Существует много инструментов для выполнения архивации данных на линуксе. Сегодня хочу рассмотреть программу duplicity, с помощью которой можно выполнить полный бэкап linux сервера. Она проста в использовании, но при этом очень удобна и функциональна.

Если вас интересует готовое бесплатное решение для бэкапа и переноса всего сервера, читайте статью с описанием такого решения — Veeam Agent for Linux. В статье отдельно на конкретном примере рассмотрен вопрос бэкапа и переноса всего сервера целиком на другое железо.

Введение

Обычно я использую для бэкапов rsync. Это гибкое и удобное средство, но в некоторых случаях им неудобно пользоваться. У него есть как плюсы, так и минусы. Как я использую и настраиваю rsync для бэкапа, я рассказал в отдельной статье. Если вы хотите получить компактный бэкап всей системы, или хранить на удаленном сервере бэкап с множеством файлов и директорий, вам придется как-то упаковывать файлы в архивы и передавать их. Кучу мелких файлов в сыром виде передавать медленно и неудобно.

Я часто использую для хранения бэкапов Yandex.Disk. Готовый кейс по настройке бэкапа сайта на яндекс.диск я уже приводил ранее. Диск монтируется по webdav и работает достаточно медленно. Передавать кучу мелких файлов по нему не удобно. Я решил посмотреть, что есть еще из средств бэкапа. Параллельно хотел рассмотреть вопрос удобного бэкапа всего сервера.

Нашел любопытную программу duplicity. Раньше слышал о ней, но руки не доходили проверить самому. Теперь дошли, перейдем к настройке полного бэкапа сервера.

Установка duplicity на Centos

С установкой все просто:

```
# yum install -y duplicity
```

Ставится из репозитория epel. Если у вас не ставится, проверьте, подключены ли репозитории.

Выполняем полный бэкап linux сервера

Чтобы полностью забэкапить сервер, необходимо использовать duplicity со следующими параметрами:

```
duplicity full --exclude=/proc --exclude=/sys --exclude=/dev --exclude=/proc --exclude=/sys --exclude=/mnt --exclude=/media
--exclude=/tmp --exclude=/var/spool --exclude=/var/cache --exclude=/var/tmp --exclude=/swap / file:///mnt/yadisk --no-
encryption
```

full	Указывает, что мы делаем полный бэкап, можно делать и инкрементный.
—exclude	Параметр задает списки исключений, сверьте со своим сервером и добавьте необходимые для исключения папки.
/	Источник бэкапа. В данном случае корень диска.
file:///mnt/yadisk	Локальный путь к папке /mnt/yadisk, куда делаем бэкап. У меня в эту папку смонтирован яндекс.диск.
—no-encryption	Параметр указывает на то, что шифрование не используется.

После выполнения бэкапа получите следующую информацию:

После полного бэкапа, можно выполнять инкрементный бэкап. Для этого в приведенной выше команды, вместо параметра **full** нужно использовать **incremental**.

Восстановление из бэкапа

Для того, чтобы извлечь содержимое бэкапа в папку /restore, воспользуемся командой:

```
duplicity --no-encryption --file-to-restore / file:///mnt/yadisk /restore
```

Если вам нужно восстановить какой-то отдельный файл или папку, укажите эту папку или файл следующим образом:

```
duplicity --no-encryption --file-to-restore var/log file:///mnt/yadisk /restore/var/log
duplicity --no-encryption --file-to-restore var/log/messages file:///mnt/yadisk /restore/var/log/messages
```

Во время восстановления каталога, папки создавать вручную не надо. Если восстанавливаете файл, то полный путь к конечной директории должен существовать.

Проверка и удаление бэкапов duplicity

Приведу еще несколько полезных команд для проверки бэкапов.

Посмотреть информацию о бэкапах в заданном каталоге:

```
duplicity collection-status --no-encryption file:///mnt/yadisk
```

Проверить содержимое бэкапа и сравнить с оригиналом:

```
duplicity verify --no-encryption file:///mnt/yadisk /
```

В данном случае не очень информативный вывод будет, так как будут отражены все файлы из исключенных директорий, а их очень много.

Посмотреть список файлов в архиве:

```
duplicity list-current-files --no-encryption file:///mnt/yadisk/duplicity
```

Необходимым функционалом является очистка старых бэкапов. Для того, чтобы удалить все бэкапы старше одного месяца, нужно воспользоваться командой:

```
duplicity --no-encryption remove-older-than 1M file:///mnt/yadisk
```

Чтобы удалить все бэкапы, кроме последнего, подойдет команда:

```
duplicity --no-encryption remove-all-but-n-full 1 --force file:///mnt/yadisk
```

На этом все, основные моменты я рассказал. Для бэкапа сервера или отдельных папок этого достаточно.

Заключение

Я рассмотрел малую часть функционала дуплисити. Большим ее плюсом является поддержка всевозможных удаленных хранилищ для бэкапа: ftp, ssh, различные облачные хранилища и другое. Хорошим преимуществом так же является возможность шифровать свои бэкапы. Мне пока нет надобности все это использовать, поэтому я рассмотрел только свой частный случай.

Что даст вам этот курс:

- Искать и эксплуатировать уязвимости или изъяны конфигурации в корпоративных сетях, web сайтах , серверах. Упор на пентест ОС Windows и на безопасность корпоративного сегмента.
- Изучение таких инструментов, как metasploit, sqlmap, wireshark, burp suite и многие другие.
- Освоение инструментария Kali Linux на практике - с ним должен быть знаком любой специалист по ИБ.

Проверьте себя на вступительном тесте и смотрите подробнее программу по .

Помогла статья? Есть возможность отблагодарить автора