L'intégration du webvpn SSO avec le Kerberos a contraint l'exemple de configuration de délégation

Contenu

Introduction

Ce document décrit comment configurer et dépanner le webvpn simple connectez-vous (SSO) pour les applications qui sont protégées par Kerberos.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration CLI des appareils de Cisco Securit (ASA) et configuration du VPN adaptatives de Protocole SSL (Secure Socket Layer)

- Services de Kerberos

Composants utilisés

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

- Logiciel de Cisco ASA, version 9.0 et ultérieures
- Client de Microsoft Windows 7
- Serveur de Microsoft Windows 2003 et plus tard

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Le Kerberos est un protocole d'authentification de réseau qui permet à des entités réseau pour authentifier entre eux d'une manière sécurisée. Il utilise un tiers de confiance, le centre serveur de distribution de clé (KDC), qui accorde des tickets aux entités réseau. Ces tickets sont utilisés par les entités afin de vérifier et confirmer l'accès au service demandé.

Il est possible de configurer le webvpn SSO pour les applications qui sont protégées par Kerberos avec la délégation appelée par caractéristique de Cisco ASA Kerberos Constrained (KCD). Avec cette configuration, l'ASA peut demander des tickets Kerberos au nom de l'utilisateur portail de webvpn, alors qu'il des applications d'accès protégées par Kerberos.

Quand vous accédez à de telles applications par le portail de webvpn, vous n'avez besoin de ne fournir aucune qualification plus ; au lieu de cela, le compte qui a été utilisé afin de se connecter dans le portail de webvpn est utilisé.

Référez-vous à la compréhension comment section de travaux KCD du pour en savoir plus de guide de configuration ASA.

Interaction de Kerberos avec l'ASA

Pour le webvpn, l'ASA doit demander des tickets au nom de l'utilisateur (parce que l'utilisateur portail de webvpn a accès seulement au portail, pas au service de Kerberos). Pour le ce, l'ASA utilise des extensions de Kerberos pour la délégation contrainte. Voici l'écoulement :

1. L'ASA joint le domaine et obtient un ticket (Ticket1) pour un compte d'ordinateur avec des qualifications configurées sur ASA (ordre de kcd-**serveur**). Ce ticket est utilisé dans les étapes suivantes pour l'accès aux services de Kerberos.

2. L'utilisateur clique sur le lien portail de webvpn pour l'application Kerberos-protégée.

3. L'ASA demande (**TGS-REQ**) un ticket pour le compte d'ordinateur avec son adresse Internet comme principal. Cette demande inclut le champ **PA-TGS-REQ** avec **PA-FOR-USER** avec le

principal comme nom d'utilisateur portail de webvpn, qui est **Cisco** dans ce scénario. Le ticket pour le service de Kerberos de l'étape 1 est utilisé pour l'authentification (délégation correcte).

4. Comme réponse, l'ASA reçoit un ticket personnifié (Ticket2) au nom de l'utilisateur WebVPN (**TGS_REP**) pour le compte d'ordinateur. Ce ticket est utilisé afin de demander des tickets d'application au nom de cet utilisateur WebVPN.

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

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

7. Ce ticket est utilisé d'une manière transparente par l'ASA afin d'accéder au service protégé, et l'utilisateur WebVPN n'a pas besoin de n'entrer dans aucune qualification. Pour l'application de HTTP, le mécanisme simple et protégé de la négociation GSS-API (SPNEGO) est utilisé afin de négocier la méthode d'authentification, et le ticket correct est passé par l'ASA.

Configurez

Topologie

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

Application 7 de l'Internet Information Services (IIS) : test.kra-sec.cisco.com (10.211.0.223)

Contrôleur de domaine (C.C) : 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 de webvpn : Cisco/Cisco

Fichier relié : asa-join.pcap (réussi joignez au domaine)

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

Contrôleur de domaine et configuration d'application

Configurations de domaine

On le suppose qu'il y a déjà une application IIS7 fonctionnelle protégée par Kerberos (sinon, lisez la section de conditions préalables). Vous devez vérifier les configurations pour les délégations des utilisateurs :

Assurez-vous que le niveau fonctionnel de domaine est élevé aux Windows Server 2003 (au moins). Le par défaut est les Windows Server 2000 :

Placez le nom principal de service (SPN)

Vous devez configurer n'importe quel compte sur l'AD avec la délégation correcte. Un compte administrateur est utilisé. Quand les utilisations ASA qui rendent compte, il peut demander un ticket au nom d'un autre utilisateur (délégation contrainte) pour le service spécifique (application de HTTP). Pour que ceci se produise, la délégation correcte doit être créée pour l'application/service.

Afin de faire cette délégation par l'intermédiaire du CLI avec le **setspn.exe, qui** est une partie du WindowsServer des outils d'assistance de 2003 Service Pack 1, sélectionnez cette commande :

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

Ceci indique que le nom d'utilisateur d'**administrateur** est fait confiance expliquent la délégation du service HTTP chez **test.kra-sec.cisco.com**.

La commande **SPN** est également nécessaire afin de lancer l'onglet de **délégation** pour cet utilisateur. Une fois que vous sélectionnez la commande, l'onglet de délégation pour l'administrateur apparaît. Il est important d'activer la « utilisation n'importe quel protocole d'authentification, » parce que le « Kerberos d'utilisation seulement » ne prend en charge pas l'extension contrainte de délégation.

Sur l'**onglet Général**, il est également possible de désactiver la pré-authentification de Kerberos. Cependant, ceci n'est pas informé, parce que cette caractéristique est utilisée afin de protéger le C.C contre des attaques par relecture. L'ASA peut fonctionner avec la pré-authentification correctement.

Cette procédure s'applique également avec la délégation pour le compte d'ordinateur (l'ASA est introduite dans le domaine comme un ordinateur afin d'établir des relations 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
```

Vérifiez

L'ASA joint le domaine

Après que l'ordre de kcd-serveur soit utilisé, les essais ASA pour 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 avec succès le domaine. Après l'authentification correcte, l'ASA reçoit un ticket pour le principal : Administrateur en paquet **AS_REP** (Ticket1 décrit dans Step1).

Demande du service

Le lien de webvpn de clics d'utilisateur :

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

> Remarque: La valeur **PA-FOR-USER** est **Cisco** (utilisateur WebVPN). **PA-TGS-REQ** contient le ticket reçu pour la demande de service de Kerberos (l'adresse Internet ASA est le principal).

L'ASA obtient une réponse correcte avec le ticket personnifié pour l'utilisateur **Cisco** (Ticket2 décrit dans étape 4) :

Voici la demande du ticket pour le service HTTP (une partie met au point est omise pour la 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 personnifié correct pour le service HTTP (Ticket3 décrit dans étape 6).

Les deux tickets peuvent être vérifiés. Le premier est le ticket personnifié pour l'utilisateur Cisco, qui est utilisé afin de demander et recevoir le deuxième ticket pour le service HTTP qui est accédé à :

```
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 de HTTP (Ticket3) est utilisé pour l'accès HTTP (avec SPNEGO), et l'utilisateur n'a pas besoin de fournir toutes les qualifications.

Dépannez

Parfois vous pourriez rencontrer un problème de délégation incorrecte. Par exemple, l'ASA emploie un ticket afin de demander le service **HTTP/test.kra-sec.cisco.com (étape 5), mais la** réponse est KRB-ERROR avec **ERR_BADOPTION** :

C'est un problème rencontré typique quand la délégation n'est pas configurée correctement. Les états ASA que **« KDC ne peut pas accomplir ont demandé l'option »** :

```
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
```

C'est fondamentalement le même problème qui est décrit dans les captures - la panne est à TGS_REQ avec BAD_OPTION.

Si la réponse est succès, alors 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 panne, le LAN Manager de NT (NTLM) est négocié, et l'utilisateur doit fournir des qualifications :

Assurez-vous que le SPN est inscrit à un compte seulement (script d'article précédent). Quand vous recevez cette erreur, KRB_AP_ERR_MODIFIED, il signifie habituellement que le SPN n'est pas inscrit au compte correct. Il devrait être inscrit au compte qui est utilisé afin d'exécuter l'application (groupe d'application sur IIS).

Quand vous recevez cette erreur, KRB_ERR_C_PRINCIPAL_UNKNOWN, il signifie qu'il n'y a aucun utilisateur sur le C.C (utilisateur WebVPN : Cisco).

Vous pourriez rencontrer ce problème quand vous joignez le domaine. L'ASA reçoit AS-REP, mais échoue au niveau LSA avec l'erreur : STATUS_ACCESS_DENIED :

Afin de réparer ce problème, vous devez activer/la pré-authentification sur le C.C pour cet utilisateur (administrateur).

Voici quelques autres problèmes que vous pourriez rencontrer :

- Il pourrait y avoir des problèmes quand vous joignez le domaine. Si le serveur C.C a de plusieurs adaptateurs du contrôleur d'interface réseau (NIC) (plusieurs adresses IP), assurez-vous que l'ASA peut accéder à tous afin de joindre le domaine (choisi aléatoirement par le client basé sur la réponse de Domain Name Server (DN)).

- Ne placez pas SPN comme HOST/dc.kra-sec.cisco.com pour le compte administrateur. Il est possible de perdre la Connectivité au C.C en raison de cette configuration.

- Après que l'ASA joigne le domaine, il est possible de vérifier que le compte correct d'ordinateur est créé sur le C.C (adresse Internet ASA). Assurez-vous que l'utilisateur a les autorisations correctes afin d'ajouter des comptes d'ordinateur (dans cet exemple, l'administrateur a les autorisations correctes).

- Souvenez-vous la configuration correcte de Protocole NTP (Network Time Protocol) sur l'ASA. Par défaut, le C.C reçoit une distorsion minute de l'horloge cinq. Ce temporisateur peut être changé sur le C.C.

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

- C.C : quand vous apportez des changements de politique, souvenez-vous le gpupdate /force.

- ASA : le test d'authentification avec la commande d'**AAA de test**, mais se souviennent que c'est seulement une authentification simple.

- Afin de dépanner sur le site C.C, il est utile d'activer le Kerberos met au point : Comment activer se connecter d'événement de Kerberos.

Id de bogue Cisco

Voici une liste d'id appropriés de bogue Cisco :

- ID de bogue Cisco CSCsi32224 - L'ASA ne commute pas au TCP après réception de code d'erreur 52 de Kerberos
- ID de bogue Cisco CSCtd92673 - L'authentification Kerberos échoue avec le pre-auth activé
- ID de bogue Cisco CSCuj19601 - Webvpn KCD ASA - essayant de joindre l'AD seulement après la réinitialisation
- ID de bogue Cisco CSCuh32106 - ASA KCD est cassée dans 8.4.5 en avant

Informations connexes

- Au sujet du Kerberos délégation contrainte
- Comprenant comment KCD fonctionne
- PIX/ASA : Authentification Kerberos et groupes de serveurs d'autorisation de LDAP pour des utilisateurs de client vpn par l'intermédiaire d'exemple de configuration ASDM/CLI
- Référence de commandes de gamme de Cisco ASA
- KDC_ERR_BADOPTION en tentant la délégation contrainte
- Comment forcer le Kerberos pour utiliser le TCP au lieu de l'UDP dans Windows
- Support et documentation techniques - Cisco Systems