This article describes how to configure Kerberos Constrained Delegation (KCD) on a NetScaler appliance.
# Table of Content

1. Introduction ........................................................................................................................................ 3  
   1.1 Protocol Transition (S4U2Self) ....................................................................................................... 3  
   1.2 Constrained Delegation (S4U2Proxy) .......................................................................................... 3  
2. Goal .................................................................................................................................................... 5  
3. Application of KPT and Kerberos Constrained Delegation (KCD) on a NetScaler Appliance .......... 6  
   3.1 Workflow ....................................................................................................................................... 6  
   3.2 Explanation of Workflow Sequence ............................................................................................... 7  
   3.3 Integration with Existing Authentication Methods .......................................................................... 8  
4. Configuration ...................................................................................................................................... 9  
   4.1 Active Directory Configuration ...................................................................................................... 9  
      4.1.1 Create a Kerberos Constrained Delegation (KCD) User Account ........................................ 9  
      4.1.2 Enable the Delegation Tab for the Created User ................................................................. 9  
      4.1.3 Add the Services .................................................................................................................. 13  
      4.1.4 Generate Keytab file ............................................................................................................ 14  
   4.2 Web Application Server Configuration ....................................................................................... 16  
      4.2.1 Configuring the IIS Server ................................................................................................. 17  
      4.2.2 Web Server - Protocol Negotiation ................................................................................... 17  
   4.3 Setting up NetScaler for Constrained Delegation ..................................................................... 19  
      4.3.1 Joining a NetScaler Appliance to the KDC ...................................................................... 19  
      4.3.2 Create Backend Servers and Services ............................................................................... 20  
      4.3.3 Create TM and Authentication Virtual Server .................................................................... 21  
      4.3.4 Create KcdAccount ............................................................................................................ 21  
      4.3.5 Create Traffic/Session Profile ........................................................................................... 21  
      4.3.6 Enable Client Side Authentication (Form-based/401basic) .............................................. 22
5. Troubleshooting .................................................................................................................................. 23

5.1 Ensuring that lWagent Process and All Likewise Daemons are Running ............................................. 23

5.2 How to Know if KCD is Working? ....................................................................................................... 24

5.3 Kinit string: Verifying if NetScaler appliance is Requesting a Forwardable Ticket: S4U2SELF ............ 27

5.4 Kinit String: Verifying if Kinit Request Fails or if you Get Any of the Following Errors ......................... 27

5.5 t_s4u request .................................................................................................................................... 27

6. Firewall Ports Required to be Open for KCD Communication .............................................................. 30

7. Reference ............................................................................................................................................ 31
1. Introduction

Kerberos is considered 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 Application Delivery Controller (ADC) is unable to obtain a ticket for services on behalf of the client, it has created challenges in implementing secure architectures by an ADC.

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

1.1 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 restricts to using Internet Explorer. You do not require user credentials for the transition. Applications might transition into Kerberos even though you complete the actual authentication by using another authentication method, such as HTTP Basic, form-based, NTLM, Radius, LDAP, SAML, RSA SecureID, PKI, or Certificates and other OTP systems.

1.2 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 you present a service ticket that you get either through the TGS_REQ protocol, as defined in IETF RFC 1510, or in the protocol transition extension.

The constrained delegation extension is available in Windows Server 2003 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 you can delegate a Kerberos principal identity. That is, 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. Applications are exposed to broader impersonation risks that might span across resource domains that have different levels of security policy requirements. Some of the security policies might not be as strict as the applications security requirements. From the domain administrator point of view, it is risky to enable unconstrained Kerberos delegation in the enterprise, because you cannot 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).

2. Goal

- To support Kerberos Protocol Transition and Constrained Delegation (Kerberos SSO) on nCore build of the NetScaler software release
- Integrated with all existing supported authentication methods
3. Application of KPT and Kerberos Constrained Delegation (KCD) on a NetScaler Appliance

3.1 Workflow
3.2 Explanation of Workflow Sequence

1. The client makes a request to a traffic management (TM) virtual server on a NetScaler appliance, which can be a Load Balancing (LB) or a Content Switching (CS) virtual server.

2. Depending on the authentication policy configured on the TM virtual server, the handshake of client side authentication starts and eventually the TM virtual server receives the complete credential from the client.

3. The TM virtual server verifies the client credential either directly, or through external authentication server.

4. If the authentication succeeds, then the TM virtual server selects a backend service and forwards the request to the service.

5. If Kerberos authentication is required or enabled on the service, then it responds with a 401 status code with WWW-Authenticate headers as follows:

   
   HTTP/1.1 401 Unauthorized
   ...
   WWW-Authenticate: Negotiate
   WWW-Authenticate: NTLM

   The two WWW-Authentication headers provide the receiver with the information that the more secured Negotiate or Kerberos authentication is preferred. If the receiver does not support Negotiate or Kerberos authentication, then the receiver sends the authentication to NTLM.

   When the TM virtual server receives the 401 response and if you had enabled single sign on (SSO) at the global level or on the virtual server, then the SSO handler for Kerberos triggers.

6. The authentication service request/response (AS-REQ/REP) exchange is the Kerberos TGT request and reply messages that the NetScaler sends to the KDC. If the exchange is successful, then the NetScaler appliance gets and caches a Kerberos ticket-granting ticket (TGT).

7. Through the TGS-REQ/REP exchange with the KDC, the NetScaler appliance gets the S4U2Self ticket with the TGT, user principle, and TM virtual server principle.

8. Through the TGS-REQ/REP exchange with the KDC, the NetScaler appliance eventually gets the S4U2Proxy service ticket with the S4U2Self ticket and the back end service principle.
9. The service ticket is encoded by base64 and then sent to the requested service in the HTTP Authorization header.

\[
\text{GET} / \\
\text{Authorization: Negotiate 89a8742aa8729a8b028}
\]

10. The backend service verifies the ticket in the HTTP request. If it is valid, then the service allows the user to access and reply with the right HTTP 200 OK response.

11. The NetScaler appliance receives the response, inserts session cookie, and forwards the response to the client.

12. All the subsequent HTTP requests to the same TM virtual server have the session cookie. As long as the cookie is still valid, no further client side authentication is required.

### 3.3 Integration with Existing Authentication Methods

Kerberos PT and CD are designed to support all existing authentication methods provided on a TM virtual server. The following matrix summarizes these authentication methods:

**Note:** Currently, Certificate-based authentication is not supported in 401-based TM VIP.

<table>
<thead>
<tr>
<th>Client Side Authentication</th>
<th>Server Side Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Kerberos</td>
</tr>
<tr>
<td></td>
<td>HTTP – Basic, Digest, NTLM</td>
</tr>
<tr>
<td></td>
<td>Constrained Delegation</td>
</tr>
<tr>
<td>Non-Kerberos</td>
<td>SAML</td>
</tr>
<tr>
<td>NTLM</td>
<td>Version 1</td>
</tr>
<tr>
<td></td>
<td>Version 2</td>
</tr>
<tr>
<td>CAC (Smart Card): at SSL/TLS Layer</td>
<td></td>
</tr>
<tr>
<td>HTTP Basic</td>
<td></td>
</tr>
<tr>
<td>Form-based</td>
<td></td>
</tr>
<tr>
<td>Kerberos</td>
<td>Kerberos</td>
</tr>
</tbody>
</table>
4. Configuration

This section outlines how to set up Kerberos Constrained Delegation with a NetScaler appliance. This involves setting up an account in the Active Directory, setting up the Server hosting the services, and configuring a NetScaler appliance.

The only new CLI commands introduced on a NetScaler appliance are to optionally specify domain or realm for a LB or CS virtual server in section 4.3.

4.1 Active Directory Configuration

This section explains the configuration steps required in the Active Directory to enable Constrained Delegation with NetScaler Secure Access.

4.1.1 Create a Kerberos Constrained Delegation (KCD) User Account

You must create a User account to get Constrained Delegation to work. This account must have the rights to do the Protocol Transition and Delegation. This is the account that has the rights to request a Kerberos Ticket on behalf of a user logging into the NetScaler appliance.

Start by creating a new user in the Active Directory.

In this example, create the kcdtest as the account to provide Constrained Delegation Access to Web server.

4.1.2 Enable the Delegation Tab for the Created User

Delegation is not enabled by default for a User account, you must enable it. This involves the use of the SETSPN command-line tool and a standard Windows 2003 installation does not include this tool.

Check in Active Directory User properties if delegation tab is available, if not download the 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 Windows 2003 server, it can be found in the C:\Program Files\Support Tools folder.

To get the latest version of setspn tool see http://support.microsoft.com/kb/970536.

Use the following command to run the setspn tool:

```
setspn -A host/kcdvserver.example.com example\kcdtest
```

**Note:** In this example, `example` is the **Domain** and `kcdtest` is the **user account**. In this register `kcdtest` user is with SPN: `host/kcdvserver.example.com`. 
This enables the Delegation tab in the kcdtest Properties.

If the Delegation Tab does not appear, then the Active Directory probably is running in mixed or native mode and must raise it to the Windows 2003 functional level.

**NOTE** that the following steps changes the Active Directory behavior and the support for older Windows clients. If you are uncertain, then you should not raise the Domain Functional Level without checking if this has any impact to the environment because this step cannot be reversed.

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

The Delegation tab should now be visible. Ensure that you enable the options **Trust this user for delegation to specified services only** and **Use any Authentication protocol**.
Even though other options might seem more accurate, the Kerberos only options do not work because these options do not enable Protocol Transition and Constrained Delegation.
4.1.3 Add the Services

You must specify the Services this applies to because this is constrained delegation. Select Add.

Click Users or Computers to select the Computer hosting these services.

In this example, SPH07.example.com hosts the Web service. Therefore, in the preceding SPH07 is selected. This can be any other Server in the Domain.

Note that Constrained Delegation does not support Services hosted in other Domains even though there is a trust relationship to those Domains. Add the Services on the selected Server.
The http service is selected because this example is about setting up Constrained Delegation to Web Server. This is the same for any other Web based applications running on this server such as Share Point/Outlook Web Access. Review the settings and click Apply/OK.

4.1.4 Generate Keytab file

Create the Keytab file for the kcdtest user with SPN:
host/kcdvserver.example.com@example.COM

You can select any of the following two options available to generate a keytab file:

- NetScaler GUI has a utility that helps in creating a batch file which can be run on Domain Controller to generate a keytab file. Select AAA-Application Traffic > Batch file to generate keytab to open this utility. Copy the generated script and run it from a Domain controller cmd prompt.

  Note: This GUI option is only available in NetScaler software release 10.1.
Domain User Name*: kcdtest
Domain Password*: ********
Service Principal*: host/kcdvserver@domain.com@com.com
Output File Name*: c:\ns_kcd.keytab

Create Domain User Account

Generate Script

```batch
@echo off
set kcdusername=kcdtest
set kcdpassword=freebsd
echo %kcdusername%
setspsn -A HTTP/%kcdusername% %USERDOMAIN%\%kcdusername%
setspsn -A host/host/kcdvserver@domain.com@f.com\%USERDNSDOMAIN% %USERDOMAIN%\%kcdusername%
kttpass -out c:\ns_kcd.keytab /princ
host/host/kcdvserver = "domain.com@f.com\%USERDNSDOMAIN%"
```

Run this script in AD Domain Controller and copy the keytab file to /nsconfig/krb/ folder in Netscaler.
• Run the following command to generate a keytab file:
  ```
  ktpass /princ host/kcdvserver.example.com@example.COM /ptype KRBS_NT_PRINCIPAL
  /mapuser example\kcdtest /pass freebsd -out C:\kcdvserver.keytab
  ```

  **Note:** host/kcdvserver.example.com@example.COM is case sensitive.

  Copy the kcdvserver.keytab file to the `/nsconfig/krb` directory on the NetScaler appliance.

  Active Directory configuration is complete.

4.2 Web Application Server Configuration

This section describes the configuration required on the server hosting the Web application. In this example, the application is Internet Information Services (IIS) Web server SPH07. This could be any Web application hosted on any server within the domain.
4.2.1 Configuring the IIS Server
Open the Internet Information Services Manager and select the Web site you want to enable Constrained Delegation.

Note: The Authentication settings might be set up at the top level (Default Web Site) for all sub-services or it could be setup for each service such as Exchange, Exadmin, ExchWeb, and Public to meet the requirements to log on properly to the required applications.

Open Properties and select the Directory Security tab. Select to edit the authentication and access control.

Ensure that you disable anonymous access and enable Integrated Windows authentication (only).

4.2.2 Web Server - Protocol Negotiation
After you select Integrated Windows authentication for IIS the Web Server protocol negotiation should be set to Negotiate,NTLM allowing Kerberos authentication with potential fallback to NTLM for non-Kerberos capable devices.
There might be scenarios where this is changed and Kerberos Authentication is disabled or fallback to NTLM does not work. If this is unknown, you can run the following command in C:\inetpub\AdminScripts to enable it:

```vbscript
C:\inetpub\AdminScripts>cscript adsutil.vbs
Usage:
    ADSUTIL.VBS <cmd> [path] [value]
Description:
    IIS administration utility that enables the configuration of metabase properties
    Supported Command:
    GET, SET, ENUM, DELETE, CREATE, COPY,
    APPCREATEINPROC, APPCREATEOUTPROC, APPCREATEGPOOLPROC, APPDELETE, APPUNLOAD, APPGETSTATUS
Samples:
    adsutil.vbs GET W3SVC/1/ServerBindings
    adsutil.vbs SET W3SVC/1/ServerBindings "":81:"
    adsutil.vbs CREATE W3SVC/1/Root/MyVirtualDir "IIsWebVirtualDir"
    adsutil.vbs START_SERVER W3SVC/1
    adsutil.vbs ENUM /P W3SVC
For Extended Help type:
    adsutil.vbs HELP
C:\inetpub\AdminScripts>cscript adsutil.vbs set w3svc/1/root/NTAuthenticationProviders "Negotiate:NTLM"
C:\inetpub\AdminScripts>cscript adsutil.vbs get w3svc/1/root/NTAuthenticationProviders
C:\inetpub\AdminScripts>cscript adsutil.vbs set w3svc/1/root/NTAuthenticationProviders : STRING "Negotiate:NTLM"
C:\inetpub\AdminScripts>cscript adsutil.vbs get w3svc/1/root/NTAuthenticationProviders
```

cscript adsutil.vbs get w3svc/WebSite/root/NTAuthenticationProviders

In this command, Website is a placeholder for the ID number of the Web site. The ID number of the default Web site is 1.
In the preceding screen shot the Authentication Protocol Negotiation is set to the required Negotiate,NTLM. If the returned string was something else, such as (STRING) "NTLM", then only NTLM is enabled.

To set this back to its default, run the following command:
```
cscript adsutil.vbs set w3svc/1/root/NTAuthenticationProviders "Negotiate,NTLM"
```

4.3 Setting up NetScaler for Constrained Delegation

4.3.1 Joining a NetScaler Appliance to the KDC

For Constraint Delegation to work, a NetScaler appliance should be part of the Kerberos Domain. To join the appliance to the domain, use Kerberos Domain Join option from AAA-Application Traffic and create a Negotiate Action as shown in the following screenshot.

User account used to join the domain should have Domain Administrator Privileges.
Ensure that you complete the following actions before joining the appliance to the domain:

- Add Name server in the appliance and point to Domain DNS server.
- Verify if the appliance can resolve to Domain, by using the Ping or Dig commands.
- Ensure that you synchronize the appliance and the domain controller with the same time, if not add NTP server to both.

**Note:** If the Domain Forest has multiple Domain Controllers, than add a static DNS entry pointing to the Domain.

Run the following command to join the appliance to a domain by using the command line interface:

```plaintext
add authentication negotiateAction neg1 -domain example.COM -domainUser <DomainAdmin> -domainUserPasswd d83d154575d426 -encrypted -OU TEST
bind aaa global -windowsProfile neg1
```

### 4.3.2 Create Backend Servers and Services

```plaintext
add server sph07 sph07.example.com
Or
add server sph07 10.217.28.93
```

**Note:** Here sph07 resembles the backend server name, the server name should match with backend server real name.

```plaintext
add service s1 sph07 HTTP 80
```
4.3.3 Create TM and Authentication Virtual Server

There are new commands introduced for the NetScaler appliance to specify domain or realm for a LB or CS virtual server when you define the virtual server. These parameters are optional.

```
add lb vserver accesslb1 HTTP 10.217.28.20 80
```

Create Authentication Virtual Server

```
add authentication vserver auth1 SSL 10.217.28.20 443
set authentication vserver auth1 –authenticationdomain Example.COM
```

4.3.4 Create KcdAccount

To extract SPN from the keytab file use Kcdaccount, NetScaler appliance reads the keytab file and extracts SPN listed from the keytab file.

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

**Note:** You must copy the Kcdvserver.keytab file to the /nsconfig/krb/ directory. If the file is not found in the /nsconfig/krb directory, then the NetScaler appliance rejects it.

```
show kcdAccount kcdaccount2
1)  KCD Account : kcdaccount2
    Keytab : /nsconfig/krb/kcdvserver.keytab
    Vserver Principle : host/kcdvserver.example.com@example.COM
Done
```

**Set/unset/rm** commands are allowed on Kcdaccount.

4.3.5 Create Traffic/Session Profile

You can provide Kcdaccount in session_action/traffic_action, NetScaler Administrator can select different rules. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address.
**Note:** When you specify kcdaccount in traffic/session profile with SSO: ON, NetScaler appliance completes a Kerberos constraint delegation to the backend servers. If KcdAccount is set to none, then the NetScaler appliance also completes a NTLM SSO.

**Setting in Session Profile**

```
add tm sessionAction myss01 -SSO ON –kcdaccount kcdaccount1
add tm sessionPolicy myss01 ns_true myss01
bind authentication vserver auth1 -policy myss01
```

**Setting in Traffic Profile**

```
add tm trafficAction mytraffic1 -SSO ON –kcdAccount kcdaccount1
add tm trafficPolicy myss01 TRUE myss01
bind lb vserver accesslb1 –policy myss01 –priority 100
```

**Setting at Global Level**

```
set tm sessionparameter -sso on –kcdaccount kcdaccount1
```

### 4.3.6 Enable Client Side Authentication (Form-based/401basic)

Enable the authentication method that you want on the TM virtual server. The following are examples to enable 401 Basic and form-based authentication:

```
set lb vs accesslb1 –authentication on –authenticationhost authvs.example.com
```

Or

```
set lb vs accesslb1 –authn401 –authnvsname auth1
bind lb vserver accesslb1 s1
```

If there is any error associated with running the preceding commands, see [Troubleshooting section 5.1](#).
5. Troubleshooting

5.1 Ensuring that lwagent Process and All Likewise Daemons are Running

Likewise daemons are lwsmd, lwregd, netlogond, lwiod, and lsassd.

Run the following command at the BSD shell:

```
ps ax | grep likewise
```

If you do not see all likewise daemons running, then run the following commands:

```
# rm –rf /var/lib/likewise/db
# /opt/likewise/bin/nslw.sh stop
# /opt/likewise/bin/nslw.sh start
```

You can see the following output:

```
# rm -rf /var/lib/likewise/db
# /opt/likewise/bin/nslw.sh stop
nslw: Likewise Open 6.1:
nslw: process 493 killed
nslw: lwagent stopped
Stopping service: lwreg
# /opt/likewise/bin/nslw.sh start
nslw: Likewise Open 6.1:
./
./local/
./local/lib/
./local/lib/pam_lsass.so
./local/lib/pam_lsass.la
./local/lib/nss_lsass.so.1
./local/lib/nss_lsass.la
./
./lib/
./lib/likewise/
./lib/likewise/lwconfig.xml
nslw: Found Likewise Open version 6.1
nslw: lwagent started
root@chrisns# nslw: Likewise Open 6.1:
Refreshing service manager
Starting service dependency: netlogon
Starting service dependency: lwiod
Starting service dependency: rdr
Starting service: lsass
nslw: lsassd started
```
Run the following command to verify if all processes are started:
```
ps ax | grep likewise
```

To verify if KCD is Working:

The following is a sample aaad.debug log when you access LB virtual server enabled with KCD and when KCD is successful:

```
lwagent.c[1198]: lw_start_get_s4u Call /opt/likewise/bin/kinit -k -t /nsconfig/krb/kcdvserver.keytab -f 'host/kcdvserver.example.com@example.COM'
Sun Jun 10 20:34:20 2012
lwagent.c[993]: get_s4u Get S4U2Proxy for:
User: abc@example.COM; Target: http/sph07.example.com;
Keytab: /nsconfig/krb/kcdvserver.keytab; spnego:0
Sun Jun 10 20:34:20 2012
lwagent.c[1015]: get_s4u Protocol transition tests follow
Sun Jun 10 20:34:20 2012
lwagent.c[1016]: get_s4u -----------------------------------
Sun Jun 10 20:34:20 2012
lwagent.c[1044]: get_s4u
```

The following is a trace at the Active Directory:

Pkt.514 shows Ticket request from NetScaler appliance to Active Directory and asking for a Ticket.
Pkt.515 shows Ticket is granted.
Pkt.520 S4U2SELF Request for host SPN: kcdvserver.example.com
Pkt.530 Constraint Delegation request for backend service http/sph07.example.com

NSIP: 10.217.28.2 AD: 10.217.28.93
MSG Type: AS-REQ (10)
- paddata: PA-ENC-TIMESTAMP Unknown:149
- Type: PA-ENC-TIMESTAMP (2)
- Type: Unknown (149)
- KDE_REQ_BODY
  - Padding: 0
  - KDE_OPTIONS: 40000010 (Forwardable, Renewable OK)
  - Client Name (Principal): host/kcdvserver. \com
    - Name-type: principal (1)
    - Name: host
    - Name: kcdvserver. \com
  - Realm: FDM2.COM
  - Server Name (Service and Instance): krbtgt/\com
    - from: 2012-06-11 03:37:42 (UTC)
    - till: 2012-06-12 03:37:42 (UTC)
    - Nonce: 78842123
  - Encryption Types: rc4-hmac

Frame 51 (133 bytes on wire, 132 bytes captured)
- Ethernet II, Src: 06:a7:d8:56:00:df (06:a7:d8:56:00:00:df), Dst: 00:1f:22:86:13:15 (00:1f:22:86:13:15)
- Internet Protocol, Src: 10.217.28.93, Dst: 10.217.28.2 (10.217.28.2)
- User Datagram Protocol, Src Port: 60952 (60952), Dst Port: kerberos (88)
- Kerberos AS-REP
  - Pync: 5
  - MSG Type: AS-REP (11)
  - Client Realm: FDM2.COM
  - Client Name (Principal): host/kcdvserver. \com
    - Name-type: Principal (1)
    - Name: host
    - Name: kcdvserver. \com
  - Ticket
    - Tkt-type: FDM2.COM
    - Realm: FDM2.COM
    - Server Name (Service and Instance): krbtgt/\com
      - Name-type: service and instance (2)
      - Name: krbtgt
      - Name: \com
<table>
<thead>
<tr>
<th>Source IP Address</th>
<th>Source Port</th>
<th>Destination IP Address</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.17.28.2</td>
<td>10.217.28.2</td>
<td>10.217.28.93</td>
<td></td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>10.17.28.2</td>
<td>10.217.28.2</td>
<td>10.217.28.93</td>
<td></td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>10.17.28.2</td>
<td>10.217.28.2</td>
<td>10.217.28.93</td>
<td></td>
<td>TCP</td>
<td></td>
</tr>
</tbody>
</table>

Kerberos TGS-REQ
- Record Mark: 1489 bytes

- MSG Type: TGS-REQ (12)
- pdata: PA-TGS-REQ PA-S4U2SELF Unknown:130
  - Type: PA-TGS-REQ (1)
  - Type: PA-S4U2SELF (129)
  - Type: Unknown (130)
- KDC_REQ_BODY
  - Padding: 0
  - koptions: 40810000 (Forwardable, Renewable, Canonicalize)
  - Server Name (Principal): host/kcdvserver.1.com
    - Name-type: Principal (1)
    - Name: host
    - Name: kcdvserver.1.com
    - till: 2012-06-11 13:37:49 (UTC)
    - nonce: 1339385869
- Pseudo-Data: 2538 bytes

Kerberos TGS-REQ
- Record Mark: 2233 bytes

- MSG Type: TGS-REQ (12)
- pdata: PA-TGS-REQ
  - Type: PA-TGS-REQ (1)
- KDC_REQ_BODY
  - Padding: 0
  - koptions: 40830000 (Forwardable, Renewable, Constrained Delegation, Canonicalize)
  - Realm: .COM
  - Server Name (Principal): www/sph07.1.com
    - name-type: Principal (1)
    - Name: www
    - Name: sph07.1.com
    - till: 2012-06-11 13:37:49 (UTC)
    - nonce: 1339385869

Encryption Types: rc4-hmac

Tickets:
5.3 Kinit string: Verifying if NetScaler appliance is Requesting a Forwardable Ticket: S4U2SELF

Run the following command from the shell prompt of the NetScaler appliance:

```
# /opt/likewise/bin/kinit -k -t /nsconfig/krb/kcdvserver.keytab -f 'host/kcdvserver.example.com@example.COM'
```

NetScaler appliance should send an AS-REQ to the Active Directory with Client Principal Name as host/kcdvserver.example.com@example.COM.

5.4 Kinit String: Verifying if Kinit Request Fails or if you Get Any of the Following Errors

```
# /opt/likewise/bin/kinit -k -t /nsconfig/krb/kcdvserver.keytab -f 'host/kcdvserver.example.com@example.COM'
gss_init_sec_context: Unspecified GSS failure. Minor code might provide more information
gss_init_sec_context: Matching credential not found
```

Fix: Create a new keytab file and specify in kcdaccount. Delete if there is any duplicate SPN in Active Directory.

5.5 t_s4u request

If you get any of the following errors, try the fix provided.

- `/opt/likewise/bin/t_s4u xyz@example.COM http/sph07.example.com /nsconfig/krb/kcdvserver.keytab`
  - Warning: no delegated credentials handle returned
- Verify if the TGT for the impersonating service can be forwarded.
- Verify if the T2A4D flag set on the impersonating service is UAC.
- Verify if the user is not marked sensitive and cannot be delegated.
Fix: Ensure that you enable the **Use Any Authentication Protocol** option.

- "Server not found in Kerberos database" when you run `/opt/likewise/bin/t_s4u xyz@example.COM www/nsi-dc1-2008.example.com /nsconfig/krb/kcdvserver.keytab` command.
  
  **Fix:** Check `/etc/krb5.conf`, if it is pointing to the wrong domain, take a backup of the file and change it to correct domain and save it.

- `/opt/likewise/bin/t_s4u administrator@example.COM http/sharepoint.example.com /nsconfig/krb/kcdvserver.keytab`

  Protocol transition tests follow

  -------------------------------

  gss_acquire_cred_impersonate_name: Unspecified GSS failure. Minor code may provide more information

  gss_acquire_cred_impersonate_name: Client not found in Kerberos database
**Fix:** Verify if the Do not require kerberos preauthentication option is enabled or disabled. You must disable this option.

![User logon name (pre-Windows 2000):](image)

- Logon Hours...  
- Log On To...

Account options:
- Smart card is required for interactive logon
- Account is sensitive and cannot be delegated
- Use DES encryption type for this account
- **Do not require Kerberos preauthentication**

Account expires:
- Never
- End of: Thursday, November 22, 2012

- If the procedure to join the appliance to the domain fails or takes longer time, as in the case of Cross Domain Forests, then add nameserver to the /etc/hosts file. For example; 10.217.22.241 nsi-dc1-2008.example.com nsi-dc1-2008

And add KDC to the /etc/resolve.conf file
For example; search example.com nameserver 10.217.22.241
6. Firewall Ports Required to be Open for KCD Communication

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>UDP/TCP</td>
<td>DNS</td>
</tr>
<tr>
<td>88</td>
<td>UDP/TCP</td>
<td>Kerberos</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>NTP</td>
</tr>
<tr>
<td>135</td>
<td>TCP</td>
<td>RPC Endpoint Mapper</td>
</tr>
<tr>
<td>137</td>
<td>UDP</td>
<td>NetBIOS Name Service</td>
</tr>
<tr>
<td>139</td>
<td>TCP</td>
<td>NetBIOS Session (SMB)</td>
</tr>
<tr>
<td>389</td>
<td>UDP/TCP</td>
<td>LDAP</td>
</tr>
<tr>
<td>445</td>
<td>TCP</td>
<td>SMB over TCP</td>
</tr>
<tr>
<td>464</td>
<td>UDP/TCP</td>
<td>Machine password changes (typically after 30 days)</td>
</tr>
<tr>
<td>3268</td>
<td>TCP</td>
<td>Global Catalog Search</td>
</tr>
</tbody>
</table>
7. Reference
http://support.citrix.com/article/CTX139133