Microsoft Windows 2012和OpenSSL下带OCSP验证的ASA远程访问VPN

目录

简介

本文档介绍如何在思科自适应安全设备(ASA)上对VPN用户提供的证书使用在线证书状态协议(OCSP)验证。提供了两个OCSP服务器（Microsoft Windows Certificate Authority [CA]和OpenSSL）的配置示例。“验证”部分描述数据包级别的详细流程，“故障排除”部分重点介绍典型错误和问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科自适应安全设备命令行界面(CLI)配置和安全套接字层(SSL)VPN配置
- X.509证书
- Microsoft Windows Server
- Linux/OpenSSL

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科自适应安全设备软件8.4版及更高版本
- 带Cisco AnyConnect安全移动客户端的Microsoft Windows 7，版本3.1
- Microsoft Server 2012 R2
- 使用OpenSSL 1.0.0j或更高版本的Linux

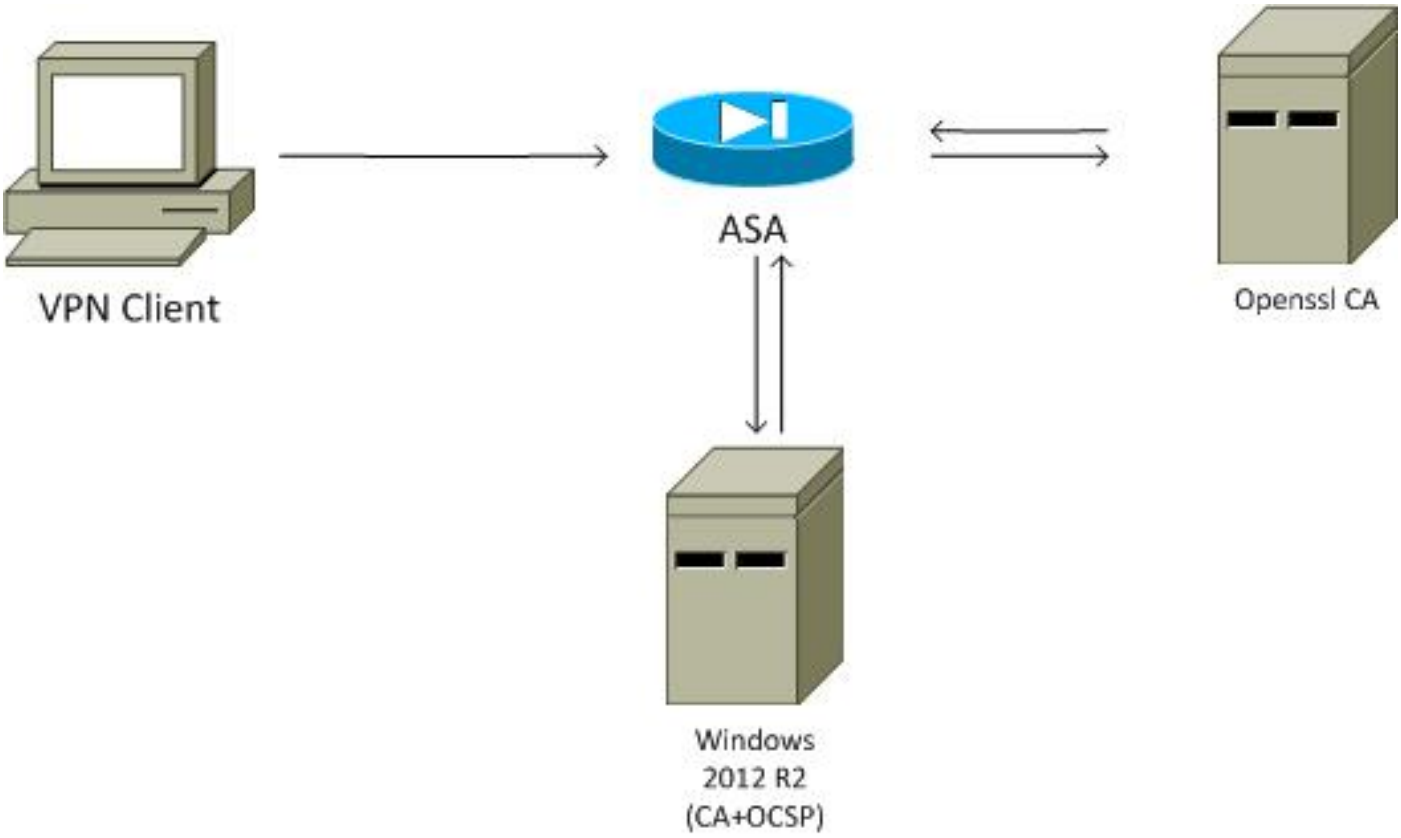
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

> **注意：要获取有关本部分中所使用命令的更多信息，可使用命令查找工具（仅限已注册客户）。**

网络图

客户端使用远程访问VPN。此访问可以是Cisco VPN Client(IPSec)、Cisco AnyConnect Secure Mobility(SSL/Internet Key Exchange Version 2 [IKEv2])或WebVPN（门户）。为了登录，客户端提供正确的证书，以及在ASA上本地配置的用户名/密码。客户端证书通过OCSP服务器进行验证。



带OCSP的ASA远程访问

为SSL访问配置了ASA。客户端使用AnyConnect登录。ASA使用简单证书注册协议(SCEP)请求证书：

```
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
```

创建证书映射以标识其主题名称包含单词administrator（不区分大小写）的所有用户。这些用户已绑定到名为RA的隧道组：

```
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配置需要成功的授权（即经过验证的证书）。它还要求本地定义的用户名(authentication aaa)具有正确的凭证：

```
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

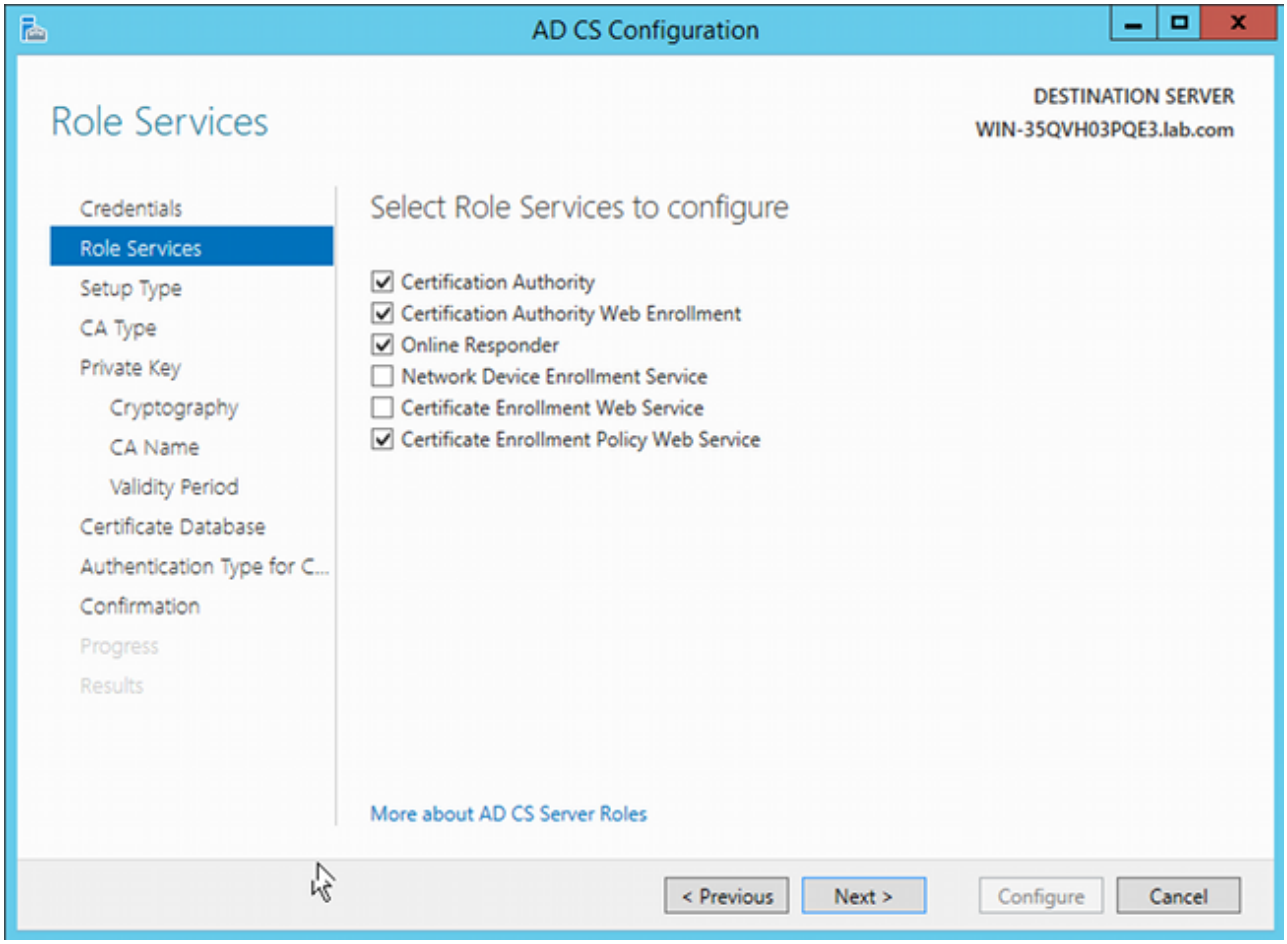
> **注意**：有关通过CLI配置ASA的详细信息，请参阅使用CLI、8.4和8.6配置外部服务器以进行安全设备用户授权的思科ASA 5500系列配置指南。

服务安装

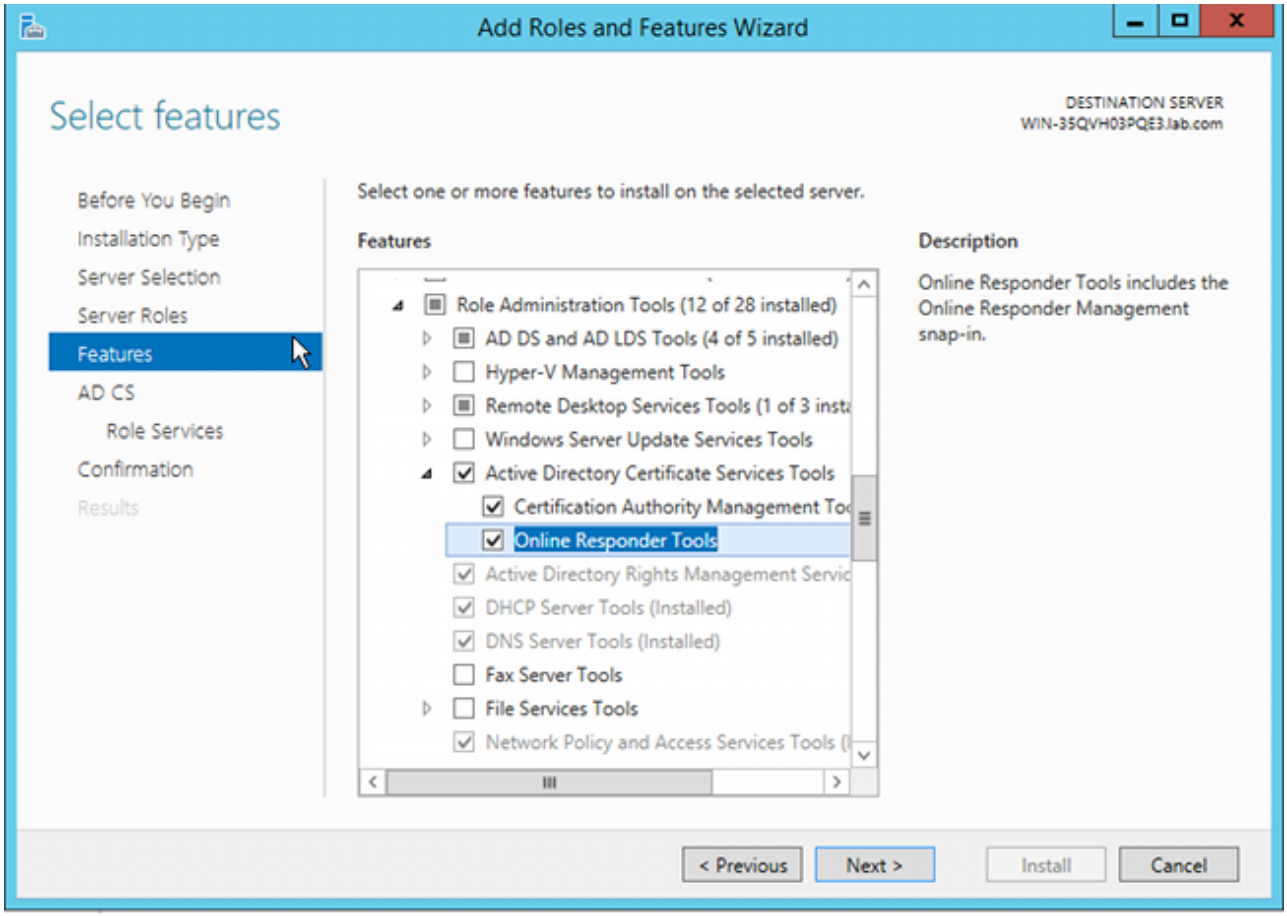
此过程介绍如何为Microsoft服务器配置角色服务：

1. 导航到**Server Manager > Manage > Add Roles and Features**。Microsoft服务器需要以下角色服务：

   证书颁发机构客户端使用的证书颁发机构Web注册Online Responder，OCSP需要网络设备注册服务，包含ASA使用的SCEP应用 如果需要，可以添加带策略的Web服务。



2.
3.
4. 添加功能时，请务必包括Online Responder Tools，因为它包含稍后使用的OCSP管理单元：



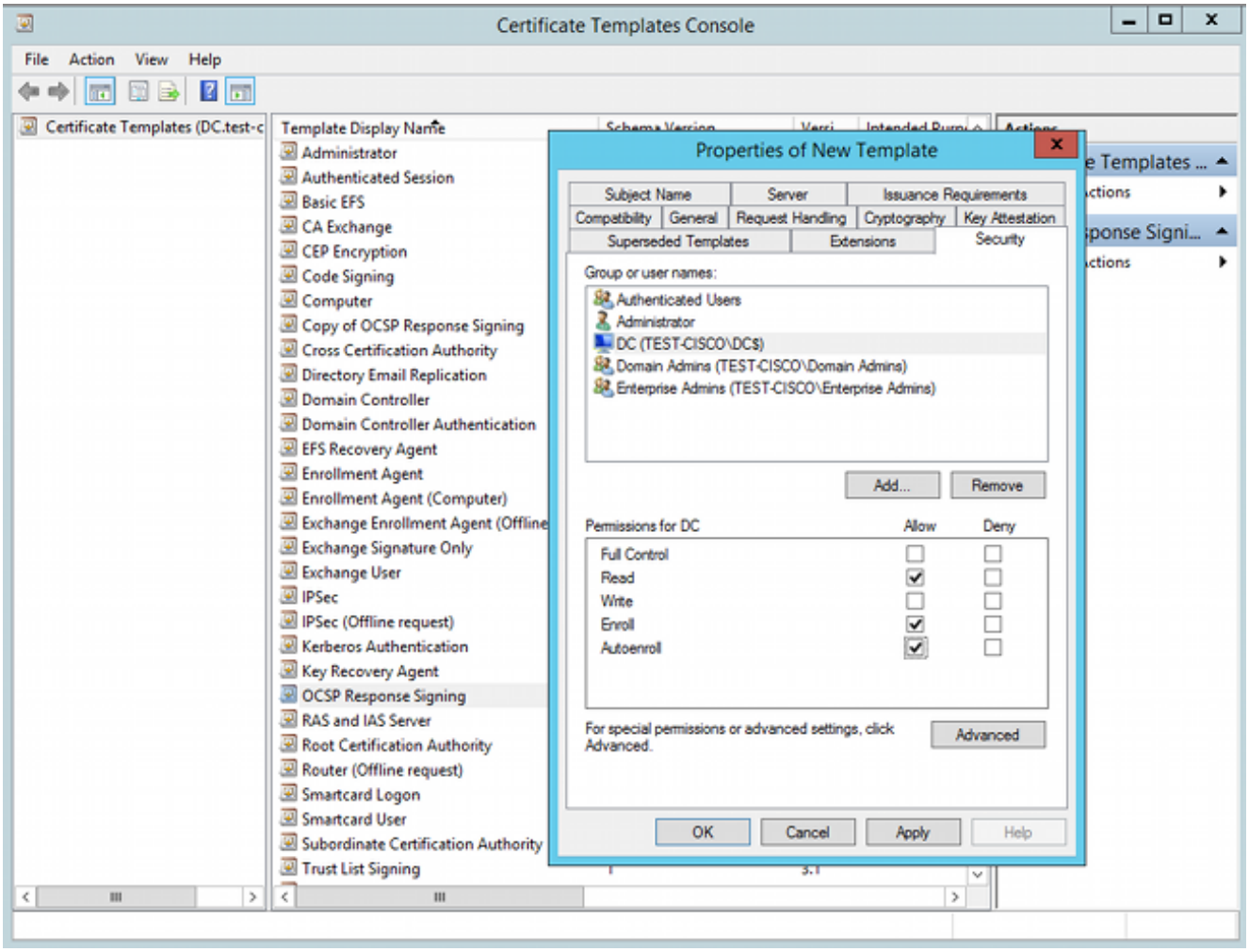
OCSP模板的CA配置

OCSP服务使用证书对OCSP响应进行签名。必须在Microsoft服务器上生成特殊证书，并且必须包括：

- 扩展密钥使用= OCSP签名
- OCSP无撤销检查

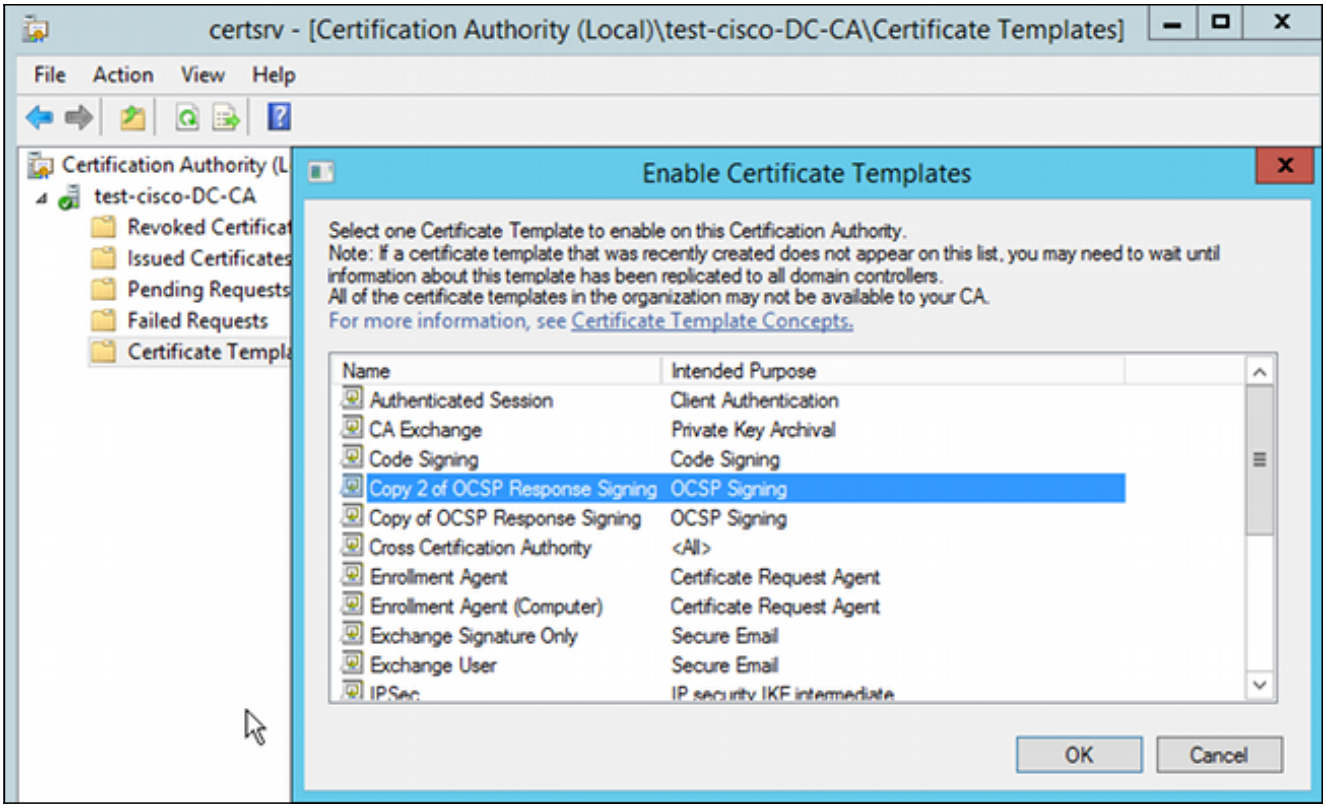
需要此证书以防止OCSP验证循环。ASA不使用OCSP服务尝试检查OCSP服务提供的证书。

1. 在CA上为证书添加模板。导航到**CA > Certificate Template > Manage**，选择**OCSP Response Signing**，然后复制模板。查看新创建的模板的属性，然后单击**Security**选项卡。权限描述允许哪个实体请求使用该模板的证书，因此需要正确的权限。在本示例中，实体是在同一主机(TEST-CISCO\DC)上运行的OCSP服务，并且OCSP服务需要自动注册权限：



模板的所有其他设置都可以设置为默认值。

2. 激活模板。导航到**CA > Certificate Template > New > Certificate Template to Issue**，然后选择复制模板：

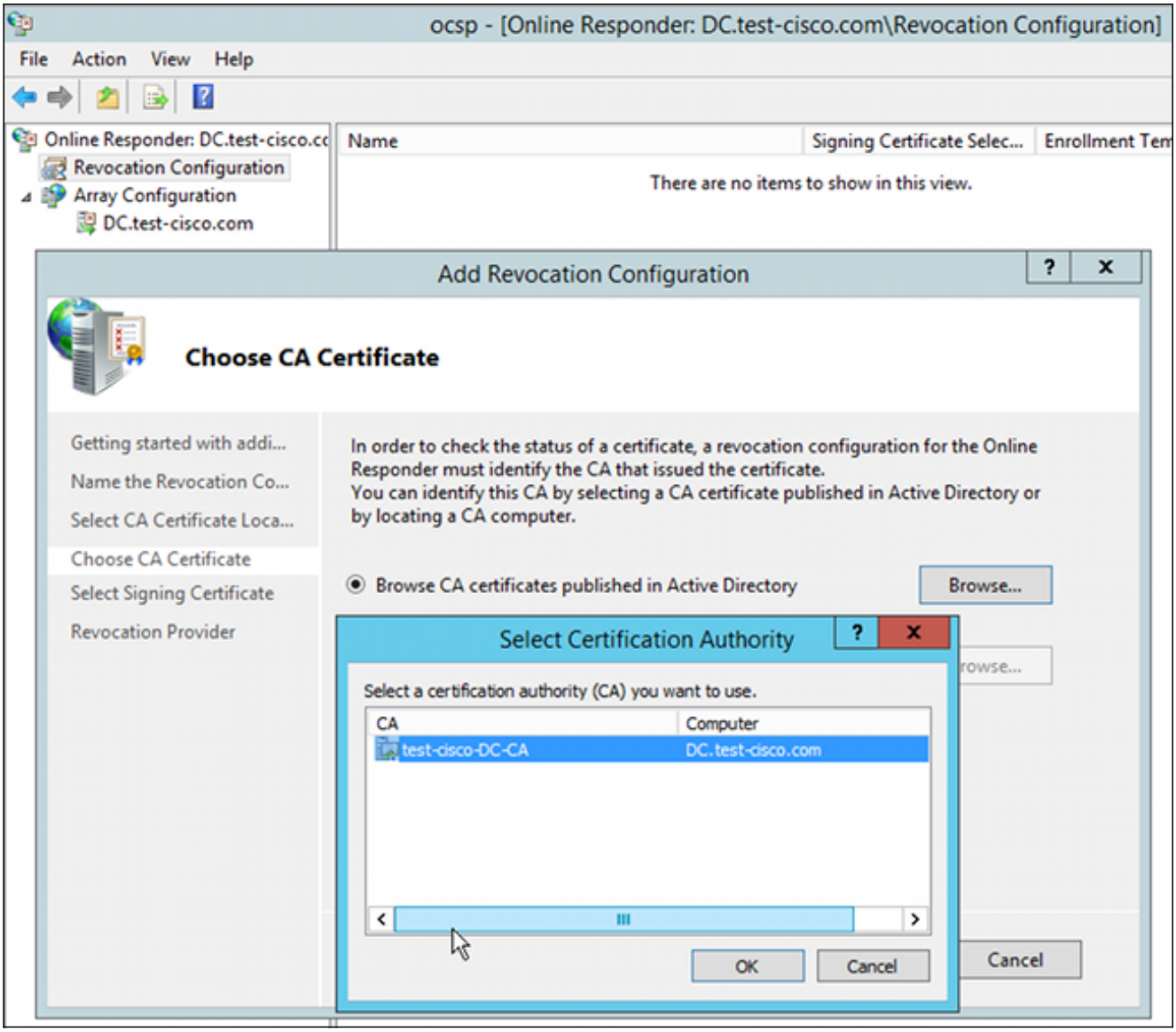


OCSP服务证书

以下过程介绍如何使用在线配置管理来配置OCSP:

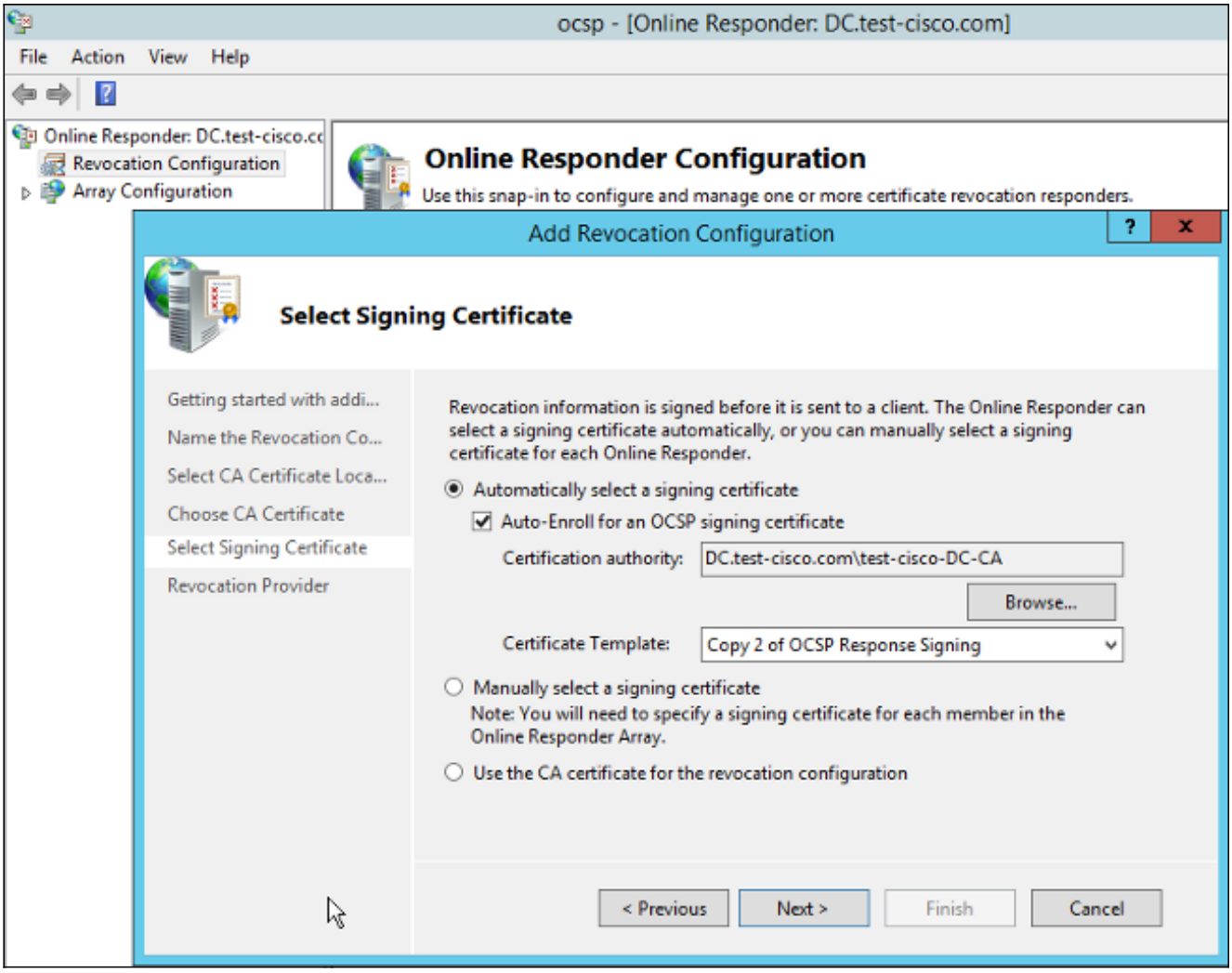
1. 导航到**服务器管理器 > 工具**。

2. 导航到**撤销配置 > 添加撤销配置**以添加新配置：

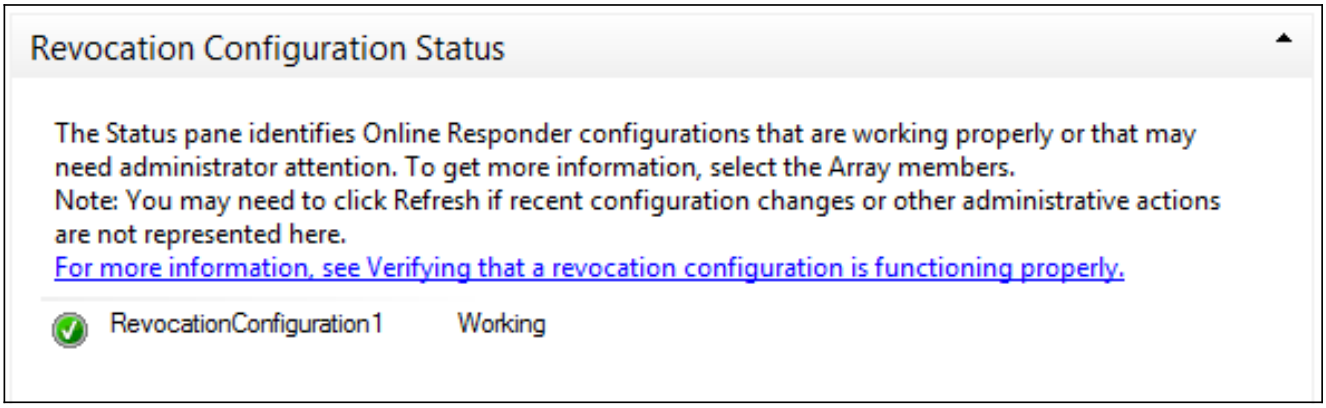


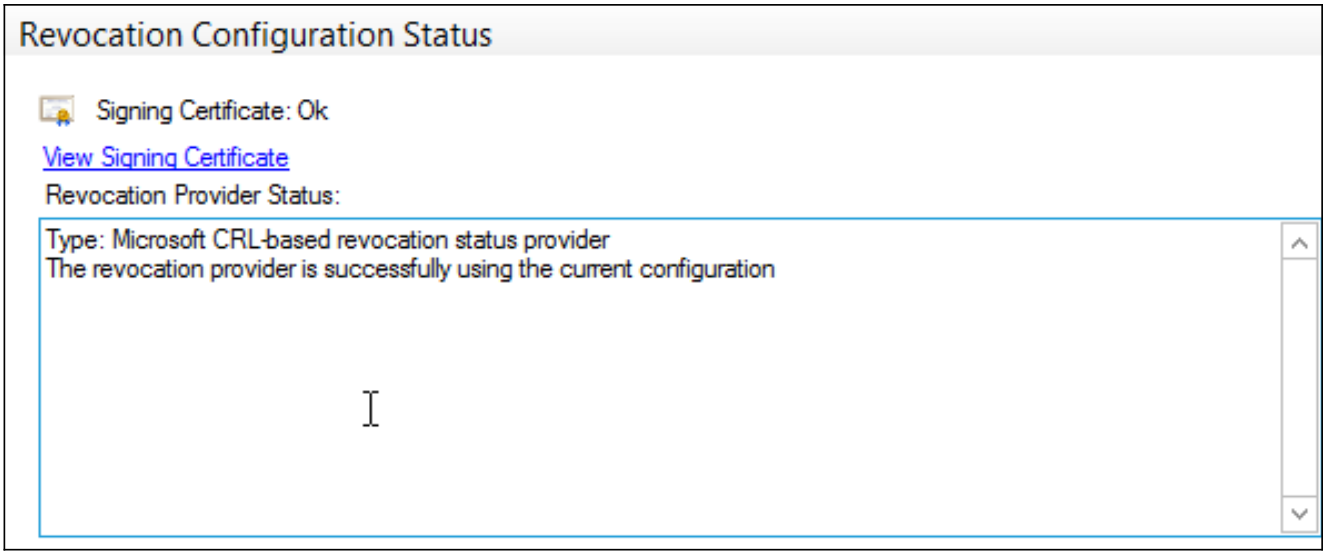
OCSP可以使用相同的企业CA。生成OCSP服务的证书。

3. 使用选定的企业CA，并选择之前创建的模板。自动注册证书：

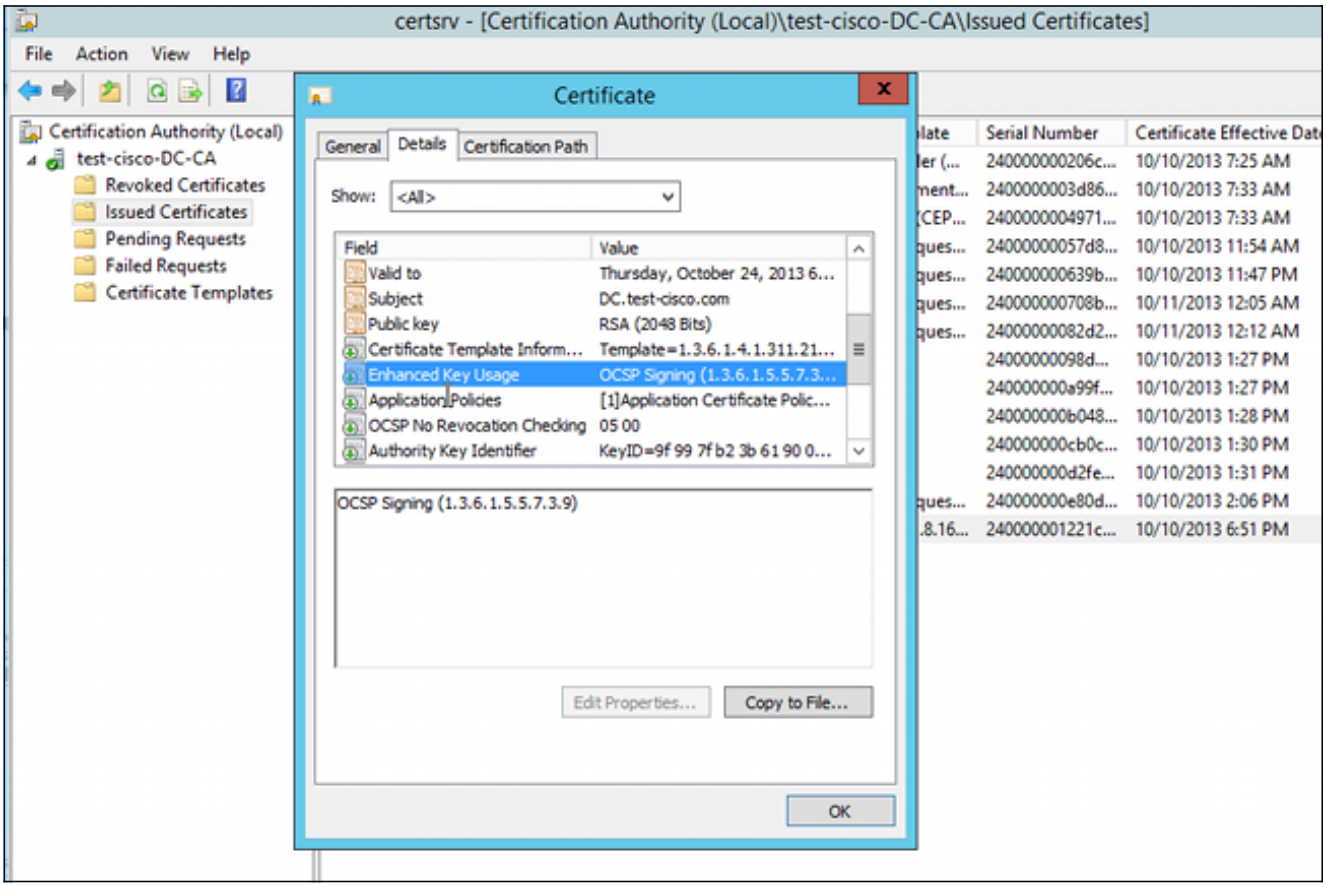


4. 确认证书已注册，其状态为Working/OK:





5. 导航到**CA > Issued Certificates**以验证证书详细信息：



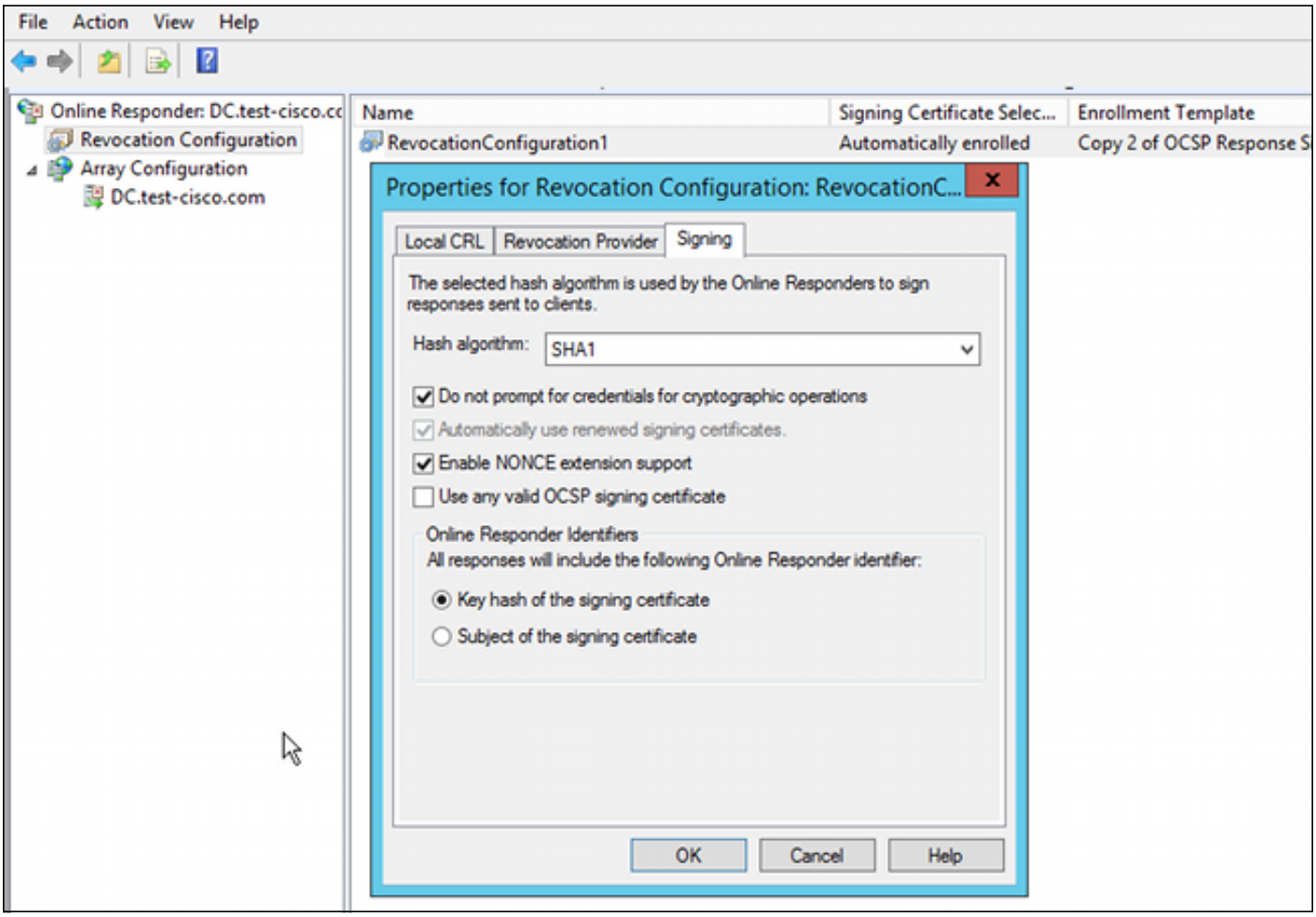
OCSP服务非计数

OCSP的Microsoft实施符合[RFC 5019 The Lightweight Online Certificate Status Protocol(OCSP)Profile for High-Volume Environments](适用于大容量环境的轻型在线证书状态协议(OCSP)配置文件)，这是[RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP的简化版本]。

ASA对OCSP使用RFC 2560。这两个RFC的区别之一是RFC 5019不接受ASA发送的签名请求。

可以强制Microsoft OCSP服务接受这些已签名的请求并使用正确的已签名的响应进行回复。导航到**Revocation Configuration > RevocationConfiguration1 > Edit Properties**，然后选择**Enable NONCE**

extension support的选项。



OCSP服务现在可以使用。

虽然Cisco不建议这样做，但是可以在ASA上禁用nonce:

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

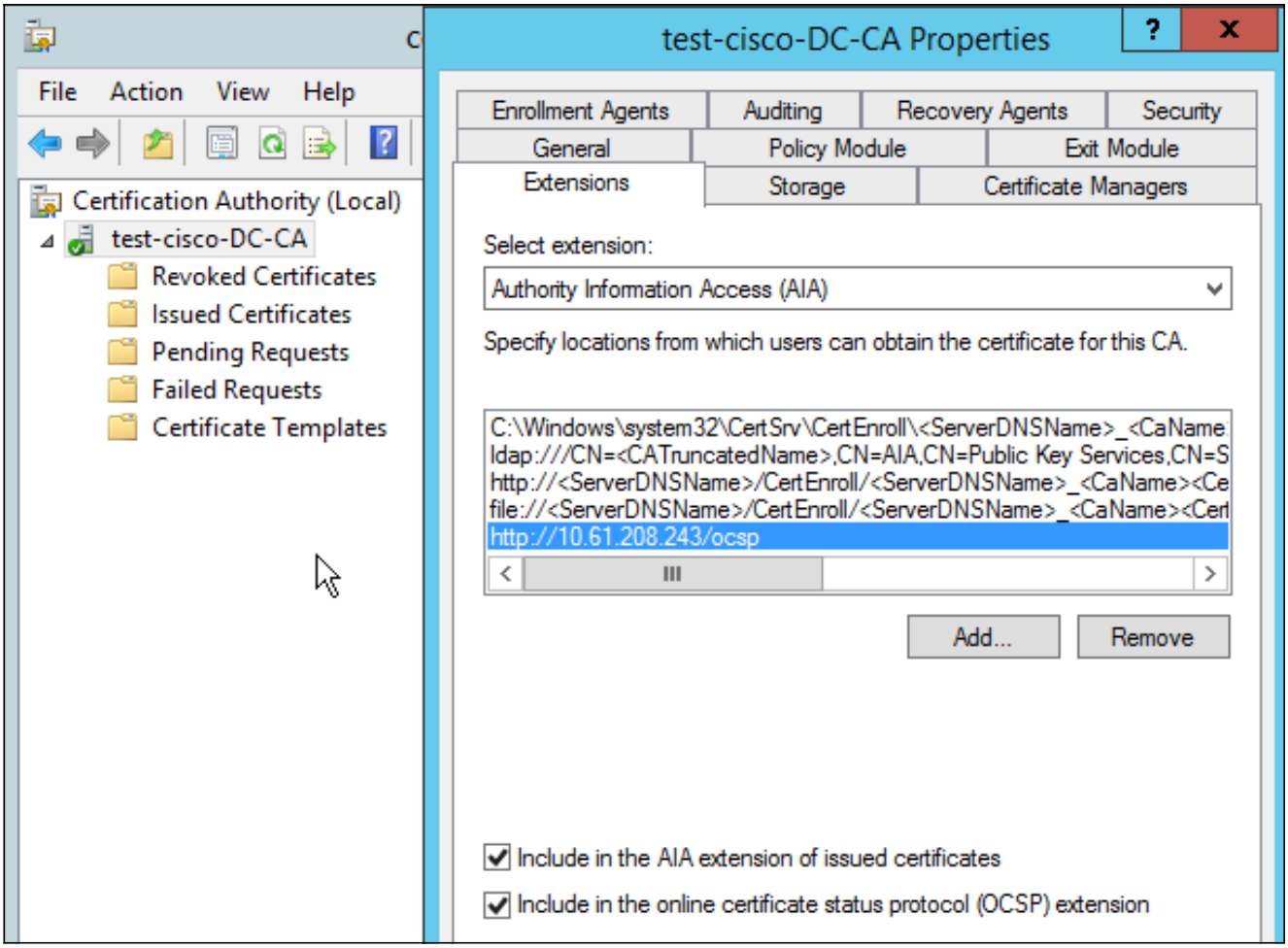
OCSP扩展的CA配置

现在必须重新配置CA，以便将OCSP服务器扩展包含在所有已颁发的证书中。ASA使用该扩展名中的URL以在验证证书时连接到OCSP服务器。

1. 在CA上打开服务器的“属性”对话框。

2. 单击**Extensions**选项卡。需要指向OCSP服务的授权信息访问(AIA)扩展；在本例中，它是http://10.61.208.243/ocsp。为AIA扩展启用以下两个选项：

   包括在已颁发证书的AIA扩展中包括在在线证书状态协议(OCSP)扩展中



这可确保所有已颁发的证书具有指向OCSP服务的正确分机。

OpenSSL

注意：有关通过CLI配置ASA的详细信息，请参阅[使用CLI、8.4和8.6配置外部服务器以进行安全设备用户授权的思科ASA 5500系列配置指南]。

本示例假设已配置OpenSSL服务器。本节仅介绍OCSP配置和CA配置所需的更改。

此过程介绍如何生成OCSP证书：

1. OCSP响应器需要以下参数：

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

2. 用户证书需要以下参数：

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

3. 证书需要由CA生成并签名。

4. 启动OCSP服务器：

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

5. 测试示例证书：

```
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网站上找到。

与ASA一样，OpenSSL支持OCSP非ce；可以使用 — nonce和 — no_nonce开关控制nonce。

具有多个OCSP源的ASA

ASA可以覆盖OCSP URL。即使客户端证书包含OCSP URL，它也会被ASA上的配置覆盖：

```
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
```

可以显式定义OCSP服务器地址。此命令示例匹配主题名称中管理员的所有证书，使用OPENSSL信任点验证OCSP签名，并使用http://11.11.11.11/ocsp的URL发送请求：

```
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
```

用于查找OCSP URL的顺序为：

1. 使用**match certificate**命令设置的OCSP服务器
2. 使用**ocsp url**命令设置的OCSP服务器
3. 客户端证书的AIA字段中的OCSP服务器

由不同CA签名的ASA with OCSP

OCSP响应可以由其他CA签名。在这种情况下，需要使用**match certificate**命令才能在ASA上使用不同的信任点进行OCSP证书验证。

```
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
```

在本例中，ASA使用包含管理员的使用者名称的所有证书的OCSP URL重写。ASA被迫根据另一个信任点OPENSSL验证OCSP响应器证书。用户证书仍在WIN2012信任点中验证。

由于OCSP响应器证书具有“OCSP no revocation checking”扩展名，因此即使在OCSP强制根据OPENSSL信任点进行验证时，也不会验证证书。

默认情况下，当ASA尝试验证用户证书时，将搜索所有信任点。OCSP响应器证书的验证不同。ASA仅搜索已找到的信任点用户证书（本示例中为WIN2012）。

因此，必须使用**match certificate**命令强制ASA使用不同的信任点进行OCSP证书验证（本示例中为OPENSSL）。

根据第一个匹配的信任点（本例中为WIN2012）验证用户证书，然后确定用于OCSP响应器验证的默认信任点。

如果**match certificate**命令中未提供特定信任点，则会根据与用户证书相同的信任点验证OCSP证书（本示例中为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
```

验证

使用本部分可确认配置能否正常运行。

> **注意**:Output Interpreter Tool(仅注册客户)支持某些**show**命令。使用输出解释器工具来查看show 命令输出的分析。

ASA — 通过SCEP获取证书

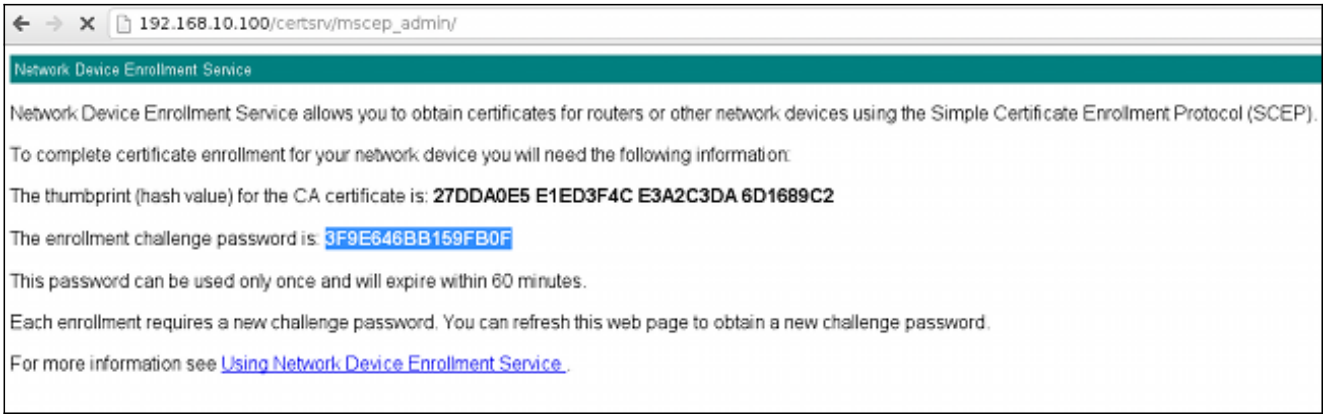
此过程介绍如何使用SCEP获取证书：

1. 这是用于获取CA证书的信任点身份验证过程：

```
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. 要请求证书，ASA需要具备可从管理员控制台(http://IP/certsrv/mscep_admin)获取的一次性SCEP密码：



3. 使用该密码在ASA上请求证书：

```
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
```

为清楚起见，省略了部分输出。

4. 验证CA和ASA证书：

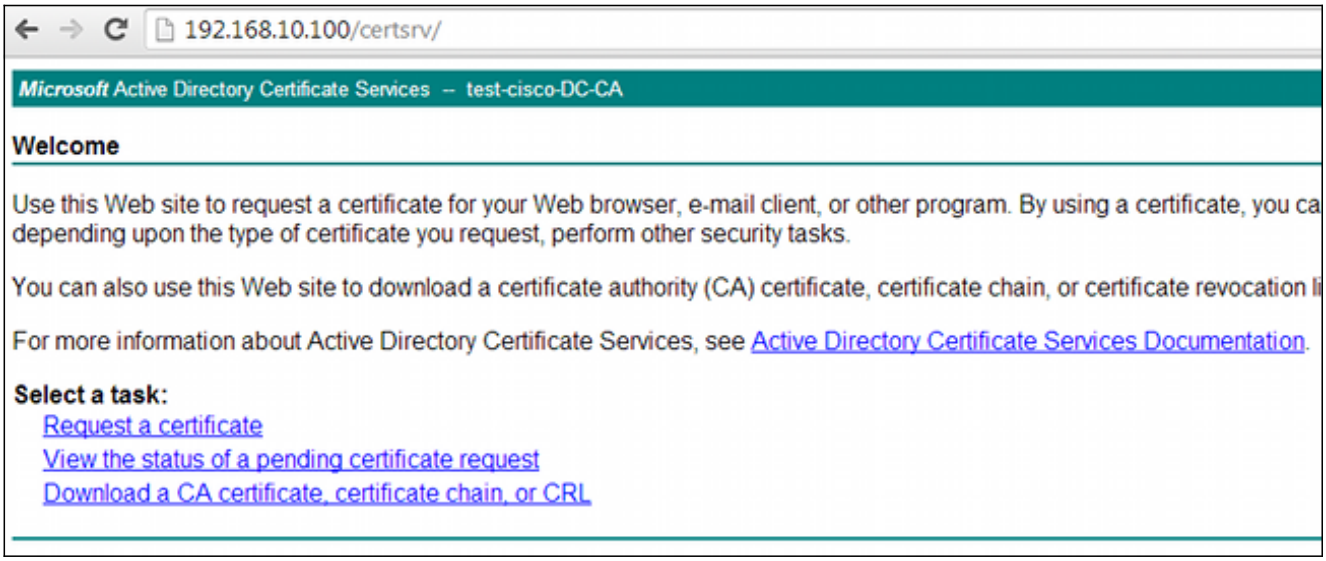
```
BSNS-ASA5510-3(config)# show crypto ca certificates
Certificate
 Status: Available
 Certificate Serial Number: 240000001cbf2fc89f44fe819700000000001c
 Certificate Usage: General Purpose
 Public Key Type: RSA (1024 bits)
 Signature Algorithm: SHA1 with RSA Encryption
 Issuer Name:
   cn=test-cisco-DC-CA
   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不显示大多数证书扩展。即使ASA证书包含“AIA中的OCSP URL”扩展，ASA CLI也不提供该扩展。Cisco Bug ID CSCui44335“ASA ENH Certificate x509 extensions displayed”（显示ASA增强型证书x509扩展）请求此增强功能。

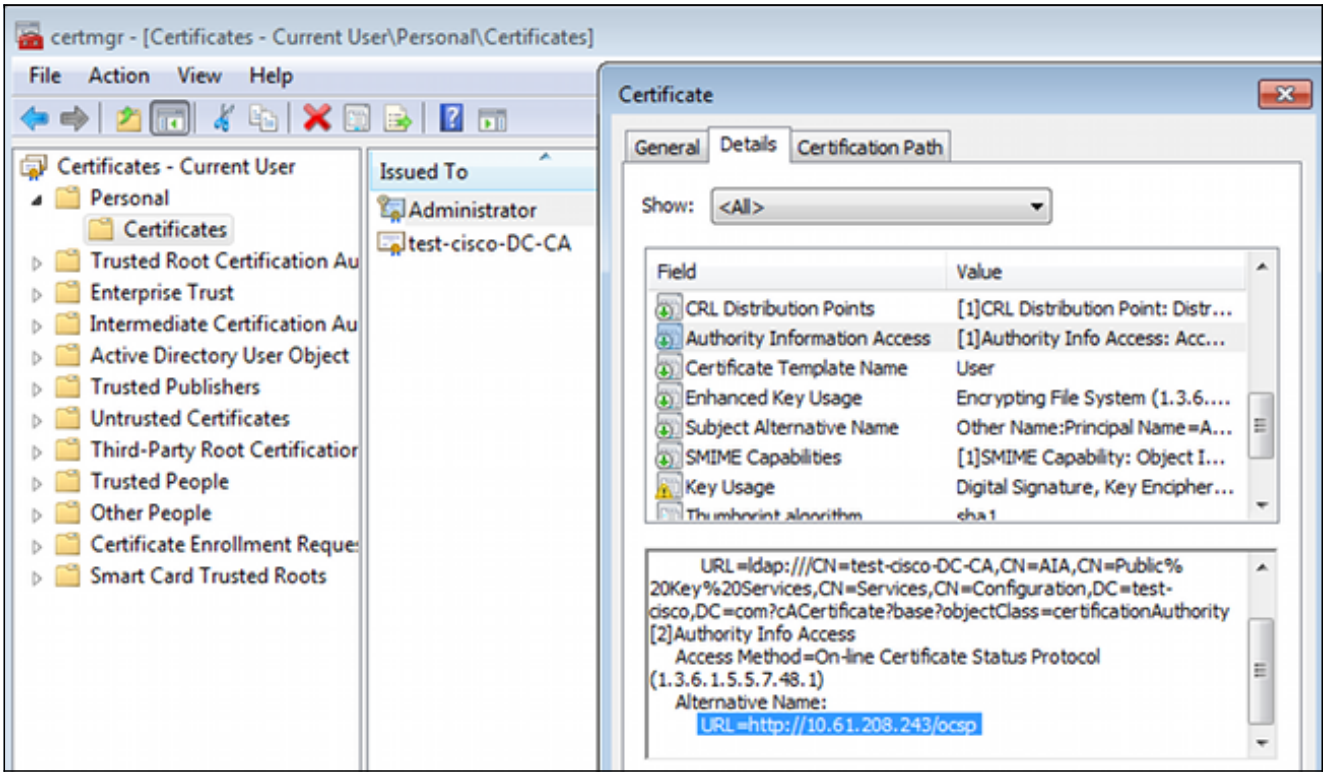
AnyConnect — 通过网页获取证书

以下过程介绍如何使用客户端上的Web浏览器获取证书：

1. 可以通过网页请求AnyConnect用户证书。在客户端PC上，使用Web浏览器转到CA，地址为http://*IP*/certsrv:



2. 用户证书可以保存在Web浏览器存储中，然后导出到Microsoft存储中，AnyConnect会搜索该存储区。使用certmgr.msc验证收到的证书：



只要有正确的AnyConnect配置文件，AnyConnect也可以请求证书。

带OCSP验证的ASA VPN远程访问

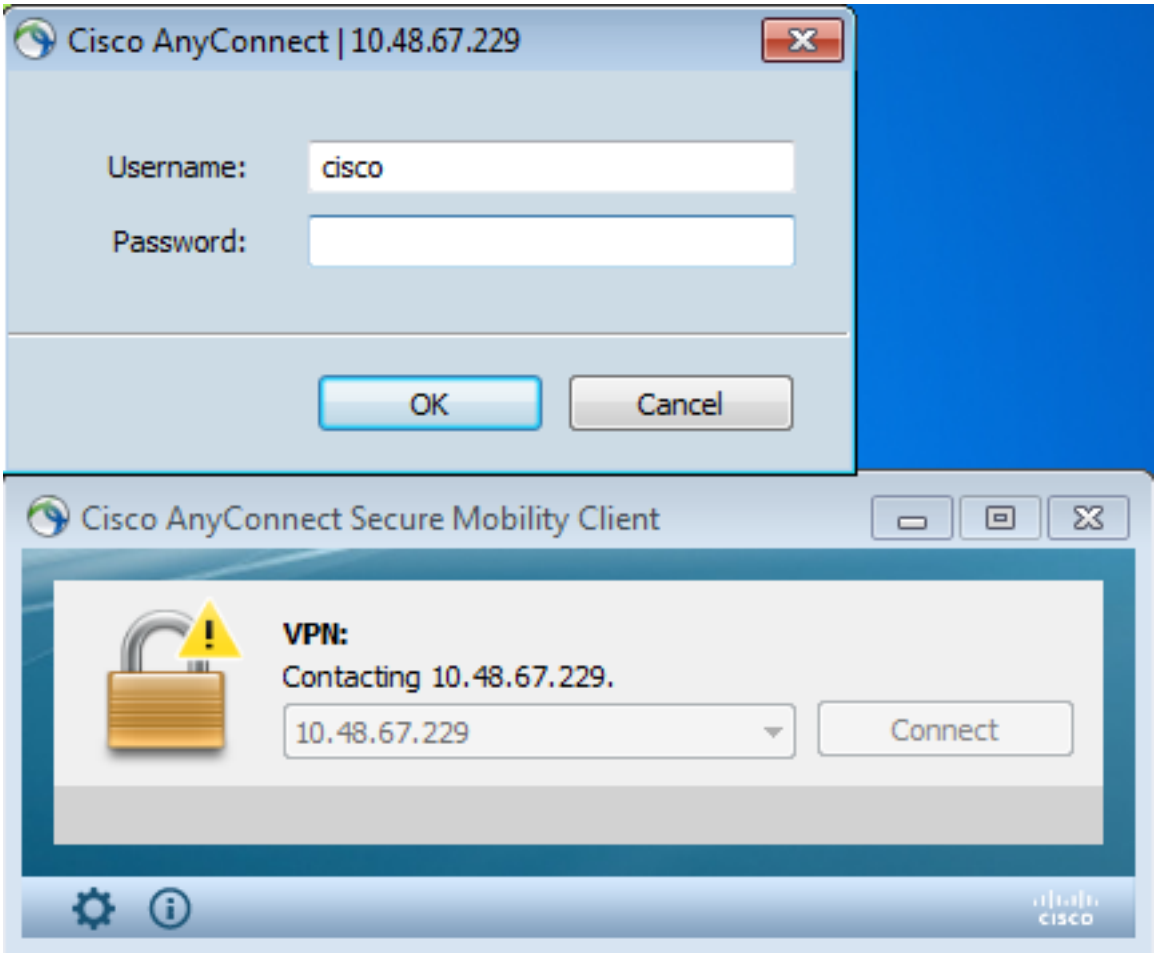
此过程介绍如何检查OCSP验证：

1. 在尝试连接时，ASA报告正在检查证书的OCSP。此处，OCSP签名证书具有无检查扩展名，且未通过OCSP检查：

```
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.
```

为清楚起见，省略了部分输出。

2. 最终用户提供用户凭证：



3. VPN会话已正确完成：

```
%ASA-7-717036: Looking for a tunnel group match based on certificate maps
for peer certificate with serial number:
240000001B2AD208B12811687400000000001B, 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: 240000001B2AD208B12811687400000000001B,
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. 会话创建成功：

```
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
```

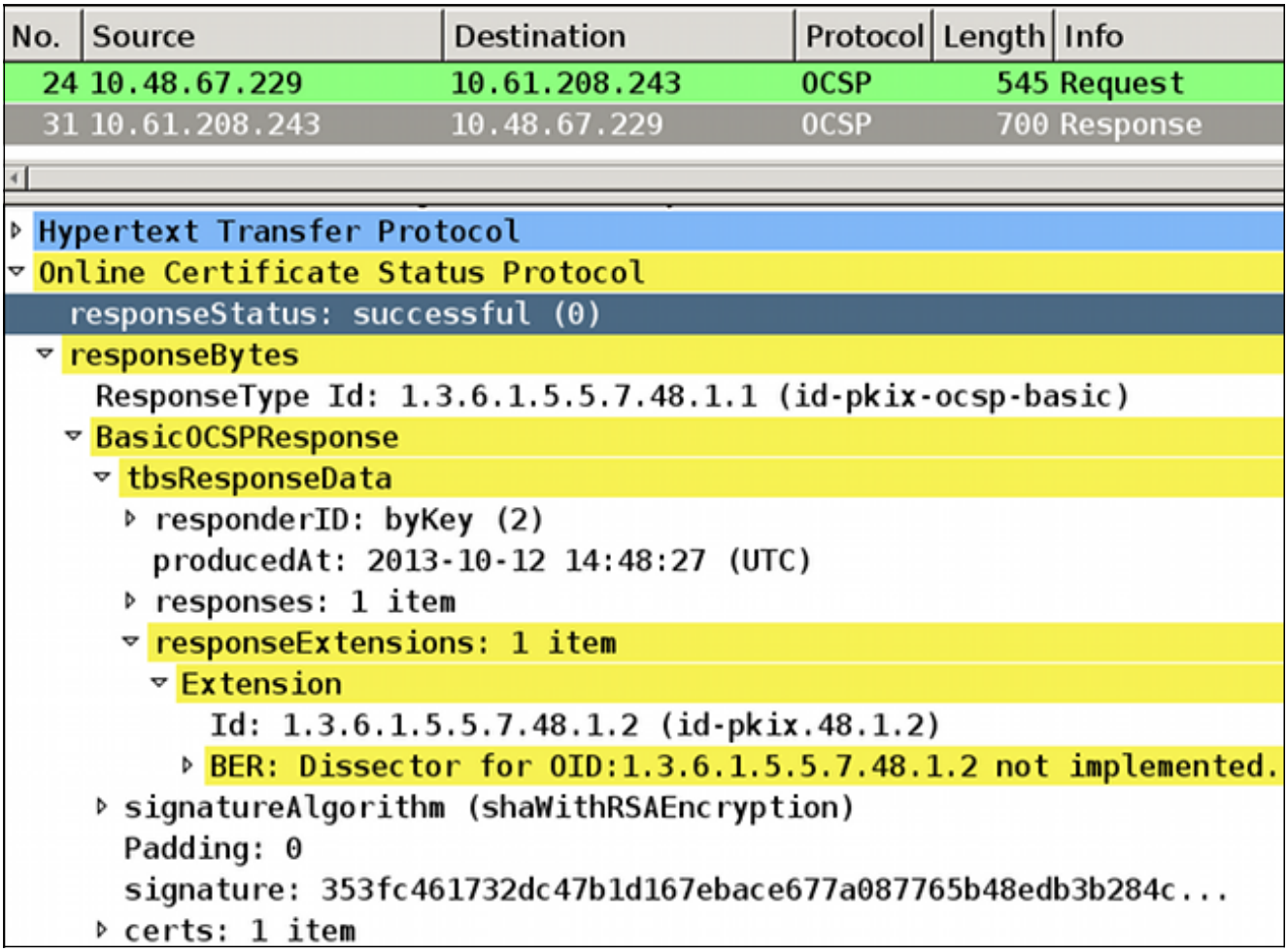
```
 Encryption   : RC4                    Hashing      : SHA1
 Encapsulation: TLSv1.0                TCP Src Port : 51406
 TCP Dst Port : 443                    Auth Mode    : Certificate and
userPassword
 Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
 Client OS    : Windows
 Client 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. 您可以使用详细调试进行OCSP验证：

```
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. 在数据包捕获级别，这是OCSP请求和正确的OCSP响应。响应包含在Microsoft OCSP上启用的正确签名 — nonce扩展：



具有多个OCSP源的ASA VPN远程访问

如果根据ASA with Multiple OCSP Sources中的说明配置匹配证书，则优先使用：

```
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
```

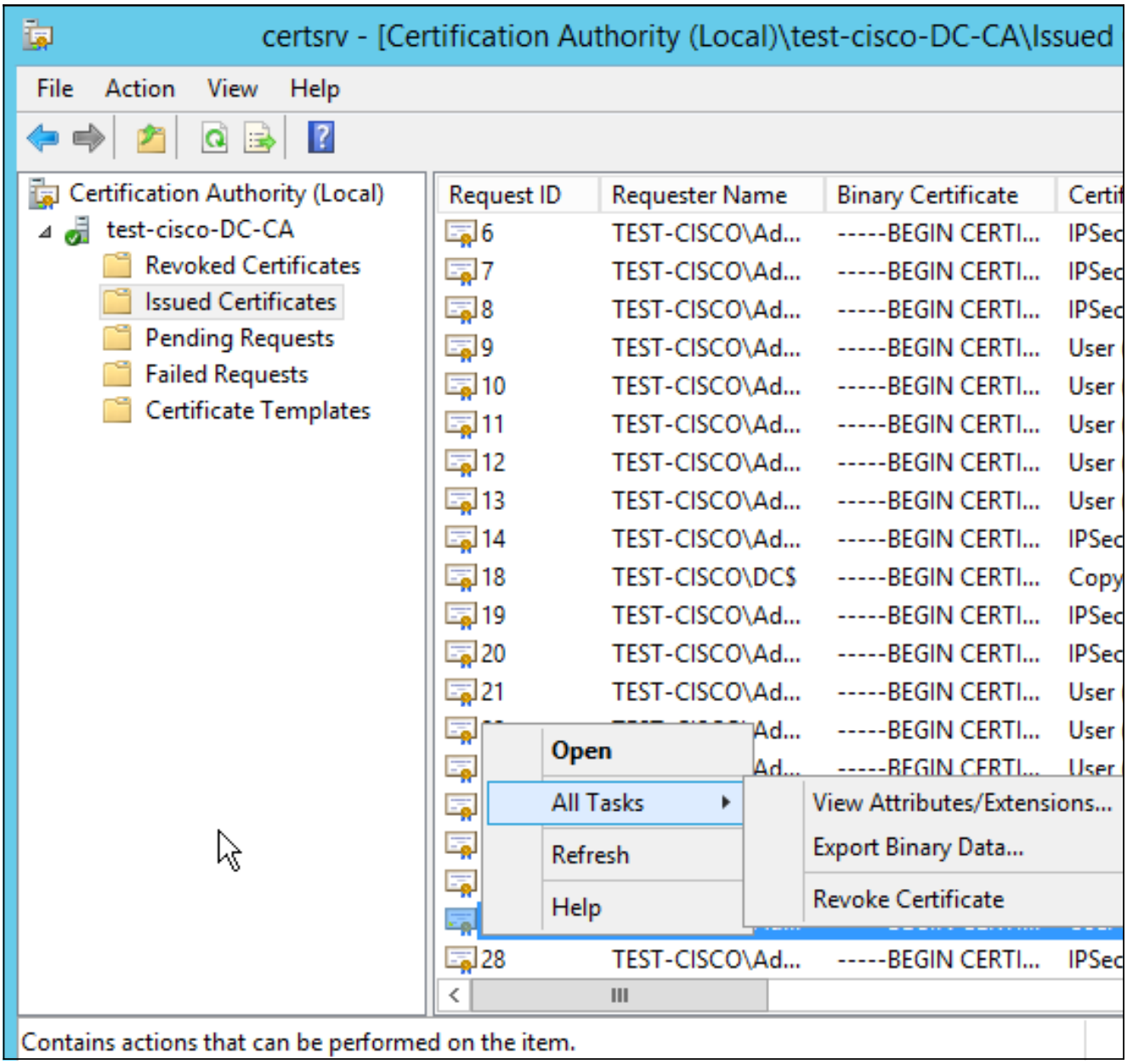
当使用OCSP URL覆盖时，调试为：

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

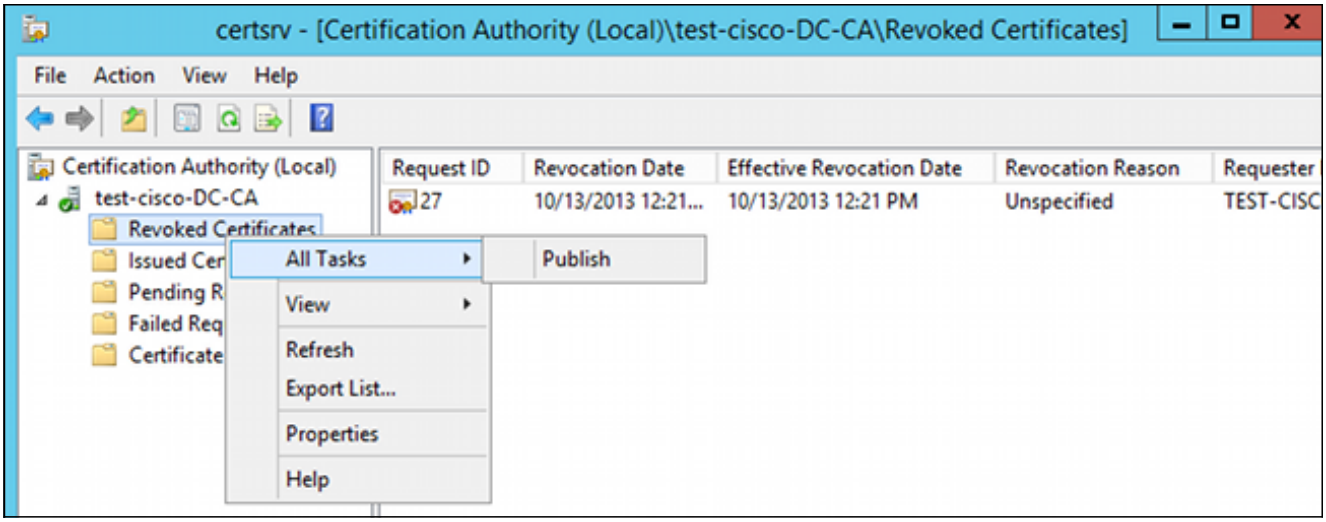
具有OCSP和已撤销证书的ASA VPN远程访问

此过程介绍如何撤销证书和确认撤销状态：

1. 撤销客户端证书：



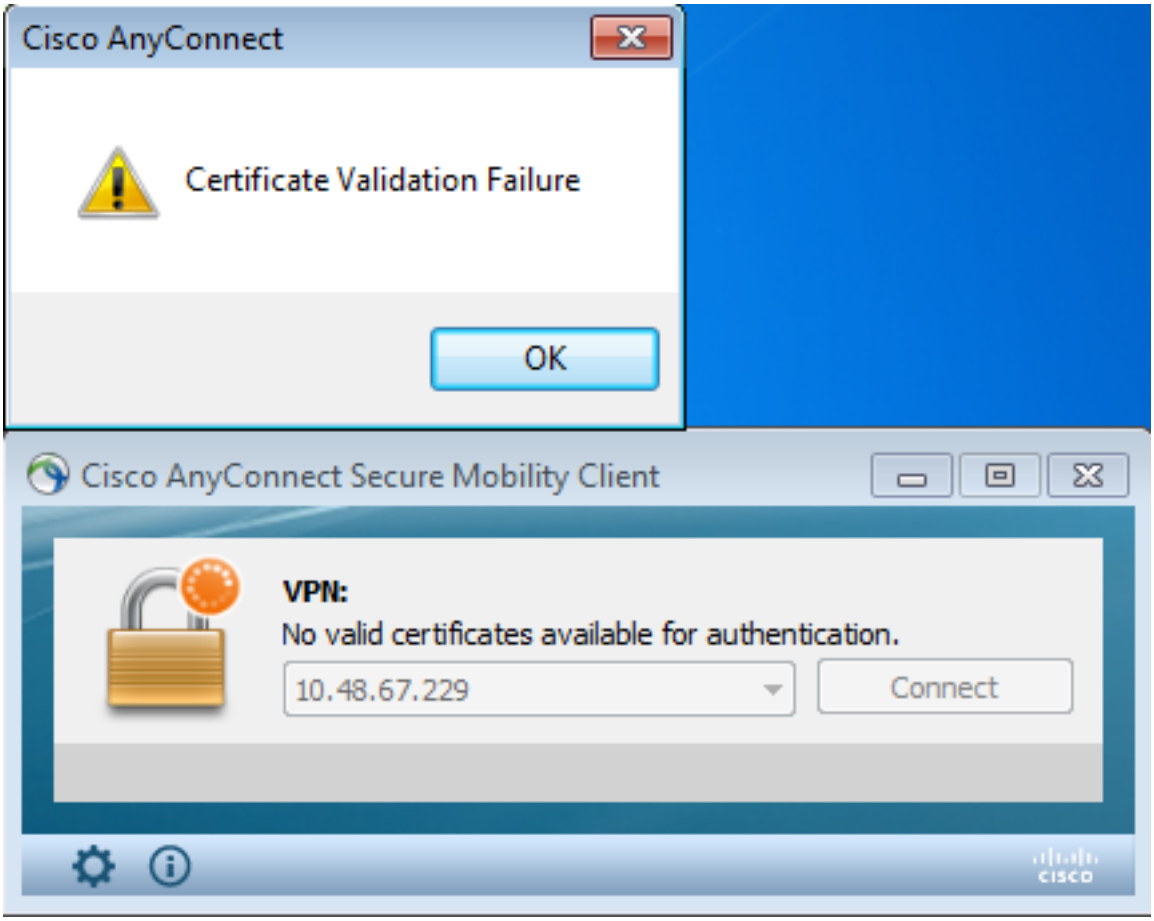
2. 发布结果：



3. [可选]步骤1和2也可以通过Power Shell中的certutil CLI实用程序来完成：

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

4. 当客户端尝试连接时，出现证书验证错误：



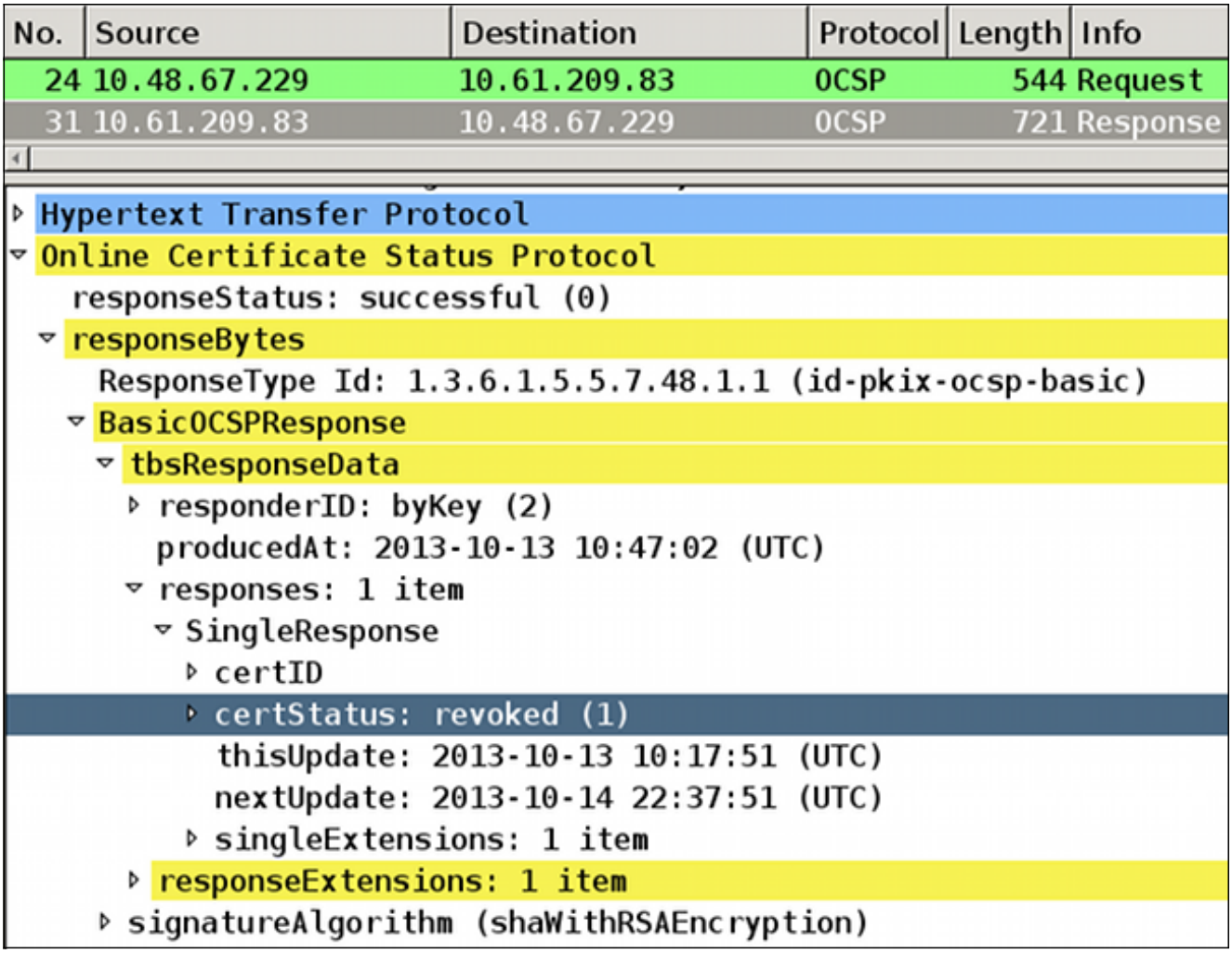
5. AnyConnect日志还指示证书验证错误：

```
[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报告证书状态已撤销：

```
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: 240000001B2AD208B12811687400000000001B, 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. 数据包捕获显示一个成功的OCSP响应，证书状态为revoked:



故障排除

本部分提供的信息可用于对配置进行故障排除。

OCSP服务器关闭

ASA报告OCSP服务器关闭的时间：

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

数据包捕获还可帮助进行故障排除。

时间不同步

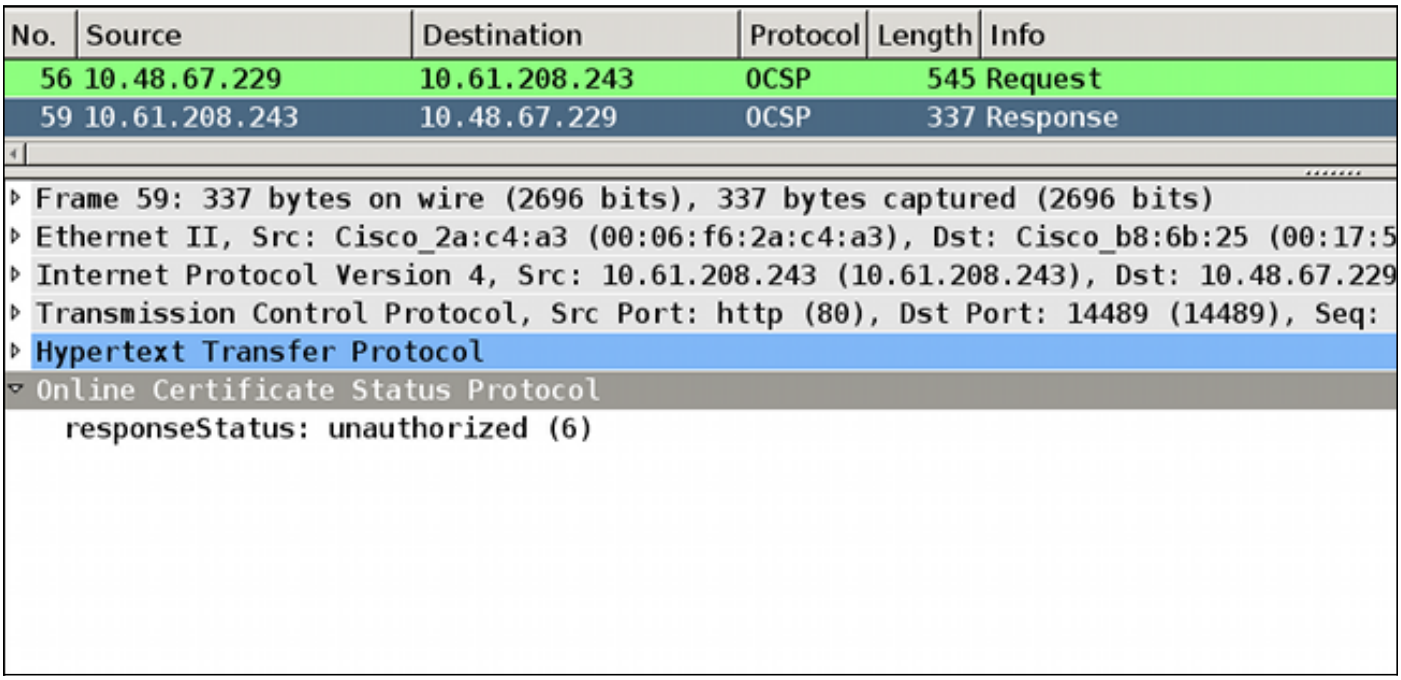
如果OCSP服务器上的当前时间早于ASA上的时间（可以接受较小的差异），则OCSP服务器会发送未经授权的响应，ASA会报告该响应：

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

当ASA收到来自未来时间的OCSP响应时，也会发生故障。

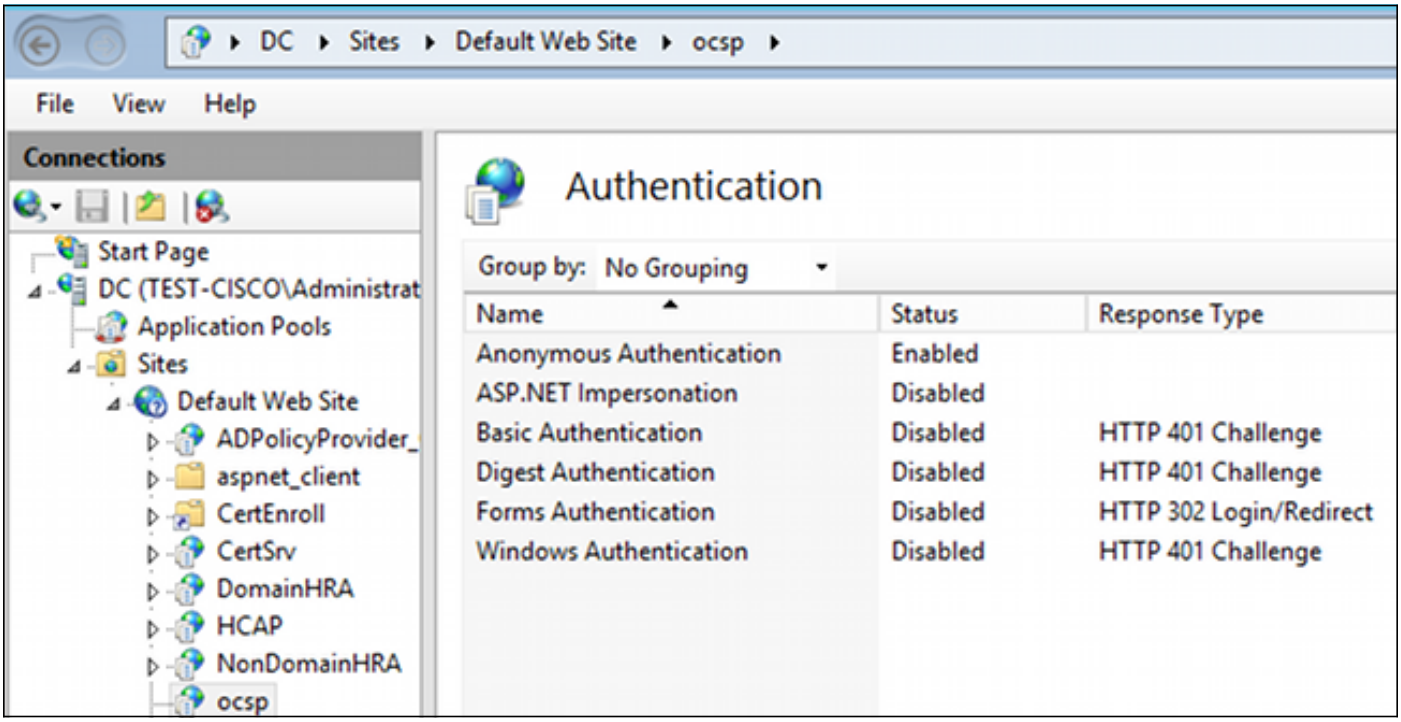
不支持签名的Nonce

如果服务器上的nonce不受支持（Microsoft Windows 2012 R2上的默认设置），则会返回未经授权的响应：



IIS7服务器身份验证

SCEP/OCSP请求的问题通常是由于Internet Information Services 7(IIS7)上的身份验证不正确造成的。确保配置了匿名访问：



相关信息

- Microsoft TechNet: Online Responder安装、配置和故障排除指南
- Microsoft TechNet：配置CA以支持OCSP响应器
- Cisco ASA系列命令参考
- 技术支持和文档 - Cisco Systems

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。