Exemplo de configuração de integração SSO de WebVPN com delegação restrita de Kerberos

Contents

Introduction

Este documento descreve como configurar e solucionar problemas de SSO (Single Sign On, login único) do WebVPN para aplicativos protegidos por Kerberos.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico sobre estes tópicos:

- Configuração da CLI do Cisco Adaptive Security Appliance (ASA) e configuração de VPN SSL (Secure Socket Layer)
- Serviços Kerberos

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Software Cisco ASA, versão 9.0 e posterior
- Cliente Microsoft Windows 7
- Microsoft Windows 2003 Server e posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

Kerberos é um protocolo de autenticação de rede que permite que as entidades de rede se autentiquem entre si de forma segura. Ele usa um terceiro confiável, o Centro de Distribuição de Chaves (KDC), que concede tíquetes para as entidades de rede. Esses tíquetes são usados pelas entidades para verificar e confirmar o acesso ao serviço solicitado.

Épossível configurar o SSO do WebVPN para aplicativos protegidos por Kerberos com o recurso Cisco ASA chamado Kerberos Constrained Delegation (KCD). Com esse recurso, o ASA pode solicitar tíquetes Kerberos em nome do usuário do portal WebVPN, enquanto acessa aplicativos protegidos por Kerberos.

Ao acessar esses aplicativos pelo portal WebVPN, você não precisa mais fornecer credenciais; em vez disso, a conta que foi usada para fazer login no portal WebVPN é usada.

Consulte a seção Understanding How KCD Works do guia de configuração do ASA para obter mais informações.

Interação Kerberos com o ASA

Para WebVPN, o ASA deve solicitar tíquetes em nome do usuário (porque o usuário do portal WebVPN tem acesso apenas ao portal, não ao serviço Kerberos). Para isso, o ASA usa extensões Kerberos para delegação restrita. Aqui está o fluxo:

1. O ASA ingressa no domínio e obtém um tíquete (Ticket1) para uma conta de computador com credenciais configuradas no ASA (comando **kcd-server**). Esse tíquete é usado nas próximas etapas para o acesso aos serviços Kerberos.

2. O usuário clica no link do portal WebVPN para o aplicativo protegido por Kerberos.

3. O ASA solicita (**TGS-REQ**) um tíquete para a conta do computador com seu nome de host como principal. Esta solicitação inclui o campo **PA-TGS-REQ** com **PA-FOR-USER** com o principal como o nome de usuário do portal WebVPN, que é **cisco** neste cenário. O tíquete do serviço Kerberos da Etapa 1 é usado para autenticação (delegação correta).

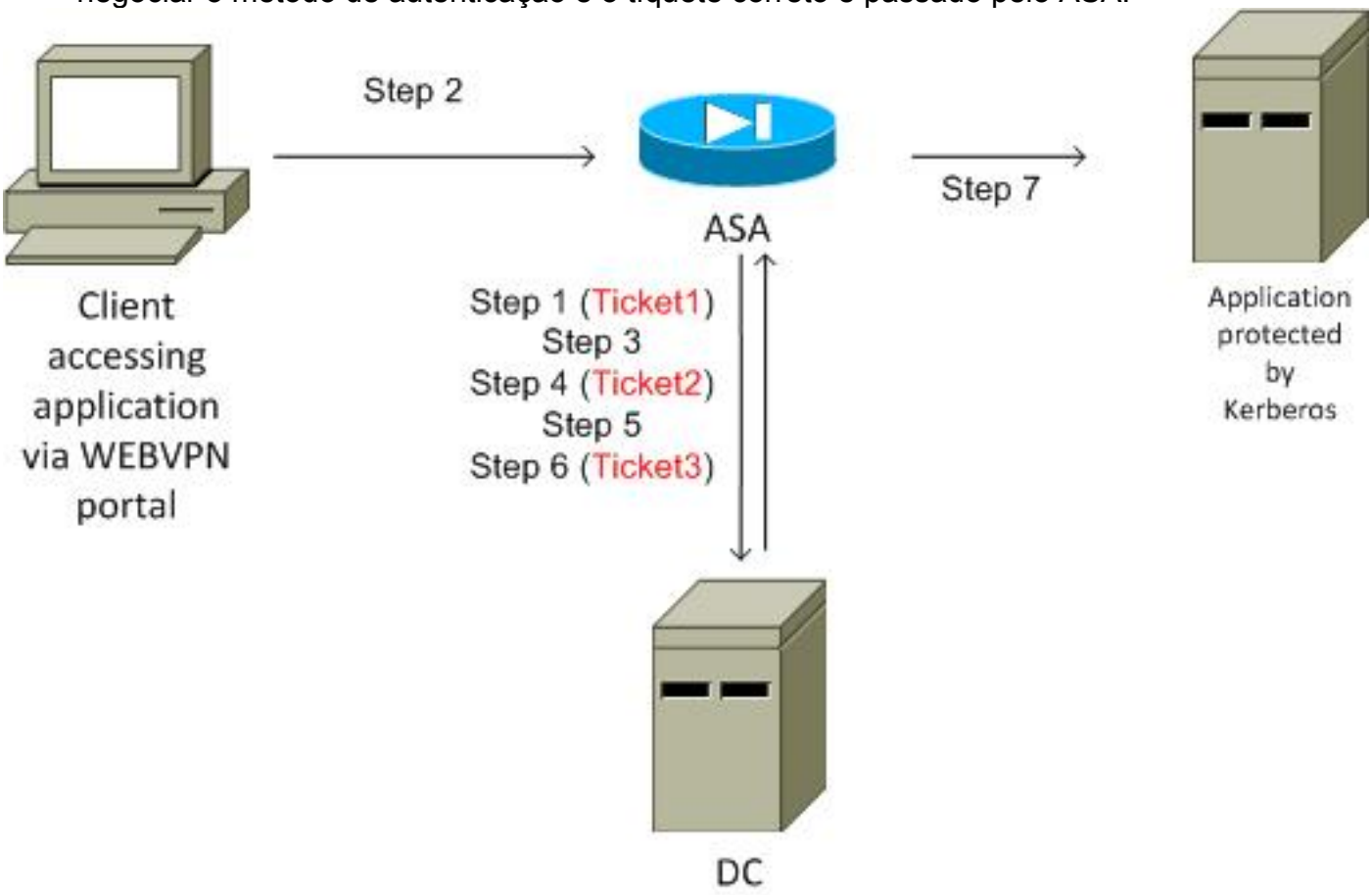
4. Como resposta, o ASA recebe um tíquete personalizado (Ticket2) em nome do usuário

WebVPN (**TGS_REP**) para a conta do computador. Esse tíquete é usado para solicitar tíquetes de aplicativo em nome deste usuário WebVPN.

5. O ASA inicia outra solicitação (**TGS_REQ**) para obter o tíquete para o aplicativo (**HTTP/test.kra-sec.cisco.com**). Esta solicitação novamente usa o campo **PA-TGS-REQ**, desta vez **sem o** campo **PA-FOR-USER**, mas com o tíquete personalizado recebido na Etapa 4.

6. A resposta (**TGS_REQ**) com o tíquete personalizado (Ticket3) para o aplicativo é retornada.

7. Esse tíquete é usado de forma transparente pelo ASA para acessar o serviço protegido e o usuário do WebVPN não precisa inserir nenhuma credencial. Para o aplicativo HTTP, o mecanismo de negociação de API GSS simples e protegida (SPNEGO) é usado para negociar o método de autenticação e o tíquete correto é passado pelo ASA.



Configurar

Topologia

Domínio: kra-sec.cisco.com (10.211.0.221 ou 10.211.0.216)

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

Controlador de domínio (DC): dc.kra-sec.cisco.com (10.211.0.221 ou 10.211.0.216) - Windows2008

ASA: 10.211.0.162

Nome de usuário/senha do WebVPN: Cisco/Cisco

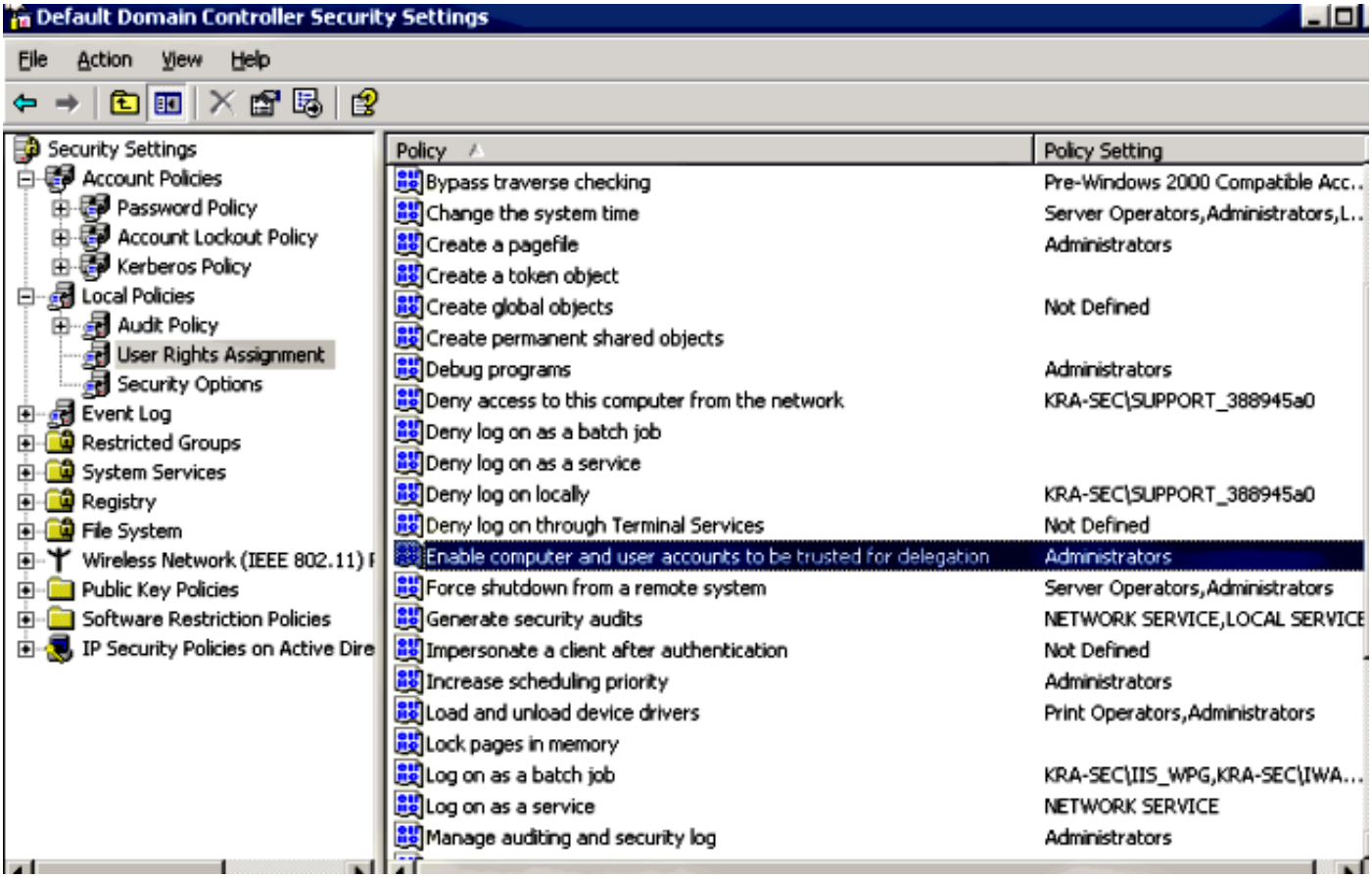
Ficheiro anexado: asa-join.pcap (associação bem-sucedida ao domínio)

Ficheiro anexado: asa-kerberos-bad.pcap (solicitação de serviço)

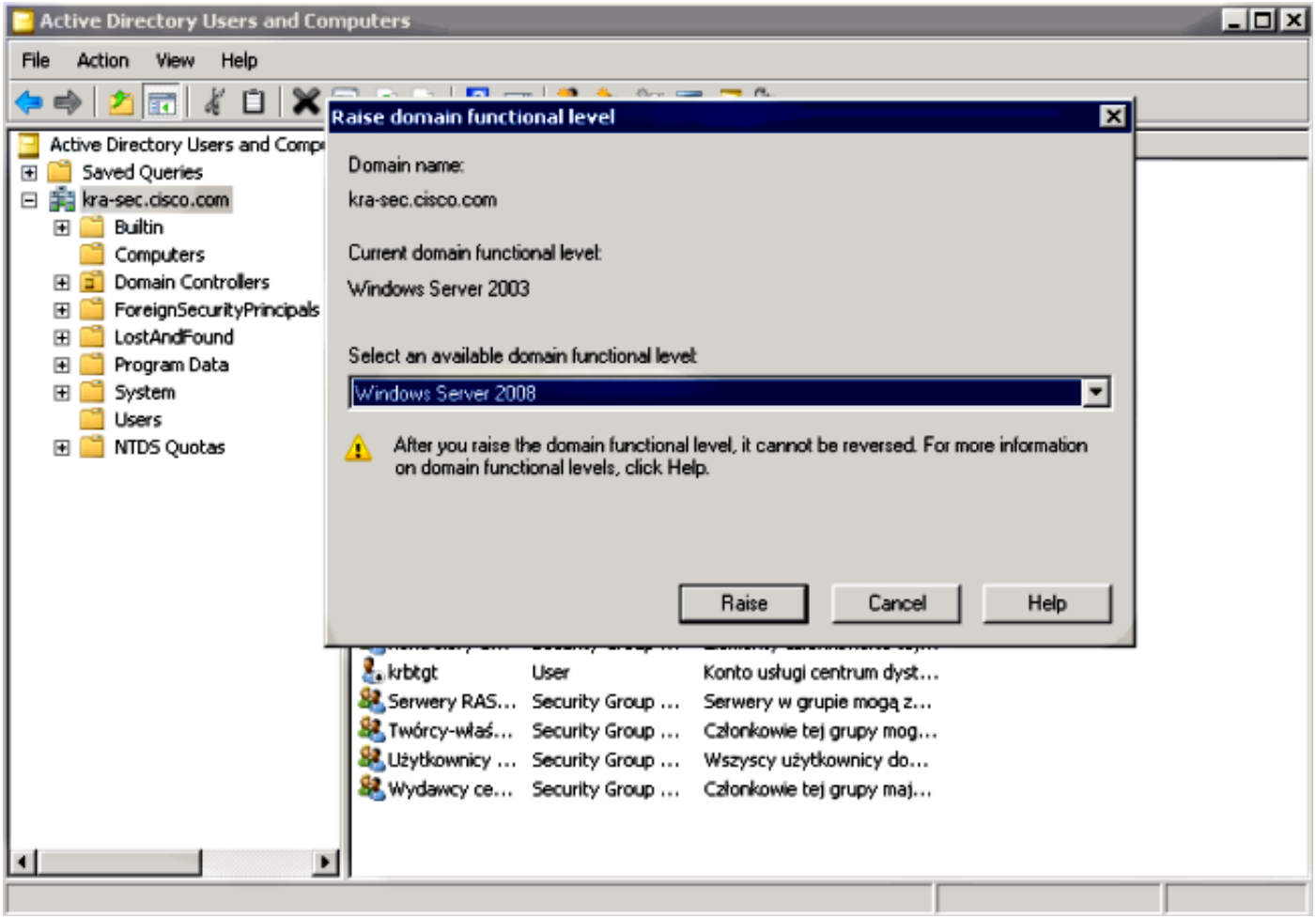
Configuração do controlador de domínio e do aplicativo

Configurações de domínio

Supõe-se que já existe um aplicativo IIS7 funcional protegido por Kerberos (se não, leia a seção Pré-requisitos). Você deve verificar as configurações das delegações dos usuários:



Certifique-se de que o nível de domínio funcional seja elevado ao Windows Server 2003 (pelo menos). O padrão é Windows Server 2000:



Definir o nome do principal de serviço (SPN)

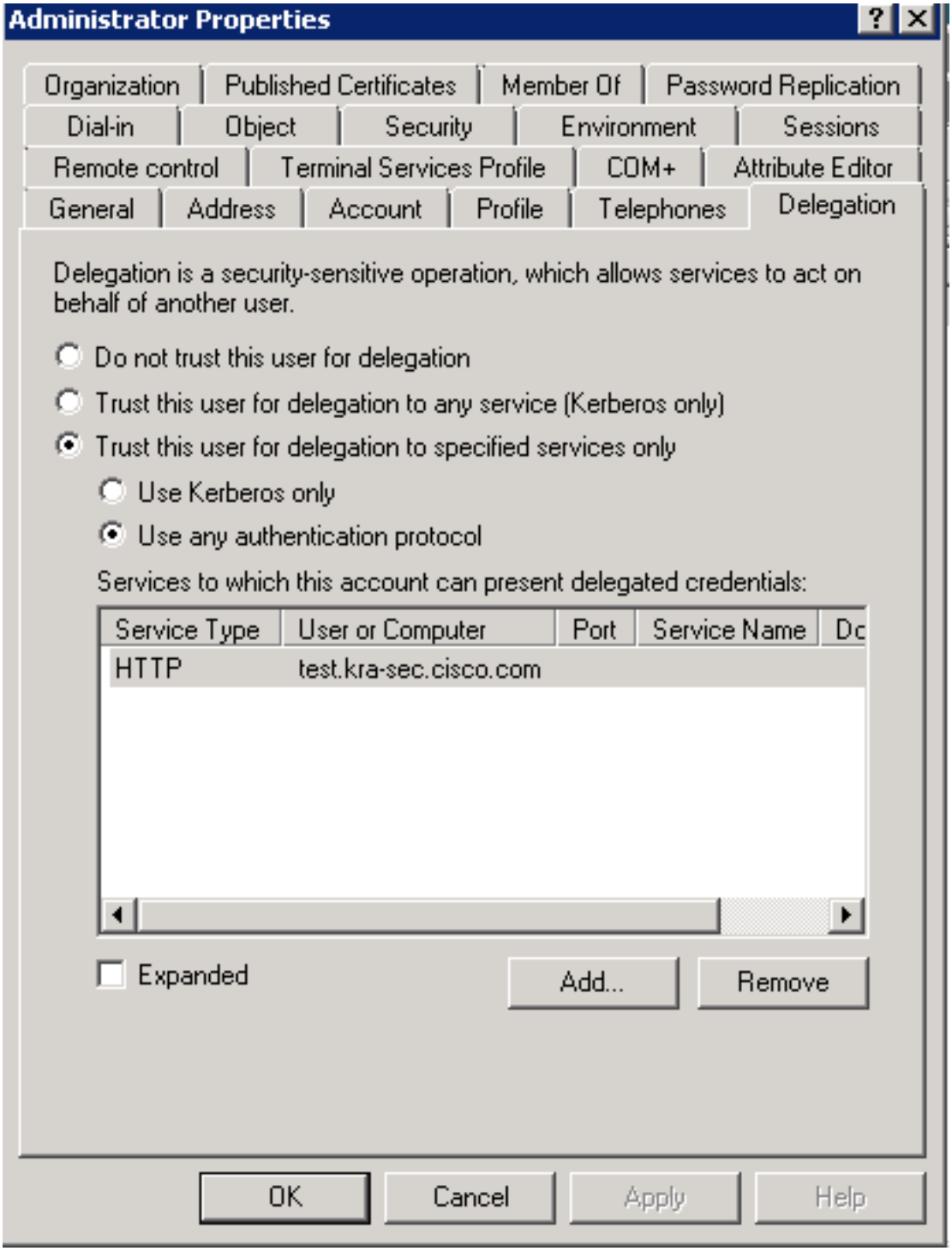
Você deve configurar qualquer conta no AD com a delegação correta. Uma conta de administrador é usada. Quando o ASA usa essa conta, ele pode solicitar um tíquete em nome de outro usuário (Delegação restrita) para o serviço específico (aplicativo HTTP). Para que isso ocorra, a delegação correta deve ser criada para o aplicativo/serviço.

Para fazer esta delegação via CLI com o **setspn.exe**, que faz parte das Ferramentas de Suporte do Windows Server 2003 Service Pack 1 , digite este comando:

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

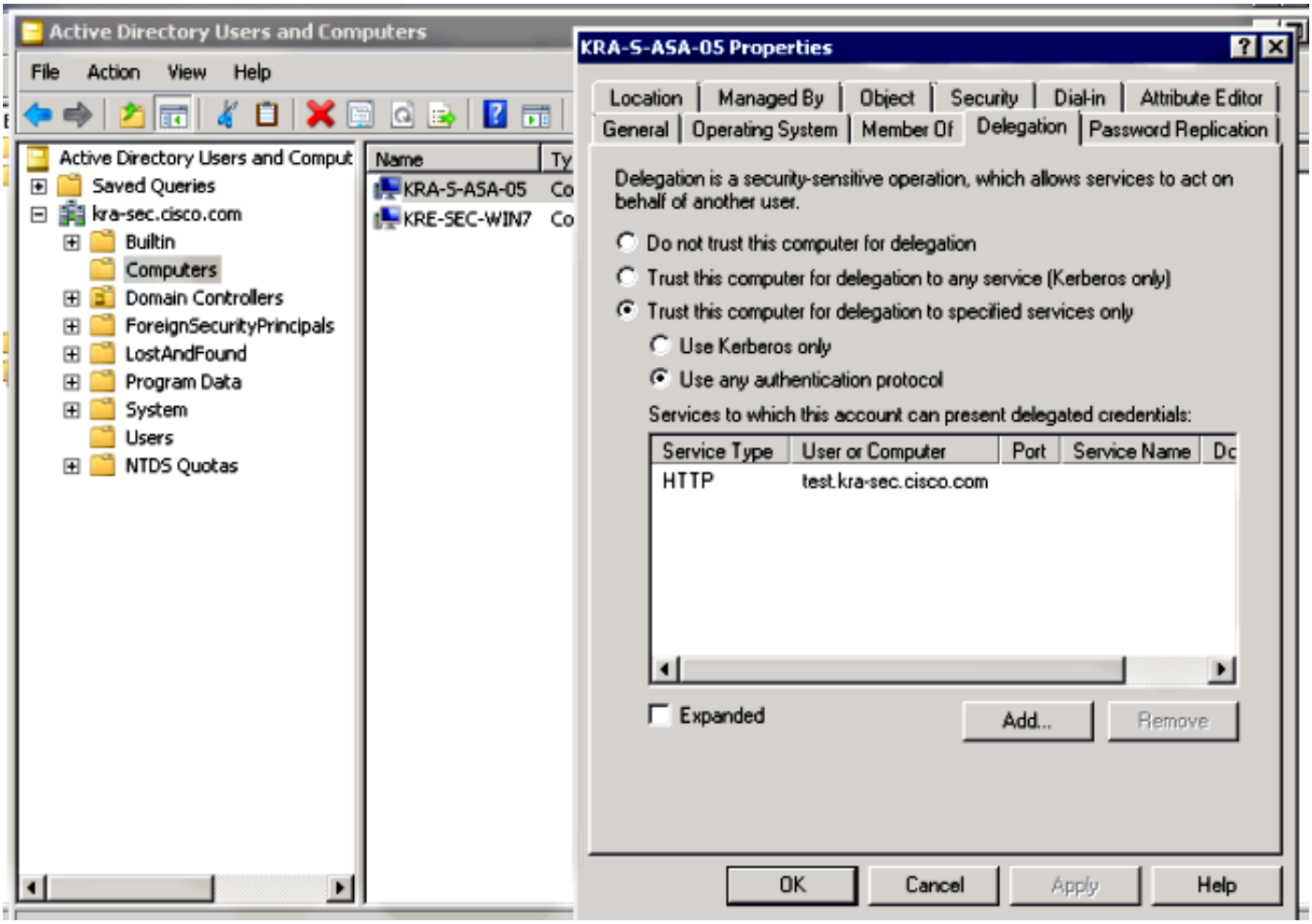
Isso indica que o nome de usuário **Administrador** é a conta confiável para a delegação do serviço HTTP em **test.kra-sec.cisco.com**.

O comando **SPN** também é necessário para ativar a guia **Delegação** para esse usuário. Quando você digita o comando, a guia Delegação do Administrador é exibida. É importante ativar "Usar qualquer protocolo de autenticação", pois "Usar somente Kerberos" não suporta a extensão da delegação restrita.



Na guia **Geral**, também é possível desativar a pré-autenticação Kerberos. No entanto, isso não é recomendado, pois esse recurso é usado para proteger o DC contra ataques de repetição. O ASA pode trabalhar com a pré-autenticação corretamente.

Este procedimento também se aplica à delegação para a conta do computador (o ASA é trazido para o domínio como um computador para estabelecer uma relação de "confiança"):



Configuração no 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
```

Verificar

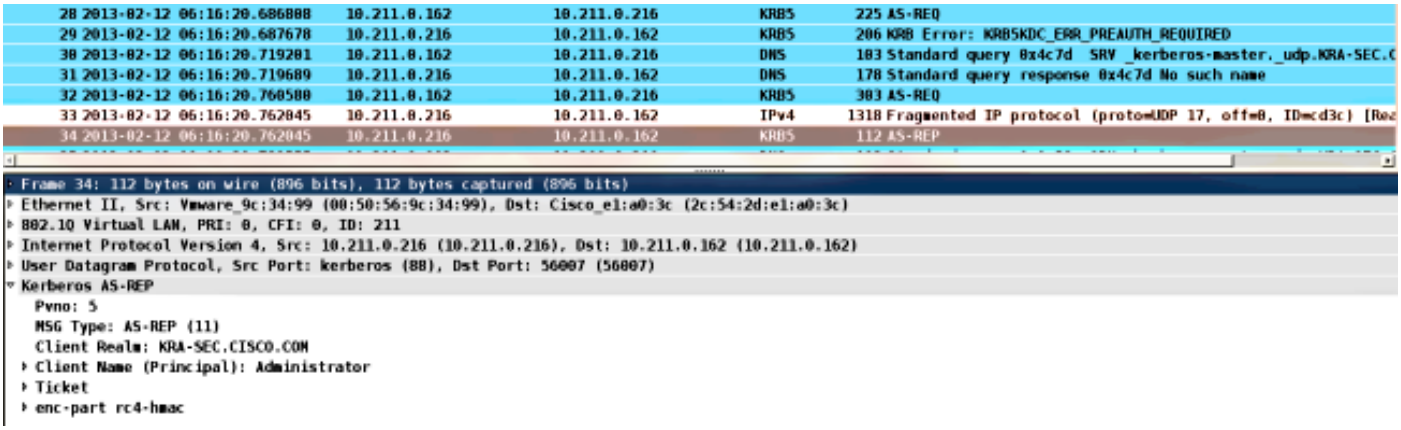
O ASA ingressa no domínio

Depois que o comando **kcd-server** é usado, o ASA tenta ingressar no domínio:

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

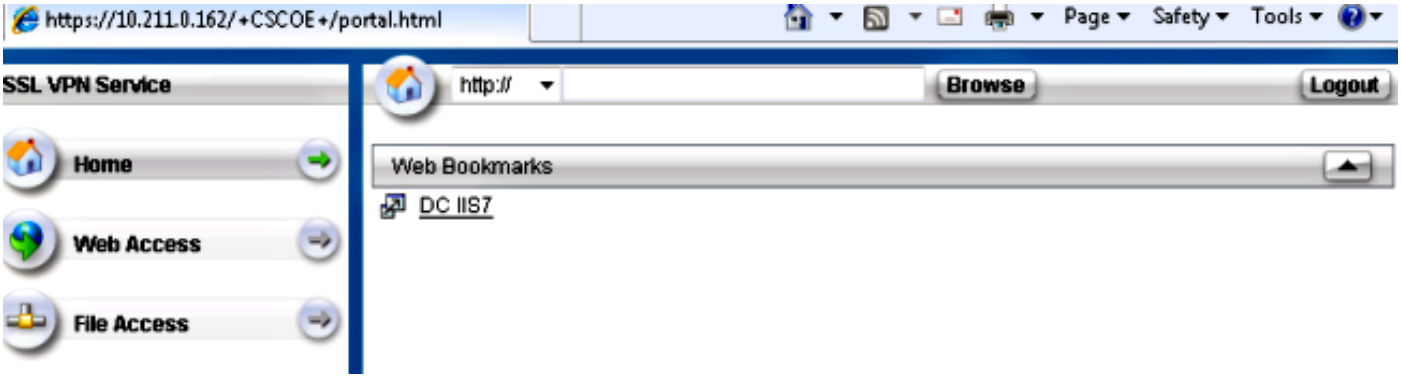
```
Kerberos: Server Name krbtgt
Kerberos: Start time 0
Kerberos: End time -878667256
Kerberos: Renew until time -878672192
Kerberos: Nonce 0xa9db408e
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4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

O ASA pode ingressar no domínio com êxito. Após a autenticação correta, o ASA recebe um tíquete para o principal: Administrador no pacote **AS_REP** (Ticket1 descrito na Etapa 1).

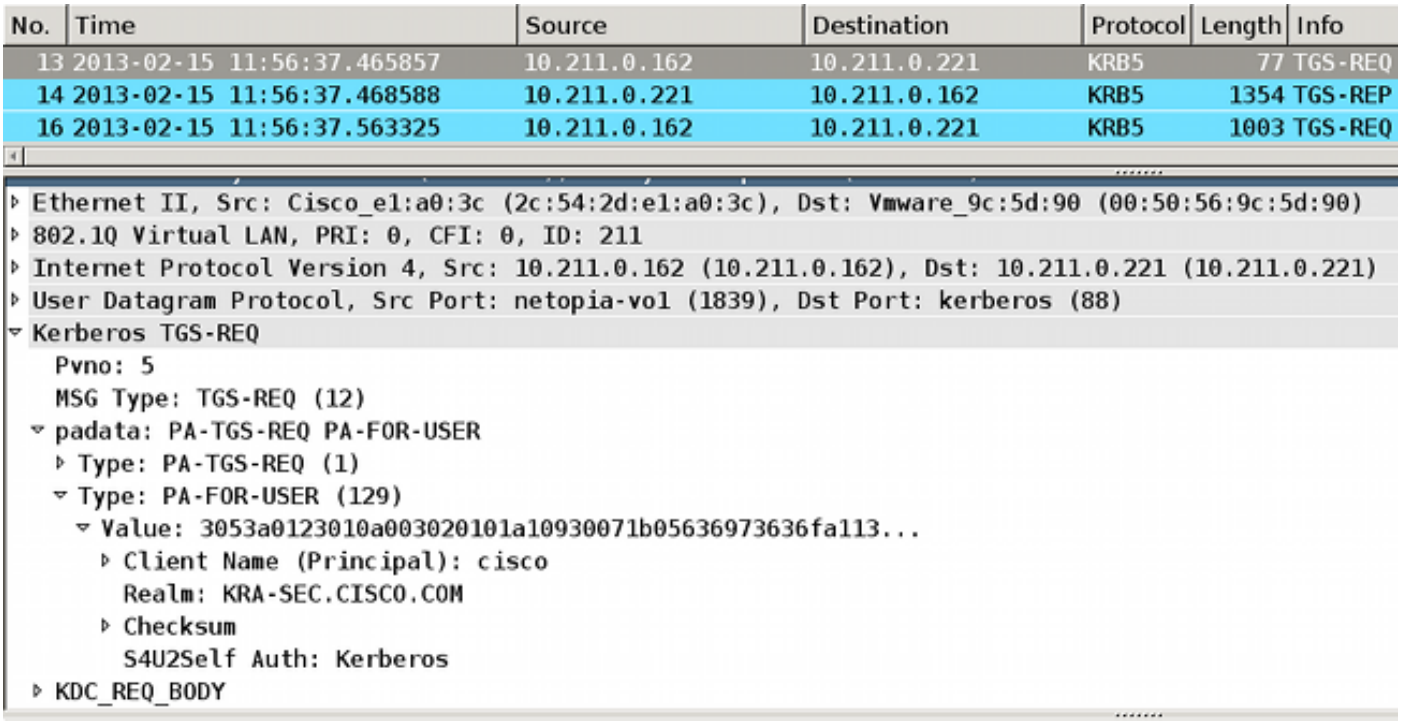


Solicitação de serviço

O usuário clica no link WebVPN:

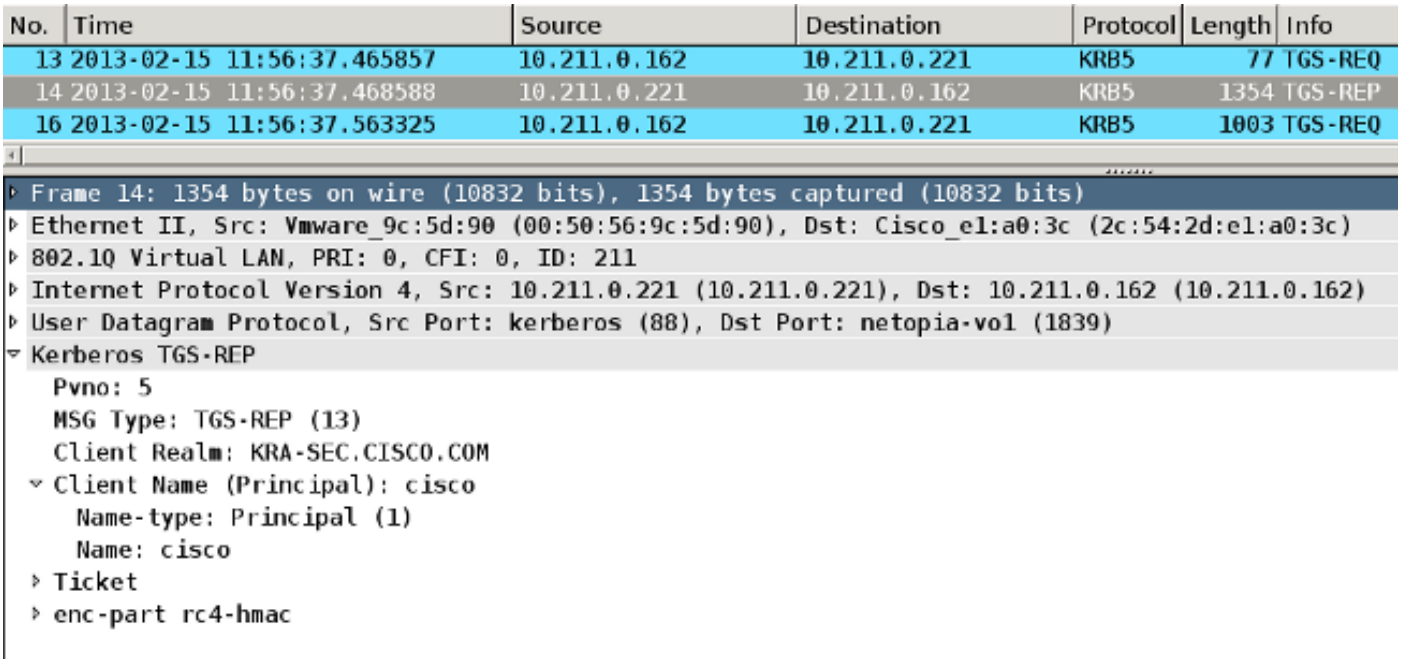


O ASA envia o **TGS_REQ** para um tíquete personalizado com o tíquete recebido no pacote **AS_REP**:



Note: O valor **PA-FOR-USER** é **cisco** (usuário WebVPN). **PA-TGS-REQ** contém o tíquete recebido para a solicitação de serviço Kerberos (o nome de host ASA é o principal).

O ASA recebe uma resposta correta com o tíquete personalizado para o usuário **cisco** (tíquete2 descrito na Etapa 4):



Aqui está a solicitação para o tíquete do serviço HTTP (algumas depurações são omitidas para maior clareza):

```
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
```

O ASA recebe o tíquete representado correto para o serviço HTTP (tíquete3 descrito na Etapa 6).

Os dois tíquetes podem ser verificados. O primeiro é o tíquete personalizado para o usuário **cisco**, que é usado para solicitar e receber o segundo tíquete para o serviço HTTP acessado:

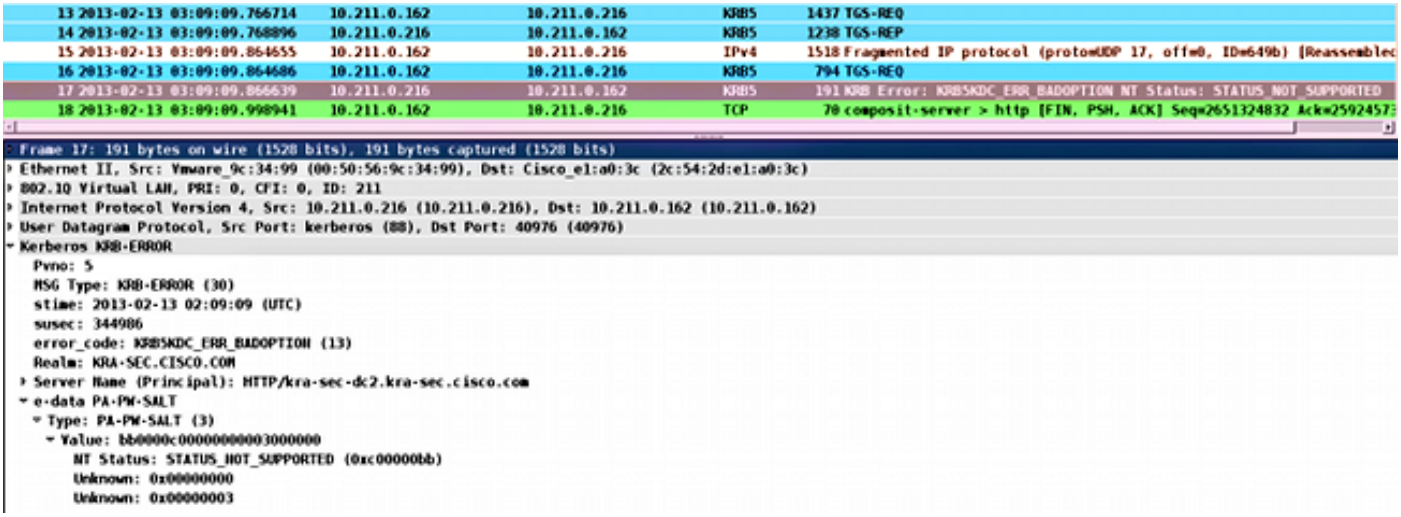
```
KRA-S-ASA-05(config)# show aaa kerberos
Default Principal: cisco@KRA-SEC.CISCO.COM
Valid Starting       Expires              Service Principal
19:38:10 CEST Oct 2 2013 05:37:33 CEST Oct 3 2013 KRA-S-ASA-05@KRA-SEC.CISCO.COM
```

```
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
```

Esse tíquete HTTP (Ticket3) é usado para acesso HTTP (com SPNEGO), e o usuário não precisa fornecer nenhuma credencial.

Troubleshoot

Às vezes, você pode encontrar um problema de delegação incorreta. Por exemplo, o ASA usa um tíquete para solicitar o serviço **HTTP/test.kra-sec.cisco.com** (Etapa 5), mas a resposta é **KRB-ERROR** com **ERR_BADOPTION**:



Esse é um problema típico encontrado quando a delegação não está configurada corretamente. O ASA relata que **"o KDC não pode atender à opção solicitada"**:

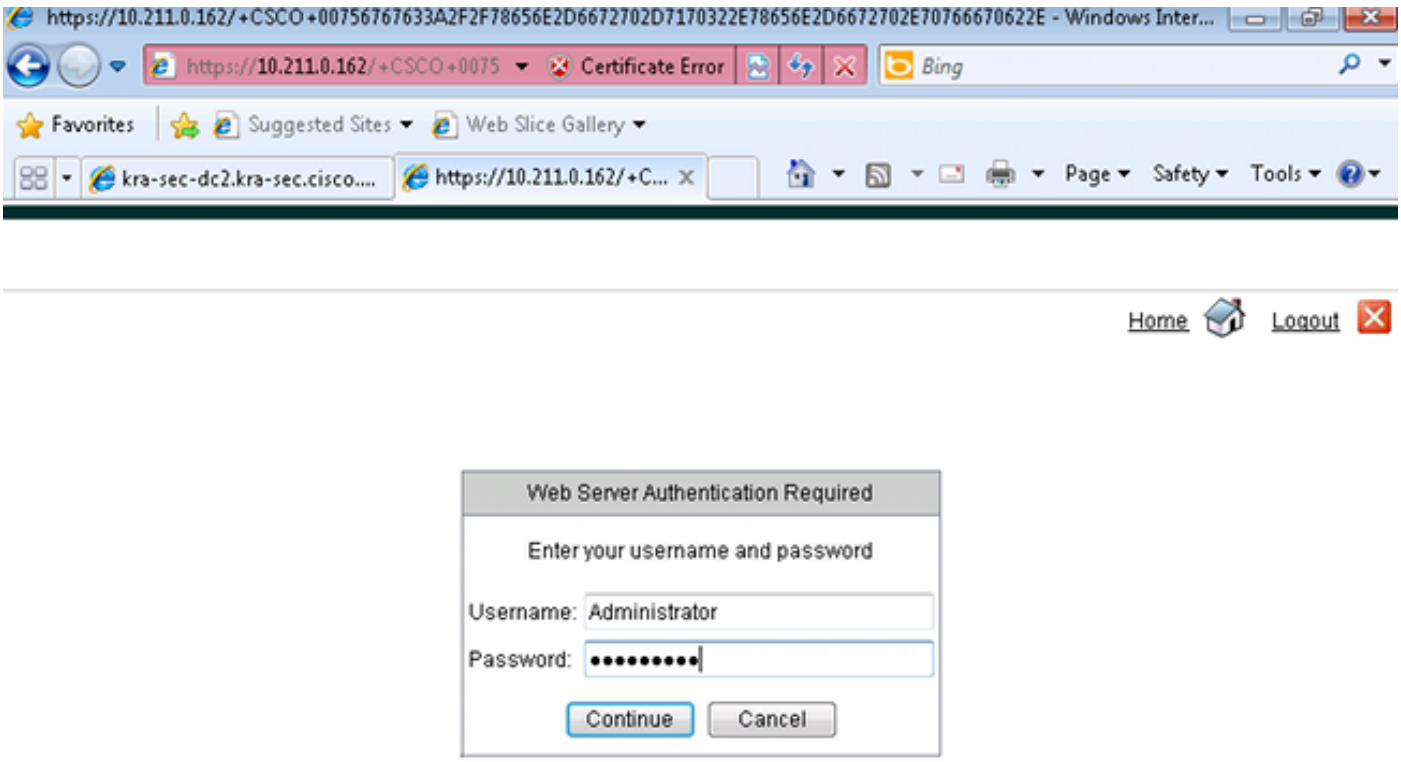
```
KRA-S-ASA-05# ucte_krb_get_auth_cred(): ctx = 0xcc4b5390,
WebVPN_session = 0xc919a260, protocol = 1
find_spn_in_url(): URL - /
build_host_spn(): host - test.kra-sec.cisco.com
build_host_spn(): SPN - HTTP/test.kra-sec.cisco.com
KCD_unicorn_get_cred(): Attempting to retrieve required KCD tickets.
In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

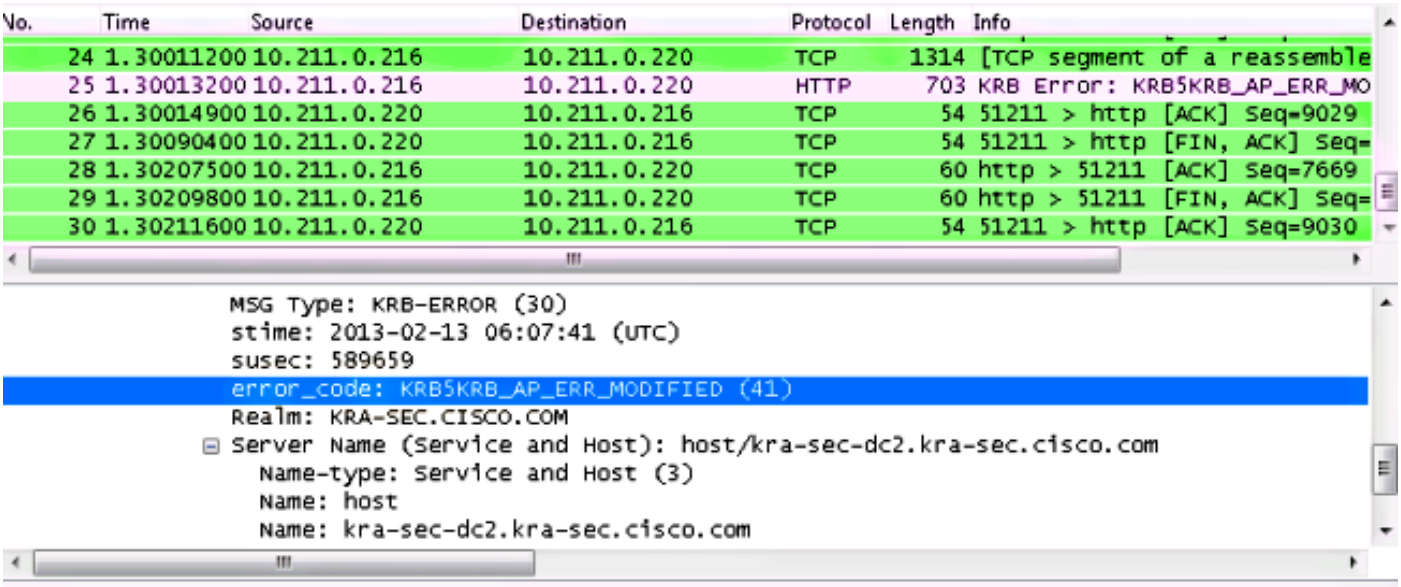
Este é basicamente o mesmo problema descrito nas capturas - a falha é **em TGS_REQ com BAD_OPTION**.

Se a resposta for **Success**, o ASA receberá um tíquete para o serviço **HTTP/test.kra-sec.cisco.com**, que é usado para a negociação **SPNEGO**. No entanto, devido à falha, o **NT LAN Manager (NTLM)** é negociado e o usuário deve fornecer credenciais:

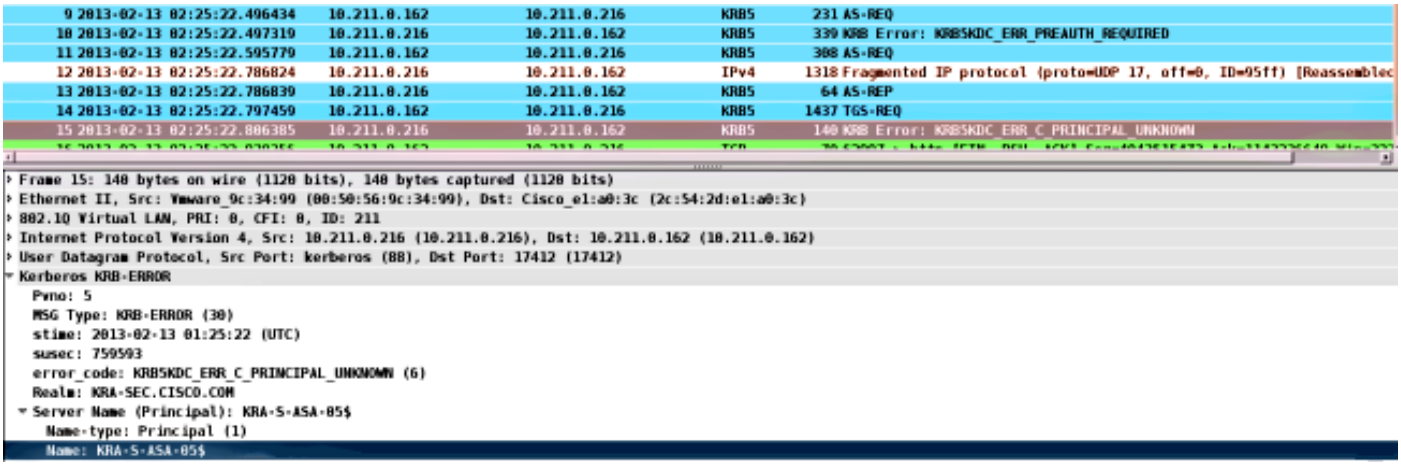


Verifique se o SPN está registrado somente para uma conta (script do artigo anterior). Quando você recebe esse erro, **KRB_AP_ERR_MODIFIED**, isso geralmente significa que o **SPN** não está

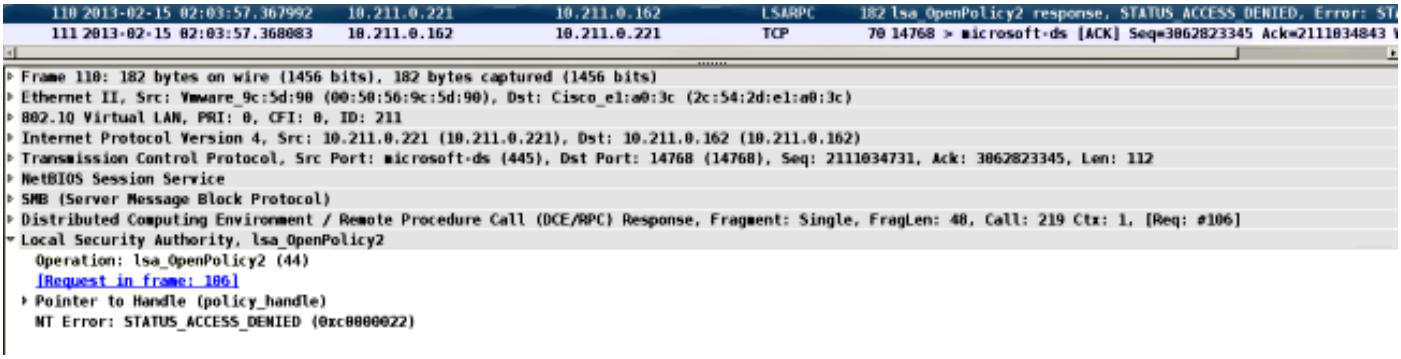
registrado para a conta correta. Ele deve ser registrado para a conta usada para executar o aplicativo (pool de aplicativos no IIS).



Quando você recebe este erro, **KRB_ERR_C_PRINCIPAL_UNKNOWN**, significa que não há usuário no DC (usuário WebVPN: **cisco**).



Você pode encontrar esse problema quando ingressar no domínio. O ASA recebe **AS-REP**, mas falha no nível **LSA** com o erro: **STATUS_ACCESS_DENIED**:



Para corrigir esse problema, você deve habilitar/desabilitar a pré-autenticação no DC desse usuário (**Administrador**).

Aqui estão alguns outros problemas que você pode encontrar:

- Pode haver problemas quando você ingressar no domínio. Se o servidor DC tiver vários adaptadores de Controlador de Interface de Rede (NIC) (vários endereços IP), certifique-se de que o ASA possa acessar todos eles para ingressar no domínio (escolhido aleatoriamente pelo cliente com base na resposta do Servidor de Nome de Domínio (DNS)).

- Não defina o **SPN** como o **HOST/dc.kra-sec.cisco.com** para a conta **do administrador**. É possível perder a conectividade com o DC devido a essa configuração.

- Depois que o ASA ingressar no domínio, será possível verificar se a conta do computador correta foi criada no DC (nome de host ASA). Verifique se o usuário tem as permissões corretas para adicionar contas de computador (neste exemplo, o **Administrador** tem as permissões corretas).

- Lembre-se da configuração correta do **Network Time Protocol (NTP)** no ASA. Por padrão, o DC aceita uma inclinação do relógio de cinco minutos. Esse temporizador pode ser alterado no DC.

- Verifique se a conectividade Kerberos para o pequeno pacote **UDP/88** é usada. Após o erro do DC, **KRB5KDC_ERR_RESPONSE_TOO_BIG**, o cliente muda para **TCP/88**. É possível forçar o cliente Windows a usar **TCP/88**, mas o **ASA usará o UDP por padrão**.

- CC: quando fizer alterações de política, lembre-se de **gpupdate /force**.

- ASA: teste a autenticação com o comando **test aaa**, mas lembre-se de que é apenas uma autenticação simples.

- Para solucionar problemas no site DC, é útil ativar as depurações de Kerberos: Como ativar o registro de eventos Kerberos.

IDs de bug da Cisco

Aqui está uma lista de IDs de bug relevantes da Cisco:

- ID de bug da Cisco CSCsi32224 - O ASA não muda para TCP após receber o código de erro Kerberos 52
- ID de bug da Cisco CSCtd92673 - Falha na autenticação Kerberos com pré-autenticação habilitada
- ID de bug da Cisco CSCuj19601 - ASA Webvpn KCD - tentando ingressar no AD somente após a reinicialização
- ID de bug da Cisco CSCuh32106 - O ASA KCD foi quebrado em 8.4.5 para frente

Informações Relacionadas

- **Sobre a delegação restrita de Kerberos**
- **Entendendo como o KCD funciona**
- **PIX/ASA: Exemplo de Configuração de Autenticação Kerberos e Grupos de Servidor de Autorização LDAP para Usuários de Clientes VPN via ASDM/CLI**

- Referência de comandos do Cisco ASA Series
- KDC_ERR_BADOPTION ao tentar delegação restrita
- Como forçar o Kerberos a usar TCP em vez de UDP no Windows
- Suporte Técnico e Documentação - Cisco Systems