|  |  |
| --- | --- |
|  | |
| Canpar Express | |
| Sybase security – Single Sign-on Configuration |  |
|  | |

#### Document information

|  |  |  |  |
| --- | --- | --- | --- |
| Client name: | Internal | Project name: | Single Sign-on Configuration |
| Project manager: | Rafael Leandro |  |  |

#### Version History

| Version | Date | Done By | Change Description |
| --- | --- | --- | --- |
| 1.00 | 2020-05-02 | Rafael LEANDRO | Document creation |
| 1.01 | 2020-05-14 | Rafael Leandro | Added info about local (server) SSO and more troubleshooting info |
| 1.02 | 2020-11-09 | RAFAEL LEANDRO | Layout adjustments. general corrections |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Index

[1. Introduction 3](#_Toc55850964)

[2. SAP ASE Configuration 4](#_Toc55850965)

[3. Enable server-side client connection 10](#_Toc55850966)

[4. Client Configuration 12](#_Toc55850967)

[5. C# application configuration 14](#_Toc55850968)

[6. VB application configuration 15](#_Toc55850969)

[7. Crystal Reports configuration 15](#_Toc55850970)

[8. ODBC and OLEDB configuration 15](#_Toc55850971)

[9. Troubleshooting 15](#_Toc55850972)

# Introduction

As of April 2020, our users authenticated to the database using server logins that used the same password. This poses a high security threat for obvious reasons. To mitigate this, we decided to configure AD authentication for Sybase going forward. This would allow us enhance our password policy (which could not be done before due to application architecture restrictions). This document provides the steps necessary to enable single sign-on to allow integration with Windows Active Directory.

As of 2020, the version of the Trustbroker software we’re using is 4.6.1-38740. In case you need support, email CyberSafe Support (TrustBroker) at support-trustbroker@cybersafe.com.

Each step in this document will contain the command, the output expected and a little explanation about that step like below.

|  |
| --- |
| COMMAND |
| EXPECTED OUTPUT |
| NOTES |

# SAP ASE Configuration

Attention! Before proceding make sure you replace the server name (CPDB2 in this case) with the server you’re configuring in all relevant steps. All the steps below were performed with user ‘sybase’ using sudo where necessary.

|  |
| --- |
| Install TrustBroker Secure Client for Servers (CSTBscs) and install the license key file as previously explained. Get both the binaries and license key from Cybersafe.  tar -xvf CSTBscs-4.6.1-38740.rhel7.Linux.x86\_64.z  cd CSTBscs-4.6.1-38740.rhel7.Linux.x86\_64/  cd Package/  sudo ./cstb\_install  cd /krb5/license #copy the license file to this folder |
|  |
| More details for CSTBscs installation check [here](https://tficourier.sharepoint.com/:b:/s/IT/AppDev/Edn3k17syj9BtHoXvhJAYt0B_ctICxsm9-fxVuHRuywOzg?e=C0x4Xe). If you don’t have the binaries or the license file, contact Cybersafe at support-trustbroker@cybersafe.com. |

|  |
| --- |
| Look in $SYBASE/config/objectid.dat  Check that [secmech] section contains the 1.3.6.1.4.1.897.4.6.6 = csfkrb5 entry.  This should already be in the file. |
|  |

|  |
| --- |
| Look in $SYBASE/$SYBASE\_OCS/config/libtcl.cfg  Uncomment the CSFKRB5= line and change CSFKRB5 to lower case. Line now has something like:  csfkrb5=libsybskrb.so secbase=@CANPAR.COM libgss=/krb5/lib/libgss.so  Note: The secbase should be set to your Active Directory domain name in upper case with an @ prefix as suggested above. |
|  |

|  |
| --- |
| Look in $SYBASE/$SYBASE\_OCS/config/libtcl64.cfg. Uncomment the CSFKRB5= line and change CSFKRB5 to lower case. Line now has something like:  [SECURITY]  csfkrb5=libsybskrb64.so secbase=@CANPAR.COM libgss=/krb5/appsec-rt/lib/64/libgss.so |
|  |

|  |
| --- |
| Add secmech= entry to $SYBASE/interfaces  CPDB2  master tcp ether servername port  query tcp ether servername port  secmech 1.3.6.1.4.1.897.4.6.6 |
|  |

|  |
| --- |
| Create a key table entry where <server name> = <principal name>. For example:  [sybase@CPDB2 ~]$ sudo /krb5/sbin/64/ktutil --allow-user-principal -x CPDB1@CANPAR.COM |
|  |

|  |
| --- |
| Add the following entries to $SYBASE/SYBASE.sh  #Set Kerberos environment variables  export KRB5\_CONFIG="/etc/krb5.conf"  export KRB5\_KTNAME="/krb5/v5srvtab.keytab"  export SYBASE\_PRINCIPAL="CPDB1@CANPAR.COM"  export LD\_LIBRARY\_PATH="/krb5/lib":$LD\_LIBRARY\_PATH  export LD\_LIBRARY\_PATH\_64="/krb5/appsec-rt/lib/64":$LD\_LIBRARY\_PATH\_64  export CSFC5KTNAME="/krb5/v5srvtab"  After that run: source $SYBASE/SYBASE.sh |
|  |
| The environment variables explained (in order of appearance):  Set to specify the location of the krb5.conf file  Set to allow the ASE to pick up the keytab file  Set to allow the ASE to pick up the Service principal name  Add the Kerberos library to LD\_LIBRARY\_PATH and LD\_LIBRARY\_PATH\_64  Add the Cybersafe keytab file location |

|  |
| --- |
| Set the permissions on the keytab so that ASE can read it:  sudo chmod 604 /krb5/v5srvtab |
|  |
|  |

|  |
| --- |
| Logon to ASE and enable security services (isql -Usa -SCPDB1):  use master  go  sp\_configure "use security services",1  go |
|  |

|  |
| --- |
| Add users to the database, which are same name as Kerberos user principals. If using MS AD domain, they would be same as AD account names. So in my case my account is canpar\rafael\_leandro. So I'm going to add the user rafael\_leandro to ASE.  $ isql -Usa -SCPDB1  1> sp\_addlogin rafael\_leandro, anypassword  2> go |
| Password correctly set.  Account unlocked.  New login created.  (return status = 0)  1> sp\_adduser rafael\_leandro  2> go  New user added.  (return status = 0)  1> |
| Note: Although rafael\_leandro user was created with a password, this password will not be used when Kerberos is used to authenticate to ASE |

|  |
| --- |
| Now go to your ASE RUN\_file and edit it to add the -k option to your service principal  vi /opt/sap/ASE-16\_0/install/RUN\_CPDB1  -kCPDB1@CANPAR.COM \ |
|  |

|  |
| --- |
| Restart ASE. Check in the log (on the “install” folder) for the following:  server successfully initialized the security mechanism 'csfkrb5'. ASE will support use of this security mechanism. |

# Enable server-side client connection

The steps below are only needed if you want to be able to connect with a specific user via Kerberos (you don’t have to type or store any passwords). This can be interesting if you want to execute the server-side jobs with a user without worrying about storing any passwords on secondary encrypted/obfuscated files (not the best practice anyway). In this case, we are using user ‘sybase’ to execute certain jobs so we’re going to configure Kerberos to store the credentials metadata for that user inside a temporary key table, then we’ll distribute this keytable and merge with the primary Kerberos key table in each server.

|  |
| --- |
| Copy the file libCSTBpbsa\_client.so to the server folder /krb5/appsec-rt/lib/64. You can grab this file from Sharepoint. Remember to log as root during the copy. |
|  |

|  |
| --- |
| #run the command below to create the key table for the sybase user.  sudo /krb5/sbin/64/ktutil -P2 -x -t /tmp/keytab --allow-user-principal sybase@CANPAR.COM |
|  |
| The -P2 flag tells ktutil to exclude the current host name when encrypting the key table  The -t flag tells ktutil to export the key table to a file instead of actually changing the official key table located at /krb5/v5srvtab by default (you don’t want to change the official key table right now). |

|  |
| --- |
| #next copy the recently created key table file to the other servers  sudo scp -p /tmp/keytab sybase@CPDB1:/tmp/keytab  sudo scp -p /tmp/keytab sybase@CPDB2:/tmp/keytab  sudo scp -p /tmp/keytab sybase@CPDB4:/tmp/keytab |

|  |
| --- |
| #next merge the key table from the file with the system key table on all servers that are going to authenticate with that user (in this case user sybase). In this configuration, we have to run the command below on cpdb2, cpdb1, cpdb4 and cpsybtest.  sudo /krb5/sbin/64/ktutil -c /tmp/keytab |
|  |

|  |
| --- |
| #next initialize the user on each server so that it can be used for authentication locally. In this configuration, we have to run the command below on cpdb2, cpdb1, cpdb4 and cpsybtest.  /krb5/bin/64/kinit -k sybase@CANPAR.COM |

|  |
| --- |
| #Log in to ASE as sa and verify that the user sybase exists on the ASE server. If not, create it and assign the appropriate permissions  exec master..sp\_displayroles sybase |
|  |

|  |
| --- |
| Change any jobs running on the server under the sybase user to authenticate without the -U and -P options. Change these jobs to use the -V flag. Also change these jobs to use isql\_r instead of isql. Examples below. Be sure to include the kinit command in the script to make sure the credentials are renewed if necessary. |
| Before:  isql -Usybmaint -w900 -P\`/opt/sap/cron\_scripts/getpass.pl sybmaint\` -S$prodserver -b  isql -Usa -P\`/opt/sap/cron\_scripts/getpass.pl sa\` -S$prodserver -b –n  After:  /krb5/bin/64/kinit -k sybase@CANPAR.COM  isql\_r -w900 -V -S$prodserver –b  /krb5/bin/64/kinit -k sybase@CANPAR.COM  isql\_r -V -S$prodserver -b -n |

# Client Configuration

|  |
| --- |
| Install the Trustbroker software on the client machine. You can use the default options.  Copy the license file (the same you used on the database server) to the folder %ProgramData%\CyberSafe\license. |

|  |
| --- |
| Configure the libtcl.cfg file in your client machine. This file is located in %SYBASE%\OCS-XX\_0\ini. If the environment variable SYBASE is not defined, check if the ASE drivers are properly installed.  Uncomment and change the corresponding Kerberos entry. Change the values of secbase according to your AD domain.  CSFKRB5=LIBSYBSKRB secbase=@CANPAR.COM libgss=gssapi32.dll |
|  |

|  |
| --- |
| Make sure you have the server entry in your sql.ini file. This file is located at %SYBASE%\ini. If the environment variable SYBASE is not defined, check if the ASE drivers are properly installed. |
|  |
| Below are the entries in my sql.ini file for an easy copy  [CPDB1]  master=TCP,cpdb1.canpar.com,4100  query=TCP,cpdb1.canpar.com,4100  [cpsybtest]  master=TCP,cpsybtest2.canpar.com,4100  query=TCP,cpsybtest2.canpar.com,4100  [CPDB1]  master=TCP,CPDB1.canpar.com,4100  query=TCP,CPDB1.canpar.com,4100  [CPDB1]  master=TCP,CPDB1.canpar.com,4100  query=TCP,CPDB1.canpar.com,4100 |

|  |
| --- |
| Test the connection in a client machine (while logged with an AD account). Make sure you have the correspondent login created in ASE like shown in the steps above. You should be able to login without problems. When querying the authentication mechanism, it should return Kerberos.  isql -V –SCPDB1 |

# C# application configuration

|  |
| --- |
| Before |
| "Data Source='cpdb1';Port=4100;Database='cpscan';UID='dan\_pham';PWD='canpar';charset=iso\_1; Max Pool Size=50; Connection Timeout=240;" |
| After |
| ?connectionString= "Data Source='cpsybtest';Port=4100;Database='cmf\_data\_lm';AuthenticationClient=cybersafekerberos;ServerPrincipal= CPSYBTEST@CANPAR.COM;charset=iso\_1; Max Pool Size=50; Connection Timeout=240;" |

# VB application configuration

Change the connection string removing the user and password from it and adding the properties and values highlighted below. Change the server name, database and other properties as needed.

|  |
| --- |
| Before |
| Data Source='cpdb1';Port=4100;Database='cpscan';UID='dan\_pham';PWD='canpar';charset=iso\_1; Max Pool Size=50; Connection Timeout=240 |
| After |
| Data Source='cpdb1';Port=4100;Database='cpscan';charset=iso\_1; Max Pool Size=50; Connection Timeout=240;WA2=16;AuthenticationClient=cybersafekerberos;ServerPrincipal=CPSYBTEST@CANPAR.COM |

# Crystal Reports configuration

As of May 2nd 2020, Crystal Reports is still pending connection testing. Crystal Reports uses ODBC to connect to the database so take a look at the ODBC section in this document for more details.

# ODBC and OLEDB configuration

1. Any application connecting through ODBC, must be at least at ODBC version 15.0 or above.
2. Applications connecting through ODBC, do not require any changes in the programs themselves.
3. Once ODBC is modified, programs can continue to operate as before, AD authentication will be handled by ODBC DSN and Kerberos installed on the host.
4. OLEDB version must be at least 15.0 or above.
5. Connection string within the program must be modified to use Kerberos based authentication.

# Troubleshooting

Below are the main problems you can find when configuring single sign-on. Before we dive into it though, let’s take a look at the most important files when the matter is troubleshooting.

|  |  |  |
| --- | --- | --- |
| **File** | **Purpose** | **Notes** |
| /krb5/logs/CSTBk564.0.log | Kerberos log | Use to find out why authentication is not working on the server side |
| /krb5/logs/v5srvtab | Keytab file. Contains the users that authenticate with AD to generate user tickets | Generated by the ktutil command (see the configuration steps for more info) |
| /krb5/lib/\* | CSTB connection libraries |  |

Now let’s get to the errors and their solution. Messages in red are from Kerberos log, in green from ASE log and in blue from the client.

|  |
| --- |
| Error message (server side):  isql64 -V -Stest -R'test@KRBTEST '  00:0006:00000:00022:2013/04/08 14:15:35.09 server Received LOGINREC  LOGINREC at 0x10002cd3ad8  host=`ldkim-sun' user=`' hostproc=`21523'  int2=2 int4=0 char=6 flt=4 date=8  usedb=1 dmpld=1 interface=0 netconn\_type=0  appname=`isql' servername=`test'  tds\_vers=(5.0.0.0) progname=`CT-Library' prog\_vers=(15.7.0.4)  noshort=0 flt4=12 date4=16  language=`' setlang=0  SECURITY: hier=0 e2e option: 0x10 db bulk reserved: 0x00  HA: ssn option: 0x08 ssn handle:(0x00, 0x00, 0x00, 0x00, 0x00, 0x00)  UNUSED: slunused:(0x00)  role=0  charset=`iso\_1' setcharset=0 packetsize=`512'  00:0006:00000:00022:2013/04/08 14:15:35.17 kernel Connectivity Library (Security Control Layer) Error: Consistency checks performed on the credential failed (minor status 0).  00:0006:00000:00022:2013/04/08 14:15:35.17 server SCL error in function: sec\_get\_cred. Operation: sec\_cred\_acquire().  00:0006:00000:00022:2013/04/08 14:15:35.17 server SCL error in function: sec\_setup. Operation: sec\_get\_cred().  00:0006:00000:00022:2013/04/08 14:15:35.17 kernel Connectivity Library (Security Control Layer) Error: Consistency checks performed on the credential failed (minor status 0).  Msg 4053, Level 14, State 1:  Server 'test':  Security session setup failed during security session establishment.  CT-LIBRARY error:  ct\_connect(): protocol specific layer: external error: The attempt to connect to the serve r failed. |
| Last known occurrence: May 2nd 2020 |
| Solution:  moved keytab to a location where ASE could read it.  Also opened up permissions so ASE could read it.  Check your ASE and make sure SYBASE\_PRINCIPAL is set to the correct Service Principal  or you have -k set correctly in your RUN file |
| Additional info: |

|  |
| --- |
| Error message (server side):  00:0006:00000:00012:2013/04/08 15:18:21.98 kernel Connectivity Library (Security Control Layer) Error: Security service provider internal error -1765328196: 'Unknown code 188' occurred.  00:0006:00000:00012:2013/04/08 15:18:21.98 server SCL error in function: sec\_negotiate. Operation: scl\_sess\_bind().  Msg 4054, Level 14, State 1:  Server 'test':  Protocol negotiation failed during security session establishment.  CT-LIBRARY error:  ct\_connect(): protocol specific layer: external error: The attempt to connect to the server failed. |
| Last known occurrence: Never |
| Solution:  Bad encryption type. This means your encryption isn’t being set correctly or the library isn’t able to use the encryption that was distributed.  Type klist -e  This will show you the encryption used. If it says “unsupported” then try a different encryption type or newer Kerberos library. I ran into this issue with aes 256 encryption with older Kerberos library. |
| Additional info: |

|  |
| --- |
| Error message (server side):  00:0006:00000:00012:2013/04/08 15:18:21.98 kernel Connectivity Library (Security Control Layer) Error: Security service provider internal error -1765328184 |
| Last known occurrence: Never |
| Solution:  The real message is: Invalid KDC option combination (library internal error). This one took a bit to figure out. To resolve this, make sure your ASE is picking up and loading the libraries used by the KDC.  In my case I was loading older libraries that were in the default host location.  /lib  The ASE booted successfully, however when trying to connect this error came up. I shut down the ASE. Edited the libtcl64.cfg file so it was pointing to the KDC libraries and added the LD\_LIBRARY\_PATH\_64 to the KDC libraries and booted. Reboot and check for the successful load of Kerberos. Then login. This resolved the issue. |
| Additional info: |

|  |
| --- |
| Error message (server side):  00:0006:00000:00012:2013/04/08 15:18:21.98 kernel Connectivity Library (Security Control Layer) Error: … file too short… |
| Last known occurrence: May 14 2020 |
| Solution: make sure the client libraries were copied correctly. What happened to me is that I copied the file while using an sftp after the connection was closed. So the file showed up in the destination folder but had 0 kb. After I reconnected and copied the file again overwriting the previous one, the problem went away. |
| Additional info: |

|  |
| --- |
| Error message (server side):  Loading /krb5/appsec-rt/lib/64/libCSTBpbsa\_client.so failed. System Error Details: /krb5/appsec-rt/lib/64/libCSTBpbsa\_client.so: file too short ( 0x0000002a 42 ) |
| Last known occurrence: May 14 2020 |
| Solution: make sure the client libraries were copied correctly. What happened to me is that I copied the file while using an sftp after the connection was closed. So the file showed up in the destination folder but had 0 kb. After I reconnected and copied the file again overwriting the previous one, the problem went away. |
| Additional info: |

|  |
| --- |
| Error message (server side): when running kinit you get the error below.  Keytable entry not found for user <user name> |
| Last known occurrence: May 14 2020 |
| Solution: You probably forgot to run ktutil. Go back to the guide and run the command for the user you’re trying to use. |
| Additional info: |

|  |
| --- |
| Error message (server side): Credentials cache error while running /krb5/bin/64/kinit –k |
| Last known occurrence: May 14 2020 |
| Solution: try unsetting the 2 env variables below and then try again. If that does not work, make sure you ran ktutil for the user and then try again.  unset CSFC5DPN  unset CSFC5CCNAME  echo $CSFC5DPN  echo $CSFC5CCNAME |
| Additional info: |

|  |
| --- |
| Error message (client side):  C:\Sybase\_15\_7\_32bit\OCS-16\_0\bin>isql -V -SCPSYBTEST  CT-LIBRARY error:  ct\_con\_props(SET): security service layer: internal security control layer error: Configuration file error.  Msg 4002, Level 14, State 1:  Server 'CPSYBTEST':  Login failed.  CT-LIBRARY error:  ct\_connect(): protocol specific layer: external error: The attempt to connect to the server failed. |
| Last known occurrence: April 28 2020 |
| Solution:  Check the event viewer and look for events with source CSTBk5 to see the actual error. In this case the problem was that I was pointing to the 64 bit Kerberos library and was trying to run the 32 bit version of isql. The problem was gone when I used isql64 instead of isql. To point to the 64 bit library, change from ‘gssapi32’ to ‘gssapi64’ in the libtcl.cfg file. |
| Additional info: |

|  |
| --- |
| Error message (client side):  C:\Sybase\_15\_7\_32bit\OCS-15\_0\bin>isql -V -SCPDB2  ct\_con\_props(SET): security service layer: internal security control layer error: Unable to open security driver.  Msg 4002, Level 14, State 1:  Server 'CPDB2':  Login failed.  CT-LIBRARY error:  ct\_connect(): protocol specific layer: external error: The attempt to connect to the server failed.  No log entries for CSTBk5 in event viewer |
| Last known occurrence: Nov 10 2020 |
| Solution: Check your Sybase driver. It might not have installed correctly. On my machine I had the ASE 16 driver that comes with the SDK downloaded from the SAP download portal when the problem occurred. After I installed the drivers of version 15.7 using the method below, the problem was gone. Attention! After installing the drivers following the procedure below, make sure you run the SYBASE.bat script in the installation folder to set the environment variables before trying to connect via Kerberos again.  Instructions for installing ASE 15.7 drivers on Windows10 (silent install):  Get an Administrator command prompt (not powershell)  Net use z: \\hqvfs2.canpar.com\datavol /user:{canparnt\a\_myadminuser} {password} \*\*replace the {stuff in brackets} with your admin user and password  Z:  Cd \Common\MigrationProject\Rollout\ASENETSYBASE157\pcclient32\ESD  setupConsole.exe -f CP\_Syb\_32\_ESD -i silent -DAGREE\_TO\_SYBASE\_LICENSE=true |
| Additional info: |

|  |
| --- |
| Error message (client side):  C:\Sybase\_15\_7\_32bit\OCS-15\_0\bin>isql -V -SCPDB2  CT-LIBRARY error:  ct\_connect(): security service layer: internal security control layer error: Security service provider internal error -1073741718 occurred.  In lsacache.c, at line 817, for application All Applications, from pid 16876, by user <username>, in function ms\_lsa\_get\_ticket, Error getting ticket using LSA, ticketFlags: 0x0, encryptionType: 0, cacheOptions: 0x1, server: krbtgt/CANPAR.COM, protocolStatus: 0xc000006a ('When trying to update a password, this return status indicates that the value provided as the current password is not correct.'), LsaNtStatusToWinError?(): 0x56 |
| Last known occurrence: Nov 11 2020 |
| Solution:  As you can see, Kerberos tells that there is a problem with the password provided. But since we’re not providing any password, how can this be? The last time this happened to me it was because Windows hadn’t updated the local credentials cache yet after I reset my domain account password. All that I had to do was to lock the workstation and log back in (or unlock) using the new password. That updated the credentials cache and the problem was gone. |
| Additional info: |