Abstract
This white paper explains how to setup Kerberos environment for CenterStage with Single / Multi-Repository, Multi-Docbase and Multi-Domain Setup. This also explains how to troubleshoot common errors while configuring Kerberos setup.

July 2013
## Table of Contents

Executive Summary .......................................................................................................................... 4  
Purpose........................................................................................................................................4  
Audience.........................................................................................................................................4  
Introduction ....................................................................................................................................4  
Prerequisites....................................................................................................................................5  
Creating Active Directory .............................................................................................................6  
References .......................................................................................................................................32  
Conclusion ........................................................................................................................................32
Executive Summary

This white paper explains the Kerberos Architecture in brief and ideal way to successfully setup in windows environment with explanation on creating Active Directory, adding users to Active Directory, generating keytab files for users, Setup On Content Server, setup on Application Server, and setup on client side browsers. The white paper also explains troubleshooting steps and tools recommended for it. The white paper covers Kerberos with multi-repository setup as well as an additional advantage.

As part of the effort to improve and enhance the performance and capabilities of its product line, EMC, from time to time releases revisions of its hardware and software. Therefore, some functions described in this guide may not be supported by all revisions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product Release Notes document.

If a product does not function properly or does not function as described in this document, please contact your EMC representative.

Note: We vouch that the content in this document is accurate at the time of publication. However, as information is added, new versions of this document may be released to the EMC online support website. Check the website to ensure that you are using the latest version of this document.

Purpose

This document explains the process of implementing Kerberos Authentication Protocol with respect to CenterStage with single and Multi-Docbase, Multi-Repository and Multi-Domain environment. (The setup can also be used for other Documentum products like, Webtop and TaskSpace).

Audience

The audience for this white paper comprises personnel responsible for the configuration and administration of the Kerberos environment with regard to CenterStage. This document is intended for internal EMC personnel, partners, and customers.

Introduction

This guide discusses how to create Kerberos for CenterStage with Apache Tomcat application server, which is configured for accessing requests from Kerberos client.

The process of implementing Kerberos Authentication for CenterStage with Apache Tomcat application server involves the following steps:
• Creating Active Directory
• Installing Support Tools for executing ‘ktpass’ commands to generate keys
• Enabling cryptography in machines other than Windows 2000 or Windows Server 2003
• Adding machines to domain
• Adding computers and users to Active Directory
• Creating keytab files for Content Server and Application servers by executing ‘ktpass’ command
• Enable tracing in Content Server
• Configure Application Server for Kerberos
• Configure browsers on Kerberos client
• Test CenterStage for Kerberos Authentication

Prerequisites

Below are the environment details where this setup was configured and tested. This is one of the working scenarios, not requirement of OS.

Active Directory Machine:
Windows 2003 OS 32 bit machine
Setup Active Directory and domain in the machine and make it domain controller. Add users and computers to it. Install support tools for executing ktpass commands to generate Keytab files.

Application server machines:
Windows 2003 OS 32 bit machine
Install the desired Application Server version (Apache Tomcat and jdk-1_5_0_22) and CenterStage/Webtop will be deployed in the respective Application Server.

Content Server Machines:
Windows 2003 OS 32 bit machine
Install Documentum 6.6 or above Content Server which is added to the Kerberos domain. For CenterStage, you'll need to install required DAR files in it.
Kerberos Client Machines:
Windows XP OS 32 bit machine
Configure browsers with java enabled, to access CenterStage through Kerberos Authentication.

CenterStage
CenterStage 1.2 Sp1 has been used to deploy in the Apache Tomcat application server.

Creating Active Directory
Important Prerequisite: Install support tools in the machine with respective operating system which has ktpass.exe packaged inside it.

The download is available here,

The following article describes how to install and configure a new Active Directory installation in a laboratory environment that includes Windows Server 2003 and Active Directory. Note that you will need two networked servers that are running Windows Server 2003 for this purpose in a laboratory environment.

After you have installed Windows Server 2003 on a stand-alone server, run the Active Directory Wizard to create the new Active Directory forest or domain, and then convert the Windows Server 2003 computer into the first domain controller in the forest. To convert a Windows Server 2003 computer into the first domain controller in the forest, follow these steps:

1. Insert the Windows Server 2003 CD-ROM into your computer’s CD-ROM or DVD-ROM drive.
2. Click Start, click Run, and then type dcpromo.
3. Click OK to start the Active Directory Installation Wizard, and then click Next.
4. Click Domain controller for a new domain, and then click Next.
5. Click Domain in a new forest, and then click Next.
6. Specify the full DNS name for the new domain. Note that because this procedure is for a laboratory environment and you are not integrating this environment into your existing DNS infrastructure, you can use something generic, such as mycompany.local, for this setting. Click Next.
7. Accept the default domain NetBIOS name (this is "mycompany" if you used the suggestion in step 6). Click Next.

8. Set the database and log file location to the default setting of the c:\winnt\ntds folder, and then click Next.

9. Set the Sysvol folder location to the default setting of the c:\winnt\sysvol folder, and then click Next.

10. Click Install and configure the DNS server on this computer, and then click Next.

11. Click Permissions compatible only with Windows 2000 or Windows Server 2003 servers or operating systems, and then click Next.

12. Because this is a laboratory environment, leave the password for the Directory Services Restore Mode Administrator blank. Note that in a full production environment, this password is set by using a secure password format. Click Next.

13. Review and confirm the options that you selected, and then click Next.

14. The installation of Active Directory proceeds. Note that this operation may take several minutes.

15. When you are prompted, restart the computer. After the computer restarts, confirm that the Domain Name System (DNS) service location records for the new domain controller have been created. To confirm that the DNS service location records have been created, follow these steps:

   a. Click Start, point to Administrative Tools, and then click DNS to start the DNS Administrator Console.

   b. Expand the server name, expand Forward Lookup Zones, and then expand the domain.

   c. Verify that the _msdcs, _sites, _tcp, and _udp folders are present. These folders and the service location records they contain are critical to Active Directory and Windows Server 2003 operations.

For more info and pictured steps refer, http://www.petri.co.il/installing-active-directory-windows-server-2008.htm

(Or raise an 'lrm' ticket for creating Active Directory for Kerberos setup)

Note: Follow these steps only for machines other than Windows 2000 or Windows Server 2003 (Windows 2008 server)

{ We have to enable OLD cryptography in ActiveDirectory m/c(windows2008r2{KDC})like as mentioned in the following URL:}
To work around this problem, make sure that client computers use the cryptography algorithms that are compatible with Windows Server 2008. You may have to request software updates from the product vendors.

If you cannot install software updates because a service outage will occur, follow these steps:

1. Log on to a Windows Server 2008-based domain controller.
2. Click Start, click Run, type gpmc.msc, and then click OK.
3. In the Group Policy Management console, expand Forest: DomainName, expand DomainName, expand Domain Controllers, right-click Default Domain Controllers Policy, and then click Edit.
4. In the Group Policy Management Editor console, expand Computer Configuration, expand Policies, expand Administrative Templates, expand System, click Net Logon, and then double-click Allow cryptography algorithms compatible with Windows NT 4.0.
5. In the Properties dialog box, click the Enabled option, and then click OK.

**Notes**

- By default, the Not Configured option is set for the Allow cryptography algorithms compatible with Windows NT 4.0 policy in the following Group Policy objects (GPO):
  - Default Domain Policy
  - Default Domain Controllers Policy
  - Local Computer Policy

By default, the behavior for the Allow cryptography algorithms compatible with Windows NT 4.0 policy on Windows Server 2008-based domain controllers is to programmatically prevent connections from using cryptography algorithms that are used in Windows NT 4.0. Therefore, tools that enumerate effective policy settings on a member computer or on a domain controller will not detect the Allow cryptography algorithms compatible with Windows NT 4.0 policy unless you explicitly enable or disable the policy.

- Windows 2000 Server-based domain controllers and Windows Server 2003-based domain controllers do not have the Allow cryptography algorithms compatible with Windows NT 4.0 policy. Therefore, pre-Windows Server 2008-based domain controllers accept security channel requests from client computers even if the client computers use the old cryptography algorithms that are used in Windows NT 4.0. If security channel requests are intermittently processed by Windows Server 2008-based domain controllers, you will experience inconsistent results.
6. Install third-party software updates that fix the problem, or remove client computers that use incompatible cryptography algorithms.

7. Repeat steps 1 through 4.

8. In the Properties dialog box, click the Disabled option, and then click OK.

**Important** For security reasons, you should set the option for this policy back to Disabled.

In every machine other than 2000 and 2003, (windows2008R2SP1) we have to allow encryption types for Kerberos in below path

Start-->Run-->gpedit.msc


Double Click on Network security: Configure encryption types allowed for Kerberos and check the checkboxes for DES_CBC_CRC,DES_CBC_MD5,RC4_HMAC_MD5.
Adding Users and Computers to the Active Directory Domain

After the new Active Directory domain is established, create a user account in that domain to use as an administrative account. When that user is added to the appropriate security groups, use that account to add computers to the domain.

1. To create a new user, follow these steps:
   - Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers** to start the Active Directory Users and Computers console.
   - Click the domain name that you created, and then expand the contents.
   - For creating **Right-click Users**, point to **New**, and then click **User**.
   - Type the first name (any unique name), last name, and user logon name of the new user, and then click **Next**.
Type a new password, confirm the password, and then click to select one of the following check boxes:

- Users must change password at next logon (recommended for most users)
- User cannot change password
- Password never expires
- Account is disabled

Click **Next**.
• Review the information that you provided, and if everything is correct, click Finish.

Adding machine to the domain
The final step in this process is to add a member server to the domain. This process also applies to workstations. To add a computer to the domain, follow these steps:

Log on to the computer that you want to add to the domain.

• Right-click My Computer, and then click Properties.
• Click the Computer Name tab, and then click Change.
• In the Computer Name Changes dialog box, click Domain under Member Of, and then type the domain name. Click OK.
• When you are prompted, type the user name and password of the account that you previously created, and then click OK.

A message that welcomes you to the domain is generated.
• Click OK to return to the Computer Name tab, and then click OK to finish.
• Restart the computer if you are prompted to do so.
Note: Add all other machines to active directory by setting ‘Preferred DNS Server’ to IP of Active Directory Machine and add it to the domain.

Content Server

In Active Directory,

Create a user for content server as described above. Once done, set the property “Use DES encryption type for this account” (In Windows 2008 “Use Kerberos DES encryption types for this account”) to true by enabling the checkbox in “Account” tab from user properties.

Now to generate the keytab file for the user,
Open ‘cmd’ from Run and choose the path to support tools installed.

For Ex:
C:\Program Files\Support Tools>

Type the following command to generate keytab file

ktpass /pass <password > -out <keytab-file> -princ <SPN> -crypto DES-CBC-MD5 +DumpSalt -ptype KRB5_NT_PRINCIPAL +desOnly /mapOp set /mapUser <user-name>

Where,

password : The password of the user created in Active Directory
DES-CBC-MD5: Type of cryptography being used
keytab-file : Location to save the keytab file

Note: The keytab file should be named as <repositoryname>.<uniqueno>.keytab (for E.g: kerbrepo.988.keytab).

SPN - The SPN for the Docbase/Content Server is like CS/repositoryname@DOMAINNAMEINCAPS (E.g: CS/kerberos66 @WDKBLR.COM)

user-name : User name (E.g. better to create a user with name same as repository)
For Ex:

C:\Program Files\Support Tools>ktpass /pass Password@123 -out kerbrepo.1234.keytab -princ CS/kerbrepo@WIN2K3AD.COM -crypto DES-CBC-MD5 +DumpSalt -ptype KRB5_NT_PRINCIPAL +desOnly /mapOp set /mapUser kerbrepo

Note: Be careful while defining SPNs and generating keytab files for a user and note the parameters defined and also generated by system after executing the ktpass command (Ex: vno number details).

After generating the keytab, go to User Properties to verify the SPN registered to the user. The user logon name now shows the registered SPN.

Check the box for “Use DES encryption types for this account”.
Note: ktpass will register the SPN to a user, registering more than one SPN to a same user causes issues while authentication. To reuse the same user, delete the user and recreate the user and generate the keytab again. User can register more than one SPNs.

Just like in Windows 2008 For Windows 7, DES services should be enabled under Local Security Policy (Go to Local Security Policies(By typing “Local Security Policies” in run dialog)->Local Policies->Security Options->Network security: Configure encryption types allowed for Kerberos: and check the boxes for cryptographic type needed)

In Windows 2008 server after generating the keytab in Windows 2008 server a new tab “Delegation” will be created for the user properties. Check the radio for “Trust this user for delegation to any service (Kerberos only)”.

Click OK to apply the properties.

Copy the repository keytab file to Content Server machine.

to %DCTMHOMEx%\ dba\auth\kerberos folder.
Default path is “C:\Documentum\dba\auth\kerberos”
Note: Add “-otrace_authentication” string at the start of command in Documentum Server Manager’s “Edit Service” to trace Kerberos logs.

Restart the content server.

In Addition, if user wants to use multiple Docbases, generate keytab file for each of them and place the file under %DCTMHOMEdbauthkerberos folder.

**Defining SPNs for a user with multiple Repositories**

First check for the SPNs defined for a user by executing the following command,

`setspn –L <Kerberos User Name>`

To define an additional SPN for a user for accessing two repositories from same machine content server,

Execute this command,

`setspn –A CS/<Repository Name> <Kerberos User for Content Server>`

For Ex:

`setspn -A CS/kerbrp1 kerbrp`

where kerbrp1 is second repository and kerbrp is the content server user defined for first repository while generating the keytab file.

Check for SPNs defined by executing the following command,

`setspn -L kerbrp`

Result should be like,

```
C:\Program Files\Support Tools>setspn -l kerbrp
Registered ServicePrincipalNames for CN=kerbrp,CN=Users,DC=win2k3ad,DC=com:
```
CS/kerbrp1
CS/kerbrp

Where,

CS/kerbrp1
CS/kerbrp

Are the SPNs for two repositories: kerbrp1 and kerbrp. Then, execute the RawSalt command to map the user for both repositories as following:

ktpass /pass <Password> -out <Keytab File> -princ <SPN For Repository> -crypto DES-CBC-MD5 +DumpSalt -ptype KRB5_NT_PRINCIPAL +desOnly /mapOp set +RawSalt <salt result from first ktpass command for first repository> -in <Keytab name for first repository> -kvno <vno number from first ktpass command for first repository>

For Example:

ktpass /pass Password@123 -out kerbrp1.2234.keytab -princ CS/kerbrp1@WIN2K3AD.COM -crypto DES-CBC-MD5 +DumpSalt -ptype KRB5_NT_PRINCIPAL +desOnly /mapOp set +RawSalt WIN2K3AD.COMCSkerbrp -in kerbrp.1234.keytab -kvno 3

Where,

Kerbrp1.2234.keytab is new and unique keytab file name.

CS/kerbrp1@WIN2K3AD.COM is SPN for second repository.

WIN2K3AD.COMCSkerbrp is salt result generated while generating the keytab file for the first repository.
Single/Multi-Repository, Multi-Docbase and Multi-Domain Kerberos Environment setup for CenterStage

Kerbrp.1234.keytab is keytab file name used while generating the keytab file for the first repository first time.

Kvno 3 is vno number generated while generating the keytab file for the first repository first time.

Copy both the keytab files for both repositories Kerbrp1.2234.keytab and Kerbrp.1234.keytab to content server Kerberos folder.

Restart the content server with all the repositories.

Now you should be able to access the application (Webtop) with two repositories to choose at the beginning without asking for user credentials.

Application Server:

Note: Start application server for Documentum Administrator and mention the Domain name under user properties/’User Login Domain’ for Administrator or a Kerberos user.

In Active Directory,

Create a user for App server as described above. Once done, set the property “Use DES encryption type for this account” and “Account is Trusted for delegation” (In Windows 2008 “Use Kerberos DES encryption types for this account” after generating the keytab in Windows 2008 server a new tab “Delegation” will be created for the user properties. Check the radio for “Trust this user for delegation to any service (Kerberos only)”.

) to true by enabling the checkboxes in “Account” tab from user properties.

Now to generate the keytab file for the user,

Type the following command to generate keytab file
ktpass /pass <password> -out <keytab-file> -princ <SPN> -crypto DES-CBC-MD5 +DumpSalt -ptype KRB5_NT_PRINCIPAL +desOnly /mapOp set /mapUser <user-name>

Where,

password : The password of the user created in Active Directory
keytab-file - Location to save the keytab file
DES-CBC-MD5: Type of cryptography being used
SPN - The SPN framed by the browser is like
HTTP/hostnameappservicemachine.domainnameinsmall@DOMAINNAMEINCAPS
(E.g: HTTP/NEWWIN2K3APP.win2k3ad.com@WIN2K3AD.COM)
user-name - User name (E.g. centerspn1)

For Ex:

C:\Program Files\Support Tools\ktpass /pass Password@123 –out kerbrepocenterspn1.keytab –princ HTTP/NEWWIN2K3APP.win2k3ad.com@WIN2K3AD.COM -crypto DES-CBC-MD5 +DumpSalt -ptype KRB5_NT_PRINCIPAL +desOnly /mapOp set /mapUser centerspn1

After generating the keytab, go to User Properties to verify the SPN registered to the user. The user logon name now shows the registered SPN.
Check the boxes for “Account is trusted for delegation” and “Use DES encryption types for this account”.

Note: ktpass will register the SPN to a user, registering more than one SPN to a same user causes issues while authentication. To reuse the same user, delete the user and recreate the user and generate the keytab again. User can register more than one SPNs.

Just like in Windows 2008 For Windows 7 For Windows 7 DES services should be enabled under Local Security Policy (Go to Local Security Policies(By typing “Local Security Policies” in run dialog)->Local Policies->Security Options->Network security: Configure encryption types allowed for Kerberos: and check the boxes for cryptographic type needed)

In Windows 2008 server after generating the keytab in Windows 2008 server a new tab “Delegation” will be created for the user properties. Check the radio for “Trust this user for delegation to any service (Kerberos only)”. 
Click OK to apply the properties.

Copy the keytab file generated from the ktpass command to `<web-app-root>/WEB-INF` folder

C:\ApacheTomcat\Webapps\'Application'\WEB-INF

Create krb5Login.conf file at `<web-app-root>/WEB-INF` folder for JAAS with the following contents

HTTP-newwin2k3app-win2k3ad-com
{
    com.sun.security.auth.module.Krb5LoginModule required
debug=true
principal="HTTP/newwin2k3app.win2k3ad.com@WIN2K3AD.COM"
refreshKrb5Config=true
useKeyTab=true
storeKey=true
doNotPrompt=true
useTicketCache=false
isInitiator=false
keyTab="C:\apache-tomcat-5.5.34\webapps\webtop\WEB-INF\kerbrepocenterspn1.keytab";
);

Modify the krb5Login.conf with the following details.

- The login context name (HTTP-newwin2k3app-win2k3ad-com) should match with the SPN registered where, newwin2k3app is hostname of application server machine as defined in SPN. Replace '/' and '.' with '-' in the SPN to get the login context name. and should be in small letters.
- Set the principal to SPN which also should be in small letters.
- The keytab should point to the location of the keytab file in the WEB-INF folder of Tomcat.
- Please avoid any extra space, tabs or new-line entries in the details.

Create krb5.ini file at %WINDIR% (C:\WINDOWS in Windows 2003 and C:\WINNT in windows 2008) folder with the following contents,

```
[libdefaults]
default_realm = Domain name in caps
forwardable = true
ticket_lifetime = 24h
clockskew = 72000
default_tkt_enctypes = des-cbc-md5 des-cbc-crc des3-cbc-sha1
default_tgs_enctypes = des-cbc-md5 des-cbc-crc des3-cbc-sha1
permitted_enctypes = des-cbc-md5 des-cbc-crc des3-cbc-sha1

[realms]
Domain name in caps = {
```
kdc = Active Directory hostname with domain
admin_server = Active Directory hostname with domain
}

Modify the krb5.ini with the following details
- default_realm - specify the Kerberos domain name
- realms section should point to the KDC server
- Please avoid any extra space, tabs or new-line entries

Edit the catalina.bat file of Tomcat and specify the following java options.

```
set JAVA_OPTS=%JAVA_OPTS% -Djava.security.krb5.conf=%WINDIR%/krb5.ini -Djava.security.auth.login.config=<web-app-root>/WEB-INF/krb5Login.conf -Djavax.security.auth.useSubjectCredsOnly=false
```

For Ex:

```
set JAVA_OPTS=%JAVA_OPTS% -Djava.security.krb5.conf=C:\WINDOWS\krb5.ini -Djava.security.auth.login.config="C:\apache-tomcat-5.5.34\webapps\webtop\WEB-INF\krb5Login.conf" -Djavax.security.auth.useSubjectCredsOnly=false
```

add the below lines to define heap size,
```
set JAVA_OPTS=%JAVA_OPTS% -Xms256m -Xmx1024m -Xdebug -Xnoagent -Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=10000
```

Deploy CenterStage/Webtop in application server for Kerberos repository.

**Kerberos setup with multiple Domains**

Create two or more child domains in Kerberos setup, with a parent domain.

For Ex:

Parent Domain: WIN2K3AD.COM
Child Domain 1: WIN2K3AD2.COM
Child Domain 2: WIN2K3AD3.COM
Child Domain 3: WIN2K3AD4.COM
Child Domain 4: WIN2K3AD5.COM

Define SPN and create Keytab for a repository in Active Directory as defined above.

Create krb5Login.conf file at <web-app-root>/WEB-INF folder for JAAS with the following contents,

```plaintext
HTTP-newwin2k3app-win2k3ad4-win2k3ad-com
{
  com.dstc.security.kerberos.jaas.KerberosLoginModule required
debug=true
principal="HTTP/newwin2k3app.win2k3ad4.win2k3ad.com"
refreshKrb5Config=true
useKeyTab=true
storeKey=true
doNotPrompt=true
useTicketCache=false
noTGT=true
keyTab="C:\apache-tomcat-5.5.34\webapps\webtop\WEB-INF\kerbrepocenterspn1.keytab"
realm="WIN2K3AD4.WIN2K3AD.COM";
}
```
Create krb5.ini file at %WINDIR% (C:\WINDOWS in Windows 2003 and C:\WINNT in windows 2008) folder with the following contents,

```
[libdefaults]
default_realm = WIN2K3AD4.WIN2K3AD.COM
forwardable = true
ticket_lifetime = 24h
clockskev = 72000
default_tkt_enctypes = aes128-cts des-cbc-md5 des-cbc-crc des3-cbc-sha1 rc4-hmac
default_tgs_enctypes = aes128-cts des-cbc-md5 des-cbc-crc des3-cbc-sha1 rc4-hmac
permitted_enctypes = aes128-cts des-cbc-md5 des-cbc-crc des3-cbc-sha1 rc4-hmac

[realms]
WIN2K3AD4.WIN2K3AD.COM = {
  kdc = Active Directory hostname/IP with domain
  admin_server = Active Directory hostname/IP with domain
}

[domain.realm]
.domain.com = DOMAIN.COM
.win2k3ad.com = WIN2K3AD.COM
.WIN2K3AD.com = WIN2K3AD.COM
.WIN2K3AD4. WIN2K3AD.com = WIN2K3AD4. WIN2K3AD.COM
.WIN2K3AD5. WIN2K3AD.com = WIN2K3AD5. WIN2K3AD.COM

[logging]
kdc = CONSOLE
```

**Webtop Configurations**

1. Edit the wdk\app.xml kerberos section
2. Set enabled to true
3. Specify the kerberos domain name (E.g: NEW2K3AD.COM)
4. Restart the app server by clearing the cache

Note: Please wait for some time till Kerberos gets enabled (usually for an hour)
If it's not and asking for webtop connections, then please log-off the client and login
again to the machine. User created in Active Directory and same in repository should
be able to acces the application if he can connect to client machine by RDC.

**Client Machine:**

**Setup**

Edit `%WINDIR%/system32/drivers/etc/hosts` file and map appserver machine IP to it
with fully qualified domain name

**IE Setup**

Launch IE

Go to Tools > Internet Options > Security tab.
For IE7 and IE8, "Uncheck Enable Protected Mode" option for Internet, Local Intranet.
Select the Local intranet icon and click Sites
In the Local intranet window, ensure that the "check box" to include all local (intranet) not listed in other zones is selected, then click Advanced

Add webtop url to the Websites. (E.g: [http://newwin2k3app.win2k3ad.com](http://newwin2k3app.win2k3ad.com))
Click OK

On the Internet Options window, click the “Advanced” tab and scroll to Security settings. Check 'Enable Integrated Windows Authentication (requires restart)' option is enabled.
Click OK

Restart the browser

Firefox Setup

At the address field, type about:config

In the Filter, type network.n

Edit network.negotiate-auth.trusted-uris and add the webtop URL

(E.g. http://newwin2k3app.win2k3ad.com)

Edit network.negotiate-auth.delegation-uris and add the webtop URL

(E.g. http://newwin2k3app.win2k3ad.com)
Restart the browser

Test It:

Access the CenterStage application with SPN name in URL, (http://<appserver hostname>.<domainname>:<port number>(default tomcat port is 8080)/<application>/#<repository>).

For Ex: http://newwin2k3app.win2k3ad.com:8080/CenterStagePro/#kerbrepo

The application will take the Desktop Credentials to login and user can access application as desktop user.

Summary:

Active Directory:
Create a user for Content Server and a user for Application Server and generate keytab files for both users. Create a user to use as a client to login to the application and the same user should be in the repository. (The user need not be created for accessing
client machine. The user created in Active Directory should be able to access all the machines in the same domain)

Content Server:
Place the keytab file generated in Active Directory in “Documentum/dba/auth/Kerberos” folder and restart the Documentum Content Server.

Application Server:
In Application Server, create a configuration file named “krb5Login.conf” with proper Principal SPN and location of keytab file details and place it into “webapps/<web application>/WEB-INF” folder along with the keytab file created in Active Directory for application server. Create an initialization file (.ini) named “krb5.ini” with default_realm details pointing to the domain in use and Active directory (KDC and admin_server) details. Restart the application server.

Client machine:
Any machine in the same domain can be a client machine for a user who is in Active Directory and repository to access the application via Kerberos. In Internet explorer 8, go to “tools>internet options>security tab” and select “Local intranet”. Open ‘sites’ and uncheck “Automatically detect intranet network” and select all other options. Click ‘Advanced’ and add SPN name registered for Kerberos (http://<appserver hostname>.<domainname>). Save the settings and restart the browser.

Access the CenterStage application with SPN name in URL, (http://<appserver hostname>.<domainname>:<port number>(default tomcat port is 8080)/<application>/#<repository>).

When a user accesses the application, the browser should not ask him to provide the credentials to login, instead, it should take the desktop credentials and take him to the application home-page.

Common Errors:

If browser on client is not accepting windows credentials then please check domain name for Kerberos user in Documentum Administrator and try connecting again.

For troubleshooting Kerberos on windows you can use either of the tools mentioned below,
3. Or you can use Wireshark to monitor key distribution under Kerberos environment

References


Conclusion

This white paper explains how to implement Kerberos multi-repository, multi-docbase and multi-domain on Windows systems and configure to access CenterStage through Kerberos.