WebVPN SSO와 Kerberos 제한 위임 구성 통합 예

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[ASA와의 Kerberos 상호 작용](#)
[구성](#)
[토폴로지](#)
[도메인 컨트롤러 및 애플리케이션 구성](#)
[도메인 설정](#)
[SPN(서비스 사용자 이름) 설정](#)
[ASA의 컨피그레이션](#)
[다음을 확인합니다.](#)
[ASA가 도메인에 가입함](#)
[서비스 요청](#)
[문제 해결](#)
[Cisco 버그 ID](#)
[관련 정보](#)

소개

이 문서에서는 Kerberos로 보호되는 애플리케이션에 대해 WebVPN SSO(Single Sign On)를 구성하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- Cisco ASA(Adaptive Security Appliance) CLI 컨피그레이션 및 SSL(Secure Socket Layer) VPN 컨피그레이션
- Kerberos 서비스

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco ASA 소프트웨어 버전 9.0 이상
- Microsoft Windows 7 클라이언트
- Microsoft Windows 2003 Server 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Kerberos는 네트워크 엔티티가 안전한 방식으로 상호 인증할 수 있도록 하는 네트워크 인증 프로토콜입니다.신뢰할 수 있는 서드파티인 KDC(Key Distribution Center)를 사용하여 네트워크 엔터티에 티켓을 부여합니다.이러한 티켓은 엔티티가 요청한 서비스에 대한 액세스를 확인하고 확인하기 위해 사용합니다.

Kerberos로 보호되는 애플리케이션에 대해 KCD(Kerberos Constrained Delegation)라는 Cisco ASA 기능을 사용하여 WebVPN SSO를 구성할 수 있습니다. 이 기능을 사용하면 ASA는 WebVPN 포털 사용자 대신 Kerberos 티켓을 요청할 수 있으며 Kerberos로 보호되는 애플리케이션에 액세스할 수 있습니다.

WebVPN 포털을 통해 이러한 애플리케이션에 액세스할 때 더 이상 자격 증명을 제공할 필요가 없습니다.대신 WebVPN 포털에 로그인하기 위해 사용한 계정이 사용됩니다.

자세한 내용은 ASA 컨피그레이션 가이드의 KCD 작동 방식 이해 섹션을 참조하십시오.

ASA와의 Kerberos 상호 작용

WebVPN의 경우 WebVPN 포털 사용자는 Kerberos 서비스가 아니라 포털에 대한 액세스 권한을 가지므로 ASA는 사용자를 대신하여 티켓을 요청해야 합니다. 이를 위해 ASA는 Constrained Delegation에 Kerberos 확장을 사용합니다.플로우는 다음과 같습니다.

1. ASA는 도메인에 가입하고 ASA(kcd-server 명령)에 구성된 자격 증명을 사용하여 컴퓨터 계정에 대한 티켓(Ticket1)을 가져옵니다. 이 티켓은 Kerberos 서비스에 액세스하기 위한 다음 단계에서 사용됩니다.

2. 사용자는 Kerberos 보호 애플리케이션에 대한 WebVPN 포털 링크를 클릭합니다.

3. ASA 요청(TGS-REQ)은 호스트 이름을 주도자로 가진 컴퓨터 계정에 대한 티켓을 요청합니다.이 요청에는 PA-TGS-REQ 필드와 주도자가 WebVPN 포털 사용자 이름인 PA-FOR-USER가 포함됩니다. 이 경우는 cisco입니다.1단계의 Kerberos 서비스 티켓은 인증(올바른 위임)에 사용됩니다.

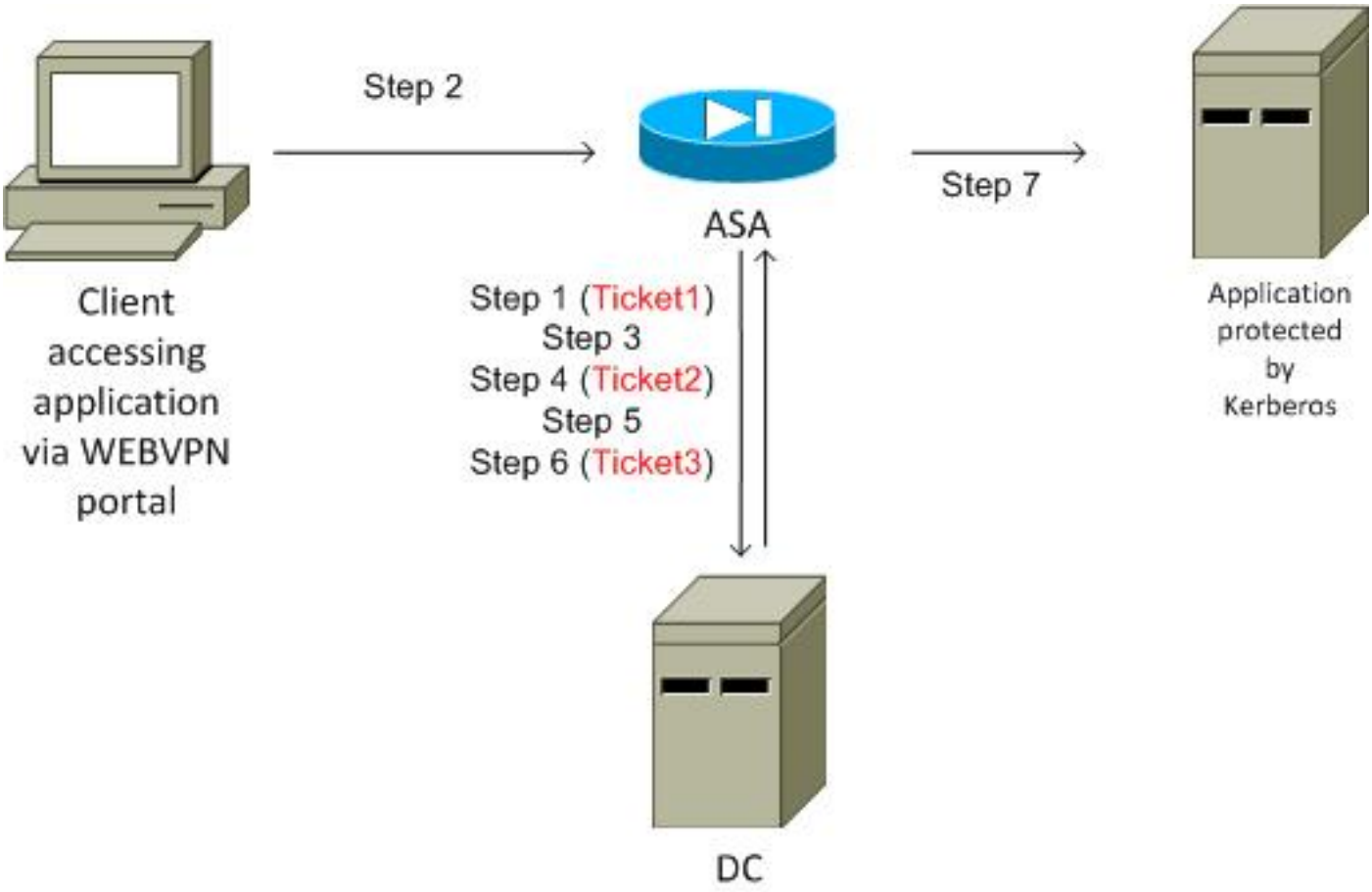
4. 응답으로 ASA는 컴퓨터 계정에 대해 WebVPN 사용자(TGS_REP) 대신 가장된 티켓(Ticket2)을 받습니다.이 티켓은 이 WebVPN 사용자를 대신하여 애플리케이션 티켓을 요청하

기 위해 사용됩니다.

5. ASA는 애플리케이션에 대한 티켓(HTTP/test.kra-**sec.cisco.com**)을 얻기 위해 다른 요청(**TGS_REQ**)을 시작합니다. 이 요청은 다시 **PA-TGS-REQ** 필드**를** 사용하는데, 이번에는 **PA-FOR-USER** 필드가 없지만 단계 4에서 가장된 티켓이 사용됩니다.

6. 애플리케이션에 대해 가장된 티켓(Ticket3)**과** 함께 응답(TGS_REQ)이 반환됩니다.

7. 이 티켓은 ASA에서 보호 서비스에 액세스하기 위해 투명하게 사용되며 WebVPN 사용자는 자격 증명을 입력할 필요가 없습니다.HTTP 애플리케이션의 경우 인증 방법을 협상하기 위해 SPNEGO(Simple and Protected GSS-API Negotiation) 메커니즘이 사용되며 ASA에서 올바른 티켓을 전달합니다.



구성

토폴로지

도메인:kra-sec.cisco.com(10.211.0.221 또는 10.211.0.216)

IIS(인터넷 정보 서비스) 7 응용 프로그램:test.kra-sec.cisco.com(10.211.0.223)

도메인 컨트롤러(DC):dc.kra-sec.cisco.com(10.211.0.221 또는 10.211.0.216) - Windows2008

ASA:10.211.0.162

WebVPN 사용자 이름/비밀번호:cisco/cisco

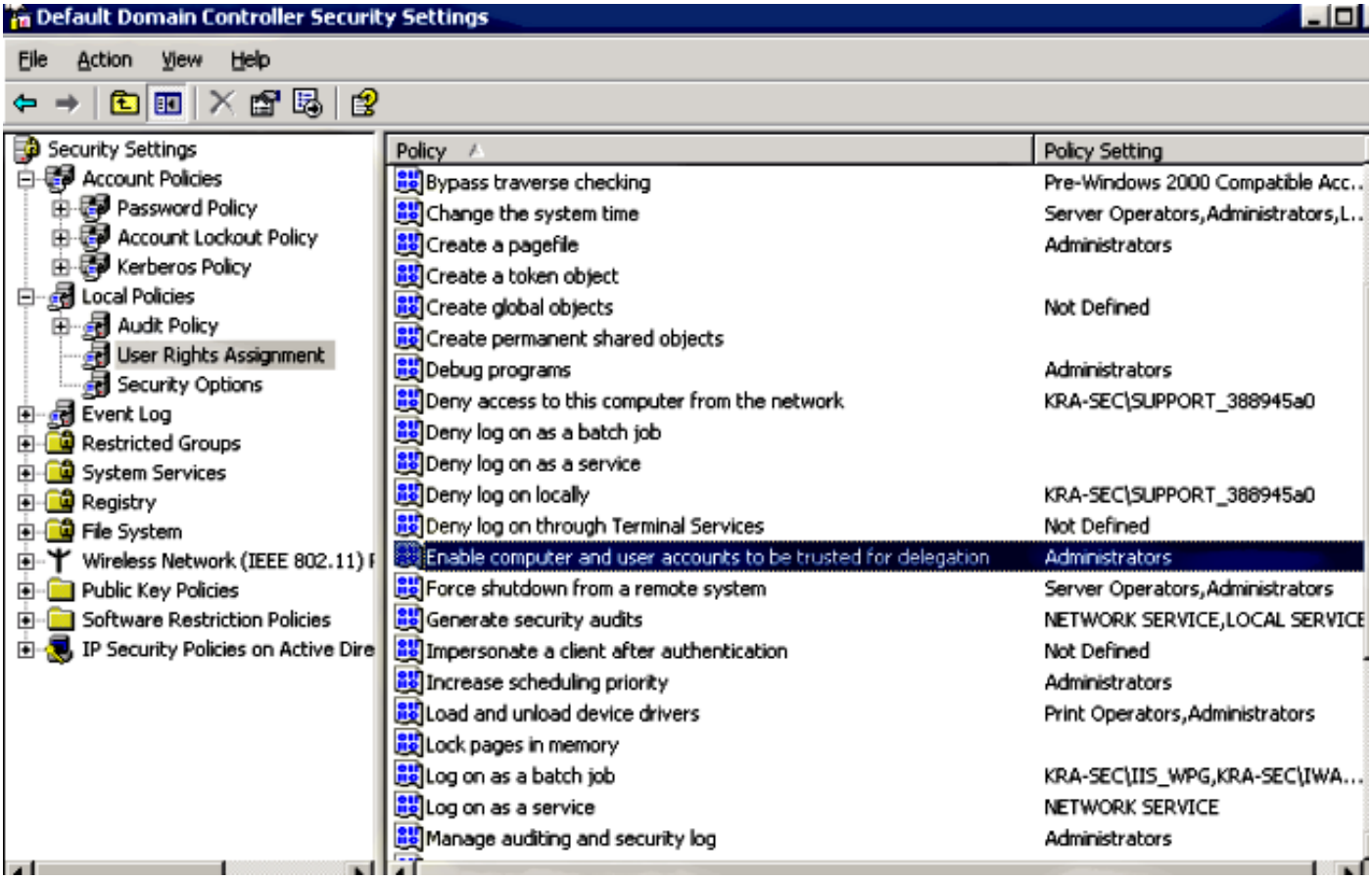
첨부 파일:asa-join.pcap(도메인에 성공적으로 가입)

첨부 파일:asa-kerberos-bad.pcap(서비스 요청)

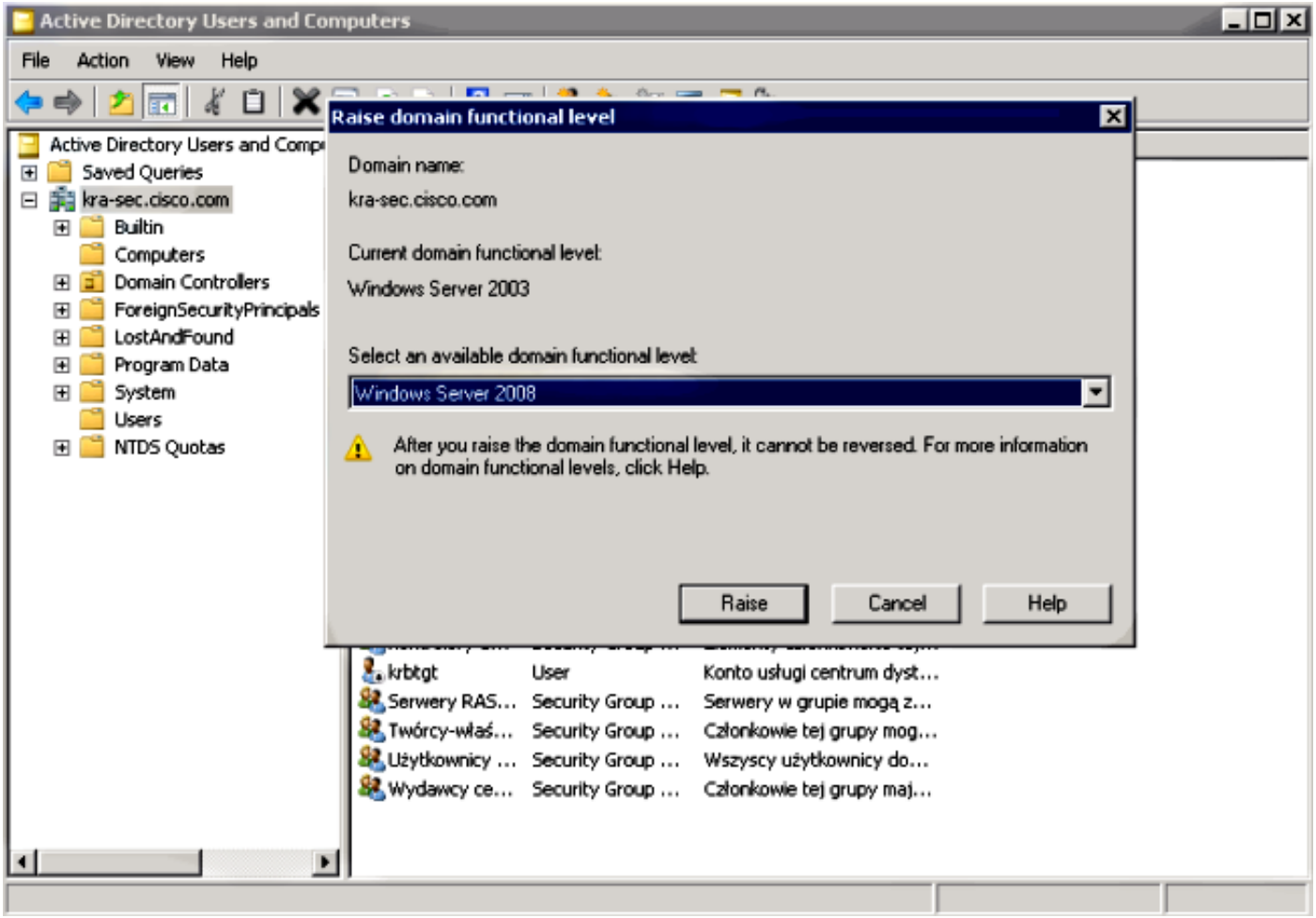
도메인 컨트롤러 및 애플리케이션 구성

도메인 설정

Kerberos로 보호되는 기능 IIS7 응용 프로그램이 이미 있다고 가정합니다(그렇지 않은 경우 필수 구성 요소 섹션을 읽으십시오). 사용자 위임을 위한 설정을 확인해야 합니다.



기능 도메인 수준이 Windows Server 2003(최소)으로 올라가야 합니다. 기본값은 Windows Server 2000입니다.



SPN(서비스 사용자 이름) 설정

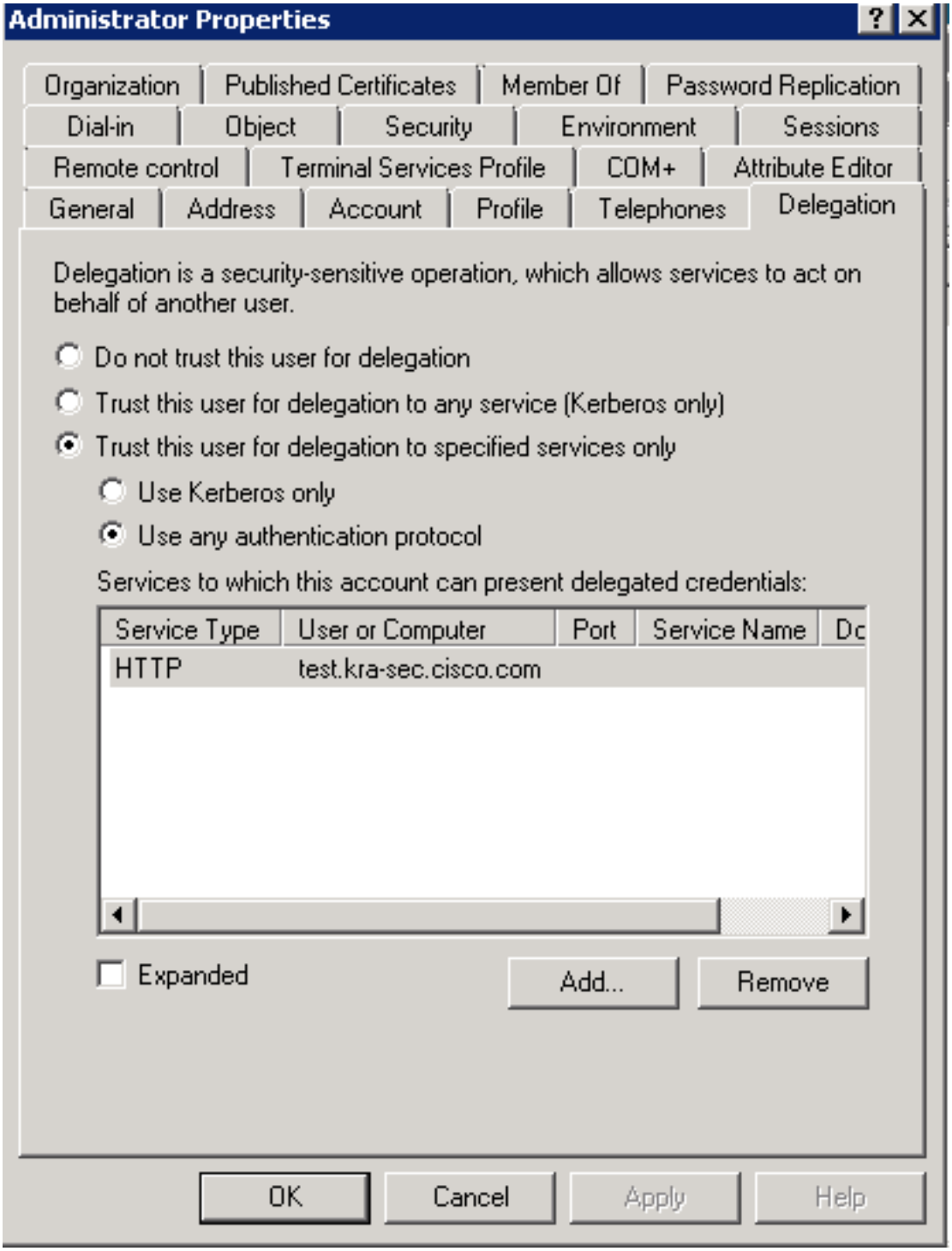
올바른 위임으로 AD의 모든 계정을 구성해야 합니다.관리자 계정이 사용됩니다.ASA가 해당 계정을 사용하는 경우 특정 서비스(HTTP 애플리케이션)에 대해 다른 사용자(Constrained Delegation)를 대신하여 티켓을 요청할 수 있습니다. 이 문제가 발생하려면 애플리케이션/서비스에 대해 올바른 위임을 만들어야 합니다.

Windows Server 2003 서비스 팩 1 지원 도구의 일부인 setspn.**exe**를 사용하여 CLI를 통해 이 위임을 수행하려면 다음 명령을 입력합니다.

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

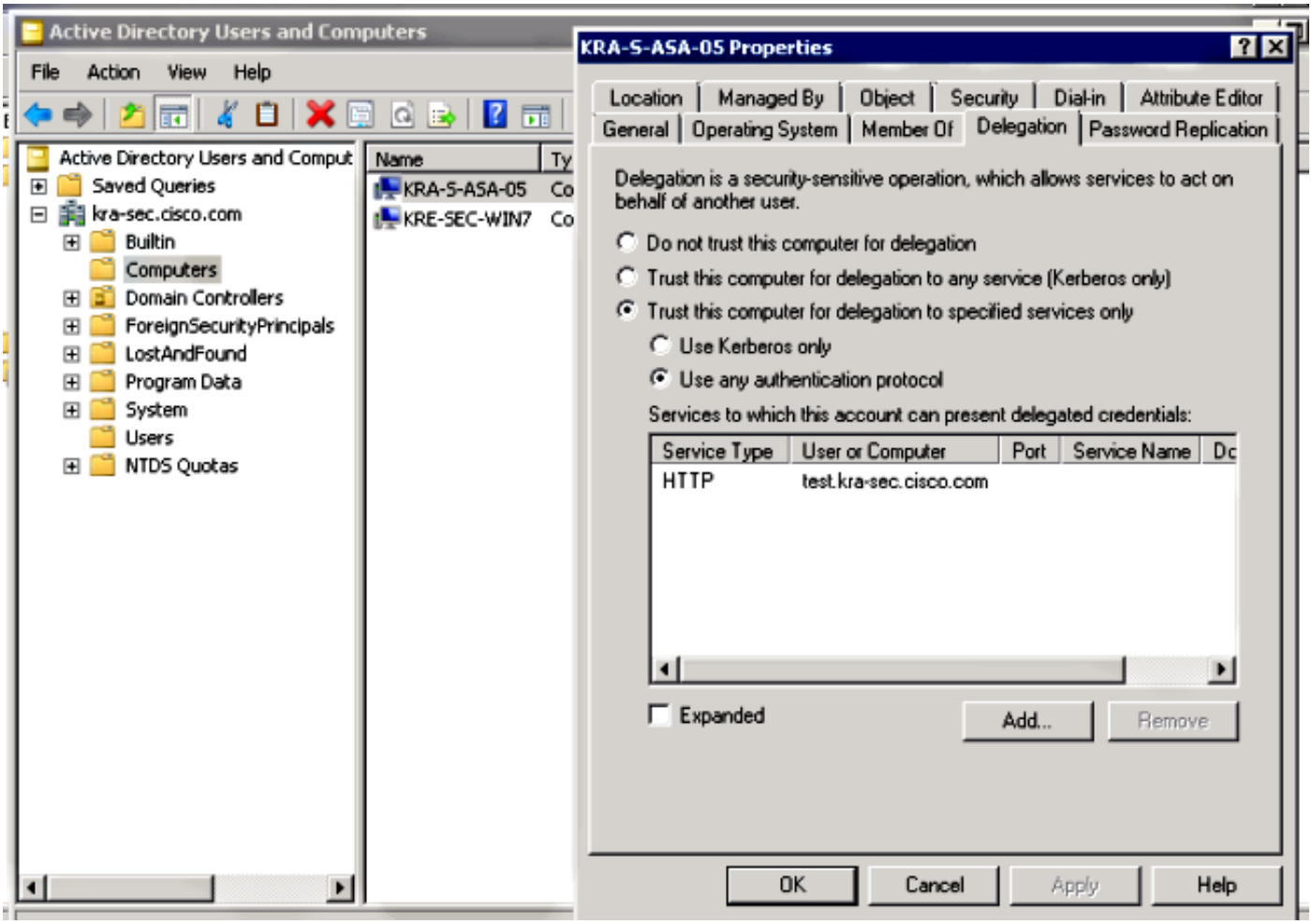
이는 **Administrator** 사용자 이름이 **test.kra-sec.cisco.com**에서 HTTP 서비스 위임을 위한 신뢰할 수 있는 계정임을 나타냅니다.

SPN 명령**은** 해당 사용자의 **위임** 탭을 활성화하려면 필요합니다.명령을 입력하면 관리자의 위임 탭이 나타납니다."Use any authentication protocol(모든 인증 프로토콜 사용)"은 제한된 위임 확장을 지원하지 않으므로 활성화해야 합니다.



General 탭에서 Kerberos 사전 인증을 비활성화할 수도 있습니다.그러나 이 기능은 재생 공격으로부터 DC를 보호하기 위해 사용되므로 권장되지 않습니다.ASA는 사전 인증과 올바르게 작동할 수 있습니다.

이 절차는 컴퓨터 계정에 대한 위임에도 적용됩니다(ASA는 "신뢰" 관계를 설정하기 위해 도메인으로 가져오기).



ASA의 컨피그레이션

```
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
```

다음을 확인합니다.

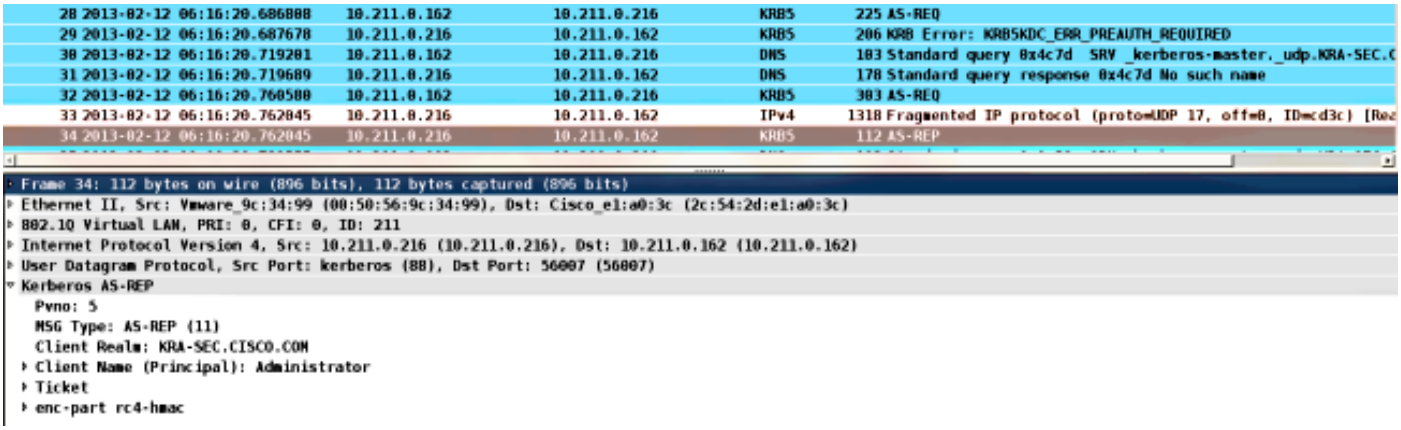
ASA가 도메인에 가입함

kcd-server 명령을 사용한 후 ASA는 도메인 가입을 시도합니다.

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

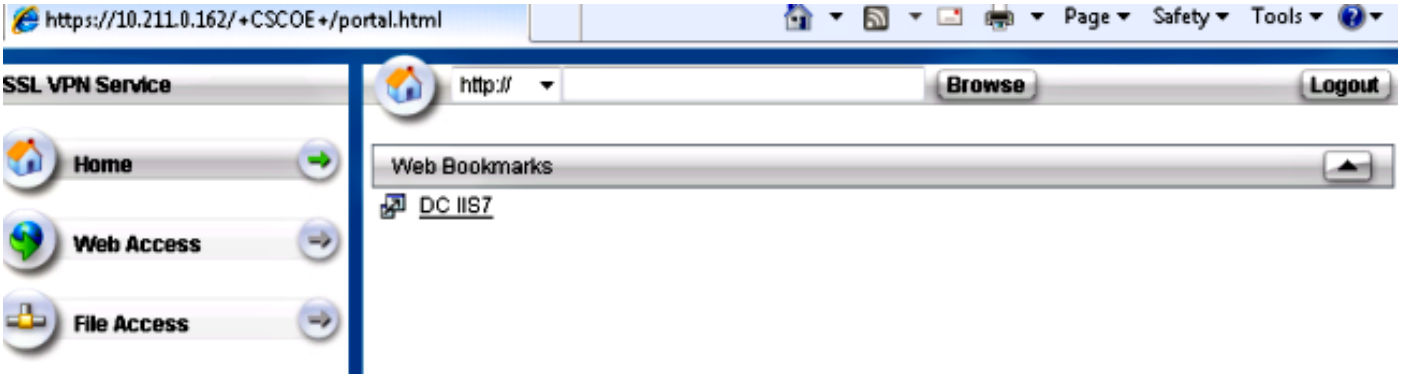
```
Kerberos: Server Name krbtgt
Kerberos: Start time 0
Kerberos: End time -878667256
Kerberos: Renew until time -878672192
Kerberos: Nonce 0xa9db408e
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4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

ASA가 도메인에 성공적으로 가입할 수 있습니다.올바른 인증 후 ASA는 주도자에 대한 티켓을 받습니다.AS_REP 패킷의 관리자(1단계에서 설명한 티켓1).

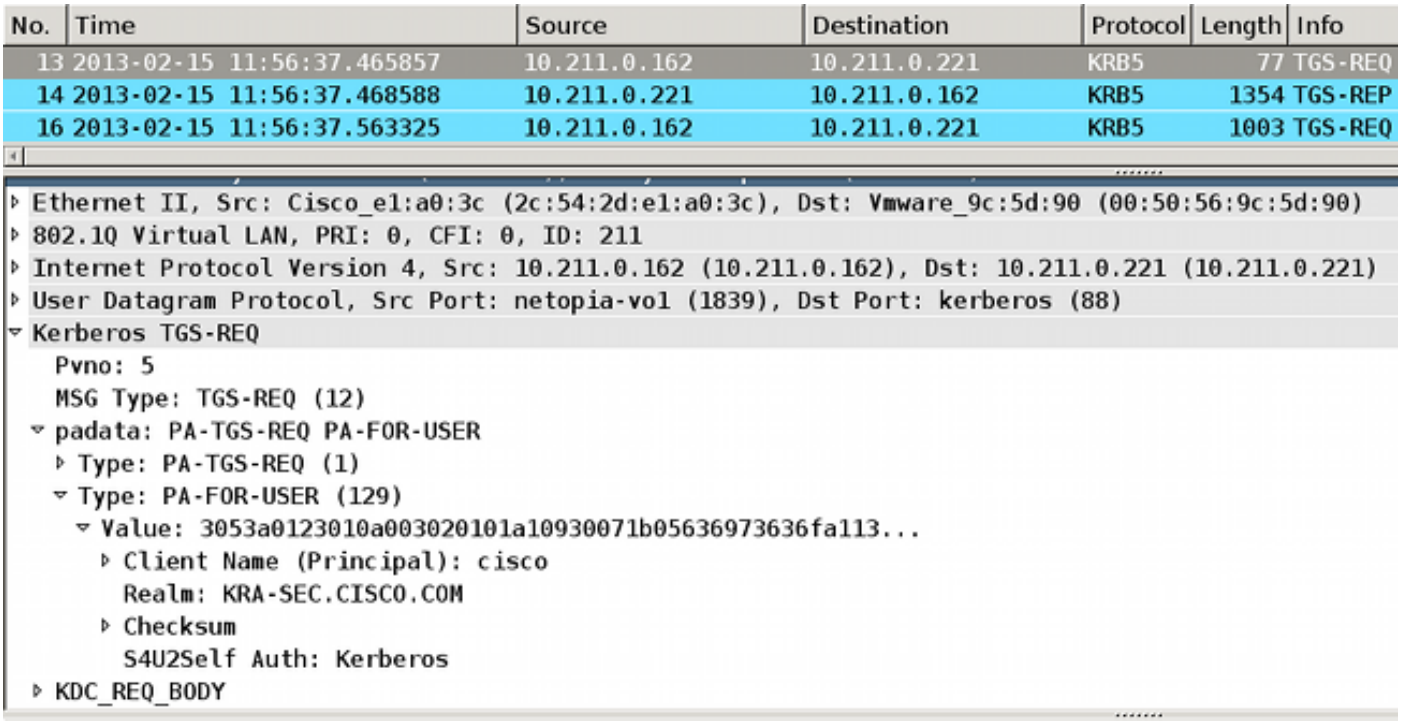


서비스 요청

사용자가 WebVPN 링크를 클릭합니다.

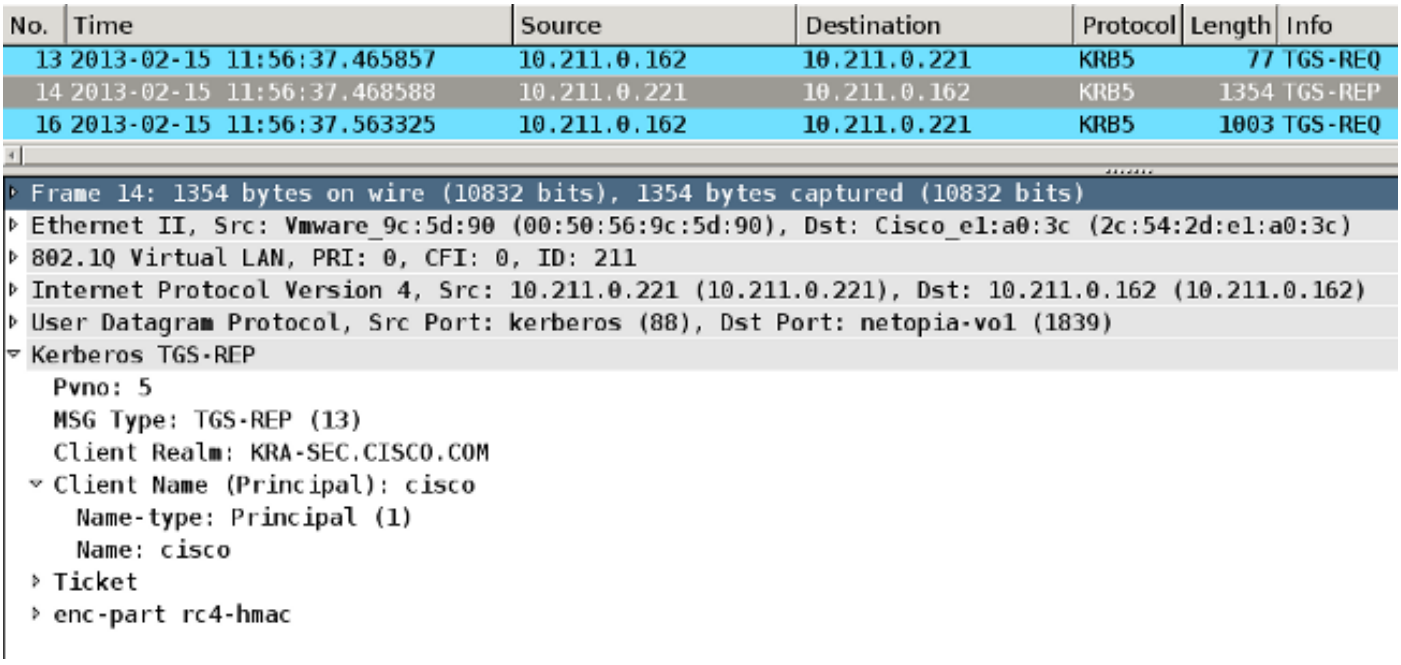


ASA는 AS_REP 패킷에서 수신되는 티켓과 함께 가장된 티켓에 대해 TGS_REQ를 전송합니다.



참고:PA-FOR-USER 값은 **cisco**(WebVPN 사용자)입니다.**PA-TGS-REQ**에는 Kerberos 서비스 요청에 대해 수신된 티켓이 포함되어 있습니다(ASA 호스트 이름은 주도자).

ASA는 사용자 **cisco**에 대해 가장된 티켓과 함께 올바른 응답을 받습니다(4단계에서 설명한 Ticket2).



다음은 HTTP 서비스에 대한 티켓 요청입니다(일부 디버그는 명확성을 위해 생략됨).

```
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
```

ASA는 HTTP 서비스에 대해 올바른 가장된 티켓을 받습니다(6단계에서 설명한 Ticket3).

두 티켓 모두 확인할 수 있습니다.첫 번째는 사용자 cisco에 대한 가장된 티켓입니다. 이는 액세스되는 HTTP 서비스에 대한 두 번째 티켓을 요청하고 받기 위해 사용됩니다.

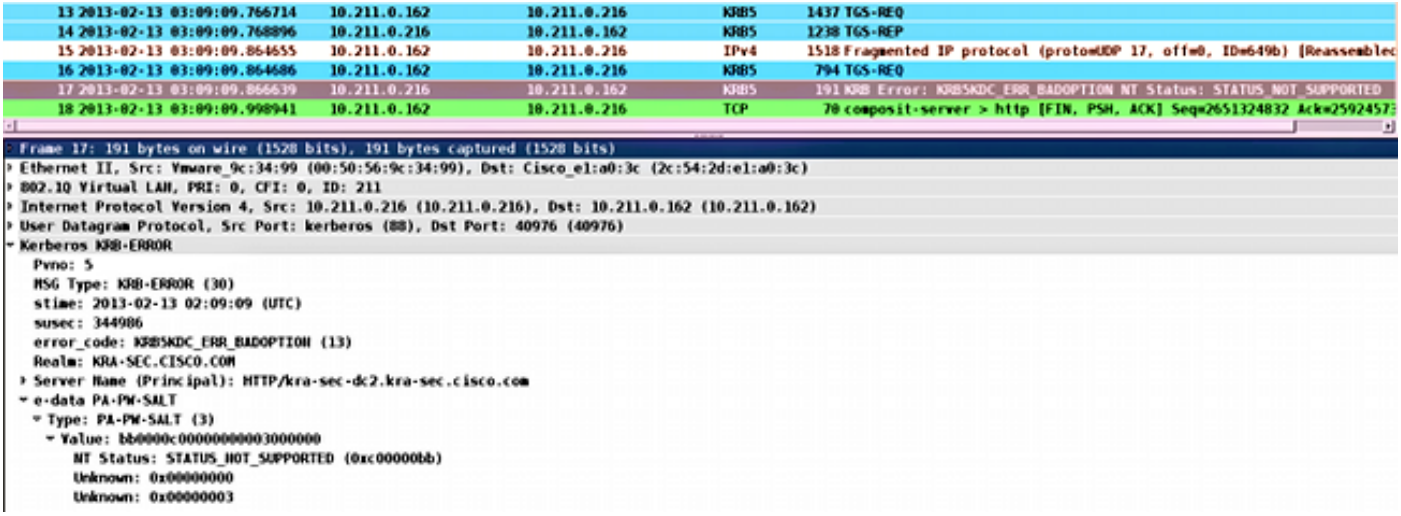
```
KRA-S-ASA-05(config)# show aaa kerberos
Default Principal: cisco@KRA-SEC.CISCO.COM
Valid Starting       Expires              Service Principal
19:38:10 CEST Oct 2 2013 05:37:33 CEST Oct 3 2013 KRA-S-ASA-05@KRA-SEC.CISCO.COM
```

```
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
```

이 HTTP 티켓(Ticket3)은 HTTP 액세스(SPNEGO 사용)에 사용되며 사용자가 어떤 자격 증명도 제공할 필요가 없습니다.

문제 해결

가끔 잘못된 위임 문제가 발생할 수 있습니다.예를 들어, ASA는 HTTP/test.kra-sec.cisco.com(5단계) 서비스를 요청하기 위해 티켓을 사용하지만, 응답은 ERR_BADOPTION과 함께 KRB-ERROR입니다.



위임이 올바르게 구성되지 않은 경우 발생하는 일반적인 문제입니다.ASA에서는 **"KDC가 요청된 옵션을 이행할 수 없음"이라고 보고합니다**.

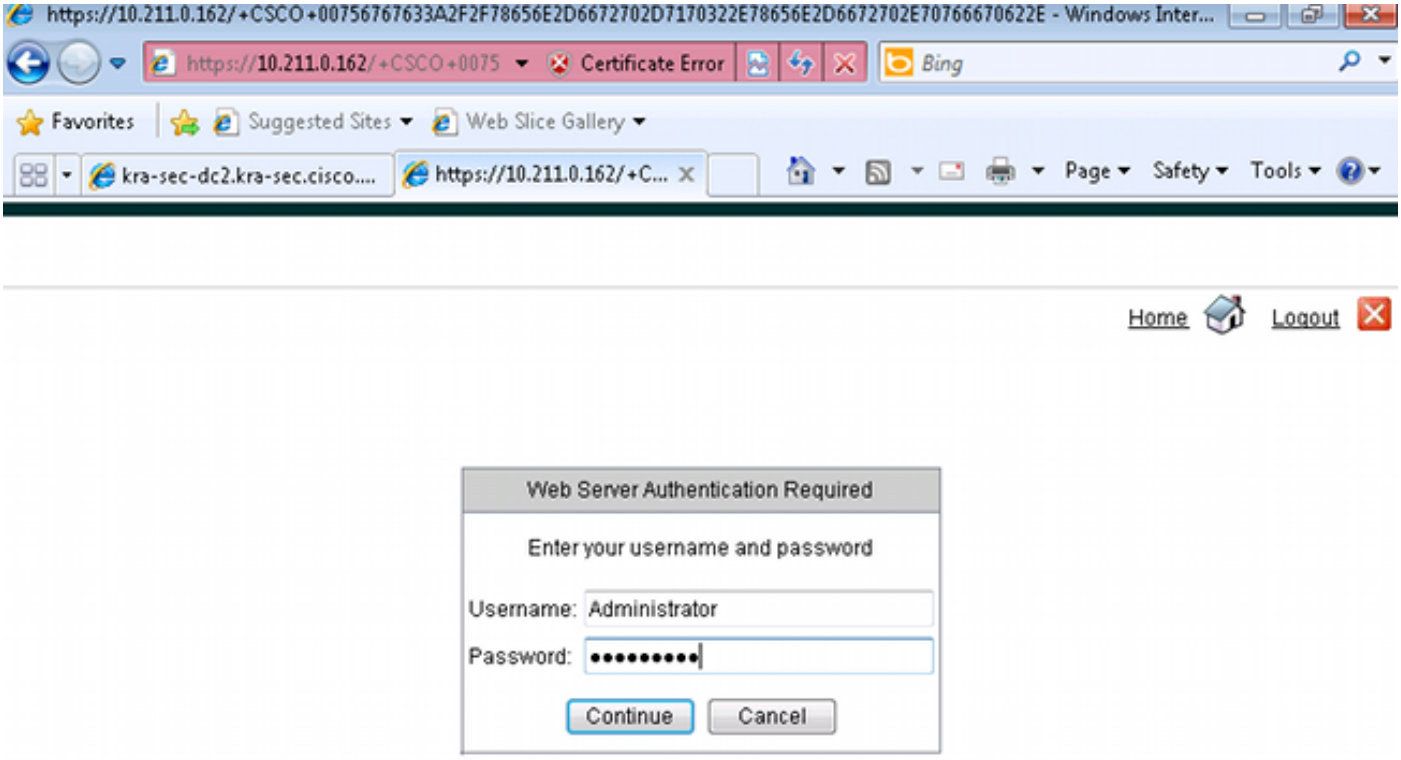
```
KRA-S-ASA-05# ucte_krb_get_auth_cred(): ctx = 0xcc4b5390,
WebVPN_session = 0xc919a260, protocol = 1
find_spn_in_url(): URL - /
build_host_spn(): host - test.kra-sec.cisco.com
build_host_spn(): SPN - HTTP/test.kra-sec.cisco.com
KCD_unicorn_get_cred(): Attempting to retrieve required KCD tickets.
In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

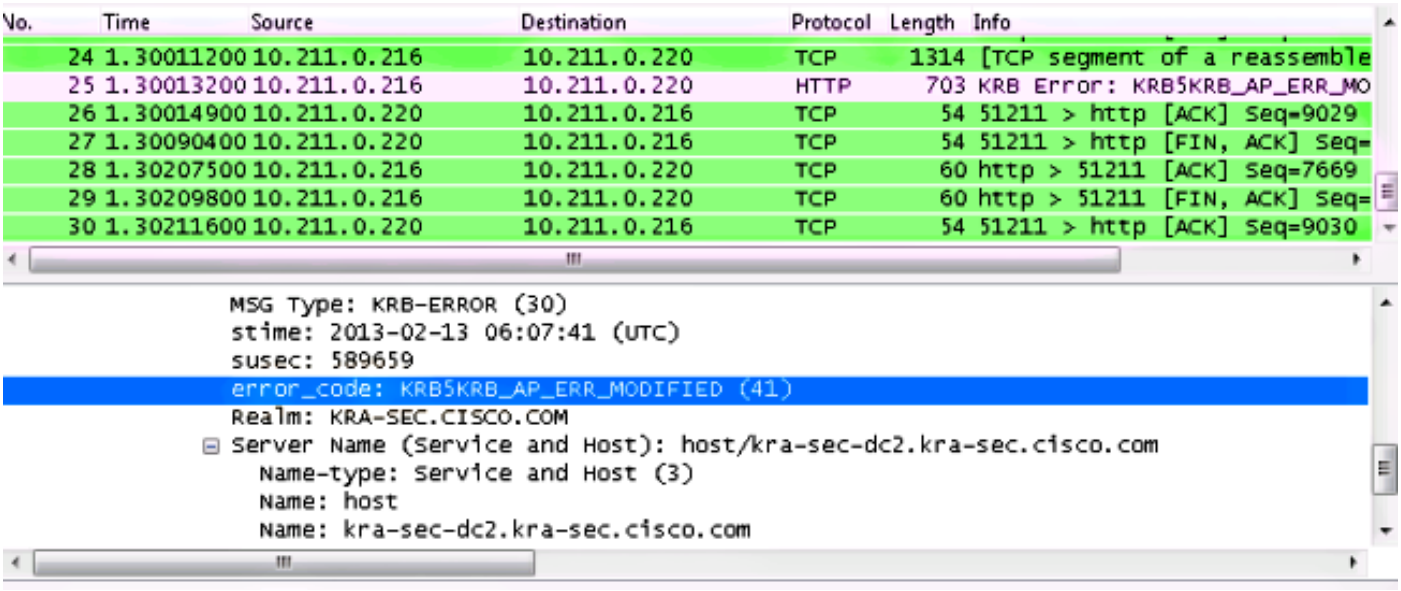
이는 기본적으로 캡처에서 설명하는 것과 동일한 문제입니다. BAD_OPTION을 사용하는 **TGS_REQ에 오류가 있습니다**.

응답이 **Success**이면 ASA는 SPNEGO 협상에 사용되는 HTTP/test.kra**-sec.cisco.com** 서비스에 대한 티켓**을** 받습니다.그러나 장애로 인해 NTLM**(NT LAN Manager)**이 협상되고 사용자는 다음 자격 증명을 제공해야 합니다.

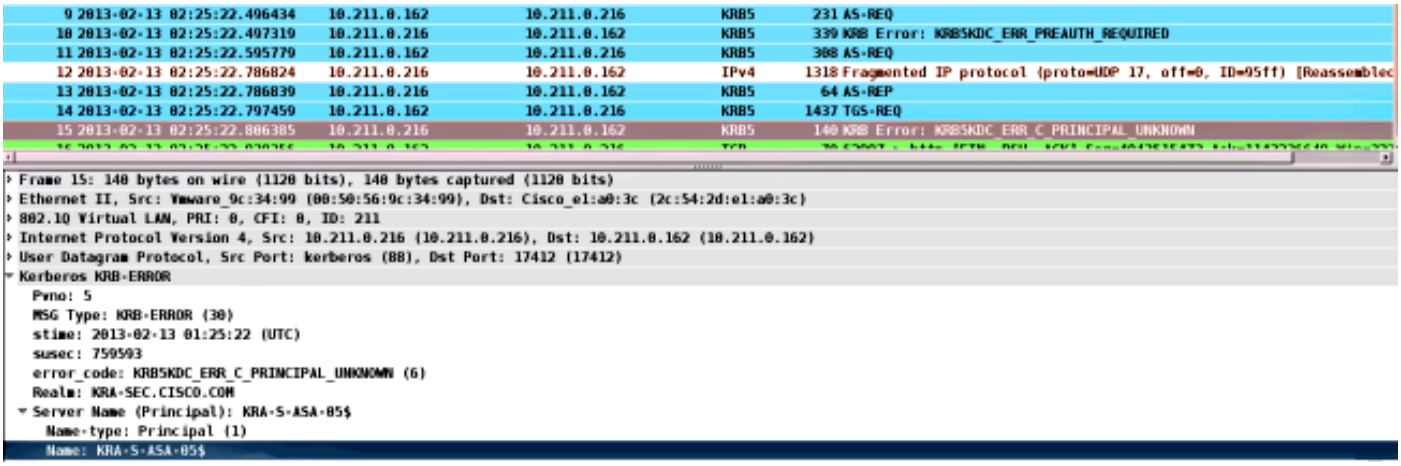


SPN이 하나의 계정에만 등록되어 있는지 확인하십시오(이전 문서의 스크립트). 이 오류(KRB_AP_ERR_MODIFIED)가 표시되면 일반적으로 **SPN**이 올바른 계정에 등록되지 않았음을 의미합니다.응용 프로그램(IIS의 응용 프로그램 풀)을 실행하기 위해 사용되는 계정에 등록해야 합니

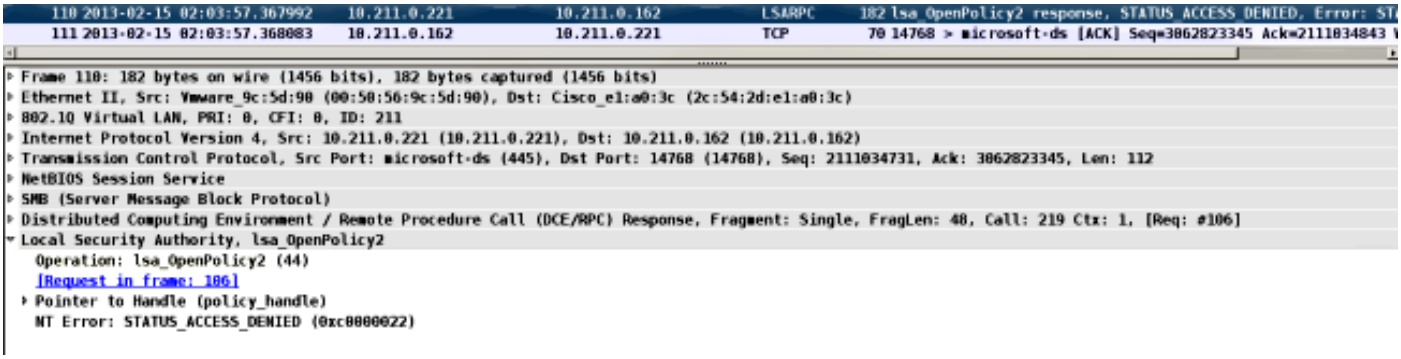
다.



이 오류(KRB_**ERR_C_PRINCIPAL_UNKNOWN)가** 표시되면 DC(WebVPN 사용자:**cisco**)를 선택합니다.



도메인에 가입하면 이 문제가 발생할 수 있습니다.ASA는 **AS-REP**를 수신하지만 **LSA** 레벨에서 다음 오류로 실패합니다.**STATUS_ACCESS_DENIED**:



이 문제를 해결하려면 해당 사용자의 DC에서 사전 인증을 활성화/비활성화해야 합니다(**관리자**).

다음과 같은 다른 문제가 발생할 수 있습니다.

- 도메인에 가입할 때 문제가 있을 수 있습니다.DC 서버에 여러 NIC(Network Interface Controller) 어댑터(여러 IP 주소)가 있는 경우 ASA가 도메인에 가입하기 위해 모든 어댑터에 액

세스할 수 있는지 확인합니다(DNS(Domain Name Server) 응답을 기반으로 클라이언트가 임의로 선택).

- **관리자** 계정에 대해 **SPN**을 HOST/dc.kra-**sec.cisco.com**으로 설정하지 마십시오.이 설정으로 인해 DC와의 연결이 끊어질 수 있습니다.
- ASA가 도메인에 가입하면 올바른 컴퓨터 계정이 DC(ASA 호스트 이름)에 생성되었는지 확인할 수 있습니다. 컴퓨터 계정을 추가하려면 사용자에게 올바른 권한이 있는지 확인합니다(이 예에서는 **관리자**가 올바른 권한을 가지고 있음).
- ASA에서 올바른 **NTP(Network Time Protocol)** 컨피그레이션을 기억하십시오.기본적으로 DC는 5분 클럭 기울기를 허용합니다.DC에서 타이머를 변경할 수 있습니다.
- 소형 패킷 **UDP/88**에 대한 Kerberos 연결**이** 사용되는지 확인합니다.DC, KRB**5KDC_ERR_RESPONSE_TOO_BIG**의 오류 후 클라이언트는 **TCP/88**로 전환됩니다. Windows 클라이언트가 **TCP/88**을 사용하도록 강제할 수 있지만 **ASA는 기본적으로 UDP를 사용합니다**.
- DC:정책을 변경할 때 gpupdate **/force를** 기억하십시오.
- ASA:**test aaa** 명령을 사용하여 인증을 테스트하지만 단순 인증일 뿐입니다.
- DC 사이트에서 문제를 해결하려면 Kerberos 디버그를 활성화하는 것이 좋습니다.Kerberos 이벤트 로깅을 활성화하는 방법.

Cisco 버그 ID

다음은 관련 Cisco 버그 ID 목록입니다.

- Cisco 버그 ID CSCsi32224 - Kerberos 오류 코드 52를 수신한 후 ASA가 TCP로 전환되지 않습니다.
- Cisco 버그 ID CSCtd92673 - 사전 인증이 활성화되면 Kerberos 인증이 실패합니다.
- Cisco 버그 ID CSCuj19601 - ASA Webvpn KCD - 재부팅 후에만 AD에 가입하려고 합니다.
- Cisco 버그 ID CSCuh32106 - ASA KCD가 8.4.5으로 중단됨

관련 정보

- Kerberos 제한 위임 정보
- KCD 작동 방식 이해
- PIX/ASA:ASDM/CLI 컨피그레이션을 통해 VPN 클라이언트 사용자를 위한 Kerberos 인증 및 LDAP 권한 부여 서버 그룹 예
- Cisco ASA Series 명령 참조
- 제한된 위임을 시도할 때 KDC_ERR_BADOPTION
- Windows에서 Kerberos가 UDP 대신 TCP를 사용하도록 하는 방법
- 기술 지원 및 문서 – Cisco Systems