Exemple de configuration de l'intégration SSO WebVPN avec délégation contrainte Kerberos

Contenu

Introduction

Ce document décrit comment configurer et dépanner WebVPN Single Sign On (SSO) pour les applications protégées par Kerberos.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration CLI de l'appliance de sécurité adaptative (ASA) Cisco et configuration VPN SSL (Secure Socket Layer)
- Services Kerberos

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Logiciel Cisco ASA, versions 9.0 et ultérieures
- Client Microsoft Windows 7
- Microsoft Windows 2003 Server et versions ultérieures

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.

Informations générales

Kerberos est un protocole d'authentification réseau qui permet aux entités réseau de s'authentifier mutuellement de manière sécurisée. Il utilise un tiers de confiance, le Key Distribution Center (KDC), qui accorde des tickets aux entités réseau. Ces tickets sont utilisés par les entités afin de vérifier et de confirmer l'accès au service demandé.

Il est possible de configurer WebVPN SSO pour les applications qui sont protégées par Kerberos avec la fonctionnalité Cisco ASA appelée KCD (Kerberos Constrned Delegated Délégation). Grâce à cette fonctionnalité, l'ASA peut demander des tickets Kerberos au nom de l'utilisateur du portail WebVPN, tout en accédant aux applications protégées par Kerberos.

Lorsque vous accédez à de telles applications via le portail WebVPN, vous n'avez plus besoin de fournir d'informations d'identification ; au lieu de cela, le compte utilisé pour se connecter au portail WebVPN est utilisé.

Référez-vous à la section Comprendre comment fonctionne KCD du guide de configuration ASA pour plus d'informations.

Interaction Kerberos avec l'ASA

Pour WebVPN, l'ASA doit demander des tickets au nom de l'utilisateur (car l'utilisateur du portail WebVPN a accès uniquement au portail, et non au service Kerberos). Pour cela, l'ASA utilise les extensions Kerberos pour la délégation limitée. Voici le flux :

1. L'ASA rejoint le domaine et obtient un ticket (ticket1) pour un compte d'ordinateur avec des informations d'identification configurées sur l'ASA (commande **kcd-server**). Ce ticket est utilisé dans les étapes suivantes pour l'accès aux services Kerberos.

2. L'utilisateur clique sur le lien du portail WebVPN pour l'application protégée par Kerberos.

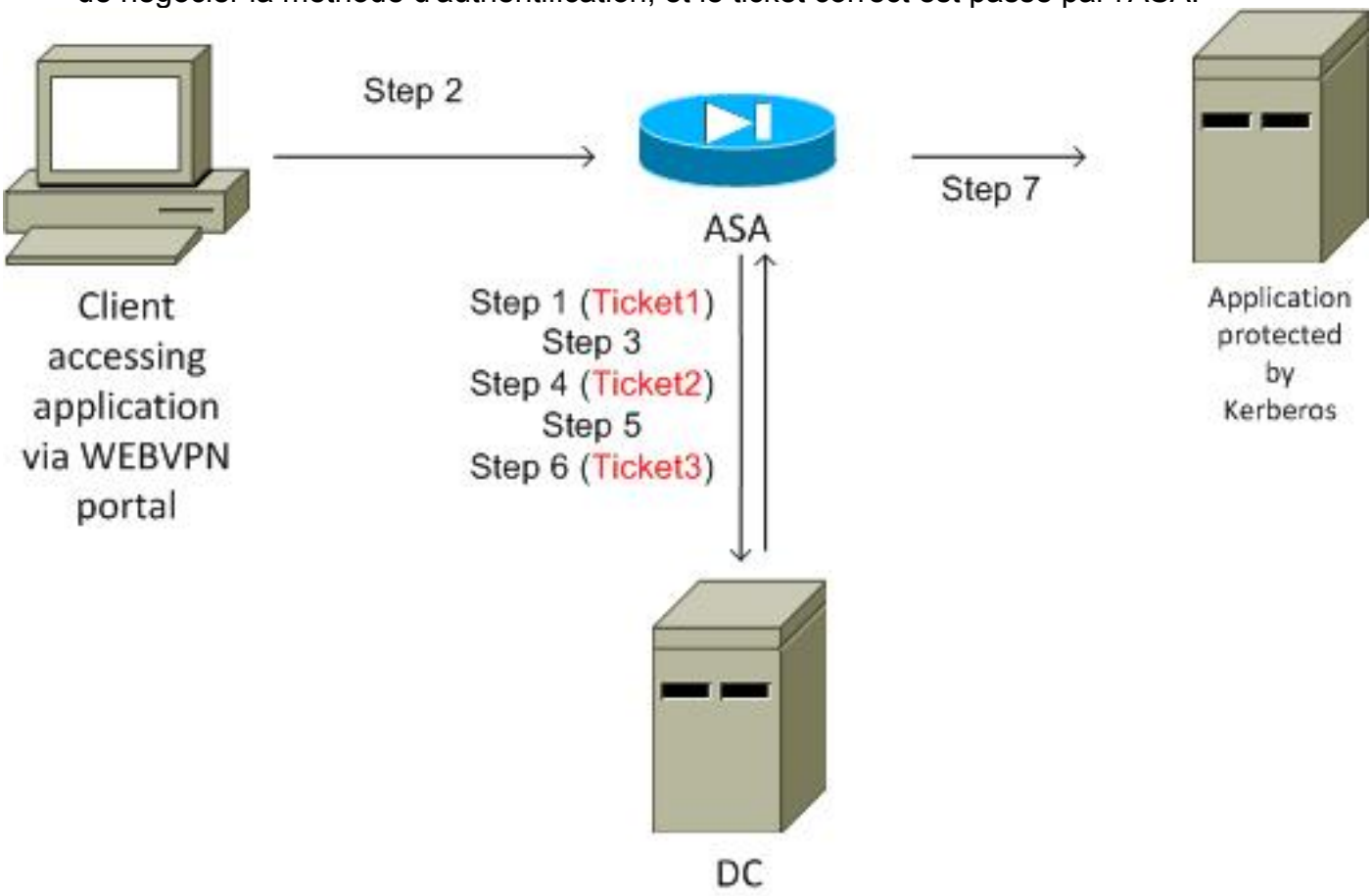
3. L'ASA demande (**TGS-REQ**) un ticket pour le compte d'ordinateur avec son nom d'hôte comme principal. Cette demande inclut le champ **PA-TGS-REQ** avec **PA-FOR-USER** avec le principal comme nom d'utilisateur du portail WebVPN, qui est **cisco** dans ce scénario. Le ticket pour le service Kerberos de l'étape 1 est utilisé pour l'authentification (délégation correcte).

4. En réponse, l'ASA reçoit un ticket usurpé (Billet 2) au nom de l'utilisateur WebVPN (**TGS_REP**) pour le compte d'ordinateur. Ce ticket est utilisé afin de demander des tickets d'application pour le compte de cet utilisateur WebVPN.

5. L'ASA lance une autre demande (**TGS_REQ**) afin d'obtenir le ticket pour l'application (**HTTP/test.kra-sec.cisco.com**). Cette demande utilise à nouveau le champ **PA-TGS-REQ**, cette fois **sans le** champ **PA-FOR-USER**, mais avec le ticket usurpé reçu à l'étape 4.

6. La réponse (**TGS_REQ**) avec le ticket usurpé (Ticket3) pour l'application est retournée.

7. Ce ticket est utilisé de manière transparente par l'ASA afin d'accéder au service protégé, et l'utilisateur WebVPN n'a pas besoin d'entrer d'informations d'identification. Pour l'application HTTP, le mécanisme SPNEGO (Simple and Protected GSS-API Negotiation) est utilisé afin de négocier la méthode d'authentification, et le ticket correct est passé par l'ASA.



Configuration

Topologie

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

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

Contrôleur de domaine (DC) : dc.kra-sec.cisco.com (10.211.0.221 ou 10.211.0.216) -

Windows2008

ASA : 10.211.0.162

Nom d'utilisateur/mot de passe WebVPN : cisco/cisco

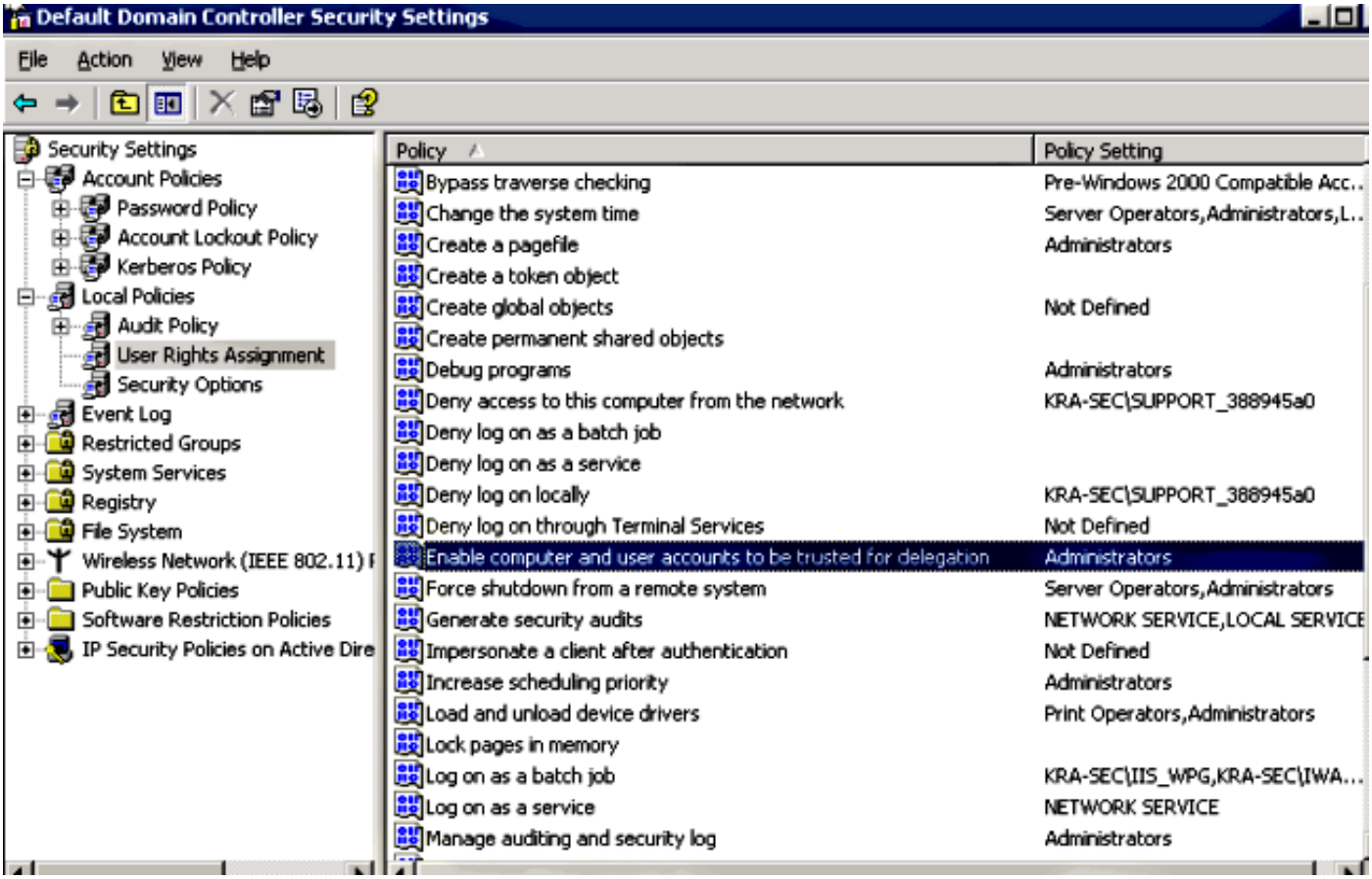
Fichier joint : asa-join.pcap (jointure réussie vers le domaine)

Fichier joint : asa-kerberos-bad.pcap (demande de service)

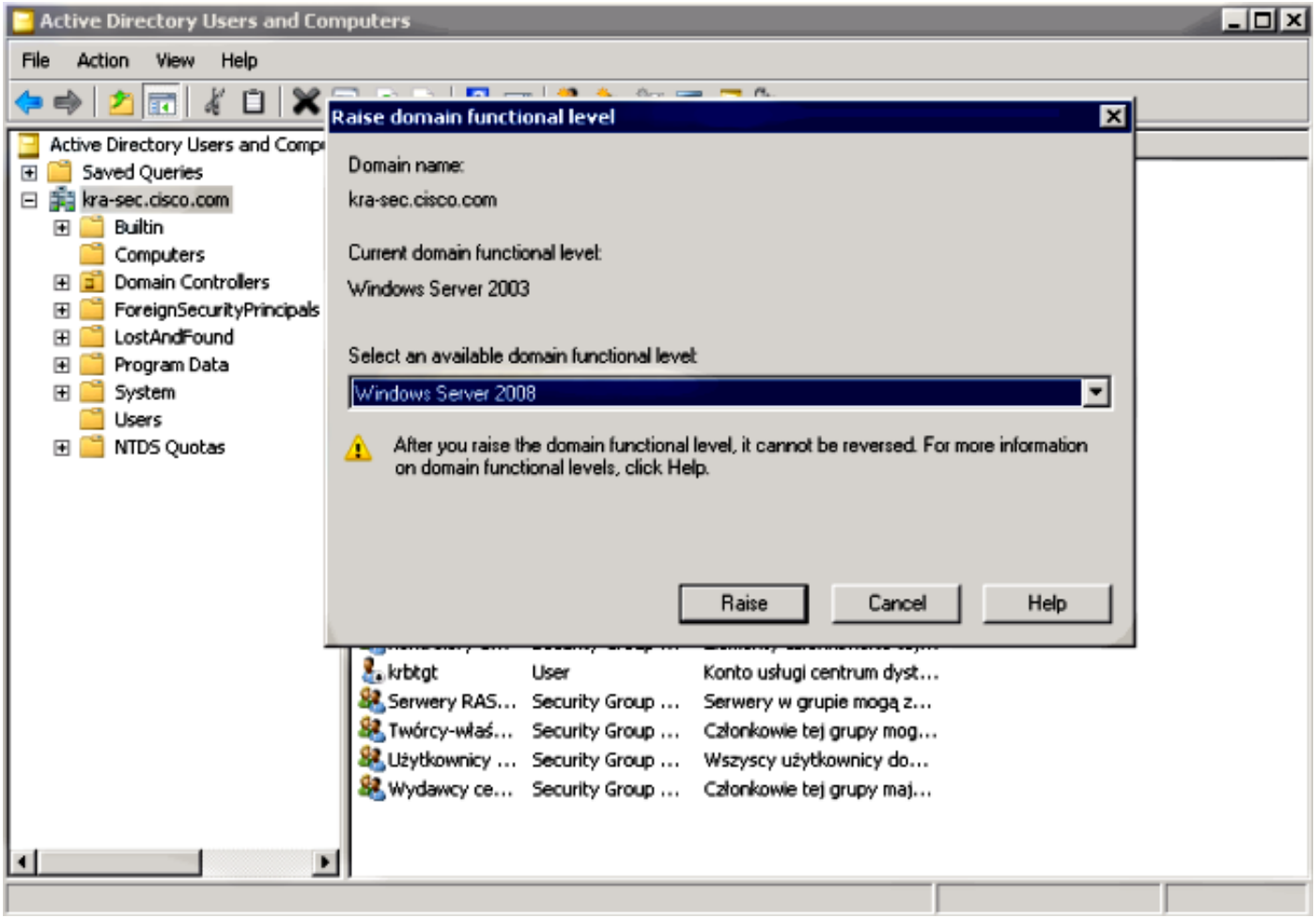
Configuration du contrôleur de domaine et des applications

Paramètres du domaine

Il est supposé qu'il existe déjà une application IIS7 fonctionnelle protégée par Kerberos (si ce n'est pas le cas, lisez la section Prérequis). Vous devez vérifier les paramètres des délégations des utilisateurs :



Assurez-vous que le niveau de domaine fonctionnel est élevé à Windows Server 2003 (au moins). La valeur par défaut est Windows Server 2000 :



Définir le nom principal du service (SPN)

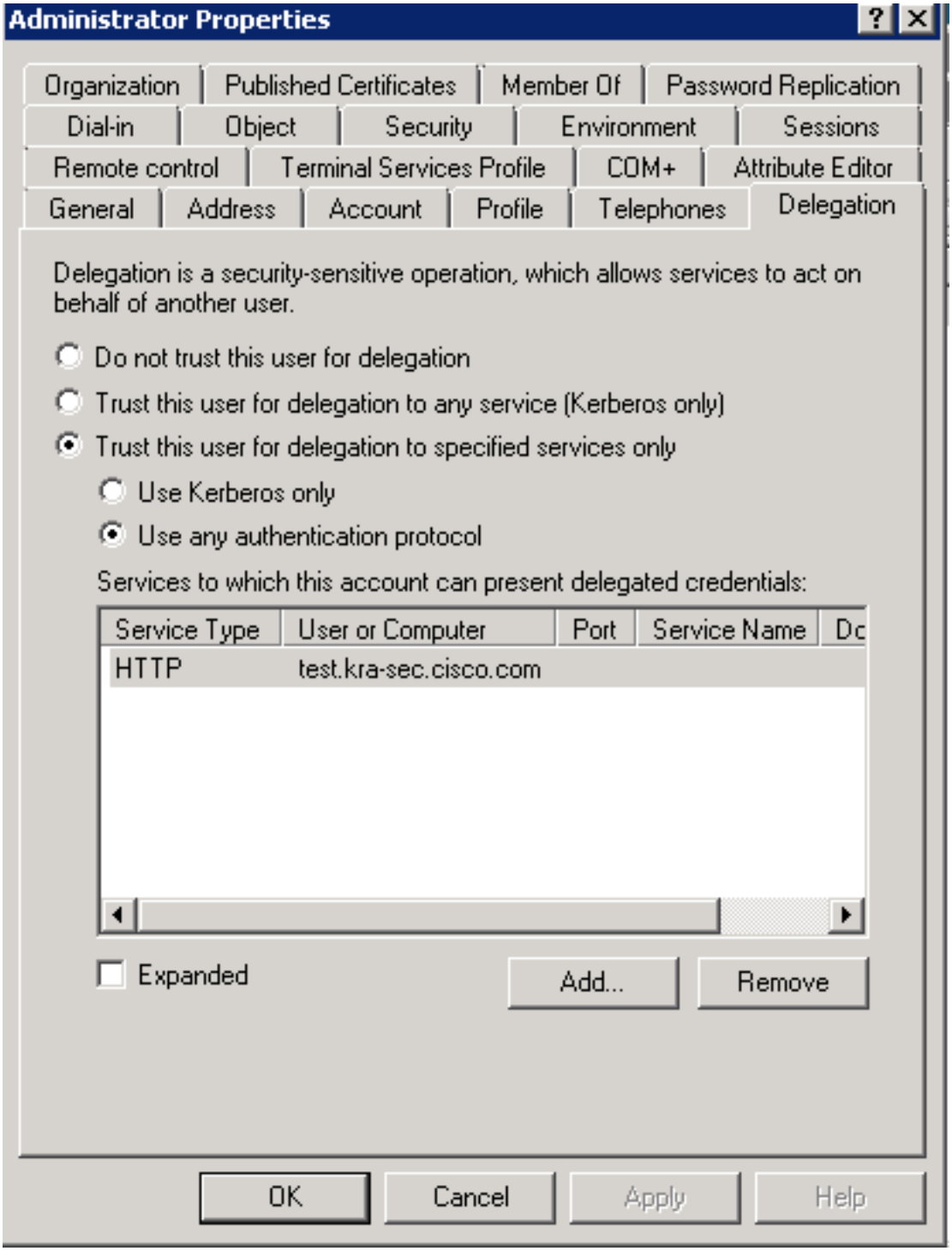
Vous devez configurer n'importe quel compte sur AD avec la délégation correcte. Un compte Administrateur est utilisé. Lorsque l'ASA utilise ce compte, il peut demander un ticket au nom d'un autre utilisateur (délégation limitée) pour le service spécifique (application HTTP). Pour que cela se produise, la délégation correcte doit être créée pour l'application/service.

Afin de faire cette délégation via l'interface de ligne de commande avec le **fichier setspn.exe**, qui fait partie des outils de support du Service Pack 1 de Windows Server 2003, entrez cette commande :

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

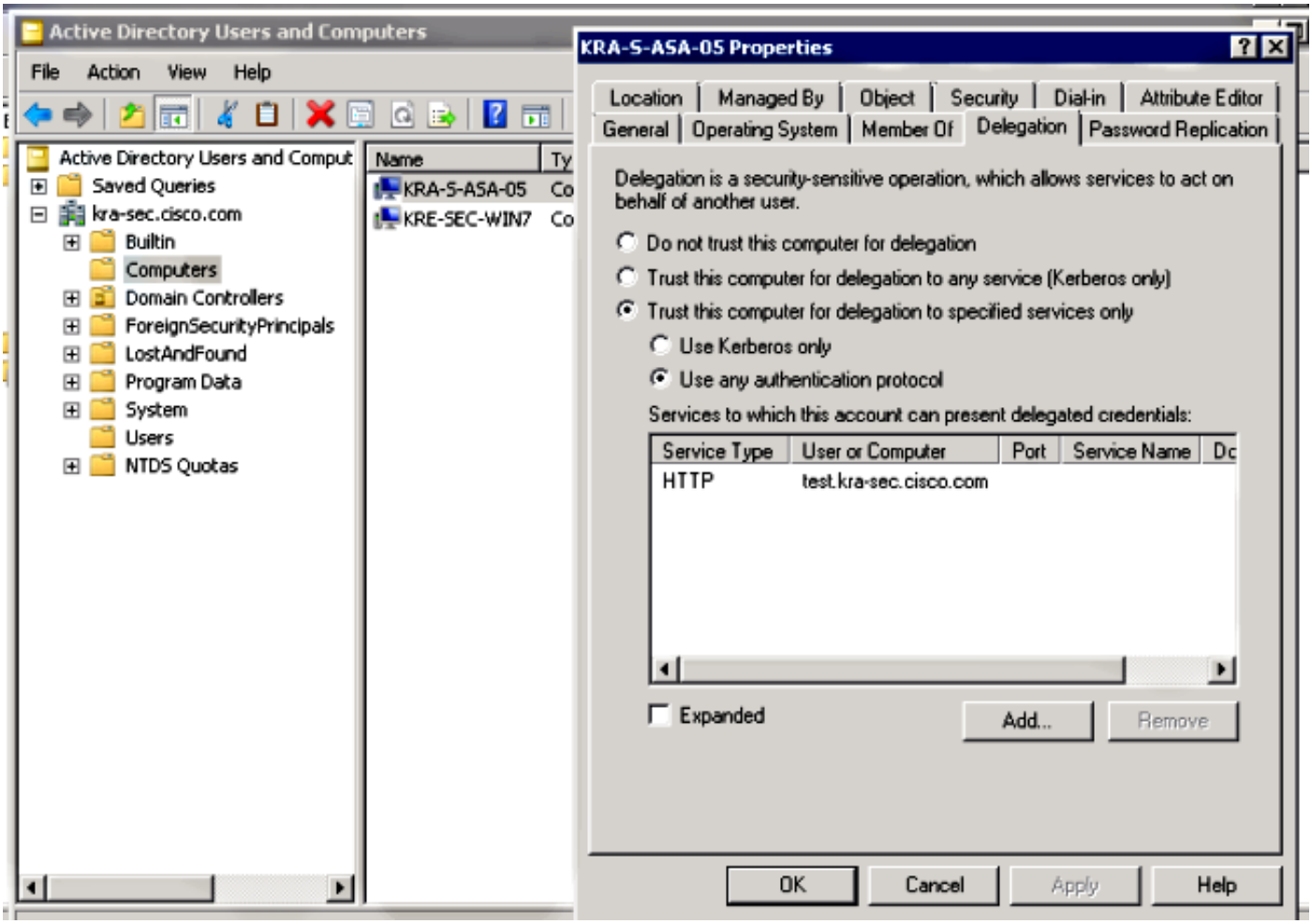
Cela indique que le nom d'utilisateur **Administrateur** est le compte approuvé pour la délégation du service HTTP à **test.kra-sec.cisco.com**.

La commande **SPN** est également nécessaire pour activer l'onglet **Délégation** de cet utilisateur. Une fois la commande saisie, l'onglet Délégation de l'administrateur s'affiche. Il est important d'activer « Use any authentication protocol », car « Use Kerberos only » ne prend pas en charge l'extension Délégation contrainte.



Dans l'onglet **Général**, il est également possible de désactiver la pré-authentification Kerberos. Cependant, ceci n'est pas conseillé, car cette fonctionnalité est utilisée afin de protéger le contrôleur de domaine contre les attaques de relecture. L'ASA peut fonctionner correctement avec la pré-authentification.

Cette procédure s'applique également à la délégation pour le compte d'ordinateur (l'ASA est introduit dans le domaine en tant qu'ordinateur afin d'établir une relation de confiance) :



Configuration sur l'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
```

Vérification

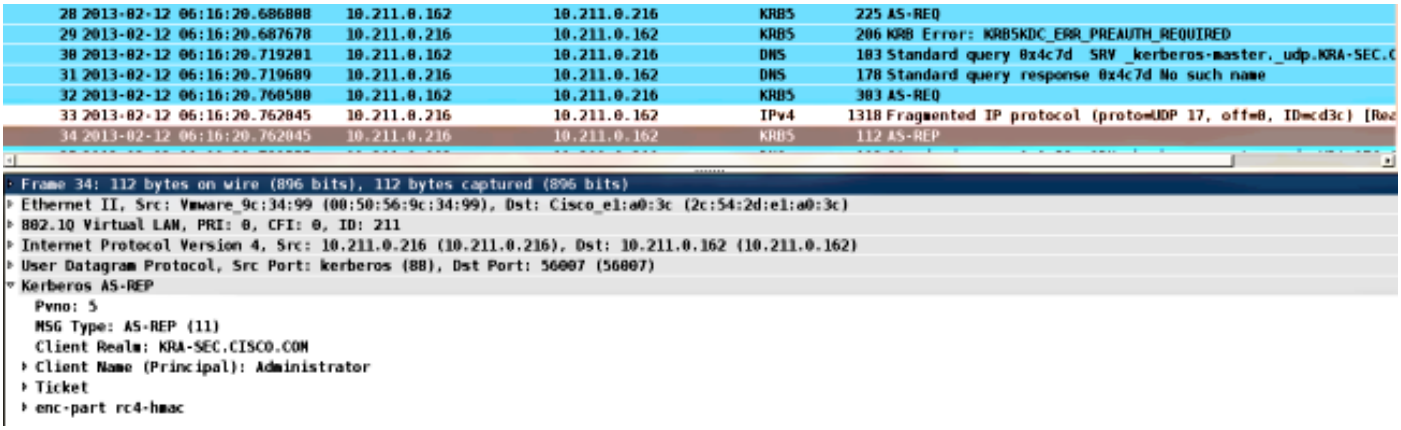
L'ASA rejoint le domaine

Une fois la commande **kcd-server** utilisée, l'ASA tente de joindre le domaine :

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

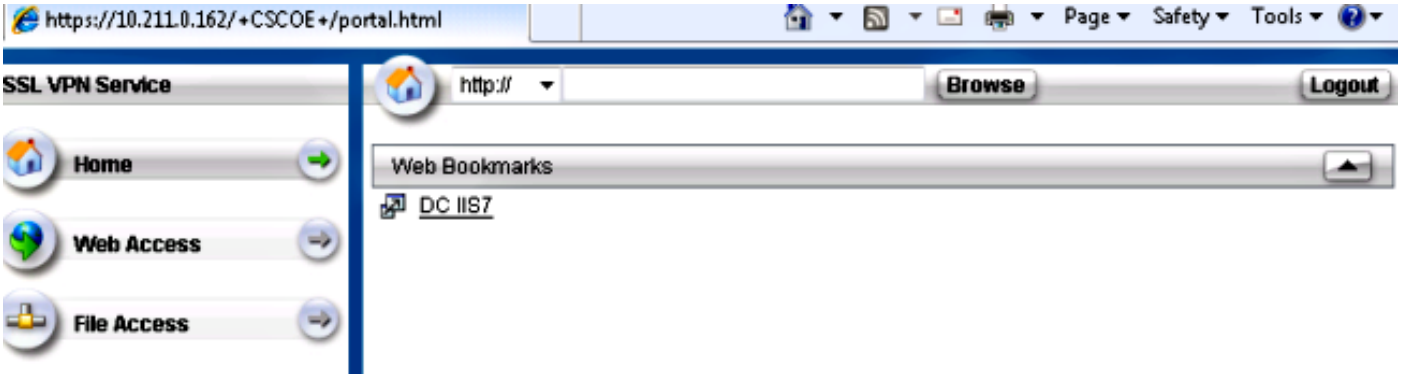
```
Kerberos: Server Name krbtgt
Kerberos: Start time 0
Kerberos: End time -878667256
Kerberos: Renew until time -878672192
Kerberos: Nonce 0xa9db408e
Kerberos: Encryption type rc4-hmac-md5
Kerberos: Encryption type des-cbc-md5
Kerberos: Encryption type des-cbc-crc
Kerberos: Encryption type des-cbc-md4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

L'ASA peut joindre le domaine avec succès. Après l'authentification correcte, l'ASA reçoit un ticket pour le principal : Administrateur dans le paquet **AS_REP** (Billet1 décrit à l'étape 1).

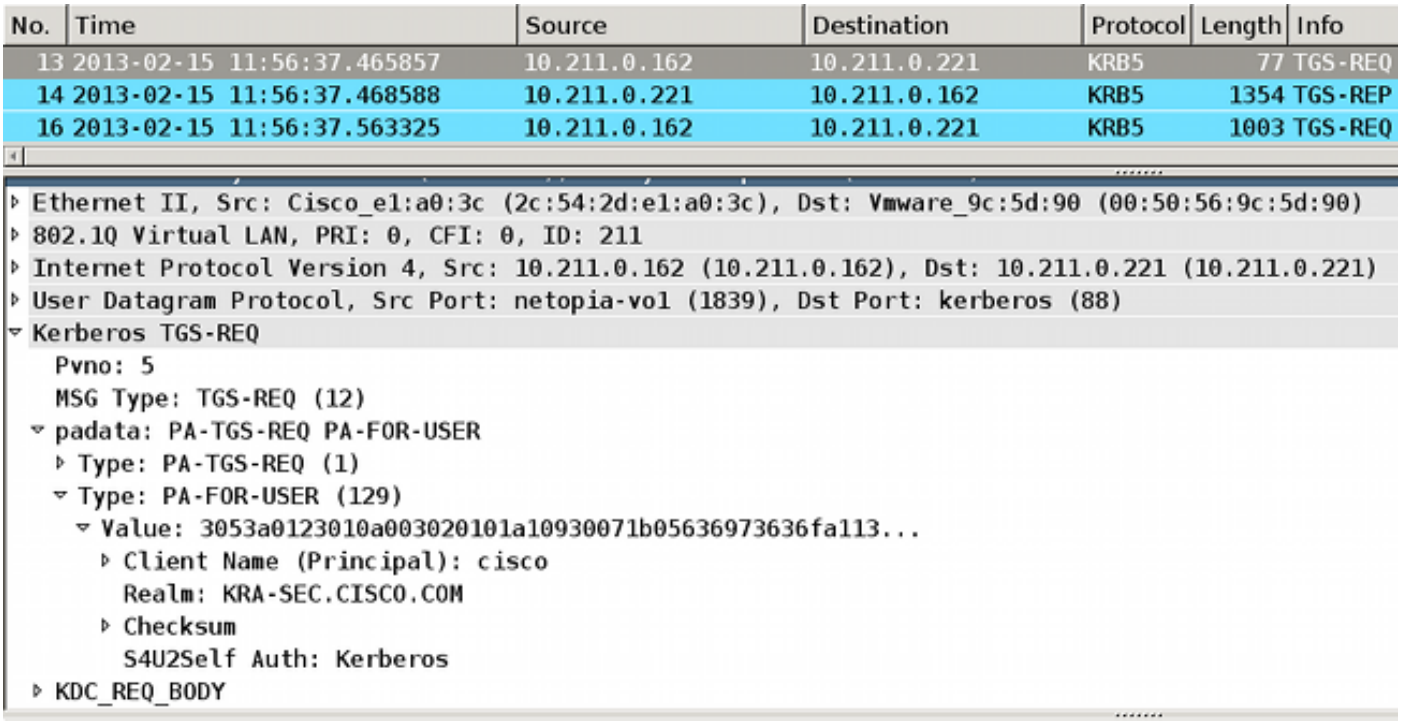


Demande de service

L'utilisateur clique sur le lien WebVPN :

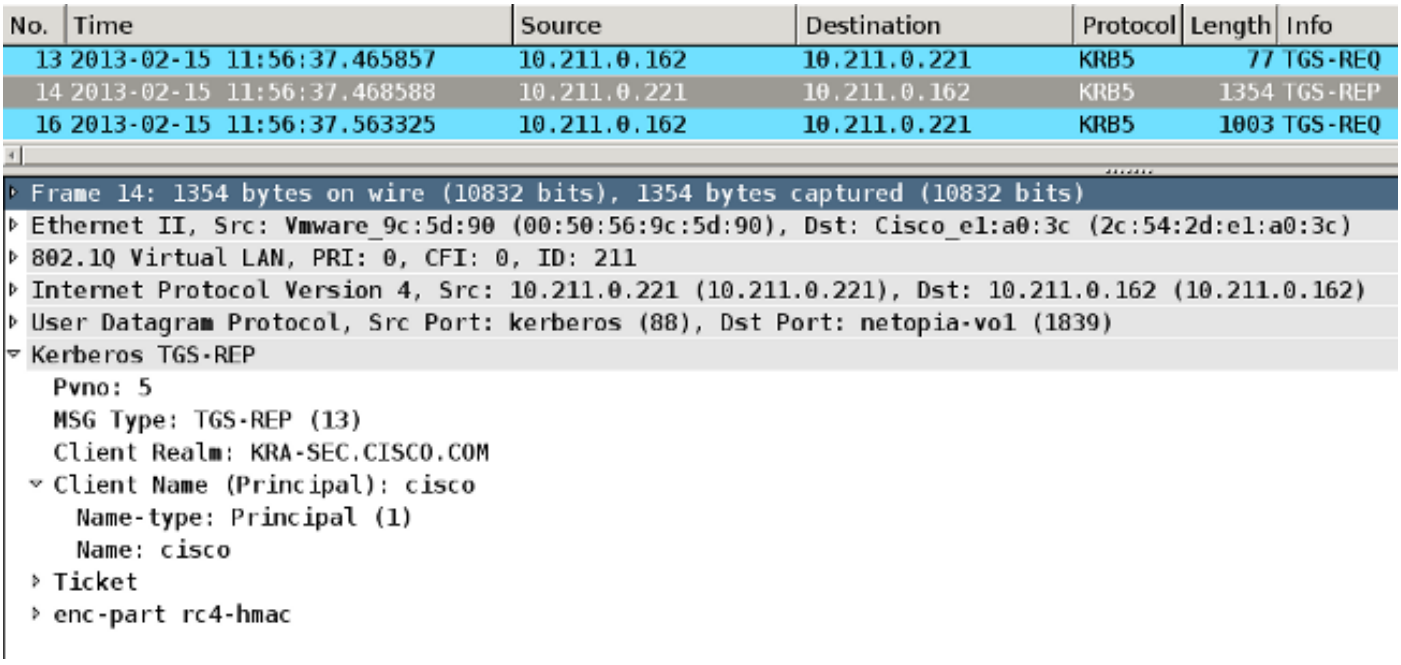


L'ASA envoie le **TGS_REQ** pour un ticket emprunté avec le ticket reçu dans le paquet **AS_REP** :



Note: La valeur **PA-FOR-USER** est **cisco** (utilisateur WebVPN). **PA-TGS-REQ** contient le ticket reçu pour la demande de service Kerberos (le nom d'hôte ASA est le principal).

L'ASA obtient une réponse correcte avec le ticket usurpé pour l'utilisateur **cisco** (Billet 2 décrit à l'étape 4) :



Voici la demande de ticket pour le service HTTP (certains débogages sont omis pour plus de clarté) :

```
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
```

L'ASA reçoit le ticket d'emprunt d'identité correct pour le service HTTP (Billet 3 décrit à l'étape 6).

Les deux billets peuvent être vérifiés. Le premier est le ticket d'emprunt d'identité de l'utilisateur **cisco**, qui est utilisé pour demander et recevoir le deuxième ticket pour le service HTTP auquel on accède :

```
KRA-S-ASA-05(config)# show aaa kerberos
Default Principal: cisco@KRA-SEC.CISCO.COM
Valid Starting       Expires              Service Principal
```

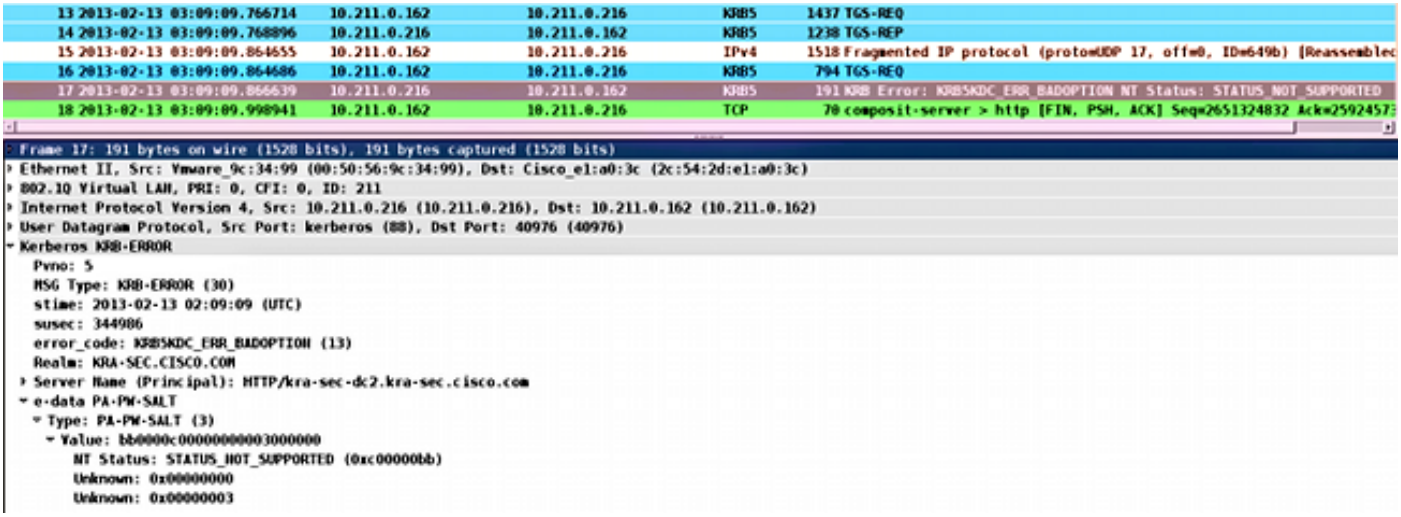
```
19:38:10 CEST Oct 2 2013 05:37:33 CEST Oct 3 2013 KRA-S-ASA-05@KRA-SEC.CISCO.COM

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
```

Ce ticket HTTP (Ticket3) est utilisé pour l'accès HTTP (avec SPNEGO), et l'utilisateur n'a pas besoin de fournir d'informations d'identification.

Dépannage

Il peut arriver que vous rencontriez un problème de délégation incorrecte. Par exemple, l'ASA utilise un ticket pour demander le service **HTTP/test.kra-sec.cisco.com** (Étape 5), mais la réponse est **KRB-ERROR** avec **ERR_BADOPTION** :



Il s'agit d'un problème typique rencontré lorsque la délégation n'est pas configurée correctement. L'ASA rapporte que **« KDC ne peut pas remplir l'option demandée »** :

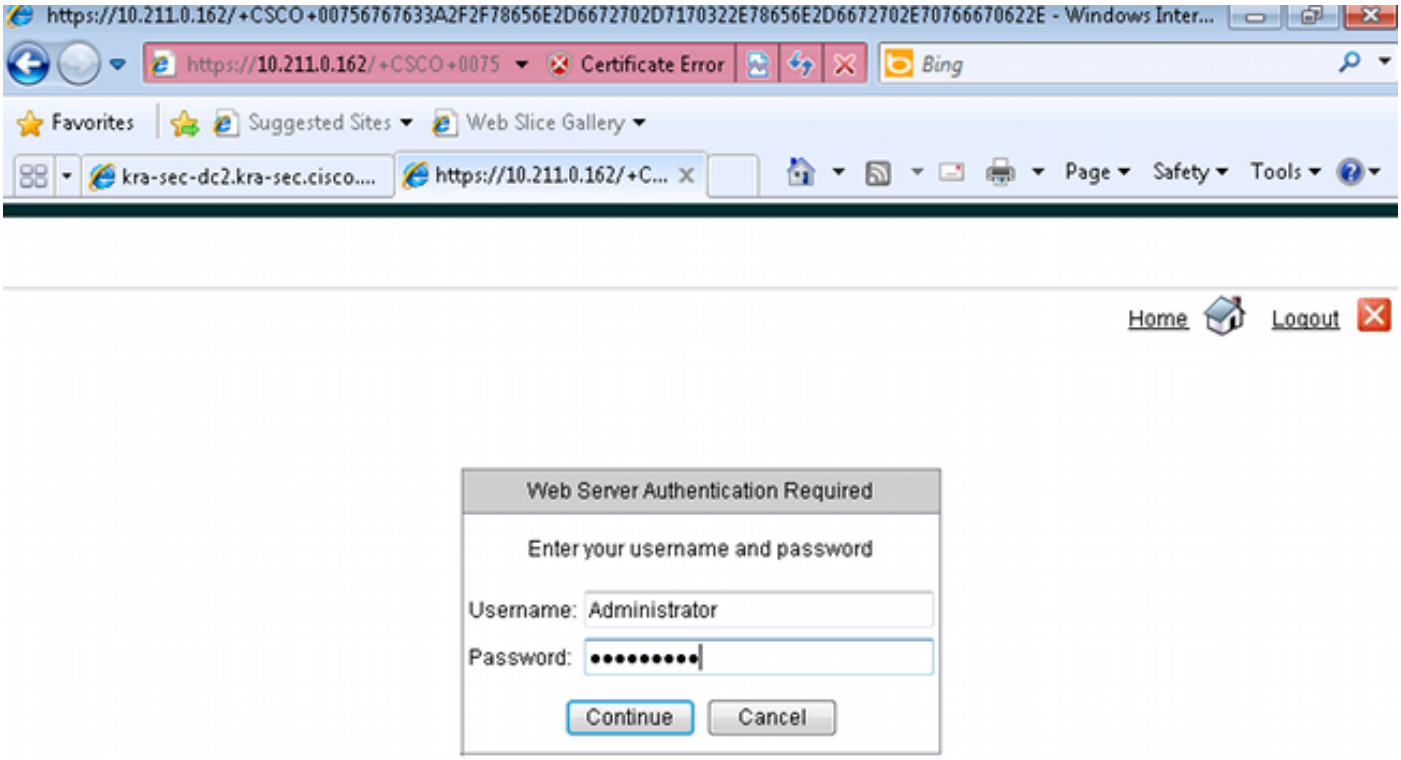
```
KRA-S-ASA-05# ucte_krb_get_auth_cred(): ctx = 0xcc4b5390,
WebVPN_session = 0xc919a260, protocol = 1
find_spn_in_url(): URL - /
build_host_spn(): host - test.kra-sec.cisco.com
build_host_spn(): SPN - HTTP/test.kra-sec.cisco.com
KCD_unicorn_get_cred(): Attempting to retrieve required KCD tickets.
In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

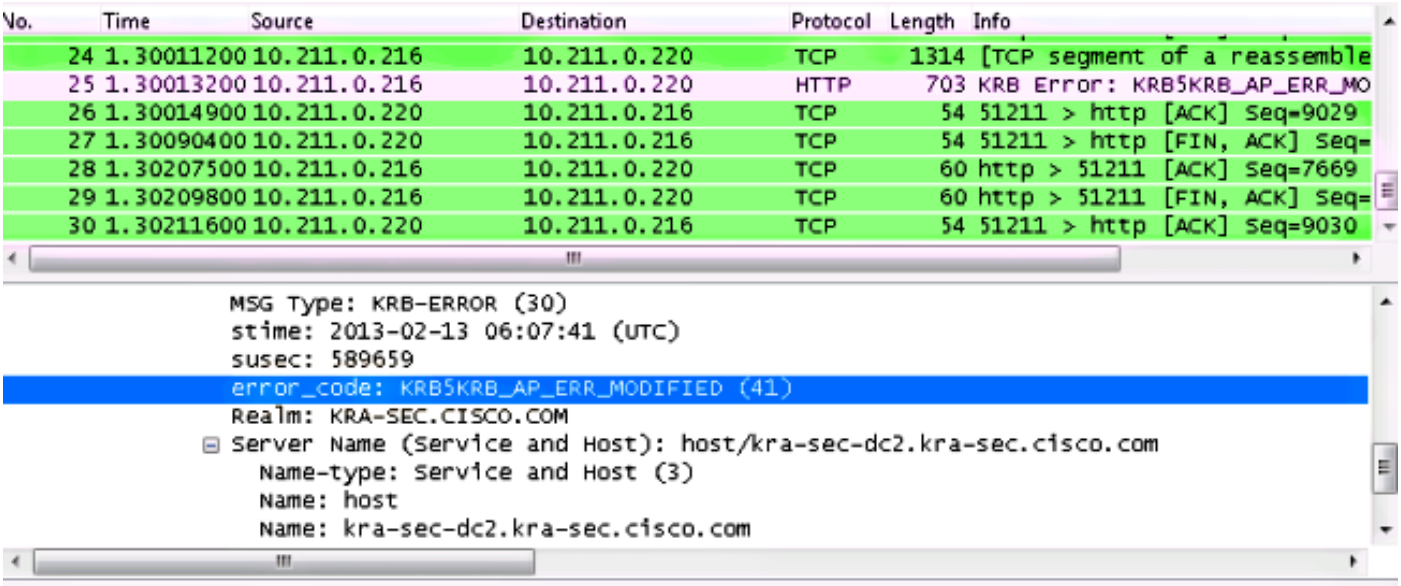
Il s'agit essentiellement du même problème que celui décrit dans les captures - l'échec est **à TGS_REQ avec BAD_OPTION**.

Si la réponse est **Success**, l'ASA reçoit un ticket pour le service **HTTP/test.kra-sec.cisco.com**, qui est utilisé pour **la** négociation **SPNEGO**. Cependant, en raison de la défaillance, le **NT LAN Manager (NTLM)** est négocié et l'utilisateur doit fournir les informations d'identification suivantes :

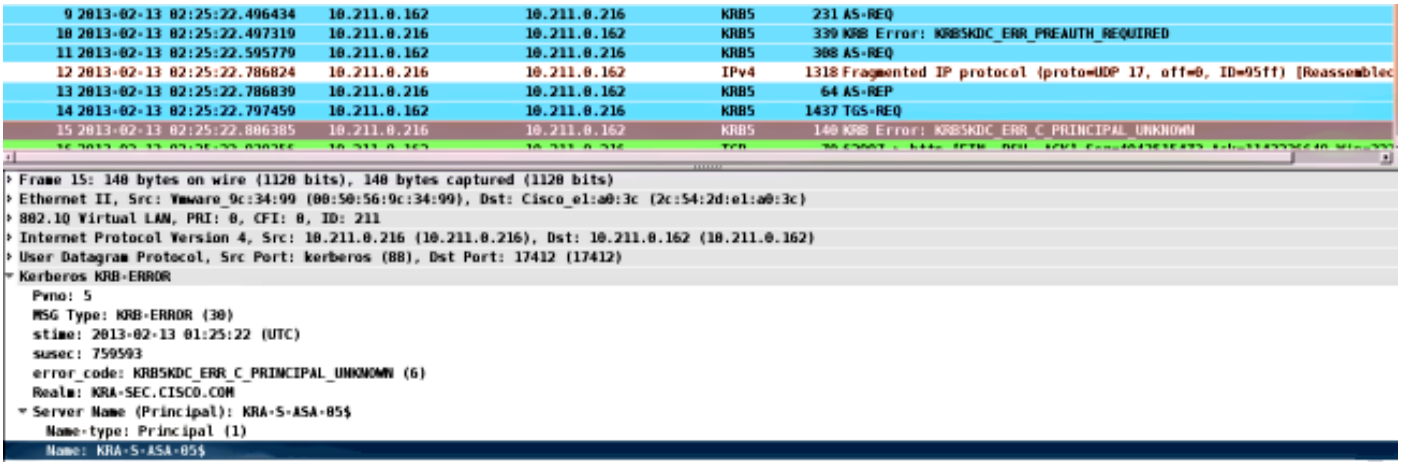


Assurez-vous que le SPN est enregistré pour un seul compte (script de l'article précédent).

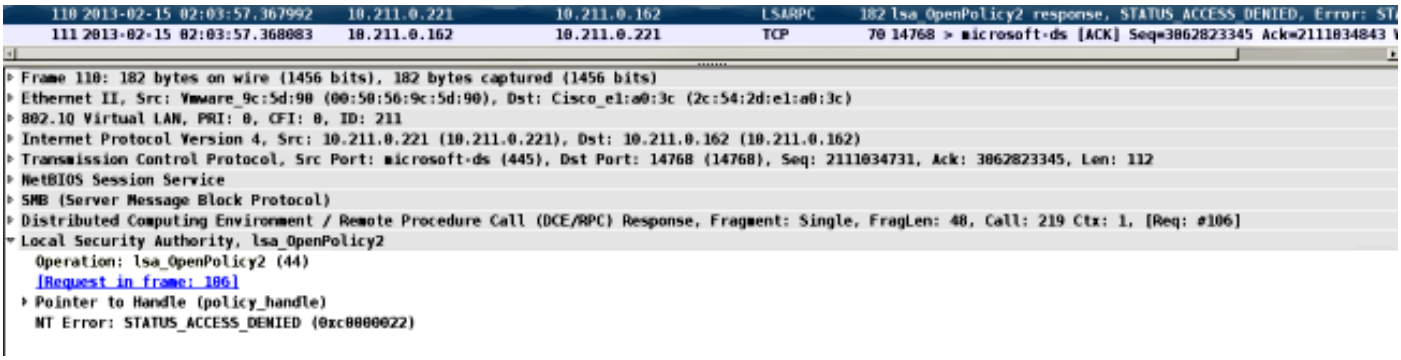
Lorsque vous recevez cette erreur, **KRB_AP_ERR_MODIFIED**, cela signifie généralement que le **SPN** n'est pas enregistré pour le compte correct. Il doit être enregistré pour le compte utilisé afin d'exécuter l'application (pool d'applications sur IIS).



Lorsque vous recevez cette erreur, **KRB_ERR_C_PRINCIPAL_UNKNOWN**, cela signifie qu'il n'y a aucun utilisateur sur le contrôleur de domaine (utilisateur WebVPN : **cisco**).



Vous pouvez rencontrer ce problème lorsque vous rejoignez le domaine. L'ASA reçoit **AS-REP**, mais échoue au niveau **LSA** avec l'erreur : **STATUS_ACCESS_REFUSÉ** :



Pour résoudre ce problème, vous devez activer/désactiver la pré-authentification sur le contrôleur de domaine de cet utilisateur (**administrateur**).

Voici quelques autres problèmes que vous pourriez rencontrer :

- Il peut y avoir des problèmes lorsque vous rejoignez le domaine. Si le serveur DC dispose de plusieurs cartes réseau (NIC) (plusieurs adresses IP), assurez-vous que l'ASA peut accéder à toutes ces cartes afin de rejoindre le domaine (choisi aléatoirement par le client en fonction de la réponse DNS).

- Ne définissez pas **SPN** en tant que **HOST/dc.kra-sec.cisco.com** pour le compte **Administrateur**. Il est possible de perdre la connectivité au contrôleur de domaine en raison de ce paramètre.

- Une fois que l'ASA a rejoint le domaine, il est possible de vérifier que le compte d'ordinateur correct est créé sur le contrôleur de domaine (nom d'hôte ASA). Assurez-vous que l'utilisateur dispose des autorisations appropriées pour ajouter des comptes d'ordinateur (dans cet exemple, l'**administrateur** dispose des autorisations appropriées).

- Souvenez-vous de la configuration correcte **NTP (Network Time Protocol)** sur l'ASA. Par défaut, le contrôleur de domaine accepte un décalage de cinq minutes. Ce compteur peut être modifié sur le contrôleur de domaine.

- Vérifiez que la connectivité Kerberos pour le petit paquet **UDP/88** est utilisée. Après l'erreur du contrôleur de domaine, **KRB5KDC_ERR_RESPONSE_TOO_BIG**, le client passe à **TCP/88**. Il est possible de forcer le client Windows à utiliser **TCP/88**, mais **ASA utilisera UDP par défaut**.

- DC : lorsque vous apportez des modifications à la stratégie, n'oubliez pas **gpupdate /force**.

- ASA : testez l'authentification à l'aide de la commande **test aaa**, mais rappelez-vous qu'il ne s'agit que d'une authentification simple.

- Afin de dépanner sur le site DC, il est utile d'activer les débogages Kerberos : Comment activer la journalisation des événements Kerberos.

ID de bogue Cisco

Voici une liste des ID de bogue Cisco pertinents :

- ID de bogue Cisco CSCsi32224 - ASA ne bascule pas vers TCP après réception du code d'erreur Kerberos 52
- ID de bogue Cisco CSCtd92673 - Échec de l'authentification Kerberos avec pré-authentification activée
- ID de bogue Cisco CSCuj19601 - KCD Webvpn ASA - tentative de jointure AD uniquement après redémarrage
- ID de bogue Cisco CSCuh32106 - Le KCD ASA est cassé dans la version 8.4.5 à partir de

Informations connexes

- À propos de la délégation contrainte Kerberos
- Compréhension du fonctionnement de KCD

- PIX/ASA : Exemple de configuration de l'authentification Kerberos et des groupes de serveurs d'autorisation LDAP pour les utilisateurs de clients VPN via ASDM/CLI
- Référence des commandes de la gamme Cisco ASA
- KDC_ERR_BADOPTION lors d'une tentative de délégation contrainte
- Comment forcer Kerberos à utiliser TCP au lieu d'UDP dans Windows
- Support et documentation techniques - Cisco Systems