

Inštalácia tomcatspnego

Postup inštalácie modulu tomcatspnego pre podporu TCL autentifikácie do webservera Apache Tomcat

Tento dokument popisuje inštaláciu a konfiguráciu autentifikovaného modulu tomcatspnego do webservera Apache Tomcat na platforme Windows. Modul umožňuje, aby tenký klient využíval [TCL autentifikáciu](#), t.j. užívatelia vo Windows doméne (v intranete alebo prihlásení cez VPN) majú prístup k aplikácii na základe svojho prihlásenia do domény, bez nutnosti zadávať užívateľské meno a heslo v prihlasovacom dialógu v internetovom prehliadači.

Predpokladá sa, že webserver Apache Tomcat je [nainštalovaný](#) do adresára `C:\Program Files\Apache Software Foundation\Tomcat 6.0`.

Postup inštalácie

1. Stiahnite zo stránky projektu tomcatspnego (<http://tomcatspnego.codeplex.com>), zo sekcie Download, aktuálnu verziu (použitý [trunk-20022010.zip](#)).
2. Zo stiahnutého súboru vyextrahujte súbor, ktorého meno začína *trunk-dll* (použitý *trunk-dll-20022010.zip*).
3. Z tohto súboru vyextrahujte dynamické knižnice *dll\vc90\SSPAuthentication.dll* a *dll\vc90\SSPAuthentication64x.dll* a nakopírujte ich do adresára `C:\Program Files\Apache Software Foundation\Tomcat 6.0\bin`.

Poznámka: *SSPAuthentication.dll* sa použije pre 32-bitovú inštaláciu Tomcat na 32 a 64 bitových Windows, *SSPAuthentication64x.dll* sa použije pre 64-bitovú inštaláciu Tomcat na 64 bitových Windows. Pokiaľ by autentifikácia nefungovala, sú k dispozícii ešte verzie súborov *dll\PlatformSDK2003x64\SSPAuthenticationx64.dll* a *dll\vc2003\SSPAuthentication.dll*.

4. Vyextrahujte aj súbor *jar\tomcat6\rdoumesppitc6.jar* a nakopírujte ho do adresára `C:\Program Files\Apache Software Foundation\Tomcat 6.0\lib`.
5. Pokiaľ ste ešte nedistribuovali web aplikáciu na web server pomocou programu [TCLDeployer](#), urobte tak teraz. alší postup predpokladá, že web aplikácia sa nachádza v adresári `C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\mojaApp`.
6. Do adresára `C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\mojaApp` nakopírujte vyextrahovaný adresár *example\authbyssp\META-INF*. Obsahuje súbor *context.xml* s textom:

```
<?xml version='1.0' encoding='utf-8'?>
<Context>
  <Valve className="fr.doume.authenticator.SSPAAuthenticator" />
  <Realm className="fr.doume.realm.WindowsRealm" />
</Context>
```

7. Do súboru `C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\mojaApp\WEB-INF\web.xml` doplňte bezpečnostnú sekciu na konci sekcie `<web-app>`:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app>

...
<security-constraint>
<display-name>Example Security Constraint</display-name>
<web-resource-collection>
  <web-resource-name>Protected Area</web-resource-name>
  <!-- Define the context-relative URL(s) to be protected -->
  <url-pattern>/idom.html</url-pattern>
  <url-pattern>/d2was_service2</url-pattern>
  <!-- If you list http methods, only those methods are protected -->
  <http-method>DELETE</http-method>
  <http-method>GET</http-method>
  <http-method>POST</http-method>
  <http-method>PUT</http-method>
</web-resource-collection>
<auth-constraint>
  <!-- Anyone with one of the listed roles may access this area -->
  <role-name>MYDOMAIN\MYGRP</role-name>
</auth-constraint>
</security-constraint>

<!-- Default login configuration -->
<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>Example Spnego</realm-name>
</login-config>

<security-role>
  <role-name>MYDOMAIN\MYGRP</role-name>
</security-role>
</web-app>
```

Pre prihlásenie do domény použite v URL *idom.html* namiesto *index.html*.

Príklad:

`http://hostname[:port]/mojaApp/idom.html[?alias]`

Názov domény a skupiny užívateľov *MYDOMAINMYGRP* nahraťe vlastnou doménou a skupinou užívateľov, ktorí majú povolený prístup k web aplikácii s povolenou [TCL autentifikáciou](#).

Poznámka: Možné je špecifikovať aj doménu a skupinu užívateľov *MYDOMAIN\everyone* alebo iba *everyone*, takže prebehne úspešná autentifikácia všetkých doménových užívateľov voči web serveru. Zjednoduší to správu užívateľov a z bezpečnostného hľadiska to nie je veľké riziko, keďže následne ešte D2000 server kontroluje, či užívateľ existuje v konfigurácii aplikácie a či má povolenú TCL autentifikáciu v [Metódach autentifikácie](#).

8. Ak ste ešte nevytvorili na doménovom serveri skupinu užívateľov (v našom prípade *MYGRP*), môžete tak urobiť teraz.
9. Všetkým užívateľom, ktorí majú mať povolenú [TCL autentifikáciu](#), treba povoliť túto možnosť v konfigurácii [Metód autentifikácie](#). Prítom názov užívateľa v D2000 a názov užívateľa v doméne musí byť rovnaký.
10. Názov domény musí byť nakonfigurovaný v parametri [Doména](#).

Poznámka 1: Aby [TCL autentifikácia](#) fungovala v prehliadači Mozilla Firefox (od verzie 3.0), treba ho nakonfigurovať, aby podporoval Kerberos autentifikáciu pre konkrétny web server:

1. Choďte na URL adresu `about:config`. Pokiaľ sa zobrazí varovanie, potvrdte ho.
2. Vo filtroch zadajte masku `network.negotiate`.
3. Do nastavení `network.negotiate-auth.delegation-uris` a `network.negotiate-auth.trusted-uris` pridajte názov vášho web servera, voči ktorému má Firefox použiť Kerberos autentifikáciu, na ktorej je [TCL autentifikácia](#) založená. Pokiaľ sa aplikácia nachádza na viacerých web serveroch alebo máte viacero aplikácií, názvy serverov treba oddelovať iarkou.

Príklad: `myweb1,myweb2,myapp3`

Poznámka 2: Po pridaní doménového užívateľa do skupiny užívateľov (v našom prípade *MYGRP*) sa musí užívateľ odhlásiť a znovu prihlásiť do Windows, aby bol naozaj v skupine užívateľov (keďže získavanie oprávnení sa deje počas procesu prihlasovania). Medzitým užívateľ nebude úspešne prihlásený [TCL autentifikáciou](#) a zobrazí sa zvyčajné prihlasovacie okno ponúkajúce zadanie užívateľského mena a hesla.



Súvisiace stránky:

[D2000 Tenký klient](#)
[D2000 Tenký klient - inštalácia](#)