شبكة VPN للوصول عن بعد ASA مع التحقق من OCSP بموجب Microsoft Windows 2012 و OpenSSL

المحتويات

المقدمة

يوضح هذا المستند كيفية إستخدام التحقق من صحة بروتوكول حالة الشهادة عبر الإنترنت (OCSP) على جهاز الأمان القابل للتكيف (ASA) من Cisco للشهادات المقدمة من قبل مستخدمي شبكة VPN. يتم تقديم مثال لتكوينات خادمي

OCSP (المرجع المصدق ل CA] Microsoft Windows] و OpenSSL). يصف قسم التحقق التدفقات التفصيلية على مستوى الحزمة، ويركز قسم أستكشاف الأخطاء وإصلاحها على الأخطاء والمشاكل النموذجية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين واجهة سطر الأوامر (CLI) الخاصة بجهاز الأمان القابل للتكيف (SSL) من Cisco وتكوين طبقة مأخذ التوصيل الآمنة (SSL) VPN
- شهادات X.509
- نظام التشغيل Microsoft Windows Server
- Linux/OpenSSL

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج أجهزة الأمان المعدلة Cisco Adaptive Security Appliance، الإصدار 8.4 والإصدارات الأحدث
- Microsoft Windows 7 مع Cisco AnyConnect Secure Mobility Client، الإصدار 3.1
- نظام التشغيل Microsoft Server 2012 R2
- Linux مع OpenSSL 1.0.0j أو إصدار أحدث

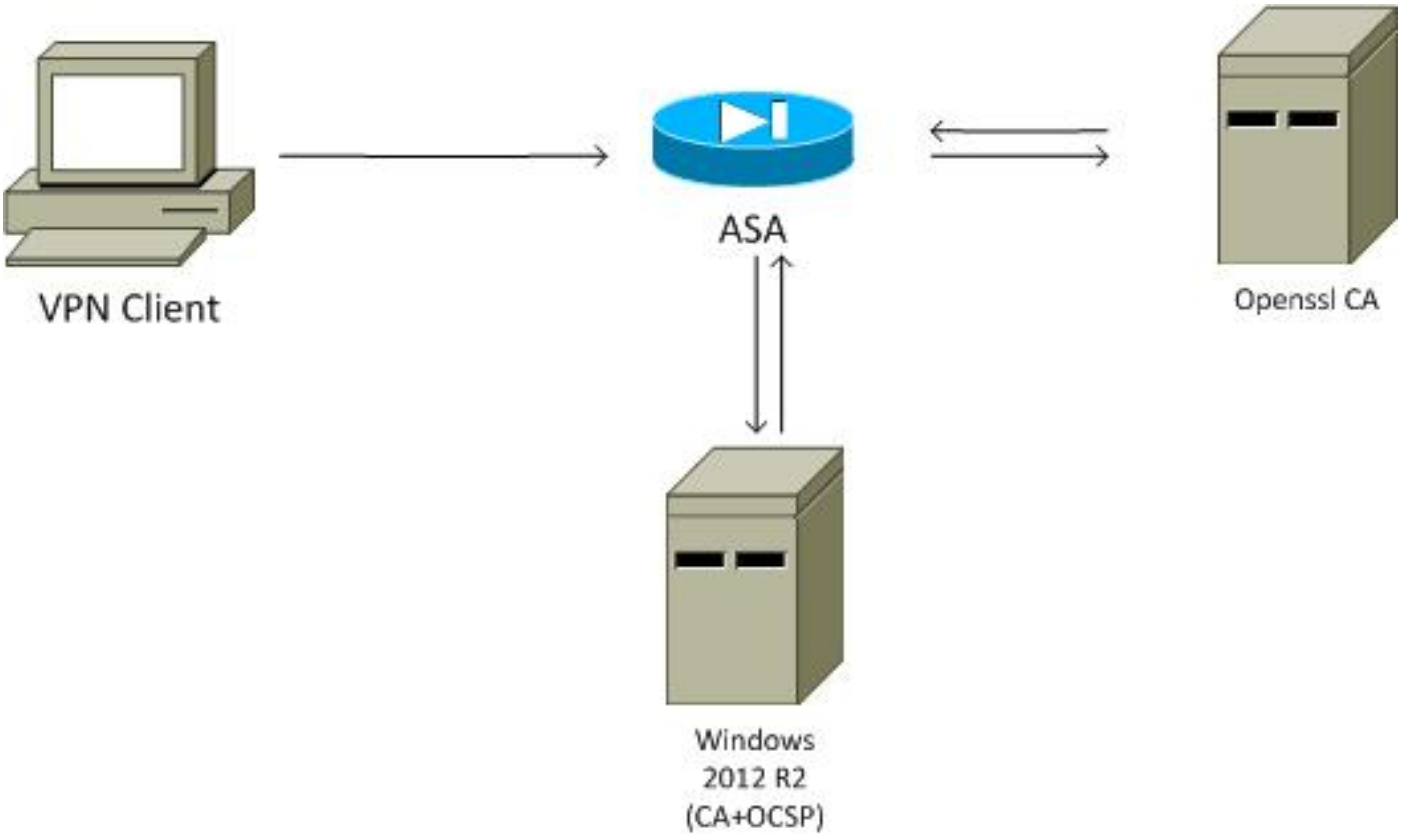
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم العميل شبكة VPN للوصول عن بعد. يمكن أن يكون هذا الوصول هو IPSec) Cisco VPN Client) أو Cisco AnyConnect Secure Mobility (SSL/Internet Key Exchange الإصدار 2 [IKEv2]]) أو WebVPN portal)). لتسجيل الدخول، يوفر العميل الشهادة الصحيحة، بالإضافة إلى اسم المستخدم/كلمة المرور التي تم تكوينها محليا على ASA. يتم التحقق من شهادة العميل عبر خادم OCSP.



الوصول عن بعد إلى ASA باستخدام OCSP

تم تكوين ASA للوصول إلى SSL. يستخدم العميل AnyConnect لتسجيل الدخول. يستخدم ASA بروتوكول تسجيل الشهادة البسيط (SCEP) لطلب الشهادة:

```
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
```

يتم إنشاء خريطة شهادات لتحديد كافة المستخدمين الذين يحتوي اسم الموضوع الخاص بهم على كلمة مسؤول (غير حساس لحالة الأحرف). هؤلاء المستخدمون موحدون بمجموعة أنفاق تحمل اسم 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
```

يتطلب تكوين الشبكة الخاصة الظاهرية (VPN) تفويضا ناجحا (أي شهادة تم التحقق من صحتها). كما يتطلب بيانات الاعتماد الصحيحة لاسم المستخدم المحدد محليا (المصادقة والتفويض والمحاسبة (AAA)):

```
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
```

نظام التشغيل Microsoft Windows 2012 CA

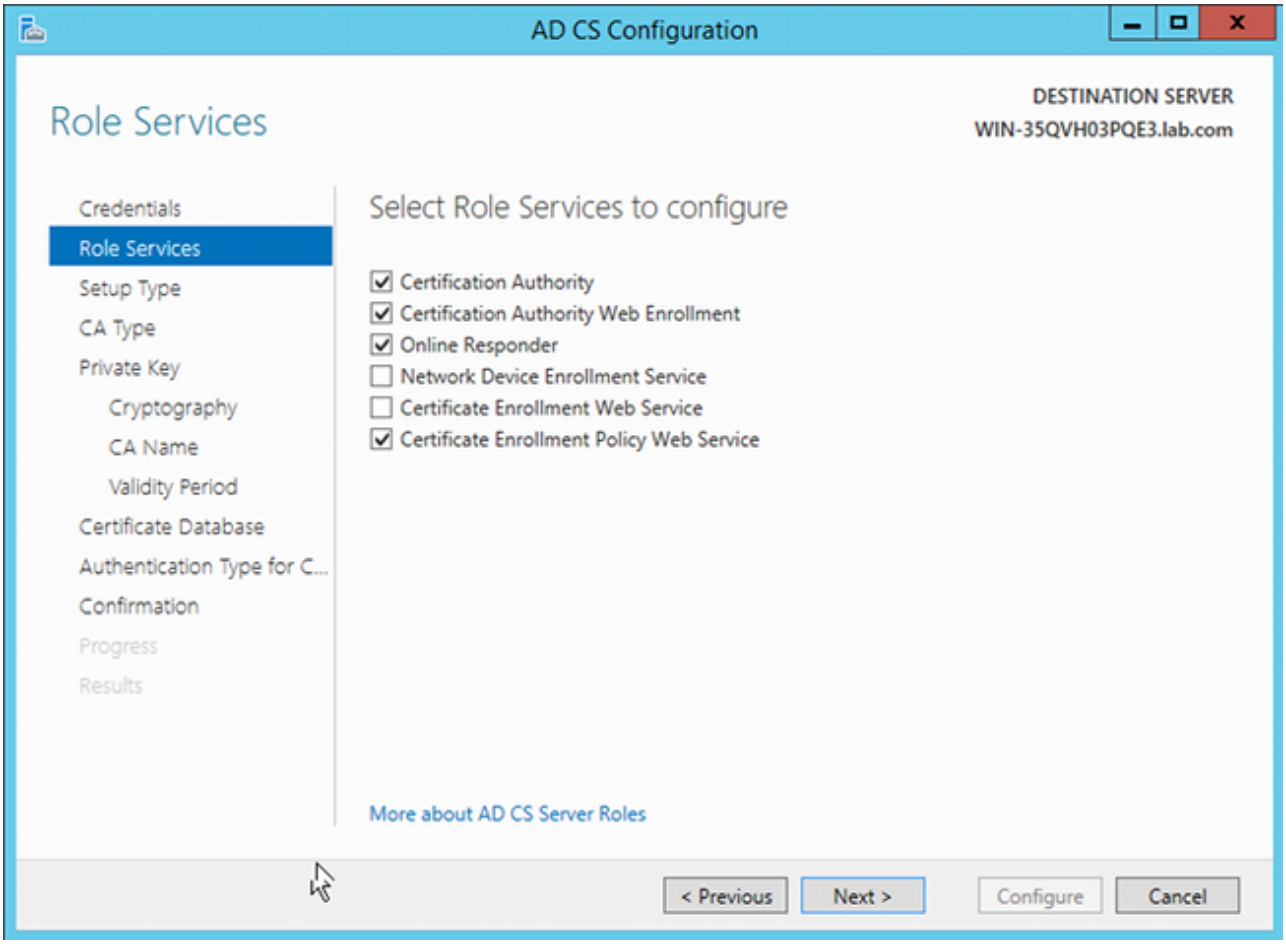
ملاحظة: راجع دليل تكوين السلسلة Cisco ASA 5500 باستخدام CLI، 8.4 و 8.6: تكوين خادم خارجي لتفويض مستخدم جهاز الأمان للحصول على تفاصيل حول تكوين ASA من خلال CLI (واجهة سطر الأوامر).

تثبيت الخدمات

يوضح هذا الإجراء كيفية تكوين خدمات الأدوار لخادم Microsoft:

1. انتقل إلى **مدير الخادم > إدارة > إضافة أدوار وميزات**. يحتاج خادم Microsoft إلى خدمات الأدوار التالية:

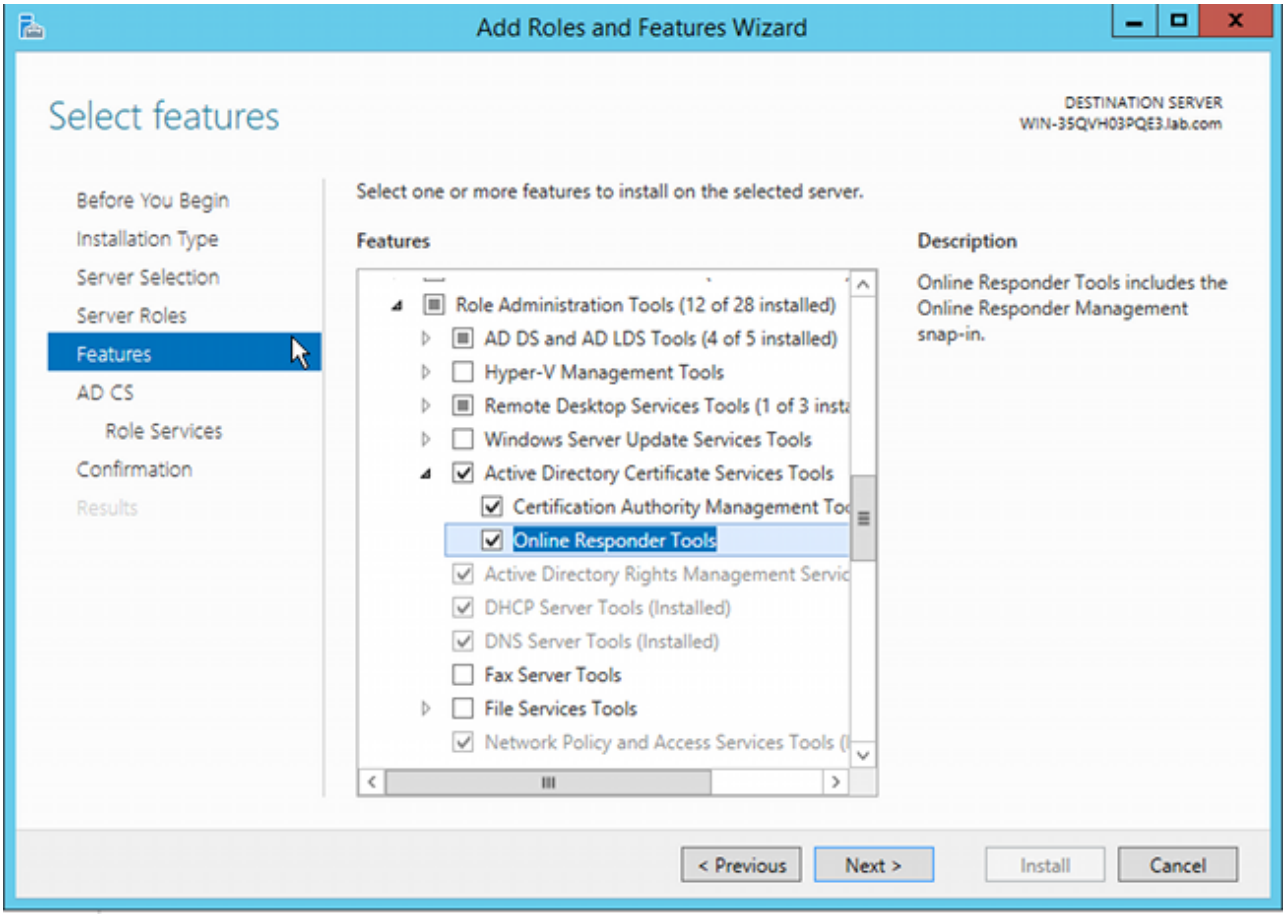
   هيئة الشهاداتتسجيل ويب ل Certificate Authority الذي يستخدمه العميلOnline Responder، المطلوب ل OCSPخدمة تسجيل جهاز الشبكة، والتي تحتوي على تطبيق SCEP المستخدم من قبل ASA يمكن إضافة خدمة ويب ذات النهج إذا لزم الأمر.



.2

.3

.4 عندما تقوم بإضافة ميزات، تأكد من تضمين "أدوات المستجيب عبر الإنترنت" لأنها تتضمن أداة OCSP إضافية يتم إستخدامها لاحقا:



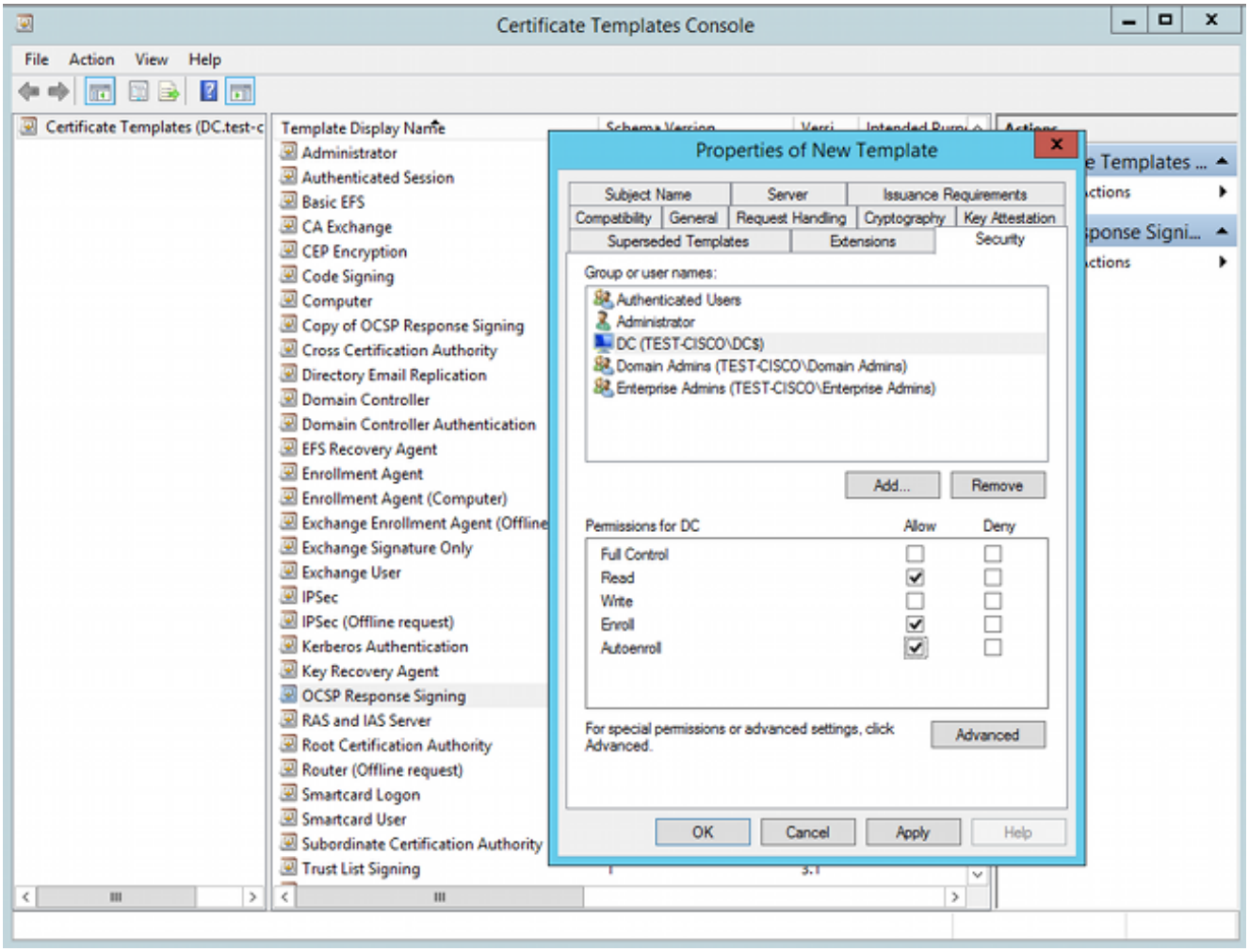
تكوين CA لقالب OCSP

تستخدم خدمة OCSP شهادة لتوقيع إستجابة OCSP. يجب إنشاء شهادة خاصة على خادم Microsoft ويجب أن تتضمن:

- إستخدام المفتاح الموسع = توقيع OCSP
- OCSP لا تدقيق إبطال

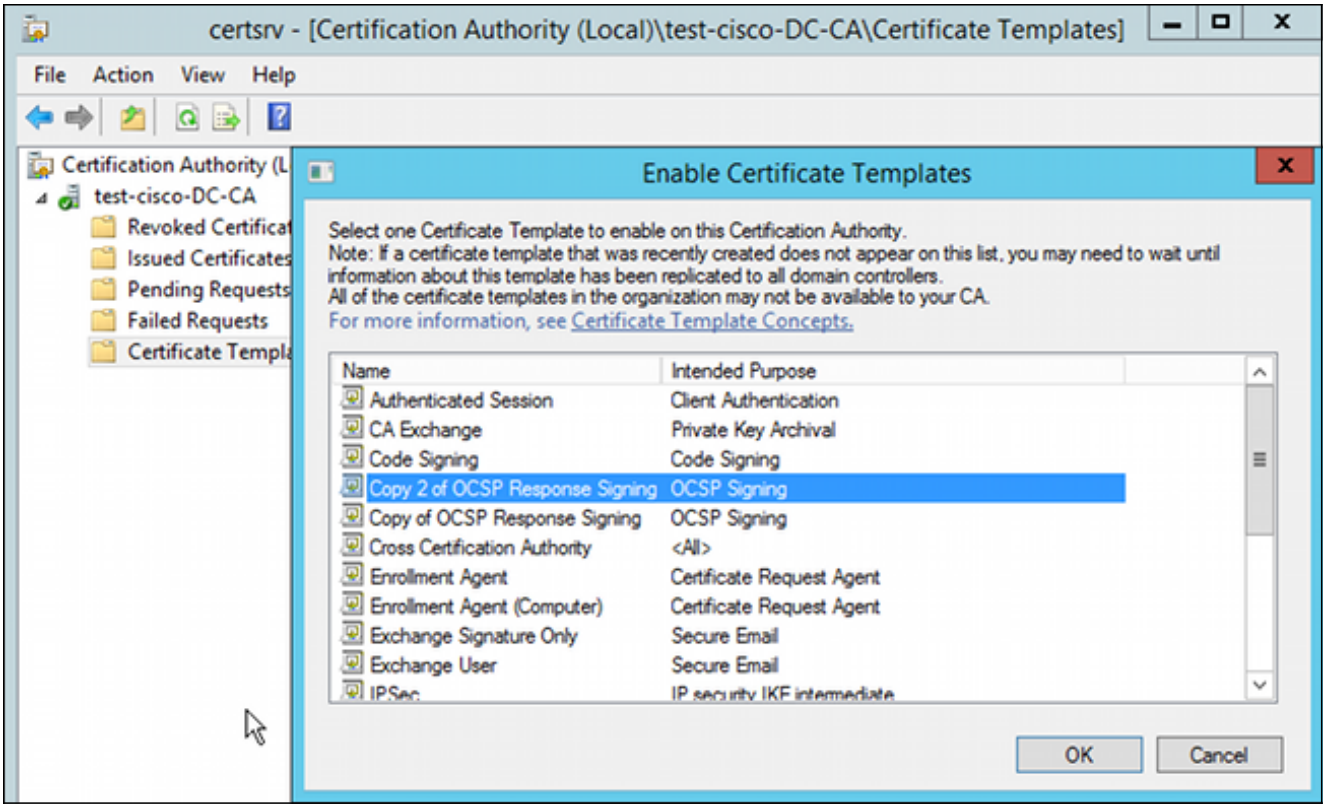
هذه الشهادة مطلوبة لمنع حلقات التحقق من صحة OCSP. لا يستخدم ASA خدمة OCSP لمحاولة التحقق من الشهادة المقدمة من خدمة OCSP.

1. إضافة قالب للشهادة على المرجع المصدق. انتقل إلى **CA > قالب الشهادة > إدارة**، حدد **توقيع إستجابة OCSP**، وقم بمضاعفة القالب. قم بعرض خصائص القالب الذي تم إنشاؤه حديثا، وانقر فوق علامة التبويب **أمان**. تصف الأذونات الكيان المسموح له بطلب شهادة تستخدم هذا القالب، لذلك يلزم توفر أذونات صحيحة. في هذا المثال، الكيان هو خدمة OCSP التي يتم تشغيلها على المضيف نفسه (TEST-CISCO\DC)، وتحتاج خدمة OCSP إلى امتيازات التسجيل التلقائي:



يمكن تعيين كافة الإعدادات الأخرى للقالب إلى الإعداد الافتراضي.

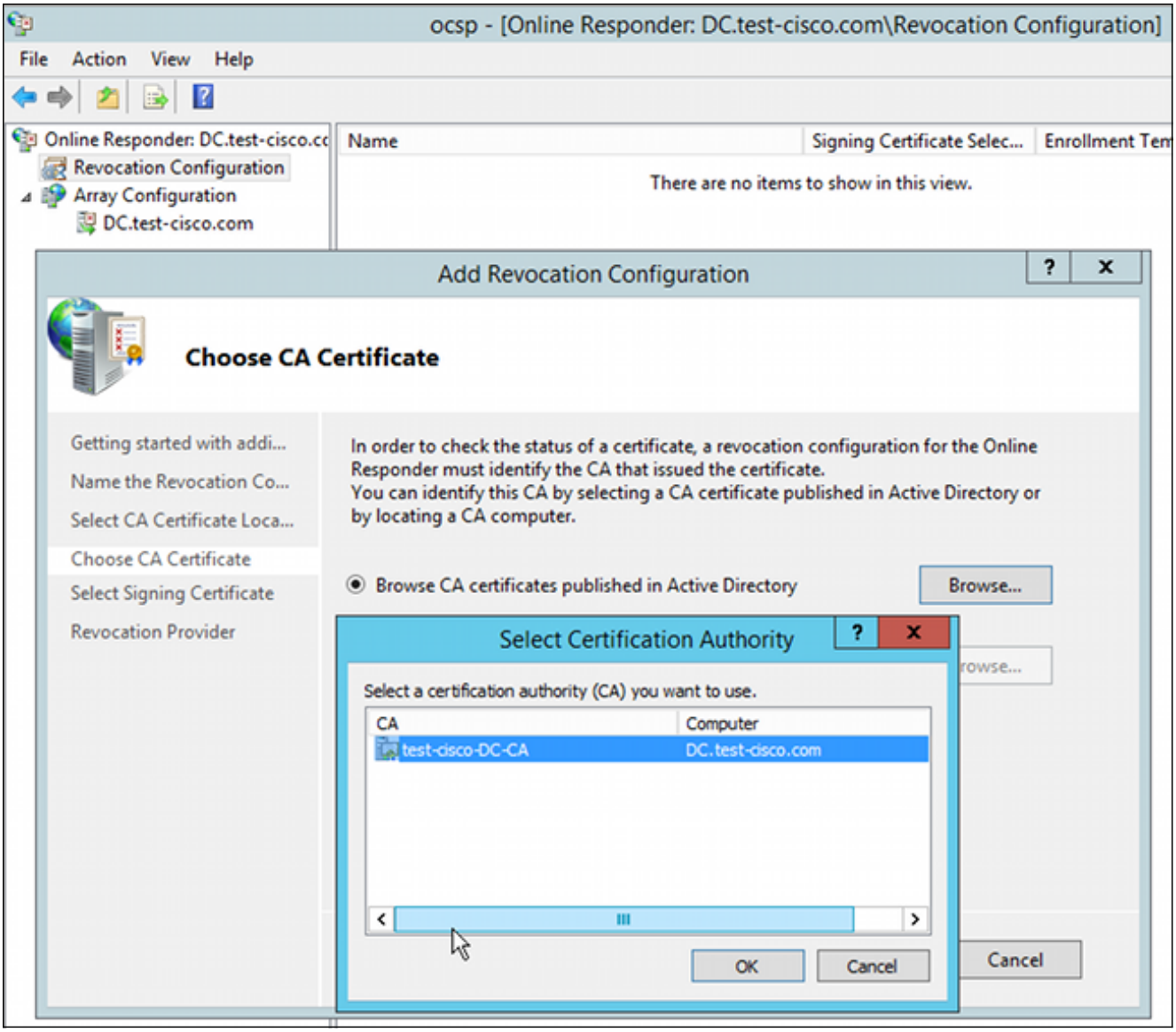
2. قم بتنشيط القالب. انتقل إلى **CA > قالب الشهادة > جديد > قالب الشهادة المراد إصداره**، ثم حدد القالب المكرر:



شهادة خدمة OCSP

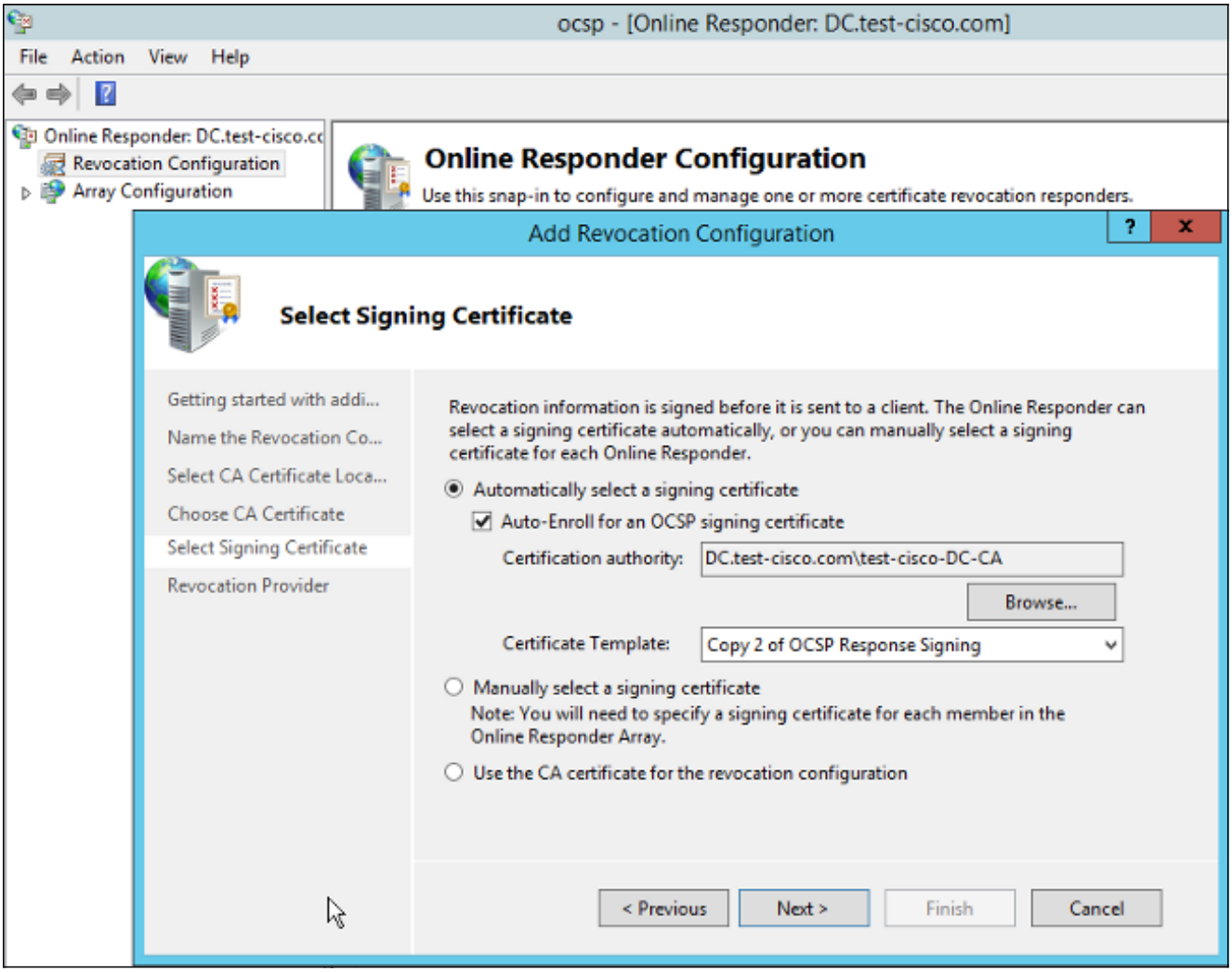
يصف هذا الإجراء كيفية إستخدام إدارة التكوين عبر الإنترنت من أجل تكوين OCSP:

1. انتقل إلى **مدير الخادم > الأدوات**.
2. انتقل إلى **تكوين الإبطال > إضافة تكوين الإبطال** لإضافة تكوين جديد:

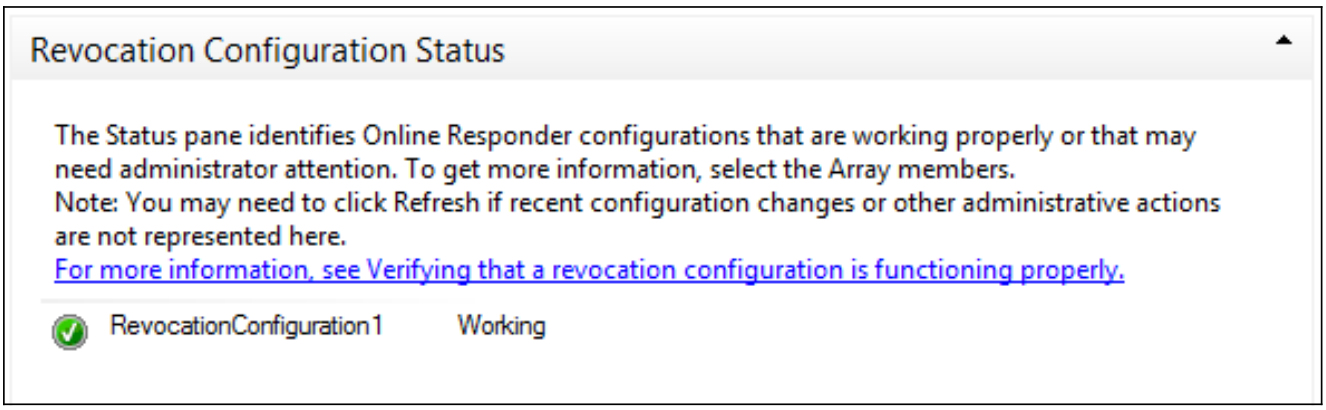


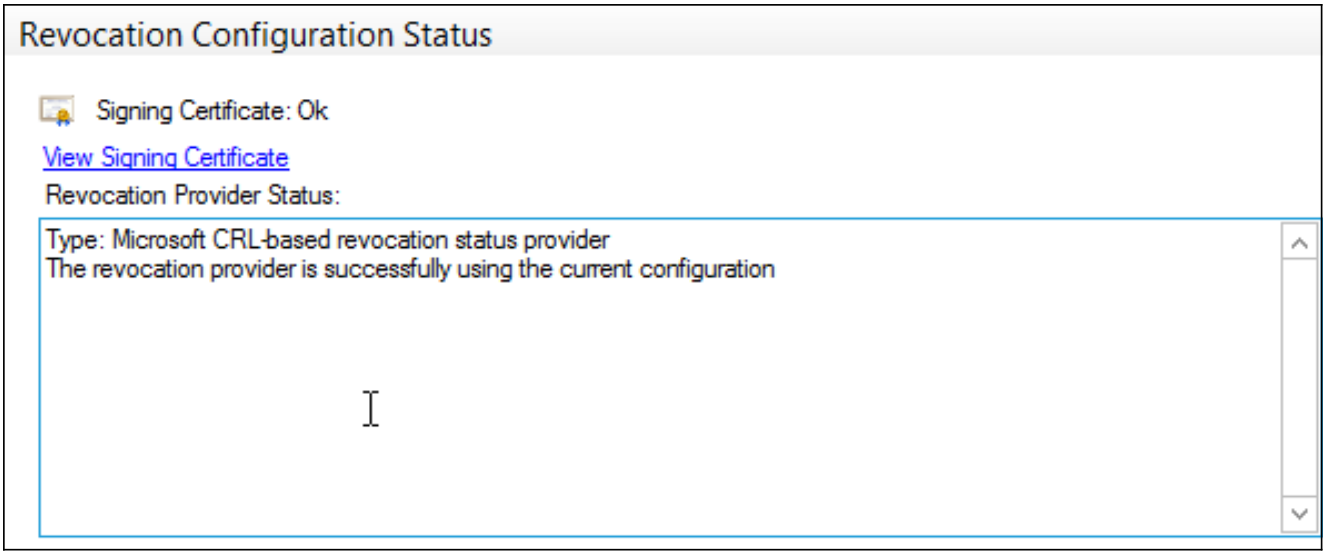
يمكن ل OCSP إستخدام المرجع المصدق للمؤسسة نفسه. يتم إنشاء شهادة خدمة OCSP.

أستخدم المرجع المصدق للمؤسسة المحدد، واختر القالب الذي تم إنشاؤه مسبقا. تم تسجيل الشهادة تلقائيا: 3.

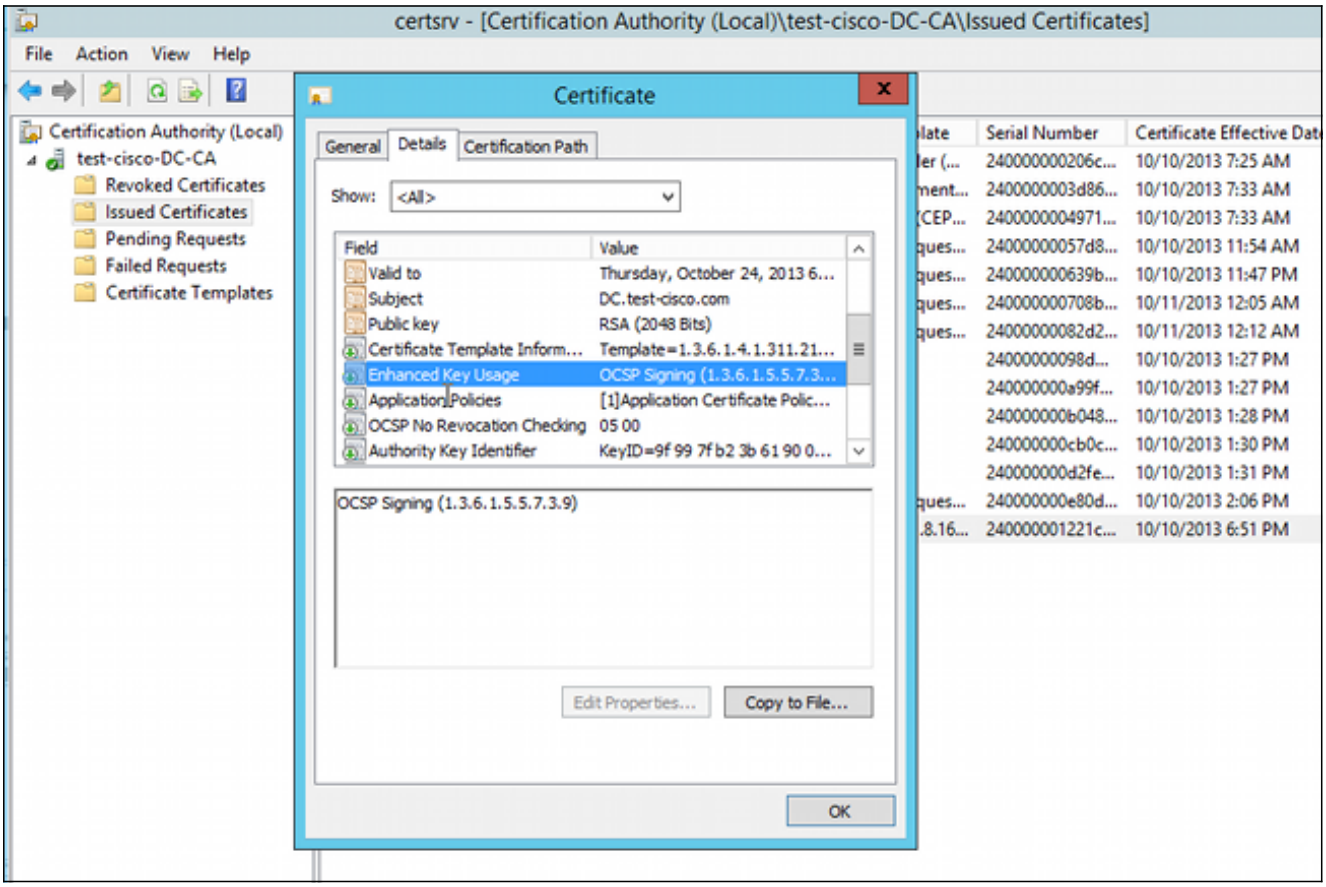


4. تأكد من تسجيل الشهادة ومن أن حالتها تعمل/موافق:





5. انتقل إلى **CA > الشهادات الصادرة** للتحقق من تفاصيل الشهادة:



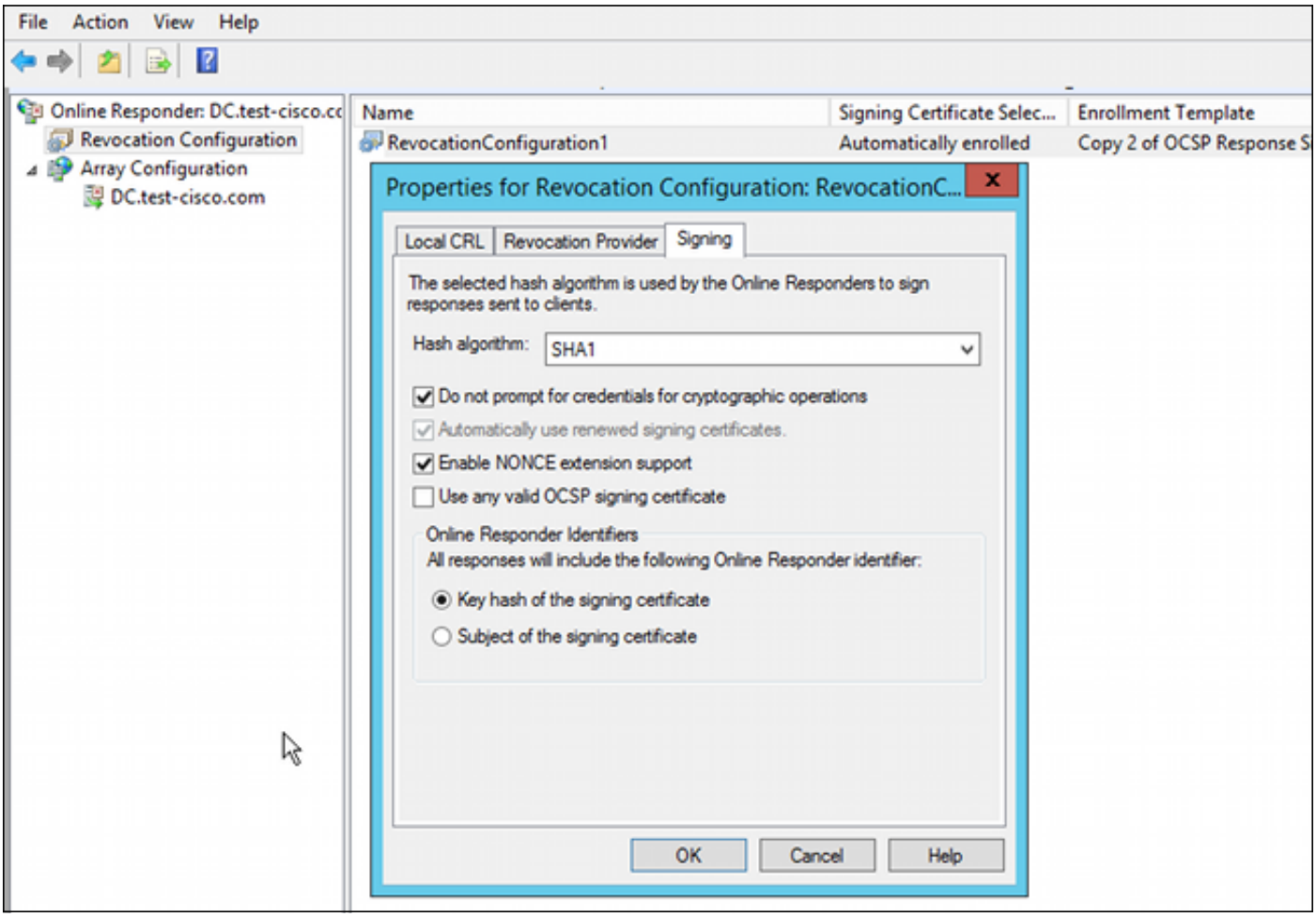
حالات عدم اتصال خدمة OCSP

يتوافق تنفيذ Microsoft ل OCSP مع RFC 5019 ملف تعريف بروتوكول حالة الشهادة عبر الإنترنت (OCSP) خفيف الوزن للبيئات كبيرة الحجم، وهو إصدار مبسط من بروتوكول حالة الشهادة عبر الإنترنت الخاص ب RFC 2560 X.509 Internet Key Public Infrastructure Certificate Protocol - OCSP .

يستخدم ASA RFC 2560 ل OCSP. أحد الفروق في شبكتي RFC هو أن RFC 5019 لا يقبل الطلبات الموقعة التي تم إرسالها من قبل ASA.

من الممكن إجبار خدمة OCSP ل Microsoft على قبول هذه الطلبات الموقعة والرد باستخدام الاستجابة الصحيحة الموقعة. انتقل إلى **تكوين الإبطال>RevocationConfiguration1>تحرير الخصائص**، وحدد الخيار **لتمكين دعم**

ملحق NONCE.



خدمة OCSP جاهزة الآن للاستخدام.

على الرغم من أن Cisco لا توصي بهذا، يمكن تعطيل الاتصالات على ASA:

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

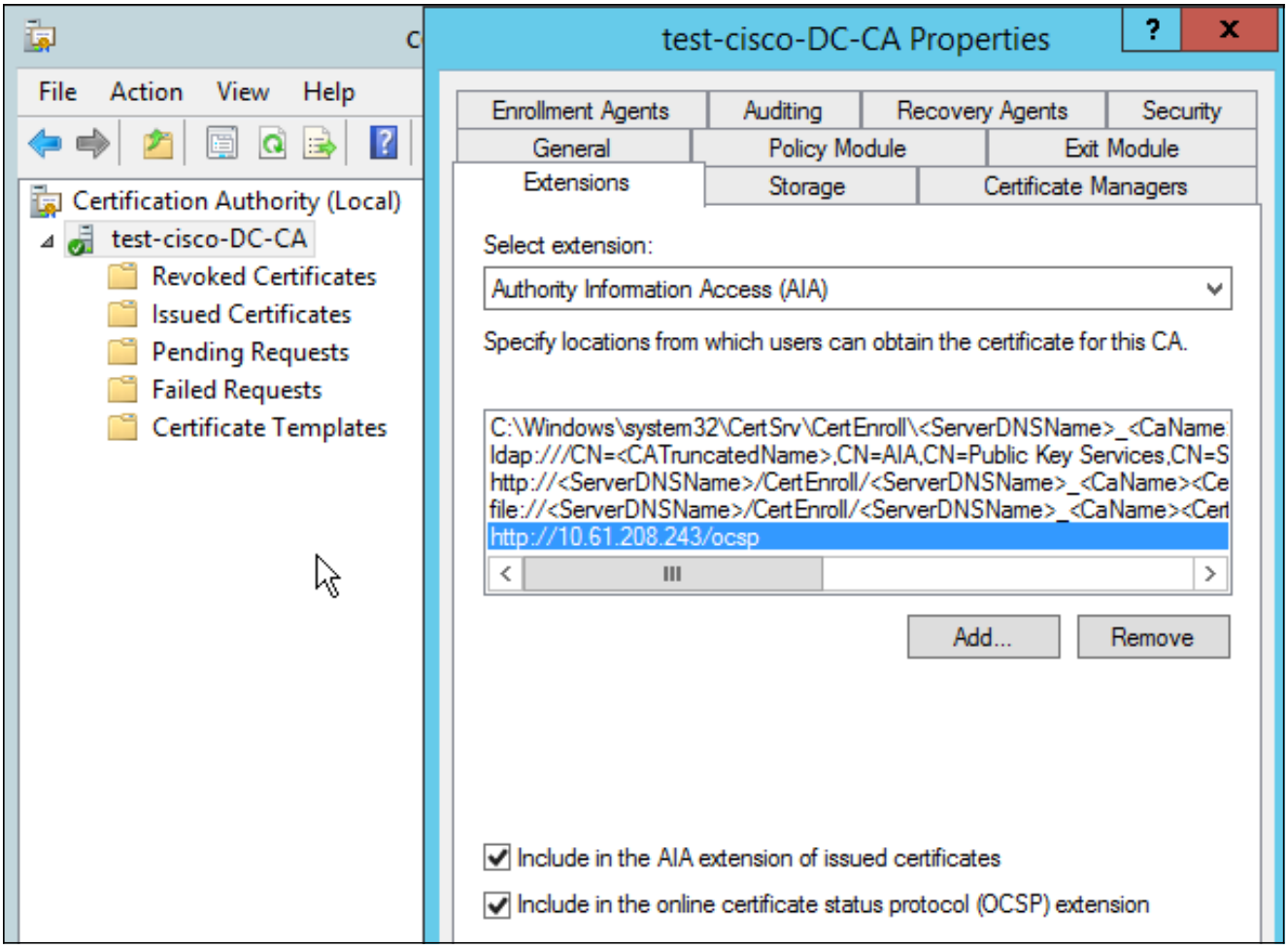
تكوين CA لملحقات OCSP

أنت ينبغي الآن reconfigure ال CA أن يتضمن ال OCSP نادل ملحق في كل شهادة صدرت. يتم إستخدام عنوان URL من هذا الملحق من قبل ASA للاتصال بخادم OCSP عند التحقق من صحة شهادة.

1. افتح مربع الحوار "خصائص" للخادم الموجود على المرجع المصدق.

2. انقر فوق علامة التبويب **الملحقات**. هناك حاجة إلى توسيع AIA (Authority Information Access) الذي يشير إلى خدمة OCSP، وهو في هذا المثال http://10.61.208.243/ocsp. مكنت كلا من هذا خيار ل ال AIA ملحق:

تضمين ملحق AIA للشهادات الصادرةتضمين في ملحق بروتوكول حالة الشهادة عبر الإنترنت (OCSP)



وهذا يضمن أن جميع الشهادات الصادرة لها ملحق صحيح يشير إلى خدمة OCSP.

OpenSSL

ملاحظة: راجع دليل تكوين السلسلة Cisco ASA 5500 باستخدام CLI، 8.4 و 8.6: تكوين خادم خارجي لتفويض مستخدم جهاز الأمان للحصول على تفاصيل حول تكوين ASA من خلال CLI (واجهة سطر الأوامر).

يفترض هذا المثال أن خادم OpenSSL تم تكوينه بالفعل. يصف هذا القسم تكوين OCSP والتغييرات اللازمة لتكوين CA فقط.

يوضح هذا الإجراء كيفية إنشاء شهادة OCSP:

1. هذه المعلمات مطلوبة لمستجيب OCSP:

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

2. هذه المعلمات مطلوبة لشهادات المستخدم:

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

3. يجب إنشاء الشهادات وتوقيعها من قبل المرجع المصدق.

4. بدء تشغيل خادم OCSP:

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

5. إختبار نموذج الشهادة:

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

يتوفر المزيد من الأمثلة على موقع OpenSSL على الويب .

يدعم OpenSSL، مثل ASA، طرق OCSP، ويمكن التحكم في المنافذ باستخدام محولات -nonce و-no_nonce.

ASA مع مصادر OCSP متعددة

يمكن أن يتجاوز ASA عنوان OCSP URL. حتى إذا كانت شهادة العميل تحتوي على عنوان OCSP URL، فإنه تتم الكتابة فوقها بواسطة التكوين الموجود على ASA:

```
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
```

يمكن تعريف عنوان خادم OCSP بشكل صريح. يتطابق مثال الأمر هذا مع كل الشهادات مع المسؤول في اسم الموضوع، ويستخدم OpenSSL TrustPoint للتحقق من توقيع OCSP، ويستخدم عنوان URL الخاص ب http://11.11.11.11/ocsp لإرسال الطلب:

```
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
```

الترتيب المستخدم للبحث عن OCSP URL هو:

1. خادم OCSP الذي قمت بضبطه باستخدام الأمر **مطابقة الشهادة**
2. خادم OCSP الذي قمت بضبطه باستخدام الأمر **ocsp url**
3. خادم OCSP في حقل AIA لشهادة العميل

ASA مع OCSP موقع من قبل CA مختلف

يمكن توقيع إستجابة OCSP من قبل مرجع مصدق مختلف. في مثل هذه الحالة، من الضروري إستخدام الأمر **match certificate** لاستخدام نقطة ثقة مختلفة على ASA للتحقق من شهادة OCSP.

```
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
```

في هذا المثال، يستخدم ASA إعادة كتابة عنوان OCSP URL لجميع الشهادات ذات اسم الموضوع الذي يحتوي على المسؤول. يتم فرض ASA على التحقق من صحة شهادة المستجيب OCSP مقابل نقطة ثقة أخرى، OpenSSL. لا تزال شهادات المستخدم معتمدة في Win2012 TrustPoint.

بما أن شهادة المستجيب OCSP تحتوي على الملحق 'OCSP no revocation check'، فلا يتم التحقق من الشهادة، حتى عندما يتم فرض التحقق من صحة OCSP مقابل OpenSSL TrustPoint.

بشكل افتراضي، يتم البحث في جميع نقاط الثقة عندما يحاول ASA التحقق من شهادة المستخدم. التحقق من صحة شهادة المستجيب OCSP مختلف. يبحث ASA فقط في TrustPoint التي تم العثور عليها بالفعل لشهادة المستخدم (WIN2012 في هذا المثال).

وبالتالي، من الضروري إستخدام الأمر **match certificate** لإجبار ASA على إستخدام نقطة ثقة مختلفة للتحقق من شهادة OCSP (OpenSSL في هذا المثال).

يتم التحقق من صحة شهادات المستخدم مقابل أول TrustPoint (WIN2012 في هذا المثال)، والذي يحدد بعد ذلك النقطة الموثوق بها الافتراضية للتحقق من إستجابة OCSP.

إذا لم يتم توفير أي نقطة ثقة محددة في الأمر **match certificate**، يتم التحقق من صحة شهادة OCSP مقابل نفس نقطة الثقة مثل شهادات المستخدم (WIN2012 في هذا المثال).:

```
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
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

ملاحظة: تدعم أداة مترجم الإخراج (العملاء المسجلون فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

ASA - الحصول على الشهادة عبر SCEP

يوضح هذا الإجراء كيفية الحصول على الشهادة من خلال إستخدام SCEP:

1. هذه هي عملية مصادقة TrustPoint للحصول على شهادة CA:

```
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
```

من أجل طلب الشهادة، يحتاج ASA إلى وجود كلمة مرور SCEP مرة واحدة يمكن الحصول عليها من وحدة 2. تحكم المسؤول على http://IP/certsrv/mscep_admin:

3. استعملت أن كلمة أن يطلب الشهادة على ال ASA:

```
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
```

تم حذف بعض المخرجات من أجل الوضوح.

4. دققت على حد سواء ال CA و ASA شهادة:

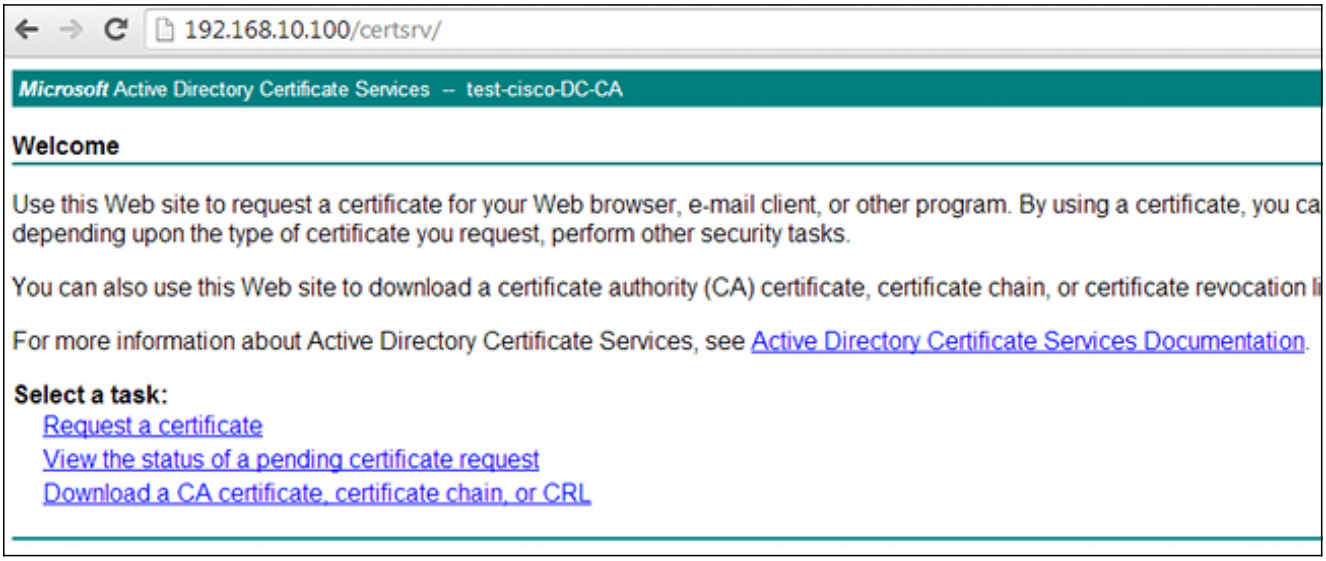
```
                                    BSNS-ASA5510-3(config)# show crypto ca certificates
                                                                  Certificate
                                                               Status: Available
                                Certificate Serial 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
                                                  ,ldap:///CN=test-cisco-DC-CA,CN=DC,CN=CDP  [1]
                                          ,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
```

لا يعرض ASA معظم ملحقات الشهادة. على الرغم من أن شهادة ASA تحتوي على URL 'OCSP' في امتداد AIA'، إلا أن ASA CLI لا يقدمها. يتطلب معرف تصحيح الأخطاء من ASA ENH"، CSCui44335 Cisco Certificate x509 Extensions المعروض" هذا التحسين.

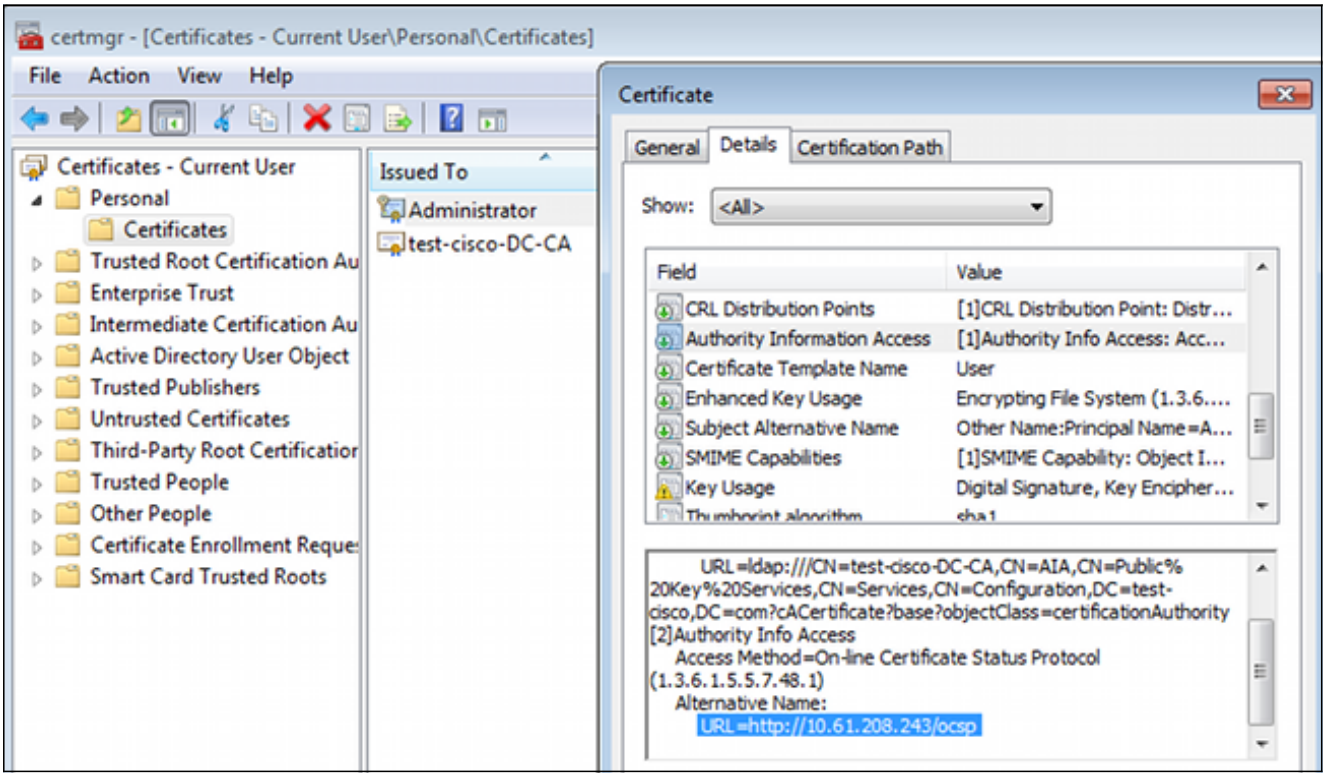
AnyConnect - الحصول على شهادة عبر صفحة الويب

يوضح هذا الإجراء كيفية الحصول على الشهادة من خلال إستخدام مستعرض الويب على العميل:

1. يمكن طلب شهادة مستخدم AnyConnect من خلال صفحة الويب. على جهاز الكمبيوتر العميل، أستخدم مستعرض ويب للانتقال إلى المرجع المصدق على http:///*IP*/CERTSRV:



2. يمكن حفظ شهادة المستخدم في مخزن مستعرض الويب، ثم تصديرها إلى مخزن Microsoft، والذي يتم البحث فيه بواسطة AnyConnect. أستخدم certmgr.msc للتحقق من الشهادة المستلمة:



كما يمكن ل AnyConnect طلب الشهادة طالما كان هناك توصيف AnyConnect صحيح.

الوصول عن بعد إلى ASA VPN مع التحقق من OCSP

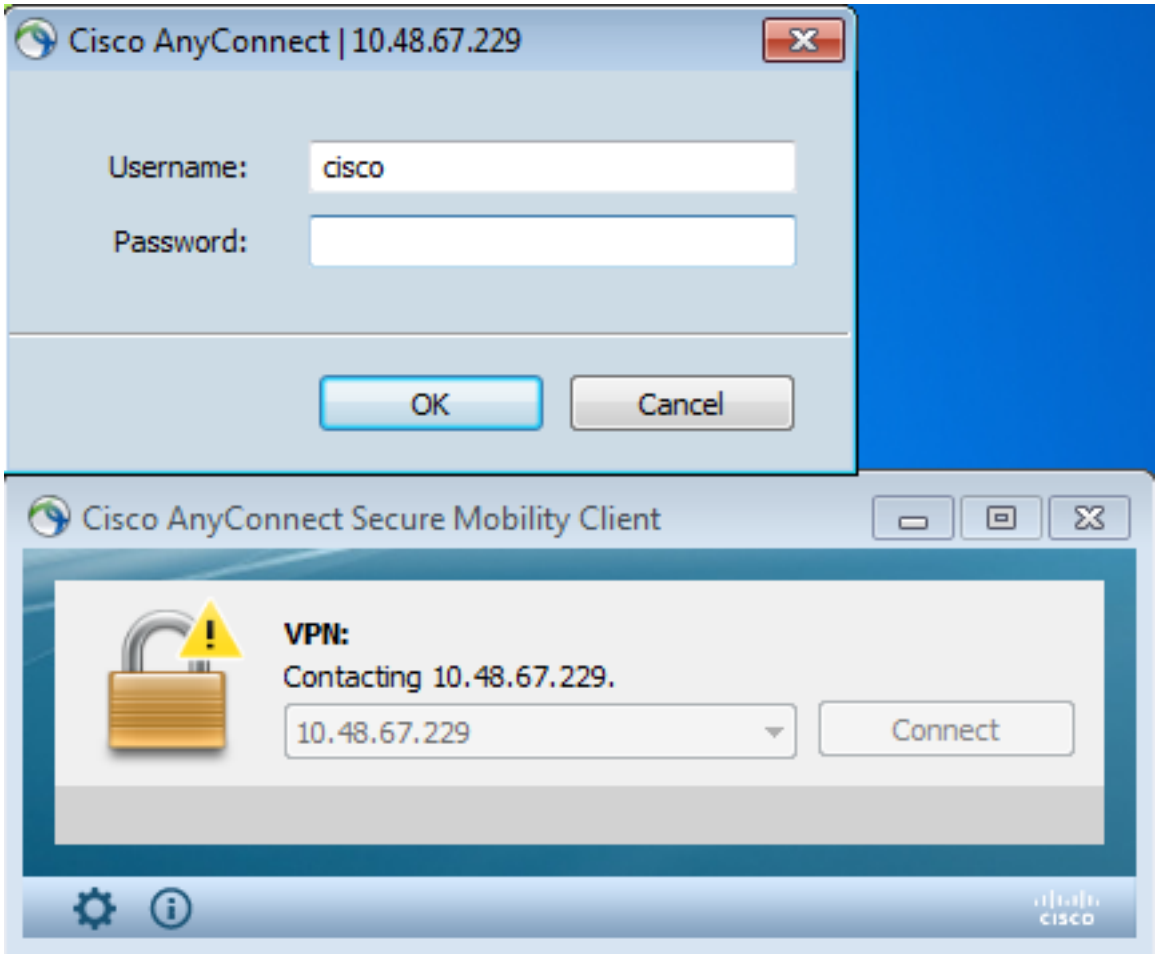
يصف هذا الإجراء كيفية التحقق من صحة OCSP:

1. بينما تحاول الاتصال، يبلغ ASA أنه يتم التحقق من الشهادة ل OCSP. هنا، تحتوي شهادة توقيع OCSP على ملحق بدون فحص ولم يتم فحصها عبر OCSP:

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

:ASA-6-725001: Starting SSL handshake with client outside%
.for TLSv1 session 10.61.209.83/51262
.(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%
to identity:10.48.67.229/35751 (10.61.209.83/80) 10.61.209.83/80
(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
```

تم حذف بعض المخرجات من أجل الوضوح.

2. يقدم المستخدم النهائي مسوغات المستخدم:



3. انتهت جلسة VPN بشكل صحيح:

```
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. خلقت الجلسة:

```
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
```

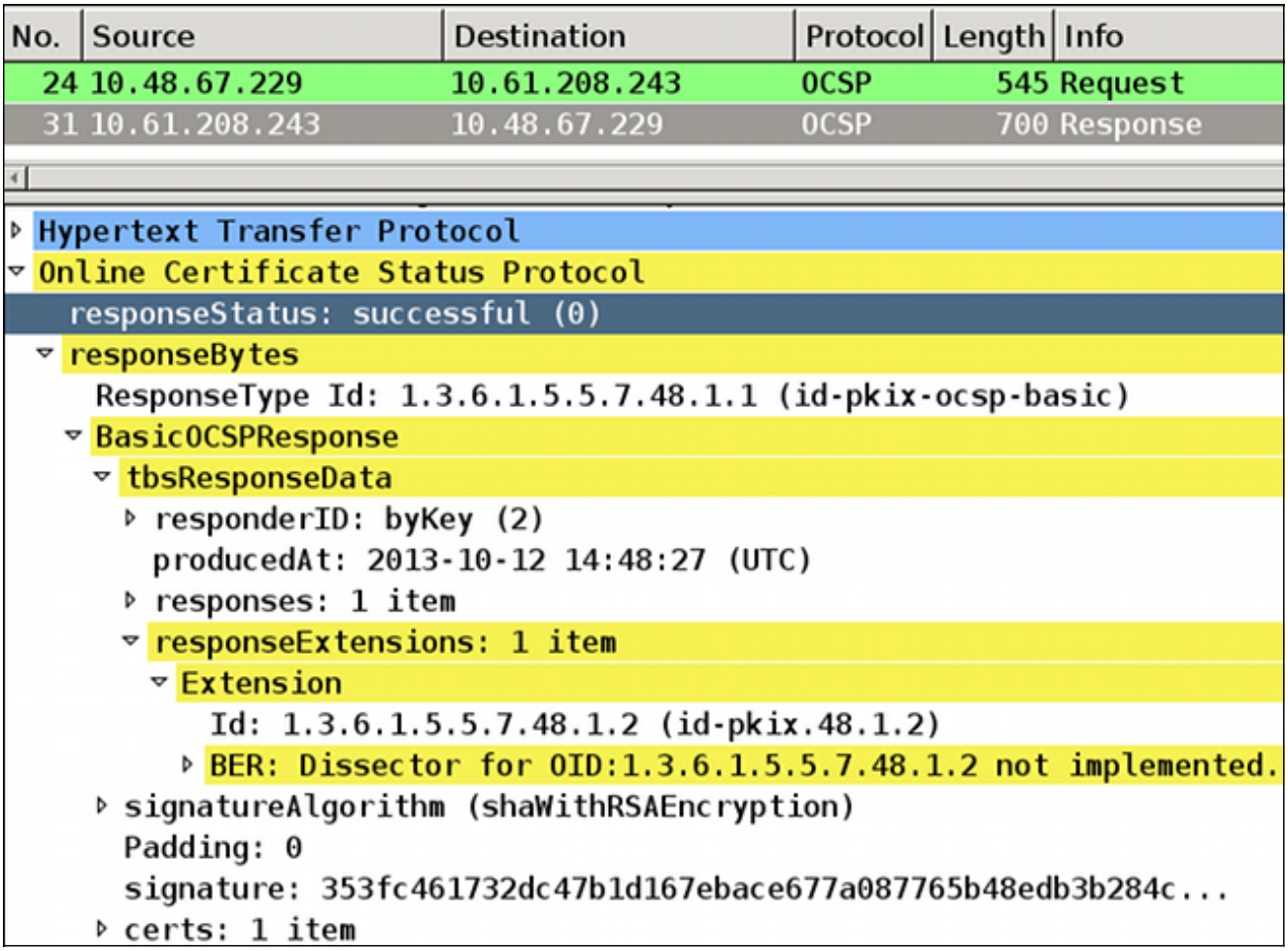
```
        Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
                                                  DTLS-Tunnel: (1)SHA1
             Bytes Tx     : 10540                 Bytes Rx     : 32236
               Pkts Tx      : 8                     Pkts Rx      : 209
                 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. يمكنك إستخدام تصحيح الأخطاء التفصيلي للتحقق من OCSP:

```
                                                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. في مستوى التقاط الحزمة، هذا هو طلب OCSP واستجابة OCSP الصحيحة. تتضمن الاستجابة التوقيع الصحيح - تم تمكين الملحق مرة واحدة على Microsoft OCSP:



الوصول عن بعد إلى ASA VPN مع مصادر OCSP متعددة

إذا تم تكوين شهادة مطابقة كما هو موضح في ASA مع مصادر OCSP متعددة، فإنها تأخذ الأسبقية:

```
...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
```

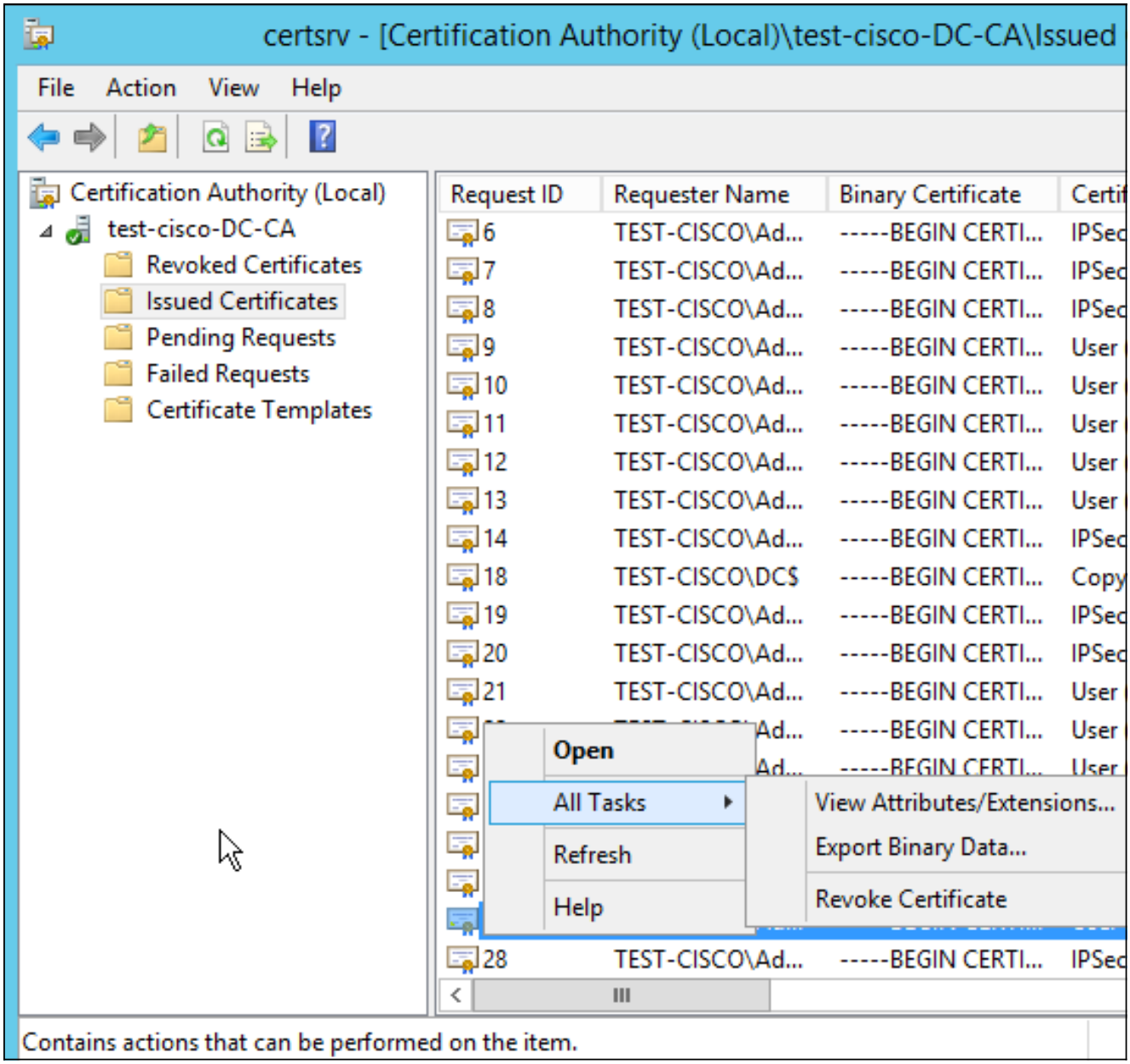
عند إستخدام تجاوز عنوان OCSP URL، تكون تصحيح الأخطاء:

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

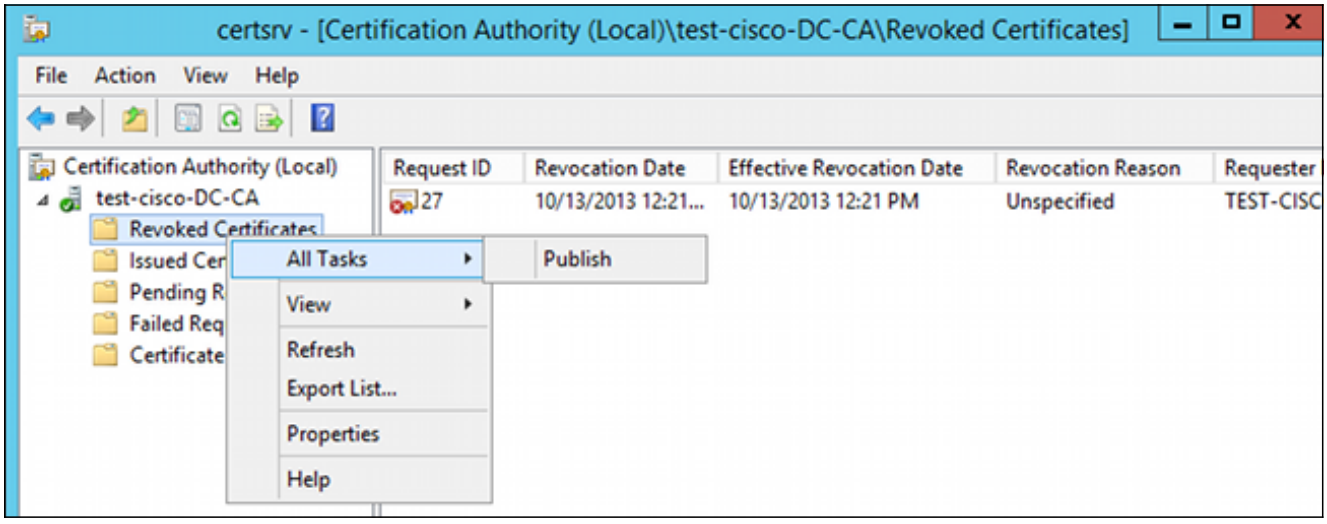
الوصول عن بعد إلى ASA VPN مع OCSP والشهادة الملغاة

يوضح هذا الإجراء كيفية إبطال الشهادة وتأكيد الحالة الملغاة:

1. إبطال شهادة العميل:



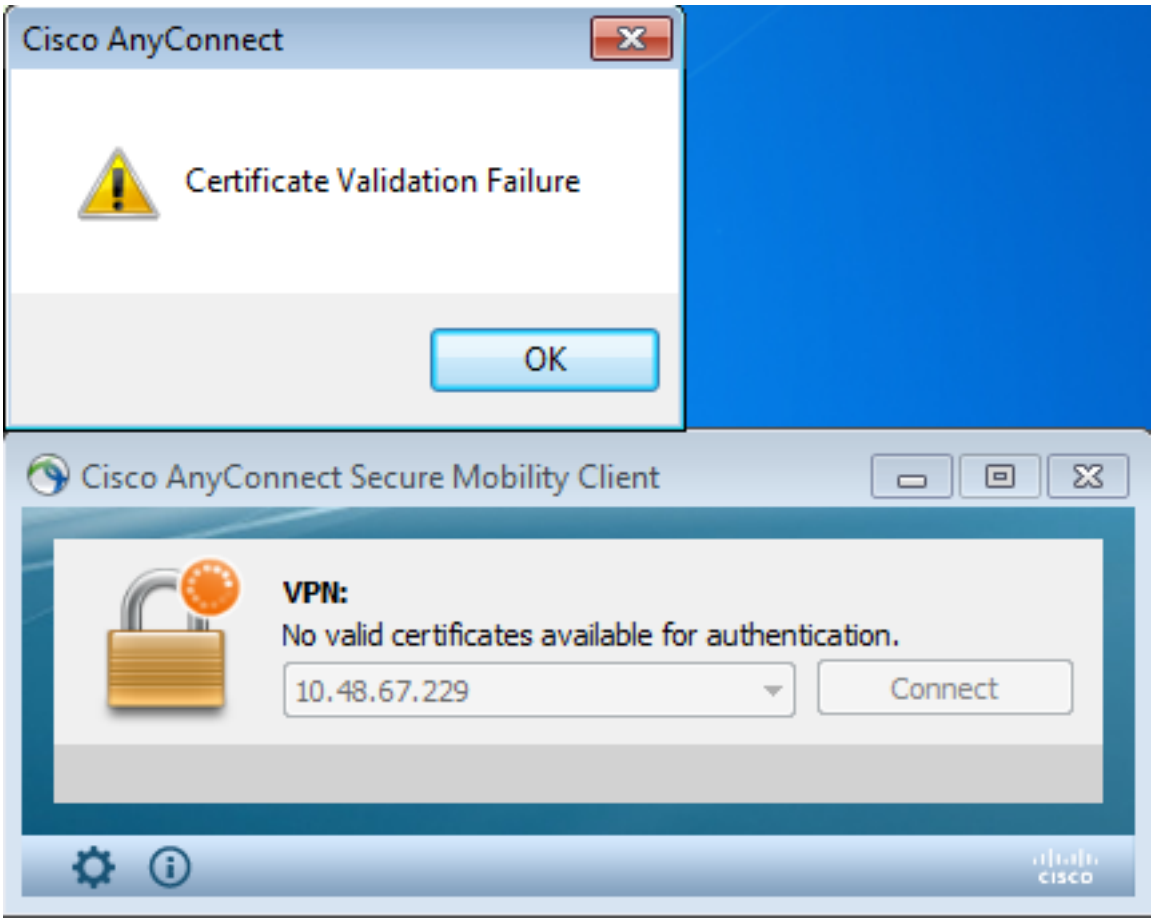
نشر النتائج: .2



3. [إختياري] يمكن أيضا تنفيذ الخطوات 1 و 2 باستخدام الأداة المساعدة لواجهة سطر الأوامر (CLI) الرئيسية في Power Shell:

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

4. عندما يحاول العميل الاتصال، يوجد خطأ في التحقق من صحة الشهادة:



5. تشير سجلات AnyConnect أيضا إلى خطأ التحقق من صحة الشهادة:

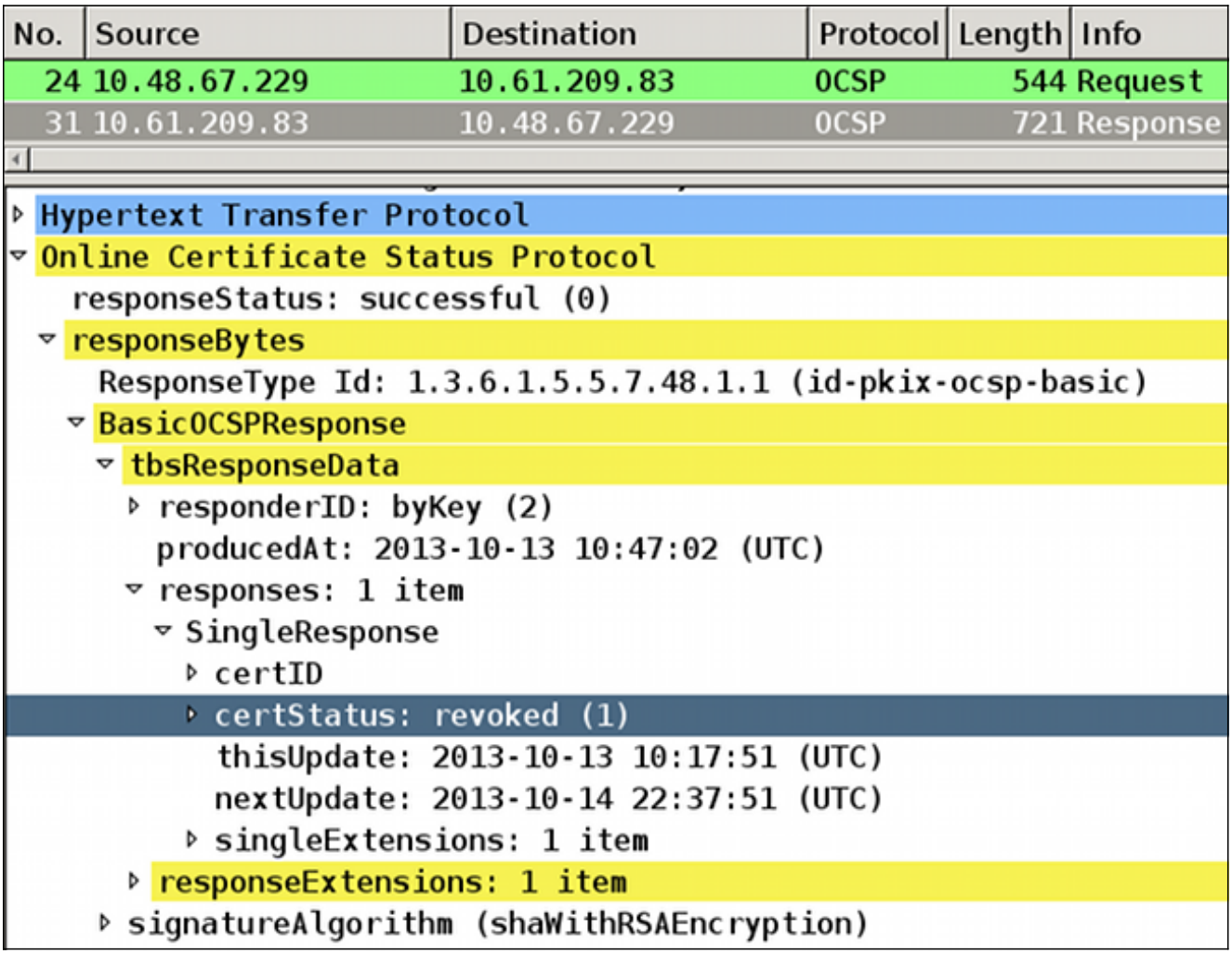
```
.Contacting 10.48.67.229 [12:49:53 2013-10-13]
.No valid certificates available for authentication [12:49:54 2013-10-13]
Certificate Validation Failure [12:49:55 2013-10-13]
```

6. يبلغ ASA عن إبطال حالة الشهادة:

```
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: 240000001B2AD208B128116874000000000001B, 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. تظهر حزم الالتقاط إستجابة OCSP ناجحة بحالة الشهادة لإبطال:



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

خادم OCSP معطل

تقرير ASA عند تعطل خادم OCSP:

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

يمكن أن تساعد عمليات التقاط الحزم أيضا في أستكشاف الأخطاء وإصلاحها.

الوقت غير متزامن

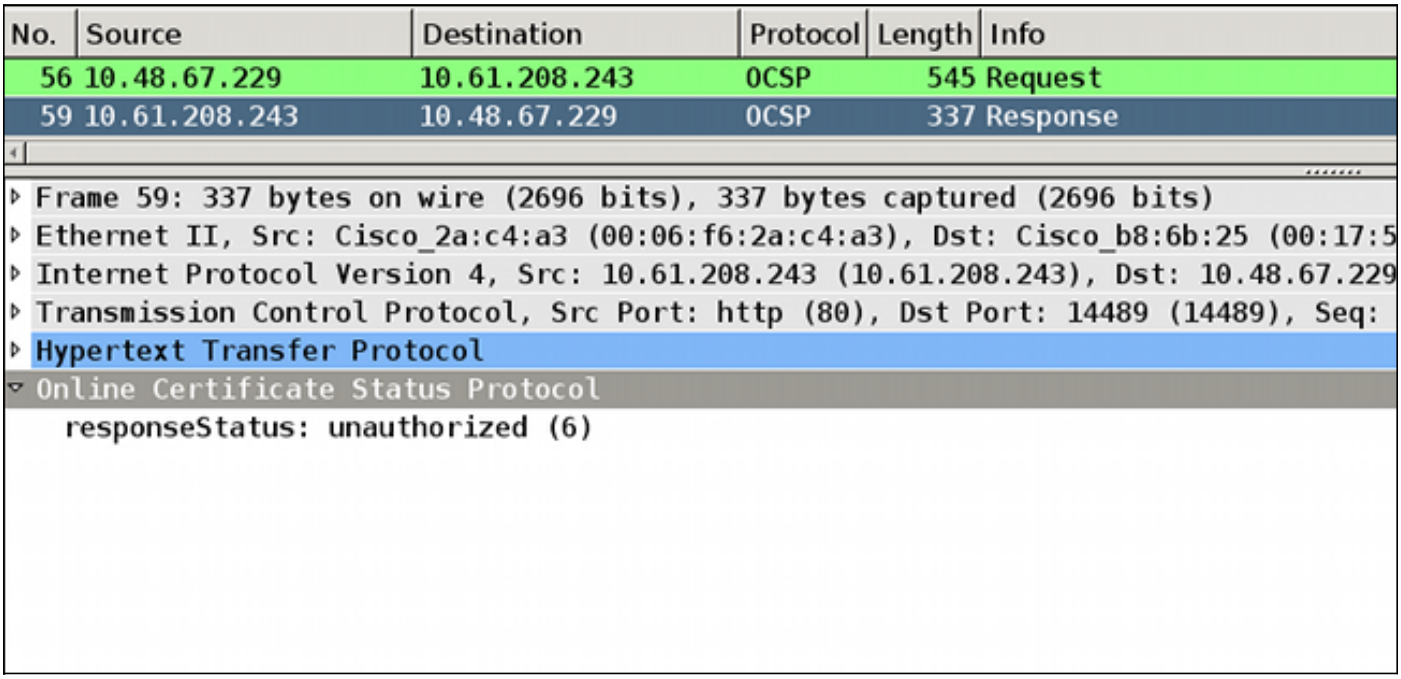
إذا كان الوقت الحالي على خادم OCSP أقدم من الوقت على ASA (الفوارق الصغيرة مقبولة)، يرسل خادم OCSP إستجابة غير مصرح بها، ويبلغ ASA عنها:

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

عندما يتلقى ASA إستجابة OCSP من أوقات المستقبل، فإنه يفشل أيضا.

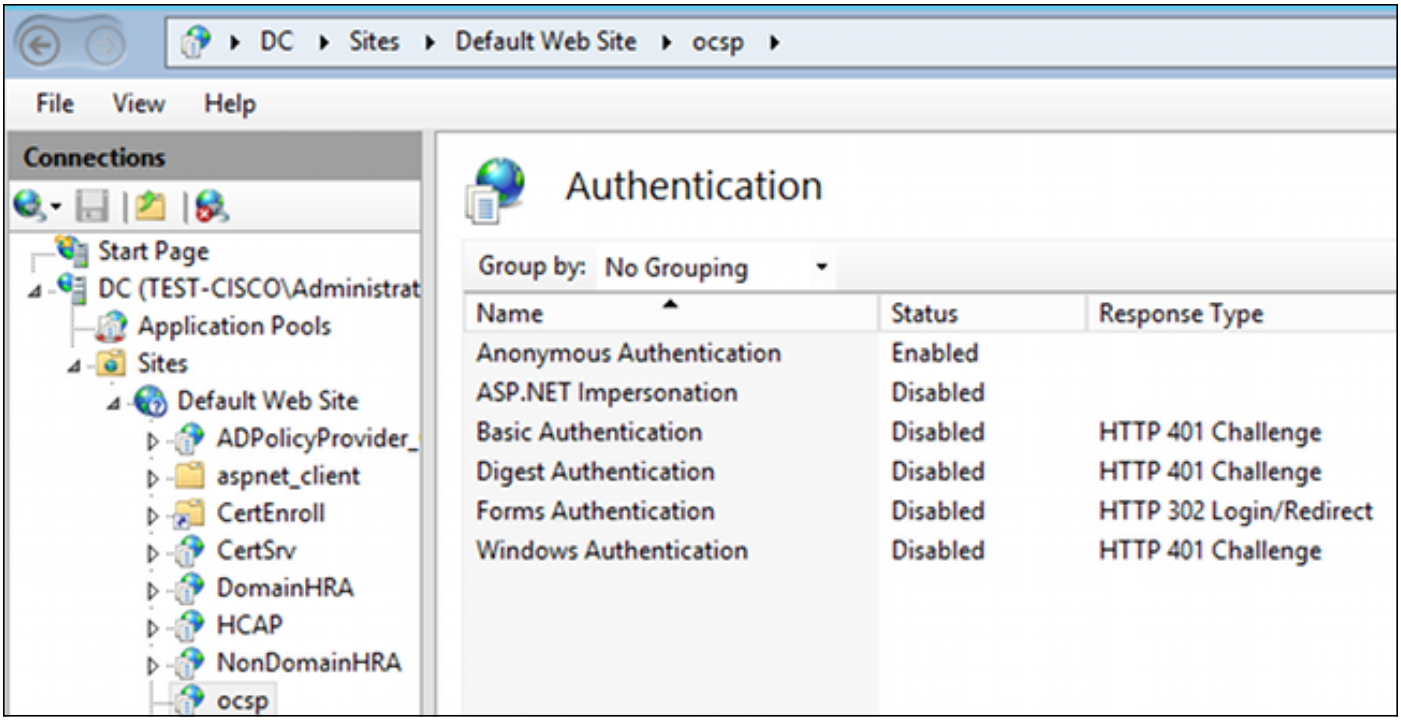
لا يتم دعم نقاط الاتصال الموقعة

إذا لم يتم دعم عمليات عدم الاتصال على الخادم (وهو الإعداد الافتراضي على نظام التشغيل Microsoft Windows 2012 R2)، يتم إرجاع إستجابة غير معتمدة:



مصادقة خادم IIS7

غالبا ما تكون المشاكل المتعلقة بطلب SCEP/OCSP ناتجة عن مصادقة غير صحيحة على Internet Information Services 7 (IIS7). تأكد من تكوين الوصول المجهول:



معلومات ذات صلة

- Microsoft TechNet: دليل تثبيت Online Responder وتكوينه واستكشاف الأخطاء وإصلاحها
- Microsoft TechNet: تكوين مرجع مصدق لدعم مستجيبي OCSP
- مرجع أوامر سلسلة ASA من Cisco
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).