# Configuring Kerberos Constrained Delegation for NetScaler DataStream

## Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Author</th>
<th>Contributors</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Dec. 2011</td>
<td>Raymond</td>
<td></td>
<td>Initial draft</td>
</tr>
<tr>
<td>1.1</td>
<td>May. 2012</td>
<td>Raymond</td>
<td></td>
<td>Added configuration section</td>
</tr>
<tr>
<td>1.2</td>
<td>06/10/2012</td>
<td>Naresh</td>
<td></td>
<td>Added Trouble-shooting section and more details and pictures to configuration section.</td>
</tr>
<tr>
<td>1.3</td>
<td>06/11/2012</td>
<td>Raymond</td>
<td></td>
<td>Minor changes and reorg.</td>
</tr>
<tr>
<td>1.4</td>
<td>10/26/2012</td>
<td>Naresh</td>
<td>Pratap</td>
<td>Adding KCDAccount in configuration.</td>
</tr>
<tr>
<td>1.5</td>
<td>10/29/2012</td>
<td>Naresh</td>
<td>Pratap</td>
<td>Adding review comments from Pratap</td>
</tr>
<tr>
<td>1.6</td>
<td>30/10/2012</td>
<td>Sudish</td>
<td></td>
<td>Adding SQL windows Auth</td>
</tr>
<tr>
<td>1.7</td>
<td>24/06/2014</td>
<td>Sudish</td>
<td>Pratap</td>
<td>Updated trouble-shooting section.</td>
</tr>
</tbody>
</table>
# Table of Content

1. Introduction ......................................................................................................................... 3

   Protocol Transition (S4U2Self) ............................................................................................... 3

   Constrained Delegation (S4U2Proxy) ....................................................................................... 3

2. Goal ........................................................................................................................................ 4

3. SQL Windows Authentication ................................................................................................. 4

4. SQL KCD Workflow .............................................................................................................. 5

5. Configuration .......................................................................................................................... 6

   5.1 Active Directory Configuration ......................................................................................... 6

      5.1.1 Create a Kerberos Constrained Delegation (KCD) User Account ................................. 6

      5.1.2 Enable the Delegation tab for the created user ............................................................... 6

      5.1.3 Add the Services ........................................................................................................... 11

   5.2 SetUp Configuration: ....................................................................................................... 12

   5.3 SQL server configuration.................................................................................................... 13

   5.4 NetScaler Configuration: .................................................................................................. 14

      5.4.1 Kerberos configuration ................................................................................................. 14

      5.4.2 NTLM configuration ..................................................................................................... 17

6. Troubleshooting ..................................................................................................................... 18

   6.1 SetUp Verification .............................................................................................................. 18

   6.2 SQL Verification ................................................................................................................ 20

7. Reference ................................................................................................................................ 22

8. Authors ................................................................................................................................. 22
1. Introduction

Kerberos has been considered as the most secure and widely used, but most complex authentication system. However, when a remote client is unable to obtain a ticket, or when the ADC is unable to obtain a ticket for services on behalf of the client, unfortunately, it has created challenges in implementing secure architectures by an Application Delivery Controller (ADC).

Kerberos version 5 resolved the problem through two new extensions implemented in Windows Server 2003 to the authentication protocol: Protocol transition and constrained delegation.

Protocol Transition (S4U2Self)

The protocol transition extension allows a service to obtain a Kerberos service ticket to the Service on behalf of a user or proxy without requiring the user or proxy to be part of the Kerberos domain, or restricted to using Internet Explorer. No user credential is required for the transition. Applications may transition into Kerberos even though the actual authentication is done via another authentication method, such as HTTP Basic, form-based, NTLM, Radius, LDAP, SAML, RSA SecureID, PKI/Certificates and other OTP systems.

Constrained Delegation (S4U2Proxy)

The constrained delegation extension allows a service to obtain service tickets under the delegated users identity to a subset of other services after it has been presented with a service ticket that is obtained either through the TGS_REQ protocol, as defined in IETF RFC 1510, or in the protocol transition extension.

The reason why the constrained delegation extension is introduced in Windows Server 2003 was to address limitations in the Windows 2000 implementation of Kerberos delegation. In the Windows 2000 Kerberos delegation model, the Kerberos Key Distribution Center (KDC) does not limit the scope of services to which a Kerberos principal's identity can be delegated. In other words, after a service account is trusted for delegation, it can request service tickets on behalf of an authenticated user to any other service accounts. This delegation method does not provide precise mechanisms for an application to specify a subset of service accounts that it determines to be trustworthy for delegation. Essentially, applications are exposed to broader impersonation risks that may span across resource domains that have different levels of security policy requirements; some of the security policies may not be as strict as the applications security requirements. From the domain administrator’s point of view, it is too risky to enable unconstrained Kerberos delegation in the enterprise because there is no way to exclude untrusted servers from participating in delegation. With constrained delegation, domain administrators can configure service accounts so that they delegate only to specific sets of service accounts.

For more information about RFC 1510, see the IETF Web site (http://www.ietf.org).
For more information about Kerberos and the two extensions, see,


2. Goal

- To support Kerberos Protocol Transition and Constrained Delegation (Kerberos SSO) on nCore
- Integrated with all existing supported authentication methods;

3. SQL Windows Authentication

SQL Windows Authentication: SQL Windows authentication requires both client and server to be registered with AD (basically both of them can talk to AD). For login, client will get the Kerberos ticket for SQL server from AD and send the same to SQL Server for authentication (instead of username and password). The SQL Server verifies the ticket and sends authentication response (Done, Error). SQL server may send one additional token (0xed) before sending Done Packet.

SQL windows authentication support on NetScaler enables MSSQL lb/cs vserver to authenticate the client and authenticate itself on behalf of client to the backend server, and pass on the requests/response coming from client/server to server/client respectively. When client sends login request to lb vserver, it talks to nskrb daemon to verify the ticket, nskrb on verification sends the response which is sent to client with 0xed token and then Done packet(it indicate successful login) is sent to the client. If nskrb rejects the ticket then Error packet is sent to client with message “Windows Authentication failed.” and client connection is closed. While establishing the server side connection, once TCP connection is established, a request is sent to nskrb to get the ticket for backend server on behalf of user authenticated on client side connection, nskrb responds with a ticket which is encapsulated in the login packet and login packet is sent to backend server. Backend server respond with Done Packet and then client query (if any) is forwarded to backend server. The diagram in next section describes different phases in the client as well as server side authentication.
SQL KCD Workflow

1. TGT_REQ
2. TGT_RES
3. TGS_REQ
4. TGS_RES
5. SQL Login Request
6. Send client credentials
7. Validation Response
8. Token 0xed + Done Packet
9. SQL Query
10. Request for Token
11. AS_REQ/AS_RES
   S4U2Self
   S4U2Proxy
12. Token Response
13. SQL Login Request
14. Token (0xed) + Done Packet
15. SQL Query
16. SQL response
17. SQL response
18. SQL Query
19. SQL Query
20. SQL response
21. SQL response
5. Configuration

This section outlines how to set up Kerberos Constrained Delegation with NetScaler. This involves setting up an account in the Active Directory, setting up the Server hosting the services and finally configuring the NetScaler. The only new CLI command introduced on NetScaler is to add a kcdaccount for a dbprofile, which will be described in detail in Section 5.4.

5.1 Active Directory Configuration

This part explains the configuration steps needed on the Active Directory to enable Constrained Delegation with NetScaler Secure Access.

5.1.1 Create a Kerberos Constrained Delegation (KCD) User Account

In order to get Constrained Delegation to work a User account has to be created. This account must have the rights to do the Protocol Transition and Delegation. Essentially this is the account that has the rights to request a Kerberos Ticket on behalf of a user logging into the NetScaler.

Start by creating a new user in the Active Directory or use an existing user account. In this example user `kcdtest` is created as the account to provide Constrained Delegation to a webserver.

5.1.2 Enable the Delegation tab for the created user

Delegation is not enabled by default for a User account and need to be enabled. This involves the use of the SETSPN command-line tool that isn’t included in any standard Windows 2003 installation.
Check in Active directory User properties if delegation tab is available, if not download windows package.
Install the Windows Server 2003 Support Tools from the product CD or from the Microsoft Download Center (http://go.microsoft.com/fwlink/?LinkId=100114).

For more information about how to install Windows Support Tools from the product CD, see Install Windows Support Tools (http://go.microsoft.com/fwlink/?LinkId=62270).

If this is installed in your Windows 2003 server it can be found in C:\Program Files\Support Tools

Use the command:

```
setspn -A MSSQLSvc\kcdvserver.sql2012.com sql2012\kcdtest
```

NOTE: In this example SQL2012 is the Domain and kcdtest is the user account we just created. In this we are registering kcdtest user with SPN: MSSQLSvc\kcdvserver.sql2012.com

This will enable the Delegation tab in the kcdtest properties.
If the Delegation Tab does not appear the Active Directory probably is running in mixed or native mode and need to be raised to Windows 2003 functional level.

**NOTE that the following steps will change your Active Directory behavior and Support for older Windows clients. If you are uncertain you should not raise the Domain Functional Level without checking if this has any impact to your Environment since this step cannot be reversed.**

Once the Active Directory is at Windows 2003 functional level you can continue Configuration.

The Delegation tab will now be visible. Make sure to enable the **“Trust this user for delegation to specified services only”** and **“Use any Authentication protocol”**.

Even though other selections might seem more accurate the “Kerberos only” options will not work since they do not enable Protocol Transition and Constrained Delegation.
Creating Keytab file for user kcdtest with SPN: host/kcdvserver.sql2012.com@SQL2012.COM

Note: ‘host/kcdvserver.sql2012.com@SQL2012.COM’ is case sensitive.

After ktpass is issued, user ‘kcdtest’ will be registered with SPN: host/kcdvserver.sql2012.com@SQL2012.COM
Check the `kcdtest` user Account properties, it looks as follows:

![User Account Properties](image)

After `ktpass` command is successful, copy that keytab file to NetScaler `/nsconfig/krb` directory.

**Note:** Set "password never expire" option for `kcdtest`, if password is expired then we need to regenerate `ktpass` and copy back to NetScaler.
5.1.3 Add the Services.

Since this is “constrained” delegation there is a need to specify the “Services” it applies to, Select “Add” in kcdtest user Delegation property.

Use the Users or Computers button to select the Computer hosting these services.

In this example we are doing Constraint Delegation to a service account running sql server on: Node1, this could have been any other Server in the Domain though.
Note that Constrained Delegation does not support Services hosted in other Domains even though there is a trust relationship to those Domains.

Now add the “Services” on the selected Server.

Since this example is about setting up Constrained Delegation to SQL Server the MSSQLSvc service is selected. Now review the settings and Apply / OK these settings. You are now finished setting up the Active Directory part of the configuration.

5.2 SetUp Configuration:

Sharing Secret Key between NS and AD: ktpass utility is used to generate the keytab and share the keytab between NS and AD. ktpass configures the server principal name for the host or service in Active Directory and generates an MIT-style Kerberos "keytab" file containing the shared secret key of the service.

Ktpass for lb vserver as server (required for client side kerberos auth): Command for keytab generation. ktpass /out sqlkeytab /princ MSSQLSvc/kcdvserver.sql2012.com:1433@KRB.com / pass password /mapuser KRB\user /ptype KRBS_NT_PRINCIPAL
a) MSSQLSvc - indicate mssql service type  
b) kcdvserver.sql2012.com:1433 - lb vserver name with port  
c) password – password for mapped user  
d) user – trusted AD user.

c) KRB5_NT_PRINCIPAL - principal type general

The keytab can be generated dynamically on NS using ktutil(with addent command) utility instead of generating on AD machine and then moving to NS.

```
/NetScaler/nskrb ktutil -k user.keytab add -p kcdtest@SQL2012.COM
-e arcfour-hmac-md5 -V 1 --password=abcd1234
```

To view the Keytab file, use following command

```
#/NetScaler/nskrb klist -k user.keytab -K
```

Keytab name: user.keytab  
KVNO Principal

```
------------------------------------------
1 kcdtest@SQL2012.COM (0xb3ec3e03e2a202cbd54fd104b8504fef)
```

**Ktpass for lb vserver as host** (required for kcd): Command for keytab generation.

```
ktpass /out sqlkeytab /princ host/lbsql.krb.com@KRB.com / pass password /mapuser KRB\user /ptype KRB5_NT_PRINCIPAL
```

Enable constrained delegation for the user as mentioned in 5.1 and select the SQL service for delegation. **5.3 SQL server configuration**

*Add a login with authentication as windows. There is no need to add a db user on NetScaler.*
5.4 NetScaler Configuration:

5.4.1 Kerberos configuration

(change ip, domain name, domain username and domain userpassword as per your setup.)

5.4.1.1 Add Service

add service sqlauth node1 MSSQL <port>
add server node1 node1.sql2012.com
bind lb vserver sqllb sqlauth
5.4.1.2 KCD Account and DB Profile

Create KcdAccount

Kcdaccount is used to extract SPN from keytab file, NetScaler reads keytab file and extracts SPN listed from keytab file.

CLI:

add kcdaccount kcdaccount1 –keytab kcdvserver.keytab
Or
add kcdaccount kcdaccount1 –keytab /nsconfig/krb/kcdvserver.keytab

Note: Kcdvserver.keytab file has to be copied under /nsconfig/krb/, if the file is not found in /nsconfig/krb NS will reject it.

sh kcdAccount kcdaccount2
1) KCD Account : kcdaccount2
Keytab : /nsconfig/krb/kcdvserver.keytab
Vserver Principle : host/kcdvserver.sql2012.com@SQL2012.COM
Done

Set/unset/rm commands are allowed on Kcdaccount.
Create DBProfile
DB Profile can be used with LB and CS vservers

CLI:
add dbProfile profile_name –kcdaccount myacc
5.4.1.3 LB VSERVER
add lb vserver <lb vserver name> MSSQL <ip address> <port> –dbprofile profile_name
bind lb vserver <lb vserver name> sqlauth

5.4.1.4 DNS Server
add dns nameServer <ip address>

**Important:** Following parameters needs to be taken care while adding configuration.

**Server Name:** While adding a server (add server), the dns name of the server should match with its service principal name for MSSQLSvc service type.

5.4.2 NTLM configuration

Add a db user with the domain password on NetScaler. If the client failed to obtain service tickets and does an NTLM fallback NetScaler will be able to authenticate the connection using the db user and password added on NetScaler

add db user dbserviceuser –password dbpasswd
6. Troubleshooting

6.1 SetUp Verification

The KCD requires steps which involve keytab generation (ktpass), addition of service principle name (setspn) and enabling KCD for user. Any wrong configuration (name wrongly typed, some option missed) can cause KCD to fail. If KCD fails to work then it can be checked if there is any issue with setup using following two shell commands on NetScaler. (change the lb vserver name, service name and service port as per requirement)

1. Log on using the keytab file. It should not show any error and klist should show the TGT.

```
root@ns# /NetScaler/nslcli kinit -k -t /nsconfig/krb/kerbtabfile.txt -f 'host/kcdvserver.sql2012.com@SQL2012.COM'
```

```
root@ns# /NetScaler/nslcli klist
Credentials cache: FILE:/tmp/krb5cc_0

    Principal: host/kcdvserver.sql2012.com@SQL2012.COM

        Issued    Expires    Principal
```

2. Do a s4u2self using the TGT ticket just created. Klist should show the TGT ticket created for self.

```
root@ns# /NetScaler/nslcli kgetcred -c /tmp/krb5cc_0 --out-cache=/tmp/imper_cache -- impersonate=Sqluser@SQL2012.COM 'host/kcdvserver.sql2012.com@SQL2012.COM'
```

```
root@ns# /NetScaler/nslcli klist -c /tmp/imper_cache
Credentials cache: FILE:/tmp/imper_cache

    Principal: Sqluser@SQL2012.COM

        Issued    Expires    Principal
```
3. Do a s4u2proxy using the service ticket for self and get ticket on behalf of user for a service

```
root@ns# /NetScaler/nskrb kgetcred --delegation-credential-cache=/tmp/imper_cache --out-cache=/tmp/kcd_cache MSSQLSvc/node2.sql2012.com:1433@SQL2012.COM

root@ns# /NetScaler/nskrb klist -c /tmp/kcd_cache

Credentials cache: FILE:/tmp/kcd_cache

Principal: Sqluser@SQL2012.COM

<table>
<thead>
<tr>
<th>Issued</th>
<th>Expires</th>
<th>Principal</th>
</tr>
</thead>
</table>
```
6.2 SQL Verification

Login Packet: Packet 3230 shows the login packet from sql client. The most significant bit of option flag2 indicates (ON for yes, OFF for no) whether windows authentication will be used or not. If this bit is ON then kerberos ticket will be there in this packet (as shown below).

Login Response Token (Oxed): This token is sent by SQL Server in response to the windows auth login. This is not a mandatory packet, server can send directly Done Packet which indicate successful login.

Packet 3238 shows Oxed token from SQL Server, this token also contain the authentication response for kerberos ticket.
7. Reference
http://support.citrix.com/article/CTX139133

8. Authors
- Raymond Li, Raymond.Li@citrix.com
- Naresh Jampani, Naresh.Jampani@citrix.com
- Sudish Kumar Sah, sudishkumar.sah@citrix.com