UMT 部署文档

1.概要说明

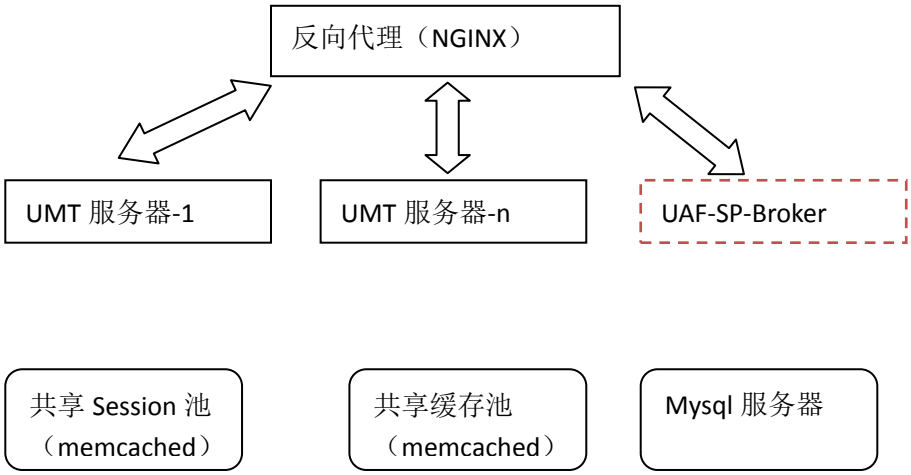
1.1 部署需求清单

以后端部署两个 UMT 服务器节点

编号	需求内容	说明
1.	一个公网 IP (正式上线后需要)	由于对外服务的需要，反向代理服务器需要有一个外部能访问的 IP 地址。
2.	一个有效的域名 (正式上线后需要)	请指向反向代理服务器
3.	一个 HTTPS 服务器证书 (正式上线后需要)	用于配置 HTTPS 服务器时使用。要求证书的 CN 指向需求 2 中的域名。同时这个证书最好是由浏览器信任的 CA 签发的(避免用户安装根证书)。
4.	服务器 6 台	一台装反向代理服务器，公网 IP 两台安装 UMT 服务器，内网 IP 两台安装 Memcached 服务，共启动 4 个 memcached 进程。 一台安装 Mysql(版本大于 5.0)服务器

1.2 部署图

UMT 是现在科技网通行证使用的基础软件。为了获得系统的高可用性（HA），在实际部署中采用了集群部署的方式。部署图如下图所示：



1.3 部署图说明

从上面的部署图可以看出，整个系统需要一组服务器来配合完成。其中：

- 反向代理服务器（部署 NGINX）一台：负责 Web 请求的转发和负载均衡功能。这台服务器要求有公网的 IP 地址，同时希望有一个正式的域名和一个浏览器认的有效的证书（用于提供 HTTPS 服务）。
- UMT 服务器 1～n：这个建议至少部署两台服务器，这几台服务器的要求是计算能力稍高，不需要公网的 IP 地址，有内部的地址即可。
- UAF-SP-Broker：第一步暂时不装，用于部署科技云认证联盟的 SP 代理使用。
- 共享的 Session 池：用于在多个 UMT 服务器之间维护 Session 时使用，一般由两个 Memcache 进程共同组成。建议由两个运行在不同服务器上的 memcached 进程组成。
- 共享缓存池：提供 UMT 程序内部的缓存服务，用于提高系统的访问性能。同样也是用 memcached 服务器组成。建议由两个运行在不同服务器上的 memcached 进程组成。共享 Session 池的 memcached 服务器和共享缓存池的 memached 服务进程不能共享。

2.按模块部署说明

2.1 共享 Session 池部署

在提供服务之前，需要安装 memcached 服务，下面以 CentOS 为例的安装 memcached 的步骤：

1. 安装 memcached　respo

   wget http://dag.wieers.com/rpm/packages/rpmforge-release/rpmforge-release-0.5.2-2.rf.src.rpm

   rpm -ivh rpmforge-release-0.5.2-2.rf.src.rpm

2. 安装 memcached

   yum install memcached

   请根据服务器的类型安装合适的版本安装。

安装完成以后，在两台服务器上都以下面的命令启动服务(注意，如果服务器启动了防火墙，请将 TCP 11211 端口打开):

memcached –p 11212 –d

2.2 共享缓存池部署

共享缓存池的部署和共享 Session 池的部署一样，如果已经在两台缓存服务器上安装过了 Memcached 服务器，则不需要重新安装。请在这两台服务器上，以下面的命令启动 Memcached 服务器：

memcached –d –p 11211

2.3 UMT 服务器部署

UMT 服务是部署与 Tomcat 中的 Java Web 服务，因此整个系统需要安装 jdk 1.7、tomcat7 和 umt。

JDK 安装

UMT 系统使用 JDK 1.7，可以从
http://www.oracle.com/technetwork/java/javase/downloads/index.html
选择下载最新版本的 JDK 1.7 安装。

部署步骤

1) cd /usr/local
2) tar zxvf jdk-7u17-linux-x64.tar.gz
3) ln -s /usr/local/jdk1.7.0_17 /usr/local/jdk
4) vi /etc/profile
   在最后加入下段代码：
   export JAVA_HOME=/usr/local/jdk
   export CLASSPATH=.:$JAVA_HOME/lib:$JAVA_HOME/jre/lib:$JAVA_HOME/lib/tools.jar
   export PATH=$JAVA_HOME/bin:$JAVA_HOME/jre/bin:$PATH
   export CATALINA_HOME=/usr/local/tomcat

   source /etc/profile

tomcat 部署

Tomcat 版本使用 7.0，见附件中的 apache-tomcat-7.0.26_msm.zip

部署步骤

1) cd /usr/local
2) unzip apache-tomcat-7.0.26_msm.zip
3) ln -s /usr/local/apache-tomcat-7.0.26 /usr/local/tomcat
4) vi conf/context.xml
   在<WatchedResource>WEB-INF/web.xml</WatchedResource>下面加入下段代码，其中黄色部位需单独配置：

```
<Manager className="de.javakaffee.web.msm.MemcachedBackupSessionManager"
        sticky="true"
        memcachedNodes="n1:10.10.1.76:11212 n2:10.10.1.77:11212"
        failoverNodes=""
```

requestUriIgnorePattern=".*\.(png|gif|jpg|css|js|ico)$"
sessionBackupAsync="false"
sessionBackupTimeout="100"

transcoderFactoryClass="de.javakaffee.web.msm.serializer.kryo.KryoTranscoderFactory"

customConverter="de.javakaffee.web.msm.serializer.kryo.JodaDateTimeRegistration,
de.javakaffee.web.msm.serializer.kryo.WicketSerializerFactory,
net.duckling.serializer.CustomKryoRegistration"
/>

5) vi tomcat/conf/server.xml
在</Host>前加入下行代码：
<Context path="" docBase="umt" debug="0" reloadable="true" crossContext="true"/>
其中，黄色标出的部分，请替换成实际的服务器 IP 地址。

UMT 部署

从文档的附件中获得 umt.war
1) cd /usr/local/tomcat/webapps/
2) mkdir umt
3) cd umt
4) unzip umt.war
5) cd WEB-INF/conf/
6) vi umt.properties
以下为配置文件全文,以测试环境配置为例,黄色部分为需要更改的配置:
#Config file for Resource Management
#All configed properties must be configed like
key=value
#This file support vairiable value, example:
A=Hello
B=${A} world
#B's value will be "Hello world"

###
# #
Database Config
# #
###
#Database's login name

database.username=${mysql_database_username}
#Database's password

```
database.password=${mysql_database_password}


#Database's host
database.dbhost=${host_ip_of_mysql}
database.dbname=${myql_database}



#Database's connection URL
database.conn-url=jdbc:mysql://${database.dbhost}/${database.dbname}?useUnicode=true
&characterEncoding=UTF-8

#Database driver
database.driver=com.mysql.jdbc.Driver

#Max connection count of the connection pool
database.maxconn=10

#Max idle connection of the connection pool
database.maxidle=3


#####################################################################
#                                                                   #
#                    Mail Config                                #
#                                                                   #
#####################################################################
#mail server's host
mail.host=smtp.cnic.cn

#mail server's username
mail.username=mailAccount@ihep.ac.cn

#mail server's password
mail.password=mailPassword

#mail box's name
mail.boxname=mailAccount@ihep.ac.cn

#mail content template dir
mail.temlate.dir=/WEB-INF/message
```

```
#####################################################################
#                                                                   #
#                    Certificate Config                             #
#                                                                   #
#####################################################################
#UMT cert's file
umt.cert.keyfile=/WEB-INF/umtcert.txt

#UMT des key file
umt.des.keyfile=/WEB-INF/umtkey.bin

#can be MD2,MD5,SHA,SHA-256,SHA-384,SSHA,NONE
PASSWORDS_ENCRYPTION_ALGORITHM=SHA

#####################################################################
#                                                                   #
#                    CoreMail API Config                            #
#                                        --add by lvly              #
#####################################################################
umt.coremail.api.ip=159.226.14.143
umt.coremail.api.port=6195

umt.coremail.api.providerId=1
umt.coremail.api.orgId=a
umt.coremail.api.email.domain=cstnet.cn

umt.coremail.api.user.status=0
umt.coremail.api.user.cosId=1
umt.coremail.api.user.quotaDelta=0

#please set absolute url,don't end with '/'
umt.this.base.url=http://passporttest.escience.cn
umt.memcachedURL=10.10.1.76:11211 10.10.1.77:11211
uaf.login.url=http://passporttest.escience.cn/sp-broker/login
uaf.logout.url=http://passporttest.escience.cn/sp-broker/logout
```

需要修改的配置基本上分三个部分：

1. 数据库配置

```
database.password=${mysql_database_password}
#Database's host
database.dbhost=${host_ip_of_mysql}
database.dbname=${myql_database}
```

这里可以直接配置一个空的数据库，UMT 在系统启动时自动创建数据库表。

2. 邮件配置

```
#mail server's username
```

mail.username=mailAccount@ihep.ac.cn
#mail server's password
mail.password=mailPassword
#mail box's name
mail.boxname=mailAccount@ihep.ac.cn

这个邮箱用来发送重置密码邮件。

3. URL 配置

umt.this.base.url=http://passporttest.escience.cn
uaf.login.url=http://passporttest.escience.cn/sp-broker/login
uaf.logout.url=http://passporttest.escience.cn/sp-broker/logout

umt.this.base.url 指向 NGINX 服务器的域名
uaf.login.url、uaf.logout.url 是认证联盟的配置，可暂时不管

4. 缓存服务器配置

umt.memcachedURL=10.10.1.76:11211 10.10.1.77:11211

指向刚才配置的共享缓存池服务器，多个机器之间以空格分开。

反向代理服务部署

1. 安装 nginx repository

wget http://nginx.org/packages/centos/6/noarch/RPMS/nginx-release-centos-6-0.el6.ngx.noarch.rpm

rpm –ivh nginx-release-rhel-6-0.el6.ngx.noarch.rpm

2. 安装 nginx 服务器

yum install nginx

3. 配置 NGINX

编辑/etc/nginx/nginx.conf 配置文件，并将下面配置中黄色部分修改成合适的值

```
user    nginx nginx;
worker_processes    4;

#error_log    logs/error.log;
#error_log    logs/error.log    notice;
#error_log    logs/error.log    info;

#pid              logs/nginx.pid;

worker_rlimit_nofile    102400;

events
{
      use epoll;
      worker_connections    102400;
```

```
}

http {
    include       mime.types;
    default_type  application/octet-stream;


    log_format  passport  '$remote_addr - $remote_user [$time_local] - $upstream_addr - "$request" '
                          '$status $body_bytes_sent "$http_referer" '
                          '"$http_user_agent" "$http_x_forwarded_for"';

    sendfile        on;

    keepalive_timeout  65;

    gzip  on;
    gzip_min_length 1024;
    gzip_proxied  any;
    gzip_types  text/plain text/css image/jpeg application/x-javascript application/octet-stream application/json;

    upstream passport_pool{
        server 159.226.27.32:80 weight=1 max_fails=1 fail_timeout=5s;
        server 159.226.27.33:80 weight=1 max_fails=1 fail_timeout=5s;
        ip_hash;
    }

    server {
        listen       443;
        listen  [::]:443;

        server_name passport.escience.cn;

        ssl                  on;
        ssl_certificate      cert.pem;
        ssl_certificate_key  cert.key;

        ssl_session_timeout  5m;

        ssl_protocols  SSLv2 SSLv3 TLSv1;
        ssl_ciphers  HIGH:!aNULL:!MD5;
        ssl_prefer_server_ciphers  on;
```

```
        location / {
        proxy_pass http://passport_pool;
        proxy_set_header REMOTE-HOST $remote_addr;
            proxy_set_header X-Real-IP $remote_addr;
            proxy_set_header Host $host;
            proxy_set_header X-Forward-For $remote_addr;
            proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
            client_max_body_size       2000m;
            client_body_buffer_size 128m;
        }
      }
}
```

这个配置

upstream passport_pool 部分配置的是反向代理的服务器池，这里指向之前要求的几台 UMT 服务器就行。

server_name passport.escience.cn：是该 NGINX 反向代理服务器所在机器的域名

ssl_certificate 、ssl_certificate_key，是分别指向 HTTPS 服务器的证书链和私钥。

如果暂时没有合适的证书，可以先自己创建一个测试用的证书，例子见

http://blog.sina.com.cn/s/blog_870c35680101bws1.html

NGINX 证书链的创建

和 Apache 不一样，Nginx 没有 Certificat Chain 这个参数，所以你要把你的证书和中间证书合并。合并证书很简单，创建一个先的文件 oschina-chain.crt，内容如下：

```
-----BEGIN CERTIFICATE-----
这里是你证书的内容
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
这里是中间证书的内容
-----END CERTIFICATE-----
```

4.部署验证

访问URL: http://${nginx_domain}

进入登录界面即部署成功！