Tomcat

- description : 톰캣 운영과 관련된 내용
- author : 주레피
- email : dhan@repia.com
- lastupdate : 2020-03-09

Tomcat Versions

Apache Tomcat Version	Servlet Spec	Jsp Spec	Web Socket Spec	JDK	다운로드
Apache Tomcat 9.0.33	4.0	2.3	1.1	JDK 8이상	다운로드
Apache Tomcat 8.5.53	3.1	2.3	1.1	JDK 7이상	다운로드
Apache Tomcat 8.0.53	3.1	2.3	1.1	JDK 7이상	다운로드
Apache Tomcat 7.0.103	3.0	2.2	1.1	JDK 6이상	다운로드
Apache Tomcat 6.0.53	2.5	2.1	-	JDK 5이상	다운로드
Apache Tomcat 5.5.36	2.4	2.0	-	JDK 1.4이상	다운로드
Apache Tomcat 4.1.40	2.3	1.2	-	JDK 1.3이상	다운로드
Apache Tomcat 3.3.2	2.2	1.1	-	JDK 1.1이상	다운로드

보안 취약점

2020.02.24 CVE-2020-1938 Apache Tomcat 취약점(Ghostcat)
조치방법(김토피아) , CVE-2020-1938

```
조치 방법
1. 톰캣 버전별 최신으로 업그레이드
2. server.xml, workers.properties 설정 수정
```

workers.properties

```
worker.list=loadbalancer

worker.loadbalancer.type=lb
worker.loadbalancer.balanced_workers=worker1,worker2
worker.loadbalancer.sticky_session=1

worker.worker1.type=ajp13
worker.worker1.host=127.0.0.1
worker.worker1.port=8020
worker.worker1.lbfactor=1
worker.worker1.secret=${random문자열}
```

server.xml

```
<Connector protocol="AJP/1.3"
           secret="${random문자열}"
           address="127.0.0.1"
           port="8020"
           redirectPort="8443" />
```

> 기본 포트가 '8009' 인데, 설정하면서 변경하는 것을 추천함

catalina.sh (라인은 다를 수 있음)

```
    284
    285 # Set UMASK unless it has been overridden
    286 if [ -z "$UMASK" ]; then
    287     UMASK="0027" --> 0022로 변경
    288 fi
    289 umask $UMASK
```

> Tomcat이 root로 구동중 인 경우 UMASK가 0022로 바뀌어야 함
> 0022의 의미 해석방법: Reading - 4, Writing - 2, Executing - 1, 계산방법: 0777 - 0022 = 0755 -> chmod 755 와 같은 의미 첫번째7: 소유자 권한, 두번째5: 그룹사용자권한, 세번째5: 기타 사용자 권한

오류 페이지 대응

오류 코드에 대해서 상응하는 사용자가 직접 만든 페이지가 나올 수 있도록 조치하는 방법을 기술
사용자가 만든 오류 페이지가 존재하지 않으면 was의 정보가 노출 됨을 방지

> {RSA_WEB_ROOT}/WEB-INF/web.xml에 내용 추가, 필요에 따라 {TOMCAT_ROOT}/conf/web.xml 에도 내용 추가
> <error-code>에 에러코드(숫자) 입력
> 코드번호: 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 500, 501, 502, 503, 504, 505
> JSP의 위치는 Context 디렉토리와 front 디렉토리에 둠 (필요에 따라 {TOMCAT_ROOT}/webapps/ROOT에 넣음

* HTTP 상태 코드 정리

{TOMCAT_ROOT}/conf/web.xml

```
 <error-page>
     <error-code>401</error-code>
     <location>/error.jsp</location>
 </error-page>
 <error-page>
    <error-code>402</error-code>
    <location>/error.jsp</location>
</error-page>
..... 생략
```

> error.jsp 소스

```
    <%@ page language="java" contentType="text/html; charset=utf-8"%>
    <!DOCTYPE HTML>
    <html>

          <head>
            <meta http-equiv="Content-Type" content="text/html;
charset=UTF-8">
            <title>웹 페이지를 표시할 수 없습니다.</title>
            <style type="text/css">
                body { background-repeat: repeat-x; background-color: white;
font-family: "맑은 고딕", "Segoe UI", "verdana", "arial"; margin: 0em; color:
#575757; }
                .mainContent { margin-top:80px; width: 700px; margin-left:
120px ; margin-right: auto ; }
                /* title { color: #2778ec; font-size: 30pt; font-weight:
300; vertical-align:bottom; margin-bottom: 20px; font-family: "맑은 고딕",
"Segoe UI", "verdana"; position: relative; } */
                .title { color: #228b22; font-size: 30pt; font-weight: 300;
vertical-align:bottom; margin-bottom: 20px; font-family: "맑은 고딕", "Segoe
UI", "verdana"; position: relative; }
                .errorExplanation { color: #000000; font-size: 12pt; font-
family: "맑은 고딕", "Segoe UI", "verdana", "arial"; text-decoration: none; }
                .taskSection { margin-top: 20px; margin-bottom: 40px;
position: relative; }
                .tasks { color: #000000; font-family: "맑은 고딕", "Segoe
UI", "verdana"; font-weight:200; font-size: 12pt; padding-top: 5px; }
                li { margin-top: 8px; }
                .diagnoseButton { outline: none; font-size: 9pt; }
                .webpageURL { direction:ltr; }
                .hidden { display:none; }
                /* a { color: #0066cc; font-family: "맑은 고딕", "Segoe UI",
"verdana", "arial"; font-size: 11pt; text-decoration: none; } */
                a { color: #008000; font-family: "맑은 고딕", "Segoe UI",
"verdana", "arial"; font-size: 11pt; text-decoration: none; }
                a:hover { text-decoration: underline; }
                .lineBottom { border-bottom: 1px solid; }
                .lineTop { border-top: 1px solid; }
                .r { text-align: right; }
                .l { text-align: left; }
            </style>
        </head>

        <body>
            <div id="contentContainer" class ="mainContent">
                <div id="mainTitle" class="title">이 페이지를 표시할 수 없습니
다.</div>
                <div class="taskSection" id="taskSection">
                    <ul id="taskList" class="tasks">
                        <li id="task1">웹 주소 <span id="webpage"
class="webpageURL"></span>이(가) 올바른지 확인하세요.</li>
                        <li id="task2">검색 엔진으로 페이지를 찾아보세요.</li>
```

```
                        <li id="task3">몇 분 후에 페이지를 새로 고치세요.</li>
                        <li id="task4">TLS 및 SSL 프로토콜이 사용되고 있는지 확인하세요. 도구 > 인터넷 옵션 > 고급 > 설정 > 보안으로 이동하세요.</li>
                    </ul>
                    <ul id="cantDisplayTasks" class="tasks hidden">
                        <li id="task1-1">웹 주소가 올바른지 확인하세요.</li>
                        <li id="task1-2">검색 엔진으로 페이지를 찾아보세요.</li>
                        <li id="task1-3">몇 분 후에 페이지를 새로 고치세요.</li>
                    </ul>
                    <ul id="notConnectedTasks" class="tasks hidden">
                        <li id="task2-1">모든 네트워크 케이블이 연결되어 있는지 확인하세요.</li>
                        <li id="task2-2">비행기 모드가 꺼져 있는지 확인하세요.</li>
                        <li id="task2-3">무선 스위치가 켜져 있는지 확인하세요.</li>
                        <li id="task2-4">모바일 광대역에 연결할 수 있는지 확인하세요.</li>
                        <li id="task2-5">라우터를 다시 시작하세요.</li>
                    </ul>
                </div>
                <div class="lineTop l"><a href="http://<%=request.getServerName()%>" title="페이지 이동">http://<%=request.getServerName()%></a></div>
                <% response.setStatus(404); %>
            </div>
        <script type="text/javascript">
        try { document.getElementById("webpage").innerHTML = location.href; } catch(e) {}
        </script>
        </body>
    </html>
```

로깅

톰캣 로그 관리 절차

1. 삭제 없이 생성되는 *.log
    1. crontab을 이용하여 최근 30일 이후 데이터를 주기적으로 삭제
2. catalina.out 계속 커지는 문제
    1. logrotate.d (리눅스 로그 관리툴 이용)로 관리

삭제 없이 생성되는 *.log

crontab에서 사용할 SHELL 프로그램 작성(${CATALINA_HOME}/bin/log_delete.sh)

```
#!/bin/sh
#30일이 지난 *.log, *.txt 삭제
cd ${CATALINA_HOME}
find ./logs -mtime +30 -name '*.log' -exec rm -f {} \;
```

```
find ./logs -mtime +30 -name '*.txt' -exec rm -f {} \;
```

crontab 등록 or LogProc나 actctl.sh에 등록해도 됨

```
// 실행 권한 추가
$> chmod +x ${CATALINA_HOME}/bin/log_delete.sh
// 크론탭 등록, 사용자에 따른 크론탭 실행 권한이 허용되어야 됨
$> crontab -l  // 크론탭 리스트 보기
$> crontab -e  // 크론탭 수정
0 5 * * * ${CATALINA_HOME}/bin/log_delete.sh # 매일 새벽 5시에 수행
```

logrotate에 등록하여 처리

```
// /etc/logrotate.d 아래에 tomcat 파일 생성
$> cat /etc/logrotate.d/tomcat //파일명은 편하게 생성하되 무엇을 가르키는지 명확하게 작성
/usr/local/tomcat/*log { // *log 또는 catalina.out 가능
    copytruncate
    daily
    rotate 200
    compress
    missingok
    notifempty
    dateext
    dateformat .%Y-%m-%d
}

$> // 로그파일 순환 테스트
$> $logrotate -f /etc/logrotate.d/tomcat
$> // 디버그 모드
$> $logrotate -d /etc/logrotate.d/tomcat
```

> copytruncate : 기존 파일을 백업해서 다른 파일로 이동하고 기존 파일은 지워버리는 옵션
> daily : 로그파일을 날짜별로 변환
> compress : 지나간 로그파일들을 gzip으로 압축
> dateext : 순환된 로그파일의 날짜확장자
> missingok : 로그파일이 없더라도 오류를 발생시키지 않음
> rotate 30 : 로그 파일은 30개만큼 저장된 다음 제거되거나 메일로 보내짐
> notifempty : 파일의 내용이 없으면 새로운 로그 파일을 생성 안함
> dateformat .%Y-%m-%d

catalina.out 계속 커지는 문제

linux tomcat catalina.out 안나오게 하는 방법 / linux tomcat catalina.out 이 나오지 않는다 / linux tomcat catalina.out 용량이 너무 클때 https://mycup.tistory.com/216|Tomcat 로그 관리 (logrotate.d)]]
logrotate.d 더 많은 옵션 정리
Tomcat 무분별하게 catalina.out 크기 커지는 것 막기
리눅스에서 logrotate 사용하기

https 적용

```
> https를 사용하기 위하여 SSL 적용 하기
> 모든 tomcat이 아래의 방법을 사용하지는 않음
> keystoreFile와 keystorePass 추가
```

```
    <Connector port="8443"
protocol="org.apache.coyote.http11.Http11Protocol"
               maxThreads="150" SSLEnabled="true" scheme="https"
secure="true"
               clientAuth="false" sslProtocol="TLS" keystoreFile="인증서경
로/sslcert.co.kr_xxxxx.jks 파일" keystorePass=".jks 패스워드"/>
```

설정

[Tomcat] apache-tomcat secretRequired 설정 방법 (AJP Connecter SSL, secret key, secret password)

컨텍스트 경로

```
컨텍스트 경로는 빈 문자열("") 이거나 '/'로 시작해야 하며
'/'로 끝나서는 안된다.
```

Apache-tomcat 연동하기

- [CentOS] apache-tomcat 연동하기 httpd 2.4.x, tomcat-connectors-1.2.46-src
- [CentOS7] 아파치와 톰캣 연동하기 (mod_jk) & 로드밸런스 설정
- Apache-Tomcat-7.0.100 이상 server.xml AJP 설정

Linux 설치

- 시스템 부팅시 자동 시작 스크립트

Windows 설치

서비스 등록/삭제

[tomcat]윈도우 톰캣 서비스 등록

```
service.bat install
```

> 서비스 등록은 prompt에서 진행
> 등록하기 전에 service.bat 내용 수정해야 됨

서비스 삭제

```
sc delete 서비스명
```

> 서비스 삭제는 prompt에서 진행
> 서비스명은 제어판 > 관리도구 > 서비스에서 확인

Optimization, Tunning

- JAVA_OPTS

```
JAVA_OPTS="-Djava.awt.headless=true -server -Xms512m -Xmx8192m -
XX:NewSize=256m -XX:MaxNewSize=256m -XX:PermSize=256m -XX:MaxPermSize=512m -
XX:+DisableExplicitGC"
```

> -Xms: Heap 최소 크기
> -Xmx: Heap 최대 크기
> setenv.sh, setenv.bat에 넣는 것이 바람직함

Tomcat8 Heap memory size

setenv.bat

```

```

setenv.sh

```
    export CATALINA_OPTS="$CATALINA_OPTS -Xms512m"
```

Tip

- 톰캣 캐시 사용 안하기
- Tomcat 버전 정보 숨기기
- Tomcat 보안

Troubleshooting

톰캣 구동시에 'Creation of SecureRandom instance for session ID generation using [SHA1PRNG] took' 메시지와 함께 멈춤현상 발생시 조치 방안
해결법: JAVA_OPTS="$JAVA_OPTS -Djava.security.egd=file:/dev/./urandom tomcat 구동 시 /dev/random 블로킹 이슈

윈도우 서비스 등록시 구동이 잘 안될 경우
설치 경로에서 공백 제거 (Apache Tomcat 8.5 → ApacheTomcat85)

tomcat7 시작시 the basedir environment variable is not defined tomcat7 메시지와 함께 시작이 안될 경우

환경 변수 CATALINA_HOME, JAVA_HOME를 지정하면 됨 /etc/profile, ~/.bash_profile, catalina.sh 에서 지정하면 됩니다.

80포트로 실행(not root)

```
1~1024까지의 포트는 root 사용자 이외에는 bind가 불가능하다.
iptables를 활용하여 모든 인바운드를 8080포트로 리다이렉트하여 같은 효과를 얻을 수 있음
# iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8080
```

TOMCAT서버를 ROOT가 아닌 일반사용자로 80포트를 서비스 하는 경우

“Catalina”; 프로토콜 핸들러 시작 실패

```
심각: Failed to start connector [Connector[AJP/1.3-8009]]
org.apache.catalina.LifecycleException: service.getName(): "Catalina";  프로토콜 핸들러 시작 실패
    at
org.apache.catalina.connector.Connector.startInternal(Connector.java:1065)
    at org.apache.catalina.util.LifecycleBase.start(LifecycleBase.java:183)
    at
org.apache.catalina.core.StandardService.startInternal(StandardService.java:460)
    at org.apache.catalina.util.LifecycleBase.start(LifecycleBase.java:183)
    at
org.apache.catalina.core.StandardServer.startInternal(StandardServer.java:744)
    at org.apache.catalina.util.LifecycleBase.start(LifecycleBase.java:183)
    at org.apache.catalina.startup.Catalina.start(Catalina.java:712)
    at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
    at
sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57)
    at
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
    at java.lang.reflect.Method.invoke(Method.java:606)
    at org.apache.catalina.startup.Bootstrap.start(Bootstrap.java:294)
    at org.apache.catalina.startup.Bootstrap.main(Bootstrap.java:428)
Caused by: java.lang.IllegalArgumentException: AJP 연결자는 secretRequired="true"로 구성되었으나 보안 속성이 널 또는 ""입니다. 이 조합은 유효하지 않습니다.
    at
org.apache.coyote.ajp.AbstractAjpProtocol.start(AbstractAjpProtocol.java:211)
    at
org.apache.catalina.connector.Connector.startInternal(Connector.java:1058)
    ... 12 more
```

해결법: server.xml의 Connector에 secretRequired=“false” 추가

```
    <Connector secretRequired="false" connectionTimeout="20000" port="8080"
protocol="HTTP/1.1" redirectPort="8443"/>
```

Invalid byte tag in constant pool: 19
해결법: 톰캣 버그로 아래의 것을 사용하자

```
Tomcat 9.0.x : 9.0.0.M18 이후
Tomcat 8.5.x : 8.5.12 이상
Tomcat 8.0.x : 8.0.42 이상
Tomcat 7.0.x : 7.0.76 이상
```

https://avaiable.tistory.com/261

- hot deploy

Ref

- Apache Tomcat Versions
- 톰캣 버전별 서블릿 스펙
- 톰켓 버추얼 호스팅 + server.xml 설정

tomcat

From:
http://125.132.25.164/dokuwiki/ - **문제를 잘 정의하는 것은 문제를 절반 해결한 것이다. - 2023.12**

Permanent link:
http://125.132.25.164/dokuwiki/doku.php?id=wiki:was:tomcat&rev=1658383774

Last update: **2022/07/21 15:09**