一. 前言

【版权与独立性说明】 1. 本文声明所介绍技术产品是基于北京君云时代科技有限公司进行的研究工作和取得的研究成果，“君云时代”（简称，下同）对本文及相应技术产品内容单独完全享有版权，任何形式的侵权盗用行为将会被依法追究责任。 2. 文中介绍技术流程与操作要点不一定完全体现镜像功能，具体细节以实际操作为准，解释权归“君云时代”所有，欢迎广大用户及技术爱好者参与使用并提出宝贵建议。 3. 如有各类建议及投诉意见，请及时拨打技术支持电话: 4008005185 转10449，我们将真诚为您反馈处理结果。

【公司简介】
北京君云时代科技有限公司成立于 2015 年，是国内内少数几家业务完全基于云计算的服务型 公司， 专注互联网业务，提供一站式运维服务解决方案，包括但不仅限于云上咨询服务、方案设计、系统实施、应用迁移、系统管理、混合云管理，数据中心建设等服务，为企业搭建云计算时代的 IT 基础技术框架及运维服务。我们的使命是帮助企业建立标准化的运维体系促进开发规范，并通过专业的运营分析数据 帮助企业节省成本，创造更多的业务营收，从而真正帮助企业有效的使用云计算和大数据， 实现运维真正的价值。

【联系我们】

1. 公司地址：
   北京市朝阳区大望路 SOHO 现代城 5 号楼 1002
2. 公司网站：
   http://www.cldera.com
3. 通讯联络：
   电话技术支持: 4008005185 转 10449

二. 产品属性

产品亮点

> 相较于普通版本的JAVA运行环境镜像，安全加固的镜像，锁定了系统用户的，修改应用程序的权限，关闭部分应用程序自启、关闭SELinux、ip6tables，限制ssh最大登录次数,禁止DNS反向解析，配置了时间同步、DNS服务器解析地址以及编译环境。

产品说明

- 功能亮点
  1. Tomcat以及JDK采用源码编译安装，软件的安装目录集中在/usr/local/src下，并在/usr/local/下有java与tomcat的软连接，便于配置，灵活性高
  2. 镜像部署了最新版本的环境：CentOS7.4，Nginx1.13，Tomcat8，JDK8，MariaDB10.1

3. 采用了Nginx反代Tomcat的方式，性能更加高效，适用于对性能要求较高的站点。1. 锁定系统用户密码，比如ftp，shuitdown等
4. 限制所有用户的最大进程数为16384，超出10240会发出警告。
5. 限制所有用户能打开文件的最大数目为65535个，超出10240会发出警告。
6. 限制重要程序权限，finger、who、locate、whereis、ifconfig、编译、rpm安装，其命令执行权限为700，只有root用户才有执行权限
7. 禁止删除/root/.bash_history文件内容以及文件本身，只能够对其进行追加操作。便于在排查误操作或是其他恶意行为
8. 关闭SELinux
9. 自动同步时间、添加了DNS服务器地址
10. ssh最大登录次数为6，禁止DNS反向解析

- 售后支持

> 5*8旺旺在线技术支持
> 支持范围：初始环境，JDK、Tomcat、Nginx不能正常使用，如有任何配置修改，不在售后支持范围
> 业务范围：服务器环境配置，故障排查（不含程序自身问题），数据库配置更改，数据库权限、账户，数据迁移，程序迁移，数据库故障排查等； 费用范围：详情参照本公司服务类商品定价，或咨询在线技术支持。

- 关于阿里云控制台使用方法请下载获取镜像通用手册，下载链接：http://pan.baidu.com/s/1sllpaZr，里面有详细的使用说明，如需技术讨论可访问阿里云技术交流论坛http://bbs.cldera.com/forum-59-1.html。

三. Tomcat镜像使用指南

1. 产品参数

交付方式	镜像
基础系统	CentOS7.4
可用区域	华北 1, 华北 2, 华北 3, 华东 1, 华东 2, 华南 1, 华南 1 金融云

2. MariaDB初始化以及密码更改、远程访问

```
##初始化
mysql_secure_installation
Enter current password for root (enter for none):<-初次运行直接回车
Set root password? [Y/n] <- 是否设置root用户密码，输入y并回车或直接回车
New password: <- 设置root用户的密码
Re-enter new password: <- 再输入一次你设置的密码
Remove anonymous users? [Y/n] <- 是否删除匿名用户,生产环境建议删除，所以直接回车
Disallow root login remotely? [Y/n] <-是否禁止root远程登录,根据自己的需求选择Y/n并回车,建议禁止
Remove test database and access to it? [Y/n] <- 是否删除test数据库,直接回车
Reload privilege tables now? [Y/n] <- 是否重新加载权限表，直接回车

##远程访问
mysql -uroot -pPASSWORD -hIP
use mysql;
update user set host='%' where user='root';
flush privileges;
```

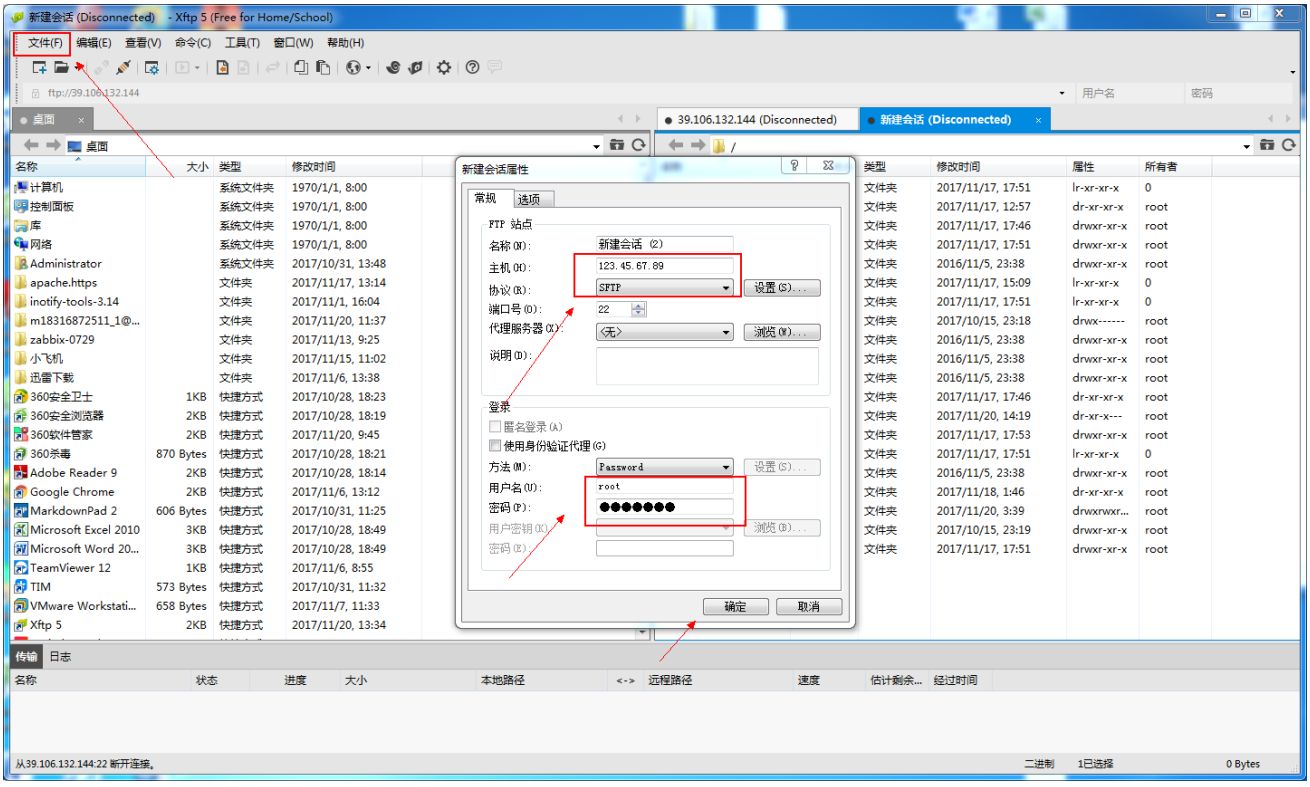
```
##简单配置示例
vim /etc/my.cnf.d/server.cnf
    [mysqld]
    datadir=/data/mysql/                        #自定义目录位置
    socket=/var/lib/mysql/mysql.sock
    #default-character-set=utf8
    character_set_server=utf8
    slow_query_log=on
    slow_query_log_file=/usr/local/ieternal/mysql_data/slow_query_log.log
    long_query_time=2
    ...
```

3. MySQL基本操作

连接	`mysql -uUSER -pPASSWORD -hIP`
创建库	`CREATE DATABASE <数据库名>;`
创建表	`CREATE TABLE <表名> (<字段名1> <类型1> [,..<字段名n> <类型n>]);`
创建用户并授权	`CREATE USER 'username'@'host' IDENTIFIED BY 'password';`
授权	`GRANT privileges ON databasesname.tablename TO 'username'@'host'`

4. Ftp使用方法

- 首先下载xftp软件，打开，界面的左上角进入新建，选择sftp并输入账号密码，IP地址为服务器IP，若无法连接，请检查防火墙以及安全组策略



5. 软件目录以及配置列表

- Nginx配置文件：`/etc/nginx/nginx.conf` , `/etc/nginx/conf.d/`
- Tomcat目录：`/usr/local/tomcat/ --> /usr/local/src/apache-tomcat-8.5.23`
- Tomcat默认网站目录：`/usr/local/tomcat/webapps/`
- MySQL数据库目录：`/var/lib/mysql`
- MySQL配置文件：`/etc/my.cnf`
- 查看Nginx以及Mysql相应文件的方法：`rpm -ql nginx` , `rpm -ql MariaDB-server`

6. 日志目录

- Nginx日志目录：`/var/log/nginx/ error.log` , `/var/log/nginx/access.log`

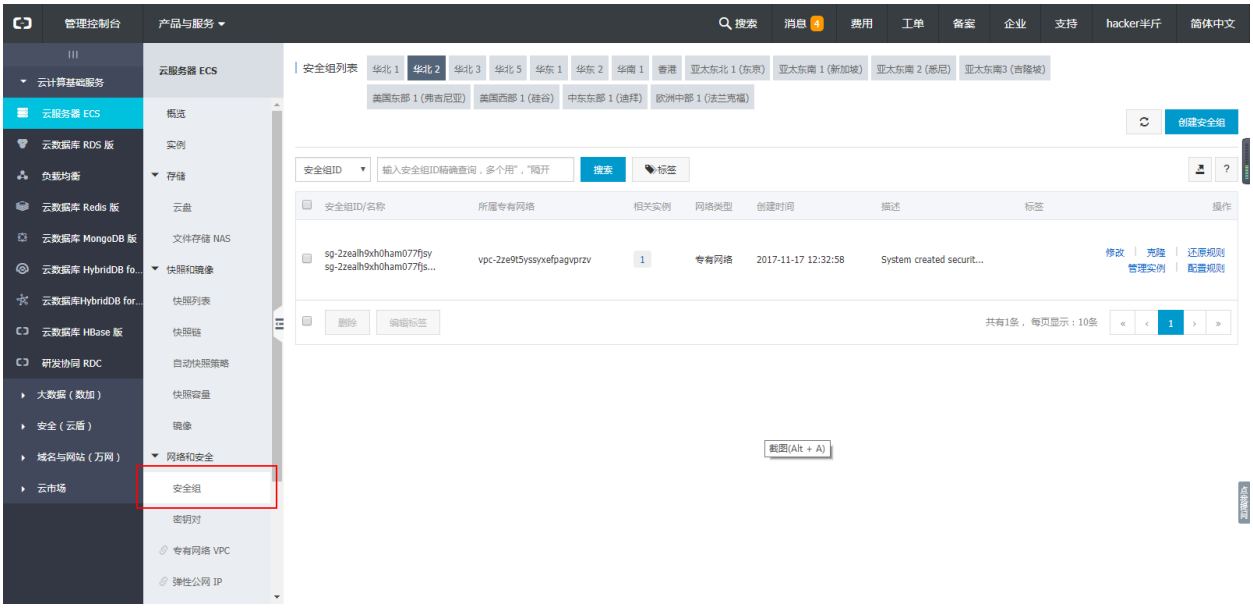
四. 软件操作命令汇总

- 启停方式，配置文件

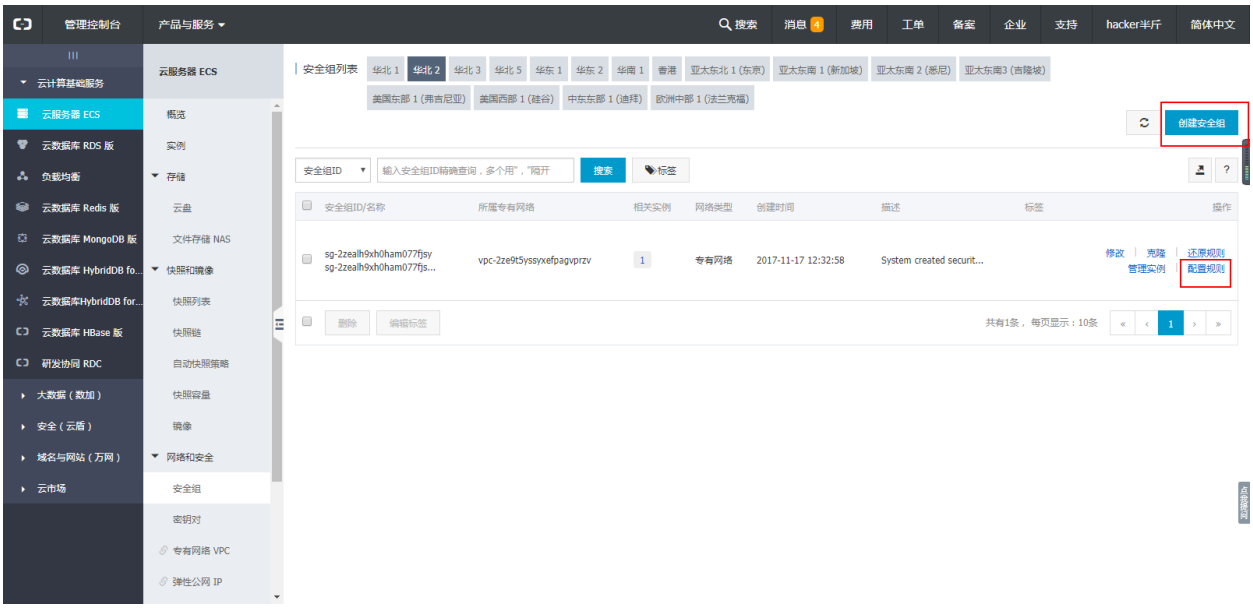
应用程序	Nginx	Tomcat	JDK	MySQL
配置文件路径	`/etc/nginx/`	`/usr/local/tomcat/`	`/usr/local/java/`	`/etc/my.cnf.d/server.cnf`
启动方式	`systemctl start nginx`	`service tomcat start`		`systemctl start mysql`
停止方式	`systemctl stop nginx`	`service tomcat stop`		`systemctl stop mysql`

- 阿里云安全组操作

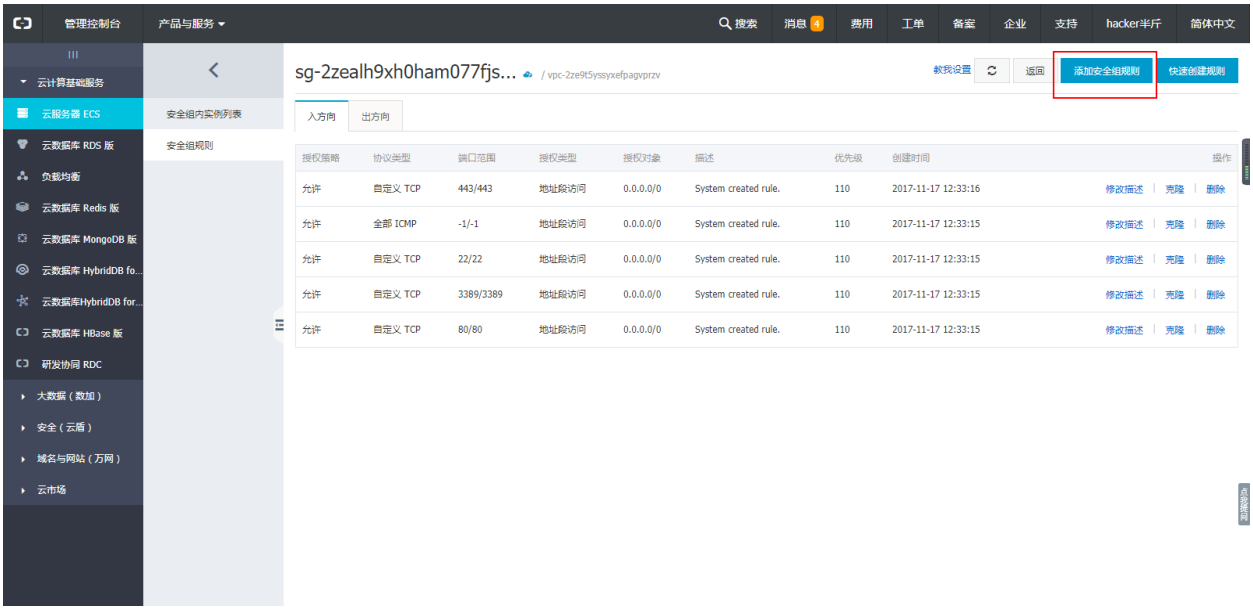
- 进入



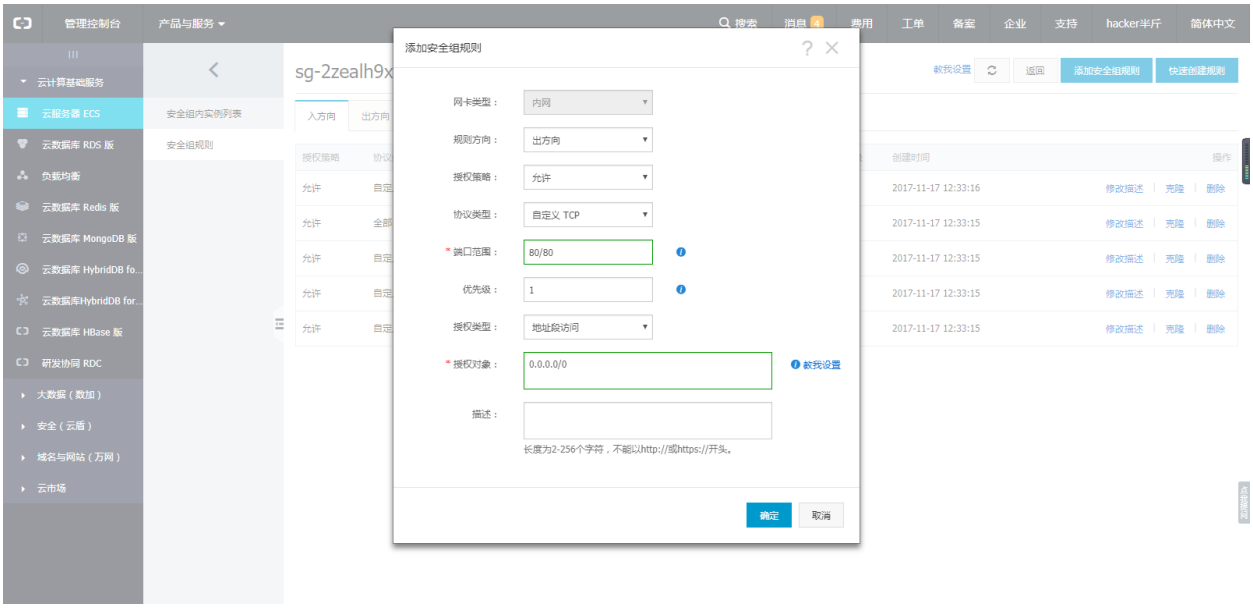
- 创建与配置



- 添加规则



- 实例：当外网无法访问网站，配置安全组端口策略，增加入、出方向80端口



- xshell登录方式

  首先下载xmanger，进入软件操作界面后执行如下命令，IP请替换为您的公网地址

  `ssh root@IP`

五. 附录

部署项目

- 在使用镜像安装系统之后，在/etc/nginx/conf.d/目录下，我们可以看到一个默认的配置文件，default.conf 。关于如何配置网站，我们可以参考该文件中的内容（#号后面为注释说明）：

```
server {
      listen       80 default;                  #默认监听80端口
      server_name  _;                           #默认ip/域名都可访问
      index index.html index.htm index.jsp;             #定义索引文件的名称
      root /alidata/www/default;                        #定义服务器的默认网站根目录位置
      location / {
          proxy_pass     http://127.0.0.1:8080;         #因为是JAVA运行环境，所以直接代理到8080端口
      }

      location ~ .*\.(gif|jpg|jpeg|png|bmp|swf)$ {
           expires 30d;
      }
      location ~ .*\.(js|css)?$ {
           expires 1h;
      }
      access_log  /alidata/log/nginx/access/default.log;
}
```

  - 因为是JAVA运行环境，所以JAVA项目应该在tomcat相印的位置运行以及配置

```
##找到server.xml

vim /usr/local/tomcat/conf/server.xml
```

```
<Server>        #顶层元素，代表一个服务器
    <Service>   #顶层元素，是Connector的集合，只有一个Engine
        <Connectior/>         #连接器类元素，代表通信接口
            <Engine>         #容器类元素，为特定的Service组件处理所有客户请求，可包含多个Host
                <Host>    #为特定的虚拟主机处理所有客户请求
                    <Context>     #为特定的WEB应用处理所有客户请求
                    </Context>
                </Host>
            </Engine>
    </Service>
</Server>
##TOMCAT中真正处理客户请求与生成响应的三个组件是Engine 、Host、 Context
```