# WebVPN SSO Integration with Kerberos Constrained Delegation Configuration Example

**Document ID: 116722**

Contributed by Michal Garcarz, Cisco TAC Engineer.
Nov 11, 2013

## Contents



## Introduction

This document describes how to configure and troubleshoot WebVPN Single Sign On (SSO) for applications that are protected by Kerberos.

## Prerequisites

### Requirements

Cisco recommends that you have basic knowledge of these topics:

- Cisco Adaptive Securit Appliance (ASA) CLI Configuration and Secure Socket Layer (SSL) VPN Configuration
- Kerberos Services

### Components Used

The information in this document is based on these software versions:

- Cisco ASA Software, Version 9.0 and Later
- Microsoft Windows 7 Client

- Microsoft Windows 2003 Server and Later

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.

# Background Information

Kerberos is a network authentication protocol that allows network entities to authenticate to each other in a secure manner. It uses a trusted third party, the Key Distribution Center (KDC), which grants tickets to the network entities. These tickets are used by the entities in order to verify and confirm the access to the requested service.

It is possible to configure WebVPN SSO for applications that are protected by Kerberos with the Cisco ASA feature called Kerberos Constrained Delegation (KCD). With this feature, the ASA can request Kerberos tickets on behalf of the WebVPN portal user, while it accesses applications protected by Kerberos.

When you access such applications through the WebVPN portal, you do not need to provide any credentials anymore; instead, the account that was used in order to log into the WebVPN portal is used.

Refer to the Understanding How KCD Works section of the ASA configuration guide for more information.

# Kerberos Interaction with the ASA

For WebVPN, the ASA must request tickets on behalf of the user (because the WebVPN portal user has access only to the portal, not the Kerberos service). For that, the ASA uses Kerberos extensions for Constrained Delegation. Here is the flow:

1. The ASA joins the domain and obtains a ticket (Ticket1) for a computer account with credentials configured on ASA (***kcd−server*** command). This ticket is used in the next steps for the access to Kerberos services.

2. The user clicks the WebVPN portal link for the Kerberos−protected application.

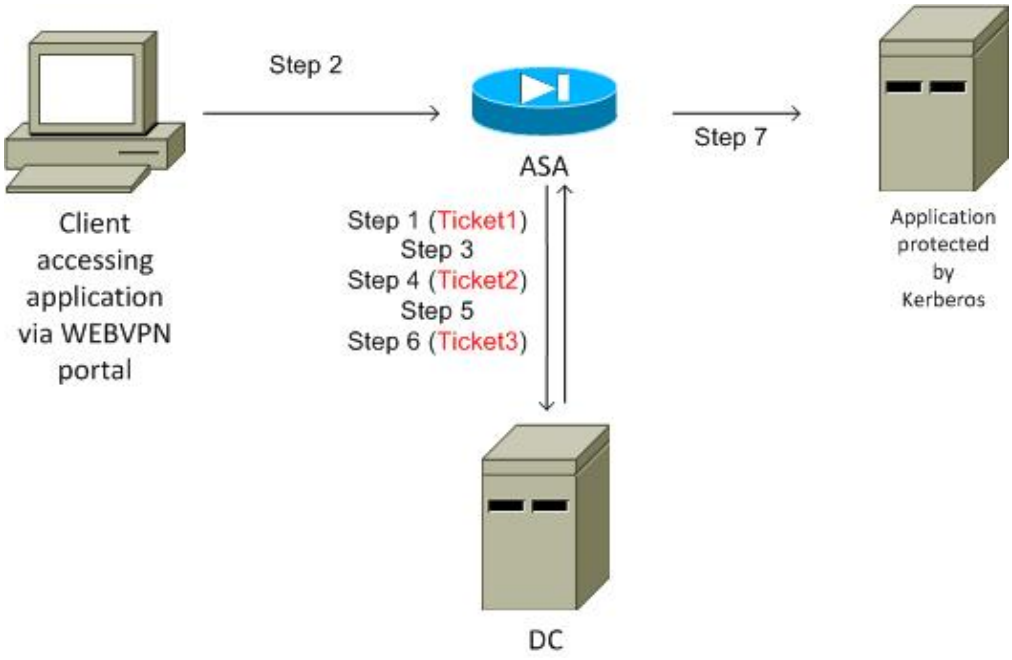
3. The ASA requests (***TGS−REQ***) a ticket for the computer account with its hostname as the principal. This request includes the ***PA−TGS−REQ*** field with ***PA−FOR−USER*** with the principal as the WebVPN portal username, which is ***cisco*** in this scenario. The ticket for Kerberos service from Step 1 is used for authentication (correct delegation).

4. As a response, the ASA receives an impersonated ticket (Ticket2) on behalf of the WebVPN user (***TGS_REP***) for the computer account. This ticket is used in order to request application tickets on behalf of this WebVPN user.

5. The ASA initiates another request (***TGS_REQ***) in order to obtain the ticket for the application (***HTTP/test.kra−sec.cisco.com***). This request again uses the ***PA−TGS−REQ*** field, this time ***without the PA−FOR−USER*** field, but with the impersonated ticket received in Step 4.

6. The response (***TGS_REQ***) with the impersonated ticket (Ticket3) for the application is returned.

7. This ticket is used transparently by the ASA in order to access the protected service, and the WebVPN user does not need to enter any credentials. For the HTTP application, the Simple and Protected GSS−API Negotiation (SPNEGO) mechanism is used in order to negotiate the authentication method, and the correct ticket is passed by the ASA.




# Configure

## Topology

***Domain***: kra−sec.cisco.com (10.211.0.221 or 10.211.0.216)

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

***Domain Controller (DC)***: dc.kra−sec.cisco.com (10.211.0.221 or 10.211.0.216) − Windows2008

***ASA***: 10.211.0.162

***WebVPN username/password***: cisco/cisco

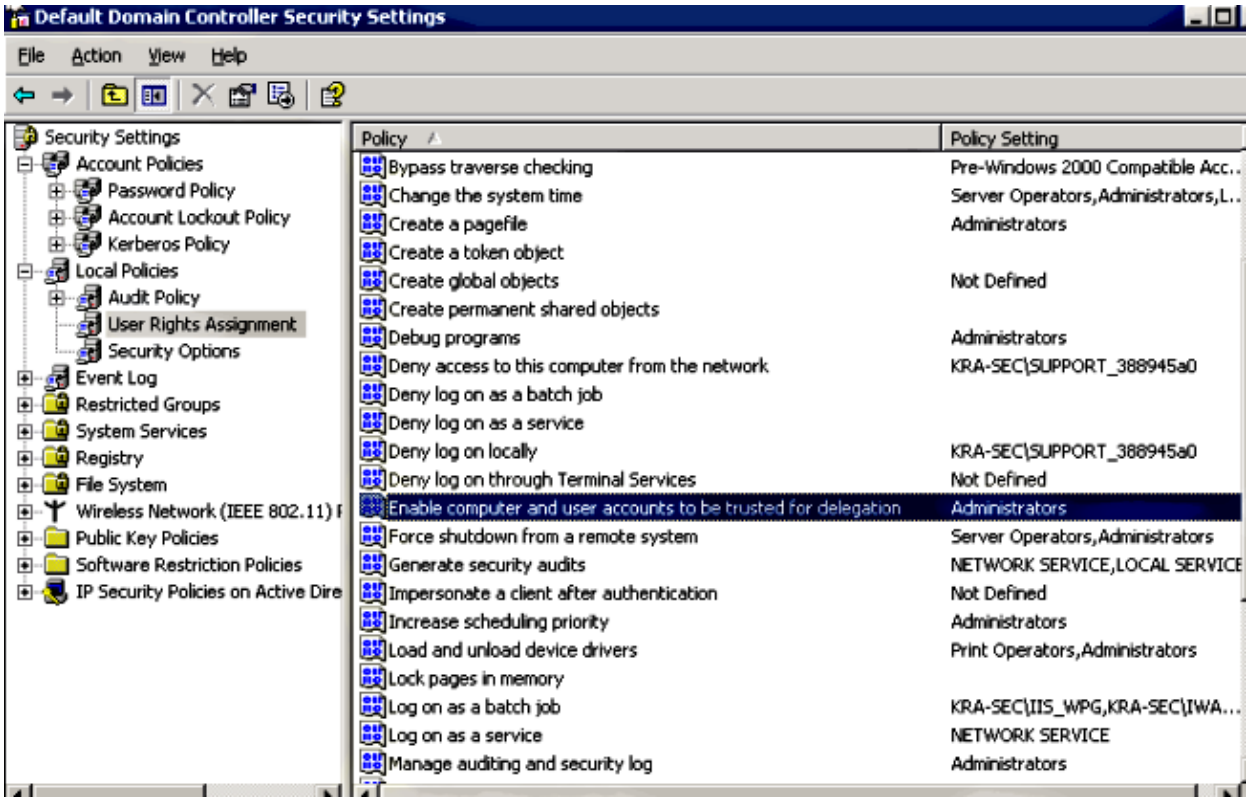
***Attached file***: asa−join.pcap (successful join to the domain)

***Attached file***: asa−kerberos−bad.pcap (request for service)

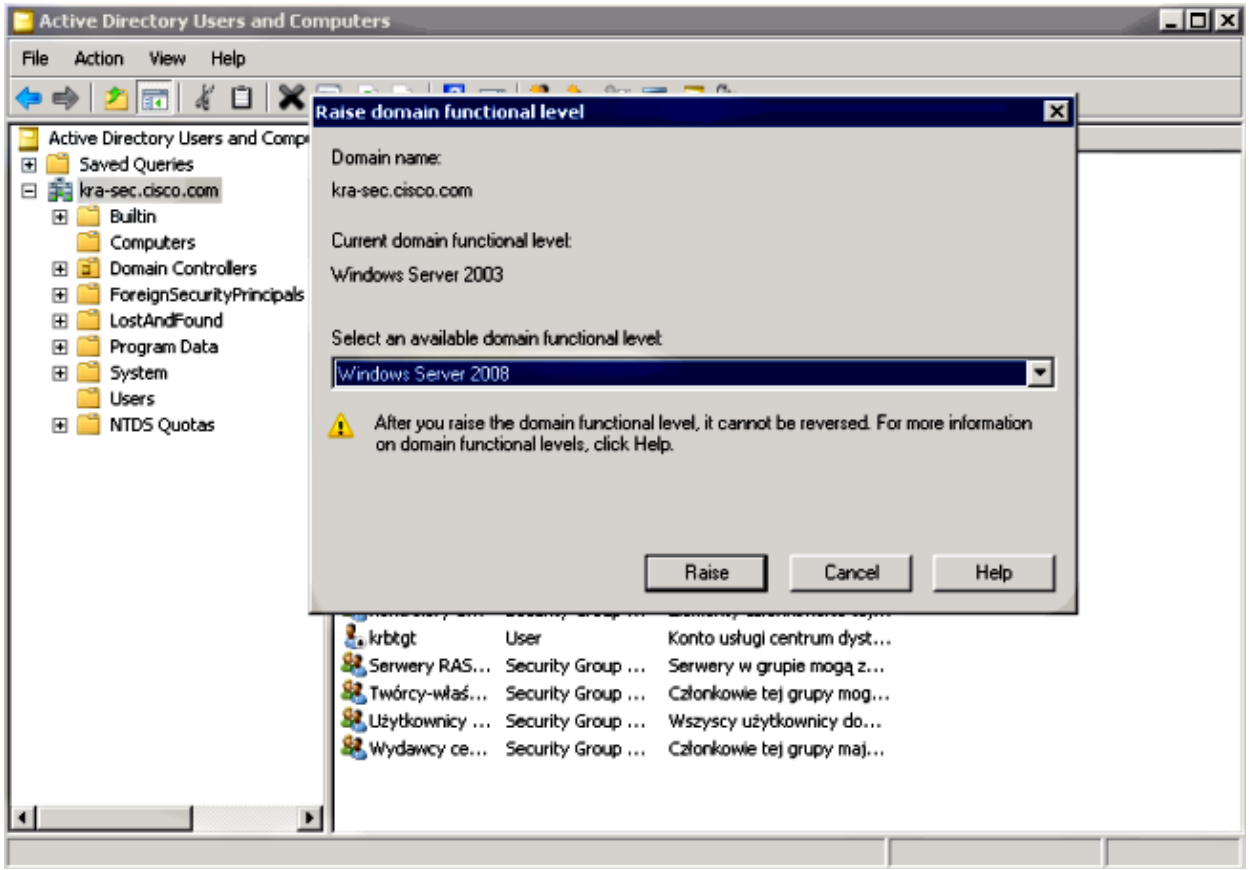
## Domain Controller and Application Configuration

### Domain Settings

It is assumed that there is already a functional IIS7 application protected by Kerberos (if not, read the Prerequisites section). You must check the settings for the delegations of the users:




Ensure that the functional domain level is raised to Windows Server 2003 (at least). The default is Windows Server 2000:



### Set the Service Principal Name (SPN)

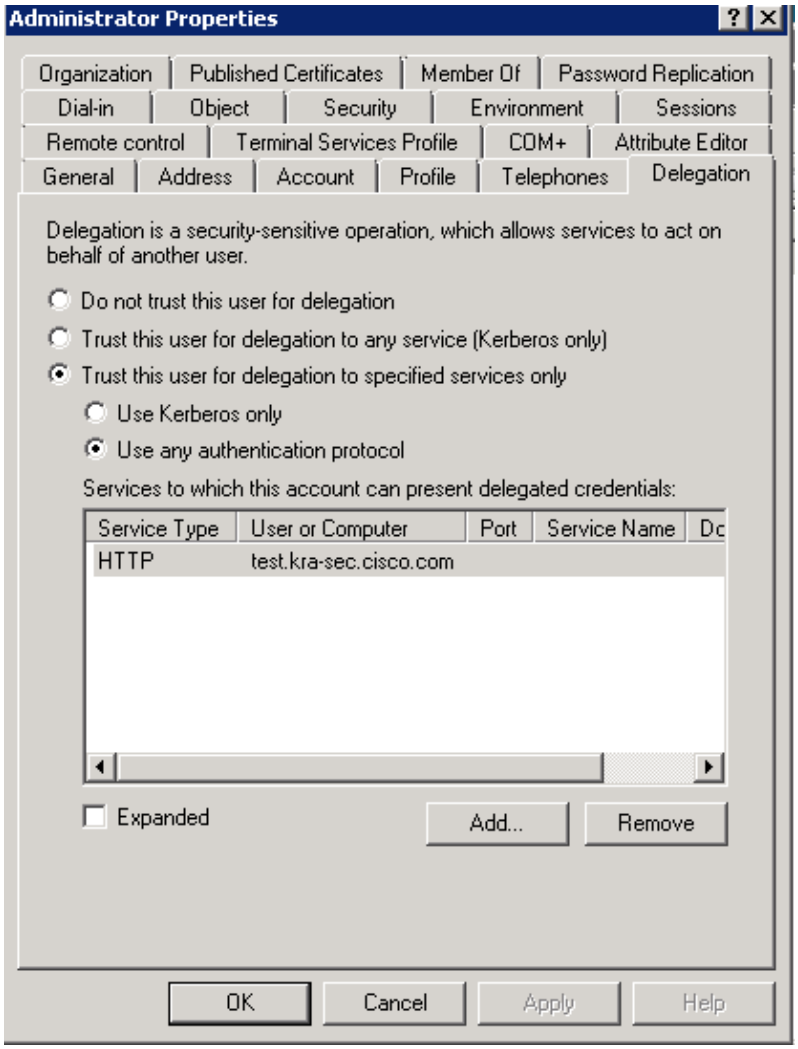
You must configure any account on the AD with the correct delegation. An Administrator account is used. When the ASA uses that account, it is able to request a ticket on behalf of another user (Constrained Delegation) for the specific service (HTTP application). In order for this to occur, the correct delegation must be created for the application/service.

In order to make this delegation via the CLI with the ***setspn.exe***, which is a part of the Windows Server 2003 Service Pack 1 Support Tools , enter this command:

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

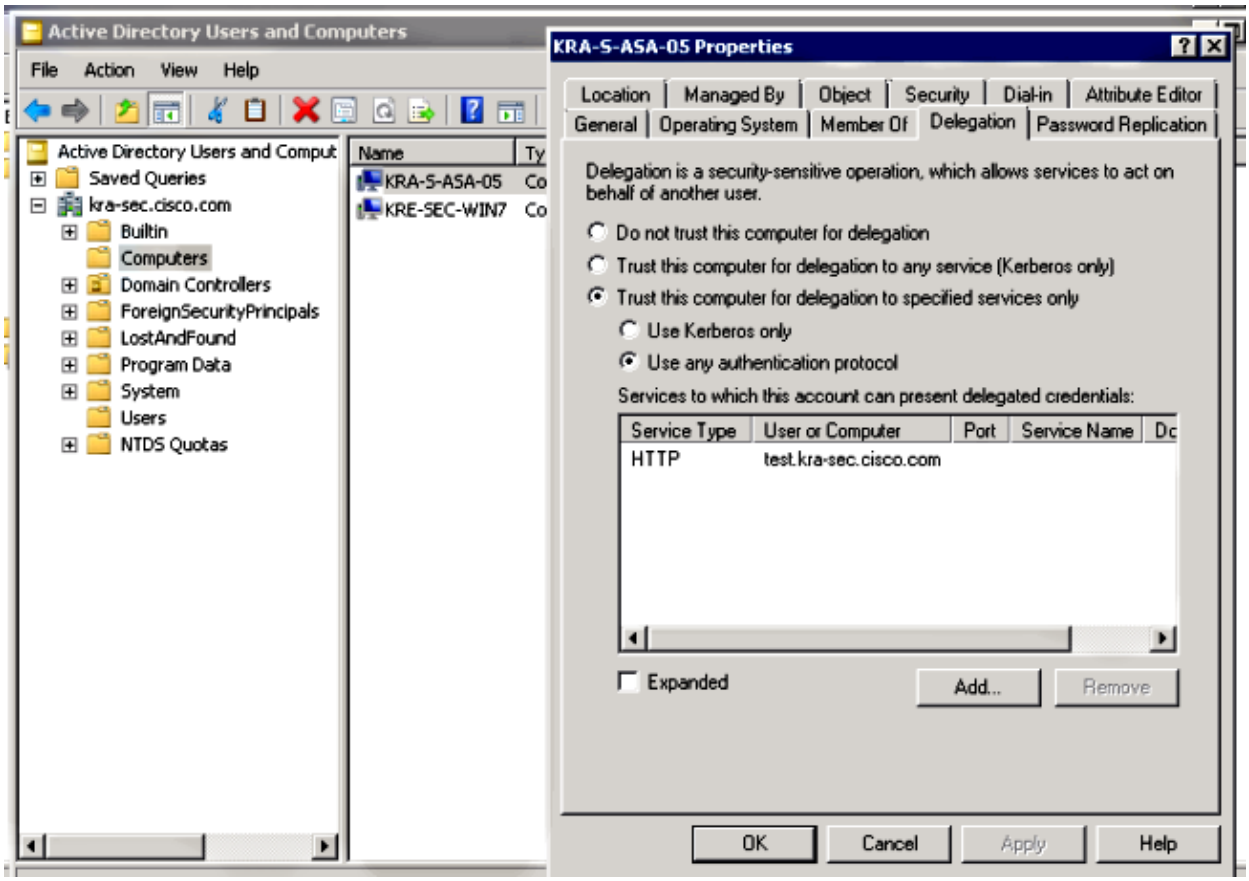
This indicates that the ***Administrator*** username is the trusted account for the delegation of the HTTP service at ***test.kra−sec.cisco.com***.

The ***SPN*** command is also necessary in order to activate the ***Delegation*** tab for that user. Once you enter the command, the Delegation tab for the Administrator appears. It is important to enable "Use any authentication protocol," because "Use Kerberos only" does not support the Constrained Delegation extension.




On the ***General*** tab, it is also possible to disable the Kerberos pre−authentication. However, this is not advised, because this feature is used in order to protect the DC against replay attacks. The ASA can work with pre−authentication correctly.

This procedure also applies with delegation for the computer account (the ASA is brought into the domain as a computer in order to establish a "trust" relationship):




## Configuration on the 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
```

# Verify

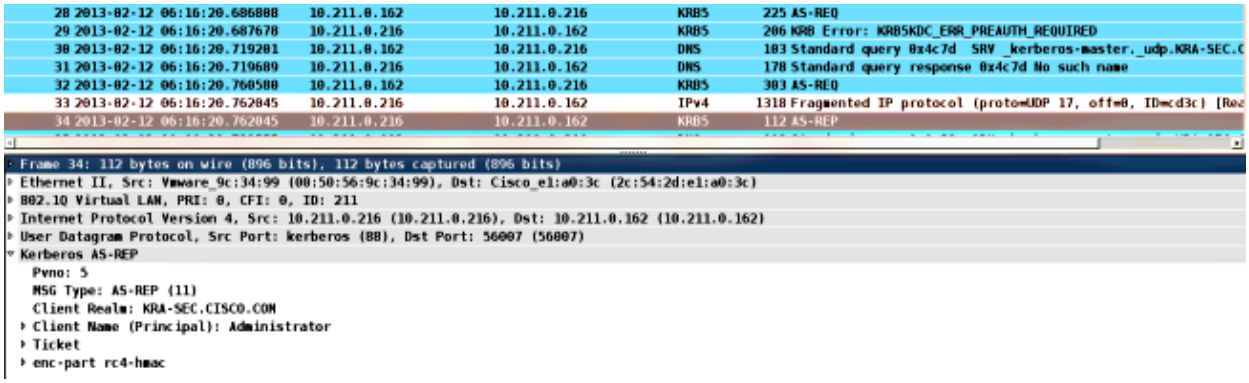
## The ASA Joins the Domain

After the ***kcd-server*** command is used, the ASA tries to join the domain:

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

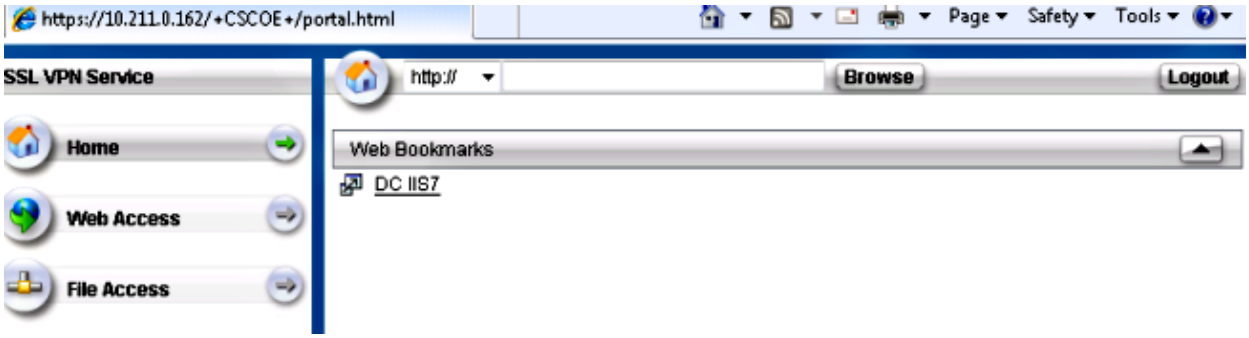
```
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4
Kerberos: Encryption type des3-cbc-sha1
********** END: KERBEROS PACKET DECODE ************
In kerberos_recv_msg
In KCD_self_tkt_process_response
********** START: KERBEROS PACKET DECODE ************
Kerberos: Message type 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
```

The ASA is able to successfully join the domain. After the correct authentication, the ASA receives a ticket for the principal: Administrator in ***AS_REP*** packet (Ticket1 described in Step1).

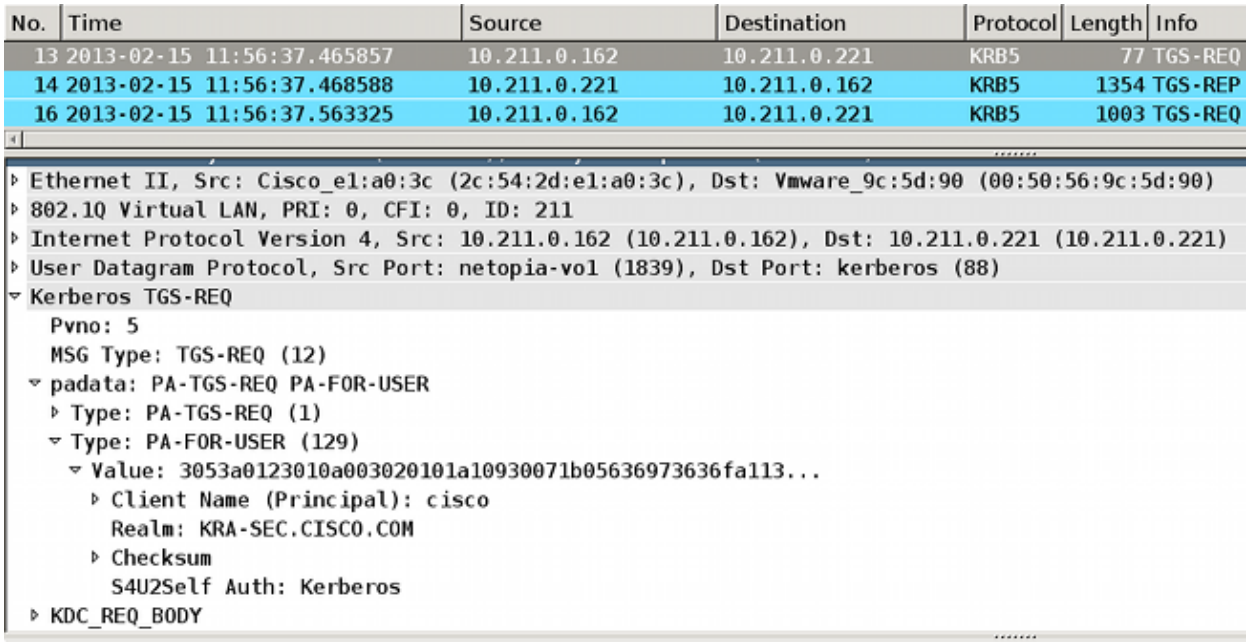



## Request for the Service

The user clicks WebVPN link:

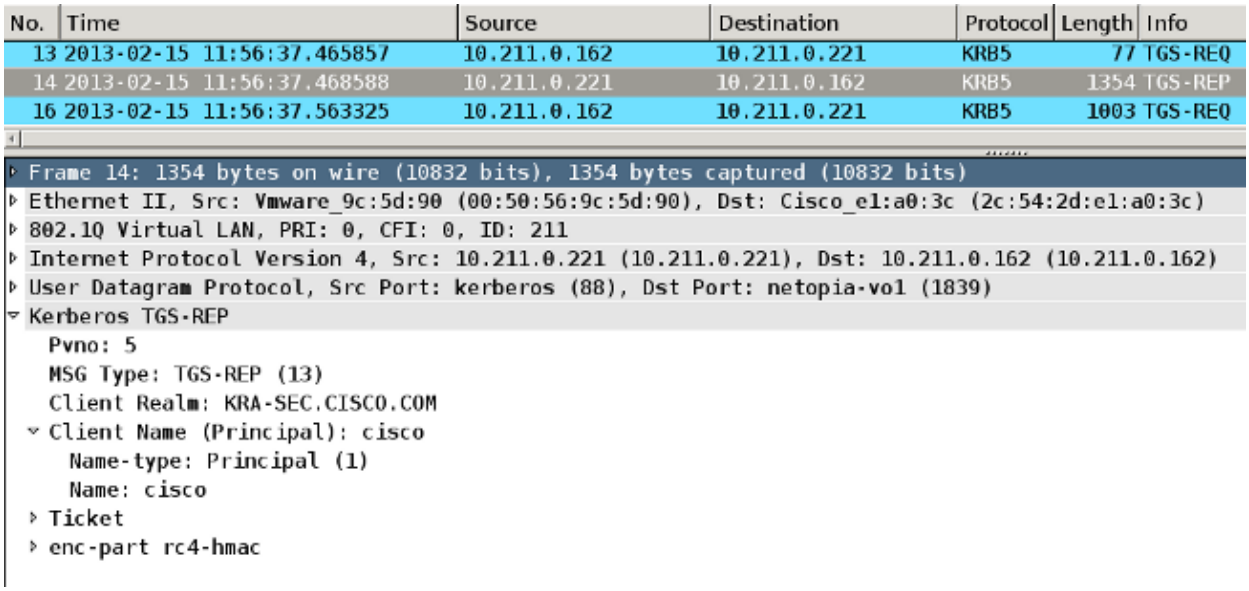



The ASA sends the ***TGS_REQ*** for an impersonated ticket with the ticket that is received in the ***AS_REP*** packet:




***Note***: The ***PA−FOR−USER*** value is ***cisco*** (WebVPN user). ***PA−TGS−REQ*** contains the ticket received for the Kerberos service request (the ASA hostname is the principal).

The ASA gets a correct response with the impersonated ticket for user ***cisco*** (Ticket2 described in Step 4):




Here is the request for the ticket for the HTTP service (some debugs are omitted for clarity):

```
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
```

The ASA receives the correct impersonated ticket for the HTTP service (Ticket3 described in Step 6).

Both tickets can be verified. The first one is the impersonated ticket for the user ***cisco***, which is used in order to request and receive the second ticket for the HTTP service that is accessed:

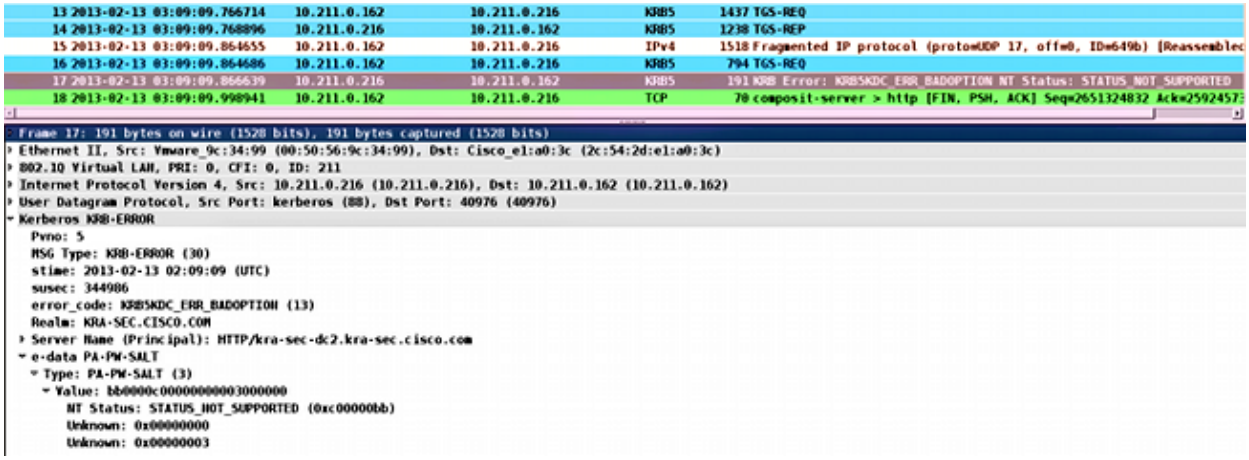
```
KRA−S−ASA−05(config)# show aaa kerberos
Default Principal: cisco@KRA−SEC.CISCO.COM
Valid Starting       Expires              Service Principal
19:38:10 CEST Oct 2 2013 05:37:33 CEST Oct 3 2013 KRA−S−ASA−05@KRA−SEC.CISCO.COM

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
```

This HTTP ticket (Ticket3) is used for HTTP access (with SPNEGO), and the user does not need to provide any credentials.

# Troubleshoot

Sometimes you might encounter a problem of incorrect delegation. For example, the ASA uses a ticket in order to request the service ***HTTP/test.kra−sec.cisco.com*** (Step 5), but the response is ***KRB−ERROR*** with ***ERR_BADOPTION***:




This is a typical problem encountered when the delegation is not configured correctly. The ASA reports that ***"KDC can't fulfill requested option"***:

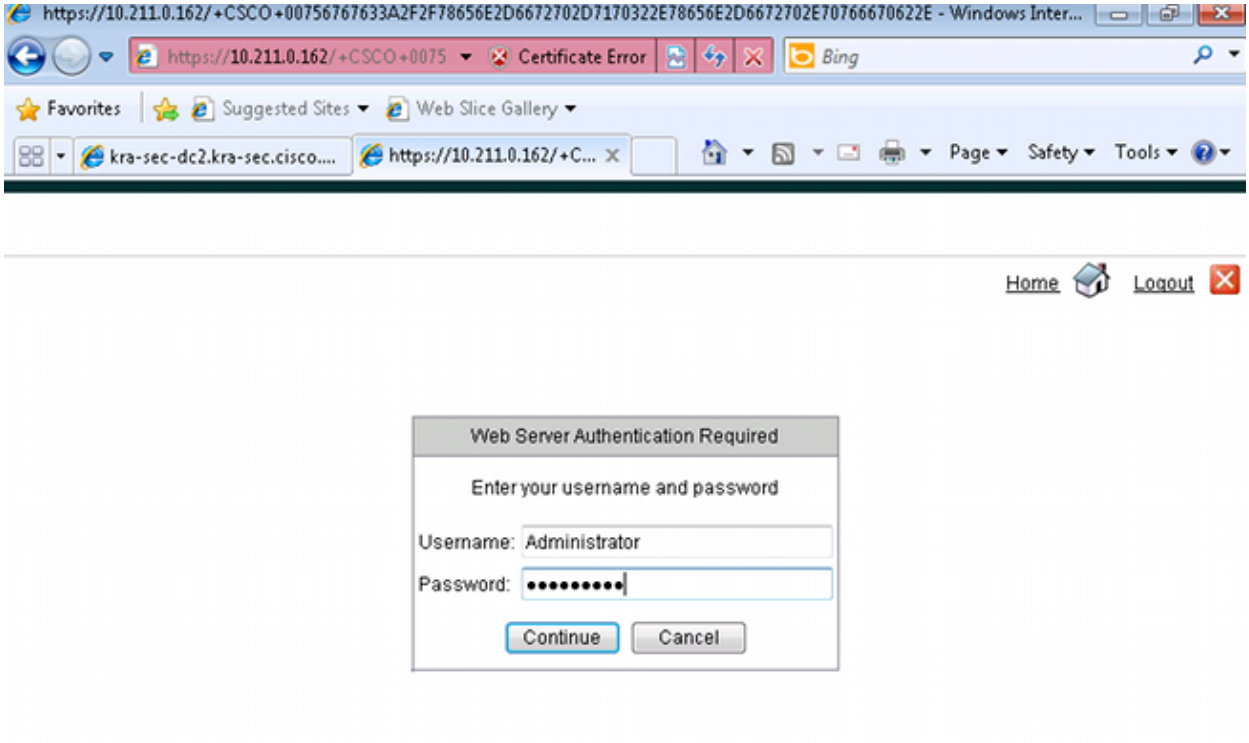
```
KRA−S−ASA−05# ucte_krb_get_auth_cred(): ctx = 0xcc4b5390,
WebVPN_session = 0xc919a260, protocol = 1
find_spn_in_url(): URL − /
build_host_spn(): host − test.kra−sec.cisco.com
build_host_spn(): SPN − HTTP/test.kra−sec.cisco.com
KCD_unicorn_get_cred(): Attempting to retrieve required KCD tickets.
In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

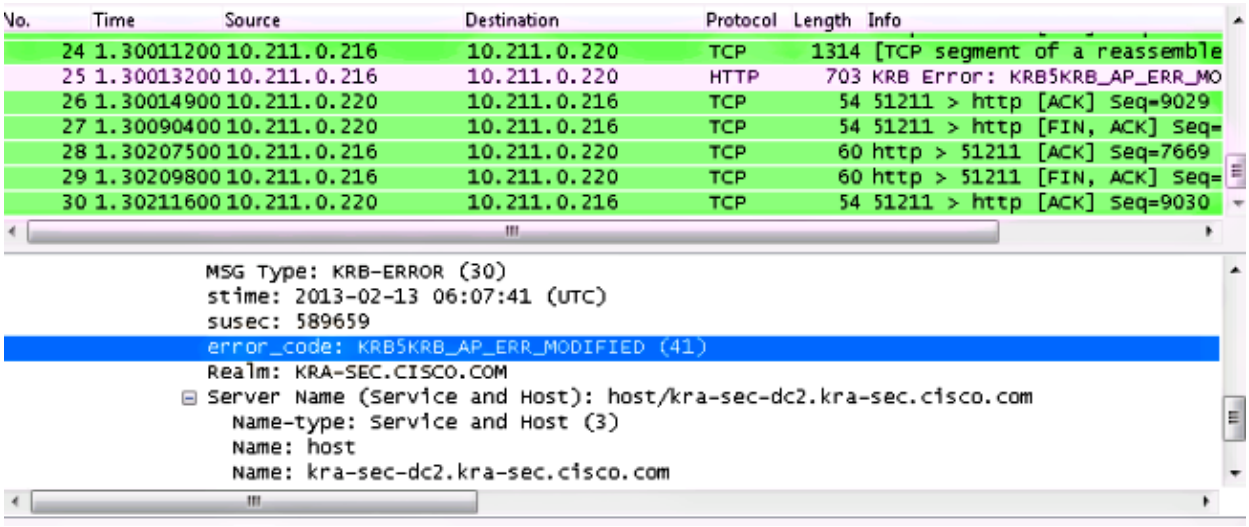
```
Kerberos: Realm KRA-SEC.CISCO.COM
Kerberos: Server Name HTTP
********** END: KERBEROS PACKET DECODE ************
Kerberos library reports: "KDC can't fulfill requested option"
KCD_unicorn_callback(): called with status: -3.
KCD callback called with AAA error -3.
In kerberos_close_connection
remove_req 0xcc09ad18 session 0x5 id 2
free_kip 0xcc09ad18
kerberos: work queue empty
```

This is basically the same problem that is described in the captures − the failure is ***at TGS_REQ with BAD_OPTION***.

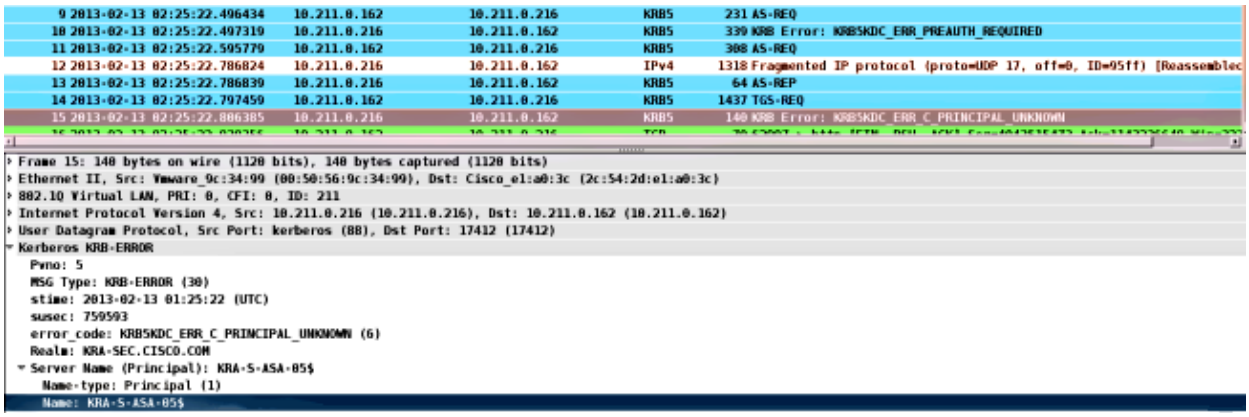
If the response is ***Success***, then the ASA receives a ticket for the ***HTTP/test.kra−sec.cisco.com*** service, which is used for ***SPNEGO*** negotiation. However, because of the failure, the ***NT LAN Manager (NTLM)*** is negotiated, and the user must provide credentials:



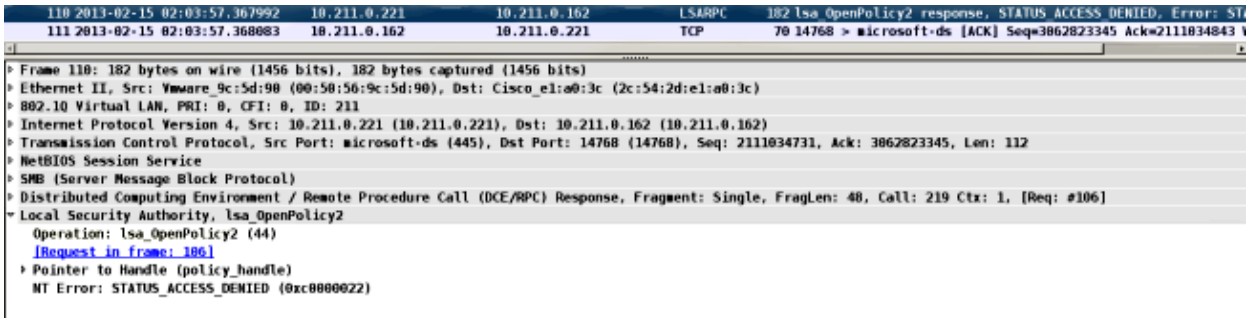

Make sure that the SPN is registered for one account only (script from previous article). When you receive this error, ***KRB_AP_ERR_MODIFIED***, it usually means that the ***SPN*** is not registered for the correct account. It should be registered for the account that is used in order to run the application (application pool on IIS).




When you receive this error, ***KRB_ERR_C_PRINCIPAL_UNKNOWN***, it means that there is no user on the DC (WebVPN user: ***cisco***).




You might encounter this problem when you join the domain. The ASA receives ***AS−REP***, but fails on the ***LSA*** level with the error: ***STATUS_ACCESS_DENIED***:




In order to fix this problem, you must enable/disable pre−authentication on the DC for that user (***Administrator***).

Here are some other problems you might encounter:

- There might be problems when you join the domain. If the DC server has multiple Network Interface Controller (NIC) adapters (multiple IP addresses), make sure that the ASA can access all of them in order to join the domain (chosen randomly by the client based on the Domain Name Server (DNS) response).

- Do not set ***SPN*** as the ***HOST/dc.kra−sec.cisco.com*** for the ***Administrator*** account. It is possible to lose connectivity to the DC because of that setting.

- After the ASA joins the domain, it is possible to verify that the correct computer account is created on the DC (ASA hostname). Make sure that the user has the correct permissions in order to add computer accounts (in this example, the ***Administrator*** has the correct permissions).

- Remember the correct ***Network Time Protocol (NTP)*** configuration on the ASA. By default, the DC accepts a five minute clock skew. That timer can be changed on the DC.

- Verify Kerberos connectivity for the small packet ***UDP/88*** is used. After the error from the DC, ***KRB5KDC_ERR_RESPONSE_TOO_BIG***, the client switches to ***TCP/88***. It is possible to force the Windows client to use ***TCP/88***, but ***ASA will use UDP by default***.

- DC: when you make policy changes, remember ***gpupdate /force***.

- ASA: test authentication with the ***test aaa*** command, but remember that it is only a simple authentication.

- In order to troubleshoot on the DC site, it is useful to enable Kerberos debugs: How to enable Kerberos event logging.

# Cisco Bug IDs

Here is a list of relevant Cisco bug IDs:

- Cisco bug ID CSCsi32224 − ASA does not switch to TCP after receiving Kerberos error code 52
- Cisco bug ID CSCtd92673 − Kerberos authentication fails with pre−auth enabled
- Cisco bug ID CSCuj19601 − ASA Webvpn KCD − trying to join AD only after reboot
- Cisco bug ID CSCuh32106 − ASA KCD is broken in 8.4.5 onwards

# Related Information

- ***About Kerberos constrained delegation***
- ***Understanding How KCD Works***
- ***PIX/ASA : Kerberos Authentication and LDAP Authorization Server Groups for VPN Client Users via ASDM/CLI Configuration Example***
- ***Cisco ASA Series Command Reference***
- ***KDC_ERR_BADOPTION when attempting constrained delegation***
- ***How to force Kerberos to use TCP instead of UDP in Windows***
- ***Technical Support & Documentation − Cisco Systems***

---

Updated: Nov 11, 2013 Document ID: 116722