WebVPN SSO與Kerberos約束委派整合配置示例

目錄

簡介

本文檔介紹如何為受Kerberos保護的應用程式配置WebVPN單一登入(SSO)並對其進行故障排除。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- Cisco Adaptive Security Appliance(ASA)CLI配置和安全套接字層(SSL)VPN配置
- Kerberos服務

採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco ASA軟體9.0版及更高版本
- Microsoft Windows 7客戶端
- Microsoft Windows 2003 Server及更高版本

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

背景資訊

Kerberos是一種網路身份驗證協定，允許網路實體以安全方式相互進行身份驗證。它使用受信任的第三方，即金鑰分發中心(KDC)，向網路實體授予票證。實體使用這些票證以驗證和確認對請求的服務的訪問。

可以使用稱為Kerberos約束委派(KCD)的Cisco ASA功能為受Kerberos保護的應用程式配置WebVPN SSO。 通過此功能，ASA可以代表WebVPN門戶使用者請求Kerberos票證，同時訪問受Kerberos保護的應用程式。

當您通過WebVPN門戶訪問此類應用時，不再需要提供任何憑證；而是使用用於登入WebVPN門戶的帳戶。

有關詳細資訊，請參閱ASA配置指南的瞭解KCD的工作原理部分。

Kerberos與ASA的互動

對於WebVPN，ASA必須代表使用者請求票證（因為WebVPN門戶使用者只能訪問門戶，而不能訪問Kerberos服務）。 為此，ASA對約束委託使用Kerberos擴展。以下是流程：

1. ASA加入域並獲取具有在ASA上配置的憑據的電腦帳戶的票證(**kcd-server**命令)。 此票證將用於訪問Kerberos服務的後續步驟。

2. 使用者按一下受Kerberos保護的應用程式的WebVPN門戶連結。

3. ASA請求(**TGS-REQ**)票證以電腦帳戶的主機名作為主體。此請求包括**PA-TGS-REQ**欄位，該欄位採用**PA-FOR-USER**，主體作為WebVPN門戶使用者名稱，在此場景中為**cisco**。步驟1中的Kerberos服務票證用於身份驗證（正確的委派）。

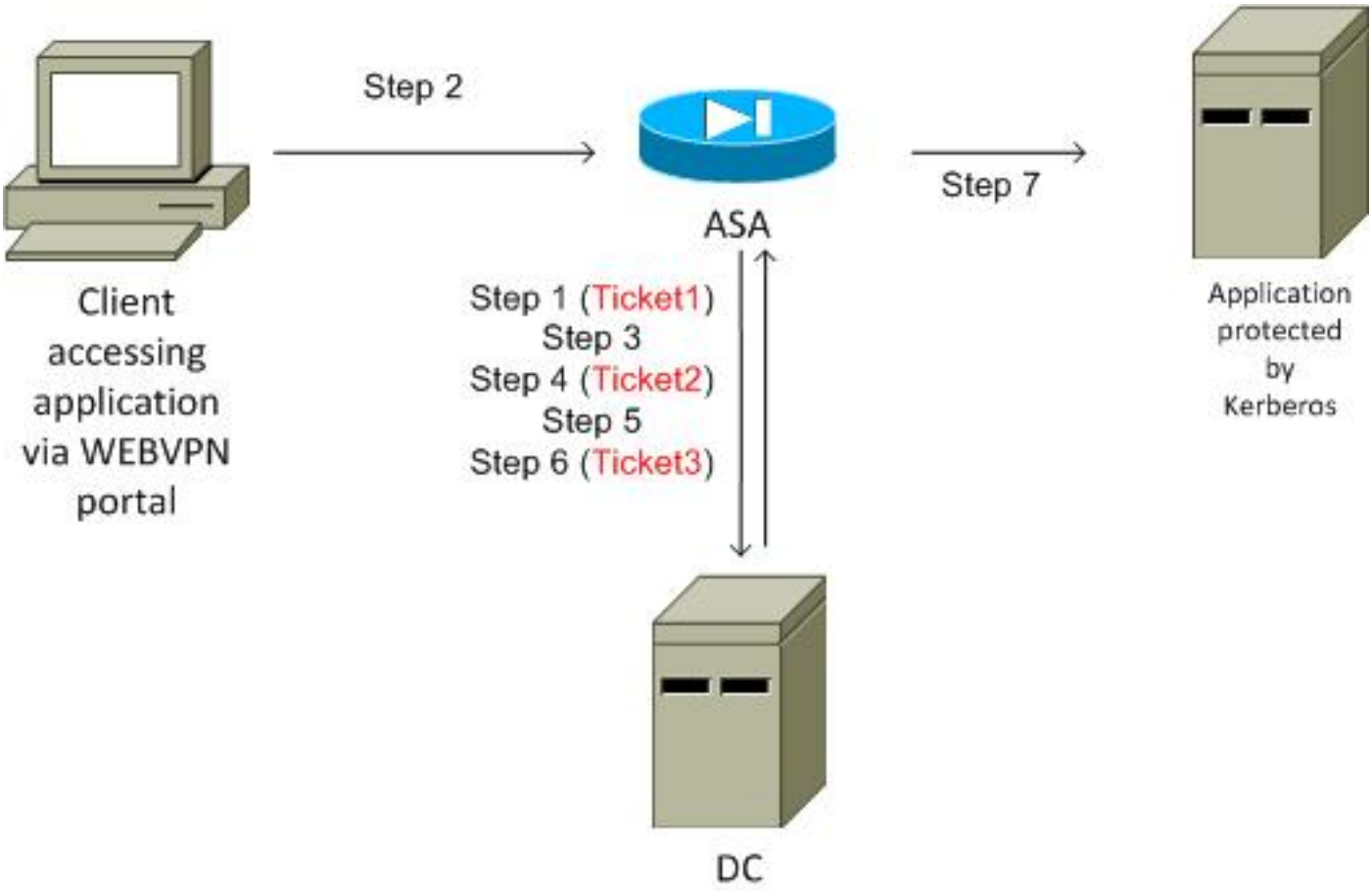
4. 作為響應，ASA代表WebVPN使用者(**TGS_REP**)接收電腦帳戶的模擬票證（票證2）。此票證用於代表此WebVPN使用者請求應用票證。

5. ASA發起另一個請求(**TGS_REQ**)以獲取應用程式的票證(**HTTP/test.kra-sec.cisco.com**)。 此請求再次使用**PA-TGS-REQ**欄位，這次不帶**PA-FOR-USER**欄位，但使用步驟4中接收的模擬票證。

6. 返回應用程式的模擬票證(Ticket3)的響應(**TGS_REQ**)。

7. ASA透明使用此票證以訪問受保護的服務，並且WebVPN使用者無需輸入任何憑證。對於HTTP應用，使用簡單受保護的GSS-API協商(SPNEGO)機制協商身份驗證方法，ASA將傳遞

正確的票證。



設定

拓撲

域:kra-sec.cisco.com（10.211.0.221或10.211.0.216）

Internet Information Services(IIS)7應用程式:test.kra-sec.cisco.com(10.211.0.223)

域控制器(DC):dc.kra-sec.cisco.com（10.211.0.221或10.211.0.216）— Windows2008

ASA:10.211.0.162

WebVPN使用者名稱/密碼:cisco/cisco

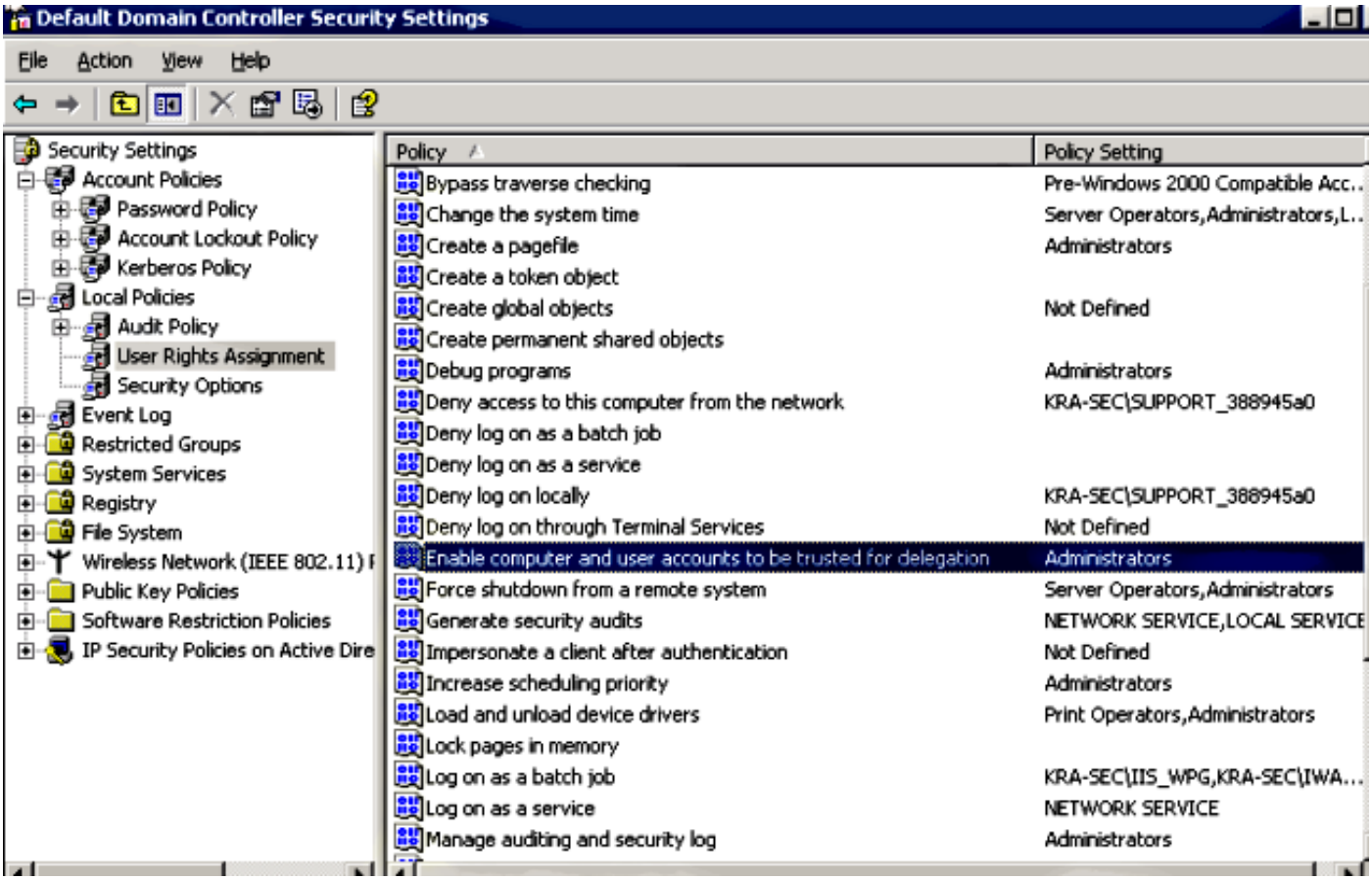
附加檔案:asa-join.pcap（成功加入域）

附加檔案:asa-kerberos-bad.pcap（請求服務）

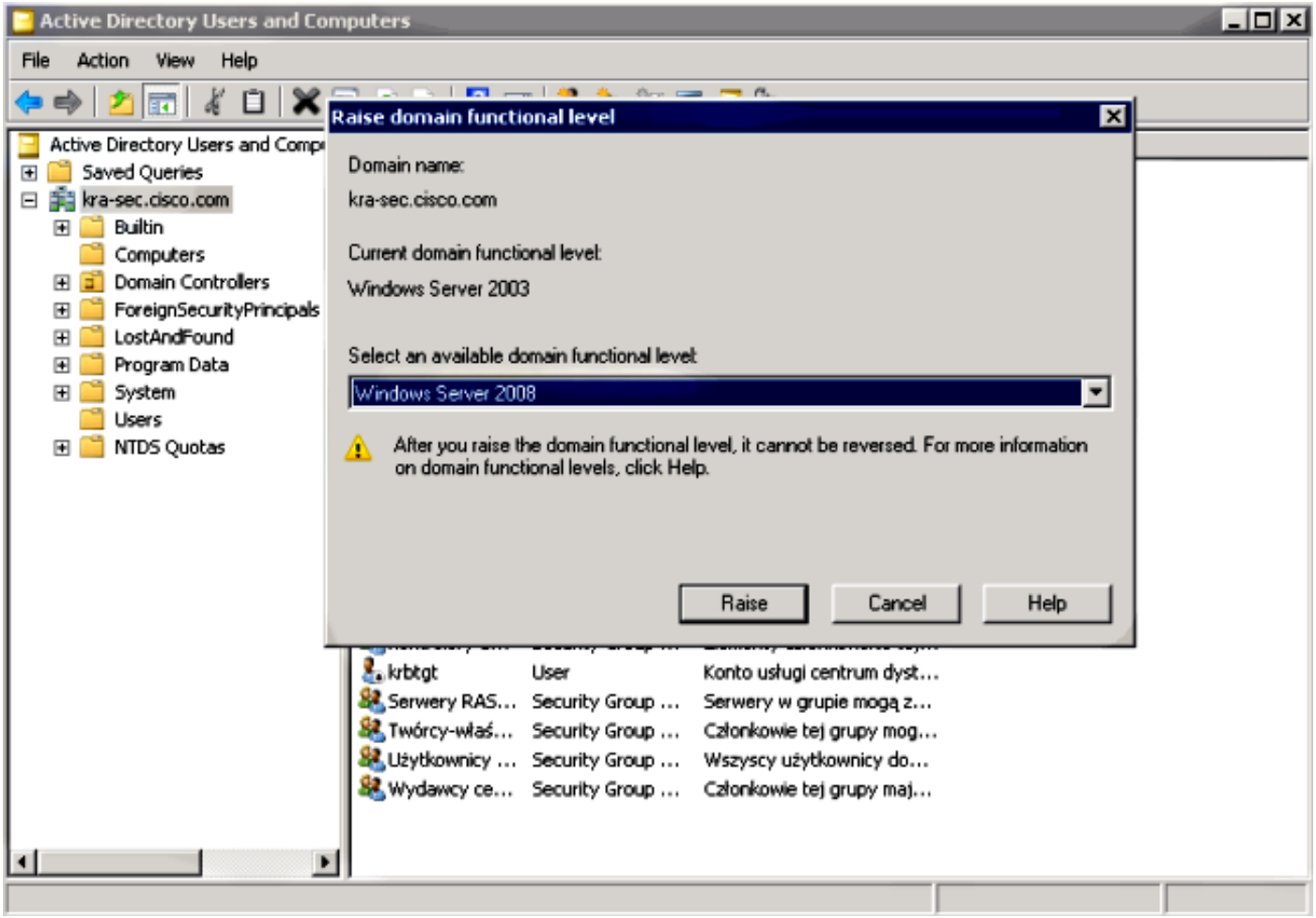
域控制器和應用配置

域設定

假定已經有一個受Kerberos保護的功能性IIS7應用程式（如果沒有，請閱讀必要條件部分）。 您必須檢查使用者委託的設定：



確保將功能域級別提升到Windows Server 2003（至少）。 預設值為Windows Server 2000:



設定服務主體名稱(SPN)

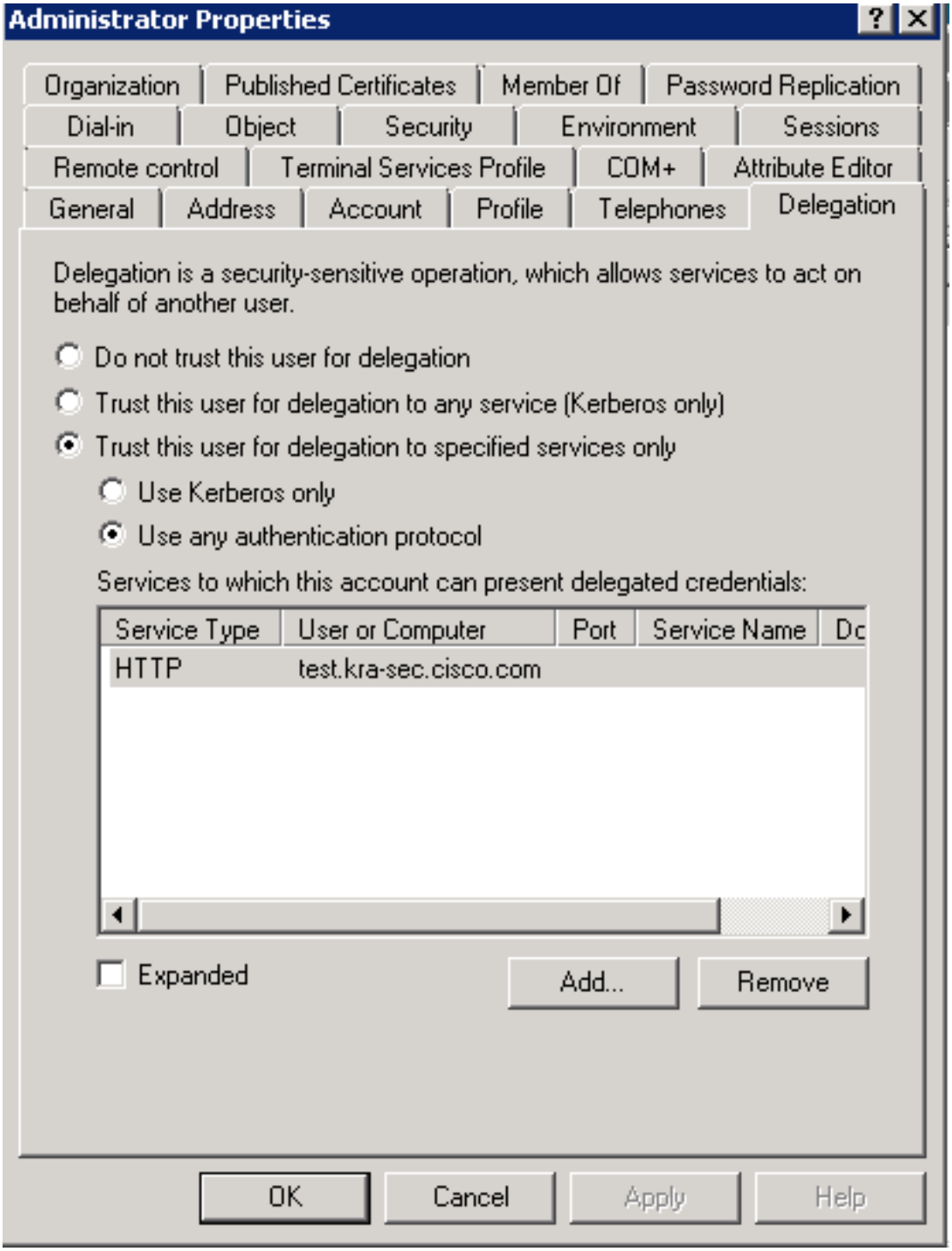
您必須使用正確的委派在AD上配置任何帳戶。使用管理員帳戶。當ASA使用該帳戶時，它能夠代表其他使用者（受約束的委派）為特定服務（HTTP應用程式）請求票證。 為了發生這種情況，必須為應用程式/服務建立正確的委派。

若要使用**setspn.exe**(是Windows Server 2003 Service Pack 1支援工具的一部分)通過CLI進行此委派，請輸入以下命令：

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

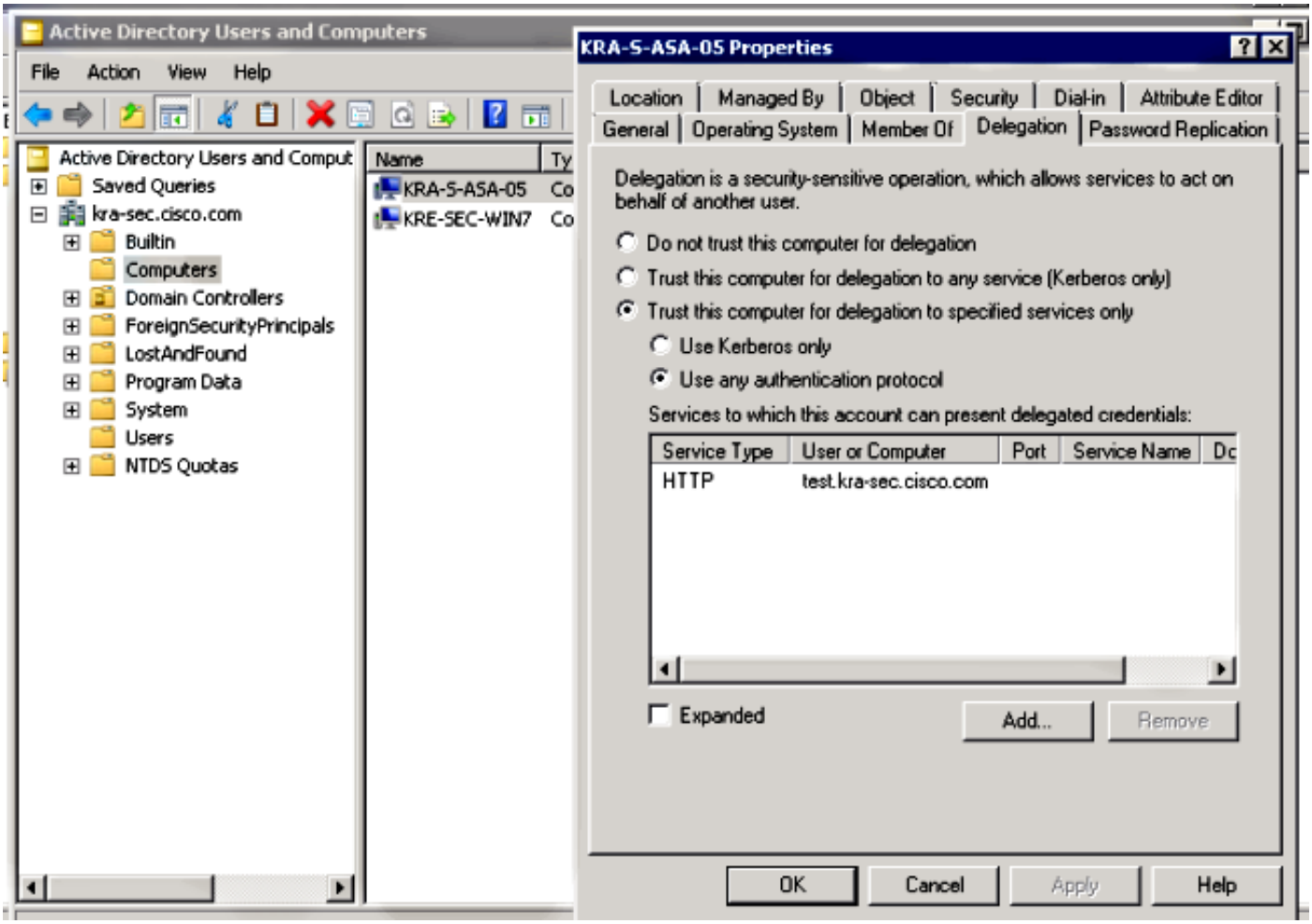
這表示**Administrator**使用者名稱是在**test.kra-sec.cisco.com**中委派HTTP服務的受信任帳戶。

還必須使用**SPN**命令才能啟用該使用者的**委派**頁籤。輸入命令後，將顯示管理員的「委派」頁籤。啟用「使用任何身份驗證協定」非常重要，因為「僅使用Kerberos」不支援約束委派擴展。



在**General**索引標籤上，也可以停用Kerberos預先驗證。但是不建議這樣做，因為此功能用於保護DC免受重放攻擊。ASA可以正確使用預身份驗證。

此過程也適用於電腦帳戶的委派（ASA作為電腦進入域以建立「信任」關係）：



ASA上的配置

```
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
```

驗證

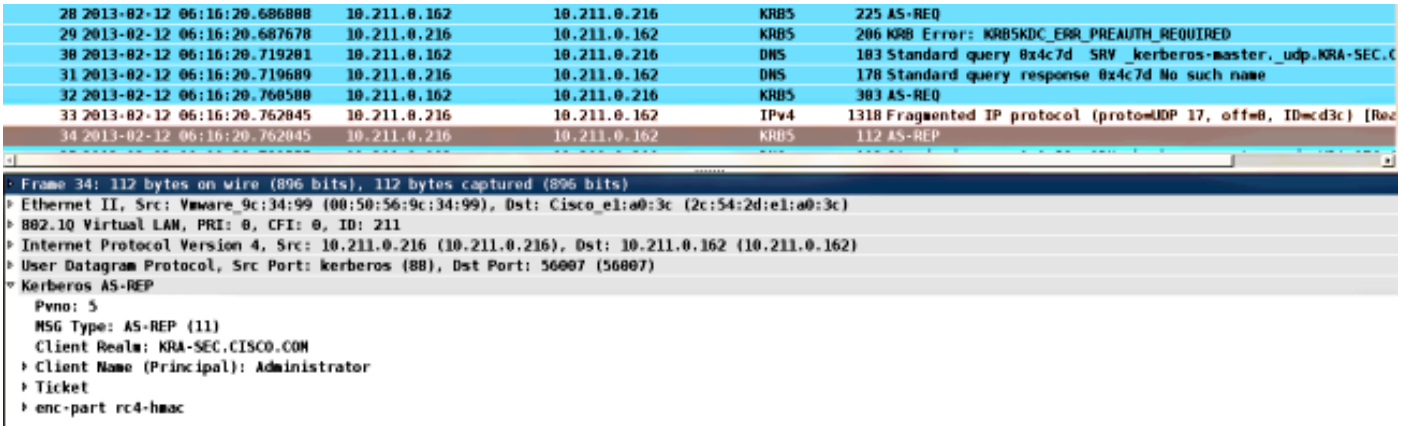
ASA加入域

使用kcd-server命令後，ASA嘗試加入域：

```
********** 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
```

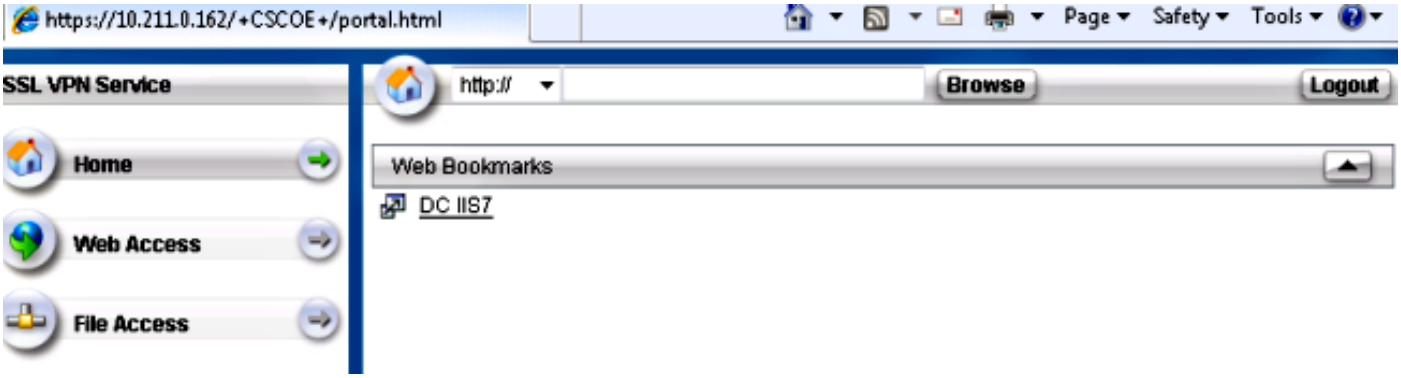
```
Kerberos: Server Name krbtgt
Kerberos: Start time 0
Kerberos: End time -878667256
Kerberos: Renew until time -878672192
Kerberos: Nonce 0xa9db408e
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4
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
```

ASA能夠成功加入域。經過正確的身份驗證後，ASA會收到主體票證：**AS_REP資料包**中的管理員（步驟1中描述的Ticket1）。

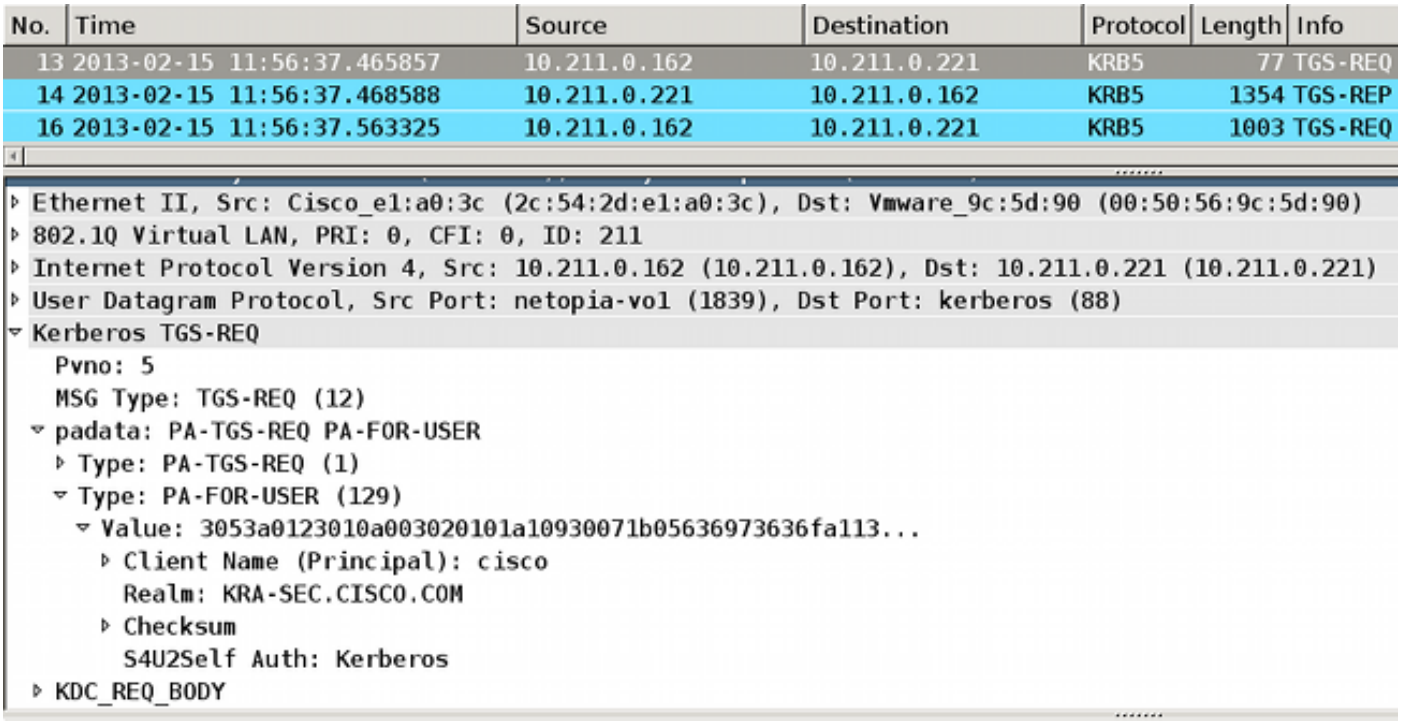


服務請求

使用者按一下WebVPN連結：

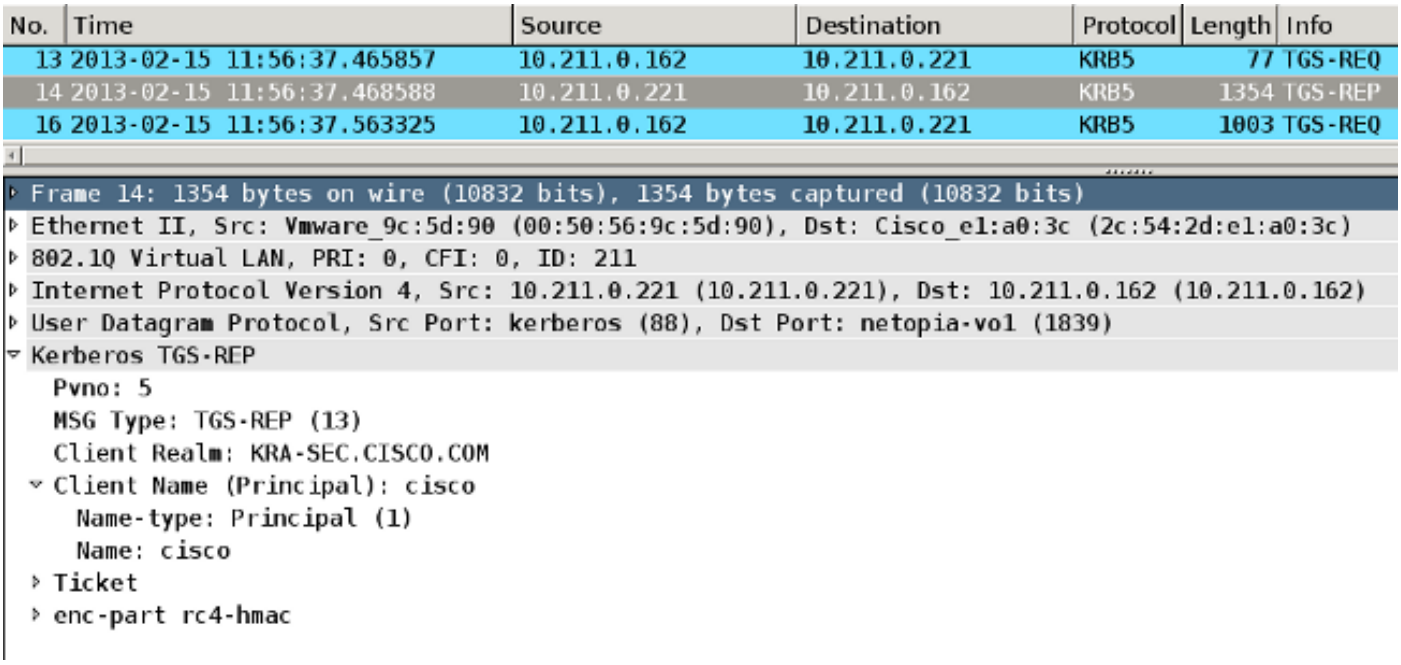


ASA為模擬票證傳送**TGS_REQ**，其中包含**AS_REP資料包中接收**的票證：



附註：**PA-for-USER值為cisco**（WebVPN使用者）。**PA-TGS-REQ包含**為Kerberos服務請求接收的票證（ASA主機名是主體）。

ASA通過使用者**cisco**（步驟4中描述的Ticket2）的模擬票證獲得正確的響應：



以下是HTTP服務的票證請求（為清楚起見，省略了某些調試）：

```
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
```

ASA接收HTTP服務的正確模擬票證（步驟6中介紹的票證3）。

兩個票證均可驗證。第一個票證是使用者cisco的模擬票證，用於請求和接收所訪問的HTTP服務的第二個票證：

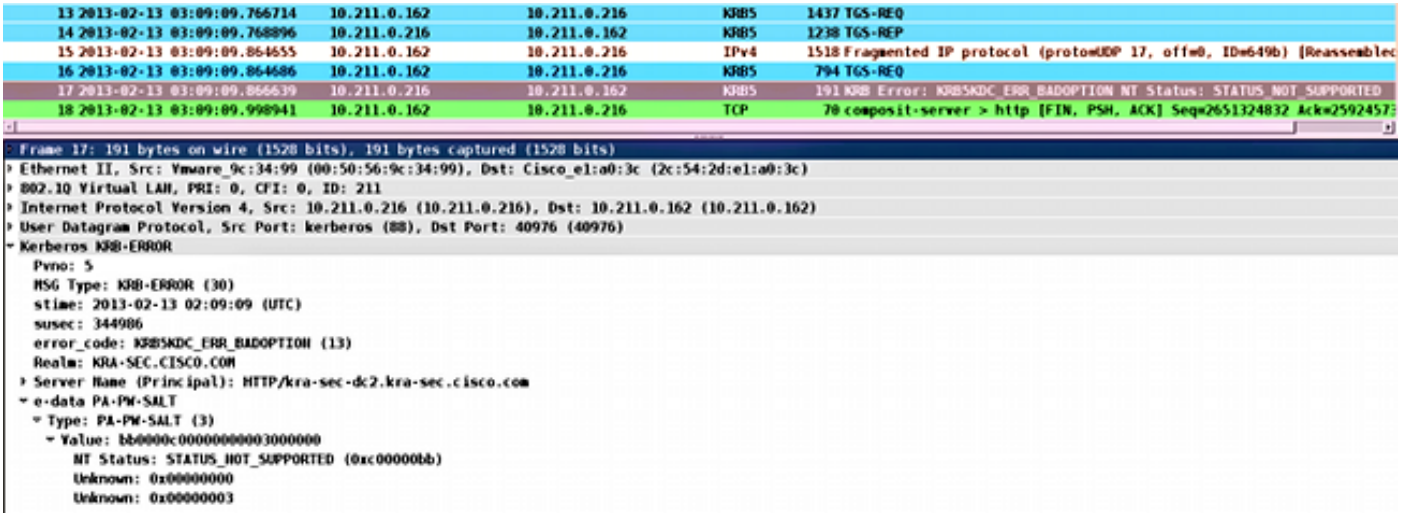
```
KRA-S-ASA-05(config)# show aaa kerberos
Default Principal: cisco@KRA-SEC.CISCO.COM
Valid Starting       Expires              Service Principal
19:38:10 CEST Oct 2 2013 05:37:33 CEST Oct 3 2013 KRA-S-ASA-05@KRA-SEC.CISCO.COM

Default Principal: cisco@KRA-SEC.CISCO.COM
```

```
Valid Starting       Expires              Service Principal
19:38:10 CEST Oct 2 2013 05:37:33 CEST Oct 3 2013
HTTP/test.kra-sec.cisco.com@KRA-SEC.CISCO.COM
```

此HTTP票證（票證3）用於HTTP訪問（使用SPNEGO），使用者不需要提供任何憑證。

疑難排解

有時您可能會遇到委派不正確的問題。例如，ASA使用票證來請求服務HTTP/test.kra-sec.cisco.com（步驟5），但響應為KRB-ERROR(帶有ERR_BADOPTION):



這是未正確配置委派時遇到的典型問題。ASA報告「KDC無法實現請求的選項」：

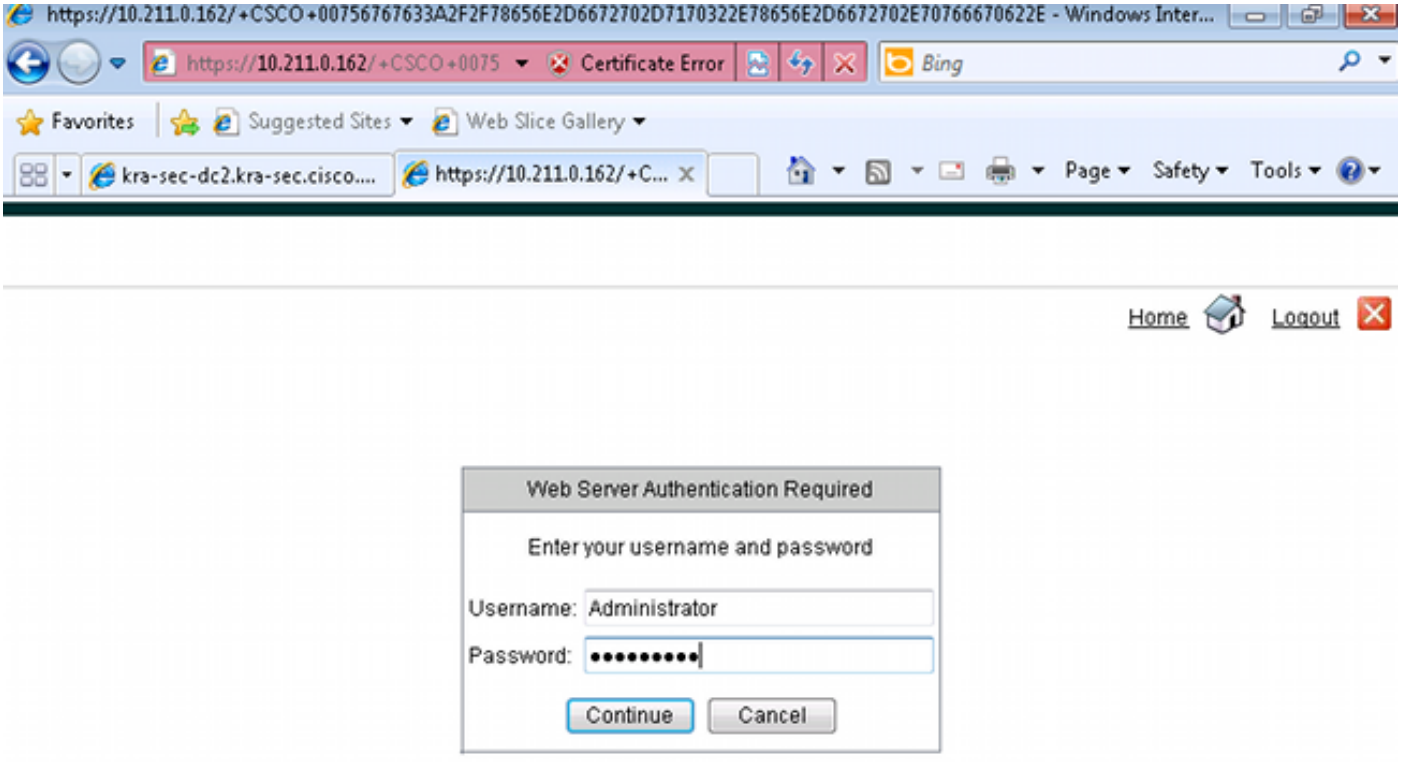
```
KRA-S-ASA-05# ucte_krb_get_auth_cred(): ctx = 0xcc4b5390,
WebVPN_session = 0xc919a260, protocol = 1
find_spn_in_url(): URL - /
build_host_spn(): host - test.kra-sec.cisco.com
build_host_spn(): SPN - HTTP/test.kra-sec.cisco.com
KCD_unicorn_get_cred(): Attempting to retrieve required KCD tickets.
In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

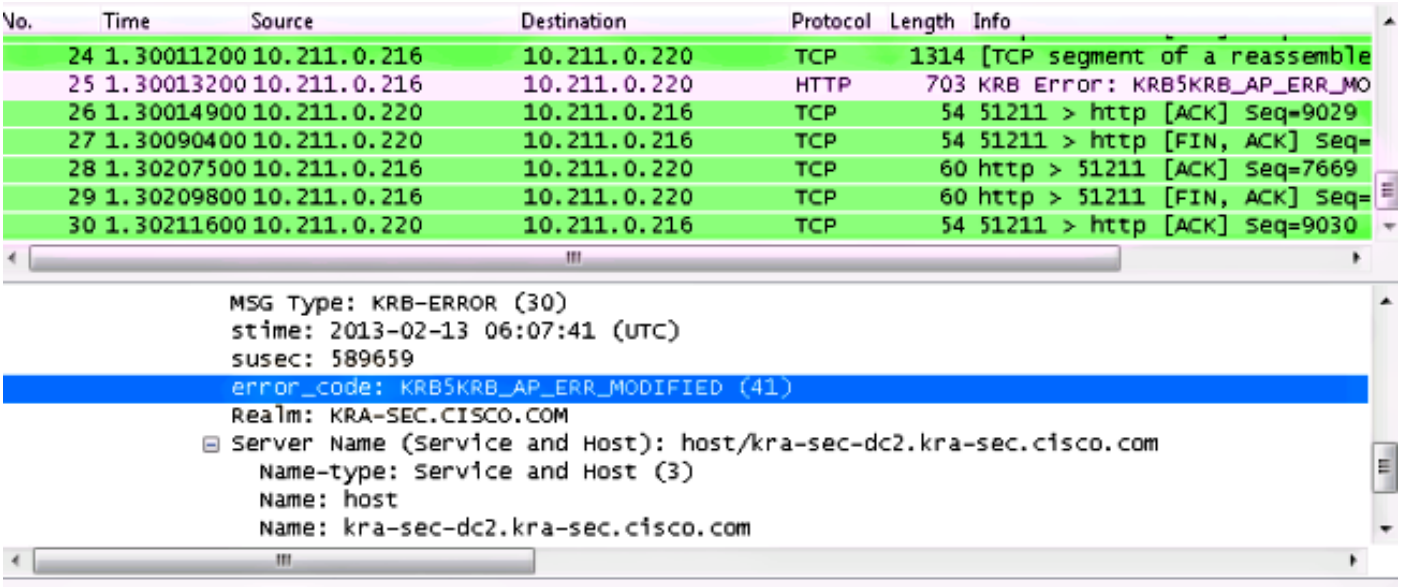
```
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4
********** END: KERBEROS PACKET DECODE ************
In kerberos_recv_msg
In KCD_cred_tkt_process_response
********** START: KERBEROS PACKET DECODE ************
Kerberos: Message type 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
```

這基本上與捕獲中描述的問題相同 — 故障在TGS_REQ with BAD_OPTION處。

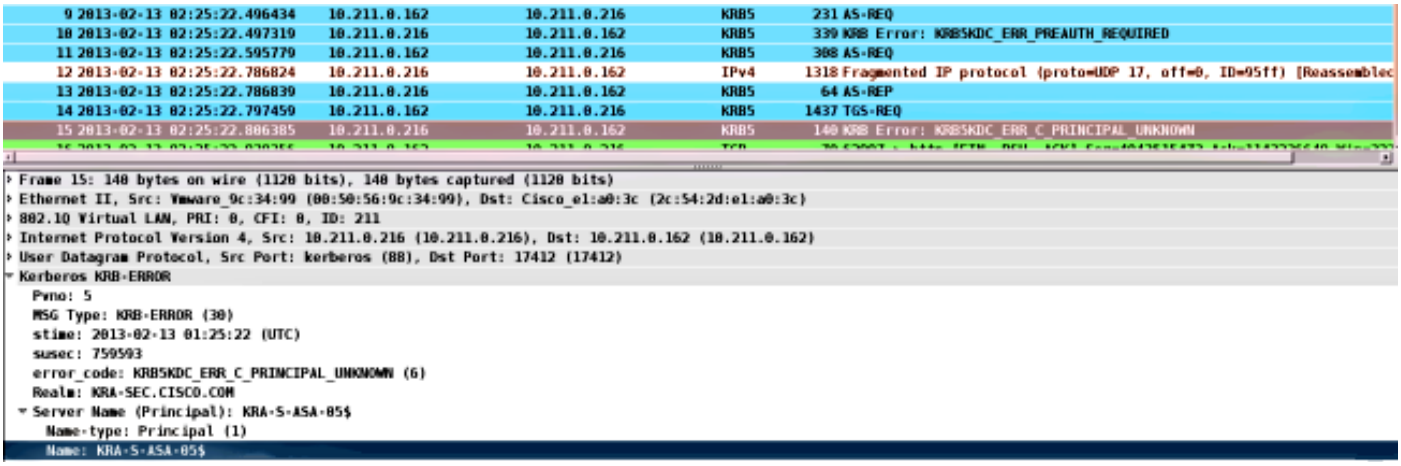
如果響應為Success，則ASA會收到HTTP/test.kra-sec.cisco.com服務的票證，該服務用於SPNEGO協商。但是，由於發生故障，NT LAN Manager(NTLM)會進行協商，並且使用者必須提供憑據：



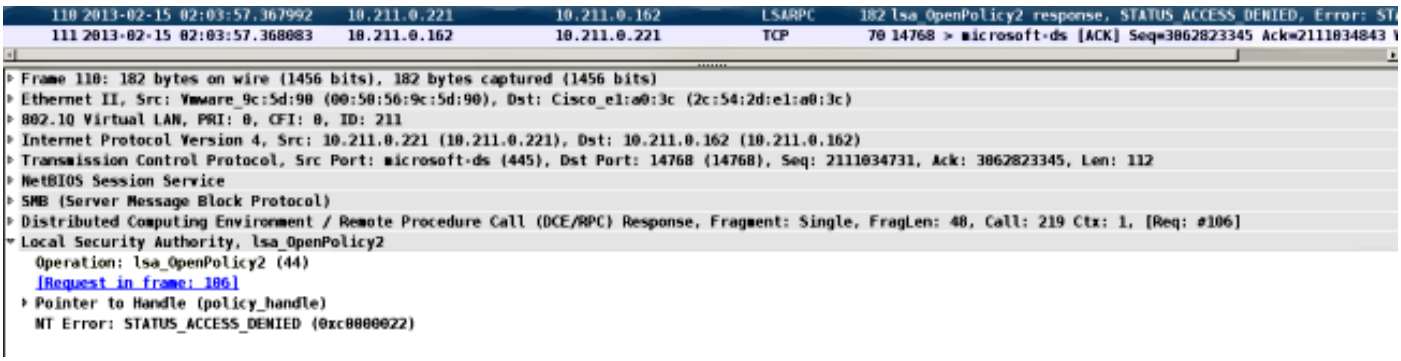
確保僅為一個帳戶註冊SPN（上一篇文章中的指令碼）。 收到此錯誤KRB_AP_ERR_MODIFIED時，通常表示SPN未針對正確的帳戶註冊。應為用於運行應用程式（IIS上的應用程式池）的帳戶註冊該帳戶。



收到此錯誤**KRB_ERR_C_PRINCIPAL_UNKNOWN**時，它表示DC上沒有使用者(WebVPN使用者：**cisco**)。



加入域時可能會遇到此問題。ASA收到**AS-REP**，但在LSA級別**失敗**，錯誤為：**STATUS_ACCESS_DENIED**:



為了解決此問題，您必須為該使用者(**Administrator**)啟用/禁用DC上的預身份驗證。

以下是您可能會遇到的其他問題：

- 加入域時可能有問題。如果DC伺服器有多個網路介面控制器(NIC)介面卡（多個IP地址），請確保ASA可以訪問所有介面卡，以便加入域(由客戶端根據域名伺服器(DNS)響應隨機選擇)。
- 請勿將**SPN**設為**HOST/dc.kra-sec.cisco.com**作為**Administrator**帳戶。由於該設定，可能會丟失

與DC的連線。

- 在ASA加入域後，可以驗證在DC（ASA主機名）上建立正確的電腦帳戶。 確保使用者具有正確的許可權以便新增電腦帳戶(在本例中，**Administrator**具有正確的許可權)。
- 請記住ASA上**的正確網路時間協**議(**NTP**)配置。預設情況下，DC接受五分鐘時鐘偏差。可以在DC上更改該計時器。
- 驗證是否已使用小型封**包UDP/88**的Kerberos連線。從DC(**KRB5KDC_ERR_RESPONSE_TOO_BIG**)發出錯誤後，客戶端切換到**TCP/88**。可以強制Windows客戶端使用**TCP/88**，但ASA預設情況下將使用**UDP**。
- 資料中心:進行策略更改時，請記住**gpupdate /force**。
- ASA:使用**test aaa**命令測試身份驗證，但是請記住它只是一個簡單的身份驗證。
- 要在DC站點上進行故障排除，啟用Kerberos調試非常有用：如何啟用Kerberos事件記錄。

思科錯誤ID

以下是相關思科錯誤ID的清單：

- 思科錯誤ID CSCsi3224 - ASA在收到Kerberos錯誤代碼52後不會切換到TCP
- 思科錯誤ID CSCtd92673 - Kerberos驗證失敗，且已啟用預先驗證
- 思科漏洞ID CSCuj19601 - ASA Webvpn KCD — 僅在重新啟動後嘗試加入AD
- 思科錯誤ID CSCuh32106 - ASA KCD從8.4.5開始損壞

相關資訊

- **關於Kerberos約束委派**
- **瞭解KCD的工作原理**
- **PIX/ASA:通過ASDM/CLI配置VPN客戶端使用者的Kerberos身份驗證和LDAP授權伺服器組示例**
- **Cisco ASA系列命令參考**
- **嘗試受約束委託時KDC_ERR_BADOPTION**
- **如何在Windows中強制Kerberos使用TCP而不是UDP**
- **技術支援與文件 - Cisco Systems**