Интеграция WebVPN SSO с примером конфигурации ограниченного делегирования Kerberos

Содержание

Введение

Этот документ описывает, как настроить и устранить неполадки Единой точки входа (SSO) WebVPN для приложений, которые защищены Kerberos.

Предварительные условия

Требования

Cisco рекомендует иметь базовые знания об этих темах:

- Конфигурация интерфейса командой строки Адаптивного устройства Securit (ASA) Cisco и конфигурация VPN протокола SSL

- Сервисы Kerberos

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Программное обеспечение Cisco ASA, версия 9.0 и позже
- Microsoft Windows 7 клиентов
- Microsoft Windows 2003 Server и позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Kerberos является сетевым протоколом аутентификации, который позволяет объектам сети аутентифицироваться друг на друге безопасным способом. Это использует доверенную третью сторону, Key Distribution Center (KDC), который предоставляет билеты объектам сети. Эти билеты используются объектами, чтобы проверить и подтвердить доступ к запрошенному сервису.

Возможно настроить WebVPN SSO для приложений, которые защищены Kerberos с функцией Cisco ASA, названной Ограниченным делегированием Kerberos (KCD). С этой функцией ASA может запросить билеты Kerberos от имени пользователя портала WebVPN, в то время как это обращается к приложениям, защищенным Kerberos.

При доступе к таким приложениям через портал WebVPN вы не должны больше предоставлять учетные данные; вместо этого, учетная запись, которая использовалась для вхождения в портал WebVPN используется.

См. Понимание, Как KCD Работает раздел руководства по конфигурации ASA для получения дополнительной информации.

Взаимодействие Kerberos с ASA

Для WebVPN ASA должен запросить билеты от имени пользователя (потому что у пользователя портала WebVPN есть доступ только к порталу, не Сервису Kerberos). Для этого ASA использует расширения Kerberos для Ограниченного делегирования. Вот поток:

1. ASA присоединяется к домену и получает билет (Ticket1) на учетную запись компьютера с учетными данными, настроенными на ASA **(kcd-команда-сервера)**. Этот билет используется в следующих шагах для доступа к Сервисам Kerberos.

2. Пользователь щелкает по ссылке портала WebVPN для защищенного приложения Kerberos.

3. ASA запрашивает **(TGS-REQ)** билет на учетную запись компьютера с ее именем хоста как принципал. Этот запрос включает поле **PA-TGS-REQ** с **ПОЛЬЗОВАТЕЛЕМ FOR PA** с принципалом как имя пользователя портала WebVPN, которое является **Cisco** в этом сценарии. Билет для Сервиса Kerberos от Шага 1 используется для аутентификации (корректная делегация).

4. Как ответ, ASA получает явленный олицетворением билет (Ticket2) от имени пользователя WebVPN **(TGS_REP)** для учетной записи компьютера. Этот билет используется для запроса билетов приложения от имени этого пользователя WebVPN.

5. ASA инициирует другой запрос **(TGS_REQ)** для получения билета на приложение (**HTTP/test.kra-sec. cisco . com**). Этот запрос снова использует поле **PA-TGS-REQ**, на этот раз **без поля PA-FOR-USER**, но с явленным олицетворением билетом, полученным в Шаге 4.

6. Ответ **(TGS_REQ)** с явленным олицетворением билетом (Ticket3) на приложение возвращен.

7. Этот билет используется прозрачно ASA для доступа к защищенному сервису, и пользователь WebVPN не должен вводить учетные данные. Для приложения HTTP Простое и Защищенное Согласование GSS-API (SPNEGO) механизм используется для согласования о методе аутентификации, и корректный билет передает ASA.

Настройка

Топология

Домен: kra-сек.. cisco . com (10.211.0.221 или 10.211.0.216)

Информационные сервисы интернета (IIS) 7 приложений: test.kra-сек.. cisco . com (10.211.0.223)

Контроллер домена (DC): dc.kra-сек.. cisco . com (10.211.0.221 или 10.211.0.216) - Windows2008

ASA: 10.211.0.162

Имя пользователя WebVPN / пароль: cisco/cisco

Прикрепленный файл: asa-join.pcap (успешное соединение к домену)

Прикрепленный файл: asa-kerberos-bad.pcap (запрашивают на сервис),

Контроллер домена и конфигурация приложения

Доменные параметры настройки

Предполагается, что уже существует функциональное приложение IIS7, защищенное Kerberos (в противном случае читает раздел Предварительных условий). Необходимо проверить параметры настройки для делегаций пользователей:

Гарантируйте, что функциональный доменный уровень повышен до Windows Server 2003 (по крайней мере). По умолчанию является Windows Server 2000:

Установите Сервисное главное имя (SPN)

Необходимо настроить любую учетную запись на AD с корректной делегацией. Учетная запись администратора используется. Когда использование ASA, которое считает, это в состоянии запросить билет от имени другого пользователя (Ограниченное делегирование) для определенного сервиса (приложение HTTP). Для этого для появления корректная делегация должна быть создана для приложения/сервиса.

Для создания этой делегации через CLI с **setspn.exe**, который является частью Пакета обновления Windows Server 2003 1 Инструмент поддержки , введите эту команду:

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

Это указывает, что **Имя пользователя администратора** является доверяемой учетной записью на делегацию сервиса HTTP в **test.kra-сек.. cisco . com**.

Команда **SPN** также необходима для активации вкладки **Delegation** для того пользователя. Как только вы вводите команду, вкладка Delegation для Администратора появляется. Важно включить "Использованию любой протокол аутентификации", потому что "Kerberos использования только" не поддерживает расширение Ограниченного делегирования.

На **Вкладке Общие** также возможно отключить процедуры, предшествующие аутентификации Kerberos. Однако это не рекомендуется, потому что эта функция использована для защиты DC против атак с повторением пакетов. ASA может работать с процедурами, предшествующими аутентификации правильно.

Эта процедура также применяется с делегацией к учетной записи компьютера (ASA принесен в домен как компьютер для установления "трастового" отношения):

Конфигурация на 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
```

Проверка

ASA присоединяется к домену

После того, как **kcd-команда-сервера** используется, ASA пытается присоединиться к домену:

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

ASA в состоянии успешно присоединиться к домену. После корректной аутентификации ASA получает билет для принципала: Администратор в пакете AS_REP (Ticket1, описанный в Step1).

Запрос о сервисе

Пользователь щелкает по ссылке WebVPN:

ASA передает TGS_REQ за явленным олицетворением билетом с билетом, который получен в пакете AS_REP:

> **Примечание:** Значение ПОЛЬЗОВАТЕЛЯ FOR PA является Cisco (пользователь WebVPN). PA-TGS-REQ содержит билет, полученный для запроса Сервиса Kerberos (имя хоста ASA является принципалом).

ASA получает корректный ответ с явленным олицетворением билетом для пользовательского Cisco (Ticket2, описанный в Шаге 4):

Вот запрос о билете для сервиса HTTP (некоторые отладки опущены для ясности):

```
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
```

ASA получает корректный явленный олицетворением билет для сервиса HTTP (Ticket3, описанный в Шаге 6).

Могут быть проверены оба билета. Первый является явленным олицетворением билетом для пользовательского Cisco, который используется, чтобы запросить и получить второй

билет для сервиса HTTP, к которому обращаются:

```
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
```

Этот билет (Ticket3) HTTP используется для доступа HTTP (с SPNEGO), и пользователь не должен предоставлять учетные данные.

Устранение неполадок

Иногда вы могли бы встретиться с проблемой неправильной делегации. Например, ASA использует билет для запроса сервисного **HTTP/test.kra-sec. cisco . com** (Шаг 5), но ответ является **KRB-ОШИБКА** с **ERR_BADOPTION**:

Когда делегация не настроена правильно, это - типичная проблема, с которой встречаются. ASA сообщает, что **"KDC не может выполнить запрошенный параметр"**:

```
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
```

Это - в основном та же проблема, которая описана в перехватах - сбой **в TGS_REQ с BAD_OPTION**.

Если ответом является **Успех**, то ASA получает билет для **HTTP/test.kra-sec. cisco** . сервис **com**, который используется для согласования **SPNEGO**. Однако из-за сбоя, **о LAN Manager NT (NTLM)** выполняют согласование, и пользователь должен предоставить учетные данные:

Удостоверьтесь, что SPN зарегистрирован для одной учетной записи только (сценарий от предыдущей статьи). При получении этой ошибки, **KRB_AP_ERR_MODIFIED**, это обычно означает, что **SPN** не зарегистрирован для корректной учетной записи. Это должно быть зарегистрировано для учетной записи, которая используется для запуска приложения (пул приложений на IIS).

При получении этой ошибки, **KRB_ERR_C_PRINCIPAL_UNKNOWN**, это означает, что нет никакого пользователя на DC (пользователь WebVPN: **cisco .**

Вы могли бы встретиться с этой проблемой при присоединении к домену. ASA получает **REP AS**, но отказывает на уровне **LSA** с ошибкой: **STATUS_ACCESS_DENIED**:

Для решения этой проблемы вы должны процедуры, предшествующие аутентификации позволить/запретить на DC для того пользователя **(Администратор)**.

Вот некоторые другие проблемы, с которыми вы могли бы встретиться:

- Могли бы быть проблемы при присоединении к домену. Если сервер DC имеет несколько сетей Контроллер интерфейса (NIC) адаптеры (несколько IP - адресовы), удостоверьтесь, что ASA может обратиться ко всем ним для присоединения к домену (выбранный случайным образом клиентом на основе ответа Сервера доменных имен (DNS)).

- Сделайте "not set" **SPN** как **HOST/dc.kra-sec. cisco . com** для **Учетной записи администратора**. Возможно потерять подключение DC из-за той установки.

- После того, как ASA присоединяется к домену, возможно проверить, что корректная учетная запись компьютера создана на DC (имя хоста ASA). Удостоверьтесь, что у пользователя есть соответствующие разрешения для добавления учетных записей компьютера (в данном примере, **у Администратора** есть соответствующие разрешения).

- Помните **нужную сеть Протокол времени (NTP)** конфигурация на ASA. По умолчанию

DC принимает пятиминутную расфазировку тактовых сигналов. Тот таймер может быть изменен на DC.

- Проверьте, что используется подключение Kerberos для **UDP/88** небольшого пакета. После ошибки от DC, **KRB5KDC_ERR_RESPONSE_TOO_BIG**, клиент переключается на **TCP/88**. Возможно вынудить Windows - клиента использовать **TCP/88**, но **ASA будет использовать UDP по умолчанию**.

- DC: при создании изменений политики помните **gpupdate / сила**.

- ASA: тестовая аутентификация с **командой test aaa**, но помнят, что это - только простая проверка подлинности.

- Для устранения проблем на узле DC полезно включить отладки Kerberos: Как включить регистрацию событий Kerberos.

Идентификаторы ошибок Cisco

Вот список соответствующих идентификаторов ошибок Cisco:

- Идентификатор ошибки Cisco CSCsi32224 - ASA не переключается к TCP после получения кода ошибки Kerberos 52
- Идентификатор ошибки Cisco CSCtd92673 - сбои проверки подлинности Kerberos с предаутентификацией включил
- Идентификатор ошибки Cisco CSCuj19601 - Webvpn ASA KCD - пытающийся присоединиться к AD только после перезагрузки
- Идентификатор ошибки Cisco CSCuh32106 - ASA KCD сломан в 8.4.5 и далее

Дополнительные сведения

- Об ограниченном делегировании Kerberos
- Понимание, как работает KCD
- PIX/ASA: Проверка подлинности Kerberos и Группы серверов авторизации LDAP для Пользователей VPN-клиента через Пример ASDM/КОНФИГУРАЦИИ ИНТЕРФЕЙСА КОМАНДОЙ СТРОКИ
- Справочник по командам серии Cisco ASA
- KDC_ERR_BADOPTION при попытке ограниченного делегирования
- Как вынудить Kerberos использовать TCP вместо UDP в Windows
- Cisco Systems – техническая поддержка и документация