Microsoft Windows 2012和OpenSSL下帶OCSP驗證的ASA遠端訪問VPN

目錄

簡介

本文檔介紹如何在Cisco Adaptive Security Appliance(ASA)上對VPN使用者提供的證書使用線上證書狀態協定(OCSP)驗證。提供了兩個OCSP伺服器（Microsoft Windows Certificate Authority [CA]和OpenSSL）的配置示例。「驗證」部分描述資料包級別的詳細流程，「故障排除」部分重點介紹典型錯誤和問題。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco自適應安全裝置命令列介面(CLI)配置和安全套接字層(SSL)VPN配置
- X.509憑證
- Microsoft Windows Server
- Linux/OpenSSL

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Adaptive Security Appliance軟體8.4版及更高版本
- 搭載Cisco AnyConnect安全行動化使用者端的Microsoft Windows 7，版本3.1
- Microsoft Server 2012 R2
- 使用OpenSSL 1.0.0j或更高版本的Linux

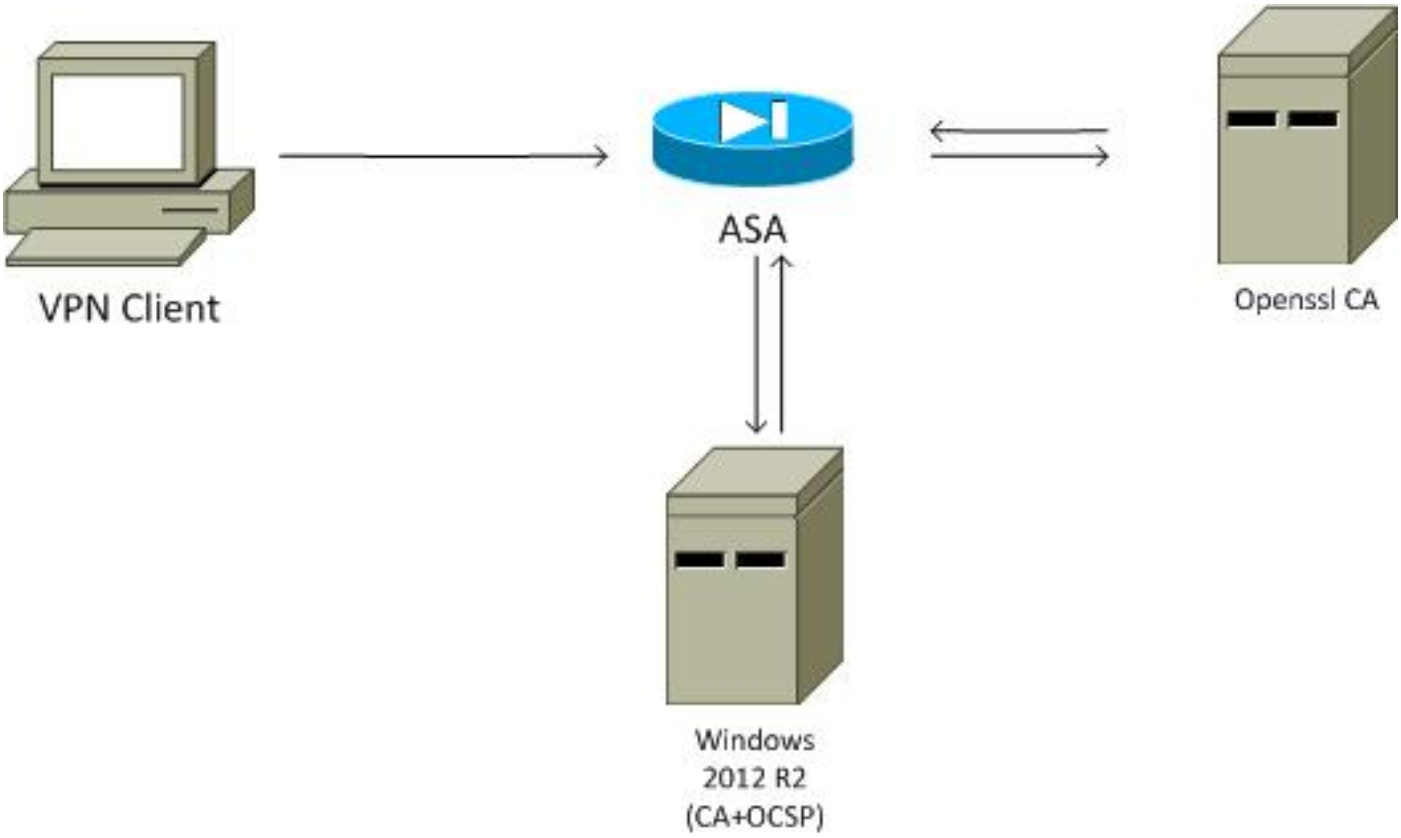
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

> **註**：使用命令查詢工具(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

客戶端使用遠端訪問VPN。此訪問可以是Cisco VPN Client(IPSec)、Cisco AnyConnect Secure Mobility(SSL/Internet Key Exchange Version 2 [IKEv2])或WebVPN（門戶）。為了登入，客戶端提供正確的證書以及在ASA本地配置的使用者名稱/密碼。客戶端證書通過OCSP伺服器進行驗證。



帶OCSP的ASA遠端訪問

ASA配置為SSL訪問。使用者端正在使用AnyConnect進行登入。ASA使用簡單證書註冊協定(SCEP)來請求證書：

```
crypto ca trustpoint WIN2012
 revocation-check ocsp
 enrollment url http://10.147.25.80:80/certsrv/mscep/mscep.dll

crypto ca certificate map MAP 10
 subject-name co administrator
```

建立證書對映以標識其主題名稱包含單詞administrator（不區分大小寫）的所有使用者。這些使用者已繫結到名為RA:

```
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 certificate-group-map MAP 10 RA
```

VPN配置需要成功授權（即經過驗證的證書）。它還要求本地定義的使用者名稱（身份驗證aaa）具有正確的憑據：

```
username cisco password xxxxxxx
ip local pool POOL 192.168.11.100-192.168.11.105 mask 255.255.255.0

aaa authentication LOCAL
aaa authorization LOCAL
```

```
group-policy MY internal
group-policy MY attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 address-pool POOL
 default-group-policy MY
 authorization-required
tunnel-group RA webvpn-attributes
 authentication aaa certificate
 group-alias RA enable
```

Microsoft Windows 2012 CA

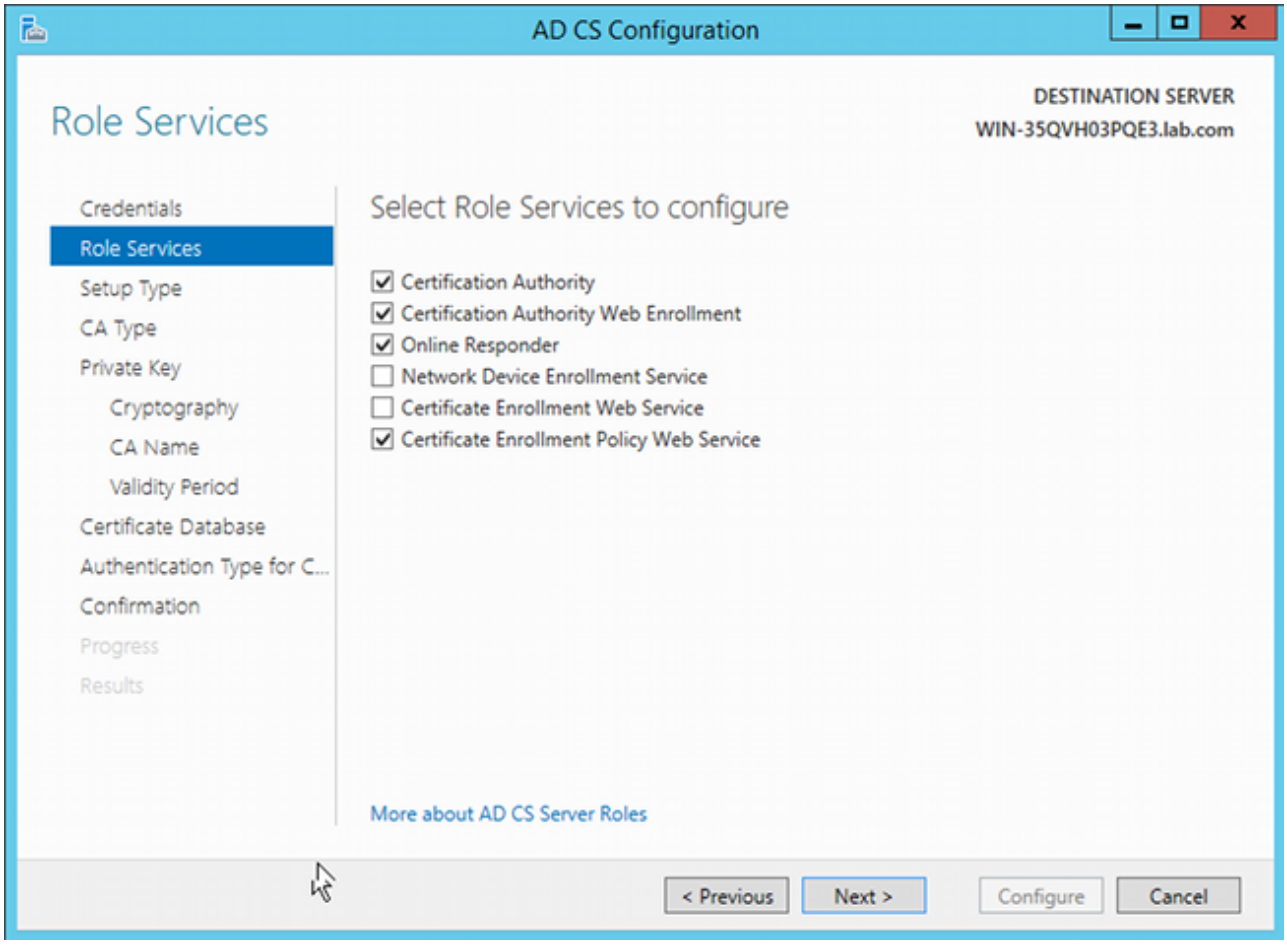
> **注意**：有關通過CLI配置ASA的詳細資訊，請參閱Cisco ASA 5500系列使用CLI的配置指南8.4和8.6：配置外部伺服器以進行安全裝置使用者授權。

服務安裝

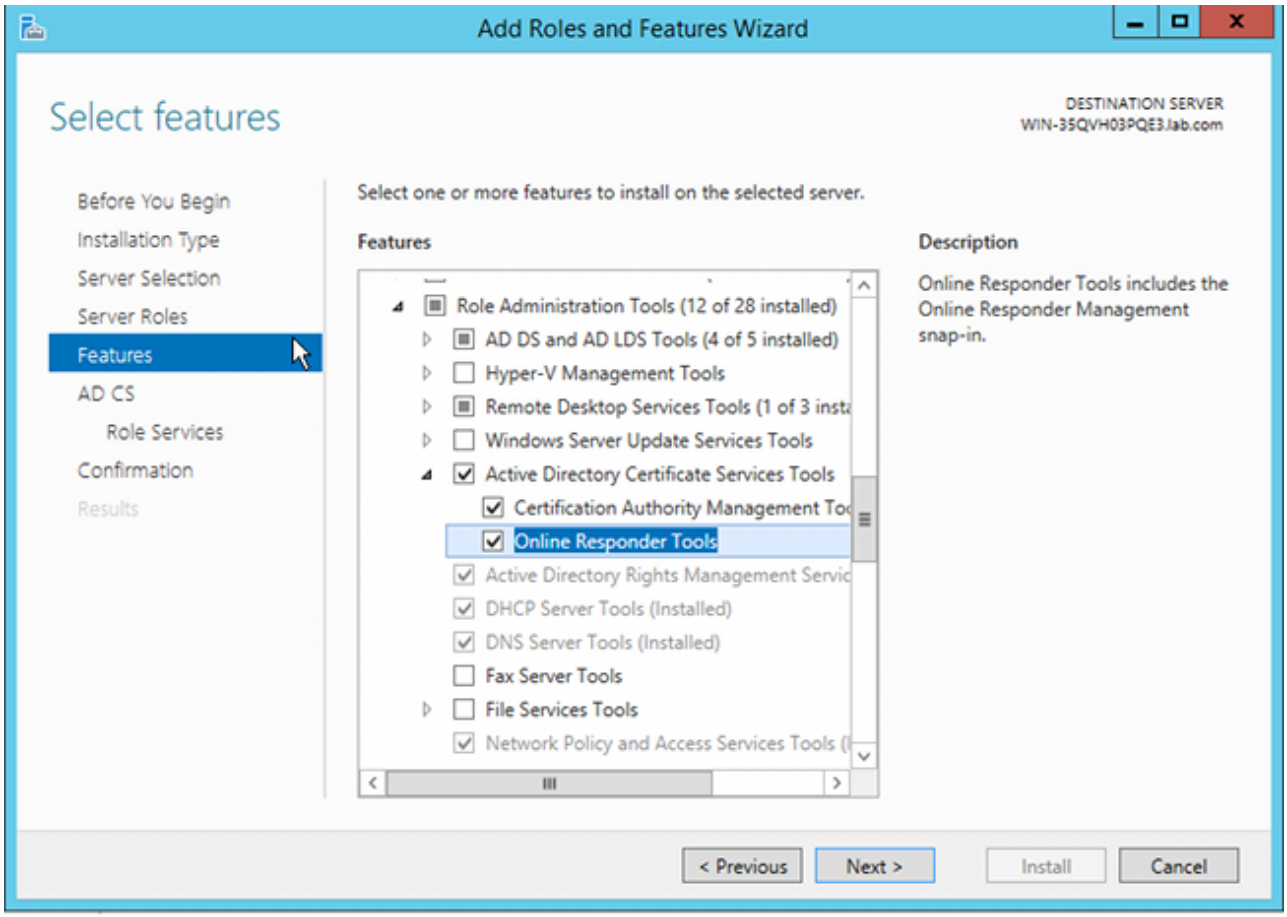
以下過程介紹了如何為Microsoft伺服器配置角色服務：

1. 導覽至**Server Manager > Manage > Add Roles and Features**。Microsoft伺服器需要以下角色服務：

   證書頒發機構客戶端使用的證書頒發機構Web註冊線上響應程式，OCSP需要該程式網路裝置註冊服務，包含ASA使用的SCEP應用程式 如果需要，可以新增帶策略的Web服務。



2.
3.
4. 新增功能時，請確保包含聯機響應程式工具，因為它包含稍後使用的OCSP管理單元：



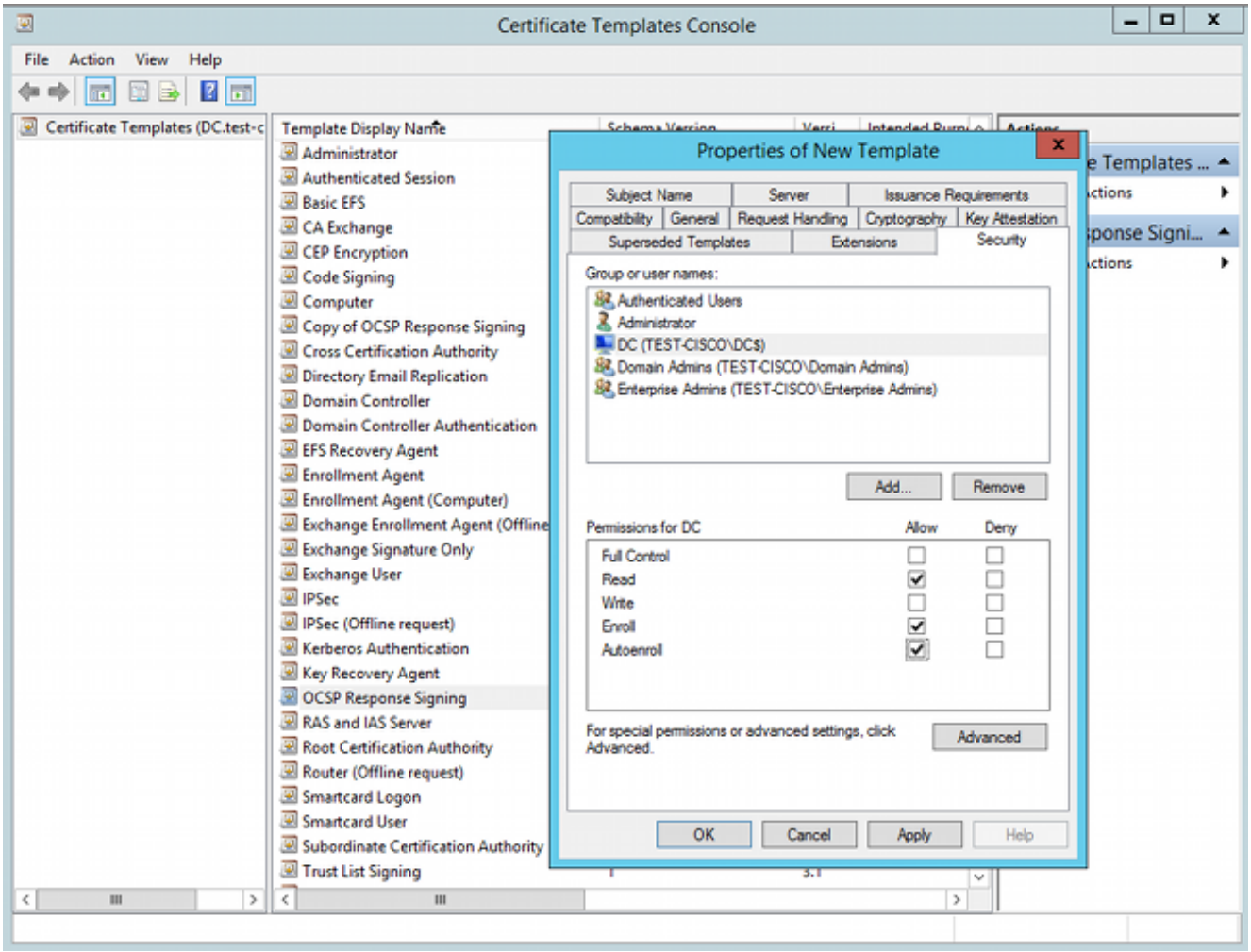
OCSP的CA配置模板

OCSP服務使用證書對OCSP響應進行簽名。必須在Microsoft伺服器上生成特殊證書，並且必須包括：

- 擴展金鑰用法= OCSP簽名
- OCSP無吊銷檢查

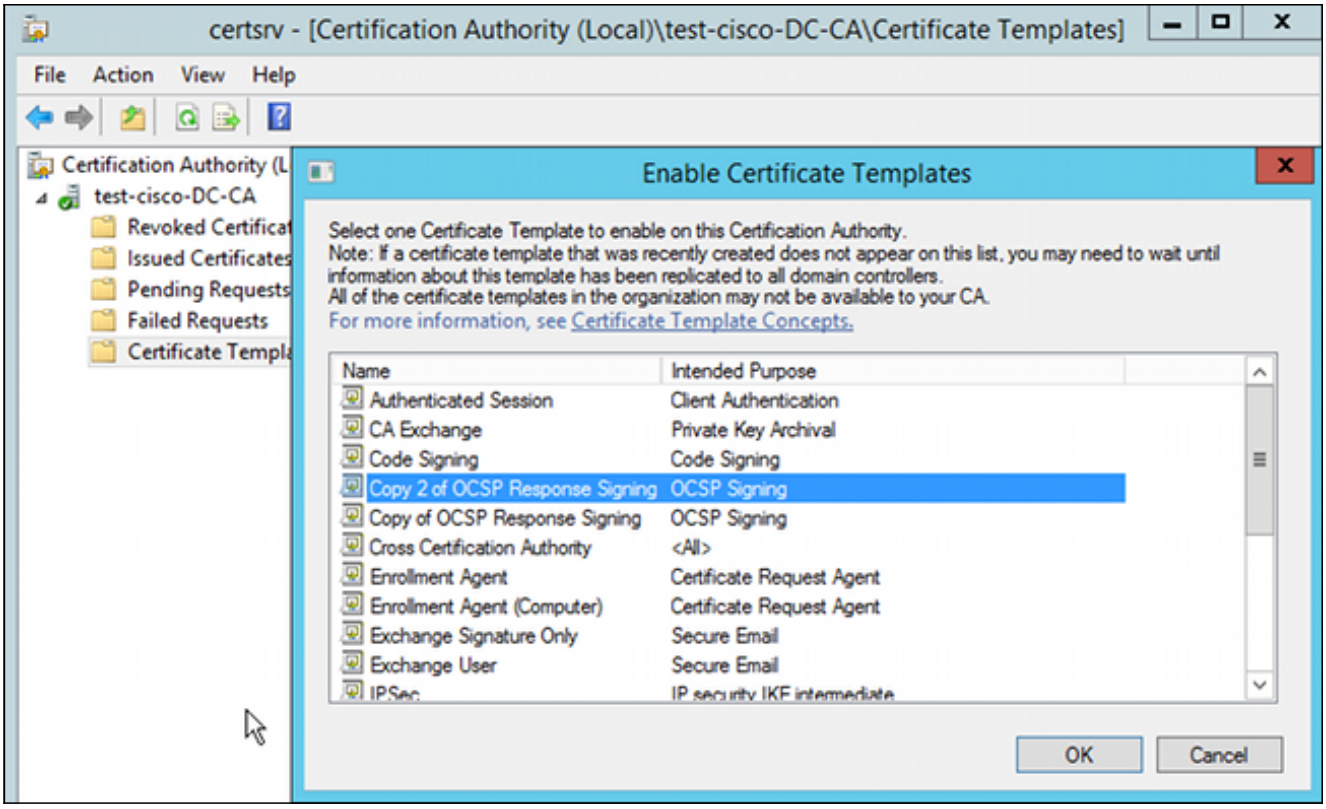
需要此證書以防止OCSP驗證循環。ASA不使用OCSP服務嘗試檢查OCSP服務提供的證書。

1. 為CA上的證書新增模板。導航到**CA > Certificate Template > Manage**，選擇**OCSP Response Signing**，然後複製模板。檢視新建立的模板的屬性，然後按一下**Security**頁籤。許可權描述允許哪個實體請求使用該模板的證書，因此需要正確的許可權。在本示例中，實體是在同一主機上運行的OCSP服務(TEST-CISCO\DC)，並且OCSP服務需要自動註冊許可權：



模板的所有其他設定都可以設定為預設值。

2. 啟用模板。導覽至**CA > Certificate Template > New > Certificate Template to Issue**，然後選擇重複模板：

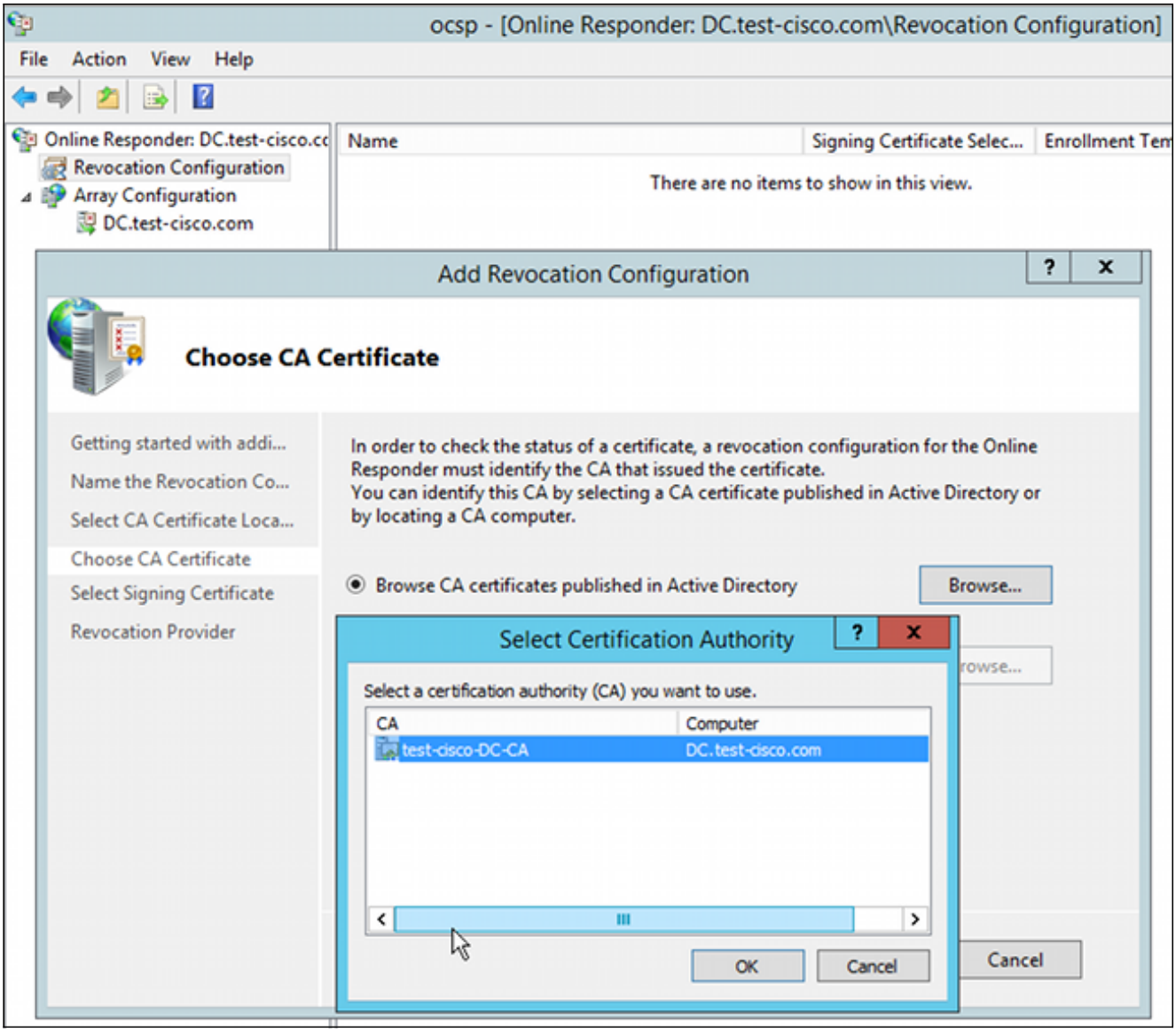


OCSP服務證書

以下過程介紹了如何使用聯機配置管理來配置OCSP:

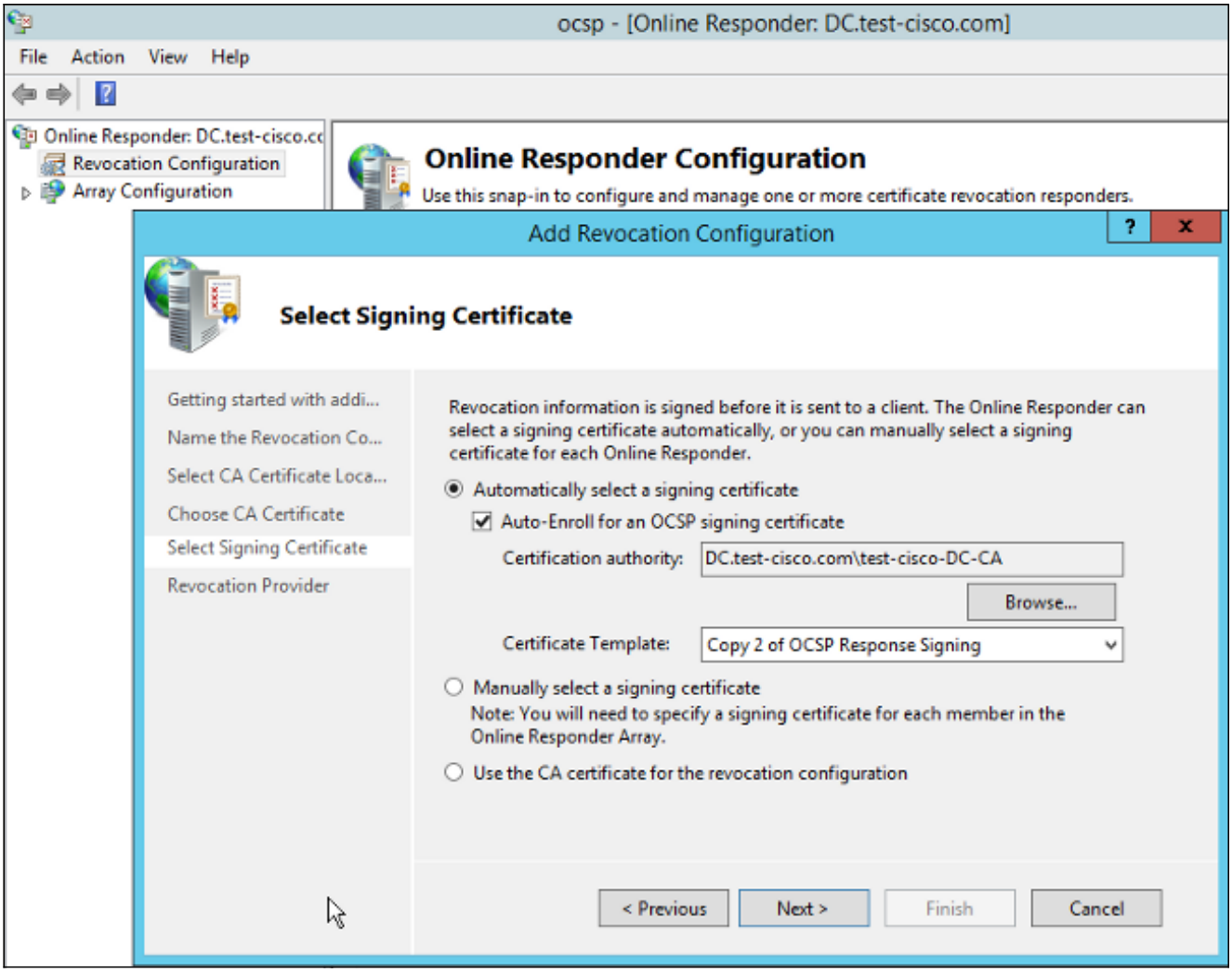
1. 導覽至**Server Manager > Tools**。

2. 導覽至**吊銷配置 > 新增吊銷配置**，以便新增新配置：

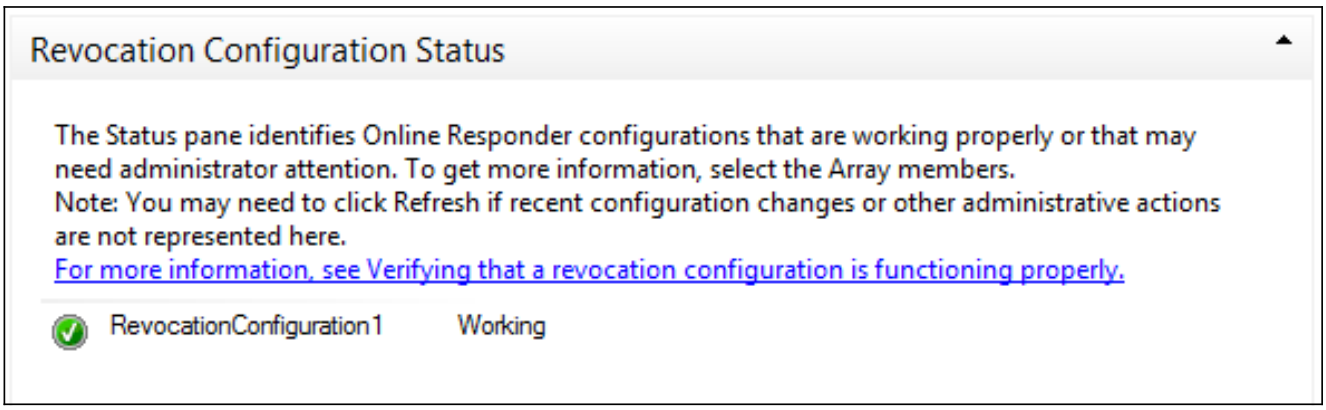


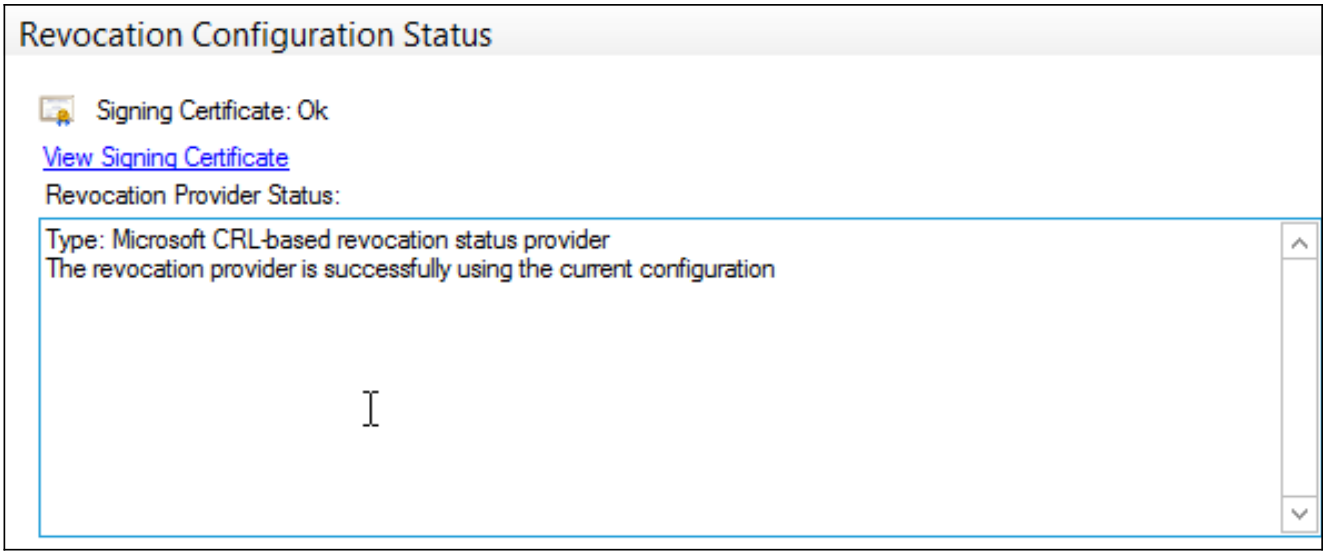
OCSP可以使用相同的企業CA。生成OCSP服務的證書。

3. 使用選定的企業CA，並選擇之前建立的模板。自動註冊證書：

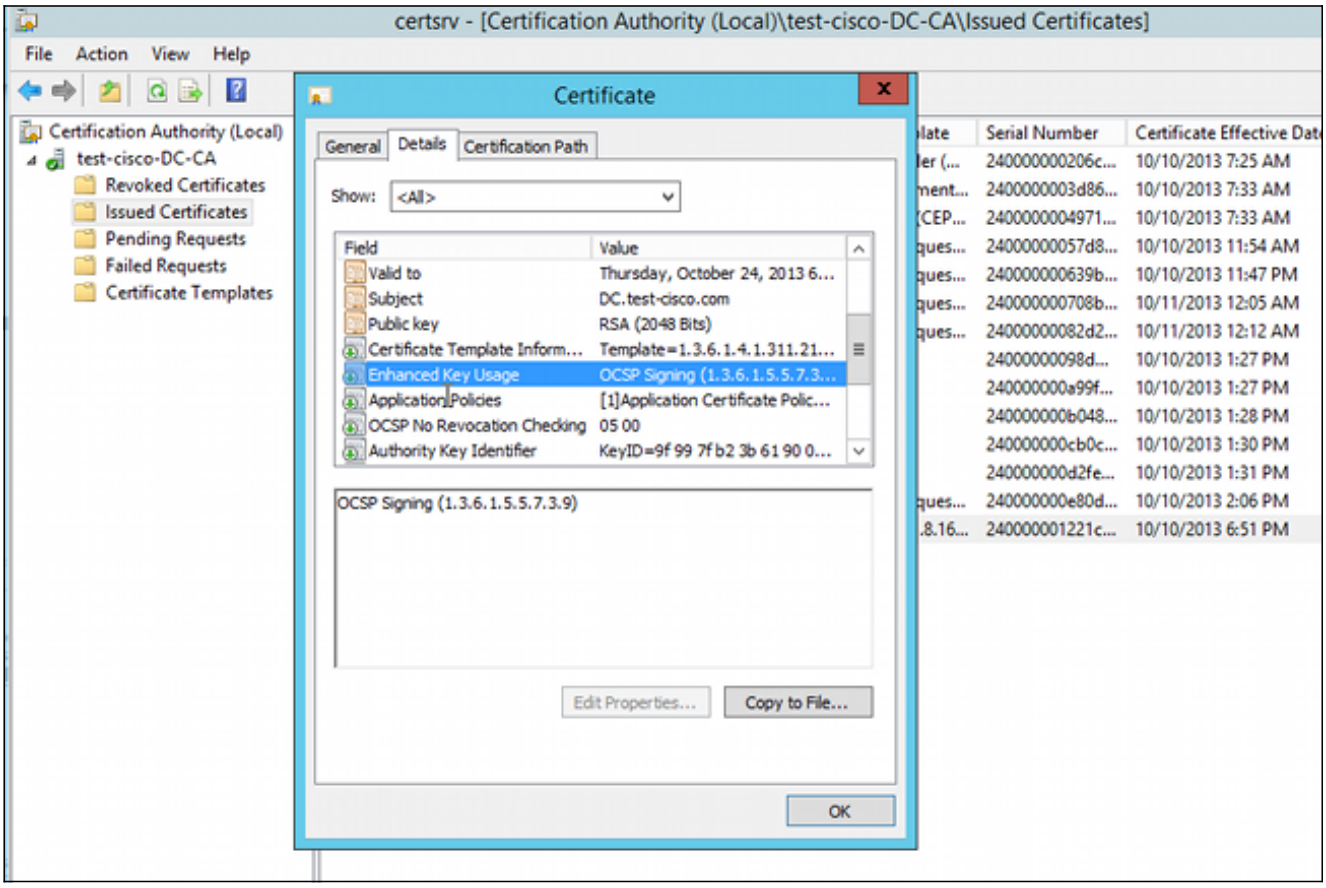


4. 確認憑證已註冊，且其狀態為工作/正常：





5. 導覽至**CA > Issued Certificates**，以驗證憑證詳細資訊：

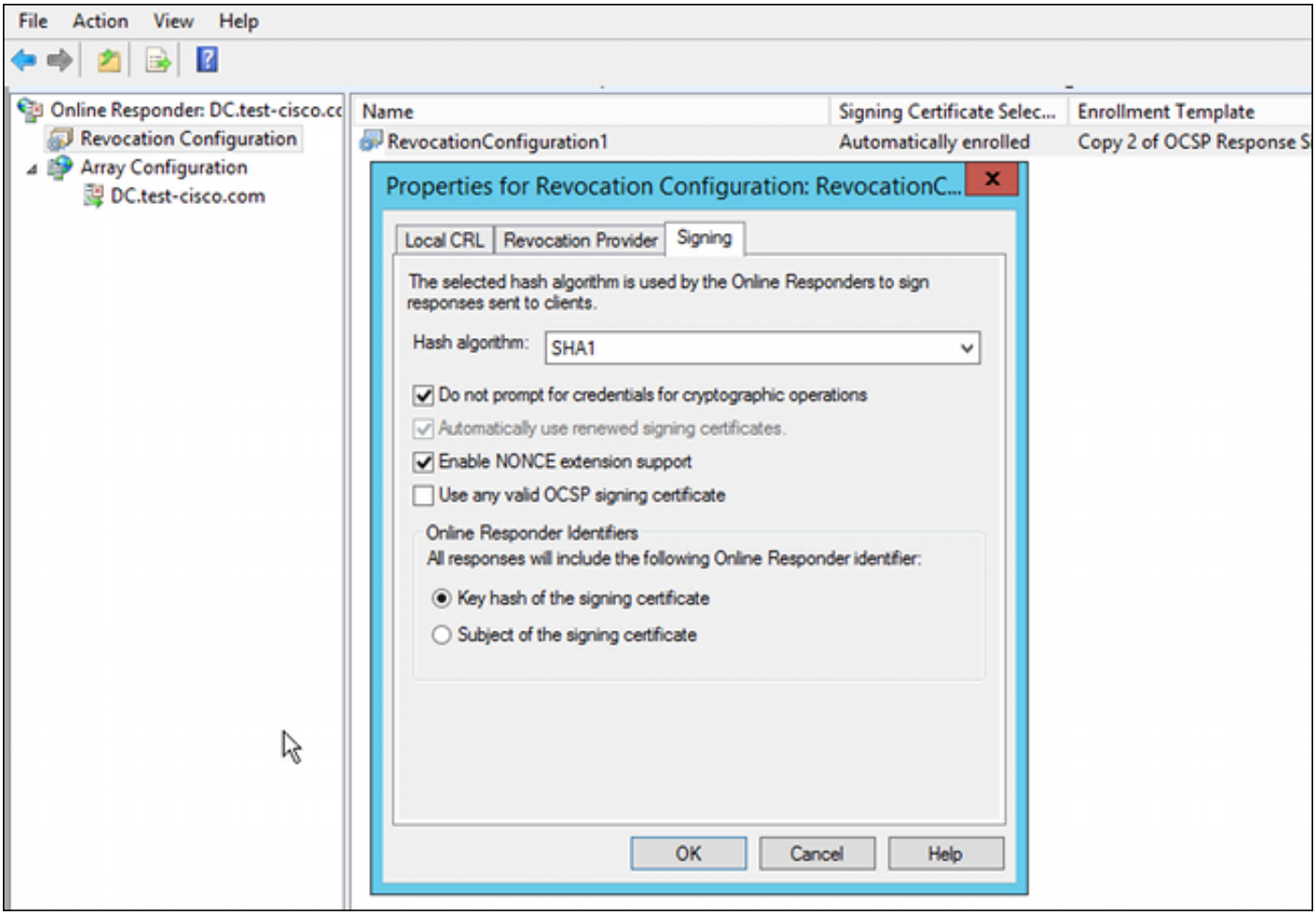


OCSP服務節點

OCSP的Microsoft實施符合RFC 5019適用於高容量環境的輕型線上證書狀態協定(OCSP)配置檔案(這是簡化版本的RFC 2560 X.509 Internet公鑰基礎設施線上證書狀態協定 — OCSP)。

ASA對OCSP使用RFC 2560。這兩個RFC的區別之一是RFC 5019不接受ASA傳送的簽名請求。

可以強制Microsoft OCSP服務接受這些已簽名的請求，並使用正確的已簽名的響應進行回覆。導航到**Revocation Configuration > RevocationConfiguration1 > Edit Properties**，然後選擇選項以**啟用NONCE擴展支援**。



OCSP服務現已可供使用。

雖然Cisco不建議這樣做，但是可以在ASA上禁用nonces:

```
BSNS-ASA5510-3(config-ca-trustpoint)# ocsp disable-nonce
```

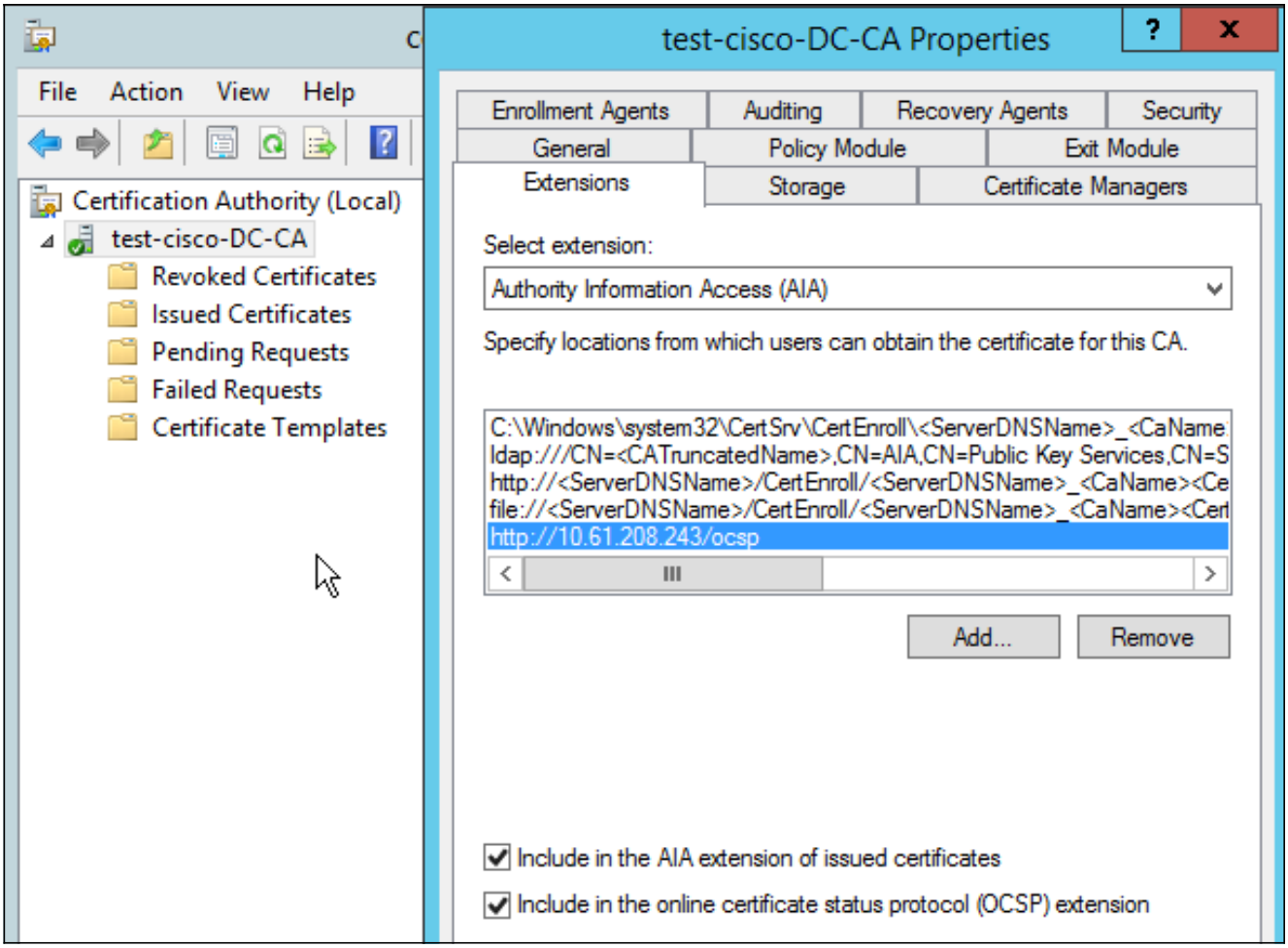
OCSP擴展的CA配置

現在，必須重新配置CA，以便在所有頒發的證書中包括OCSP伺服器擴展。驗證證書時，ASA使用該擴展的URL以連線到OCSP伺服器。

1. 開啟CA上伺服器的屬性對話方塊。

2. 按一下**Extensions**頁籤。需要指向OCSP服務的授權資訊訪問(AIA)擴展；在本示例中，該擴展為http://10.61.208.243/ocsp。為AIA擴展啟用以下兩個選項：

   包括在已頒發證書的AIA擴展中包括在線上證書狀態協定(OCSP)擴展中



這可確保所有簽發的證書都有一個指向OCSP服務的正確擴展。

OpenSSL

注意：有關通過CLI配置ASA的詳細資訊，請參閱Cisco ASA 5500系列使用CLI的配置指南8.4和8.6：配置外部伺服器以進行安全裝置使用者授權。

此範例假設已設定OpenSSL伺服器。本節僅介紹OCSP配置和CA配置所需的更改。

以下過程介紹了如何生成OCSP證書：

1. OCSP響應程式需要以下引數：

```
[ OCSPresponder ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = OCSPSigning
```

2. 使用者證書需要以下引數：

```
[ UserCerts ]
authorityInfoAccess = OCSP;URI:http://10.61.208.243
```

3. 證書需要由CA生成並簽名。

4. 啟動OCSP伺服器：

```
openssl ocsp -index ourCAwebPage/index.txt -port 80 -rsigner
ocspresponder.crt -rkey ocspresponder.key -CA cacert.crt -text -out
log.txt
```

5. 測試示例證書：

```
openssl ocsp -CAfile cacert.crt -issuer cacert.crt -cert example-cert.crt
-url http://10.61.208.243 -resp_text
```

更多示例可在OpenSSL網站上找到。

與ASA一樣，OpenSSL支援OCSP會話；可以使用 — nonce和 — no_nonce開關控制nonce。

具有多個OCSP源的ASA

ASA可以覆蓋OCSP URL。即使客戶端證書包含OCSP URL，它也會被ASA上的配置覆蓋：

```
crypto ca trustpoint WIN2012
 revocation-check ocsp
 enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll
 ocsp url http://10.10.10.10/ocsp
```

可以顯式定義OCSP伺服器地址。此命令示例匹配主題名稱中帶有管理員的所有證書，使用OPENSSL信任點驗證OCSP簽名，並使用http://11.11.11.11/ocsp的URL傳送請求：

```
crypto ca trustpoint WIN2012
 revocation-check ocsp
 enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll
 match certificate MAP override ocsp trustpoint OPENSSL 10 url
http://11.11.11.11/ocsp

crypto ca certificate map MAP 10
 subject-name co administrator
```

用於查詢OCSP URL的順序為：

1. 使用**match certificate**命令設定的OCSP伺服器
2. 使用**ocsp url**命令設定的**OCSP伺服器**
3. 客戶端證書的AIA欄位中的OCSP伺服器

具有由不同CA簽名的OCSP的ASA

OCSP響應可以由其他CA簽名。在這種情況下，必須使用**match certificate**命令才能在ASA上使用不同的信任點進行OCSP證書驗證。

```
crypto ca trustpoint WIN2012
 revocation-check ocsp
 enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll
 match certificate MAP override ocsp trustpoint OPENSSL 10 url
http://11.11.11.11/ocsp
```

```
crypto ca certificate map MAP 10
 subject-name co administrator

crypto ca trustpoint OPENSSL
enrollment terminal
revocation-check none
```

在此示例中，ASA對包含管理員的使用者名稱的所有證書使用OCSP URL重寫。ASA被迫根據另一個信任點OPENSSL驗證OCSP響應方證書。使用者證書仍在WIN2012信任點中驗證。

由於OCSP響應方證書具有「OCSP無撤銷檢查」擴展，因此即使強制對OPENSSL信任點進行OCSP驗證，也不會驗證證書。

預設情況下，當ASA嘗試驗證使用者證書時，將搜尋所有信任點。OCSP響應方證書的驗證不同。ASA僅搜尋已找到的使用者證書的信任點（在本例中為WIN2012）。

因此，必須使用**match certificate**命令來強制ASA使用不同的信任點進行OCSP證書驗證（在此示例中為OPENSSL）。

根據第一個匹配的信任點（本例中為WIN2012）驗證使用者證書，然後確定用於OCSP響應方驗證的預設信任點。

如果**match certificate**命令中未提供特定信任點，則會根據與使用者證書相同的信任點驗證OCSP證書（在本示例中為WIN2012）：

```
crypto ca trustpoint WIN2012
 revocation-check ocsp
 enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll
 match certificate MAP override ocsp 10 url http://11.11.11.11/ocsp
```

驗證

使用本節內容，確認您的組態是否正常運作。

> **註**:Output Interpreter Tool(僅供已註冊客戶)支援某些**show**命令。使用Output Interpreter工具檢視**show**指令輸出的分析。

ASA — 通過SCEP獲取證書

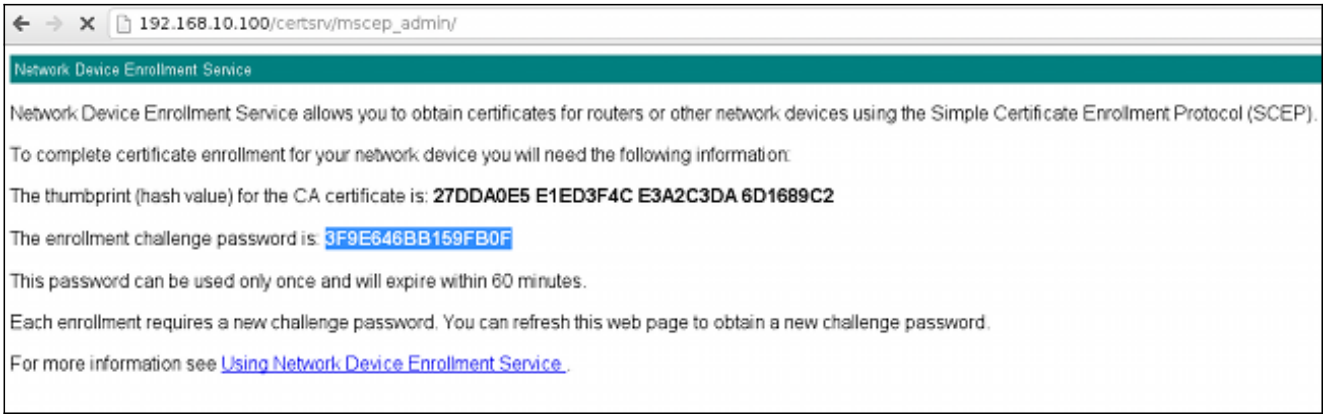
以下程式說明如何使用SCEP取得憑證：

1. 這是用於獲取CA證書的信任點身份驗證過程：

```
debug crypto ca
debug crypto ca messages
debug crypto ca transaction

BSNS-ASA5510-3(config-ca-crl)# crypto ca authenticate WIN2012
Crypto CA thread wakes up!

CRYPTO_PKI: Sending CA Certificate Request:
```

```
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=
WIN2012 HTTP/1.0
Host: 10.61.209.83

CRYPTO_PKI: http connection opened

INFO: Certificate has the following attributes:
Fingerprint:     27dda0e5 e1ed3f4c e3a2c3da 6d1689c2
Do you accept this certificate? [yes/no]:

% Please answer 'yes' or 'no'.
Do you accept this certificate? [yes/no]:
yes

Trustpoint CA certificate accepted.
```

2. 要請求證書，ASA需要一次性SCEP密碼，該密碼可從管理員控制檯(http://IP/certsrv/mscep_admin)獲取：



3. 使用該密碼在ASA上請求證書：

```
BSNS-ASA5510-3(config)# crypto ca enroll WIN2012
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the
configuration.
  Please make a note of it.
Password: ****************
Re-enter password: ****************


% The fully-qualified domain name in the certificate will be:
BSNS-ASA5510-3.test-cisco.com
% Include the device serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: JMX1014K16Y

Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
BSNS-ASA5510-3(config)#

CRYPTO_PKI: Sending CA Certificate Request:
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=
WIN2012 HTTP/1.0
Host: 10.61.209.83
```

```
CRYPTO_PKI: http connection opened

CRYPTO_PKI: Found a subject match - inserting the following cert record
into certList
```

為清楚起見，省略了部分輸出。

4. 驗證CA和ASA證書：

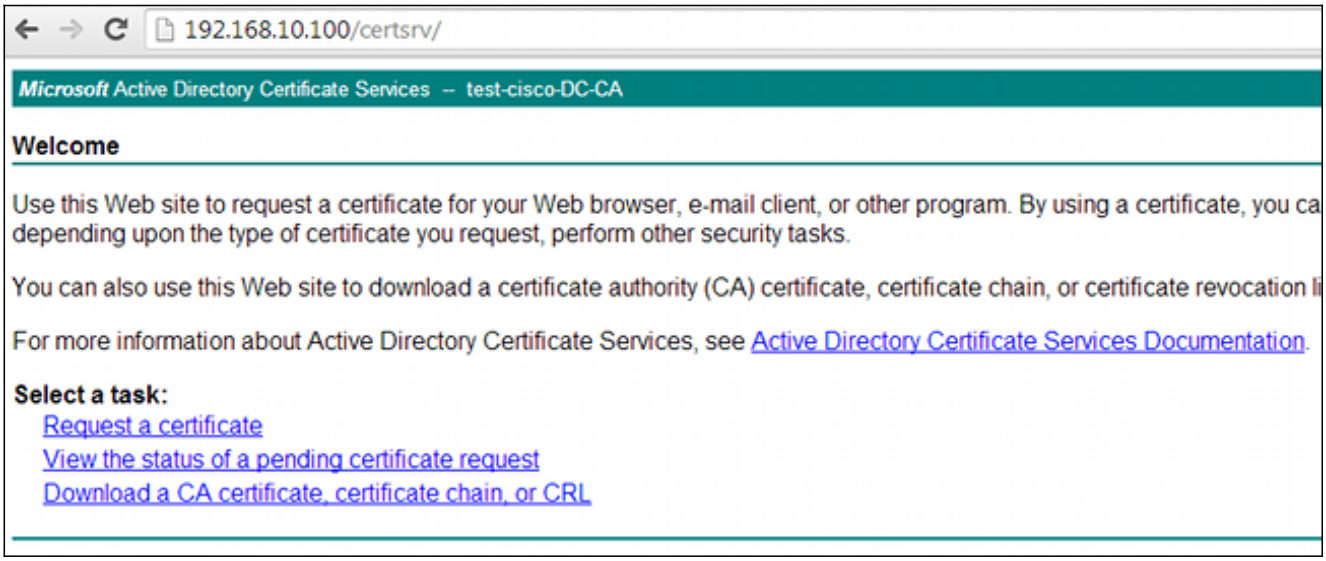
```
BSNS-ASA5510-3(config)# show crypto ca certificates
Certificate
 Status: Available
 Certificate Serial Number: 240000001cbf2fc89f44fe819700000000001c
 Certificate Usage: General Purpose
 Public Key Type: RSA (1024 bits)
 Signature Algorithm: SHA1 with RSA Encryption
 Issuer Name:
   cn=test-cisco-DC-CA
   dc=test-cisco
   dc=com
 Subject Name:
    hostname=BSNS-ASA5510-3.test-cisco.com
   serialNumber=JMX1014K16Y
 CRL Distribution Points:
   [1]  ldap:///CN=test-cisco-DC-CA,CN=DC,CN=CDP,
CN=Public%20Key%20Services,CN=Services,CN=Configuration,
DC=test-cisco,DC=com?certificateRevocationList?base?objectClass=
cRLDistributionPoint
 Validity Date:
   start date: 11:02:36 CEST Oct 13 2013
   end   date: 11:02:36 CEST Oct 13 2015
 Associated Trustpoints: WIN2012

CA Certificate
 Status: Available
 Certificate Serial Number: 3d4c0881b04c799f483f4bbe91dc98ae
 Certificate Usage: Signature
 Public Key Type: RSA (2048 bits)
 Signature Algorithm: SHA1 with RSA Encryption
 Issuer Name:
    cn=test-cisco-DC-CA
   dc=test-cisco
   dc=com
 Subject Name:
   cn=test-cisco-DC-CA
   dc=test-cisco
   dc=com
 Validity Date:
   start date: 07:23:03 CEST Oct 10 2013
   end   date: 07:33:03 CEST Oct 10 2018
 Associated Trustpoints: WIN2012
```

ASA不顯示大多數證書擴展。即使ASA證書包含「AIA中的OCSP URL」擴展，ASA CLI也不會顯示它。思科錯誤ID CSCui44335、「ASA ENH Certificate x509 extensions displayed（已顯示ASA增強型證書x509擴展）」請求此增強功能。

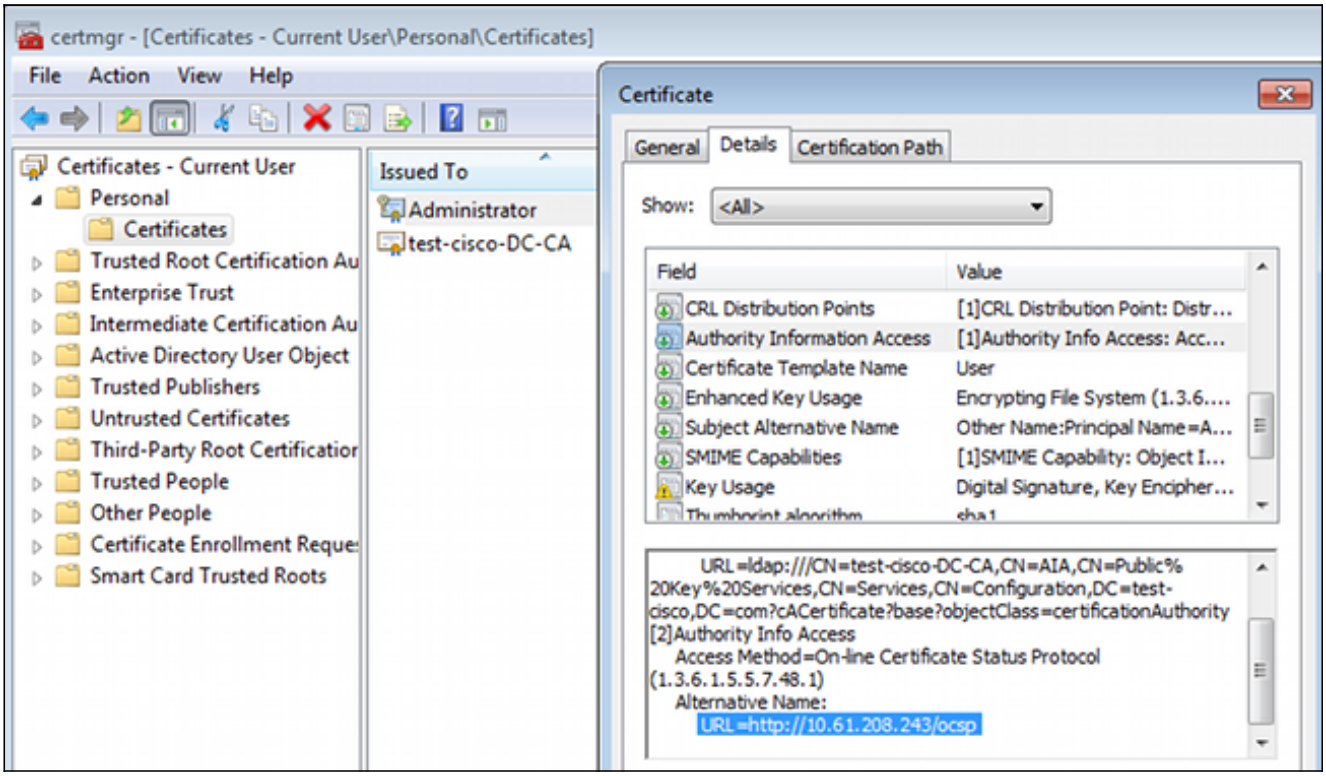
AnyConnect — 通過網頁獲取證書

以下程式說明如何在使用者端上使用Web瀏覽器來取得憑證：

1. 可以通過網頁請求AnyConnect使用者證書。在客戶端PC上，使用Web瀏覽器轉到CA，地址為http://*IP*/certsrv:



2. 使用者證書可以儲存在Web瀏覽器儲存中，然後匯出到Microsoft儲存中，AnyConnect將搜尋該儲存區。使用certmgr.msc驗證收到的證書：



AnyConnect還可以請求證書，只要有正確的AnyConnect配置檔案。

帶OCSP的ASA VPN遠端訪問驗證

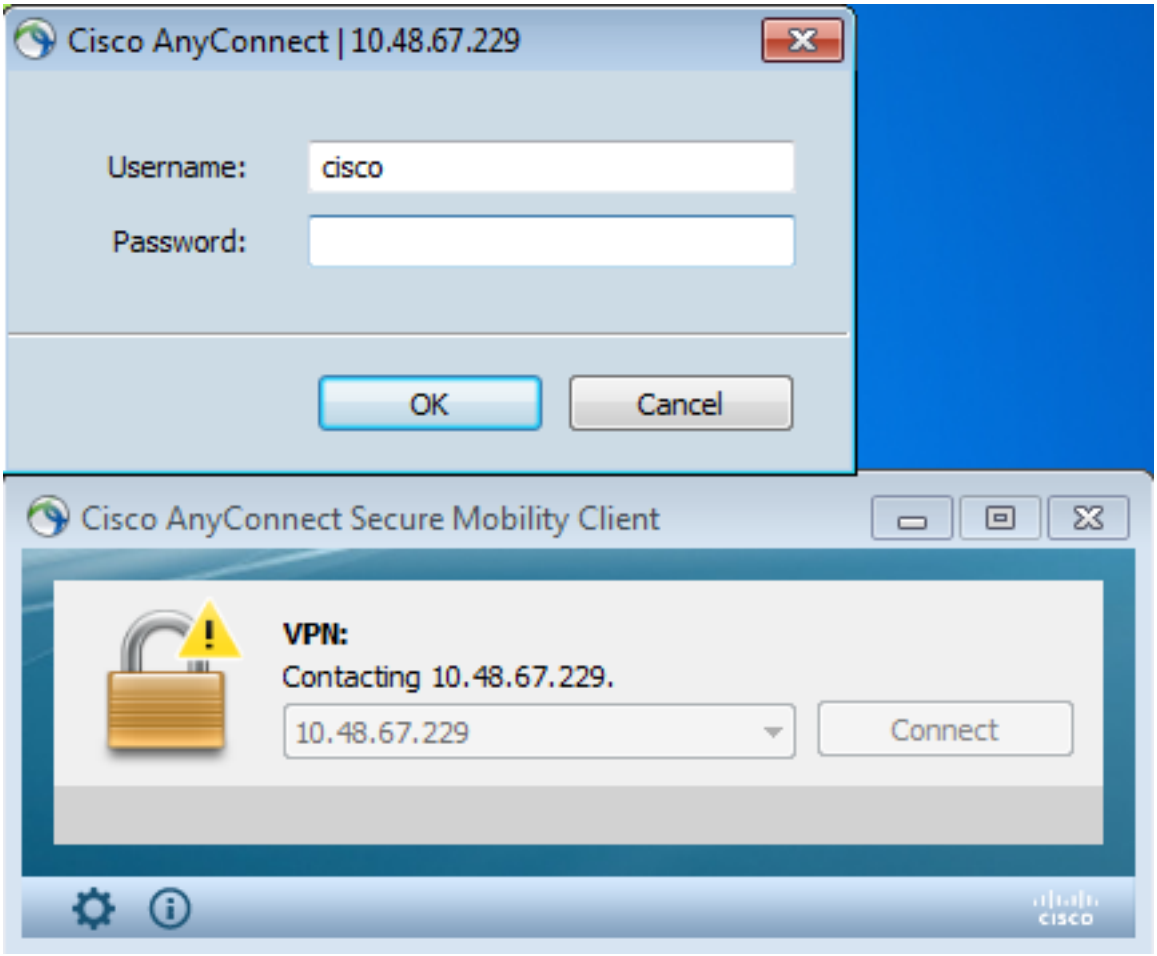
以下過程介紹了如何檢查OCSP驗證：

1. 在嘗試連線時，ASA報告正在檢查證書的OCSP。此處，OCSP簽名證書具有無檢查副檔名，且尚未通過OCSP檢查：

```
debug crypto ca
debug crypto ca messages
debug crypto ca transaction

%ASA-6-725001: Starting SSL handshake with client outside:
10.61.209.83/51262 for TLSv1 session.
%ASA-7-717025: Validating certificate chain containing 1 certificate(s).
%ASA-7-717029: Identified client certificate within certificate chain.
serial number: 240000001B2AD208B12811687400000000001B, subject name:
cn=Administrator,cn=Users,dc=test-cisco,dc=com.
Found a suitable trustpoint WIN2012 to validate certificate.
%ASA-7-717035: OCSP status is being checked for certificate. serial
number: 240000001B2AD208B12811687400000000001B, subject name:
cn=Administrator,cn=Users,dc=test-cisco,dc=com.
%ASA-6-302013: Built outbound TCP connection 1283 for outside:
10.61.209.83/80 (10.61.209.83/80) to identity:10.48.67.229/35751
(10.48.67.229/35751)
%ASA-6-717033: CSP response received.
%ASA-7-717034: No-check extension found in certificate. OCSP check
bypassed.
%ASA-6-717028: Certificate chain was successfully validated with
revocation status check.
```

為清楚起見，省略了部分輸出。

2. 終端使用者提供使用者憑證：



3. VPN作業階段已正確完成：

```
%ASA-7-717036: Looking for a tunnel group match based on certificate maps
for peer certificate with serial number:
240000001B2AD208B128116874000000000001B, subject name: cn=Administrator,
cn=Users,dc=test-cisco,dc=com, issuer_name: cn=test-cisco-DC-CA,
dc=test-cisco,dc=com.
%ASA-7-717038: Tunnel group match found. Tunnel Group: RA, Peer
certificate: serial number: 240000001B2AD208B128116874000000000001B,
subject name: cn=Administrator,cn=Users,dc=test-cisco,dc=com,
issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,dc=com.

%ASA-6-113012: AAA user authentication Successful : local database :
user = cisco
%ASA-6-113009: AAA retrieved default group policy (MY) for user = cisco
%ASA-6-113039: Group <MY> User <cisco> IP <10.61.209.83> AnyConnect parent
session started.
```

4. 會話已建立：

```
BSNS-ASA5510-3(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : cisco                  Index        : 4
Assigned IP  : 192.168.11.100         Public IP    : 10.61.209.83
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1)SHA1
Bytes Tx     : 10540                  Bytes Rx     : 32236
Pkts Tx      : 8                      Pkts Rx      : 209
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : MY                     Tunnel Group : RA
Login Time   : 11:30:31 CEST Sun Oct 13 2013
Duration     : 0h:01m:05s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
 Tunnel ID    : 4.1
 Public IP    : 10.61.209.83
 Encryption   : none                   Hashing      : none
 TCP Src Port : 51401                  TCP Dst Port : 443
 Auth Mode    : Certificate and userPassword
 Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
 Client OS    : Windows
 Client Type  : AnyConnect
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 5270                   Bytes Rx     : 788
 Pkts Tx      : 4                      Pkts Rx      : 1
 Pkts Tx Drop : 0                      Pkts Rx Drop : 0

SSL-Tunnel:
 Tunnel ID    : 4.2
 Assigned IP  : 192.168.11.100         Public IP    : 10.61.209.83
```

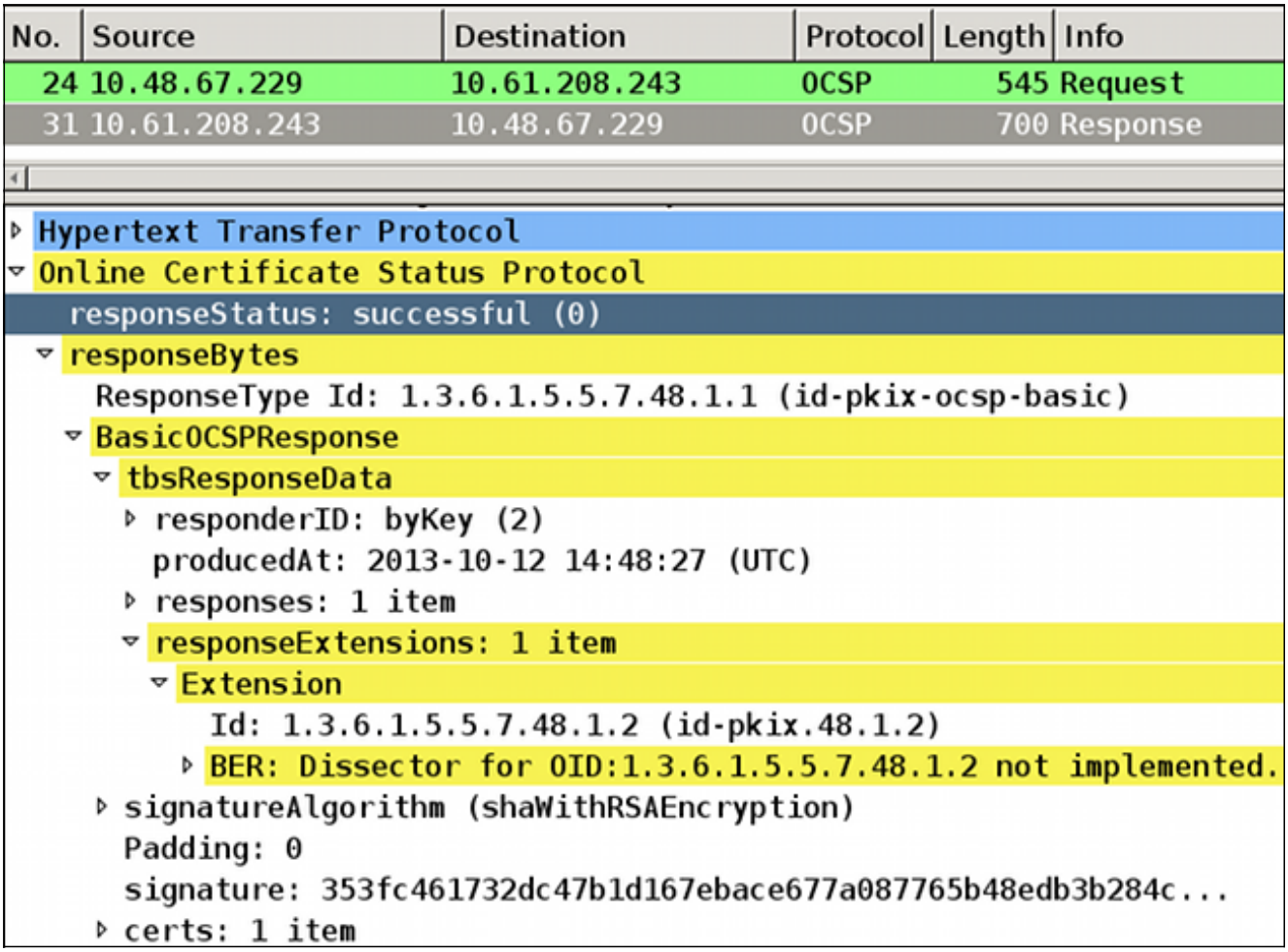
```
 Encryption   : RC4                    Hashing      : SHA1
 Encapsulation: TLSv1.0                TCP Src Port : 51406
 TCP Dst Port : 443                    Auth Mode    : Certificate and
userPassword
 Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
 Client OS    : Windows
 Client Type  : SSL VPN Client
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 5270                   Bytes Rx     : 1995
 Pkts Tx      : 4                      Pkts Rx      : 10
 Pkts Tx Drop : 0                      Pkts Rx Drop : 0

DTLS-Tunnel:
 Tunnel ID    : 4.3
 Assigned IP  : 192.168.11.100         Public IP    : 10.61.209.83
 Encryption   : AES128                 Hashing      : SHA1
 Encapsulation: DTLSv1.0               UDP Src Port : 58053
 UDP Dst Port : 443                    Auth Mode    : Certificate and
userPassword
 Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
 Client OS    : Windows
 Client Type  : DTLS VPN Client
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 0                      Bytes Rx     : 29664
 Pkts Tx      : 0                      Pkts Rx      : 201
 Pkts Tx Drop : 0                      Pkts Rx Drop : 0
```

5. 您可以使用詳細調試進行OCSP驗證：

```
CRYPTO_PKI: Starting OCSP revocation
CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial number:
2400000019F341BA75BD25E91A000000000019, subject name: cn=Administrator,
cn=Users,dc=test-cisco,dc=com, issuer_name: cn=test-cisco-DC-CA,
dc=test-cisco,dc=com.
CRYPTO_PKI: No OCSP overrides found. <-- no OCSP url in the ASA config

CRYPTO_PKI: http connection opened
CRYPTO_PKI: OCSP response received successfully.
CRYPTO_PKI: OCSP found in-band certificate: serial number:
240000001221CFA239477CE1C0000000000012, subject name:
cn=DC.test-cisco.com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,
dc=com
CRYPTO_PKI: OCSP responderID byKeyHash
CRYPTO_PKI: OCSP response contains 1 cert singleResponses responseData
sequence.

Found response for request certificate!
CRYPTO_PKI: Verifying OCSP response with 1 certs in the responder chain
CRYPTO_PKI: Validating OCSP response using trusted CA cert: serial number:
3D4C0881B04C799F483F4BBE91DC98AE, subject name: cn=test-cisco-DC-CA,
dc=test-cisco,dc=com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,
dc=com

CERT-C: W ocsputil.c(538) : Error #708h
CERT-C: W ocsputil.c(538) : Error #708h

CRYPTO_PKI: Validating OCSP responder certificate: serial number:
240000001221CFA239477CE1C0000000000012, subject name:
cn=DC.test-cisco.com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,
dc=com, signature alg: SHA1/RSA

CRYPTO_PKI: verifyResponseSig:3191
CRYPTO_PKI: OCSP responder cert has a NoCheck extension
```

```
CRYPTO_PKI: Responder cert status is not revoked <-- do not verify
responder cert
CRYPTO_PKI: response signed by the CA
CRYPTO_PKI: Storage context released by thread Crypto CA

CRYPTO_PKI: transaction GetOCSP completed
CRYPTO_PKI: Process next cert, valid cert. <-- client certificate
validated correctly
```

6. 在資料包捕獲級別，這是OCSP請求和正確的OCSP響應。響應包含在Microsoft OCSP上啟用的正確簽名 — nonce擴展：



具有多個OCSP源的ASA VPN遠端訪問

如果按照具有多個OCSP源的ASA中的說明配置匹配證書，則優先使用：

```
CRYPTO_PKI: Processing map MAP sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:  =
cn=Administrator,cn=Users,dc=test-cisco,dc=com, map rule: subject-name
  co administrator.
CRYPTO_PKI: Peer cert has been authorized by map: MAP sequence: 10.
CRYPTO_PKI: Found OCSP override match. Override URL: http://11.11.11.11/ocsp,
Override trustpoint: OPENSSL
```

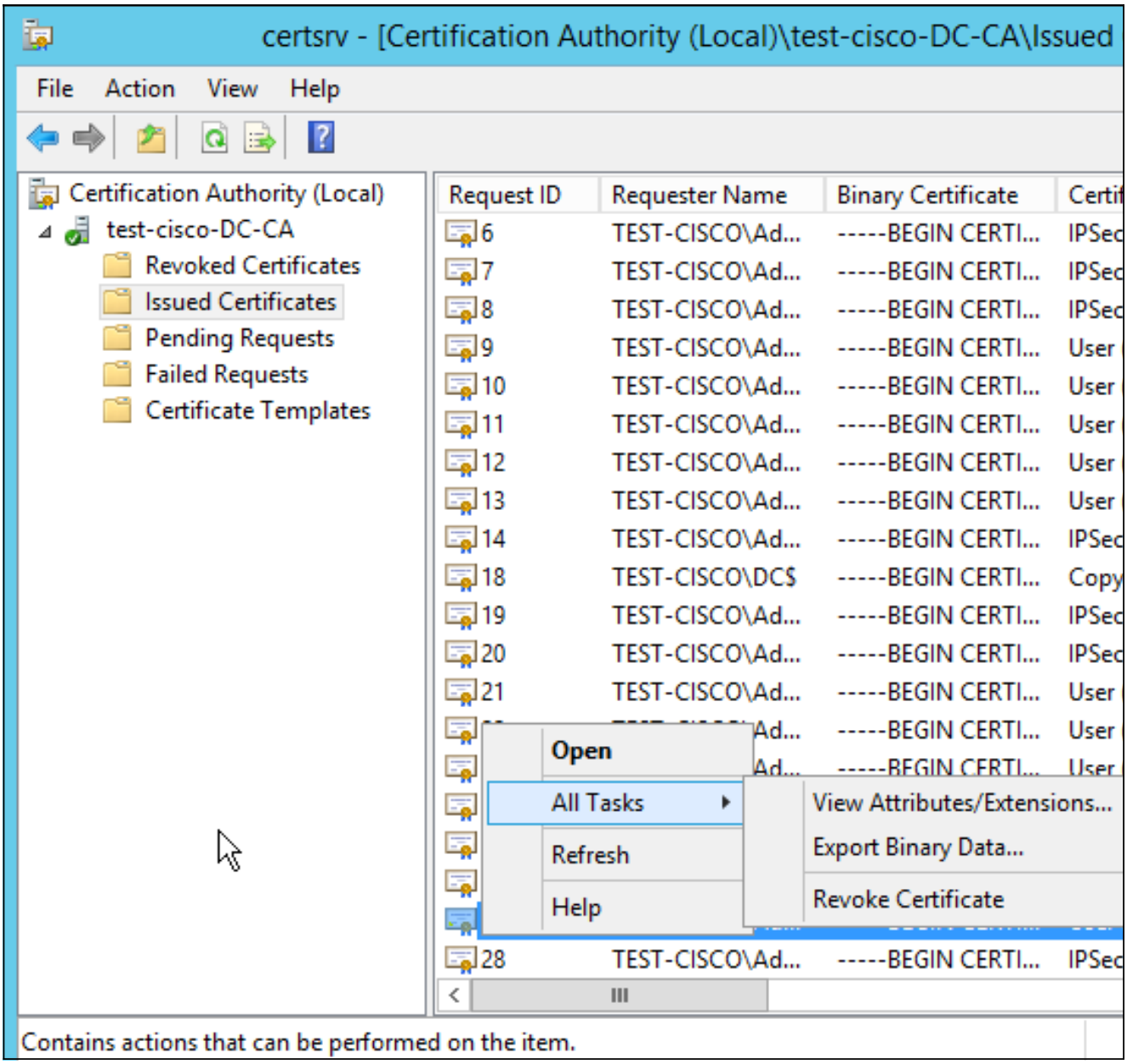
使用OCSP URL覆蓋時，調試程式為：

```
CRYPTO_PKI: No OCSP override via cert maps found. Override was found in
trustpoint: WIN2012, URL found: http://10.10.10.10/ocsp.
```

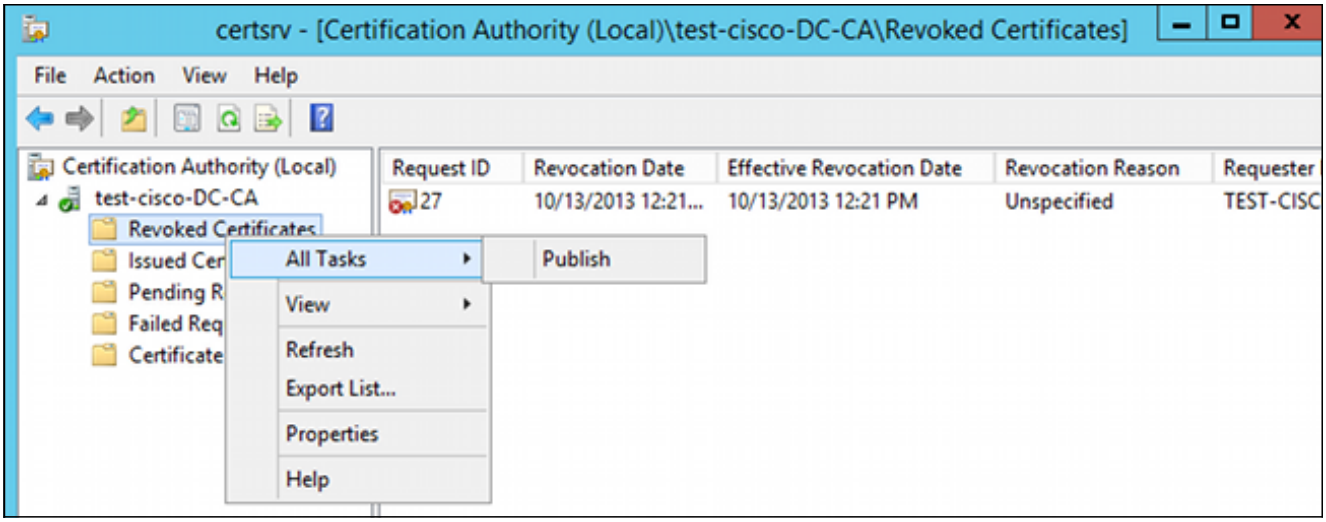
具有OCSP和已撤銷證書的ASA VPN遠端訪問

以下過程介紹了如何撤銷證書和確認撤銷狀態：

1. 吊銷客戶端證書：



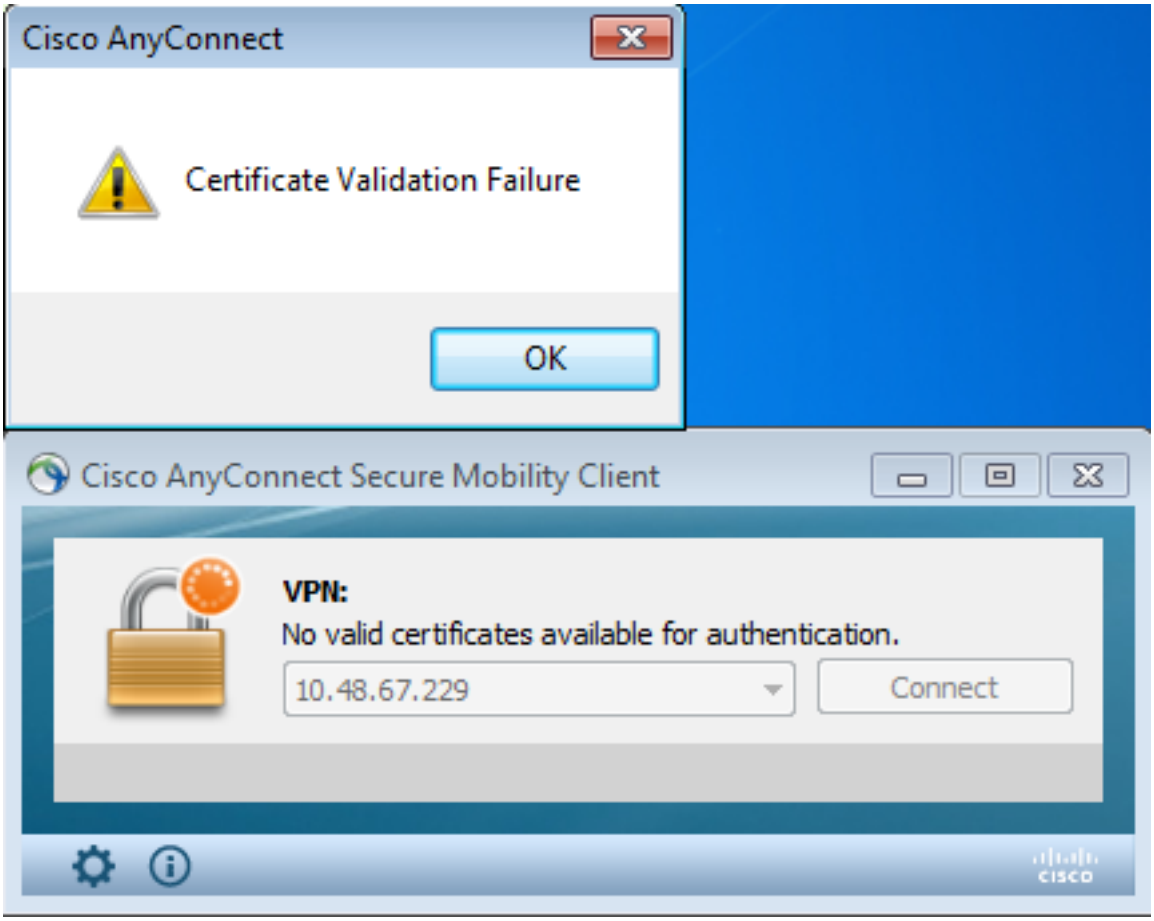
2. 發佈結果：



3. [可選]步驟1和2也可以使用Power Shell中的certutil CLI實用程式來完成：

```
c:\certutil -crl
CertUtil: -CRL command completed succesfully.
```

4. 使用者端嘗試連線時，存在憑證驗證錯誤：



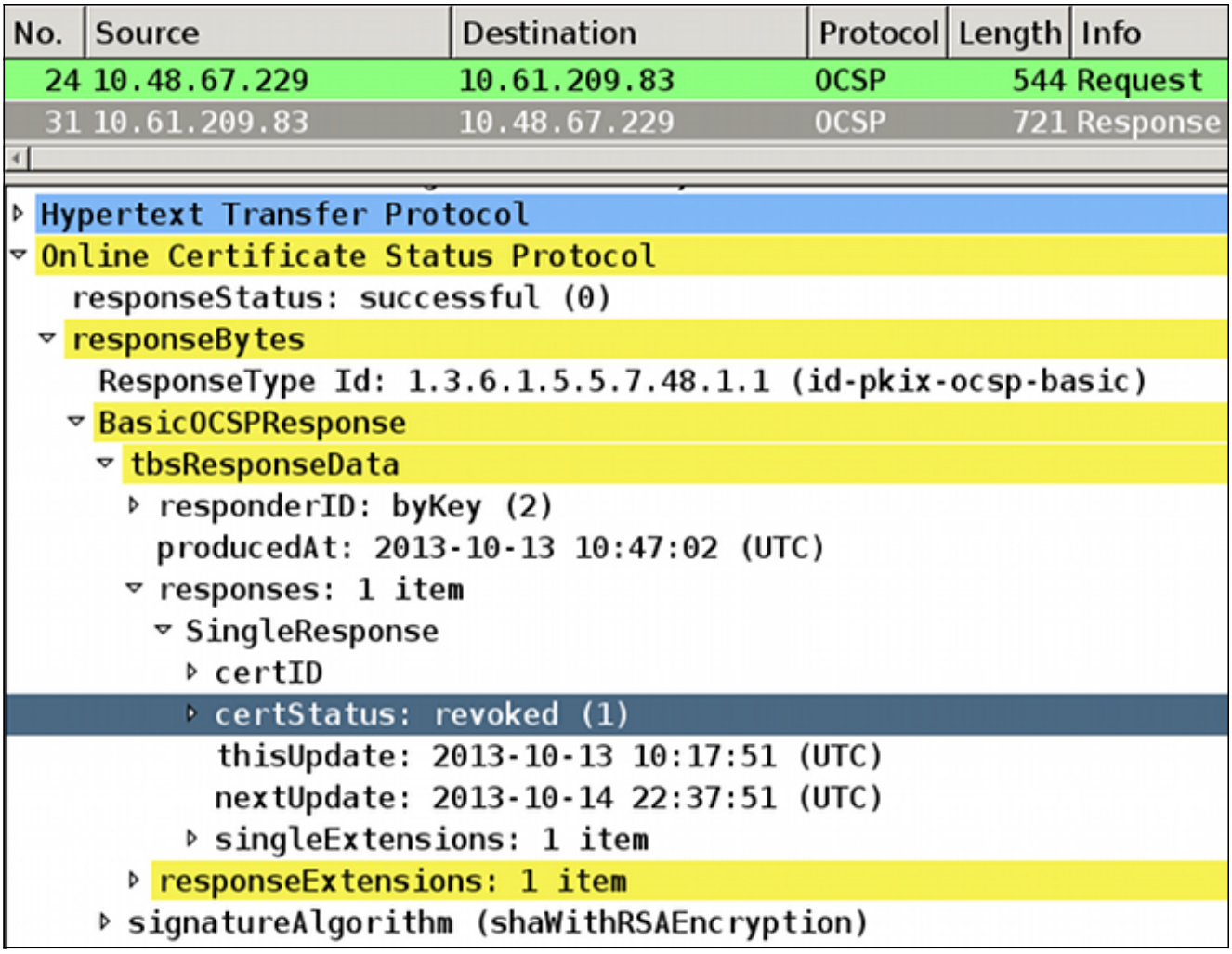
5. AnyConnect日誌還指示證書驗證錯誤：

```
[2013-10-13 12:49:53] Contacting 10.48.67.229.
[2013-10-13 12:49:54] No valid certificates available for authentication.
[2013-10-13 12:49:55] Certificate Validation Failure
```

6. ASA報告證書狀態已吊銷：

```
CRYPTO_PKI: Starting OCSP revocation
CRYPTO_PKI: OCSP response received successfully.
CRYPTO_PKI: OCSP found in-band certificate: serial number:
240000001221CFA239477CE1C0000000000012, subject name:
cn=DC.test-cisco.com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,
dc=com
CRYPTO_PKI: OCSP responderID byKeyHash
CRYPTO_PKI: OCSP response contains 1 cert singleResponses responseData
sequence.

Found response for request certificate!
CRYPTO_PKI: Verifying OCSP response with 1 certs in the responder chain
CRYPTO_PKI: Validating OCSP response using trusted CA cert: serial number:
3D4C0881B04C799F483F4BBE91DC98AE, subject name: cn=test-cisco-DC-CA,
dc=test-cisco,dc=com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,
dc=com

CRYPTO_PKI: verifyResponseSig:3191
CRYPTO_PKI: OCSP responder cert has a NoCheck extension
CRYPTO_PKI: Responder cert status is not revoked
CRYPTO_PKI: response signed by the CA
CRYPTO_PKI: Storage context released by thread Crypto CA

CRYPTO_PKI: transaction GetOCSP completed

CRYPTO_PKI: Received OCSP response:Oct 13 2013 12:48:03: %ASA-3-717027:
Certificate chain failed validation. Generic error occurred, serial
number: 240000001B2AD208B1281168740000000001B, subject name:
cn=Administrator,cn=Users,dc=test-cisco,dc=com.

CRYPTO_PKI: Blocking chain callback called for OCSP response (trustpoint:
WIN2012, status: 1)
CRYPTO_PKI: Destroying OCSP data handle 0xae255ac0
CRYPTO_PKI: OCSP polling for trustpoint WIN2012 succeeded. Certificate
status is REVOKED.
CRYPTO_PKI: Process next cert in chain entered with status: 13.
CRYPTO_PKI: Process next cert, Cert revoked: 13
```

7. 封包擷取顯示成功的OCSP回應，且憑證狀態為已撤銷：



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

OCSP伺服器關閉

ASA在OCSP伺服器關閉時報告：

```
CRYPTO_PKI: unable to find a valid OCSP server.
CRYPTO PKI: OCSP revocation check has failed.  Status: 1800.
```

封包擷取也有助於進行疑難排解。

時間不同步

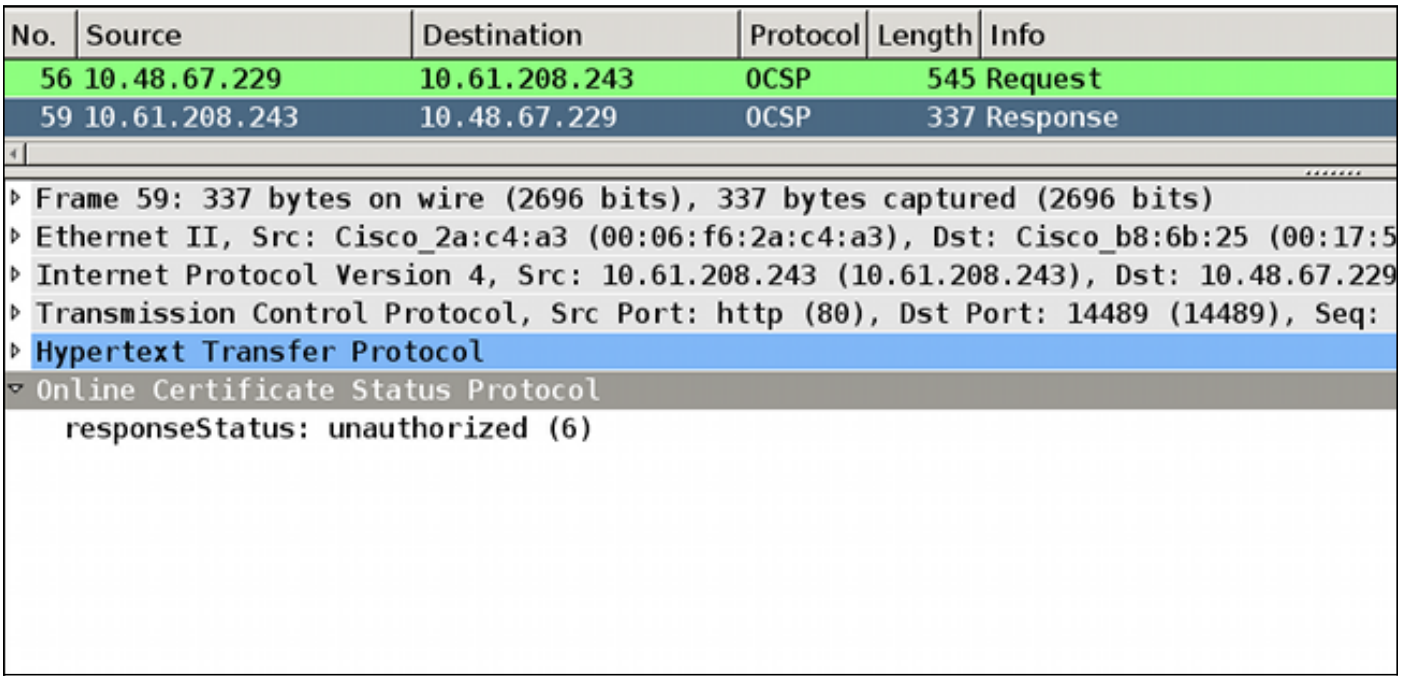
如果OCSP伺服器上的當前時間早於ASA上的時間（可以接受較小的差異），則OCSP伺服器將傳送未經授權的響應，ASA將報告該響應：

```
CRYPTO_PKI: OCSP response status - unauthorized
```

當ASA收到來自未來時間的OCSP響應時，也會失敗。

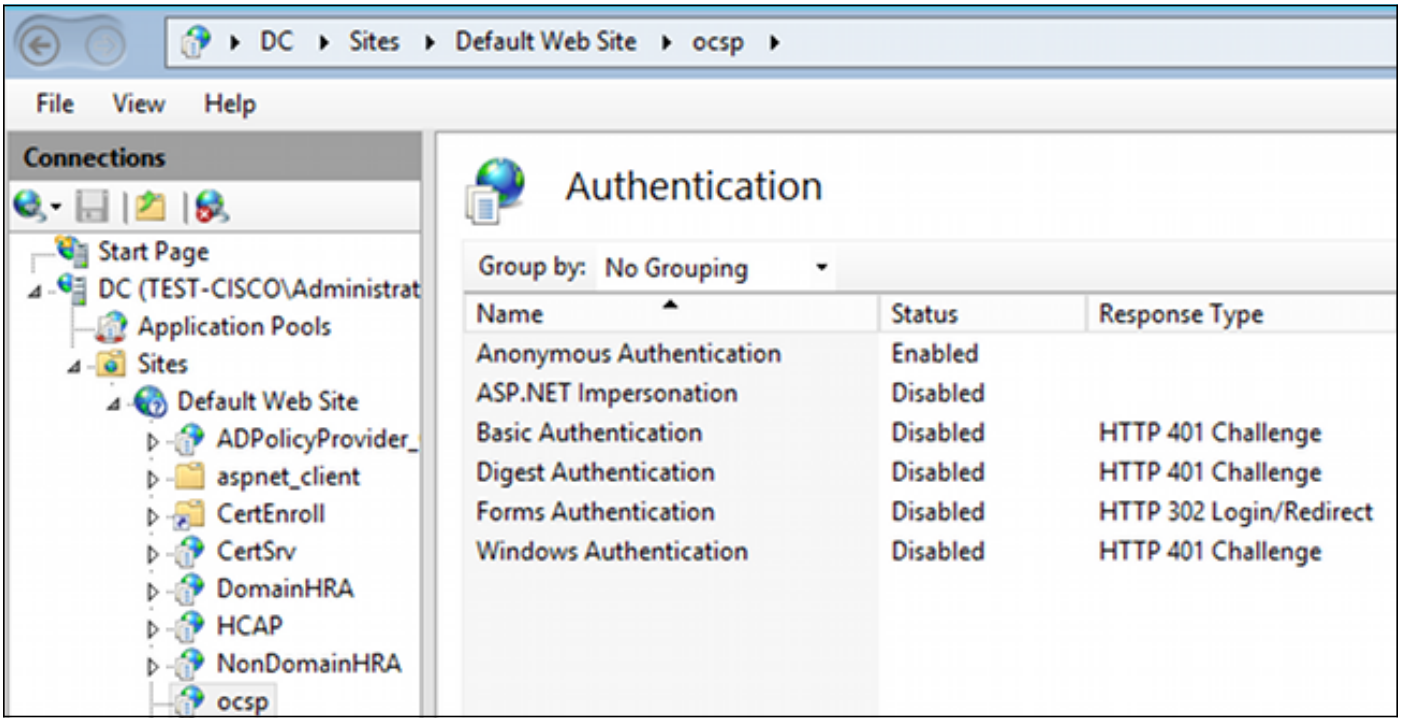
不支援簽名的Nonces

如果伺服器上的nonces不受支援（這是Microsoft Windows 2012 R2的預設設定），則會返回未經授權的響應：



IIS7伺服器身份驗證

SCEP/OCSP請求的問題通常是由於Internet資訊服務7(IIS7)上的身份驗證不正確造成的。確保配置了匿名訪問：



相關資訊

- Microsoft TechNet: Online Responder安裝、配置和故障排除指南
- Microsoft TechNet：配置CA以支援OCSP響應程式
- Cisco ASA系列命令參考
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。