Step-By-Step Comprehensive Guide: How to configure Citrix NetScaler for User Client Certificate Based Authentication with Kerberos Constrained Delegation Single Sign-On (KCD SSO) for Microsoft Exchange ActiveSync 2007 / 2010 / 2013 (without Microsoft ForeFront TMG)

Created by Rafyel G. Brooks (Sr. Network Engineer) - August 8, 2014

Expectations & Benefits:

1. **User Experience:** Upon changing their Active Directory network password users will NOT be prompted to enter or update it on their mobile device(s).
2. **Security:** Reverse Proxy (CSW) if configured, Authentication Redirection by 401-Challenge Response (AAA), and User Certificate requirement.
3. **SSL Offloading:** the ability to unload heavy CPU transactions from your Windows Servers (Exchange CAS).
4. **Access Control:** Management of who can access email on mobile device (User Client Certificates)

Informational Notes:

Document updates are marked in **RED**.

The reference version and build number of Citrix NetScaler ADC used in this guide is **v10.1.128.8**

This guide is written in Seventeen (17) steps to easily reference the configuration components and is organized in the order in which configuration features will be needed. I encourage you to read through this guide in its entirety before beginning configuration just to ensure you have a general understanding of the architecture and what is to be expected during setup.

This guide can be configured with the use of a CSW (Content Switching) Virtual Server quite easily for the added benefit and security of a Reverse Proxy, but for simplicity it is written with use of only a TM (Traffic Management) Virtual Server, as there are multiple methods for configuring Exchange CAS services in a CSW. The benefits of configuring a CSW and SSL Offloading is the security of a Reverse Proxy, removing CPU load from your Windows servers, and the ability to utilize a single Public IP for all your Exchange CAS services, if desired. If you are new to CSW find a guide on Google or Bing for Exchange CAS and simply follow the steps mentioned here on the TM and AAA virtual servers only, do not apply these steps to the CSW vServer itself.

STEP #1:

PREPARATION

First and foremost, you will need a working ActiveSync configuration on your Exchange CAS already! Also, it is assumed that your website SSL Certificate(s) (**Server Certificate**) along with matching Root Certificate(s) (**CA Certificate**) are installed on the NetScaler(s) properly. For this guide I am using internal CA certificates. You will need to configure them as such for each Virtual Server mentioned here. With that said, for this guide, it is also assumed you have a working internal CA to issue User certificates and Server certificates, as well as revoke them by CRL (third-party certificates may work just the same).

In this guide I use the following to reference the SSL certificates that will configured on the NetScaler: "ExchangeCAS.domain.com" (**Server Certificate**), "RootCA.domain.com" (**CA Certificate**)

*Replace the User and Virtual Server names I've entered in Bold with your chosen names.

If you have multiple sites you can setup a KCD user account in Active Directory for each site. Example: You have a NetScaler or local HA pair on the East Coast (NY) and on the West Coast (SF). I.e. **svcKCD01NY** and **svcKCD01SF**
Password = **Password123**
(Be sure to set the DO NOT to expire password option on the account)

Define a "FQDN" for the TM virtual server(s) you will create to load-balance your Exchange CAS servers by using your internal domain name in the actual virtual servers name. Think of your TM virtual server name as the FQDN for a host server.
i.e. "**KCDvServer.domain.com";** OR **KCDvServer.corp.domain.com** (this name example is if your Active Directory domain name was setup according to the latest recommendations for organizations with internal and external domains of the same name - References: http://support.microsoft.com/kb/909264, http://technet.microsoft.com/en-us/library/cc738121%28WS.10%29.aspx, http://acbrownit.wordpress.com/2013/04/15/active-directory-domain-naming-in-the-modern-age/, or http://www.mdmarra.com/2012/11/why-you-shouldnt-use-local-in-your.html).

TIP: Use a name easily identifiable to eliminate confusion of vServers and SPN's. Example: "ActiveSync2013vSRV.domain.com"; or "ExchangeCAS13vSRV.corp.domain.com" (if you intend to use the same authentication method for publishing all CAS services)

Open the DMZ Firewall ports From your SNIP To your internal servers (Exchange CAS, Domain Controllers, and DNS servers).
*Note you must open UDP & TCP where specified!

Port	Protocol	Use
53	UDP/ TCP	DNS
88	UDP/TCP	Kerberos
123	UDP	NTP

135	TCP	RPC Endpoint Mapper
137	UDP	NetBIOS Name Service
139	TCP	NetBIOS Session (SMB)
389	UDP/TCP	LDAP
445	TCP	SMB over TCP
464	UDP/TCP	Machine password changes (typically after 30 days)
3268	TCP	Global Catalog Search

* Make certain you can reach / ping your sites Domain Controllers from the NetScalers GUI or PUTTY. Your Firewall must open DNS ports (source is SNIP with destination as your Domain Controllers.) Create a DNS Virtual Server pointing to your Domain Controllers as UDP and create another using TCP.

* Create a DNS “A” record on the NetScaler with your internal Domain Name. (i.e. DOMAIN.com = DNS IP’s; CORP.DOMAIN.com = DNS IP’s)

* Make certain your NetScalers NTP is setup, correctly matching your Domain Controllers time within 5min or less, and configured to sync for updates. TIP: If NTP is setup correctly in the GUI but the NetScalers System Time is still offset, reconfigure your NTP settings via PUTTY using the “CONFIGNS” cmd.

STEP #2:

Setup IIS for "Window Authentication", "Client Certificate Mapping", and “Negotiate,NTLM” Providers on each Exchange CAS that will be load-balanced

1. Search on the Internet for how to do this if not already configured, maybe you're using ForeFront TMG for this and it’s already set. You could read the Citrix article CTX139133. It varies slightly depending on the version of IIS you’re using.

STEP #3:

HOW-TO: Citrix NetScaler configuration setup of ActiveSync with Client Certificate Authentication and KCD SSO.

Active Directory User Service Account for KCD

1. Create a new service account for KCD in Active Directory. I.e. "**svcKCD01NY**" (it doesn't need admin right's when setup is complete but start with Domain Admins just to get setup for joining the NetScaler to the Domain. i.e. KCD Domain Join)
2. Logon to a Domain Controller and open an Administrative Command-Prompt.
3. Run the following command to create an SPN that will enable the Delegation tab on the KCD account in Active Directory: "setspn -A host/kcdvserver.domain.com DOMAIN\svcKCD01NY" OR "setspn -A host/kcdvserver.corp.domain.com CORP\svcKCD01NY" (remove the double-quotes when typing)
4. After you've created the SPN via the command-line the Delegation tab should now be available in the properties of the KCD user account but you will not see the SPN you've just set in the Delegation tab. (to see the list of SPN's for the account: "setspn -l DOMAIN\svcKCD01NY") (to remove an SPN type: setspn –d "*spn*" DOMAIN\svcKCD01NY").
5. In the Delegation tab of the user account select the radio button for "Trust this user for delegation to specified services on" AND "Use any authentication protocol"
6. Click the "Add" button and enter the name of each of your Exchange CAS servers that will be servicing ActiveSync for that site with the service type as "HTTP".
7. Click OK to close the window.

STEP #4:

Generating the Keytab File - for the NetScaler KCD account to use the Active Directory KCD user service account. GUI and CMD-Line explained. (The account can be created as a Computer account with a password defined but this guide is written with a User account and password)

1. Info: In the Keytab script we will be creating a new SPN for the Active Directory KCD user service account as: "**host/kcdvserver.domain.com**"; OR "**host/kcdvserver.corp.domain.com**" (this is done in the next step via the GUI in v10.1.x
2. Navigate to "Security > AAA - Application Traffic"
3. Click "Batch file to generate Keytab" listed under the heading **Kerberos Constrained Delegation**
4. Type the requested information just as shown here: Domain User Name* = "svcKCD01NY"; Domain Password* = "Password123"; Service Principal* = "kcdvserver.domain.com@DOMAIN.COM"; OR "kcdvserver.corp.domain.com@CORP.DOMAIN.COM"; Output File Name* = "C:\kcdvserver.keytab" (based on v10.1.127.10 reference, "host/", will automatically be added in front of the vServer name when the script is generated, so just type it as shown here).
5. Click **Generate Script**. In the script you should see two SPN's, likely on the 5th and 6th lines, defined as: "setspn -A HTTP/%kcdusername% %USERDOMAIN%\%kcdusername%" and "setspn -A host/kcdvserver.domain.com@DOMAIN.COM"; OR "host/kcdvserver.corp.domain.com@CORP.DOMAIN.COM"
6. Select and Copy the text in the script, paste into a text file and save with ".bat" or ".cmd" extension and run the file from a Domain Controller. After complete, type the following in the cmd-line to see a list of all SPN's for the service account: "setspn -l

DOMAIN\svcKCD01NY" OR "CORP\svcKCD01NY" (** if you're are using the recommended domain naming format mentioned above, i.e. Corp.Domain.com, and have also defined a global SPN for your user accounts to match your external domain name as part of their email address then also use "DOMAIN\svcKCD01NY")

7. You will find the newly generated file at "C:\kcdvserver.keytab"
8. Skip if using the GUI - **CMD-Line Method**: Alternatively, you can generate the keytab file via the cmd prompt on a Domain Controller: "ktpass /princ host/kcdvserver.domain.com@DOMAIN.COM / type KRB5_NT_PRINCIPAL /mapuser DOMAIN\svcKCD01NY /pass Password123 -out C:\kcdvserver.keytab"; OR "ktpass /princ host/kcdvserver.corp.domain.com@CORP.DOMAIN.COM / type KRB5_NT_PRINCIPAL /mapuser CORP\svcKCD01NY /pass Password123 -out C:\kcdvserver.keytab"
9. Copy the C:\kcdvserver.keytab file to the /nsconfig/krb directory on the NetScaler appliance using WinSCP.

STEP #5:

Create the NetScaler KCD Account

1. On the NetScaler GUI navigate to Security > AAA - Application Traffic > KCD Accounts.
2. Click "Add" and create a name for your NetScalers local KCD Account. (i.e. "NetScalerKCD-NY")
3. Select the radio button for "Use Key Tab File"
4. Choose "Browse" to look on your local NetScaler in the directory where you placed the keytab file with WinSCP in "/nsconfig/krb"
5. Click OK.
6. The entry on the NetScaler should now read as: Name = "NetScalerKCD-NY"; Keytab File Path = "/nsconfig/krb/kcdvserver.keytab"; Host SPN = "host/kcdvserver.domain.com@DOMAIN.COM"; OR "host/kcdvserver.corp.domain.com"

STEP #6:

KCD Domain Join

Note: You may not see an object in your Active Directory farm when these steps are complete. You must have the DNS steps completed and working as described in Step #1 - PREPARATION, before going forward!

1. Navigate to; "Security > AAA - Application Traffic"
2. Choose "Kerberos Domain Join"
3. Click the plus-sign "+" to create a new Windows Profile
4. A "Create Negotiate Server" window will appear. Enter the requested information by creating any **Name = "**KCDNEGSERVER"; **Domain Name* =** "DOMAIN.com"; OR "CORP.DOMAIN.com"; **Password*** = "Password123"
5. Click OK

STEP #7:

Create your TM (Traffic Management) Load-Balancing Virtual Server for your Exchange CAS

1. Add the Exchange CAS servers in TM using the DNS name and NOT the IP Address.
2. Create an SSL Service for the Exchange CAS servers
3. Create an SSL load-balancing Virtual Server and name it exactly as “kcdvserver.domain.com”; OR “kcdvserver.corp.domain.com” and add the SSL service created in the step above. Use an IP that can be externally accessed via a NAT such as a DMZ IP.
4. For the Method and Persistence tab choose; "Least Connection" for the Method, and “COOKIEINSERT" with Time-out (min) = “0” for the Persistence.
5. Select the SSL Settings tab.
6. Import your SSL certificates from the Available field to the Configured field by choosing the Add button as follows; “ExchangeCAS.domain.com” (**Server Certificate**), “RootCA.domain.com” (**CA Certificate**).

STEP #8:

Create a AAA Virtual Server (i.e. "ActiveSync-AAA")

1. Navigate to; Security > AAA - Application Traffic > Virtual Server
2. Click “Add”, give it a name,"ActiveSync-AAA”, and an IP from within your DMZ.
3. In the Domain field enter your internal AD Domain Name: i.e. “DOMAIN.com"; OR “CORP.DOMAIN.com”
4. Import your SSL certificates from the Available field to the Configured field by choosing the Add button as follows; “ExchangeCAS.domain.com” (**Server Certificate**), “RootCA.domain.com” (**CA Certificate**).

STEP #9:

Create a Session policy

1. Navigate to; Security > AAA - Application Traffic > Policies > Session.
2. Select the Profile tab and click **Add**.
3. In the Configure Session Profile window set the following; **Name** = “SSOsession_Profile"; **Session Time-out (mins)** = “43829"; **Default Authentication Action*** = “ALLOW"; enable "**Single Sign-on to Web Applications**"; **Credential Index*** = “PRIMARY"; **Single Sign-on Domain** = “DOMAIN.com"; OR “CORP.DOMAIN.com"; **HTTPOnly Cookie*** = “YES"; enable "**Enable Persistent Cookie**"; **Persistent Cookie Validity** = “43828"; **KCD Account** = “NetScalerKCD-NY"
4. Click OK.
5. Select the Policies tab and click **Add**.
6. Assign a name to the Policy; **Name** = “SSOsession_Policy"; **Expression** = “ns_true"; **Request Profile*** = select the "*SSOsession_Profile*" you just created in the drop-down.
7. Click OK

STEP #10:

Create a CERT policy

1. Navigate to; Security > AAA - Application Traffic > Policies > Authentication > CERT
2. Select the Servers tab and click **Add**.
3. Enter the following in the Configure Authentication Server window; **Name*** = “CERT_server"; **Two Factor** = “OFF"; **User Name Field** = “SubjectAltName:PrincipalName"
4. Click OK.
5. Select the Policies tab and click **Add**.
6. Enter the following in the Configure Authentication Policy window; **Name*** = “CERT_policy"; **Expression** = “ns_true"; **Server** = select the “*CERT_server*” you just created in from the drop-down menu.
7. Click OK.

STEP #11:

Configure Client Certificate Based Authentication in AAA Virtual Server

1. Navigate to; Security > AAA - Application Traffic > Virtual Server
2. Select and open the AAA Virtual Server you created in Step #8; “ActiveSync-AAA"
3. Click the "SSL Parameters" radio button.
4. Enable the “Client Authentication” check box and select “*Mandatory*” from the drop-down menu.
5. Click OK.

STEP #12:

Configure Client Certificate Based Authentication in TM (Traffic Management) Virtual Server

1. Navigate to; Traffic Management > Load Balancing > Virtual Server
2. Select and open the TM Virtual Server you created in Step #7; “kcdvserver.domain.com"; OR “kcdvserver.corp.domain.com"
3. Select the SSL Settings tab.
4. Click the "SSL Parameters” radio button.
5. Enable the “Client Authentication” check box and select “*Mandatory*” from the drop-down menu.
6. Click OK.

STEP #13:

Bind the CERT Policy to the AAA Virtual Server

1. Navigate to; Security > AAA - Application Traffic > Virtual Server
2. Select and open the AAA Virtual Server you created in Step #8; “ActiveSync-AAA”
3. Select the Authentication tab.
4. Click “Insert Policy” in the bottom windowpane and select the “*CERT_Policy*” you created earlier from the drop-down menu.
5. Click OK.

STEP #15:

Bind the Session Policy to the AAA Virtual Server

1. Navigate to; Security > AAA - Application Traffic > Virtual Server
2. Select and open the AAA Virtual Server you created in Step #8; “ActiveSync-AAA”
3. Select the Policies tab.
4. Select the "Session” sub-category.
5. Click “Insert Policy” in the bottom windowpane and select the “*Session_Policy*” you created earlier from the drop-down menu.
6. Click OK.

STEP #16:

Bind the AAA Virtual Server to the TM virtual server

1. Navigate to; Traffic Management > Load Balancing > Virtual Server
2. Select and open the TM Virtual Server you created in Step #7; “kcdvserver.domain.com"; OR “kcdvserver.corp.domain.com"
3. Select the Advanced tab.
4. Scroll to the bottom of the page expanding Authentication Settings, select the check box next to “401 Based Authentication”, and next to Authentication VServer select your AAA Virtual Server “*ActiveSync-AAA*”.

Test your configuration setup with a mobile device!!! ("iPhone, iPad (iOS Configuration Utility or AirWatch), Android (TouchDown Mail Client or AirWatch), Windows Phone (AirWatch)")

Limitations Impact and Explanation:

HA Failover: SSL Traffic Management Virtual Servers cannot be configured with Connection Failover in the Advanced tab. All sessions will be dropped but no authentication prompt will be presented on the device, this is the same behavior as with Microsoft Forefront TMG. However, devices will automatically initiate communications with the new Primary NetScaler (if configured with local HA or a GSLB). There will be a minimum delay for the arrival of new mail onto the devices as new Kerberos TGT tickets will need to be generated on the new Primary NetScaler for each user & device. Currently, Citrix provides no solution or workaround as sharing SSL sessions. However, Citrix may provide a newer firmware build to this as a much desired solution. (NetScaler appliances are known for their reliability and under normal working conditions the primary appliance would be Up servicing uninterrupted SSL sessions unless the primary NetScaler is powered-Off, or a failover occurs).

Disclaimer - I have no affiliations with the mentioned vendors or any products and services mentioned. It is your responsibilities backup your NetScalers configuration before making any changes for recovery if needed. You are responsible for all risks and support of the changes made by the configurations described.*

———>

Volume. 2 - Troubleshooting Guide:

Kerberos Live Logging

To see a live log of KCD authentication for users run the following CMD in PuTTy or from the GUI:

shell

cat /tmp/nskrb.debug

_____

To export a copy recent KCD log events type:

shell

cat /tmp/nskrb.debug > /var/nskrb.debug tail -f /var/nskrb.debug

_____

To see a list of Kerberos TGT tickets for each user type:

shell

cd /var/krb

ls

_____

If any errors codes are reported in the logs for authentication check against the following list for descriptions:

Reference = https://andromeda.rutgers.edu/~sysmail/krb5_error.html

Quick View:

Error Number	Symbolic Name	Descriptive Text
-1765328383	KRB5KDC_ERR_NAME_EXP	Client's entry in database has expired
-1765328382	KRB5KDC_ERR_SERVICE_EXP	Server's entry in database has expired
-1765328381	KRB5KDC_ERR_BAD_PVNO	Requested protocol version not supported
-1765328380	KRB5KDC_ERR_C_OLD_MAST_KVNO	Client's key is encrypted in an old master key
-1765328379	KRB5KDC_ERR_S_OLD_MAST_KVNO	Server's key is encrypted in an old master key
-1765328378	KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN	Client not found in Kerberos database
-1765328377	KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN	Server not found in Kerberos database
-1765328376	KRB5KDC_ERR_PRINCIPAL_NOT_UNIQUE	Principal has multiple entries in Kerberos database
-1765328375	KRB5KDC_ERR_NULL_KEY	Client or server has a null key
-1765328374	KRB5KDC_ERR_CANNOT_POSTDATE	Ticket is ineligible for postdating

-1765328373	KRB5KDC_ERR_NEVER_VALID	Requested effective lifetime is negative or too short
-1765328372	KRB5KDC_ERR_POLICY	KDC policy rejects request
-1765328371	KRB5KDC_ERR_BADOPTION	KDC can't fulfill requested option
-1765328370	KRB5KDC_ERR_ETYPE_NOSUPP	KDC has no support for encryption type
-1765328369	KRB5KDC_ERR_SUMTYPE_NOSUPP	KDC has no support for checksum type
-1765328368	KRB5KDC_ERR_PADATA_TYPE_NOSUPP	KDC has no support for padata type
-1765328367	KRB5KDC_ERR_TRTYPE_NOSUPP	KDC has no support for transited type
-1765328366	KRB5KDC_ERR_CLIENT_REVOKED	Clients credentials have been revoked
-1765328365	KRB5KDC_ERR_SERVICE_REVOKED	Credentials for server have been revoked
-1765328364	KRB5KDC_ERR_TGT_REVOKED	TGT has been revoked
-1765328363	KRB5KDC_ERR_CLIENT_NOTYET	Client not yet valid - try again later
-1765328362	KRB5KDC_ERR_SERVICE_NOTYET	Server not yet valid - try again later
-1765328361	KRB5KDC_ERR_KEY_EXP	Password has expired
-1765328360	KRB5KDC_ERR_PREAUTH_FAILED	Preauthentication failed
-1765328359	KRB5KDC_ERR_PREAUTH_REQUIRED	Additional pre-authentication required
-1765328358	KRB5KDC_ERR_SERVER_NOMATCH	Requested server and ticket don't match
-1765328357	KRB5PLACEHOLD_27	KRB5 error code 27
-1765328356	KRB5PLACEHOLD_28	KRB5 error code 28
-1765328355	KRB5PLACEHOLD_29	KRB5 error code 29
-1765328354	KRB5PLACEHOLD_30	KRB5 error code 30
-1765328353	KRB5KRB_AP_ERR_BAD_INTEGRITY	Decrypt integrity check failed
-1765328352	KRB5KRB_AP_ERR_TKT_EXPIRED	Ticket expired
-1765328351	KRB5KRB_AP_ERR_TKT_NYV	Ticket not yet valid
-1765328350	KRB5KRB_AP_ERR_REPEAT	Request is a replay
-1765328349	KRB5KRB_AP_ERR_NOT_US	The ticket isn't for us
-1765328348	KRB5KRB_AP_ERR_BADMATCH	Ticket/authenticator don't match
-1765328347	KRB5KRB_AP_ERR_SKEW	Clock skew too great
-1765328346	KRB5KRB_AP_ERR_BADADDR	Incorrect net address
-1765328345	KRB5KRB_AP_ERR_BADVERSION	Protocol version mismatch
-1765328344	KRB5KRB_AP_ERR_MSG_TYPE	Invalid message type
-1765328343	KRB5KRB_AP_ERR_MODIFIED	Message stream modified
-1765328342	KRB5KRB_AP_ERR_BADORDER	Message out of order
-1765328341	KRB5KRB_AP_ERR_ILL_CR_TKT	Illegal cross-realm ticket
-1765328340	KRB5KRB_AP_ERR_BADKEYVER	Key version is not available
-1765328339	KRB5KRB_AP_ERR_NOKEY	Service key not available
-1765328338	KRB5KRB_AP_ERR_MUT_FAIL	Mutual authentication failed
-1765328337	KRB5KRB_AP_ERR_BADDIRECTION	Incorrect message direction
-1765328336	KRB5KRB_AP_ERR_METHOD	Alternative authentication method required
-1765328335	KRB5KRB_AP_ERR_BADSEQ	Incorrect sequence number in message
-1765328334	KRB5KRB_AP_ERR_INAPP_CKSUM	Inappropriate type of checksum in message
-1765328333	KRB5PLACEHOLD_51	KRB5 error code 51
-1765328332	KRB5PLACEHOLD_52	KRB5 error code 52
-1765328331	KRB5PLACEHOLD_53	KRB5 error code 53

-1765328330	KRB5PLACEHOLD_54	KRB5 error code 54
-1765328329	KRB5PLACEHOLD_55	KRB5 error code 55
-1765328328	KRB5PLACEHOLD_56	KRB5 error code 56
-1765328327	KRB5PLACEHOLD_57	KRB5 error code 57
-1765328326	KRB5PLACEHOLD_58	KRB5 error code 58
-1765328325	KRB5PLACEHOLD_59	KRB5 error code 59
-1765328324	KRB5KRB_ERR_GENERIC	Generic error (see e-text)
-1765328323	KRB5KRB_ERR_FIELD_TOOLONG	Field is too long for this implementation
-1765328322	KRB5PLACEHOLD_62	KRB5 error code 62
-1765328321	KRB5PLACEHOLD_63	KRB5 error code 63
-1765328320	KRB5PLACEHOLD_64	KRB5 error code 64
-1765328319	KRB5PLACEHOLD_65	KRB5 error code 65
-1765328318	KRB5PLACEHOLD_66	KRB5 error code 66
-1765328317	KRB5PLACEHOLD_67	KRB5 error code 67
-1765328316	KRB5PLACEHOLD_68	KRB5 error code 68
-1765328315	KRB5PLACEHOLD_69	KRB5 error code 69
-1765328314	KRB5PLACEHOLD_70	KRB5 error code 70
-1765328313	KRB5PLACEHOLD_71	KRB5 error code 71
-1765328312	KRB5PLACEHOLD_72	KRB5 error code 72
-1765328311	KRB5PLACEHOLD_73	KRB5 error code 73
-1765328310	KRB5PLACEHOLD_74	KRB5 error code 74
-1765328309	KRB5PLACEHOLD_75	KRB5 error code 75
-1765328308	KRB5PLACEHOLD_76	KRB5 error code 76
-1765328307	KRB5PLACEHOLD_77	KRB5 error code 77
-1765328306	KRB5PLACEHOLD_78	KRB5 error code 78
-1765328305	KRB5PLACEHOLD_79	KRB5 error code 79
-1765328304	KRB5PLACEHOLD_80	KRB5 error code 80
-1765328303	KRB5PLACEHOLD_81	KRB5 error code 81
-1765328302	KRB5PLACEHOLD_82	KRB5 error code 82
-1765328301	KRB5PLACEHOLD_83	KRB5 error code 83
-1765328300	KRB5PLACEHOLD_84	KRB5 error code 84
-1765328299	KRB5PLACEHOLD_85	KRB5 error code 85
-1765328298	KRB5PLACEHOLD_86	KRB5 error code 86
-1765328297	KRB5PLACEHOLD_87	KRB5 error code 87
-1765328296	KRB5PLACEHOLD_88	KRB5 error code 88
-1765328295	KRB5PLACEHOLD_89	KRB5 error code 89
-1765328294	KRB5PLACEHOLD_90	KRB5 error code 90
-1765328293	KRB5PLACEHOLD_91	KRB5 error code 91
-1765328292	KRB5PLACEHOLD_92	KRB5 error code 92
-1765328291	KRB5PLACEHOLD_93	KRB5 error code 93
-1765328290	KRB5PLACEHOLD_94	KRB5 error code 94
-1765328289	KRB5PLACEHOLD_95	KRB5 error code 95
-1765328288	KRB5PLACEHOLD_96	KRB5 error code 96

-1765328287	KRB5PLACEHOLD_97	KRB5 error code 97
-1765328286	KRB5PLACEHOLD_98	KRB5 error code 98
-1765328285	KRB5PLACEHOLD_99	KRB5 error code 99
-1765328284	KRB5PLACEHOLD_100	KRB5 error code 100
-1765328283	KRB5PLACEHOLD_101	KRB5 error code 101
-1765328282	KRB5PLACEHOLD_102	KRB5 error code 102
-1765328281	KRB5PLACEHOLD_103	KRB5 error code 103
-1765328280	KRB5PLACEHOLD_104	KRB5 error code 104
-1765328279	KRB5PLACEHOLD_105	KRB5 error code 105
-1765328278	KRB5PLACEHOLD_106	KRB5 error code 106
-1765328277	KRB5PLACEHOLD_107	KRB5 error code 107
-1765328276	KRB5PLACEHOLD_108	KRB5 error code 108
-1765328275	KRB5PLACEHOLD_109	KRB5 error code 109
-1765328274	KRB5PLACEHOLD_110	KRB5 error code 110
-1765328273	KRB5PLACEHOLD_111	KRB5 error code 111
-1765328272	KRB5PLACEHOLD_112	KRB5 error code 112
-1765328271	KRB5PLACEHOLD_113	KRB5 error code 113
-1765328270	KRB5PLACEHOLD_114	KRB5 error code 114
-1765328269	KRB5PLACEHOLD_115	KRB5 error code 115
-1765328268	KRB5PLACEHOLD_116	KRB5 error code 116
-1765328267	KRB5PLACEHOLD_117	KRB5 error code 117
-1765328266	KRB5PLACEHOLD_118	KRB5 error code 118
-1765328265	KRB5PLACEHOLD_119	KRB5 error code 119
-1765328264	KRB5PLACEHOLD_120	KRB5 error code 120
-1765328263	KRB5PLACEHOLD_121	KRB5 error code 121
-1765328262	KRB5PLACEHOLD_122	KRB5 error code 122
-1765328261	KRB5PLACEHOLD_123	KRB5 error code 123
-1765328260	KRB5PLACEHOLD_124	KRB5 error code 124
-1765328259	KRB5PLACEHOLD_125	KRB5 error code 125
-1765328258	KRB5PLACEHOLD_126	KRB5 error code 126
-1765328257	KRB5PLACEHOLD_127	KRB5 error code 127
-1765328256	KRB5_ERR_RCSID	$Id: krb5_err.et,v 1.1 1998/05/06 20:23:54 mione Exp $
-1765328255	KRB5_LIBOS_BADLOCKFLAG	Invalid flag for file lock mode
-1765328254	KRB5_LIBOS_CANTREADPWD	Cannot read password
-1765328253	KRB5_LIBOS_BADPWDMATCH	Password mismatch
-1765328252	KRB5_LIBOS_PWDINTR	Password read interrupted
-1765328251	KRB5_PARSE_ILLCHAR	Illegal character in component name
-1765328250	KRB5_PARSE_MALFORMED	Malformed representation of principal
-1765328249	KRB5_CONFIG_CANTOPEN	Can't open/find Kerberos configuration file
-1765328248	KRB5_CONFIG_BADFORMAT	Improper format of Kerberos configuration file
-1765328247	KRB5_CONFIG_NOTENUFSPACE	Insufficient space to return complete information
-1765328246	KRB5_BADMSGTYPE	Invalid message type specified for encoding
-1765328245	KRB5_CC_BADNAME	Credential cache name malformed

-1765328244	KRB5_CC_UNKNOWN_TYPE	Unknown credential cache type
-1765328243	KRB5_CC_NOTFOUND	Matching credential not found
-1765328242	KRB5_CC_END	End of credential cache reached
-1765328241	KRB5_NO_TKT_SUPPLIED	Request did not supply a ticket
-1765328240	KRB5KRB_AP_WRONG_PRINC	Wrong principal in request
-1765328239	KRB5KRB_AP_ERR_TKT_INVALID	Ticket has invalid flag set
-1765328238	KRB5_PRINC_NOMATCH	Requested principal and ticket don't match
-1765328237	KRB5_KDCREP_MODIFIED	KDC reply did not match expectations
-1765328236	KRB5_KDCREP_SKEW	Clock skew too great in KDC reply
-1765328235	KRB5_IN_TKT_REALM_MISMATCH	Client/server realm mismatch in initial ticket request
-1765328234	KRB5_PROG_ETYPE_NOSUPP	Program lacks support for encryption type
-1765328233	KRB5_PROG_KEYTYPE_NOSUPP	Program lacks support for key type
-1765328232	KRB5_WRONG_ETYPE	Requested encryption type not used in message
-1765328231	KRB5_PROG_SUMTYPE_NOSUPP	Program lacks support for checksum type
-1765328230	KRB5_REALM_UNKNOWN	Cannot find KDC for requested realm
-1765328229	KRB5_SERVICE_UNKNOWN	Kerberos service unknown
-1765328228	KRB5_KDC_UNREACH	Cannot contact any KDC for requested realm
-1765328227	KRB5_NO_LOCALNAME	No local name found for principal name
-1765328226	KRB5_MUTUAL_FAILED	Mutual authentication failed
-1765328225	KRB5_RC_TYPE_EXISTS	Replay cache type is already registered
-1765328224	KRB5_RC_MALLOC	No more memory to allocate (in replay cache code)
-1765328223	KRB5_RC_TYPE_NOTFOUND	Replay cache type is unknown
-1765328222	KRB5_RC_UNKNOWN	Generic unknown RC error
-1765328221	KRB5_RC_REPLAY	Message is a replay
-1765328220	KRB5_RC_IO	Replay I/O operation failed XXX
-1765328219	KRB5_RC_NOIO	Replay cache type does not support non-volatile storage
-1765328218	KRB5_RC_PARSE	Replay cache name parse/format error
-1765328217	KRB5_RC_IO_EOF	End-of-file on replay cache I/O
-1765328216	KRB5_RC_IO_MALLOC	No more memory to allocate (in replay cache I/O code)
-1765328215	KRB5_RC_IO_PERM	Permission denied in replay cache code
-1765328214	KRB5_RC_IO_IO	I/O error in replay cache i/o code
-1765328213	KRB5_RC_IO_UNKNOWN	Generic unknown RC/IO error
-1765328212	KRB5_RC_IO_SPACE	Insufficient system space to store replay information
-1765328211	KRB5_TRANS_CANTOPEN	Can't open/find realm translation file
-1765328210	KRB5_TRANS_BADFORMAT	Improper format of realm translation file
-1765328209	KRB5_LNAME_CANTOPEN	Can't open/find lname translation database
-1765328208	KRB5_LNAME_NOTRANS	No translation available for requested principal
-1765328207	KRB5_LNAME_BADFORMAT	Improper format of translation database entry
-1765328206	KRB5_CRYPTO_INTERNAL	Cryptosystem internal error
-1765328205	KRB5_KT_BADNAME	Key table name malformed
-1765328204	KRB5_KT_UNKNOWN_TYPE	Unknown Key table type
-1765328203	KRB5_KT_NOTFOUND	Key table entry not found
-1765328202	KRB5_KT_END	End of key table reached

-1765328201	KRB5_KT_NOWRITE	Cannot write to specified key table
-1765328200	KRB5_KT_IOERR	Error writing to key table
-1765328199	KRB5_NO_TKT_IN_RLM	Cannot find ticket for requested realm
-1765328198	KRB5DES_BAD_KEYPAR	DES key has bad parity
-1765328197	KRB5DES_WEAK_KEY	DES key is a weak key
-1765328196	KRB5_BAD_ENCTYPE	Bad encryption type
-1765328195	KRB5_BAD_KEYSIZE	Key size is incompatible with encryption type
-1765328194	KRB5_BAD_MSIZE	Message size is incompatible with encryption type
-1765328193	KRB5_CC_TYPE_EXISTS	Credentials cache type is already registered.
-1765328192	KRB5_KT_TYPE_EXISTS	Key table type is already registered.
-1765328191	KRB5_CC_IO	Credentials cache I/O operation failed XXX
-1765328190	KRB5_FCC_PERM	Credentials cache file permissions incorrect
-1765328189	KRB5_FCC_NOFILE	No credentials cache file found
-1765328188	KRB5_FCC_INTERNAL	Internal file credentials cache error
-1765328187	KRB5_CC_WRITE	Error writing to credentials cache file
-1765328186	KRB5_CC_NOMEM	No more memory to allocate (in credentials cache code)
-1765328185	KRB5_CC_FORMAT	Bad format in credentials cache
-1765328184	KRB5_INVALID_FLAGS	Invalid KDC option combination (library internal error)
-1765328183	KRB5_NO_2ND_TKT	Request missing second ticket
-1765328182	KRB5_NOCREDS_SUPPLIED	No credentials supplied to library routine
-1765328181	KRB5_SENDAUTH_BADAUTHVERS	Bad sendauth version was sent
-1765328180	KRB5_SENDAUTH_BADAPPLVERS	Bad application version was sent (via sendauth)
-1765328179	KRB5_SENDAUTH_BADRESPONSE	Bad response (during sendauth exchange)
-1765328178	KRB5_SENDAUTH_REJECTED	Server rejected authentication (during sendauth exchange)
-1765328177	KRB5_PREAUTH_BAD_TYPE	Unsupported preauthentication type
-1765328176	KRB5_PREAUTH_NO_KEY	Required preauthentication key not supplied
-1765328175	KRB5_PREAUTH_FAILED	Generic preauthentication failure
-1765328174	KRB5_RCACHE_BADVNO	Unsupported replay cache format version number
-1765328173	KRB5_CCACHE_BADVNO	Unsupported credentials cache format version number
-1765328172	KRB5_KEYTAB_BADVNO	Unsupported key table format version number
-1765328171	KRB5_PROG_ATYPE_NOSUPP	Program lacks support for address type
-1765328170	KRB5_RC_REQUIRED	Message replay detection requires rcache parameter
-1765328169	KRB5_ERR_BAD_HOSTNAME	Hostname cannot be canonicalized
-1765328168	KRB5_ERR_HOST_REALM_UNKNOWN	Cannot determine realm for host
-1765328167	KRB5_SNAME_UNSUPP_NAMETYPE	Conversion to service principal undefined for name type
-1765328166	KRB5KRB_AP_ERR_V4_REPLY	Initial Ticket response appears to be Version 4 error
-1765328165	KRB5_REALM_CANT_RESOLVE	Cannot resolve KDC for requested realm
-1765328164	KRB5_TKT_NOT_FORWARDABLE	Requesting ticket can't get forwardable tickets
-1765328163	KRB5_FWD_BAD_PRINCIPAL	Bad principal name while trying to forward credentials
-1765328162	KRB5_GET_IN_TKT_LOOP	Looping detected inside krb5_get_in_tkt
-1765328161	KRB5_CONFIG_NODEFREALM	Configuration file does not specify default realm
-1765328160	KRB5_SAM_UNSUPPORTED	Bad SAM flags in obtain_sam_padata
-1765328159	KRB5_KT_NAME_TOOLONG	Keytab name too long

-1765328158	KRB5_KT_KVNONOTFOUND	Key version number for principal in key table is incorrect