



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。 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、iptables，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：Ubuntu16，Nginx1.12，Tomcat9，JDK8，MySQL5.7
 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	Ubuntu16
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. MySQL初始化以及密码更改、远程访问

- Mysql5.7版本与之前版本有许多不同之处，在安装mysql时会生成一个随机字符串作为连接密码
 - 连接数据库

```
mysql -uroot -pJUNyun@3210 #JUNyun@3210为安装时配置的初始密码
```

- 修改数据库密码

```
##首先需要连接数据库，再使用mysql库
mysql -uroot -pJUNyun@3210
use mysql;
update user set authentication_string = password('Ej7VxkEkF,q') where user='root' and host='localhost';
##将JUNyun@3210 替换为想要更改的字符串即可
```

- mysql账号密码忘记时的修改方法

```
vim /etc/my.cnf #编辑配置文件
skip-grant-tables=1 #在[mysqld]下添加之后保存退出
systemctl restart mysqld #重启mysql让配置文件生效
mysql #在命令行下直接执行mysql
##登录之后再行上面的修改密码方法即可
```

- 初始化

```
mysql_secure_installation #在命令行执行初始化命令
Securing the MySQL server deployment.
```

```

Enter password for user root:          #输入密码, JUNyun@3210
Change the password for root ? ((Press y|Y for Yes, any other key for No) :      #是否更改root用户密码, Y为是, N为否
New password:                          #新密码, 密码字符串是不会在命令行显示的, 所以保证输入正确即可
Re-enter new password:                  #再确认一次输入的密码, 同上
Do you wish to continue with the password provided?(Press y|Y for Yes, any other key for No) :      #您希望继续吗? (按y|Y为Yes, 任何其
Remove anonymous users? (Press y|Y for Yes, any other key for No) :              #删除匿名用户?(按y| y为Yes, 任何其他
Disallow root login remotely? (Press y|Y for Yes, any other key for No) :        #不允许远程root登录吗?(按y| Y为Yes, 任何其他
Remove test database and access to it? (Press y|Y for Yes, any other key for No) :      #删除测试数据库并禁用对其的访问
Reload privilege tables now? (Press y|Y for Yes, any other key for No) :          #现在重新加载权限表吗?(按y| y为Yes, 任何其他

##尝试用新密码登录数据库
mysql -uroot -pJUNyun@1230.com          #JUNyun@1230.com为更改的密码字符串

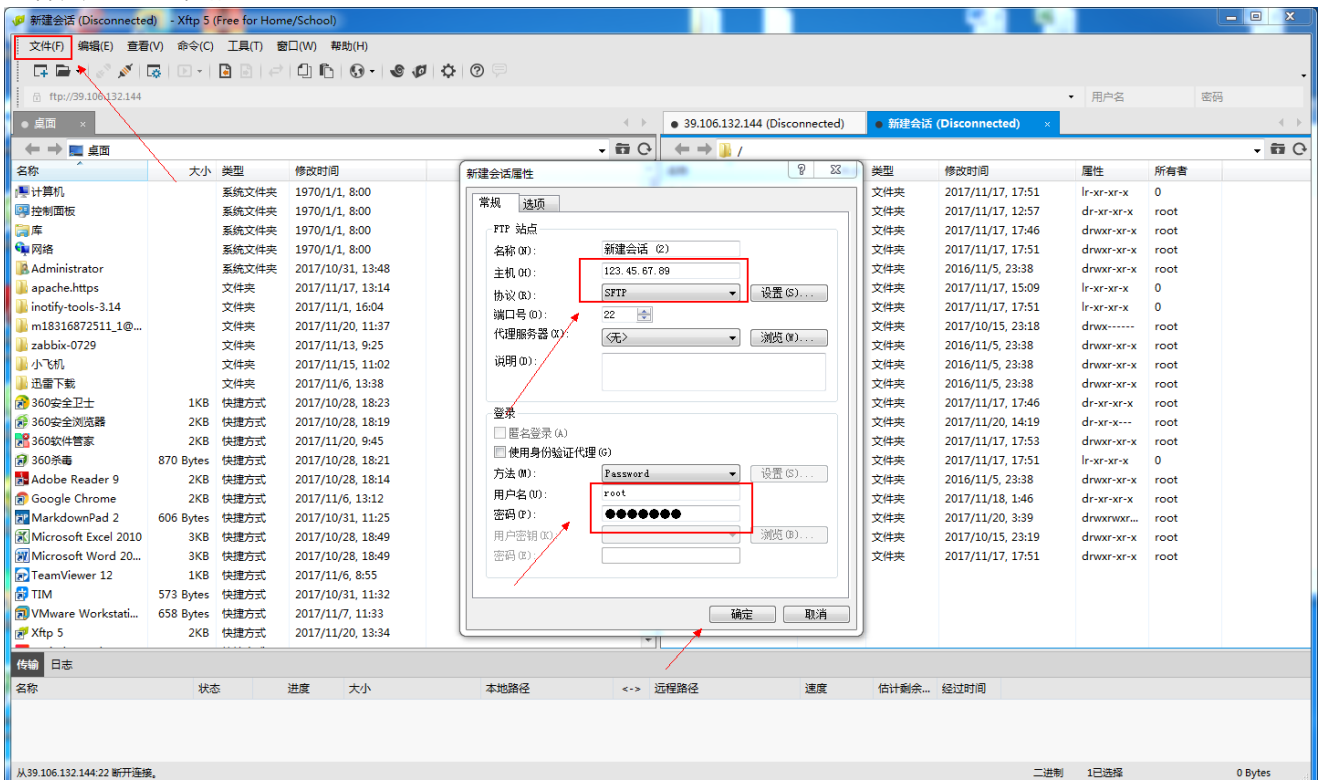
```

3. MySQL基本操作

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

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默认网站目录：`/usr/local/tomcat/webapps/`
Tomcat目录：`/usr/local/tomcat --> /usr/local/src/apache-tomcat-9.0.1`
MySQL数据库目录：`/var/lib/mysql`
MySQL配置文件：`/etc/mysql/mysql.conf.d/mysql.cnf`
查看Nginx以及Mysql相应文件的方法：`find / -name "nginx*" find / -name "mysql*"`

6. 日志目录

- Nginx日志目录：`/var/log/nginx/ error.log` , `/var/log/nginx/access.log`
- MySQL日志目录：`/var/log/mysql.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	<code>/etc/nginx/</code>	<code>/usr/local/tomcat/</code>	<code>/usr/local/java/</code>	<code>/etc/mysql/mysql.conf.d/mysql.cnf</code>
启动方式	<code>systemctl start nginx</code>	<code>service tomcat start</code>		<code>systemctl start mysql</code>
停止方式	<code>systemctl stop nginx</code>	<code>service tomcat stop</code>		<code>systemctl stop mysql</code>

- 阿里云安全组操作

。 进入

管理控制台 产品与服务 搜索 消息 费用 工单 备案 企业 支持 hacker半斤 简体中文

云服务器 ECS 安全组列表 华北1 华北2 华北3 华北5 华东1 华东2 华南1 香港 亚太东北1(东京) 亚太东南1(新加坡) 亚太东南2(悉尼) 亚太东南3(吉隆坡) 美国东部1(弗吉尼亚) 美国西部1(硅谷) 中东东部1(迪拜) 欧洲中部1(法兰克福)

安全组ID 输入安全组ID精确查询, 多个用“,”隔开 搜索 标签

安全组ID/名称	所属专有网络	相关实例	网络类型	创建时间	描述	操作
sg-2zeal9xh0ham077fjsy sg-2zeal9xh0ham077fjs...	vpc-2ze9l5yssyxfpavprzv	1	专有网络	2017-11-17 12:32:58	System created securit...	修改 克隆 还原规则 管理实例 配置规则

共有1条, 每页显示: 10条

删除 编辑标签

视图(Alt + A)

。 创建与配置

管理控制台 产品与服务 搜索 消息 费用 工单 备案 企业 支持 hacker半斤 简体中文

云服务器 ECS 安全组列表 华北1 华北2 华北3 华北5 华东1 华东2 华南1 香港 亚太东北1(东京) 亚太东南1(新加坡) 亚太东南2(悉尼) 亚太东南3(吉隆坡) 美国东部1(弗吉尼亚) 美国西部1(硅谷) 中东东部1(迪拜) 欧洲中部1(法兰克福)

安全组ID 输入安全组ID精确查询, 多个用“,”隔开 搜索 标签

安全组ID/名称	所属专有网络	相关实例	网络类型	创建时间	描述	操作
sg-2zeal9xh0ham077fjsy sg-2zeal9xh0ham077fjs...	vpc-2ze9l5yssyxfpavprzv	1	专有网络	2017-11-17 12:32:58	System created securit...	修改 克隆 还原规则 管理实例 配置规则

共有1条, 每页显示: 10条

删除 编辑标签

视图(Alt + A)

。 添加规则

管理控制台 产品与服务 搜索 消息 费用 工单 备案 企业 支持 hacker半斤 简体中文

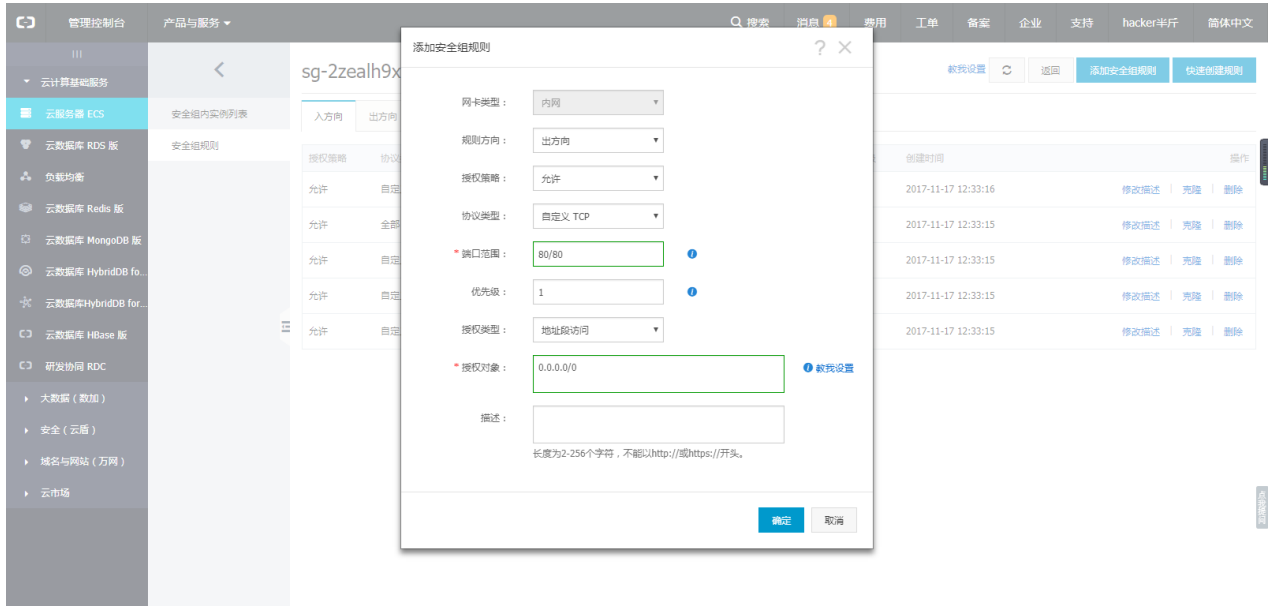
云服务器 ECS 安全组实例列表 安全组规则

sg-2zeal9xh0ham077fjsy... / vpc-2ze9l5yssyxfpavprzv 快捷设置 返回 添加安全组规则 快速创建规则

入方向 出方向

授权策略	协议类型	端口范围	授权类型	授权对象	描述	优先级	创建时间	操作
允许	自定义 TCP	443/443	地址段访问	0.0.0/0	System created rule.	110	2017-11-17 12:33:16	修改描述 克隆 删除
允许	全部 ICMP	-1/-1	地址段访问	0.0.0/0	System created rule.	110	2017-11-17 12:33:15	修改描述 克隆 删除
允许	自定义 TCP	22/22	地址段访问	0.0.0/0	System created rule.	110	2017-11-17 12:33:15	修改描述 克隆 删除
允许	自定义 TCP	3389/3389	地址段访问	0.0.0/0	System created rule.	110	2017-11-17 12:33:15	修改描述 克隆 删除
允许	自定义 TCP	80/80	地址段访问	0.0.0/0	System created rule.	110	2017-11-17 12:33:15	修改描述 克隆 删除

- 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xmanager，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
```

```
<Connector/> #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