دمج SSO ل WebVPN مع مثال تكوين Kerberos المقيد التفويض

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين تسجيل الدخول الأحادي ل WebVPN (SSO) 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 (SSL) VPN
- 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 وتأكيدها.

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؛ وبدلا من ذلك، يتم إستخدام الحساب الذي تم إستخدامه 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 إستخدام هذه التذكرة في الخطوات التالية للوصول إلى خدمات Kerberos.

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

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

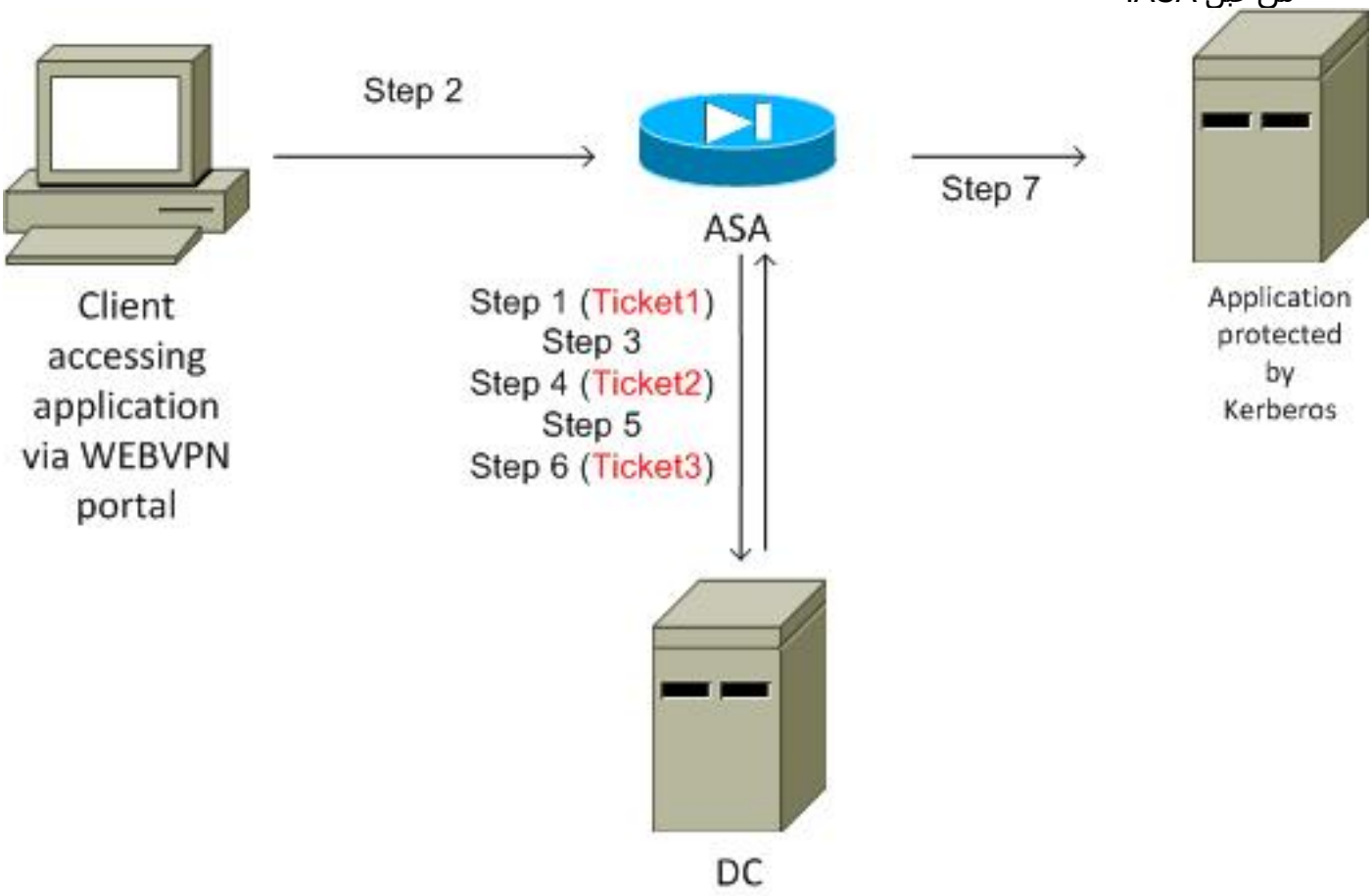
4. واستجابة لذلك، يتلقى مكتب خدمات المحاسبة تذكرة منتحلة (التذكرة 2) بالنيابة عن مستخدم شبكة WebVPN (**TGS_REP**) لحساب الكمبيوتر. يتم إستخدام هذه التذكرة لطلب تذاكر التطبيق نيابة عن مستخدم WebVPN هذا.

5. ويبدأ مكتب المحاسبة طلبا 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 المنتحلة المستلمة في الخطوة 4.

6. يتم إرجاع الاستجابة (**TGS_REQ**) باستخدام التذكرة المنتحلة (TICKET3) للتطبيق.

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



التكوين

طوبولوجيا

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

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

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

ASA: 10.211.0.162

اسم مستخدم/كلمة مرور WebVPN: cisco/cisco

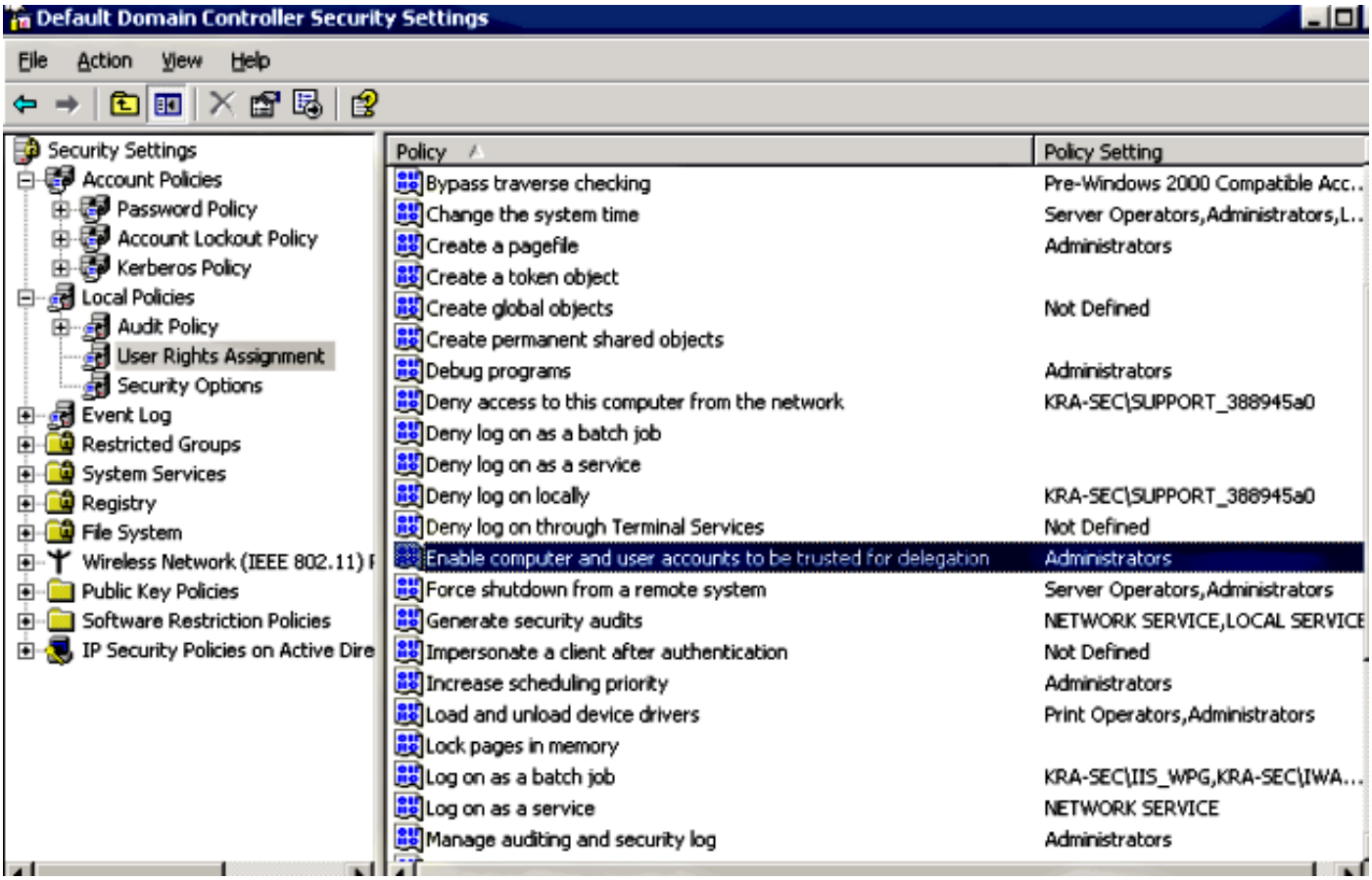
الملف المرفق: asa-join.pcap (انضمام ناجح إلى المجال)

الملف المرفق: asa-kerberos-bad.pcap (طلب الخدمة)

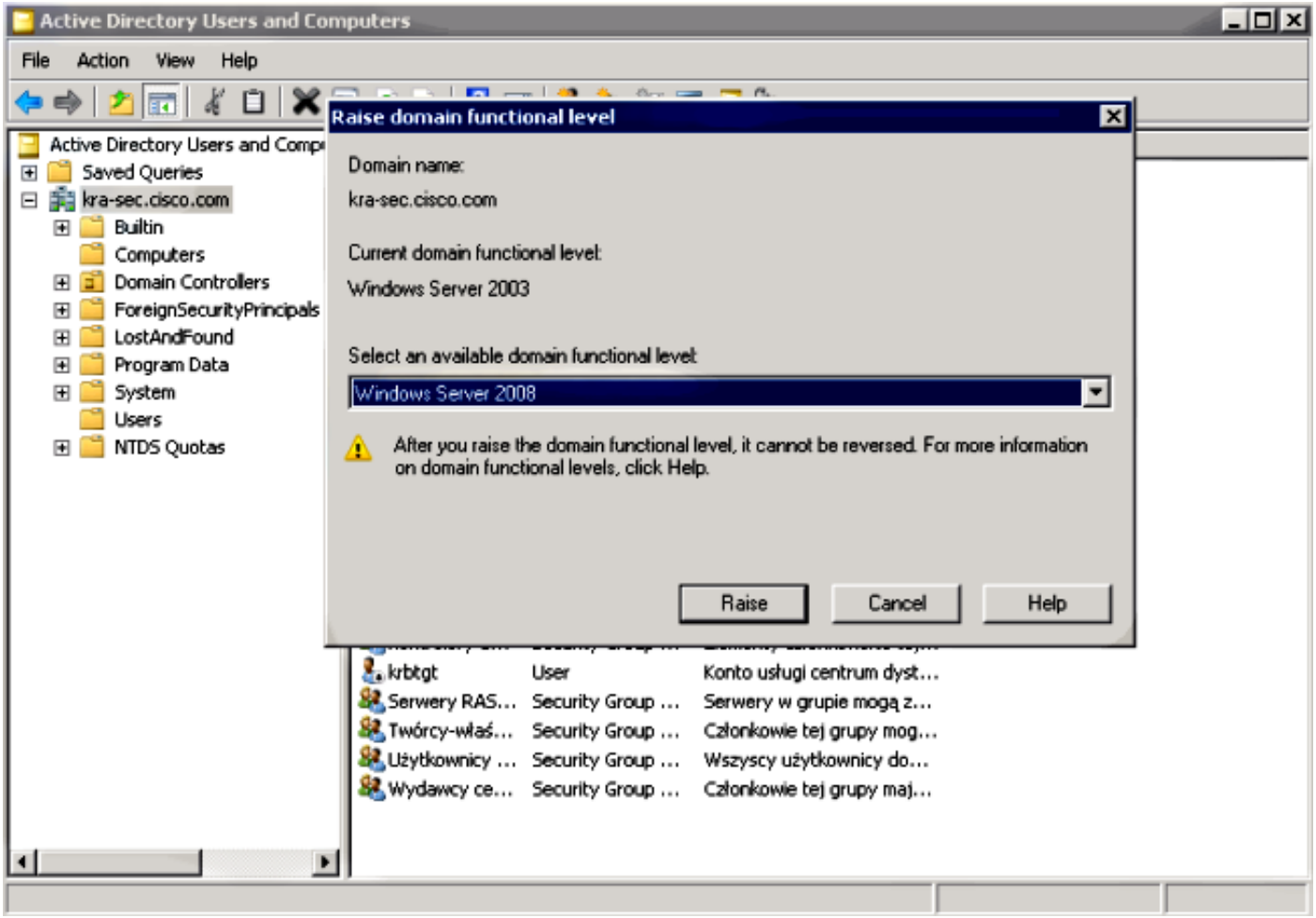
وحدة التحكم بالمجال وتكوين التطبيق

إعدادات المجال

من المفترض أن هناك بالفعل تطبيق IIS7 وظيفي محمي بواسطة Kerberos (إذا لم يكن الأمر كذلك، فاقرأ 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)

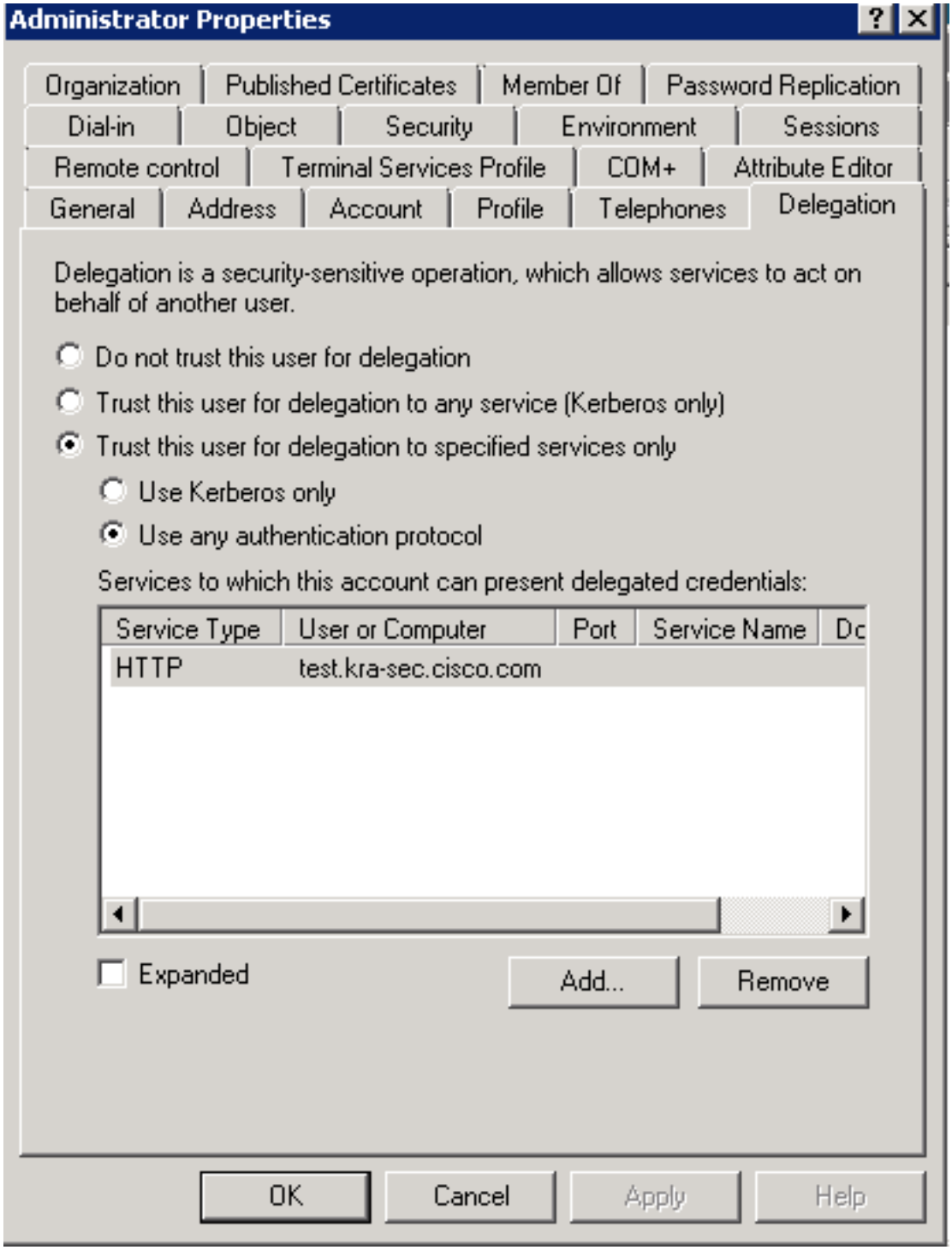
يجب تكوين أي حساب على AD بتفويض صحيح. يتم إستخدام حساب مسؤول. وعندما يستخدم مكتب المحاسبة هذا الحساب، يكون قادرا على طلب تذكرة بالنيابة عن مستخدم آخر (تفويض مقيد) للخدمة المحددة (تطبيق HTTP). ولكي يحدث ذلك، يجب إنشاء التفويض الصحيح للتطبيق/الخدمة.

من أجل جعل هذا التفويض عبر واجهة سطر الأوامر مع **setSPN.exe**، والذي يعد جزءا 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
```

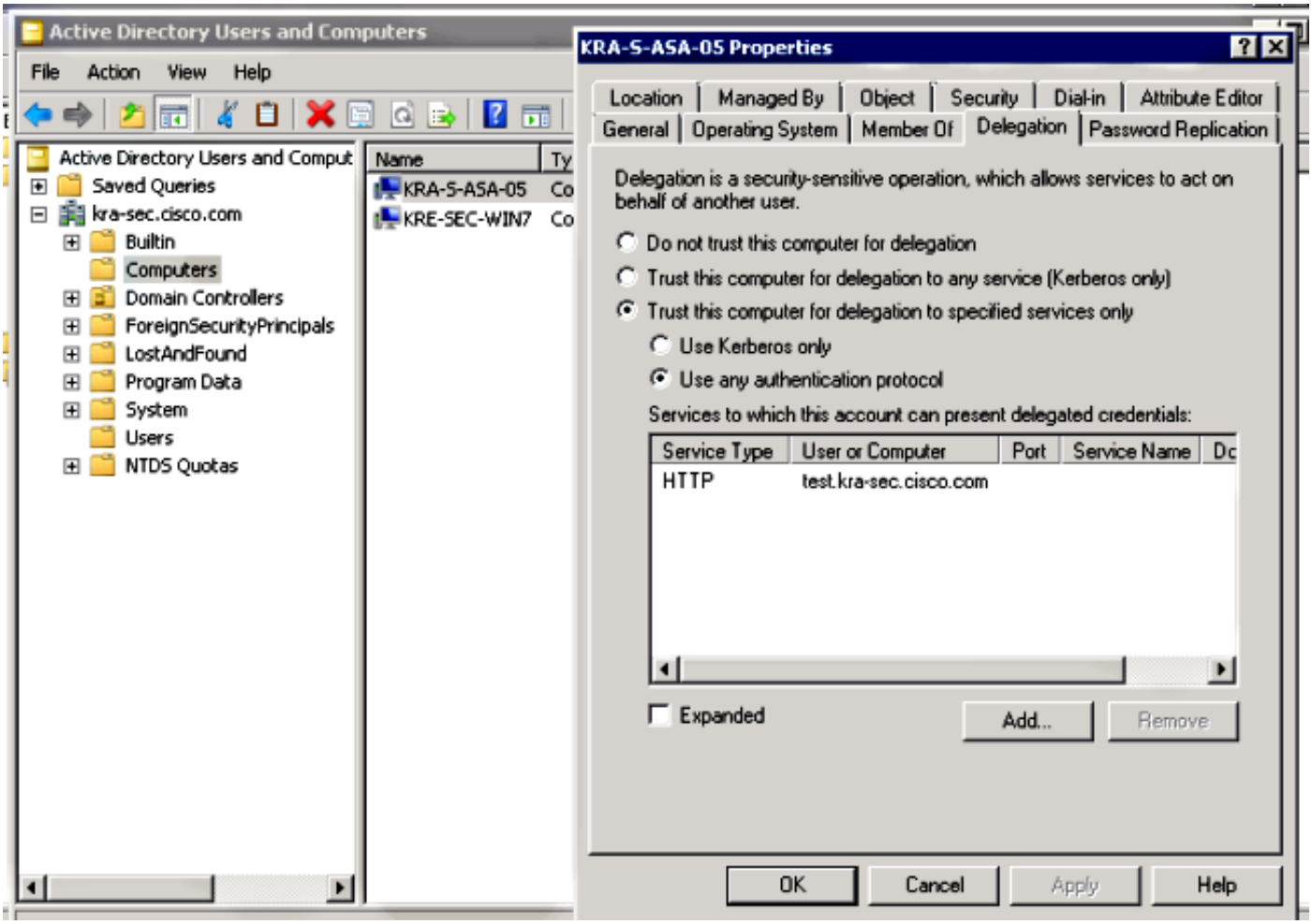
وهذا يشير إلى أن اسم مستخدم **Administrator** هو الحساب الموثوق به لتفويض خدمة HTTP في **test.kra-sec.cisco.com**.

يعد الأمر **SPN** ضروريا أيضا لتنشيط علامة التبويب **تفويض** لذلك المستخدم. بمجرد إدخال الأمر، تظهر علامة التبويب "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 إستخدام 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"):



تشكيل على 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 3USUcOPFUiMCO4Jk 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

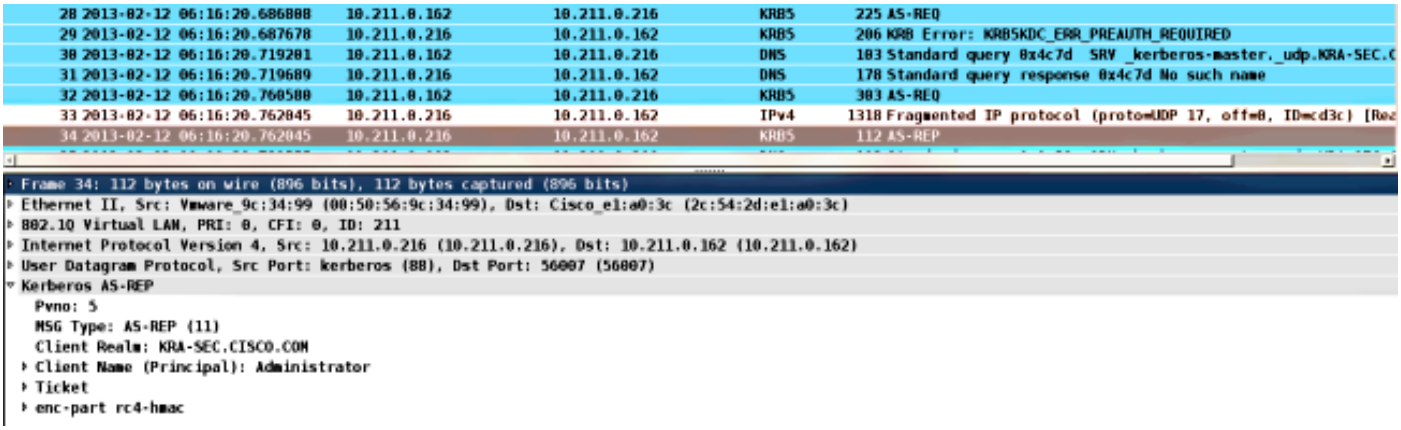
ينضم ASA إلى المجال

بعد إستخدام 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
```

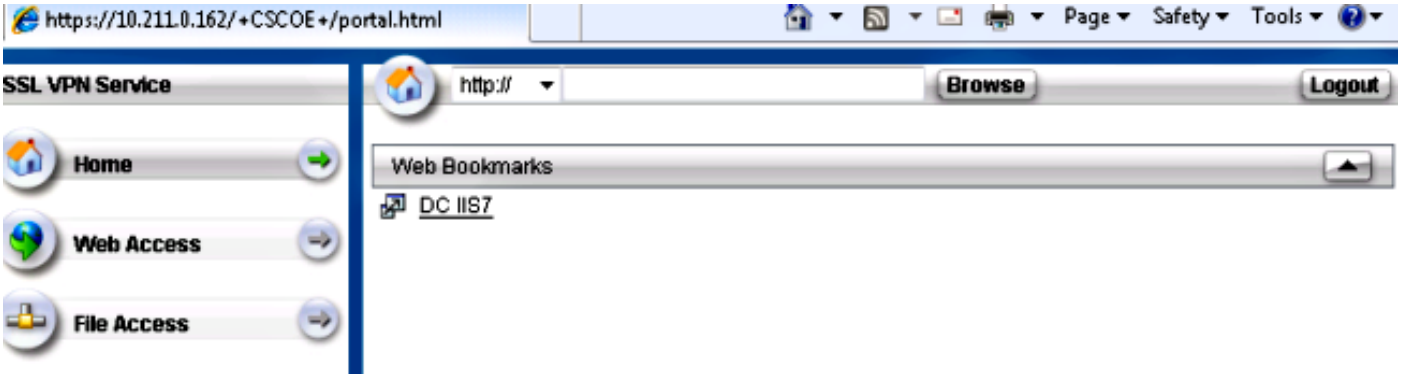
```
                                    Kerberos: Server Name krbtgt
                                          Kerberos: Start time 0
                                   Kerberos: End time -878667256
                                Kerberos: Renew until time -878672192
                                     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).

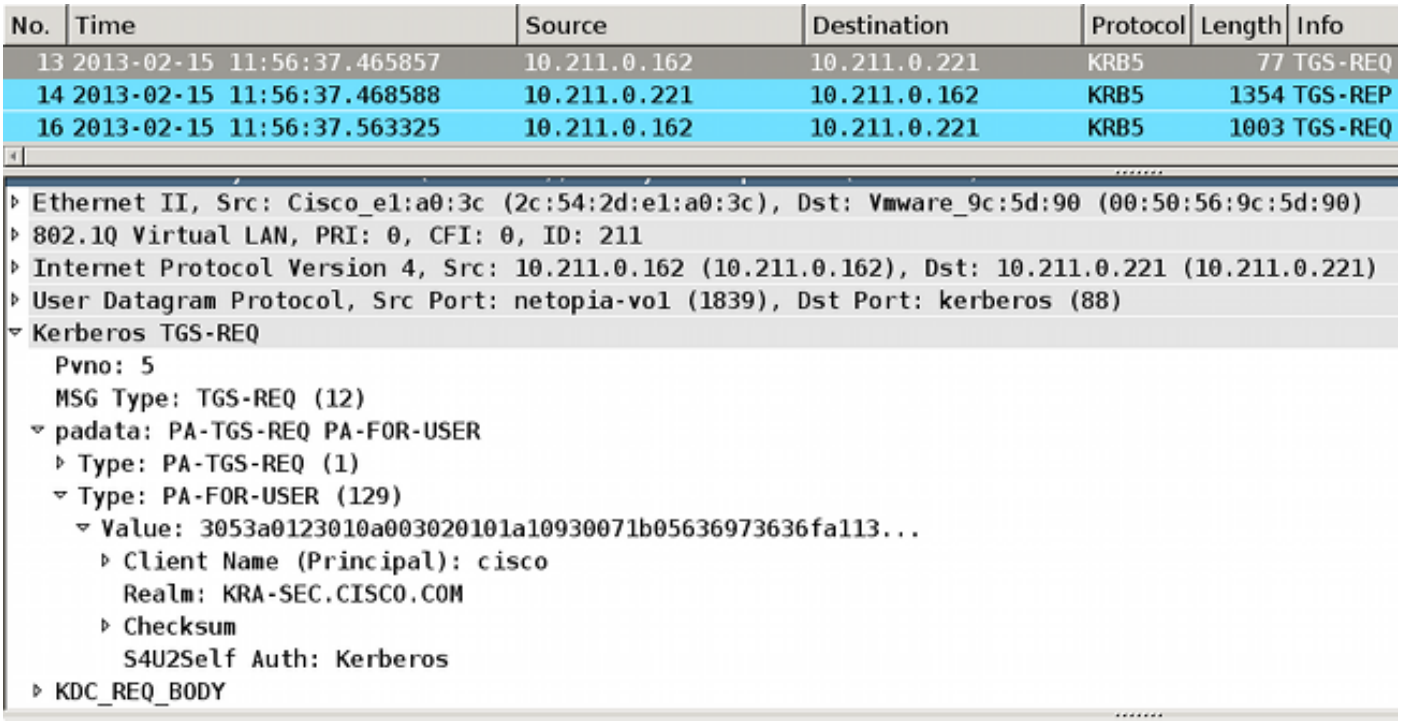


طلب الخدمة

المستخدم ينقر إرتباط WebVPN:

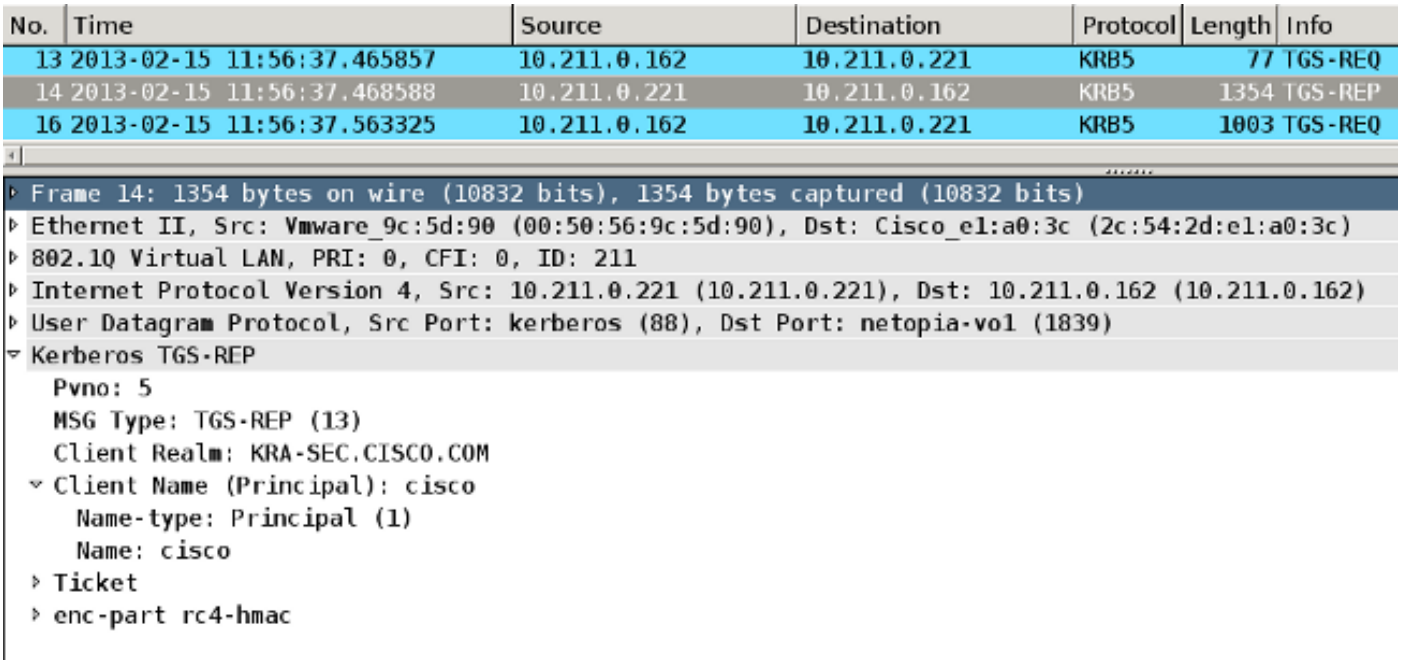


يرسل ASA TGS_REQ للتذكرة المنتحلة مع التذكرة التي يتم استقبالها في حزمة AS_REP:



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 المنتحلة للمستخدم **cisco** (التذكرة 2 الموضحة في الخطوة 4):



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_recv_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_recv_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 المنتحلة الصحيحة لخدمة HTTP (التذكرة 3 الموضحة في الخطوة 6).

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

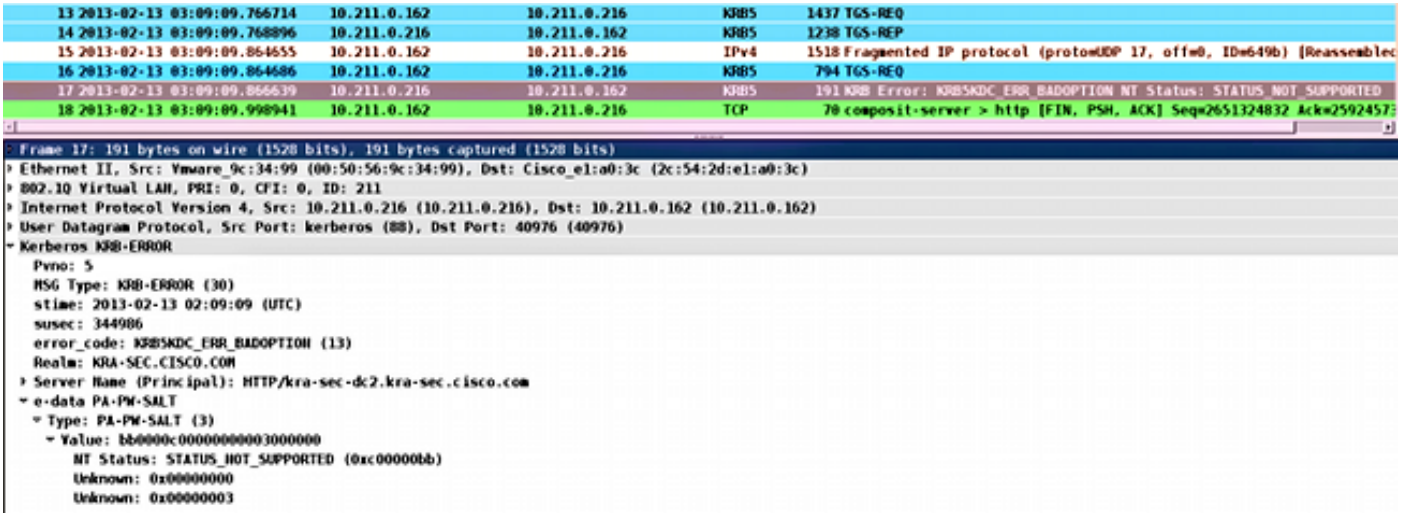
```
                                                    KRA-S-ASA-05(config)# show aaa kerberos
                                                  Default Principal: cisco@KRA-SEC.CISCO.COM
                                  Valid Starting       Expires              Service Principal
CEST Oct 2 2013 05:37:33 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 إستخدام تذكرة TICKET3) HTTP) 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 **HTTP/test.kra-sec.cisco.com** (الخطوة 5)، ولكن الاستجابة هي **KRB-ERROR** مع **ERR_BADOPTION**:



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

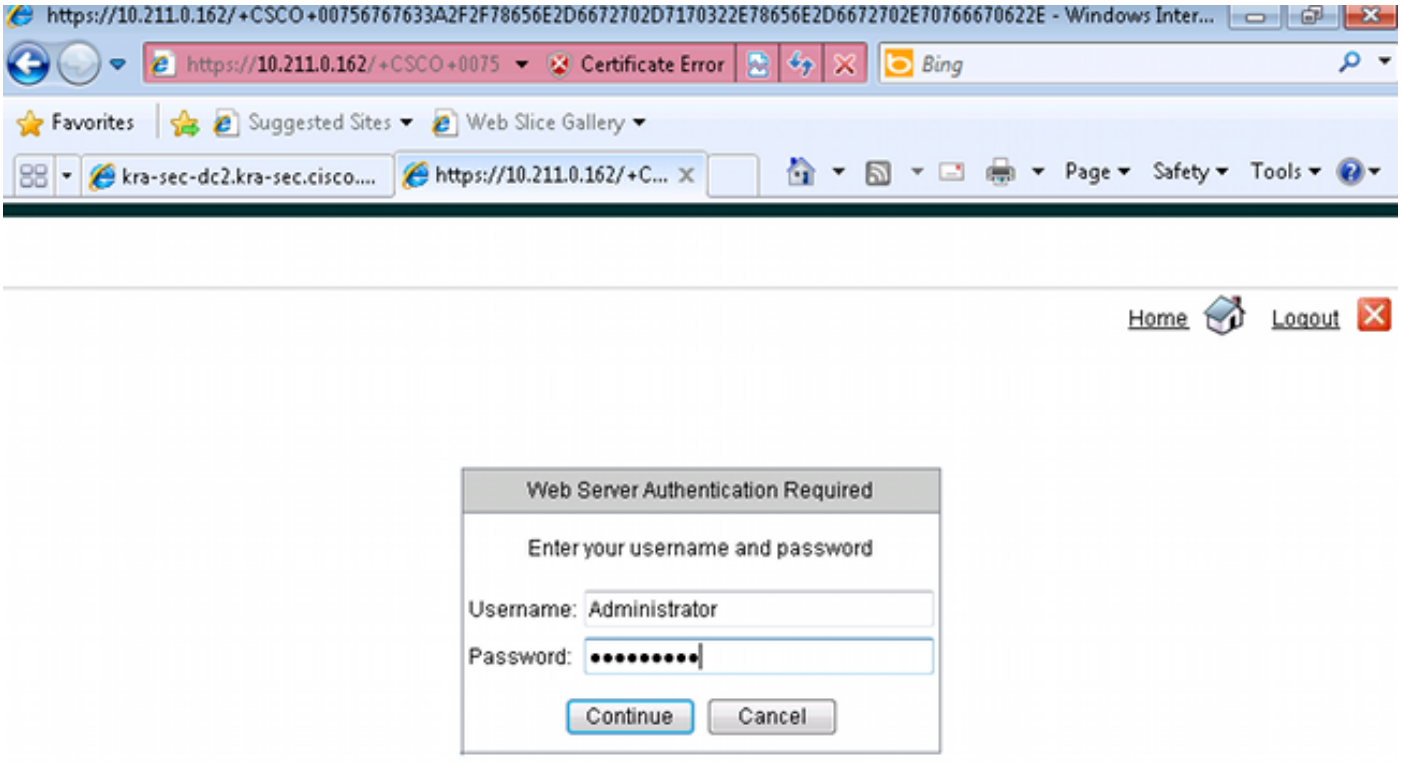
```
,KRA-S-ASA-05# ucte_krb_get_auth_cred(): ctx = 0xcc4b5390
WebVPN_session = 0xc919a260, protocol = 1
/ - find_spn_in_url(): URL
build_host_spn(): host - test.kra-sec.cisco.com
build_host_spn(): SPN - HTTP/test.kra-sec.cisco.com
.KCD_unicorn_get_cred(): Attempting to retrieve required KCD tickets
In 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_recv_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
```

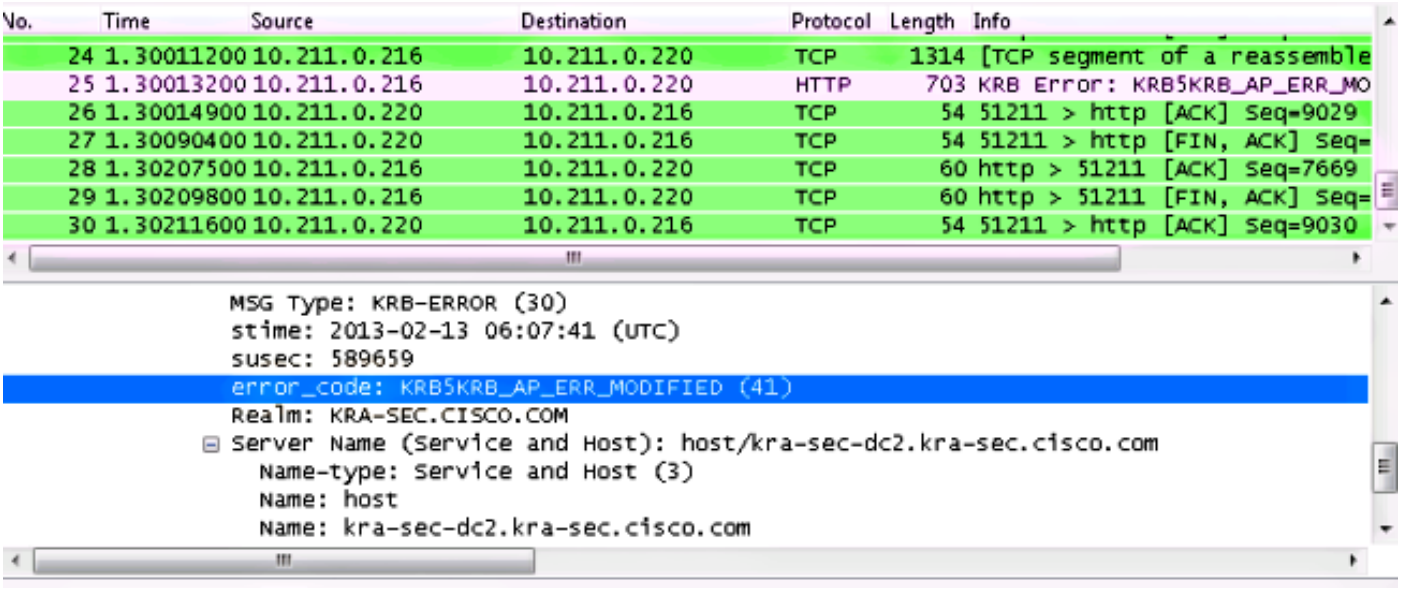
```
                                    Kerberos: Encryption type rc4-hmac-md5
                                    Kerberos: Encryption type des3-cbc-sha
                                     Kerberos: Encryption type des-cbc-md5
                                     Kerberos: Encryption type des-cbc-crc
                                     Kerberos: Encryption type des-cbc-md4
                          ************ END: KERBEROS PACKET DECODE **********
                                                    In kerberos_recv_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.

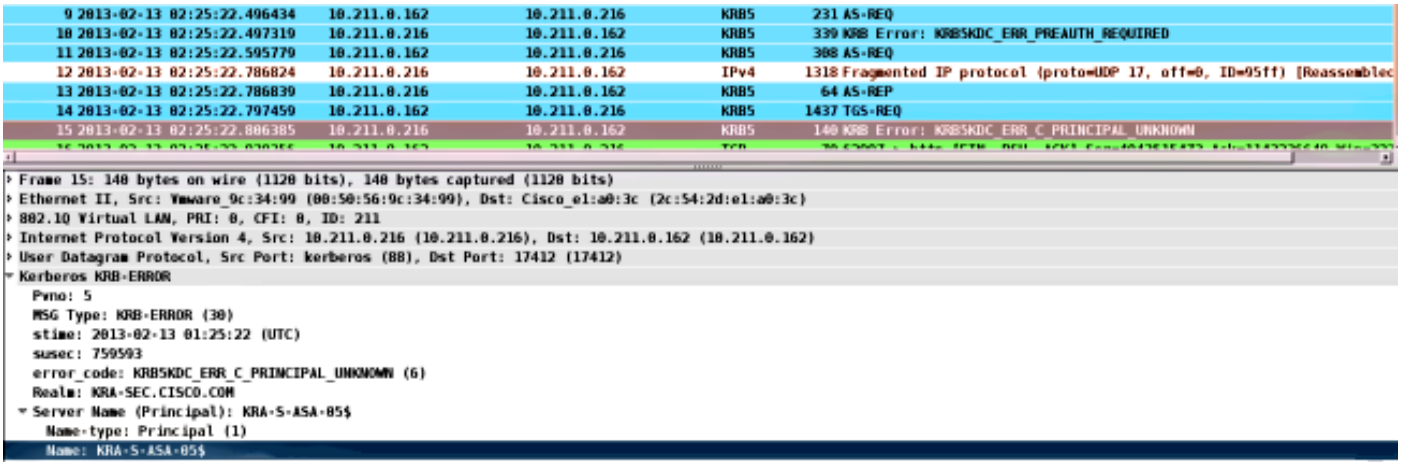
إذا كانت الاستجابة **ناجحة**، فيستلم ASA تذكرة لخدمة HTTP/test.kra-sec.cisco.com، والتي يتم إستخدامها لمفاوضات SPNEGO. ومع ذلك، بسبب الفشل، يتم التفاوض مع **مدير شبكة** LAN NT (NTLM)، ويجب على المستخدم توفير بيانات الاعتماد:



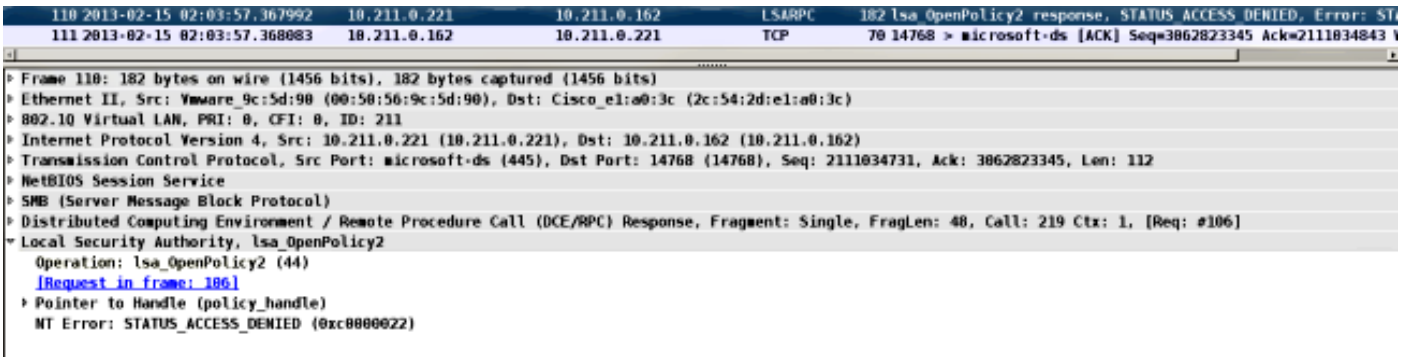
تأكد من تسجيل SPN لحساب واحد فقط (برنامج نصي من المقالة السابقة). عندما تتلقى هذا الخطأ، KRB_AP_ERR_MODIFIED، فإنه يعني عادة أن SPN غير مسجل للحساب الصحيح. يجب أن يتم تسجيله للحساب الذي يتم إستخدامه لتشغيل التطبيق (تجمع التطبيقات على IIS).



عندما تتلقى هذا الخطأ، **KRB_ERR_C_PRINCIPAL_UNKNOWN**، فهذا يعني أنه لا يوجد مستخدم على DC (مستخدم **cisco** :WebVPN).



قد تواجه هذه المشكلة عند الانضمام إلى المجال. يستلم **as-rep** ASA، ولكنه يفشل على **LSA** مستوى مع الخطأ: **STATUS_ACCESS_DENY**:



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 استنادا إلى إستجابة خادم اسم المجال (DNS).

- لا تقم بتعيين **SPN** على أنه **HOST/dc.kra-sec.cisco.com** لحساب **Administrator**. من الممكن فقدان الاتصال ب 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 إستخدام اتصال Kerberos للحزمة الصغيرة **UDP/88**. بعد الخطأ من وحدة التحكم بالمجال **DC** و**KRB5KDC_ERR_RESPONSE_TOO_BIG**، يتحول العميل إلى **TCP/88**. من الممكن إجبار عميل Windows على إستخدام **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 أستكشاف الأخطاء وإصلاحها على موقع وحدة التحكم بالمجال (DC)، من المفيد تمكين تصحيح أخطاء Kerberos: كيفية تمكين تسجيل أحداث Kerberos.

معرفات الأخطاء من Cisco

هنا قائمة بمعرفات الأخطاء ذات الصلة من Cisco:

- معرف تصحيح الأخطاء من Cisco CSCsi32224 - ASA 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 Cisco CSCuj19601 - ASA WebVPN KCD - يحاول الانضمام إلى AD فقط بعد إعادة التمهيد
- معرف تصحيح الأخطاء من Cisco CSCuh32106 - ASA KCD 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 عبر مثال تكوين ASDM/CLI
- مرجع أوامر سلسلة ASA من Cisco
- KDC_ERR_BADOPTION عند محاولة التفويض المقيد
- كيفية إجبار Kerberos على إستخدام TCP بدلا من UDP في Windows
- 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).