CAS with Spnego & Kerberos (Windows)

# Set up AD on CAS server:

* Install Active Directory on Windows Server
* Create Domain for server. Ex: example.com

# Install Java 8 and Tomcat 8 (CAS):

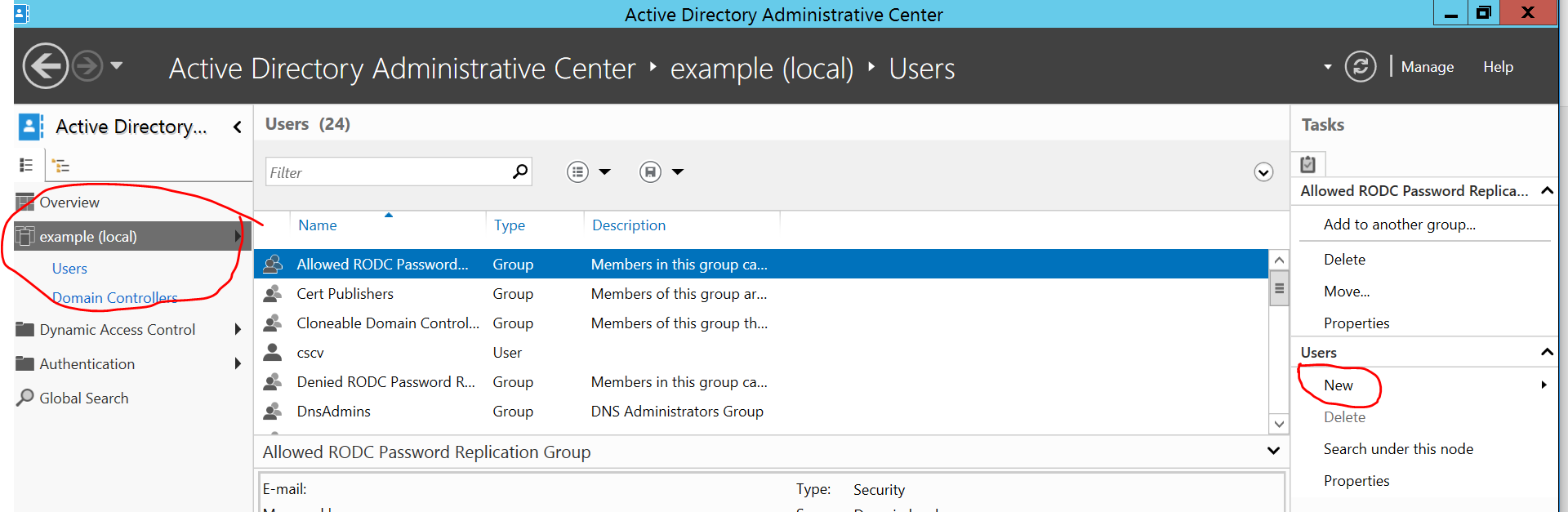
* Install Java 8 and set environment JAVA\_HOME = {PATH}\jdk8
* Setup Tomcat 8 with cas server.

# Install Kerberos for Windows:

* Go to site: <http://web.mit.edu/kerberos/dist/index.html>
* Download MIT Kerberos for windows: 64-bit MSI Installer [kfw-4.1-amd64.msi](http://web.mit.edu/kerberos/dist/kfw/4.1/kfw-4.1-amd64.msi)
* Install Kerberos.

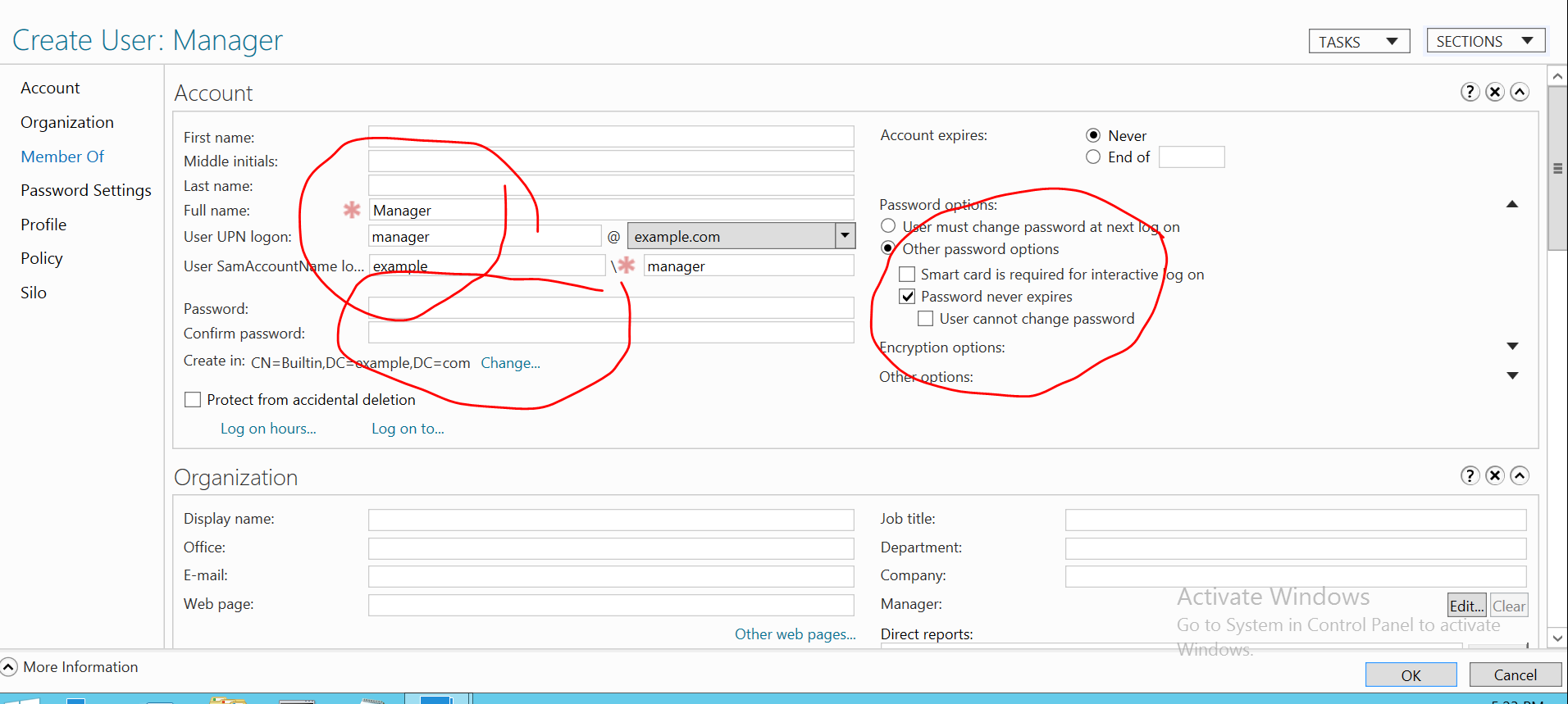
# Create Principle Account and generate key tap:

* First, we create account in AD below:
* Open Active Directory Administrative Center, go to container Users:



* Create a new user:

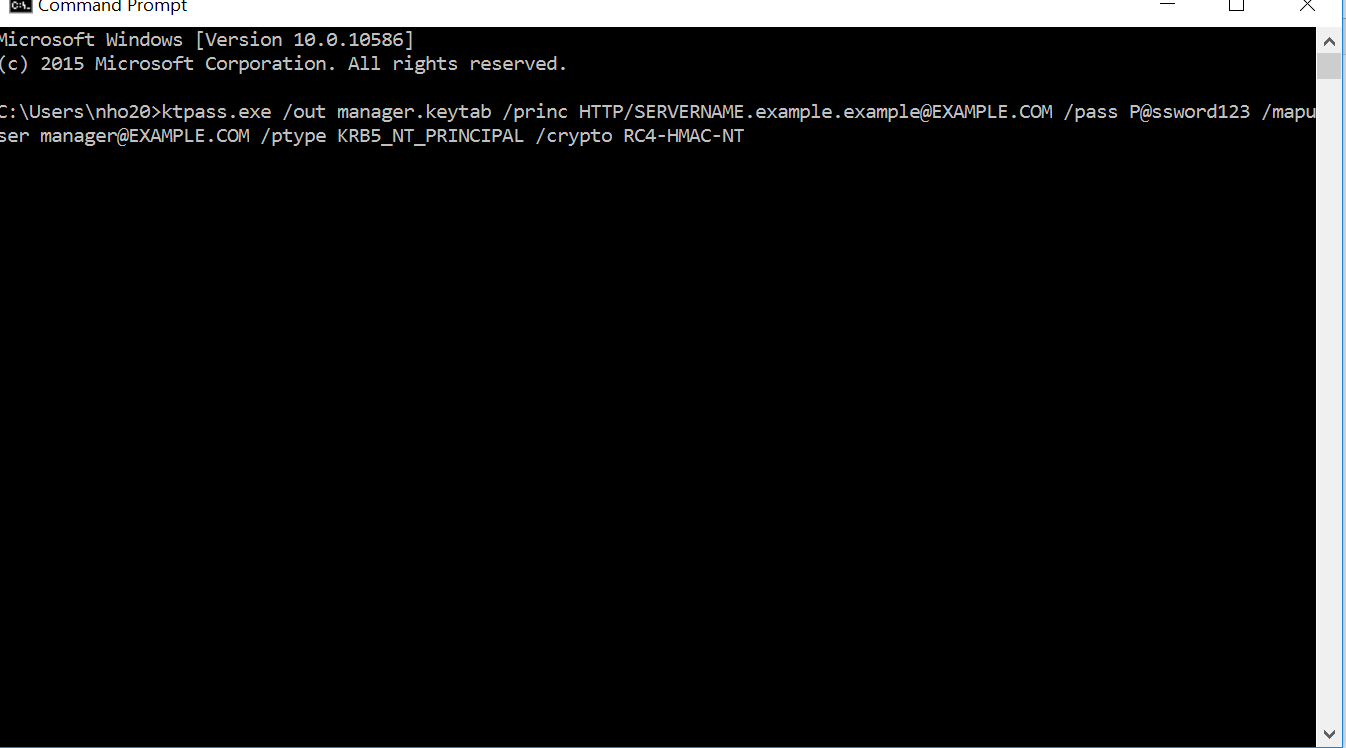
Example: create user “manager”



Click OK.

* Then Go to cmd (Administator) create file .keytap:

Use command line: ktpass.exe /out manager.keytab /princ HTTP/SERVERNAME.example.com@EXAMPLE.COM /pass P@ssword123 /mapuser manager@EXAMPLE.COM /ptype KRB5\_NT\_PRINCIPAL /crypto RC4-HMAC-NT



When create done.

* Then verify that your are able to read the keytab file, go to JAVA\_HOME/bin use command line:
* klist -k
* Then verify that your are able to read the keytab file:
* kinit manager@EXAMPLE.COM
* klist

# Config KBR5.INI with CAS server:

* Create file kbr5.ini below:

[libdefaults]

ticket\_lifetime = 24000

default\_realm = EXAMPLE.COM

default\_keytab\_name = C:\kerberos\manager.keytab

dns\_lookup\_realm = false

dns\_lookup\_kdc = false

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

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

forwardable=true

[realms]

EXAMPLE.COM = {

kdc = w2k12-svr-tmp.example.com:88

}

[domain\_realm]

.EXAMPLE.COM = EXAMPLE.COM

EXAMPLE.COM = EXAMPLE.COM

* Create file login.conf below:

jcifs.spnego.initiate {

com.sun.security.auth.module.Krb5LoginModule required storeKey=true useKeyTab=true keyTab="C:\PATH\manager.keytab";

};

jcifs.spnego.accept {

com.sun.security.auth.module.Krb5LoginModule required storeKey=true useKeyTab=true keyTab="C:\PATH \manager.keytab";

};

* Go to Tomcat/bin create setenv.bat:

set JAVA\_OPTS= "-Djava.security.krb5.conf=C:\PATH\krb5.ini -Djava.security.auth.login.config=C:\PATH\ login.conf"

* Go to Tomcat\webapps\cas\WEB-INF modify:
* Add two bean definitions in cas-servlet.xml:
* **<bean** id="negociateSpnego" class="org.jasig.cas.support.spnego.web.flow.SpnegoNegociateCredentialsAction" **/>**
* **<bean** id="spnego" class="org.jasig.cas.support.spnego.web.flow.SpnegoCredentialsAction"
* p:centralAuthenticationService-ref="centralAuthenticationService" **/>**
* Define two new action states in login-webflow.xml before the viewLoginForm state:
* **<action-state** id="startAuthenticate"**>**
* **<evaluate** expression="negociateSpnego" **/>**
* **<transition** on="success" to="spnego" **/>**
* **</action-state>**
* **<action-state** id="spnego"**>**
* **<evaluate** expression="spnego" **/>**
* **<transition** on="success" to="sendTicketGrantingTicket" **/>**
* **<transition** on="error" to="viewLoginForm" **/>**
* **</action-state>**

Note: Additionally, find action generateLoginTicket - replace viewLoginForm with startAuthenticate.

* Update deployerConfigContext.xml according to the following template:
* **<bean** id="jcifsConfig"
* class="org.jasig.cas.support.spnego.authentication.handler.support.JCIFSConfig"
* p:jcifsServicePrincipal=[HTTP/SERVERNAME.example.com@EXAMPLE.COM](mailto:HTTP/SERVERNAME.example.com@EXAMPLE.COM)
* p:jcifsServicePassword="P@ssword123"
* p:jcifsDomain="example.com"
* p:jcifsDomainController="W2K12-SVR-TMP.example.com"
* p:kerberosDebug="true"
* p:kerberosConf="C:\PATH\kbr5.ini"
* p:kerberosDebug="false"
* p:kerberosRealm="EXAMPLE.COM"
* p:kerberosKdc="IP\_SERVER\_KERBEROS"
* p:loginConf="C:\PATH\login.conf" **/>**
* **<bean** id="spnegoAuthentication" class="jcifs.spnego.Authentication" **/>**
* **<bean** id="spnegoHandler"
* class="org.jasig.cas.support.spnego.authentication.handler.support.JCIFSSpnegoAuthenticationHandler"
* p:authentication-ref="spnegoAuthentication"
* p:principalWithDomainName="false"
* p:NTLMallowed="true" **/>**
* **<bean** id="spnegoPrincipalResolver"
* class="org.jasig.cas.support.spnego.authentication.principal.SpnegoPrincipalResolver" **/>**
* **<bean** id="authenticationManager"
* class="org.jasig.cas.authentication.PolicyBasedAuthenticationManager"**>**
* **<constructor-arg>**
* **<map>**
* **<entry** key-ref="spnegoHandler" value-ref="spnegoPrincipalResolver"**/>**
* <entry key-ref="ldapAuthenticationHandler" value-ref="usernamePassword CredentialsResolver" />
* <entry key-ref="ldapAuthenticationHandler" value-ref="httpBasedCredentialsResolver" />
* **</map>**
* **</constructor-arg>**
* **<property** name="authenticationMetaDataPopulators"**>**
* **<list>**
* **<bean** class="org.jasig.cas.authentication.SuccessfulHandlerMetaDataPopulator" **/>**
* **</list>**
* **</property>**
* **</bean>**

# Start TOMCAT CAS server and config Browser:

## Start Tomcat.

## Set up Browser of Other Computers on same as Domain.

#### Internet Explorer (min 5.01)

1. In Internet Explorer, click Internet Options on the Tools menu.
2. Click on the Advanced tab, click to select the Enable Integrated Windows Authentication (requires restart) check box in the Security section, and then click OK.
3. Click on the Security tab, click to select Local Intranet then click on Sites, then click on Advanced.
4. Enter <https://servername.example.com>  and validate by clicking on \_Add and OK.
5. Restart Internet Explorer.

#### Firefox (min 0.9)

#### In Firefox, enter about:config as url and click on Go.

#### On the line network.negotiate-auth.trusted-uris, right click on Modify and enter \_https://servername.example.com\_

WE CAN USE CAS WITH URL:

https://servername.example.com/cas/login.