移动支付平台

KeepAlived+Apache+Tomcat负载均衡集成手册

**深圳信息中心应用维护室**

**2017年7月26日**

目录

[移动支付平台 1](#_Toc509567278)

[KeepAlived+Apache+Tomcat负载均衡集成手册 1](#_Toc509567279)

[1 系统架构图 4](#_Toc509567280)

[2 规划 5](#_Toc509567281)

[2.1 文件系统规划 5](#_Toc509567282)

[2.1.1 TOMCAT服务器 5](#_Toc509567283)

[2.1.2 APACHE服务器： 5](#_Toc509567284)

[2.2 用户规划 6](#_Toc509567285)

[2.2.1 TOMCAT服务器 6](#_Toc509567286)

[2.2.2 APACHE服务器 6](#_Toc509567287)

[2.3 IP规划 6](#_Toc509567288)

[2.3.1 PORPAPP 6](#_Toc509567289)

[2.3.2 MPPMGM 7](#_Toc509567290)

[2.3.3 PORTCOM 7](#_Toc509567291)

[2.3.4 MPPCOM 8](#_Toc509567292)

[2.3.5 INAPACHE 8](#_Toc509567293)

[2.3.6 OUTAPACHE 8](#_Toc509567294)

[2.4 端口规划 9](#_Toc509567295)

[2.4.1 TOMCAT服务器 9](#_Toc509567296)

[2.4.2 APACHE服务器 9](#_Toc509567297)

[3 安装Apache 10](#_Toc509567298)

[3.1 Hosts文件配置 10](#_Toc509567299)

[3.2 安装pcre 10](#_Toc509567300)

[3.3 升级openssl 10](#_Toc509567301)

[3.4 安装zlib 11](#_Toc509567302)

[3.5 安装Apache 11](#_Toc509567303)

[3.6 Apache自动启动及关闭 11](#_Toc509567304)

[3.7 Apache安全加固 12](#_Toc509567305)

[3.7.1 取消Indexes选项 12](#_Toc509567306)

[3.7.2 只允许GET和POST方法 12](#_Toc509567307)

[3.7.3 禁止所有对根目录的访问 12](#_Toc509567308)

[3.7.4 以专门的用户账号运行Apache 13](#_Toc509567309)

[3.7.5 非超级用户无根目录的写权限 13](#_Toc509567310)

[3.7.6 删除缺省安装的无用文件 13](#_Toc509567311)

[3.7.7 隐藏Apache版本号及其他敏感信息 13](#_Toc509567312)

[3.7.8 配置错误日志文件 14](#_Toc509567313)

[3.7.9 设置错误页面重定向 14](#_Toc509567314)

[3.8 负载均衡配置 14](#_Toc509567315)

[3.9 Apache日志分割配置 16](#_Toc509567316)

[4 KeepAlived安装配置 17](#_Toc509567317)

[4.1 KeepAlived依赖包安装配置 17](#_Toc509567318)

[4.2 KeepAlived安装 17](#_Toc509567319)

[4.3 KeepAlived配置 17](#_Toc509567320)

[4.4 KeepAlived日志分离配置 22](#_Toc509567321)

[4.5 启动KeepAlived 23](#_Toc509567322)

[4.6 切换测试 24](#_Toc509567323)

[5 Tomcat安装 25](#_Toc509567324)

[5.1 JDK安装配置 25](#_Toc509567325)

[5.2 Tomcat用户及组创建 25](#_Toc509567326)

[5.3 Tomcat安装配置 26](#_Toc509567327)

[5.3.1 安装 26](#_Toc509567328)

[5.3.2 配置 26](#_Toc509567329)

[5.3.3 Tomcat日志分割配置 28](#_Toc509567330)

[5.4 Tomcat安全加固 29](#_Toc509567331)

[5.4.1 禁止Tomcat列表显示文件 29](#_Toc509567332)

[5.4.2 禁用manager功能 29](#_Toc509567333)

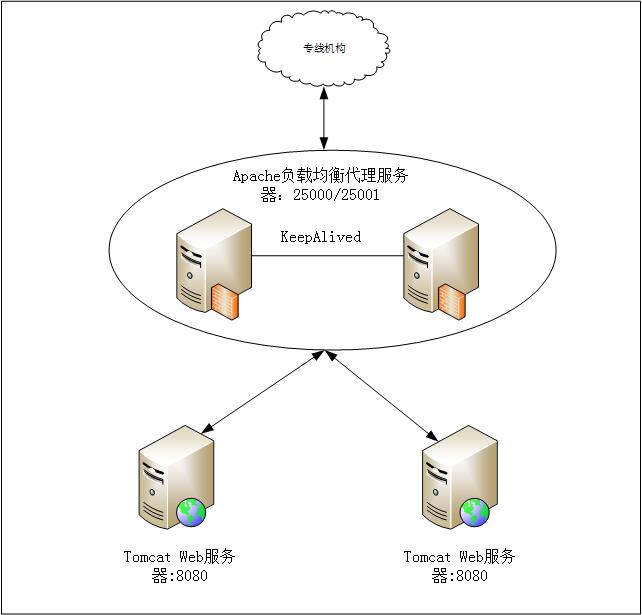
[5.4.3 tomcat用户具有远程管理权限 29](#_Toc509567334)

[5.4.4 密码长度不小于8位 29](#_Toc509567335)

[5.4.5 移除错误页面中的版本信息 30](#_Toc509567336)

[5.4.6 配置Tomcat错误页面重定向 30](#_Toc509567337)

# 系统架构图



说明：

1. Apache负载均衡代理服务器有两台服务器组成，通过KeepAlived双机热备。
2. 专线机构通过KeepAlived的VIP和25000端口访问Apache服务器，Apache服务器内部通过25001端口将session负载均衡转发到2两台Tomcat Web服务器。

# 规划

## 文件系统规划

### TOMCAT服务器

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 主机名 | 文件系统 | 大小（G) | 用途 | 备注 |
|  | /appset/tomcat | 20G | 安装tomcat及应用程序发布 |  |
| /applog/tomcat/logs | 10G | 存放tomcat日志 |  |
|  | /appset/tomcat | 20G | 安装tomcat及应用程序发布 |  |
| /applog/tomcat/logs | 10G | 存放tomcat日志 |  |

### APACHE服务器：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 主机名 | 文件系统 | 大小（G) | 用途 | 备注 |
|  | /appset/apache | 20 | Apache安装目录 |  |
| /applog/apache\_log | 10 | 存放apache运行日志 |  |
| /applog/alived\_log | 存放KeepAlived运行日志 |  |
| /usr/local/keepalived |  | Keepalived安装目录 |  |
| /etc/keepalived |  | 存放KeepAlived配置文件 |  |
|  | /appset/apache | 20 | 用于安装Apache |  |
| /applog/apache\_log | 10 | 存放apache运行日志 |  |
| /applog/alived\_log | 存放KeepAlived运行日志 |  |
| /usr/local/keepalived |  | Keepalived安装目录 |  |
| /etc/keepalived |  | 存放KeepAlived配置文件 |  |

## 用户规划

### TOMCAT服务器

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 主机名 | 用户名 | 用户ID | 用户组 | 组ID | 备注 |
|  | tomcat | 1040 | tomcat | 1040 |  |
|  | tomcat | 1040 | tomcat | 1040 |  |

### APACHE服务器

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 主机名 | 用户名 | 用户ID | 用户组 | 组ID | 备注 |
|  | umps | 1060 | umps | 1060 |  |
|  | umps | 1060 | umps | 1060 |  |

## IP规划

### PORPAPP

|  |  |  |
| --- | --- | --- |
| 主机名 | IP地址 | 备注 |
| PORPAPP21 | 184.41.32.38 | 对外服务 |
| 184.46.32.38 | 文件同步（保留） |
| 184.36.32.38 | 管理 |
| PORPAPP22 | 184.41.32.39 | 对外服务 |
| 184.46.32.39 | 文件同步（保留） |
| 184.36.32.39 | 管理 |

### MPPMGM

|  |  |  |
| --- | --- | --- |
| 主机名 | IP地址 | 备注 |
| MPPMGM21 | 184.41.32.36 | 对外服务 |
| 184.46.32.36 | 文件同步（保留） |
| 184.36.32.36 | 管理 |
| MPPMGM22 | 184.41.32.37 | 对外服务 |
| 184.46.32.37 | 文件同步（保留） |
| 184.36.32.37 | 管理 |

### PORTCOM

|  |  |  |
| --- | --- | --- |
| 主机名 | IP地址 | 备注 |
| PORTCOM21 | 184.41.16.4 | 对外服务 |
| 184.41.16.6 | VIP |
| 184.41.48.4 | 对内服务 |
| 184.41.48.6 | VIP |
| 184.46.48.4 | 保留（以后做文件传输用） |
| 184.36.48.4 | 管理IP |
| PORTCOM22 | 184.41.16.5 | 对外服务 |
| 184.41.16.6 | VIP |
| 184.41.48.5 | 对内服务 |
| 184.41.48.6 | VIP |
| 184.46.48.5 | 保留（以后做文件传输用） |
| 184.36.48.5 | 管理IP |

### MPPCOM

|  |  |  |
| --- | --- | --- |
| 主机名 | IP地址 | 备注 |
| MPPCOM21 | 184.41.16.36 | 对外服务 |
| 184.41.16.38 | VIP |
| 184.41.48.36 | 对内服务 |
| 184.41.48.38 | VIP |
| 184.46.48.36 | 保留（以后做文件传输用） |
| 184.36.48.36 | 管理IP |
| MPPCOM22 | 184.41.16.37 | 对外服务 |
| 184.41.16.38 | VIP |
| 184.41.48.37 | 对内服务 |
| 184.41.48.38 | VIP |
| 184.46.48.37 | 保留（以后做文件传输用） |
| 184.36.48.37 | 管理IP |

### INAPACHE

|  |  |  |
| --- | --- | --- |
| 主机名 | IP地址 | 备注 |
| INAPACHE21 | 184.41.48.7 | 对外服务 |
| 184.41.48.9 | VIP |
| 184.46.48.7 | 对内服务 |
| 184.36.48.7 | 管理IP |
| INAPACHE22 | 184.41.48.8 | 对外服务 |
| 184.41.48.9 | VIP |
| 184.46.48.8 | 对内服务 |
| 184.36.48.8 | 管理IP |

### OUTAPACHE

|  |  |  |
| --- | --- | --- |
| 主机名 | IP地址 | 备注 |
| OUTAPACHE21 | 184.41.24.36 | 对外服务 |
| 184.41.24.38 | VIP |
| 184.41.56.36 | 对内服务 |
| 184.41.56.38 | VIP |
| 184.46.56.36 | 保留（以后做文件传输用） |
| 184.36.56.36 | 管理IP |
| OUTAPACHE22 | 184.41.24.37 | 对外服务 |
| 184.41.24.37 | VIP |
| 184.41.56.37 | 对内服务 |
| 184.41.56.37 | VIP |
| 184.46.56.37 | 保留（以后做文件传输用） |
| 184.36.56.37 | 管理IP |

## 端口规划

### TOMCAT服务器

|  |  |  |
| --- | --- | --- |
| 主机名 | 端口 | 备注 |
|  | 8080 |  |
|  | 8080 |  |

### APACHE服务器

|  |  |  |
| --- | --- | --- |
| 主机名 | 端口 | 备注 |
|  | 25000 | 对外服务 |
| 25001 | 对内服务 |
|  | 25000 | 对外服务 |
| 25001 | 对内服务 |

# 安装Apache

## Hosts文件配置

修改/etc/hosts文件，添加类似如下内容

|  |
| --- |
| 184.41.16.4 PORTCOM21 |

## 安装pcre

|  |
| --- |
| # tar –zxvf pcre-8.40.tar.gz  # cd pcre-8.40  # ./ configure --prefix=/usr/local/pcre  # make  # make install |

## 升级openssl

|  |
| --- |
| --备份原版本ssl便于回退  #mv /etc/ssl /etc/ssl.old  # tar -zxvf openssl-1.1.0e.tar.gz  # cd openssl-1.1.0e  # ./config -fPIC --openssldir=/etc/ssl shared  # make  # make install  #mv /usr/bin/openssl /usr/bin/openssl.old  #ln -s /usr/local/bin/openssl /usr/bin/openssl  #echo "/usr/local/lib64/" >>/etc/ld.so.conf  #ldconfig -v |

## 安装zlib

|  |
| --- |
| #tar –zxvf zlib-1.2.8.tar.gz  #cd zlib-1.2.8  #./config  #make && make install |

## 安装Apache

本次安装方法采用在测试环境上将Aapche编译好，tar包到安装环境上进行解压。

以下为在测试环境上编译安装apache的命令

|  |
| --- |
| #tar –zxvf httpd-2.4.26.tar.gz  # cd httpd-2.4.26  #export LDFLAGS=-ldl  # ./configure --prefix=/usr/local/apache --enable-modules=all --enable-dav --enable-maintainer-mode -enable-rewrite --enable-so --enable-proxy --enable-http --enable-vhost-alias --enable-proxy-ftp --enable-proxy-http --enable-proxy-ajp --enable-status --enable-proxy-balancer --enable-proxy-connect --enable-mods-shared="all" --with-mpm=worker --enable-ssl --with-pcre=/usr/local/pcre  # make  # make install |

## Apache自动启动及关闭

创建/etc/init.d/rc5.d/S99Apache启动服务脚本，内容如下

|  |
| --- |
| su - umps -c "/appset/apache/bin/apachectl -k start" |

赋予脚本可执行权限

|  |
| --- |
| #chmod +x /etc/init.d/rc5.d/S99Apache |

创建/etc/init.d/rc5.d/K01Apache关闭服务脚本，内容如下

|  |
| --- |
| kill -9 $(ps -ef|grep httpd |grep -v grep |awk '{print $2}') |

赋予脚本可执行权限

|  |
| --- |
| #chmod +x /etc/init.d/rc5.d/K01Apache |

## Apache安全加固

### 取消Indexes选项

在配置文件中，将所有Options关键字后的Indexes去掉，如

|  |
| --- |
| <Directory "/Web">  Options FollowSymlinks  </Directory> |

### 只允许GET和POST方法

在httpd.conf中，添加如下内容

|  |
| --- |
| <LimitExcept GET POST OPTIONS>  Deny from all  </LimitExcept> |

### 禁止所有对根目录的访问

在配置文件httpd.conf中添加如下语句，禁止对根目录的访问

|  |
| --- |
| <Directory />  Order deny,allow  Deny from all  </Directory> |

### 以专门的用户账号运行Apache

在配置文件中添加如下语句:

User apache

说明：apache为apache进程所属用户名，应指定专门的用户名

### 非超级用户无根目录的写权限

在httpd.conf中有如下语句：

ServerRoot "/appset/apache"，则执行如下命令改变权限：

chmod -R a-w /appset/apache

注：普通用户管理apache则不适用

### 删除缺省安装的无用文件

* 删除缺省CGI脚本

|  |
| --- |
| rm –rf /appset/apache/cgi-bin/\* |

* 删除Apache说明文件

|  |
| --- |
| rm –rf /appset/apache/manual |

* 删除缺省HTML文件

|  |
| --- |
| rm -rf /usr/local/apache2/htdocs/\* |

### 隐藏Apache版本号及其他敏感信息

* 隐藏版本号

在httpd.conf中增加如下语句

|  |
| --- |
| ServerTokens Prod |

* 隐藏签名

在httpd.conf中设置ServerSignature字段如下

|  |
| --- |
| ServerSignature Off |

### 配置错误日志文件

* 设置日志信息级别

在httpd.conf中配置如下语句

|  |
| --- |
| LogLevel notice |

* 设置错误日志文件

在配置文件httpd.conf中设置错误日志文件路径，例如：ErrorLog logs/error\_log，其中logs/error\_log为相应的文件路径。

### 设置错误页面重定向

在httpd.conf中，配置500、401、405、400、404、403错误重定向页面

|  |
| --- |
| ErrorDocument 500 /custom500.html  ErrorDocument 401 /custom401.html  ErrorDocument 405 /custom405.html  ErrorDocument 400 /custom400.html  ErrorDocument 404 /custom404.html  ErrorDocument 403 /custom403.html |

## 负载均衡配置

修改/appset/apache/conf/httpd.conf，添加如下内容

|  |
| --- |
| <Directory /token\_web>  AllowOverride none  Order deny,allow  Allow from all  </Directory> |

将#Include conf/extra/httpd-vhosts.conf前面的“#”取消

将ServerName一行注释并添加类似如下两行

|  |
| --- |
| ServerName 184.41.16.6:25000  ServerName 184.41.48.6:25001 |

修改Listen一行，并添加一行，最后如下

|  |
| --- |
| Listen 25000  Listen 25001 |

修改/appset/apache/conf/extra/httpd-vhost.conf

添加如下代码

|  |
| --- |
| <VirtualHost \*:25000>  DocumentRoot "/appset/apache"  ServerName 184.41.16.6  ServerAlias 184.41.16.6  ProxyRequests Off  ProxyPass /token\_web balancer://portalapp/ stickysession=JSESSIONID|jsessionid nofailover=On  ProxyPassReverse /token\_web balancer://portalapp/  <Proxy balancer://portalapp>  BalancerMember <http://184.41.32.38:8080/token_web> route=jvm1  BalancerMember <http://184.41.32.39:8080/token_web> route=jvm2  ProxySet lbmethod=byrequests  </Proxy>  ErrorLog "/applog/apache\_log/reverse\_error\_log"  CustomLog "/applog/apache\_log/reverse\_proxy\_log" common  </VirtualHost>  <VirtualHost \*:25001>  ServerName 184.41.48.6  ServerAlias 184.41.48.6  ProxyRequests On  SSLProxyEngine On  <Proxy \*>    </Proxy>  ProxyVia On  </VirtualHost> |

## Apache日志分割配置

使用Apache自带工具rotatelogs，将Apache日志按天进行分割，配置如下

1. 修改apache配置文件httpd.conf

将

|  |
| --- |
| ErrorLog "/applog/apache\_log/error\_log" |

修改为

|  |
| --- |
| ErrorLog "| /appset/apache/bin/rotatelogs /applog/apache\_log/error\_log-%Y-%m-%d 86400 480" |

将

|  |
| --- |
| CustomLog "/applog/apache\_log/access\_log" common |

修改为

|  |
| --- |
| CustomLog "| /appset/apache/bin/rotatelogs /applog/apache\_log/access\_log-%Y-%m-%d 86400 480" common |

1. 修改虚拟主机配置文件httpd-vhosts.conf文件

将

|  |
| --- |
| ErrorLog "/applog/apache\_log/reverse\_error\_log" |

修改为

|  |
| --- |
| ErrorLog "| /appset/apache/bin/rotatelogs /applog/apache\_log/reverse\_error\_log-%Y-%m-%d 86400 480" |

将

|  |
| --- |
| CustomLog "/applog/apache\_log/reverse\_proxy\_log" common |

修改为

|  |
| --- |
| CustomLog "| /appset/apache/bin/rotatelogs /applog/apache\_log/reverse\_proxy\_log-%Y-%m-%d 86400 480" common |

# KeepAlived安装配置

## KeepAlived依赖包安装配置

KeepAlived需要加载ip\_vs模块，SuseLinux 11sp4系统默认未加载此模块，需要安装系统包cluster-network-kmp-default-1.4\_3.0.101\_63-2.30.38.x86\_64.rpm，此包位于Suse Linux 11 sp4 HA第一张光盘（镜像）里。

|  |
| --- |
| #rpm -ivh cluster-network-kmp-default-1.4\_3.0.101\_63-2.30.38.x86\_64.rp |

安装完成后执行modprobe ip\_vs进行加载

|  |
| --- |
| #modprobe ip\_vs |

检查是否加载成功

|  |
| --- |
| #lsmod |grep ip\_vs |

将modprobe ip\_vs添加到/etc/init.d/boot.local文件里面，让系统启动自动加载

## KeepAlived安装

|  |
| --- |
| #cd /dbbak/soft  #tar -zxvf keepalived-1.2.24.tar.gz  #cd keepalived-1.2.24  #./configure --prefix=/usr/local/keepalived  #make && make install |

## KeepAlived配置

1. 将配置文件拷贝到系统对应目录下

|  |
| --- |
| #mkdir -p /etc/keepalived  #cp /usr/local/keepalived/etc/keepalived/keepalived.conf /etc/keepalived/keepalived.conf  #cp /usr/local/keepalived/etc/rc.d/init.d/keepalived /etc/init.d/keepalived  #cp /usr/local/keepalived/etc/sysconfig/keepalived /etc/sysconfig/keepalived |

如果不存在/usr/local/keepalived/etc/rc.d/init.d/keepalived，则

|  |
| --- |
| #cp /dbbak/soft/keepalived-1.2.24/keepalived/etc/init.d/keepalive.suse.init /etc/init.d/keepalived |

1. 设置KeepAlived开机启动

|  |
| --- |
| #chmod +x /etc/init.d/keepalived  #chkconfig keepalived on  ln -s /usr/local/keepalived/sbin/keepalived /usr/sbin/ |

1. 修改配置文件/etc/keepalived/keepalived.conf

INAPACHE23

|  |
| --- |
| ! Configuration File for keepalived  global\_defs {  router\_id INAPACHE23  }  vrrp\_instance VI\_1 {  state BACKUP  interface eth0  virtual\_router\_id 51  priority 100  advert\_int 1  nopreempt  authentication {  auth\_type PASS  auth\_pass 1111  }  virtual\_ipaddress {  184.41.16.6 dev eth0  184.41.48.6 dev eth1  }  }  virtual\_server 184.41.16.6 25000 {  delay\_loop 2  lb\_algo wrr  lb\_kind DR  persistence\_timeout 60  protocol TCP  real\_server 184.41.16.4 25000 {  weight 3  notify\_down /etc/keepalived/stop\_alived.sh  TCP\_CHECK {  connect\_timeout 10  nb\_get\_retry 3  delay\_before\_retry 3  connect\_port 25000  }  }  }  virtual\_server 184.41.48.6 25001 {  delay\_loop 2  lb\_algo wrr  lb\_kind DR  persistence\_timeout 60  protocol TCP  real\_server 184.41.48.4 25000 {  weight 3  notify\_down /etc/keepalived/stop\_alived.sh  TCP\_CHECK {  connect\_timeout 10  nb\_get\_retry 3  delay\_before\_retry 3  connect\_port 25001  }  }  } |

INAPACHE24

|  |
| --- |
| ! Configuration File for keepalived  global\_defs {  router\_id INAPACHE24  }  vrrp\_instance VI\_1 {  state BACKUP  interface eth0  virtual\_router\_id 51  priority 90  advert\_int 1  nopreempt  authentication {  auth\_type PASS  auth\_pass 1111  }  virtual\_ipaddress {  184.41.16.6 dev eth0  184.41.48.6 dev eth1  }  }  virtual\_server 184.41.16.6 25000 {  delay\_loop 2  lb\_algo wrr  lb\_kind DR  persistence\_timeout 60  protocol TCP  real\_server 184.41.16.5 25000 {  weight 3  notify\_down /etc/keepalived/stop\_alived.sh  TCP\_CHECK {  connect\_timeout 10  nb\_get\_retry 3  delay\_before\_retry 3  connect\_port 25000  }  }  }  virtual\_server 184.41.48.6 25001 {  delay\_loop 2  lb\_algo wrr  lb\_kind DR  persistence\_timeout 60  protocol TCP  real\_server 184.41.48.5 25001 {  weight 3  notify\_down /etc/keepalived/stop\_alived.sh  TCP\_CHECK {  connect\_timeout 10  nb\_get\_retry 3  delay\_before\_retry 3  connect\_port 25001  }  }  } |

stop\_alived.sh

|  |
| --- |
| #!/bin/bash  pkill keepalived |

注：以上操作均在两节点执行。

## KeepAlived日志分离配置

将KeepAlived日志从系统日志messages里面分离出来，可进行如下配置

1. 安装rsyslog-5.10.1-0.11.1.x86\_64.rpm系统包

|  |
| --- |
| #rpm -ivh rsyslog-5.10.1-0.11.1.x86\_64.rpm |

1. 修改rsyslog配置文件/etc/rsyslog.conf

将

|  |
| --- |
| \*.\*;mail.none;news.none -/var/log/messages |

修改为

|  |
| --- |
| \*.\*;mail.none;news.none;local0.none -/var/log/messages |

将

|  |
| --- |
| local0,local1.\* -/var/log/localmessages |

修改为

|  |
| --- |
| local0.\* -/var/log/keepalived.log  local1.\* -/var/log/localmessages |

1. 修改配置文件/etc/sysconfig/syslog

将

|  |
| --- |
| SYSLOG\_DAEMON="syslog-ng" |

修改为

|  |
| --- |
| SYSLOG\_DAEMON="rsyslogd" |

1. 修改启动脚本/etc/init.d/keepalived

将

|  |
| --- |
| DAEMON\_OPT="-d " |

修改为

|  |
| --- |
| DAEMON\_OPT="-d -D -S 0" |

1. 启动rsyslog服务

|  |
| --- |
| #service syslog start |

1. 重启KeepAlived服务

|  |
| --- |
| #service keepalived restart |

1. 检查/var/log/keepalived.log日志

## 启动KeepAlived

1. 启动keepalived进程

|  |
| --- |
| #service keepalived start |

1. 进程检查

|  |
| --- |
| #ps –ef|grep keepalived |

返回结果应三个进程

## 切换测试

关闭vip所在节点Apache，测试VIP是否能正常切换。

1. 关闭节点INAPACHE23数据库

|  |
| --- |
| #/appset/apache/bin/apachectl -k stop |

1. 检查VIP是否存在节点INAPACHE23

|  |
| --- |
| #ip addr |grep 184.41.16.6  #ip addr |grep 184.41.48.6 |

1. 启动节点INAPACHE23数据库及keepalived服务

|  |
| --- |
| #/appset/apache/bin/apachectl -k start  #service keepalived start |

1. 检查节点INAPACHE23是否抢占VIP

|  |
| --- |
| #ip addr |grep 184.41.16.6  #ip addr |grep 184.41.48.6 |

注：正常情况下不抢占

1. 关闭节点INAPACHE24节点Apache

|  |
| --- |
| #/appset/apache/bin/apachectl -k stop |

1. 检查VIP是否存在节点INAPACHE24

|  |
| --- |
| #ip addr |grep 184.41.16.6  #ip addr |grep 184.41.48.6 |

1. 启动INAPACHE24节点数据库及keepalived服务

|  |
| --- |
| #/appset/apache/bin/apachectl -k start  #service keepalived start |

1. 检查节点INAPACHE24是否抢占VIP

|  |
| --- |
| # ip addr |grep 184.41.16.6  #ip addr |grep 184.41.48.6 |

注：正常情况下不抢占

# Tomcat安装

## JDK安装配置

将JDK安装介质jdk-7u75-linux-x64.rpm上传至服务器PORTAPP21、PORTAPP22

执行如下命令进行安装

|  |
| --- |
| #rpm -ivh jdk-7u75-linux-x64.rpm |

修改/etc/profile文件，添加jdk环境变量，如下

|  |
| --- |
| export JAVA\_HOME=/usr/java/jdk1.7.0\_75  export PATH=$JAVA\_HOME/bin:$PATH  export CLASSPATH=.:$JAVA\_HOME/lib/dt.jar:$JAVA\_HOME/lib/tools.jar |

## Tomcat用户及组创建

创建tomcat用户组

|  |
| --- |
| #groupoadd -g 1040 tomcat |

创建tomcat用户

|  |
| --- |
| #useradd -g 1040 -d /home/tomcat -m -u 1040 tomcat |

修改tomcat用户密码

|  |
| --- |
| #passwd tomcat |

添加tomcat用户环境变量，vi .profile，添加如下内容

|  |
| --- |
| export JAVA\_HOME=/usr/java/jdk1.7.0\_75  export PATH=$JAVA\_HOME/bin:/appset/tomcat/bin:$PATH  export CLASSPATH=.:$JAVA\_HOME/lib/dt.jar:$JAVA\_HOME/lib/tools.jar  export CATALINA\_BASE=/appset/tomcat  export CATALINA\_HOME=/appset/tomcat |

## Tomcat安装配置

### 安装

将tomcat介质包apache-tomcat-7.0.69.zip上传至服务器PORTAPP21、PORTAPP22

解压tomcat软件包

|  |
| --- |
| #unzip apache-tomcat-7.0.69.zip |

将解压的tomcat拷贝到安装目录

|  |
| --- |
| #cp -rf apache-tomcat-7.0.69 /appset/tomcat |

修改/appset/tomcat属主为tomcat:tomcat及赋予相应权限

|  |
| --- |
| #chown -R tomcat:tomcat /appset/tomcat  #chmod -R 755 /appset/tomcat |

### 配置

配置/appset/tomcat/conf/server.xml文件，修改<Connector executor="tomcatThreadPool"段值为如下

|  |
| --- |
| <Connector executor="tomcatThreadPool" port="8080" protocol="HTTP/1.1" maxThreads="600" minSpareThreads="30"  connectionTimeout="20000"  enableLookups="false"  redirectPort="8443" /> |

修改

|  |
| --- |
| <Engine name="Catalina" defaultHost="localhost" > |

为

|  |
| --- |
| <Engine name="Catalina" defaultHost="localhost" jvmRoute="jvm1"> |
| <Engine name="Catalina" defaultHost="localhost" jvmRoute="jvm2"> |

配置tomcat日志文件路径，修改/appset/tomcat/conf/ logging.properties文件

|  |
| --- |
| 1catalina.org.apache.juli.FileHandler.level = FINE  1catalina.org.apache.juli.FileHandler.directory = ${catalina.base}/logs  1catalina.org.apache.juli.FileHandler.prefix = catalina.  2localhost.org.apache.juli.FileHandler.level = FINE  2localhost.org.apache.juli.FileHandler.directory = ${catalina.base}/logs  2localhost.org.apache.juli.FileHandler.prefix = localhost.  3manager.org.apache.juli.FileHandler.level = FINE  3manager.org.apache.juli.FileHandler.directory = ${catalina.base}/logs  3manager.org.apache.juli.FileHandler.prefix = manager.  4host-manager.org.apache.juli.FileHandler.level = FINE  4host-manager.org.apache.juli.FileHandler.directory = ${catalina.base}/logs  4host-manager.org.apache.juli.FileHandler.prefix = host-manager. |

将${catalina.base}修改为/applog/tomcat

修改/appset/tomcat/bin/catalina.sh文件，将

|  |
| --- |
| if [ -z "$CATALINA\_OUT" ] ; then  CATALINA\_OUT="$CATALINA\_BASE"/logs/catalina.out  fi |

修改为

|  |
| --- |
| if [ -z "$CATALINA\_OUT" ] ; then  CATALINA\_OUT=/applog/tomcat/logs/catalina.out  fi |

### Tomcat日志分割配置

* 安装日志分割工具cronolog

|  |
| --- |
| #tar -zxvf cronolog-1.6.2.tar.gz  #cd cronolog-1.6.2  #./configure  #make && make install |

* 日志分割配置

编辑/appset/tomcat/bin/catalina.sh文件，查找

|  |
| --- |
| if [ -z "$CATALINA\_OUT" ] ; then  CATALINA\_OUT=/applog/tomcat/logs/catalina.out  fi |

修改为

|  |
| --- |
| if [ -z "$CATALINA\_OUT" ] ; then  CATALINA\_OUT=/applog/tomcat/logs/catalina.%Y-%m-%d.out  fi |

注释掉touch "$CATALINA\_OUT"

|  |
| --- |
| # touch "$CATALINA\_OUT" |

将（有两处）

|  |
| --- |
| org.apache.catalina.startup.Bootstrap "$@" start \>> "$CATALINA\_OUT" 2>&1 "&" |

修改为

|  |
| --- |
| org.apache.catalina.startup.Bootstrap "$@" start 2>&1 \  | /usr/local/sbin/cronolog "$CATALINA\_OUT" >> /dev/null & |

修改完成后重启tomcat服务

## Tomcat安全加固

### 禁止Tomcat列表显示文件

编辑web.xml，修改如下：

|  |
| --- |
| <init-param>  <param-name>listings</param-name>  <param-value>true</param-value>  </init-param> |

将true改为false

### 禁用manager功能

将以下目录$CATALINA\_HOME/server/webapps/manager，移除到非$CATALINA\_HOME/server/webapps目录

### tomcat用户具有远程管理权限

在tomcat-users.xml中，修改tomcat用户的role值包含manager，如：

<user username="tomcat" password="\*\*\*" roles="manager">

注：不启用web远程管理功能则不用配置

### 密码长度不小于8位

密码包括数字、小写字母、大写字母和特殊符号中至少两类，在tomcat-users.xml中按要求设置密码

注：不启用web远程管理功能则不用配置，设置的密码也是明文

### 移除错误页面中的版本信息

进入在Tomcat安装目录下的 lib 目录,然后逐次新建org/apache/catalina/util，进入util目录，新建文件 ServerInfo.properties。编辑ServerInfo.properties，配置 server.info信息。例如：server.info=abc，等号后面为不是Tomcat的版本信息内容。保存，重启Tomcat生效。

### 配置Tomcat错误页面重定向

编辑web.xml文件，添加如下内容：

|  |
| --- |
| <!-- 400错误 -->  <error-page>  <error-code>400</error-code>  <location>/err\_400.jsp</location>  </error-page>  <!-- 404 页面不存在错误 -->  <error-page>  <error-code>404</error-code>  <location>/err\_404.jsp</location>  </error-page>  <!-- 500 服务器内部错误 -->  <error-page>  <error-code>500</error-code>  <location>/err\_500.jsp</location>  </error-page>  <!-- java.lang.Exception异常错误,依据这个标记可定义多个类似错误提示 -->  <error-page>  <exception-type>java.lang.Exception</exception-type>  <location>/error.jsp</location>  </error-page>  <!-- java.lang.NullPointerException异常错误,依据这个标记可定义多个类似错误提示 -->  <error-page>  <exception-type>java.lang.NullPointerException </exception-type>  <location>/error.jsp</location>  </error-page>  <error-page>  <exception-type>javax.servlet.ServletException</exception-type>  <location>/error.jsp</location>  </error-page> |

新建err\_400.jsp err\_404.jsp err\_500.jsp exception.jsp等文件，放入../webapps/ROOT目录下，内容分别为：

err\_400.jsp

|  |
| --- |
| <%@ page contentType="text/html; charset=UTF-8" %>  <%@ page import="java.io.\*" %>  <%@ page import="java.util.\*" %>  <html>  <header>  <title>400 page</title>  <body>  <pre>  <%  Enumeration<String> attributeNames = request.getAttributeNames();  while (attributeNames.hasMoreElements())  {  String attributeName = attributeNames.nextElement();  Object attribute = request.getAttribute(attributeName);  out.println("request.attribute['" + attributeName + "'] = " + attribute);  }  %>  </pre> |

err\_404.jsp

|  |
| --- |
| <%@ page contentType="text/html; charset=UTF-8" %>  <%@ page import="java.io.\*" %>  <%@ page import="java.util.\*" %>  <html>  <header>  <title>404 page</title>  <body>  <pre>  <%  Enumeration<String> attributeNames = request.getAttributeNames();  while (attributeNames.hasMoreElements())  {  String attributeName = attributeNames.nextElement();  Object attribute = request.getAttribute(attributeName);  out.println("request.attribute['" + attributeName + "'] = " + attribute);  }  %>  </pre> |

err\_500.jsp

|  |
| --- |
| <%@ page contentType="text/html; charset=UTF-8" %>  <%@ page import="java.io.\*" %>  <%@ page import="java.util.\*" %>  <html>  <header>  <title>500 page</title>  <body>  <pre>  <%  Enumeration<String> attributeNames = request.getAttributeNames();  while (attributeNames.hasMoreElements())  {  String attributeName = attributeNames.nextElement();  Object attribute = request.getAttribute(attributeName);  out.println("request.attribute['" + attributeName + "'] = " + attribute);  }  %>  </pre> |

exception.jsp

|  |
| --- |
| <%@ page contentType="text/html; charset=UTF-8" isErrorPage="true" %>  <%@ page import="java.io.\*" %>  <html>  <header>  <title>exception page</title>  <body>  <hr/>  <pre>  <%  response.getWriter().println("Exception: " + exception);    if(exception != null)  {  response.getWriter().println("<pre>");  exception.printStackTrace(response.getWriter());  response.getWriter().println("</pre>");  }    response.getWriter().println("<hr/>");  %> |