

WebVPN SSO与Kerberos约束委派集成配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[与ASA的Kerberos交互](#)

[配置](#)

[拓扑](#)

[域控制器和应用配置](#)

[域设置](#)

[设置服务主体名称\(SPN\)](#)

[ASA上的配置](#)

[验证](#)

[ASA加入域](#)

[服务请求](#)

[故障排除](#)

[思科漏洞ID](#)

[相关信息](#)

简介

本文档介绍如何为受Kerberos保护的应用配置WebVPN单点登录(SSO)并对其进行故障排除。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- 思科自适应安全设备(ASA)CLI配置和安全套接字层(SSL)VPN配置
- Kerberos服务

使用的组件

本文档中的信息基于以下软件版本：

- Cisco ASA软件9.0版及更高版本
- Microsoft Windows 7客户端
- Microsoft Windows 2003 Server及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

Kerberos是一种网络身份验证协议，允许网络实体以安全方式相互进行身份验证。它使用可信第三方密钥分发中心(KDC)，该中心向网络实体授予票证。实体使用这些票证来验证和确认对所请求服务的访问。

可以为受Kerberos保护的应用配置WebVPN SSO，并使用称为Kerberos约束委派(KCD)的Cisco ASA功能。通过此功能，ASA可以代表WebVPN门户用户请求Kerberos票证，同时访问受Kerberos保护的应用。

当您通过WebVPN门户访问此类应用时，不再需要提供任何凭证；而是使用用于登录WebVPN门户的帐户。

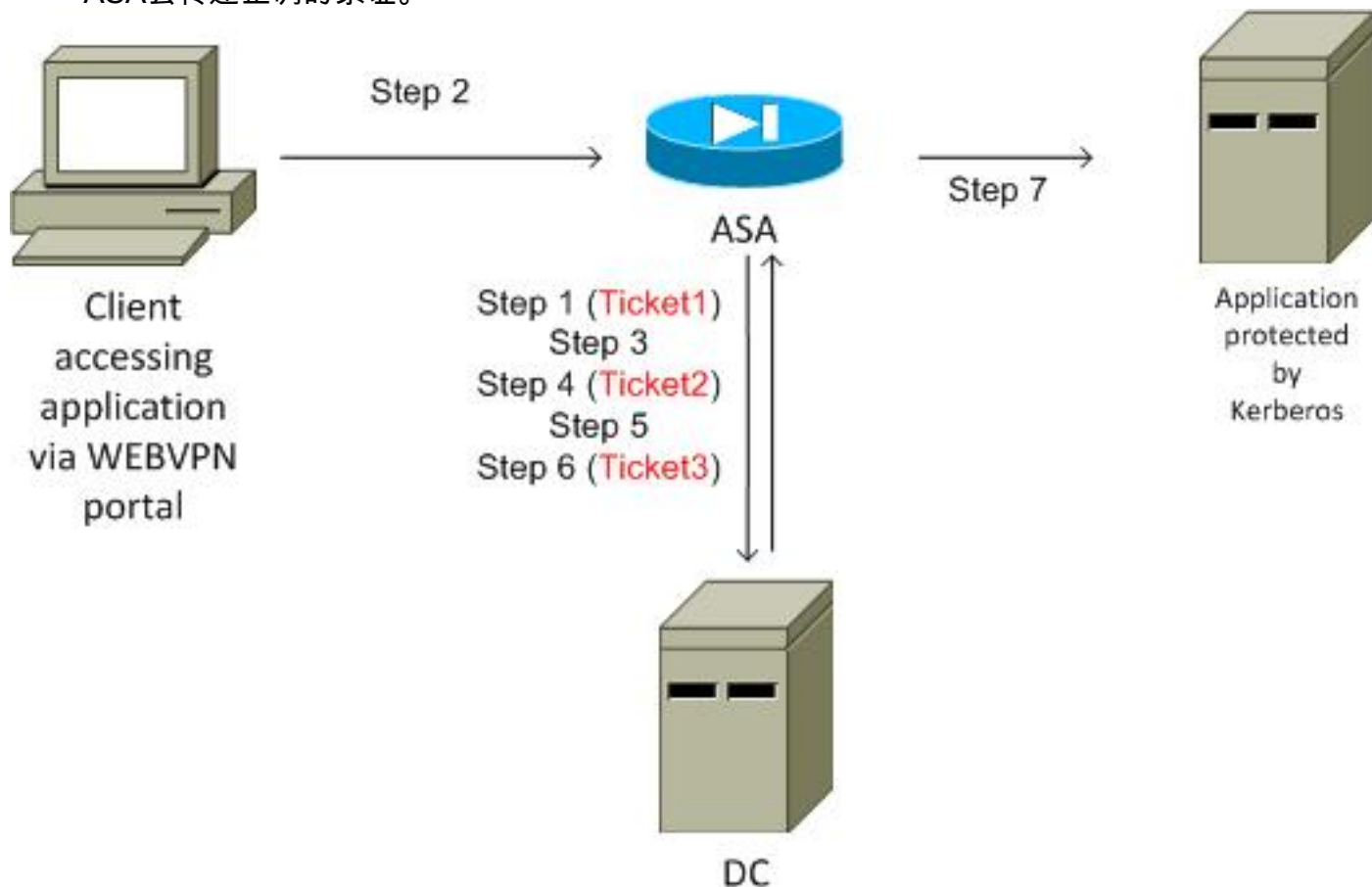
有关详细信息，[请参阅ASA配置指南的了解KCD的工作方式部分](#)。

与ASA的Kerberos交互

对于WebVPN，ASA必须代表用户请求票证（因为WebVPN门户用户仅有权访问该门户，而无权访问Kerberos服务）。为此，ASA使用Kerberos扩展进行约束委派。流程如下：

1. ASA加入域并获取计算机帐户的票证（票证1），该帐户具有在ASA(kcd-server命令)上配置的凭证。此票证用于访问Kerberos服务的后续步骤。
2. 用户点击Kerberos保护应用的WebVPN门户链接。
3. ASA请求(TGS-REQ)计算机帐户的票证，其主机名作为主体。此请求包括PA-TGS-REQ字段，其中PA-FOR-USER作为WebVPN门户用户名，在本场景中为cisco。第1步中的Kerberos服务票证用于身份验证（正确委派）。
4. 作为响应，ASA代表计算机帐户的WebVPN用户(TGS_REP)收到**模拟的**票证(Ticket2)。此票证用于代表此WebVPN用户请求应用票证。
5. ASA启动另一个请求(TGS_REQ)，以便获取应用程序(HTTP/test.kra-sec.cisco.com)的票证。此请求再次使用PA-TGS-REQ字段，此次**不使用**PA-FOR-USER字段，但在步骤4中收到模拟票证。
6. 返回具有**应用的模拟票证**（票证3）的响应(TGS_REQ)。
7. 此票证由ASA透明地使用，以访问受保护的服务，WebVPN用户无需输入任何凭证。对于HTTP应用，使用简单和受保护的GSS-API协商(SPNEGO)机制来协商身份验证方法，并且

ASA会传递正确的票证。



配置

拓扑

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

Internet信息服务(IIS)7应用程序:test.kra-sec.cisco.com(10.211.0.223)

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

ASA : 10.211.0.162

WebVPN用户名/密码:思科/思科

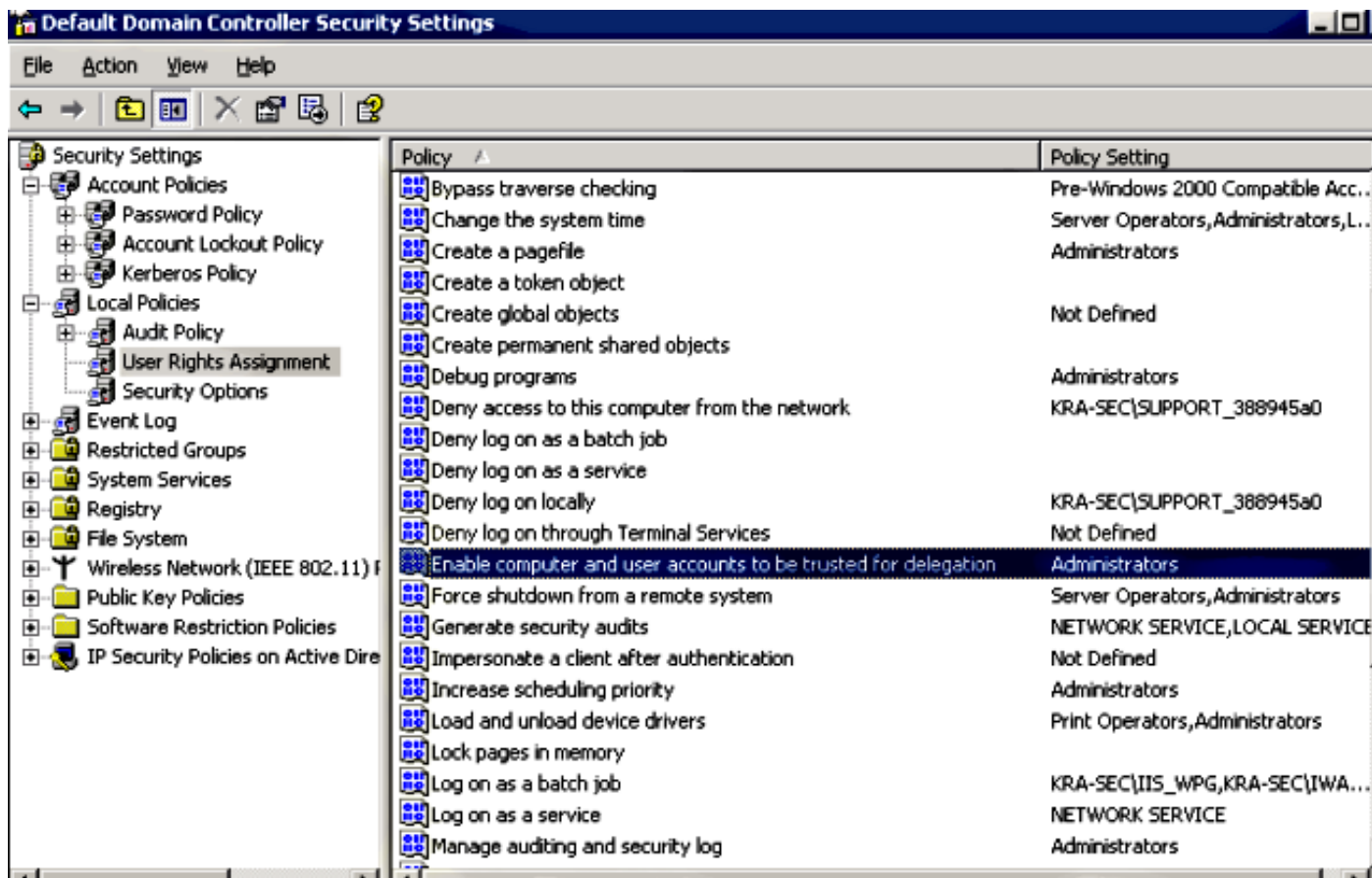
附件:asa-join.pcap (成功加入域)

附件:asa-kerberos-bad.pcap (服务请求)

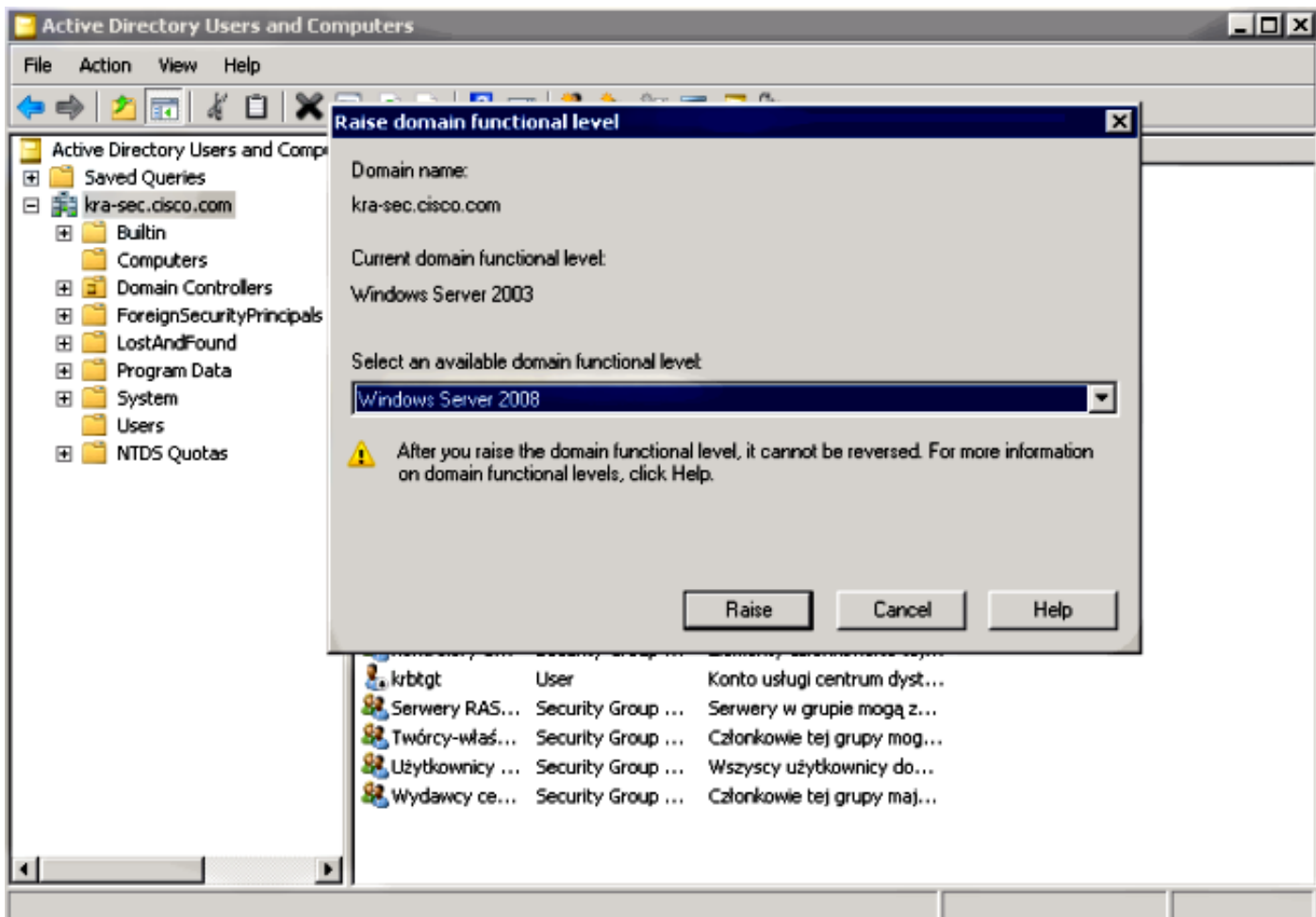
域控制器和应用配置

域设置

假设已有一个功能正常的IIS7应用程序受Kerberos保护（如果没有，请阅读“先决条件”部分）。您必须检查用户委托的设置：



确保功能域级别提升到Windows Server 2003（至少）。默认为Windows Server 2000:



设置服务主体名称(SPN)

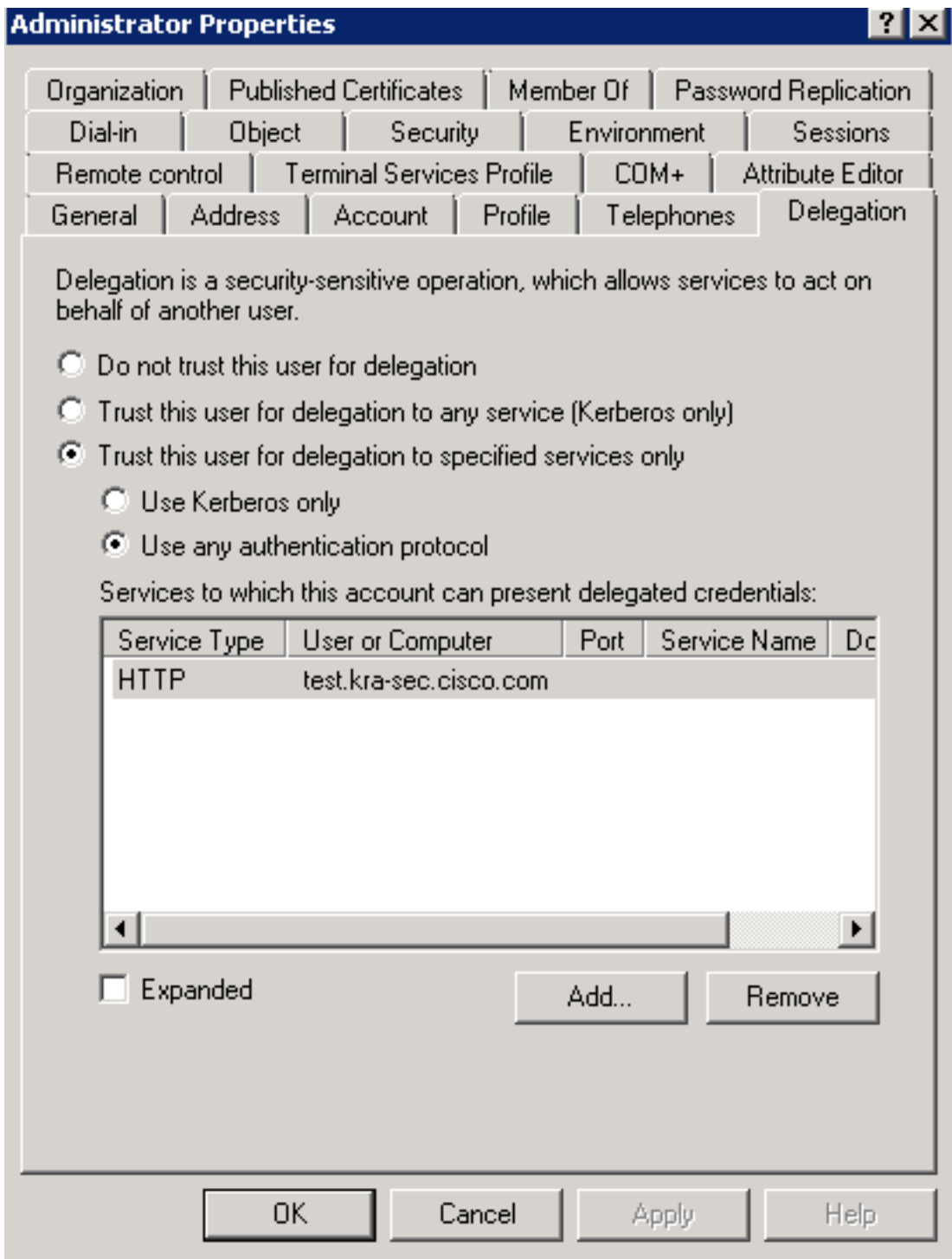
您必须使用正确的委派配置AD上的任何帐户。使用管理员帐户。当ASA使用该帐户时，它可以代表另一用户（受约束委派）为特定服务（HTTP应用）请求票证。为了实现此目的，必须为应用/服务创建正确的委派。

要通过CLI使用**setspn.exe**（Windows Server 2003 Service Pack 1支持工具的一部分）进行此委派，[请输入以下命令：](#)

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

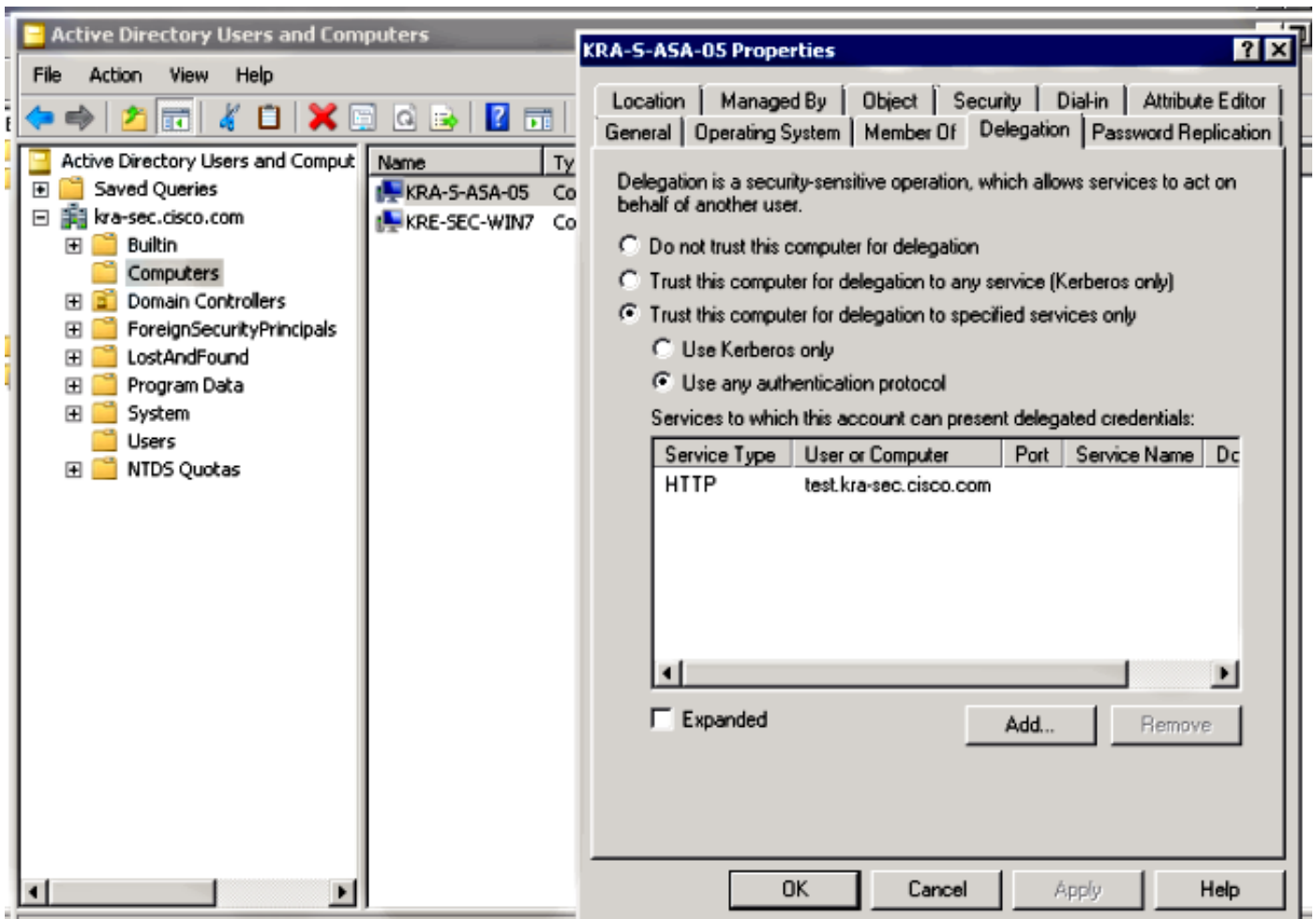
这表示管理员用户名是用于委派HTTP服务的受信任帐户，地址为test.kra-sec.cisco.com。

要激活该用户的“委派”选项卡，也需要使用SPN命令。输入命令后，系统将显示管理员的“委派”选项卡。启用“使用任何身份验证协议”非常重要，因为“仅使用Kerberos”不支持约束委派扩展。



在**General**选项卡上，也可以禁用Kerberos预身份验证。但是，不建议使用此功能，因为此功能用于保护数据中心免受重播攻击。ASA可以正确使用预身份验证。

此过程也适用于计算机帐户的委派（ASA作为计算机引入域以建立“信任”关系）：



ASA上的配置

```

interface Vlan211
 nameif inside
 security-level 100
 ip address 10.211.0.162 255.255.255.0

hostname KRA-S-ASA-05
domain-name kra-sec.cisco.com

dns domain-lookup inside
dns server-group DNS-GROUP
 name-server 10.211.0.221
domain-name kra-sec.cisco.com

aaa-server KerberosGroup protocol kerberos
aaa-server KerberosGroup (inside) host 10.211.0.221
 kerberos-realm KRA-SEC.CISCO.COM

webvpn
 enable outside
 enable inside
 kcd-server KerberosGroup username Administrator password *****

group-policy G1 internal
group-policy G1 attributes
 WebVPN
 url-list value KerberosProtected
username cisco password 3USUcOPFUimCO4Jk encrypted

```

```
tunnel-group WEB type remote-access
tunnel-group WEB general-attributes
  default-group-policy G1
tunnel-group WEB webvpn-attributes
  group-alias WEB enable
dns-group DNS-GROUP
```

验证

ASA加入域

使用kcd-server命令后，ASA将尝试加入域：

```
***** START: KERBEROS PACKET DECODE *****
Kerberos: Message type KRB_AS_REQ
Kerberos: Option forwardable
Kerberos: Client Name KRA-S-ASA-05$
Kerberos: Client Realm KRA-SEC.CISCO.COM
Kerberos: Server Name krbtgt
Kerberos: Start time 0
Kerberos: End time -878674400
Kerberos: Renew until time -878667552
Kerberos: Nonce 0xa9db408e
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4
Kerberos: Encryption type des3-cbc-shal
***** END: KERBEROS PACKET DECODE *****
In kerberos_recv_msg
In KCD_self_tkt_process_response
***** START: KERBEROS PACKET DECODE *****
Kerberos: Message type KRB_ERROR
Kerberos: Error type: Additional pre-authentication required, -1765328359
(0x96c73a19)
Kerberos: Encrypt Type: 23 (rc4-hmac-md5)
Salt: "" Salttype: 0
Kerberos: Encrypt Type: 3 (des-cbc-md5)
Salt: "KRA-SEC.CISCO.COMhostkra-s-asa-05.kra-sec.cisco.com" Salttype: 0
Kerberos: Encrypt Type: 1 (des-cbc-crc)
Salt: "KRA-SEC.CISCO.COMhostkra-s-asa-05.kra-sec.cisco.com" Salttype: 0
Kerberos: Preauthentication type unknown
Kerberos: Preauthentication type encrypt timestamp
Kerberos: Preauthentication type unknown
Kerberos: Preauthentication type unknown
Kerberos: Server time 1360917305
Kerberos: Realm KRA-SEC.CISCO.COM
Kerberos: Server Name krbtgt
***** END: KERBEROS PACKET DECODE *****
Attempting to parse the error response from KCD server.
Kerberos library reports: "Additional pre-authentication required"
In kerberos_send_request
***** START: KERBEROS PACKET DECODE *****
Kerberos: Message type KRB_AS_REQ
Kerberos: Preauthentication type encrypt timestamp
Kerberos: Option forwardable
Kerberos: Client Name KRA-S-ASA-05$
Kerberos: Client Realm KRA-SEC.CISCO.COM
```



```

Kerberos: Server Name krbtgt
Kerberos: Start time 0
Kerberos: End time -878667256
Kerberos: Renew until time -878672192
Kerberos: Nonce 0xa9db408e
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4
Kerberos: Encryption type des3-cbc-sha1
***** END: KERBEROS PACKET DECODE *****
In kerberos_recv_msg
In KCD_self_tkt_process_response
***** START: KERBEROS PACKET DECODE *****
Kerberos: Message type KRB_AS_REP
Kerberos: Client Name KRA-S-ASA-05$
Kerberos: Client Realm KRA-SEC.CISCO.COM
***** END: KERBEROS PACKET DECODE *****
INFO: Successfully stored self-ticket in cache a6588e0
KCD self-ticket retrieval succeeded.
In kerberos_close_connection
remove_req 0xcc09ad18 session 0x1 id 0
free_kip 0xcc09ad18
kerberos: work queue empty

```

ASA能够成功加入域。经过正确的身份验证后，ASA将收到主体的票证：AS_REP数据包中的管理员（步骤1中介绍的Ticket1）。

28	2013-02-12 06:16:20.686888	10.211.0.162	10.211.0.216	KRB5	225 AS-REQ
29	2013-02-12 06:16:20.687678	10.211.0.216	10.211.0.162	KRB5	206 KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
30	2013-02-12 06:16:20.719281	10.211.0.162	10.211.0.216	DNS	183 Standard query 0x4c7d SRV_kerberos-master_udp.KRA-SEC.C
31	2013-02-12 06:16:20.719689	10.211.0.216	10.211.0.162	DNS	178 Standard query response 0x4c7d No such name
32	2013-02-12 06:16:20.760508	10.211.0.162	10.211.0.216	KRB5	303 AS-REQ
33	2013-02-12 06:16:20.762045	10.211.0.216	10.211.0.162	IPv4	1318 Fragmented IP protocol (proto=UDP 17, off=0, ID=cd3c) [Ro
34	2013-02-12 06:16:20.762045	10.211.0.216	10.211.0.162	KRB5	112 AS-REP


```

Frame 34: 112 bytes on wire (896 bits), 112 bytes captured (896 bits)
  Ethernet II, Src: Vmware_9c:34:99 (00:50:56:9c:34:99), Dst: Cisco_el:a0:3c (2c:54:2d:e1:a0:3c)
  802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 211
  Internet Protocol Version 4, Src: 10.211.0.216 (10.211.0.216), Dst: 10.211.0.162 (10.211.0.162)
  User Datagram Protocol, Src Port: kerberos (88), Dst Port: 56007 (56007)
  Kerberos AS-REP
    Pvno: 5
    MSG Type: AS-REP (11)
    Client Realm: KRA-SEC.CISCO.COM
    Client Name (Principal): Administrator
    Ticket
    enc-part rc4-hmac

```

服务请求

用户点击WebVPN链接：

ASA发送模拟票证的TGS_REQ，该票证在AS_REP数据包中接收：

No.	Time	Source	Destination	Protocol	Length	Info
13	2013-02-15 11:56:37.465857	10.211.0.162	10.211.0.221	KRB5	77	TGS-REQ
14	2013-02-15 11:56:37.468588	10.211.0.221	10.211.0.162	KRB5	1354	TGS-REP
16	2013-02-15 11:56:37.563325	10.211.0.162	10.211.0.221	KRB5	1003	TGS-REQ


```

Ethernet II, Src: Cisco_e1:a0:3c (2c:54:2d:e1:a0:3c), Dst: Vmware_9c:5d:90 (00:50:56:9c:5d:90)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 211
Internet Protocol Version 4, Src: 10.211.0.162 (10.211.0.162), Dst: 10.211.0.221 (10.211.0.221)
User Datagram Protocol, Src Port: netopia-vol (1839), Dst Port: kerberos (88)
Kerberos TGS-REQ
  Pvno: 5
  MSG Type: TGS-REQ (12)
  padata: PA-TGS-REQ PA-FOR-USER
    Type: PA-TGS-REQ (1)
    Type: PA-FOR-USER (129)
      Value: 3053a0123010a003020101a10930071b05636973636fa113...
        Client Name (Principal): cisco
        Realm: KRA-SEC.CISCO.COM
        Checksum
        S4U2Self Auth: Kerberos
    KDC_REQ_BODY

```

注意：PA-FOR-USER值是cisco（WebVPN用户）。PA-TGS-REQ包含为Kerberos服务请求（ASA主机名是主体）接收的票证。

ASA通过用户cisco的模拟票证（步骤4中描述的票证2）获得正确的响应：

No.	Time	Source	Destination	Protocol	Length	Info
13	2013-02-15 11:56:37.465857	10.211.0.162	10.211.0.221	KRB5	77	TGS-REQ
14	2013-02-15 11:56:37.468588	10.211.0.221	10.211.0.162	KRB5	1354	TGS-REP
16	2013-02-15 11:56:37.563325	10.211.0.162	10.211.0.221	KRB5	1003	TGS-REQ


```

Frame 14: 1354 bytes on wire (10832 bits), 1354 bytes captured (10832 bits)
Ethernet II, Src: Vmware_9c:5d:90 (00:50:56:9c:5d:90), Dst: Cisco_e1:a0:3c (2c:54:2d:e1:a0:3c)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 211
Internet Protocol Version 4, Src: 10.211.0.221 (10.211.0.221), Dst: 10.211.0.162 (10.211.0.162)
User Datagram Protocol, Src Port: kerberos (88), Dst Port: netopia-vol (1839)
Kerberos TGS-REP
  Pvno: 5
  MSG Type: TGS-REP (13)
  Client Realm: KRA-SEC.CISCO.COM
  Client Name (Principal): cisco
    Name-type: Principal (1)
    Name: cisco
  Ticket
  enc-part rc4-hmac

```

以下是HTTP服务的票证请求（为清楚起见，省略了一些调试）：

```

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 adab04f81.
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_rcv_msg
In KCD_cred_tkt_process_response
```

```
***** START: KERBEROS PACKET DECODE *****
Kerberos: Message type KRB_TGS_REP
Kerberos: Client Name cisco
Kerberos: Client Realm KRA-SEC.CISCO.COM
***** END: KERBEROS PACKET DECODE *****
```

```
KCD_unicorn_callback(): called with status: 1.
```

```
Successfully retrieved service ticket
for user cisco, spn HTTP/test.kra-sec.cisco.com
```

```
In kerberos_close_connection
remove_req 0xaceaf560 session 0x5 id 2
free_kip 0xaceaf560
kerberos: work queue empty
ucte_krb_authenticate_connection(): ctx - 0xad045dd0, proto - http,
host - test.kra-sec.cisco.com
In kerberos_cache_open: KCD opening cache adab04f8S.
Source: cisco@KRA-SEC.CISCO.COM
Target: HTTP/test.kra-sec.cisco.com@KRA-SEC.CISCO.COM
```

ASA收到HTTP服务的正确模拟票证（步骤6中描述的Ticket3）。

两张票都可以验证。第一个是用户cisco的模拟票证，用于请求和接收所访问的HTTP服务的第二个票证：

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

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

Valid Starting Expires Service Principal

19:38:10 CEST Oct 2 2013 05:37:33 CEST Oct 3 2013

HTTP/test.kra-sec.cisco.com@KRA-SEC.CISCO.COM

此HTTP票证 (票证3) 用于HTTP访问 (使用SPNEGO) , 用户不需要提供任何凭据。

故障排除

有时, 您可能会遇到不正确委派的问题。例如, ASA使用票证来请求服务HTTP/test.kra-sec.cisco.com (步骤5) , 但响应是KRB-ERROR,ERR_BAPPOTION:

```
13 2013-02-13 03:09:09.766714 10.211.0.162 10.211.0.216 KRB5 1437 TGS-REQ
14 2013-02-13 03:09:09.768896 10.211.0.216 10.211.0.162 KRB5 1238 TGS-REP
15 2013-02-13 03:09:09.864655 10.211.0.162 10.211.0.216 IPv4 1518 Fragmented IP protocol (proto=UDP 17, off=0, ID=649b) [Reassembled]
16 2013-02-13 03:09:09.864686 10.211.0.162 10.211.0.216 KRB5 794 TGS-REQ
17 2013-02-13 03:09:09.866639 10.211.0.216 10.211.0.162 KRB5 191 KRB Error: KRB5KDC_ERR_BADOPTION NT Status: STATUS_NOT_SUPPORTED
18 2013-02-13 03:09:09.998941 10.211.0.162 10.211.0.216 TCP 70 composit-server > http [FIN, PSH, ACK] Seq=2651324832 Ack=2592457

Frame 17: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)
  Ethernet II, Src: Vmware_9c:34:99 (00:50:56:9c:34:99), Dst: Cisco_e1:a0:3c (2c:54:2d:e1:a0:3c)
  802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 211
  Internet Protocol Version 4, Src: 10.211.0.216 (10.211.0.216), Dst: 10.211.0.162 (10.211.0.162)
  User Datagram Protocol, Src Port: kerberos (88), Dst Port: 40976 (40976)
  Kerberos KRB-ERROR
    Ptype: 5
    MSG Type: KRB-ERROR (30)
    stime: 2013-02-13 02:09:09 (UTC)
    susec: 344906
    error_code: KRB5KDC_ERR_BADOPTION (13)
    Realm: KRA-SEC.CISCO.COM
    Server Name (Principal): HTTP/kra-sec-dc2.kra-sec.cisco.com
  e-data PA-PW-SALT
    Type: PA-PW-SALT (3)
    Value: bb0000c00000000003000000
    NT Status: STATUS_NOT_SUPPORTED (0xc00000bb)
    Unknown: 0x00000000
    Unknown: 0x00000003
```

这是委派配置不正确时遇到的典型问题。ASA报告“KDC无法执行请求的选项”:

```
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
```

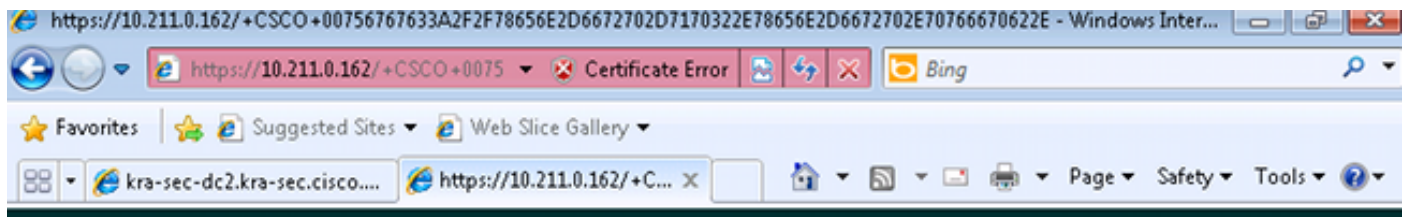
```

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

```

这基本上与捕获中描述的问题相同 — 故障在TGS_REQ和BAD_OPTION处。

如果响应为**Success**，则ASA将收到用于SPNEGO协商的HTTP/test.kra-sec.cisco.com服务的票证。但是，由于故障，NT LAN Manager(NTLM)是协商的，用户必须提供凭据：



Home  Logout 

Web Server Authentication Required

Enter your username and password

Username:

Password:

确保SPN仅注册一个帐户（上一文章中的脚本）。当您收到此错误KRB_AP_ERR_MODIFIED时，这通常意味着SPN未注册到正确的帐户。应为用于运行应用程序（IIS上的应用程序池）的帐户注册该帐户。

No.	Time	Source	Destination	Protocol	Length	Info
24	1.30011200	10.211.0.216	10.211.0.220	TCP	1314	[TCP segment of a reassemble
25	1.30013200	10.211.0.216	10.211.0.220	HTTP	703	KRB Error: KRB5KRB_AP_ERR_MO
26	1.30014900	10.211.0.220	10.211.0.216	TCP	54	51211 > http [ACK] Seq=9029
27	1.30090400	10.211.0.220	10.211.0.216	TCP	54	51211 > http [FIN, ACK] Seq=
28	1.30207500	10.211.0.216	10.211.0.220	TCP	60	http > 51211 [ACK] seq=7669
29	1.30209800	10.211.0.216	10.211.0.220	TCP	60	http > 51211 [FIN, ACK] seq=
30	1.30211600	10.211.0.220	10.211.0.216	TCP	54	51211 > http [ACK] Seq=9030


```

MSG Type: KRB-ERROR (30)
stime: 2013-02-13 06:07:41 (UTC)
susec: 589659
error_code: KRB5KRB_AP_ERR_MODIFIED (41)
Realm: KRA-SEC.CISCO.COM
  Server Name (Service and Host): host/kra-sec-dc2.kra-sec.cisco.com
    Name-type: Service and Host (3)
    Name: host
    Name: kra-sec-dc2.kra-sec.cisco.com

```

当您收到此错误KRB_ERR_C_PRINCIPAL_UNKNOWN时，这表示DC上没有用户(WebVPN用户：cisco)。

9	2013-02-13 02:25:22.496434	10.211.0.162	10.211.0.216	KRB5	231	AS-REQ
10	2013-02-13 02:25:22.497319	10.211.0.216	10.211.0.162	KRB5	339	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
11	2013-02-13 02:25:22.595779	10.211.0.162	10.211.0.216	KRB5	388	AS-REQ
12	2013-02-13 02:25:22.786824	10.211.0.216	10.211.0.162	IPV4	1318	Fragmented IP protocol (proto=UDP 17, off=0, ID=951f) [Reassembled
13	2013-02-13 02:25:22.786839	10.211.0.216	10.211.0.162	KRB5	64	AS-REP
14	2013-02-13 02:25:22.797459	10.211.0.162	10.211.0.216	KRB5	1437	TGS-REQ
15	2013-02-13 02:25:22.886385	10.211.0.216	10.211.0.162	KRB5	140	KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN


```

> Frame 15: 148 bytes on wire (1128 bits), 148 bytes captured (1128 bits)
> Ethernet II, Src: VMware_9c:34:99 (00:50:56:9c:34:99), Dst: Cisco_e1:a0:3c (2c:54:2d:e1:a0:3c)
> 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 211
> Internet Protocol Version 4, Src: 10.211.0.216 (10.211.0.216), Dst: 10.211.0.162 (10.211.0.162)
> User Datagram Protocol, Src Port: kerberos (88), Dst Port: 17412 (17412)
Kerberos KRB-ERROR
  Pyno: 5
  MSG Type: KRB-ERROR (30)
  stime: 2013-02-13 01:25:22 (UTC)
  susec: 759593
  error_code: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN (6)
  Realm: KRA-SEC.CISCO.COM
  Server Name (Principal): KRA-S-ASA-05$
    Name-type: Principal (1)
    Name: KRA-S-ASA-05$

```

加入域时，可能会遇到此问题。ASA接收AS-REP，但在LSA级别失败，出现错误：STATUS_ACCESS_DENIED:

110	2013-02-15 02:03:57.367992	10.211.0.221	10.211.0.162	LSARPC	182	lsa OpenPolicy2 response, STATUS_ACCESS_DENIED, Error: ST
111	2013-02-15 02:03:57.368083	10.211.0.162	10.211.0.221	TCP	70	14768 > microsoft-ds [ACK] Seq=3862823345 Ack=2111834843 V


```

> Frame 110: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits)
> Ethernet II, Src: VMware_9c:3d:98 (00:50:56:9c:3d:98), Dst: Cisco_e1:a0:3c (2c:54:2d:e1:a0:3c)
> 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 211
> Internet Protocol Version 4, Src: 10.211.0.221 (10.211.0.221), Dst: 10.211.0.162 (10.211.0.162)
> Transmission Control Protocol, Src Port: microsoft-ds (445), Dst Port: 14768 (14768), Seq: 2111834731, Ack: 3862823345, Len: 112
> NetBIOS Session Service
> SMB (Server Message Block Protocol)
> Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Response, Fragment: Single, FragLen: 48, Call: 219 Ctx: 1, [Req: #106]
Local Security Authority, lsa_OpenPolicy2
  Operation: lsa_OpenPolicy2 (44)
  [Request in frame: 186]
  Pointer to Handle (policy_handle)
  NT Error: STATUS_ACCESS_DENIED (0xc0000022)

```

要解决此问题，必须在DC上为该用户（管理员）启用/禁用预身份验证。

您可能会遇到以下其他问题：

- 加入域时可能会出现问题。如果DC服务器有多个网络接口控制器(NIC)适配器（多个IP地址），请确保ASA可以访问所有适配器以加入域(由客户端根据域名服务器(DNS)响应随机选择)。
- 不要将SPN设置为管理员帐户的HOST/dc.kra-sec.cisco.com。由于该设置，可能会失去与

DC的连接。

- 在ASA加入域后，可以验证在DC (ASA主机名) 上创建了正确的计算机帐户。确保用户具有正确的权限以添加计算机帐户(在本例中，Administrator 具有正确的权限)。
- 请记住ASA上正确的网络时间协议(NTP)配置。默认情况下，DC接受五分钟时钟偏差。该计时器可在直流电上更改。
- 验证是否使用了小数据包UDP/88的Kerberos连接。在DC KRB5KDC_ERR_RESPONSE_TOO_BIG发生错误后，客户端将切换到TCP/88。可以强制Windows客户端使用TCP/88，但ASA将默认使用UDP。
- DC:更改策略时，请记住gpupdate /force。
- ASA : 使用test aaa命令测试身份验证，但请记住，它只是简单的身份验证。
- 要在DC站点上进行故障排除，启用Kerberos调试非常有用：[如何启用Kerberos事件日志记录](#)。

思科漏洞ID

以下是相关思科漏洞ID的列表：

- Cisco Bug ID [CSCsi32224](#) - ASA在收到Kerberos错误代码52后未切换到TCP
- Cisco Bug ID [CSCtd92673](#) — 启用预身份验证后Kerberos身份验证失败
- Cisco Bug ID [CSCuj19601](#) - ASA Webvpn KCD — 仅在重新启动后尝试加入AD
- Cisco Bug ID [CSCuh32106](#) - ASA KCD在8.4.5后断开

相关信息

- [关于Kerberos约束委派](#)
- [了解KCD的工作原理](#)
- [PIX/ASA：通过ASDM/CLI为VPN客户端用户配置的Kerberos身份验证和LDAP授权服务器组配置示例](#)
- [Cisco ASA系列命令参考](#)
- [尝试约束委派时的KDC_ERR_BAPPOTION](#)
- [如何在Windows中强制Kerberos使用TCP而不是UDP](#)
- [技术支持和文档 - Cisco Systems](#)