Kerberos Constrained Delegation を使った WebVPN の SSO 統合の設定例

目次

概要

このドキュメントでは、Kerberos で保護されているアプリケーションに対する WebVPN シングル サインオン（SSO）の設定とトラブルシューティングの方法を説明します。

前提条件

要件

Cisco では、次の項目について基本的な知識があることを推奨しています。

- Cisco 適応型セキュリティ アプライアンス（ASA）CLI の設定とセキュア ソケット レイヤ（SSL）VPN の設定
- Kerberos サービス

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- Cisco ASA ソフトウェア バージョン 9.0 以降
- Microsoft Windows 7 クライアント
- Microsoft Windows Server 2003 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

Kerberos はネットワーク認証プロトコルであり、ネットワーク エンティティ間で相互にセキュアな認証を実行できるようにします。 信頼されるサード パーティのキー発行局（KDC）を使用します。KDC はネットワーク エンティティへチケットを付与します。 これらのチケットは、要求されたサービスへのアクセスを検証、確定するためにエンティティにより使用されます。

Cisco ASA の Kerberos Constrained Delegation（KCD）と呼ばれる機能により、Kerberos により保護されているアプリケーションに対して WebVPN SSO を設定できます。 この機能により、ASA は WebVPN ポータル ユーザの代理として Kerberos チケットを要求でき、また Kerberos により保護されているアプリケーションにアクセスします。

これで、WebVPN ポータルからこのようなアプリケーションにアクセスするときに、クレデンシャルを指定する必要がなくなります。 その代わりに、WebVPN ポータルへのログインに使用するアカウントが使用されます。

詳細については、ASA コンフィギュレーション ガイドの「KCD の機能について」を参照してください。

Kerberos と ASA のインタラクション

WebVPN では、ASA はユーザの代理としてチケットを要求する必要があります。これは、WebVPN ポータル ユーザはポータルだけにアクセスでき、Kerberos サービスにはアクセスできないためです。 このことから、ASA は Constrained Delegation のための Kerberos 拡張を使用します。 ここで、フローを示します。

1. ASA がドメインに参加し、ASA でクレデンシャルが設定されているコンピュータ アカウントのチケット（Tiecket1）を取得します（**kcd-server** コマンド）。 このチケットは、次のステップで Kerberos サービスにアクセスするために使用されます。

2. ユーザは Kerberos で保護されているアプリケーションの WebVPN ポータル リンクをクリックします。

3. ASA は、ホスト名がプリンシパルとして設定されているコンピュータ アカウントのチケットを要求します（**TGS-REQ**）。 この要求には、**PA-TGS-REQ** フィールドと **PA-FOR-**

USER（プリンシパルが WebVPN ポータル ユーザ名（このシナリオでは **cisco**））が含まれています。 ステップ 1 で取得した Kerberos サービスのチケットが認証に使用されます（正しい委任）。

4. ASA は、コンピュータ アカウントの WebVPN ユーザの代理で、応答として偽装チケット（Ticket2）を受け取ります（**TGS_REP**）。 このチケットは、この WebVPN ユーザの代理としてアプリケーション チケットを要求するために使用されます。

5. ASA は、アプリケーション（**HTTP/test.kra-sec.cisco.com**）のチケットを入手するため、別の要求（**TGS_REQ**）を開始します。 **この要求は再び** PA-TGS-REQ **フィールドを使用しますが、今回は** PA-FOR-USER **フィールドは使用せず、ステップ 4 で受信した偽装チケットを使用します。**

6. アプリケーションの偽装チケット（Ticket3）を含む応答（**TGS_REQ**）が返されます。

7. ASA は保護されているサービスへアクセスするためにこのチケットを透過的に使用するため、WebVPN ユーザはクレデンシャルを入力する必要がありません。 HTTP アプリケーションの場合、認証方式のネゴシエーションに Simple and Protected GSS-API Negotiation（SPNEGO）メカニズムが使用され、ASA により正しいチケットが渡されます。

設定

トポロジ

ドメイン： kra-sec.cisco.com（10.211.0.221 または 10.211.0.216）

Internet Information Services（IIS）7 アプリケーション： test.kra-sec.cisco.com（10.211.0.223）

ドメイン コントローラ（DC）： dc.kra-sec.cisco.com（10.211.0.221 または 10.211.0.216）：Windows2008

ASA： 10.211.0.162

WebVPN ユーザ名/パスワード： cisco/cisco

添付ファイル： asa-join.pcap（ドメインに正常に参加）

添付ファイル： asa-kerberos-bad.pcap（サービスの要求）

ドメイン コントローラおよびアプリケーションの設定

ドメインの設定

Kerberos により保護されており機能している IIS7 アプリケーションがあることを前提とします

（該当しない場合は「前提条件」を参照してください）。 ユーザの委任の設定を確認する必要があります。

機能ドメイン レベルが Windows Server 2003（以上）に引き上げられていることを確認します。 デフォルトは Windows Server 2000 です。

サービス プリンシパル名（SPN）の設定

正しい委任が設定されている AD でアカウントを設定する必要があります。 Administrator アカウントを使用します。 ASA はそのアカウントを使用するときに、別のユーザの代理として（Constrained Delegation）、固有のサービス（HTTP アプリケーション）のチケットを要求できます。 この処理を実現するには、アプリケーション/サービスに対して正しい委任が作成されている必要があります。

CLI から **setspn.exe**（Windows Server 2003 Service Pack 1 Support Tools の一部）を使用してこの委任を行うには、次のコマンドを入力します。

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

これは、**Administrator username** が、**test.kra-sec.cisco.com** で HTTP サービスの委任対象として信頼されているアカウントであることを示します。

そのユーザの [Delegation] タブを有効にするため、**SPN** コマンドも必要です。 このコマンドを入力すると、Administrator の [Delegation] タブが表示されます。 [Use any authentication protocol] を有効にすることが重要です。これは、[Use Kerberos only] では Constrained Delegation 拡張がサポートされていないためです。

[General] タブで、Kerberos 事前認証を無効にすることもできます。 ただし、この機能はリプレイ攻撃から DC を保護するために使用されるため、これは推奨されません。 ASA は、事前認証を適切に処理できます。

この手順は、コンピュータ アカウントの委任にも適用されます（「信頼」関係を確立するため、ASA はコンピュータとしてドメインに組み込まれます）。

ASA での設定

```
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
```

確認

ドメインへの ASA の参加

kcd-server コマンドの実行後、ASA はドメインへの参加を試行します。

```
********** 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 は、ドメインに正常に参加できます。 認証が正しく完了すると、ASA はプリンシパルのチケットを受信します。 AS_REP パケット（ステップ 1 で説明した Ticket1）の管理者。

サービスの要求

ユーザが WebVPN リンクをクリックします。

ASA が、AS_REP パケットで受信したチケットを使用して、偽装チケットを求める TGS_REQ を送信します。

> **注: PA-FOR-USER** の値は **cisco** です（WebVPN ユーザ）。 **PA-TGS-REQ** には、Kerberos サービス要求に対して受信したチケットが含まれています（ASA ホスト名がプリンシパル）。

ASA は、ユーザ cisco の偽装チケット（ステップ 4 で説明する Ticket2）を含む正しい応答を受信します。

HTTP サービスのチケットに対する要求を次に示します（読みやすくするため一部のデバッグは省略されています）。

```
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 は、HTTP サービスの正しい偽装チケット（ステップ 6 で説明した Ticket3）を受信します。

両方のチケットを検証できます。1 番目のチケットは、ユーザ cisco の偽装チケットです。これは、アクセスする HTTP サービスの 2 番目のチケットを要求および受信するために使用されます。

```
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
```

HTTP チケット（Ticket3）が（SPNEGO を使用した）HTTP アクセスに使用されるので、ユーザはクレデンシャルを入力する必要がありません。

トラブルシューティング

不正確な委任の問題が発生することがあります。 たとえば、ASA はサービス **HTTP/test.kra-sec.cisco.com** を要求するためにチケットを使用しますが（ステップ 5）、応答として **ERR_BADOPTION** の KRB-ERROR が返されます。

これは、委任が正しく設定されていない場合によく発生する問題です。 ASA は「**KDC can't fulfill requested option**」を報告します。

```
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
```

これは、キャプチャで記述されている問題と基本的に同じであり、エラーは BAD_OPTION がある TGS_REQ で発生しています。

応答が Success の場合、ASA は HTTP/test.kra-sec.cisco.com サービスのチケットを受信します。これは、SPNEGO ネゴシエーションに使用されます。 ただし、このエラーが原因で NT LAN Manager (NTLM) がネゴシエートされ、ユーザはクレデンシャルを入力する必要があります。

SPN が 1 つのアカウントだけに登録されていることを確認してください (前の記事のスクリプト)。 エラー KRB_AP_ERR_MODIFIED が発生する場合、一般に、正しいアカウントに SPN が登録されていません。 これは、アプリケーションの実行に使用するアカウントに登録されている必要があります (IIS のアプリケーション プール)。

エラー KRB_ERR_C_PRINCIPAL_UNKNOWN が発生する場合、DC にユーザ (WebVPN ユーザ : cisco) がありません。

ドメインに参加するときにこの問題が発生することがあります。 ASA は AS-REP を受信しますが、LSA レベルで次のエラーで失敗します。 STATUS_ACCESS_DENIED:

この問題を修正するには、DC で該当ユーザ (Administrator) に対する事前認証を有効/無効にする必要があります。

発生する可能性のあるその他の問題の一部を次に説明します。

- ドメインに参加するときに問題が発生する可能性があります。 DC サーバに複数のネットワーク インターフェイス コントローラ (NIC) アダプタ (複数の IP アドレス) が装着されている場合は、ASA がドメインに参加するためにこれのアダプタすべてにアクセスできることを確認します (ドメインは、ドメイン ネーム サーバ (DNS) 応答に基づいてクライアントによりランダムに選択されます)。

- Administrator アカウントの HOST/dc.kra-sec.cisco.com として SPN を設定しないでください。 その設定が原因で DC への接続が失われる可能性があります。

- ASA がドメインに参加した後で、正しいコンピュータ アカウントが DC に作成されていることを検証できます (ASA ホスト名)。 ユーザに、コンピュータ アカウントを追加するための正しい権限が付与されていることを確認します (この例では Administrator が正しい権限を持っています)。

- ASA の正しい Network Time Protocol (NTP) 設定を覚えておいてください。 DC ではデフォルトで、時間の誤差として 5 分が受け入れられます。 このタイマーは DC で変更できます。

- 小さなパケット UDP/88 の Kerberos 接続が使用されていることを検証します。 DC でエラー KRB5KDC_ERR_RESPONSE_TOO_BIG が発生すると、クライアントは TCP/88 に切り替えます。 Windows クライアントが TCP/88 を使用することを強制できますが、ASA はデフォ

ルトで UDP を使用します。

- DC： ポリシーを変更するときには、gpupdate /force を覚えておいてください。
- ASA： test aaa コマンドを使用して認証をテストします。ただし、これは単純な認証である点に注意してください。
- DC サイトでトラブルシューティングを行うには、Kerberos デバッグを有効にしておくと便利です（「Kerberos イベント ロギングを有効にする方法」）。

Cisco Bug ID

関連する Cisco Bug ID の一覧を次に示します。

- Cisco Bug ID CSCsi32224：ASA が Kerberos エラー コード 52 の受信後に TCP に切り替わらない
- Cisco Bug ID CSCtd92673：事前認証が有効な場合に Kerberos 認証が失敗する
- Cisco Bug ID CSCuj19601：ASA Webvpn KCD：再起動後にだけ AD への参加が試行される
- Cisco Bug ID CSCuh32106：8.4.5 以降で ASA KCD が破損している

関連情報

- About Kerberos constrained delegation
- KCD の機能概要
- PIX/ASA： ASDM/CLI を介した VPN クライアント ユーザに対する Kerberos 認証および LDAP 認証サーバ グループの設定例
- Cisco ASA シリーズ コマンド リファレンス
- KDC_ERR_BADOPTION when attempting constrained delegation
- How to force Kerberos to use TCP instead of UDP in Windows
- テクニカルサポートとドキュメント - Cisco Systems