Pre-Authentication User: communicates between AD and Tomcat

EXAMPLE.COM= SERI.SAILPOINTDEMO.COM

example.com=seri.sailpointdemo.com

EXAMPLE= SERI.SAILPOINTDEMO

Service Account = SERI\svc\_tomcat\_iiq

Firstname = Tomcat

Lastname = Service

EXAMPLE\svc\_tomcat\_iiq= SERI.SAILPOINTDEMO\svc\_tomcat\_iiq

DNS Comparision:

HTTP/TESTLABDC.example.com@example.com= [HTTP/TESTLABDC.seri.com@seri.sailpointdemo.com](mailto:HTTP/TESTLABDC.seri.com@seri.sailpointdemo.com)

SPN Comparison:

[HTTP/TESTLABDC.example.com@EXAMPLE.COM](mailto:HTTP/TESTLABDC.example.com@EXAMPLE.COM) = [HTTP/TESTLABDC.seri.com@SERI.SAILPOINTDEMO.COM](mailto:HTTP/TESTLABDC.seri.com@SERI.SAILPOINTDEMO.COM)

KeyTab generation:

To map <http://seri.sailpointdemo.com>) with SPN in the domain.

Registering SPNs:

Register svc\_tomcat\_iiq as the owner of SPN

setspn -a http/testlabdc svc\_tomcat\_iiq

setspn -a HTTP/TESTLABDC.seri.com svc\_tomcat\_iiq

setspn -a HTTP/TESTLABDC.seri.com:8080 svc\_tomcat\_iiq

Kerberos Config File generation:

[libdefaults]

default\_realm = SERI.SAILPOINTDEMO.COM

default\_keytab\_name = FILE:C:/Prog/Tomcat/conf/tomcat.keytab

default\_tkt\_enctypes = aes256-cts-hmac-sha1-96,aes128-cts-hmac-sha1-96,aes128-cts,rc4-hmac

default\_tgs\_enctypes = aes256-cts-hmac-sha1-96,aes128-cts-hmac-sha1-96,aes128-cts,rc4-hmac

permitted\_enctypes = aes256-cts-hmac-sha1-96,aes128-cts-hmac-sha1-96,aes128-cts,rc4-hmac

[realms]

SERI.SAILPOINTDEMO.COM = {

kdc = 192.168.84.194

default\_domain = SERI.SAILPOINTDEMO.COM

}

[domain\_realm]

seri.sailpointdemo.com = SERI.SAILPOINTDEMO.COM

.SERI.SAILPOINTDEMO.COM = SERI.SAILPOINTDEMO.COM

SPNEGO Config File:

spnego-client {

com.sun.security.auth.module.Krb5LoginModule required;

};

spnego-server {

com.sun.security.auth.module.Krb5LoginModule required

storeKey=true

principal="HTTP/TESTLABDC.seri.com@seri.sailpointdemo.com"

isInitiator=true

useKeyTab=true

keyTab="C:\Prog\Tomcat\conf\tomcat.keytab";

};