Esempio di configurazione dell'integrazione di WebVPN SSO con la delega vincolata Kerberos

Sommario

Introduzione

In questo documento viene descritto come configurare WebVPN Single Sign On (SSO) e risolverne i problemi per le applicazioni protette da Kerberos.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Configurazione CLI di Cisco Adaptive Security Appliance (ASA) e configurazione VPN SSL (Secure Sockets Layer)
- Servizi Kerberos

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Software Cisco ASA versione 9.0 e successive
- Client di Microsoft Windows 7
- Microsoft Windows 2003 Server e versioni successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Kerberos è un protocollo di autenticazione di rete che consente alle entità di rete di autenticarsi reciprocamente in modo sicuro. Utilizza una terza parte attendibile, il Centro distribuzione chiavi (KDC), che concede i ticket alle entità di rete. Tali ticket sono utilizzati dalle entità per verificare e confermare l'accesso al servizio richiesto.

Èpossibile configurare WebVPN SSO per le applicazioni protette da Kerberos con la funzionalità Cisco ASA chiamata Kerberos Constrained Delegation (KCD). Con questa funzione, l'ASA può richiedere i ticket Kerberos per conto dell'utente del portale WebVPN, mentre accede alle applicazioni protette da Kerberos.

Quando si accede a tali applicazioni tramite il portale WebVPN, non è più necessario fornire credenziali. viene invece utilizzato l'account utilizzato per accedere al portale WebVPN.

Per ulteriori informazioni, consultare la sezione Descrizione del funzionamento del KCD della guida alla configurazione dell'ASA.

Interazione Kerberos con l'appliance ASA

Per WebVPN, l'ASA deve richiedere i ticket per conto dell'utente (in quanto l'utente del portale WebVPN ha accesso solo al portale, non al servizio Kerberos). A tale scopo, l'appliance ASA utilizza le estensioni Kerberos per la delega vincolata. Ecco il flusso:

1. L'ASA si aggiunge al dominio e ottiene un ticket (Ticket1) per un account computer con le credenziali configurate sull'ASA (comando **kcd-server**). Questo ticket viene utilizzato nei passaggi successivi per l'accesso ai servizi Kerberos.

2. L'utente fa clic sul collegamento al portale WebVPN per l'applicazione protetta con Kerberos.

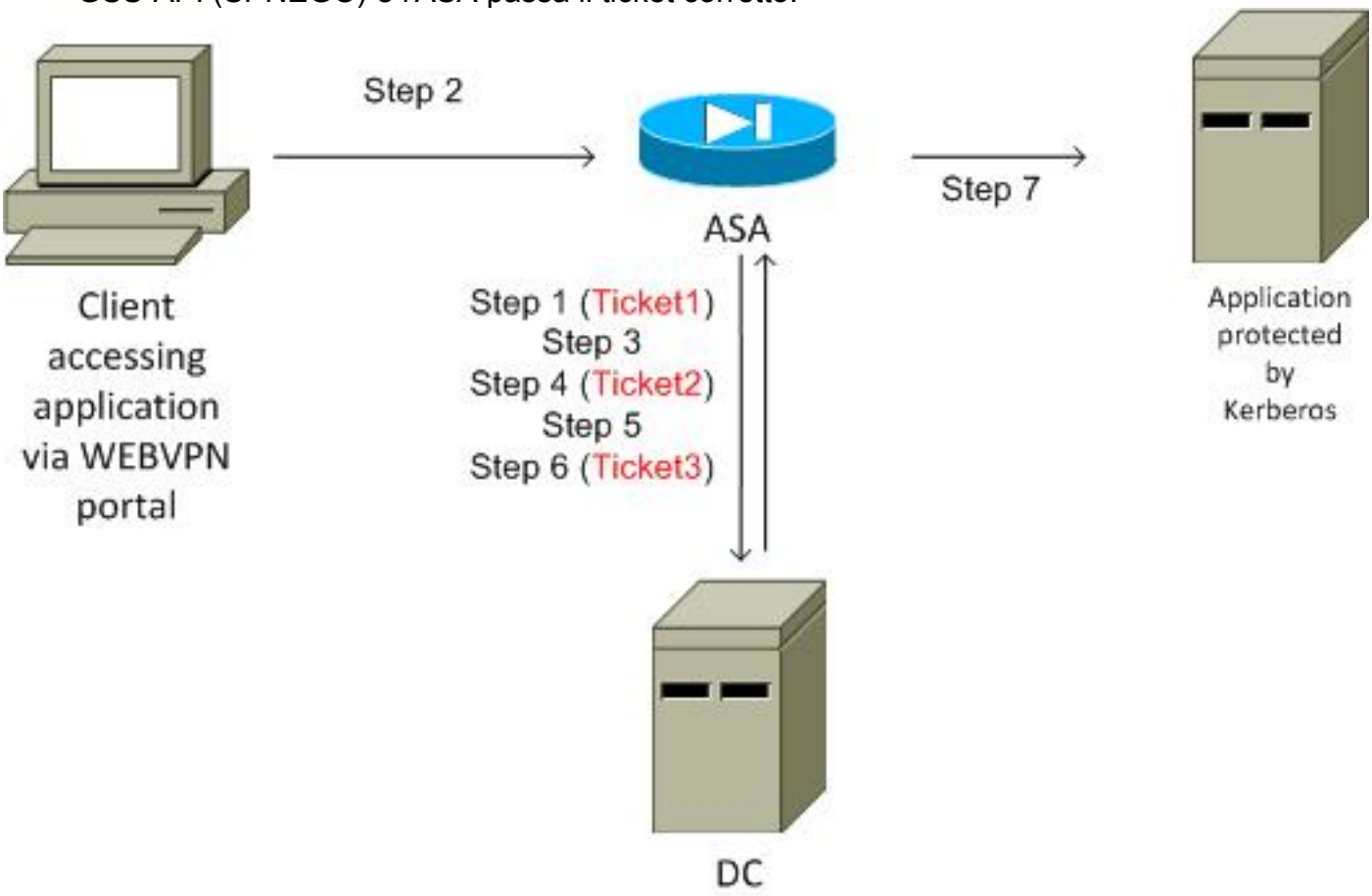
3. L'appliance ASA richiede (**TGS-REQ**) un ticket per l'account computer con il nome host come utente/gruppo/ruolo. La richiesta include il campo **PA-TGS-REQ** con **PA-FOR-USER** impostato come nome utente del portale WebVPN, ossia **cisco** in questo scenario. Il ticket per il servizio Kerberos dal passaggio 1 viene utilizzato per l'autenticazione (delega corretta).

4. In risposta, l'ASA riceve un ticket rappresentato (Ticket2) per conto dell'utente WebVPN (**TGS_REP**) per l'account computer. Questo ticket viene utilizzato per richiedere i ticket dell'applicazione per conto di questo utente WebVPN.

5. L'ASA avvia un'altra richiesta (**TGS_REQ**) per ottenere il ticket per l'applicazione (**HTTP/test.kra-sec.cisco.com**). Questa richiesta utilizza di nuovo il campo **PA-TGS-REQ**, questa volta **senza il** campo **PA-FOR-USER**, ma con il ticket rappresentato ricevuto al punto 4.

6. Viene restituita la risposta (**TGS_REQ**) con il ticket rappresentato (Ticket3) per l'applicazione.

7. Questo ticket viene utilizzato in modo trasparente dall'ASA per accedere al servizio protetto e l'utente WebVPN non deve immettere credenziali. Per l'applicazione HTTP, per negoziare il metodo di autenticazione viene utilizzato il meccanismo di negoziazione semplice e protetta GSS-API (SPNEGO) e l'ASA passa il ticket corretto.



Configurazione

Topologia

Dominio: kra-sec.cisco.com (10.211.0.221 o 10.211.0.216)

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

Controller di dominio (DC): dc.kra-sec.cisco.com (10.211.0.221 o 10.211.0.216) - Windows2008

ASA: 10.211.0.162

Nome utente/password WebVPN: cisco/cisco

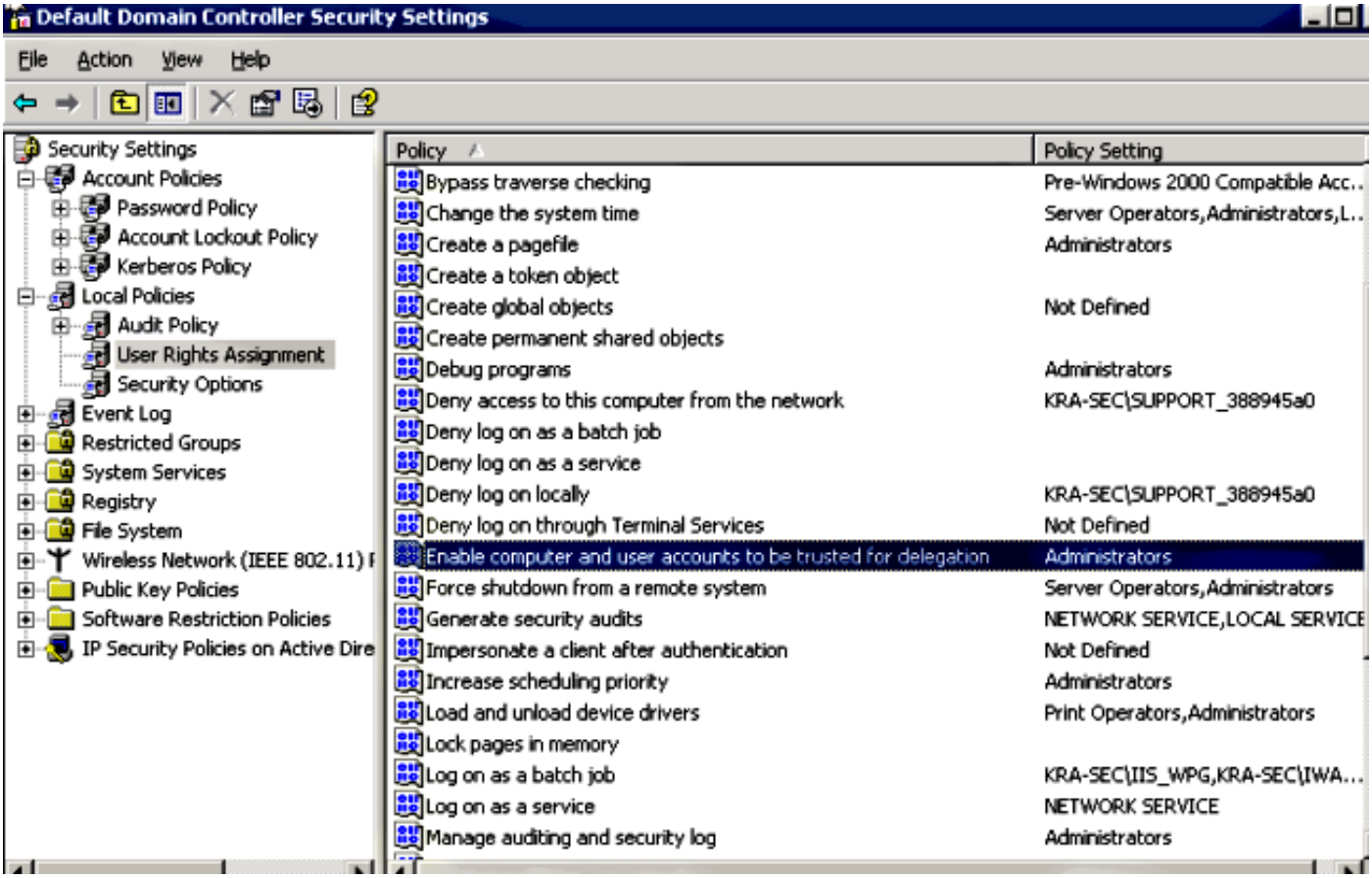
File allegato: asa-join.pcap (aggiunta riuscita al dominio)

File allegato: asa-kerberos-bad.pcap (richiesta di assistenza)

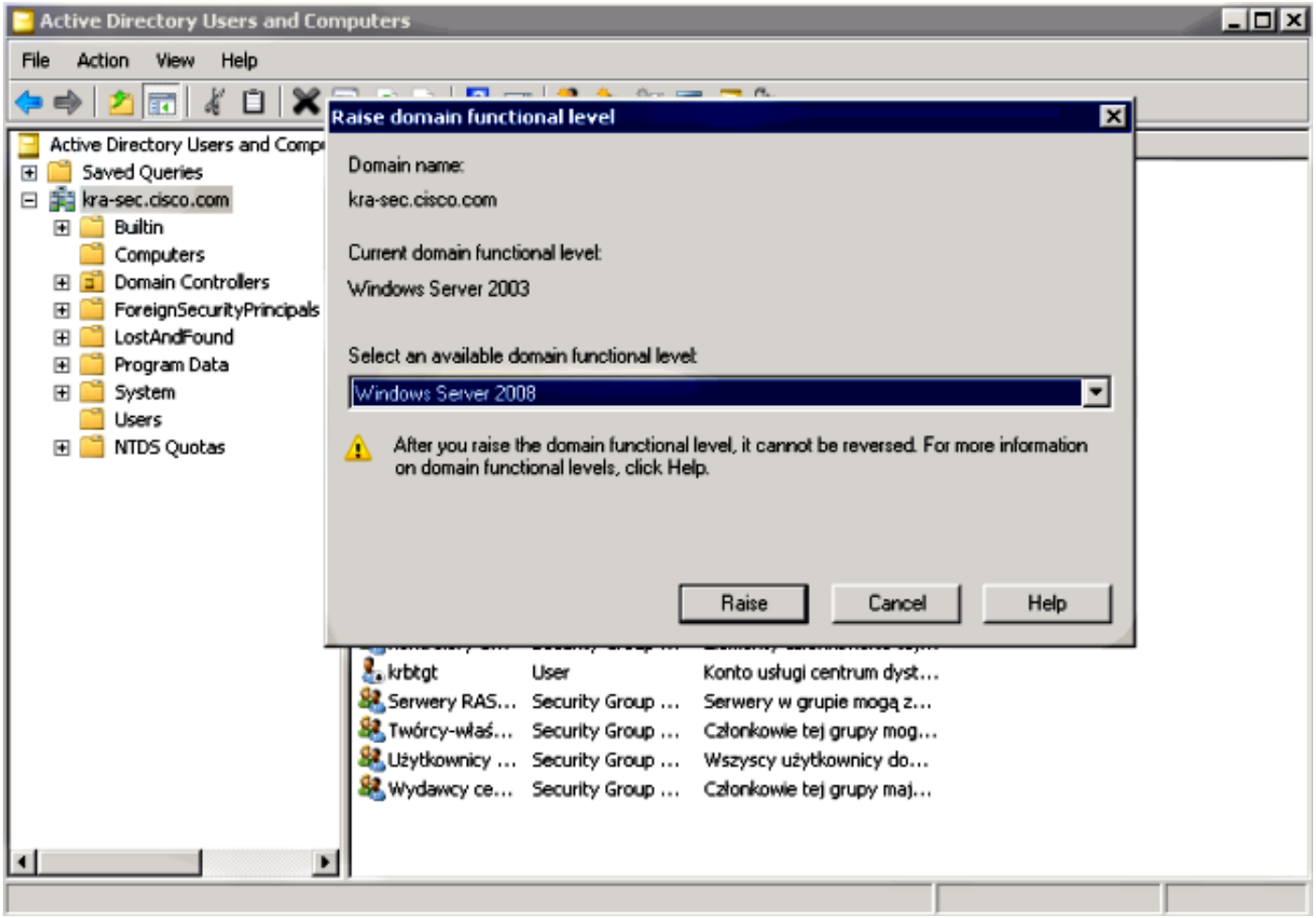
Controller di dominio e configurazione applicazione

Impostazioni dominio

Si presume che esista già un'applicazione IIS7 funzionale protetta da Kerberos. In caso contrario, leggere la sezione Prerequisiti. È necessario verificare le impostazioni per le deleghe degli utenti:



Accertarsi che il livello del dominio funzionale sia elevato a Windows Server 2003 (almeno). Il valore predefinito è Windows Server 2000:



Impostare il nome principale di servizio (SPN)

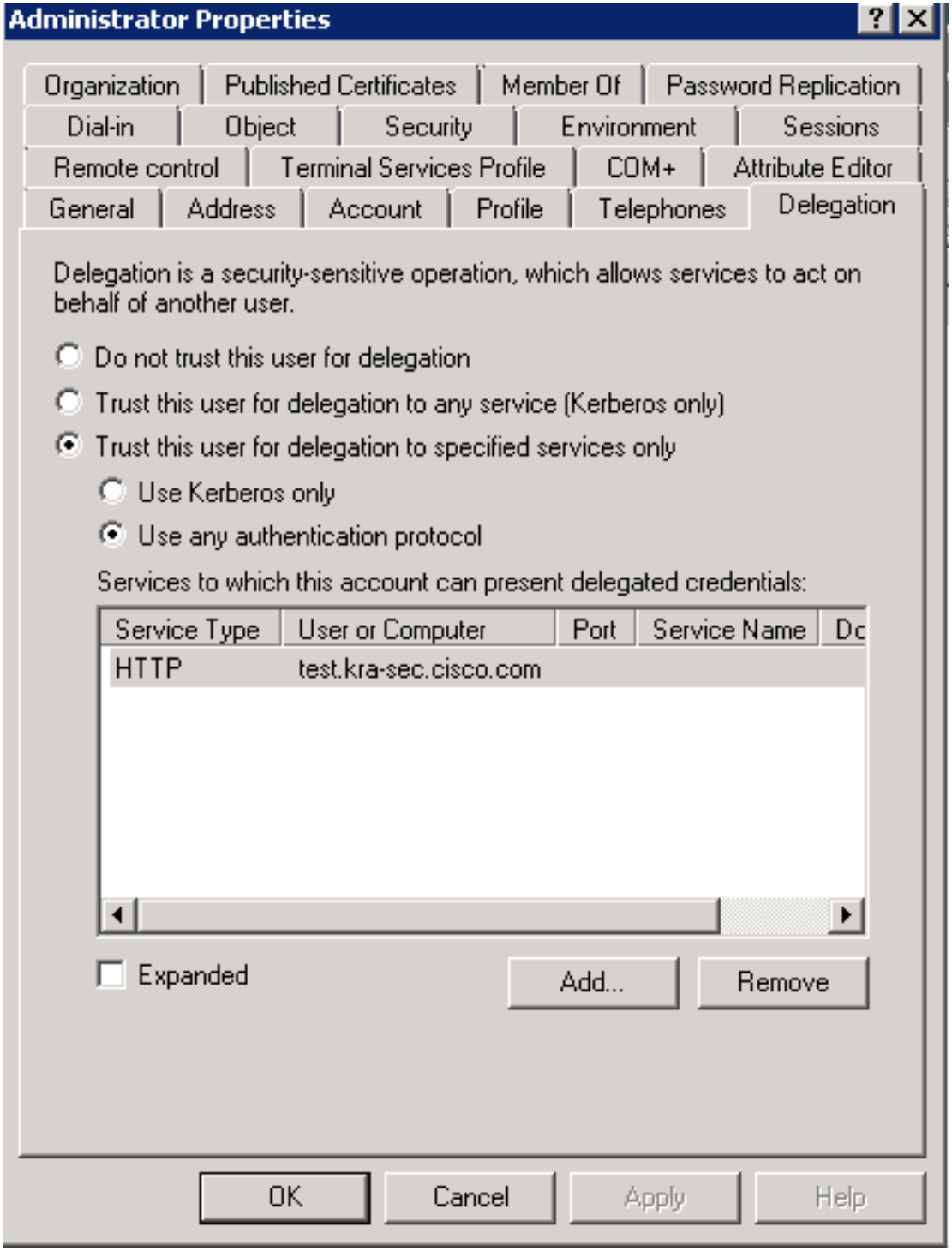
Ènecessario configurare qualsiasi account in Active Directory con la delega corretta. Viene utilizzato un account Administrator. Quando l'ASA utilizza tale account, è in grado di richiedere un ticket per conto di un altro utente (delega vincolata) per il servizio specifico (applicazione HTTP). Affinché ciò avvenga, è necessario creare la delega corretta per l'applicazione o il servizio.

Per eseguire questa delega tramite la CLI con **setspn.exe**, che fa parte degli strumenti di supporto di Windows Server 2003 Service Pack 1, immettere questo comando:

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

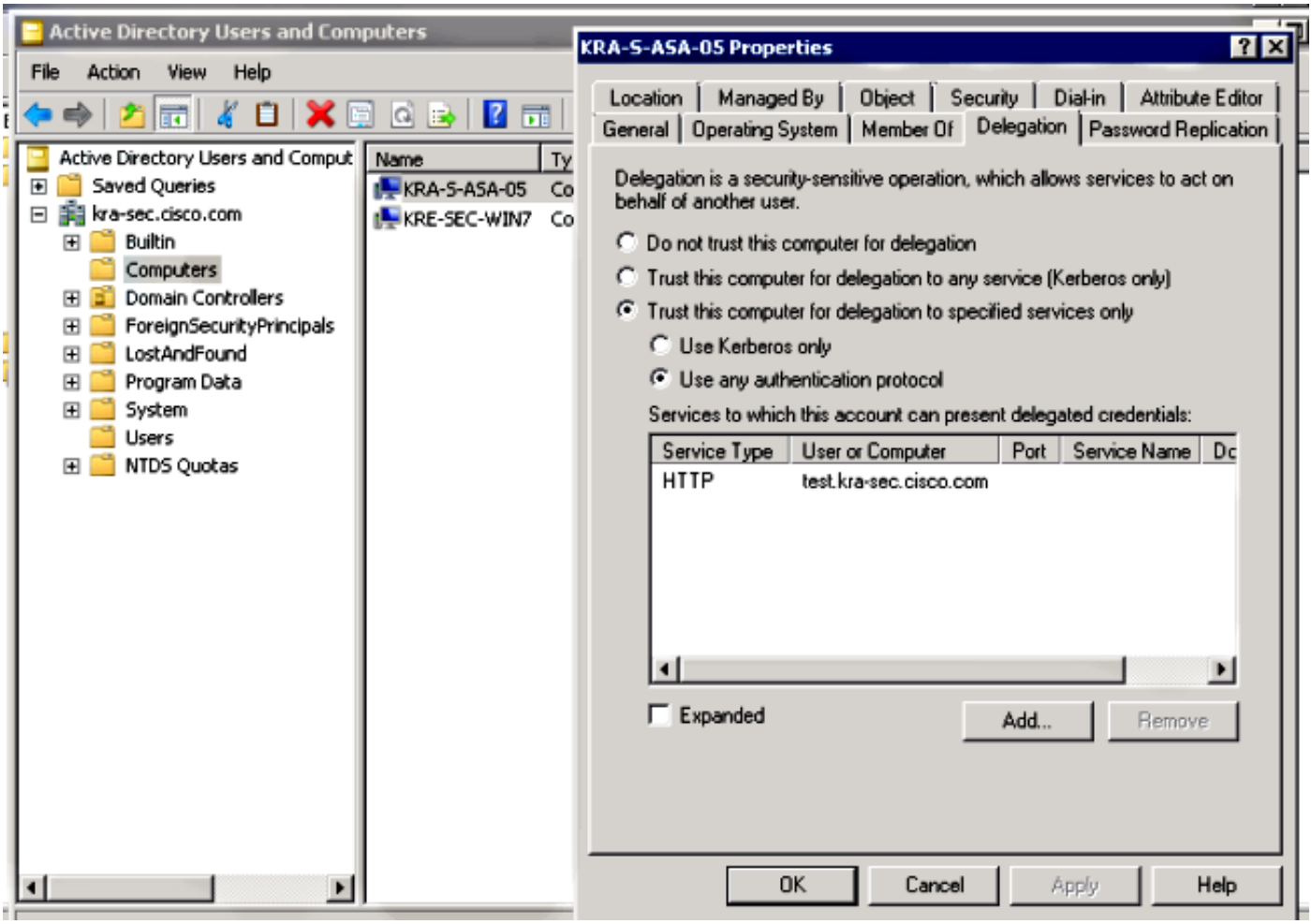
Ciò indica che il nome utente **Administrator** è l'account trusted per la delega del servizio HTTP in **test.kra-sec.cisco.com**.

Il comando **SPN** è necessario anche per attivare la scheda **Delega** per l'utente. Dopo aver immesso il comando, viene visualizzata la scheda Delega per l'amministratore. È importante abilitare l'opzione "Usa qualsiasi protocollo di autenticazione", poiché l'opzione "Usa solo Kerberos" non supporta l'estensione Delega vincolata.



Nella scheda **Generale** è inoltre possibile disattivare la preautenticazione Kerberos. Tuttavia, questa operazione non è consigliata, poiché questa funzione viene utilizzata per proteggere il controller di dominio dagli attacchi di tipo replay. L'ASA può funzionare correttamente con la preautenticazione.

Questa procedura si applica anche alla delega per l'account computer (l'ASA viene inserita nel dominio come computer per stabilire una relazione di "trust"):



Configurazione sull'appliance 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
```

Verifica

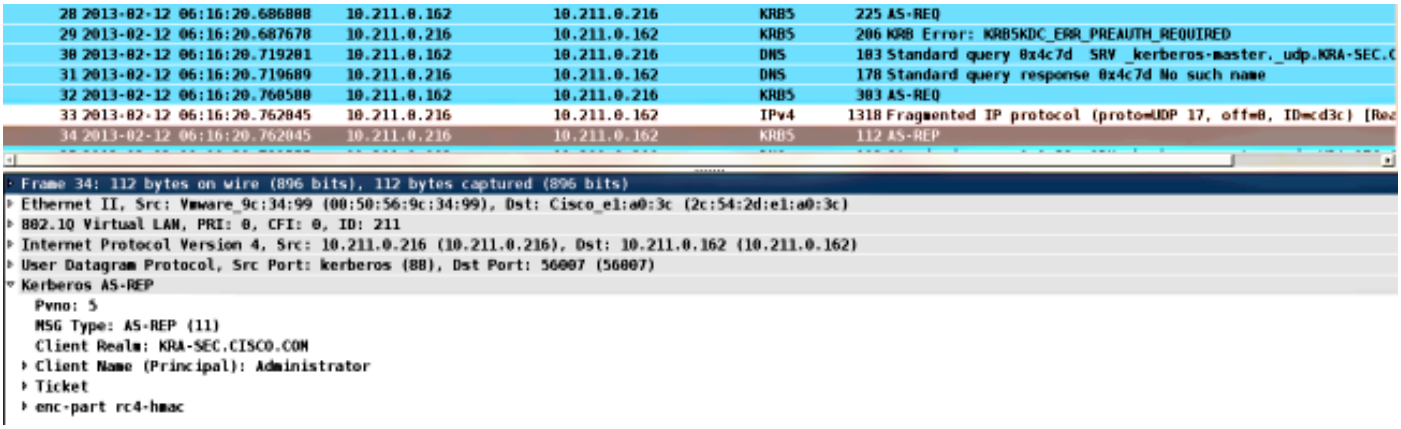
L'appliance ASA viene aggiunta al dominio

Dopo aver usato il comando **kcd-server**, l'ASA tenta di aggiungere il dominio:

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

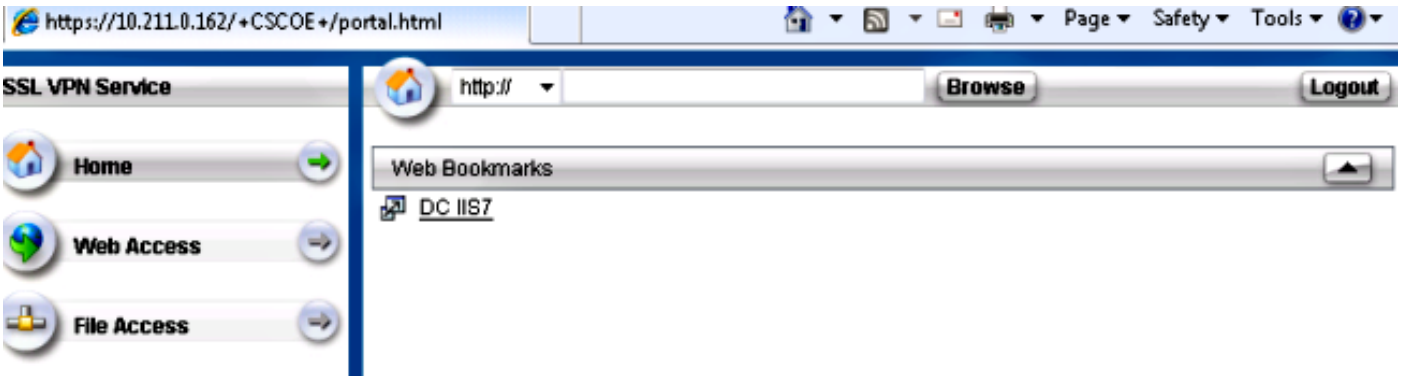
```
Kerberos: Server Name krbtgt
Kerberos: Start time 0
Kerberos: End time -878667256
Kerberos: Renew until time -878672192
Kerberos: Nonce 0xa9db408e
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4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

L'appliance ASA può essere aggiunta correttamente al dominio. Dopo la corretta autenticazione, l'ASA riceve un ticket per l'utente/gruppo/ruolo: Amministratore nel pacchetto **AS_REP** (ticket 1 descritto al punto 1).

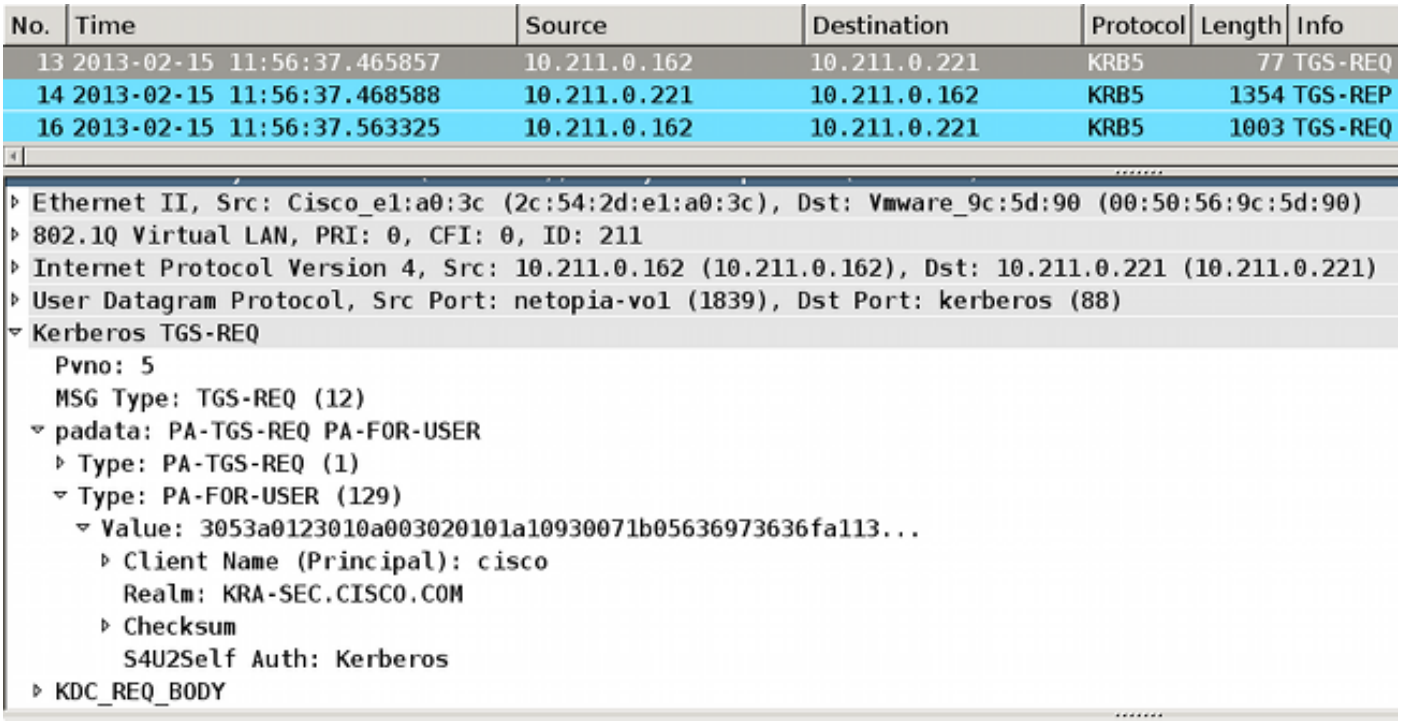


Richiesta di servizio

L'utente fa clic sul collegamento WebVPN:

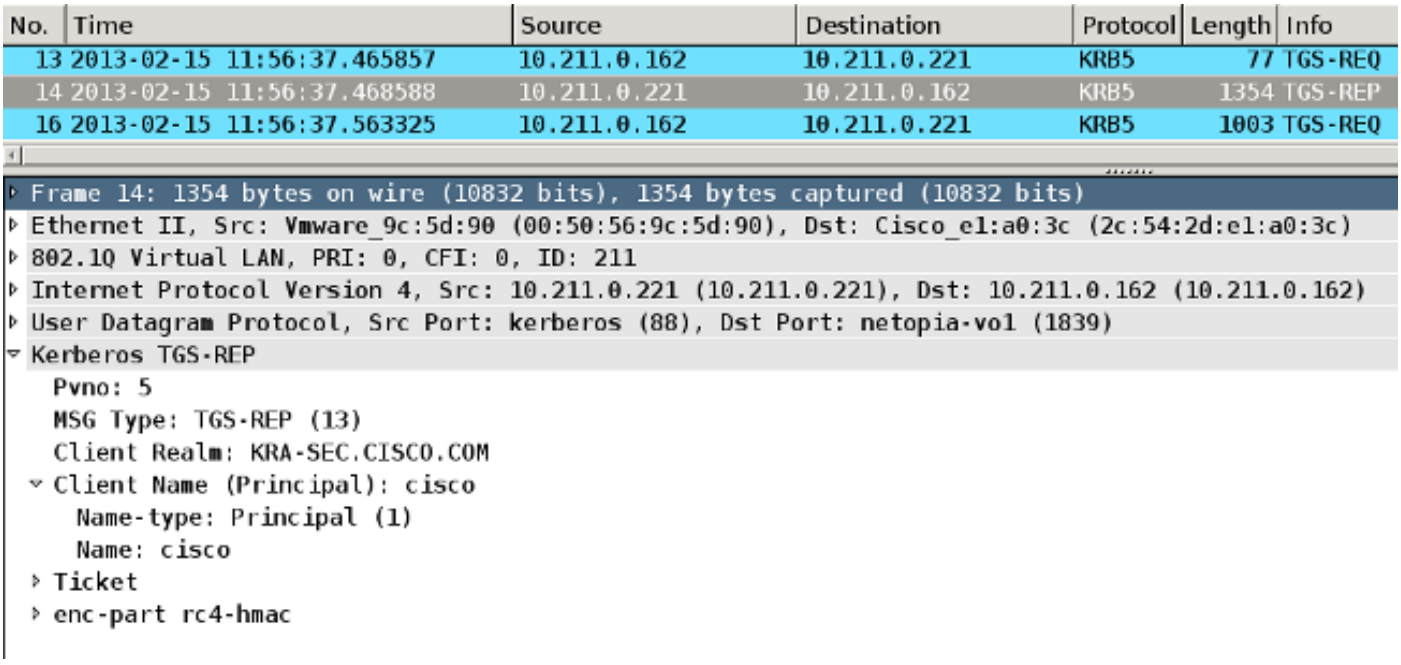


L'ASA invia al **TGS_REQ** un ticket rappresentato con il ticket ricevuto nel pacchetto **AS_REP**:



Nota: Il valore **PA-PER-UTENTE** è **cisco** (utente WebVPN). **PA-TGS-REQ** contiene il ticket ricevuto per la richiesta di servizio Kerberos (il nome host ASA è l'entità).

L'ASA riceve una risposta corretta con il ticket rappresentato per l'utente **cisco** (ticket 2 descritto nel passaggio 4):



Di seguito è riportata la richiesta di ticket per il servizio HTTP (alcuni debug sono omessi per chiarezza):

```
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
```

L'ASA riceve il ticket rappresentato corretto per il servizio HTTP (ticket 3 descritto nel passaggio 6).

Entrambi i biglietti possono essere verificati. Il primo è il ticket rappresentato per l'utente **cisco**, utilizzato per richiedere e ricevere il secondo ticket per il servizio HTTP a cui si accede:

```
KRA-S-ASA-05(config)# show aaa kerberos
Default Principal: cisco@KRA-SEC.CISCO.COM
Valid Starting       Expires              Service Principal
```

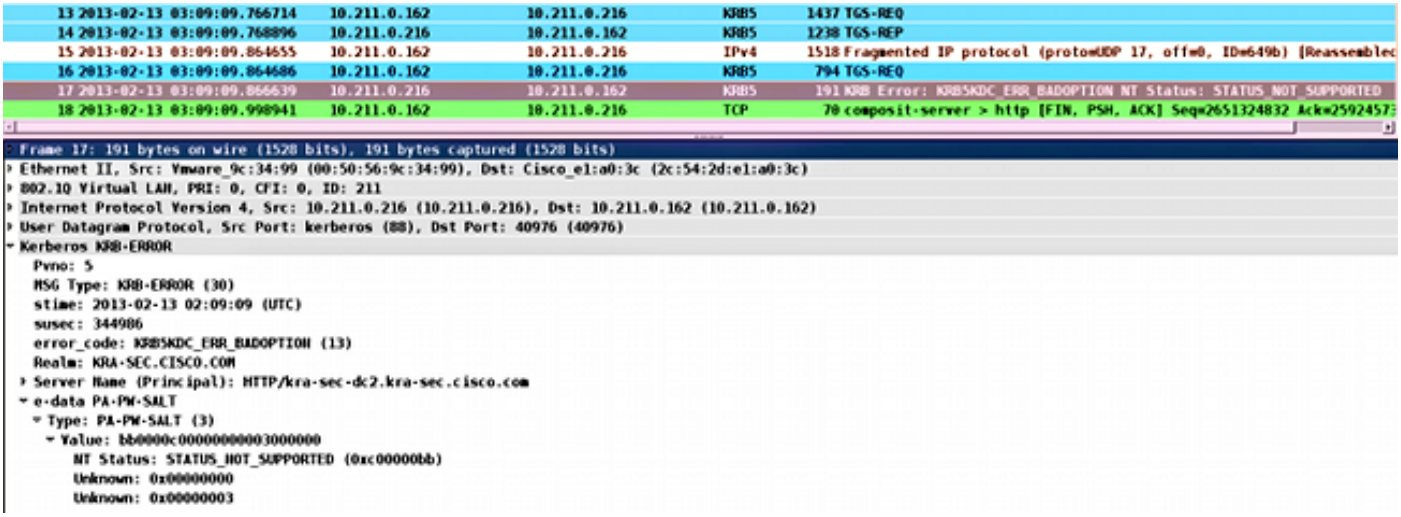
```
19:38:10 CEST Oct 2 2013 05:37:33 CEST Oct 3 2013 KRA-S-ASA-05@KRA-SEC.CISCO.COM

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
```

Questo ticket HTTP (Ticket3) viene utilizzato per l'accesso HTTP (con SPNEGO) e l'utente non deve fornire credenziali.

Risoluzione dei problemi

A volte può verificarsi un problema di delega non corretta. Ad esempio, l'ASA utilizza un ticket per richiedere il servizio **HTTP/test.kra-sec.cisco.com** (passaggio 5), ma la risposta è **KRB-ERROR** con **ERR_BADOBE**:



Si tratta di un problema tipico che si verifica quando la delega non è configurata correttamente. L'ASA riporta che **"KDC non può soddisfare l'opzione richiesta"**:

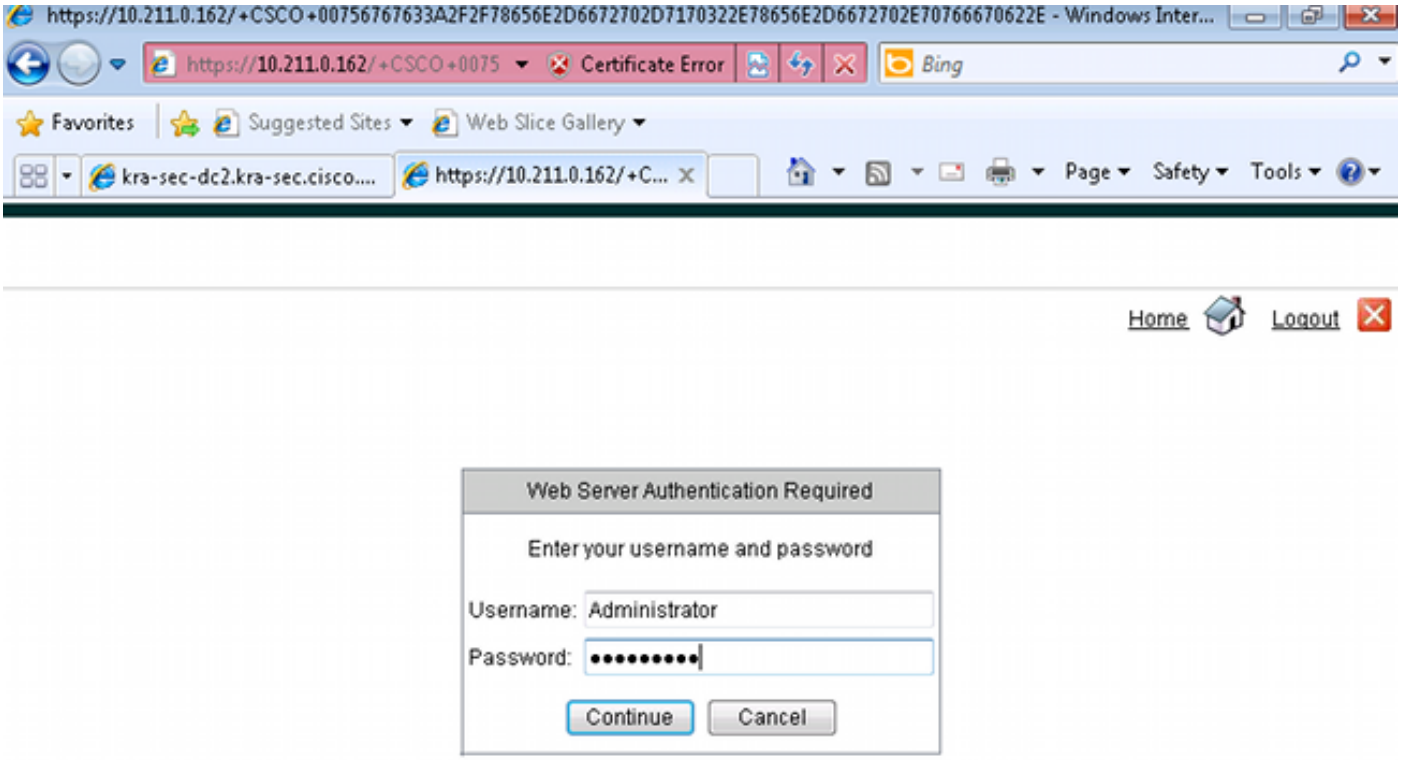
```
KRA-S-ASA-05# ucte_krb_get_auth_cred(): ctx = 0xcc4b5390,
WebVPN_session = 0xc919a260, protocol = 1
find_spn_in_url(): URL - /
build_host_spn(): host - test.kra-sec.cisco.com
build_host_spn(): SPN - HTTP/test.kra-sec.cisco.com
KCD_unicorn_get_cred(): Attempting to retrieve required KCD tickets.
In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

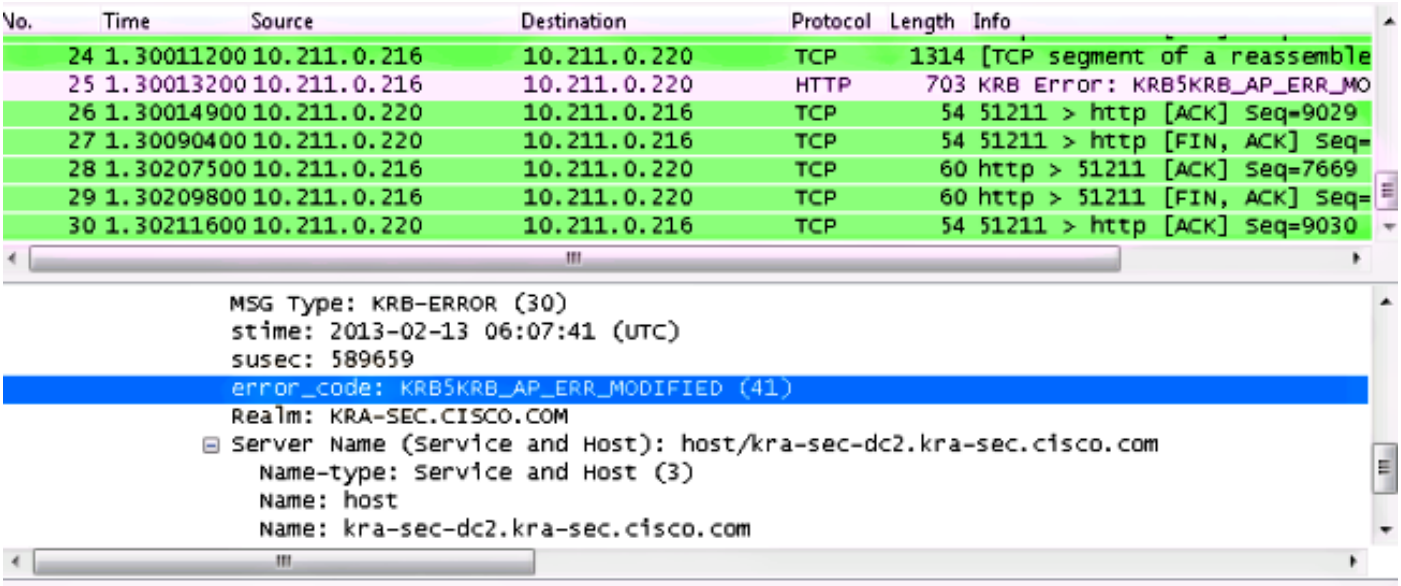
Si tratta fondamentalmente dello stesso problema descritto nelle acquisizioni: il guasto si verifica **a TGS_REQ con BAD_OPTION**.

Se la risposta è **Riuscita**, l'ASA riceve un ticket per il servizio **HTTP/test.kra-sec.cisco.com**, utilizzato per la negoziazione **SPNEGO**. Tuttavia, a causa dell'errore, **NT LAN Manager (NTLM)** viene negoziato e l'utente deve fornire le credenziali:

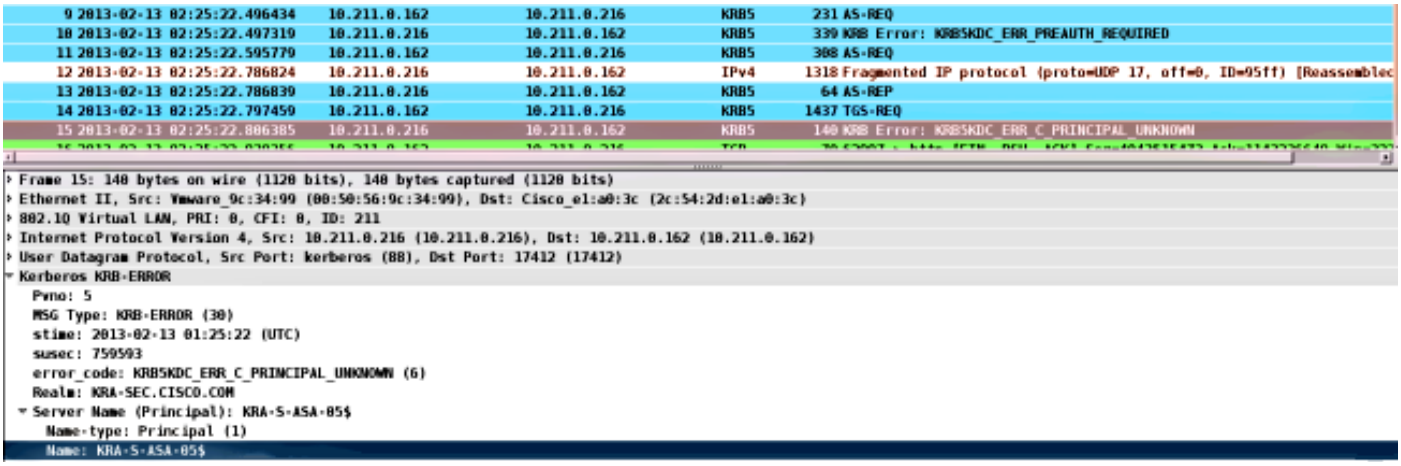


Verificare che l'SPN sia registrato per un solo account (script dall'articolo precedente). Quando si

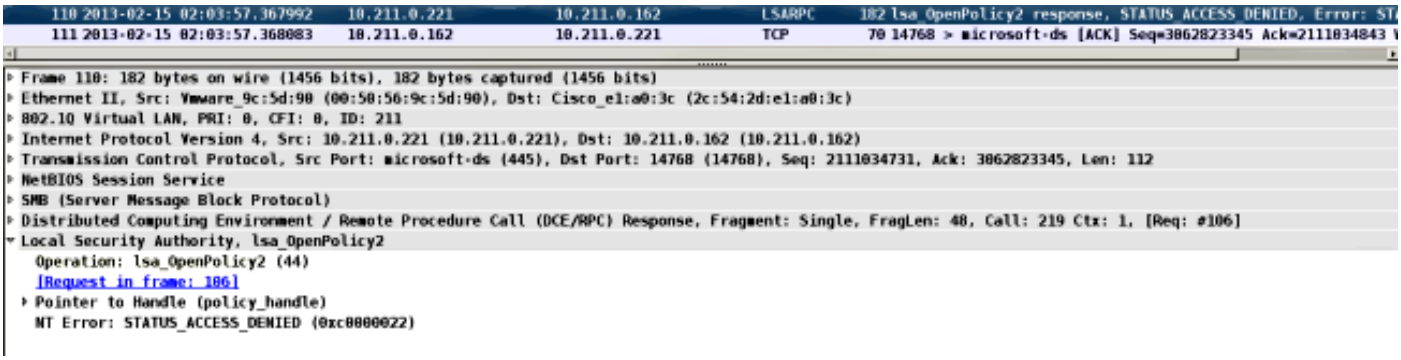
riceve questo errore, **KRB_AP_ERR_MODIFIED**, in genere significa che l'**SPN** non è registrato per l'account corretto. Deve essere registrato per l'account utilizzato per eseguire l'applicazione (pool di applicazioni in IIS).



Quando viene visualizzato questo errore, **KRB_ERR_C_PRINCIPAL_UNKNOWN**, significa che non è presente alcun utente nel controller di dominio (utente WebVPN: **cisco**).



Èpossibile che questo problema si verifichi quando si accede al dominio. L'ASA riceve il comando **AS-REP**, ma ha esito negativo a livello **LSA** con il seguente errore: **STATUS_ACCESS_DENIED**:



Per risolvere il problema, è necessario abilitare/disabilitare la preautenticazione sul controller di dominio per l'utente (**amministratore**).

Di seguito sono riportati altri problemi che possono verificarsi:

- L'aggiunta al dominio potrebbe causare problemi. Se il server controller di dominio ha più schede NIC (Network Interface Controller) (indirizzi IP multipli), verificare che l'ASA possa accedervi tutte per poter aggiungere il server al dominio (scelta casuale dal client in base alla risposta DNS (Domain Name Server)).

- Non impostare **SPN** come **HOST/dc.kra-sec.cisco.com** per l'account **Administrator**. A causa di tale impostazione è possibile perdere la connettività al controller di dominio.

- Dopo l'aggiunta dell'ASA al dominio, è possibile verificare che sul controller di dominio sia stato creato l'account computer corretto (nome host ASA). Verificare che l'utente disponga delle autorizzazioni corrette per aggiungere account computer (in questo esempio, l'**amministratore** dispone delle autorizzazioni corrette).

- Memorizzare la configurazione **NTP (Network Time Protocol)** corretta sull'appliance ASA. Per impostazione predefinita, il controller di dominio accetta uno sfasamento di cinque minuti. Il timer può essere modificato sul controller di dominio.

- Verificare la connettività Kerberos per il pacchetto di piccole dimensioni **UDP/88**. Dopo l'errore del controller di dominio **KRB5KDC_ERR_RESPONSE_TOO_BIG**, il client passa a **TCP/88**. È possibile forzare il client Windows a utilizzare **TCP/88**, ma per impostazione predefinita **ASA utilizzerà UDP**.

- CC: quando si apportano modifiche ai criteri, ricordare **gpupdate /force**.

- ASA: verificare l'autenticazione con il comando **test aaa**, ma ricordare che si tratta solo di un'autenticazione semplice.

- Per risolvere i problemi nel sito controller di dominio, è utile abilitare i debug Kerberos: Come abilitare la registrazione degli eventi Kerberos.

ID bug Cisco

Di seguito è riportato un elenco degli ID dei bug Cisco pertinenti:

- ID bug Cisco CSCsi3224 - L'ASA non passa al TCP dopo aver ricevuto il codice di errore Kerberos 52
- ID bug Cisco CSCtd92673 - Autenticazione Kerberos non riuscita con preautenticazione abilitata
- ID bug Cisco CSCuj19601 - ASA Webvpn KCD - tentativo di accesso ad Active Directory solo dopo il riavvio
- ID bug Cisco CSCuh32106 - Il KCD ASA viene interrotto a partire dalla versione 8.4.5

Informazioni correlate

- Informazioni sulla delega vincolata Kerberos
- Funzionamento di KCD
- PIX/ASA: Esempio di configurazione dell'autenticazione Kerberos e dei gruppi di server di

autorizzazione LDAP per utenti client VPN tramite ASDM/CLI

- Guida di riferimento ai comandi di Cisco ASA serie 1000
- KDC_ERR_BAPPROVAL durante il tentativo di delega vincolata
- Come forzare Kerberos a utilizzare TCP anziché UDP in Windows
- Documentazione e supporto tecnico – Cisco Systems