CloudStack故障排查手册

# 1.网络问题

## 1.1 VLAN配置

### 1.1.1高级隔离网络

如果使用Advanced区域配置，并使用Isolated隔离模式，则来宾流量类型的起止vlan段必须配置，否则在部署虚拟机时将会因为无法为来宾网络分配vlan号而失败。修改位置如下：



### 1.1.2 Hypervisor支持

如果在配置物理网络时使用了Hypervisor流量标签的功能，则必须保证相应Hypervisor主机的网络配置上已经有相应标签，否则将导致主机添加失败。



## 1.2安全组

### XenServer中使用安全组

如果XenServer版本高于或等于6.1，不需要进行额外的补丁即可支持安全组。

如果XenServer版本小于6.1，默认不支持安全组设置，需要管理员手动在每台XenServer主机上安装CloudStack Securitygroup Package，即CSP安全组支持包。这个软件包可以在官方网站下载到，或者直接在Google或百度中搜索xenserver-cloud-supp。

下载地址

XenServer 6.0.2:

<http://download.cloud.com/releases/3.0.1/XS-6.0.2/xenserver-cloud-supp.tgz>

XenServer 5.6 SP2:

<http://download.cloud.com/releases/2.2.0/xenserver-cloud-supp.tgz>

XenServer 6.0:

<http://download.cloud.com/releases/3.0/xenserver-cloud-supp.tgz>

如果XenServer版本高于或等于6.1，XenServer的CSP已经默认集成到了安装ISO文件中。

安装时，解压tar包并安装

tar xf xenserver-cloud-supp.tgz

xe-install-supplemental-pack xenserver-cloud-supp.iso

需要手动在主机上关闭OVS（Open vSwitch），执行如下命令，完成后重启主机。

xe-switch-network-backend bridge

如果使用XenServer6.1，还需要执行下列命令

echo 1 > /proc/sys/net/bridge/bridge-nf-call-iptables

echo 1 > /proc/sys/net/bridge/bridge-nf-call-arptables

保存配置，避免重启后失效。

sysctl -p /etc/sysctl.conf

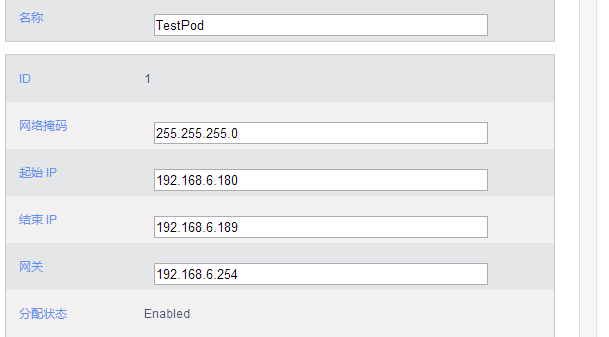
修改配置如下

net.bridge.bridge-nf-call-iptables = 1

net.bridge.bridge-nf-call-arptables = 1

## 1.3主机网络配置

创建Zone时，指定的管理网络cidr，必须包含Hypervisor主机的IP，否则将导致主机添加失败，可以通过修改Pod详情界面进行修改。



# 2.主机连接问题

## 2.1 Hypervisor

### 2.1.1 XenServer

同一个XenServer集群中的所有Hypervisor主机应当保持license的一致，并且license没有过期，否则将无法添加和连接XenServer主机。

### 2.1.2 KVM

KVM主机连接时通过cloud-agent服务，所以保证KVM主机上的cloud-agent服务开机启动，并且能够正常运行。包括相关联的libvirtd、cggroup、cfconfig等服务，也要配置成开机启动。

## 2.2系统虚拟机

系统虚拟机与管理节点之间的通信通过8250端口实现，同时NFS等服务也需要开放相应端口。测试时可以直接关闭防火墙，但实际环境中，必须操作官方安装指南，配置iptables，打开特定范围内的端口。

系统虚拟机密码：CloudStack4.2.x之前版本，系统虚拟机默认用户名/密码为

root/6m1ll10n

CloudStack4.3的系统虚拟机升级为64位（必须升级，否则无法创建虚拟机），系统虚拟机默认用户名/密码为

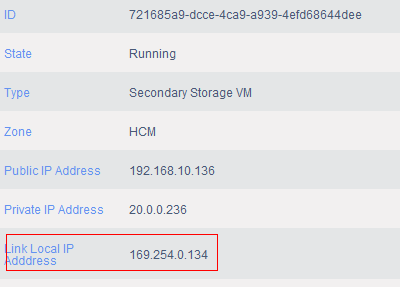
root/password

### 远程连接系统虚拟机

系统虚拟机的SSH服务默认端口为3922，并且只能使用公钥方式远程登录，如果是XenServer或者KVM主机，在Hypervisor主机上执行如下命令即可登录：

ssh -i /root/.ssh/id\_rsa.cloud -p 3922 root@CONTROL IP

上面的CONTROL IP对应虚拟机的控制网卡IP，一般是UI上的链接本地地址，

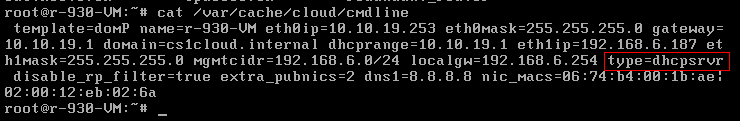
 

对SSVM和CPVM，如果链接本地地址为空，可以使用私有IP地址进行连接

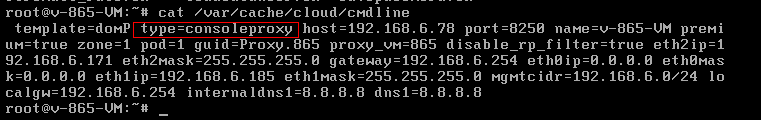
### 系统虚拟机的初始化配置

系统虚拟机模板中定制了cloud-early-config开机启动服务，它通过检测系统虚拟机所在的Hypervisor，根据Hypervisor的不同按照不同的方式获得虚拟机的启动参数，根据启动参数中的配置，将系统虚拟机配置成不同类型。这个启动参数最终会持久化保存到系统虚拟机内部的/var/cache/cloud/cmdline中，供系统虚拟机的相关服务启动时使用。

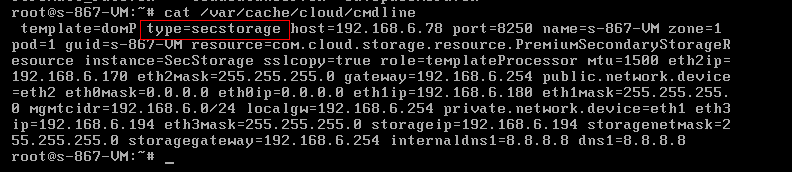
vRouter的启动参数



CPVM的启动参数



SSVM的启动参数



## 2.3二级存储

二级存储的连接状态依赖于SSVM的运行，当SSVM启动出现问题或者SSVM的网络出现故障时，二级存储可能无法使用。

如果二级存储的状态为Alert，一般情况下不影响虚拟机的创建和使用。

# 3.vRouter问题

## 3.1 DHCP&DNS

来宾网络中虚拟机的DHCP和DNS默认由vRouter提供，通过dnsmasq服务提供小型内网的DHCP。其配置文件为/etc/dhcphosts.txt和/etc/dhcphopts.txt，并将用户虚拟机的主机名与IP的映射记录到了/etc/hosts，供DNS使用。

当虚拟机无法获取IP或者网络出现问题时，可以检查dnsmasq服务是否正常工作。

## 3.2重置密码

CloudStack中虚拟机的密码操作通过vRouter作为中转，当虚拟机的模板启动密码时，通过管理节点的脚本调用，将密码保存在vRouter的/var/cache/cloud/passwords文件中，并通过socat启动服务监听用户虚拟机的请求，当虚拟机启动完成并且到vRouter的网络通畅后，通过cloud-set-guest-password服务向vRouter请求密码，并设置到本虚拟机上，设置成功后，通知vRouter将密码设置为saved\_password。

因此，如果虚拟机的密码设置失败时，首先检查vRouter的网络是否正常工作，并且保证vRouter和用户虚拟机之间的网络是通畅的。

## 3.3 userdata

在CloudStack中，虚拟机的某些用户自定义加密数据是通过vRouter进行转发的，当vRouter支持userdata服务时，vRouter会在虚拟机启动时，根据管理节点发来的命令，将虚拟机的用户信息保存到相应目录。用户虚拟机启动完成后，可以直接通过HTTP请求，将自己的数据取回来，并且vRouter会自动根据请求者的IP保证用户虚拟机只能拿到自己的userdata，而不会是别人的userdata，保证了安全性。

参考

<http://note.youdao.com/share/?id=093a6a7209688b9212b79b4c88bda311&type=note>

# 4.虚拟机启动问题

虚拟机部署时最常出现的异常就是Unable to create a

deployment for VM，但实际的异常原因是多方面的，例如：

cpu、内存、主存储的空闲容量及阈值限制；

主机状态；

网络可用性和剩余IP；

vRouter、SSVM是否正常工作；

VC、XenServer等API工作超时。

如果出现了这个错误，可以参考第5章的日志分析过程，自行分析下原因，再找开发人员处理。

# 5.日志分析过程说明

## 5.1日志位置及作用

### 5.1.1管理节点日志

/var/log/cloud/management目录有以下重要日志文件

localhost.log，CloudStack自带的tomcat的启动日志。如果将SkyFormRes、mcloud、rsg等包部署到CloudStack启动目录导致CloudStack服务无法启动，可以从这个日志开始分析。

api-server.log，CloudStack的所有API请求及响应的记录日志，作用不是很大。

management-server.log，CloudStack管理节点的核心日志，记录了完整的功能执行日志。

catalina.out，CloudStack的完整日志，在management-server.log的基础上，一般会多出一些异常信息供分析使用。

管理节点上还有一个日志/var/log/cloud/setupManagement.log，但意义不大，是记录管理节点安装过程的日志。

### 5.1.2Hypervisor主机

XenServer，/var/log/SMlog目录，xensource.log记录从管理节点发来的API请求及执行过程的日志。

KVM，/var/log/cloud/agent目录下主要日志为agent.log，一般是KVM使用的，记录了KVM agent的执行日志，可用于分析KVM故障问题

同时/var/log/cloud/setupAgent.log，类似管理节点的安装日志，记录了agent的安装过程，可以用于分析KVM主机的可用性（如网络、服务、安全组等设置的准备是否完成）。

/var/log/libvirt/libvirtd.log，libvirt的运行日志，可以用于辅助分析。

VMWare，可以直接从vSphere上看日志。

### 5.1.3系统虚拟机日志

系统虚拟机上的日志有如下三个位置。

/var/log/cloud/cloud.out：服务启动日志，如果cloud服务无法启动，通常可以在这里找到出错原因

/var/log/cloud.log：cloud服务的配置日志，根据CPVM、SSVM、vRouter的角色不同（从cloud-early-config脚本入手分析），进行不同的业务配置

/usr/loca/cloud/system/cloud.log：系统虚拟机执行业务、与管理节点通信的日志记录。

/var/log/messges：系统虚拟机在执行脚本时（主要是vRouter），会将DHCP设置、密码设置等操作的通信日志记录在系统日志中，

/var/log/dnsmasq：vRouter使用，提供DHCP、DNS等服务时的工作日志

## 5.2分析过程

主要从management-server.log中进行分析。

### 5.2.1关键词

WARN, ERROR, Exception, Unable, Failed

虚拟机的主机名，这是因为在日志记录中，通畅使用虚拟机的主机名（i-账户ID-虚拟机ID-VM）而不是显示名。

UI上显示的错误信息，一般情况下UI上显示的错误信息可以直接在日志中找到相应的记录，根据错误信息向前翻阅一些行数，可以找到为什么出现了错误信息。

Type of task that failed，这种信息通常是调用Vmware或者XenServer的API时产生的，比较容易定位出问题。

avoid set，这个错误出现在部署虚拟机时。当发现avoid set后，首先检查avoid set里面的主机、集群是否确实资源不足或者资源使用打到阈值上限，然后在出现avoid set日志的更前面几行，一般都可以找到这个集群、主机为什么在avoid set中。

### 5.2.2分析过程demo

比如说，销毁虚拟机时在UI上出现，



根据这条异常信息，搜索managementserver.log，找到相应的jobid

2014-07-24 04:11:08,193 DEBUG [cloud.async.AsyncJobManagerImpl] (Job-Executor-16:**job-733**) Complete async job-733, jobStatus: 2, resultCode: 530, result: Error Code: 530 Error text: Failed to destroy vm with specified vmId

根据**job-733**，从头搜索managementserver.log，从任务开始执行检查日志。一般，异步任务是这样开始的

2014-07-24 04:11:08,093 DEBUG [cloud.async.AsyncJobManagerImpl] (catalina-exec-25:null) **submit async job-733**, details: AsyncJobVO {id:733, userId: 2, accountId: 2, sessionKey: null, instanceType: null, instanceId: 940, cmd: com.cloud.api.commands.DestroyVMCmd, cmdOriginator: null, cmdInfo: {"response":"json","id":"940","sessionkey":"dI1jJoW6/yIfI/xhAiTfm1FMogM\u003d","ctxUserId":"2","\_":"1406189948366","ctxAccountId":"2","ctxStartEventId":"7462"}, cmdVersion: 0, callbackType: 0, callbackAddress: null, status: 0, processStatus: 0, resultCode: 0, result: null, initMsid: 345051249244, completeMsid: null, lastUpdated: null, lastPolled: null, created: null}

2014-07-24 04:11:08,166 DEBUG [cloud.async.AsyncJobManagerImpl] (Job-Executor-16:job-733) **Executing** com.cloud.api.commands.DestroyVMCmd **for job-733**

再向下搜索，直到找到异常Exception等关键字信息。

2014-07-24 04:11:08,182 WARN [cloud.vm.VirtualMachineManagerImpl] (Job-Executor-16**:job-733**) **Unable to stop vm VM**[User|i-2-940-VM]

2014-07-24 04:11:08,188 DEBUG [cloud.capacity.CapacityManagerImpl] (Job-Executor-16:job-733) VM state transitted from :Stopping to Running with event: OperationFailedvm's original **host id: 49** new host id: 49 host id before state transition: 49

从日志信息可以看出，ID为49的Hypervisor主机可能是问题根源，从CloudStack的界面上找到ID为49的主机，发现它的状态为Disconnected



剩下的就是检查主机为什么是Disconnected了。

# 6.常见异常

## 6.1 管理节点服务启动异常

### 6.1.1：清除所有日志后重启服务失败

/usr/sbin/tomcat6: line 30: /usr/share/cloud/management/logs/catalina.out: Permission denied

在清除所有日志文件后，偶尔会出现这个问题，chmod 777 catalina.out之后，重启管理节点服务即可服务。

### 6.1.2：使用hostname命令临时修改主机名，无法再启动

如果使用命令hostname临时修改主机名使CloudStack安装成功，下次启动时，就有可能导致CloudStack服务启动时因为主机名设置问题而启动失败，出现如下问题

net.sf.ehcache.CacheException: Unable to create CacheManagerPeerListener. Initial cause was localhost.localhost.cn: localhost.localhost.cn

修改/etc/hosts、/etc/sysconfig/network文件中的主机名，并通过hostname命令临时使主机名生效，再次验证，如果启动成功，则重启机器。

### 6.1.3 数据库问题导致无法启动

如果服务在成功启动，但经过若干秒之后进程死掉了，通过命令

service cloud-management status

可以发现OS要求清理process dead，but pid exists

通过查看catalina.out日志，可以发现如下错误

Unexpected exception:

com.mysql.jdbc.exceptions.jdbc4.MySQLNonTransientConnectionException: Could not create connection to database server. Attempted reconnect 3 times. Giving up.

通常的原因是数据库服务没有正常启动或配置不正确

service mysqld restart重新启动服务

将mysqld配置成开机启动，并且保证配置的用户名密码可以远程访问数据库

### 6.1.4配置文件缺失导致无法启动

如果出现

Starting cloud-management: /etc/rc.d/init.d/tomcat6 line 191: /var/log/cloud-management/initd.log No Such File

错误。可以直接在在对应目录下创建一个空文件，然后重启服务即可。

## 6.2 模板问题

1、上传或下载模板时，可能会发生无法Connection Refuse或者连接不到网页之类的错误，发生此类错误，如果保证网络通畅，则可能是由于全局配置中的 secstorage.allowd.internal.sites 没有添加相关网络范围导致。

解决方案：在全局配置中加入相关设置，重启ms，将相关zone的ssvm破坏掉，等待系统重建ssvm

2、网络畅通，secstorage.allowd.internal.sites 正确配置，但是依然无法上传或下载模板，可能的原因是由于ssvm 的多个网卡都在同一网络中，会有几率导致route表中只有第一项可以正常通信，其他网卡arp无响应。此时状态是ping ssvm的public ip会不通

解决方案：重启ssvm可以恢复网卡通信

3、网络畅通，secstorage.allowd.internal.sites 正确配置，也可以ping通public ip，但是依然无法下载模板，提示权限错误，可能是由于db中的链接未过期删除，手动删除update表中的相关链接，然后重新登录UI点击下载模板，可以生成新的url并更新到update表中。

## 6.3系统虚拟机问题

### 6.3.1 系统虚拟机无法创建

系统虚拟机无法创建，通常都是系统虚拟机模板的问题。如果主机、主存储、二级存储的状态都是Up，则检查template、template\_host\_ref和template\_spool\_ref，storage\_pool\_host\_ref，保证系统虚拟机创建的前提都是满足的。

### 6.3.2 SSVM或者vRouter一直Starting，而VC上已经Running

SSVM如果一直是Starting，并且没有自动重建，一般是因为使用的通信端口8250被封闭导致的，关闭防火墙试试。

vRouter一直Starting，有可能是使用的来宾网络的vlan没有在交换机上进行配置，导致vlan无法使用，有时删除路由规则可以解决问题。

# 参考资料

《CloudStack安装-故障排查-英文版》，**有更多的分析例子**

《CloudStack中国社区[共享资料](http://www.cloudstack-china.org/materials)》，**常见异常的绝大多数来源**

《cloudstack常见问题解答-20130123-ChinaCloud》