WebVPN与Kerberos的SSO集成限制条件授权配置示例

目录

简介

本文描述如何配置和排除故障WebVPN单个符号(SSO)由Kerberos保护的应用程序的。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- 思科可适应Securit设备(ASA) CLI配置和安全套接字层SSL VPN配置
- Kerberos服务

使用的组件

本文档中的信息基于以下软件版本：

- Cisco ASA软件，版本9.0和以上
- Microsoft Windows 7客户端
- Microsoft Windows 2003服务器和以后

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

Kerberos是允许网络实体彼此验证以安全方式的网络验证协议。它使用委托第三方，密钥分配中心(KDC)，授权到网络实体的票。实体用于这些票为了验证和确认对请求的服务的访问。

是可能的配置由与思科ASA功能呼叫的Kerberos Constrained的授权的应用程序的WebVPN SSO (KCD)的Kerberos保护。使用此功能， ASA能代表WebVPN门户用户请求Kerberos票，而它Kerberos保护的访问应用程序。

当您通过WebVPN门户时访问这样应用程序，您不需要再提供任何凭证;反而，使用为了登录WebVPN门户使用的帐户。

参考了解KCD如何工作ASA配置指南的部分欲知更多信息。

与ASA的Kerberos交互作用

对于WebVPN， ASA必须代表用户(因为WebVPN门户用户访问仅门户，不是Kerberos服务)请求票。为此， ASA使用Kerberos扩展Constrained授权。这是流：

1. ASA加入域并且获取一张票(Ticket1)与在ASA配置的凭证的一个计算机帐户的(kcd**服务器**命令)。此票用于以下步骤对Kerberos服务的访问。

2. 用户点击Kerberos保护的应用程序的WebVPN门户链路。

3. ASA请求(**TGS-REQ**)计算机帐户的一张票与其主机名作为负责人。此请求包括有**PA-FOR-USER的PA-TGS-REQ**字段与负责人作为WebVPN门户用户名，是在此方案的**cisco**。Kerberos服务的票从Step1使用验证(正确授权)。

4. 作为答复， ASA代表WebVPN用户(**TGS_REP**)接收一张被扮演的票(Ticket2)计算机帐户的。此票用于为了代表此WebVPN用户请求应用程序票。

5. ASA启动另一请求(**TGS_REQ**)为了获取应用程序的(**HTTP/test.kra-sec.cisco.com)票。此请求**再使用PA-TGS-REQ字段**，这次**，不用**PA-FOR-USER字段，但是以**接收的被扮演的票在步骤4。

6. 答复(**TGS_REQ**)与被扮演的票(Ticket3)应用程序的返回。

7. ASA用于此票透明地为了访问已保护服务，并且WebVPN用户不需要输入任何凭证。对于Http应用，简单和已保护GSS-API协商(SPNEGO)机制用于为了协商认证方法，并且正确票由

ASA通过。

配置

拓扑

域：kra-sec.cisco.com (10.211.0.221或10.211.0.216)

互联网信息服务(IIS) 7应用程序：test.kra-sec.cisco.com (10.211.0.223)

域控制器(DC) ：dc.kra-sec.cisco.com (10.211.0.221或10.211.0.216) - Windows2008

ASA ：10.211.0.162

WebVPN用户名/密码：cisco/cisco

附加的文件：ASAjoin.pcap (对域的成功的加入)

附加的文件：ASA Kerberosbad.pcap (要求服务)

域控制器和应用程序配置

域设置

假设，已经有Kerberos保护的一功能IIS7应用程序(如果没有，请读Prerequisites部分)。您必须检查设置用户的授权：

保证功能域标准提高到Windows服务器2003年(至少)。默认是Windows服务器2000年：

设置服务主体名称(SPN)

您必须配置在AD的所有帐户与正确授权。使用管理员帐户。当认为的ASA用途，它能代表另一个用户(限制条件的授权)请求票特定服务的(Http应用)。为了此能发生，正确授权必须为应用程序/服务创建。

为了通过与**setspn.exe的**CLI做此授权，是WindowsServer部分2003个服务包1支持工具，请输入此命令：

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

这表明**管理员用户名**是HTTP服务的授权的信托帐户在**test.kra-sec.cisco.com**。

SPN命令也是必要为了激活该用户的**授权**选项卡。一旦输入命令，管理员的授权选项卡出现。启用“使用所有认证协议是重要的”，因为“使用Kerberos”只不支持限制条件的授权分机。

在**常规选项卡**，禁用Kerberos预验证也是可能的。然而，因为此功能用于为了保护DC以防止重放攻

击，这没有建议。ASA能正确地与预验证一起使用。

此步骤也适用与授权为计算机帐户(ASA被带领进入域作为计算机为了建立“信任”关系)：

在ASA的配置

```
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
```

验证

ASA加入域

在使用后kcd**服务器**命令，ASA设法加入域：

```
********** 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能顺利地加入域。在正确验证， ASA接收负责人的后一张票：AS_REP数据包的(在Step1描述的Ticket1管理员)。

要求服务

用户点击WebVPN链路：

ASA发送一张被扮演的票的**TGS_REQ**与在**AS_REP**数据包接收的票：

> **Note**:**PA-FOR-USER**值是**cisco** (WebVPN用户)。**PA-TGS-REQ**包含为Kerberos服务请求接收的票(ASA主机名是负责人)。

ASA获得与被扮演的票的一正确答复用户的**cisco** (在步骤描述的Ticket2 4) ：

这是要求HTTP服务的票(一些调试为了清晰省略) ：

```
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
```

ASA接收HTTP服务的(在步骤描述的Ticket3正确被扮演的票6)。

两张票可以验证。第一个是用户的**cisco**被扮演的票，用于为了请求和接收HTTP服务的第二张票访问：

```
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
```

此HTTP票(Ticket3)使用HTTP访问(与SPNEGO)和用户不需要提供所有凭证。

故障排除

有时您也许遇到不正确授权问题。例如， ASA使用一张票为了请求服务**HTTP/test.kra-sec.cisco.com (步骤5)，但是**答复是与**ERR_BADOPTION的**KRB-ERROR ：

当授权没有正确地时，配置这是遇到的一典型的问题。ASA报道**"KDC不能执行请求的选项"**：

```
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
```

这基本上是在捕获描述-的同一问题失败是**在与BAD_OPTION的TGS_REQ**。

如果答复是**成功**，则ASA接收**HTTP/test.kra-sec.cisco.com服务的**一张票，使用SPNEGO协商**。然而**，由于失败， NT LAN Manager (NTLM)**协商，**并且用户必须提供凭证：

确保SPN为仅一个帐户注册(从上一个条款的脚本)。当您收到此错误，**KRB_AP_ERR_MODIFIED时**，通常意味着**SPN没有**为正确帐户注册。应该为使用为了运行应用程序的帐户注册它(IIS的应用程序池)。

当您收到此错误时， **KRB_ERR_C_PRINCIPAL_UNKNOWN**，意味着没有DC的(WebVPN用户用户：**cisco**)。

当您加入域时，您也许遇到此问题。ASA在与错误的**LSA**级别上接收**AS-REP**，但是失效：**STATUS_ACCESS_DENIED** ：

为了解决此问题，您必须启用/禁用在DC的预验证该用户的(**管理员**)。

这是您也许遇到的一些其他问题：

- 当您加入域时，也许有问题。如果DC Server有多个网络网络界面控制器(NIC)适配器(多个IP地址)，请确保ASA能访问所有为了加入域(随机地选择由根据域名服务器(DNS)答复)的客户端。
- 请勿设置**SPN**作为**管理员帐户的HOST/dc.kra-sec.cisco.com。**丢失连接到设置的DC因此**是**可能的。
- 在ASA加入域后，验证是可能的正确计算机帐户在DC (ASA主机名)创建。确保用户有正确权限

为了添加计算机帐户(在本例中，**管理员**有正确权限)。

- 切记在ASA的正确**网络时间协议(NTP)**配置。默认情况下， DC接受五分钟时滞。该计时器在DC可以更改。
- 验证使用小数据包的**UDP/88**连接的Kerberos。在从DC的错误以后，**KRB5KDC_ERR_RESPONSE_TOO_BIG**，客户端换成**TCP/88**。迫使Windows客户端使用**TCP/88**是可能的，**默认情况下，**但是**ASA将使用UDP**。
- DC:当您做策略变更时，请记住**gpupdate /force**。
- ASA ：测试与**aaa命令的测验的**验证，但是记住它是仅简单验证。
- 为了排除故障在DC站点，启用Kerberos调试是有用的：如何启用Kerberos事件日志。

Cisco Bug ID

这是相关Cisco Bug ID列表：

- Cisco Bug ID CSCsi32224 - ASA不换成TCP在接收Kerberos错误代码以后52
- Cisco Bug ID CSCtd92673 - Kerberos认证失效与启用的PRE验证
- Cisco Bug ID CSCuj19601 - ASA WebVPN KCD -尝试在重新启动之后加入AD
- Cisco Bug ID CSCuh32106 - ASA KCD向前是残破的在8.4.5

相关信息

- **关于Kerberos限制条件的授权**
- **知道KCD如何工作**
- **PIX/ASA：VPN客户端用户的Kerberos认证和LDAP授权服务器组通过ASDM/CLI配置示例**
- **思科ASA系列命令参考**
- **KDC_ERR_BADOPTION，当尝试限制条件的授权时**
- **如何强制Kerberos使用TCP而不是UDP在Windows**
- **技术支持和文档 - Cisco Systems**