Kako ispravno instalirati Apache Tomcat na Linux server

čet, 2018-12-06 14:29 - Ratko Žižek

"*Kako pravilno instalirati Tomcat?!? Pfff, samo zaguglaš i biraš između prvih dvadesetak naputaka, problema nema jer Tomcat je vrlo popularan web serverčić za Java aplikacije, dugo je na terenu* (i bla-bla)". Realnost je ovakva: na službenom Tomcatovom siteu ova tema je - ajmo reć' - čudno obrađena; što se tiče weba - uputa i savjeta ima puno, definitivno previše uzevši u obzir da su neki od njih zastarjeli, neki su necjeloviti, u nekima se autoru potkradu greške ili nešto improvizira... pa nakon višednevnih isprobavanja shvatimo da, doduše, možemo Tomcat postaviti na Linux server i-'vako-i-'nako ali ne i **pravilno** tj. **tako da brzo dobijemo funkcionalan web server, ujedno dostatno zaštićen i spreman za učinkovito administriranje**.

Dobro je znati:

- Tomcat i Javu, najnovije verzije u vrijeme pisanja ovog članka, postavljamo na CentOS 7.5.x;
- taj server treba završiti u predprodukcijskoj ili produkcijskoj okolini (instalacije za potrebe razvoja su jednostavnije, također, redovito se primjenjuje Java Development Kit a ne Java Runtime Environment).
- naredbama prisutnim u nižim primjerima dodajte **sudo** kao prefiks ili prijeđite u kontekst *roota.*

I. JAVA

Zato što je nužan preduvjet za nesmetan rad Tomcata, posvetit ćemo dio ovog članka potencijalno glavobolnoj temi odabira određene verzije/izvedenice Java platforme te, dakako, pravilnog postavljanja odabrane Jave u računalo. Koje su verzije Jave preporučene za Tomcat 9.x lako ćemo naći u njegovoj dokumentaciji - Java SE verzija 8.x i više - i to je ok. Ostaje nam zapetljaniji dio priče: hoćemo li instalirati Oracleovu komercijalnu verziju Jave SE (Hotspot), Oracleovu besplatnu izvedenicu te iste verzije (OpenJDK) ili onu verziju i varijantu OpenJDK Jave koja se nalazi u službenom repozitoriju naše Linux distribucije. Razrada prethodne rečenice bez poteškoća se može pretvoriti u zaseban članak ali mi ćemo se zadovoljiti s par relevantnih smjernica:

- Oracleova komercijalna Java redovito prednjači u optimiziranosti i novim značajkama, donoseći kupcu i službenu podršku korporacije;
- Oracelovu besplatnu Javu ne krase odlike komercijalne ali je stabilna i spremna za samoinicijativne prilagodbe nekoj specifičnoj potrebi;
- Oracleova besplatna Java učlanjena u repozitorij SW paketa određene Linux distribucije u nekim je aspektima prilagođena baš tom OS-u; isplati ju se rabiti ukoliko je riječ o dobro podržanom i perspektivnom OS-u;
- ponekad nemamo slobodu odabira verzije i izdanja Jave, naime, ako se autor neke aplikacije kategorički izjasni da je preduvjet za nesmetan rad njegovog uratka ta-i-ta Java, onda nije mudro nametati svoj odabir.

Slijedi instaliranje Jave. Ukoliko favoriziramo OpenJDK iz repozitorija CentOS-a, **yum** će tu najnoviju instalaciju postaviti kao aktivnu. Pozor! Ovakav način instaliranja OpenJDK može zbuniti jer akronim JDK sugerira da u sustav postavljamo Java Development Kit (JDK) dok u stvarnosti yum preferira - upražnjavamo li napredne tehnike uporabe tipkovnice, što je najčešći slučaj - Java Runtime

Environment (JRE). U pravilu mi i želimo JRE, ali postaje nezgodno ako je neophodna baš JDK jer ćemo u tom slučaju, s instaliranom JRE, dobijati svakojake greške. Da ne duljimo, upišite **yum install java-1.8** (trenutno najnovija verzija CentOS Jave), triput pritisnite tipku TAB i vidjet ćete da se defaultno nudi instalacija JRE te da OpenJDK dolazi u ovećem broju modula kako bismo mogli instalirati samo potrebne.

```
[root@catak3 ~]# yum install java-1.8.0-openjdk = JRE
java-1.8.0-openjdk-accessibility-debug.i686    java-1.8.0-openjdk-devel.x86_64 = JDK
java-1.8.0-openjdk-accessibility-debug.x86_64  java-1.8.0-openjdk-headless-debug.i686
java-1.8.0-openjdk-accessibility.i686          java-1.8.0-openjdk-headless-debug.x86_64
java-1.8.0-openjdk-accessibility.x86_64        java-1.8.0-openjdk-headless.i686
java-1.8.0-openjdk-debug.i686                  java-1.8.0-openjdk.i686
java-1.8.0-openjdk-debug.x86_64                java-1.8.0-openjdk-javadoc-debug.noarch
java-1.8.0-openjdk-demo-debug.i686             java-1.8.0-openjdk-javadoc.noarch
java-1.8.0-openjdk-demo-debug.x86_64           java-1.8.0-openjdk-javadoc-zip-debug.noarch
java-1.8.0-openjdk-demo.i686                   java-1.8.0-openjdk-javadoc-zip.noarch
java-1.8.0-openjdk-demo.x86_64                 java-1.8.0-openjdk-src-debug.i686
java-1.8.0-openjdk-devel-debug.i686            java-1.8.0-openjdk-src-debug.x86_64
java-1.8.0-openjdk-devel-debug.x86_64          java-1.8.0-openjdk-src.i686
java-1.8.0-openjdk-devel.i686                  java-1.8.0-openjdk-src.x86_64
```

Sad ćemo u CentOS "natočiti" najnoviju komercijalnu verziju Jave SE s Oracleovog sitea. Provjeravamo postoje li i koje su Jave u sustavu; izvještaj pokazuje da već imamo OpenJDK JRE.

alternatives --config java

```
There is 1 program that provides 'java'.

Selection  Command

-----------------------------------------------

*+ 1  java-1.8.0-openjdk.x86_64
(/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.191.b12-0.el7_5.x86_64/jre/bin/java)
```

Skinemo s Oracleovog web mjesta .rpm paket - najnovija Oracleova verzija Jave je 11 - i naredbom oblika ***yum localistall <paket>*** instaliramo je u sustav; sad će naredba *alternatives --config java* prikazati niže podatke. Znakovi **+** i ***** su preraspoređeni ali ne moramo se zamarati smislom te poruke, samo ukucamo u prompt broj **2** i potvrdimo.

alternatives --config java

```
There are 2 programs which provide 'java'.

Selection  Command

-----------------------------------------------

 + 1  java-1.8.0-openjdk.x86_64
(/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.191.b12-0.el7_5.x86_64/jre/bin/java)

*  2  /usr/java/jdk-11.0.1/bin/java

 Enter to keep the current selection[+], or type selection number: 2
```

Nakon ove operacije Oracle Java je defaultna i prioritetna, uvjerimo se s *alternatives --config java* ili nižom naredbom.

java -version

```
java version "11.0.1" 2018-10-16 LTS

Java(TM) SE Runtime Environment 18.9 (build 11.0.1+13-LTS)

Java HotSpot(TM) 64-Bit Server VM 18.9 (build 11.0.1+13-LTS, mixed mode)
```

Zgodan trik: praktičan način aktiviranja potrebne Jave je deinstalacija svih drugih (na produkcijskom serveru to ionako moramo učiniti) jer tada se OS nema oko čega dvoumiti.

I Tomcat i CentOS su *open-source* pa ćemo nadalje u primjerima rabiti OpenJDK.

II. TOMCAT

I ovdje, kao maloprije s Javom, trebamo odlučiti: hoćemo li instalirati originalni Tomcat kojega stvara i nudi Apache Software Foundation ili onaj već učlanjen u neku Linux distribuciju. "Posvojeni" Tomcat je, kažu upućeni, bolje integriran s OS-om domaćinom, lakše se instalira... ali redovito u razvoju značajno zaostaje za ASF-ovim Tomcatom. Mi se opredjeljujemo za izvorni i (trenutno) najnoviji ASF-ov Tomcat 9.0.13.

1. Uvažavajući FHS smjernice, Tomcat ćemo na datotečni sustav CentOS-a smjestiti u direktorij /opt, poddirektorij tomcat9.

2. Kreiramo servisni račun tomsvc. Primjećujete da osobni direktorij tog sistemskog korisnika odgovara Tomcatovom, razlog je taj što servisni račun shvaćamo integralnim dijelom konkretne Tomcat instalacije. Također, smatramo da je najbolji pristup onemogućiti tom računu ulogiravanje u sustav. Ako nakon izvršene naredbe u datoteci *shadow* vidimo da redak tomsvc ima dva uzastopna uskličnika umjesto enkriptirane lozinke, naš servisni račun je neprobojan.

useradd -m -U -d /opt/tomcat9 -s /bin/false tomsvc

3. Na disku imamo Tomcat 9.0.13, skinut s https://tomcat.apache.org u formatu *.tar.gz* (**ne** .zip) te raspakiran u /install direktorij; sad ćemo u direktorij /opt/tomcat9 premjestiti sve što je unutar distribucijskog direktorija, ne i sam taj direktorij.

mv /install/apache-tomcat-9.0.13/* /opt/tomcat9

4. Servisnom računu i njegovoj grupi predajemo vlasništvo nad cijelim tomcat9 ogrankom direktorija i datoteka. Ne primjenjujemo mogućnost kreiranja korisnika bez primarne grupe - kako neki sugeriraju - jer bismo time prekršili standard a ne znamo (niti možemo znati) koje bi to neželjene nuspojave izazvalo.

chown -R tomsvc:tomsvc /opt/tomcat9

5. Prihvaćamo se pretvaranja Tomcata u boot-time servis, znači, kreirat ćemo datoteku instrukcija tomcat9.service u /etc/systemd/system. Kako to biva sa softverom, Tomcat i Java, pa i sam Systemd Manager, prepuni su tzv. defaultnih (inicijalnih, podrazumijevanih) vrijednosti, utoliko u tomcat9.service navodimo samo one stavke kojima mijenjamo podrazumijevanu vrijednost. Slijedi jedna datoteka instrukcija opće namjene s pojašnjenjima, nadamo se da će poslužiti kao dobra osnovica za daljnje prilagodbe nekoj konkretnoj implementaciji.

```
[Unit]

Description=ApacheTomcat9
```

```
Wants=network.target

After=network.target

[Service]

Type=forking

Environment="JAVA_HOME=/usr/lib/jvm/jre"

# Koristimo li apsolutnu putanju poput
/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.191.b12-0.el7_5.x86_64/jre,

# morat ćemo rekonfigurirati sve pokazivače u svim skriptama na izvršni Java modul nakon

# svakog značajnijeg ažuriranja Jave.

Environment="CATALINA_PID=/opt/tomcat9/temp/tomcat.pid"

Environment="CATALINA_HOME=/opt/tomcat9"

Environment="CATALINA_OPTS=-Xms2048M -Xmx2048M -server -XX:+UseG1GC"

# U varijablu CATALINA_OPTS stavljamo one parametre koji trebaju zahvatiti samo Tomcat,

# ne i druge Java aplikacije na serveru. Poštujući Oracleovu preporuku, koristimo istu

# vrijednost za inicijalnu i maksimalnu količinu RAM-a. Parametar -server je defaultan za

# 64-bitnu JVM, ovdje je zbog potrebe testiranja parametra -XX:+UseG1GC.

Environment="JAVA_OPTS=-Djava.awt.headless=true -Djava.security.egd=file:///dev.urandom
-Djava.net.preferIPv4Stack=true"

# Parametri varijable JAVA_OPTS su strongly recommended za Tomcat, njihovo značenje i implikacije
lako ćemo saznati guglanjem.

ExecStart=/opt/tomcat9/bin/startup.sh

ExecStop=/opt/tomcat9/bin/shutdown.sh

User=tomsvc

Group=tomsvc

UMask=0007

#RestartSec=10s

#Restart=on-failure

[Install]

WantedBy=multi-user.target
```

6. Preostaje nam par uobičajenih postupaka kojima osiguravamo punopravno članstvo Tomcata među auto-start servisima.

systemctl daemon-reload, potom **systemctl start tomcat9** pa **systemctl enable tomcat9**

7. Ovaj korak znamo i žmirećki odradit', prisutan je samo zbog cjelovitosti naputka.

firewall-cmd --zone=public --permanent --add-port=8080/tcp

firewall-cmd --reload

8. Ekspresna provjera cjelokupnog posla:

- Reboot servera;
- u browser na admin stanici upisati http://IP:8080/examples;
- pokrenuti poneku demo aplikacijicu iz svake grupe primjera.

9. Radi? Naaravno da radi! Ne radi?!? ehh... nemam vremena, krenite od logova u /opt/tomcat9/logs, sretno! :o)

Ovime završava uobičajena, rekli bismo standardna instalacija Tomcata. Sad možemo krenuti s podešavanjem njegovim za prihvat aplikacija, baviti se anti-intruder zaštitom... ali možemo i nastaviti s jednom od dvije nestandardne instalacije (u kontekstu postavljanja Tomcata na jedno-te-isto računalo). Takozvana *multi-instance* instalacija Tomcata nastavlja se na gore opisanu instalaciju tako da se dosta složenim zahvatima kreiraju kolekcije određenih Tomcatovih mapa i konfiguracijskih datoteka koje se nadalje nezavisno konfiguriraju, pogodno za hosting scenarije. Drugi način nestandardne instalacije Tomcata u jedno računalo je instaliranje i zasebno konfiguriranje u svemu nezavisnih Tomcata, primjerice, instaliramo Tomcat 8.5 u /opt/tomcat8 i Tomcat 9.x u /opt/tomcat9 - sada je svaka instalacija u svojoj JVM; praktično rješenje kad s jedne glavne verzije migriramo aplikacije na drugu. Na nižoj slici vidimo miroljubivu koegzistenciju Osmice i Devetke.

```
[root@catak1 ~]# systemctl status tomcat8 tomcat9
● tomcat8.service - Tomcat8Server
   Loaded: loaded (/etc/systemd/system/tomcat8.service; enabled; vendor preset: disab
led)
   Active: active (running) since Tue 2018-11-27 07:13:32 CET; 3h 41min ago
  Process: 1088 ExecStart=/opt/tomcat8/bin/startup.sh (code=exited, status=0/SUCCESS)
 Main PID: 1114 (java)
    Tasks: 43
   CGroup: /system.slice/tomcat8.service
           └─1114 /usr/lib/jvm/jre/bin/java -Djava.util.logging.config.file=/opt/tomc
● tomcat9.service - Tomcat9Server
   Loaded: loaded (/etc/systemd/system/tomcat9.service; enabled; vendor preset: disab
led)
   Active: active (running) since Tue 2018-11-27 07:13:32 CET; 3h 41min ago
  Process: 1100 ExecStart=/opt/tomcat9/bin/startup.sh (code=exited, status=0/SUCCESS)
 Main PID: 1153 (java)
    Tasks: 61
   CGroup: /system.slice/tomcat9.service
           └─1153 /usr/lib/jvm/jre/bin/java -Djava.util.logging.config.file=/opt/tomc
```

Nestandardne instalacije podrazumijevaju ne samo dobro poznavanje Tomcata već i specifične operativne scenarije (ta nećemo si bezrazložno komplicirati život), trenutno nam je zanimljivija problematika portova na kojima sluša naš tek postavljeni web serverčić. Naime, IT profesionalci, zamalo pa izdresirani pravilom da web server zaprima HTTP konekcije na TCP port 80 a HTTPS konekcije na 443, imaju jaku potrebu rekonfigurirati Tomcatove defaultne 8080 i 8443 portove... i potom se bez ikakve stvarne potrebe nerviraju zbog toga što se Tomcat uporno ruši! Mačak je ovdje zaista nevin, to Linux OS ne dopušta pristup niskim portovima softveru pokrenutom u kontekstu

običnog korisnika. Nije na odmet znati preporuku samog Apache projekta: Tomcat je prvenstveno aplikacijski server i treba se "skrivati" iza proxy sloja (poput Apache web servera, F5 BIG-IP, Citrix Netscalera...) od kojega se ujedno očekuju TLS terminacija i load balancing. Zaključujemo da su u takvoj sistemskoj arhitekturi visoki portovi koje Tomcat rabi sasvim u redu. No, postoji li opravdana potreba da Tomcatovi konektori zaista "sjede" na portovima ispod 1024, primijenit ćemo jedno od ovoga:

- Zavrtjeti Tomcat u kontekstu *root* accounta = najlakše rješenje, ujedno i najteži mogući grijeh, znamo zašto;
- koristiti authbind aplikaciju = stara je 4 godine, nikad se ne zna kad će biti "pregažena" nekim updateom OS-a;
- kombinacijom iptables/firewalld postaviti redirekciju prometa s porta 80 na 8080. E, to već obećava! Slijedi primjer redirekcije koja preživljava restart računala:

firewall-cmd --zone=public --add-masquerade --permanent

firewall-cmd --zone=public --add-forward-port=port=80:proto=tcp:toport=8080 --permanent

Slijedi primjena TLS-a te prateće mjere zaštite podataka i Tomcata, do čitanja!

Vijesti: Linux [1]
Kuharice: Za sistemce [2]
Kategorije: Sistemci [3]
Vote: 0

No votes yet

story_tag: tomcat [4]
Linux [5]
centos [6]
instalacija [7]
java [8]

Source URL: https://sysportal.carnet.hr/node/1834

Links
[1] https://sysportal.carnet.hr/taxonomy/term/11
[2] https://sysportal.carnet.hr/taxonomy/term/22
[3] https://sysportal.carnet.hr/taxonomy/term/36
[4] https://sysportal.carnet.hr/taxonomy/term/285
[5] https://sysportal.carnet.hr/taxonomy/term/119
[6] https://sysportal.carnet.hr/taxonomy/term/286
[7] https://sysportal.carnet.hr/taxonomy/term/287
[8] https://sysportal.carnet.hr/taxonomy/term/288