Подготовка сетевого хранилища

Подготовка сетевого хранилища

Подготовка хранилища NFS

Подготовка хранилища iSCSI

Подготовка хранилища FCP

Подготовка сетевого хранилища

Необходимо осуществить подготовку хранилища для использования в новой среде виртуализации. В РЕД ВИРТ должен быть хотя бы один домен хранения данных, но рекомендуется добавлять больше.

В области данных хранятся виртуальные жесткие диски и файлы всех виртуальных машин и шаблонов, и они не могут совместно использоваться дата-центрами, когда они активны (но могут быть перенесены между дата-центрами). Домены данных нескольких типов хранения могут быть добавлены в один и тот же дата-центр при условии, что они являются общими, а не локальными доменами.

Дополнительно необходимо настроить домен данных, выделенный для виртуальной машины Engine. Этот домен создается во время развертывания системы и должен иметь объем не менее 120 ГБ. Перед началом развертывания необходимо подготовить хранилище для этого домена.

Можно использовать один из следующих типов хранения:

- NFS;
- iSCSI;
- Fibre Channel (FC);
- Gluster Storage.

Если вы используете хранилище iSCSI, домен хранения **Engine** должен использовать собственный LUN iSCSI. Любые дополнительные домены хранения должны использовать другой LUN iSCSI.

Подготовка хранилища NFS

ВАЖНО!

Крайне не рекомендуется размещать NFS сервер на хостах виртуализации в

виду того, что при выходе из строя оборудования или при необходимости перезапуска хоста виртуализации, на котором размещен NFS сервер, используемый как домен хранения, будет нарушена работа РЕД ВИРТ или возникнет необходимость полной остановки работы системы.

Чтобы **Engine** мог хранить данные в доменах хранения, представленных экспортируемыми каталогами, в них должны быть определенные учетные записи системных пользователей и их группы.

Дальнейшие действия выполняются на сервере с операционной системой РЕД ОС, который используется в качестве сетевого хранилища данных.

Если не установлен пакет NFS, его необходимо установить командой:

```
dnf install nfs-utils nfs4-acl-tools
```

Приведенная ниже процедура устанавливает разрешения для одного каталога (в примере /**data**). Вам необходимо повторить chown и chmod шаги для всех каталогов, которые вы собираетесь использовать в качестве доменов хранения в РЕД ВИРТ.

1. Создайте каталог **data**:

   ```
   mkdir /data
   ```

2. Создайте группу **kvm**:

   ```
   groupadd kvm -g 36
   ```

3. Создайте пользователя **vdsm** в группе **kvm**:

   ```
   useradd vdsm -u 36 -g 36
   ```

4. Измените владельца экспортируемого каталога на **36:36 (vdsm:kvm)**:

   ```
   chown -R 36:36 /data
   ```

5. Измените режим каталога, чтобы права на чтение и запись были предоставлены владельцу, а права на чтение и выполнение были предоставлены группе и другим пользователям:

   ```
   chmod 0755 /data
   ```

6. Все настройки сервера хранятся в файле **/etc/exports**. Откройте его на редактирование:

   ```
   
   ```

```
nano /etc/exports
```

7. Добавьте в конец файла строки вида (строк может быть произвольное количество):

```
/data 192.168.1.1/255.255.255.0(rw,insecure,nohide,all_squash,anonuid=36,
anongid=36,no_subtree_check)
```

где:

- **/data** – путь к папке, для которой раздается доступ;
- **192.168.1.1** – IP-адрес, которому раздается доступ к папке (можно указать всю сеть, тогда запись примет вид **192.168.1.0/24**).

Чтобы запустить службу и добавить её в автозагрузку, выполните команду:

```
systemctl enable nfs-server.service –now
```

Примечание.

Если в системе, где происходит развёртывание хранилища **NFS** установлен и запущен **firewall**, внесите в него необходимые изменения:

```
 firewall-cmd --permanent --add-service=nfs
firewall-cmd --permanent --add-service=mountd
firewall-cmd --permanent --add-service=rpc-bind
firewall-cmd --reload
```

Подготовка хранилища iSCSI

РЕД ВИРТ поддерживает хранилище iSCSI, которое представляет собой домен хранилища, созданный из группы томов, состоящей из LUN. Группы томов и LUN нельзя подключать более чем к одному домену хранения одновременно.

Если вы используете блочное хранилище и собираетесь развернуть виртуальные машины на необработанных устройствах или прямых LUN и управлять ими с

помощью диспетчера логических томов, вы должны создать фильтр, чтобы скрыть гостевые логические тома. Это предотвратит активацию гостевых логических томов при загрузке хоста, что может привести к устареванию логических томов и повреждению данных.

ВАЖНО!

РЕД ВИРТ в настоящее время не поддерживает хранилище с размером блока 4K. Вы должны настроить блочное хранилище в устаревшем режиме (блок 512 байт).

Если ваш хост загружается из хранилища SAN и теряет возможность подключения к хранилищу, файловые системы хранилища становятся доступными только для чтения и остаются в этом состоянии после восстановления подключения.

Чтобы предотвратить эту ситуацию, добавьте в корневую файловую систему SAN файл конфигурации с несколькими путями для загрузочного LUN, чтобы гарантировать, что он будет поставлен в очередь при наличии соединения:

```
cat /etc/multipath/conf.d/host.conf
```

```
multipaths {
multipath {
wwid boot_LUN_wwid
no_path_retry queue
}
}
```

Подготовка хранилища FCP

РЕД ВИРТ поддерживает хранилище SAN, создавая домен хранилища из группы томов, состоящей из уже существующих LUN. Ни группы томов, ни LUN нельзя подключать более чем к одному домену хранения одновременно.

Если вы используете блочное хранилище и собираетесь развернуть виртуальные машины на необработанных устройствах или прямых LUN и управлять ими с помощью диспетчера логических томов, вы должны создать фильтр, чтобы скрыть гостевые логические тома. Это предотвратит активацию гостевых логических томов при загрузке хоста, что может привести к устареванию логических томов и повреждению данных.

ВАЖНО!

РЕД ВИРТ в настоящее время не поддерживает хранилище с размером блока 4K. Вы должны настроить блочное хранилище в устаревшем режиме (блок 512 байт).

Если ваш хост загружается из хранилища SAN и теряет возможность подключения к хранилищу, файловые системы хранилища становятся доступными только для чтения и остаются в этом состоянии после восстановления подключения.

Чтобы предотвратить эту ситуацию, добавьте в корневую файловую систему SAN файл конфигурации с несколькими путями для загрузочного LUN, чтобы гарантировать, что он будет поставлен в очередь при наличии соединения:

```
cat /etc/multipath/conf.d/host.conf
```

```
multipaths {
multipath {
wwid boot_LUN_wwid
no_path_retry queue
}
}
```

Источник: https://redvirt.red-soft.ru/base/red-virtualizatsiya-8-0/podgotovka-setevogo-hranilicha-8/