# La integración del WebVPN SSO con el Kerberos obligó el ejemplo de configuración de la delegación

## Contenido



## Introducción

Este documento describe cómo configurar y resolver problemas la sola muestra del WebVPN encendido (SSO) para las aplicaciones que son protegidas por el Kerberos.

## Prerequisites

### Requisitos

Cisco recomienda que usted tiene conocimiento básico de estos temas:

- Configuración CLI del dispositivo de Cisco Securit (ASA) y configuración VPN adaptantes del Secure Socket Layer (SSL)

- Servicios Kerberos

### Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Software de Cisco ASA, versión 9.0 y posterior
- Cliente de Microsoft Windows 7
- Servidor de Microsoft Windows 2003 y posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Antecedentes

El Kerberos es un Network Authentication Protocol que permite que las entidades de red autentiquen el uno al otro en una forma segura. Utiliza otro vendedor de confianza, el Key Distribution Center (KDC), que concede los boletos a las entidades de red. Estos boletos son utilizados por las entidades para verificar y confirmar el acceso al servicio pedido.

Es posible configurar el WebVPN SSO para las aplicaciones que son protegidas por el Kerberos con la delegación llamada característica de Cisco ASA Kerberos Constrained (KCD). Con esta característica, el ASA puede pedir los boletos del Kerberos en nombre del usuario porta del WebVPN, mientras que él las aplicaciones de accesos protegidas por el Kerberos.

Cuando usted accede tales aplicaciones a través del portal del WebVPN, usted no necesita proporcionar ningunas credenciales más; en lugar, se utiliza la cuenta que fue utilizada para registrar en el WebVPN el portal.

Refiera a la comprensión cómo KCD trabaja la sección de la guía de configuración ASA para más información.

## Interacción del Kerberos con el ASA

Para el WebVPN, el ASA debe pedir los boletos en nombre del usuario (porque el usuario porta del WebVPN tiene acceso solamente al portal, no al servicio Kerberos). Para ese, el ASA utiliza las Extensiones del Kerberos para la delegación obligada. Aquí está el flujo:

1. El ASA se une al dominio y obtiene un boleto (Ticket1) para una cuenta del ordenador con las credenciales configuradas en ASA (comando del kcd-**servidor**). Este boleto se utiliza en los siguientes pasos para el acceso a los servicios Kerberos.

2. El usuario hace clic el link porta del WebVPN para la aplicación Kerberos-protegida.

3. El ASA pide (**TGS-REQ**) un boleto para la cuenta del ordenador con su nombre de host como el principal. Esta petición incluye el campo **PA-TGS-REQ** con **PA-FOR-USER** con el

principal como el nombre de usuario porta del WebVPN, que es **Cisco** en este escenario. El boleto para el servicio Kerberos del paso 1 se utiliza para la autenticación (delegación correcta).

4. Como respuesta, el ASA recibe un boleto personificado (Ticket2) en nombre del usuario de WebVPN (**TGS_REP**) para la cuenta del ordenador. Este boleto se utiliza para pedir los boletos de la aplicación en nombre de este usuario de WebVPN.

5. El ASA inicia otra petición (**TGS_REQ**) para obtener el boleto para la aplicación (**HTTP/test.kra-sec.cisco.com). Esta petición** utiliza otra vez el campo PA-TGS-REQ**, este vez** sin el **campo PA-FOR-USER, pero con el** boleto personificado recibido en el paso 4.

6. La respuesta (**TGS_REQ**) con el boleto personificado (Ticket3) para la aplicación se vuelve.

7. Este boleto es utilizado transparente por el ASA para acceder el servicio protegido, y el usuario de WebVPN no necesita ingresar ningunas credenciales. Para la aplicación HTTP, el mecanismo simple y protegido de la negociación del GSS API (SPNEGO) se utiliza para negociar el método de autentificación, y el boleto correcto es pasado por el ASA.

# Configurar

## Topología

Dominio: kra-sec.cisco.com (10.211.0.221 o 10.211.0.216)

**Aplicación 7 de los Servicios de Internet Information Server (IIS)**: test.kra-sec.cisco.com (10.211.0.223)

**Controlador de dominio (DC)**: dc.kra-sec.cisco.com (10.211.0.221 o 10.211.0.216) - Windows2008

**ASA**: 10.211.0.162

**Nombre de usuario de WebVPN/contraseña**: Cisco/Cisco

**Archivo adjunto**: asa-join.pcap (acertado únase a al dominio)

**Archivo adjunto**: asa-kerberos-bad.pcap (pedido el servicio)

## Controlador de dominio y configuración de aplicación

### Configuraciones del dominio

Se asume que hay ya una aplicación funcional IIS7 protegida por el Kerberos (si no, lea la sección de los requisitos previos). Usted debe marcar las configuraciones para las delegaciones de los usuarios:

Asegúrese de que el nivel funcional del dominio esté aumentado al Servidor Windows 2003 (por lo menos). El valor por defecto es el Servidor Windows 2000:

### Fije el nombre principal del servicio (SPN)

Usted debe configurar cualquier cuenta en el AD con la delegación correcta. Se utiliza una cuenta del administrador. Cuando las aplicaciones ASA que consideran, él pueden pedir un boleto en nombre de otro usuario (delegación obligada) para el servicio específico (aplicación HTTP). Para que esto ocurra, la delegación correcta debe ser creada para la aplicación/el servicio.

Para hacer a esta delegación vía el CLI con el **setspn.exe, que** es una parte del WindowsServer 2003 instrumentos de apoyo del Service Pack 1, ingrese este comando:

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

Esto indica que el **nombre de usuario del administrador** es el de confianza explica a la delegación del servicio HTTP en **test.kra-sec.cisco.com**.

El comando **SPN** es también necesario para activar la lengueta de la **delegación** para ese usuario. Una vez que usted ingresa el comando, la lengueta de la delegación para el administrador aparece. Es importante habilitar el “uso cualquier protocolo de autenticación,” porque el “Kerberos del uso” no soporta solamente la extensión obligada de la delegación.

En la **ficha general**, es también posible inhabilitar la PRE-autenticación del Kerberos. Sin embargo, esto no se aconseja, porque esta característica se utiliza para proteger DC contra los ataques con paquetes copiados. El ASA puede trabajar con la PRE-autenticación correctamente.

Este procedimiento también se aplica con la delegación para la cuenta del ordenador (el ASA se trae en el dominio como un ordenador para establecer una relación de la “confianza”):

## Configuración en el 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
```

# Verificación

## El ASA se une al dominio

Después de que se utilice el comando del kcd-**servidor**, el ASA intenta unirse al dominio:

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

El ASA puede unirse a con éxito el dominio. Después de la autenticación correcta, el ASA recibe un boleto para el principal: Administrador en el paquete **AS_REP** (Ticket1 descrito en Step1).

## Pedido el servicio

El link del WebVPN de los tecleos del usuario:

El ASA envía el **TGS_REQ** para un boleto personificado con el boleto que se recibe en el paquete **AS_REP**:

> **Note**: El valor **PA-FOR-USER** es **Cisco** (usuario de WebVPN). **PA-TGS-REQ** contiene el boleto recibido para la petición del servicio Kerberos (el nombre de host ASA es el principal).

El ASA consigue una respuesta correcta con el boleto personificado para el usuario **Cisco** (Ticket2 descrito en el paso 4):

Aquí está el pedido el boleto para el servicio HTTP (algunos debugs se omiten para mayor clareza):

```
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
```

El ASA recibe el boleto personificado correcto para el servicio HTTP (Ticket3 descrito en el paso 6).

Ambos boletos pueden ser verificados. Primer es el boleto personificado para el usuario Cisco, que se utiliza para pedir y recibir el segundo boleto para el servicio HTTP se accede que:

```
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
```

Este boleto HTTP (Ticket3) se utiliza para el acceso HTTP (con SPNEGO), y el usuario no necesita proporcionar cualquier credencial.

# Troubleshooting

Usted puede ser que encuentre a veces un problema de la delegación incorrecta. Por ejemplo, el ASA utiliza un boleto para pedir el servicio **HTTP/test.kra-sec.cisco.com (el paso 5), solamente la** respuesta es KRB-ERROR con **ERR_BADOPTION**:

Esto es problemas comunes encontrados cuando no configuran a la delegación correctamente. El ASA señala que el **"KDC no puede satisfacer la opción solicitada"**:

```
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
```

Éste es básicamente el mismo problema que se describe en las capturas - el error está **en TGS_REQ con BAD_OPTION**.

Si la respuesta es **éxito**, después el ASA recibe un boleto para el **servicio HTTP/test.kra-sec.cisco.com, que** se utiliza para la negociación SPNEGO**. Sin embargo**, debido al error, **negocian al** administrador de LAN de NT **(NTLM),** y el usuario debe proporcionar las credenciales:

Aseegurese que el SPN está registrado para una cuenta solamente (script del artículo anterior). Cuando usted recibe este error, **KRB_AP_ERR_MODIFIED**, significa generalmente que el **SPN** no está registrado para la cuenta correcta. Debe ser registrado para la cuenta que se utiliza para ejecutar la aplicación (grupo de aplicaciones en el IIS).

Cuando usted recibe este error, **KRB_ERR_C_PRINCIPAL_UNKNOWN**, significa que no hay usuario en DC (usuario de WebVPN: **Cisco**).

Usted puede ser que encuentre este problema cuando usted se une al dominio. El ASA recibe **AS-REP**, pero falla en el nivel **LSA** con el error: **STATUS_ACCESS_DENIED**:

Para reparar este problema, usted debe habilitar/PRE-autenticación de la neutralización en DC para ese usuario (**administrador**).

Aquí están algunos otros problemas que usted puede ser que encuentre:

- Pudo haber problemas cuando usted se une al dominio. Si el servidor de DC tiene adaptadores del regulador de la interfaz de Red múltiple (NIC) (IP Addresses múltiples), aseegurese que el ASA puede acceder todos para unirse al dominio (elegido aleatoriamente por el cliente basado en la respuesta del Domain Name Server (DNS)).

- No fije **SPN** como el **HOST/dc.kra-sec.cisco.com para la cuenta del administrador. Es** posible perder la Conectividad a DC debido a esa configuración.

- Después de que el ASA se una al dominio, es posible verificar que la cuenta correcta del ordenador está creada en DC (nombre de host ASA). Aseegurese que el usuario tiene los permisos correctos para agregar las cuentas del ordenador (en este ejemplo, el **administrador** tiene los permisos correctos).

- Recuerde la configuración correcta del **Network Time Protocol (NTP)** en el ASA. Por abandono, DC valida una posición oblicua del reloj de cinco minutos. Ese temporizador se puede cambiar en DC.

- Verifique el Kerberos que la Conectividad para el pequeño paquete **UDP/88** se utiliza. Después del error de DC, **KRB5KDC_ERR_RESPONSE_TOO_BIG**, el Switches del cliente a **TCP/88**. Es posible forzar al cliente de Windows a utilizar **TCP/88**, pero el **ASA utilizará el**

**UDP por abandono**.

- DC: cuando usted realiza los cambios de política, recuerde el **gpupdate /force**.
- ASA: la prueba de la autentificación con el **comando aaa de la prueba**, pero recuerda que es solamente una autenticación simple.
- Para resolver problemas en el sitio de DC, es útil habilitar los debugs del Kerberos: Cómo habilitar el registro de evento del Kerberos.

## Bug Cisco ID

Aquí está una lista del bug Cisco relevante ID:

- Id. de bug Cisco CSCsi32224 - El ASA no conmuta al TCP después de recibir el código de error 52 del Kerberos
- Id. de bug Cisco CSCtd92673 - La autenticación de Kerberos falla con el PRE-auth habilitado
- Id. de bug Cisco CSCuj19601 - ASA Webvpn KCD - intentando unirse al AD sólo después de la reinicialización
- Id. de bug Cisco CSCuh32106 - El ASA KCD está quebrado en 8.4.5 hacia adelante

## Información Relacionada

- Sobre la delegación obligada Kerberos
- Entendiendo cómo KCD trabaja
- PIX/ASA: Autenticación de Kerberos y grupos de servidor de autorización LDAP para los usuarios de cliente VPN vía el ejemplo de configuración ASDM/CLI
- Referencia de comandos de la serie de Cisco ASA
- KDC_ERR_BADOPTION al intentar a la delegación obligada
- Cómo forzar el Kerberos para utilizar el TCP en vez del UDP en Windows
- Soporte Técnico y Documentación - Cisco Systems