**RH318红帽虚拟化**

**Day01**

1. **虚拟化、云计算、容器docker之间的比较？**

docker容器：直接运行在系统上，本质上是一个进程。

虚拟化：在物理主机上启用有限资源，假定虚拟机长期使用

云计算：把计算资整合，形成资源池，假定虚拟机是有使用期限

1. **红帽虚拟化**
2. 名称：
   1. RHEV（红帽企业级虚拟化）、
   2. RHV（红帽虚拟化）
3. 虚拟化中，物理主机被称作Host，虚拟机被称作Guest
4. **红帽虚拟化安全认证**
5. 安全通信概念
   1. 认证：
   2. 加密：

1. 对称加密：加解密算法和密钥一样。DES/3DES/AES。加密效率高；密钥传输、保管不方便。

2. 非对称加密：公钥加密、私钥解密。RSA。密钥传输、保管方便。加密效率低。

3. 单向加密：哈希md5、sha。数据加密，只能向一个方向进行。相同的原始数据，总是得到长度相同的乱码。可用于存储加密密码、数据完整性校验。

4. 证书包含：服务器公钥、服务器信息（公司名、FQDN）、证书颁发机构CA的信息

1. SSO: Single Sign On单一登陆，一处登陆，多处授权
2. AAA:
   * 1. Authentication：认证
     2. Authorization：授权
     3. Audit：审计
3. **RHV组件：**

DNS:独立于RHV环境，classroom。

RHVM: Manager管理端

RHVH: Host

NIC（网卡）：至少有一块1G带宽网卡，推荐2块以上。

1. **部署配置**

需要启动classroom、utility和workstation。启动必须的虚拟机

$ rht-vmctl status all

$ rht-vmctl start workstation

$ rht-vmctl start utility

$ rht-vmctl start rhvm

如果虚拟机有故障，可以彻底重置：

$ rht-vmctl fullreset workstation

在rhvm上安装软件包

$ ssh root@rhvm

# cd /etc/yum.repos.d/

# wget http://materials.example.com/rhvm.repo

# yum repolist enabled => 6035

# yum update -y

# yum install -y rhevm

启动安装过程

# engine-setup

大多数的问题都采用默认值，直接回车即可，密码设置为redhat，询问是否继续使用Weak弱密码，回答Yes

安装完RHVM后，信任CA：打开浏览器，输入以下内容：

rhvm.lab.example.com/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA

1. **在serverd上安装宿主机软件**

安装首页选第一项Install RHVH4.1

时区Region->Etc; City选第一项

键盘选择美国英语式键盘

分区选择自动

网络->eth0点击On按钮，再点击Configure->General->Automatically Connect勾选

Host name: serverd.lab.example.com ->Apply

注意：一定要启动utility这台虚拟机，否则serverd获取不到IP地址

安装时，把root密码设置为redhat

安装完毕后，点击reboot，重启后，出现菜单按ESC，输入local从本地启动，启动后以root身份登陆，然后shutdown -h now。

1. **将servera注册到虚拟化中**

环境中，servera是已经安装好RHVH的宿主机，启动它。用户名和密码是root/redhat。它的IP地址是172.25.254.10。

注册RHVH到虚拟化中

在rhvm的web管理界面，点击“主机”->“新建”，弹出的菜单，“名称”->servera.lab.example.com;“地址”-> 172.25.250.10;“密码”->redhat；在高级选项里，确认“自动配置防火墙”是选中状态。

这个过程大概持续10分钟以上

安装完成后，需要把servera重启，确保相应的服务是正常的。在WEB页面中，右击servera->管理->ssh管理->重启。如果servera已经重启，但是web页面仍然显示等待状态，可以登陆到servera的控制台，手工reboot。

每个宿主机也拥有一个名为Cockpit的WEB管理页面。

https://servera.lab.example.com:9090。跳出连接不安全的页面，在高级里选择添加安全例外。用户名root和密码是redhat，可以看到node status的health是OK表示宿主机正常。

**Day02**

**Data domain & iso domain**

1. **Data domain**
   1. 概念和应用

数据域，存储虚拟机磁盘文件、模板。一个数据中心可以有多个Data domain。但是一个Data domain不能同时挂接到多个datacenter上。

* 1. Dota domain可用的后端存储

NFS

GlusterFS

iSCSI

FCP光纤

直连到宿主机的本地存储

1. **Iso domain**
   1. 概念和应用

只能用NFS实现。一个datacenter只能有最多一个ISO domain，但是一个ISO domain可以被多个datacenter共用。

* 1. 注意点

NFS服务器共享输出的顶级目录属主必须vdsm(UID=36)， 属组必须是kvm(GID=36)，权限要求是755

ISO domain配置的时候必须在datacenter中有一台可用的宿主机。因为ISO domain的配置信息需要由一台被称作SPM(Storage Pool Master)的服务器写入

1. **案例：配置iso domain**
2. 在workstation上执行

# lab install-storage setup

1. 在utility上配置NFS服务器

配置共享输出

# vim /etc/exports

/exports/data1 \*.lab.example.com(rw)

/exports/iso \*.lab.example.com(rw)

# exportfs -rv

修改权限

# chown 36:36 /exports/iso

# chown 36:36 /exports/data1

# ll -d /exports/iso

1. 在rhvm上创建相应的域

存储🡪新建域

Datadomain

名称：datadomain

路径：utility.lab.example.com:/exports/data1

类型：data

Isodomain

名称：isodomain

路径：utility.lab.example.com:/exports/iso

类型：iso

1. 上传光盘镜像：
   * + - 1. 使用rhv的工具：优点是简单，缺点是慢

$ ssh root@rhvm

# engine-iso-uploader list

🡺密码：redhat

# wget http://content.example.com/rhel7.3/x86\_64/isos/rhel-server-7.3-x86\_64-dvd.iso

[root@rhvm ~]# engine-iso-uploader --iso-domain=isodomain upload ~/rhel-server-7.3-x86\_64-dvd.iso

* + - * 1. 手工上传：优点是快，缺点是需要单独再修改权限等

$ ssh root@utility

# cd /exports/iso/3249dd1f-9e4b-4497-821f-7a61112efc6a/images/11111111-1111-1111-1111-111111111111/

# wget http://content.example.com/rhel7.3/x86\_64/extraisos/rhel-7-server-supplementary-20170731.iso

# chown 36:36 rhel-7-server-supplementary-20170731.iso

# chmod 640 rhel-7-server-supplementary-20170731.iso

1. 创建虚拟机

创建虚拟机时，硬盘的提供方式有：Thick/Thin

Thin：瘦。不会立即占用存储指定空间。比如为VM分配50G空间，那么也是以实际使用情况为准进行分配。

Thick：厚。提前把指定的空间全部分配。比如为VM分配50G空间，不管虚拟机现在有没有用到50G都提前分配。

创建虚拟机

进入虚拟机console控制台时，选第一项 Install RHEL7.3，然后按tab键，在下面的输出填写：空格inst.ks=http://materials.example.com/small.cfg

安装完毕后，在系统的倒计时页面按方向键取消倒计时，再点击rhvm中的关闭按钮。这样系统再启动就不会从光盘引导了。

安装好的虚拟机用户名密码：root/redhat

**Day03**

1. **创建和管理数据中心**

数据中心：RHV环境中的顶级组织对象。由一些物理和逻辑资源构成。如集群、宿主机、逻辑网络、存储域。

新建数据中心的原因：为不同的组织、团队隔离资源

新建数据中心：

Rhvm dashboard中点击“数据中心”->新建，名字为primarydc。存储类型一般都选择“共享的”表示存储可以用网络共享存储；如果选择了“本地的”，那么意味着使用本机的存储作为存储域，这样集群将只有一台Host，实现单一服务器集群。

1. **集群**

群集是共享相同存储域并具有相同类型的中央处理器(英特尔或AMD )。如果主机有不同代的中央处理器模型，它们只使用所有模型中存在的共同特性。集群是虚拟机的迁移域。

可以按功能划分集群。

新建集群：

集群->新建->数据中心选择primarydc，名称填clusterone，选择正确的CPU类型

额外的练习：创建配置、管理数据中心和集群

1. **用户和角色管理**

1、用户帐号的识别方式采用UPN名称

2、UPN：User Principal Name用户主体名称

默认情况下，RHV创建了一个本地域，名为internal。Internal这个本地域中包含的都是本地用户，管理员的UPN名称为admin@internal。

3、新建额外的本地用户可以使用命令：ovirt-aaa-jdbc-tools

4、用户管理也可以使用网络认证的方式集中管理。比如OpenLDAP、微软活动目录

1. **目录服务**

在workstation上执行以下命令：

[kiosk@foundation0 ~]$ ssh student@workstation

[student@workstation ~]$ lab manage-ipa setup

在rhvm上安装LDAP扩展包

[root@rhvm ~]# yum install -y ovirt-engine-extension-aaa-ldap-setup.noarch

配置rhvm加入到utility创建的域中

[root@rhvm ~]# ovirt-engine-extension-aaa-ldap-setup

>回车，使用DNS名称->1,single server-> utility.lab.example.com ->回车，startTLS -> URL, 获取CA证书的方式 -> <https://utility.lab.example.com/ipa/config/ca.crt> -> uid=rhvadmin,cn=users,cn=accounts,dc=lab,dc=example,dc=com -> redhat，rhvadmin的密码->回车->回车，虚拟机不采用sso -> lab.example.com, 外部域的配置文件名 -> Login, 测试到域服务器的连接方法 -> rhvadmin，用户名 -> redhat，密码 -> Done，测试成功 -> 最后抛出异常是bug不用管。

重启ovirt-engine服务，在web页面中，可以看到登陆有不同的域选项。

[root@rhvm ~]# systemctl restart ovirt-engine



**用户和角色管理**

1. **域用户**

当域用户集成到rhvm中后，域用户可以登陆了，但是没有相关的权限。我们可以在rhvm管理门户中为域用户授权。

1. **角色role：**

为了简化管理，把多种权限组合到一起形成不同的角色。把某种角色赋予一个用户，该用户就得到了相应的权限。

**3、RHV授权基于以下三个组件：**

（1）用户执行的动作

（2）动作的类型

（3）动作操作的对象

**4、内建角色的类型：**

（1）Administrator Role：管理员角色可以访问“管理门户”

（2）User Role：用户角色只能访问“用户门户”

**5、用户可以拥有的user role权限**：

（1）User role用户角色：访问“用户门户”，允许用户操作指定的虚拟机。

（2）PowerUserRole：超级用户角色。可以创建虚拟机和模板。

（3）UserVmManager：允许管理虚拟机，创建使用快照。如果一个用户通过“用户门户”创建了一台虚拟机，它自动对这台虚拟机就有此种角色。

**6、管理角色**

（1）SuperUser：在RHV中拥有全部的权限。如用户admin@internal拥有此角色

修改本地管理员密码：

[root@rhvm] # ovirt-aaa-jdbc-tool user password-reset admin --password-valid-to=”2025-08-01 12:00:00Z”

（2）CluterAdmin：在指定的集群中拥有管理权限

（3）DataCenterAdmin：在指定的数据中心，对除了存储以外的所有对象拥有管理权限。

**实验：**

1. **为rhvadmin@lab.example.com指定SuperUser角色**
2. 用admin@internal登陆
3. Configure -> System Permission -> Add ->把搜索范围改为lab.example.com -> Go ->选择rhvadmin -> 要分配的角色选择SuperUser
4. 退出当前用户，使用rhvadmin@lab.example.com登陆
5. **验证normaluser权限**
6. 退出rhvadmin@lab.example.com
7. 用normaluser登陆“管理门户”，可以登陆成功，但是进入不了“管理门户”，因为没有权限
8. 点击“用户门户”，可以进入。用户能够 操作虚拟rhel-test。
9. **验证power user权限**
10. 退出normaluser@lab.example.com
11. 用poweruser登陆“管理门户”，可以登陆成功，但是进入不了“管理门户”，因为没有权限
12. 点击“用户门户”，可以进入。在该页面中可以创建新的虚拟机。
13. **验证dcadmin权限**
14. 退出poweruser@lab.example.com
15. 用dcadmin登陆“管理门户”。可以登陆到管理门户，但是只能管理datacenter。
16. 创建一个存储域，但是不会成功。因为dcadmin对存储域没有权限。
17. 创建一个新的数据中心，也不允许。但是修改primarydc的属性，如描述，可以成功。
18. **添加额外的宿主机**
19. 登陆到utility创建ks文件

[root@utility ~]# mkdir /ks

[root@utility ~]# vim /etc/exports 尾部追加

/ks \*.lab.example.com(ro)

[root@utility ~]# exportfs -rv

[root@utility ~]# vim /ks/rhvh.cfg

liveimg --url=http://content.example.com/rhv4.1/x86\_64/dvd/squashfs.img

clearpart --all

autopart --type=thinp

rootpw --plaintext redhat

timezone Etc/UTC --isUtc

zerombr

text

reboot

%post --erroronfail

nodectl init

%end

1. 启动serverb

$ rht-vmctl start serverb

$ rht-vmctl view serverb

启动后，按向下箭头，通过网络启动，回车，在出现的安装rhvh界面（Install RHVH）按tab键，追加下面内容：

空格inst.ks=nfs://utility.lab.example.com:/ks/rhvh.cfg

1. 将主机添加到数据中心

按照将servera加入到default数据中心一样的步骤，把serverb添加到primarydc的clusterone集群中。

Serverc是已经安装好的和serverb一样的rhvh，采用同样的方法把serverc加入到secondary数据中心的clusstertwo集群中。

**Day04**

练习：

将serverc加入到secondary数据中心

1. **修改数据中心**

原因：升级、改变底层存储结构

方法：使用“维护模式”。RHV环境中很多资源都有维护模式，在对资源进行改动时，必须先把资源设置为“维护模式”。

1. **实验：将主机移除数据中心**
   1. 将虚拟机关机
   2. 将isodomain和datadomain置为“维护模式”
   3. 将servera置为“维护模式”
   4. 将servera迁出到primarydc的cluterone集群中
   5. 激活servera
2. **RHV网络**

为了更好的性能和安全性，可以通过创建VLAN或物理网络实现。

RHV的逻辑网络：可以数据中心上创建，然后分配给集群使用。创建逻辑网络时，可以指定 vlan tag，网络名称，是不是VM网络，甚至可以指定Qos。

VM网络提供给虚拟机使用，非VM网络只给宿主机使用。VM网络的后端使用的Linux网桥。

网络分类：

* 1. 管理网络：RHVM和RHVH之间通信
  2. 显示网络：用于虚拟机的控制台显示
  3. 迁移网络：虚拟机迁移
  4. 还可以创建存储网络

网络还可以分成：Required网络（必须的网络）和可选网络。当虚拟机的Required网络不可用，将导致迁移的发生，可选网络不会。

逻辑网络可以跨越集群，提供集群间虚拟机的通信。

1. **实验：创建逻辑网络**

在primarydc中创建名为VMnet的逻辑网络，描述是VM Network,启用vlan tag -> 10

VLAN:虚拟局域网。它将物理网络划分出了彼此隔离的很多虚拟网络。为了实现不同交换机上的相同VLAN可以通信，需要在交换机之间相连的端口上配置trunk中继。其实就是交换机修改了原始的数据帧，在帧的内部加上该帧属于哪个VLAN。

数据帧结构：6字节目标MAC+6字节源MAC+2字节类型/长度+46－1500字节数据+4字节FCS。

为了实现不同VLAN的节点可以通信，需要配置三层交换。

1. **实验：创建存储网络**
2. **实验：把主机接入到逻辑网络**

存储域和SPM（Storage Pool Master）

SPM用于在数据中心中接收RHVM发来的指令，对存储域进行配置更改。数据中心中，任意主机都可以修改数据，但是只有SPM可以修改配置。

数据域可以是NFS底层，也可以是iSCSI作为底层存储。如果是NFS的话，SPM将会创建RAW或qcow2格式的磁盘镜像作为虚拟机的磁盘；如果底层是iSCSI或FCP，将多个LUN组合成VG，创建虚拟机的时候，将从VG上创建LV作为虚拟机磁盘。虚拟机如果选择server，LV的大小就是指定server的磁盘大小；如果是destktop，LV大小为512M，如果空间不足时，LV会自动每次再增加512M。

1. **实验：创建存储域**

1、Servera和serverb已经安装了iSCSI initiator，查看它们的iqn名称：

[root@foundation0 ~]# ssh root@workstation

[root@workstation ~]# ssh servera cat /etc/iscsi/initiatorname.iscsi

InitiatorName=iqn.1994-05.com.redhat:a89603284aca

[root@workstation ~]# ^servera^serverb

InitiatorName=iqn.1994-05.com.redhat:34d791d736b0

2、在utiility上授权

/> cd /iscsi/iqn.2003-01.org.linux-iscsi.utility.x8664:sn.3c3f2957d79b/tpg1/acls

/iscsi/iqn.20...79b/tpg1/acls> create iqn.1994-05.com.redhat:a89603284aca

/iscsi/iqn.20...79b/tpg1/acls> create iqn.1994-05.com.redhat:34d791d736b0

1. **虚拟机默认硬件配置：**

Tiny: 1vcpu/512M

Small: 1vcpu/2048M

Medium: 2vcpu/4096M

Large: 2vcpu/8192M

XLage: 4vcpu/16384M

1. **在虚拟机上安装agent**

（相当于是vmware workstation的vmtools）

[root@rhel-vm yum.repos.d]# wget http://materials.example.com/rhvm.repo

[root@rhel-vm yum.repos.d]# yum install -y ovirt-guest-agent-common

[root@rhel-vm ~]# systemctl start ovirt-guest-agent

[root@rhel-vm ~]# systemctl enable ovirt-guest-agent

[root@rhel-vm ~]# systemctl start qemu-guest-agent

[root@rhel-vm ~]# systemctl enable qemu-guest-agent

如果系统是windows，可以把rhvm的iso光盘挂载到windows并安装。

/usr/share/rhev-guest-tools-iso/RHEV-toolsSetup\_4.1\_5.iso

1. **虚拟机控制台如果是全屏状态，可以按shift+f11退出**