ASA 8.0:為WebVPN使用者配置LDAP身份驗證

目錄

簡介

本文檔演示如何配置思科自適應安全裝置(ASA)以使用LDAP伺服器進行WebVPN使用者身份驗證。本示例中的LDAP伺服器是Microsoft Active Directory。此配置通過自適應安全裝置管理器(ASDM)6.0(2)在運行軟體版本8.0(2)的ASA上執行。

注意：在此示例中，為WebVPN使用者配置了輕量級目錄訪問協定(LDAP)身份驗證，但是此配置也可用於所有其他型別的遠端訪問客戶端。只需將AAA伺服器組分配給所需的連線配置檔案（隧道組），如下所示。

必要條件

需要基本VPN配置。本示例使用WebVPN。

背景資訊

在此示例中，ASA會對LDAP伺服器進行檢查，以驗證其驗證的使用者身份。此程式不像傳統遠端驗證撥入使用者服務(RADIUS)或終端存取控制器存取控制系統Plus(TACACS+)交換那樣運作。這些步驟從較高層面解釋了ASA如何使用LDAP伺服器檢查使用者憑證。

1. 使用者啟動與ASA的連線。
2. ASA配置為使用Microsoft Active Directory(AD)/LDAP伺服器對該使用者進行身份驗證。
3. ASA使用在ASA上配置的憑據（本例中為admin）繫結到LDAP伺服器，並查詢提供的使用者名稱。**admin**使用者還獲取相應的憑據以列出Active Directory中的內容。有關如何授予LDAP查詢許可權的詳細資訊，請參閱http://support.microsoft.com/?id=320528 。**附註**

：Microsoft網站http://support.microsoft.com/?id=320528 由第三方提供商管理。思科對其內容不負責。
4. 如果找到使用者名稱，ASA將嘗試使用使用者在登入時提供的憑據繫結到LDAP伺服器。
5. 如果第二次繫結成功，則身份驗證成功，ASA處理使用者的屬性。**注意**：在本示例中，屬性不用於任何內容。請參閱ASA/PIX:通過LDAP將VPN客戶端對映到VPN組策略配置示例，以檢視ASA如何處理LDAP屬性的示例。

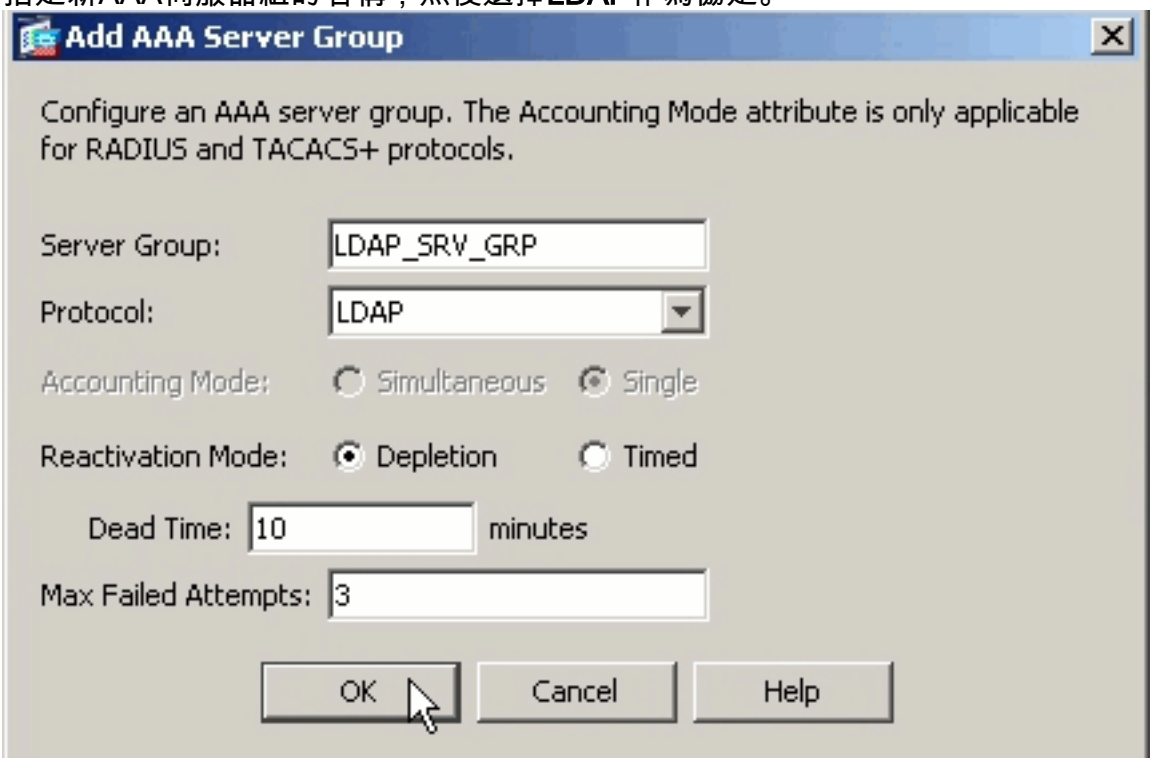
配置LDAP身份驗證

本節提供配置ASA以使用LDAP伺服器進行WebVPN客戶端身份驗證的資訊。

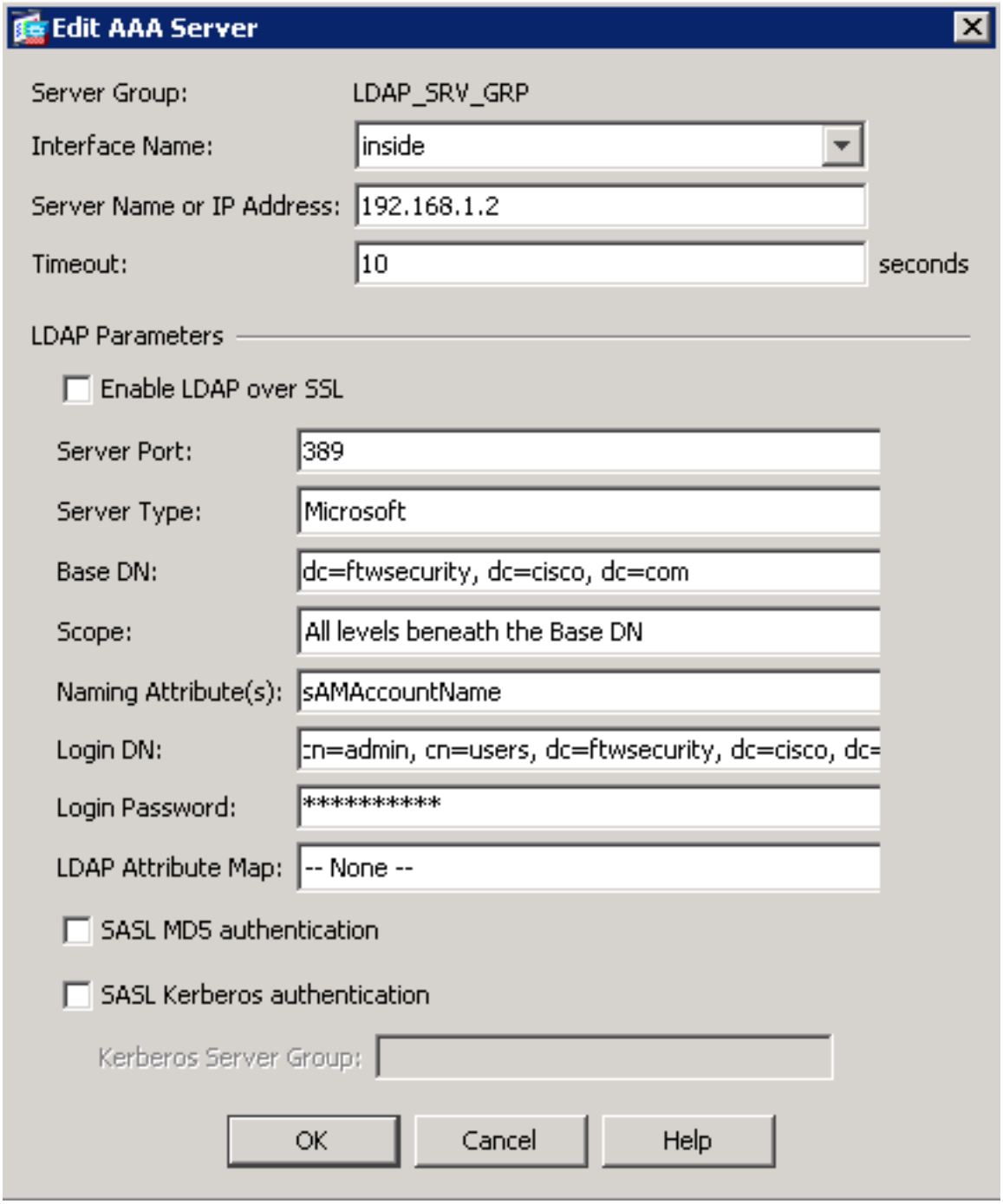
ASDM

在ASDM中完成以下步驟，以配置ASA與LDAP伺服器通訊並驗證WebVPN客戶端。

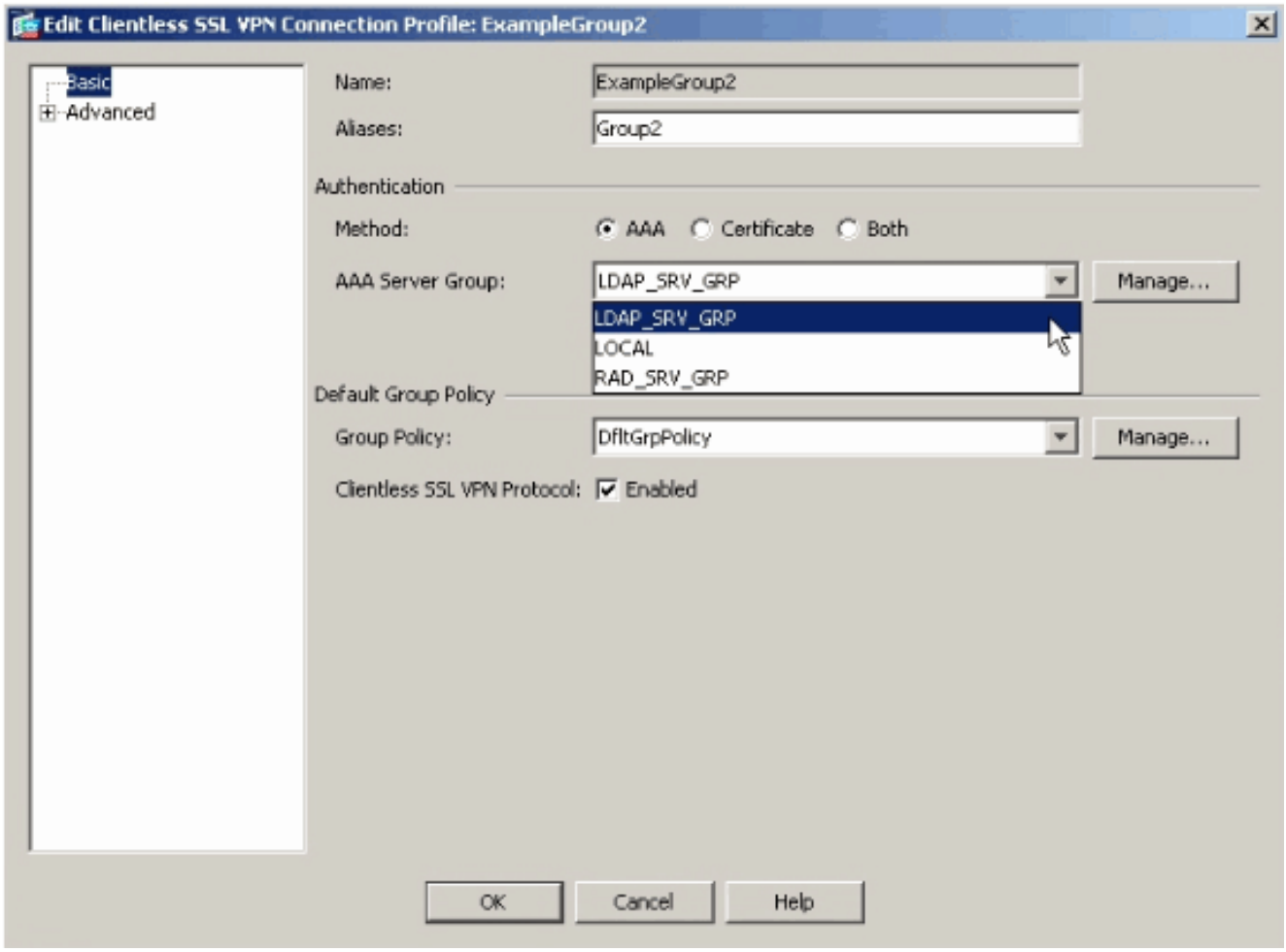
1. 導航到Configuration > Remote Access VPN > AAA Setup > AAA Server Groups。
2. 點選AAA Server Groups旁邊的**Add**
3. 指定新AAA伺服器組的名稱，然後選擇**LDAP**作為協定。



4. 確保在頂部窗格中選擇了您的新組，然後按一下**Selected Group**窗格中**Servers**旁邊的**Add**。
5. 提供LDAP伺服器的配置資訊。後續螢幕截圖說明了示例配置。以下是許多組態選項的說明：**Interface Name** - ASA用於訪問LDAP伺服器的介面**伺服器名稱或IP**地址 — ASA用於訪問LDAP伺服器的地址**伺服器**型別 — LDAP伺服器的型別，例如Microsoft**基本DN** — 伺服器必須開始搜尋的LDAP層次結構中的位置**範圍** — 伺服器必須在LDAP層次結構中進行的搜尋範圍**命名屬**性 — 唯一標識LDAP伺服器上條目的相對可分辨名稱屬性（或屬性）。**sAMAccountName**是Microsoft Active Directory中的預設屬性。其他常用屬性包括CN、UID和userPrincipalName。**Login DN** — 具有足夠許可權以便在LDAP伺服器中搜尋/讀取/查詢使用者的DN**Login Password** - DN帳戶的密碼**LDAP屬性對映** — 用於此伺服器的響應的LDAP屬性對映。請參閱ASA/PIX:通過LDAP將VPN客戶端對映到VPN組策略配置示例，以瞭解有關如何配置LDAP屬性對映的詳細資訊。



6. 配置AAA伺服器組並向其中新增伺服器後，必須配置連線配置檔案（隧道組）以使用新的AAA配置。導航至Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles。
7. 選擇要為其配置AAA的連線配置檔案（隧道組），然後按一下**Edit**
8. 在**Authentication**下，選擇之前建立的LDAP伺服器組。



命令列介面

在命令列介面(CLI)中完成以下步驟，以配置ASA與LDAP伺服器通訊並驗證WebVPN客戶端。

```
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
```

執行多域搜尋（可選）

可選。ASA當前不支援多域搜尋的LDAP引用機制(思科錯誤ID CSCsj32153)。 AD在全域性目錄伺服器模式下支援多域搜尋。為了執行多域搜尋，請將AD伺服器設定為全域性目錄伺服器模式，通常使用ASA中LDAP伺服器條目的這些關鍵引數。關鍵是使用目錄樹中必須唯一的ldap-name-attribute。

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

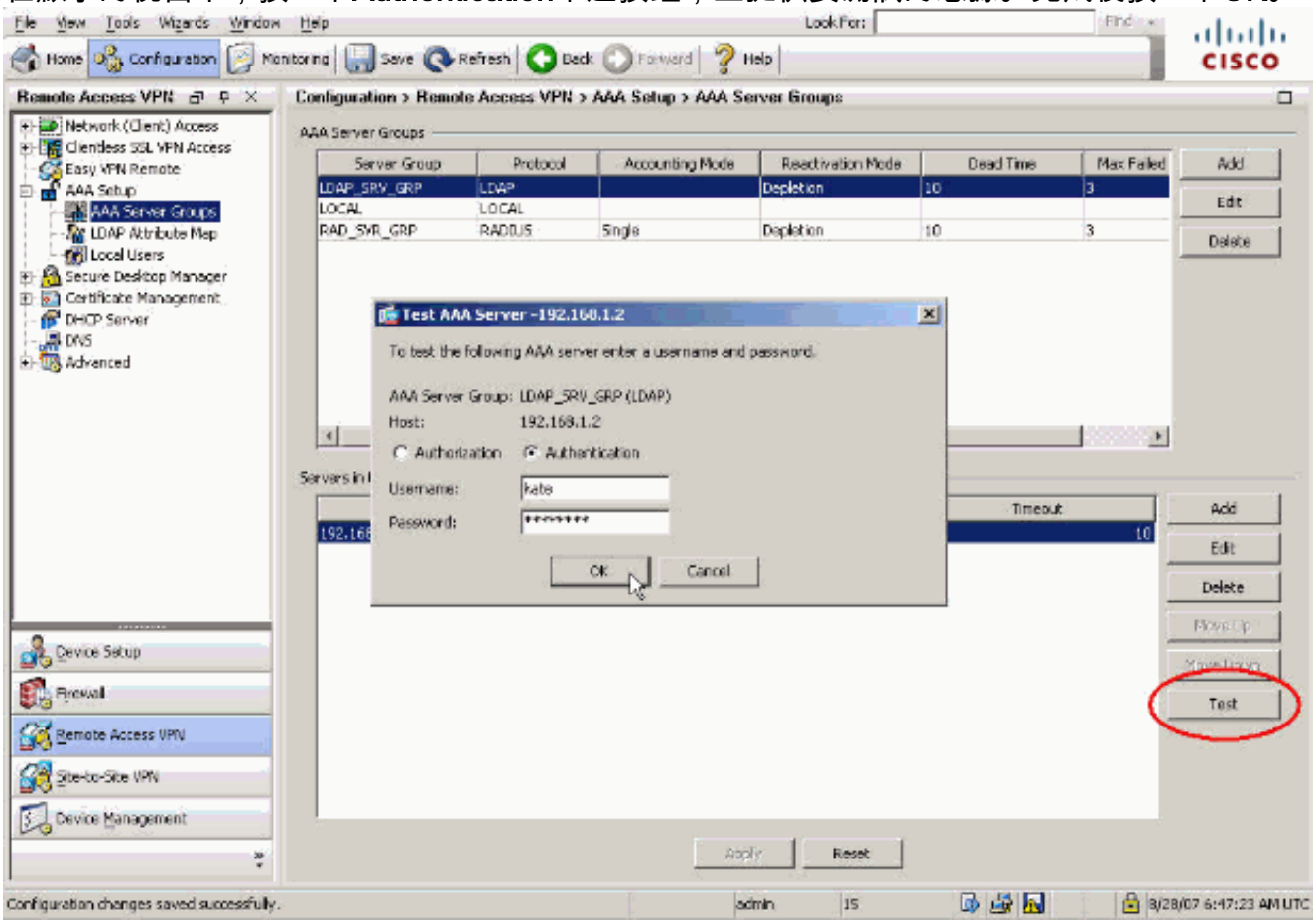
驗證

使用本節內容，確認您的組態是否正常運作。

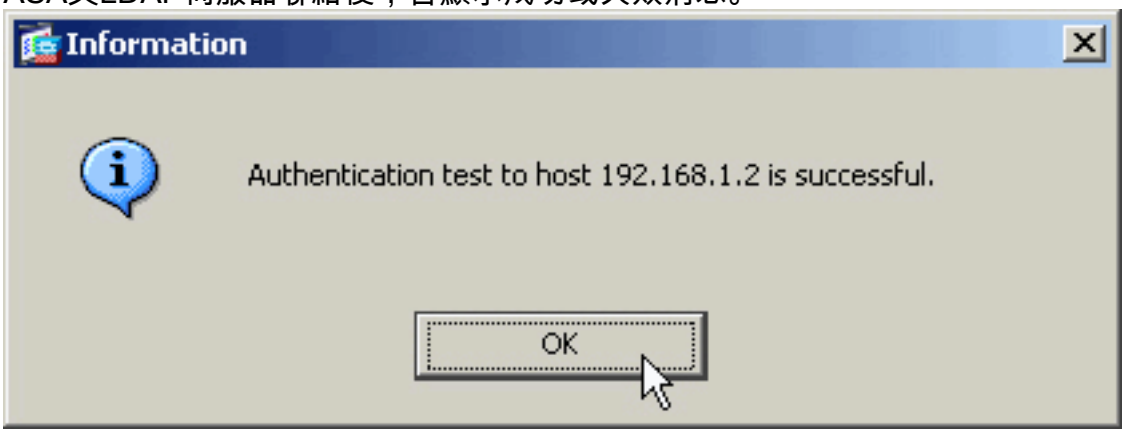
使用ASDM測試

使用AAA Server Groups configuration螢幕上的**Test**按鈕驗證LDAP配置。提供使用者名稱和密碼後，此按鈕允許您向LDAP伺服器傳送測試身份驗證請求。

1. 導航到Configuration > Remote Access VPN > AAA Setup > AAA Server Groups。
2. 在頂部窗格中選擇所需的AAA伺服器組。
3. 在下窗格中選擇要測試的AAA伺服器。
4. 按一下下方窗格右側的**Test**按鈕。
5. 在顯示的視窗中，按一下**Authentication**單選按鈕，並提供要測試的憑據。完成後按一下**OK**。



6. ASA與LDAP伺服器聯絡後，會顯示成功或失敗消息。



使用CLI測試

您可以在命令列中使用**test**命令來測試AAA設定。向AAA伺服器傳送測試請求，並在命令列中顯示結果。

```
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
```

疑難排解

如果不確定要使用的當前DN字串，則可以通過命令提示符在Windows Active Directory伺服器上發出**dsquery**命令，以驗證使用者對象的適當DN字串。

```
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命令可幫助解決此場景中的身份驗證問題。此命令啟用LDAP調試，並允許您監視ASA用於連線到LDAP伺服器的進程。此輸出顯示了本文檔的背景資訊部分中概述的ASA連線到LDAP伺服器。

此調試顯示成功的身份驗證：

```
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
```

此調試顯示由於密碼錯誤而失敗的身份驗證：

```
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
```

此調試顯示由於在LDAP伺服器上找不到使用者而失敗的身份驗證：

```
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
```

當ASA和LDAP身份驗證伺服器之間的連線不起作用時，調試將顯示以下錯誤消息：

```
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.
```

相關資訊

- 技術支援與文件 - Cisco Systems