Service) oder TACACS+ (Terminal Access Controller Access Control System Plus). In diesen Schritten wird auf allgemeiner Ebene erklärt, wie die ASA einen

LDAP-Server verwendet, um Benutzeranmeldeinformationen zu überprüfen.

1. Der Benutzer initiiert eine Verbindung zur ASA.
2. Die ASA ist so konfiguriert, dass dieser Benutzer vom Microsoft Active Directory (AD)-/LDAP-Server authentifiziert wird.
3. Die ASA bindet sich mit den auf der ASA konfigurierten Anmeldeinformationen an den LDAP-Server (in diesem Fall Admin) und sucht den angegebenen Benutzernamen. Der **Admin-**Benutzer erhält auch die entsprechenden Anmeldeinformationen für die Auflistung von Inhalten in Active Directory. Weitere Informationen zum Gewähren von LDAP-Abfrageberechtigungen finden Sie unter http://support.microsoft.com/?id=320528 .**Hinweis:** Die Microsoft-Website unter http://support.microsoft.com/?id=320528 wird von einem Drittanbieter verwaltet. Cisco ist für die Inhalte nicht verantwortlich.
4. Wenn der Benutzername gefunden wird, versucht die ASA, mit den Anmeldeinformationen, die der Benutzer bei der Anmeldung angegeben hat, eine Verbindung zum LDAP-Server herzustellen.
5. Wenn die zweite Bindung erfolgreich ist, ist die Authentifizierung erfolgreich, und die ASA verarbeitet die Attribute des Benutzers.**Hinweis:** In diesem Beispiel werden die Attribute für nichts verwendet. Weitere Informationen finden Sie unter ASA/PIX: Zuordnen von VPN-Clients zu VPN-Gruppenrichtlinien mithilfe des LDAP-Konfigurationsbeispiels, um ein Beispiel zu sehen, wie die ASA LDAP-Attribute verarbeiten kann.

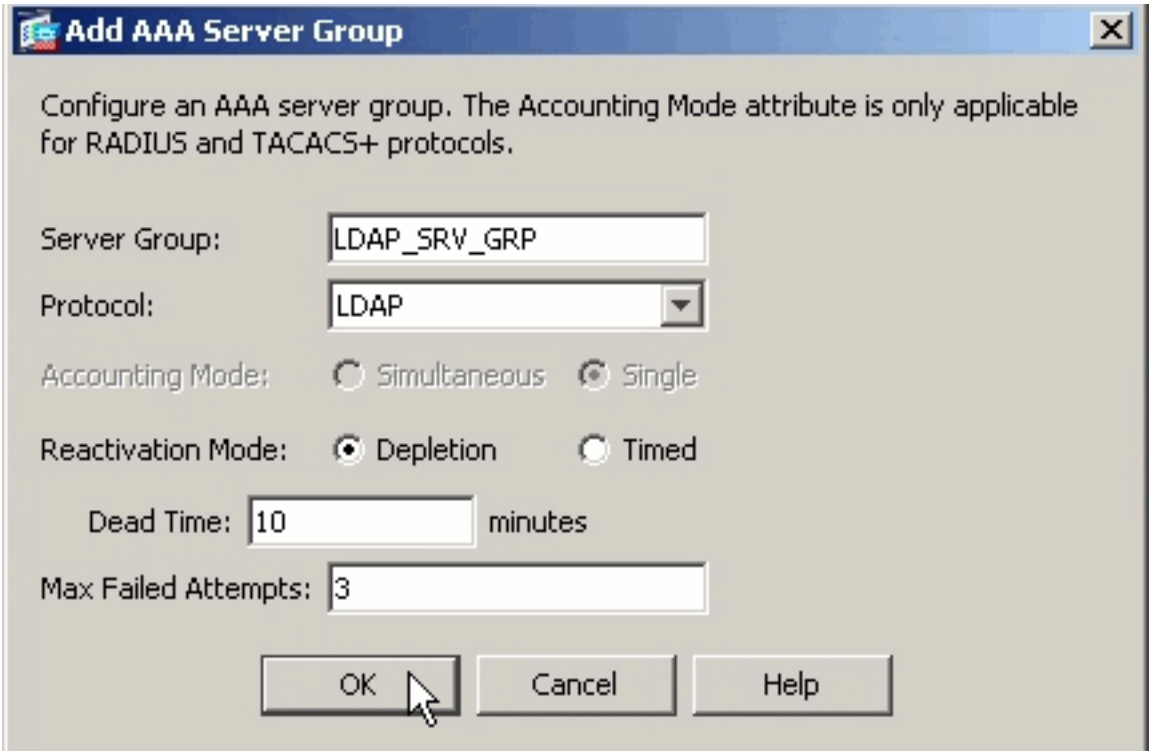
LDAP-Authentifizierung konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der ASA zur Verwendung eines LDAP-Servers für die Authentifizierung von WebVPN-Clients.

ASDM

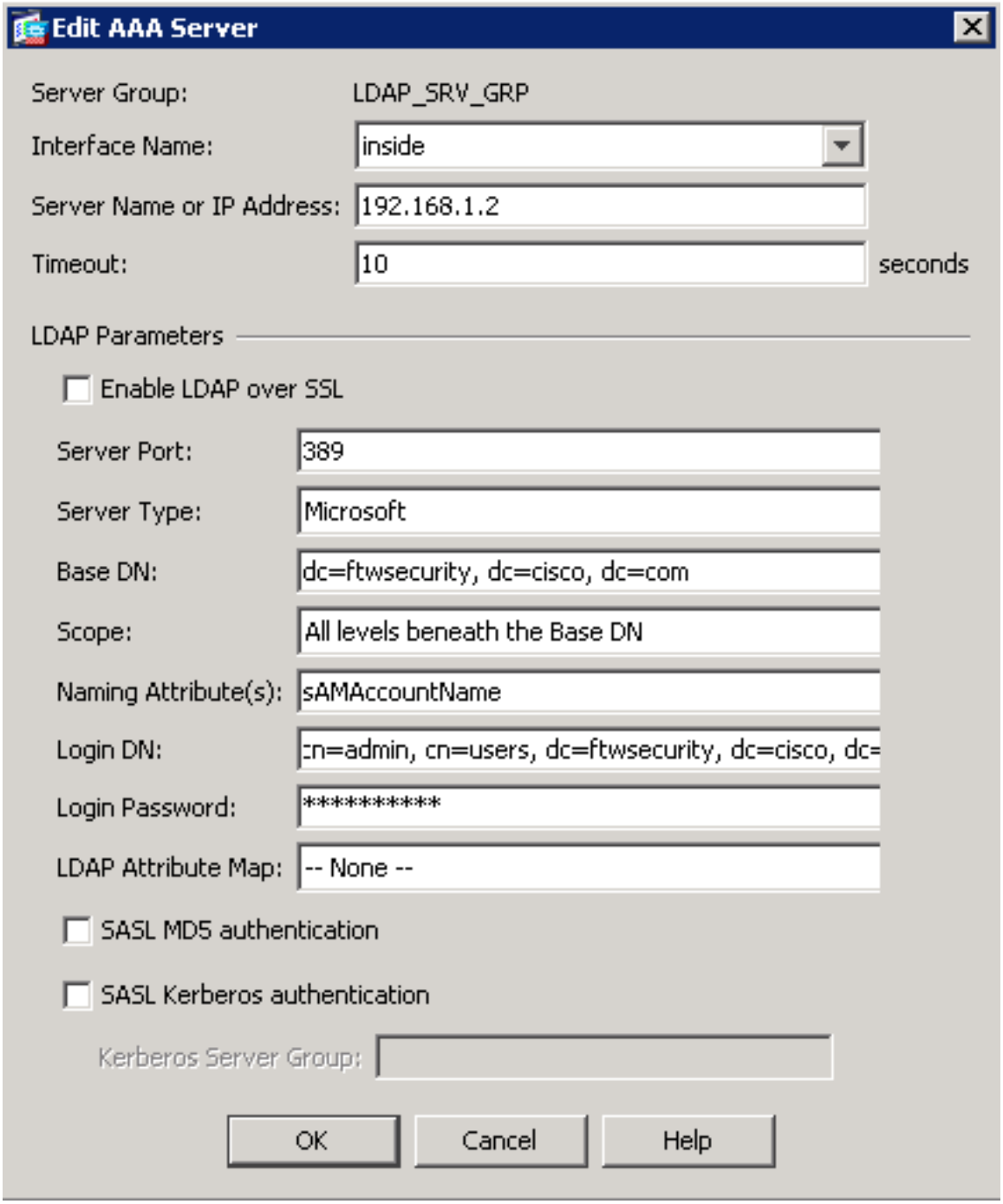
Führen Sie diese Schritte im ASDM aus, um die ASA für die Kommunikation mit dem LDAP-Server und die Authentifizierung von WebVPN-Clients zu konfigurieren.

1. Navigieren Sie zu Configuration > Remote Access VPN > AAA Setup > AAA Server Groups.
2. Klicken Sie neben AAA-Servergruppen **auf Hinzufügen**
3. Geben Sie einen Namen für die neue AAA-Servergruppe an, und wählen Sie **LDAP** als Protokoll

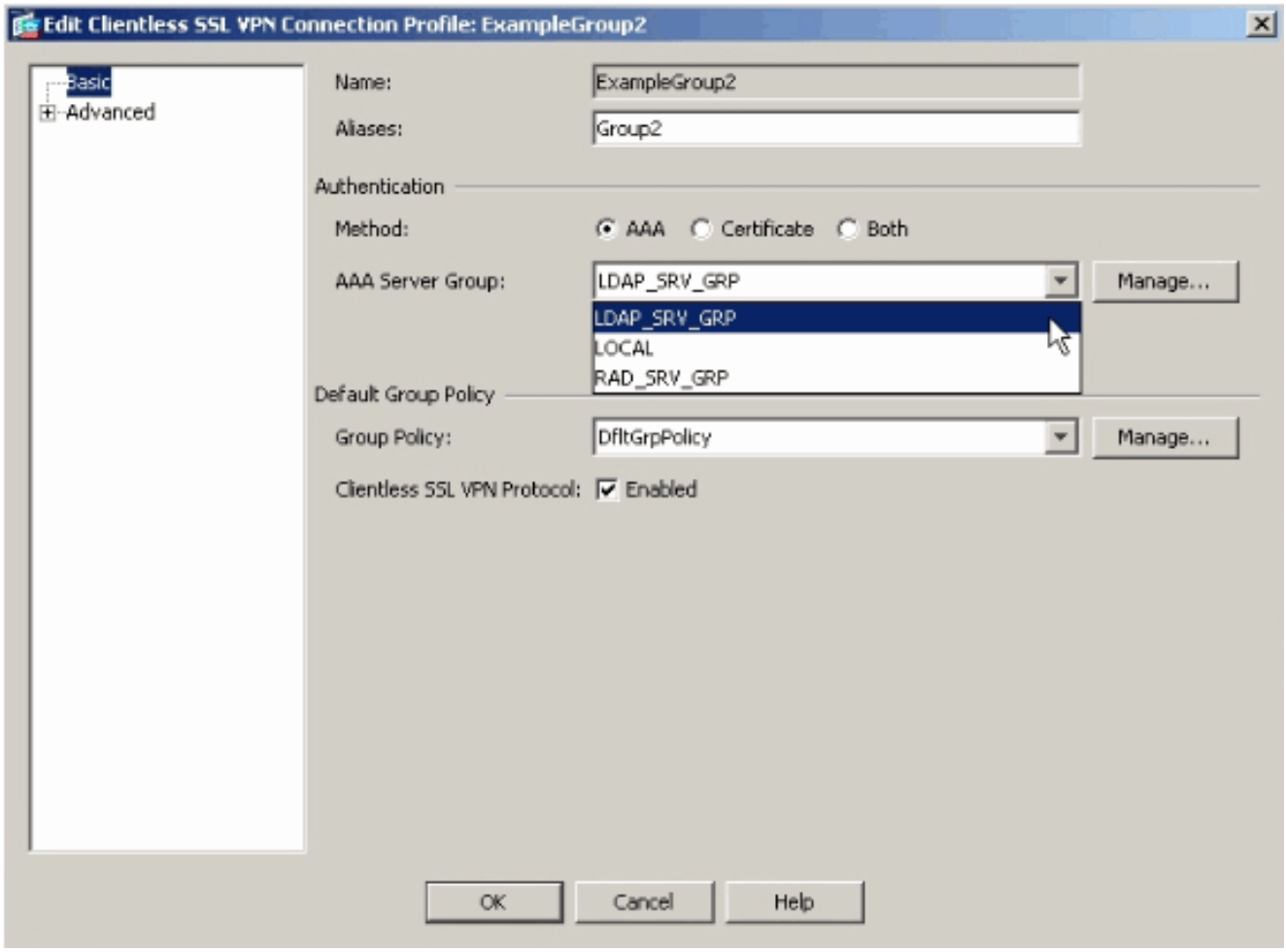


aus.

4. Stellen Sie sicher, dass Ihre neue Gruppe im oberen Bereich ausgewählt ist, und klicken Sie neben den **Servern im** Bereich **"Ausgewählte Gruppe" auf Hinzufügen**.
5. Geben Sie die Konfigurationsinformationen für Ihren LDAP-Server an. Im folgenden Screenshot wird eine Beispielkonfiguration veranschaulicht. Dies ist eine Erklärung für viele der Konfigurationsoptionen:**Schnittstellenname** - die Schnittstelle, die die ASA verwendet, um den LDAP-Server zu erreichen.**Servername oder IP-Adresse** - die Adresse, die die ASA verwendet, um den LDAP-Server zu erreichen.**Servertyp**: Der Typ des LDAP-Servers, z. B. Microsoft**Basis-DN** - Der Speicherort in der LDAP-Hierarchie, an dem der Server mit der Suche beginnen muss.**Umfang** - Der Umfang der Suche in der LDAP-Hierarchie, die der Server durchführen muss**Naming Attribute**: das Attribut für den relativen Distinguished Name (oder Attribute), das einen Eintrag auf dem LDAP-Server eindeutig identifiziert. **sAMAccountName** ist das Standardattribut im Microsoft Active Directory. Weitere häufig verwendete Attribute sind CN, UID und userPrincipalName.**Anmelde-DN** - der DN mit genügend Berechtigungen, um Benutzer im LDAP-Server suchen/lesen/suchen zu können.**Login Password** (Anmeldekennwort) - das Kennwort für das DN-Konto**LDAP-Attributzuordnung** - eine LDAP-Attributzuordnung, die mit Antworten von diesem Server verwendet wird. Weitere Informationen finden Sie unter [ASA/PIX: Zuordnen von VPN-Clients zu VPN-Gruppenrichtlinien mithilfe des LDAP-Konfigurationsbeispiels] für weitere Informationen zum Konfigurieren von LDAP-Attributzuordnungen.



6. Nachdem Sie die AAA-Servergruppe konfiguriert und einen Server hinzugefügt haben, müssen Sie Ihr Verbindungsprofil (Tunnelgruppe) so konfigurieren, dass die neue AAA-Konfiguration verwendet wird. Navigieren Sie zu Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles.
7. Wählen Sie das Verbindungsprofil (Tunnelgruppe) aus, für das Sie AAA konfigurieren möchten, und klicken Sie auf **Bearbeiten.**
8. Wählen Sie unter **Authentifizierung** die zuvor erstellte LDAP-Servergruppe aus.



Befehlszeilenschnittstelle

Führen Sie diese Schritte in der Befehlszeilenschnittstelle (CLI) aus, um die ASA für die Kommunikation mit dem LDAP-Server und die Authentifizierung von WebVPN-Clients zu konfigurieren.

```
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
```

Durchsuchen mehrerer Domänen (optional)

Optional. Die ASA unterstützt derzeit keinen LDAP-Referenzmechanismus für domänenübergreifende Suchen (Cisco Bug ID CSCsj32153). Multi-Domain-Suchen werden im Modus "Global Catalog Server" mit dem AD unterstützt. Um eine Suche in mehreren Domänen durchzuführen, richten Sie den AD-Server für den globalen Katalog-Server-Modus ein, in der Regel mit den folgenden Schlüsselparametern für den LDAP-Servereintrag in der ASA. Der Schlüssel besteht darin, ein ldap-name-Attribut zu verwenden, das in der Verzeichnisstruktur eindeutig sein muss.

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

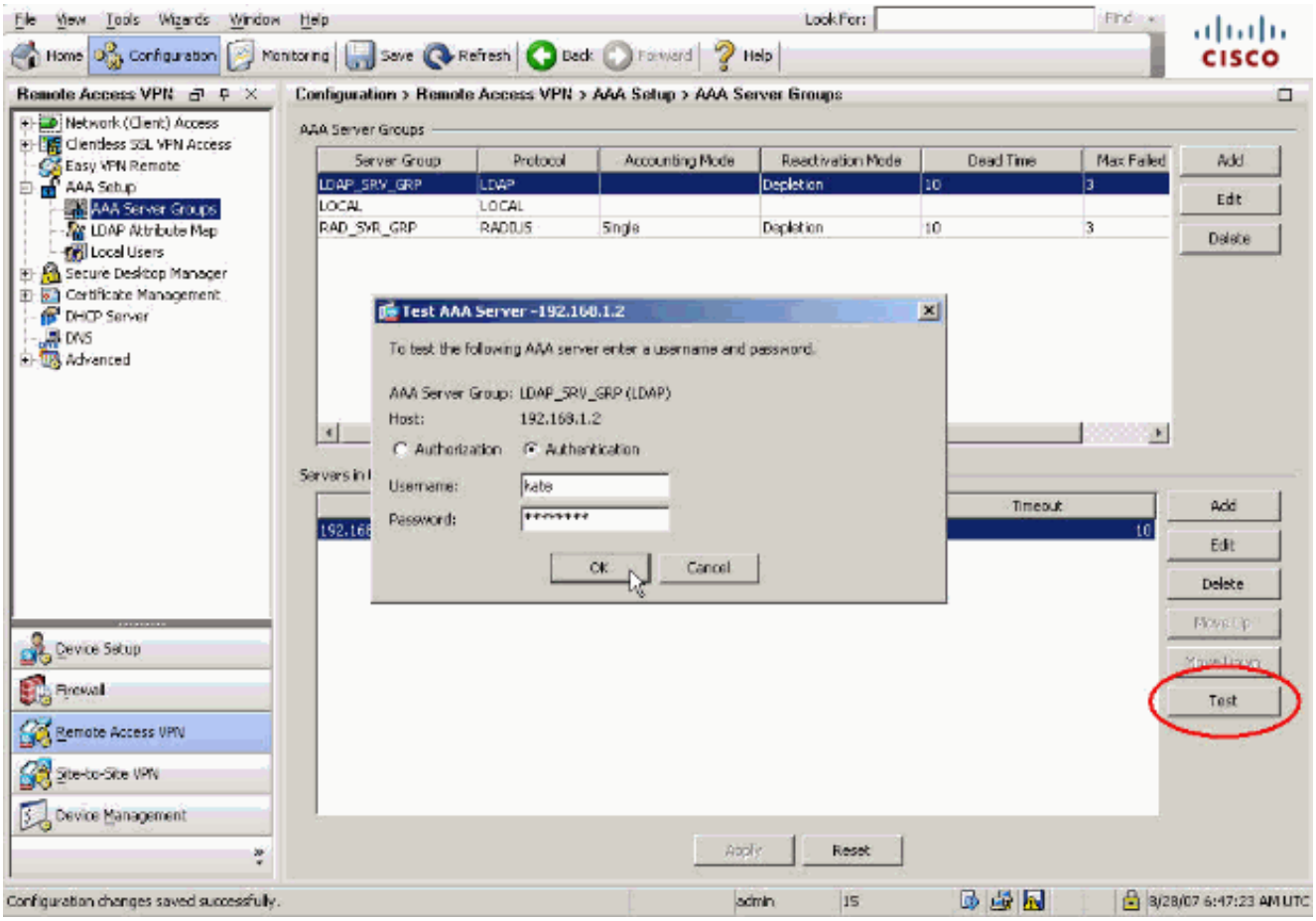
Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

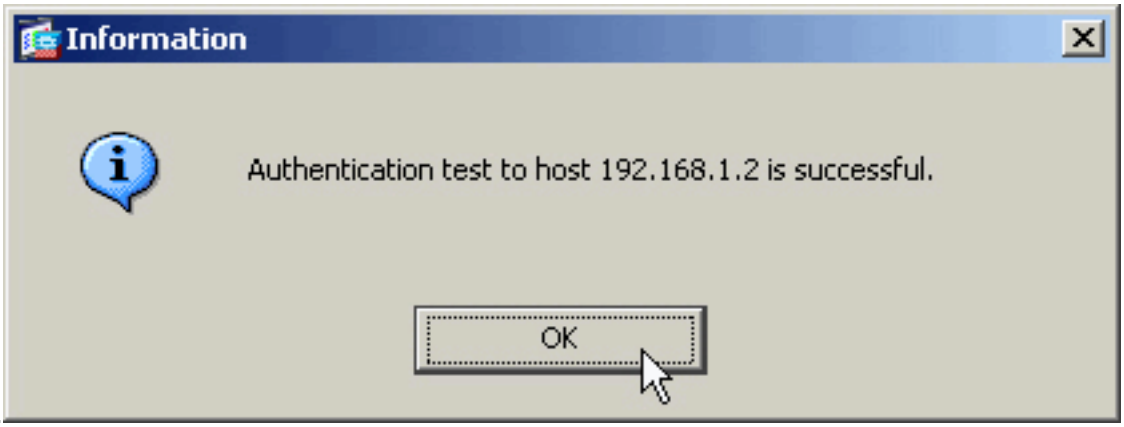
Test mit ASDM

Überprüfen Sie Ihre LDAP-Konfiguration mit der Schaltfläche **Test** im Konfigurationsbildschirm AAA-Servergruppen. Wenn Sie einen Benutzernamen und ein Kennwort eingegeben haben, können Sie über diese Schaltfläche eine Testauthentifizierungsanfrage an den LDAP-Server senden.

1. Navigieren Sie zu Configuration > Remote Access VPN > AAA Setup > AAA Server Groups.
2. Wählen Sie im oberen Teilfenster die gewünschte AAA-Servergruppe aus.
3. Wählen Sie im unteren Bereich den AAA-Server aus, den Sie testen möchten.
4. Klicken Sie auf die Schaltfläche **Test** rechts neben dem unteren Bereich.
5. Klicken Sie im sich öffnenden Fenster auf das Optionsfeld **Authentifizierung** und geben Sie die Anmeldeinformationen an, mit denen Sie testen möchten. Klicken Sie abschließend auf **OK**.



6. Wenn die ASA den LDAP-Server kontaktiert hat, wird eine Erfolgs- oder Fehlermeldung

angezeigt. 

Test mit CLI

Sie können den **Test-**Befehl in der Befehlszeile verwenden, um Ihre AAA-Konfiguration zu testen. Eine Testanforderung wird an den AAA-Server gesendet, und das Ergebnis wird in der Befehlszeile angezeigt.

```
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
```

Fehlerbehebung

Wenn Sie sich nicht sicher sind, welche DN-Zeichenfolge aktuell verwendet wird, können Sie den Befehl **dsquery** auf einem Windows Active Directory-Server über eine Eingabeaufforderung ausführen, um die entsprechende DN-Zeichenfolge eines Benutzerobjekts zu überprüfen.

```
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"
```

Der Befehl **debug ldap 255** kann bei der Behebung von Authentifizierungsproblemen in diesem Szenario helfen. Dieser Befehl aktiviert das LDAP-Debugging und ermöglicht Ihnen, den Prozess zu überwachen, den die ASA verwendet, um eine Verbindung zum LDAP-Server herzustellen. Diese Ausgaben zeigen die ASA-Verbindung zum LDAP-Server an, wie im Abschnitt Hintergrundinformationen dieses Dokuments beschrieben.

Dieses Debuggen zeigt eine erfolgreiche Authentifizierung:

```
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
```

Dieses Debuggen zeigt eine Authentifizierung an, die aufgrund eines falschen Kennworts fehlschlägt:

```
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
```

Dieses Debuggen zeigt eine Authentifizierung an, die fehlschlägt, weil der Benutzer nicht auf dem LDAP-Server gefunden werden kann:

```
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
```

Die Fehlermeldung wird angezeigt, wenn die Verbindung zwischen ASA und dem LDAP-Authentifizierungsserver nicht funktioniert:

```
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.
```

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems