Konfigurationsbeispiel für die WebVPN SSO-Integration mit Kerberos Constrained Delegation (einschränkte Delegation)

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie WebVPN Single Sign On (SSO) für Anwendungen konfiguriert und Fehler bei diesen behoben werden, die durch Kerberos geschützt sind.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- CLI-Konfiguration der Cisco Adaptive Security Appliance (ASA) und SSL-VPN-Konfiguration (Secure Socket Layer)

- Kerberos-Services

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Cisco ASA Software, Version 9.0 und höher
- Microsoft Windows 7-Client
- Microsoft Windows 2003 Server und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Kerberos ist ein Netzwerkauthentifizierungsprotokoll, das es Netzwerkentitäten ermöglicht, sich sicher zu authentifizieren. Dabei wird ein vertrauenswürdiger Drittanbieter, das Key Distribution Center (KDC), verwendet, der den Netzwerkentitäten Tickets gewährt. Diese Tickets werden von den Entitäten verwendet, um den Zugriff auf den angeforderten Service zu überprüfen und zu bestätigen.

Es ist möglich, WebVPN SSO für Anwendungen zu konfigurieren, die durch Kerberos mit der Cisco ASA-Funktion, der Kerberos Constrained Delegation (KCD), geschützt sind. Mit dieser Funktion kann die ASA Kerberos-Tickets im Namen des WebVPN-Portalbenutzers anfordern, während sie auf durch Kerberos geschützte Anwendungen zugreift.

Wenn Sie über das WebVPN-Portal auf solche Anwendungen zugreifen, müssen Sie keine Anmeldeinformationen mehr angeben. Stattdessen wird das Konto verwendet, das für die Anmeldung beim WebVPN-Portal verwendet wurde.

Weitere Informationen finden Sie im Abschnitt Funktionsweise von KCD im ASA-Konfigurationsleitfaden.

Kerberos-Interaktion mit der ASA

Für WebVPN muss die ASA Tickets im Namen des Benutzers anfordern (da der Benutzer des WebVPN-Portals nur Zugriff auf das Portal hat, nicht auf den Kerberos-Service). Dazu verwendet die ASA Kerberos-Erweiterungen für eingeschränkte Delegation. Hier ist der Ablauf:

1. Die ASA tritt der Domäne bei und erhält ein Ticket (Ticket1) für ein Computerkonto mit auf ASA konfigurierten Anmeldeinformationen (**kcd-server-**Befehl). Dieses Ticket wird in den nächsten Schritten für den Zugang zu Kerberos-Services verwendet.

2. Der Benutzer klickt auf den WebVPN-Portallink für die Anwendung mit Kerberos-Schutz.

3. Die ASA fordert (**TGS-REQ**) ein Ticket für das Computerkonto mit dem Hostnamen als

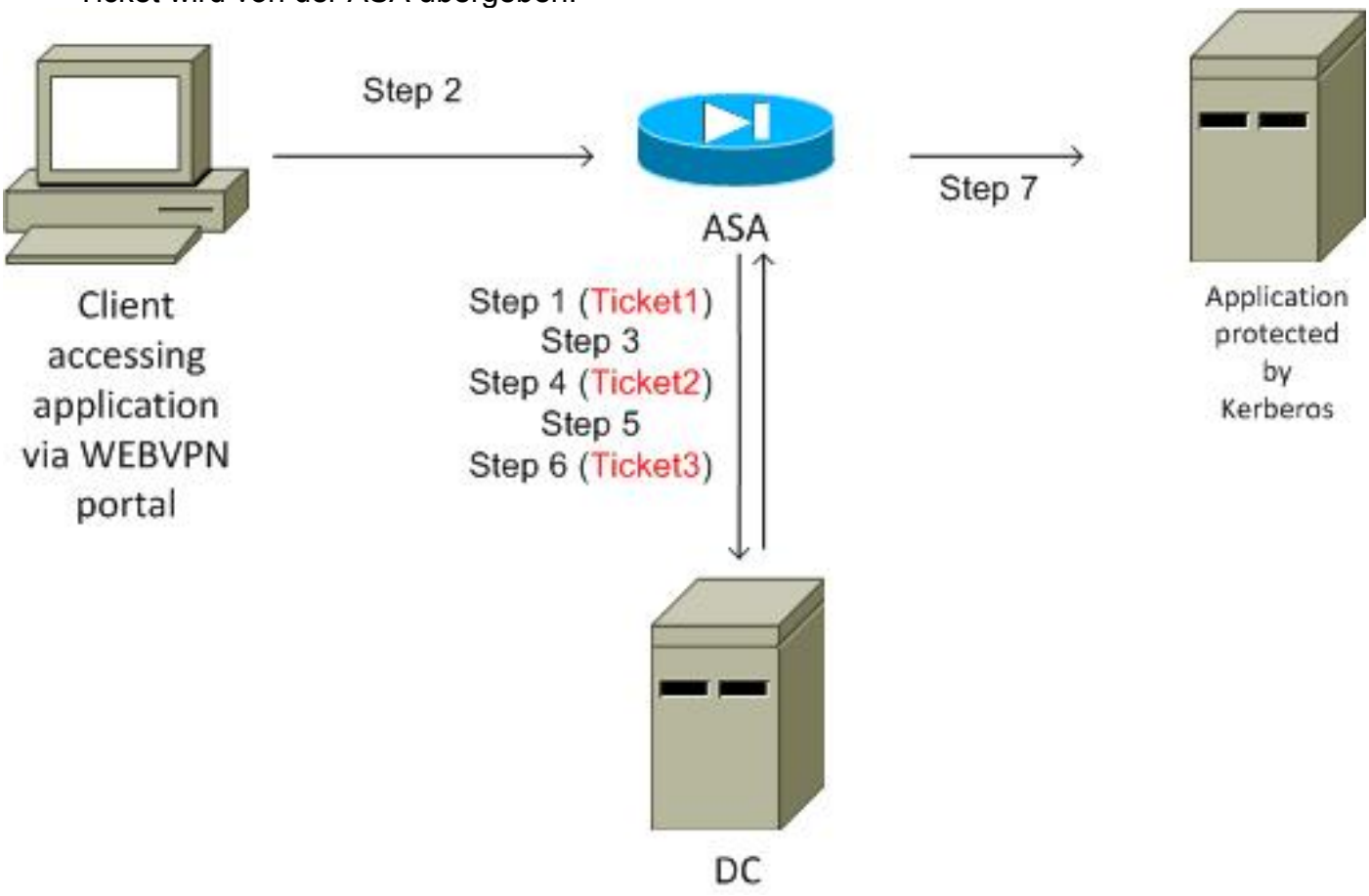
Principal an. Diese Anforderung umfasst das Feld **PA-TGS-REQ** mit **PA-FOR-USER** mit dem Principal als Benutzernamen für das WebVPN-Portal, der in diesem Szenario **cisco** ist. Das Ticket für den Kerberos-Service aus Schritt 1 dient der Authentifizierung (korrekte Delegation).

4. Als Antwort erhält die ASA ein Identitätsticket (Ticket2) für den WebVPN-Benutzer (**TGS_REP**) für das Computerkonto. Dieses Ticket wird zum Anfordern von Anwendungstickets für diesen WebVPN-Benutzer verwendet.

5. Die ASA initiiert eine weitere Anfrage (**TGS_REQ**), um das Ticket für die Anwendung zu erhalten (**HTTP/test.kra-sec.cisco.com**). Diese Anforderung verwendet erneut das Feld **PA-TGS-REQ**, dieses Mal **ohne das** Feld **PA-FOR-USER**, aber mit dem in Schritt 4 erhaltenen imitierten Ticket.

6. Die Antwort (**TGS_REQ**) mit dem imitierten Ticket (Ticket3) für die Anwendung wird zurückgegeben.

7. Dieses Ticket wird von der ASA transparent für den Zugriff auf den geschützten Dienst verwendet, und der WebVPN-Benutzer muss keine Anmeldeinformationen eingeben. Für die HTTP-Anwendung wird der SPNEGO-Mechanismus (Simple and Protected GSS-API Negotiation) verwendet, um die Authentifizierungsmethode auszuhandeln, und das richtige Ticket wird von der ASA übergeben.



Konfigurieren

Topologie

Domäne: kra-sec.cisco.com (10.211.0.221 oder 10.211.0.216)

Anwendung Internetinformationsdienste (IIS) 7: test.kra-sec.cisco.com (10.211.0.223)

Domänencontroller (RZ): dc.kra-sec.cisco.com (10.211.0.221 oder 10.211.0.216) - Windows2008

ASA: 10.211.0.162

WebVPN-Benutzername/Kennwort: Cisco/Cisco

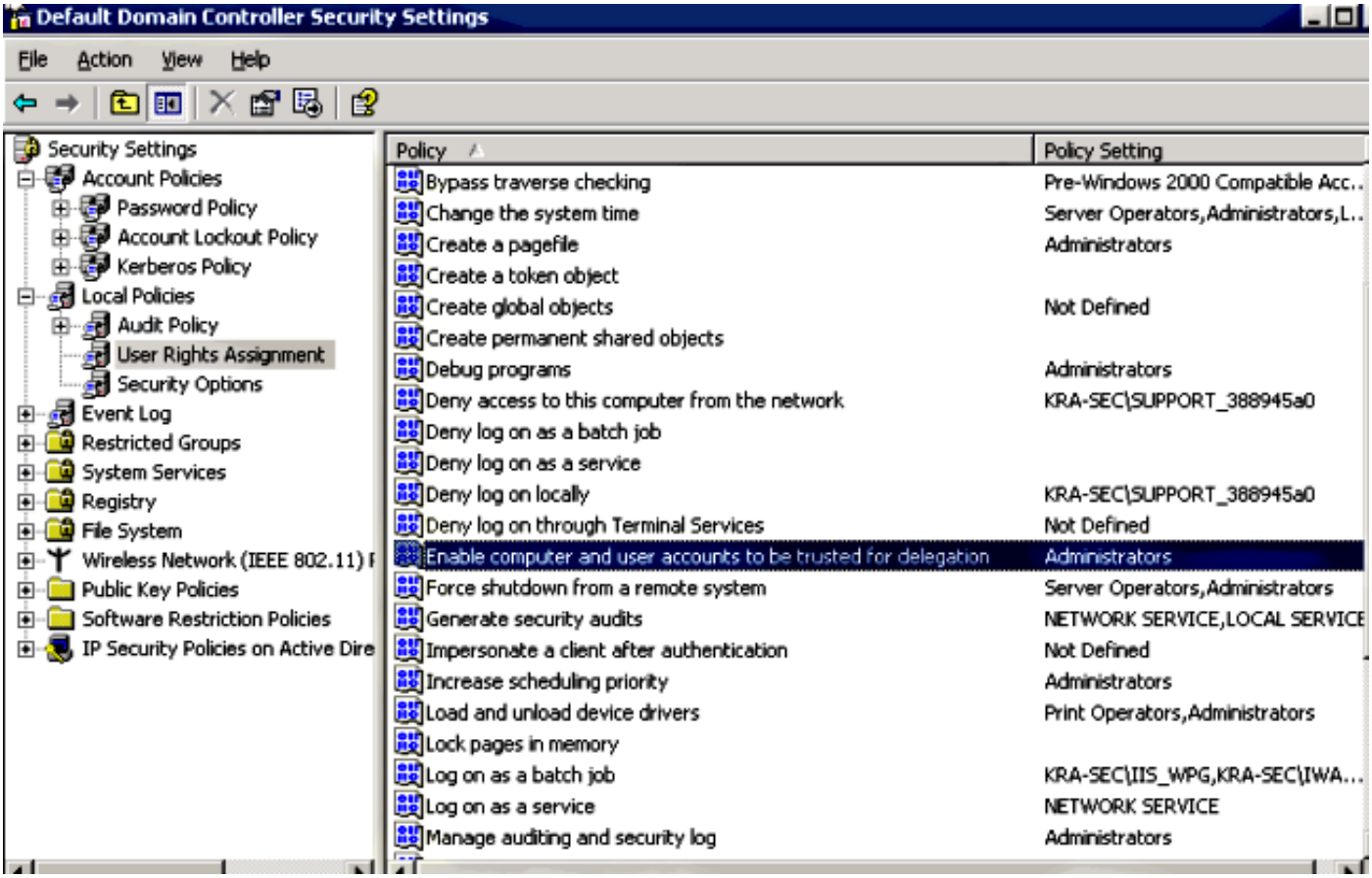
Angehängte Datei: asa-join.pcap (erfolgreicher Beitritt zur Domäne)

Angehängte Datei: asa-kerberos-bad.pcap (Service-Anfrage)

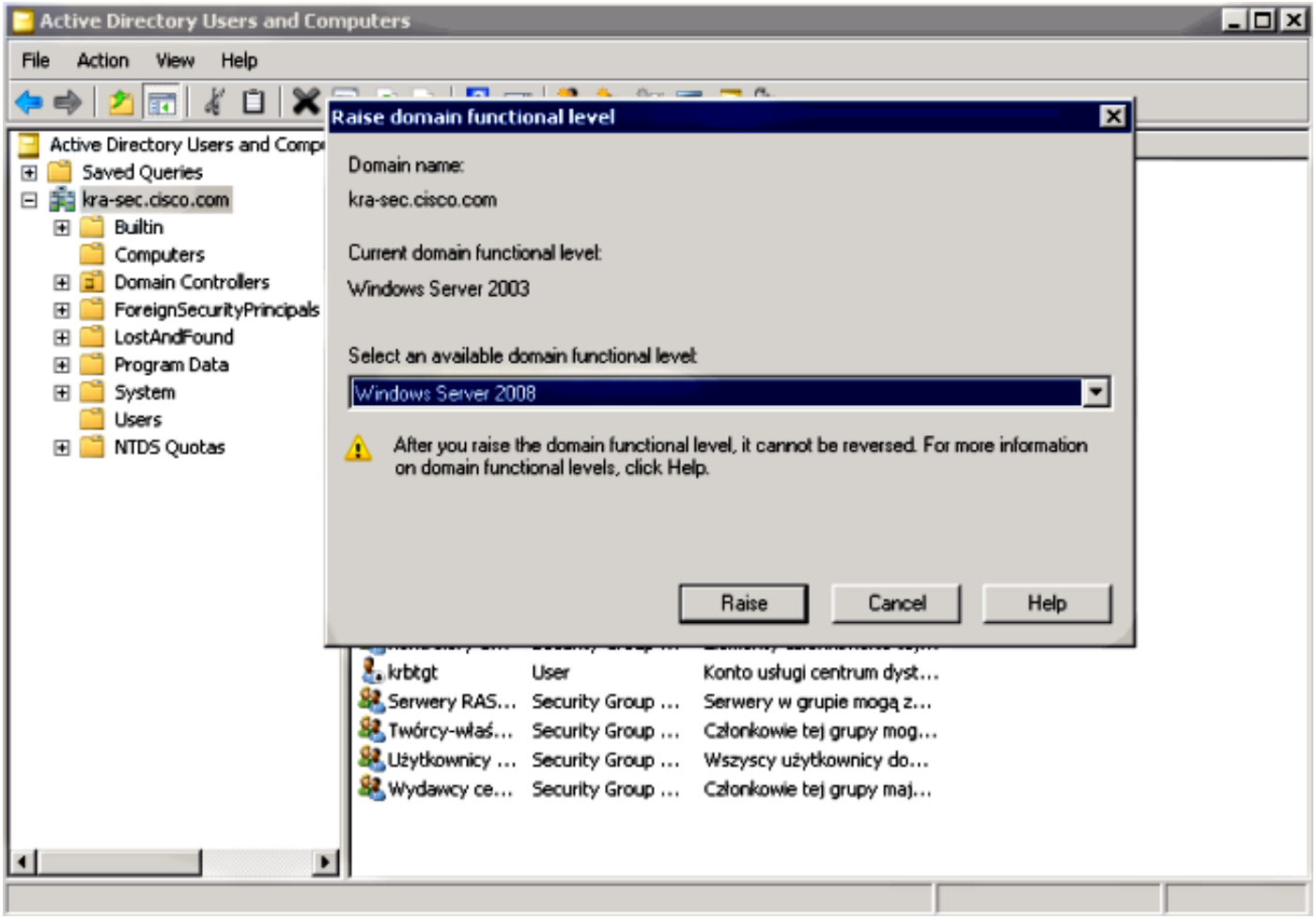
Domänencontroller und Anwendungskonfiguration

Domäneneinstellungen

Es wird davon ausgegangen, dass es bereits eine funktionale IIS7-Anwendung gibt, die durch Kerberos geschützt ist (falls nicht, lesen Sie den Abschnitt Erforderliche Komponenten). Sie müssen die Einstellungen für die Benutzerdelegationen überprüfen:



Stellen Sie sicher, dass die funktionale Domänenebene auf Windows Server 2003 (mindestens) erhöht wird. Der Standardwert ist "Windows Server 2000:



Festlegen des Dienstprinzipalnamens (SPN)

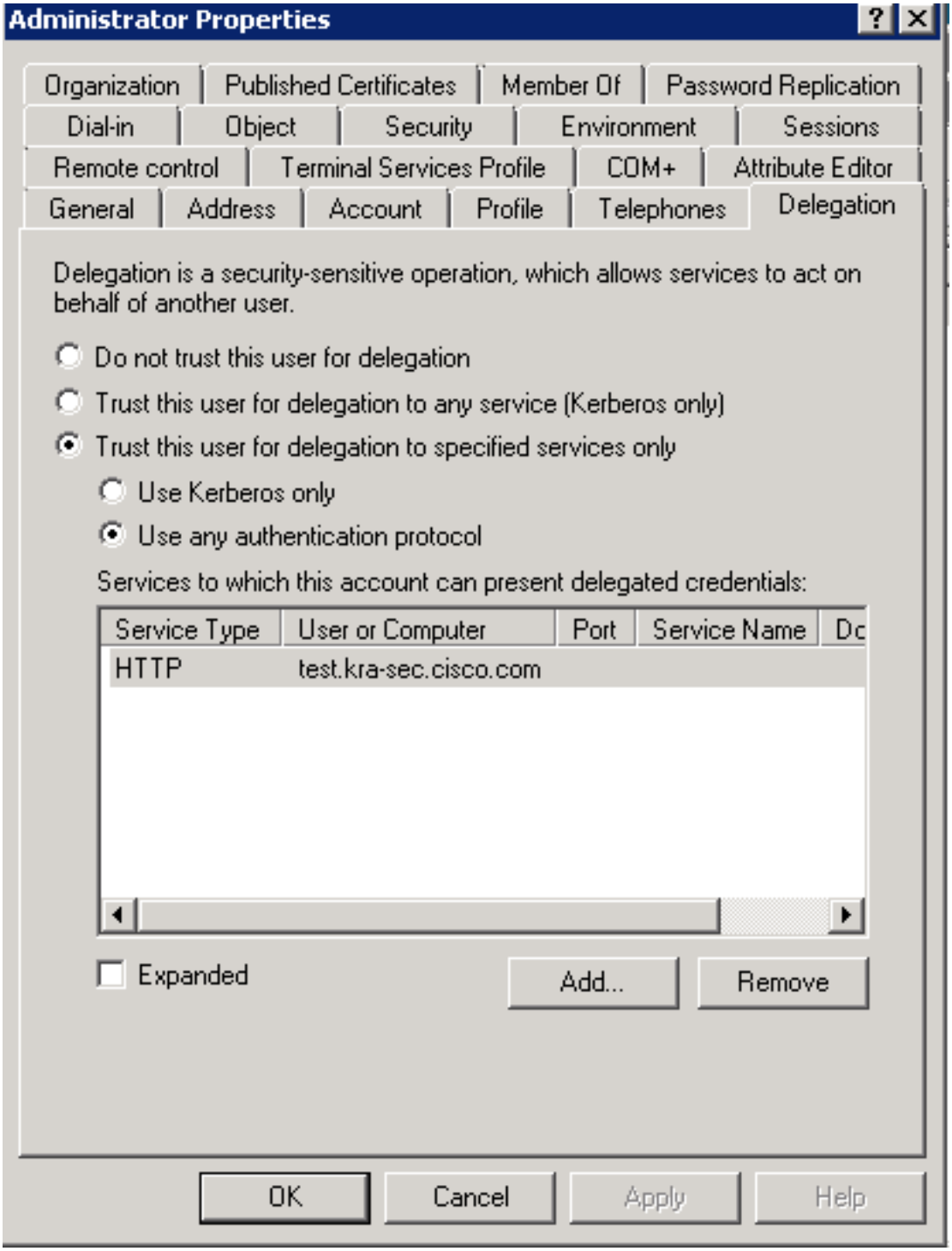
Sie müssen jedes Konto im AD mit der richtigen Delegation konfigurieren. Ein Administratorkonto wird verwendet. Wenn die ASA dieses Konto verwendet, kann sie ein Ticket für einen anderen Benutzer (Constrained Delegation) für den jeweiligen Dienst (HTTP-Anwendung) anfordern. Damit dies geschieht, muss die richtige Delegation für die Anwendung/den Dienst erstellt werden.

Um diese Delegierung über die CLI mit der **setspn.exe** durchzuführen, die Teil der Support-Tools für Windows Server 2003 Service Pack 1 ist, geben Sie den folgenden Befehl ein:

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

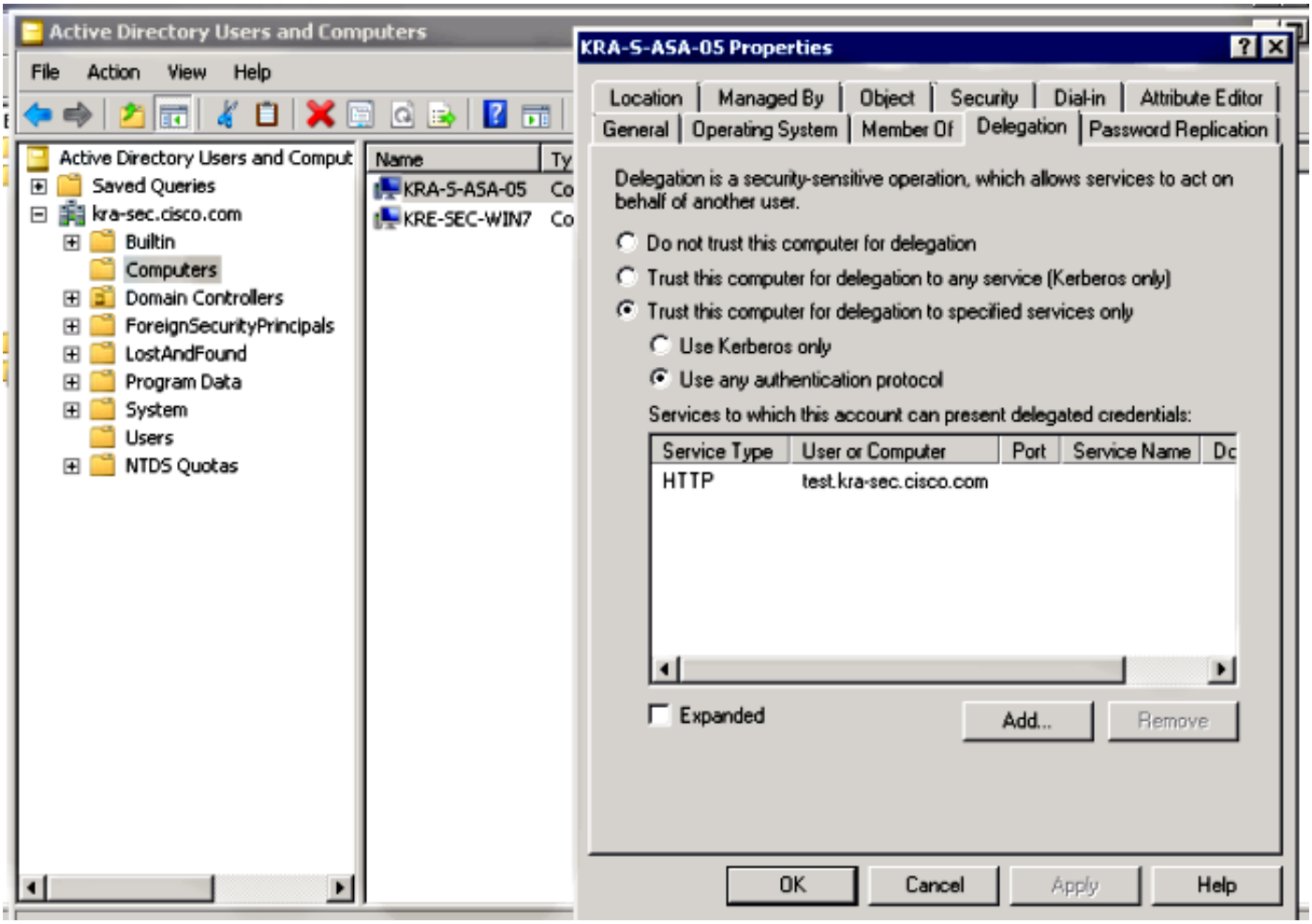
Dies weist darauf hin, dass der **Administrator-**Benutzername das vertrauenswürdige Konto für die Delegation des HTTP-Dienstes unter **test.kra-sec.cisco.com** ist.

Der **SPN-**Befehl ist ebenfalls erforderlich, um die **Delegation-**Registerkarte für diesen Benutzer zu aktivieren. Sobald Sie den Befehl eingegeben haben, wird die Registerkarte Delegation für den Administrator angezeigt. Es ist wichtig, "Use any authentication protocol" zu aktivieren, da "Use Kerberos only" die Erweiterung Constrained Delegation nicht unterstützt.



Auf der Registerkarte **Allgemein** ist es auch möglich, die Kerberos-Vorauthentifizierung zu deaktivieren. Dies wird jedoch nicht empfohlen, da diese Funktion verwendet wird, um das Rechenzentrum vor Wiederholungsangriffen zu schützen. Die ASA kann mit der Vorabauthentifizierung ordnungsgemäß arbeiten.

Dieses Verfahren gilt auch für die Übertragung des Computerkontos (die ASA wird als Computer in die Domäne integriert, um eine "Vertrauensbeziehung" herzustellen):



Konfiguration auf der 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
```

Überprüfen

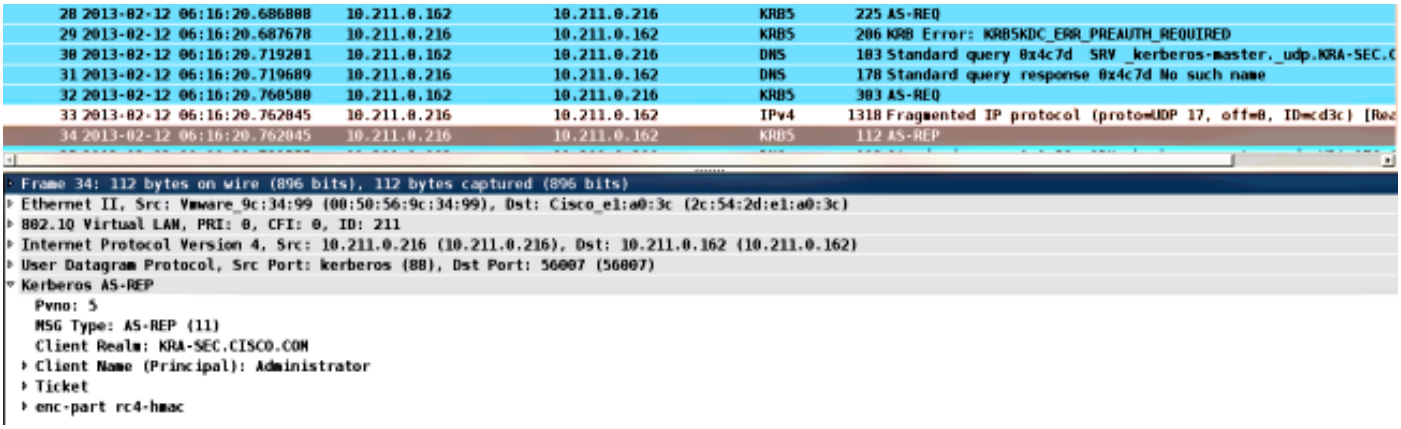
Die ASA tritt der Domäne bei

Nachdem der Befehl **kcd-server** verwendet wurde, versucht die ASA, der Domäne beizutreten:

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

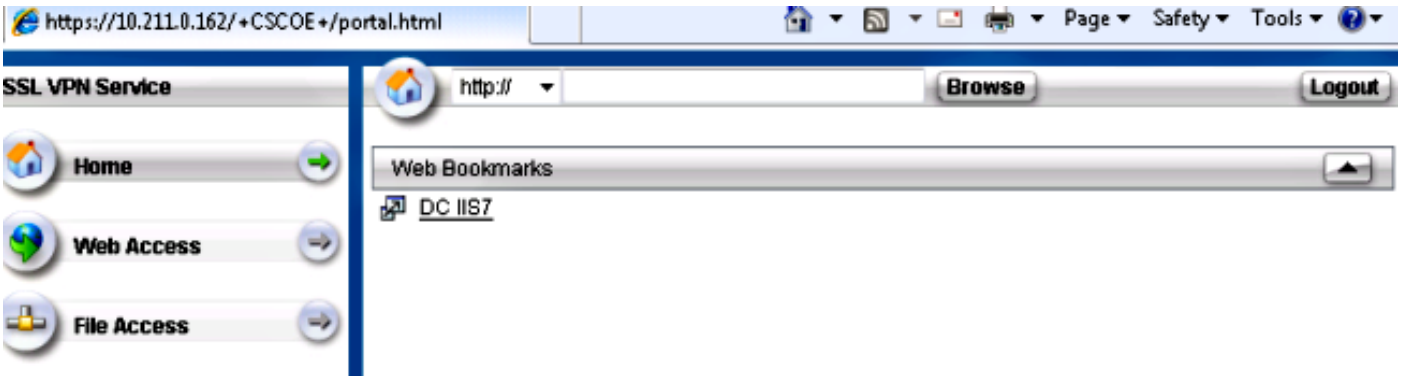
```
Kerberos: Server Name krbtgt
Kerberos: Start time 0
Kerberos: End time -878667256
Kerberos: Renew until time -878672192
Kerberos: Nonce 0xa9db408e
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4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

Die ASA kann der Domäne erfolgreich beitreten. Nach der richtigen Authentifizierung erhält die ASA ein Ticket für den Auftraggeber: Administrator im **AS_REP-**Paket (Ticket1 in Schritt 1 beschrieben).



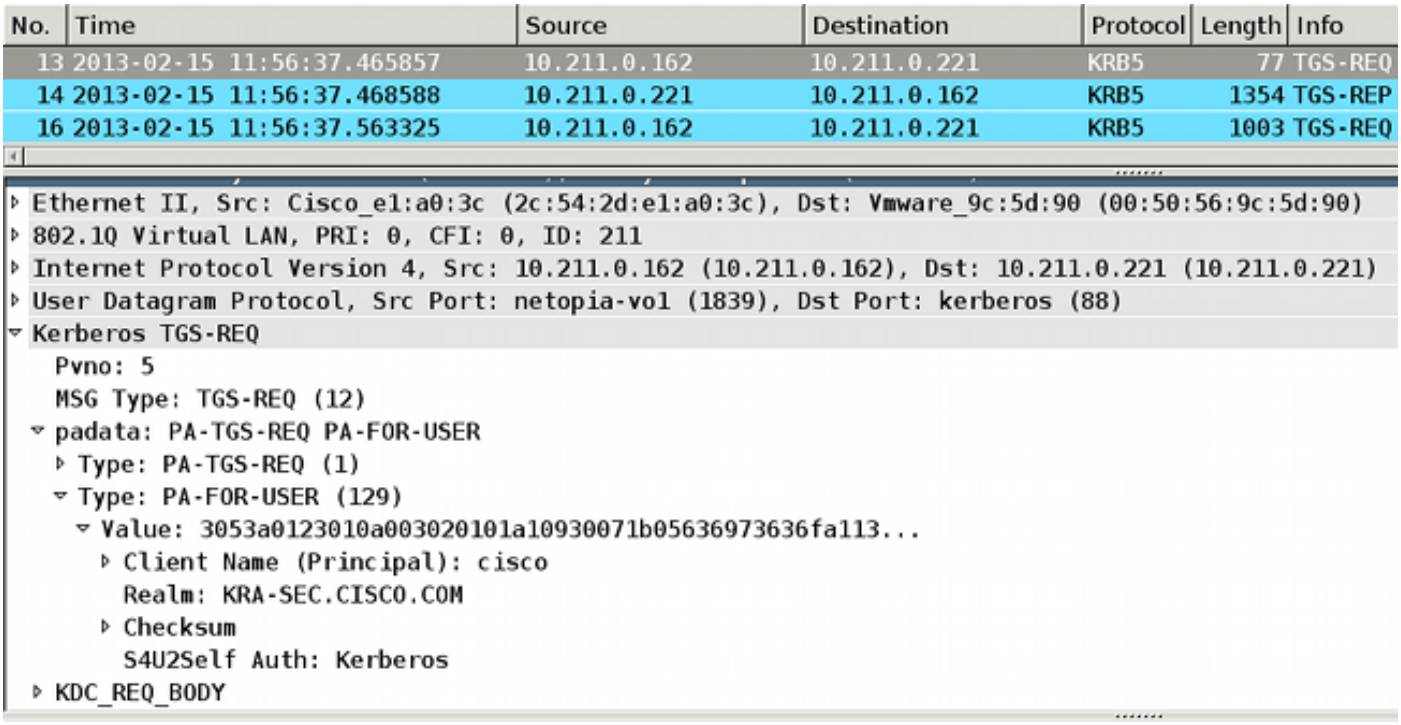
Serviceanfrage

Der Benutzer klickt auf den WebVPN-Link:



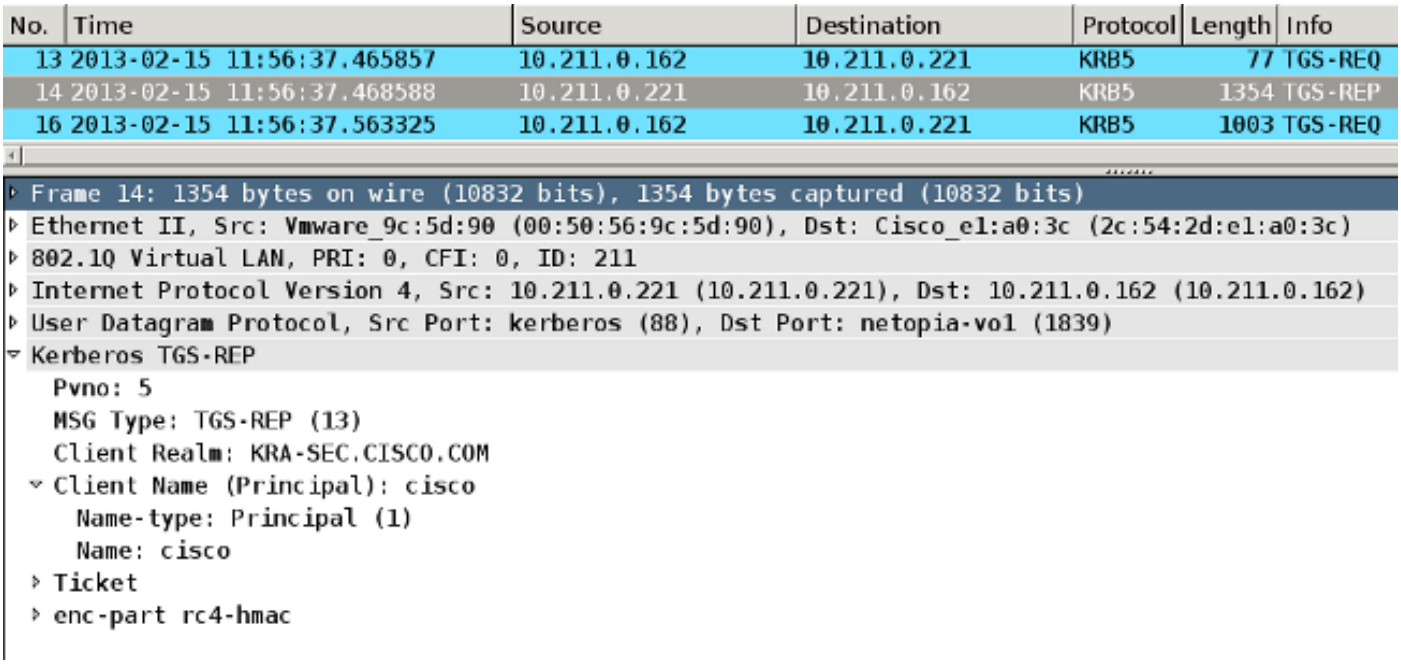
Die ASA sendet das **TGS_REQ** für ein imitiertes Ticket mit dem Ticket, das im **AS_REP-**Paket

empfangen wird:



Hinweis: Der **PA-FOR-USER-**Wert ist **cisco** (WebVPN-Benutzer). **PA-TGS-REQ** enthält das Ticket, das für die Kerberos Service Request empfangen wurde (der Hauptname ist der ASA-Hostname).

Die ASA erhält eine richtige Antwort mit dem imitierten Ticket für den Benutzer **cisco** (Ticket2 in Schritt 4 beschrieben):



Hier ist die Anfrage für das Ticket für den HTTP-Dienst (einige Debuggen werden aus Gründen der Klarheit weggelassen):

```
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 ticket**s.
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
```

Die ASA erhält das korrekte imitierte Ticket für den HTTP-Service (Ticket3, beschrieben in Schritt 6).

Beide Tickets können überprüft werden. Das erste ist das imitierte Ticket für den Benutzer **cisco**, das zum Anfordern und Empfangen des zweiten Tickets für den HTTP-Dienst verwendet wird, auf den zugegriffen wird:

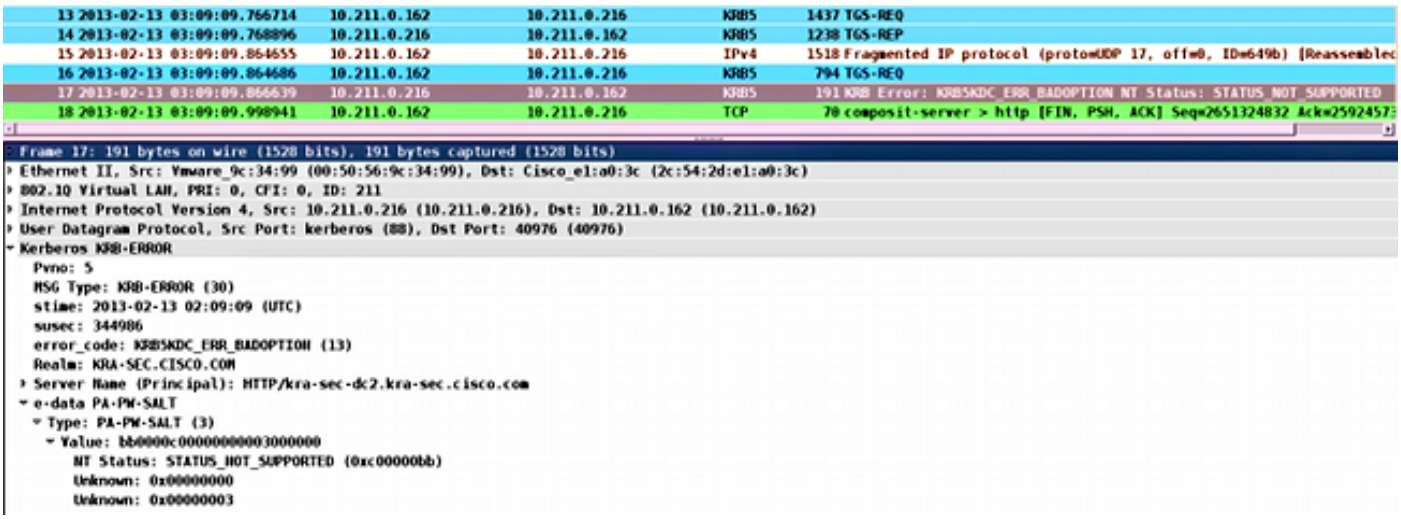
```
KRA-S-ASA-05(config)# show aaa kerberos
Default Principal: cisco@KRA-SEC.CISCO.COM
Valid Starting       Expires              Service Principal
19:38:10 CEST Oct 2 2013 05:37:33 CEST Oct 3 2013 KRA-S-ASA-05@KRA-SEC.CISCO.COM

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
```

Dieses HTTP-Ticket (Ticket3) wird für den HTTP-Zugriff (mit SPNEGO) verwendet, und der Benutzer muss keine Anmeldeinformationen angeben.

Fehlerbehebung

Manchmal kann es vorkommen, dass Sie ein Problem der falschen Delegierung haben. Beispielsweise verwendet die ASA ein Ticket, um den Dienst **HTTP/test.kra-sec.cisco.com** (Schritt 5) anzufordern, aber die Antwort ist **KRB-ERROR** mit **ERR_BADOPTION**:



Dies ist ein typisches Problem, das auftritt, wenn die Delegation nicht richtig konfiguriert ist. Die ASA berichtet, dass **"KDC die angeforderte Option nicht erfüllen kann"**:

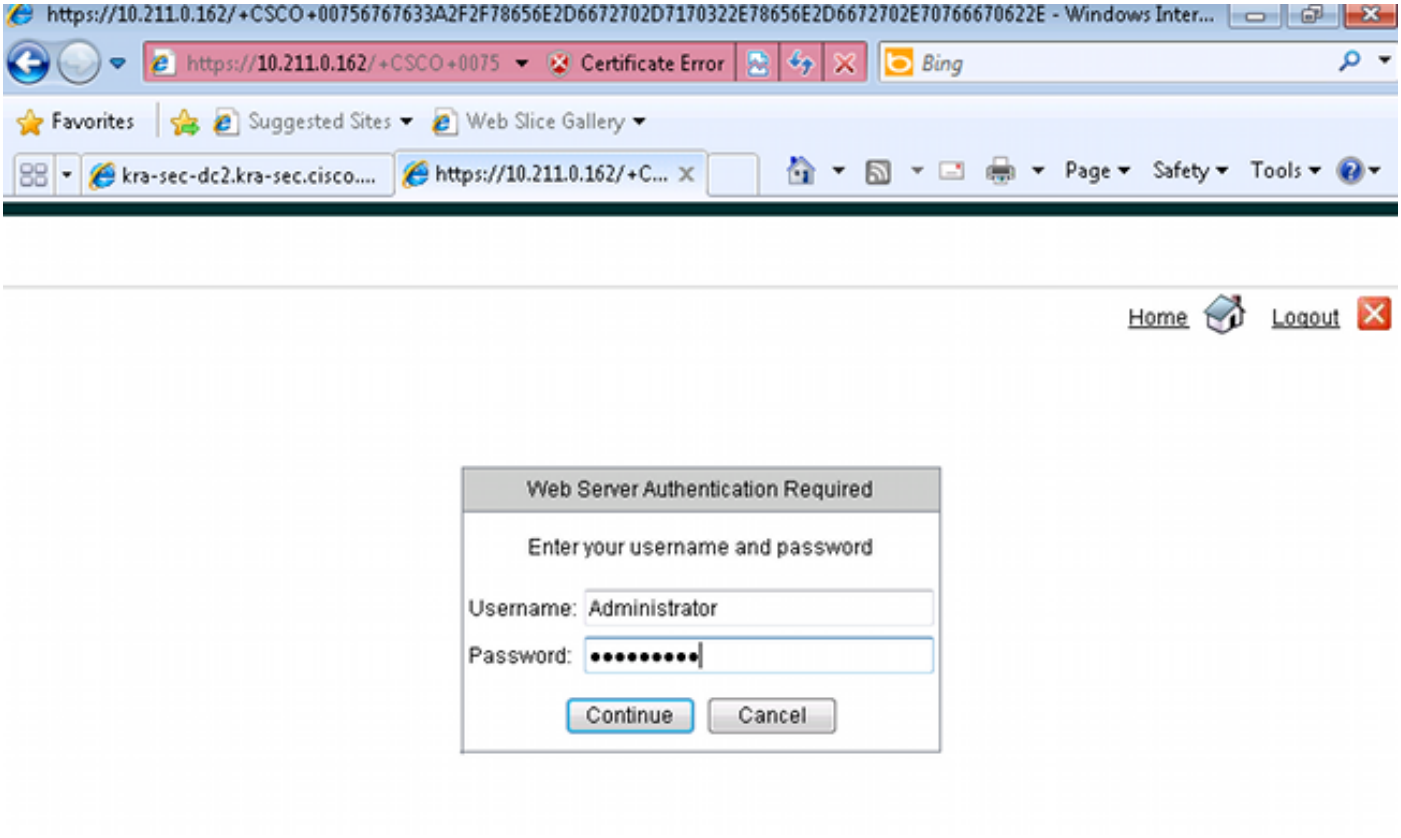
```
KRA-S-ASA-05# ucte_krb_get_auth_cred(): ctx = 0xcc4b5390,
WebVPN_session = 0xc919a260, protocol = 1
find_spn_in_url(): URL - /
build_host_spn(): host - test.kra-sec.cisco.com
build_host_spn(): SPN - HTTP/test.kra-sec.cisco.com
KCD_unicorn_get_cred(): Attempting to retrieve required KCD tickets.
In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

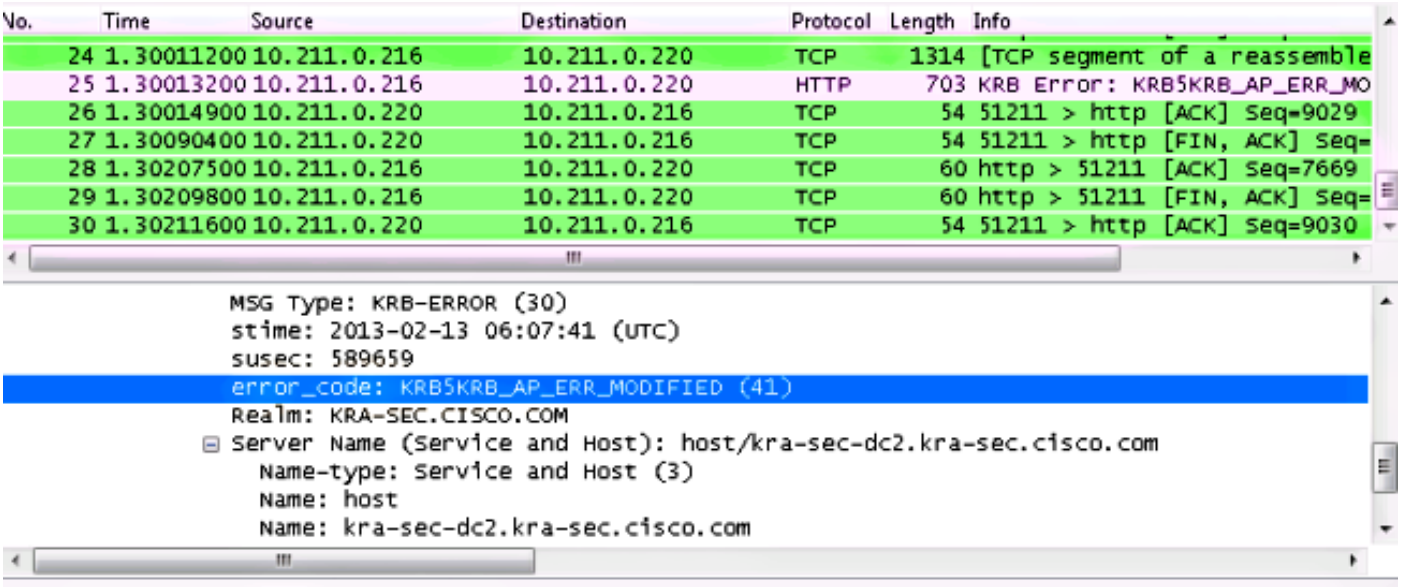
```
Kerberos: Option forwardable
Kerberos: Option renewable
Kerberos: Client Realm KRA-SEC.CISCO.COM
Kerberos: Server Name HTTP
Kerberos: Start time 0
Kerberos: End time -856104568
Kerberos: Renew until time 0
Kerberos: Nonce 0xf84c9385
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type 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
```

Dies ist im Grunde das gleiche Problem, das in den Captures beschrieben wird - der Fehler ist **bei TGS_REQ mit BAD_OPTION**.

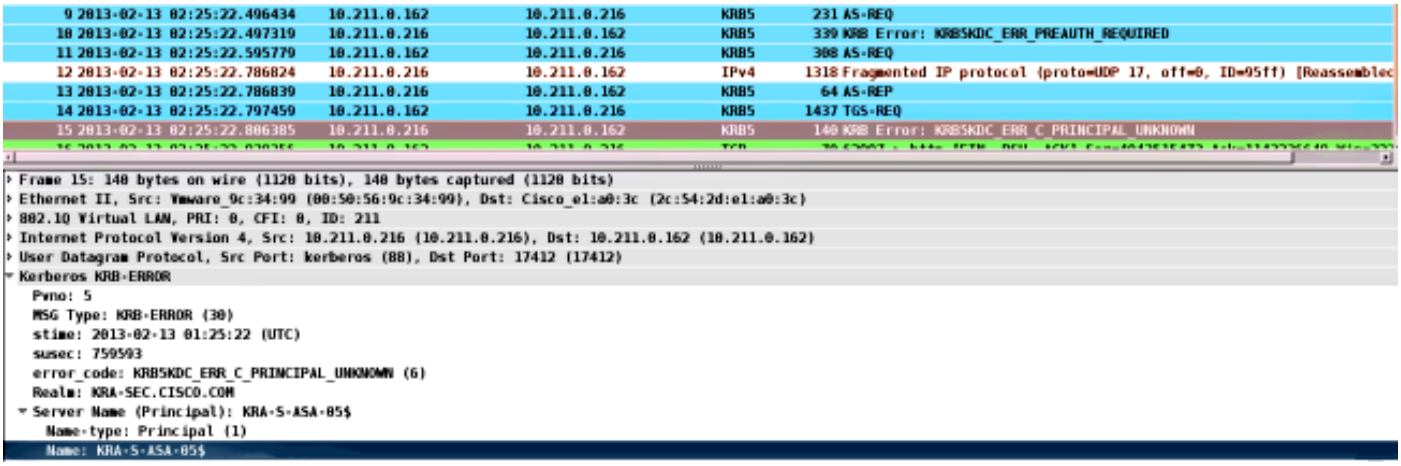
Wenn die Antwort **Success** lautet, erhält die ASA ein Ticket für den **HTTP/test.kra-sec.cisco.com**-Dienst, der für **SPNEGO-**Aushandlung verwendet wird. Aufgrund des Fehlers wird jedoch der **NT LAN Manager (NTLM)** ausgehandelt, und der Benutzer muss Anmeldeinformationen angeben:



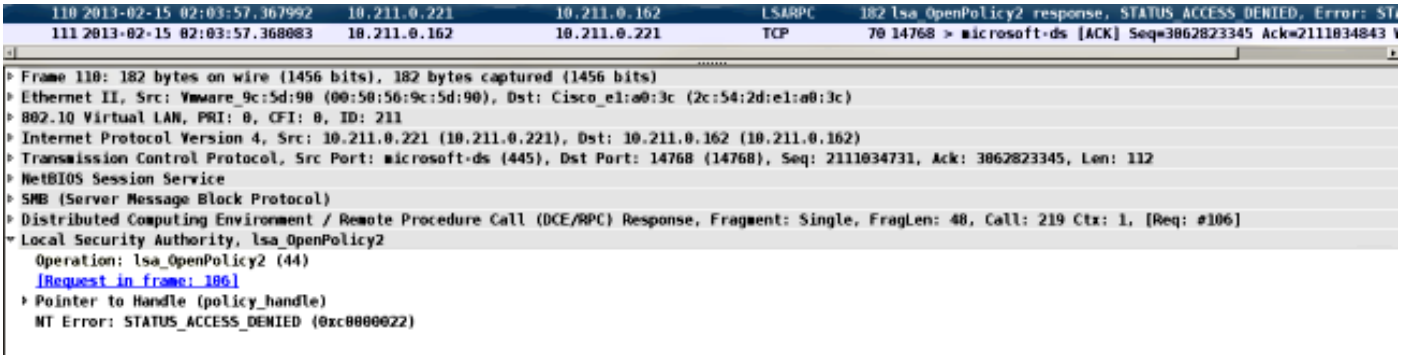
Stellen Sie sicher, dass die SPN nur für ein Konto registriert ist (Skript aus dem vorherigen Artikel). Wenn Sie diesen Fehler erhalten, **KRB_AP_ERR_MODIFIED**, bedeutet dies normalerweise, dass der **SPN** nicht für das richtige Konto registriert ist. Sie sollte für das Konto registriert werden, das zum Ausführen der Anwendung (Anwendungspool auf IIS) verwendet wird.



Wenn Sie diesen Fehler erhalten, **KRB_ERR_C_PRINCIPAL_UNKNOWN**, bedeutet dies, dass kein Benutzer im Rechenzentrum vorhanden ist (WebVPN-Benutzer: **cisco**).



Dieses Problem kann auftreten, wenn Sie der Domäne beitreten. Die ASA empfängt **AS-REP**, schlägt aber auf der **LSA**-Ebene fehl, mit dem Fehler: **STATUS_ACCESS_DENIED**:



Um dieses Problem zu beheben, müssen Sie die Vorabauthentifizierung für diesen Benutzer (**Administrator**) im Rechenzentrum aktivieren/deaktivieren.

Hier einige weitere Probleme, auf die Sie stoßen könnten:

- Beim Beitritt zur Domäne können Probleme auftreten. Wenn der RZ-Server über mehrere Network Interface Controller (NIC)-Adapter (mehrere IP-Adressen) verfügt, stellen Sie sicher, dass die ASA auf alle zugreifen kann, um der Domäne beizutreten (die vom Client basierend auf der DNS-Antwort (Domain Name Server) nach dem Zufallsprinzip ausgewählt wird).

- Legen Sie **SPN** nicht als **HOST/dc.kra-sec.cisco.com** für das **Administratorkonto fest**. Aufgrund dieser Einstellung kann die Verbindung zum Rechenzentrum unterbrochen werden.

- Wenn die ASA der Domäne beitritt, kann überprüft werden, ob das richtige Computerkonto im Rechenzentrum erstellt wurde (ASA-Hostname). Stellen Sie sicher, dass der Benutzer über die richtigen Berechtigungen zum Hinzufügen von Computerkonten verfügt (in diesem Beispiel verfügt der **Administrator** über die richtigen Berechtigungen).

- Denken Sie an die richtige **NTP-Konfiguration (Network Time Protocol)** auf der ASA. Standardmäßig nimmt das Rechenzentrum einen 5-minütigen Taktskew an. Dieser Timer kann im Rechenzentrum geändert werden.

- Überprüfen Sie, ob die Kerberos-Verbindung für das kleine Paket **UDP/88** verwendet wird. Nach dem Fehler vom Rechenzentrum, **KRB5KDC_ERR_RESPONSE_TOO_BIG**, wechselt der Client zu **TCP/88**. Es ist möglich, den Windows-Client zur Verwendung von **TCP/88** zu

zwingen, **ASA verwendet jedoch standardmäßig UDP**.

- Gleichstrom: Wenn Sie Richtlinienänderungen vornehmen, denken Sie an **gpupdate /force**.
- ASA: Testauthentifizierung mit dem **Test aaa**-Befehl, aber bedenken Sie, dass es sich nur um eine einfache Authentifizierung handelt.
- Um eine Fehlerbehebung auf der DC-Site durchzuführen, ist es hilfreich, Kerberos-Debug zu aktivieren: Aktivieren der Kerberos-Ereignisprotokollierung.

Cisco Bug-IDs

Hier finden Sie eine Liste der relevanten Cisco Bug-IDs:

- Cisco Bug ID CSCsi3224 - ASA schaltet nach dem Empfang des Kerberos-Fehlercodes 52 nicht auf TCP um
- Cisco Bug ID CSCtd92673 - Kerberos-Authentifizierung schlägt fehl, wenn Pre-Authorization aktiviert ist
- Cisco Bug-ID CSCuj19601 - ASA Webvpn KCD - versucht, erst nach einem Neustart bei AD einzutreten
- Cisco Bug ID CSCuh32106 - ASA KCD ist ab 8.4.5 defekt

Zugehörige Informationen

- Über einschränkte Delegation von Kerberos
- Funktionsweise von KCD
- PIX/ASA: Konfigurationsbeispiel für die Kerberos-Authentifizierung und LDAP-Autorisierungsserver-Gruppen für VPN-Client-Benutzer über ASDM/CLI
- Cisco ASA-Serie - Befehlsreferenz
- KDC_ERR_BADOPTION beim Versuch einer eingeschränkten Delegation
- Erzwingen der Verwendung von TCP anstelle von UDP in Windows durch Kerberos
- Technischer Support und Dokumentation - Cisco Systems