

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. užívateľa vo Windows doméne (v intranete alebo prihlásení cez VPN) majú prístup k aplikácii na základe svojho prihlásenia do domény, bez nutnosti zadáva užívateské meno a heslo v prihlásovacom dialógu v internetovom prehliadai.

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 zaína *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 používa pre 32-bitovú inštaláciu Tomcat na 32 a 64 bitových Windows, SSPAuthentication64.dll sa používa pre 64-bitovú inštaláciu Tomcat na 64 bitových Windows. Pokiaľ by autentifikácia nefungovala, sú k dispozícii ešte verzie súborov *dll\PLatf ormSDK2003x64\SSPAuthenticationx64.dll* a *dll\vc2003\SSPAuthentication.dll*.
4. Vyextrahujte aj súbor *jar\tomcat6\frdoumesppitc6.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. Či už 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\IMETA-INF*. Obsahuje súbor *context.xml* s textom:

```
<?xml version='1.0' encoding='utf-8'?>
<Context>
    <Valve className="fr.doume.authenticator.SSPAuthenticator" />
    <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 doplte bezpenostnú 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\[?alias\]](http://hostname[:port]/mojaApp/idom.html[?alias])

Názov domény a skupiny užívateov *MYDOMA\N\WYGRP* nahrate vlastnou doménou a skupinou užívateov, ktorí majú povolený prístup k web aplikácii s povolenou [TCL autentifikáciou](#).

Poznámka: Možné je špecifikova aj doménu a skupinu užívateov *MYDOMA\N\everyone* alebo *everyone*, takže prebehne úspešná autentifikácia všetkých doménových užívateov voi web serveru. Zjednoduší to správu užívateov a z bezpenostného hadiska to nie je veké riziko, keže následne ešte D2000 server kontroluje, i užívate existuje v konfigurácii aplikácie a i má povolenú TCL autentifikáciu v [Metódach autentifikácie](#).

8. Ak ste ešte nevytvorili na doménovom serveri skupinu užívateov (v našom príklade *WYGRP*), môžete tak urobi teraz.
9. Všetkým užívateom, ktorí majú ma povolenú [TCL autentifikáciu](#), treba povoli túto možnos v konfigurácii [Metód autentifikácie](#). Pritom názov užívatea v D2000 a názov užívatea v doméne musí by rovnaký.
10. Názov domény musí by nakonfigurovaný v parametri [Doména](#).

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

1. Chote na URL adresu `about:config`. Pokia sa zobrazí varovanie, potvrte ho.
2. Vo filtri zadajte masku `network.negotiate`.
3. Do nastavení `network.negotiate-auth.delegation-uris` a `network.negotiate-auth.trusted-uris` pridajte názov vášho web servera, voi ktorému má Firefox použi Kerberos autentifikáciu, na ktorej je [TCL autentifikácia](#) založená. Pokia sa aplikácia nachádza na viacerých web servery alebo máte viacero aplikácií, názvy serverov treba oddeova iarkou.
Príklad: `myweb1,myweb2,myapp3`

Poznámka 2: Po pridaní doménového užívatea do skupiny užívateov (v našom príklade *WYGRP*) sa musí užívate odhlási a znova prihlási do Windows, aby bol naozaj v skupine užívateov (keže získavanie oprávnení sa deje poas procesu prihlasovania). Medzitým užívate nebude úspešne prihlásený [TCL autentifikáciou](#) a zobrazí sa zvyajné prihlasovacie okno ponúkajúce zadanie uživateského mena a hesla.



Súvisiace stránky:

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