IBM Software Group

WebSphere Application Server V7 - SPNEGO Basics

Josh Kessler (joshkess@us.ibm.com)
WebSphere Application Server L2 Support
25 January 2012

WebSphere® Support Technical Exchange

Agenda

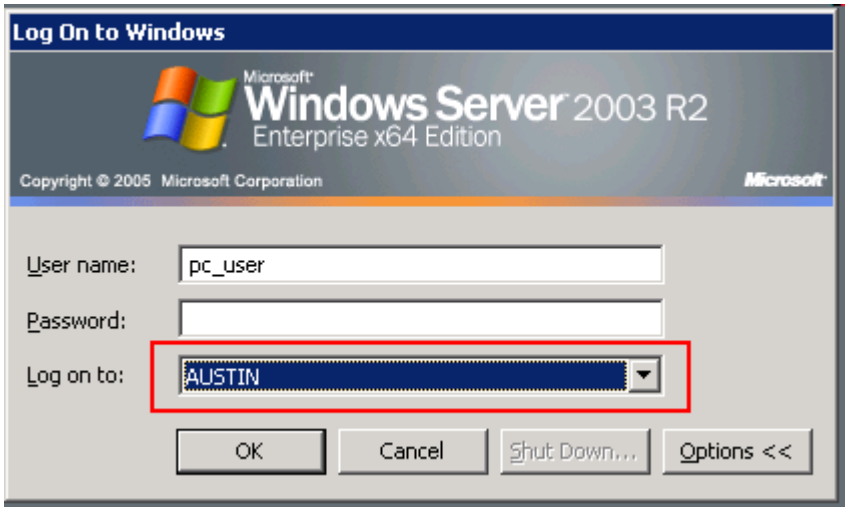
- This presentation will discuss SPNEGO Web authentication WebSphere v7.0.
- To provide a high level overview and basic configuration of how SPNEGO is used for SSO in a WebSphere environment.
- Remember, the goal of SPNEGO is to ultimately have clients use LTPA tokens for Single Sign On.

SPNEGO Overview

- Microsoft Windows® provides for desktop Single Sign On over HTTP using SPNEGO
  - PC User authenticates once to desktop PC via AD domain login and then can securely access other systems transparently (SSO)
- The desire is for WebSphere Application Server (WAS) to support SSO from Windows desktops transparently.
- Kerberos credentials are carried via SPNEGO (Negotiate) HTTP header to WebSphere, where they are validated and then inserted into an LTPA token. This is how SSO is possible using SPNEGO with WebSphere.
- This presentation is about that solution.

Basic Kerberos - Obtaining a TGT

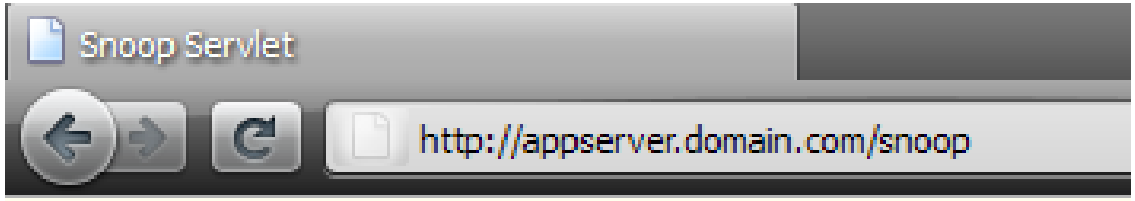
- Client obtains a ticket-granting-ticket (TGT) by making a request to the KDC authentication service (AS).
- This happens automatically when the PC user logs into their AD domain.



This is the entry point of *most* SPNEGO authentication requests.

Basic Kerberos - Obtaining a Service Ticket

- Using this TGT, the client later makes a request to the KDC ticket-granting service (Active Directory) to obtain a service ticket to a desired server (WebSphere), without the client needing to provide its password again.
- This occurs when the client accesses an SPNEGO protected URL / resource :



ACCESS URL Hostname = appserver.domain.com

- It is important to know what exact URL the client is accessing the appserver or webserver with. We need to know which hostname they are using and if that hostname is an alias in DNS or not due to hostname canonicalization.

SPNEGO Web Authentication v7 Enhancements

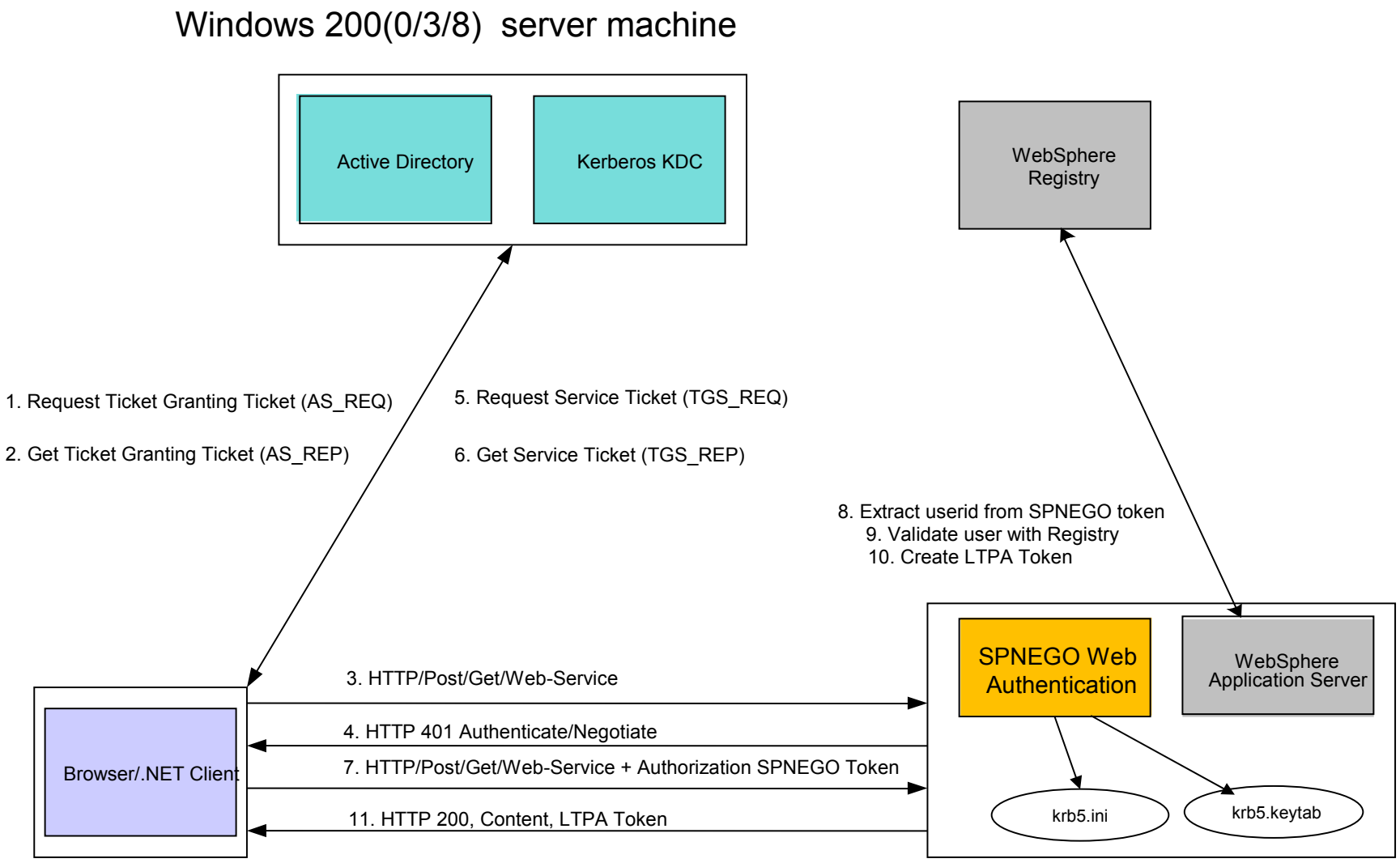
- WCCM model SPNEGO and Filter classes
- Simplify the SPNEGO configuration on WebSphere Application Server machine
- Configurable options
  - Fallback from SPNEGO Web authentication to an application login method
  - Dynamically update the SPNEGO run time when SPNEGO filter changes and Kerberos configuration or keytab file name changes occur without stop/restart the server.
- SPNEGO TAI is deprecated in v7.
- SPNEGO web authentication command tasks

Single sign-on for HTTP requests using SPNEGO Web Authentication

- Support all User Registries and platforms that are supported by WebSphere Application Server.
- *Support one or more Microsoft (MS) Active Directory (AD) in the same or different forests.

  http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.nd.doc/info/ae/ae/csec_kerb_auth_explain.html
- Kerberos configuration and keytab file path now support WebSphere variables. Also if you have a mixed platform environment, you can use variable ${CONF_OR_INI} for a Kerberos configuration file, the security configure code will expand it to “ini” for Windows or “conf” for none Windows platforms
  - ${WAS_INSTALL_ROOT}\etc\krb5\krb5.${CONF_OR_INI}
- Support WebSphere Multi security domains
- Officially supported web browser clients:
  - Microsoft Internet Explorer V6.0 SP1 or newer
  - Mozilla V1.7.8 and Firefox V1.5 or newer

Challenge-responses process between web browser and SPNEGO Web Auth



Domain controller machine – Mapping an SPN to an AD user

- Create a user name "**spnegoweb**" in AD and ensure not to check the option "**Use DES encryption types for this account"** in user properties. This option should **ONLY** be used if you have a mixed Windows version environment. Otherwise it should use default RC4-HMAC encryption. (You don't have to select anything for this)

- DES is old and uses 56-bit encryption and is less secure than RC4-HMAC (128-bit).

- Use Microsoft "setspn" tool to map the SPN, **HTTP**/< **fully qualified host name** >, to the user account.
- The <fully qualified hostname> is the *SAME* hostname used by the client when they access the application /URL.

```
C:\>setspn -a HTTP/appserver.domain.com spnegoweb
Registering ServicePrincipalNames for CN=appserver,DC=domain,DC=com
        HTTP/appserver.domain.com
Updated object
```

- Common problems for setspn command:
  - The host name must be a fully qualified host name.
  - Make sure the user name spnegoweb is unique in Active Directory users and computers.
  - Do not map the same SPN to more than one AD user.

Domain controller machine – Creating a Kerberos keytab file for the SPN

- Use MS ktpass tool to create a keytab file krb5.keytab for the SPN and map the SPN account. (Instead of using setspn to map the user, you an specify mapuser here)

```
C:\>ktpass -out c:\temp\krb5.keytab
        -princ HTTP/appserver.domain.com@DOMAIN.COM  -mapUser spnegoweb -mapOp set
        -pass test123 –ptype KRB5_NT_PRINCIPAL

Successfully mapped HTTP/appserver.domain.com to  spnegoweb.
Key created.
Output keytab to c:\temp\krb5.keytab:
Keytab version: 0x502
keysize 79 HTTP/appserver.domain.com@DOMAIN.COM ptype 1 (KRB5_NT_PRINCIPAL) vno
        1 etype 0x3 (RC4-HMAC) keylength 8 (0x9898f76e3bd05438)
```

- Copy the krb5.keytab file to the WebSphere Application Server machine at the location specified in the Kerberos configuration file (krb5.ini or krb5.conf).
- Note:
  - Windows 2003 server ktpass support both DES and RC4-HMAC
  - Always use the latest version of the ktpass for the right Windows version.
  - The realm name is all uppercase for the MS AD domain name

SPNEGO filterCriteria and operation

Operand	Description	Example
==	Exact match	*host==appserver.domain.com*
%=	Partially match (includes)	*user-agent%=IE 6*
^=	Partially match (includes) one of many	*request-url^=snoop|webApp1*
!=	Not included	request-url!=noSPNEGO
>	Greater than	remote-address>9.3.97.87
<	Less than	remote-address<9.3.97.99

SPNEGO Web Authentication commands tasks

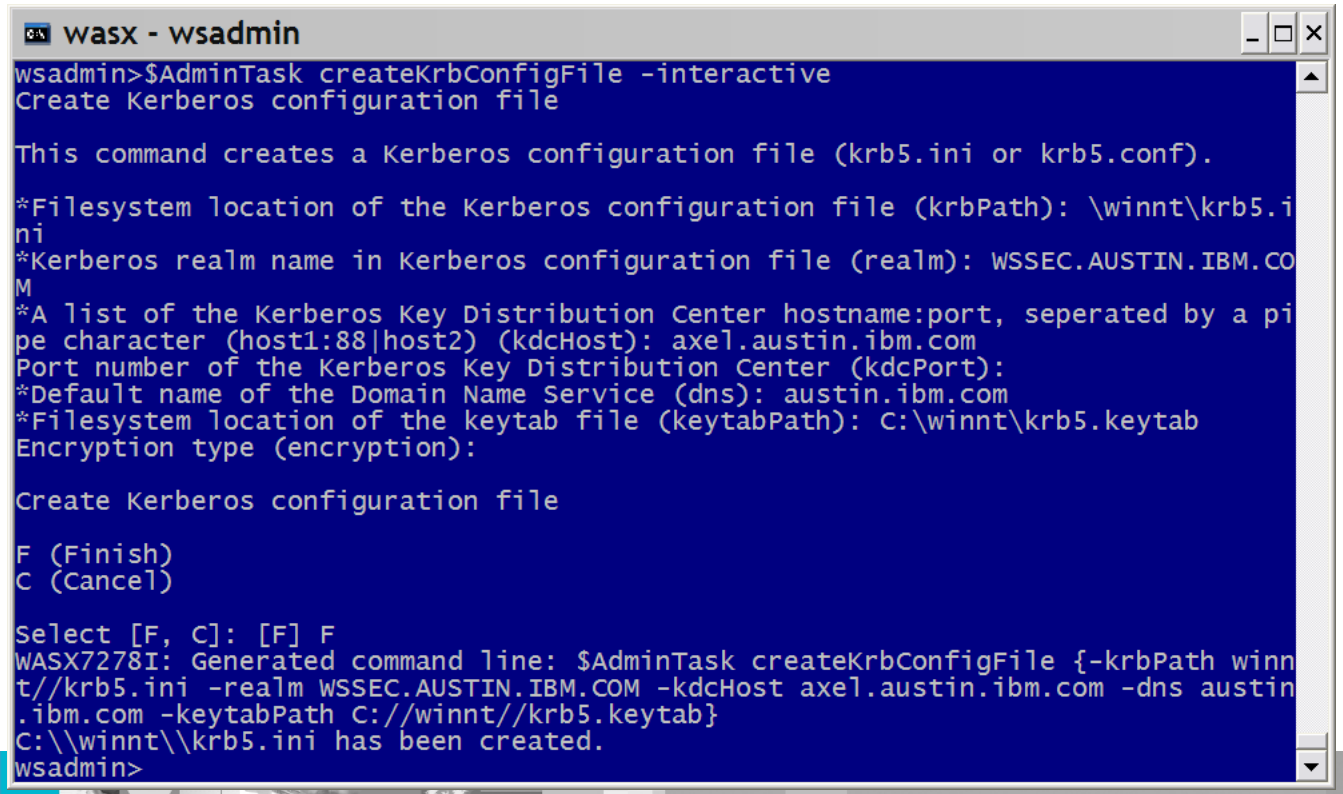
- SPNEGO web authentication command tasks:
  - createKrbConfigFile - This command creates a Kerberos configuration file (krb5.ini or krb5.conf).
  - configureSpnego - This command configure SPNEGO as a Web Authenticator in the security configuration.
  - unconfigureSpnego - This command unconfigures the Web Authenticator in the security configuration.
  - showSpnego - This command displays the SPNEGO configuration in the security configuration.
  - ValidateKrbConfig - Validate the Kerberos configuration data either in the global security configuration file security.xml or specified as an input parameters.

SPNEGO Web Authentication commands (cont.)

- SPNEGO Filter command tasks
  - addSpnegoFilter - This command adds SPNEGO filter in the security configuration.
  - deleteSpnegoFilter - This command removes SPNEGO Filter from the security configuration. If a host name is not specified, all the SPNEGO Filters are removed.
  - modifySpnegoFilter - This command modifies SPNEGO Filter attributes in the security configuration.
  - showSpnegoFilter - This command displays the SPNEGO Filter in the security configuration. If a host name is not specified, all the SPNEGO Filters are displayed.

On WAS machine - Configure a Kerberos client (krb5.ini or krb5.conf)

- Configure a Kerberos client by creating the Kerberos configuration file (krb5.ini or krb5.conf) on a WAS machine.
- Use the admin command task createKrbConfigFile to create krb5.ini file



Location of the Kerberos configuration file on the WAS machine

- The following is the order of precedence for JGSS and KRB5 looking for a Kerberos configuration file.
  - System property: -Djava.security.krb5.conf=/etc/krb5.conf
  - System property: -Djava.home=c:/WebSphere/AppServer/java/jre
    - Location: ${java.home}/lib/security/krb5.conf
  - If Windows platform, c:\winnt\krb5.ini
  - If Linux® platform, /etc/krb5.conf
  - If other Unix® platform, /etc/krb5/krb5.conf
  - If zSeries, /etc/krb5/krb5.conf
  - If iSeries, /etc/krb5/krb5.conf ??
- Add krb5.ini or krb5.conf to each WebSphere Application Server host

On WAS machine - Configure a Kerberos client (Cont)

- A sample output of the Kerberos configuration file (krb5.ini or krb5.conf).

```
[libdefaults]
        default_realm = DOMAIN.COM
        default_keytab_name = FILE:c:\winnt\krb5.keytab
        default_tkt_enctypes = des-cbc-md5 rc4-hmac
        default_tgs_enctypes = des-cbc-md5 rc4-hmac
        kdc_default_options = 0x54800000
[realms]
        DOMAIN.COM = {
                kdc =  AD_SERVER.domain.com:88
                default_domain = domain.com
        }
[domain_realm]
        .domain.com = DOMAIN.COM
```

On the WAS machine - Kerberos keytab file (krb5.keytab)

- Manage the Kerberos keytab file with ktab or ktpass
  - Use the Java™ ktab command to merge keytab files
  - Use the Java ktab command to add/delete a key from the keytab file

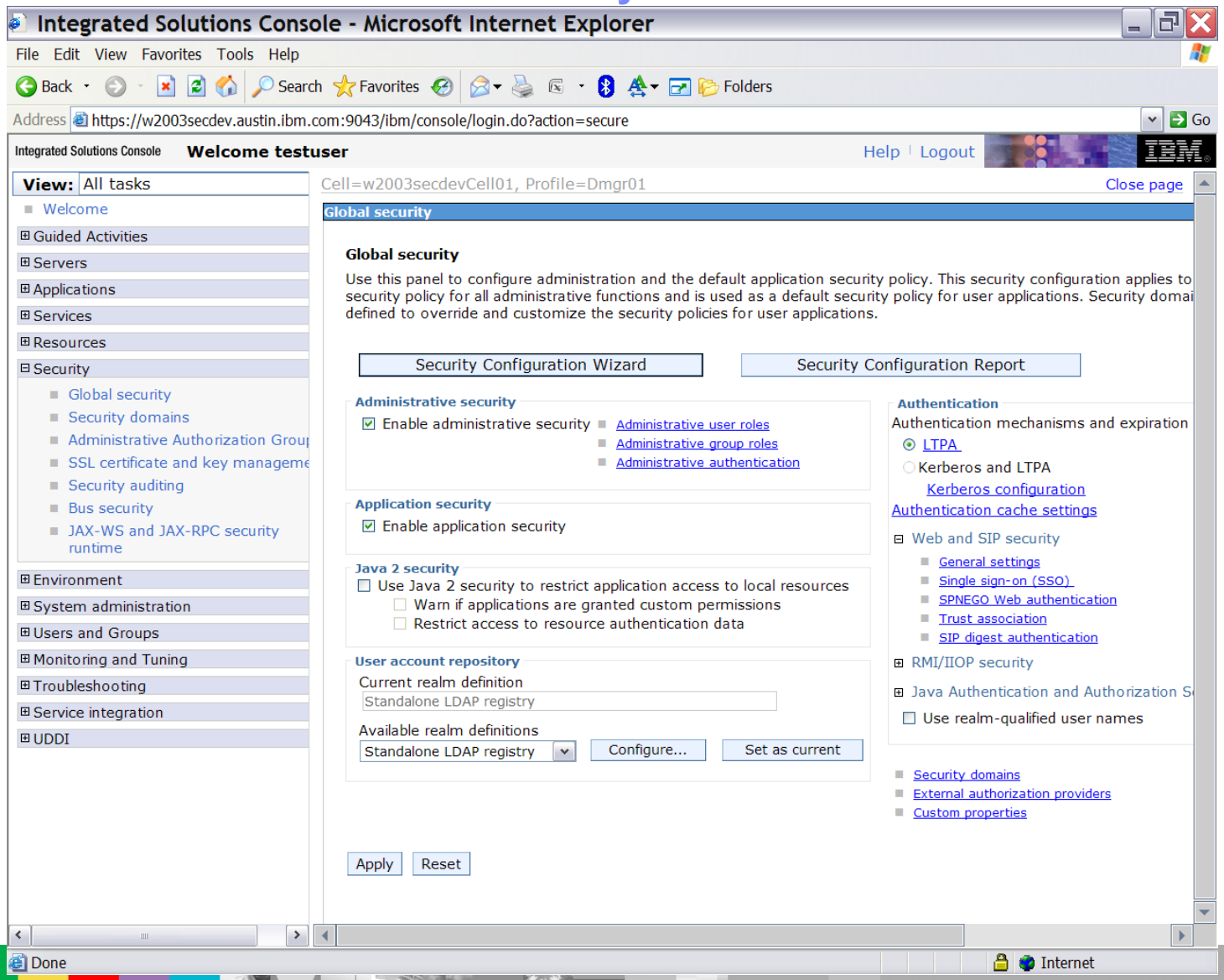
- Copy the krb5.keytab file that created on the AD machine to WAS machine

- Use Java klist –k command to view the krb5.keytab file content

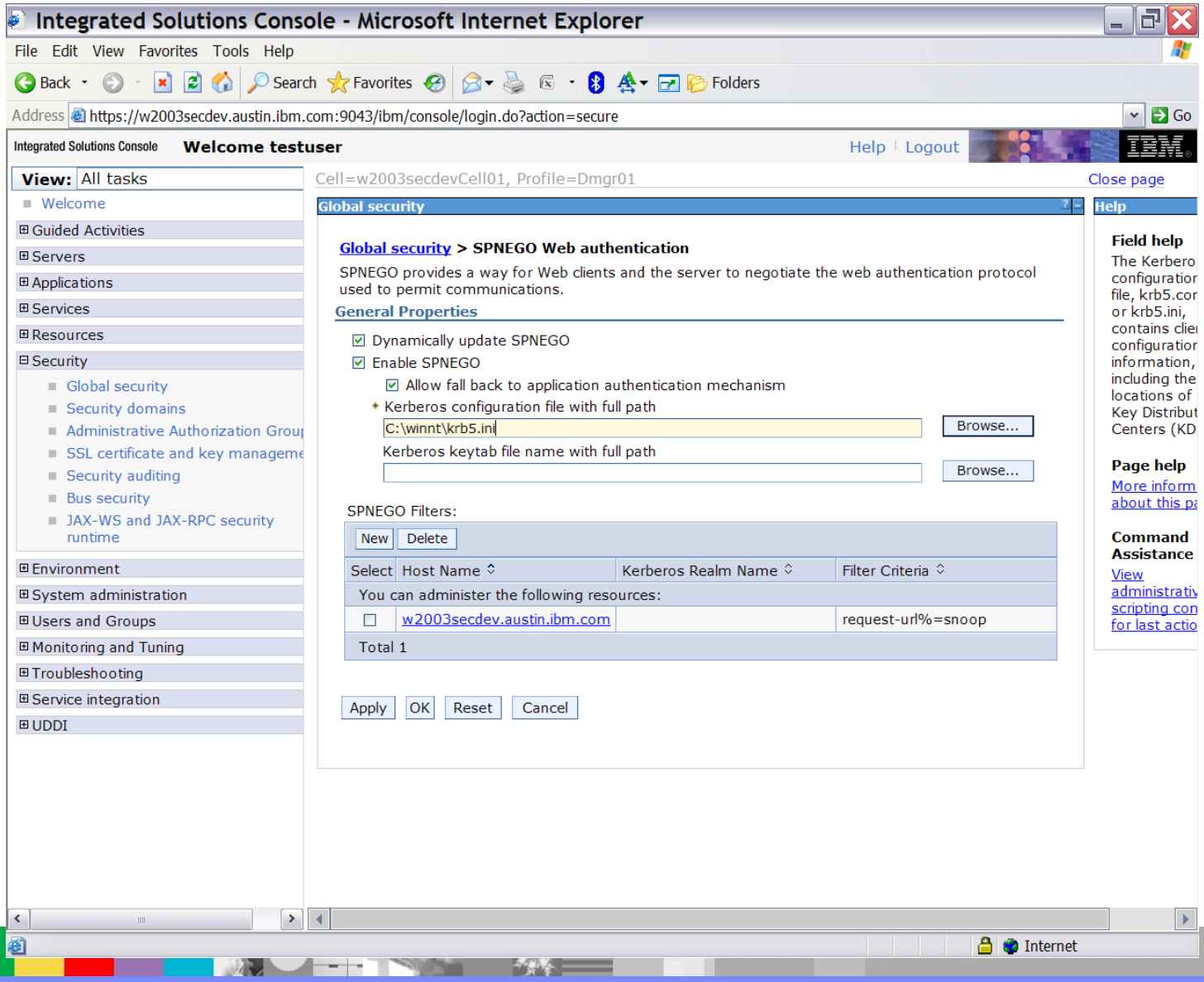
C:\IBM\WebSphere\AppServer\java\jre\bin> java com.ibm.security.krb5.internal.tools.Klist -e -k C:\WINNT\krb5.keytab

- Note:
  - At this point you can use the admin command task validateKrbConfig to validate the krb5.conf and krb5.keytab files.
  - We do not recommend customer to use the distributed Kerberos ktutil command to merge keytab files

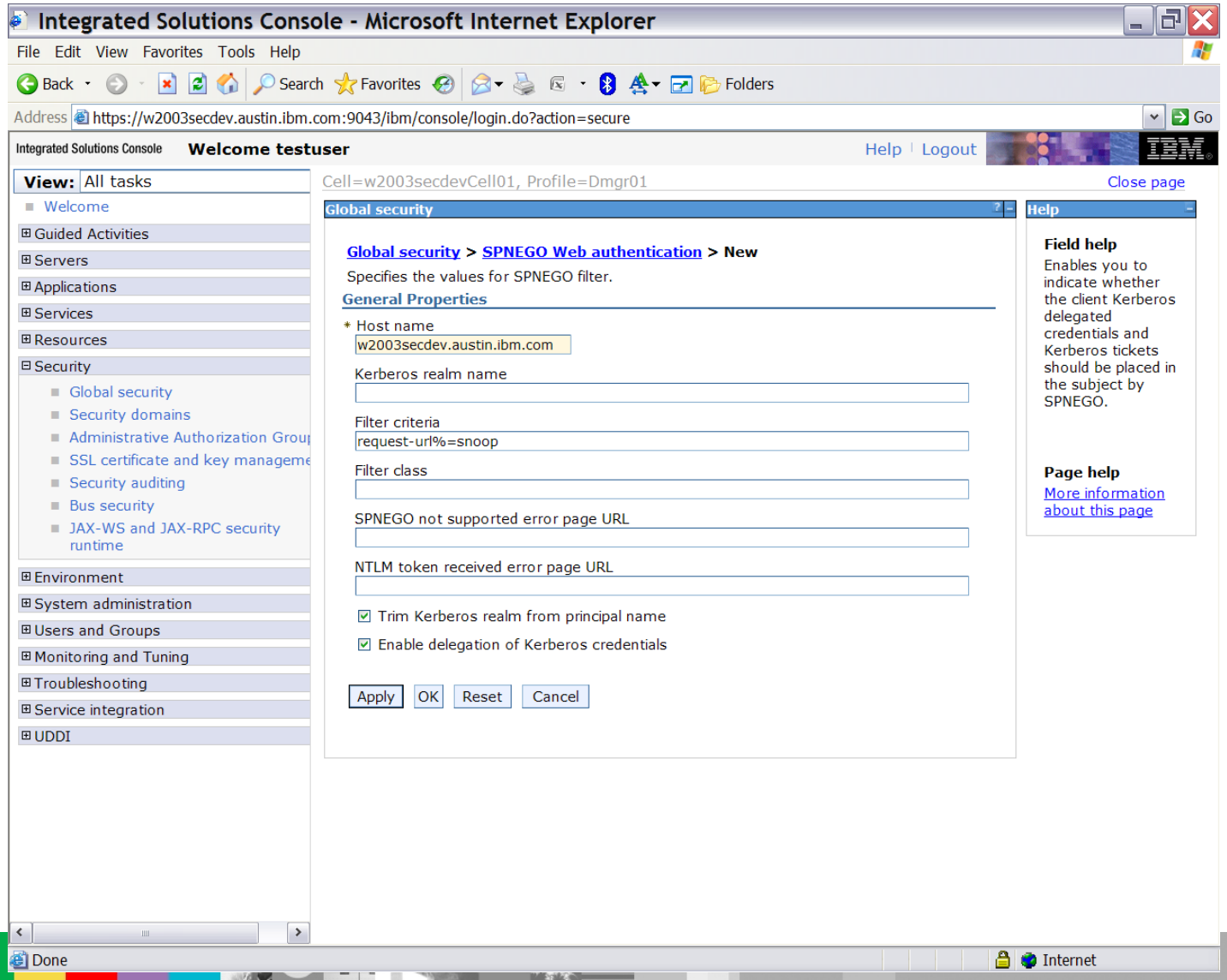
Admin Console – Global security



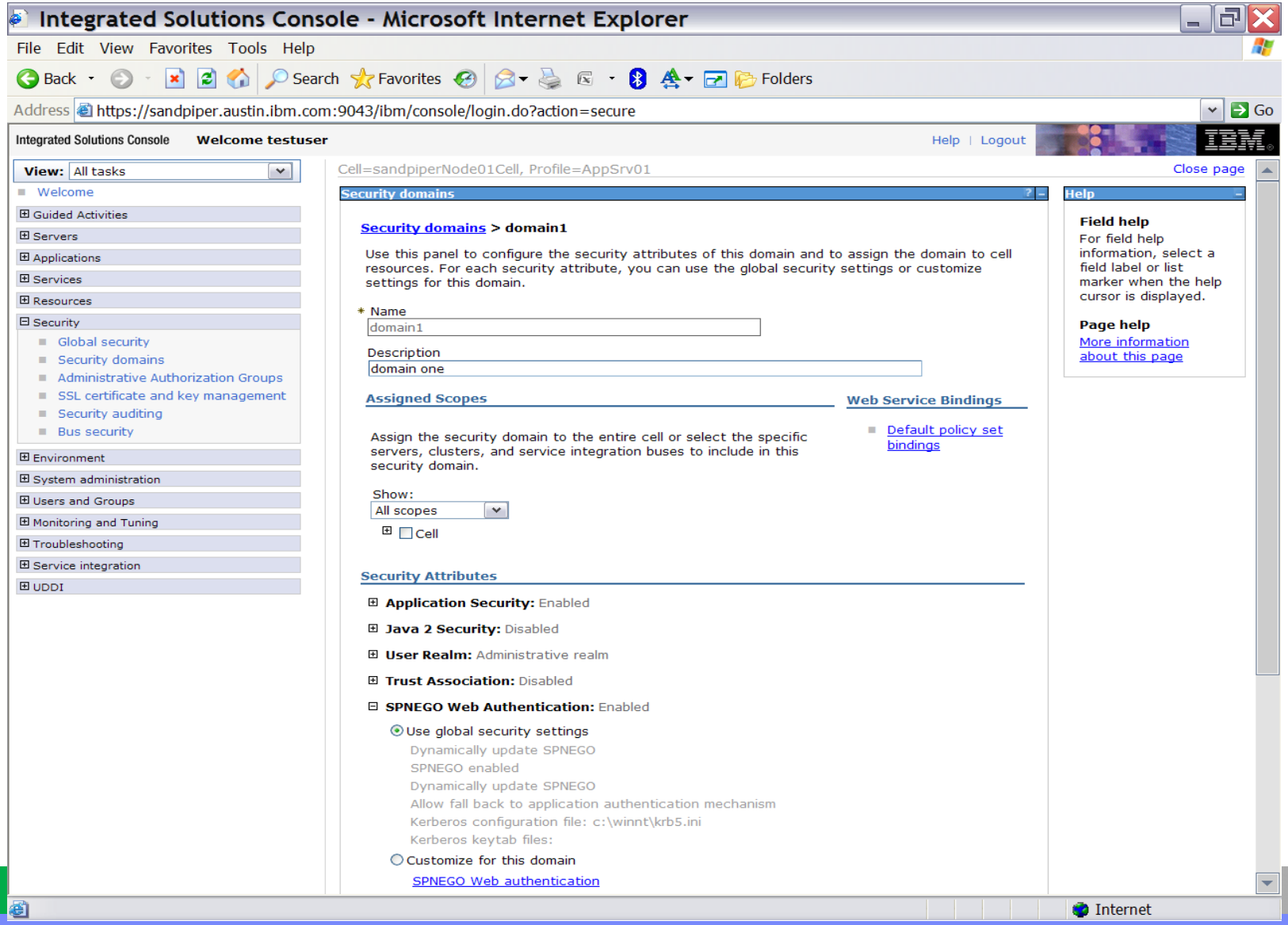
Admin Console – Enable SPNEGO Web Authentication



Admin Console – Add a new SPNEGO Filter



Admin Console – Security domains and SPNEGO Web authentication



On a Client machine - Configure MS IE browser to use SPNEGO authentication

Make sure the client machine is a member of a domain for which SSO has been defined.

In the following example, the machine w2003secdev.austin.ibm.com is a member of the domain controller **WSSEC.AUSTIN.IBM.COM**. Log on to the Windows Desktop with a user name from the domain.

1. Open the browser, go to menu bar **Tools -> Internet Options**
2. Select the **Security** tab.
3. Select **Local intranet** icon.
4. Click **Sites**.
5. Click **Advanced**.
6. Add the URL for the host name that SSO should be enabled for, to the list. For example: **http://w2003secdev.austin.ibm.com**
7. Click **OK.**
8. Click **OK.**
9. Select the **Advanced** tab.
10. Scroll down to security section and ensure that **Enable integrated Windows Authentication(requires restart)** is checked.
11. Close the browser.
12. Start the browser.

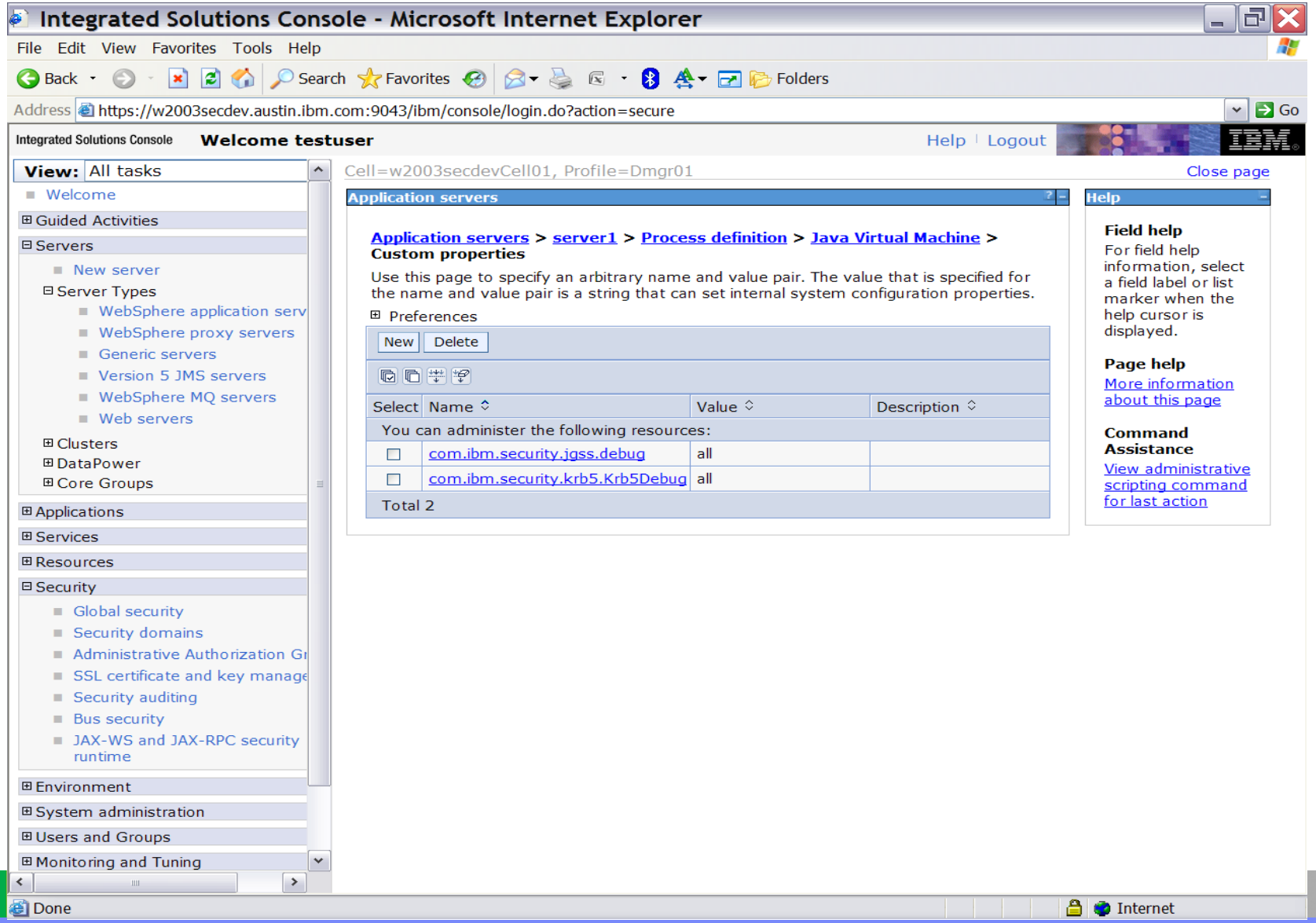
On a Client machine - Configure Mozilla or FireFox browser to use SPNEGO authentication

1. Open the browser.
2. At the address field, type **about:config**
3. In the filter, type **network.n*uris**

1. Double click on network.negotiate-auth.trusted-uris. This preference lists the sites that are permitted to engage in SPNEGO Authentication with the browser.
2. Enter a comma delimited list of trusted domains or URLs. For example: w2003secdev.austin.ibm.com

   Do NOT use wildcards (*) in the hostnames.
3. Double click the network.negotiate-auth.delegation-uris and set it to the exact same hostnames.
4. Close the browser.
5. Start the browser.

Enabled JGSS and KRB5 debugging per server using Admin Console



Enabled SPNEGO Web Authentication debugging

- In the Administrative Console, navigate to **Servers > Application Servers > server_name.** Under Server Infrastructure, expand **Java and process management.** Select **Process Definition > Java Virtual Machine > Custom Properties**. Create two new Java ™ Virtual Machine (JVM) properties:

  Name: com.ibm.security.jgss.debug
  Value: all

  Name: com.ibm.security.krb5.Krb5Debug
  Value: all

- Enable tracing with :

  com.ibm.ws.security.*=all

SPNEGO Web Authentication debugging

- Validate the Kerberos configuration file (krb5.in/krb5.conf)
  - java/jre/bin/kinit command
- Validate the Kerberos Keytab
  - java/jre/bin/kinit –k HTTP/appserver.austin.ibm.com
- Validate the SPN
  - setspn –l <AD user>
- Make sure the encryption type are the same for the following
  - krb5.ini/krb5.conf
  - krb5.keytab
  - MS Active Directory Users and Computers -> Users-> <user> ->properties->account options
    - Confirm if “Use DES encryption” checkbox is enabled

SPNEGO Web Authentication troubleshooting tips

- Find out if SPN is mapped to multiple usernames :
  - On Active Directory Server, run following command:

    ldifde -f output.txt –r "(servicePrincipalName=HTTP/hostname.domain.com)“
- We do not officially support any mobile browsers
- Test access with Firefox when possible as there are known defects with Internet Explorer
- Prevent setspn from modifying UPN (Login username):
  - setspn -setupn
- Java command to view keytab contents :
  - E:\IBM\WebSphere\AppServer\java\jre\bin>java com.ibm.security.krb5.internal.tools.Klist -e -k E:\IBM\WebSphere\wp_profile\krb\krb_qa.keytab

SPNEGO Web Authentication Documents

Single sign-on for HTTP requests using SPNEGO Web authentication

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/csec_SPNEGO_explain.html

Administering SPNEGO within WebSphere Application Server: Tips on using Kerberos service principal names

http://www.ibm.com/developerworks/websphere/library/techarticles/0809_lansche/0809_lansche.html

SPNEGO troubleshooting tips

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.base.doc/info/aes/ae/rsec_SPNEGO_troubles.html?

This appears to be periodically updated by Martin Lansche with known errors and how to resolve them.

Related Information

RFC 2478 - The Simple and Protected GSS-API Negotiation Mechanism

http://www.ietf.org/rfc/rfc2478.txt

IBM® Techdocs White Paper: WebSphere with a side of SPNEGO

http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101065

First Time Call Questions

- 1) WebSphere version :
- Active Directory version :
- 2) What is the AD_username used to map to SPN's ?
- 3) What is the SPN used to map the AD_username above: (HTTP/hostname.domain.com) ?
- 4) Please provide commands issued to create the keytab and SPN mappings on the AD server. If possible, also provide the command output.
- 5) What is the full web request URL accessed by the client browser ?
- 6) Is this an alias(CNAME Record) or real_hostname(A Record) in DNS ?
- 7) List all AD_username SPN mappings on AD server:
- C:\setspn -l AD_username:
- 8) Screenshot of SPN filter entries in WebSphere adminconsole.

- 9) Are additional SPNEGO access filters being used ? If yes, what are they ?

- 10) Find all SPN mapping occurrences mapped to AD usernames:
- On the Active Directory Server, run following command:
- C:\ldifde -f output.txt -r "(servicePrincipalName=HTTP/hostname.domain.com)"

- 11) Are there loadbalancers, firewalls, proxies, or webservers in the mix, or any devices/appliances
- between the client browser and WebSphere ? If you can please provide the login flow with relovent
- topology involved.
- 12) Screenshots of client browser SPNEGO settings.

- 13) Please capture a trace and collector data using the mustgather below: (Skip step1)
- IBM MustGather: Problems with Spnego - United States
- http://www-01.ibm.com/support/docview.wss?uid=swg21255030

- 14) Also provide your krb5 config and keytab files.

SPNEGO Trace Analysis Q & A

First, check startup log to see if SPNEGO initialized successfully.

Now search for the first occurrence of “Checking host match for” to begin review of this spnego login request.

[3/24/10 13:31:26:906 CDT] 0000003b TrustAssociat 2 com.ibm.ws.security.spnego.TrustAssociationInterceptorImpl isTargetInterceptor **Checking host match** for ruby59a.austin.ibm.com

…

[3/24/10 13:31:26:906 CDT] 0000003b ServerCredent > com.ibm.ws.security.spnego.ServerCredentialsFactory hasServerCredentialsFor ENTRY ruby59a.austin.ibm.com

[3/24/10 13:31:26:906 CDT] 0000003b ServerCredent < com.ibm.ws.security.spnego.ServerCredentialsFactory hasServerCredentialsFor RETURN **true**

This means that SPNEGO *will* intercept this request for ruby59a.austin.ibm.com. If you see false here, then SPNEGO will not intercept you need to check that the browser configuration matches the SPNEGO filter entries we have set in WebSphere.

Trace example continued

Assuming **no** authorization header is already present, WebSphere will then send a 401 challenge to the client who will send back a Negotiate header, then we decrypt this to obtain the user which we validate using our Global Security user registry. Once validated, we send the LTPA token back to the client.

[3/24/10 13:31:26:906 CDT] 0000003b SpnegoHandler 2 com.ibm.ws.security.spnego.SpnegoHandler handleRequest No Authorization header found, sending 401 challenge to the client

This is **normal** to see this 401 challenge.

At this point I will review a scenario capturing successful SPNEGO login in a trace.log file.

I will go over additional useful SPNEGO trace points there.

Additional WebSphere Product Resources

- Learn about upcoming WebSphere Support Technical Exchange webcasts, and access previously recorded presentations at:
  http://www.ibm.com/software/websphere/support/supp_tech.html
- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at:
  http://www.ibm.com/developerworks/websphere/community/
- Join the Global WebSphere Community:
  http://www.websphereusergroup.org
- Access key product show-me demos and tutorials by visiting IBM Education Assistant:
  http://www.ibm.com/software/info/education/assistant
- View a webcast replay with step-by-step instructions for using the Service Request (SR) tool for submitting problems electronically:
  http://www.ibm.com/software/websphere/support/d2w.html
- Sign up to receive weekly technical My Notifications emails:
  http://www.ibm.com/software/support/einfo.html

Connect with us!

1. **Get notified on upcoming webcasts**
   Send an e-mail to wsehelp@us.ibm.com with subject line “wste subscribe” to get a list of mailing lists and to subscribe
2. **Tell us what you want to learn**
   Send us suggestions for future topics or improvements about our webcasts to wsehelp@us.ibm.com
3. **Be connected!**
   Connect with us on Facebook
   Connect with us on Twitter

Questions and Answers