от Windows к Linux

- Скрипты
  - Установка WireGuard
  - Тест
- Docker контейнеры
  - Управление контейнерами
- Нубские дела
  - Смена имени хоста и IP
  - Пользователи
  - Добавление ssh ключа - id_rsa.pub
  - Команда sudo без пароля в LINUX
  - Как сбросить root-пароль в CentOS 6 и CentOS 7
  - Linux iptables delete prerouting rule command
  - Как просмотреть историю команд другого пользователя в Linux?
  - Open VPN
  - Запуск с несколькими конфиг файлами...
  - Секреты Notepad++
- Zimbra
  - Чистка почты
  - Экспорт и импорт почты
- ESXi
  - How to Identify disks and Datastore in VMware ESXi 5 / 6
  - vSphere замена истекшего сертификата

- Windows
  - Connect Office 365 Exchange Online Services to PowerShell
  - Автоматическая репликация областей отказоустойчивого DHCP сервера Windows Server
  - Полный список переменных сред в Windows 10
  - Управление ролями и функциями Windows Server с помощью PowerShell
  - Сертификат для Linux в центре сертификации Active Directory
  - Репликация Active Directory
  - Подпись файлов signtool.exe
- Сети
  - Кто слушает порт в Linux
- Работа с дисками
  - Работа с дисками parted
  - Работа с дисками lvm
  - Изменения размера раздела
  - How to expand /dev/mapper/cl-root (/dev/mapper/centos-root)
- PostgreSQL
  - How to create read only user in PostgreSQL
- NGINX
  - Nginx – обратный прокси для Docker контейнеров
- tmp

Скрипты

Установка WireGuard

Поддерживаемые дистрибутивы:

- Ubuntu >= 16.04
- Debian 10
- Fedora
- CentOS
- Arch Linux

Скачивание и запуск скрипта

```
curl -O https://raw.githubusercontent.com/angristan/wireguard-install/master/wireguard-install.sh
chmod +x wireguard-install.sh
./wireguard-install.sh
```

1. Скачиваем скрипт
2. Разрешаем его исполнение
3. Запускаем

При повторном запуске скрипта можно удалить или добавить клиента.

Скрипты

Тест

Docker контейнеры

Управление контейнерами

`docker container ls -a` - отображает все контейнеры и их статус.

`docker image ls -a` - отображает все образы, размер и тэг

Нубские дела

Нубские дела

Смена имени хоста и IP

`hostname` - Вывод имени хоста

`sudo hostname servername` - изменяет имя хоста на *servername.* Так же рекомендуется подкорректировать файл *hosts* и сделать перезапуск

`ifconfig` - отображает IP адреса

`ip addr` or `ip a` - список интерфейсов, адресов и статуса

`ls /etc/netplan/` - необходимо отредактировать файл заканчивающийся на *.yaml* по адресу */etc/netplan.* Если файла нет вводим `sudo netplan generate` . Название файла конфигурации в *netplan* может отличаться, *“00-installer-config.yaml”*, у вас скорей всего будет иное название.

`sudo nano /etc/netplan/00-installer-config.yaml` - открывает файл *00-installer-config.yaml* в редакторе *nano*

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      dhcp6: no
      addresses: [10.0.2.15/24]
      gateway4: 10.0.2.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

> Не используйте табуляцию - клавишу `Tab` , интерпретатор файла реагирует на отступы!

Нубские дела

Пользователи

Введение

Команда `sudo` служит механизмом для предоставления прав администратора, которые обычно доступны только пользователю **root** user, для обычных пользователей. Из этого руководства вы узнаете, как создать нового пользователя с привилегиями `sudo` в Ubuntu 18.04 без изменения файла `/etc/sudoers` на вашем сервере. Если вы хотите настроить `sudo` для существующего пользователя, перейдите к шагу 3.

Шаг 1 — Выполнение входа на ваш сервер

Выполните вход через подключение SSH на ваш сервер как **root** user:

```
ssh root@your_server_ip_address
```

Шаг 2 — Добавление нового пользователя в систему

Используйте команду `adduser` для добавления нового пользователя в вашей системе:

```
adduser sammy
```

Обязательно замените `sammy` на имя пользователя, которое вы хотите использовать. Вам будет предложено создать и проверить пароль пользователя:

```
Output
Enter new UNIX password:
Retype new UNIX password:
```

```
passwd: password updated successfully
```

Далее вам будет предложено ввести определенную информацию о вашем новом пользователе.

```
utput
Changing the user information for sammy
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n]
```

Шаг 3 — Добавление пользователя в группу *sudo*

Воспользуйтесь командой `usermod` для добавления пользователя в группу **sudo**:

```
usermod -aG sudo sammy
```

Не забудьте заменить `sammy` на имя пользователя, которое вы только что добавили. По умолчанию в Ubuntu все участники группы **sudo** имеют полный набор привилегий `sudo`.

Отображение групп пользователя

`id -Gn имя_пользователя`

Шаг 4 — Тестирование доступа к *sudo*

Чтобы проверить, что новые разрешения `sudo` доступны, сначала нужно воспользоваться командой `su` для переключения на новую учетную запись пользователя:

```
su - sammy
```

Используя нового пользователя, убедитесь, что вы можете использовать `sudo`, добавив `sudo` перед командой, которую вы хотите запустить с привилегиями суперпользователя:

```
sudo command_to_run
```

Например, вы можете вывести список содержимого директории `/root`, которое обычно доступно только для пользователя root user:

```
sudo ls -la /root
```

При первом использовании `sudo` в сеансе вам будет предложено ввести пароль учетной записи данного пользователя. Введите пароль, чтобы продолжить:

```
Output:
[sudo] password for sammy:
```

> **Примечание:** это *не* запрос пароля **root**! Введите пароль пользователя с привилегиями sudo, а не пароль **root**.

Если ваш пользователь находится в соответствующей группе и вы ввели правильный пароль, команда с `sudo` будет запущена с правами **root**.

Нубские дела

Добавление ssh ключа - id_rsa.pub

Копирование публичного ключа вручную

Необходимо убедиться, что директория *~/.ssh* существует (в папке пользователя)

`mkdir -p ~/.ssh` - Если ее нет то данная команда создаст. Далее можно создать или отредактировать файл *authorized_keys*, это можно сделать командой `echo` **`строка_публичного_ключа`** `>> ~/.ssh/authorized_keys` Строка должна начинаться с *ssh-rsa AAAA...*

Далее убедимся, что директория *~/.ssh* и файл *authorized_keys* имеют подходящие права доступа: `chmod -R go= ~/.ssh`

`chmod 700 ~/.ssh` - ограничьте права доступа к этому каталогу только себе!

Эта команда удаляет права доступа для “group” и “other” для директории *~/.ssh/.*

Если вы используете аккаунт *root* для настройки ключей для аккаунта пользователя, важно, чтобы директория *~/.ssh* принадлежала этому самому пользователю, а не пользователю *root* :

`chown -R yuzer:yuzer ~/.ssh`

В нашем руководстве мы используем пользователя с именем ***yuzer*** , вам же следует использовать имя своего пользователя в команде выше.

Аутентификация на сервере Ubuntu с использованием ключей SSH

`ssh username@remote_host` - вход на сервер по *ssh*

Если вы заходите на удалённый хост по SSH в первый раз, вы можете увидеть вывод следующего вида:

```
The authenticity of host '203.0.113.1 (203.0.113.1)' can't be established.
ECDSA key fingerprint is fd:fd:d4:f9:77:fe:73:84:e1:55:00:ad:d6:6d:22:fe.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

Это означает, что ваш локальный компьютер не узнал удалённый хост. Напечатайте “*yes*” и нажмите `ENTER` для продолжения.

Отключение аутентификации по паролю на вашем сервере

вход на сервер с использованием пароля всё есть активен, что означает, что сервер уязвим для атак с перебором пароля (brute-force attacks). Вход *ssh* по паролю можно отключить отредактировав файл *sshd_config*

`sudo nano /etc/ssh/sshd_config`

Внутри файла найдите директиву *PasswordAuthentication*. Она может быть закомментирована. Раскомментируйте её при необходимости и установите её значение в “*no* ”. Это отключит возможность входа на сервер по паролю.

```
...
PasswordAuthentication no
...
```

Для применения внесённых изменений нам необходимо перезапустить сервис *sshd* - `sudo systemctl restart ssh`

В качестве меры предосторожности откроем новое окно терминала и проверим, что соединение по *ssh* работает корректно, перед тем, как закрывать текущую сессию.

Скопировать ключ так же можно с помощю scp (с одного хоста на другой)

`scp -p /home/yuzer/.ssh/authorized_keys yuzer@10.0.10.48:/home/yuzer/.ssh/`

```
scp [OPTION] [user@]SRC_HOST:]file1 [user@]DEST_HOST:]file2   #Пример синтакса
```

> SCP - перезапишет уже сущесвующий файл!

Нубские дела

Команда sudo без пароля в LINUX

Чтобы отключить пароль sudo, надо добавить к строчке настройки пользователя или группы директиву NOPASSWD. Синтаксис такой:

имя_пользователя ALL=(ALL) NOPASSWD: ALL

Для того чтобы отключить пароль sudo для определенного пользователя нужно открыть файл конфигурации sudo и отключить запрос пароля следующей строчкой, например для пользователя losst:

```
 sudo visudo
```

```
losst ALL=(ALL) NOPASSWD: ALL
```

Сохраните изменения и закройте файл, на всякий случай напомню что в vi для перехода в режим вставки используется клавиша **i**, для сохранения команда **:w** и команда **:q** для выхода. Теперь sudo не будет запрашивать пароль у выбранного пользователя при выполнении любых команд.

Для того чтобы разрешить пользователю выполнять только некоторые команды без пароля (например apt и reboot) добавьте следующую строчку:

```
losst ALL=(ALL) NOPASSWD: /usr/bin/apt, /sbin/reboot
```

Чтобы отключить пароль для группы пользователей используйте следующий код:

```
%имя_группы ALL=(ALL) NOPASSWD: ALL
```

Теперь у пользователей группы имя_группы утилита sudo не будет спрашивать пароль, а у всех остальных будет.

Как сбросить root-пароль в CentOS 6 и CentOS 7

Общий алгоритм сброса пароля

- Откройте VNC-консоль сервера
- Перезагрузите сервер и измените параметры загрузки ядра для загрузки в однопользовательский режим
- Установите новый пароль root без необходимости ввода старого

1. Доступ к VNC-консоли

Этот шаг одинаков для всех разновидностей Linux. Для облачного сервера найдите свой сервер в разделе "Облачные серверы > Создание и управление" в панели управления. Для выделенного сервера зайдите в "Выделенные серверы > Управление", соответственно. Откройте VNC-консоль с помощью одноименной кнопки:

54f9b2bc86ec3da8afe661c8758eabe7.png

Вид VNC-консоли может немного отличаться в зависимости от типа сервера и ОС.

2. Перезагрузка сервера и редактирование параметров загрузки ядра

Чтобы загрузить сервер в однопользовательский режим, вам потребуется отредактировать параметры загрузки ядра с помощью меню загрузчика GRUB. Поведение меню и параметры загрузки зависят от версии ОС и от того, является сервер облачным или выделенным.

2.1. CentOS 6, выделенный сервер

Перезагрузите сервер, нажав CTRL + ALT + DEL в окне VNC-консоли.

После меню BIOS, перед запуском ОС, появляется таймер. Нажмите ESC, чтобы остановить таймер и войти в меню загрузки GRUB.

11f1eadbdcc46f43538823ba8bd0f057.png

Используйте клавиши ↓ и ↑ для перемещения по меню. Выберите загрузочную строку и нажмите "e", чтобы отредактировать ее.

338100ab3da5ba5896da71d098791aba.png

Выберите строку, начинающуюся с "kernel /vmlinuz- ". Нажмите "e", чтобы отредактировать ее.

7619c18d4f450fda7f196dec9be2cc0d.png

Добавьте параметр "single" после пробела в конце строки.

5c4ec12d20c649ec100e94a0d115077d.png

Нажмите ENTER, чтобы сохранить изменения. Изменения будут сохранены до следующей перезагрузки.

Нажмите "b", чтобы запустить систему в однопользовательском режиме. Перейдите к разделу "Установка нового пароля root" в этой статье.

2.2. CentOS 6, облачный сервер

Перезагрузите сервер, нажав кнопку "Send CtrlAltDel" в окне VNC-консоли. Загрузочное меню с таймером появится сразу после меню BIOS.

Нажмите TAB, чтобы остановить таймер и отредактировать параметры загрузки. Изменения будут сохранены до следующей перезагрузки.

ddeec4ea727061773b8cfc845b2a82a6.png

Удалите параметры, выделенные красным цветом на рисунке ниже. Добавьте "1" (без кавычек и через пробел) в конце строки.

4540dd57c0762eae45aabed440e4d68b.png

Строка параметров должна выглядеть следующим образом:

6e45f8d0dfbaccdebfc33d2177dda0be.png

Нажмите ENTER, чтобы чтобы запустить систему в однопользовательском режиме.

Перейдите к разделу "Установка нового пароля root" в этой статье.

2.3. CentOS 7, выделенный сервер

Перезагрузите сервер, нажав CTRL + ALT + DEL в VNC-консоли. После меню BIOS, перед запуском ОС, появляется меню GRUB.

6b11b0562eae117a965828044bb4c801.png

Используйте клавиши ↓ и ↑ для навигации по меню, выберите свою загрузочную строку и нажмите "e", чтобы отредактировать ее.

Найдите строку, которая начинается с "linux" в 64-разрядной версии IBM Power Series или "linux16" в системах на базе BIOS x86-64 или "linuxefi" в системах UEFI. Измените параметр "ro" на "rw", удалите параметры "rhgb" и "quiet"; добавьте "rd.break enforcing=0" в конце строки.

22b4ac28da366b0790a1473056c63b16.png

0aac8bbae746dd3c252fdaaed857c267.png

Нажмите CTRL + X, чтобы запустить систему в однопользовательском режиме. Перейдите к разделу "Установка нового пароля root" в этой статье.

2.3. CentOS 7, облачный сервер

Перезагрузите сервер, нажав кнопку "Send CtrlAltDel" в окне VNC-консоли. После меню BIOS, перед запуском ОС, появляется загрузочное меню.

Используйте клавиши ↓ и ↑ для навигации по меню, выберите загрузочную строку и нажмите "e", чтобы отредактировать ее.

02364966866b1e20225ad9a11b7cbf95.png

Найдите строку, которая начинается с "linux" в 64-разрядной версии IBM Power Series или "linux16" в системах на базе BIOS x86-64 или "linuxefi" в системах UEFI. Измените параметр "ro" на "rw", удалите параметры, отмеченные красным на изображении ниже:

a7ec5fc253e55595a8b9e86bb4ef2b24.png

Добавьте "rd.break enforcing=0" в конце строки. Строка параметров должна выглядеть следующим образом:

77024959610bb9c8aa853cdb90b8b332.png

Нажмите CTRL + X, чтобы запустить систему в однопользовательском режиме. Перейдите к разделу "Установка нового пароля root" в этой статье.

3. Установка нового пароля root

В однопользовательском режиме вы работаете с правами пользователя root. Выполните следующие команды для изменения пароля root и перезагрузки:

3.1 **CentOS 6**

```
passwd root
reboot
```

3.2 **CentOS 7**

```
chroot /sysroot
passwd root
touch /.autorelabel
exit
reboot
```

Linux iptables delete prerouting rule command

Step 1 – List the pretrouting rules

The syntax is as follows:
`sudo iptables -t nat -v -L PREROUTING -n --line-number`
OR
`sudo iptables -t nat -v -L -n --line-number`
Iptables list the pretrouting rules on Linux
Where,

- **`-t nat`** : Select nat table.
- **`-v`** : Verbose output.
- **`-L`** : List all rules in the selected chain. In other words, show all rules in nat table.
- **`-L PREROUTING`** – Display rules in PREROUTING chain only.
- **`-n`** : Numeric output. IP addresses and port numbers will be printed in numeric format.
- **`--line-number`** : When listing rules, add line numbers to the beginning of each rule, corresponding to that rule's position in the chain. You need to use line numbers to delete nat rules.

Step 2 – Iptables delete prerouting nat rule

The syntax is:
`sudo iptables -t nat -D PREROUTING {rule-number-here}`
To delete rule # 1 i.e. the following rule:

```
1    15547  809K DNAT       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0
tcp dpt:80 to:10.147.164.8:80
```

Type the following command:

```
sudo iptables -t nat -D PREROUTING 1
```

OR

```
sudo iptables -t nat --delete PREROUTING 1
```

Verify that rule has been deleted from the PREROUTING chain , enter:

```
sudo iptables -t nat -v -L PREROUTING -n --line-number
```

Linux iptables remove prerouting command

Here is another DMZ rule:

```
sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to-destination 10.147.164.8:443
```

To remove prerouting command, run:

```
sudo iptables -t nat -D PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to-destination 10.147.164.8:443
```

Make sure you save updated firewall rules, either modifying your shell scripts or by running iptables-save command as described here.

Alternate syntax to remove specific PREROUTING rules from iptables

Say, you execute the following iptables PREROUTING command for port redirection:

```
sudo iptables -t nat -A PREROUTING -i eth0 -p tcp -m tcp --dport 443 -j DNAT --to-destination 10.147.164.8:443
```

To delete, run the same above command but replace the "`-A`" with "`-D`":

```
sudo iptables -t nat -D PREROUTING -i eth0 -p tcp -m tcp --dport 443 -j DNAT --to-destination 10.147.164.8:443
```

Another example, run the same command but replace the "`-I" with "-D". For example, say you have the following rule that redirect SSH (TCP 22) from port 2222 to port 22:`

```
sudo iptables -t nat -I PREROUTING -p tcp --dport 2222 -j REDIRECT --to-ports 22
```

`Becomes:`

```
sudo iptables -t nat -D PREROUTING -p tcp --dport 2222 -j REDIRECT --to-ports 22
```

OR

```
sudo iptables -t nat --delete PREROUTING -p tcp --dport 2222 -j REDIRECT --to-ports 22
```

Нубские дела

Как просмотреть историю команд другого пользователя в Linux?

```
sudo vim /home/USER_YOU_WANT_TO_VIEW/.bash_history
```

Open VPN

Игнорировать маршрут прописанным сервером.

Добавить в конфиг клиента:

```
pull-filter ignore "route 10.0.10.0 255.255.255.0"
```

Гоним весь трафик через впн.

```
redirect-gateway def1
```

Запуск с несколькими конфиг файлами...

```
/usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.adv.cfg -f /etc/haproxy/listen.cfg -f
/etc/haproxy/wildcard.cfg -f /etc/haproxy/backends.cfg -f /etc/haproxy/userlists.cfg
```

выполняет следующее:

- **Исполняемый файл**:
  Запускает бинарный файл HAProxy, расположенный по пути `/usr/sbin/haproxy`.
- **Используемые параметры**:
  - Флаг `-W` указывает HAProxy работать в однопроцессном режиме.
  - Флаг `-s` часто используется в сочетании с другими флагами для указания режима работы HAProxy (например, в некоторых версиях он может относиться к сигналам для мастер-рабочего режима); точное поведение может варьироваться в зависимости от версии HAProxy. Рекомендуется ознакомиться с документацией HAProxy или выполнить команду `haproxy -h`, чтобы получить подробности для вашей версии.
- **Конфигурационные файлы**:
  Команда указывает несколько конфигурационных файлов с помощью опции `-f`. HAProxy загрузит эти конфигурационные файлы в порядке, указанном в команде:
  - `/etc/haproxy/haproxy.adv.cfg`: Вероятно, содержит продвинутые или глобальные настройки.
  - `/etc/haproxy/listen.cfg`: Содержит определения для секции `listen` (объединяющей настройки frontend и backend).
  - `/etc/haproxy/wildcard.cfg`: Может определять правила или настройки, связанные с wildcard-доменами.
  - `/etc/haproxy/backends.cfg`: Определяет пул серверов backend.
  - `/etc/haproxy/userlists.cfg`: Содержит определения списков пользователей, часто используемых для базовой аутентификации или контроля доступа.

Как это работает

HAProxy читает и объединяет эти конфигурационные файлы последовательно. Такой подход полезен для организации конфигурации по различным аспектам (глобальные настройки, фронтенды, бэкенды и т. д.), что упрощает управление и обновление.

Дополнительные заметки

- **Порядок имеет значение**: Поскольку HAProxy обрабатывает конфигурационные файлы в указанном порядке, настройки в более поздних файлах могут переопределять предыдущие, если есть конфликтующие директивы.
- **Отладка/Проверка**: Если вам нужно проверить загруженную конфигурацию и возможные ошибки, вы можете использовать

Нубские дела

Секреты Notepad++

Искать ^((?!\b(?:\d{1,3}\.){3}\d{1,3}\b).)*$\R? заменить на "NULL-пустое значение" - Оставит в файле только строки с IP-адресами

Искать - -.* заменить на "NULL-пустое значение" - Удаляет указанный текс (- -) и все после него в строке

Zimbra

Чистка почты

Чиста ящика

`zmmailbox -z -m example@domain.com emptyFolder /Inbox` - Удаление писем из "Входящих"

`zmmailbox -z -m example@domain.com -A emptyDumpster` - Удаление файлов-писем с диска, без возможности восстановления

`su - zimbra all_accounts=`zmprov -l gaa`; for account in $all_accounts; do mbox_size=`zmmailbox -z -m $account gms`; echo "Mailbox size of $account = $mbox_size"; done ;` - Отображение размера каждого "ящика"

Экспорт и импорт почты

Экспорт

```
zmmailbox -z -m example@domain.com getRestURL "//?fmt=tgz" >
/opt/zimbra/docs/user_backup.tar.gz
```

Импорт

```
zmmailbox -z -m example@domain.com postRestURL "//?fmt=tgz&resolve=skip"
/opt/zimbra/docs/user_backup.tar.gz
```

Параметр `skip` - Игнорировать повторяющиеся элементы, найденные в файле резервной копии

`modify` - Обновите текущие элементы почтового ящика содержимым того, что импортируется из файла резервной копии

`reset` - Удалите старую почту и замените содержимое содержимым файла резервной копии

> Источник https://nwildner.com/posts/2019-09-27-zimbra-cli-tips/

ESXi

ESXi

How to Identify disks and Datastore in VMware ESXi 5 / 6

There are a few reasons that will degrade the performance of virtual machines such as a disk I/O bottleneck, resource contention, misconfigurations and other problems.

When too many VMs compete for limited resources, results will inevitably suffer.

The effort it takes to solve the storage I/O bottleneck is a variety of ways, it may be from physical infrastructure choices to configuration changes.

The starting point for solving your I/O problems will be VM monitoring and establishing baseline performance.

From there, you can examine the IOPS read vs. write IOPS, network cards, and certain points which may contribute to the I/O bottlenecks.

With the right approach and the right technology, administrators can resolve the problems that caused the dismal performance of the infrastructure.

When performing troubleshooting with ESXi/ESX storage, use command line tools which require you to identify a specific disk or LUN connected to ESXi/ESX.

This article provides information on different ways to identify these disks. This can be part of troubleshooting, primarily due to the storage component of the virtual environment.

Display availabke command for esxcli storage :

```
~ # esxcli storage
Usage: esxcli storage {cmd} [cmd options]

Available Namespaces:
  core                  VMware core storage commands.
  nfs                   Operations to create, manage, and remove Network Attached Storage
```

```
filesystems.
  nmp                   VMware Native Multipath Plugin (NMP). This is the VMware default
implementation of the Pluggable Storage Architecture.
  san                   IO device management operations to the SAN devices on the system.
  vflash                virtual flash Management Operations on the system.
  vmfs                  VMFS operations.
  filesystem            Operations pertaining to filesystems, also known as datastores, on the
ESX host.
```

Display availabke command for esxcli storage -> vmfs :

```
~ # esxcli storage vmfs
Usage: esxcli storage vmfs {cmd} [cmd options]

Available Namespaces:
  snapshot              Manage VMFS snapshots.
  extent                Manage VMFS extents.

Available Commands:
  unmap                 Reclaim the space by unmapping free blocks from VMFS Volume
  upgrade               Upgrade a VMFS3 volume to VMFS5.
```

```
~ # esxcli storage vmfs extent
Usage: esxcli storage vmfs extent {cmd} [cmd options]

Available Commands:
  list                  List the VMFS extents available on the host.
```

List the VMFS extents available on the host :

```
~ # esxcli storage vmfs extent list
Volume Name  VMFS UUID                            Extent Number  Device
Name                                                                Partition
-----------  -----------------------------------  -------------
-------------------------------------------------------------------------  ---------
datastore1   52a0db3f-d87636dc-61bb-28924a2f1bc0              0
t10.ATA_____VB0250EAVER_____________________________Z3TDY30B_____________            3
datastore2   53f6103b-e2c46411-13e9-28924a2f1bc0              0
t10.ATA_____WDC_WD1600AAJS2D00L7A0_____________________________WD2DWCAV36165769          1
```

```
~ # esxcli storage filesystem
Usage: esxcli storage filesystem {cmd} [cmd options]

Available Commands:
  automount             Request mounting of known datastores not explicitly unmounted.
  list                  List the volumes available to the host. This includes VMFS, NAS, VFAT
and UFS partitions.
  mount                 Connect to and mount an unmounted volume on the ESX host.
  rescan                Issue a rescan operation to the VMkernel to have is scan storage
devices for new mountable filesystems.
  unmount               Disconnect and unmount and existing VMFS or NAS volume. This will not
delete the configuration for the volume, but will remove the
                        volume from the list of mounted volumes.
```

List the volumes available to the host. This includes VMFS, NAS and VFAT partitions :

```
~ # esxcli storage filesystem list
Mount Point                                         Volume Name
UUID                                 Mounted  Type            Size         Free
--------------------------------------------------  -----------
-----------------------------------  -------  ------  ------------  -----------
/vmfs/volumes/52a0db3f-d87636dc-61bb-28924a2f1bc0  datastore1   52a0db3f-d87636dc-61bb-
28924a2f1bc0     true  VMFS-5  244544700416  52979302400
/vmfs/volumes/53f6103b-e2c46411-13e9-28924a2f1bc0  datastore2   53f6103b-e2c46411-13e9-
28924a2f1bc0     true  VMFS-5  159987531776  14871953408
/vmfs/volumes/556a99d3-4dc8997f-b819-28924a2f1bc0               556a99d3-4dc8997f-b819-
28924a2f1bc0     true  vfat      4293591040   4255121408
/vmfs/volumes/4a052e7f-ed60f807-e327-66c4dcb34a59  Hypervisor1  4a052e7f-ed60f807-e327-
66c4dcb34a59     true  vfat       261853184     96874496
/vmfs/volumes/25230d7e-4dcb47f9-390e-25a3db175fe7  Hypervisor2  25230d7e-4dcb47f9-390e-
25a3db175fe7     true  vfat       261853184     96976896
/vmfs/volumes/2da668ef-40e5d96b-90bf-855ddb9c5547  Hypervisor3  2da668ef-40e5d96b-90bf-
855ddb9c5547     true  vfat       299778048     96681984
```

```
~ # esxcli storage nmp
Usage: esxcli storage nmp {cmd} [cmd options]

Available Namespaces:
  psp                   Operations pertaining to the Path Selection Policy Plugins for the
VMware Native Multipath Plugin.
```

```
  satp                  Operations pertaining to the Storage Array Type Plugins for the VMware
Native Multipath Plugin.
  device                Operations pertaining to the devices currently claimed by the VMware
Native Multipath Plugin.
  path                  Operations pertaining to the paths currently claimed by the VMware
Native Multipath Plugin.
```

```
~ # esxcli storage nmp device
Usage: esxcli storage nmp device {cmd} [cmd options]

Available Commands:
  list                  List the devices currently controlled by the VMware NMP Multipath
Plugin and show the SATP and PSP information associated with that
                        device.
  set                   Allow setting of the Path Selection Policy (PSP) for the given device
to one of the loaded policies on the system.
```

List the devices currently controlled by the VMware NMP Multipath Plugin and show the SATP and PSP information associated with that device :

```
~ # esxcli storage nmp device list
t10.ATA_____VB0250EAVER_____________________________Z3TDY30B______________
   Device Display Name: Local ATA Disk
(t10.ATA_____VB0250EAVER_____________________________Z3TDY30B______________)
   Storage Array Type: VMW_SATP_LOCAL
   Storage Array Type Device Config: SATP VMW_SATP_LOCAL does not support device
configuration.
   Path Selection Policy: VMW_PSP_FIXED
   Path Selection Policy Device Config: {preferred=vmhba0:C0:T0:L0;current=vmhba0:C0:T0:L0}
   Path Selection Policy Device Custom Config:
   Working Paths: vmhba0:C0:T0:L0
   Is Local SAS Device: false
   Is USB: false
   Is Boot USB Device: false

t10.ATA_____WDC_WD1600AAJS2D00L7A0_____________________________WD2DWCAV36165769
   Device Display Name: Local ATA Disk
(t10.ATA_____WDC_WD1600AAJS2D00L7A0_____________________________WD2DWCAV36165769)
   Storage Array Type: VMW_SATP_LOCAL
   Storage Array Type Device Config: SATP VMW_SATP_LOCAL does not support device
```

```
configuration.
   Path Selection Policy: VMW_PSP_FIXED
   Path Selection Policy Device Config: {preferred=vmhba32:C0:T0:L0;current=vmhba32:C0:T0:L0}
   Path Selection Policy Device Custom Config:
   Working Paths: vmhba32:C0:T0:L0
   Is Local SAS Device: false
   Is USB: false
   Is Boot USB Device: false
```

ESXi

vSphere замена истекшего сертификата

vSphere замена истекшего сертификата vCenter Appliance

18 января 2022 1 Maxim Zhukov

Недавно наш заказчик пришел с проблемой **потери управления виртуализированной инфраструктурой.**

356e0c6b-5b18-f0c2-3727-73a398523848?imagePreview=1

При попытке авторизации в консоль vSphere
An error occurred during authentication

```
Please configure certool.cfg file with proper values before proceeding to next step.
Press Enter key to skip optional parameters or use Default value.
Enter proper value for 'Country' [Default value : US] : (Note: Value for Country should be
only 2 letters)
Enter proper value for 'Name' [Default value : CA] :
Enter proper value for 'Organization' [Default value : VMware] :
Enter proper value for 'OrgUnit' [Default value : VMware Engineering] :
Enter proper value for 'State' [Default value : California] :
Enter proper value for 'Locality' [Default value : Palo Alto] :
Enter proper value for 'IPAddress' [optional] :
Enter proper value for 'Email' [Default value : email@acme.com] :
Enter proper value for 'Hostname' [Enter valid Fully Qualified Domain Name(FQDN), For Example
: example.domain.com] :
Enter proper value for VMCA 'Name':
```

Ошибку следует диагностировать просмотром сертификата – который истек (видно из браузера).

При попытке входа в vCenter консоль (**Appliance Management**) для просмотра состояния сервисов

```
Exception in invoking authentication handler
[SSL.CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:719)
```

Проблема в том, что при истекшем сертификате не попасть в консоль управления так как не может аутентифицировать, где по процедуре можно заменить сертификат из web- консоли.

7e776b5c-520a-e13c-40ac-3c1aa9dfddb3?imagePreview=1

Причину подтвердим просмотром трейса ошибки:

```
javax.net.ssl.SSLHandshakeException:
com.vmware.vim.vmomi.client.exception.VlsiCertificateException:
Server certificate chain is not trusted and thumbprint verification is not configured
```

Ошибки при истекшем сертификате будут вида

Что **такая-то служба** не может соединиться (так как **не устанавливается защищенное соединение с vCenter Appliance** из-за невалидного сертификата)

```
Authentication failed, Update Manager server could not be contacted.


An unexpected error has occurred.
```

> В том числе **не будет работать и служба Аутентификации vSphere**, а это, сами понимаете, «привет» управлению инфраструктурой и работе служб vSphere.

Что делать?

Нужно заменить истекший сертификат в vCenter Appliance. Но есть ньюансы.

При отсутствии доступа в web-консоль **vCenter Appliance Management**

```
Exception in invoking authentication handler
[SSL.CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:719)
```

Остается доступ через коммандную строку в виртуальную машину.

В ситуации с истекшим сертификатом работоспособность запущенных виртуальных машин не затронута, и можно зайти на узлы гипервизора ESXi и временно поуправлять вручную запуском и выключением виртуальных машин.

Собственно этот путь (**через подключения к ESXi**) с вызовом консоли машины с vCenter Appliance и потребуется проделать для замены истекшего сертификата, если на машине выключен **SSH** в целях безопасности.

Но где лежит сертификат и как его правильно заменить?

Оказывается, что для генерации сертификата vCenter Server Appliance имеет утилиту **Certificate Manager.**

Для начала подключитесь к vCenter через ssh или через консоль виртуальной машины с vCenter через гипервизор ESXi где она функционирует.

Если у Вас много хостов в инфраструктуре, возможно придется поискать последовательно подключаясь на каждый пока не отыщите свой запущенный vCenter.

1. # Запустите /usr/lib/vmware-vmca/bin/certificate-manager

    1. # Если Вам приемлем Self-Signed Certificate и нужно быстро восстановить доступ

        1. Выбирите пункт **4 Regenerate a new VMCA Root Certificate and replace all certificates** и введите пароль для administrator@vsphere.local
        2. Далее последовательно заполните поля с учетом того, что **Name, Hostname и VMCA должны соответствовать Primary Network Identifier PNID** .
        3. Значение PNID можно посмотреть выполнив /usr/lib/vmware-vmafd/bin/vmafd-cli get-pnid --server-name localhost
        4.
        5. Нажмите Y (Yes) для продолжения.
        6. В случае неактуального сертификата в веб-консоли vCenter перезагрузите vCenter.

    2. # Если Вы хотите валидный сертификат полученный через центр сертификации

        1. В меню выберите пункт **1. Replace Machine SSL certificate with Custom Certificate** и введите пароль для administrator@vsphere.local
        2. Укажите директорию, где будут помещены запросы на выпуск, например /tmp/ssl/
        3. Далее последовательно заполните поля с учетом того, что **Name, Hostname и VMCA должны соответствовать Primary Network Identifier PNID** .
        4. Значение PNID можно посмотреть выполнив /usr/lib/vmware-vmafd/bin/vmafd-cli get-pnid --server-name localhost

5.
```
Country      : Two uppercase letters only (Eg. US), the country where your company is located.
Name         : FQDN of the vCenter Server(This will be your Certificate Subject Alternate Name)
Organization : Company Name
OrgUnit      : The name of your department within the organization. Example: "IT"
State        : The state/province where your company is located
Locality     : The city where your company is located.
IPAddress    : IP Address of vCenter Server, this field is Optional
Email        : Email Address
Hostname     : FQDN of vCenter Server(This field accepts multiple entries separated by comma.
```

6. Файл /tmp/ssl/vmca_issued_csr.csr передаем в центр сертификации для выпуска SSL сертификата.
7. Помещаем выпущенный сертификат на систему, например, в /tmp/ssl/ в отдельной сессии
8. Продолжаем импорт

```
Provide a valid custom certificate for Machine SSL.
File : /tmp/ssl/machine_name_ssl.cer

Provide a valid custom key for Machine SSL.
File : /tmp/ssl/machine_name_ssl.key

Provide the signing certificate of the Machine SSL certificate.
File : /tmp/ssl/Root64.cer
```

9. Нажмите Y (Yes) для продолжения.
10. В случае неактуального сертификата в веб-консоли vCenter перезагрузите vCenter.

Windows

Windows

Connect Office 365 Exchange Online Services to PowerShell

How to Connect Office 365 Exchange Online Services to PowerShell

The default method for managing Microsoft Office 365 with all included applications is by using a web browser and connecting to the web interface of Office 365 Admin Center and Exchange Admin Center. This standard method has an intuitive graphical interface, but sometimes the capabilities of the graphical user interface are not enough. For example, when you need to perform similar actions with tens or hundreds of user accounts, it is better to use the CLI (command line interface) rather than the GUI (graphical user interface). Moreover, some actions that can be done with Exchange Online cmdlets are not available in the Admin Center.

Microsoft provides PowerShell to manage the products in the command line interface. Many administrators have the habit of managing Microsoft Exchange Server via PowerShell. However, standard commands of the Exchange PowerShell module that work in the local environment with a standalone instance of Microsoft Exchange Server installed on a physical server or a virtual machine cannot be used with Exchange 365 running in the cloud. This is because standard PowerShell commands cannot connect to cloud services such as Azure and Office 365 backup, including Exchange Online. For this reason, you will need to install special PowerShell modules that allow you to connect to Office 365. The details of this process are covered in today's blog post that explains multiple methods of how to connect to Exchange Online PowerShell and consists of the following parts:

- Requirements
- The Working Principle
- Manual Configuration
- Automated Configuration
- The Alternative Method

NAKIVO Backup & Replication offers improved backup capabilities by adding Microsoft Office 365 backup to its feature set. Start the Free Trial of our product, discover how NAKIVO Backup & Replication works in your environment, and receive an Amazon eGift card for your feedback.

Requirements

There are some requirements that must be met to connect to Exchange Online PowerShell.

- You should use PowerShell on Windows 7 SP1, or newer desktop Windows versions and Windows Server 2008 R2 SP1, or newer server Windows versions. Be aware that you need to install .NET Framework 4.5 or later in addition to installing an updated version of Windows Management Framework 3.0, 4.0, or 5.1.
- An internet connection is required. TCP port 80 must be opened to connect from your local machine to the destination host.
- Access to Exchange Online PowerShell must be enabled for the current user (by default such access is enabled for administrators).

You can manually enable access to connect to Exchange Online PowerShell for the particular user with the command:

Set-User -Identity user@domain.com -RemotePowerShellEnabled $true

Working Principle

You can connect to Exchange Online PowerShell, but this process is more complicated than using PowerShell for managing a local Exchange Server. However, you can use the built-in PowerShell console to manage remote cloud infrastructures. In this case, the console is called *remote PowerShell* or *PowerShell Remoting*. The process of initiating a remote PowerShell session for Office 365 and Exchange Online is slightly different. You should download and install special components before you can open a remote Office 365 session. Fortunately, the cmdlets required to initiate a remote Exchange Online PowerShell are downloaded automatically when you create a remote PowerShell session. Different sets of PowerShell cmdlets are used to manage Microsoft Office 365 and Microsoft Exchange Online.

The main reasoning behind connecting to Microsoft Exchange Online in PowerShell entails the following:

- Creating a remote session to Exchange Online in PowerShell opened on your local machine.
- Providing connection settings, passing authentication.
- Importing PowerShell cmdlets that are needed to manage Exchange Online remotely.

In today’s blog post, we will run PowerShell cmdlets on Windows 10.

Manual Configuration

Let’s review the manual method first, to understand the configuration principle better.

1. Open Windows PowerShell. You can do this with at least two methods.

1a. Click **Start**, type **cmd**, right click the **Command Prompt** item and select *Run as Administrator* in the context menu.

1b. Go to **Start > Windows PowerShell**. Right click Windows PowerShell, and hit *Run as Administrator* to make sure that you can run PowerShell commands without restrictions.

2. Enable running scripts (it is better to run this command in the beginning of preparing PowerShell to manage Exchange Online and Office 365), otherwise you will get the error in future when running the **Import-PSSession** command:

Import-PSSession : Files cannot be loaded since running scripts has been disabled on this system. Provide a valid certificate with which to sign the files.

In order to execute scripts, the execution policy must be set to *RemoteSigned*.

Set-ExecutionPolicy RemoteSigned

Press **Y** to confirm changing the policy if prompted. You can also use the **Set-ExecutionPolicy Unrestricted** command to use the *Unrestricted* policy. By default, the execution policy mode is *Restricted*.

Change the execution policy before you connect to Exchange Online PowerShell

3. Run the command in PowerShell to get credentials and enter your administrator login/password in the popup window to access Exchange Online. The user must have global administrative permissions in Office 365.

$Credential=Get-Credential

How to connect to Office 365 PowerShell – saving credentials as the variable

The entered credentials will be saved in the variable and used in the next command as *$Credential*.

4. You have to create a remote PowerShell session with the *New-PSSession* cmdlet and running the following command:

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $Credential -Authentication Basic -AllowRedirection

Notice that in this command, the target URL of the Exchange Online server running in the cloud that must accept the request is set. After running the command, Microsoft Office 365 cloud servers will provide you access to the appropriate Exchange Online virtual server associated with your account.

How to connect to Exchange Online PowerShell – creating a new remote session

5. Exchange Online PowerShell cmdlets must be imported to the current session with the command:

Import-PSSession $Session

You can see the progress bar while receiving the commands.

How to connect to Exchange Online PowerShell – importing Exchange online cmdlets to the current s

After successfully running the command, you will see the following message.

How to connect to Exchange Online PowerShell – Exchange Online cmdlets have been imported succ

Note: If you use the MFA for your account, the standard cmdlets explained above will not work. If you want to connect Exchange Online in PowerShell using MFA, run the following command:

Connect-EXOPSSession -UserPrincipalName YOUR_UPN

Where YOUR_UPN (user principle name) is the name of the Office 365 account you are using.

You may need to install Microsoft's *Exchange Online Remote PowerShell Module.* Be aware that when using this module, the session ends after one hour, which may be inconvenient for running long scripts. Consider using *Trusted IP addresses* (i.e. the IP addresses of your organization) to bypass MFA when connecting from the network of your company to Exchange Online PowerShell.

MFA (Multi-Factor-Authentication) is the advanced method of authentication that adds a second layer of security. After entering a password, the confirmation code is sent to the user's cell phone and the user must enter the confirmation code to verify the account to get access to Office 365 cloud services.

6. Once you have connected to Office 365 and Exchange Online, you can manage your Office 365 cloud environment. Let's verify that we have connected to Exchange Online correctly and list the mailboxes of users, for example.

Get-Mailbox

Exchange Online PowerShell – checking mailboxes of users

You can list all cmdlets available for Exchange Online PowerShell with the following command:

Get-Command -Module tmp*

The names of Exchange Online PowerShell cmdlets are not converted.

7. When you end your work with Exchange 365, disconnect the session. This is the recommended practice.

Remove-PSSession $Session

Unfortunately, no messages are displayed after executing this command. You can check whether the session is disconnected by running the **Get-MailBox** command. If the session is disconnected, you will get the error explaining that you cannot run Exchange Online cmdlets after disconnecting.

Why should you disconnect the session? Well, simply because the number of active concurrent sessions that can be opened simultaneously is limited to three. If you open three Exchange Online PowerShell sessions at once and don't disconnect any of them when not in use, you will need to wait until one of these sessions expires before you can connect to Exchange Online PowerShell again from a new PowerShell console.

Automated Configuration

Now that you know the principle of how to connect to Exchange Online PowerShell manually, you can use the automated method. The advantage of this method is the lower number of commands you should enter.

1. Download the script from the Microsoft's web site. The name of the script file is *ConnectExchangeOnlinePowerShell.ps1* in this case.

2. Go to the directory where the script is located; in our example, the script is saved to *C:\temp_win*.

3. Before running the script, edit the script execution policy (similarly to what is shown in the first method), otherwise you will get the error:

The file C:\temp_win\ConnectExchangeOnlinePowerShell.ps1 is not digitally signed. You cannot run this script on the current system.

You can apply the *Bypass* execution policy to avoid this issue:

Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass

Type **Y** to confirm the execution policy change.

Connect to Exchange Online PowerShell by using a PowerShell script

4. After that, you can run the script. If you don't use MFA, run the script without additional arguments:

.\ConnectExchangeOnlinePowerShell.ps1

If MFA (Multi-Factor Authentication) is used in your Office 365 environment, try the command:

.\ConnectExchangeOnlinePowerShell.ps1 -MFA

5. Now that you have successfully connected to Exchange Online, you can manage your user accounts, their mailboxes, etc. For example, you can list the mailboxes of your users:

Get-Mailbox

Exchange Online PowerShell is now connected – checking mailboxes

This script can be used to schedule and automate tasks. For example, you can connect to Exchange Online without entering credentials in the interactive window as shown above. You can enter your login and password in the command line as command options when executing the script:

./ConnectExchangeOnlinePowerShell.ps1 -UserName admin@your_domain.com -Password your_password

Keep in mind that entering passwords as plain text in the command line may be not secure.

6. When you finish to work with Exchange Online in PowerShell, don’t forget to end the session:

./ConnectExchangeOnlinePowerShell.ps1 -Disconnect

Alternative Method

Let’s consider one more method that can be used to connect to Exchange Online PowerShell. This method can be considered as a modification of the first method.

1. Create a new profile for PowerShell with the function:

New-item -type file -force $profile

2. Edit the profile configuration file in the text editor to add the function titled *Connect-EXOnline*:

notepad $profile

3. Add the following content to the PowerShell profile configuration file and change **username@domain.com** to your account name, then save the text file.

Function Connect-EXOnline

{

$credentials = Get-Credential -Credential username@domain.com

Write-Output “Getting the Exchange Online cmdlets”

$Session = New-PSSession -ConnectionUri https://outlook.office365.com/powershell-liveid/ `

-ConfigurationName Microsoft.Exchange -Credential $credentials `

-Authentication Basic -AllowRedirection

Import-PSSession $Session

}

4. Close the current PowerShell window and open a new PowerShell window as Administrator. Run the command to connect to Exchange Online PowerShell:

Connect-ExOnline

Enter your password in the popup window.

PowerShell connect to Exchange Online

5. When you have finished working with Exchange Online PowerShell, end the session with the command:

Get-PSSession | Remove-PSSession

Windows

Автоматическая репликация областей отказоустойчивого DHCP сервера Windows Server

> Источник http://pyatilistnik.org/oshibki-20291-i-20292-na-dhcp-v-windows-server/

Как я написал выше, Microsoft до сих пор не решило проблему автоматической репликации данных, о зарезервированных IP-адресах, даже в Windows Server 2019. Тут у вас два варианта, первый самый топорный, это ручной запуск на сервере, где были изменены настройки. Для этого запустите PowerShell и введите команду:

```
Invoke-DhcpServerv4FailoverReplication -ComputerName dc01.root.pyatilistnik.org
```

- dc01.root.pyatilistnik.org - сервер с которого мы будем реплицировать настройки (**DHCP сервер-партнер**)

В этом примере реплицируются **все области** отработки отказа службы DHCP-сервера, работающей на компьютере с именем dc01.root.pyatilistnik.org, в одну или несколько соответствующих партнерских служб DHCP-сервера на основе одного или нескольких отношений отработки отказа, в которых включены службы DHCP-сервера. Обратите внимание, что у вас появится запрос на подтверждение данного действия. Если хотите его пропускать, то необходимо добавить ключ **-Force**.

```
Invoke-DhcpServerv4FailoverReplication -ComputerName dc01.root.pyatilistnik.org -Force
```

Команда Invoke-DhcpServerv4FailoverReplication -ComputerName dc01.root.pyatilistnik.org

Если вам необходимо произвести репликацию настроек отработки отказа относительно одной группы, то команда будет выглядеть вот так:

```
Invoke-DhcpServerv4FailoverReplication -ComputerName dc01.root.pyatilistnik.org -Name dc01.root.pyatilistnik.org-svt2019s01
```

В этом примере реплицируется конфигурация всех областей, которые являются частью отношения отработки отказа с именем **dc01.root.pyatilistnik.org-svt2019s01** в службе DHCP-сервера, работающей на компьютере с именем **dc01.root.pyatilistnik.org**, в службу DHCP-сервера партнера.

Репликация отработки отказа через PowerShell

Предположим, что вам необходимо выполнить репликацию отработки отказа, только для определенных областей, для этого есть параметр -ScopeId, вот пример для моих областей:

```
Invoke-DhcpServerv4FailoverReplication -ComputerName dc01.root.pyatilistnik.org -ScopeId 192.168.31.0,192.168.32.0 -Force
```

Зная теперь основные команды, вы можете создать для себя автоматический сценарий при котором у вас будет происходить репликация. Тут все просто на поможет сценарий PowerShell и планировщик заданий, который будет срабатывать на определенное событие в журналах Windows.

Хочу отметить, что я и сама Microsoft настоятельно рекомендует, всем администраторам делать изменение настроек исключительно на одном из серверов партнеров, а уже потом реплицировать на второй, так можно гарантировать, что все реплики будут корректны и минимизировано количество потерь ваших изменений

Алгоритм действий:

- Создаете в Active Directory новую учетную запись, например dhcp-replication и **делаете ее администратором на обоих DHCP серверах**, кто входит в группу репликации. Как дать права на DHCP читайте по ссылке.

Создание учетной записи для репликации областей отработки отказа

- Создаем небольшой скрипт dhcp-replication.ps1. Для этого вам просто нужно открыть PowerShell ISE и ввести там команду:

Invoke-DhcpServerv4FailoverReplication -ComputerName dc01.root.pyatilistnik.org -Force#dc01.root.pyatilistnik.org - сервер с которого мы будем реплицировать настройки (**DHCP сервер-партнер**)

Далее вам просто нужно сохранить его в формате ps1.

Создание PowerShell скрипта для репликации DHCP

- Создаем задание в планировщике Windows, которое по событию будет запускать ваш скрипт. Почему именно по событию, все просто, чтобы уменьшить количество бесполезного трафика и нагрузку на ваш сервер.

Когда вы производите новое резервирование IP-адреса на вашем DHCP сервере, у вас генерируется событие ID 106.

ID 106: Резервирование: [[192.168.31.109]] для IPv4 настроено в области [[192.168.31.0]192.168.31.0] через ROOT\Администратор.

Генерируется оно журналом **Microsoft-Windows-DHCP Server Events**.

Событие с кодом ID 106

И так, откройте планировщик событий, самый быстрый способ, это в окне "**Выполнить**", ввести **taskschd.msc**.

как открыть планировщик заданий

Щелкаем правым кликом и создаем новую, простую задачу.

Создание задания по репликации в DHCP

На первом шаге, вам необходимо придумать имя для вашей задачи, можно написать, что угодно, главное, чтобы вам было понятно.

Заполнение поля имени задачи в планировщике

Выбираем пункт "**При занесении в журнал указанного события**".

При занесении в журнал указанного события

Далее заполняем три пункта:

- Журнал - Microsoft-Windows-DHCP Server Events/Работает
- DHCP-Server
- Код события 106

> 1. создание задания в планировщике Windows по репликации областей DHCP

Оставляем пункт "**Запустить программу**".

Запуск программы через планировщик Windows

Далее в поле:

- Программа или сценарий, вы указываете powershell.exe
- В поле "Добавить аргументы" введите текст **-WindowStyle Hidden -File "C:\Scripts\dhcp-replication.ps1"**. Где **WindowStyle** - это указание не показывать диалоговое окно, а атрибут -**File** указывает путь до вашего скрипта PowerShell. Мы такое уже разбирали в методах запуска скрипта PowerShell.

Заполняем аргументы для запуска скрипта PowerShell

Смотрим сводную информацию и закрываем мастер настройки простого задания.

Завершение создания задания в планировщике

В результате ваше новое задание появится в списке.

Список заданий в планировщике

Далее нам необходимо открыть свойства вашего задания и в параметрах безопасности выбрать созданного ранее пользователя, от имени которого будет запускаться задание, далее выставить опцию "**Выполнить для всех пользователей**" и поставить галку "

Выполнить с наивысшими правами".

Все теперь ждем появления события ID 106, вы его сами можете вызвать, путем резервирования IP-адреса. Как видим у меня успешно отработало мое задание и все резервированные IP-адреса на текущем сервере, благополучно отреплецировались на DHCP-партнера.

С событием установки резервирования (ID 106) мы разобрались, но еще есть и обратная операция, это удаление резервирования IP-адреса за определенным компьютером, и тут генерируется событие **ID 107**.

ID 107: Резервирование: [[192.168.31.118]] для IPv4 удалено в области [[192.168.31.0]192.168.31.0] через ROOT\Администратор.

- Журнал Microsoft-Windows-DHCP Server Events/Работает
- Источник DHCP-Server

В итоге вам нужно создать такое же задание, как и в случае с ID 106, но сделать для ID 107 некоторые изменения. Теперь при включении и выключении аренды IP адреса, все области отработки будут автоматически согласованы и ошибок с ID 202091 и ID 20292 не должно быть.

Полный список переменных сред в Windows 10

VARIABLE	WINDOWS 10
%ALLUSERSPROFILE%	C:\ProgramData
%APPDATA%	C:\Users\{имя пользователя}\AppData\Roaming
%COMMONPROGRAMFILES%	C:\Program Files\Common Files
%COMMONPROGRAMFILES(x86)%	C:\Program Files (x86)\Common Files
%CommonProgramW6432%	C:\Program Files\Common Files
%COMSPEC%	C:\Windows\System32\cmd.exe
%HOMEDRIVE%	C:\
%HOMEPATH%	C:\Users\{имя пользователя}
%LOCALAPPDATA%	C:\Users\{имя пользователя}\AppData\Local
%LOGONSERVER%	\\{domain_logon_server}
%PATH%	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
%PathExt%	.com;.exe;.bat;.cmd;.vbs;.vbe;.js;.jse;.wsf;.wsh;.msc
%PROGRAMDATA%	C:\ProgramData
%PROGRAMFILES%	C:\Program Files
%ProgramW6432%	C:\Program Files
%PROGRAMFILES(X86)%	C:\Program Files (x86)
%PROMPT%	PG
%SystemDrive%	C:
%SystemRoot%	C:\Windows
%TEMP%	C:\Users\{имя пользователя}\AppData\Local\Temp
%TMP%	C:\Users\{имя пользователя}\AppData\Local\Temp
%USERDOMAIN%	Пользовательский домен, связанный с текущим пользователем.

VARIABLE	WINDOWS 10
%USERDOMAIN_ROAMINGPROFILE%	Пользовательский домен, связанный с перемещаемым профилем.
%USERNAME%	{имя пользователя}
%USERPROFILE%	C:\Users\{имя пользователя}
%WINDIR%	C:\Windows
%PUBLIC%	C:\Users\Public
%PSModulePath%	%SystemRoot%\system32\WindowsPowerShell\v1.0\Modules\
%OneDrive%	C:\Users\{имя пользователя}\OneDrive
%DriverData%	C:\Windows\System32\Drivers\DriverData
%CD%	Выводит текущий путь к каталогу. (Командная строка.)
%CMDCMDLINE%	Выводит командную строку, используемую для запуска текущего сеанса командной строки. (Командная строка.)
%CMDEXTVERSION%	Выводит количество текущих расширений командного процессора. (Командная строка.
%COMPUTERNAME%	Выводит имя системы.
%DATE%	Выводит текущую дату. (Командная строка.)
%TIME%	Время выхода. (Командная строка.)
%ERRORLEVEL%	Выводит число определяющих статус выхода предыдущей команды. (Командная строка.)
%PROCESSOR_IDENTIFIER%	Идентификатор процессора
%PROCESSOR_LEVEL%	Outputs processor level.
%PROCESSOR_REVISION%	Вывод ревизии процессора.
%NUMBER_OF_PROCESSORS%	Выводит количество физических и виртуальных ядер.
%RANDOM%	Выводит случайное число от 0 до 32767.
%OS%	Windows_NT

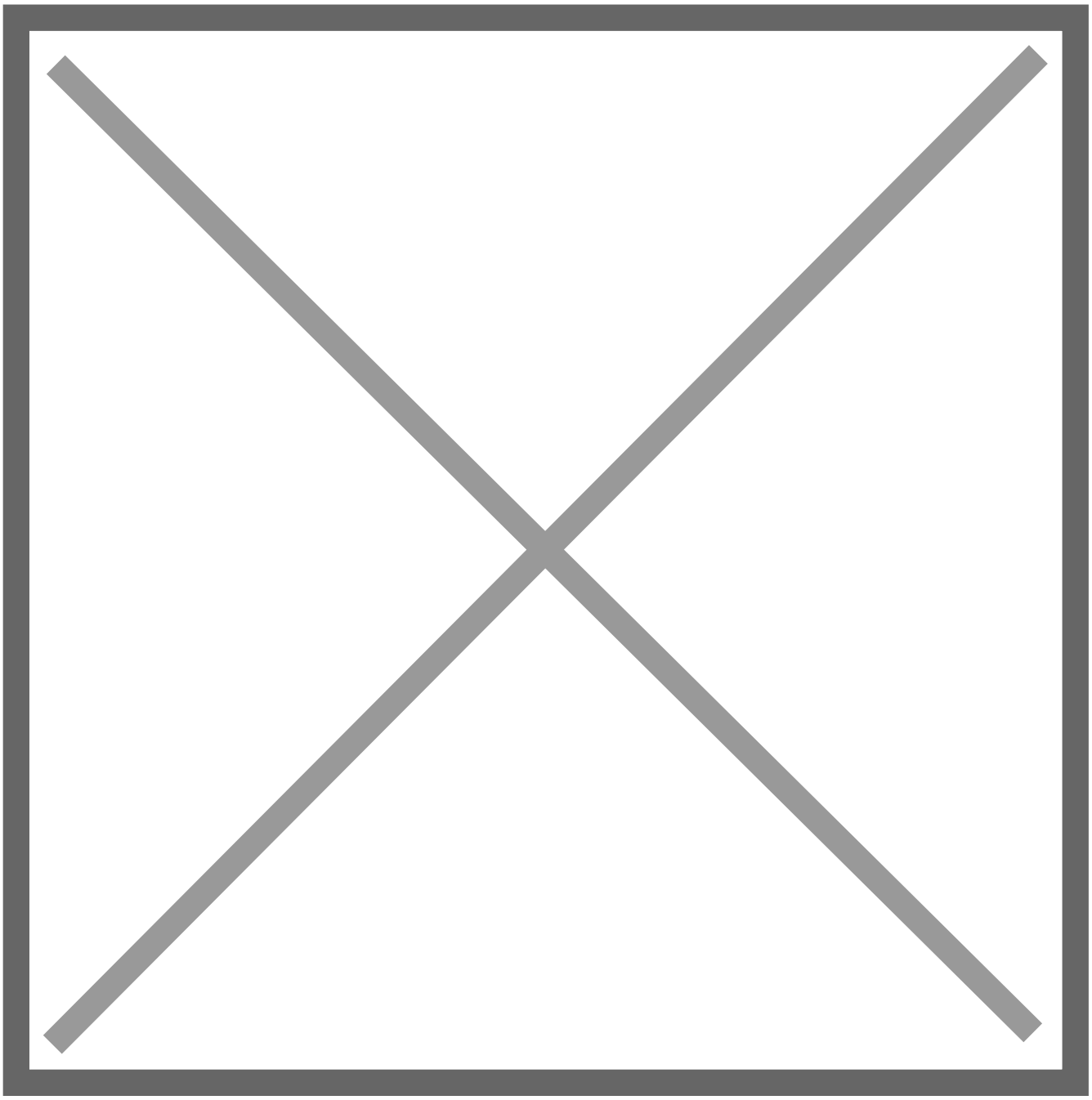
> Помните, что некоторые из упомянутых переменных не зависят от местоположения, в том числе **% COMPUTERNAME%, %PATHEXT%, %PROMPT%, %USERDOMAIN%, %USERNAME%.**

Управление ролями и функциями Windows Server с помощью PowerShell

Как через PowerShell вывести список всех установленных ролей и функций Windows Server

Используйте командлет Get-WindowsFeature, чтобы отобразить список всех доступных ролей и компонентов Windows Server. Если вы запустите его без параметров, вы увидите информацию обо всех компонентах Windows Server.

1	`Get-WindowsFeature`



Отображаются имя компонента (**Display Name**), его системное имя (**Name**) и состояние (**Install State**: **Installed**, **Available** или **Removed**). Список ролей и функций выглядит как дерево с вложенными ролями, подобное тому, которое вы видите при установке ролей в графическом интерфейсе Server Manager. Чтобы установить и удалить любые роли или компоненты с помощью PowerShell, вы должны знать их системные имена, указанные в столбце «Имя».

Подсказка: Если роль или функция удалены, это означает, что её установочные файлы удалены из системного компонента sote (для уменьшения размера папки WinSxS), и вы не сможете установить роль без доступа в Интернет или установочного ISO диска с Windows Server.

Вы можете удалить роли или компоненты из хранилища следующим образом:

1	`Uninstall-WindowsFeature -Name DHCP -Remove`

Чтобы установить удалённую роль DHCP, используйте этот командлет (вам понадобится прямой доступ в Интернет):

1	`Install-WindowsFeature DHCP`

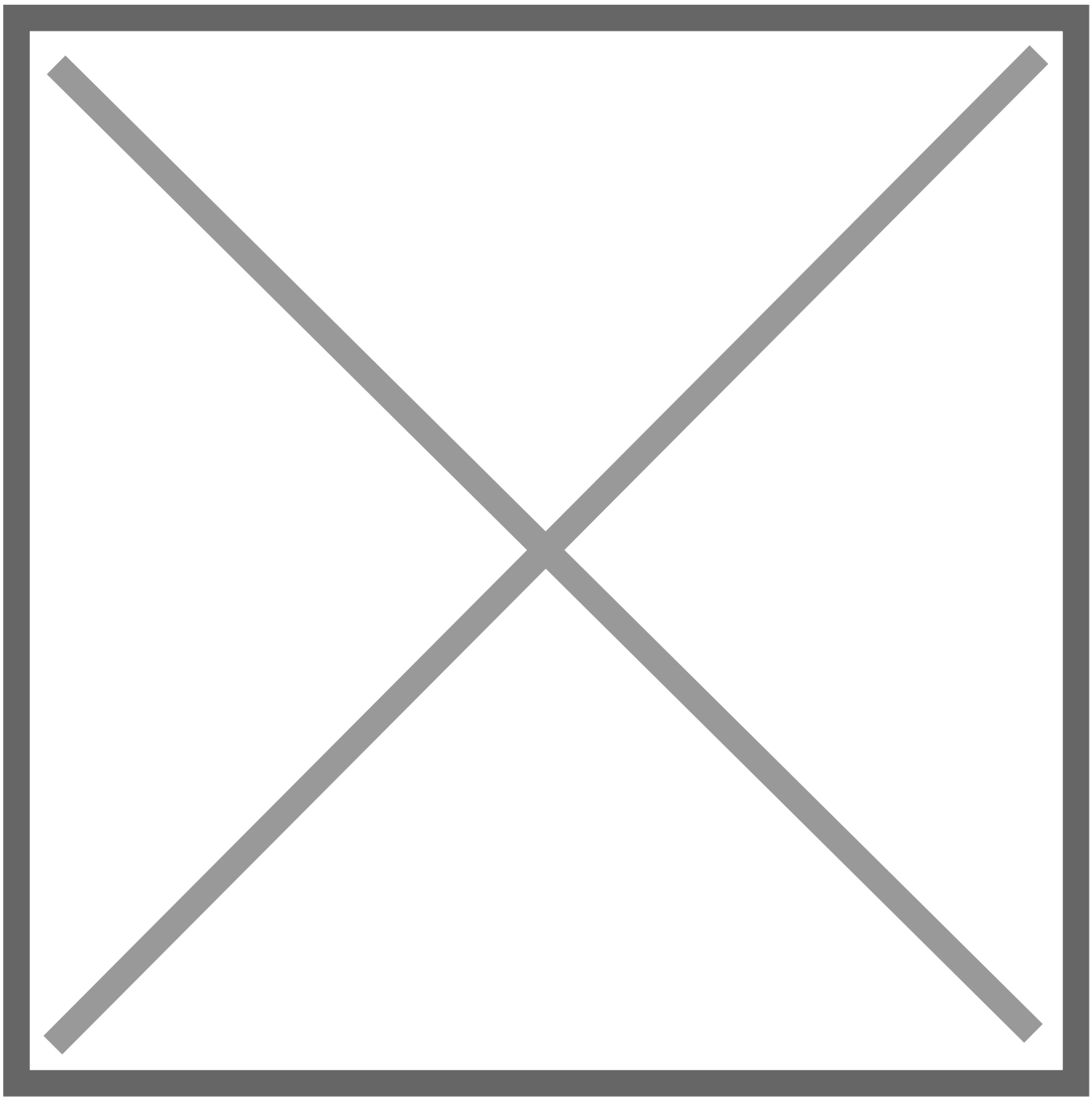
Или вы можете восстановить двоичные файлы компонентов из ISO-образа Windows Server:

1	`Install-WindowsFeature DHCP -Source E:\sources\sxs`

Вы можете перечислить установленные функции сервера:

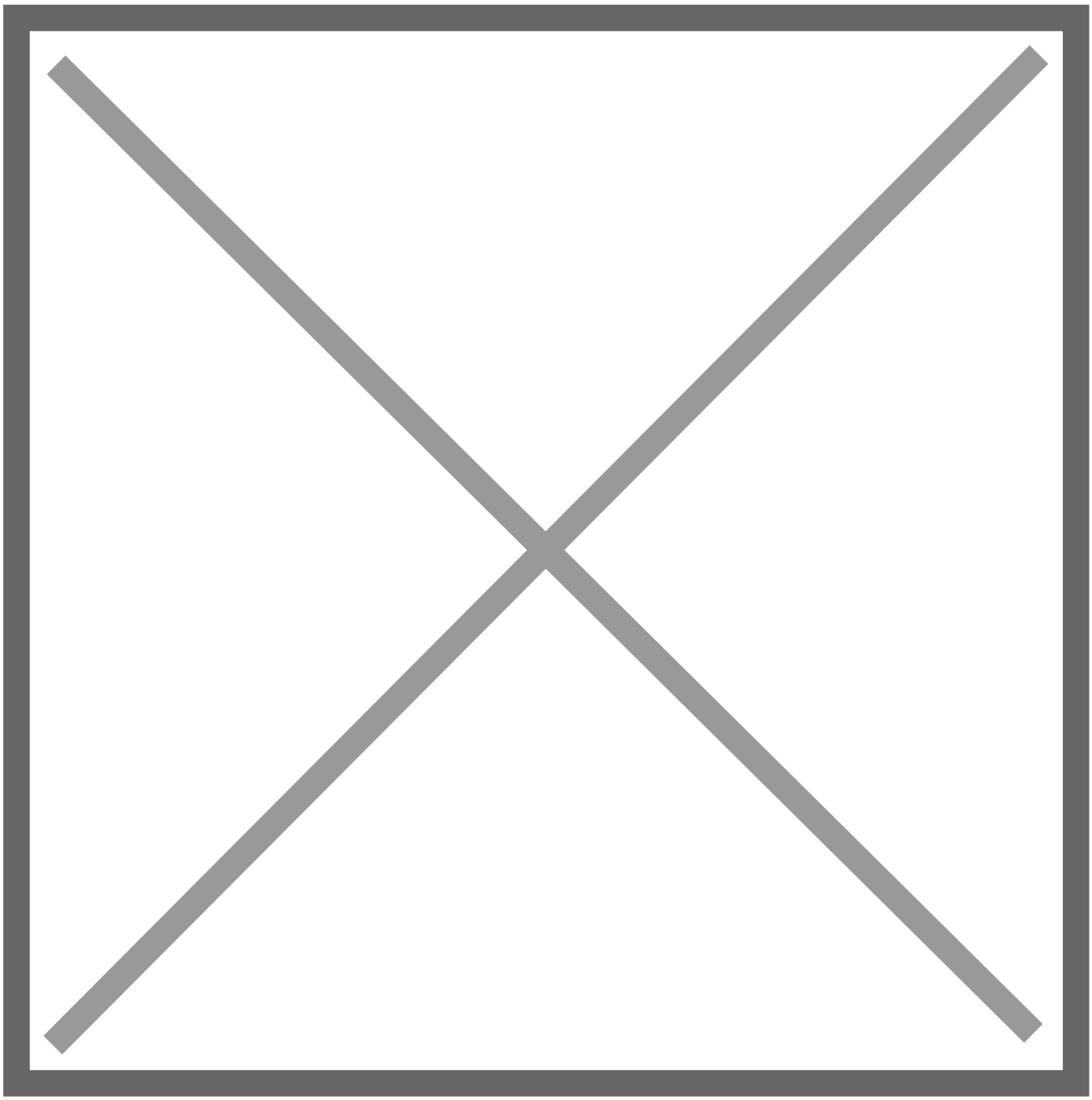
1	`Get-WindowsFeature | Where-Object {$_. installstate -` `eq` `"installed"` `} | ft Name,Installstate`

Судя по приведённому ниже снимку экрана, этот сервер используется в качестве контроллера домена (установлена роль **AD-Domain-Services**), DNS сервера (установлена роль **DNS**) и файлового сервера (установлены роли **FileAndStorage-Services**, **Storage-Services**). Большинство других компонентов используются для управления или мониторинга сервера.



Если вы точно не знаете имя роли, вы можете использовать подстановочные знаки. Например, чтобы проверить, какие веб-компоненты роли IIS установлены, выполните эту команду (синтаксис немного сокращён):

```
1 | Get-WindowsFeature -Name web-* | Where installed
```



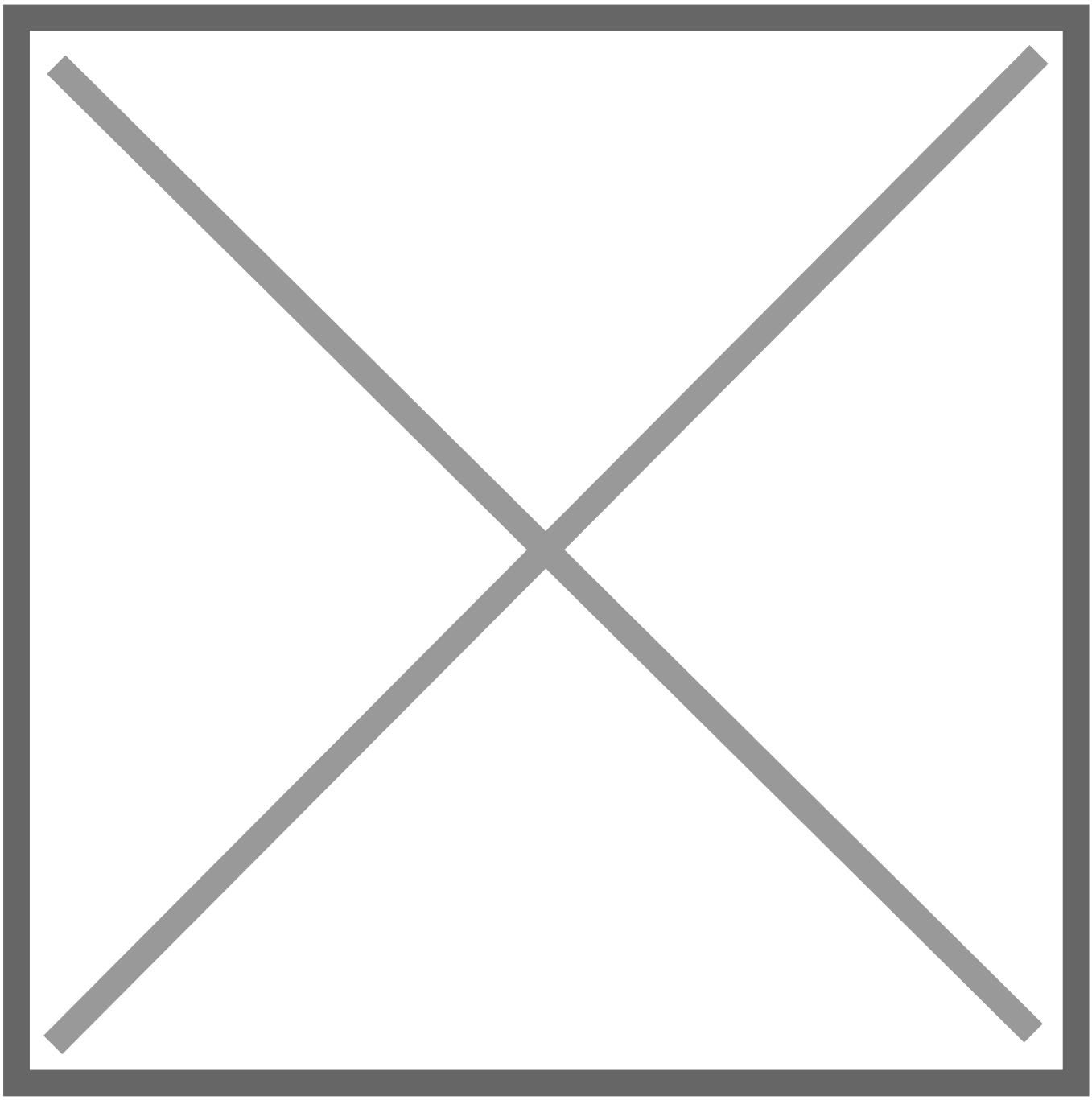
Вы можете получить список установленных компонентов на удалённом сервере Windows:

1	`Get-WindowsFeature -ComputerName ИМЯ_КОМПЬЮТЕРА | Where installed | ft Name,Installstate`

Вы можете использовать командлет **Get-WindowsFeature** для поиска серверов в вашем домене, на которых установлена определённая роль. Вы можете выполнять поиск на своих серверах в конкретном подразделении Active Directory с помощью командлета **Get-ADComputer** из модуля PowerShell ActiveDirectory или по предоставленному списку серверов **($ servers = ('server1', 'server2'))**.

Например, вы хотите найти все файловые серверы с ролью **FileAndStorage-Services** в указанном организационном подразделении AD, то используйте следующий скрипт:

```
Import-Module ActiveDirectory
$Servers=Get-ADComputer -Properties * -Filter {Operatingsystem -notlike "*2008 R2*" -and enabled -eq "true" -and Operatingsystem -like "*Windows Server*" } | select name
Foreach ($server in $Servers)
{
    Get-WindowsFeature -name FileAndStorage-Services -ComputerName $server.Name | Where installed | ft
$server.name, Name, Installstate
}
```



Пример поиска контроллера домена:

```
Import-Module ActiveDirectory
$Servers=Get-ADComputer -Properties * -Filter {Operatingsystem -notlike "*2008 R2*" -and enabled -eq "true" -and Operatingsystem -like "*Windows Server*" } | select name
Foreach ($server in $Servers)
{
    Get-WindowsFeature -name AD-Domain-Services -ComputerName $server.Name | Where installed | ft $server.name, Name, Installstate
}
```

В результате вы получите список серверов, на которых установлена конкретная роль.

Как с помощью PowerShell установить роли и компоненты Windows Server?

Для установки ролей и компонентов на Windows Server используется командлет Install-WindowsFeature.

Чтобы установить роль DNS-сервера и инструменты управления (включая модуль Powershell DNSServer) на текущий сервер, выполните следующую команду:

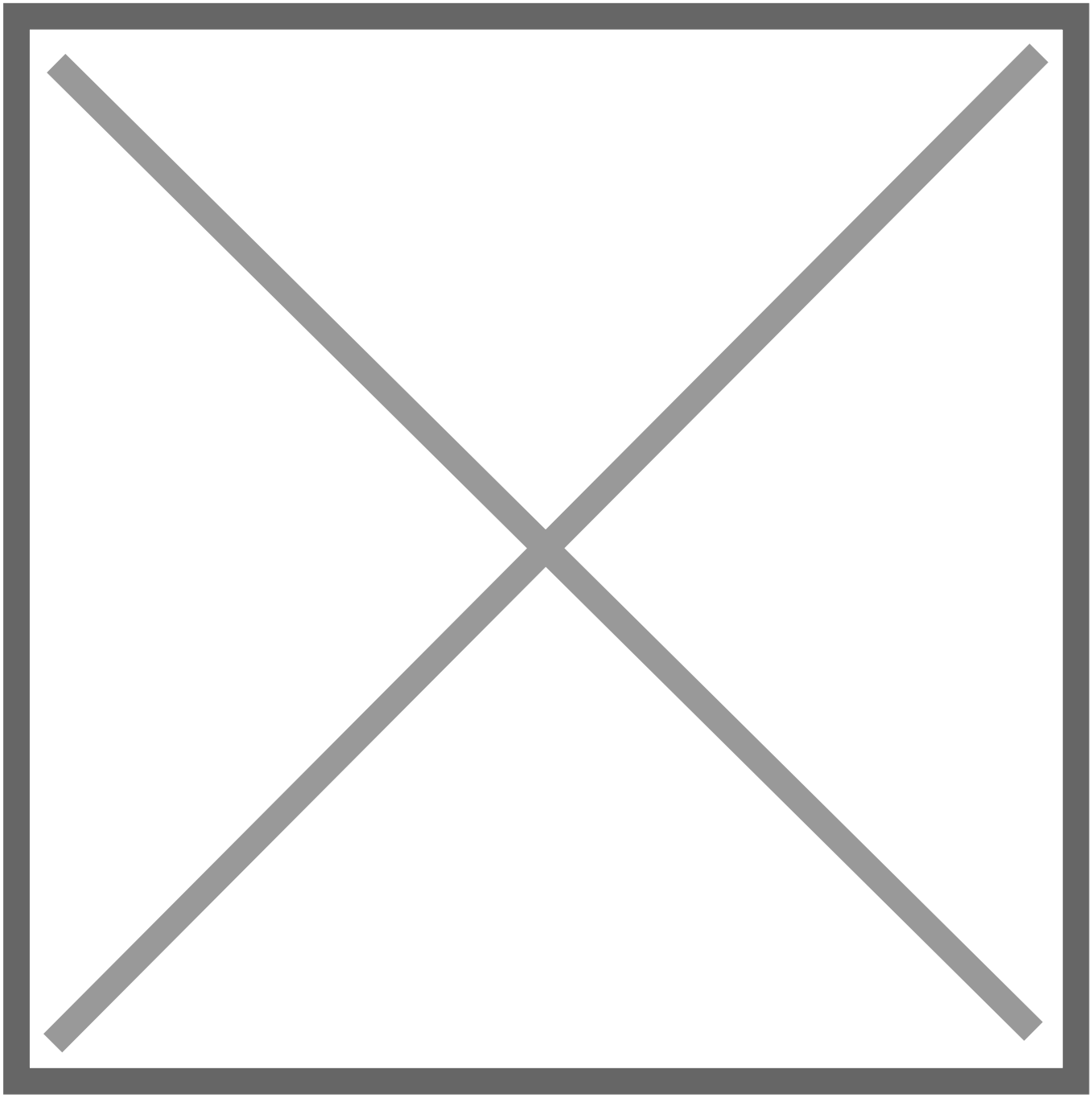
```
Install-WindowsFeature DNS -IncludeManagementTools
```

Установка роли «Active Directory Domain Services»:

```
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
```

По умолчанию командлет устанавливает все зависимые роли и компоненты. Чтобы отобразить список зависимостей перед установкой, используйте опцию **-WhatIf**:

```
Install-WindowsFeature -Name UpdateServices -WhatIf
```



Чтобы установить роль узла сеанса удалённого рабочего стола, роль лицензирования RDS и инструменты удалённого управления RDS, используйте следующую команду:

```
1 Install-WindowsFeature -ComputerName ИМЯ_КОМПЬЮТЕРА RDS-RD-Server, RDS-Licensing -IncludeAllSubFeature -IncludeManagementTools -Restart
```

Если вы добавите параметр **-Restart**, ваш сервер при необходимости будет автоматически перезагружен.

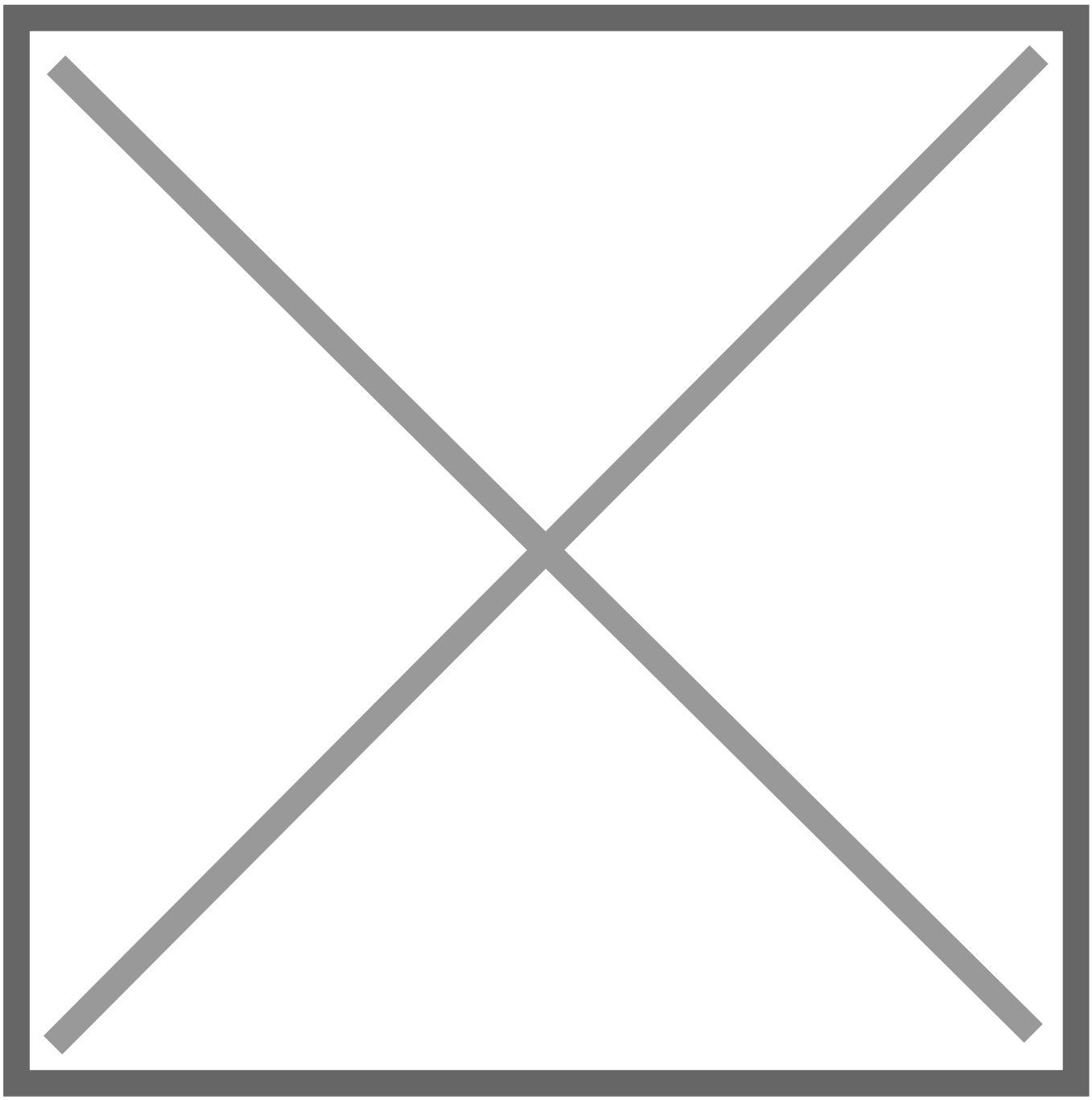
Вы также можете установить компонент с помощью следующей команды. Например, чтобы установить роль SMTP-сервера:

1	`Get-WindowsFeature -Name SMTP-Server | Install-WindowsFeature`

Как с помощью PowerShell развернуть роли на нескольких удалённых серверах Windows?

Есть ещё один интересный вариант при развёртывании типовых серверов. Вы можете установить необходимые функции на эталонном сервере Windows и экспортировать список установленных ролей в файл CSV:

1 2	`Get-WindowsFeature | where{$_.Installed -eq $True} | select name | Export-Csv C:\PS\InstalledRoles.csv -NoTypeInformation -Verbose` `Get-Content C:\PS\InstalledRoles.csv`



После этого вы сможете использовать этот CSV-файл для установки того же набора ролей на других типичных серверах:

1	`Import-Csv C:\PS\Roles.csv | foreach{ Install-WindowsFeature $_.name }`

Если роль или функция уже установлены, команда вернёт NoChangeNeeded и продолжит установку следующей роли.

Или, чтобы установить один и тот же набор ролей на нескольких удалённых серверах, вы можете использовать эту команду:

```
1
2
```

```
$servers = ( 'ny-rds1' , 'ny-rds2' ,'ny-rds3','ny-rds4')
foreach ($server in $servers) {Install-WindowsFeature RDS-RD-Server -ComputerName $server}
```

Как с помощью PowerShell удалить роль или компонент на Windows Server?

Чтобы удалить роли или функции Windows Server, используется командлет Remove-WindowsFeature.

Например, чтобы удалить роль сервера печати, выполните команду:

```
1
```

```
Remove-WindowsFeature Print-Server -Restart
```

Windows

Сертификат для Linux в центре сертификации Active Directory

Если в сети есть домен с контроллером и центр сертификации Microsoft, для внутреннего использования можно создавать собственные сертификаты, для которых браузер не будет выдавать ошибку. Если с запросом и установкой сертификата на Windows возникает меньше вопросов, то получение сертификата для Linux выполнить немного сложнее.

В этой статье мы создадим правильный сертификат с указанием альтернативного DNS-имени, без которого программы могут возвращать ошибку сертификата.

1. Формируем файл запроса (на компьютере с Linux)

Для начала создаем каталог, в котором планируем хранить сертификаты и перейдем в него, например:

mkdir -p /etc/ssl/adcs

cd /etc/ssl/adcs

Создаем закрытый ключ:

openssl genrsa -out private.key 2048

* *в данном примере создан **2048**-и битный ключ с именем **private.key***

Создаем файл с описанием запроса:

vi openssl.conf

```
[req]
default_bits = 2048
prompt = no
default_md = sha256
req_extensions = req_extensions
distinguished_name = dn

[dn]
C=RU
ST=SPb
L=SPb
O=Global Security
OU=IT Department
emailAddress=hostmaster@dmosk.ru
CN = *.dmosk.local

[req_extensions]
subjectAltName = @alter_name

[alter_name]
DNS.1 = *.dmosk.local
```

* *где стоит обратить внимание на следующее:*

- ***sha256 (или SHA-2)*** *— алгоритм шифрования;*
- ****.dmosk.local*** *— имя узла, к которому мы будем обращаться. Это очень важный пункт — нужно, чтобы имя совпадало с именем, по которому будут выполняться обращения. В данном примере создается wildcart (домен и все его поддомены)*
- **subjectAltName** — альтернативные имена стали иметь значение с 2017 года, когда некоторые браузеры перестали принимать сертификаты без указания альтернативных DNS-имен.

Далее создаем ключ запроса сертификата:

```
openssl req -new -key private.key -out request.csr -config openssl.conf
```

* *где* ***private.key*** *— закрытый ключ, который был сформирован на предыдущем шаге;* ***request.csr*** *— файл, который будет сформирован. В нем будет запрос на открытый ключ;*

После выполнения команды, в каталоге появится файл request.csr. Выведем его содержимое, чтобы посмотреть запрос:

```
cat request.csr
```

Должны увидеть что-то на подобие:

-----BEGIN CERTIFICATE REQUEST-----
MIIC1jCCAb4CAQAwgZAxCzAJBgNVBAYTAlJVMQwwCgYDVQQIDANTUGIxDDAKBgNV
BAcMA1NQYjEYMBYGA1UECgwPR2xvYmFsIFNlY3VyaXR5MRYwFAYDVQQLDA1JVCBE
ZXBhcnRtZW50MR4wHAYDVQQDDBVzaW1wbGVwbGFuLnNhdHMubG9jYWwxEzARBgNV
BAMMCnNpbXBsZXBsYW4wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDZ
ze/WOQgnlbfzlEsQUsmfUTnkYq0rCpzgjY360lFvqek5Y8NIFX/25PRbUy4N3D8r
c/7mXt2dXmcnn7zeRQOB2g0AY8Wmeg3R6C+JH7TwxtkMj7FO8R59URxFN84lu9Sj
26Aw+Ax7474XnAoUBMSmUXbV2mAP5Xm83sjvjE1OcHXN8SPbc+EchZuLVLsIGXHz
Emz7V4D/ecahfSc2hCRG2Pc7SeFIADYdjyoLtykz5WyiIoXkpEfSNQHlt2/A1kJ5
h9/GPXMVJVL02FgsI5HIGZyGnYWA+cP7sHoEDZNpLHHuEtfwx3bLxJPFnZDa0rPO
LhV/ux1e6b9ikrge0xp9AgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEAPVD2aVH8
ZDz+6s8ecKr08eT3mA9cRCa7dZYFj4/vO/ZYrDH9QS45gd0sYG+RN+JMGaFaY+X7
faE4m0BysPIbhEYLRY5GJYxmOGm05gM2HfPrcnnWXZbPQu/n5pR4ptvPYL7bilGb
z6hXb8ZtXUXwz1F2OgTPOPu4+w8lI23pzHRHlCXcVSoZxe/A2XwusB5MrtyMEYtj
rB2kcOqQRkt9uIv5IobwnYaVGDk/7wl/zkb9K+RKZt4izKfFaSSyPn7wvpKSIaAf
S3SQjJ0tBckLbtwKrxdFB0B8bpyIKUtHmpX/zOmityC8PLXe6/vQ/DmM3B6QC4Ba
KdnRkOSPv8BGog==
-----END CERTIFICATE REQUEST-----

Чтобы проверить содержимое запроса, вводим:

openssl req -noout -text -in request.csr

Мы увидем что-то на подобие:

```
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = RU, ST = SPb, L = SPb, O = Global Security, OU = IT Department, emailAddress
= hostmaster@dmosk.ru, CN = *.dmosk.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:e0:dd:17:1c:e1:24:25:80:fe:a0:b3:39:95:bf:
                    9f:3b:a6:3f:62:c6:fa:40:19:0e:11:fe:9b:22:5b:
                    0c:67:57:08:b6:f4:36:4c:9c:aa:de:0b:ee:f2:11:
                    35:fc:18:36:ed:f5:e0:f9:82:98:bf:a5:1a:6f:a8:
                    13:20:2e:96:2a:68:13:db:e6:8e:0a:ce:fc:ee:c1:
                    fb:35:55:63:3f:bd:be:21:e7:f2:f3:fc:d3:b0:fd:
                    04:84:ce:84:29:2a:66:a9:ee:53:0e:f1:06:a2:b7:
                    0d:1c:8a:b9:e3:5d:ca:55:c3:30:77:48:d3:eb:d4:
                    27:11:8f:28:33:da:d4:4d:05:b6:da:f7:ea:84:3b:
                    8f:97:7d:26:f5:6f:09:39:8a:79:fc:6e:d2:3a:db:
                    4e:e8:67:2a:a7:22:00:a0:6c:c1:99:50:ea:3c:f7:
```

```
                27:33:d3:5f:02:ed:7e:9e:66:17:fc:f3:af:f8:ef:
                36:9e:da:3d:6c:c7:d3:b3:8b:4b:45:12:2f:84:34:
                02:a5:0b:41:a1:6a:a3:91:6c:b0:87:d4:5b:cc:cc:
                f2:6c:17:4c:8b:46:40:65:5d:ca:8c:c0:f7:af:14:
                ad:58:1e:80:f5:67:16:1e:de:da:a5:7b:05:a6:f8:
                08:75:4b:8c:fe:53:e6:c8:50:00:30:ff:47:a5:49:
                47:c3
            Exponent: 65537 (0x10001)
    Attributes:
    Requested Extensions:
        X509v3 Subject Alternative Name:
            DNS:*.dmosk.local
Signature Algorithm: sha256WithRSAEncryption
     02:03:bc:8b:d3:4e:8f:2c:b2:a2:39:dd:9b:fb:33:a9:c1:49:
     95:b7:39:11:51:b2:40:dc:57:6c:3e:d5:66:6d:16:57:3f:15:
     03:cf:9b:39:95:1f:2b:13:09:86:f8:d5:69:b0:ac:cd:dc:64:
     9f:98:b7:f4:75:79:2a:16:d6:42:15:f4:1a:28:f3:3b:e3:f5:
     ec:34:98:f5:18:3e:72:95:ed:93:e5:e4:62:b3:3e:ce:71:09:
     9d:7f:ec:84:10:59:43:42:cd:0d:bd:4e:fd:c3:3e:44:ab:73:
     e0:ae:5d:67:c7:74:f0:30:0c:29:55:dc:16:4b:5f:a5:7f:be:
     8b:ec:64:3b:63:91:bb:48:d2:64:e5:8f:c0:09:db:7b:a3:10:
     8e:69:da:f7:88:00:a2:5a:60:dd:d9:3c:ef:b9:59:f4:b5:ab:
     00:d9:f9:31:6b:c1:c6:b1:ea:77:71:be:63:2c:e7:92:57:89:
     2a:5e:83:a9:e1:1c:56:c2:60:62:73:5d:bc:27:83:fb:bc:ca:
     9a:75:52:58:d6:02:d3:e8:37:b1:28:0e:89:62:97:9f:c4:f1:
     52:60:ed:95:59:2b:cd:69:29:9d:c2:30:1e:56:12:03:f4:17:
     3f:57:a2:b6:e7:b0:47:4e:0e:5a:b8:5e:0c:05:45:76:c5:49:
     f0:42:94:fa
```

2. Выпускаем сертификат

Копируем содержимое файла запроса (request.csr) и открываем веб-страницу центра сертификации — как правило, это имя сервера или IP-адрес + certsrv, например, http://192.168.0.15/certsrv/.

В открывшемся окне переходим по ссылкам **Запроса сертификата** - **расширенный запрос сертификата**.

В поле «Сохраненный запрос» вставляем скопированный запрос, в а поле «Шаблон сертификата» выбираем **Веб-сервер**:

Вводим данные для получения сертификата

Нажимаем **Выдать** и скачиваем сертификат по ссылке **Загрузить сертификат**:

3. Установка сертификата на Linux

Переносим полученный сертификат на компьютер с Linux.

После необходимо сконвертировать DER-сертификат (от AD CS) в PEM-сертификат (для Linux). Для этого вводим следующую команду:

openssl x509 -inform der -in certnew.cer -out public.pem

* *где **certnew.cer** — файл, который мы получили от центра сертификации AD CS (как правило, у него такое имя); **public.pem** — имя PEM-сертификата.*

Сертификат готов к использованию. Мы сформировали:

1. private.key — закрытый ключ.
2. public.pem — открытый ключ.

Репликация Active Directory

Repadmin: How to Check Active Directory Replication

Example 2: Summarize the replication status and view the overall health

The first command you should use is replsummary. This command will quickly show you the overall replication health. This command will show you the percentage of replication attempts that have failed as well as the largest replication deltas.

```
repadmin /replsummary
```

Results displayed

```
:\WINDOWS\system32>repadmin /replsummary
Replication Summary Start Time: 2018-03-13 04:44:54

Beginning data collection for replication summary, this may take awhile:
  .....


Source DSA          largest delta    fails/total %%   error
 DC1                       52m:48s    0 /   5    0
 DC2                       52m:46s    0 /   5    0


Destination DSA     largest delta    fails/total %%   error
```

```
DC1                     52m:46s    0 /   5    0
DC2                     52m:48s    0 /   5    0
```

Example 3: Show replication partner and status

Next, use the following command to see the replication partner as well as the replication status. This helps you understand the role of each domain controller in the replication process.

In addition, this command displays the GUID of each object that was replicated and its result. This is helpful to identify what objects are failing to replicate.

```
repadmin /showrepl
```

Results displayed

```
C:\Users\rallen>repadmin /showrepl

Repadmin: running command /showrepl against full DC dc1.ad.activedirectorypro.com
Default-First-Site-Name\DC1
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: a4d22a63-1918-492a-bcd6-7fe286941e72
DSA invocationID: a4d22a63-1918-492a-bcd6-7fe286941e72

==== INBOUND NEIGHBORS ======================================

DC=ad,DC=activedirectorypro,DC=com
    Default-First-Site-Name\DC2 via RPC
        DSA object GUID: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408
        Last attempt @ 2018-03-13 03:52:08 was successful.

CN=Configuration,DC=ad,DC=activedirectorypro,DC=com
    Default-First-Site-Name\DC2 via RPC
        DSA object GUID: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408
        Last attempt @ 2018-03-13 03:52:08 was successful.

CN=Schema,CN=Configuration,DC=ad,DC=activedirectorypro,DC=com
    Default-First-Site-Name\DC2 via RPC
        DSA object GUID: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408
        Last attempt @ 2018-03-13 03:52:08 was successful.

DC=DomainDnsZones,DC=ad,DC=activedirectorypro,DC=com
    Default-First-Site-Name\DC2 via RPC
        DSA object GUID: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408
        Last attempt @ 2018-03-13 03:52:08 was successful.
```

```
DC=ForestDnsZones,DC=ad,DC=activedirectorypro,DC=com
    Default-First-Site-Name\DC2 via RPC
        DSA object GUID: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408
        Last attempt @ 2018-03-13 03:52:08 was successful.
```

Example 4: Show replication partner for a specific domain controller

If you want to see the replication status for a specific domain controller use this command.

replace <ServerName> with the name of your domain controller.

```
repadmin /showrepl <ServerName>
```

Results displayed

```
C:\WINDOWS\system32>repadmin /showrepl dc2
Default-First-Site-Name\DC2
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408
DSA invocationID: 2eb95693-bfa7-4f3f-b52c-139737aa883f

==== INBOUND NEIGHBORS ======================================

DC=ad,DC=activedirectorypro,DC=com
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: a4d22a63-1918-492a-bcd6-7fe286941e72
        Last attempt @ 2018-03-14 04:21:02 was successful.

CN=Configuration,DC=ad,DC=activedirectorypro,DC=com
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: a4d22a63-1918-492a-bcd6-7fe286941e72
        Last attempt @ 2018-03-14 03:52:07 was successful.

CN=Schema,CN=Configuration,DC=ad,DC=activedirectorypro,DC=com
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: a4d22a63-1918-492a-bcd6-7fe286941e72
        Last attempt @ 2018-03-14 03:52:07 was successful.

DC=DomainDnsZones,DC=ad,DC=activedirectorypro,DC=com
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: a4d22a63-1918-492a-bcd6-7fe286941e72
        Last attempt @ 2018-03-14 03:52:07 was successful.

DC=ForestDnsZones,DC=ad,DC=activedirectorypro,DC=com
```

```
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: a4d22a63-1918-492a-bcd6-7fe286941e72
        Last attempt @ 2018-03-14 03:52:07 was successful.
```

Example 5: Show only Replication Errors

The showrepl command can output a lot of information. If you want to see only the errors use this command. In this example, DC2 is down, you can see the results are all errors from DC2.

```
C:\WINDOWS\system32>repadmin /showrepl /errorsonly

Repadmin: running command /showrepl against full DC dc1.ad.activedirectorypro.com
Default-First-Site-Name\DC1
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: a4d22a63-1918-492a-bcd6-7fe286941e72
DSA invocationID: a4d22a63-1918-492a-bcd6-7fe286941e72

==== INBOUND NEIGHBORS ======================================

DC=ad,DC=activedirectorypro,DC=com
    Default-First-Site-Name\DC2 via RPC
        DSA object GUID: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408
        Last attempt @ 2018-03-15 04:19:38 failed, result 8524 (0x214c):
            The DSA operation is unable to proceed because of a DNS lookup failure.
        1 consecutive failure(s).
        Last success @ 2018-03-14 07:52:08.

CN=Configuration,DC=ad,DC=activedirectorypro,DC=com
    Default-First-Site-Name\DC2 via RPC
        DSA object GUID: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408
        Last attempt @ 2018-03-15 04:19:38 failed, result 8524 (0x214c):
            The DSA operation is unable to proceed because of a DNS lookup failure.
        1 consecutive failure(s).
        Last success @ 2018-03-14 07:52:08.

CN=Schema,CN=Configuration,DC=ad,DC=activedirectorypro,DC=com
    Default-First-Site-Name\DC2 via RPC
        DSA object GUID: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408
        Last attempt @ 2018-03-15 04:19:38 failed, result 8524 (0x214c):
            The DSA operation is unable to proceed because of a DNS lookup failure.
        1 consecutive failure(s).
        Last success @ 2018-03-14 07:52:08.

DC=DomainDnsZones,DC=ad,DC=activedirectorypro,DC=com
    Default-First-Site-Name\DC2 via RPC
        DSA object GUID: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408
        Last attempt @ 2018-03-15 04:19:38 failed, result 8524 (0x214c):
            The DSA operation is unable to proceed because of a DNS lookup failure.
```

```
        1 consecutive failure(s).
        Last success @ 2018-03-14 07:52:08.

DC=ForestDnsZones,DC=ad,DC=activedirectorypro,DC=com
    Default-First-Site-Name\DC2 via RPC
        DSA object GUID: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408
        Last attempt @ 2018-03-15 04:19:38 failed, result 8524 (0x214c):
            The DSA operation is unable to proceed because of a DNS lookup failure.
        1 consecutive failure(s).
        Last success @ 2018-03-14 07:52:08.

Source: Default-First-Site-Name\DC2
******* 1 CONSECUTIVE FAILURES since 2018-03-14 07:52:08
Last error: 8524 (0x214c):
            The DSA operation is unable to proceed because of a DNS lookup failure.
```

Example 6: Show replication Queue

It is normal to see items in the queue. If you have a small environment it will often be at zero because there are few replications that occur. If you notice items sitting in the queue and they never clear out, you have a problem.

Use this command to view the replication queue

```
Repadmin /Queue
```

Results displayed

```
C:\Users\rallen>repadmin /queue

Repadmin: running command /queue against full DC dc1.ad.activedirectorypro.com
Queue contains 0 items.
```

Example 7: How to Force Active Directory Replication

Use the following command if you want to force replication between domain controllers. You will want to run this on the DC that you wish to update. For example, if DC1 is out of sync I would run this on DC1.

This will do a pull replication, which means it will pull updates from DC2 to DC1.

```
repadmin /syncall dc1 /Aed
```

If you want to push replication you will use the /P switch. For example if you make changes on DC1 and want to replicate those to other DCs use this command.

```
repadmin /syncall dc1 /APed
```

Results displayed

```
C:\WINDOWS\system32>repadmin /syncall dc1 /Aed
Syncing all NC's held on dc1.
Syncing partition: DC=ForestDnsZones,DC=ad,DC=activedirectorypro,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408._msdcs.ad.activedirectorypro.com
    To  : a4d22a63-1918-492a-bcd6-7fe286941e72._msdcs.ad.activedirectorypro.com
CALLBACK MESSAGE: The following replication completed successfully:
    From: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408._msdcs.ad.activedirectorypro.com
    To  : a4d22a63-1918-492a-bcd6-7fe286941e72._msdcs.ad.activedirectorypro.com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

Syncing partition: DC=DomainDnsZones,DC=ad,DC=activedirectorypro,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408._msdcs.ad.activedirectorypro.com
    To  : a4d22a63-1918-492a-bcd6-7fe286941e72._msdcs.ad.activedirectorypro.com
CALLBACK MESSAGE: The following replication completed successfully:
    From: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408._msdcs.ad.activedirectorypro.com
    To  : a4d22a63-1918-492a-bcd6-7fe286941e72._msdcs.ad.activedirectorypro.com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

Syncing partition: CN=Schema,CN=Configuration,DC=ad,DC=activedirectorypro,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408._msdcs.ad.activedirectorypro.com
    To  : a4d22a63-1918-492a-bcd6-7fe286941e72._msdcs.ad.activedirectorypro.com
CALLBACK MESSAGE: The following replication completed successfully:
    From: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408._msdcs.ad.activedirectorypro.com
    To  : a4d22a63-1918-492a-bcd6-7fe286941e72._msdcs.ad.activedirectorypro.com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

Syncing partition: CN=Configuration,DC=ad,DC=activedirectorypro,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408._msdcs.ad.activedirectorypro.com
    To  : a4d22a63-1918-492a-bcd6-7fe286941e72._msdcs.ad.activedirectorypro.com
CALLBACK MESSAGE: The following replication completed successfully:
    From: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408._msdcs.ad.activedirectorypro.com
    To  : a4d22a63-1918-492a-bcd6-7fe286941e72._msdcs.ad.activedirectorypro.com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

Syncing partition: DC=ad,DC=activedirectorypro,DC=com
CALLBACK MESSAGE: The following replication is in progress:
```

```
    From: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408._msdcs.ad.activedirectorypro.com
    To  : a4d22a63-1918-492a-bcd6-7fe286941e72._msdcs.ad.activedirectorypro.com
CALLBACK MESSAGE: The following replication completed successfully:
    From: 57a1cfbc-88bb-41da-a1a6-f14f5c9df408._msdcs.ad.activedirectorypro.com
    To  : a4d22a63-1918-492a-bcd6-7fe286941e72._msdcs.ad.activedirectorypro.com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
```

Example 8: Export results to text file

Sometimes these commands can display a lot of information. You can export any of the examples above to a text file, this makes it a little easier to review at a later time or save for documentation.

just add > c:\destination folder\filename.txt to the end of any of the commands

Here are a few examples

```
repadmin /replsummary > c:\it\replsummary.txt
```

```
repadmin /showrepl > c:\it\showrepl.txt
```

More examples

Find the last time your DC was backed up

```
Repadmin /showbackup *
```

Displays calls that have not yet been answered

```
repadmin /showoutcalls *
```

List the Topology information

```
repadmin /bridgeheads * /verbose
```

Inter Site Topology Generator Report

```
repadmin /istg * /verbose
```

Conclusion

As a system administrator, it is important that you know how to troubleshoot and verify replication is working correctly. The repadmin is a simple yet powerful tool that you should know how to use.

I hope you found this guide useful. If you have any questions leave a comment below. If you liked this article, check out: How to Use NSLookup to Check DNS Records.

Подпись файлов signtool.exe

> Требуется установить SDK - Windows Kits

C:\Program Files (x86)\Windows Kits\10\bin\10.0.19041.0\x64>signtool.exe sign /f C:\Users\baa\Desktop\PSO.pfx /p Qwerty123 /fd sha256 /tr http://timestamp.digicert.com /td sha256 C:\Users\baa\Desktop\pso.exe

/f C:\Users\baa\Desktop\PSO.pfx - Требуется указать путь до сертификата

/p Qwerty123 - Пароль серта

/fd sha256 - Указывает алгоритм хеширования файла

/tr http://timestamp.digicert.com - Указывает URL-адрес сервера меток времени

/td sha256 - Используется с `/tr` опцией `-` для запроса алгоритма, используемого сервером временных меток RFC 3161

C:\Users\baa\Desktop\pso.exe - Подписываемый файл

Сети

Networking

Сети

Кто слушает порт в Linux

Открытый доступ к порту хоть и является угрозой безопасности системы, но по сути ничего плохого не представляет до тех пор, пока его не начинает использовать программа. А чтобы выяснить какая программа слушает какой порт можно использовать утилиты "netstat" (или "ss") и "lsof".

Чтобы узнать информацию о программе, которая прослушивает определённый порт, можно воспользоваться командой "lsof" со следующими ключами:

```
sudo lsof -i :номер_порта
```

Здесь "номер_порта" - это цифра.

Пример результата выполнения команды с 53 портом:

```
$: sudo lsof -i :53
COMMAND   PID            USER   TYPE NODE NAME
systemd-r 818 systemd-resolve   IPv4  UDP localhost:domain
systemd-r 818 systemd-resolve   IPv4  TCP localhost:domain (LISTEN)
```

Но рекомендуем чаще запускать команду для получения списка программ, которые используют какие-либо tcp/udp порты. В этом помогает "netstat" или "ss":

```
sudo netstat -lntup
```

Опишем все ключи, которые используются в команде

- -l показать только прослушиваемые "LISTEN" порты.
- -n показывать адреса как ip, а не пытаться определять домены.
- -t показывать TCP порты.
- -u показывать UDP порты.
- -p показать название программы, которая слушает порт.

Если запустить эту команду на веб сервере, то команда распечатает в терминале такую информацию (некоторые столбцы скрыты):

```
$: sudo netstat -lntup
Prt  Local Addr     State   PID/Program
tcp  0.0.0.0:443    LISTEN  204/nginx
tcp  0.0.0.0:80     LISTEN  202/nginx
tcp  0.0.0.0:22     LISTEN  174/sshd
```

```
udp  127.0.0.1:323          233/chronyd
```

По результату можно заметить какая программа прослушивает какой порт. Если ip в секции "Local Address" равен "127.0.0.1", то это локальное обращение. Такой порт можно не закрывать фаерволом - он и так не будет доступен извне. Но ip с нулями "0.0.0.0" говорят о том, что программа слушает все адреса. То есть она примет любой запрос, в том числе внешний.

Работа с дисками

Работа с дисками parted

Before allocation:

```
server:/$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.5G     0  1.5G   0% /dev
tmpfs           301M  1.1M  300M   1% /run
/dev/sda2        16G   13G  2.4G  84% /
tmpfs           1.5G     0  1.5G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.5G     0  1.5G   0% /sys/fs/cgroup
/dev/loop0       91M   91M     0 100% /snap/core/6350
tmpfs           301M     0  301M   0% /run/user/1000
```

Now extend the partition:

```
server:/$ sudo parted
[sudo] password for username:
GNU Parted 3.2
Using /dev/sda
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) print
Model: VMware Virtual disk (scsi)
Disk /dev/sda: 32.2GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:
Number  Start   End     Size    File system  Name  Flags
 1      1049kB  2097kB  1049kB                     bios_grub
 2      2097kB  17.2GB  17.2GB  ext4
(parted) resizepart 2
Warning: Partition /dev/sda2 is being used. Are you sure you want to continue?
Yes/No? Yes
End?  [17.2GB]? 32.2GB
(parted) q
Information: You may need to update /etc/fstab.
```

5. Thereafter, grow the filesystem using the *resize2fs:*

```
server:/$ sudo resize2fs /dev/sda2
resize2fs 1.44.1 (24-Mar-2018)
Filesystem at /dev/sda2 is mounted on /; on-line resizing required
old_desc_blocks = 2, new_desc_blocks = 4
The filesystem on /dev/sda2 is now 7860816 (4k) blocks long.
```

Finally, the disk capacity has increased:

```
server:/$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.5G     0  1.5G   0% /dev
tmpfs           301M  1.1M  300M   1% /run
/dev/sda2        30G   15G   14G  53% /
tmpfs           1.5G     0  1.5G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.5G     0  1.5G   0% /sys/fs/cgroup
/dev/loop0       91M   91M     0 100% /snap/core/6350
tmpfs           301M     0  301M   0% /run/user/1000
```

Работа с дисками lvm

Команды с описанием

`df -h` - отображает статус дисков в файловой системе

`fdisk -l` - показать какие есть диски

`lsblk` - показать какие есть диски

`cfdisk /dev/sdb` - редактирование раздела sdb

`/etc/fstab` - тут прописываем новые диски

`mount /media/hdd2` - присоединяет диск, прописанный в файле *fstab* с именем *hdd2*

Обновление инфы о дисках

```
echo 1 > /sys/block/sda/device/rescan
```

```
echo "- - -" | tee /sys/class/scsi_host/host*/scan
```

How to add an extra second hard drive on Linux LVM and increase the size of storage

Author: Vivek Gite Last updated: August 6, 2023 48 comments

Ihave 250GB disk installed on my home Linux server. I just bought a brand new 250GB SATA disk and I want to add a new disk to my existing LVM volume to increase its size total size to 500GB. How do I add a disk to LVM and extend an LVM volume on Linux operating system?

Logical volume management (LVM) creates an easy to use layer over physical disks. You can combine multiple disks and create logical storage volumes. This provides specific benefits such as:

1. No restriction on disk size
2. Increased disk throughput
3. Mirroring volumes for business critical data
4. Volume snapshots
5. Easy backups and restores using snapshots
6. Easy data relocation
7. Resizing storage pools (add or remove disks) without reformatting disks

This tutorial **shows you how to make partitioning, formatting, and add a new disk to LVM volume on Linux**. For demo purpose, I am using Ubuntu VM, but the commands remain same for bare metal or any other virtualization technology such as KVM, Xen, VMware and so on.

Warning: Be careful with lvm/mkfs.ext4 and other commands, and device names as wrong device name can wipe out all data. **Proceed with caution** and always keep full backups. The nixCraft or author is not responsible for data loss.

Step 1 – Find out information about existing LVM

LVM Storage Management divided into three parts:

1. **Physical Volumes (PV)** – Actual disks (e.g. /dev/sda, /dev,sdb, /dev/vdb and so on)
2. **Volume Groups (VG)** – Physical volumes are combined into volume groups. (e.g. my_vg = /dev/sda + /dev/sdb.)
3. **Logical Volumes (LV)** – A volume group is divided up into logical volumes (e.g. my_vg divided into my_vg/data, my_vg/backups, my_vg/home, my_vg/mysqldb and so on)

Type the following commands to find out information about each part.

How to display physical volumes (pv)

Type the following pvs command to see info about physical volumes:

```
$ sudo pvs
```

Sample outputs:

Fig.01: How to display information about LVM physical volumes

Fig.01: How to display information about LVM physical volumes

So currently my LVM include a physical volume (actual disk) called /dev/vda5. To see detailed attributes information, type:

```
$ sudo pvdisplay
```

Sample outputs:

Fig.02: See attributes of a physical volume (PV)

Fig.02: See attributes of a physical volume (PV)

From above output it is clear that our volume group named ubuntu-box-1-vg is made of a physical volume named /dev/vda5.

How to display information about LVM volume Groups (vg)

Type any one of the following vgs command/vgdisplay command to see information about volume groups and its attributes:

```
$ sudo vgs
```

OR

```
$ sudo vgdisplay
```

Sample outputs:

Fig.03: How to see information about LVM volume groups (vg)

Fig.03: How to see information about LVM volume groups (vg)

How to display information about LVM logical volume (lv)

Type any one of the following lvs command/lvdisplay command to see information about volume groups and its attributes:

```
$ sudo lvs
```

OR

```
$ sudo lvdisplay
```

Sample outputs:

Fig.04: How to display information about logical volumes (lv)
Fig.04: How to display information about logical volumes (lv)

My ubuntu-box-1-vg volume group divided into two logical volumes:

1. /dev/ubuntu-box-1-vg/root – Root file system
2. /dev/ubuntu-box-1-vg/swap_1 – Swap space

Based upon above commands, you can get a basic idea how LVM organizes storage device into Physical Volumes (PV), Volume Groups (VG), and Logical Volumes (LV):

Fig.05: How LVM organizes storage device into Physical Volumes (PV), Volume Groups (VG), & Logic
Fig.05: How LVM organizes storage device into Physical Volumes (PV), Volume Groups (VG), & Logical Volumes (LV)

Step 2 – Find out information about new disk

You need to add a new disk to your server. In this example, for demo purpose I added a new disk drive, and it has 5GiB size. To find out information about new disks run:
`$ sudo fdisk -l`
OR
`$ sudo fdisk -l | grep '^Disk /dev/'`
Sample outputs:

Fig.06: Find out installed disk names on Linux
Fig.06: Find out installed disk names on Linux

Another option is to scan for all devices visible to LVM2:
`$ sudo lvmdiskscan`
Sample outputs:

```
  /dev/ram0                 [      64.00 MiB]
  /dev/ubuntu-box-1-vg/root [      37.49 GiB]
  /dev/ram1                 [      64.00 MiB]
  /dev/ubuntu-box-1-vg/swap_1 [       2.00 GiB]
  /dev/vda1                 [     487.00 MiB]
  /dev/ram2                 [      64.00 MiB]
  /dev/ram3                 [      64.00 MiB]
```

```
  /dev/ram4                  [      64.00 MiB]
  /dev/ram5                  [      64.00 MiB]
  /dev/vda5                  [      39.52 GiB] LVM physical volume
  /dev/ram6                  [      64.00 MiB]
  /dev/ram7                  [      64.00 MiB]
  /dev/ram8                  [      64.00 MiB]
  /dev/ram9                  [      64.00 MiB]
  /dev/ram10                 [      64.00 MiB]
  /dev/ram11                 [      64.00 MiB]
  /dev/ram12                 [      64.00 MiB]
  /dev/ram13                 [      64.00 MiB]
  /dev/ram14                 [      64.00 MiB]
  /dev/ram15                 [      64.00 MiB]
  /dev/vdb                   [       5.00 GiB]
  2 disks
  18 partitions
  0 LVM physical volume whole disks
  1 LVM physical volume
```

Step 3 – Create physical volumes (pv) on new disk named /dev/vdb

Type the following command:

```
$ sudo pvcreate /dev/vdb
```

Sample outputs:

```
  Physical volume "/dev/vdb" successfully created
```

Now run the following command to verify:

```
$ sudo lvmdiskscan -l
```

Sample outputs:

```
  WARNING: only considering LVM devices
  /dev/vda5                  [      39.52 GiB] LVM physical volume
  /dev/vdb                   [       5.00 GiB] LVM physical volume
  1 LVM physical volume whole disk
  1 LVM physical volume
```

Step 4 – Add newly created pv named /dev/vdb to an existing lv

Type the following command to add a physical volume /dev/vdb to “ubuntu-box-1-vg” volume group:

```
$ sudo vgextend ubuntu-box-1-vg /dev/vdb
```

Sample outputs:

```
  Volume group "ubuntu-box-1-vg" successfully extended
```

Finally, you need extend the /dev/ubuntu-box-1-vg/root to create total 45GB (/dev/vdb (5G)+ existing /dev/ubuntu-box-1-vg/root (40G))

```
$ sudo lvm lvextend -l +100%FREE /dev/ubuntu-box-1-vg/root
```

Sample outputs:

```
  Size of logical volume ubuntu-box-1-vg/root changed from 37.49 GiB (9597 extents) to 42.52 GiB
  Logical volume root successfully resized.
```

However, if you run df -h or any other command you will still see /dev/ubuntu-box-1-vg/root as 40G. You need to run the following command to enlarge the filesystem created inside the “root” volume:

```
$ sudo resize2fs -p /dev/mapper/ubuntu--box--1--vg-root
```

Sample outputs:

```
resize2fs 1.42.13 (17-May-2015)
Filesystem at /dev/mapper/ubuntu--box--1--vg-root is mounted on /; on-line resizing required
old_desc_blocks = 3, new_desc_blocks = 3
The filesystem on /dev/mapper/ubuntu--box--1--vg-root is now 11146240 (4k) blocks long.
```

Verify it again using the df command or mount command. For example:

```
$ mount
```

```
$ mount | grep '/dev/mapper/ubuntu'
```

OR

```
$ df -H
```

Sample outputs:

```
Filesystem                          Size  Used Avail Use% Mounted on
udev                                1.1G     0  1.1G   0% /dev
tmpfs                               146M   12M  135M   9% /run
/dev/mapper/ubuntu--box--1--vg-root  45G  2.3G   41G   6% /
tmpfs                               512M     0  512M   0% /dev/shm
tmpfs                               5.3M     0  5.3M   0% /run/lock
tmpfs                               512M     0  512M   0% /sys/fs/cgroup
/dev/vda1                           495M  109M  361M  24% /boot
tmpfs                               103M     0  103M   0% /run/user/0
```

Изменения размера раздела

Complete Steps and Explanation

ssh to server, sudo -i to become root

Confirm there is a limited amount of disk space. In the output below, note the / (root) volume only has 3.9 GB disk space:

```
user@server:~$ df -h
Filesystem Size Used Avail Use% Mounted on
udev 1.9G 0 1.9G 0% /dev
tmpfs 394M 1.1M 393M 1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv 3.9G 3.2G 489M 87% /
tmpfs 2.0G 0 2.0G 0% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 2.0G 0 2.0G 0% /sys/fs/cgroup
/dev/loop0 89M 89M 0 100% /snap/core/7270
/dev/sda2 976M 77M 833M 9% /boot
/dev/loop1 90M 90M 0 100% /snap/core/7713
tmpfs 394M 0 394M 0% /run/user/1000
```

Next confirm in Linux that there is actually a lot more space available. As you will see from the output below, there is `24G` on the `/dev/sda3` volume. The other 1GB is used in the boot volume and the `BIOS boot`

```
user@server:~# fdisk -l
Disk /dev/loop0: 88.5 MiB, 92778496 bytes, 181208 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
Disk /dev/loop1: 89 MiB, 93327360 bytes, 182280 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

...

Disk /dev/sda: 25 GiB, 26843545600 bytes, 52428800 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disklabel type: gpt
Disk identifier: ED41F7A6-5D09-457B-A55C-C7F1E30DE419

Device Start End Sectors Size Type
/dev/sda1 2048 4095 2048 1M BIOS boot
/dev/sda2 4096 2101247 2097152 1G Linux filesystem
/dev/sda3 2101248 52426751 50325504 24G Linux filesystem



Disk /dev/mapper/ubuntu--vg-ubuntu--lv: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
```

The one set of instructions referred to starting this process using `parted`, so parted log is below. The instructions as per Stack read something like:

“First you need to run parted and use its resizepart command to expand the partition to use the whole disk, then run pvresize to tell LVM about the new space, then run lvresize to grow the logical volume, and finally resize2fs on the logical volume to grow the filesystem to use the new space. This can be done without a reboot.”

Please note however I diverted slightly from these steps. The first command I learnt / used in parted, was just used to print the partition information:

```
user@server:~# parted
GNU Parted 3.2
Using /dev/sda
Welcome to GNU Parted! Type 'help' to view a list of commands.
```

```
(parted) print
Model: Msft Virtual Disk (scsi)
Disk /dev/sda: 26.8GB
Sector size (logical/physical): 512B/4096B
Partition Table: gpt
Disk Flags:

Number Start End Size File system Name Flags
1 1049kB 2097kB 1049kB bios_grub
2 2097kB 1076MB 1074MB ext4
3 1076MB 26.8GB 25.8GB

(parted) quit
```

This was followed by me checking and re-checking information using fdisk and df -h to make sure I was understanding the current situation.

Then I finally started the procedure:

```
user@server:~# parted
GNU Parted 3.2
Using /dev/sda
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) resizepart
Partition number? 3
End? [26.8GB]?
(parted) quit
Information: You may need to update /etc/fstab.
```

…

```
user@server:~# pvresize /dev/sda3
Physical volume "/dev/sda3" changed
1 physical volume(s) resized / 0 physical volume(s) not resized
```

At this point I tried using `lvresize` but couldn't get it to work. It appears there is both `lvresize` and `lvextend`. As per the "microhowto.info" article:

"The difference is that lvextend can only increase the size of a volume, whereas lvresize can increase or reduce it."

The first attempt at specifying 24GB did not work. After I completed the procedure I found that you can also specify a flag 100%, but unfortunately, I didn't get that information in time and just ended up specifying 23GB. If I have the time I might try and use the 100% flag. For reference, the flag is `lvextend -l +100%FREE /dev/VGNAME/LVNAME`

Below first attempt but insufficient space:

```
user@server:~# lvextend --size 24G /dev/mapper/ubuntu--vg-ubuntu--lv
Insufficient free space: 5120 extents needed, but only 5119 available
```

Second attempt reducing space to allocate:

```
user@server:~# lvextend --size 23G /dev/mapper/ubuntu--vg-ubuntu--lv
Size of logical volume ubuntu-vg/ubuntu-lv changed from 4.00 GiB (1024 extents) to 23.00 GiB
(5888 extents).
Logical volume ubuntu-vg/ubuntu-lv successfully resized.
```

After `lvextend`, one has to use `resize2fs`. This was kind of scary because it appeared I was going to work on a live disk, but it went quick.

```
user@server:~# resize2fs /dev/mapper/ubuntu--vg-ubuntu--lv
resize2fs 1.44.1 (24-Mar-2018)
Filesystem at /dev/mapper/ubuntu--vg-ubuntu--lv is mounted on /; on-line resizing required
old_desc_blocks = 1, new_desc_blocks = 3
The filesystem on /dev/mapper/ubuntu--vg-ubuntu--lv is now 6029312 (4k) blocks long.
```

TADA! The disk is now 23G big as seen by df-h output below:

```
user@server:~# df -h
Filesystem Size Used Avail Use% Mounted on
udev 1.9G 0 1.9G 0% /dev
tmpfs 394M 1.1M 393M 1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv 23G 3.2G 19G 15% /
tmpfs 2.0G 0 2.0G 0% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 2.0G 0 2.0G 0% /sys/fs/cgroup
/dev/loop0 89M 89M 0 100% /snap/core/7270
/dev/sda2 976M 77M 833M 9% /boot
/dev/loop1 90M 90M 0 100% /snap/core/7713
tmpfs 394M 0 394M 0% /run/user/1000
user@server:~#
```

В Centos 7 файловая система по умолчанию- **xfs** .

поддержка файловой системы xfs только расширяется, а не уменьшается. Поэтому, если вы хотите изменить размер файловой системы, используйте xfs_growfs, а не resize2fs.

```
xfs_growfs /dev/root_vg/root
```

Примечание: Для использования файловой системы ext4

```
resize2fs /dev/root_vg/root
```

How to expand /dev/mapper/cl-root (/dev/mapper/centos-root)

Step-by-step instructions
When adding a Code Sample, please choose the 'Normal (DIV)' formatting, in order to avoid text glitch over the page borders
---You MUST be root to perform the below steps---

1. Check the current disk status to ensure dev/mapper/cl-root /dev/mapper/centos-root) is exactly 50G and /dev/mapper/cl-home (/dev/mapper/centos-home) is much larger in size.
df -h

Example:

```
[root@ptaserver /]# df -h
Filesystem           Size  Used Avail Use% Mounted on
devtmpfs             7.8G     0  7.8G   0% /dev
tmpfs                7.8G     0  7.8G   0% /dev/shm
tmpfs                7.8G  802M  7.0G  11% /run
tmpfs                7.8G     0  7.8G   0% /sys/fs/cgroup
/dev/mapper/cl-root   50G   11G   40G  22% /
/dev/sda1           1014M  265M  750M  27% /boot
/dev/mapper/cl-home  441G   33M  441G   1% /home
tmpfs                1.6G     0  1.6G   0% /run/user/1001
tmpfs                1.6G     0  1.6G   0% /run/user/1007
tmpfs                1.6G     0  1.6G   0% /run/user/1003
tmpfs                1.6G     0  1.6G   0% /run/user/1005
tmpfs                1.6G     0  1.6G   0% /run/user/1006
tmpfs                1.6G     0  1.6G   0% /run/user/1008
tmpfs                1.6G     0  1.6G   0% /run/user/0
```

2. Stop PTA
service appmgr stop

3. Copy everything from the home directory out
cp -a /home /home2

4. Unmount the volume
umount /dev/mapper/cl-home (umount /dev/mapper/centos-home)

5. Delete the home logical volume
lvremove /dev/mapper/cl-home (lvremove /dev/mapper/centos-home)

Example:

```
[root@ptaserver /]# lvremove /dev/mapper/cl-home
Do you really want to remove active logical volume cl/home? [y/n]: y
  Logical volume "home" successfully removed
```

6. Extend the root logical volume to take up the rest of the space
lvextend -l +100%FREE /dev/mapper/cl-root (lvextend -l +100%FREE /dev/mapper/centos-root)

Example:

```
[root@ptaserver /]# lvextend -l +100%FREE /dev/mapper/cl-root
  Size of logical volume cl/root changed from 50.00 GiB (12800 extents) to 481.12 GiB (123167 ex
  Logical volume cl/root successfully resized.
```

7. Extend the xfs partition
xfs_growfs /dev/mapper/cl-root (xfs_growfs /dev/mapper/centos-root)

Example:

```
[root@ptaserver /]# xfs_growfs /dev/mapper/cl-root
meta-data=/dev/mapper/cl-root    isize=512    agcount=4, agsize=3276800 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=0 spinodes=0
data     =                       bsize=4096   blocks=13107200, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal               bsize=4096   blocks=6400, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
data blocks changed from 13107200 to 128744448
```

8. Check that /dev/mapper/cl-root (/dev/mapper/centos-root) has been increased in size and that /dev/mapper/cl-home (/dev/mapper/centos-home) has been removed
df -h

Example:

```
[root@ptaserver /]# df -h
Filesystem           Size  Used Avail Use% Mounted on
devtmpfs             7.8G     0  7.8G   0% /dev
tmpfs                7.8G     0  7.8G   0% /dev/shm
tmpfs                7.8G  810M  7.0G  11% /run
tmpfs                7.8G     0  7.8G   0% /sys/fs/cgroup
/dev/mapper/cl-root  492G   11G  481G   3% /
/dev/sda1           1014M  265M  750M  27% /boot
tmpfs                1.6G     0  1.6G   0% /run/user/1001
tmpfs                1.6G     0  1.6G   0% /run/user/0
tmpfs                1.6G     0  1.6G   0% /run/user/1007
tmpfs                1.6G     0  1.6G   0% /run/user/1003
tmpfs                1.6G     0  1.6G   0% /run/user/1005
tmpfs                1.6G     0  1.6G   0% /run/user/1006
tmpfs                1.6G     0  1.6G   0% /run/user/1008
```

9. Move the home directory data back and remove the temporary home2 directory
mv /home2/ /home/*
rmdir /home2

10. Remove the /dev/mapper/cl-home (lvremove /dev/mapper/centos-home) entry from /etc/fstab
vi /etc/fstab
DELETE the line:

```
/dev/mapper/cl-home     /home                   xfs     defaults        0 0
```

11. Start PTA
service appmgr start

12. Run Diagnostics to ensure PTA is functioning again:
RUN_DIAGNOSTICS

PostgreSQL

PostgreSQL

How to create read only user in PostgreSQL

```
-- Create a group
CREATE ROLE readaccess;

-- Grant access to existing tables
GRANT USAGE ON SCHEMA public TO readaccess;
GRANT SELECT ON ALL TABLES IN SCHEMA public TO readaccess;

-- Grant access to future tables
ALTER DEFAULT PRIVILEGES IN SCHEMA public GRANT SELECT ON TABLES TO readaccess;

-- Create a final user with password
CREATE USER tomek WITH PASSWORD 'secret';
GRANT readaccess TO tomek;
```

NGINX

NGINX

Nginx – обратный прокси для Docker контейнеров

Nginx – обратный прокси для Docker контейнеров

bac06197-32f2-4031-82c3-5c7b11bcb2c9.png
bac06197-32f2-4031-82c3-5c7b11bcb2c9.png
Nginx – обратный прокси для Docker контейнеров

- Введение
- Установка Nginx
- Пример обратного прокси для Docker контейнера
- Выпуск SSL сертификата с помощью Certbot
- Вывод

Введение

В данной небольшой заметке разберем на примере, как с помощью Nginx сделать обратный прокси для ваших Docker контейнеров, Nginx будем использовать без Docker, разберем как настроить Nginx и как получить SSL сертификат для нашего сервиса бесплатно, с помощью Certbot и Lets Encrypt

Так же, ни кто не запрещает пользоваться такой вещью как Nginx Proxy Manager, Traefik и другими способами для получения результата.

В данной заметке разберем это на примере, у нас есть контейнер с Memos в Docker, работает на **5230 порту**, мы хотим что бы он у нас открывался по нашему доменному имени memos.site.ru и использовал https соединение, а не по ip адресу с портом
Мы не хотим пробрасывать кучу портов на роутере, если мы находимся за natom, а открыть только 80 и 443 порты.

Установка Nginx

Если Nginx у вас еще не установлен, то установка на Debian/Ubuntu производится данной командой:

```
apt install nginx
```

Проверим статус Nginx:

```
systemctl status nginx
```

> 2023-11-01-12_46_32-vdsina-outline.jpg2023-11-01-12_46_32-vdsina-outline.jpg
> systemctl status nginx

Если все хорошо, продолжаем разбираться дальше, добавим конфиг в Nginx для нашего сервиса

Пример обратного прокси для Docker контейнера

Создаем конфиг, в данном случае для Memos: (далее по примеру замените **site.ru** на свое доменное имя):

```
nano /etc/nginx/sites-available/memos.site.ru
```

Добавляем туда содержимое ниже, вам нужно заменить директиву **server_name memos.site.ru;** на свое доменное имя, а в **proxy_pass http://localhost:5230;** указать свой

порт сервиса:

```
server {
    listen 80;
    server_name memos.site.ru;

    location / {
        proxy_pass http://localhost:5230;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}
```

```
ln -s /etc/nginx/sites-available/memos.site.ru /etc/nginx/sites-enabled/
```

Перезагружаем Nginx и проверяем в браузере доступность по доменному имени **http** ://memos.site.ru:

```
systemctl restart nginx
```

Если все открывается, идем далее и получаем SSL сертификат

Выпуск SSL сертификата с помощью Certbot

Установим Certbot для выпуска SSL сертификата на наше доменное имя:

```
apt install certbot python3-certbot-nginx
```

И выпустим сам SSL сертификат данной командой (замените данные на свои):

```
certbot --non-interactive -m admin@site.ru --agree-tos --no-eff-email --nginx -d memos.site.ru
```

```
systemctl restart nginx
```

Если все прошло успешно, то Certbot сам добавит редирект с 80 на 443 порт и данные по сертификату в конфиг который мы создали до этого **/etc/nginx/sites-available/memos.site.ru**, заходим в браузер и проверяем теперь **https**://memos.site.ru

tmp

SCCM Развертка [25IT — Инструкции, решения ошибок и IT-гайды для пользователей и администраторов.]

AAAB3Q0ODAoPeNqVUk1vm0AUvO+vQOolPeDuguvakZBKYO3QGOwAsZIqlw15NutiQLtA6/z68GHLb
h1bqsRlZ9mZN/PmUxiXisuEQkYKHl7XX58olh0qGtYGyBLACp6lNivAaBAV66qG0ZRHkEoltzl4b
AOGNXNd6luOOUVrLlhvd09fefPaoF5I/bnvBBR55eYFxGz5IEFIQyV7Kvon52J7pNNXyagjy0X2W
kZFrzmoMlsWv5mAHosKXoFRiBJQUL7ISPC8FWsRWrGkZIdzS1SzMwvSAkQHJp30LZOx4VrYGlvDt
0fnqcpuF/FkJcELF+5gktDI/zIx4weTbx7XMzwfJ87Nk7YO5vLrGtg2ersr75+NvRHHNqaOHVBPn
Wqkr9dehpdsBAUTzUBLlsjaCIgKRE1xY/40VR0TTyXje1e1nf4C/YLtog6t8UQGGH/DQ10naCUA0
jjLcxAXYp+XIoqZhH8Xefy6TSYXXO5TpZ7xt48PtD6qgA2HbfxwfFMJdm6Vq2YFSreDz8/XymFNy
GW8RlOWRv/fhZNSHQ96XJQLHGfKsU9cQzOxYimXXakykWRVzipIRoR8X20YT3pRtkFWlha1IK3dJ
Gd/aqc4mblFT4a9EPNOq4XPSb0D2sxUMzAtAhQc1496m4ldwUUK+quhGkbo0f3cLAIVAIEN27ieR
NtA1zkiJMOLNvonRQq1X02mm

jira software

AAAB3g0ODAoPeNqNU9FumzAUfecrkPbSPoBsyLoQCWkZUDVVSLaQZdqUl1tyCU7AIBuz8vczybJEn
dL20dfn3nvO8fGHZa7MGIRJPZMMR8Qb0YEZhEvTIc6dEQiEhlU8hAb9vmIR13KIMWUpconLrsYZl
OgH8ziOFsFkPDVmqnxCMc++SxTSt+gJGz3XTHQXgwYW9YxEPclUsLpf4jdCoZFWpQ1NAVIy4LYe0
ur+Dcq9/crSqIVCwXnIjgmw9S4IkDcojsXi2P8AMvfj4HdwHz0vWfIxclwsH7JMpYMfwdQlqxw27
ThfRD+X2Y4p5eWPknbzjrQrmI13Qzfcrv21f9I1Cf3pJEyimTV16MDV0rxXNHBVLqoCg0rxpjfnQ
LQW1Ualjd0frEs0pA1r8ULSVeR/rif6EoUm92X8a2y5hM4sev8ttsLJYGXssVtpXG8XvSPkExm6L
jW+KpHmIPHlY19XczC3Fky+i+PL99Ce+e/17dKJEM+RedRLzOQI1DHmsMVSrzBvskqUKIru36Xu2
t+aNz0J88jidj0yz8ExYmC6yoGnV7L6Nz8n55w35CYNiF5rBoVEYy62wJk8ZrQSRdXW0GLhUfp5W
wIrbK3dCCreaKWRplK8BTp8gWuYP6o1VDswLAIUWdd3uQbOQZqc3psl0CPLWnzyN2oCFApfl5gVx
rlwwEJcl80a9QaDOcY5X02mm

service management

https://github.com/haxqer/confluence/releases

https://github.com/haxqer/confluence/releases/tag/v1.2.2

https://github.com/guywiththecrack/jira-crack/tree/master

entrypoint-jira.sh

```
#!/bin/bash

# Копируем агент в нужную директорию
cp /var/atlassian/atlassian-agent.jar /opt/atlassian/jira/atlassian-agent.jar

# Добавляем javaagent в setenv.sh
set -e

LINE='export JAVA_OPTS="-javaagent:/opt/atlassian/atlassian-agent/atlassian-agent.jar
${JAVA_OPTS}"'

for FILE in /opt/atlassian/jira/bin/setenv.sh /opt/atlassian/jira/bin/setenv32.sh; do
  if [ -f "$FILE" ]; then
    # Проверяем, есть ли уже строка
    if ! grep -q "atlassian-agent.jar" "$FILE"; then
      echo "Patching $FILE"
      sed -i "1i$LINE" "$FILE"
    else
      echo "Already patched: $FILE"
    fi
  fi
done

# Запускаем оригинальный старт-скрипт Jira
exec /opt/atlassian/jira/bin/start-jira.sh -fg
```