ASA 8.0: Configura autenticazione LDAP per utenti WebVPN

Sommario

Introduzione

In questo documento viene illustrato come configurare Cisco Adaptive Security Appliance (ASA) in modo che utilizzi un server LDAP per l'autenticazione degli utenti di WebVPN. Il server LDAP in questo esempio è Microsoft Active Directory. Questa configurazione viene eseguita con Adaptive Security Device Manager (ASDM) 6.0(2) su un'appliance ASA con software versione 8.0(2).

Nota: in questo esempio l'autenticazione LDAP (Lightweight Directory Access Protocol) è configurata per gli utenti WebVPN, ma può essere utilizzata anche per tutti gli altri tipi di client di accesso remoto. Assegnare il gruppo di server AAA al profilo di connessione desiderato (gruppo di tunnel), come mostrato.

Prerequisiti

Ènecessaria una configurazione VPN di base. In questo esempio viene utilizzato WebVPN.

Premesse

In questo esempio, l'ASA controlla il server LDAP per verificare l'identità degli utenti che autentica. Questo processo non funziona come lo scambio RADIUS (Remote Authentication Dial-In User Service) tradizionale o TACACS+ (Terminal Access Controller Access-Control System Plus). In questa procedura viene spiegato ad alto livello come l'appliance ASA usa un server LDAP per controllare le credenziali dell'utente.

1. L'utente avvia una connessione all'appliance ASA.
2. L'appliance ASA è configurata per autenticare l'utente con il server Microsoft Active Directory (AD)/LDAP.
3. L'appliance ASA esegue il binding al server LDAP con le credenziali configurate sull'appliance ASA (in questo caso admin) e cerca il nome utente specificato. L'utente **admin** ottiene inoltre le credenziali appropriate per elencare il contenuto in Active Directory. Fare riferimento a http://support.microsoft.com/?id=320528 per ulteriori informazioni su come concedere i privilegi per le query LDAP.**Nota:** Il sito Web Microsoft all'indirizzo http://support.microsoft.com/?id=320528 è gestito da un provider di terze parti. Cisco non è responsabile del contenuto.
4. Se il nome utente viene trovato, l'ASA tenta di eseguire il binding al server LDAP con le credenziali fornite dall'utente al momento dell'accesso.
5. Se il secondo binding ha esito positivo, l'autenticazione ha esito positivo e l'appliance ASA elabora gli attributi dell'utente.**Nota:** in questo esempio gli attributi non vengono utilizzati. Per ulteriori informazioni, fare riferimento al documento ASA/PIX: Mappatura dei client VPN su Criteri di gruppo VPN tramite configurazione LDAP per visualizzare un esempio di come l'ASA può elaborare gli attributi LDAP.

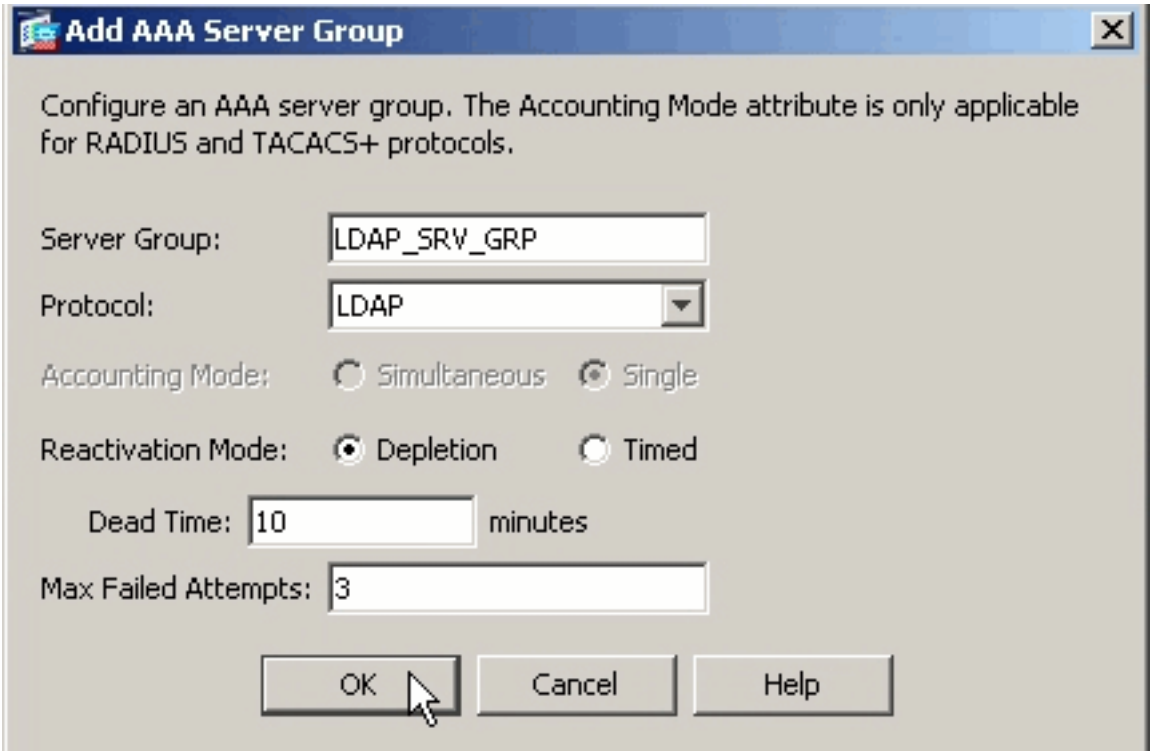
Configura autenticazione LDAP

In questa sezione vengono presentate le informazioni necessarie per configurare l'appliance ASA in modo che utilizzi un server LDAP per l'autenticazione dei client WebVPN.

ASDM

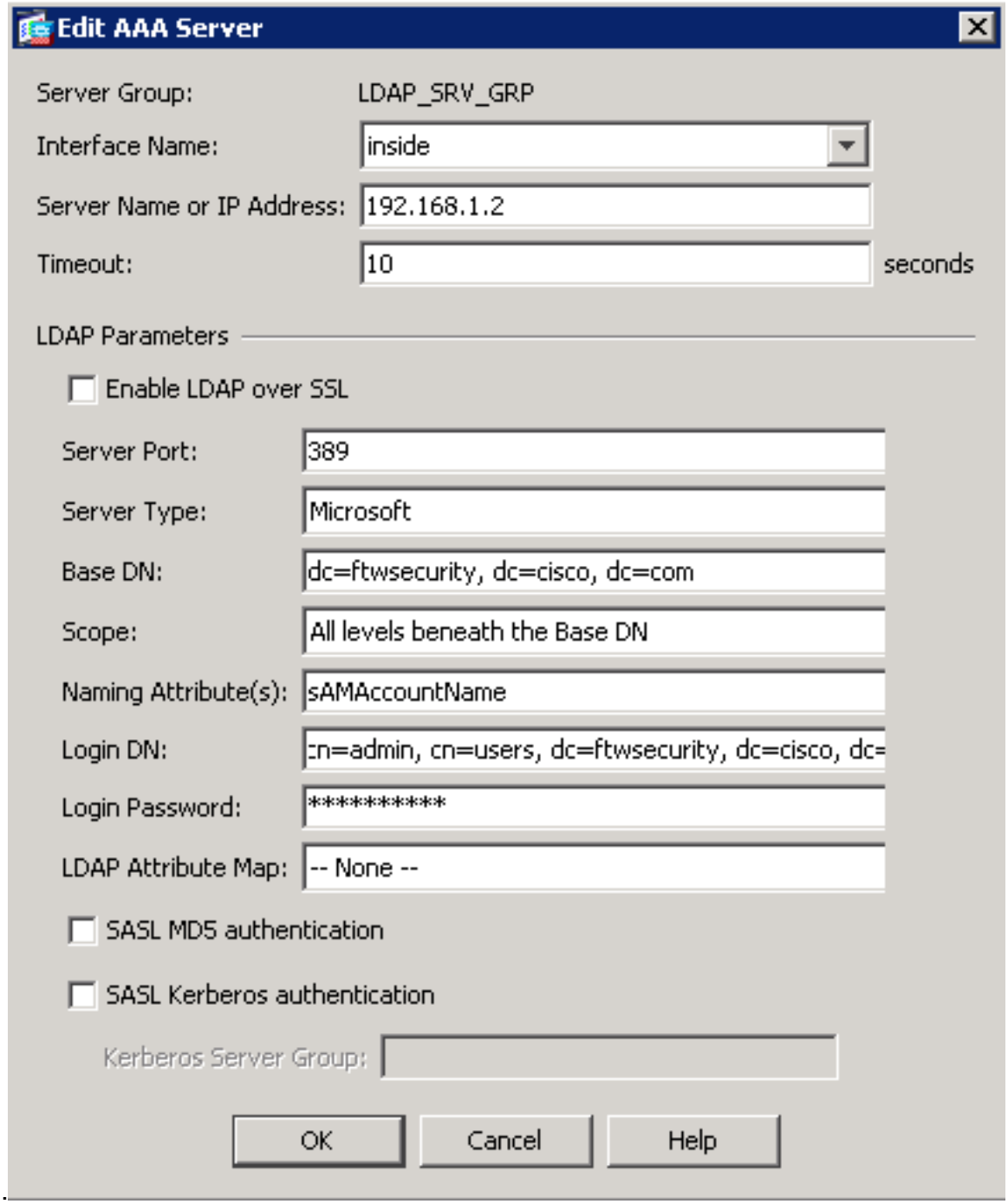
Completare la procedura descritta in ASDM per configurare l'appliance ASA in modo che comunichi con il server LDAP e autentichi i client WebVPN.

1. Selezionare Configurazione > VPN ad accesso remoto > Impostazione AAA > Gruppi di server AAA.
2. Fare clic su **Add** (Aggiungi) accanto a Gruppi di server AAA
3. Specificare un nome per il nuovo gruppo di server AAA e scegliere **LDAP** come



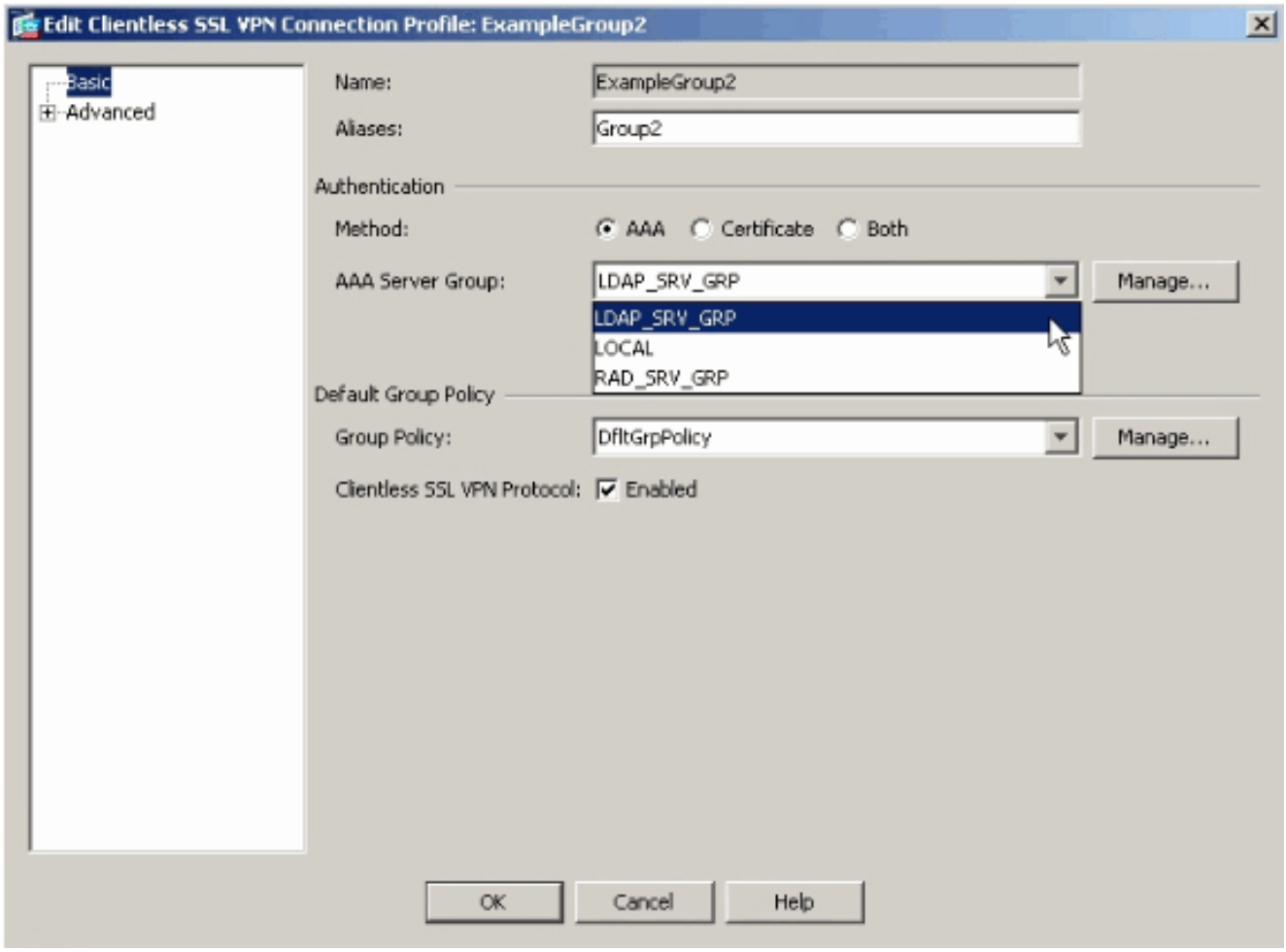
protocollo.

4. Assicurarsi che il nuovo gruppo sia selezionato nel riquadro superiore e fare clic su **Aggiungi** accanto a **Server nel** riquadro **Gruppo selezionato**.
5. Fornire le informazioni di configurazione per il server LDAP. La schermata successiva mostra un esempio di configurazione. Questa è una spiegazione di molte delle opzioni di configurazione:**Nome interfaccia**: l'interfaccia usata dall'ASA per raggiungere il server LDAP.**Nome server o indirizzo IP**: l'indirizzo usato dall'ASA per raggiungere il server LDAP.**Tipo di server**: il tipo di server LDAP, ad esempio Microsoft**DN di base**: la posizione nella gerarchia LDAP in cui il server deve iniziare la ricerca.**Ambito**: l'estensione della ricerca nella gerarchia LDAP che il server deve effettuare.**Attributo di denominazione**: l'attributo o gli attributi Nome distinto relativo che identifica in modo univoco una voce sul server LDAP. **sAMAccountName** è l'attributo predefinito in Microsoft Active Directory. Altri attributi comunemente utilizzati sono CN, UID e userPrincipalName.**DN di accesso**: il DN con privilegi sufficienti per poter eseguire ricerche, leggere e ricercare utenti nel server LDAP.**Password di login**: la password per l'account DN**Mappa attributi LDAP**: una mappa attributi LDAP da utilizzare con le risposte di questo server. Per ulteriori informazioni, fare riferimento al documento ASA/PIX: Mappatura dei client VPN a Criteri di gruppo VPN tramite configurazione LDAP Esempio per ulteriori informazioni su come configurare le mappe di attributi



LDAP.

6. Dopo aver configurato il gruppo di server AAA e avergli aggiunto un server, è necessario configurare il profilo di connessione (gruppo di tunnel) in modo che usi la nuova configurazione AAA. Selezionare Configurazione > VPN ad accesso remoto > Accesso VPN SSL senza client > Profili di connessione.
7. Scegliere il profilo di connessione (gruppo di tunnel) per cui configurare il server AAA, quindi fare clic su **Modifica**
8. In **Autenticazione** scegliere il gruppo di server LDAP creato in precedenza.



Interfaccia della riga di comando

Completare questa procedura nell'interfaccia della riga di comando (CLI) per configurare l'ASA in modo che comunichi con il server LDAP e autentichi i client WebVPN.

```
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
```

Eseguire ricerche su più domini (facoltativo)

Facoltativo. Al momento, l'ASA non supporta il meccanismo di riferimento LDAP per le ricerche su più domini (ID bug Cisco CSCsj32153). Le ricerche multidominio sono supportate con Active Directory in modalità server di catalogo globale. Per eseguire ricerche su più domini, configurare il server AD per la modalità server di catalogo globale, generalmente con questi parametri chiave per la voce server LDAP nell'appliance ASA. La chiave consiste nell'utilizzare un attributo ldap-name-attribute che deve essere univoco nella struttura di directory.

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

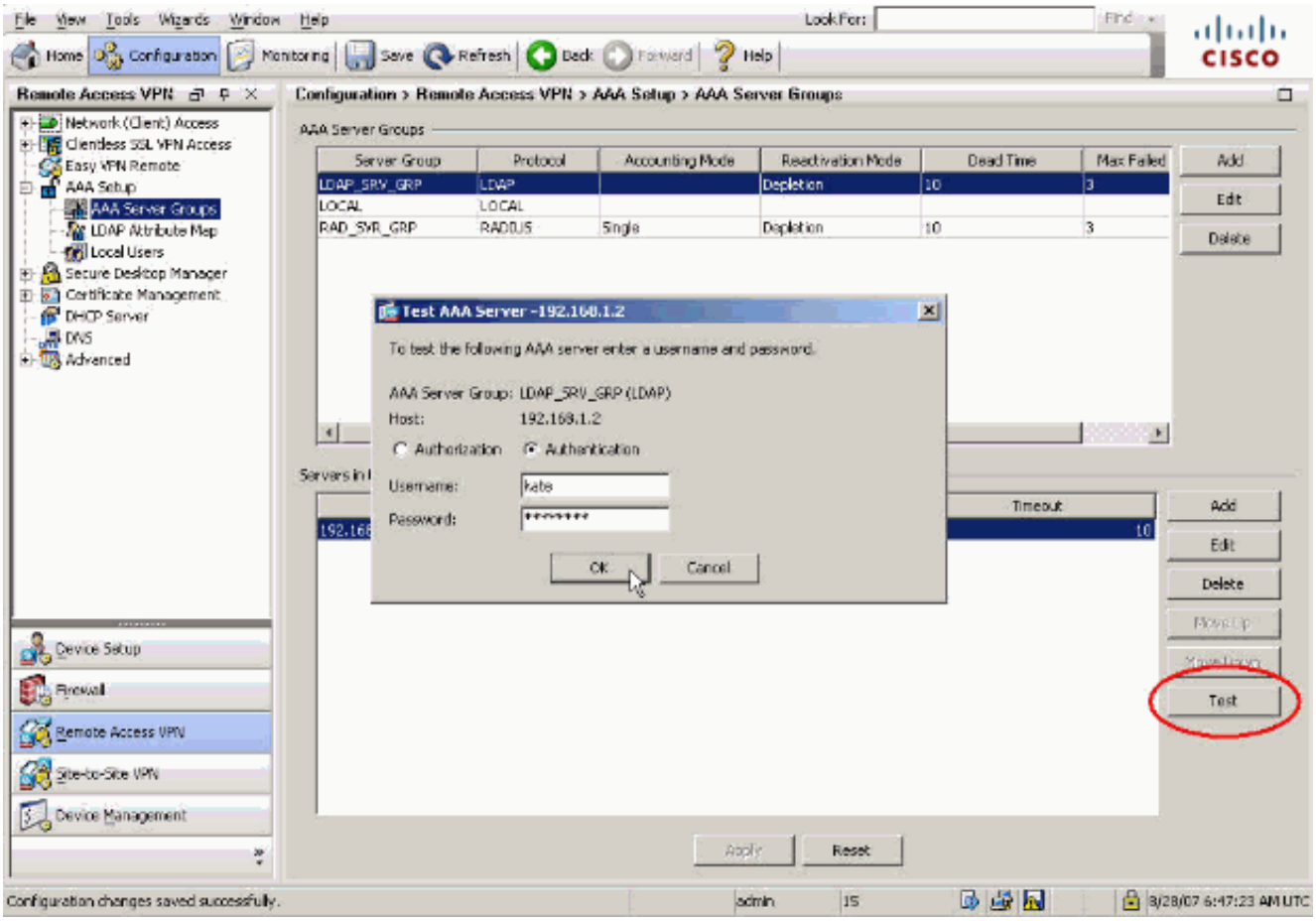
Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Test con ASDM

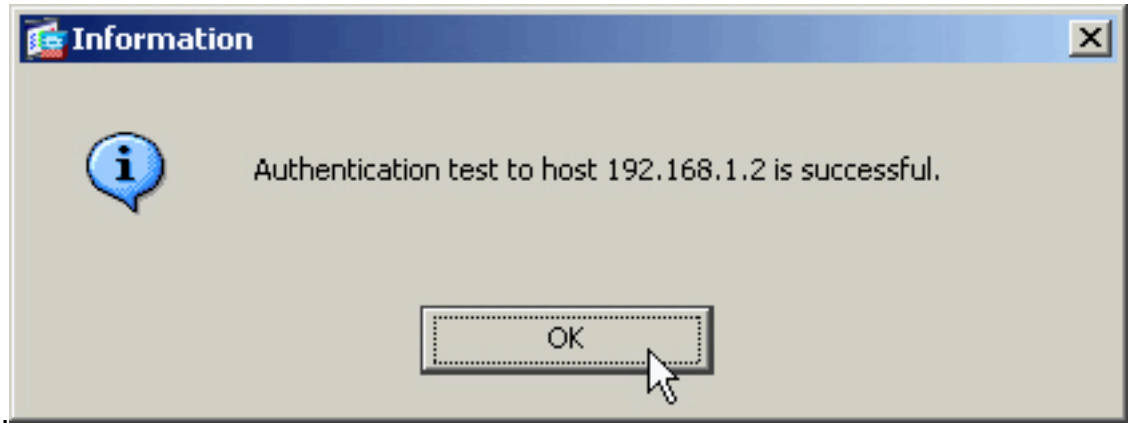
Verificare la configurazione LDAP con il pulsante **Test** nella schermata di configurazione dei gruppi di server AAA. Dopo aver fornito un nome utente e una password, questo pulsante consente di inviare una richiesta di autenticazione di prova al server LDAP.

1. Selezionare Configurazione > VPN ad accesso remoto > Impostazione AAA > Gruppi di server AAA.
2. Selezionare il gruppo di server AAA desiderato nel riquadro superiore.
3. Selezionare il server AAA che si desidera verificare nel riquadro inferiore.
4. Fare clic sul pulsante **Test** a destra del riquadro inferiore.
5. Nella finestra visualizzata fare clic sul pulsante di scelta **Autenticazione** e specificare le credenziali che si desidera verificare. Al termine, fare clic su **OK**.



6. Dopo che l'ASA ha contattato il server LDAP, viene visualizzato un messaggio di operazione riuscita o di

errore.



Test con CLI

Per verificare la configurazione del server AAA, è possibile usare il comando **test** sulla riga di comando. Una richiesta di test viene inviata al server AAA e il risultato viene visualizzato sulla riga di comando.

```
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
```

Risoluzione dei problemi

Se non si è certi della stringa DN corrente da utilizzare, è possibile eseguire il comando **dsquery** su un server Windows Active Directory da un prompt dei comandi per verificare la stringa DN appropriata di un oggetto utente.

```
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"
```

Il comando **debug ldap 255** può essere utile per risolvere i problemi di autenticazione in questo scenario. Questo comando abilita il debug LDAP e consente di controllare il processo utilizzato dall'ASA per connettersi al server LDAP. Gli output mostrati di seguito mostrano la connessione dell'ASA al server LDAP come indicato nella sezione Informazioni di base di questo documento.

Questo debug indica che l'autenticazione è stata completata:

```
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
```

Questo debug visualizza un'autenticazione non riuscita a causa di una password errata:

```
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
```

Questo debug visualizza un'autenticazione non riuscita perché l'utente non è stato trovato sul server LDAP:

```
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
```

I debug mostrano questo messaggio di errore quando la connettività tra l'ASA e il server di autenticazione LDAP non funziona:

```
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.
```

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems