

# نيوكت لاثم عم WebVPN ل SSO جمد Kerberos دي قم ل اضي وف ت ل ا

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [معلومات أساسية](#)
- [تفاعل Kerberos مع ASA](#)
- [التكوين](#)
- [طوبولوجيا](#)
- [وحدة التحكم بالمجال وتكوين التطبيق](#)
- [إعدادات المجال](#)
- [تعيين اسم الخدمة الأساسي \(SPN\)](#)
- [تشكيل على ال ASA](#)
- [التحقق من الصحة](#)
- [ينضم ASA إلى المجال](#)
- [طلب الخدمة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معرفة الأخطاء من Cisco](#)
- [معلومات ذات صلة](#)

## المقدمة

يصف هذا المستند كيفية تكوين تسجيل الدخول الأحادي ل (SSO) WebVPN) واستكشاف أخطاء هذا التسجيل وإصلاحها للتطبيقات التي يتم حمايتها بواسطة Kerberos.

## المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- تكوين واجهة سطر الأوامر (CLI) جهاز الأمان القابل للتكيف (ASA) من Cisco وتكوين طبقة مأخذ التوصيل الآمنة (VPN) SSL
- خدمات Kerberos

## المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

• برنامج Cisco ASA، الإصدار 9.0 والإصدارات الأحدث

• عميل Microsoft Windows 7

• Microsoft Windows 2003 Server والإصدارات الأحدث

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.

## معلومات أساسية

Kerberos هو بروتوكول مصادقة الشبكة الذي يسمح لكيانات الشبكة بالمصادقة لبعضها البعض بطريقة آمنة. تستخدم هذه الوحدة جهة خارجية موثوق بها، وهي "مركز توزيع المفاتيح" (KDC)، الذي يمنح تذاكر لكيانات الشبكة. تستخدم هذه التذاكر من قبل الكيانات للتحقق من الوصول إلى الخدمة المطلوبة وتأكيداتها.

من الممكن تكوين WebVPN SSO للتطبيقات المحمية بواسطة Kerberos باستخدام ميزة Cisco ASA التي تسمى تفويض Kerberos المقيد (KCD). باستخدام هذه الميزة، يمكن أن يطلب ASA تذاكر Kerberos بالنيابة عن مستخدم بوابة WebVPN، بينما يقوم بالوصول إلى التطبيقات التي محمية بواسطة Kerberos.

عند الوصول إلى هذه التطبيقات من خلال بوابة WebVPN، لن تحتاج إلى توفير أي بيانات اعتماد بعد ذلك؛ وبدلاً من ذلك، يتم استخدام الحساب الذي تم استخدامه لتسجيل الدخول إلى مدخل WebVPN.

راجع قسم [فهم كيفية عمل KCD](#) في دليل تكوين ASA للحصول على مزيد من المعلومات.

## تفاعل Kerberos مع ASA

بالنسبة ل WebVPN، يجب أن يطلب ASA التذاكر نيابة عن المستخدم (لأن مستخدم مدخل WebVPN لديه حق الوصول إلى البوابة فقط، وليس خدمة Kerberos). ولهذا الغرض، يستخدم ASA ملحقات Kerberos للتفويض المقيد. هنا هو التدفق:

1. ينضم مكتب المحاسبة الآنف إلى المجال ويحصل على تذكرة (التذكرة 1) لحساب كمبيوتر به بيانات اعتماد تم تكوينها على ASA (أمر kcd-server). يتم استخدام هذه التذكرة في الخطوات التالية للوصول إلى خدمات Kerberos.

2. يقوم المستخدم بالنقر فوق إرتباط مدخل WebVPN للتطبيق المحمي بواسطة Kerberos.

يطلب ASA (TGS-REQ) تذكرة لحساب الكمبيوتر مع اسم المضيف الخاص به كأصل. يتضمن هذا الطلب حقن PA-TGS-REQ مع PA-for-user يكون الجذر باسم مستخدم مدخل WebVPN، وهو cisco في هذا السيناريو. يتم استخدام تذكرة خدمة Kerberos من الخطوة 1 للمصادقة (التفويض الصحيح).

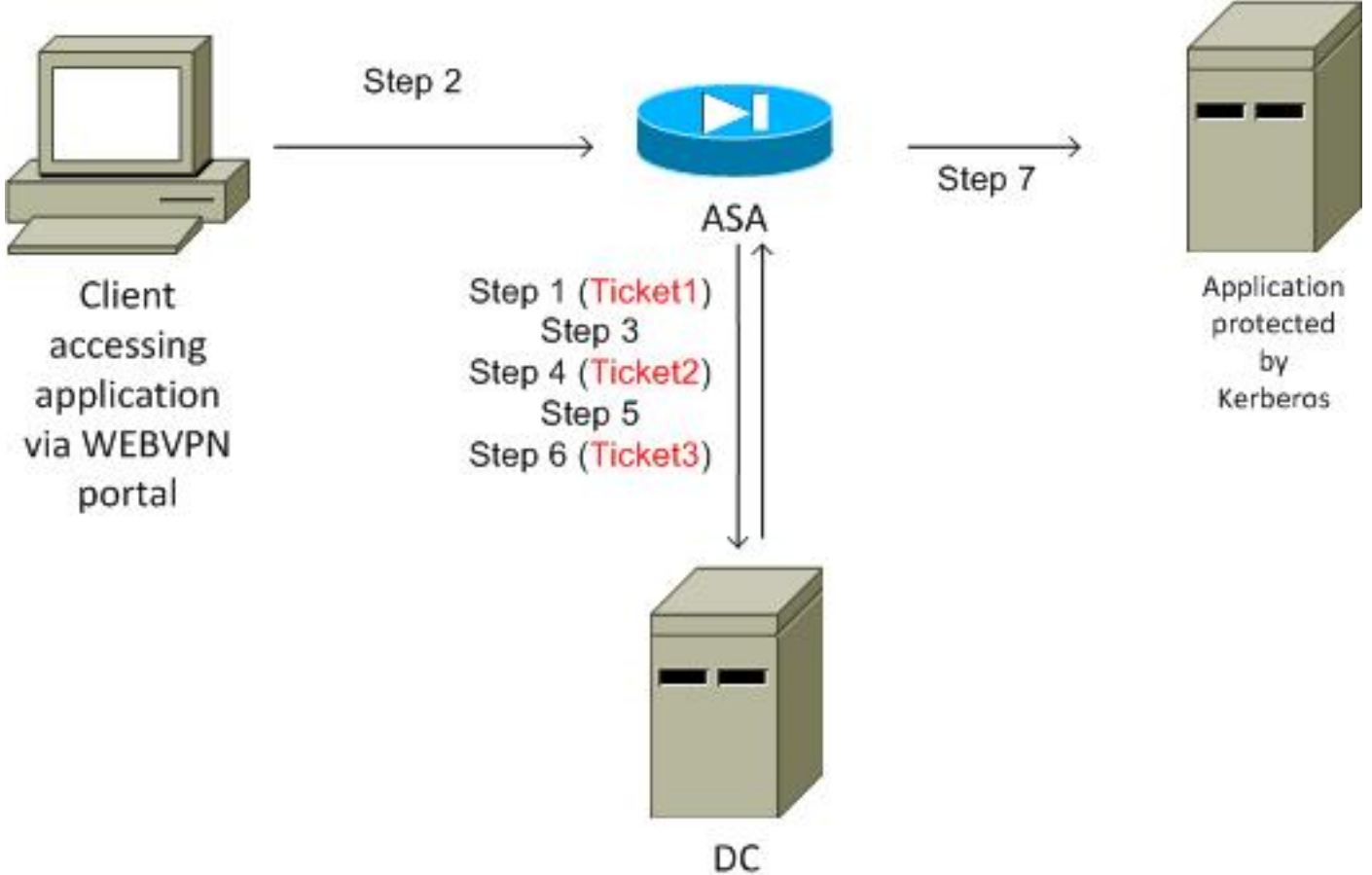
4. واستجابة لذلك، يتلقى مكتب خدمات المحاسبة تذكرة متحلة (التذكرة 2) بالنيابة عن مستخدم شبكة WebVPN. ((TGS\_REP لحساب الكمبيوتر. يتم استخدام هذه التذكرة لطلب تذاكر التطبيق نيابة عن مستخدم WebVPN هذا.

5. ويبدأ مكتب المحاسبة طلباً آخر (TGS\_REQ) للحصول على تذكرة التطبيق (-HTTP/test.kra)

sec.cisco.com). يستخدم هذا الطلب مرة أخرى حقل PA-TGS-REQ، ولكن هذه المرة بدون حقل PA-for-user، ولكن مع التذكرة المتتلة المستلمة في الخطوة 4.

6. يتم إرجاع الاستجابة (TGS\_REQ) باستخدام التذكرة المتتلة (TICKET3) للتطبيق.

7. يتم استخدام هذه التذكرة بشكل شفاف بواسطة ASA للوصول إلى الخدمة المحمية، ولا يحتاج مستخدم WebVPN إلى إدخال أي بيانات اعتماد. بالنسبة لتطبيق HTTP، يتم استخدام آلية التفاوض Simple and Protected GSS-API (SPNEGO) من أجل التفاوض على طريقة المصادقة، ويتم تمرير التذكرة الصحيحة من قبل ASA.



## التكوين

### طوبولوجيا

المجال: 10.211.0.221 أو kra-sec.cisco.com أو 10.211.0.216

التطبيق 7 لخدمات معلومات الإنترنت: 10.211.0.223 (test.kra-sec.cisco.com)

وحدة التحكم بالمجال (10.211.0.221) dc.kra-sec.cisco.com (DC أو 10.211.0.216) - Windows2008

ASA: 10.211.0.162

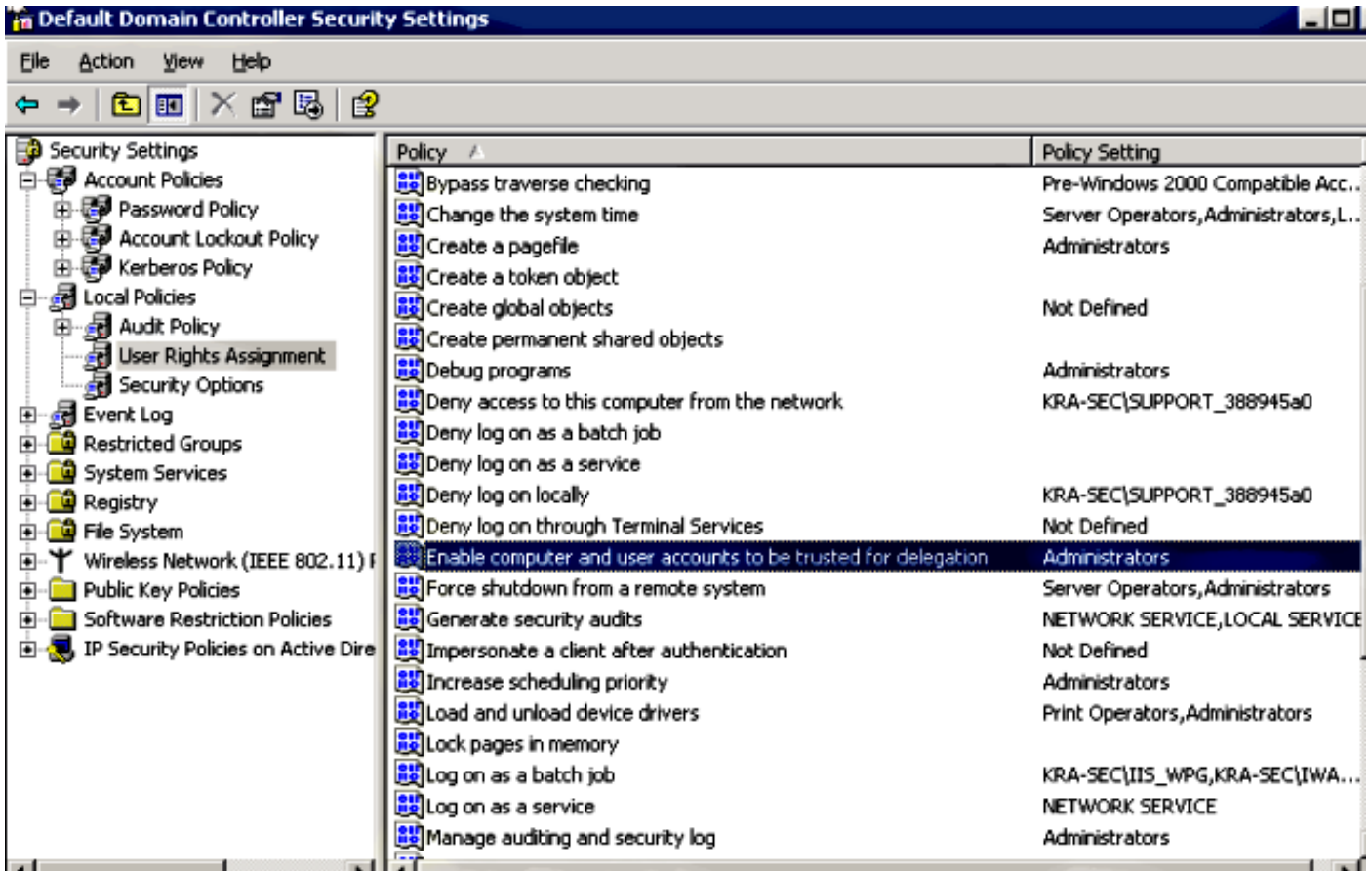
اسم مستخدم/كلمة مرور WebVPN: cisco/cisco

الملف المرفق: asa-join.pcap (انضمام ناجح إلى المجال)

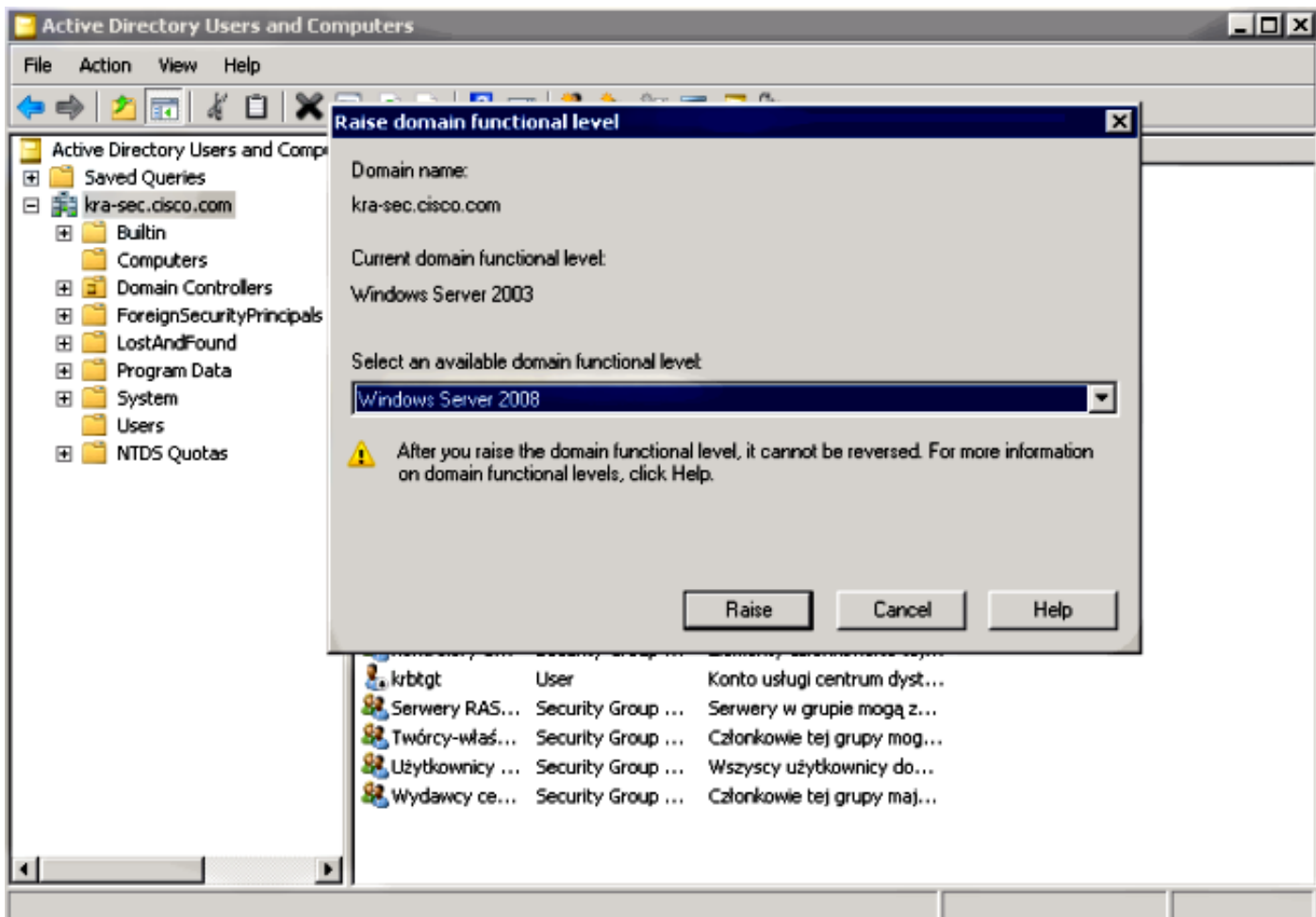
## وحدة التحكم بالمجال وتكوين التطبيق

### إعدادات المجال

من المفترض أن هناك بالفعل تطبيق IIS7 وظيفي محمي بواسطة Kerberos (إذا لم يكن الأمر كذلك، فاقراً قسم المتطلبات الأساسية). يجب التحقق من إعدادات وفود المستخدمين:



تأكد من رفع مستوى المجال الوظيفي إلى Windows Server 2003 (على الأقل). الافتراضي هو Windows Server 2000



## تعيين اسم الخدمة الأساسي (SPN)

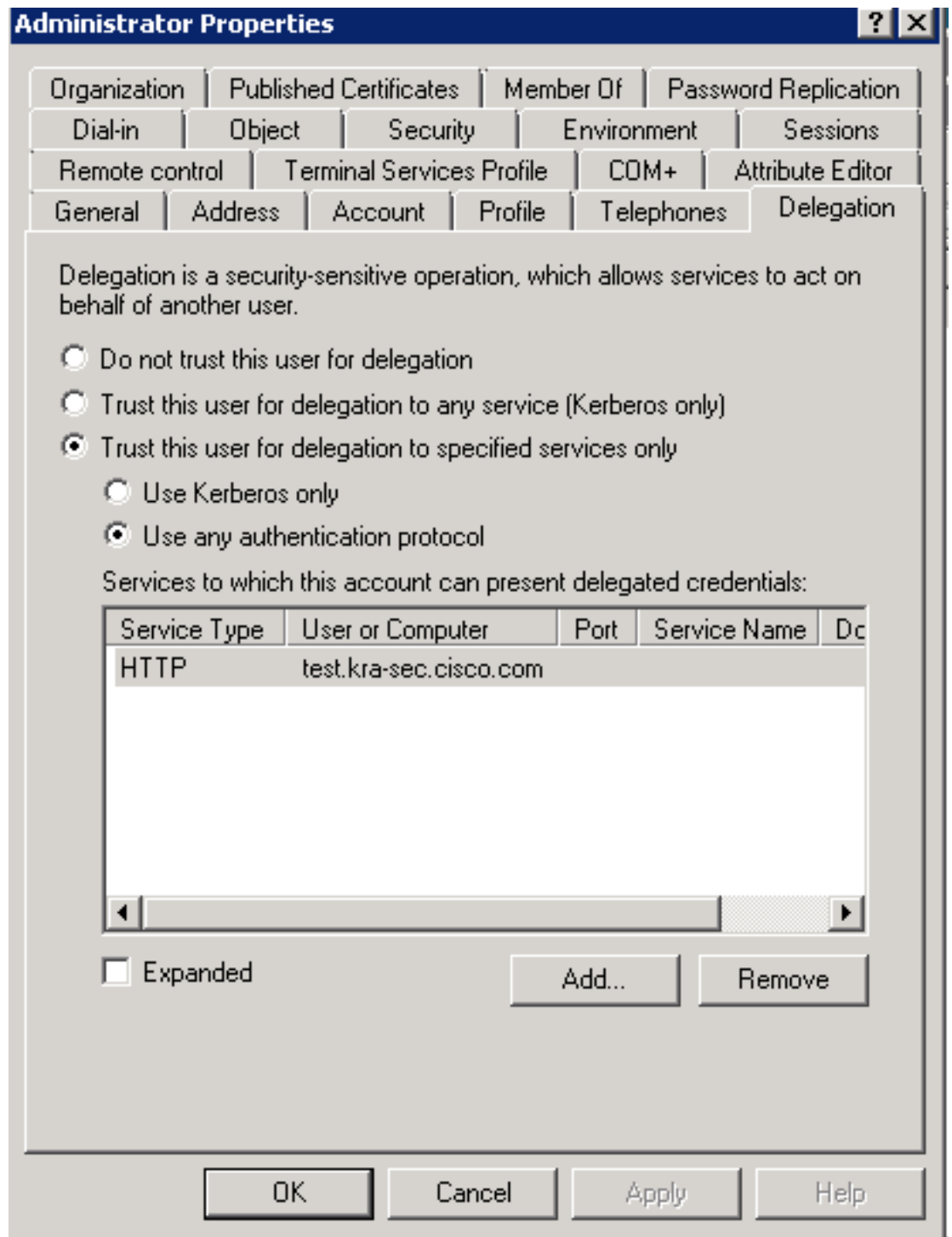
يجب تكوين أي حساب على AD بتفويض صحيح. يتم استخدام حساب مسؤول. وعندما يستخدم مكتب المحاسبة هذا الحساب، يكون قادراً على طلب تذكرة بالنيابة عن مستخدم آخر (تفويض مقيد) للخدمة المحددة (تطبيق HTTP). ولكي يحدث ذلك، يجب إنشاء التفويض الصحيح للتطبيق/الخدمة.

من أجل جعل هذا التفويض عبر واجهة سطر الأوامر مع `setSPN.exe`، والذي يعد جزءاً من [أدوات دعم Windows Server 2003 Service Pack 1](#)، أدخل هذا الأمر:

```
setspn.exe -A HTTP/test.kra-sec.cisco.com kra-sec.cisco.com\Administrator
test.kra-sec.cisco.com
```

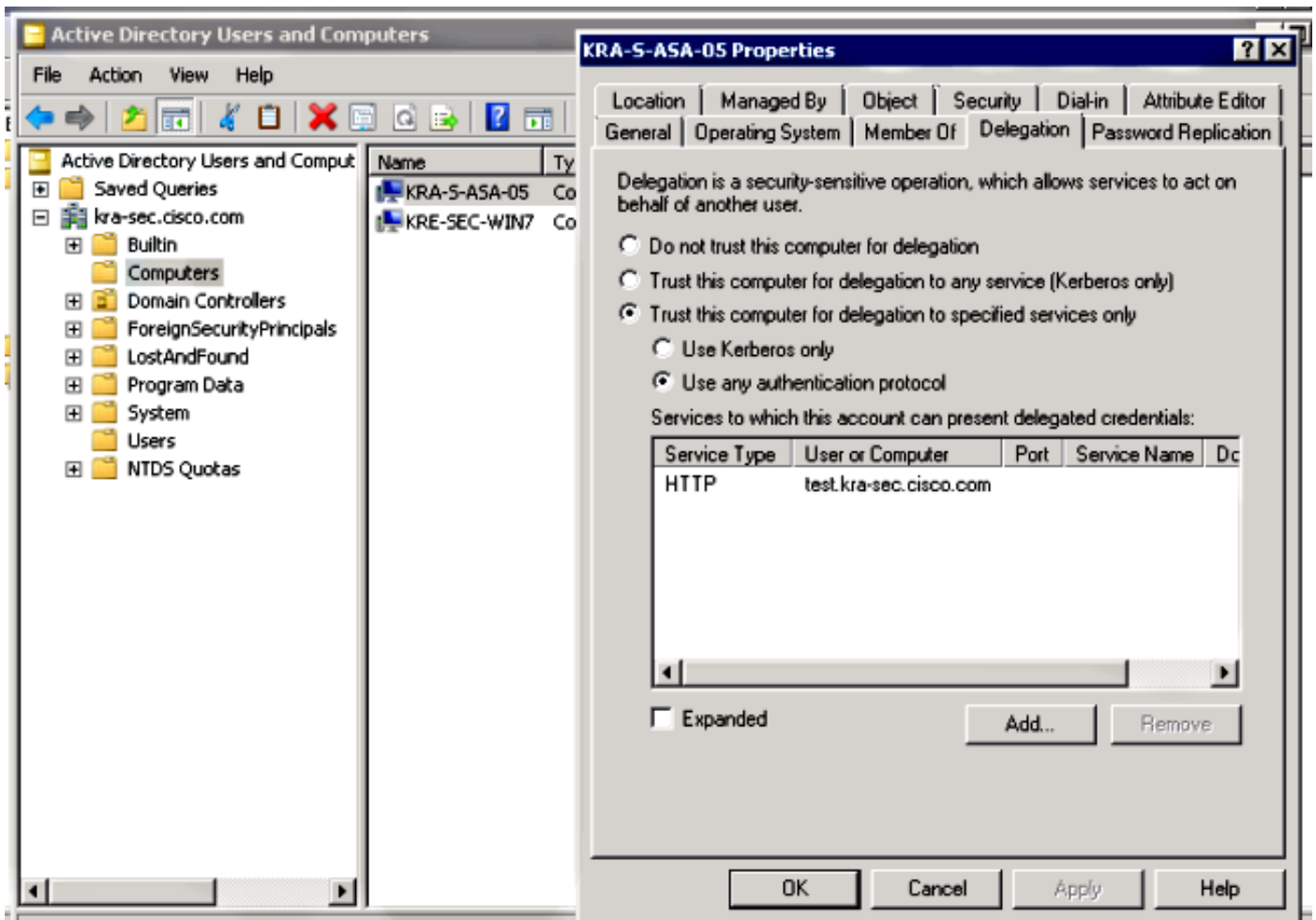
وهذا يشير إلى أن اسم مستخدم Administrator هو الحساب الموثوق به لتفويض خدمة HTTP في test.kra-

يعد الأمر SPN ضرورياً أيضاً لتنشيط علامة التوبيخ تفويض لذلك المستخدم. بمجرد إدخال الأمر، تظهر علامة التوبيخ "تفويض" للمسؤول. من المهم تمكين "إستخدام أي بروتوكول مصادقة"، لأن "إستخدام Kerberos فقط" لا يدعم امتداد التفويض المقيد.



على علامة التبويب **عام**، من الممكن أيضا تعطيل المصادقة المسبقة ل Kerberos. ومع ذلك، لا ينصح بذلك، لأنه يتم استخدام هذه الميزة لحماية DC من هجمات إعادة التشغيل. يمكن أن يعمل ASA مع المصادقة المسبقة بشكل صحيح.

ينطبق هذا الإجراء أيضا على التفويض لحساب الكمبيوتر (يتم إدخال ASA إلى المجال ككمبيوتر من أجل إنشاء علاقة "ثقة"):



## تشکیل علی ال ASA

```
interface Vlan211
    nameif inside
    security-level 100
ip address 10.211.0.162 255.255.255.0
```

```
hostname KRA-S-ASA-05
domain-name kra-sec.cisco.com
```

```
dns domain-lookup inside
dns server-group DNS-GROUP
name-server 10.211.0.221
domain-name kra-sec.cisco.com
```

```
aaa-server KerberosGroup protocol kerberos
aaa-server KerberosGroup (inside) host 10.211.0.221
kerberos-realm KRA-SEC.CISCO.COM
```

```
webvpn
    enable outside
    enable inside
**** kcd-server KerberosGroup username Administrator password
```

```
group-policy G1 internal
group-policy G1 attributes
    WebVPN
url-list value KerberosProtected
username cisco password 3USUcOPFUiMC04Jk encrypted
```

```
tunnel-group WEB type remote-access
tunnel-group WEB general-attributes
    default-group-policy G1
tunnel-group WEB webvpn-attributes
    group-alias WEB enable
dns-group DNS-GROUP
```

## التحقق من الصحة

### ينضم ASA إلى المجال

بعد استخدام الأمر **kcd-server**، يحاول ASA الانضمام إلى المجال:

```
***** START: KERBEROS PACKET DECODE *****
    Kerberos: Message type KRB_AS_REQ
        Kerberos: Option forwardable
        Kerberos: Client Name KRA-S-ASA-05$
    Kerberos: Client Realm KRA-SEC.CISCO.COM
        Kerberos: Server Name krbtgt
            Kerberos: Start time 0
            Kerberos: End time -878674400
        Kerberos: Renew until time -878667552
            Kerberos: Nonce 0xa9db408e
    Kerberos: Encryption type rc4-hmac-md5
        Kerberos: Encryption type des-cbc-md5
        Kerberos: Encryption type des-cbc-crc
        Kerberos: Encryption type des-cbc-md4
    Kerberos: Encryption type des3-cbc-sha1
***** END: KERBEROS PACKET DECODE *****
    In kerberos_recv_msg
    In KCD_self_tkt_process_response
***** START: KERBEROS PACKET DECODE *****
    Kerberos: Message type KRB_ERROR
Kerberos: Error type: Additional pre-authentication required, -1765328359
    (0x96c73a19)
    (Kerberos: Encrypt Type: 23 (rc4-hmac-md5
        Salt: "" Salttype: 0
    (Kerberos: Encrypt Type: 3 (des-cbc-md5
Salt: "KRA-SEC.CISCO.COMhostkra-s-asa-05.kra-sec.cisco.com" Salttype: 0
    (Kerberos: Encrypt Type: 1 (des-cbc-crc
Salt: "KRA-SEC.CISCO.COMhostkra-s-asa-05.kra-sec.cisco.com" Salttype: 0
    Kerberos: Preauthentication type unknown
    Kerberos: Preauthentication type encrypt timestamp
    Kerberos: Preauthentication type unknown
    Kerberos: Preauthentication type unknown
        Kerberos: Server time 1360917305
    Kerberos: Realm KRA-SEC.CISCO.COM
    Kerberos: Server Name krbtgt
***** END: KERBEROS PACKET DECODE *****
    .Attempting to parse the error response from KCD server
    "Kerberos library reports: Additional pre-authentication required
    In kerberos_send_request
***** START: KERBEROS PACKET DECODE *****
    Kerberos: Message type KRB_AS_REQ
    Kerberos: Preauthentication type encrypt timestamp
        Kerberos: Option forwardable
        Kerberos: Client Name KRA-S-ASA-05$
    Kerberos: Client Realm KRA-SEC.CISCO.COM
```



```

Kerberos: Server Name krbtgt
Kerberos: Start time 0
Kerberos: End time -878667256
Kerberos: Renew until time -878672192
Kerberos: Nonce 0xa9db408e
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4
Kerberos: Encryption type des3-cbc-sha1
***** END: KERBEROS PACKET DECODE *****
In kerberos_recv_msg
In KCD_self_tkt_process_response
***** START: KERBEROS PACKET DECODE *****
Kerberos: Message type KRB_AS_REP
Kerberos: Client Name KRA-S-ASA-05$
Kerberos: Client Realm KRA-SEC.CISCO.COM
***** END: KERBEROS PACKET DECODE *****
INFO: Successfully stored self-ticket in cache a6588e0
.KCD self-ticket retrieval succeeded
In kerberos_close_connection
remove_req 0xcc09ad18 session 0x1 id 0
free_kip 0xcc09ad18
kerberos: work queue empty

```

يمكن أن ينضم ASA إلى المجال بنجاح. بعد المصادقة الصحيحة، يستلم ASA تذكرة للأساسي: المسئول في حزمة AS\_REP (التذكرة 1 الموضحة في الخطوة 1).

|    |                            |              |              |      |  |
|----|----------------------------|--------------|--------------|------|--|
| 28 | 2013-02-12 06:16:20.686888 | 10.211.0.162 | 10.211.0.216 | KRB5 | 225 AS-REQ   |
| 29 | 2013-02-12 06:16:20.687678 | 10.211.0.216 | 10.211.0.162 | KRB5 | 206 KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED                      |
| 30 | 2013-02-12 06:16:20.719281 | 10.211.0.162 | 10.211.0.216 | DNS  | 183 Standard query 8x4c7d SRV_kerberos-master_udp.KRA-SEC.C      |
| 31 | 2013-02-12 06:16:20.719689 | 10.211.0.216 | 10.211.0.162 | DNS  | 178 Standard query response 8x4c7d No such name                  |
| 32 | 2013-02-12 06:16:20.760508 | 10.211.0.162 | 10.211.0.216 | KRB5 | 303 AS-REQ   |
| 33 | 2013-02-12 06:16:20.762045 | 10.211.0.216 | 10.211.0.162 | IPv4 | 1318 Fragmented IP protocol (proto=UDP 17, off=0, ID=c43c) [Roze |
| 34 | 2013-02-12 06:16:20.762045 | 10.211.0.216 | 10.211.0.162 | KRB5 | 112 AS-REP   |

```

Frame 34: 112 bytes on wire (896 bits), 112 bytes captured (896 bits)
Ethernet II, Src: Vmware_9c:34:99 (00:50:56:9c:34:99), Dst: Cisco_el:a0:3c (2c:54:2d:e1:a0:3c)
B82.10 Virtual LAN, PRI: 0, CFI: 0, ID: 211
Internet Protocol Version 4, Src: 10.211.0.216 (10.211.0.216), Dst: 10.211.0.162 (10.211.0.162)
User Datagram Protocol, Src Port: kerberos (88), Dst Port: 56007 (56007)
Kerberos AS-REP
  Pkno: 5
  MSG Type: AS-REP (11)
  Client Realm: KRA-SEC.CISCO.COM
  Client Name (Principal): Administrator
  Ticket
  enc-part rc4-hmac

```

## طلب الخدمة

المستخدم ينقر إرتباط WebVPN:

يرسل ASA TGS\_REQ للتذكرة المنتحلة مع التذكرة التي يتم استقبالها في حزمة AS\_REP:

| No. | Time                       | Source       | Destination  | Protocol | Length | Info    |
|-----|----------------------------|--------------|--------------|----------|--------|---------|
| 13  | 2013-02-15 11:56:37.465857 | 10.211.0.162 | 10.211.0.221 | KRB5     | 77     | TGS-REQ |
| 14  | 2013-02-15 11:56:37.468588 | 10.211.0.221 | 10.211.0.162 | KRB5     | 1354   | TGS-REP |
| 16  | 2013-02-15 11:56:37.563325 | 10.211.0.162 | 10.211.0.221 | KRB5     | 1003   | TGS-REQ |

```

Ethernet II, Src: Cisco_e1:a0:3c (2c:54:2d:e1:a0:3c), Dst: Vmware_9c:5d:90 (00:50:56:9c:5d:90)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 211
Internet Protocol Version 4, Src: 10.211.0.162 (10.211.0.162), Dst: 10.211.0.221 (10.211.0.221)
User Datagram Protocol, Src Port: netopia-vo1 (1839), Dst Port: kerberos (88)
Kerberos TGS-REQ
  Pvno: 5
  MSG Type: TGS-REQ (12)
  padata: PA-TGS-REQ PA-FOR-USER
    Type: PA-TGS-REQ (1)
    Type: PA-FOR-USER (129)
      Value: 3053a0123010a003020101a10930071b05636973636fa113...
        Client Name (Principal): cisco
        Realm: KRA-SEC.CISCO.COM
        Checksum
        S4U2Self Auth: Kerberos
    KDC_REQ_BODY

```

ملاحظة: قيمة PA للمستخدم هي Cisco (مستخدم WebVPN). يحتوي PA-TGS-REQ على التذكرة التي تم تلقيها لطلب خدمة Kerberos (اسم مضيف ASA هو الأساسي).

يحصل ASA على إستجابة صحيحة مع التذكرة المتحلة للمستخدم cisco (التذكرة 2 الموضحة في الخطوة 4):

| No. | Time                       | Source       | Destination  | Protocol | Length | Info    |
|-----|----------------------------|--------------|--------------|----------|--------|---------|
| 13  | 2013-02-15 11:56:37.465857 | 10.211.0.162 | 10.211.0.221 | KRB5     | 77     | TGS-REQ |
| 14  | 2013-02-15 11:56:37.468588 | 10.211.0.221 | 10.211.0.162 | KRB5     | 1354   | TGS-REP |
| 16  | 2013-02-15 11:56:37.563325 | 10.211.0.162 | 10.211.0.221 | KRB5     | 1003   | TGS-REQ |

```

Frame 14: 1354 bytes on wire (10832 bits), 1354 bytes captured (10832 bits)
Ethernet II, Src: Vmware_9c:5d:90 (00:50:56:9c:5d:90), Dst: Cisco_e1:a0:3c (2c:54:2d:e1:a0:3c)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 211
Internet Protocol Version 4, Src: 10.211.0.221 (10.211.0.221), Dst: 10.211.0.162 (10.211.0.162)
User Datagram Protocol, Src Port: kerberos (88), Dst Port: netopia-vo1 (1839)
Kerberos TGS-REP
  Pvno: 5
  MSG Type: TGS-REP (13)
  Client Realm: KRA-SEC.CISCO.COM
  Client Name (Principal): cisco
    Name-type: Principal (1)
    Name: cisco
  Ticket
  enc-part rc4-hmac

```

فيما يلي طلب التذكرة لخدمة HTTP (يتم حذف بعض الأخطاء للوضوح):

```

KRA-S-ASA-05# show WebVPN kcd
Kerberos Realm: TEST-CISCO.COM
Domain Join : Complete

/ - find_spn_in_url(): URL
build_host_spn(): host - test.kra-sec.cisco.com
build_host_spn(): SPN - HTTP/test.kra-sec.cisco.com
.KCD_unicorn_get_cred(): Attempting to retrieve required KCD tickets

```

```

In KCD_check_cache_validity, Checking cache validity for type KCD service
    .ticket cache name: and spn HTTP/test.kra-sec.cisco.com
    . In kerberos_cache_open: KCD opening cache
        !Cache doesn't exist
In KCD_check_cache_validity, Checking cache validity for type KCD self ticket
    .cache name: a6ad760 and spn N/A
    .In kerberos_cache_open: KCD opening cache a6ad760
        .Credential is valid
In KCD_check_cache_validity, Checking cache validity for type KCD impersonate
    .ticket cache name: and spn N/A
    . In kerberos_cache_open: KCD opening cache
        !Cache doesn't exist
:KCD requesting impersonate ticket retrieval for
user      : cisco
    in_cache : a6ad760
    out_cache: adab04f8I
    .Successfully queued up AAA request to retrieve KCD tickets
        kerberos mkreq: 0x4
    kip_lookup_by_sessID: kip with id 4 not found
        alloc_kip 0xaceaf560
        (new request 0x4 --> 1 (0xaceaf560
            add_req 0xaceaf560 session 0x4 id 1
                In KCD_cred_tkt_build_request
    .In kerberos_cache_open: KCD opening cache a6ad760
    KCD_cred_tkt_build_request: using KRA-S-ASA-05 for principal name
        In kerberos_open_connection
            In kerberos_send_request

***** START: KERBEROS PACKET DECODE *****
    Kerberos: Message type KRB_TGS_REQ
    Kerberos: Preauthentication type ap request
    Kerberos: Preauthentication type unknown
    Kerberos: Option forwardable
    Kerberos: Option renewable
    Kerberos: Client Realm KRA-SEC.CISCO.COM
    Kerberos: Server Name KRA-S-ASA-05
    Kerberos: Start time 0
    Kerberos: End time -1381294376
    Kerberos: Renew until time 0
    Kerberos: Nonce 0xe9d5fd7f
    Kerberos: Encryption type rc4-hmac-md5
    Kerberos: Encryption type des3-cbc-sha
    Kerberos: Encryption type des-cbc-md5
    Kerberos: Encryption type des-cbc-crc
    Kerberos: Encryption type des-cbc-md4
***** END: KERBEROS PACKET DECODE *****
    In kerberos_rcv_msg
    In KCD_cred_tkt_process_response

***** START: KERBEROS PACKET DECODE *****
    Kerberos: Message type KRB_TGS_REP
    Kerberos: Client Name cisco
    Kerberos: Client Realm KRA-SEC.CISCO.COM
***** END: KERBEROS PACKET DECODE *****
    .KCD_unicorn_callback(): called with status: 1
Successfully retrieved impersonate ticket for user: cisco
    :KCD callback requesting service ticket retrieval for
        user
        in_cache : a6ad760
        out_cache: adab04f8S
        DC_cache : adab04f8I
        SPN      : HTTP/test.kra-sec.cisco.com
    .Successfully queued up AAA request from callback to retrieve KCD tickets
        In kerberos_close_connection

```

```

remove_req 0xaceaf560 session 0x4 id 1
      free_kip 0xaceaf560
      kerberos mkreq: 0x5
kip_lookup_by_sessID: kip with id 5 not found
      alloc_kip 0xaceaf560
(new request 0x5 --> 2 (0xaceaf560
  add_req 0xaceaf560 session 0x5 id 2
    In KCD_cred_tkt_build_request
      .In kerberos_cache_open: KCD opening cache a6ad760
      .In kerberos_cache_open: KCD opening cache adab04f8I
        In kerberos_open_connection
          In kerberos_send_request

```

```

***** START: KERBEROS PACKET DECODE *****
      Kerberos: Message type KRB_TGS_REQ
      Kerberos: Preauthentication type ap request
      Kerberos: Option forwardable
      Kerberos: Option renewable
      Kerberos: Client Realm KRA-SEC.CISCO.COM
      Kerberos: Server Name HTTP
      Kerberos: Start time 0
      Kerberos: End time -1381285944
      Kerberos: Renew until time 0
      Kerberos: Nonce 0x750cf5ac
      Kerberos: Encryption type rc4-hmac-md5
      Kerberos: Encryption type des3-cbc-sha
      Kerberos: Encryption type des-cbc-md5
      Kerberos: Encryption type des-cbc-crc
      Kerberos: Encryption type des-cbc-md4
***** END: KERBEROS PACKET DECODE *****

```

```

In kerberos_rcv_msg
  In KCD_cred_tkt_process_response

```

```

***** START: KERBEROS PACKET DECODE *****
      Kerberos: Message type KRB_TGS_REP
      Kerberos: Client Name cisco
      Kerberos: Client Realm KRA-SEC.CISCO.COM
***** END: KERBEROS PACKET DECODE *****

```

```

.KCD_unicorn_callback(): called with status: 1
Successfully retrieved service ticket
for user cisco, spn HTTP/test.kra-sec.cisco.com

```

```

  In kerberos_close_connection
    remove_req 0xaceaf560 session 0x5 id 2
      free_kip 0xaceaf560
      kerberos: work queue empty
    ,ucte_krb_authenticate_connection(): ctx - 0xad045dd0, proto - http
      host - test.kra-sec.cisco.com
    .In kerberos_cache_open: KCD opening cache adab04f8S
      Source: cisco@KRA-SEC.CISCO.COM
Target: HTTP/test.kra-sec.cisco.com@KRA-SEC.CISCO.COM

```

يتلقى ASA التذكرة المتتلة الصحيحة لخدمة HTTP (التذكرة 3 الموضحة في الخطوة 6).

يمكن التحقق من كلا التذكرتين. الأولى هي التذكرة المتتلة للمستخدم **cisco**، والتي يتم إستخدامها لطلب التذكرة الثانية وإستلامها لخدمة HTTP التي يتم الوصول إليها:

```

KRA-S-ASA-05(config)# show aaa kerberos
Default Principal: cisco@KRA-SEC.CISCO.COM
Valid Starting Expires Service Principal
CEST Oct 2 2013 05:37:33 CEST Oct 3 2013 KRA-S-ASA-05@KRA-SEC.CISCO.COM 19:38:10
Default Principal: cisco@KRA-SEC.CISCO.COM

```

Valid Starting Expires Service Principal

CEST Oct 2 2013 05:37:33 CEST Oct 3 2013 19:38:10

HTTP/test.kra-sec.cisco.com@KRA-SEC.CISCO.COM

يتم استخدام تذكرة (HTTP (TICKET3) هذه للوصول إلى HTTP (مع SPNEGO)، ولا يحتاج المستخدم إلى توفير أي بيانات اعتماد.

## استكشاف الأخطاء وإصلاحها

قد تواجه أحيانا مشكلة في التفويض غير الصحيح. على سبيل المثال، يستخدم ASA تذكرة لطلب الخدمة :ERR\_BADOPTION مع KRB-ERROR ولكن الاستجابة هي (الخطوة 5)،

|    |                            |              |              |      |   |
|----|----------------------------|--------------|--------------|------|---|
| 13 | 2013-02-13 03:09:09.766714 | 10.211.0.162 | 10.211.0.216 | KRB5 | 1437 TGS-REQ  |
| 14 | 2013-02-13 03:09:09.768896 | 10.211.0.216 | 10.211.0.162 | KRB5 | 1238 TGS-REP  |
| 15 | 2013-02-13 03:09:09.864655 | 10.211.0.162 | 10.211.0.216 | IPv4 | 1518 Fragmented IP protocol (proto=UDP 17, off=0, ID=649b) [Reassembled |
| 16 | 2013-02-13 03:09:09.864686 | 10.211.0.162 | 10.211.0.216 | KRB5 | 794 TGS-REQ   |
| 17 | 2013-02-13 03:09:09.866639 | 10.211.0.216 | 10.211.0.162 | KRB5 | 191 KRB Error: KRB5KDC_ERR_BADOPTION NT Status: STATUS_NOT_SUPPORTED    |
| 18 | 2013-02-13 03:09:09.998941 | 10.211.0.162 | 10.211.0.216 | TCP  | 78 composit-server > http [FIN, PSH, ACK] Seq=2651324832 Ack=25924572   |

```
Frame 17: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits) on interface 0/21
Ethernet II, Src: Vmware_9c:34:99 (00:50:56:9c:34:99), Dst: Cisco_e1:a0:3c (2c:54:2d:e1:a0:3c)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 211
Internet Protocol Version 4, Src: 10.211.0.216 (10.211.0.216), Dst: 10.211.0.162 (10.211.0.162)
User Datagram Protocol, Src Port: kerberos (888), Dst Port: 40976 (40976)
Kerberos KRB-ERROR
  Pkno: 5
  MSG Type: KRB-ERROR (30)
  stime: 2013-02-13 02:09:09 (UTC)
  susec: 344906
  error_code: KRB5KDC_ERR_BADOPTION (13)
  Realm: KRA-SEC.CISCO.COM
  Server Name (Principal): HTTP/kra-sec-dc2.kra-sec.cisco.com
  e-data PA-PW-SALT (3)
    Type: PA-PW-SALT (3)
      Value: 1b0000c0000000003000000
      NT Status: STATUS_NOT_SUPPORTED (0xc00000bb)
      Unknown: 0x00000000
      Unknown: 0x00000003
```

هذه مشكلة نموذجية تمت مواجهتها عند عدم تكوين التفويض بشكل صحيح. يذكر ASA أن "KDC لا يستطيع الوفاء بالخيار المطلوب":

```
,KRA-S-ASA-05# ucte_krb_get_auth_cred(): ctx = 0xcc4b5390
WebVPN_session = 0xc919a260, protocol = 1
/ - find_spn_in_url(): URL
build_host_spn(): host - test.kra-sec.cisco.com
build_host_spn(): SPN - HTTP/test.kra-sec.cisco.com
.KCD_unicorn_get_cred(): Attempting to retrieve required KCD tickets
In KCD_check_cache_validity, Checking cache validity for type KCD service ticket
.cache name: and spn HTTP/test.kra-sec.cisco.com
. In kerberos_cache_open: KCD opening cache
!Cache doesn't exist
In KCD_check_cache_validity, Checking cache validity for type KCD self ticket
.cache name: a6588e0 and spn N/A
.In kerberos_cache_open: KCD opening cache a6588e0
.Credential is valid
In KCD_check_cache_validity, Checking cache validity for type KCD impersonate
.ticket cache name: and spn N/A
. In kerberos_cache_open: KCD opening cache
!Cache doesn't exist
:KCD requesting impersonate ticket retrieval for
user : cisco
in_cache : a6588e0
out_cache: c919a260I
.Successfully queued up AAA request to retrieve KCD tickets
kerberos mkreq: 0x4
kip_lookup_by_sessID: kip with id 4 not found
alloc_kip 0xcc09ad18
(new request 0x4 --> 1 (0xcc09ad18
```

```
add_req 0xcc09ad18 session 0x4 id 1
  In KCD_cred_tkt_build_request
    .In kerberos_cache_open: KCD opening cache a6588e0
KCD_cred_tkt_build_request: using KRA-S-ASA-05$ for principal name
  In kerberos_open_connection
    In kerberos_send_request
***** START: KERBEROS PACKET DECODE *****
  Kerberos: Message type KRB_TGS_REQ
  Kerberos: Preauthentication type ap request
  Kerberos: Preauthentication type unknown
  Kerberos: Option forwardable
  Kerberos: Option renewable
  Kerberos: Client Realm KRA-SEC.CISCO.COM
  Kerberos: Server Name KRA-S-ASA-05$
  Kerberos: Start time 0
  Kerberos: End time -856104128
  Kerberos: Renew until time 0
  Kerberos: Nonce 0xb086e4a5
  Kerberos: Encryption type rc4-hmac-md5
  Kerberos: Encryption type des3-cbc-sha
  Kerberos: Encryption type des-cbc-md5
  Kerberos: Encryption type des-cbc-crc
  Kerberos: Encryption type des-cbc-md4
***** END: KERBEROS PACKET DECODE *****
  In kerberos_rcv_msg
    In KCD_cred_tkt_process_response
***** START: KERBEROS PACKET DECODE *****
  Kerberos: Message type KRB_TGS_REP
  Kerberos: Client Name cisco
  Kerberos: Client Realm KRA-SEC.CISCO.COM
***** END: KERBEROS PACKET DECODE *****
  .KCD_unicorn_callback(): called with status: 1
Successfully retrieved impersonate ticket for user: cisco
:KCD callback requesting service ticket retrieval for
      : user
      in_cache : a6588e0
      out_cache: c919a260S
      DC_cache : c919a260I
SPN : HTTP/test.kra-sec.cisco.com
.Successfully queued up AAA request from callback to retrieve KCD tickets
  In kerberos_close_connection
    remove_req 0xcc09ad18 session 0x4 id 1
      free_kip 0xcc09ad18
      kerberos mkreq: 0x5
    kip_lookup_by_sessID: kip with id 5 not found
      alloc_kip 0xcc09ad18
      (new request 0x5 --> 2 (0xcc09ad18)
      add_req 0xcc09ad18 session 0x5 id 2
        In KCD_cred_tkt_build_request
          .In kerberos_cache_open: KCD opening cache a6588e0
          .In kerberos_cache_open: KCD opening cache c919a260I
            In kerberos_open_connection
              In kerberos_send_request
***** START: KERBEROS PACKET DECODE *****
  Kerberos: Message type KRB_TGS_REQ
  Kerberos: Preauthentication type ap request
  Kerberos: Option forwardable
  Kerberos: Option renewable
  Kerberos: Client Realm KRA-SEC.CISCO.COM
  Kerberos: Server Name HTTP
  Kerberos: Start time 0
  Kerberos: End time -856104568
  Kerberos: Renew until time 0
  Kerberos: Nonce 0xf84c9385
```

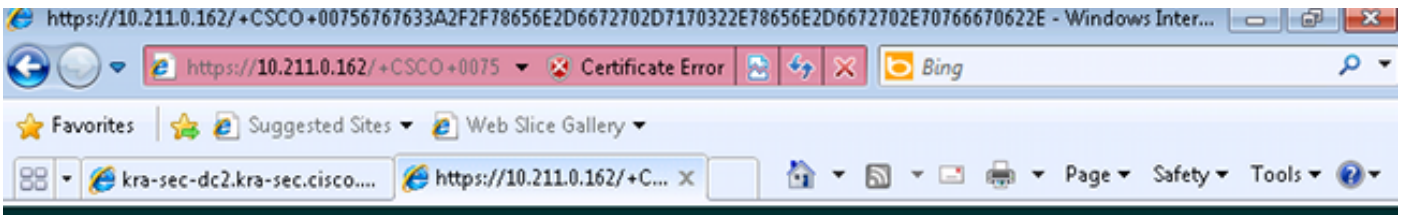
```

Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des3-cbc-sha
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4
***** END: KERBEROS PACKET DECODE *****
      In kerberos_rcv_msg
      In KCD_cred_tkt_process_response
***** START: KERBEROS PACKET DECODE *****
      Kerberos: Message type KRB_ERROR
Kerberos: Error type: KDC can't fulfill requested option, -1765328371
      (0x96c73a0d)
      Kerberos: Server time 1360917437
      Kerberos: Realm KRA-SEC.CISCO.COM
      Kerberos: Server Name HTTP
***** END: KERBEROS PACKET DECODE *****
"Kerberos library reports: "KDC can't fulfill requested option
      .KCD_unicorn_callback(): called with status: -3
      .KCD callback called with AAA error -3
      In kerberos_close_connection
      remove_req 0xcc09ad18 session 0x5 id 2
      free_kip 0xcc09ad18
      kerberos: work queue empty

```

وهي أساسا نفس المشكلة الموصوفة في الالتقاط - حيث أن الفشل هو في TGS\_REQ مع BAD\_OPTION.

إذا كانت الاستجابة ناجحة، فيستلم ASA تذكرة لخدمة [HTTP/test.kra-sec.cisco.com](http://test.kra-sec.cisco.com)، والتي يتم إستخدامها لمفاوضات SPNEGO. ومع ذلك، بسبب الفشل، يتم التفاوض مع مدير شبكة (NTLM) (LAN NT)، ويجب على المستخدم توفير بيانات الاعتماد:



Home  Logout 

Web Server Authentication Required

Enter your username and password

Username:

Password:

تأكد من تسجيل SPN لحساب واحد فقط (برنامج نصي من المقالة السابقة). عندما تتلقى هذا الخطأ، **KRB\_AP\_ERR\_MODIFIED**، فإنه يعني عادة أن SPN غير مسجل للحساب الصحيح. يجب أن يتم تسجيله للحساب الذي يتم إستخدامه لتشغيل التطبيق (تجمع التطبيقات على IIS).



| No. | Time       | Source       | Destination  | Protocol | Length | Info                         |
|-----|------------|--------------|--------------|----------|--------|------------------------------|
| 24  | 1.30011200 | 10.211.0.216 | 10.211.0.220 | TCP      | 1314   | [TCP segment of a reassemble |
| 25  | 1.30013200 | 10.211.0.216 | 10.211.0.220 | HTTP     | 703    | KRB Error: KRB5KRB_AP_ERR_MO |
| 26  | 1.30014900 | 10.211.0.220 | 10.211.0.216 | TCP      | 54     | 51211 > http [ACK] Seq=9029  |
| 27  | 1.30090400 | 10.211.0.220 | 10.211.0.216 | TCP      | 54     | 51211 > http [FIN, ACK] Seq= |
| 28  | 1.30207500 | 10.211.0.216 | 10.211.0.220 | TCP      | 60     | http > 51211 [ACK] seq=7669  |
| 29  | 1.30209800 | 10.211.0.216 | 10.211.0.220 | TCP      | 60     | http > 51211 [FIN, ACK] seq= |
| 30  | 1.30211600 | 10.211.0.220 | 10.211.0.216 | TCP      | 54     | 51211 > http [ACK] Seq=9030  |

```

MSG Type: KRB-ERROR (30)
stime: 2013-02-13 06:07:41 (UTC)
susec: 589659
error_code: KRB5KRB_AP_ERR_MODIFIED (41)
Realm: KRA-SEC.CISCO.COM
Server Name (Service and Host): host/kra-sec-dc2.kra-sec.cisco.com
Name-type: Service and Host (3)
Name: host
Name: kra-sec-dc2.kra-sec.cisco.com

```

عندما تتلقى هذا الخطأ، KRB\_ERR\_C\_PRINCIPAL\_UNKNOWN، فهذا يعني أنه لا يوجد مستخدم على DC (مستخدم Cisco WebVPN).

|    |                            |              |              |      |      |  |
|----|----------------------------|--------------|--------------|------|------|--|
| 9  | 2013-02-13 02:25:22.496434 | 10.211.0.162 | 10.211.0.216 | KRB5 | 231  | AS-REQ   |
| 10 | 2013-02-13 02:25:22.497319 | 10.211.0.216 | 10.211.0.162 | KRB5 | 339  | KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED                            |
| 11 | 2013-02-13 02:25:22.595779 | 10.211.0.162 | 10.211.0.216 | KRB5 | 388  | AS-REQ   |
| 12 | 2013-02-13 02:25:22.786824 | 10.211.0.216 | 10.211.0.162 | IPv4 | 1318 | Fragmented IP protocol (proto=UDP 17, off=0, ID=951f) [Reassembled |
| 13 | 2013-02-13 02:25:22.786839 | 10.211.0.216 | 10.211.0.162 | KRB5 | 64   | AS-REP   |
| 14 | 2013-02-13 02:25:22.797459 | 10.211.0.162 | 10.211.0.216 | KRB5 | 1437 | TGS-REQ  |
| 15 | 2013-02-13 02:25:22.886385 | 10.211.0.216 | 10.211.0.162 | KRB5 | 140  | KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN                         |

```

Frame 15: 148 bytes on wire (1128 bits), 148 bytes captured (1128 bits)
Ethernet II, Src: VMware_9c:34:99 (00:50:56:9c:34:99), Dst: Cisco_e1:a0:3c (2c:54:2d:e1:a0:3c)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 211
Internet Protocol Version 4, Src: 10.211.0.216 (10.211.0.216), Dst: 10.211.0.162 (10.211.0.162)
User Datagram Protocol, Src Port: kerberos (88), Dst Port: 17412 (17412)
Kerberos KRB-ERROR
Pvno: 5
MSG Type: KRB-ERROR (30)
stime: 2013-02-13 01:25:22 (UTC)
susec: 759593
error_code: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN (6)
Realm: KRA-SEC.CISCO.COM
Server Name (Principal): KRA-S-ASA-05$
Name-type: Principal (1)
Name: KRA-S-ASA-05$

```

قد تواجه هذه المشكلة عند الانضمام إلى المجال. يستلم ASA as-rep، ولكنه يفشل على LSA مستوى مع الخطأ: STATUS\_ACCESS\_DENY

|     |                            |              |              |        |     |   |
|-----|----------------------------|--------------|--------------|--------|-----|---|
| 110 | 2013-02-15 02:03:57.367992 | 10.211.0.221 | 10.211.0.162 | LSARPC | 182 | lsa OpenPolicy2 response, STATUS_ACCESS_DENIED, Error: ST |
| 111 | 2013-02-15 02:03:57.368083 | 10.211.0.162 | 10.211.0.221 | TCP    | 70  | 14768 > microsoft-ds [ACK] Seq=3862823345 Ack=2111834843  |

```

Frame 110: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits)
Ethernet II, Src: VMware_9c:3d:98 (00:50:56:9c:3d:98), Dst: Cisco_e1:a0:3c (2c:54:2d:e1:a0:3c)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 211
Internet Protocol Version 4, Src: 10.211.0.221 (10.211.0.221), Dst: 10.211.0.162 (10.211.0.162)
Transmission Control Protocol, Src Port: microsoft-ds (445), Dst Port: 14768 (14768), Seq: 2111834731, Ack: 3862823345, Len: 112
NetBIOS Session Service
SMB (Server Message Block Protocol)
Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Response, Fragment: Single, FragLen: 48, Call: 219 Ctx: 1, [Req: #106]
Local Security Authority, lsa_OpenPolicy2
Operation: lsa_OpenPolicy2 (44)
[Request in frame: 186]
Pointer to Handle (policy_handle)
NT Error: STATUS_ACCESS_DENIED (0xc0000022)

```

لحل هذه المشكلة، يجب تمكين/تعطيل المصادقة المسبقة على DC لذلك المستخدم (المسؤول).

هنا بعض المشاكل الأخرى التي قد تواجهك:

- قد تكون هناك مشاكل عند الانضمام إلى المجال. إذا كان لخادم DC محولات متعددة لوحدة تحكم واجهة الشبكة (NIC) (عناوين IP متعددة)، فتأكد من إمكانية وصول ASA إليها جميعها للانضمام إلى المجال (يتم إختياره بشكل عشوائي بواسطة العميل استناداً إلى إستجابة خادم اسم المجال (DNS)).



- لا تقم بتعيين SPN على أنه HOST/dc.kra-sec.cisco.com لحساب Administrator. من الممكن فقدان الاتصال بـ DC بسبب هذا الإعداد.
- بعد انضمام ASA إلى المجال، من الممكن التحقق من إنشاء حساب الكمبيوتر الصحيح على DC (اسم مضيف (ASA). تأكد من أن المستخدم لديه الأذونات الصحيحة لإضافة حسابات كمبيوتر (في هذا المثال، يمتلك المسؤول الأذونات الصحيحة).
- تذكر تكوين بروتوكول وقت الشبكة (NTP) الصحيح على ASA. بشكل افتراضي، تقبل وحدة التحكم بالمجال (DC) انحراف لمدة خمس دقائق. يمكن تغيير المؤقت في DC.
- تحقق من استخدام اتصال Kerberos للحزمة الصغيرة UDP/88. بعد الخطأ من وحدة التحكم بالمجال DC وKRB5KDC\_ERR\_RESPONSE\_TOO\_BIG، يتحول العميل إلى TCP/88. من الممكن إجبار عميل Windows على استخدام TCP/88، ولكن ASA سيستخدم UDP بشكل افتراضي.
- DC: عند إجراء تغييرات في السياسة، تذكر Gpupdate /force.
- ASA: اختبر المصادقة باستخدام الأمر test aaa، ولكن تذكر أنها مجرد مصادقة بسيطة.
- من أجل استكشاف الأخطاء وإصلاحها على موقع وحدة التحكم بالمجال (DC)، من المفيد تمكين تصحيح أخطاء Kerberos: [كيفية تمكين تسجيل أحداث Kerberos](#).

## معرفة الأخطاء من Cisco

هنا قائمة بمعرفة الأخطاء ذات الصلة من Cisco:

- معرف تصحيح الأخطاء من ASA - Cisco [CSCsi32224](#) لا يتحول إلى TCP بعد إستلام رمز خطأ Kerberos 52
- معرف تصحيح الأخطاء من Cisco [CSCtd92673](#) - تفشل مصادقة Kerberos مع تمكين المصادقة المسبقة
- معرف تصحيح الأخطاء من ASA WebVPN KCD - Cisco [CSCuj19601](#) - يحاول الانضمام إلى AD فقط بعد إعادة التمهيد
- معرف تصحيح الأخطاء من ASA KCD - Cisco [CSCuh32106](#) مكسور في 8.4.5 وما بعده

## معلومات ذات صلة

- [حول تفويض Kerberos المقيد](#)
- [فهم كيفية عمل KCD](#)
- [PIX/ASA: مجموعات خوادم مصادقة Kerberos وتفويض LDAP لمستخدمي عميل VPN غير مثال تكوين ASDM/CLI](#)
- [مرجع أوامر سلسلة ASA من Cisco](#)
- [KDC\\_ERR\\_BADOPTION عند محاولة التفويض المقيد](#)
- [كيفية إجبار Kerberos على استخدام TCP بدلا من UDP في Windows](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إلمءءاد ءوچرلاب ةصوء و تاملرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزىلچنل اءل دن تسمل